NETASQ

NETASQ UNIFIED MANAGER

NETASQ UNIFIED MANAGER

V. 8.0

MANUEL D'UTILISATION ET DE CONFIGURATION

Date	Révision	Auteur	Objet
Novembre 2008	V1.0	Valérie Tourrel	Mise à jour suite à la sortie de la version logicielle 8.0
Janvier 2009	V1.1	Valérie Tourrel	Mise en conformité Critère Communs

Référence : FRUG0109-V1.1_NUMANAGER-V8.0

Produits concernés

U30, U70, U120, U250, U450, U1100, U1500 et U6000

SOMMAIRE

AVANT-PROPOS

Copyright

Responsabilités

Ce manuel a fait l'objet de plusieurs relectures et révisions afin d'assurer l'exactitude des informations qui y sont contenues. Les descriptions et procédures qu'il comporte sont correctes pour les firewalls NETASQ. NETASQ n'accepte aucune responsabilité pour des dommages liés directement ou indirectement à des erreurs, des omissions ou des incohérences entre le produit et le manuel.

Avertissements

Directive DEEE

Tous les produits NETASQ soumis à la directive DEEE qui ont été livrés dans l'Union Européenne après le 13 août 2005 sont signalés par le pictogramme représentant une poubelle sur roues barrée d'une croix. Ce marquage stipule que le produit répond aux exigences imposées par la directive DEEE en termes de destruction et de réutilisation des DEEE.

Pour plus de détails, veuillez consulter le site NETASQ à l'adresse suivante http://www.netasq.com/recycling.html

Acceptation des termes de la licence

Présentation

Les informations contenues dans ce document sont susceptibles d'être modifiées sans préavis. Malgré tout le soin apporté à sa vérification, ce document peut comporter certaines erreurs. Dans ce cas, n'hésitez pas à prendre contact avec la société NETASQ.

La société NETASQ dégage par ailleurs toute responsabilité quant aux erreurs qui peuvent exister dans ce document et aux dommages qui pourraient en résulter.

Acceptation

En ouvrant l'emballage du produit ou en installant le logiciel d'administration, vous acceptez et serez lié aux termes et restrictions de cette licence.

Licence

NETASQ, par la présente licence et si vous en acceptez les termes, concède le droit d'usage non exclusif et non transférable du code programme du produit. Vous n'avez pas l'autorisation de copier tout ou partie du programme ou de la notice associés au produit. Vous acceptez que le code source du produit, le concept et les idées liées au produit restent valablement la propriété intellectuelle de NETASQ. Vous acceptez de ne pas copier, désassembler, décompiler, ou dériver tout ou partie du produit, ou de développer un autre produit reprenant le concept ou les idées contenus dans ce produit. Toute violation de cette obligation engagerait votre responsabilité et vous rendrait redevable de dommages-intérêts au bénéfice de NETASQ.

Limite de garanties et de responsabilités

a - Matériel

NETASQ garantit les produits matériels des défauts de pièces et main d'œuvre pour une période d'un an, sauf indication contraire au tarif valide à la date de commande du client. Cette période commence à la date d'activation du produit.

b - Logiciel

Les produits logiciels NETASQ, ci-après désignés "les logiciels", sont garantis pour une période de 90 jours (sauf mention particulière précisée à l'achat) à compter de la date d'activation du produit contre les défauts et les dysfonctionnements substantiels par rapport au manuel tel qu'il existe à la date de livraison et sous les environnements et leur version supportés par le produit.

NETASQ ne garantit pas le logiciel ou le produit pour des usages sous d'autres environnements logiciels et réseaux que ceux préconisés spécifiquement.

c - Défaut

En cas de défaut, la responsabilité de NETASQ et le seul recours du client consistent, sur décision de NETASQ, soit au remboursement des sommes reçues au titre de la vente du produit annulant ainsi la présente Licence d'utilisation, soit à la réparation ou le remplacement du produit ou support.

d - Garantie

A l'exception de la garantie limitée telle que décrite dans les paragraphes précédents, ce produit est fourni " tel quel " sans autre garantie de quelque sorte, implicite ou explicite. NETASQ ne garantit pas que le produit corresponde à votre besoin ou que son utilisation puisse être ininterrompue et exempte d'erreurs. NETASQ rejette toute garantie ou obligation commerciale considérée par le client comme implicite, ne peut garantir que le produit convient à tous les cas particuliers ni ne prend de responsabilités en cas d'usage frauduleux ou illégal.

e - Recommandations

En aucun cas NETASQ ne pourra être tenue pour responsable des dommages subis par vous ou tout autre tiers, en dehors de ceux explicitement mentionnés dans cet agrément, qu'ils soient directement ou indirectement liés à l'usage du produit, y compris d'éventuelles pertes d'exploitation dues à une interruption de service ou tout autre cause, même si NETASQ a été avisée de la possibilité de tels dommages. La responsabilité maximale de NETASQ en cas de dommages se limite au montant reçu par NETASQ pour l'achat du produit en particulier qui a pu causer ces dommages.

Tout litige éventuel relatif à la défectuosité alléguée du logiciel considéré devra être obligatoirement soumis à la compétence des juridictions du siège de NETASQ, le droit français étant seul applicable.

AVERTISSEMENTS

1) Certains produits de NETASQ permettent de récupérer et d'analyser des traces. Ces informations permettent un contrôle de l'activité des utilisateurs internes et peuvent fournir des informations nominatives. La législation en vigueur, dans le pays destinataire peut imposer d'appliquer certaines mesures (telles que notamment des déclarations administratives lorsque des personnes sont soumises à un tel contrôle. Assurez-vous que ces éventuelles mesures ont bien été mises en application avant toute utilisation du produit.
2) Certains produits de NETASQ fournissent des mécanismes de chiffrement de données dont l'usage peut être interdit ou limité par la législation en vigueur dans le pays destinataire. Malgré le contrôle réalisé par NETASQ à l'exportation, assurez-vous que vous êtes dans la légalité pour utiliser pleinement ou partiellement les produits NETASQ.
3) NETASQ dégage toute responsabilité quant à l'utilisation du présent produit dans un cadre sortant de la légalité pour le pays de destination.

Hypothèses issues de critères communs

DEFINITION

Les critères communs évaluent (sur une échelle "EAL" de 1 à 7) les capacités d'un produit à fournir les fonctions de sécurité pour lesquelles il a été conçu, ainsi que la qualité de son cycle de vie (développement, production, livraison, mise en service, mise à jour). Ils sont une convergence des différentes normes de qualité (en matière de sécurité) imaginées depuis 1980 :

Orange Book – DoD

CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)

ITSEC (Information Technology Security Evaluation Criteria)

TCSEC (Trusted Computer System Evaluation Criteria).

Présentation

L'installation d'un firewall s'inscrit bien souvent dans la mise en place d'une politique de sécurité globale. Pour garantir une protection optimale de vos biens, ressources ou informations, il ne s'agit pas seulement d'installer le firewall entre votre réseau et l'Internet. Notamment parce que la plupart des attaques viennent de l'intérieur (accident, personne mécontente de son travail, personne licenciée ayant gardé un accès interne…). Mais aussi parce que l'on conviendra qu'il ne sert à rien d'installer une porte blindée si les murs sont en papier.

Sous l'impulsion des critères communs, NETASQ vous propose donc de prendre en compte les hypothèses d'utilisation de la suite d'administration et du produit firewall énoncées ci-dessous. Ces hypothèses vous exposent les exigences d'utilisation à respecter pour garantir le fonctionnement de votre firewall dans le cadre de la certification aux critères communs.

Hypothèses sur les mesures de sécurité physiques

Les produits UTM NETASQ sont installés et stockés conformément à l'état de l'art concernant les dispositifs de sécurité sensibles : local à accès protégé, câbles blindés en paire torsadée, étiquetage des câbles, etc.

Hypothèses sur les mesures de sécurité organisationnelles

Un rôle administrateur particulier, le super-administrateur, présente les caractéristiques suivantes :

- Il est le seul à être habilité à se connecter via la console locale sur les boîtiers UTM NETASQ, et ce uniquement lors de l'installation du firewall ou pour des opérations de maintenance, en dehors de l'exploitation.
- Il est chargé de la définition des profils des autres administrateurs.
- Tous les accès dans les locaux où sont stockés les boîtiers firewalls se font sous sa surveillance, que l'accès soit motivé par des interventions sur l'Appliance ou sur d'autres équipements. Toutes les interventions sur les boîtiers firewall se font sous sa responsabilité.

Les mots de passe des utilisateurs et des administrateurs doivent être choisis de façon à retarder toutes les attaques visant à les casser, via une politique de création et/ou de contrôle de ceux-ci

> **Exemple**
> Mélange alphanumérique, longueur minimum, ajout de caractères spéciaux, pas de mots des dictionnaires usuels, etc.).

Il est de la responsabilité des administrateurs de sensibiliser tous les utilisateurs à ces bonnes pratiques (*Cf. Partie 13 : PKI, chapitre 6 Sensibilisation des utilisateurs*).

La politique de contrôle des flux d'informations à mettre en œuvre est définie, pour tous les équipements des réseaux dits "Trusted" à protéger, de manière :

- **Complète** : les cas d'utilisation standards des équipements ont tous été envisagés lors de la définition des règles et leurs limites autorisées ont été définies.
- **Stricte** : seuls les cas d'utilisation nécessaires des équipements sont autorisés.
- **Correcte** : les règles ne présentent pas de contradiction.
- **Non-ambigüe** : l'énoncé des règles fournit tous les éléments pertinents pour un paramétrage direct de l'Appliance par un administrateur compétent.

Hypothèses relatives aux agents humains

Les administrateurs sont des personnes non hostiles et compétentes, disposant des moyens nécessaires à l'accomplissement de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité. Notamment, leur compétence et leur organisation implique que :

- Différents administrateurs avec les mêmes droits ne mènent des actions d'administration qui se contredisent

> **Exemple**
> Modifications incohérentes de politique de contrôle des flux d'information.

- L'exploitation des journaux et le traitement des alarmes sont effectués dans les délais appropriés.

Hypothèses sur l'environnement de sécurité TI

Les boîtiers UTM NETASQ sont installés conformément à la politique d'interconnexion des réseaux en vigueur et sont les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle des flux d'information. Les périphériques de connexion (modem) sont interdits sur les réseaux dits "Trusted".

A part l'application des fonctions de sécurité, les boîtiers UTM NETASQ ne fournissent pas de service réseau autre que le routage et la translation d'adresse.

> **Exemple**
> Pas de DHCP, DNS, PKI, proxies applicatifs, etc.*

Les boîtiers NETASQ ne sont pas configurés pour retransmettre les flux "IPX", "NetBIOS", "Appletalk", "PPPoe" ou "IPv6".

Les boîtiers UTM NETASQ ne dépendent pas de services externes « en ligne » ("DNS", "DHCP", "RADIUS", etc.)* pour l'application de la politique de contrôle des flux d'information.

Protection des stations : les stations d'administration à distance sont sécurisées et maintenues à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées. Elles sont exclusivement dédiées à l'administration des firewalls.

Les équipements réseau avec lesquels le firewall établit des tunnels VPN sont soumis à des contraintes de contrôle d'accès physique, de protection et de maîtrise de leur configuration équivalentes à celles des boîtiers firewall-VPN.

Protection des clients : les postes sur lesquels s'exécutent les clients VPN des utilisateurs autorisés sont soumis à des contraintes de contrôle d'accès physique, de protection et de maîtrise de leur configuration équivalentes à celles des postes clients des réseau de confiance. Ils sont sécurisés et maintenus à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées

* Ces services sont disponibles sur un firewall mais ne font pas partie du cadre d'évaluation des critères communs.

PARTIE 1 : INTRODUCTION

CHAPITRE 1. A QUI S'ADRESSE CE MANUEL D'UTILISATION ?

Ce manuel s'adresse à un administrateur réseau ou à un utilisateur possédant un minimum de connaissances sur IP.
Pour configurer efficacement votre produit UTM NETASQ, vous devez connaître le fonctionnement de ces protocoles et leurs particularités :

- ICMP (*Internet Control Message Protocol*)
- IP (*Internet Protocol*)
- TCP (*Transmission Control Protocol*)
- UDP (*User Datagram Protocol*)

La connaissance du fonctionnement général des principaux services TCP/IP est appréciable :

- HTTP
- FTP
- Messagerie (SMTP, POP3, IMAP)
- Telnet
- DNS
- DHCP
- SNMP
- NTP

Si vous ne possédez pas ces connaissances, ne vous inquiétez pas : l'acquisition d'un ouvrage généraliste sur TCP/IP vous les apportera.

Meilleure est votre connaissance de TCP/IP, meilleures seront vos règles de filtrages et meilleure sera votre sécurité IP.

CHAPITRE 2. CONVENTIONS TYPOGRAPHIQUES

1.2.1. Abréviations

Pour la clarté, les abréviations usuelles ont été conservées. Par exemple, **VPN** (*Virtual Private Network/Réseau Privé Virtuel*). Les acronymes sont définis dans le Glossaire.

1.2.2. Affichage

Les noms de fenêtres, les menus et sous menus et les boutons de l'application sont représentés en utilisant la police ci-dessous :

Exemple
Menu **`Interfaces`**

1.2.3. Indications

Les indications présentés dans ce manuel fournissent des informations importantes et sont destinés à attirer votre attention sur un point important. Les différentes indications que vous pourrez trouver sont :

NOTE/REMARQUE
Ces messages vous donnent une explication plus détaillée sur un point particulier.

AVERTISSEMENT
Ces messages vous mettent en garde contre une manipulation ou une utilisation incorrecte de votre produit.

ASTUCE
Ce message vous fournit des procédés ingénieux pour utiliser les options de votre produit.

DEFINITION
Description de termes techniques liés à NETASQ ou langage réseau. Ces termes seront repris dans le glossaire.

1.2.4. Messages

Les messages au sein de l'application sont indiqués entre ""

Exemple
"Voulez-vous vraiment supprimer cette entrée ?"

1.2.5. Exemples

Exemple
Cette présentation vous permet d'avoir un exemple de ce qui a été expliqué au préalable.

1.2.6. Lignes de commandes

Lignes de commandes
`Indication de lignes de commandes (par exemple, une saisie dans la fenêtre de commandes dos.`

1.2.7. Rappels

Les rappels sont indiqués de la manière suivante :

- Texte de rappel.

1.2.8. Accès

Les accès à une fonction sont indiqués de la manière suivante :

- Accédez au menu **`Fichier\Firewall.`**

CHAPITRE 3. VOCABULAIRE UTILISE DANS LE MANUEL

Appliance	Ce terme désigne le boîtier de sécurité ou (boîtier pare-feu). Les termes Appliance et boîtier de sécurité sont indifféremment utilisés.
Dialup	Interface sur laquelle est branché le modem.
UTM Fxx	Désigne la gamme des produits NETASQ. Les termes également utilisés sont NETASQ Fxx, boîtier Fxx.
Firewall	Equipement/produit UTM NETASQ.
Prévention d'intrusion	Le terme UTM peut être également mentionné.
Slot (de configuration)	(*Ou Politique*.). Mais slot ou politique (de filtrage, de NAT…) sont utilisés.
Machine	Terme utilisé aussi bien pour les machines que pour les utilisateurs.
Traces/Logs	Indifféremment utilisés.

CHAPITRE 4. OBTENIR DE L'AIDE

Pour obtenir de l'aide aux sujet de votre produit et des différentes applications qui le composent :

- Site web : www.netasq.com. Votre espace privé vous permet d'accéder à un certain nombre de documentations et d'informations diverses.
- Manuels de l'utilisateur : NETASQ UNIFIED MANAGER, NETASQ REAL-TIME et NETASQ EVENT REPORTER.

CHAPITRE 5. GENERALITES

1.5.1. Introduction

Merci d'avoir choisi un produit NETASQ. Destinés à sécuriser des structures de toutes tailles, les firewalls de la gamme NETASQ sont des boîtiers pré-configurés : pas d'installation matérielle, ni d'installation logicielle, pas de compétences Unix nécessaires mais une configuration conviviale au moyen d'une interface graphique.

Le firewall NETASQ permet de définir les règles de contrôle d'accès entrant ou sortant. Son concept est simple : toute transmission entrante ou sortante transitant par le firewall est contrôlée, autorisée ou refusée suivant les règles, paquet par paquet.

Le firewall NETASQ est basé sur un mécanisme de filtrage de paquets évolué qui procure un haut niveau de sécurité. Tous les firewalls intègrent la technologie ASQ (*Active Security Qualification*), développée par NETASQ. Cette technologie permet la détection et le blocage, en temps réel, d'attaques informatiques : paquets illégaux, tentatives de déni de service, anomalies dans une connexion, scans de ports, buffer overflow...

En cas de tentative d'intrusion, selon les consignes spécifiées dans la politique de sécurité, le firewall bloque la transmission, génère une alarme et mémorise les informations liées au paquet ayant provoqué l'alarme. Ainsi, il vous est possible d'analyser l'attaque et de rechercher son origine.

Le firewall permet non seulement d'empêcher, ou de limiter à certains services, les connexions entrantes sur votre réseau mais aussi de contrôler l'utilisation de l'Internet faite par vos utilisateurs internes (HTTP, FTP, SMTP...). Le contrôle des utilisateurs peut aussi être réalisé au moyen d'une authentification via une base d'authentification interne ou externe.

Le firewall NETASQ gère également les mécanismes de translations d'adresses et de ports. Ces mécanismes apportent sécurité (en masquant votre adressage interne), flexibilité (en permettant d'utiliser un plan d'adressage interne privé quelconque) et réduction de coût (en permettant la mise à disposition de plusieurs serveurs sur Internet avec une seule adresse IP publique).

Avec l'ASQ, le moteur IPS (*Intrusion Prevention System*) de NETASQ, un firewall NETASQ offre d'autant plus de sécurité. Son architecture à plug-in permet de contrôler la majeure partie du trafic circulant au travers du firewall même au niveau applicatif. Ses performances en matière de débit, de nombres de règles, de tunnels, sont décuplées.

Grâce à son interface utilisateur sous Windows, il offre la possibilité de définir rapidement et simplement les règles de sécurité pour votre réseau, à partir d'un poste local sous Windows. Vous pouvez aussi monitorer, en temps réel, l'activité de votre firewall.

Le firewall NETASQ est également doté de fonctions avancées de traçabilité. En cas de tentative d'intrusion, l'administrateur du réseau peut accéder à l'ensemble des données envoyées avant l'attaque et voir comment elle est préparée. NETASQ EVENT REPORTER vous apportera une vision graphique et une analyse fine des logs générés sur le firewall.

Enfin, le firewall NETASQ intègre les fonctionnalités de passerelle VPN vous permettant d'établir des tunnels chiffrés avec d'autres équipements VPN. Ainsi, vos communications inter-sites ou avec vos utilisateurs nomades ("Road Warriors") peuvent être sécurisées même en utilisant une infrastructure de communication non sûre comme l'est Internet.

1.5.2. Précautions d'utilisation

AVERTISSEMENT
L'utilisation de piles LITHIUM de mauvais type peut entraîner l'explosion des composants. Veuillez suivre les spécifications du constructeur de piles LITHIUM (utilisées dans votre firewall) pour le recyclage des piles usagées.

AVERTISSEMENT
Le firewall doit être installé conformément à l'état de l'art correspondant aux modalités pratiques d'installation sécurisée à savoir : dans un local ou bureau à accès protégé. Pour garantir l'intégrité du produit et la non compromission de la sécurité de votre installation, tous les accès (au firewall) non autorisés doivent être évités.

AVERTISSEMENT
Veillez à placer les équipements lourds dans la partie basse de l'armoire ou du rack et les éléments plus légers dans la partie haute.

AVERTISSEMENT
La plupart des boîtiers NETASQ nécessitent une connexion à la terre. Assurez-vous que votre installation secteur dispose d'une terre de bonne qualité, correspondant aux spécifications NETASQ concernant l'alimentation des firewalls. De plus il est préférable de protéger l'alimentation par des équipements de type UPS.

AVERTISSEMENT
Les boîtiers NETASQ ne sont pas pourvus d'interrupteur secteur. Dans tous les cas, débrancher le cordon secteur de l'embase secteur permet de déconnecter le boîtier du secteur.

AVERTISSEMENT
Les firewalls NETASQ ne doivent pas être installés dans un environnement où la température peut excéder les 35°C.

AVERTISSEMENT
Assurez-vous que rien n'obstrue les ouies de ventilation du produit afin de garantir une circulation de l'air optimale.

AVERTISSEMENT
Les poignées métalliques présentes sur la face avant du produit U6000 ne doivent pas être utilisées pour porter celui-ci mais uniquement pour placer ou sortir le firewall dans le rack.

1.5.3. Dès réception de votre firewall

1.5.3.1. Intégrité du produit

Afin de garantir l'intégrité de votre produit, NETASQ a mis en place plusieurs mécanismes. Vérifiez ces mécanismes pour valider que votre produit n'a pas été manipulé frauduleusement :

- **Les étiquettes** : chaque firewall est livré dans un carton sur lequel sont apposées trois étiquettes contenant des informations d'identification du produit contenu et de sa version. De plus une étiquette « Numéro de série » est apposée directement sur le produit. La 3ème étiquette sert à identifier la configuration du produit. Vérifiez que ces informations concordent avec votre commande.

Les 3 étiquettes sont les suivantes :

Etiquette numéro de série : cette étiquette, collée sur le produit permet d'obtenir des informations au sujet du numéro de série, de la plate-forme commerciale, du code d'activation Web (code qui permet l'activation du compte client dans l'espace client du site Web NETASQ) et le code barre contenant le numéro de série du produit.

Figure 1: Etiquette numéro de série

Etiquette d'identification d'emballage : cette étiquette, collée sur l'emballage du produit donne des informations relatives à la plate-forme commerciale, au numéro de série du produit, au code barre contenant le numéro de série du produit.

Figure 2 : Etiquette d'identification d'emballage

Etiquette numéro de version : cette étiquette, collée sur l'emballage, donne des informations concernant la version logicielle installée sur le firewall. La version est définie par un numéro et un modèle de version (correspondant à une zone d'exportation). Cette étiquette permettra ensuite de vérifier si la version livrée est bien certifiée.

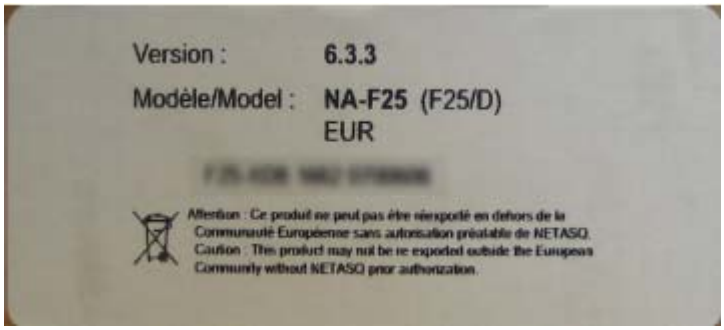


Figure 3: Etiquette de version du produit

- **Le scellé du carton** : chaque firewall est livré dans un carton sur lequel est apposée une bande de garantie spécifique à NETASQ. Vérifier la présence de cette bande de garantie sur le carton de votre produit.
Sauf pour le U6000, une étiquette de type « NETASQ QUALITY SEAL » est apposée.

Figure 4 : Etiquette "Quality seal"

Pour le U6000, l'étiquette suivante est apposée :

Figure 5 : Bande de garantie

Si cette bande est absente, contactez votre revendeur au plus vite pour connaître les raisons de l'ouverture du carton.

- **Le scellé du firewall** : une étiquette de scellé est apposée sur tous les firewalls. Il est alors impossible de remplacer ou de modifier un des éléments matériels du firewall. Cette étiquette a la particularité d'afficher un message (VOID) qui ne peut plus être effacé lorsqu'elle est décollée. Il existe deux types de scellée : une apposée par NETASQ en sortie de production et une apposée par votre partenaire si une opération de maintenance doit être réalisée sur votre produit (cette opération de maintenance doit vous être expliquée par votre partenaire par l'intermédiaire d'un certificat d'activité).

Figure 6 : scellé du firewall

Valider ces mécanismes de sécurité vous assure de l'intégrité du produit reçu. N'hésitez pas à contacter votre revendeur si un de ces éléments n'était pas conforme à leur description.

1.5.3.2. Contenu du packaging

Conservez précieusement le carton d'emballage, dans l'éventualité d'un transport. Il a été conçu pour assurer une protection optimale de votre firewall NETASQ (résistance aux chocs, aux températures...).

A la livraison, vérifiez que dans l'emballage se trouvent bien :

- Le firewall NETASQ du modèle commandé

- Un cordon secteur (réf. 1076036)
- Un câble série croisé DB9F (réf. 1076033)
- Un câble croisé RJ 45 (câble bleu, réf. 1076034)
- Une enveloppe contenant le CD-ROM de la suite logicielle NETASQ (Administration Suite)
- Une feuille contenant les remerciements et les accords de licence.
- Les équerres et système de fixation pour mise en rack
- Le bloc d'alimentation pour les boîtiers U30 et U70.

Si un élément est manquant, n'hésitez pas à contacter votre revendeur.

1.5.4. Présentation des boîtiers

Pour plus d'informations au sujet de la connectique liée aux boîtiers de la série U, veuillez vous référer à la note technique Connectique et cartes : série U (*FRTN0811_CONNECTIQUE-CARTES-U-SERIE*).

1.5.5. Ouverture du boîtier

AVERTISSEMENT
En aucun cas vous ne devez ouvrir le boîtier NETASQ.

AVERTISSEMENT
Seule la société NETASQ et ses agents de maintenance agréés sont habilités à le faire.

AVERTISSEMENT
Toute ouverture du boîtier du firewall NETASQ par vos soins entraîne l'annulation de la garantie.

1.5.6. Les châssis

Des pieds en matériau souple sont disposés sous le chassis, assurant au firewall NETASQ une très bonne stabilité (sur un bureau ou sur un autre équipement informatique).
Ces pieds peuvent être livrés installées ou livrés en kit sauf pour le U6000.

PARTIE 2 : INSTALLATION, PRE-CONFIGURATION, INTEGRATION

CHAPITRE 1 : INTERFACE GRAPHIQUE

2.1.1. Introduction

La configuration complète du firewall NETASQ se fait par un logiciel développé par la société NETASQ : NETASQ UNIFIED MANAGER. A partir de ce logiciel vous pourrez configurer entièrement votre firewall depuis un poste Windows.

L'installation de ce logiciel requiert les éléments suivants :

- CPU à 2Ghz minimum
- 512 Mo de RAM minimum (Windows XP) pour les logiciels clients, 2 Go pour les logiciels serveurs.
- La place occupée sur le disque dur après installation est d'environ 300 Mo.

Pensez à réserver plusieurs giga-octets d'espace pour la base de données (selon l'activité du/des firewall(s) connecté(s))

- Carte réseau Ethernet 100 ou 1000 Mbps

NETASQ supporte l'éxécution des logiciels dans un environnement défini :

Les logiciels clients sont supportés sur les systèmes d'exploitations 32 bits suivants :

- Microsoft Windows Serveur 2003 SP2
- Microsoft Windows XP Service Pack 2 et plus,
- Microsoft Windows Vista
- Microsoft Windows Serveur 2008

Les logiciels serveurs sont supportés sur les systèmes d'exploitation 32 bits suivants :

- Microsoft Windows Serveur 2003 SP2
- Microsoft Windows XP Service Pack 2 et plus

2.1.1.1. Pour ce chapitre, vous devez

Posséder le fichier d'installation de l'interface graphique. Ce fichier est disponible sur le CD-ROM livré avec votre firewall ou sur le site Web de NETASQ (www.netasq.com). Le fichier d'installation est bilingue.

Connaître l'adresse IP interne de votre firewall, ainsi que son numéro de série.

2.1.1.2. Utilité de cette partie

Cette partie vous présentera les éléments pour l'installation et l'utilisation générale de l'interface graphique de configuration (NETASQ UNIFIED MANAGER).

2.1.2.3. Administration suite client et serveur : choix des paquetages

Il est possible de sélectionner plusieurs paquetages :

Bibliothèque de base correspond à l'ensemble des modules nécessaires aux autres programmes. L'espace disque nécessaire est de 15,3 MB.

L'installation minimale regroupe :

- Netasq Unified Manager : Interface graphique d'administration des firewalls NETASQ
- Netasq realtime Monitor : Visualisation de votre firewall NETASQ en temps réel (2,58 MB)
- Netasq Event Reporter : Consultation et gestion des traces de votre firewall (140 MB)
- Netasq Updater : Service de téléchargement de l'aide des alarmes, événements système et vulnérabilités (10,5 MB).

Les additions serveurs regroupent :

- Netasq Autoreport : Création et Programmation de rapports automatiques selon les logs de vos firewalls, stockés en base de données (165,7 MB).
- Netasq Collector : service et base de données pour conserver les logs de vos firewalls (165, 7 MB)
- Netasq Syslog : Le Syslog est un service permettant de récupérer des logs émis par les firewalls (131,6 MB)

L'installation minimale constitue l'ensemble des outils de configuration graphique des suites NETASQ servant d'interface entre l'utilisateur et l'appliance. Ces outils sont installés sur une station d'administration.

Les additions serveurs constituent quant à elles l'ensemble des outils de communication utilisé pour récupérer les logs auprès des appliances vous appartenant. Ces outils sont généralement installés sur une machine dédiée du fait des ressources qu'elles nécessitent.

2.1.1.4. Les deux modes d'utilisation de NETASQ UNIFIED MANAGER

NETASQ UNIFIED MANAGER peut fonctionner sous deux modes différents : le mode Global Administration et le mode Firewall Manager.

- Le mode Firewall Manager permet de configurer votre produit.
- Le mode Global Administration est la solution logicielle pour gérer facilement et à moindre coût depuis un point central unique certaines actions d'administration sur l'ensemble d'un parc de produits NETASQ.

2.1.2. Installation

2.1.2.1. Procédure d'installation

Insérez le CD-ROM d'installation fourni ou téléchargez les fichiers nécessaires à partir du site Web NETASQ et exécutez le programme .EXE correspondant à la suite d'administration. Les informations d'installation apparaissent dans la langue de la version Windows.

Lorsque le CD-ROM est inséré, l'assistant d'installation de la Suite d'administration se lance automatiquement. Celui-ci vous guide étape par étape.

Figure 7 : Assistant d'installation du CD-ROM

2.1.3. Procédure de vérification

2.1.3.1. Procédure de vérification de la signature

Lorsque vous téléchargez un applicatif à partir de votre espace clients ou partenaires depuis le site www.netasq.com, un message vous demande : « Voulez-vous ouvrir un fichier ou l'enregistrer sur votre ordinateur ? ».

- Si vous choisissez l'option « Ouvrir », votre explorateur Web réalisera automatiquement la vérification de la signature et vous en avisera.
- Si vous choisissez l'option « Enregistrer » (option recommandée), vous devrez réaliser la vérification manuellement.

2.1.3.2. Vérification manuelle

Pour effectuer la vérification manuelle de la signature de l'application, effectuez la procédure suivante avant d'installer l'applicatif :

1 Effectuez un clic-droit sur l'application NETASQ dont vous voulez vérifier la signature puis sélectionnez le menu **Propriétés** dans le menu contextuel qui s'affiche.
2 Sélectionnez l'onglet **Signatures numériques** puis le nom du signataire (NETASQ).

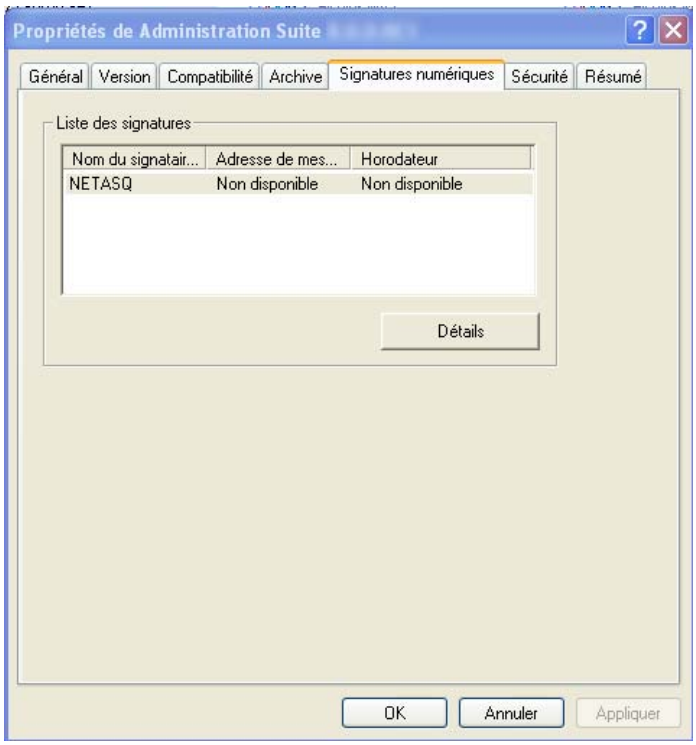


Figure 8 : Signatures numériques

3 Cliquez sur le bouton **Détails** : la validité de la signature numérique est indiquée dans cette fenêtre.

2.1.4. Enregistrement

Lors de l'installation, un enregistrement de votre produit vous est proposé. Cet enregistrement est obligatoire pour obtenir la licence de votre produit, pour télécharger les mises à jour et pour accéder au support technique NETASQ.

2.1.5. Centre d'assistance technique

NETASQ met à votre disposition différents moyens et outils pour la résolution d'un problème technique sur votre firewall.

- Une base de connaissances.
- Un réseau de distribution certifié. Vous pouvez ainsi faire appel à votre revendeur.
- Des documents : accessible sur votre espace clients ou partenaires. Vous devez posséder un compte client pour pouvoir accéder à ces documents.

Pour plus d'informations au sujet de l'assistance technique, veuillez vous référer au document « Support standard NETASQ ».

CHAPITRE 2 : LE FIREWALL NETASQ

2.2.1. Introduction

2.2.1.1. Pour ce chapitre, vous devez avoir pris connaissance des chapitres suivants :

- Partie 2/Chapitre 1 : Interface graphique

2.2.1.2. Pour ce chapitre, vous devez connaître

- L'adresse IP de votre firewall (si le produit est encore en configuration usine, l'adresse IP est : 10.0.0.254).

2.2.1.3. Utilité de ce chapitre

Nous vous conseillons de prendre le temps de lire soigneusement ce manuel avant l'installation. Il vous aidera à vous familiariser rapidement avec l'appliance et les outils afférents. Cette première lecture vous familiarisera déjà avec le firewall NETASQ.

Un firewall est une pièce maîtresse dans votre réseau, ne le négligez pas : installez-le au mieux, dans les meilleures conditions.

Ce chapitre vous permet de réaliser l'installation du boîtier et sa pré-configuration afin de l'intégrer dans l'architecture réseau désirée.

2.2.2. Préparation à l'installation physique du boîtier

2.2.2.1. Précautions d'installation

Local d'installation

Le boîtier doit être installé dans un local fermé, ou à défaut une armoire verrouillée avec une protection physique d'accès. Tout accès non autorisé au boîtier risque de compromettre la sécurité de votre installation.

Recommandation d'installation

En cas d'installation en baie, les équipements lourds doivent être placés le plus bas possible dans le rack ou l'armoire et les équipements plus légers au dessus.

Assurez-vous que l'alimentation électrique est correctement reliée à la terre, correctement dimensionnée pour supporter l'alimentation du boîtier NETASQ et qu'elle est de préférence secourue par un onduleur.

REMARQUE
Les boîtiers U30 et U70 utilisent une alimentation à double isolation, ne nécessitant pas de connexion à la terre.

N'installez pas le boîtier NETASQ dans un environnement dont la température ambiante dépasse les 35°C.

Assurez-vous que l'aération autour du produit peut être correctement réalisée et qu'aucun élément ne gêne la circulation d'air au travers des trous d'aération du produit.

Garantie

N'ouvrez jamais le boîtier. L'ouverture non autorisée du boîtier entraîne l'annulation de la garantie.

2.2.2.2. Préparation avant installation

Préparation des câbles réseau

Vous devez utiliser un câble réseau par interface du firewall connectée à votre infrastructure.

Type de câble réseau en fonction du port réseau

Type de port Ethernet	Type de câble	Connectique
Port 10/100BaseT Ethernet	Pour un fonctionnement en 100Mbits/s : paire torsadée catégorie 5 ou plus.	RJ45
Port 10/100/1000BaseT Ethernet	Pour un fonctionnement en 100Mbits/s	RJ45

	ou 1000Mbits/s : Paire torsadée catégorie 5 ou plus.	
Port 1000FX Gigabit Ethernet (câble fibre)	Câble fibre optique	LC

Type de câble réseau en fonction de l'équipement connecté

Equipement connecté au firewall	Type de câble
Hub	Câble droit
Switch	Câble droit
Modem	Câble droit ou croisé. Consultez la documentation du modem pour connaître le type de câble à utiliser. Vous pouvez aussi connecter le firewall et le modem (selon le type de modem) via la liaison série en utilisant un câble série droit.
Routeur	Câble croisé ou droit, si le routeur intégre un hub.
Autre firewall	Câble croisé
PC	Câble croisé

NOTE
Un câble croisé est livré avec le firewall NETASQ.

Préparation de l'armoire ou de la baie

Vous devez prévoir un espace minimum dans votre armoire ou votre baie pour l'installation du boîtier NETASQ. En fonction du produit l'espace minimum nécessaire en hauteur est différent :

- U30, U70 : 1U en hauteur, demi-19''
- U120, U250 et U450 : 1U en hauteur, 19'' en largeur
- U1100 et U1500 : 1U en hauteur, 19'' en largeur
- U6000 : 4U en hauteur, 19'' en largeur.

AVERTISSEMENT
Veuillez prévoir un espace vertical minimum entre chaque élément de l'armoire ou de la baie pour la circulation d'air.

Préparation de l'accès Internet

Avant l'installation du firewall NETASQ, assurez-vous que les équipements d'accès à Internet (si le firewall doit être connecté avec le réseau Internet) ont été convenablement installés et configurés.

2.2.3. Mise en baie

Tous les produits NETASQ peuvent être installés dans des armoires, baies 19 pouces. Les produits U1100 et U1500 intègrent des oreilles permettant l'installation directe du produit. Le U6000 est livré avec un système de rails permettant son intégration en baie.

Les produits U120, U250 et U450 sont livrés avec un système de fixation qui doit être ajouté au produit pour pouvoir installer celui-ci. Le système de fixation est disponible uniquement sur commande pour le U30 ou le U70.

2.2.3.1. Installation d'un U30 ou U70

Vue de dessus

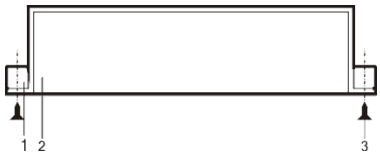


Figure 9 : U30, U70 : Mise en baie - Vue de dessus

Vue de face

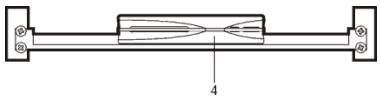


Figure 10 : U30, U70 : Mise en baie - Vue de face

1. Barres latérales de la baie
2. Plateau de support
3. Vis et écrous-cage
4. Produit

Un système de mise en baie peut être livré pour le U30 et U70 sur commande :

1 Installation du plateau sur le baie. Vissez le plateau de support sur les bords latéraux du rack au moyen d'écrous-cage.

2 Une fois le plateau installé, vous pouvez déposer (aucune fixation n'est nécessaire) un ou deux produits sur le plateau de support.

AVERTISSEMENT
Prévoyez un espace d'1U au dessus du produit pour une bonne circulation des flux d'aération.

2.2.3.2. Installation d'un U120, U250, U450

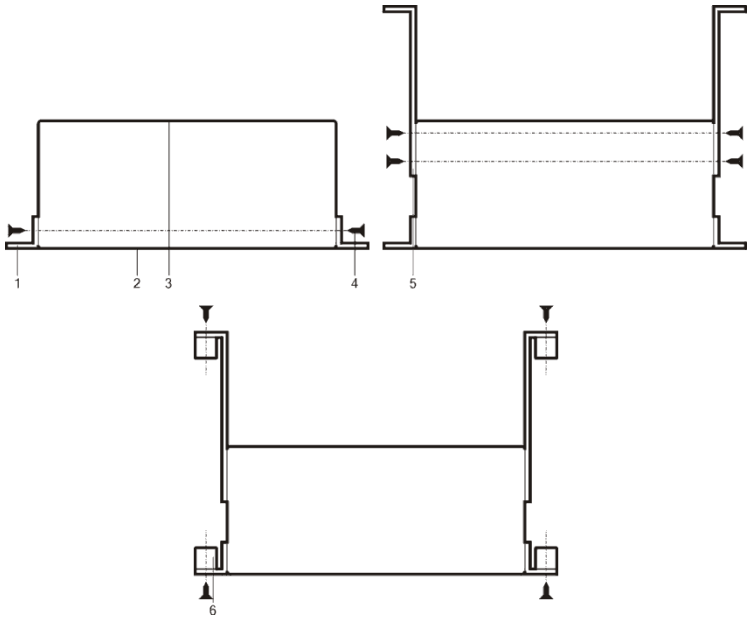


Figure 11 : U120, U250, U450 : Mise en baie

1. Barres latérales de la baie
2. Face Avant
3. Face Arrière
4. Vis et écrous-cage

Les U120, U250 et U450 sont livrés avec un kit d'équerres pour montage en baie. Les équerres n'apparaissent pas sur le plan ci-dessus.

1 Installation du boîtier dans la baie. Vissez les oreilles de fixation du chassis sur les bords latéraux de la baie.

AVERTISSEMENT
Les poignées métalliques présentes sur la face avant du produit ne doivent pas être utilisées pour porter celui-ci mais uniquement pour le placer ou le sortir dans la baie.

2.2.3.3. Installation d'un U1100, U1500, U6000

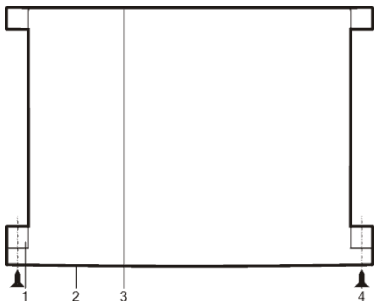


Figure 12 : U1100, U1500, U6000 : Mise en baie

1. Equerres
2. Face Avant
3. Face Arrière
4. Vis et écrous-cage
5. Barres de maintien
6. Barres latérales de la baie

Les U1100 et U1500 sont livrés avec un système d'équerres à fixer sur l'avant du boîtier et des barres de maintien latérales.

1 Mise en place des équerres de maintien. Vissez les équerres sur le boîtier. Les oreilles doivent être placées au niveau de la face avant du produit.

2 Mise en place des barres de maintien. Le positionnement des barres de maintien dépend de la taille de la baie.

3 Installation du boîtier dans le rack. Vissez les équerres et les barres de maintien sur les bords latéraux de la baie.

2.2.4. Branchements

2.2.4.1. Emplacement

Le firewall NETASQ est prévu pour fonctionner en permanence, dans un bureau ou un local. Si vous ne possédez pas de baie de brassage, choisissez une surface plane et dégagée, évitez les endroits exposés à la chaleur (rayons du soleil par exemple), à l'humidité ou à la poussière.

2.2.4.2. Raccordement de la prise secteur

Les firewalls NETASQ peuvent fonctionner sur du 230V ou du 110V.
Insérez la prise femelle du cordon secteur fourni dans l'embase secteur mâle située sur la face arrière du boîtier NETASQ. Puis, enfichez la partie mâle du cordon secteur fourni dans une prise secteur adéquate.

Le firewall démarre dès qu'il est relié au réseau électrique.

Une redondance d'alimentation est prévue sur le firewall U6000. Nous vous conseillons de raccorder chacun des deux cordons secteur à des réseaux électriques distincts, afin de vous prémunir contre une coupure d'alimentation de votre U6000. Il est en outre fortement recommandé de raccorder ces alimentations sur des onduleurs (« on line » de préférence).

AVERTISSEMENT
Il est recommandé d'utiliser une alimentation secourue par un onduleur.

2.2.4.3. Raccordement pour l'administration du boîtier

AVERTISSEMENT
L'administration du boîtier s'effectue par défaut par l'intermédiaire de son interface INTERNE. Cette interface, suivant les modèles, est identifiée par le chiffre 2 (U30, U70, U120, U250, U450).

2.2.4.4. Raccordement au réseau

Reliez les différentes interfaces du firewall aux éléments d'interconnexion réseau avec un câble RJ45. Les interfaces portent des numéros pour les modèles U30, U70, U120, U250 et U450 :

- L'interface identifiée « 1 » sur le firewall correspond à l'interface EXTERNE (appelée OUT par défaut)
- L'interface identifiée « 2 » sur le firewall correspond à l'interface INTERNE (appelée IN par défaut)
- Les interfaces identifiées « 3, 4, 5, … » sur le firewall correspondent aux interfaces DMZ (à l'instar de l'interface INTERNE, ces interfaces hébergent des réseaux internes).

Ci-dessous, vous sont indiquées les interfaces par boîtier :

U30

Figure 13 : Interfaces U30

U70

Figure 14 : Interfaces U70

U120

Figure 15 : Interfaces U120

U250

Figure 16 : Interfaces U250

U450

Figure 17 : Interfaces U450

U1100

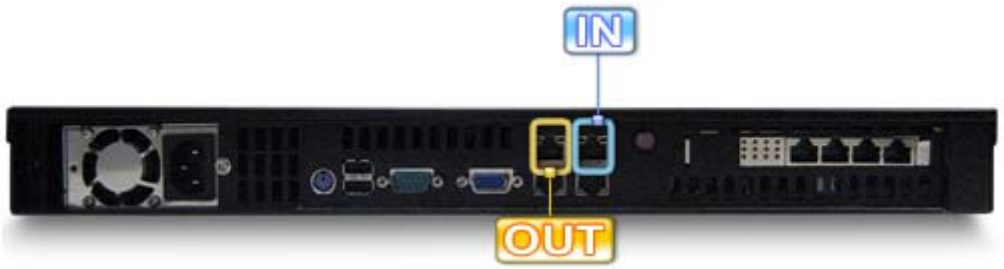


Figure 18 : Interfaces U1100

U1200

Figure 19 : Interfaces U1200

U6000

Figure 20 : Interfaces U6000

Utilisation de câble droit

Un câble droit doit être utilisé entre un firewall et un hub, un switch ou certains modems (selon le type de modem un câble droit ou croisé est nécessaire).

Utilisation de câble croisé (câble fourni avec le produit)

Un câble croisé doit être utilisé pour connecter le firewall à un élément actif de réseau (routeur, firewall, votre machine, certains modems...).

AVERTISSEMENT
Certains routeurs intègrent un hub, il faut donc dans ce cas utiliser un câble droit.

AVERTISSEMENT
En cas d'erreur de branchement, vous devrez redémarrer votre produit pour vous connecter à nouveau (En raison de la présence d'une protection contre l'usurpation d'adresses IP).

NOTE
Une succession de 8 bips successifs vous permet, si nécessaire, d'insérer une clé USB contenant une configuration.
Une succession de 2 bips successifs indique la fin de la phase de démarrage du produit.

2.2.5. Pré-configuration

A la réception de votre firewall NETASQ, celui-ci fonctionne en mode transparent et possède l'adresse IP 10.0.0.254 et le masque de sous réseau 255.0.0.0.

Ces paramètres ne correspondent pas à votre réseau, ils sont cependant nécessaires à la phase de pré-configuration.

Si vous ne savez pas ce que signifient ces paramètres, nous vous conseillons fortement de consulter un ouvrage sur TCP-IP car sans ce minimum de connaissances, la configuration de votre firewall NETASQ sera difficile.

Voici les intervalles définis par les différentes classes d'adresses IP :

Classe	Plage d'adresses IP
A	0.0.0.0 à 127.255.255.255
B	128.0.0.0 à 191.255.255.255
C	192.0.0.0 à 223.255.255.255
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

Certaines parties de ces plages d'adresses sont réservées pour des réseaux privés :

Classe	Plage d'adresses IP réservées
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255

C	192.168.0.0 à 192.168.255.255

2.2.5.1. Pré-configuration d'un poste Windows

La pré-configuration depuis un poste Windows est la méthode que nous vous conseillons. Nous allons utiliser un poste Windows. Ce poste peut être soit directement relié à l'interface interne du firewall, soit connecté au réseau local, lui-même relié à l'interface interne du firewall. Pour une connexion directe du poste sur le firewall, utilisez le câble Ethernet croisé, livré avec le produit.

> **AVERTISSEMENT**
> L'interface INTERNE du firewall est appelée 2 sur le boîtier (face avant pour les boîtiers U30, U70, U250, U450, face arrière et face arrière pour les boîtiers U1100, U1500 et U6000).

Pour vous connecter au firewall, vous devez utiliser un poste ayant une adresse IP dans le même sous-réseau que le firewall, nous vous proposons d'utiliser l'adresse 10.0.0.1 et le masque réseau 255.0.0.0.

Pour configurer votre poste Windows veuillez suivre la procédure suivante :

1. Dirigez vous vers le « Panneau de configuration » de votre poste Windows,
2. Sélectionnez le menu « Réseau »,
3. Sélectionnez le protocole TCP/IP dans la liste des éléments réseau puis « Propriétés »,
4. Indiquez les informations d'adressage nécessaire à la configuration réseau du poste :
   - Adresse IP : 10.0.0.250 ou l'adresse IP que vous avez choisie pour votre poste,
   - Masque de sous réseau : 255.0.0.0,
   - Passerelle par défaut : indiquez l'adresse actuelle de votre firewall (10.0.0.254 par défaut).

Ou configurez votre poste afin qu'il accepte une adresse IP dynamique provenant du boîtier (serveur DHCP) :

1. Ouvrez la fenêtre des **Connexions réseau**

- Windows 2000

Démarrer > Panneau de configuration > Connexions réseau et accès à distance

- Windows XP

Démarrer > Panneau de configuration > Connexions réseau

2. Cliquez-droit sur « Connexion au réseau local » et sélectionnez « Propriétés ».
3. Sélectionnez dans la liste « Protocole Internet (TCP/IP) », puis « Propriétés ».
4. Cochez **Obtenir une adresse IP automatiquement** et cliquez sur **OK.**
5. Pour valider les modifications, cliquez à nouveau sur **OK**.

2.2.5.2. Enregistrement et installation du produit

Votre produit possède un serveur web d'aide à l'installation qui peut vous guider pas à pas dans les différentes étapes de configuration.

La 1ère page du portail d'authentification permet de définir le mot de passe de votre produit.

Vous aurez ensuite la possibilité de :

- Configurer le réseau pour définir l'architecture réseau dans laquelle se trouve votre produit.
- Enregistrer votre produit pour obtenir des mises à jour
- Effectuer les 1ères mises à jour
- Obtenir la licence
- Installer les outils d'administration pour obtenir la suite logicielle Manager, Monitor et Reporter.

2.2.5.3. Pré-configuration d'un firewall

Vous pouvez désormais vous connecter au firewall grâce à l'interface graphique de configuration NETASQ : NETASQ UNIFIED MANAGER.

Après avoir installé ce logiciel de configuration sur le poste client, vous pouvez modifier les paramètres des interfaces réseau sur le firewall NETASQ pour l'adapter à vos adresses IP et choisir le mode de fonctionnement (transparent ou normal). (Cf. *Partie 5 : Configuration réseau*).

Si vous aviez changé l'adresse IP du poste client Windows pour faire cette configuration, n'oubliez pas de lui remettre son ancienne configuration.

2.2.5.4. Mécanisme antispoofing

AVERTISSEMENT

Si vous vous connectez à une interface puis débranchez le câble pour vous connecter sur une autre interface, vous déclencherez la sécurité anti-spoofing du firewall (il est alors impossible de se connecter au boîtier). Dans ce cas deux possibilités s'offrent soit vous modifiez l'adresse que vous venez d'attribuer à la machine d'administration (NETASQ recommande cette méthode) soit vous redémarrez le boîtier après avoir changé d'interface.

PARTIE 3 : PRISE EN MAIN DU MODE « FIREWALL MANAGER »

CHAPITRE 1 : DESCRIPTION

3.1.1. Pour ce chapitre, vous devez avoir pris connaissance des chapitres suivants

- Partie 2/Chapitre 1 Interface graphique
- Partie 2/Chapitre 2 Le firewall NETASQ

Vous trouverez un descriptif de ces points dans le manuel d'installation d'un équipement UTM NETASQ accessible via le CD-ROM d'installation ou l'espace client ou partenaire du site Web NETASQ.

3.1.2. Pour ce chapitre, vous devez connaître

L'adresse IP de votre firewall (si le produit est encore en configuration usine, l'adresse IP est : 10.0.0.254).

3.1.3. Utilité du chapitre

Les étapes décrites dans cette section vous accompagnent dans la découverte de votre firewall NETASQ. Une fois que vous aurez pris en main l'interface graphique, vous serez en mesure de continuer la configuration de votre produit.

CHAPITRE 2 : LANCEMENT

3.2.1. Accès

Deux exécutions sont possibles pour accéder à l'application NETASQ UNIFIED MANAGER, interface de configuration des UTM NETASQ.

- A partir du menu **`Applications\Exécuter le NETASQ UNIFIED MANAGER`** dans la barre de menus des applications NETASQ REAL-TIME MONITOR et NETASQ EVENT REPORTER de la Suite d'Administration.

A partir du menu Démarrer\Programmes\NETASQ\Administration Suite 7.0\NETASQ UNIFIED MANAGER.

L'écran principal s'affiche après la connexion :

Lorsque vous démarrez l'interface de configuration NETASQ, l'écran de démarrage de l'application vous rappelle la version du logiciel qui est installée. Puis la fenêtre principale de l'interface graphique de configuration des firewalls NETASQ s'affiche.

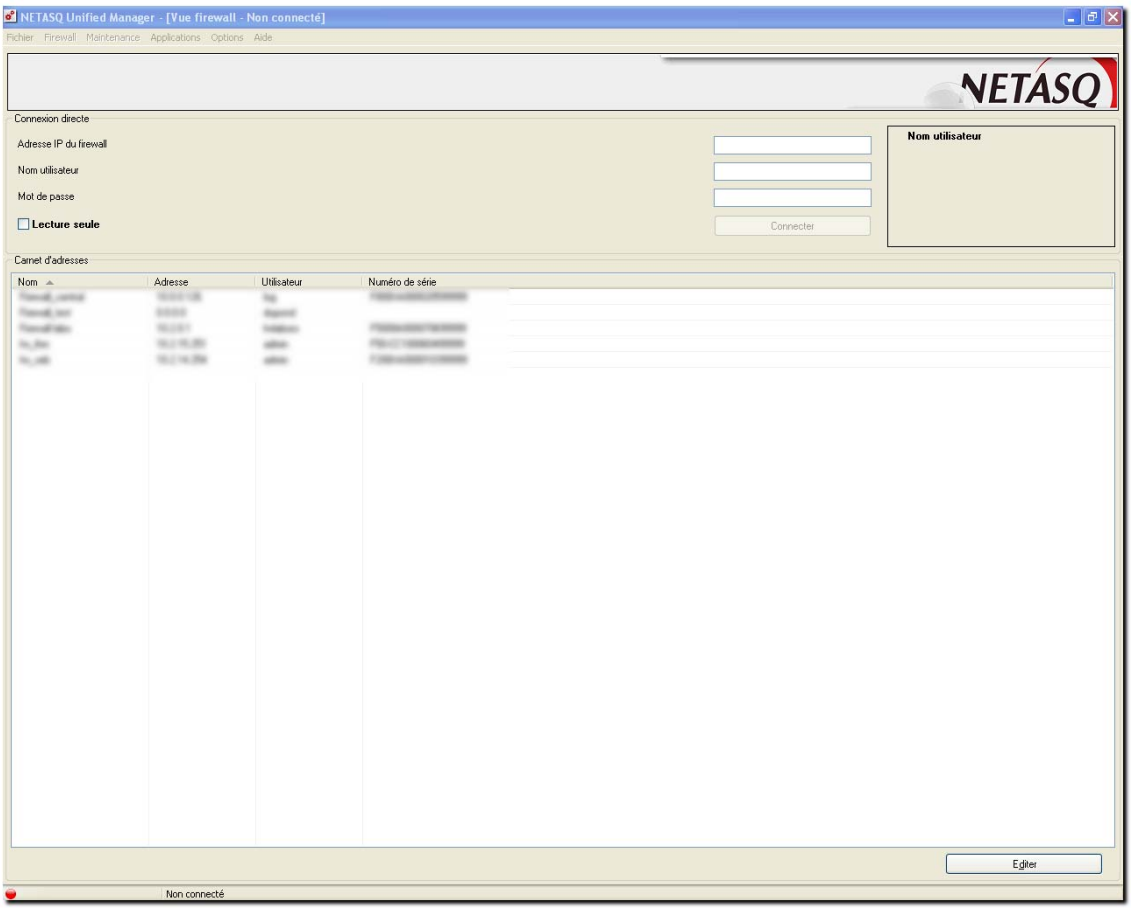


Figure 21 : Accès NETASQ UNIFIED MANAGER

A partir de cette fenêtre, vous accédez aux différentes parties de la configuration des firewalls.
Tant que vous n'êtes pas connecté à un firewall, vous ne pouvez accéder aux fonctionnalités principales de l'interface. Les menus auxquels vous avez accès sont :

- Le menu **Fichier** vous permet dans un premier temps d'accéder (entre autres) au carnet d'adresses afin de vous connecter à un firewall sélectionné. *Référez-vous à la partie Partie 19 : Actions diverses pour plus d'informations.*
- Le menu **Applications** permet de lancer directement les deux autres applications composant la suite d'administration NETASQ, NETASQ REAL-TIME MONITOR ET NETASQ EVENT REPORTER.
- Le menu **Options** permet de lancer les préférences générales de l'application.
- Le menu **Aide** vous permet d'avoir accès aux fichiers d'aide, d'effectuer la mise à jour de l'application et de connaître la version de l'interface graphique.

3.2.2. Connexion

Une connexion d'administration à un firewall s'effectue au moyen d'un logiciel de la Suite d'Administration NETASQ : NETASQ UNIFIED MANAGER pour la configuration des fonctionnalités, NETASQ REAL-TIME

MONITOR pour le monitoring et NETASQ EVENT REPORTER pour l'agrégation des traces et le reporting d'événements.

La configuration d'un firewall n'est accessible qu'aux administrateurs du produit. NETASQ définit un administrateur par un utilisateur possédant des droits d'administration. L'attribution des droits aux utilisateurs est effectuée dans la configuration de cet utilisateur *(Cf. Partie 4/Chapitre 3 : Utilisateurs)*.

3.2.2.1. La première connexion

AVERTISSEMENT
Par défaut, un produit UTM NETASQ n'est accessible qu'avec le NETASQ UNIFIED MANAGER. Ce qui signifie que : TOUT ACCES AUTRE QUE LE NETASQ UNIFIED MANAGER EST BLOQUE.

Exemple
Vous ne pouvez pas utiliser la commande PING pour vérifier le fonctionnement du boîtier.

3.2.2.2. Le compte « admin », super-administrateur

Par défaut, il n'existe qu'un seul utilisateur possédant des droits d'administration des produits NETASQ, le compte "admin" (son login est "admin"). Cet administrateur est un "super-administrateur". Il possède tous les droits plus un droit spécial "ADMIN" qu'il est le seul à pouvoir posséder. Cela lui confère le droit d'effectuer certaines opérations comme modifier la méthode d'authentification à un utilisateur par exemple. Sa configuration est impossible.

REMARQUE
Etant donné les droits du compte "admin", NETASQ conseille de n'utiliser ce compte qu'en test ou dans le cas d'une maintenance.

3.2.2.3. Processus de connexion

Le processus de connexion à un firewall est défini par une procédure en trois étapes variables suivant l'avancement de la configuration.

REMARQUE
L'étape 3 n'est spécifique qu'à la première connexion.

Etape 1 : Envoi des informations de connexion au firewall

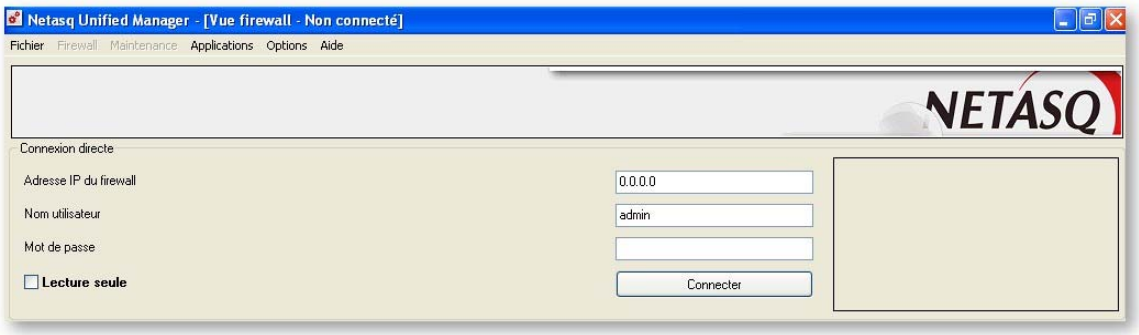


Figure 22 : Connexion à NETASQ UNIFIED MANAGER

Dans le cas de la première connexion

S'il s'agit de la première connexion à ce firewall, les informations de connexion sont les suivantes :

Adresse IP du firewall	"10.0.0.254", adresse IP du firewall NETASQ en configuration par défaut.
Nom utilisateur	"admin", seul administrateur défini en configuration par défaut.
Mot de passe	PAS DE MOT DE PASSE (champ vide), un mot de passe générique est utilisé en configuration par défaut.
Lecture Seule	Permet une connexion en mode "lecture". Ainsi vous pouvez vous connecter au firewall sans droits de modifications au moyen d'un compte possédant habituellement ces droits. Ceci permet de ne pas utiliser les droits de modifications si cela n'est pas nécessaire.

Lorsque les informations de connexion sont renseignées, cliquez sur le bouton **Connecter** pour envoyer les informations de connexion au firewall. Puis passez à l'étape suivante.

Dans le cas d'une autre connexion

La connexion auprès d'un firewall demande les informations de connexion suivantes :

Adresse IP du firewall	Adresse IP ou nom de machine du firewall NETASQ sur le réseau interne.
Nom utilisateur	nom d'utilisateur pour la configuration.
Mot de passe	mot de passe pour l'utilisateur.
Lecture Seule	Permet une connexion en mode "lecture". Ainsi vous pouvez vous connecter au firewall sans droits de modifications au moyen d'un compte possédant habituellement ces droits. Ceci permet de ne pas utiliser les droits de modifications si cela n'est pas nécessaire.

Si vous indiquez un nom de machine dans le champ **Adresse IP du firewall**, ce nom doit être ajouté dans vos tables DNS ou dans le fichier "c:\winnt\system32drivers\etc\hosts" de la machine d'administration.

AVERTISSEMENTS

1) Le firewall NETASQ fait la différence entre les majuscules et les minuscules, aussi bien pour le nom d'utilisateur que pour le mot de passe.
2) Le mot de passe doit contenir au minimum 8 caractères.

Lorsque les informations de connexion sont renseignées, cliquez sur le bouton **Connecter** pour envoyer les informations de connexion au firewall. Puis passez à l'étape suivante.

Etape 2 : validation du numéro de série du firewall contacté

REMARQUE

Etape réalisée uniquement lors de la première connexion au firewall avec une station d'administration donnée.

Lors de la première connexion au firewall avec une station d'administration donnée et que le numéro de série du firewall contacté n'est pas renseigné dans le carnet d'adresses (*Cf. Partie 3/Chapitre 2/ point Configuration du carnet d'adresses*) NETASQ UNIFIED MANAGER demande avant toute chose de valider le numéro de série du firewall contacté.

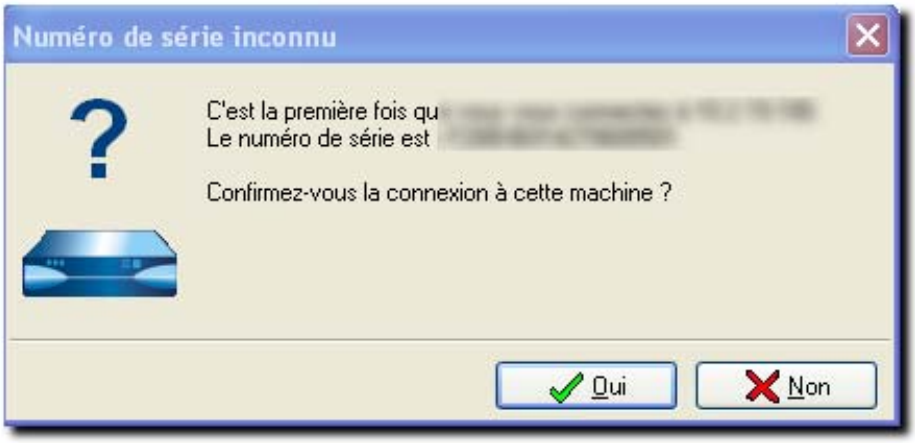


Figure 23 : Numéro de série inconnu

La fenêtre apparue indique le numéro de série que le firewall a renvoyé (auprès duquel l'administrateur effectue une tentative de connexion). Si le numéro de série ainsi affiché est identique à celui inscrit sur l'étiquette accolée sur le boîtier du firewall, confirmez la connexion sur cette machine en cliquant sur le bouton **Oui** puis passez à l'étape suivante. Sinon la connexion est interrompue.

Utilité de l'étape de connexion

Les sessions d'administration véhiculent des informations sensibles (mots de passe d'administration par exemple). Le détournement d'une telle session peut s'avérer désastreux pour la sécurité. En effet si un pirate s'empare d'un mot de passe administrateur, il peut modifier à sa guise la politique de sécurité du produit.

Chaque produit UTM NETASQ est identifié par un certificat. Ainsi la validation du numéro de série du firewall contacté permet d'éviter des attaques de type "man in the middle".

Dans ce type d'attaque, le pirate s'insère entre la station d'administration et le firewall. Il peut ainsi intercepter l'échange entre le firewall et l'administrateur. Bien que cette attaque soit très difficile à mettre en place, elle reste une menace identifiée. Il est prudent de s'en prévenir.

Etape 3 : Enregistrement du mot de passe du compte "admin"

REMARQUE
Etape réalisée uniquement lors de la première connexion au firewall.

S'il s'agit de la première connexion au firewall, le logiciel d'administration (NETASQ UNIFIED MANAGER, NETASQ REAL-TIME MONITOR ou NETASQ EVENT REPORTER) demande de définir un mot de passe indispensable pour le compte "admin".

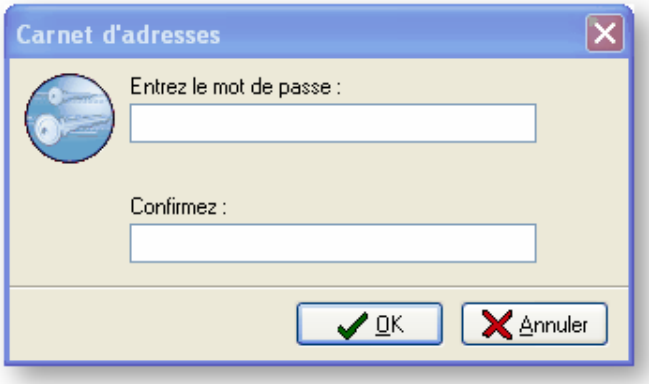


Figure 24 : Mot de passe - Carnet d'adresses

Spécifiez le mot de passe qui sera associé au compte "admin". Cliquez sur **OK** pour terminer le processus de connexion.

AVERTISSEMENT
Si ce message n'apparaît pas à votre première connexion, cela signifie que quelqu'un d'autre s'est connecté à votre produit avant vous. Contactez donc immédiatement votre partenaire.

Utilité de l'étape de connexion

Cette étape de connexion est un mécanisme de sécurité simple mis en place par NETASQ pour assurer l'intégrité du firewall jusqu'à sa livraison. En effet :

- Cette étape est indispensable lors de la première connexion. Ainsi s'il s'agit de la première connexion et que cette étape n'apparaît pas cela signifie qu'une personne tierce a eu accès à l'Appliance avant et que des modifications ont été effectuées.
- L'enregistrement du mot de passe du compte "admin", par le détenteur réel du compte "admin" permet de garantir l'entière confidentialité d'un mot de passe particulièrement sensible.
- La connexion au firewall grâce à la console d'administration de l'Appliance est impossible avant qu'un mot de passe de connexion valide soit défini. Avant la première connexion, le mot de passe de connexion "admin" ne peut être défini que par l'intermédiaire de l'interface graphique.

3.2.2.4. Restrictions d'administration

Droits d'administration

Chaque commande d'administration disponible sur un firewall est associée à un droit de consultation/modification. Ceci se traduit par l'accès ou non à certains menus d'administration dans les logiciels d'administration de la suite NETASQ. Lorsqu'un administrateur est accrédité d'un droit donné, il est habilité à effectuer toutes les commandes associées à ce droit. (*La liste des droits disponibles sur les firewalls est indiquée dans la Partie 4 : Objets*.

Multi-utilisation

Vous pouvez avoir un nombre illimité de sessions ouvertes simultanément avec des utilisateurs identiques ou différents. La seule contrainte est qu'à un moment donné vous ne pouvez avoir qu'une unique session avec les privilèges de modification "généraux" (pour éviter les conflits de modification). Ceci n'empêche pas d'autres utilisateurs de consulter la configuration, les utilisateurs possédant le droit MODIFY perdront temporairement ce droit si un utilisateur avec le droit MODIFY est déjà connecté.

Lorsqu'un administrateur est déjà connecté avec les privilèges de modification, un message vous indique que les privilèges de modification ont déjà été attribués et que vous pouvez choisir de récupérer ces droits ou de continuer la connexion sans droits de modification :

> **Confirmation**
> Vous avez perdu les privilèges de modification. Un utilisateur possédant ces privilèges est peut être déjà connecté. Voulez-vous récupérer les privilèges de modification (l'utilisateur connecté avec les droits de modification sera alors déconnecté).

La procédure permettant d'identifier l'utilisateur connecté avec les droits de modification est indiquée dans la section relative au NETASQ REAL-TIME MONITOR.

3.2.2.5. Le carnet d'adresses

Le carnet d'adresses des logiciels NETASQ est un outil central dans la gestion des accès aux menus d'administration. En effet il peut contenir l'ensemble des informations de connexion nécessaires pour une connexion à une liste de firewalls, ainsi l'accès de l'administrateur est simplifié car il ne lui est plus indispensable de retenir les mots de passe que cela implique.

Dans les versions précédant celle-ci, les modes "Firewall Manager" et "Global Administration" étaient deux applications distinctes. Aussi, il était possible d'obtenir deux carnets d'adresses : l'un au format. Dat pour le Manager et l'autre au format .Gap pour le Global Administration.

Ces deux applications, désormais fusionnées, le carnet d'adresses peut être enregistré au format. Dat en mode Manager (export). Cependant, le carnet d'adresses utilisé par les applications de la Suite d'Administration est stocké en format .Gap uniquement.
Ce format de fichier est plus extensible. Il contient les firewalls, mais aussi les serveurs. Il contient également les informations relatives aux topologies.

Cette importation du carnet d'adresses dans un projet G.A implique que, lors du premier lancement du Manager, l'utilisateur saisisse son mot de passe lié au carnet d'adresses. Un projet contenant la liste des firewalls du carnet d'adresses est alors automatiquement créé. La sauvegarde du projet est également proposée.

Le carnet d'adresses utilisé pour NETASQ UNIFIED MANAGER, NETASQ REALTIME MONITOR et NETASQ EVENT REPORTER se trouve dans C:\Documents and Settings\<USERNAME>\Application Data\Netasq\AS\8.0.
Quant au projet en mode G.A, il peut être stocké n'importe où.

Pour un fichier de sauvegarde de projet (extension *.gap) créé avec une version antérieure, il sera automatiquement converti au nouveau format en effectuant une sauvegarde de la nouvelle version de NETASQ UNIFIED MANAGER (mode Global Administration).

Configuration du carnet d'adresses

La manière d'accéder à la configuration du carnet d'adresses est la suivante :

- Depuis le menu **Fichier\Carnet d'adresses**…

Dans ce carnet d'adresses, il est possible de définir les firewalls auxquels vous désirez vous connecter. Indiquez pour chaque firewall, un nom (ce champ est arbitraire et peut ne pas correspondre au nom du firewall), une adresse IP, un mot de passe et un numéro de série.

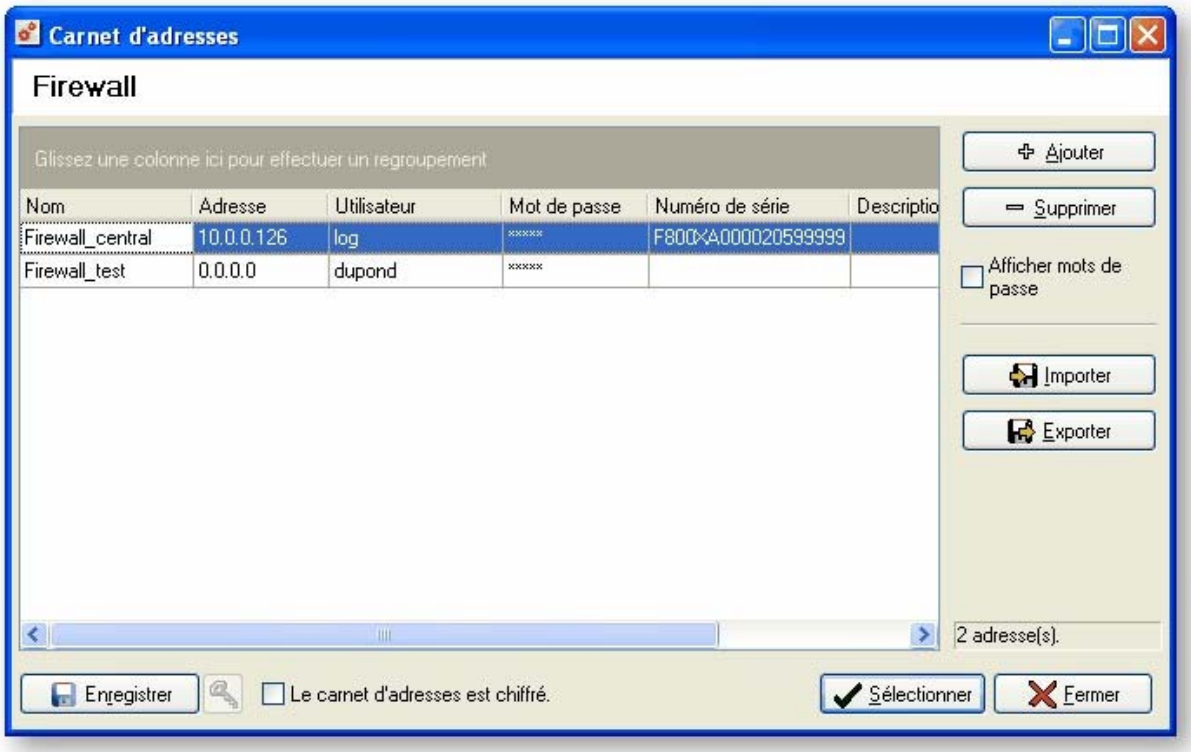


Figure 25 : Liste des firewalls - Carnet d'adresses

AVERTISSEMENT

Lorsque vous définissez un numéro de série pour un firewall, ce numéro de série est ajouté à la liste des numéros de série connus la première fois que vous vous connectez à ce firewall en utilisant le carnet d'adresses et cela sans qu'aucun message de confirmation n'apparaisse (étape 2 du processus de connexion).

Afficher les mots de passe

Cochez l'option **Afficher mots de passe** pour vérifier les mots de passe utilisés pour chacun des firewalls enregistrés dans le carnet d'adresses (les mots de passe sont affichés en clair).

Importation d'un ancien carnet d'adresses

Pour récupérer le carnet d'adresses provenant d'anciennes versions, il suffit d'effectuer l'import d'un fichier au format **.gap.**

L'accès à l''import est différent selon le mode dans lequel on se trouve.

- Dans le mode "Manager", accédez au menu **Fichier\Carnet d'adresses** puis cliquez sur le bouton **Importer.**
- Dans le mode "Global Administration", accédez au menu **Fichier** puis sélectionnez **Importer le carnet d'adresses…**

Le fichier d'importation des données doit respecter le formatage suivant :

```
BOOK]
Copyright=# Firewall Address Book (c)2001 NETASQ
AddressNumber=1

[1]
Name=Firewall_Central
Comment=Siège Social
Type=Firewall
Address=192.168.0.1
User=admin
Password=adminadmin
Serial=U70XXA0Z0899020
```

Où

- **Copyright** : Obligatoire, a pour valeur " # Firewall Address Book (c) 2001 NETASQ
- **AddressNumber** : nombre d'entrées dans le carnet d'adresses
- **[x]** : sépare chaque ligne, x représente le numéro de ligne dans le carnet
- **Name** : nom donné au firewall dans la liste du carnet d'adresses
- **Comment** : commentaire
- **Type** : le type doit être obligatoirement "Firewall"
- **Address** : adresse de connexion au firewall
- **User** : login de l'administrateur
- **Password** : mot de passe de l'administrateur
- **Serial** : numéro de série du firewall

Pour importer un carnet d'adresses existant, suivez la procédure suivante :

1. Cliquez sur le bouton **Importer à partir du mode "Firewall Manager"**. La fenêtre suivante s'affiche :

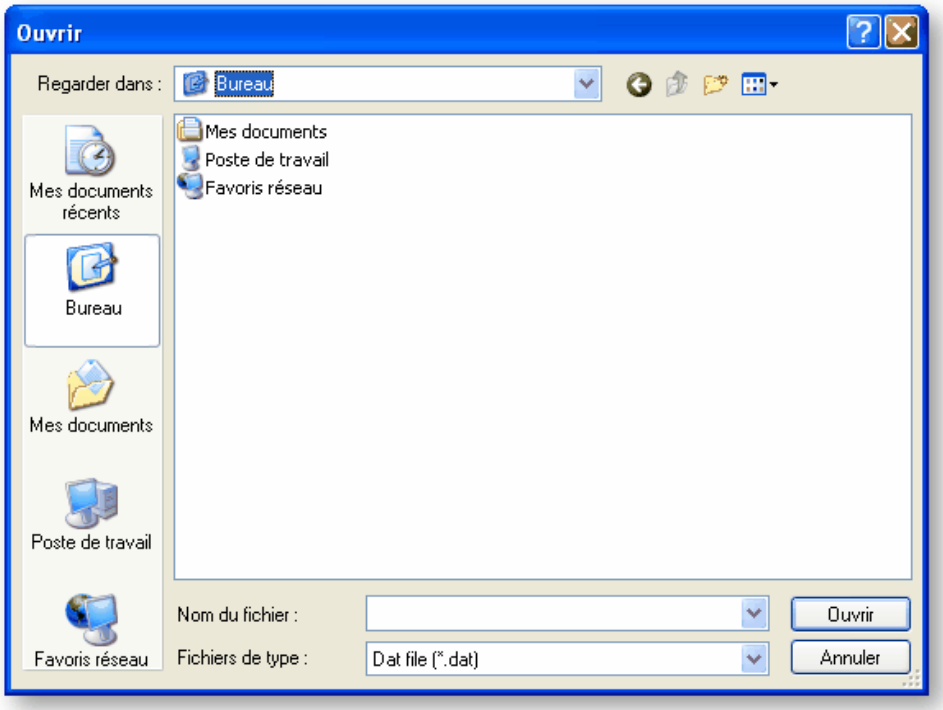


Figure 26d'importation : Sélection d'un fichier

2 Sélectionnez le fichier d'importation.

REMARQUE
Le fichier d'importation est un fichier au format **.dat**

3 Cliquez sur **Ouvrir**.

Pour des raisons évidentes de sécurité le carnet d'adresses peut être chiffré. Pour activer ce chiffrement, cochez l'option **Le carnet d'adresses est chiffré** puis définissez le mot de passe associé. Ce mot de passe est indispensable à la lecture des informations contenues dans le carnet. Le chiffrement du carnet est effectué au moyen de l'algorithme AES, algorithme de chiffrement symétrique le plus performant actuellement.

Exportation du carnet d'adresses

L'ensemble des informations présentées dans le carnet d'adresses peuvent être exportées pour servir par exemple à compléter un autre carnet d'adresses. Pour exporter un carnet d'adresses existant, suivez la procédure suivante :

1 Cliquez sur le bouton **Exporter à partir du mode "Firewall Manager"** dans la fenêtre de configuration du carnet d'adresses. La fenêtre suivante s'affiche :

2 Le message suivant s'affiche :

"Chiffrer le carnet d'adresses ? (fortement recommandé)"

3 Si vous cliquez sur **Oui**, le mot de passe du carnet d'adresses est demandé avant que la fenêtre d'enregistrement ne s'affiche :

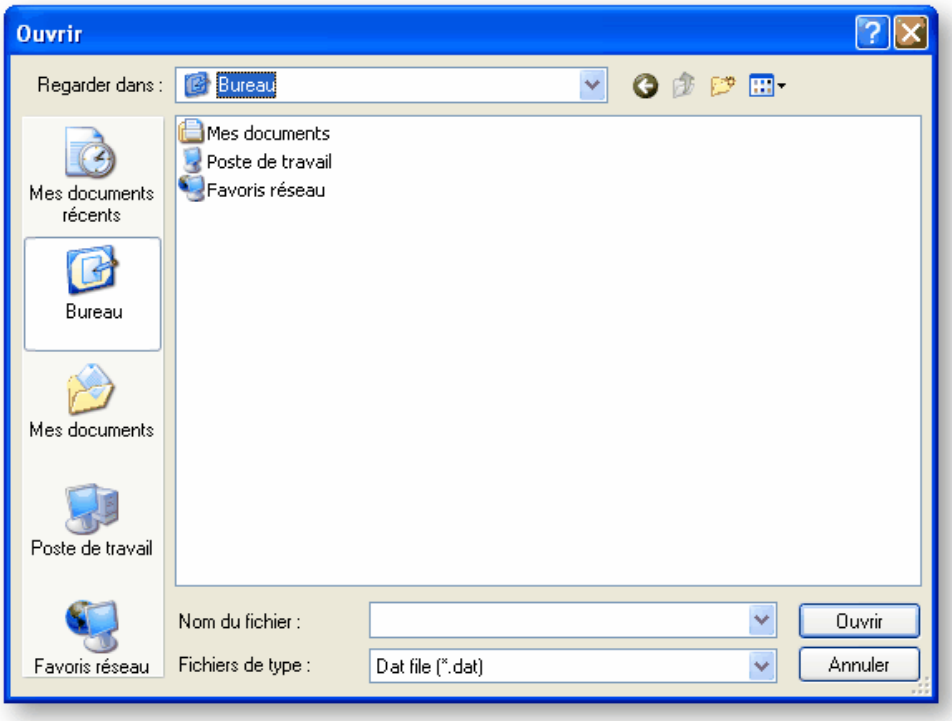


Figure 27 : Sélection d'un fichier d'exportation

REMARQUE
Le fichier d'exportation sera un fichier au format **.dat.**

4 Cliquez sur **Enregistrer**.

Le carnet d'adresses doit être chiffré

Pour des raisons évidentes de sécurité le carnet d'adresses peut être chiffré. Pour activer ce chiffrement, cochez l'option **Le carnet d'adresses est chiffré** puis définissez le mot de passe associé. Ce mot de passe est indispensable à la lecture des informations contenues dans le carnet. Le chiffrement du carnet est effectué au moyen de l'algorithme AES, algorithme de chiffrement symétrique le plus performant actuellement.

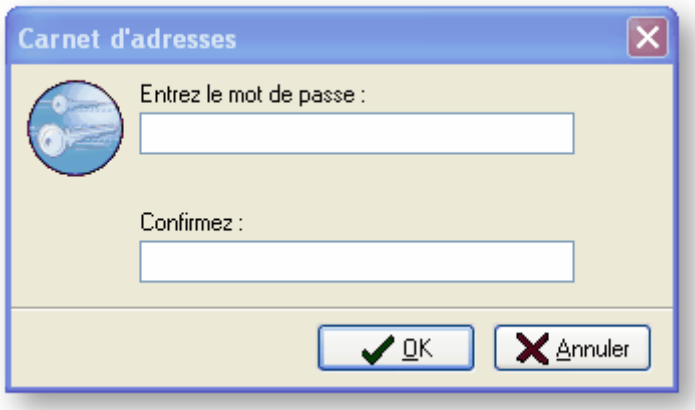


Figure 28 : Mot de passe - carnet d'adresses

Enregistrer

L'enregistrement des données ajoutées ou modifiées est indispensable avant toute fermeture du carnet d'adresses. Sinon toutes les modifications apportées sont perdues. Pour enregistrer les modifications du carnet d'adresses, cliquez sur le bouton **Enregistrer**.

REMARQUES
Les paramètres **Adresse** et **Utilisateur** saisis dans la boîte de dialogue de connexion sont sauvegardés dans la base de registres de votre PC d'administration.

Pour des raisons évidentes de sécurité, le paramètre **Mot de passe** n'est pas sauvegardé.

Fichiers du carnet d'adresses sur la machine d'administration

Sur la machine d'administration, les fichiers du carnet d'adresses se situent dans le répertoire d'installation de l'application. Il existe deux fichiers :

- **AddrBook.dat** : ce fichier contient le carnet d'adresses de la Suite d'Administration. S'il est chiffré les informations qu'il contient sont illisibles.

3.2.3. Déconnexion

Pour vous déconnecter d'un firewall, suivez la procédure suivante :

1. Sélectionnez **Fichier\ Déconnexion** dans les menus de l'interface de configuration ou cliquez sur le bouton **Déconnecter** situé sous l'arborescence des menus.
2. L'interface revient à l'écran de connexion.

Suivant les options définies par l'utilisateur, la déconnexion demande ou non une confirmation. L'annulation provoque le retour à l'écran principal, sans conséquence pour la suite de l'exécution du programme.

La déconnexion vous fait revenir à l'écran principal, mais le voyant d'état (en bas à gauche) est devenu :

3.2.4. Partition de démarrage

3.2.4.1. Introduction

Les produits UTM NETASQ permettent la sauvegarde de leur système principal sur une partition de sauvegarde. Ainsi lorsque leur système principal est corrompu ou la configuration effectuée ne permet pas la reprise en main du boîtier, il est possible de démarrer le produit NETASQ sur cette partition de backup, restée quant à elle, "propre".

Pour démarrer un Appliance UTM NETASQ sur sa partition de sauvegarde, il existe deux possibilités. La première nécessite une connexion en mode console au boitier (lien série) et n'est pas évoquée dans cette section.

Dans un deuxième temps, le menu **Maintenance\Partition de démarrage** du mode "Firewall Manager", permet quant à lui la définition de la partition de démarrage par défaut du produit UTM NETASQ.

Ainsi, sans connexion en mode console (lien série) et à distance, il est possible de redémarrer le boitier sur sa partition de sauvegarde et cela de manière automatique et systématique.

3.2.4.2. Configuration

Accédez au menu **Maintenance\Partition de démarrage.** L'écran de configuration de la partition de démarrage s'affiche :

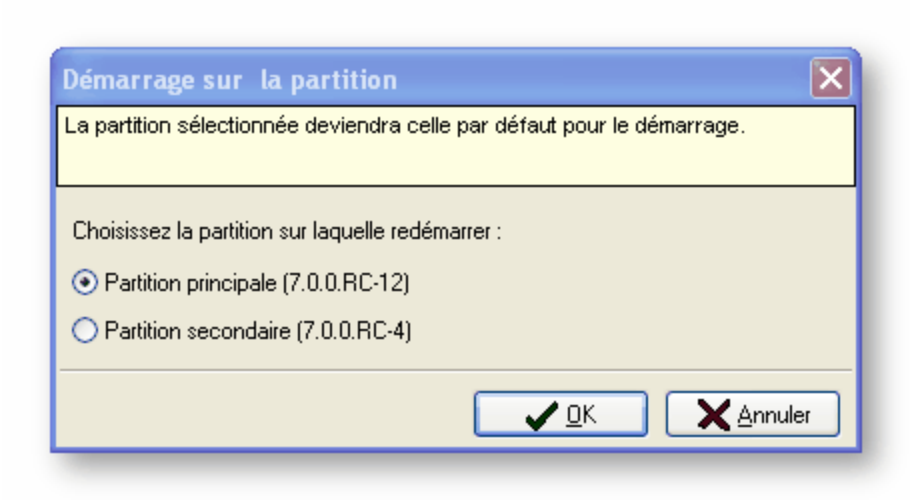


Figure 29 : Démarrage sur la partition

Cet écran indique les deux partitions détectées sur le disque dur de l'Appliance et la version disponible sur cette partition. Pour définir la partition de démarrage par défaut du firewall, choisissez la partition parmi celles proposées et cliquez sur **OK** pour valider les modifications.

3.2.5. Quitter l'application

Lors de la fermeture de l'application, une boîte de dialogue vous demande de confirmer l'action (suivant les options configurées dans le menu **Options\Préférences\Comportement**.)

Pour fermer l'application, accédez au menu **Fichier\Quitter.** Le message suivant s'affiche :

"Quitter cette application ?"

- L'annulation provoque le retour à l'écran principal, sans conséquence pour la suite de l'exécution du programme.
- La confirmation quitte l'application.

Cette boîte est également affichée quand vous quittez l'application en cliquant sur ☒ en haut à droite de la fenêtre Windows.

CHAPITRE 3 : PRESENTATION DE L'INTERFACE

3.3.1. Fenêtre principale

Une fois connecté au firewall, la fenêtre principale s'affiche. Les menus non accessibles au compte actuellement connecté sont inactifs.

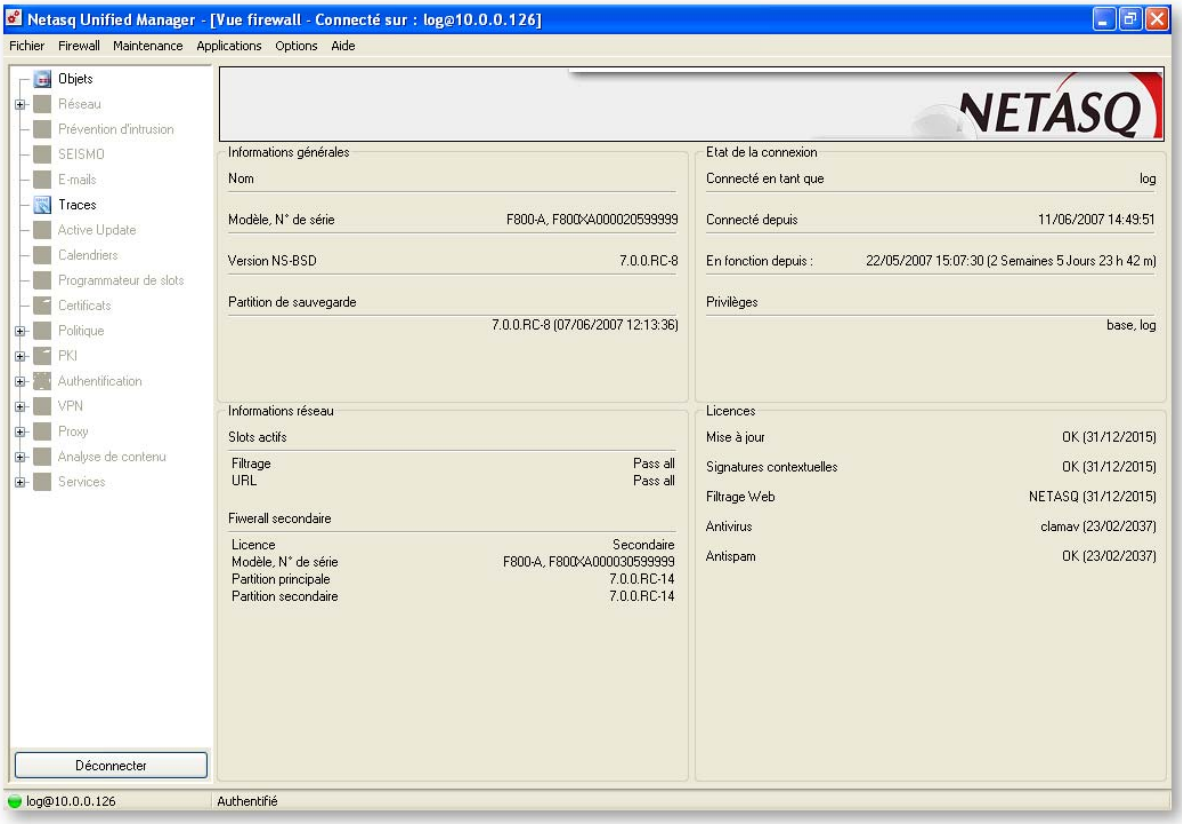


Figure 30 : Fenêtre principale - NETASQ UNIFIED MANAGER

L'écran central est divisé en quatre sections distinctes :

3.3.1.1. Informations générales

- Nom donné au firewall.
- Modèle de boîtier et n° de série.
- Version logicielle du firewall (sur la partition principale).
- Version logicielle de la partition de sauvegarde.

3.3.1.2. Informations réseau

- Slots actifs à la connexion (filtrage, translation, VPN, etc.).

Exemple
Indication de la politique de filtrage activée.

3.3.1.3. Etat de la connexion

- Le compte utilisé pour la connexion.
- La date, l'heure et la durée écoulée depuis la connexion au firewall.
- La date, l'heure et la durée écoulée depuis le démarrage du firewall.
- Les droits accordés au compte utilisé pour la connexion. *(Cf. Annexe A: Droits de la session et droits d'utilisateurs)*

3.3.1.4. Licence

- La date d'expiration de l'option Mise à jour.
- La date d'expiration de l'option Signatures contextuelles.
- La date d'expiration du filtrage Web.
- La date d'expiration de l'option Antivirus.
- La date d'expiration de l'option Antispam.

AVERTISSEMENT
Avant toute action ultérieure, vérifiez que la version logicielle du firewall indiquée dans l'écran correspond bien à la version attendue. Il existe une seconde possibilité de vérifier la version du produit. *Cf.* Référez-vous à l'*Annexe H : Commandes*.

3.3.2. Barre de menus

La fenêtre principale du mode "Firewall Manager" contient la barre de menus suivante :

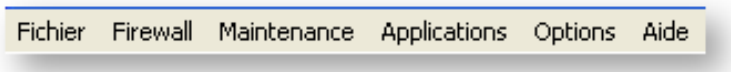


Figure 31 : Barre de menus

3.3.2.1. Explication des menus

Fichier	Déconnexion, édition du carnet d'adresses du firewall et Quitter l'application.
Firewall	Gestion des licences, Support technique, Configuration du système (date, heure, langue ...), Sécurité, configuration de la Haute Disponibilité, Configuration sécurisée, Eteindre les voyants d'alarmes.
Maintenance	Sauvegarde, Restauration, Mise à jour du firmware, Redémarrage…
Applications	Liens rapides aux applications de la Suite d'Administration, NETASQ REAL-TIME MONITOR et le NETASQ EVENT REPORTER.
Options	Gestion des préférences de l'application.
Aide	Accès aux fichiers d'aide, affichage de la boîte "A propos" indiquant le numéro de version de l'interface graphique, accès à la mise à jour de NETASQ UNIFIED MANAGER.

3.3.3. Arborescence des menus

L'arborescence contient tous les menus de configuration des fonctionnalités des firewalls. Lorsque le menu est grisé, la licence ou les droits de l'utilisateur ne permettent pas l'accès et/ou l'affichage de ce menu.

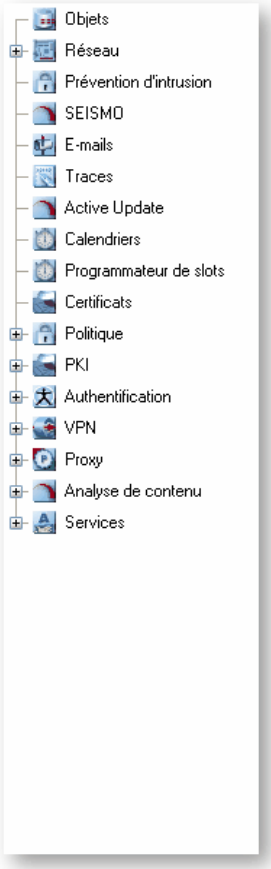


Figure 32 : Arborescence des menus

Correspondance entre les menus de l'interface et le sommaire

Objets	Partie 4 : OBJETS
Réseau	Partie 5 : CONFIGURATION RESEAU
Prévention d'intrusion	Partie 6 : PREVENTION D'INTRUSION (ASQ)
SEISMO	Partie 15 : SEISMO
E-mails	Partie 16 : CONFIGURATION DES MAILS
Traces	Partie 17 : GESTION DES TRACES
Active update	Partie 18 : MAINTENANCE : Active Update
Calendriers	Partie 7/Chapitre 3 : Calendriers
Programmateur de slots	Partie 7/Chapitre 3 : Programmateur de slots
Certificats	Partie 8 : VPN

Politique	Partie 7 : POLITIQUE
PKI	Partie 13/Point 4 : PKI
Authentification	Partie 12 : AUTHENTIFICATION
VPN	PARTIE 8 : VPN
Proxy	Partie 9 : CONFIGURATION DES PROXIES
Analyse de contenu	Partie 10 : ANALYSE DE CONTENU
Services	PARTIE 11 : SERVICES

3.3.4. Barre d'état

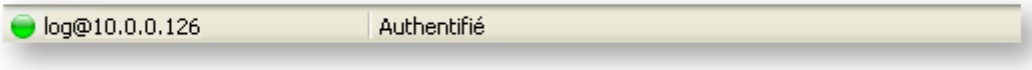


Figure 33 : Barre d'état

Au bas de la fenêtre principale se trouve la barre d'état composée de trois parties :

Voyant d'état	Vous êtes actuellement connecté à NETASQ UNIFIED MANAGER. Vous êtes déconnecté de NETASQ UNIFIED MANAGER.
Utilisateur@IP	Nom de l'utilisateur connecté et l'adresse IP du firewall.
Zone de texte	Affiche le descriptif de l'action associée à une icône, le résultat d'une action ou le descriptif d'une erreur survenue. **Exemple** "Authentifié"

CHAPITRE 4 : INTEGRATION

3.4.1. Intégration

Les firewalls NETASQ se caractérisent par une grande facilité d'intégration. Les quelques exemples d'architectures suivants le montrent.

3.4.1.1. Installation du firewall au sein d'une architecture déjà déployée

Le réseau que vous devez protéger par un firewall NETASQ est déjà connecté à Internet via un routeur dont vous n'assurez pas l'administration. Toutes les adresses IP du réseau interne ont déjà été configurées.

Solution NETASQ : insérez le firewall NETASQ entre le routeur et le LAN, en mode transparent (même adresse IP sur toutes les interfaces). Ainsi vous n'aurez à modifier ni l'adresse interne du routeur, ni les adresses IP de vos postes internes.

3.4.1.2. Installation du firewall au sein d'une architecture reposant sur une segmentation VLAN

Vous pouvez placer le firewall NETASQ en terminaison de VLAN Ethernet. Le firewall pourra assurer le filtrage et le routage entre VLAN.

3.4.1.3. Installation du firewall derrière un modem

Vous installez un firewall NETASQ derrière un accès Internet modem (ADSL, RNIS, RTC ou modem câble) sans posséder de routeur.

Solution NETASQ : le firewall NETASQ peut gérer les connexions avec les modems de type ADSL (PPTP et PPPoe), RNIS, RTC et modem câble. Il n'est donc plus nécessaire d'avoir un routeur, le firewall peut sans problème le supplanter.

3.4.1.4. Migration d'un serveur du LAN vers la DMZ

Vous désirez mettre à disposition, sur Internet, un serveur qui n'était utilisé auparavant qu'à usage interne. Ce serveur était initialement placé dans votre réseau interne et vous souhaitez le déplacer dans la DMZ afin de l'isoler. Ce serveur possède une adresse IP privée appartenant à la plage d'adresses du réseau interne et il est difficile de changer cette adresse car les applications des postes internes sont configurées pour accéder au serveur par cette adresse.
Solution NETASQ : le firewall peut être configuré en mode hybride. Les interfaces du réseau interne et de la DMZ auront la même adresse IP, donc les machines reliées à ces deux interfaces seront considérées comme faisant partie du même réseau. Mais les flux entre le réseau interne et la DMZ seront filtrés. Vous pouvez alors déplacer le serveur vers la DMZ sans modifier son adresse IP.

> **REMARQUE**
> L'interface externe du firewall pourra avoir une adresse IP appartenant à un plan d'adressage différent (public ou privé).

PARTIE 4 : OBJETS

CHAPITRE 1. INTRODUCTION

4.1.1. Pour ce chapitre, vous devez avoir franchi les étapes

- Partie 2 : Installation, pré-configuration, intégration
- Partie 5 : Configuration réseau

4.1.2. Pour ce chapitre, vous devez connaître

- Les machines et réseaux auxquels vous désirez affecter des droits particuliers
- Les données sur les utilisateurs de votre réseau interne (nom, prénom ...)
- Les protocoles et les services IP que vous allez utiliser

4.1.3. Utilité du chapitre

Ce chapitre vous permet de définir les objets que vous allez utiliser pour la configuration de votre filtrage et de votre translation d'adresses. D'une part, vous donnez ici une correspondance entre un nom de machine, groupe de machines, réseau, groupe de réseaux et son adresse IP. D'autre part, vous donnez une correspondance entre un nom de service, son protocole et son numéro de port. Vous pouvez créer des groupes de services si certaines règles s'appliquent à plusieurs services. Cela permet ainsi de simplifier l'édition des règles. Vous pourrez aussi définir ici les comptes utilisateurs pour l'authentification. Les informations sur ces comptes sont stockées dans une base LDAP interne au firewall, mais peuvent aussi être stockées dans une base LDAP externe ou avec des informations limitées sur un serveur RADIUS ou une base Active Directory.

4.1.4. Accéder à ce chapitre

Accédez au menu **Objets** de l'arborescence des menus.

Vous devez être connecté avec les privilèges de modification pour pouvoir en effectuer.

NOTE
Avant d'effectuer toute modification importante sur votre produit UTM NETASQ, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez revenir dans la configuration précédente. *(Voir Partie 18 : Sauvegarde).*

CHAPITRE 2. PRESENTATION

La base d'objets est utile dans la plupart des modules de configuration du NETASQ UNIFIED MANAGER. Elle est généralement rappelée dans les autres modules pour créer, supprimer, sélectionner des machines, des utilisateurs, des plages d'adresses, des réseaux, des protocoles, des services, des groupes d'objets.

Les objets peuvent être :

- Des utilisateurs (avec login et mots de passe pour authentification)
- Des machines (correspondance entre un nom d'objet et une adresse IP)
- Des plages d'adresses
- Des réseaux (adresse réseau et masque de sous-réseau)
- Des protocoles (correspondance entre le nom de protocole et son n°)
- Des services (nom de service, port et protocole)
- Des groupes (machines et/ou réseaux, plages, groupes d'utilisateurs, groupes de services)

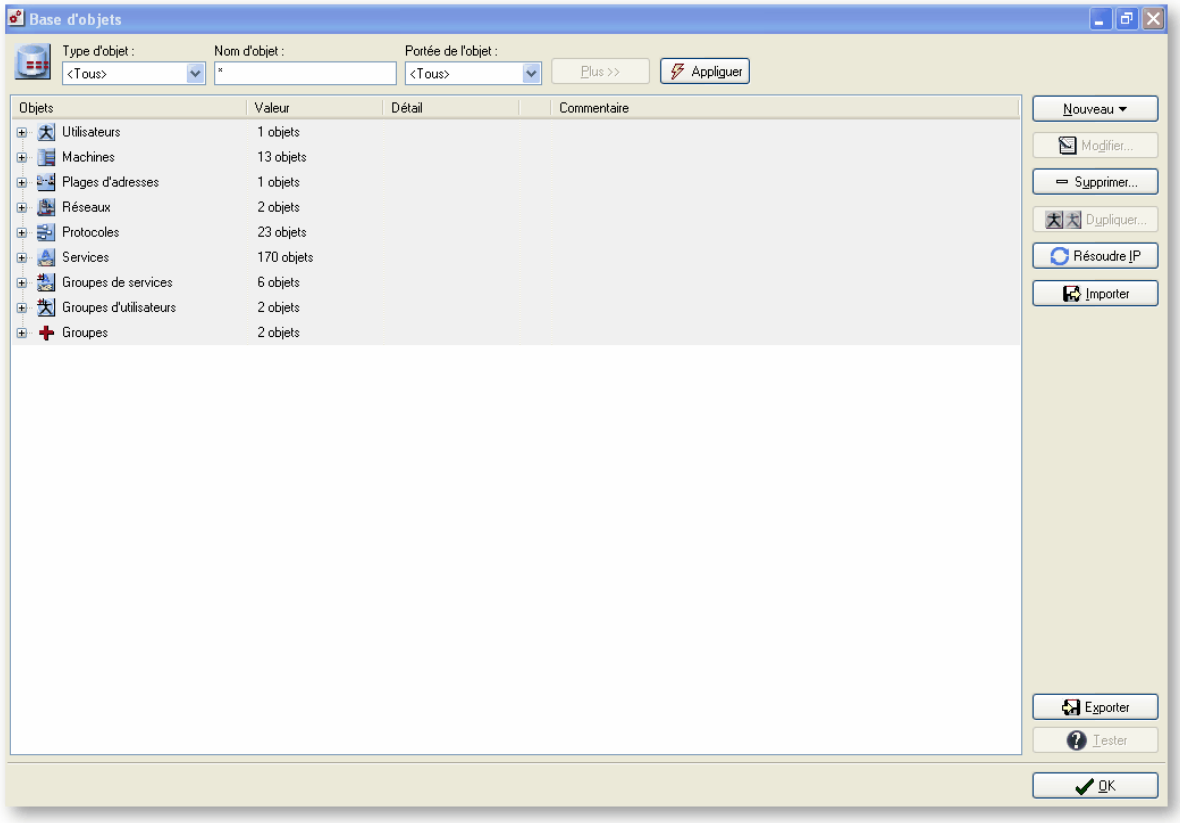


Figure 34 : Base d'objets

La fenêtre de définition des objets est divisée en trois parties :

- Une zone de tri et de sélection au haut de la fenêtre
- Une barre d'actions, sur la partie droite de la fenêtre
- Une grille de définition des objets

4.2.1. Zone de tri et de sélection

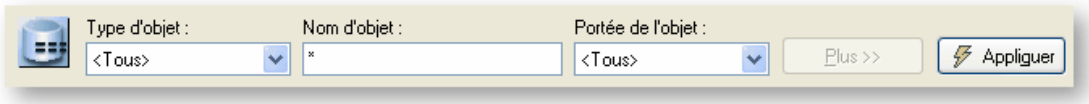


Figure 35 : Zone de tri et de sélection

La zone de tri et de sélection située au haut de la fenêtre se présente différemment selon le type d'objet sélectionné. A l'ouverture, tous les objets sont listés dans la grille de définition des objets mais lorsque vous sélectionnez un objet à l'aide du menu déroulant situé en haut à gauche, une zone de tri et de sélection apparaît.

Cette zone de tri et sélection permet une recherche rapide d'un objet parmi la liste des objets configurés sur votre firewall.

4.2.1.1. Les boutons de tri et de sélection

Cette zone contient un certain nombre de boutons d'actions qui vous permettent de valider et d'afficher votre recherche.

Type d'objet	Sélection du type d'objet affiché parmi : "Tous", "Utilisateurs", "Machines", "Plages d'adresses", "Réseaux", "Protocoles", "Services", "Groupes de services", "Groupes d'utilisateurs", "Groupes".
Nom d'objet	Recherche d'un objet contenant la chaîne de caractères indiquée.
Portée de l'objet	3 options sont possibles : "Tous", "Local" et "Global".
Plus/Moins	Affichage ou masquage de la zone de tri et sélection.
Appliquer	Appliquer la recherche.

4.2.1.2. La barre d'actions

Les actions permises par la barre d'actions sont indiquées dans le tableau suivant :

AVERTISSEMENTS

1) L'importation d'objets ne dispose pas de mécanismes de protection pour assurer l'intégrité de la configuration importée (le fichier importé peut contenir des informations volontairement erronées). Il est donc de la responsabilité de l'administrateur de valider la cohérence de l'ensemble de la base objet importée avant son envoi sur le firewall.
2) De plus il n'est pas recommandé de faire des sauvegardes de la base objets par ce moyen, préférez pour cela les fonctions de sauvegarde de configuration (qui disposent de mécanismes cryptographiques).

Figure 36 : Barre d'actions

Nouveau	Choisissez le type d'objet que vous désirez créer et l'assistant de création correspondant apparaît.
Modifier…	Modifie l'objet sélectionné.
Supprimer…	Supprime l'objet sélectionné.
Dupliquer…	Duplique l'objet sélectionné.
Résoudre IP	Effectue la résolution des adresses IP, des machines de type "manuelle".
Importer	Importe une liste d'objets.
Exporter	Exporte la liste des objets.
Tester	Effectue un test de l'utilisation de l'objet sélectionné. (*Cf.Partie 4 : Références à l'objet*).
OK	Ferme la fenêtre de configuration des objets. Une modification sur un objet est automatiquement prise en compte.

4.2.1.3. Références à l'objet

Lorsqu'on clique sur le bouton **Tester** ou lorsqu'un objet (sauf utilisateurs) est supprimé de la base d'objets, un écran de référence à l'objet apparaît. Cet écran pointe les différents modules qui utilisent dans leur configuration l'objet sélectionné.

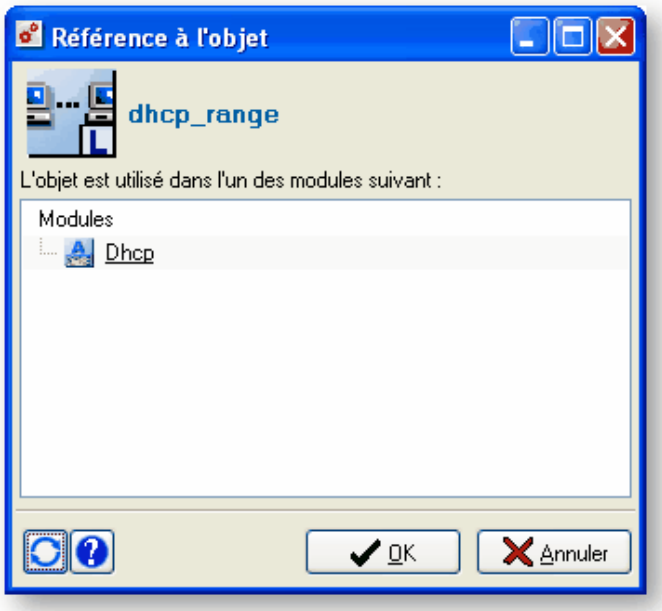


Figure 37 : Référence à l'objet

L'écran de référence à l'objet reprend en premier lieu le nom de l'objet puis indique, sous forme de liens directs, les différents modules dans lesquels l'objet est utilisé. Lorsque l'on clique sur un module listé par l'écran de référence, le menu de configuration associé est affiché permettant une visualisation et/ou une modification de la configuration avant suppression de l'objet.
L'écran de référence à l'objet possède une barre d'actions constituée de quatre boutons d'actions :

	Actualise l'affichage proposé par l'écran de référence à l'objet.
	Affiche le retour textuel exact du firewall indiquant précisément dans chaque module l'endroit où est utilisé l'objet.

Exemples
module=Filter slot=10 line=1
module=Filter slot=10 line=2
module=Route section=Default

OK	Fermeture de l'écran référence de l'objet avec validation des changements.
Forcer	Le bouton **OK** de l'écran référence de l'objet devient **Forcer** lors de la suppression d'un objet. Cette action supprime l'objet sélectionné malgré son utilisation dans les modules cités.
Annuler	Fermeture de l'écran référence de l'objet sans validation des changements.

AVERTISSEMENT
Les modifications réalisées par l'intermédiaire de l'écran de référence à l'objet, dans les modules utilisant l'objet analysé, ne peuvent pas être annulées par un clic sur le bouton **Annuler** de l'écran.

4.2.3. Remarques

Les objets prennent la couleur des interfaces dont ils dépendent. Toutes les modifications concernant les utilisateurs (LDAP) sont immédiatement appliquées.

Si un objet utilisé dans la configuration du produit UTM est modifié, cette modification est automatiquement prise en compte par l'UTM et les slots utilisant cet objet sont automatiquement réactivés.

AVERTISSEMENT
La réactivation d'un slot de NAT entraîne la perte des connexions actives.

CHAPITRE 3. UTILISATEURS

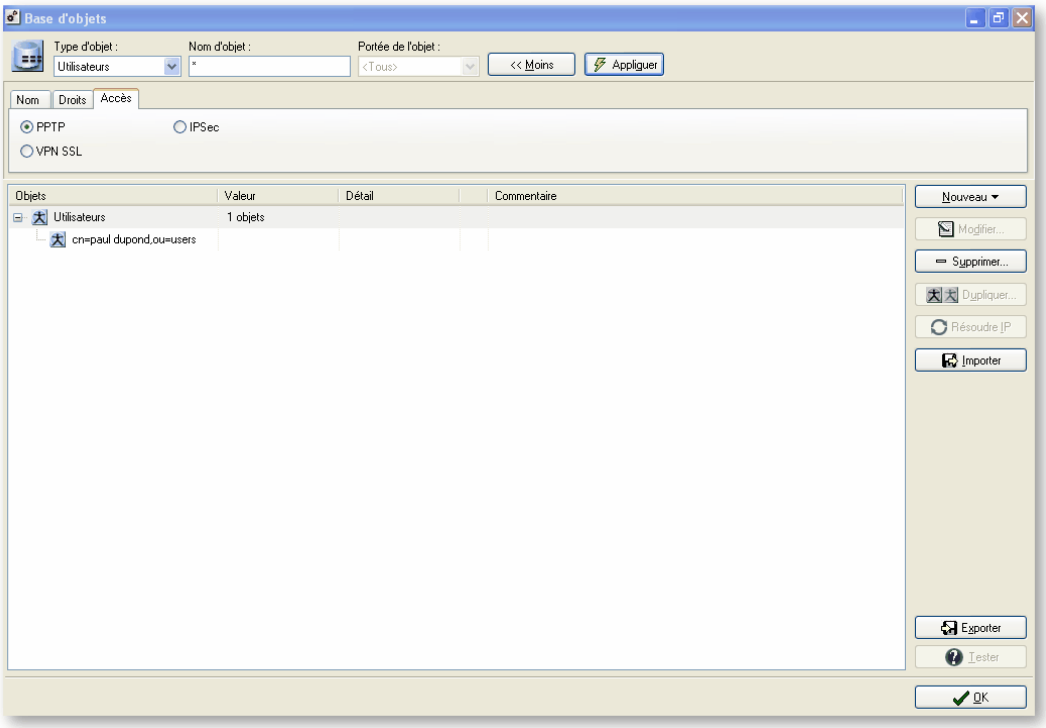


Figure 38 : Base d'objets - Accès

Le service d'authentification des utilisateurs nécessite la création de comptes utilisateurs au niveau du firewall. Ces comptes contiennent l'ensemble des informations relatives à ces utilisateurs :

- Nom
- Prénom
- Identifiant de connexion
- Mot de passe
- E-mail (optionnel)
- Numéro de téléphone (optionnel)
- Description (optionnel)
- Méthode d'authentification de l'utilisateur
- Droits d'accès VPN et droits d'administration

- Clé pré-partagée pour le VPN
- Mot de passe PPTP
- Certificat x509

4.3.1. Création d'un utilisateur

4.3.1.1. Assistant de création d'un utilisateur

La création d'un utilisateur (bouton **Nouveau\Utilisateur**) est réalisée au moyen d'un assistant. Cet assistant en une étape vous demande de renseigner les informations suivantes :

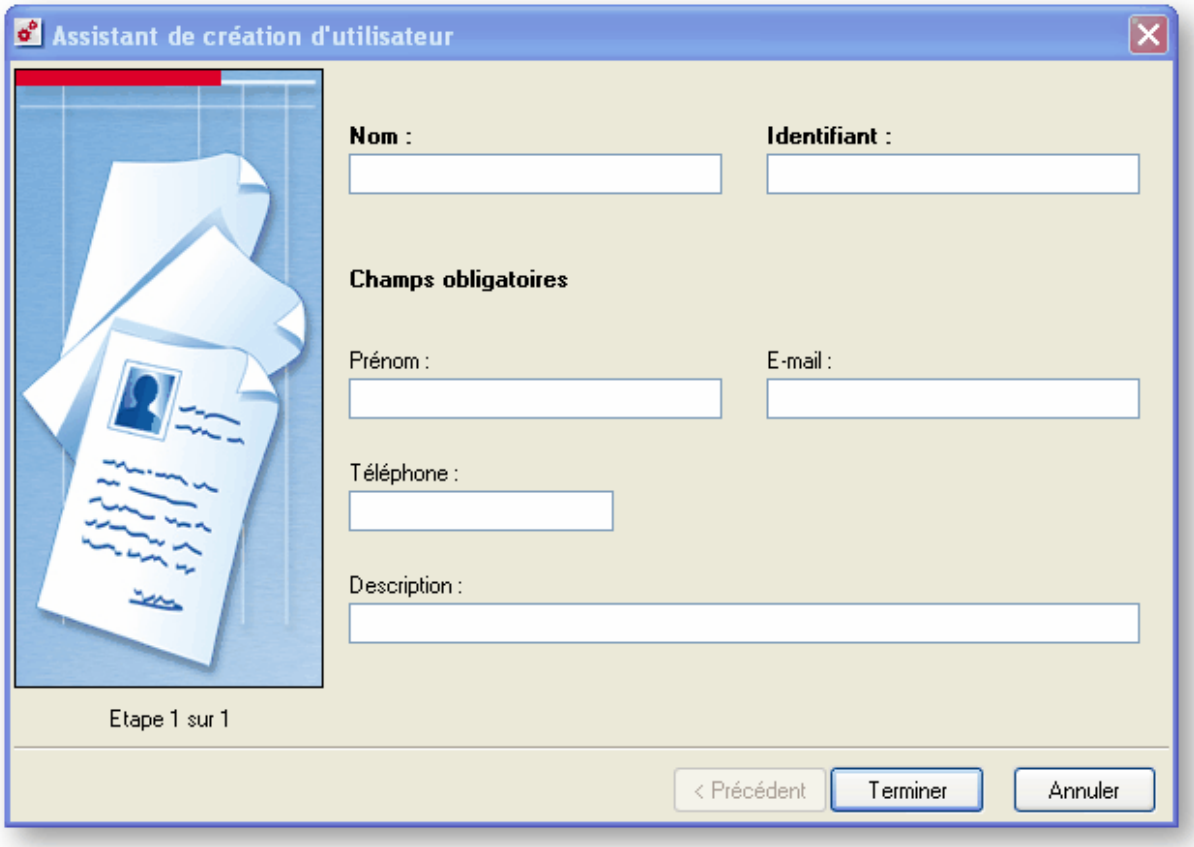


Figure 39 : Assistant de création d'un utilisateur

- Champs obligatoires (indiqués en gras) : Nom et Identifiant (login utilisé pour l'authentification de l'utilisateur).
- Champs facultatifs : Prénom, E-mail, Téléphone (courte chaine modifiable), Description (courte chaine modifiable).

> **AVERTISSEMENT**
> Si vous désirez générer un certificat x509 pour cet utilisateur vous devez forcement indiquer son adresse mail. Cette information sera utilisée dans le certificat.

L'adresse mail est également nécessaire si l'utilisateur désire se connecter au firewall en VPN avec un client mobile IPSEC.

Une fois la configuration avec l'assistant effectuée ou lorsque vous souhaitez modifier la fiche d'un utilisateur (sélectionnez l'utilisateur dans la grille d'objets, puis cliquez sur le bouton **Modifier**) les informations relatives à la configuration de l'utilisateur sont affichées dans une fenêtre comportant cinq onglets.

REMARQUE
Toutes les modifications concernant les utilisateurs sont immédiatement appliquées.

4.3.1.2. Onglet « Utilisateur »

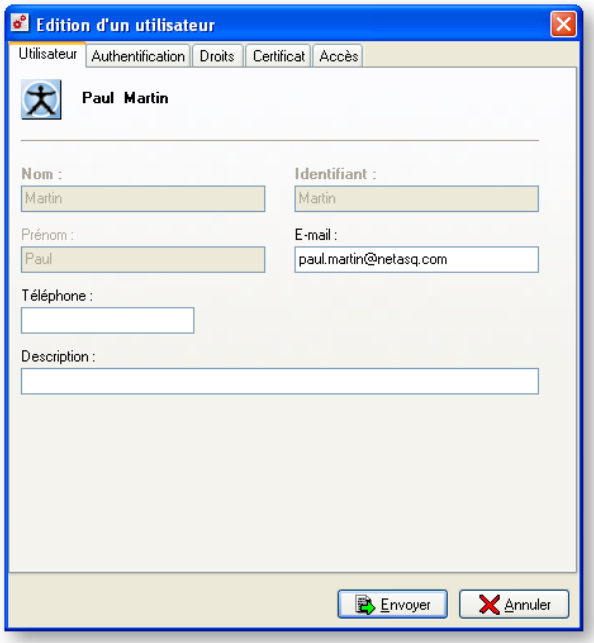


Figure 40 : Edition d'un utilisateur - Utilisateur

Cet onglet permet de modifier les informations de base sur l'utilisateur. Seules les informations suivantes peuvent être modifiées :

- E-mail (facultatif)
- Téléphone (facultatif)
- Description (facultatif)

4.3.1.3. Onglet « Authentification »

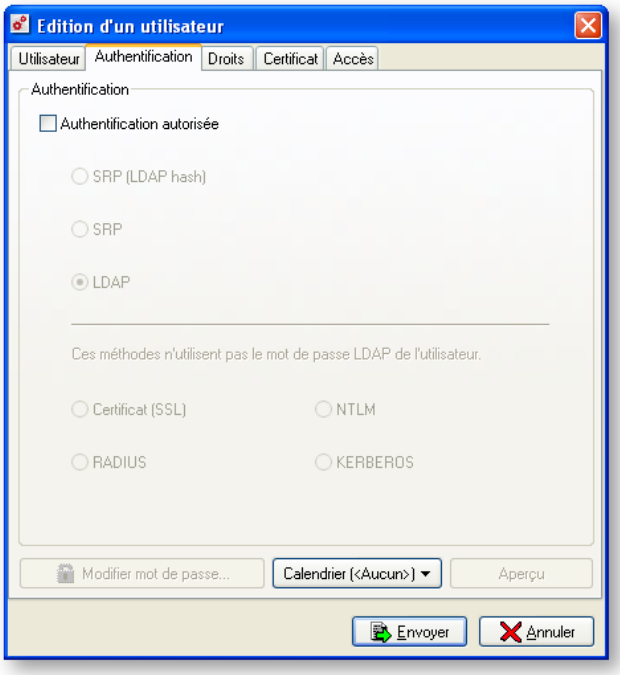


Figure 41 : Edition d'un utilisateur - Auhentification

Cet onglet donne les éléments de configuration pour l'authentification. Sélectionner l'option **Authentification autorisée** permet d'avoir accès aux options de cet écran. Cette option permet de spécifier si l'utilisateur est autorisé ou non à s'authentifier sur le firewall.
S'il est autorisé à s'authentifier, il utilisera l'une des méthodes suivantes :

- **SRP (LDAP hash)**, utilisation particulière de la méthode SRP. Cette méthode évite d'utiliser les champs identifiant, mot de passe stockés dans la fiche LDAP. Ce sont les identifiants, mots de passe utilisateur de la base LDAP qui sont utilisés.

> **AVERTISSEMENT**
> Cette méthode est un peu moins sécurisée que le SRP natif (lors d'un accès à la base LDAP, le mot de passe du SRP natif est plus résistant à la méthode de force brute que le mot de passe du SRP Hash. Par contre, les échanges réseau sont tout aussi sécurisés pour les deux méthodes) mais elle permet de réutiliser le mot de passe LDAP classique (champ "userpassword").

- **SRP** : utilisation de la méthode sécurisée SRP native, pour le calcul du mot de passe. Avec cette méthode, des champs sont ajoutés dans la fiche LDAP de l'utilisateur avec son identifiant, mot de passe.
- **LDAP** : le mot de passe transite non modifié dans un tunnel SSL (Https). (Cette méthode n'est pas conseillée).

Modifier le mot de passe de l'utilisateur en cliquant sur le bouton **Modifier mot de passe**. Ce mot de passe sera utilisé pour l'authentification au travers du firewall et si l'utilisateur désire se connecter au firewall pour lire ou modifier la configuration.

L'écran suivant s'affiche lorsque vous cliquez sur ce bouton :

Figure 42 : Mot de passe d'authentification

Le champ "Méthode de hachage" vous permet changer la méthode de hachage appliquée au mot de passe (*Cf. Partie 12 : Authentification*).

Les options proposées sont les suivantes :

- Pas de modification : vous permet de conserver la méthode déjà utilisée
- NONE
- MD5
- SMD5
- SHA
- SSHA
- CRYPT

Méthodes sans mot de passe LDAP

- **Certificat (SSL)** : utilise le certificat de l'utilisateur stocké dans la base LDAP et installé sur le poste client.
- **RADIUS** : utilise une authentification via un serveur RADIUS (*Cf. Partie 12 : Authentification*)
- **NTLM** : utilise une authentification via un serveur NTLM (*Cf. Partie 12 : Authentification*)
- **KERBEROS** : utilise une authentification via un serveur Kerberos (*Cf. Partie 12 : Authentification*)

Calendrier

Le bouton **Calendrier (<Aucun>)** permet de spécifier les périodes d'authentification permises pour l'utilisateur. Dans ce calendrier, lorsque l'authentification n'est pas permise, il est impossible pour l'utilisateur de s'authentifier. (*Cf. Partie 7 : Politique/Chapitre 3 : Programmation horaire).*

4.3.1.4. Onglet Droits

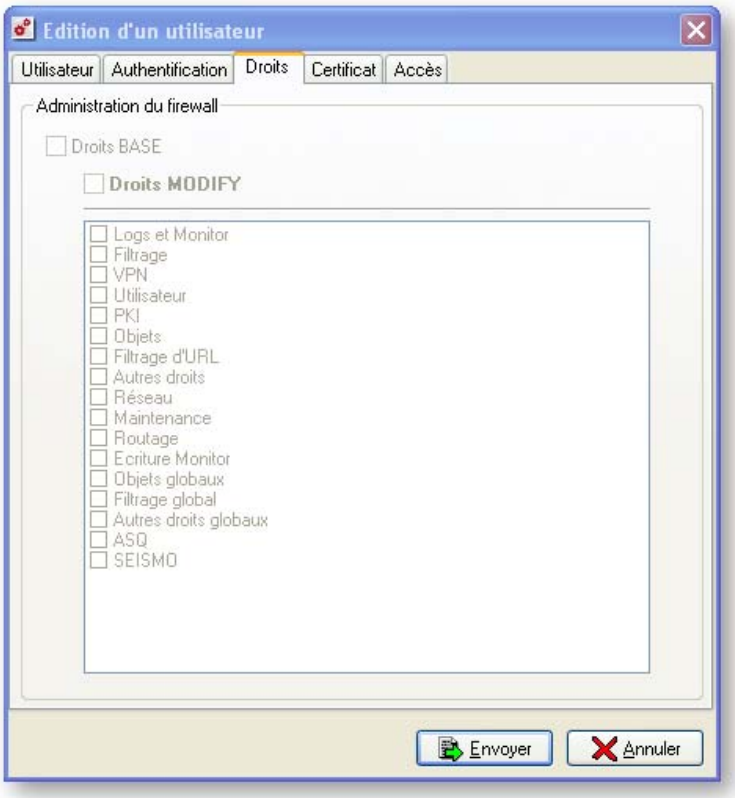


Figure 43 : Edition d'un utilisateur - Droits

Cette section vous permet de définir les droits de lecture et de modification de la configuration du firewall.

> **REMARQUE**
> Pour accorder des privilèges à un utilisateur, il faut avoir préalablement coché "Authentification autorisée" dans l'onglet **`Authentification.`**

Liste des droits :

- Droits BASE, nécessaire pour un utilisateur désirant se connecter à un firewall (droits de lecture).
- Droits MODIFY: permet d'avoir le droit de modifier la configuration du firewall.

Après avoir déterminé les droits de lecture et/ou de modification, il suffit de cocher les privilèges :

- **Logs et Monitor** : droit de consultation des traces
- **Filtrage** : droit de consultation des règles de filtrage
- **VPN** : droit de consultation des configurations VPN
- **Utilisateur** : droit de consultation des informations sur les utilisateurs
- **PKI** : droit de consultation des informations de la PKI
- **Objets** : droit de consultation des objets
- **Filtrage d'URL** : droit de consultation du filtrage d'URL
- **Autres droits**
- **Réseau** : droit d'édition de la configuration réseau (interfaces, bridges, dialups, VLANs et configuration dynamique du DNS)

- **Maintenance** : droit permettant les opérations de maintenance (sauvegarde, restauration, mise à jour, arrêt et redémarrage du firewall, modification de la fréquence de mise à jour de l'antivirus et mise à jour de l'antivirus et enfin les actions liées au RAID dans le moniteur)
- **Routage** : droit d'édition du routage sur les firewalls (route par défaut, routes statiques et réseaux de confiance)
- **Ecriture Monitor** : droit permettant d'effectuer certaines opérations nécessitant des droits de modification sans pour autant bloquer les privilèges de modification "généraux"
- **Objets globaux, Filtrage global, Autres droits globaux** : droits permettant d'accéder à la configuration globale
- **ASQ** : droit de consultation de la configuration de l'ASQ
- **SEISMO** : droit de consultation et/ou de modification des vulnérabilités

4.3.1.5. Onglet Certificat

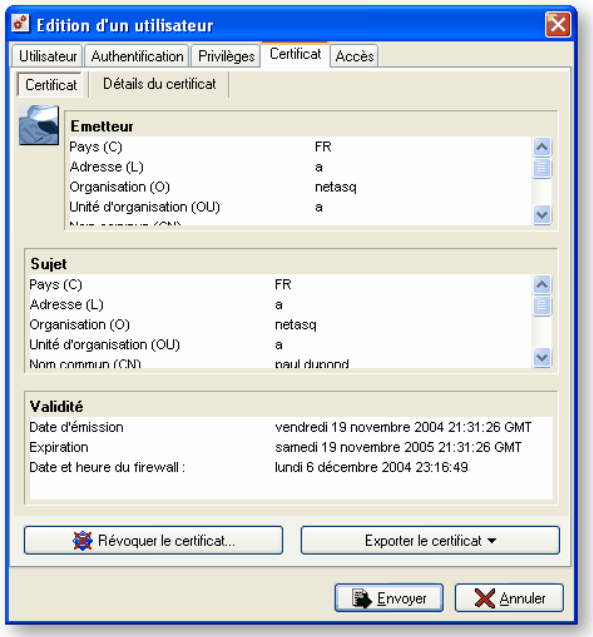


Figure 44 : Edition d'un utilisateur - Certificat

Génération d'un certificat

Cet onglet vous permet de gérer le certificat x509 de l'utilisateur.

Ce certificat peut servir dans deux cas : authentification via SSL et accès en VPN au firewall avec un client mobile IPSEC. Ce certificat peut aussi être utilisé par d'autres applications.

Pour créer un certificat, (vous devez avoir, au préalable, configuré la PKI interne (*Cf. Partie 12 : Authentification*) référez-vous à la procédure suivante :

1 Cliquez sur le bouton **Créer le certificat.** L'écran suivant s'affiche :

Figure 45 : Créer un certificat utilisateur

2 Saisissez le mot de passe que vous avez affecté à l'autorité de certification (CA) du firewall.

3 Indiquez ensuite le mot de passe choisi pour le conteneur PKCS#12 de l'utilisateur. Ce conteneur pourra être exporté sur la machine de l'utilisateur.

Une fois le certificat de l'utilisateur généré, le contenu de celui-ci s'affiche.

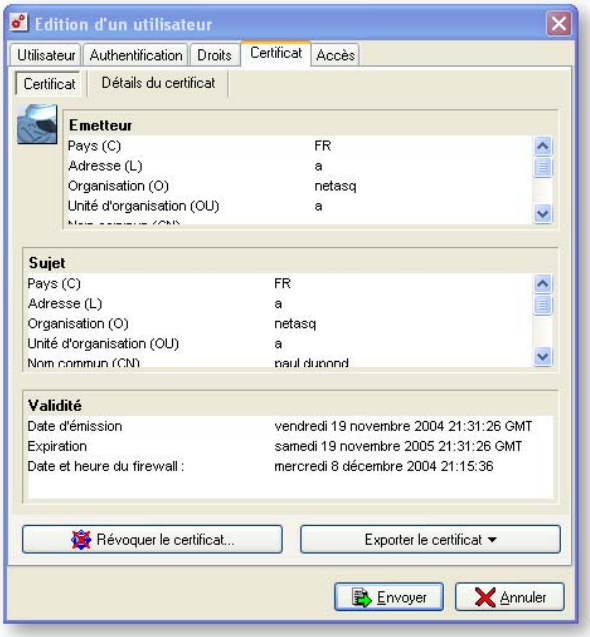


Figure 46 : Edition d'un utilisateur - Certificat

Vous pouvez alors visualiser tous les champs du certificat (Informations relatives à l'autorité de certification intégrée au firewall NETASQ, informations relatives à l'utilisateur et période de validité du certificat).
En cliquant sur l'onglet **`Détails du certificat`**, vous pourrez visualiser le contenu brut du certificat.

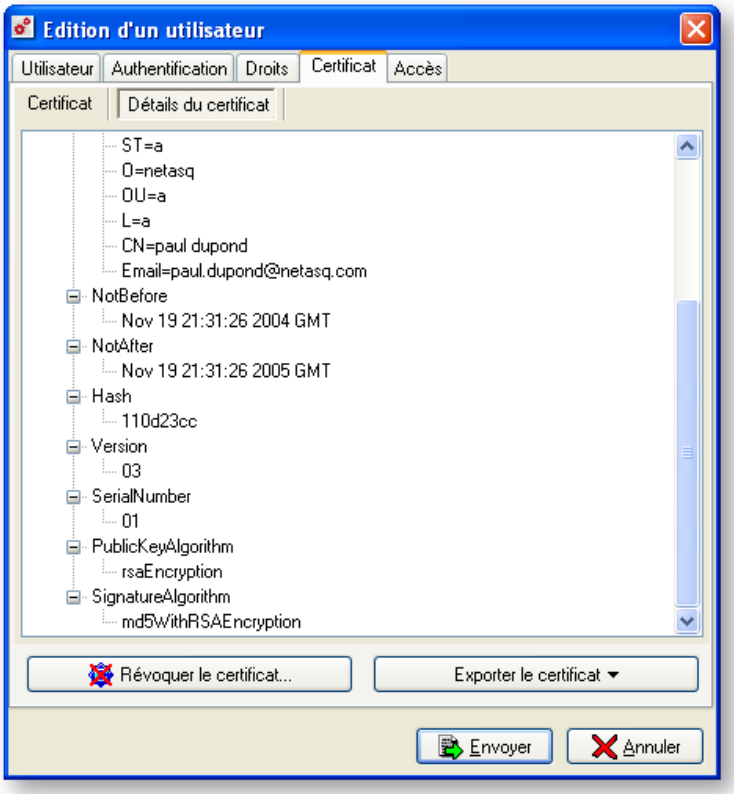


Figure 47 : Edition d'un utilisateur - Détails du certificat

Révocation d'un certificat

Le certificat d'un utilisateur peut être révoqué (annulé) à l'aide du bouton **Révoquer le certificat…**. Dans ce cas, l'utilisateur ne pourra plus s'authentifier sur le firewall (si la méthode d'authentification choisie est SSL), ni réaliser de VPN (si la méthode d'authentification est basée sur les certificats). Il ne pourra plus utiliser les applications intégrées dans la PKI (utilisant les certificats x509 de la PKI du firewall).

AVERTISSEMENT

Pour que la révocation prenne effet, il faut régénérer la CRL (*Certificate Revocation List*). (*Cf. Partie 12 : Authentification*). Si vous avez d'autres applications qui utilisent les certificats de la PKI du firewall, il faudra alors leur distribuer cette CRL. Les certificats générés par la PKI contiennent un lien vers cette CRL.

Exporter le certificat

Vous pouvez enregistrer le certificat généré. Ainsi vous pouvez l'installer sur le poste utilisateur.

Le certificat peut être exporté au format PKCS#12 (recommandé) ou au format **.der**. Le conteneur PKCS#12 contient la clé privée et le certificat utilisateur ainsi que le certificat de l'autorité de certification alors que le format **.der** ne contient que le certificat de l'utilisateur.

Installation d'un certificat sous Windows

1. Copier le certificat ou le conteneur PKCS#12 en local, sur la machine utilisateur.
2. Ouvrez le fichier. L'installation du certificat débute.
3. Le mot de passe du conteneur PKCS#12 défini lors de la création du certificat est demandé pour terminer l'installation du certificat. Le certificat est alors ajouté aux certificats déjà installés sur le poste utilisateur.

4.3.1.6. Accès VPN

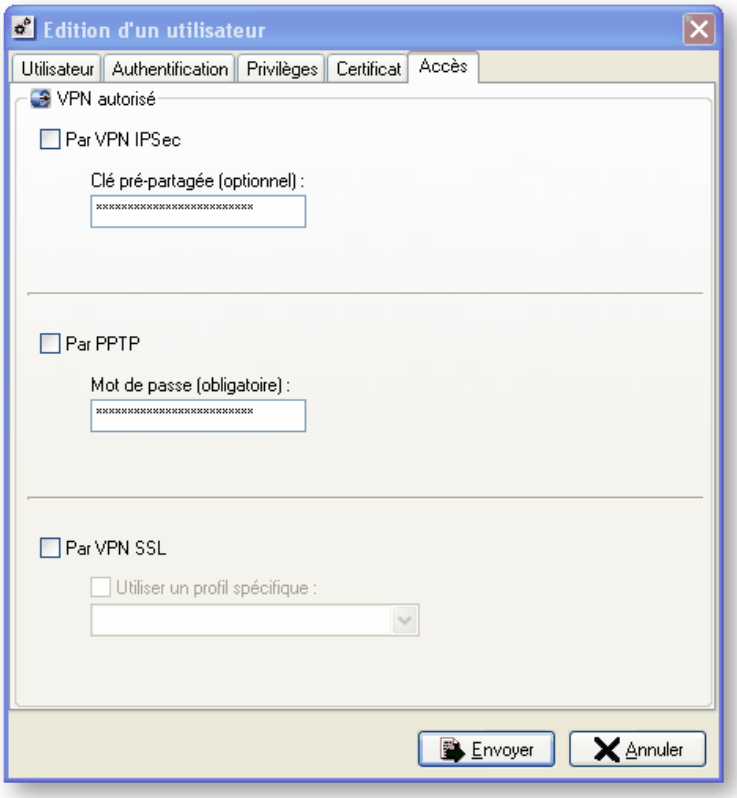


Figure 48 : Edition d'un utilisateur - Accès

Cet onglet vous permet de définir les accès VPN IPSec, PPTP et VPN SSL.

Clé pré-partagée par VPN IPSEC

Cette clé sera utilisée pour la création d'un tunnel IPSec dynamique avec un client mobile IPSec. Cette même clé devra être indiquée au niveau de la configuration du client mobile de l'utilisateur. (De même, au niveau du client mobile, l'identifiant devra être l'adresse mail de l'utilisateur, définie dans la fiche de l'utilisateur interne au firewall). Ce champ est optionnel, il n'est utilisé que dans le cas d'un tunnel en "clé pré-partagée". Dans le cas contraire, on utilise le certificat de l'utilisateur (plus besoin alors de saisir la clé "pré-partagée"). Dans tous les cas, le tunnel VPN doit être configuré (au niveau du firewall et du client mobile) en mode agressif, avec un identifiant de type user@fqdn (qui sera l'adresse e-mail de l'utilisateur pour le correspondant).

Mot de passe par PPTP

Le mot de passe indiqué ici pourra être utilisé par l'utilisateur lorsqu'il voudra se connecter au firewall en PPTP. (*Cf. Configuration*).

Par VPN SSL

Sélectionnez l'option **Par VPN SSL** pour permettre à l'utilisateur de bénéficier des fonctionnalités de VPN SSL. (*Cf. Partie 8/Chapitre 5 : VPN SSL*). Un profil d'utilisation spécifique à cet utilisateur peut être appliqué s'il a été défini dans la configuration du module VPN SSL, dans le menu de l'arborescence **Vpn\VPN SSL.**

4.3.1.7. Recherche d'un utilisateur

Trois onglets composent cet écran :

- **Nom**
- **Droits**
- **Accès**

Onglet Nom

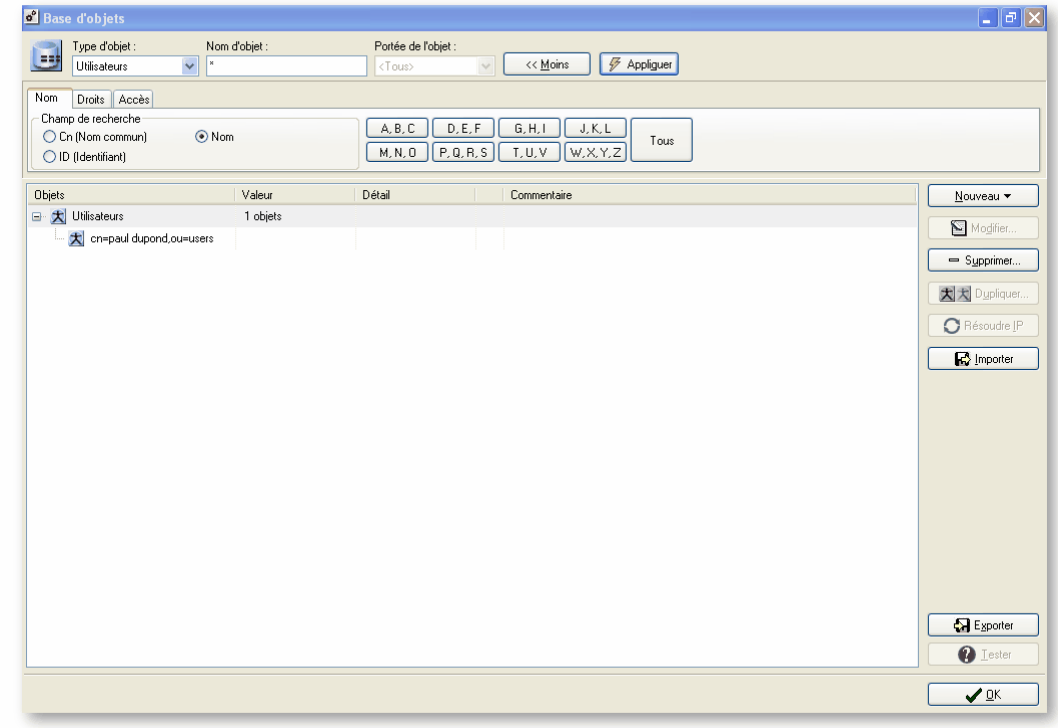


Figure 49 : Base d'objets - Nom

La recherche des utilisateurs peut être effectuée par Cn (Nom commun), par ID (Identifiant) ou par Nom de l'utilisateur.
Les boutons affichant des lettres permettent une recherche affinée.

Onglet Droits

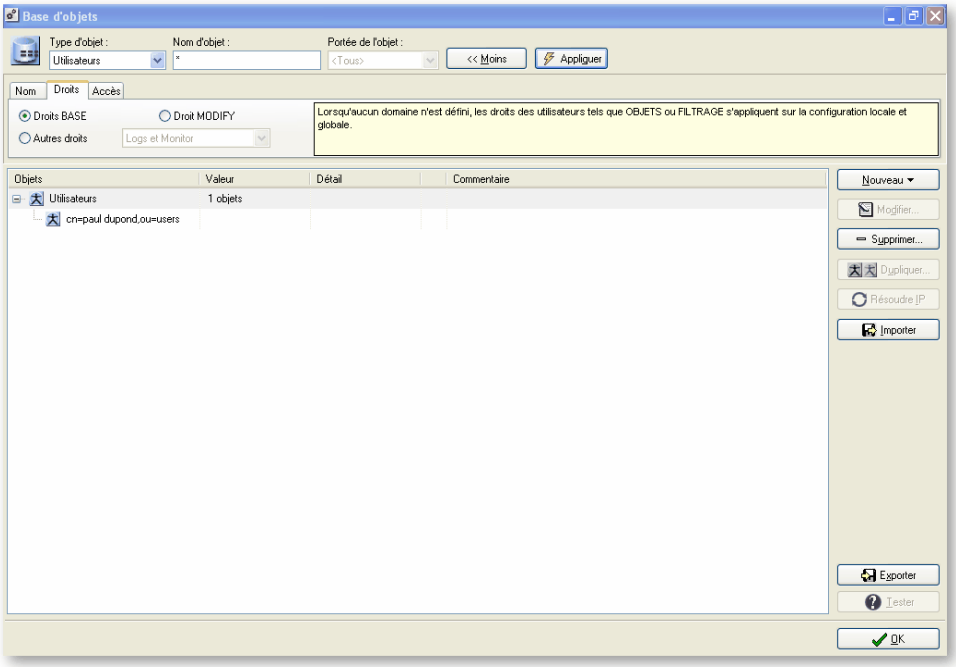


Figure 50 : Base d'objets - Droits

La recherche des utilisateurs peut être effectuée selon les droits qui leur sont accordés.
La recherche peut être affinée selon les droits "BASE", les droits MODIFY (modification) ou d'autres droits.

Onglet Accès

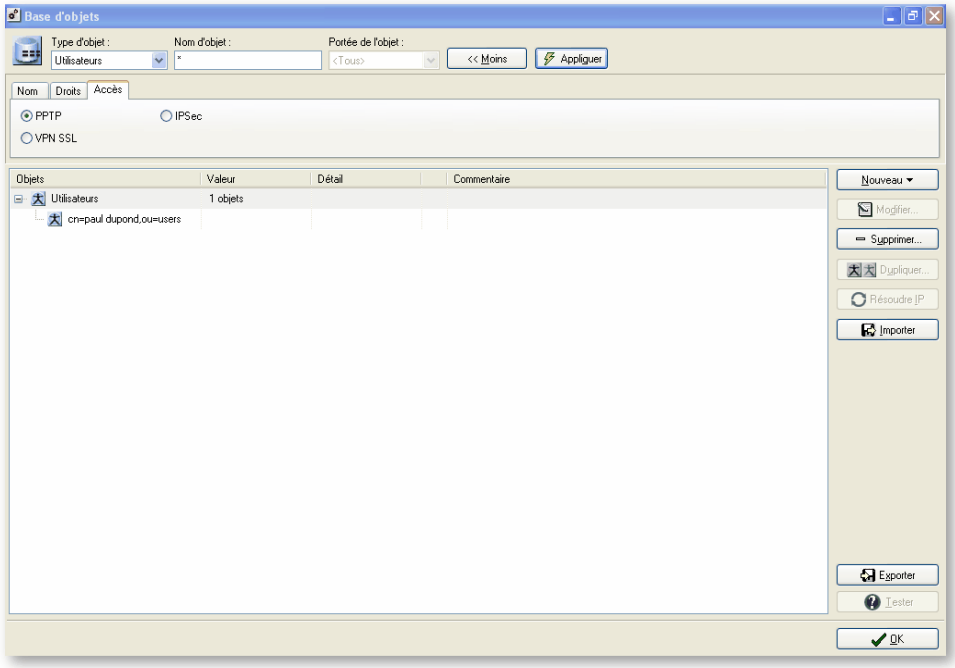


Figure 51 : Base d'objets - Accès

La recherche des utilisateurs peut être effectuée et affinée selon les accès. Vous pouvez rechercher les utilisateurs selon l'accès PPTP, VPN SSL, IPSec.

CHAPITRE 4. MACHINES

La section Machines contient les firewalls, dns, serveurs…
Pour la Haute Disponibilité, un objet a été rajouté en version 7.0 : "Firewall_HA_peer".

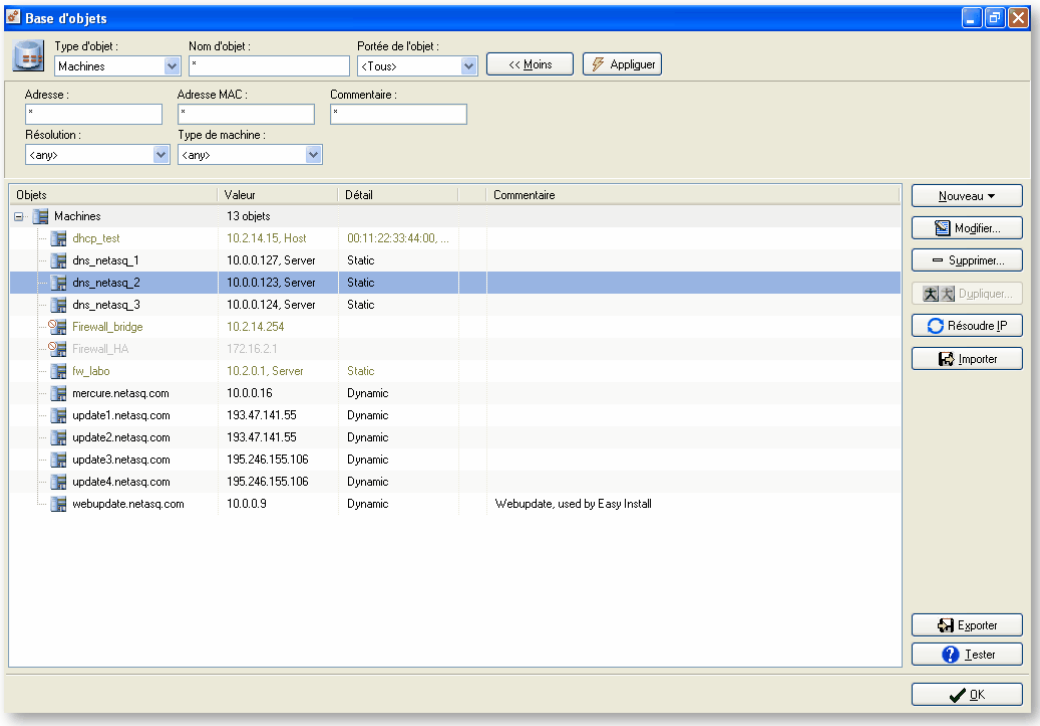


Figure 52 : Base d'objets - Sélection de machines

4.4.1. Assistant de création d'une machine

La création d'une machine (bouton **Nouveau\Machine**) est réalisée au moyen d'un assistant. Cet assistant en une étape vous demande de renseigner les informations suivantes :

Etape 1 :

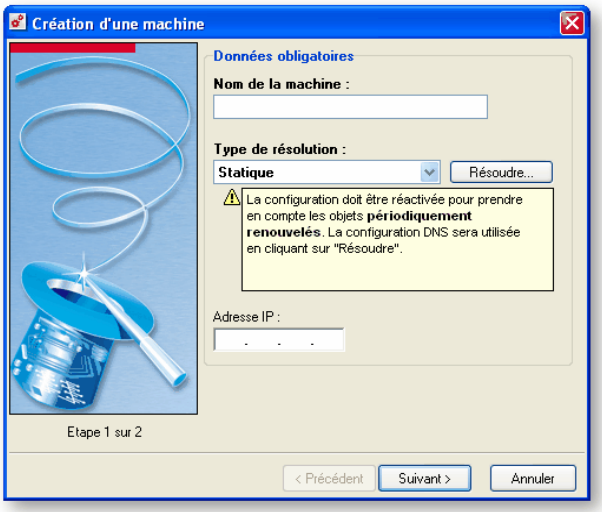


Figure 53 : Création d'une machine – Etape 1

Nom de la machine : Nom que vous associez à l'adresse IP (modifiable).
Type de résolution : Choisir parmi "Statique", "Périodique" ou "Manuelle" En sélectionnant "Statique", l'adresse saisie n'est jamais modifiée.

En sélectionnant "Manuelle", l'adresse pour ces objets est trouvée à l'aide d'une résolution DNS effectuée manuellement depuis le Manager.

En sélectionnant "Périodique", la résolution DNS est faite par le firewall de manière périodique (toutes les 5 minutes). Les fonctionnalités utilisant ces objets ne gèrent pas l'actualisation des données (réactivation manuelle du slot de filtrage nécessaire pour prendre en compte les modifications des objets).
Adresse IP : Adresse IP de la machine.

Etape 2

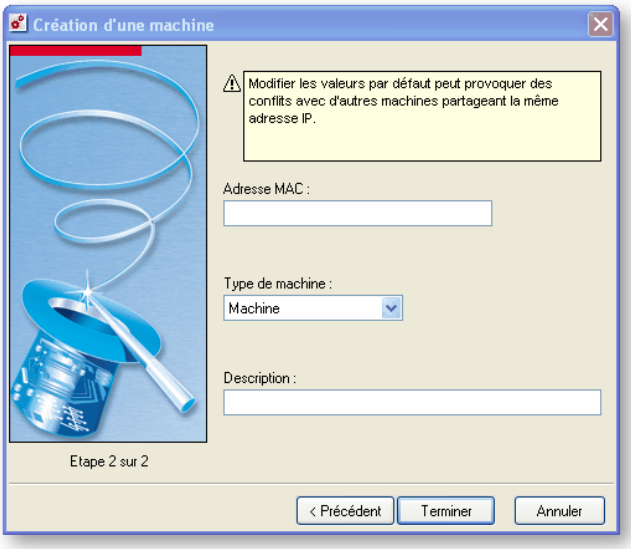


Figure 54 : Création d'une machine - Etape 2

Adresse MAC : Adresse MAC de la machine. Spécifier cette valeur vous permet d'associer une adresse MAC et une adresse IP afin d'éviter l'usurpation de la machine.
Type de machine : Champ de type informationnel vous permettant d'effectuer un niveau de recherche supplémentaire. Vous pouvez choisir parmi : "Machine", "Serveur" ou "Routeur".

NOTE
La saisie du type "Global" ou "Local" d'une machine n'est possible qu'en création.

Description : Commentaires que vous voulez associer à cet objet.

4.4.2. Modification d'une machine

Cliquez sur le bouton **Modifier** pour modifier l'objet. Si vous possédez des slots de filtrage, de filtrage d'URL, de VPN ou de translation d'adresses associés à cet objet, une fenêtre d'informations vous demande si vous voulez réactiver ces slots et prendre en compte immédiatement cette modification. Les slots pour lesquels l'objet est utilisé sont cochés, par défaut, mais vous pouvez désélectionner un type de slot afin de ne pas le réactiver.

AVERTISSEMENT
Le slot VPN n'est jamais coché même si l'objet est utilisé. Il faudra donc le sélectionner manuellement. La réactivation d'un slot de NAT entraîne la perte des connexions actives.

La résolution dynamique DNS des objets NETASQ n'a pas été conçue pour la modification des politiques de sécurité présentes sur les firewalls. En effet étant donné que cette résolution dépend d'un équipement externe au firewall, celui-ci ne peut en aucun cas valider dynamiquement les modifications de la politique de sécurité. Le contournement de ce mécanisme doit être réalisé par l'administrateur (duplication de la politique de sécurité et activation alternée de deux slots par exemple) avec les incidences que cela entraîne (activation d'une politique de sécurité compromise).

4.4.3. Suppression d'une machine

La suppression d'un nom d'objet entraîne l'affichage du message suivant :

"Supprimer l'objet "xxxx" ?"

Il existe des machines préconfigurées : "Firewall_in", "Firewall_out", "Firewall_dmz", "Firewall_bridge", "Firewall_vlan" correspondent aux adresses IP de l'interface interne, externe, DMZ, pont et vlan du firewall NETASQ. Ces adresses ne sont jamais modifiables dans la partie configuration des objets.

4.4.4. Recherche d'une machine

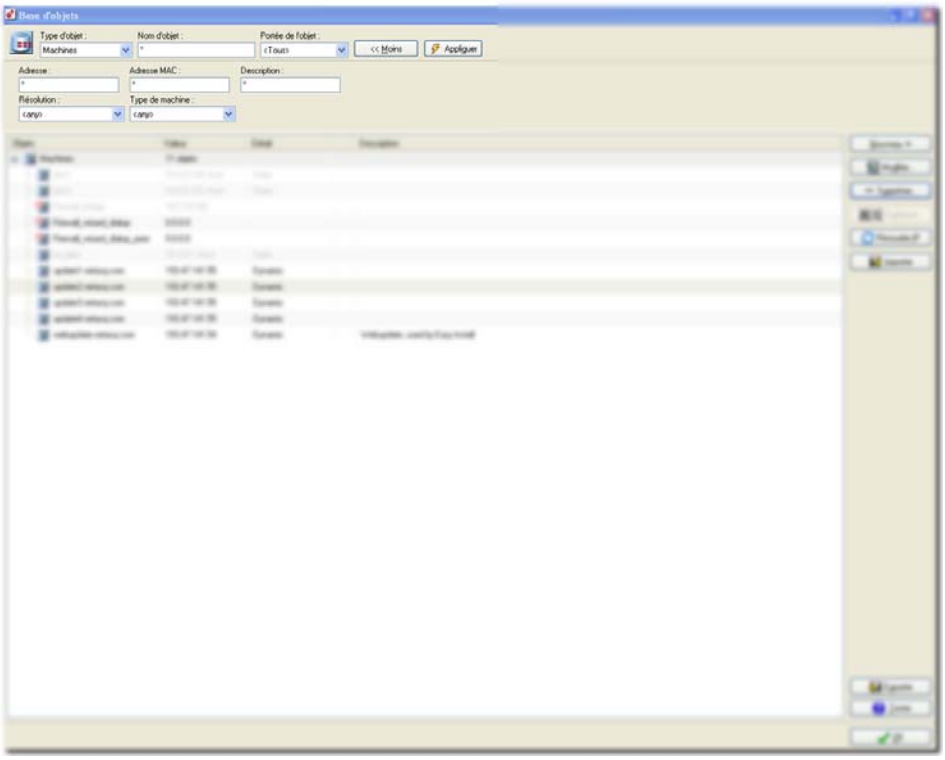


Figure 55 : Recherche d'une machine

Les recherches peuvent être effectuées à l'aide des filtres suivants :

- Adresse
- Adresse MAC
- Description
- Résolution
- Type de machine

CHAPITRE 5. PLAGE D'ADRESSES

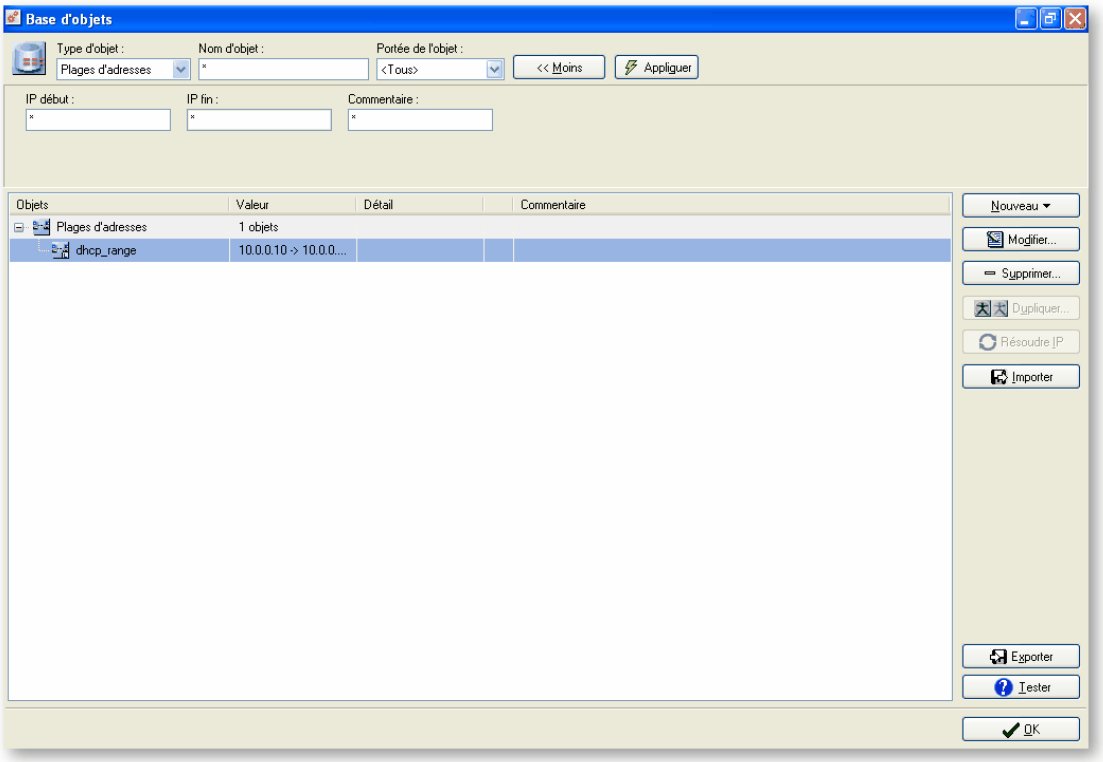


Figure 56 : Base d'objets - Plages d'adresses

Ce menu vous permet de configurer des plages d'adresses. Ces plages d'adresses pourront être utilisées lorsqu'il s'agit de spécifier un pool d'adresses particulières contigu.
Chaque entrée de la liste est composée d'un nom de plage d'adresses, d'une adresse de début, d'une adresse de fin et d'un commentaire.

Cliquez sur le bouton « Modifier » pour modifier l'objet. Si vous possédez des slots de filtrage, de filtrage d'URL, de VPN ou de translation d'adresses associés à cet objet, une fenêtre d'information vous demande si vous voulez réactiver ces slots et prendre en compte immédiatement cette modification. Les slots pour lesquels l'objet est utilisé sont cochés, par défaut, mais vous pouvez désélectionner un type de slot afin de ne pas le réactiver. Attention, le slot VPN n'est jamais coché même si l'objet est utilisé. Il faudra donc le sélectionner manuellement. Ensuite, la réactivation d'un slot de NAT entraîne la perte des connexions actives.

4.5.1. Création d'une plage d'adresses

Pour créer une plage d'adresses, cliquez sur le bouton **Nouveau** et sélectionnez **Plages d'adresses**. L'écran suivant s'affiche :

Figure 57 : Création d'une plage d'adresses

Nom de la plage d'adresses : Nom que vous associez à la plage d'adresses (il n'est pas modifiable).
IP inférieure : Indication de l'adresse IP inférieure.
IP supérieure : Indication de la plage d'adresses supérieure.
Description : Commentaire que vous voulez associer à cette plage d'adresses

REMARQUE
La saisie du type Global ou Local d'une plage n'est possible qu'en création.

CHAPITRE 6. RESEAUX

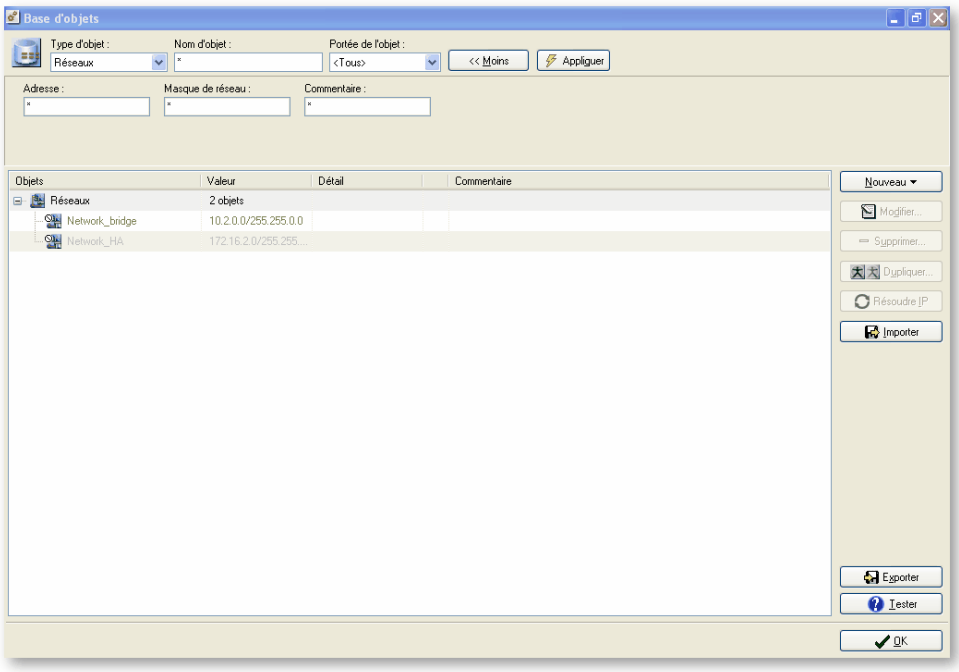


Figure 58 : Base d'objets - Réseaux

Ce menu vous permet de configurer le nom des réseaux et sous-réseaux utilisés dans vos fichiers de configuration. Cette dénomination permet au firewall NETASQ de connaître la correspondance entre un nom de réseau, son adresse IP et son masque de réseau.

Chaque entrée de la liste est composée d'un nom de réseau, de l'adresse IP de ce réseau, de son masque de réseau, de détails et de commentaires sur ce réseau.

AVERTISSEMENT
Le slot VPN n'est jamais coché même si l'objet est utilisé. Il faudra donc le sélectionner manuellement. Ensuite, la réactivation d'un slot de NAT entraîne la perte des connexions actives.

La suppression d'un réseau entraîne l'affichage d'une boîte de dialogue vous invitant à confirmer l'action et à retirer ce réseau des différents groupes de réseau où il était présent.

Il existe des réseaux préconfigurés : "Network_in", "Network_out" et "Network_dmz" correspondent aux réseaux internes, externe et à la DMZ. Si vous utilisez le firewall en mode transparent seul le "Network_bridge" est créé. Dans le cas où vous avez créé des VLAN, les réseaux "Network_vlan" seront créés. Ces noms ne peuvent pas être modifiés.

Pour créer un réseau, cliquez sur le bouton **Nouveau** puis sélectionnez **Réseau**. L'écran suivant s'affiche :

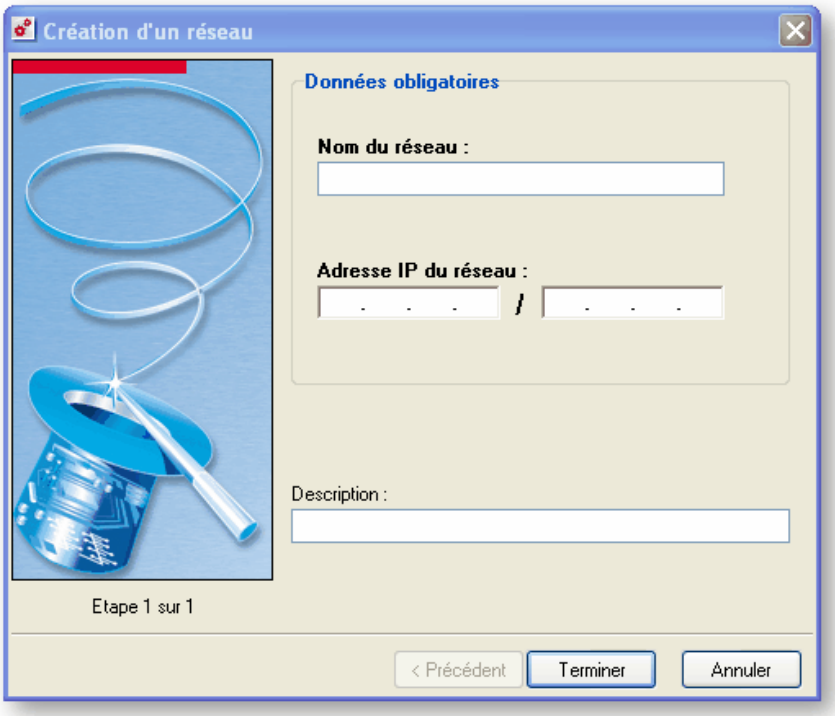


Figure 59 : Création d'un réseau

Nom du réseau (obligatoire) : Nom que vous associez au réseau. (Non modifiable ensuite)
Adresse IP du réseau (obligatoire) : Indication de l'adresse IP du réseau et du masque de sous-réseau.
Description : Commentaire que vous voulez associer à ce réseau.

REMARQUE
La saisie du type Global ou Local d'une plage n'est possible qu'en création.

CHAPITRE 7. PROTOCOLES

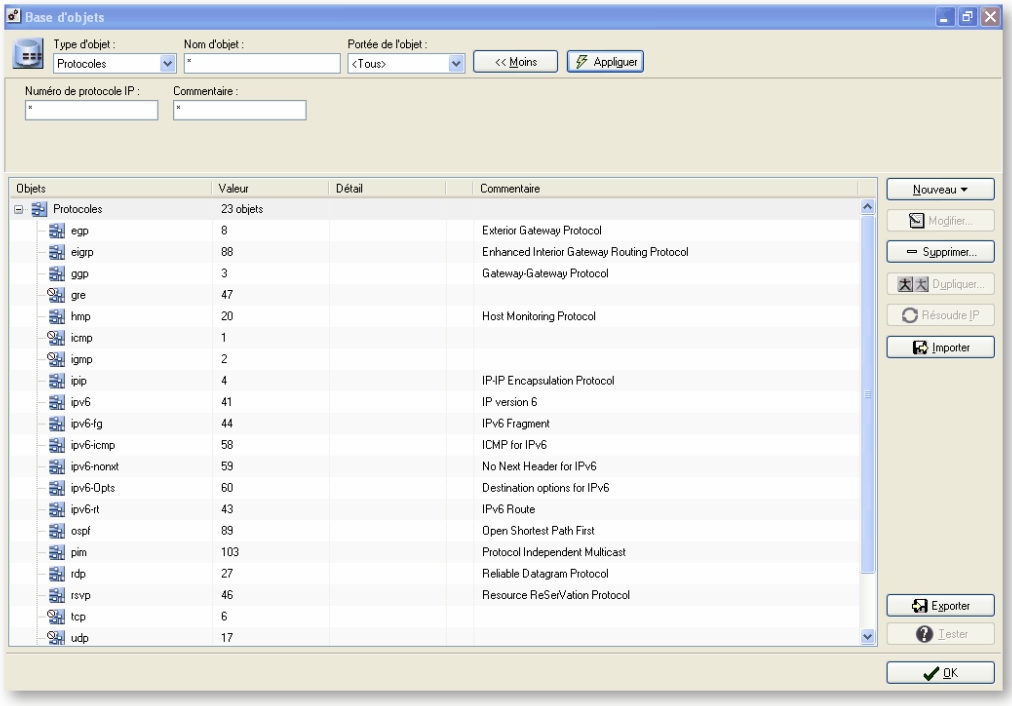


Figure 60 : Base d'objets - Protocoles

Ce menu vous permet de configurer les noms de protocoles fonctionnant sur IP utilisés dans la configuration du filtrage. Cette base renseigne le firewall sur la correspondance entre un nom et le numéro de protocole utilisé par la couche IP. Tout protocole supporté par IP peut être ajouté et géré par le firewall.
Cela vous permet ensuite d'utiliser ces noms dans les règles de filtrage et d'appliquer une politique de sécurité pour ces protocoles.

Pour créer un protocole, cliquez sur le bouton **Nouveau** puis sélectionnez **Protocole**. L'écran suivant s'affiche :

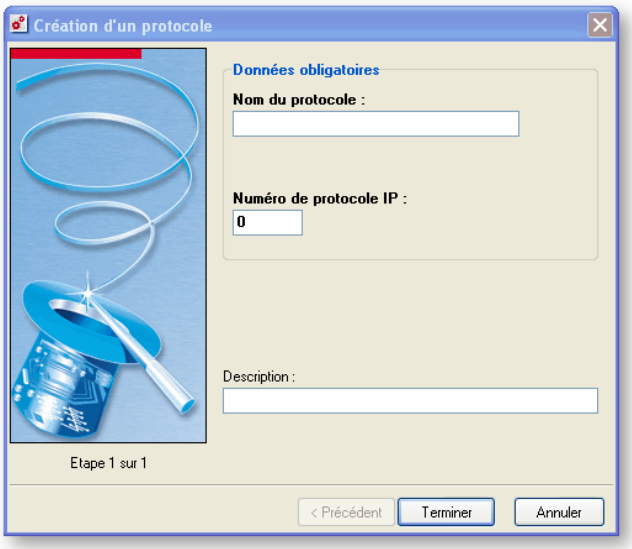


Figure 61 : Création d'un protocole

Nom du protocole (obligatoire) : Nom que vous associez au protocole. (Non modifiable)
Numéro de protocole IP : Indication du n° de protocole.

Description : Commentaire que vous voulez associer à ce protocole.

REMARQUE
La saisie du type Global ou Local d'une plage n'est possible qu'en création.

CHAPITRE 8. SERVICES

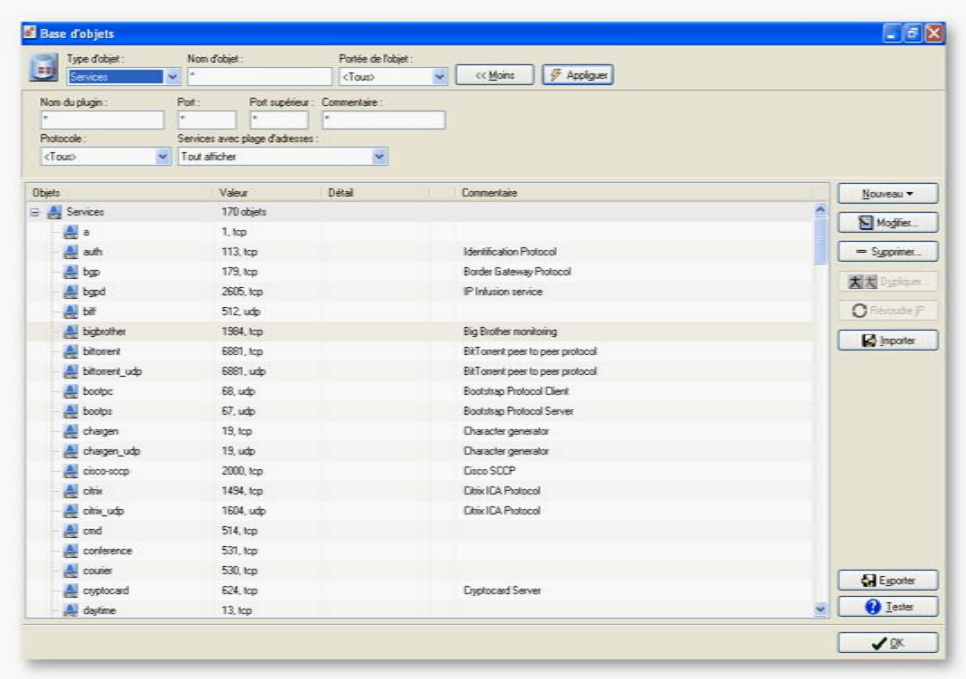


Figure 62 : Base d'objets - Services

Ce menu vous permet de configurer les noms de services utilisés dans vos fichiers de configuration de filtrage. Cette dénomination permet au firewall NETASQ de connaître la correspondance entre un nom de service, le protocole utilisé et le numéro de port associé.
De plus la colonne "Détail" vous indique quel plugin est associé à quel service. Vous pouvez activer un plugin sur plusieurs services ou activer plusieurs plugins sur un seul service. De plus un plugin n'est pas réservé à un type de service.

Exemple
Par exemple le plugin HTTP n'est pas réservé au trafic HTTP. Vous pouvez forcer l'activation du plugin pour d'autres types de services. Cela vous permet d'associer un plugin à un port généralement utilisé pour un trafic défini mais que vous utilisez pour un autre type de trafic.

Lorsque vous avez spécifié un plugin pour un service ce plugin ne s'active que lorsque le service est utilisé dans une règle de filtrage.

Pour une activation automatique du plugin, même si aucune règle directement associée au service n'a été spécifiée référez-vous à la *Partie 6/Chapitre 9 : Plugins*.

AVERTISSEMENT

Pour un maximum de sécurité, NETASQ vous recommande l'utilisation forcée du plugin plutôt qu'une activation automatique. L'activation automatique des plugins doit être réservée à la réalisation de services non critiques pour votre sécurité (la création de traces visant à réaliser un monitoring du trafic HTTP par exemple).

4.8.1. Création d'un service

2 étapes sont nécessaires pour créer un service :

Etape 1

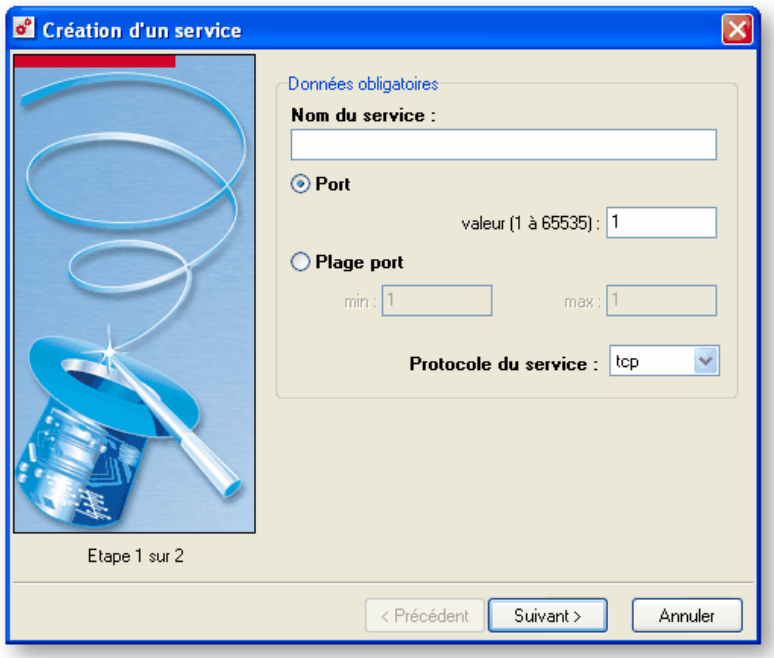


Figure 63 : Création d'un service - Etape 1

Nom du service (obligatoire) : Nom que vous associez au service. (Non modifiable)
Port (obligatoire) : N° de port associé au service.
Plage port (obligatoire) : Indication d'une plage de port encadrée par les champs "min" et "max".
Protocole du service (obligatoire) : Choix du protocole de service entre TCP ou UDP.

Etape 2

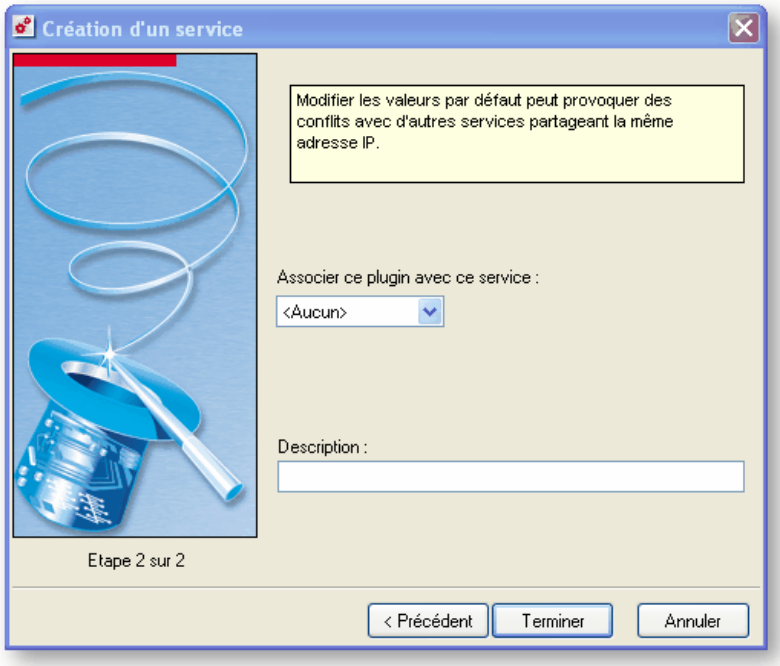


Figure 64 : Création d'un service - Etape 2

Associer ce plugin avec ce service : Les plugins qui peuvent être associés à un service sont : <Aucun>, http, FTP, EDONKEY, H323, SSL, Stream, SSH, Telnet, SMTP, POP3, IMAP4, NNTP, MySQL.
Description : Commentaire que vous voulez associer à ce service.

REMARQUE
La saisie du type Global ou Local d'une plage n'est possible qu'en création.

Cliquez sur le bouton **Modifier** pour modifier le service sélectionné. Si vous possédez des règles de filtrage associées à cet objet, une fenêtre d'information vous demande si vous voulez réactiver ces règles de filtrage et prendre en compte immédiatement cette modification.
Cette version du firewall NETASQ ne gère pas les services RPC (*Remote Procedure Call*), lesquels utilisent un numéro de port alloué dynamiquement.
Certains services ne sont pas modifiables. Par ailleurs, il existe un service réservé pour le fonctionnement du firewall :
"Firewall_srv" (port 1300) correspond à un nom de service qui gère la communication entre le firewall NETASQ et NETASQ UNIFIED MANAGER, NETASQ REAL-TIME MONITOR. Ce service est aussi utilisé pour les échanges nécessaires à la fonctionnalité de **Haute Disponibilité** entre deux firewalls.
Vous trouverez en *Annexe B : Services TCP/IP* une liste de services souvent utilisés (DNS, HTTP, FTP...), ainsi que le protocole et le numéro de port associés à ce service.

CHAPITRE 9. GROUPE DE SERVICES

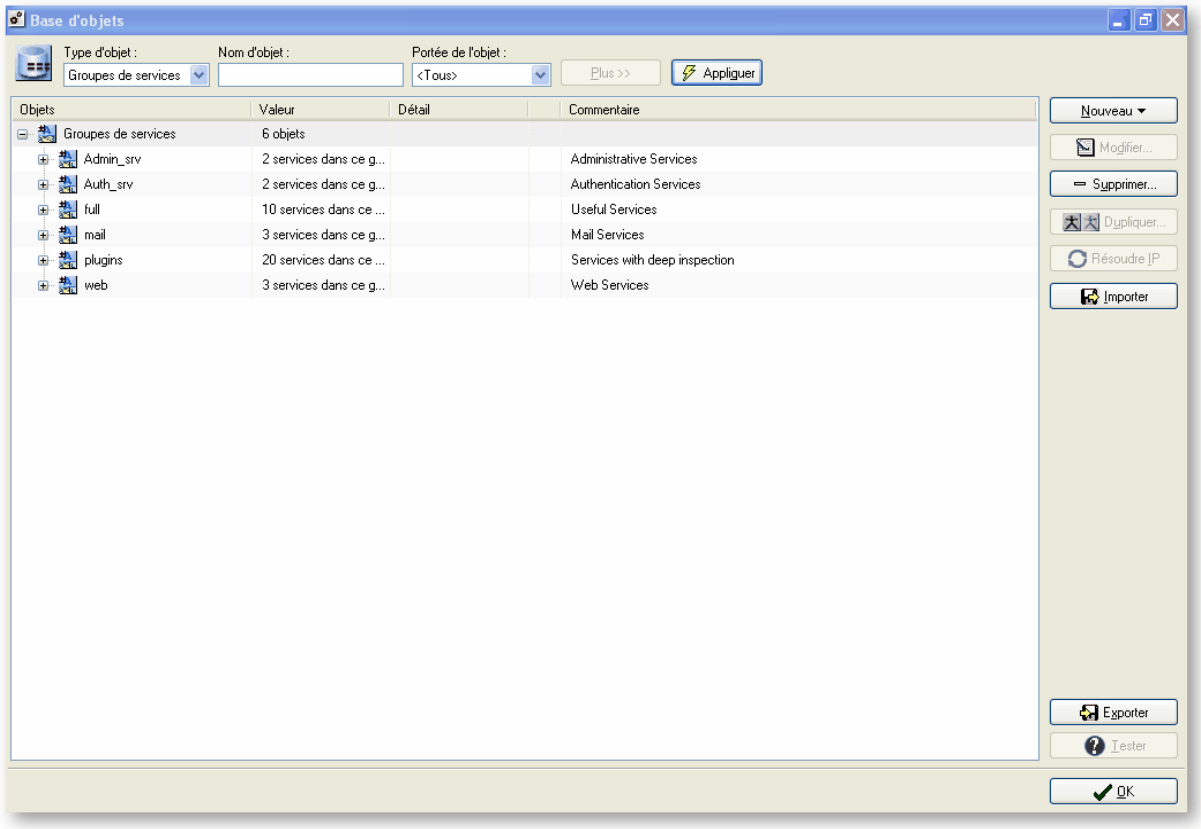


Figure 65 : Base d'objets - Groupes de services

De même que pour les utilisateurs et les équipements réseaux, vous pouvez constituer des groupes de services avec des services qui possèdent les mêmes propriétés de configuration. Ces groupes de services pourront ensuite être utilisés dans la configuration comme un seul et même service.
Ceci a pour but de simplifier la configuration et la compréhension de votre configuration en limitant le nombre de services à intégrer.

4.9.1. Création d'un groupe de services

Figure 66 : Création d'un groupe de services - Etape 1

Nom du groupe de services (obligatoire) : Nom que vous associez au groupe de service.
Description : Commentaire que vous voulez associer à ce groupe de service.

4.9.2. Ajouter un service dans un groupe

Pour ajouter un service dans un groupe, suivez la procédure suivante :

1. Sélectionnez le service que vous désirez ajouter dans la grille de définition des objets.
2. Cliquez sur le bouton droit de votre souris.
3. Sélectionnez l'option **Ajouter à** dans le menu contextuel puis **Groupes de services.**
4. Choisissez le groupe dans lequel doit être ajouté le service ou sélectionnez "Nouveau Groupe de Services".

Si vous ajoutez un service dans un nouveau groupe, le service est automatiquement ajouté au groupe.
Si un groupe utilisé dans la configuration de l'Appliance UTM est modifié, cette modification est automatiquement prise en compte par l'Appliance UTM et les slots utilisant ce groupe sont automatiquement réactivés.

AVERTISSEMENT
La réactivation d'un slot de NAT entraîne la perte des connexions actives.

Le firewall contient quelques groupes de services préconfigurés qui permettent de faciliter la configuration :

- Admin_srv : Services d'administration du firewall (SSH et firewall_srv).
- Auth_srv : Services d'authentification sur le firewall (HTTPS et firewall_auth).
- Full : Contient les services qui permettent un accès au web, mail, Telnet et les principaux services autour du web (news, ftp, DNS ...).
- Mail : Contient tous les services d'accès au mail pour les clients.
- Plugins : Services possédant un plugin spécifique et les plug-ins associés activés.
- Web : Services uniquement d'accès web (http et https).

CHAPITRE 10. GROUPE D'UTILISATEURS

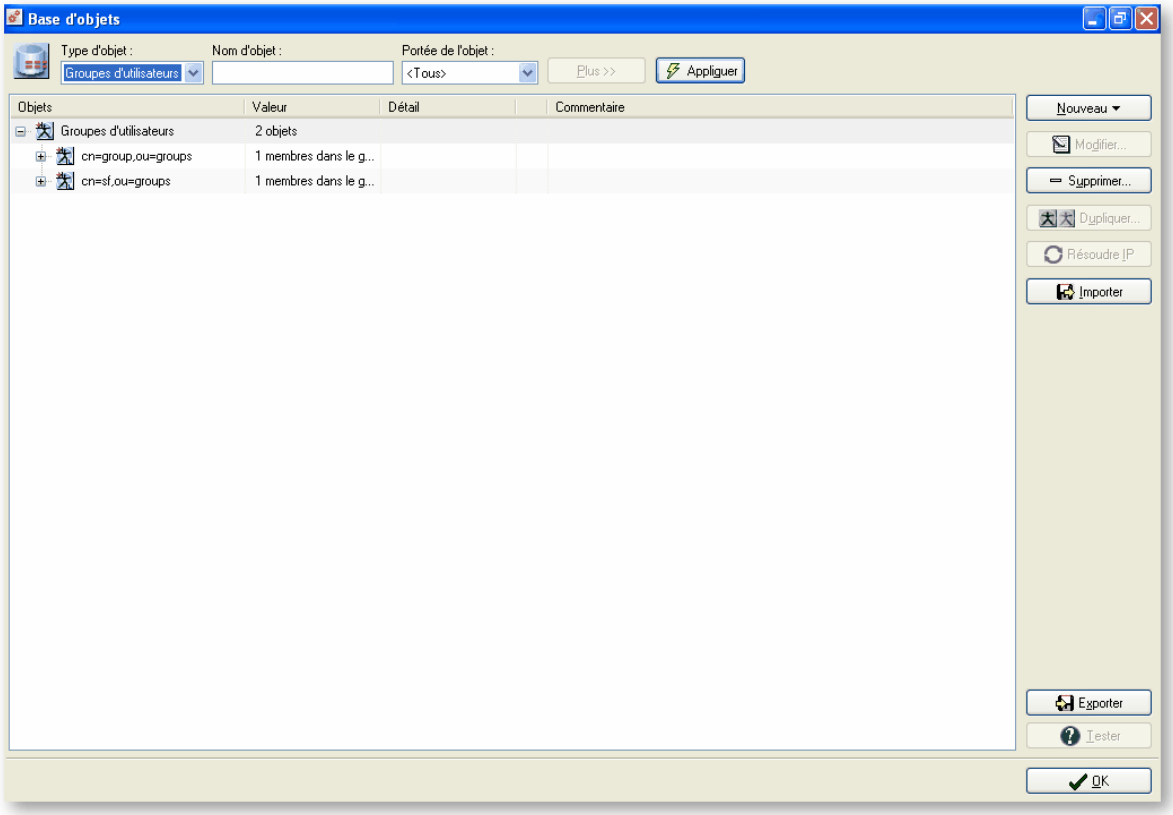


Figure 67 : Base d'objets - Groupes d'objets

Ce menu vous permet de créer des groupes d'utilisateurs. Ces groupes simplifient l'édition des règles de filtrage : au lieu de définir une règle pour chaque utilisateur, vous définissez une règle pour tous les utilisateurs ayant les mêmes droits.

Pour créer un nouveau groupe, référez-vous à la procédure suivante :

1 Cliquez sur le bouton **Nouveau**, puis sélectionnez **`Groupe d'utilisateurs`** dans le menu contextuel. Un assistant de création apparaît.

4.10.1. Ajouter un utilisateur dans un groupe

Pour ajouter un utilisateur dans un groupe d'utilisateur, suivez la procédure suivante :

1. Sélectionnez l'utilisateur que vous désirez ajouter dans la grille de définition des objets.
2. Cliquez sur le bouton droit de votre souris.
3. Sélectionnez l'option **Ajouter à** dans le menu contextuel puis **Groupes** d'utilisateurs et sélectionnez **Nouveau Groupe d'utilisateurs.** L'écran suivant s'affiche :

Figure 68 : Création d'un groupe d'utilisateurs - Etape 1

4. Choisissez le groupe dans lequel doit être ajouté l'utilisateur.

Si vous ajoutez un utilisateur dans un nouveau groupe, l'utilisateur est automatiquement spécifié dans la fenêtre de configuration du groupe. Si un groupe utilisé dans la configuration de l'Appliance UTM est modifié, cette modification est automatiquement prise en compte par l'Appliance UTM et les slots utilisant ce groupe sont automatiquement réactivés.

CHAPITRE 11. GROUPE

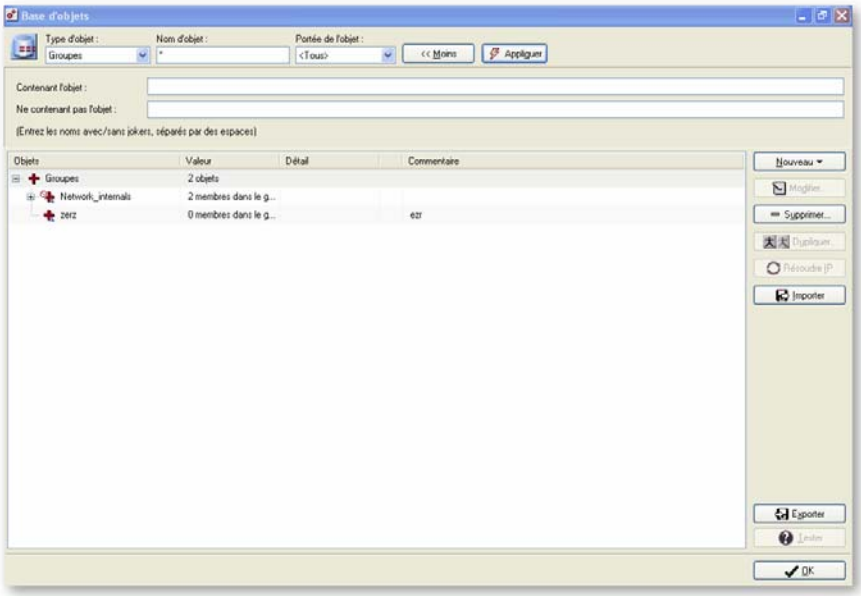


Figure 69 : Base d'objets - Groupes

Double-cliquez sur le libellé **Groupes** dans l'arborescence des menus. L'écran suivant s'affiche :
Ce menu vous permet de créer des groupes "réseaux". Ces groupes pourront contenir des machines, des réseaux, des plages d'adresses ou encore d'autres groupes "réseaux".

4.11.1. Création d'un groupe

Figure 70 : Création d'un groupe - Etape 1

Nom du groupe (obligatoire) : Nom que vous associez au groupe.
Description : Commentaire que vous voulez associer à ce groupe.

4.11.2. Ajouter un objet dans un groupe « réseaux »

Pour ajouter un objet dans un groupe "Réseaux", suivez la procédure suivante :

1. Sélectionnez l'objet que vous désirez ajouter dans la grille de définition des objets.
2. Cliquez sur le bouton droit de votre souris.
3. Sélectionnez l'option **`Ajouter à\Groupes\Nouveau groupe`** dans le menu contextuel.
4. Choisissez le groupe dans lequel doit être ajouté l'objet.

Si vous ajoutez un objet dans un nouveau groupe, le groupe est créé et l'objet est automatiquement ajouté au groupe.
Si un groupe utilisé dans la configuration de l'Appliance UTM est modifié, cette modification est automatiquement prise en compte par le boîtier UTM et les slots utilisant ce groupe sont automatiquement réactivés.

CHAPITRE 12. REMARQUES GENERALES SUR LES OBJETS

Il existe des noms d'objets réservés :

- De manière générale tous les noms d'objets commençant par "firewall_" et "network_" sont interdits.
- Les noms de protocoles GRE, ICMP, IGMP, TCP, UDP, VPN-AH, VPN-ESP sont réservés.
- Dans le cas des services : "ephemeral_fw", "ephemeral_tcp", "ephemeral_udp", "firewall_auth", "firewall_srv", "isakmp", "ssh", etc.

Ces noms d'objets réservés sont signalés dans les différentes listes d'objets par un panneau à côté du nom d'objet. Ces noms ne peuvent jamais être modifiés.

Il existe également des restrictions sur les noms d'objets :

- Caractères interdits : ", <tab>, \, #, @, <espace>
- Caractères interdits en première position : n'importe quel chiffre

PARTIE 5 : CONFIGURATION RESEAU

CHAPITRE 1 : INTRODUCTION

5.1.1. Pré-requis

5.1.1.1. Pour cette partie, vous devez avoir franchi les étapes

- PARTIE 2 : Installation, pré-configuration, intégration

5.1.1.2. Pour cette partie, vous devez connaître

- Les paramètres IP à affecter au firewall NETASQ pour chaque interface en cas de configuration avancée.
- L'adresse IP à affecter au firewall NETASQ pour sa connexion au réseau en cas de configuration en mode transparent.
- L'adresse IP du routeur par défaut à utiliser.
- Les routes statiques en cas de fonctionnement routeur.
- Les paramètres de connexion, donnés par votre fournisseur d'accès, dans le cas d'un accès dialup.

5.1.1.3. Utilité de cette partie

Cette partie vous permet de reconfigurer à distance les paramètres associés aux cartes réseau du firewall NETASQ, ainsi que l'adresse IP du routeur par défaut.
Cette partie permet de gérer, ajouter, supprimer des éléments réseaux appelés "interfaces réseau" qui représentent des éléments physiques ou non de communication entre les différents réseaux qui transitent par le boîtier.

Les différents types d'interfaces gérés par la configuration réseau sont :

- **Les Ethernets** : ces interfaces sont en réalité les seules à correspondre directement à un port physique situé sur le boîtier. Par conséquent, elles ne peuvent être ajoutées, supprimées au sein de cette configuration. Juste désactivées. Ces Ethernets peuvent ou non posséder une (ou plusieurs) adresses réseau suivant le fait qu'elles aient ou non un bridge "père".
- **Les Bridges** : il s'agit de regroupement d'interfaces. Toute interface qui possède un paramètre "Bridge" valide délègue à celui-ci la gestion de son adressage et devient ainsi un élément de ce bridge. Ainsi, on peut considérer qu'un bridge possède une ou plusieurs adresses (statique ou dynamique). D'autre part, tous les sous-réseaux de ce bridge partagent les mêmes plans d'adressage (ceux du bridge).
- **Les VLAN** : Les VLAN sont des interfaces virtuelles qui possèdent leur adressage (ou non, si elles sont rattachées à un bridge) mais dont les paquets passent physiquement par une interface Ethernet.
Par conséquent, un VLAN possède un paramètre de spécification de l'interface Ethernet auquel il est rattaché. Si l'Ethernet est dysfonctionnant ou encore désactivé, le VLAN le sera également.
- **Les dialups** : ces interfaces sont dédiées à l'établissement d'une connexion de type modem (vers un fournisseur d'accès) PPTP, PPP, PPPOE, ou, à l'accès à un tunnel L2TP.

Ces éléments sont occasionnellement liés les uns aux autres par une pseudo-relation de parentalité.

Le firewall peut fonctionner suivant trois modes :

- **Mode bridge (ou transparent)** : il s'insère dans un réseau et possède une adresse située sur ce réseau. Avec ce mode vous n'avez pas besoin de modifier la topologie de votre réseau (passerelle par défaut, routes statiques,...). Le firewall fonctionne alors comme une passerelle.
- **Mode avancé** : vous séparez votre réseau en deux ou trois ou plus (selon le nombre d'interfaces que vous possédez) et affectez des adresses réseau différentes à chacune de ces parties. Cela vous permet de distinguer clairement les différentes parties de votre réseau au niveau adressage.
- **Mode hybride** : Le mode hybride utilise une combinaison des deux modes précédents. Vous pouvez définir plusieurs interfaces en mode transparent.

5.1.1.4. Accéder à cette partie

Accédez à la configuration réseau en sélectionnant **Réseau** dans l'arborescence des menus.

Vous devez être connecté avec le droit "réseau" et les privilèges de modifications pour pouvoir effectuer des modifications sur la configuration des interfaces et le droit "routage" et les privilèges de modification pour pouvoir effectuer des modifications sur la configuration du routage.

REMARQUE
Avant d'effectuer toute modification importante sur votre firewall NETASQ, nous vous conseillons d'effectuer une sauvegarde *(Cf. PARTIE 18 : Sauvegarde)*. Ainsi, en cas de mauvaise manipulation vous pourrez vous retrouver dans l'état précédent.

5.1.2. Présentation

Les menus de configuration réseau permettent de paramétrer l'ensemble des paramètres réseau du firewall, c'est-à-dire :

- Le mode de fonctionnement des interfaces (bridge ou avancé).
- La ou les adresses IP du firewall ainsi que le réseau sur lequel il est connecté.
- Les connexions distantes sur le port-série (modem).
- Le routage que le firewall effectue.

Vous avez la possibilité de définir des interfaces virtuelles qui peuvent appartenir à des VLAN de votre réseau. Ainsi le firewall NETASQ peut gérer les VLAN de votre architecture. (*Cf. Partie 5/Chapitre 2 : Création d'un VLAN*).

Vous pouvez aussi effectuer du routage par interface : en fonction de l'interface sur laquelle est reçu un paquet par le firewall, ce paquet est renvoyé vers une passerelle différente.
Une fois l'ensemble de ces paramètres entré, il suffit d'envoyer la configuration au firewall par le bouton **Envoyer**.

AVERTISSEMENT
La modification de certains de ces paramètres nécessite le redémarrage du firewall. Toutefois lorsqu'il n'est pas nécessaire, il est quand même recommandé. Dans ce cas, un message vous préviendra avant l'envoi du firewall.

CHAPITRE 2 : INTERFACES

5.2.1. Mode de fonctionnement entre interfaces

Vous pouvez configurer le fonctionnement entre interfaces du firewall suivant trois modes différents :

- Mode avancé
- Mode transparent
- Mode hybride

5.2.1.1. Mode avancé

Avec ce mode de configuration, le firewall fonctionne comme un routeur entre ses différentes interfaces.
Cela implique certains changements d'adresses IP sur les routeurs ou serveurs lorsque vous les déplacez dans un réseau différent (derrière une interface du firewall différente).

Les avantages de ce mode sont :

- La possibilité de faire de la translation d'adresses d'une classe d'adresses vers une autre.
- Seul le trafic passant d'une interface à l'autre traverse le firewall (réseau interne vers Internet par exemple). Cela allège considérablement le firewall et fournit de meilleurs temps de réponse.
- Meilleure distinction des éléments appartenant à chaque zone (interne, externe et DMZ). La distinction se fait par les adresses IP qui sont différentes pour chaque zone. Cela permet d'avoir une vision plus claire des séparations et de la configuration à appliquer pour ces éléments. De plus, vous pouvez appliquer des règles globales sur une zone avec les objets "Réseau".

5.2.1.2. Mode Bridge ou mode transparent

Le mode transparent, aussi appelé "Bridge" en anglais, permet de conserver le même adressage entre les interfaces.
Il simule un pont filtrant, c'est-à-dire qu'il est traversé par l'ensemble du trafic du réseau.
Cependant, vous pouvez ensuite filtrer les flux qui le traversent suivant vos besoins et donc protéger telle ou telle partie du réseau.

Les avantages de ce mode sont multiples :

- Facilité d'intégration du produit car pas de changement de la configuration des postes client (routeur par défaut, routes statiques...) et aucun changement d'adresse IP sur votre réseau.
- Compatibilité avec IPX (réseau Novell), NetBIOS sous Netbeui, Appletalk ou IPv6.
- Pas de translation d'adresses, donc gain de temps au niveau du traitement des paquets par le firewall.

Ce mode est donc préconisé entre la zone externe et la/les DMZ. Il permet de conserver un adressage public sur la zone externe du firewall et les serveurs publics de la DMZ.

5.2.1.3. Mode hybride

Le mode hybride utilise une combinaison des deux modes précédents. Ce mode ne peut être employé que pour les produits NETASQ possédant plus de deux interfaces réseau. Vous pouvez définir plusieurs interfaces en mode transparent.

> **Exemple**
> Zone interne et DMZ ou zone externe et DMZ) et certaines interfaces dans un plan d'adressage différent. Ainsi vous avez une plus grande flexibilité dans l'intégration du produit.

5.2.1.4. Conclusion

Le choix d'un mode se fait uniquement au niveau de la configuration des interfaces réseau. La configuration du firewall est ensuite la même pour tous les modes.

Au niveau sécurité, tous les modes de fonctionnement sont identiques. On filtre les mêmes choses et la détection d'attaques est identique.

5.2.2. Configuration des interfaces

5.2.2.1. Présentation de l'écran de configuration

Les interfaces sont organisées de manière hiérarchique.

- Si une interface est dans un bridge, alors elle sera représentée sous forme de noeud fils par rapport au bridge . Un bridge peut donc contenir plusierus interfaces.
- Si un VLAN a pour lien physique une ethernet, alors il sera fils de cet ethernet sauf si ce VLAN fait partie du bridge. Dans ce cas, il sera le fils direct du bridge. L'arborescence de la configuration se présente donc ainsi : Bridge -> ethernet ->VLAN mais jamais plus.
- Les dialups sont toutes au même niveau, après le reste des interfaces.

Il est possible de déplacer certains éléments, soit par drag & drop, soit à l'aide du menu contextuel. Il est possible de :

- "Détacher" une interface d'un bridge en la déplaçant en dehors de celui-ci et en la déposant dans une zone vide.
- Ré-apparenter le lien physique d'un VLAN en le glissant sur une autre interface ethernet.

Lorsqu'une interface sans adresse est susceptible d'en avoir besoin d'une (pour se détacher d'un bridge par exemple), un panneau de choix d'adresse lui est proposé.
Chaque noeud (interface) de l'arborescence est textuellement représenté par le nom de l'interface associée.

Chaque interface possède en outre sa propre icône pour une identification visuelle plus immédiate. Cette icône permet également un repérage de l'état de l'interface selon qu'elle est désacivée ou non. Dans le cas d'une désactivation, l'icône est grisée.
Les ethernets possèdent un nom propre (ex : "Out") et un nom technique "ex : "0"). Le numéro est affiché entre crochets après le nom des interfaces.

Sous l'arborescence se trouvent deux boutons :

Ajouter	Permet d'ajouter une interface à la configuration.
Supprimer	Permet de supprimer (pour les VLAN et Dialups) ou détacher (pour Ethernet) suivant le type de l'interface courante.

Lorsque l'on clique sur un élément de l'arborescence de la configuration, le panneau de configuration s'adapte au type de l'interface choisie. Chaque panneau de configuration est composé d'un enble d'onglets dont un onglet Identité, un onglet Paramètres, deux onglets dédiés à l'adressage et des onglets spécialisés selon le type d'interface (choix du type de dialup par exemple).
Un onglet Etat permet d'avoir à tout moment la liste des modules du boîtier qui utilisent l'interface courante, ce qui est utile pour avoir un aperçu des changements produits sur cette interface.

La configuration des interfaces sur un firewall est effectuée dans le menu **Réseau\Interfaces** de l'arborescence des menus.

Elles peuvent être configurées de plusieurs façons :

- **En transparent (Bridge)** : les interfaces font partie du même plan d'adressage déclaré sur le bridge.
- **En avancé** : chaque interface possède une adresse IP différente et le réseau qui lui est relié fait partie de la même classe. Cela permet de configurer des règles de translation pour accéder à une autre zone du firewall.
- **En mode hybride** : certaines interfaces possèdent la même adresse IP et d'autres ont une adresse distincte.

5.2.2.2. Paramètres du Bridge

Pour modifier les paramètres d'un bridge, cliquez sur le bouton ⊞ situé à gauche du menu **Bridge** dans la partie gauche de la fenêtre. Cinq onglets permettent la modification des paramètres du bridge.

Onglet Identité

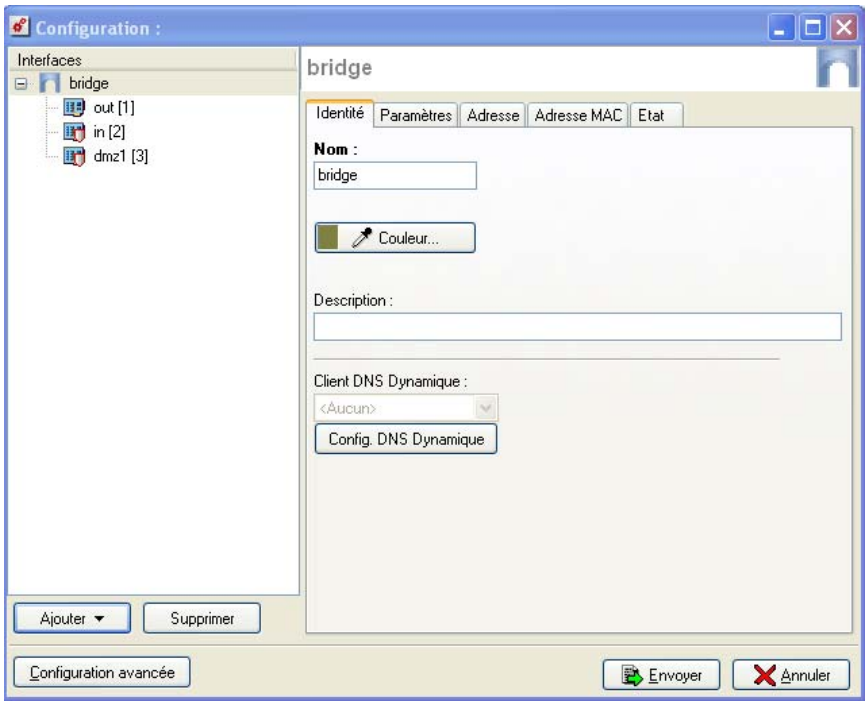


Figure 71 : Configuration Bridge - Identité

Nom (obligatoire)	Nom utilisateur de l'interface. (*Cf.* Partie 5/Chapitre 4 : Remarques générales sur la configuration réseau pour connaître les noms interdits).
Couleur…	Couleur attribuée à l'interface. Ces couleurs seront très utiles pour vous aider lors de la mise en place des règles de filtrage, des translations... En effet, chaque objet créé prendra une couleur en fonction de la zone à laquelle l'adresse IP appartient.
Description	Permet de donner un commentaire pour l'interface.
Client DNS dynamique	Lorsque votre firewall ne possède pas d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc.), il est possible d'associer via un fournisseur de services DNS (**dyndns.org** par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter ce firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique que vous avez préalablement configuré. La configuration des clients DNS dynamique est expliquée dans la suite du document (*Cf.* *Partie 5/Chapitre 2 : Client DNS dynamique*).

Définition des couleurs

Pour chaque interface définie dans la configuration réseau, une couleur peut être spécifiée. Tous les objets relatifs à une interface (machines ou réseaux) prendront la couleur définie pour cette interface.

Figure 72 : Couleur bridge

La sélection d'une couleur est réalisée en cliquant sur le rectangle coloré situé sous le nom de l'interface. Une fenêtre s'affiche, vous avez alors la possibilité de choisir la couleur désirée parmi les couleurs prédéfinies ou définir vos propres couleurs (16 millions de couleurs).

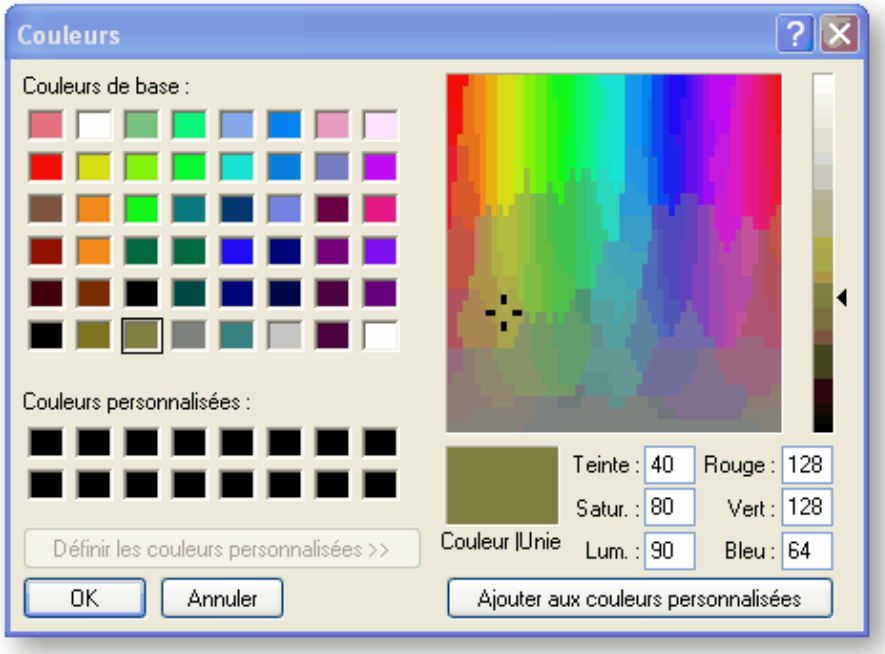


Figure 73 : Palette des couleurs

Client DNS Dynamique

Basé sur un échange entre un serveur (maintenu par un fournisseur de service DNS) et un client (intégré dans les firewalls NETASQ), le service DNS dynamique permet d'associer vos firewalls à un nom de domaine spécifique. Cela vous permet de pouvoir contacter ces firewalls même si vous ne possédez pas d'adresse IP publique statique ou d'utiliser un nom de domaine simple à retenir plutôt qu'une adresse IP difficile à mémoriser.
Actuellement **DynDNS.org** est le seul fournisseur de service DNS supporté par les firewalls. Contactez ce fournisseur pour obtenir un compte vous permettant la mise en place de ce service sur votre firewall.

➲ La configuration des clients DNS dynamique est accessible depuis la configuration des interfaces (bridge, interfaces en mode avancé, VLAN, Dialup) par le bouton **Config.DNS Dynamique**.

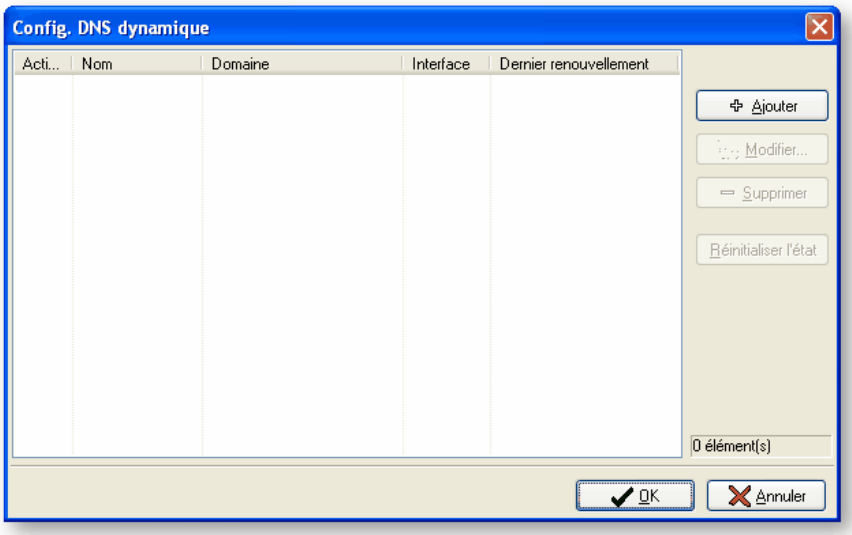


Figure 74 : Config. DNS dynamique

Les informations indiquées sur cet écran sont les suivantes :

Active	En cochant cette option, la configuration DNS dynamique créée est activée.
Nom	Nom associé à la configuration du client DNS dynamique.
Domaine	Nom de domaine attribué au client DNS dynamique. En utilisant l'option **Gestion du wildcard pour le nom de domaine,** vous pouvez couvrir tous les sous-domaines. Par exemple si vous spécifiez **netasq.dyndns.org** dans le champ "Nom de domaine" et que l'option **Gestion du wildcard pour le nom de domaine** est sélectionnée, tous les sous-domaines (commerce.netasq.dyndns.org, labo.netasq.dyndns.org, etc.) seront associés au client.
Interface	Nom de l'interface réseau utilisée pour la liaison avec le client DNS dynamique.
Dernier renouvellement	Date de dernière mise à jour du service DNS.

La configuration d'un client DNS dynamique est réalisée au moyen d'un assistant. Les informations à spécifier dans l'assistant sont décrites dans les tableaux suivants.

Pour ajouter un client dans la liste des clients DNS dynamique configurés, cliquez sur le bouton **Ajouter** à partir de l'écran de configuration du DNS dynamique.

Etape 1 : Configuration générale

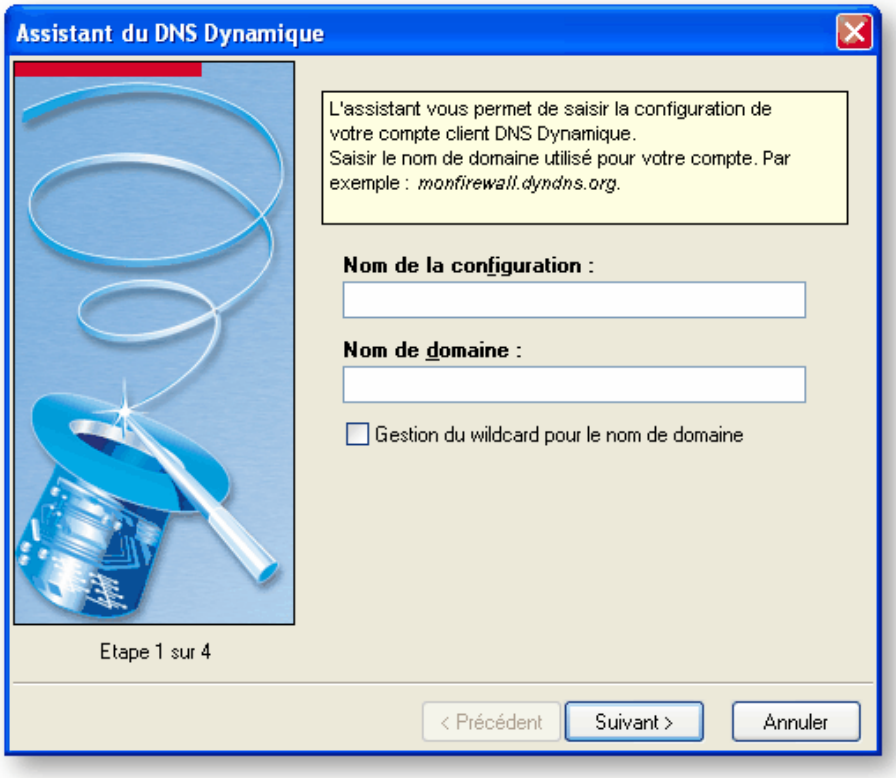


Figure 75 : Assistant du DNS Dynamique - Etape 1

Nom de la configuration (obligatoire) : Nom associé à la configuration du client DNS dynamique. Par exemple : *monfirewall.dyndns.org*.

Nom de domaine : Nom de domaine attribué au client DNS dynamique.

Gestion du wildcard pour le nom de domaine : pour couvrir tous les sous-domaines.

Etape 2 : Fournisseur et configuration du compte

Cet écran vous permet de saisir les informations d'accès de votre fournisseur de service de DNS Dynamique.

Figure 76 : Assistant du DNS Dynamique - Etape 2

Fournisseur DNS dynamique (obligatoire) : Fournisseur de services DNS. Actuellement, un seul fournisseur de services DNS est supporté : **Dyn DNS**.
Paramètres du compte : Utilisateur (obligatoire) et mot de passe (obligatoire) indiqués par le fournisseur de services DNS pour l'authentification du client DNS dynamique.

Etape 3 : Paramétrages DynDNS

Figure 77 : Assistant du DNS dynamique - Etape 3

Service : Cette option vous permet d'indiquer le service que vous avez souscrit auprès de votre fournisseur de services DNS parmi "dynamic DNS", "custom", et "static DNS".
Serveur : Serveur du fournisseur de services DNS. L'objet à spécifier dans ce champ doit obligatoirement se nommer : "members.dyndns.org" pour fonctionner avec Dyn DNS.

Dans l'étape 3, des paramétrages de configuration avancés sont disponibles en cliquant sur le bouton **Paramétrages avancés**. Ils permettent notamment de renouveler l'enregistrement du changement d'adresse. L'écran suivant s'affiche en cliquant sur le bouton :

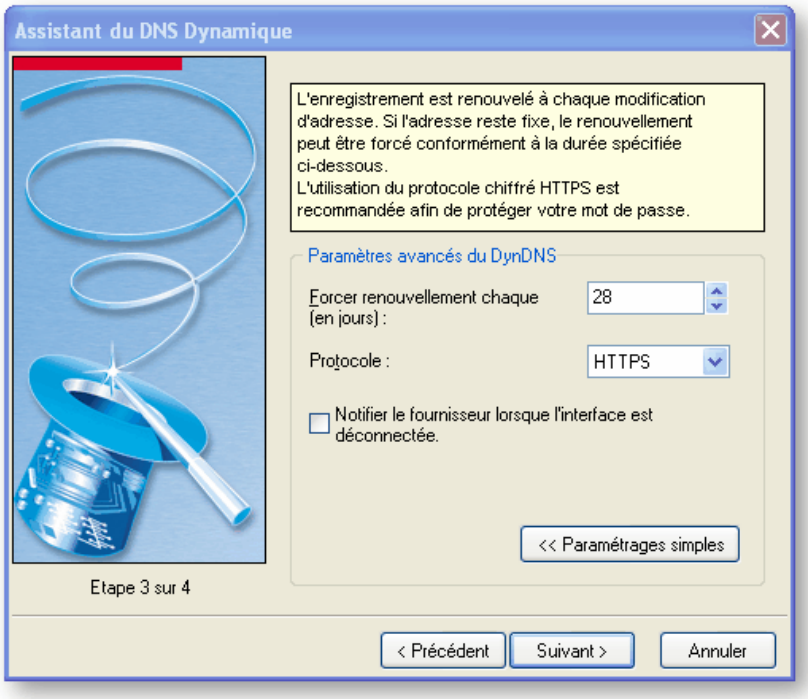


Figure 78 : Assistant du DNS dynamique - Etape 3

Forcer le renouvellement chaque (en jours) : Période de renouvellement du service DNS dynamique. Cette période est fixée à 28 jours par défaut par NETASQ.

REMARQUE
Dyn DNS punit les renouvellements abusifs (fermeture du compte…). Ainsi un renouvellement survenu avant 26 jours (après le dernier renouvellement) n'est pas permis par **Dyn DNS** De plus sans renouvellement au delà de 35 jours, le compte est clôturé. Ces informations sont toutefois susceptibles d'être modifiées étant donné qu'il s'agit d'un fonctionnement établi par **Dyn DNS**.

Protocole : Protocole utilisé lors de la phase de renouvellement du service DNS dynamique. Les choix possible sont : HTTPS et HTTP.

Notifier le fournisseur lorsque l'interface est déconnectée
Ce service, payant chez **Dyn DNS** permet de rediriger les flux à destination de votre réseau vers une page spécifique lorsque votre connexion n'est pas en activité.

Etape 4 : Activation de la configuration

Figure 79 : Assistant du DNS dynamique - Etape 4

Cet écran permet d'activer la configuration du client DNS dynamique. Pour ce faire, cliquez sur le bouton **Terminer**.

AVERTISSEMENT
N'oubliez pas de lier cette configuration à une interface réseau adéquate.

Onglet Paramètres

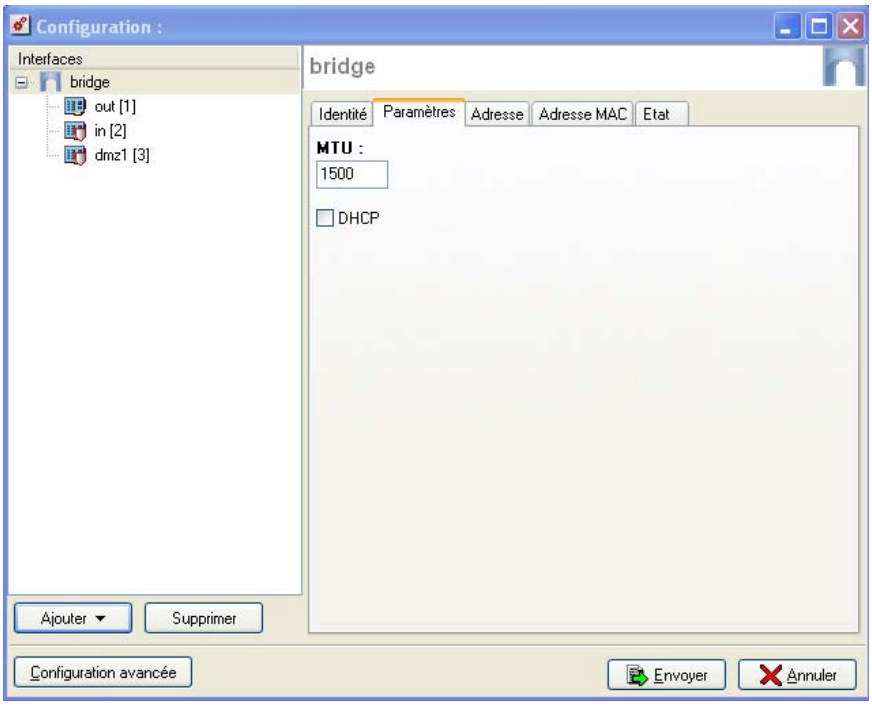


Figure 80 : Configuration Bridge - Paramètres

MTU	Longueur maximale des trames émises sur le support physique (Ethernet).
DHCP	Ce champ permet de spécifier au firewall que la configuration du bridge (adresse IP et masque) est définie par DHCP. Dans ce cas, l'onglet **Adresse** devient **DHCP**.

Onglet Adresse

Cet onglet concerne l'adressage de l'interface. Si l'interface appartient à un bridge, cet onglet est invisible. Ici, DHCP n'est pas coché, aussi, cet onglet contient une grille "Adresse/Masque", les boutons **Ajouter**/**Supprimer** et une colonne "Description".

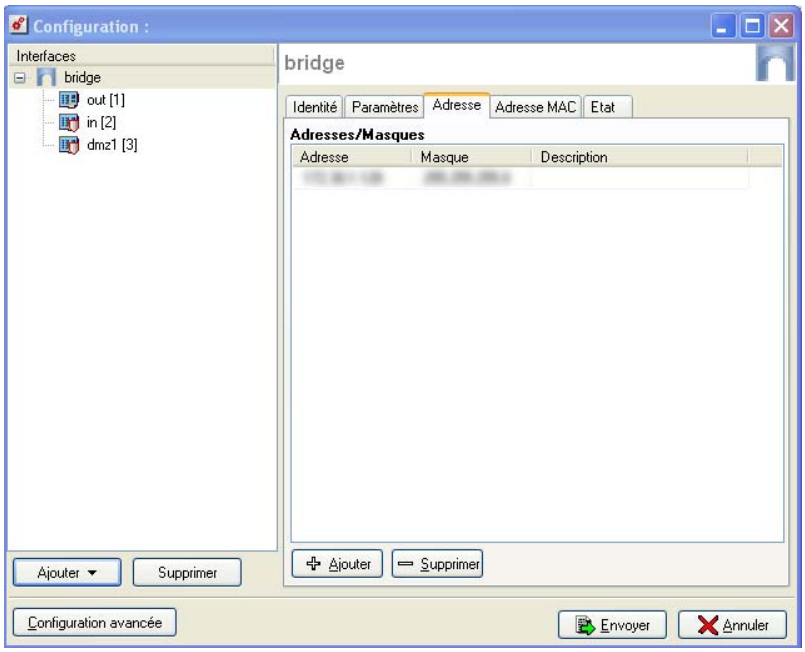


Figure 81 : Configuration Bridge - Adresse

Adresse	Adresse IP affectée au bridge. (Toutes les interfaces contenues dans le bridge possèdent la même adresse IP).
Masque	Masque de réseau du sous-réseau auquel appartient le bridge. Les différentes interfaces faisant partie du bridge ont la même adresse IP donc tous les réseaux connectés au firewall font partie du même plan d'adressage. Le masque de réseau donne au firewall les informations sur le réseau dont il fait partie.
Description	Permet de spécifier un commentaire pour l'adressage du bridge.

Dans cet onglet, plusieurs adresses IP et masques associés peuvent être définis pour le même bridge (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser ce firewall NETASQ comme un point de routage central. De ce fait, un bridge peut être connecté à différents sous-réseaux ayant un adressage différent. Pour les ajouter ou les retirer, il suffit d'utiliser les boutons d'action **Ajouter** et **Supprimer** sous les champs Adresse IP et masque réseau.

Onglet Adresse MAC

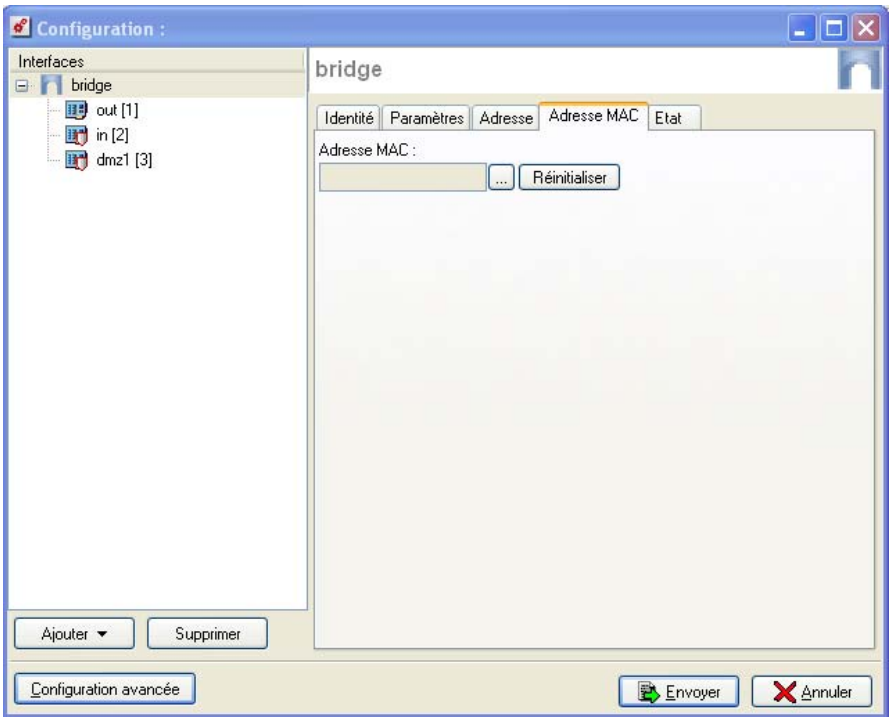


Figure 82 : Configuration Bridge - Adresse MAC

AVERTISSEMENT
Cette option n'est pas accessible pour les firewalls en Haute Disponibilité.

Cet écran vous permet de spécifier une adresse MAC pour une interface plutôt que d'utiliser l'adresse allouée par le firewall. Cela vous permet de faciliter d'autant plus l'intégration en mode transparent de votre firewall NETASQ dans votre réseau (en spécifiant l'adresse MAC de votre routeur plutôt que d'avoir à reconfigurer tous les postes utilisant cette adresse MAC).

Adresse MAC Adresse MAC affectée au bridge. (Toutes les interfaces contenues dans le bridge possèdent alors la même adresse MAC).

Pour éditer l'adresse MAC, cliquez sur le bouton  . L'écran ci-dessous s'affiche :

Figure 83 : Edition de l'adresse MAC

Réinitialiser Remise à zéro du champ "Adresse MAC".

NOTE
Cet onglet est caché lorsque l'interface appartient à un bridge.

Onglet Etat

L'onglet **Etat** permet de visualiser en temps réel les points d'utilisation de l'interface et de tous les objets et groupes d'objets générés par l'interface (Network_xx, Firewall_xx) dans la configuration de l'Appliance UTM. Cet onglet peut s'avérer utile lors de changements éventuels sur cette interface.

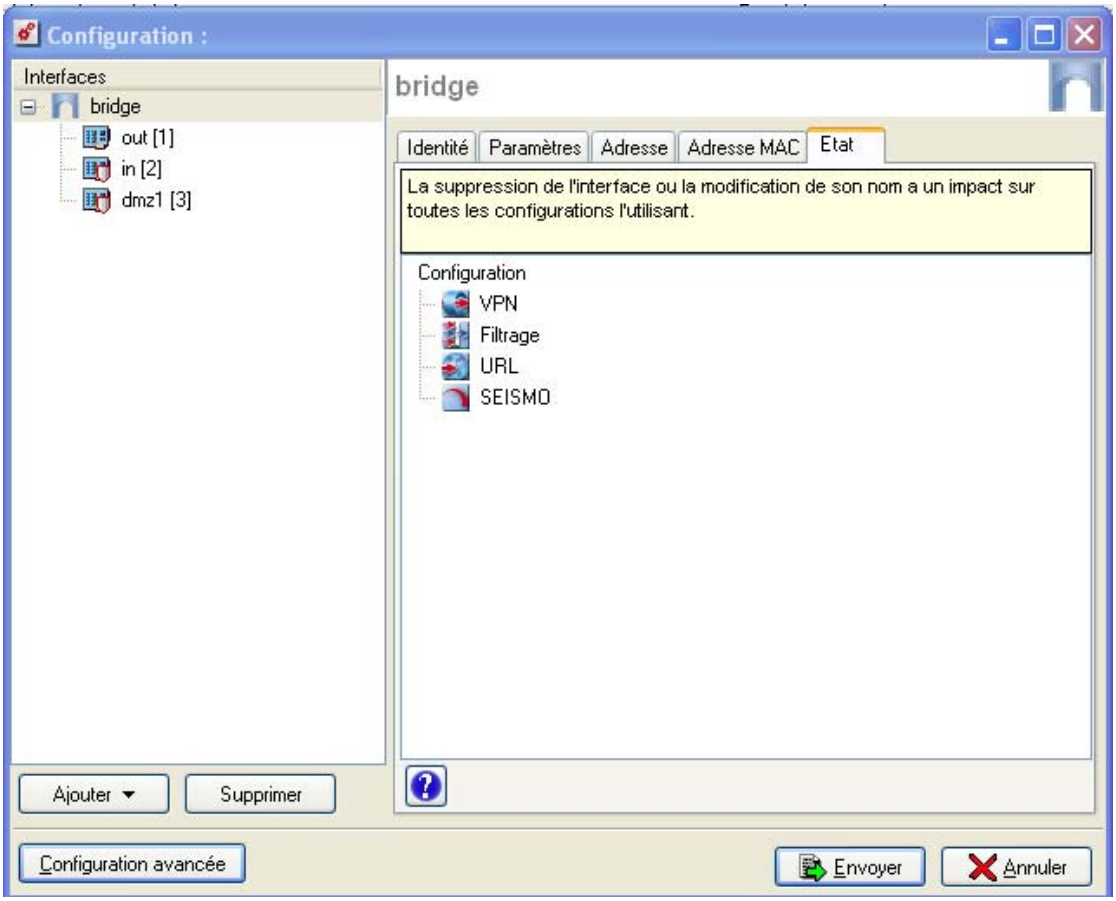


Figure 84 : Configuration Bridge - Etat

De plus en cliquant sur le bouton , vous obtenez une visualisation plus précise de l'utilisation de l'interface, module par module, ligne par ligne.

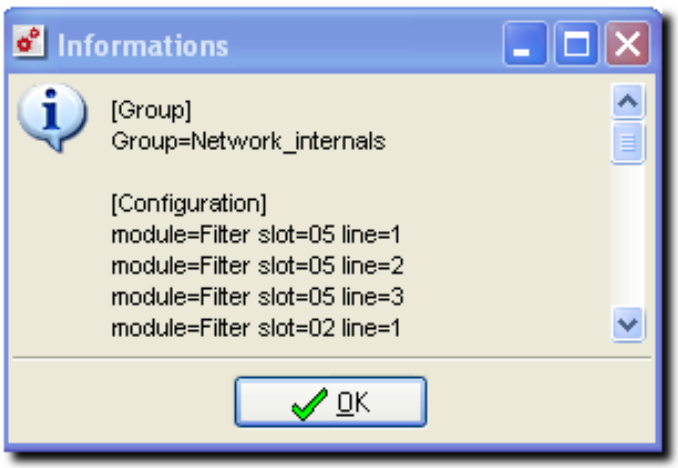


Figure 85 : Informations

5.2.2.3. Paramètres des interfaces du bridge

Une interface appartenant à un bridge est représentée sous forme de nœud fils par rapport au bridge. Un bridge peut donc contenir plusieurs nœuds fils.
Vous pouvez modifier les paramètres de chaque interface appartenant au bridge. Pour cela, sélectionnez une interface située sous un bridge dans la partie gauche de la fenêtre. Quatre onglets s'affichent :

Onglet Identité

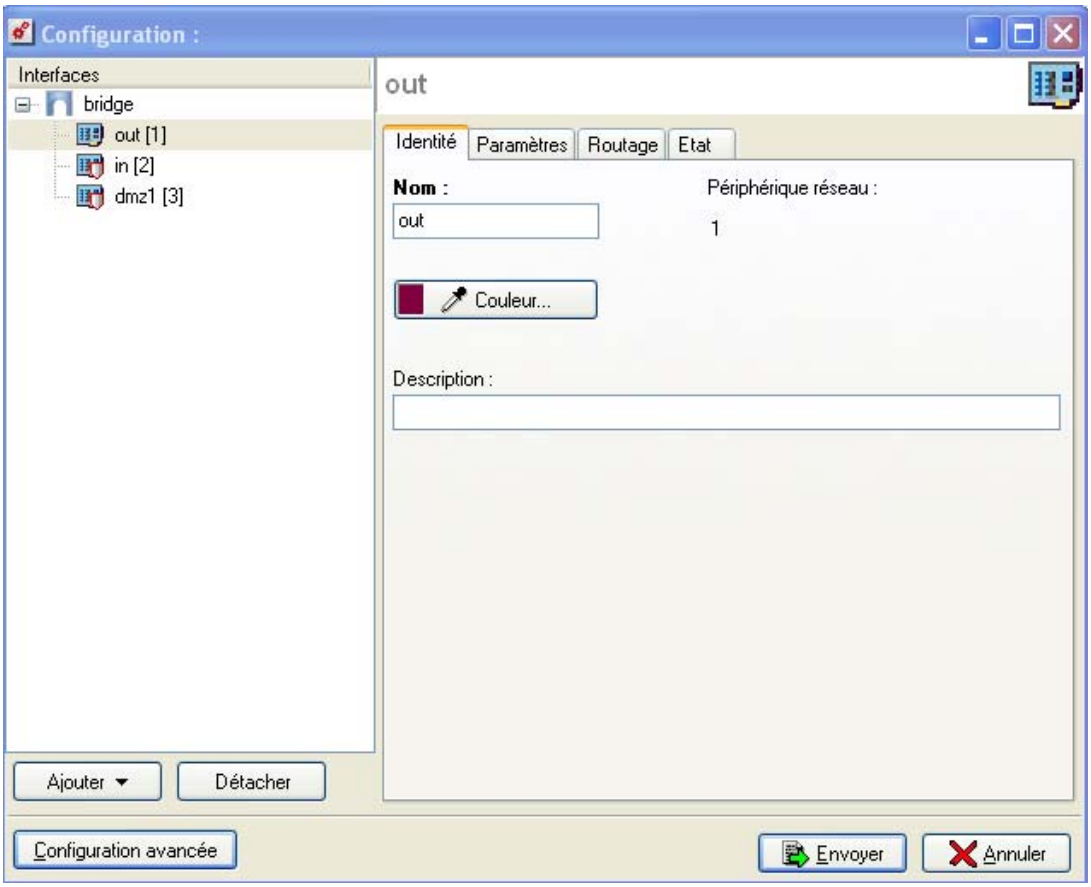


Figure 86 : Configuration - Interface Out - Identité

Nom (obligatoire)	Nom associé à l'interface du pont. *(Cf. Annexe M : Noms interdits)*
Périphérique réseau	N° du périphérique réseau.
Couleur	Couleur attribuée à l'interface. Ces couleurs seront très utiles pour vous aider lors de la mise en place des règles de filtrage, des translations... En effet, chaque objet créé prendra une couleur en fonction de la zone à laquelle l'adresse IP appartient.
Description	Permet de donner un commentaire pour l'interface.

Onglet Paramètres

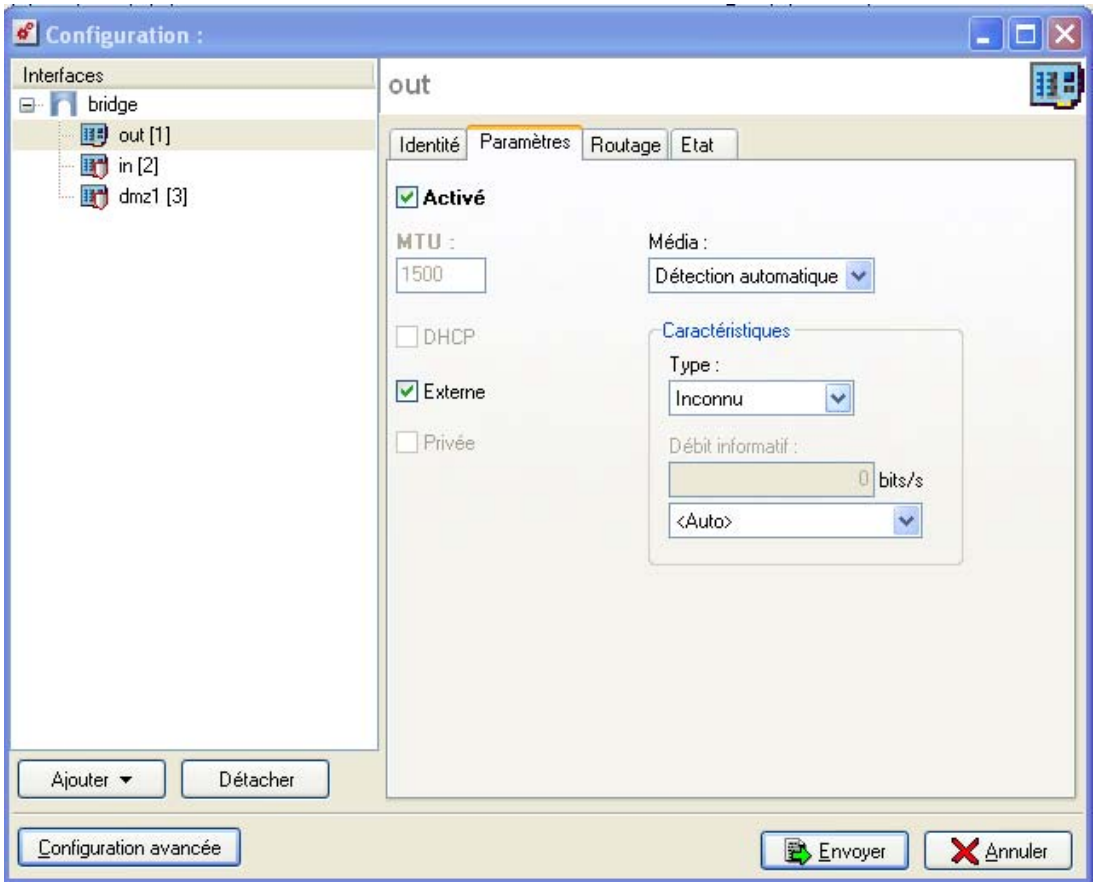


Figure 87 : Configuration- Interface Out - Paramètres

Activé	En cochant/décochant cette option on active/désactive l'interface. En désactivant une interface, on la rend inutilisable. En terme d'utilisation cela peut correspondre à une interface que l'on a prévu de déployer dans un futur proche ou éloigné mais qui n'est pas en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.
MTU	Longueur maximale des paquets émis sur le support physique (Ethernet). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
DHCP	L'adresse IP de l'interface est fournie par un serveur DHCP (utile pour les connexions Internet via le câble). (Cf. Partie 11/Chapitre 1 : *DHCP*). Ce choix n'est pas disponible pour une interface contenue dans un bridge (dans ce cas, le choix est grisé).
Externe	Cochez cette option pour indiquer que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface (matérialisé par un bouclier) disparaît lorsque cette option est cochée.
Privée	Cette option permet d'indiquer le caractère privé de l'interface. Les adresses des interfaces **Privée** ne sont pas utilisables en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. **NOTE** On notera que **Privée** implique forcement d'être sur une interface protégée. Les options **Externe** et **Privée** sont donc incompatibles.

Média	Vitesse de liaison du réseau. Par défaut le firewall le détecte automatiquement mais vous pouvez forcer l'utilisation d'un mode particulier. Les vitesses proposées sont : "Détection automatique", "10 Mb Half duplex", "10 Mb Full duplex", "100 Mb Half duplex", "100 Mb Full duplex", "1 Gb Half duplex", "1 Gb Full duplex". **AVERTISSEMENT** Si le firewall est directement connecté à un modem ADSL, NETASQ vous recommande de forcer le média que vous voulez utiliser sur l'interface en question.
Type	Cette option permet de définir quel type de machines est hébergé sur cette interface. **Machine** = machines de type hôte (utilisateurs) et **Inconnu** = type de machine non défini. Ainsi, dans les traces, vous verrez quels types de flux (machine à machine) transitent par le firewall.
Débit Informatif	En spécifiant le type de liaison Internet, il est possible de définir un débit maximal. Cette information n'est cependant pas utilisée pour réguler le trafic, elle définit l'échelle des graphiques du Monitor.

Onglet Routage

Cet onglet concerne le routage de l'interface.

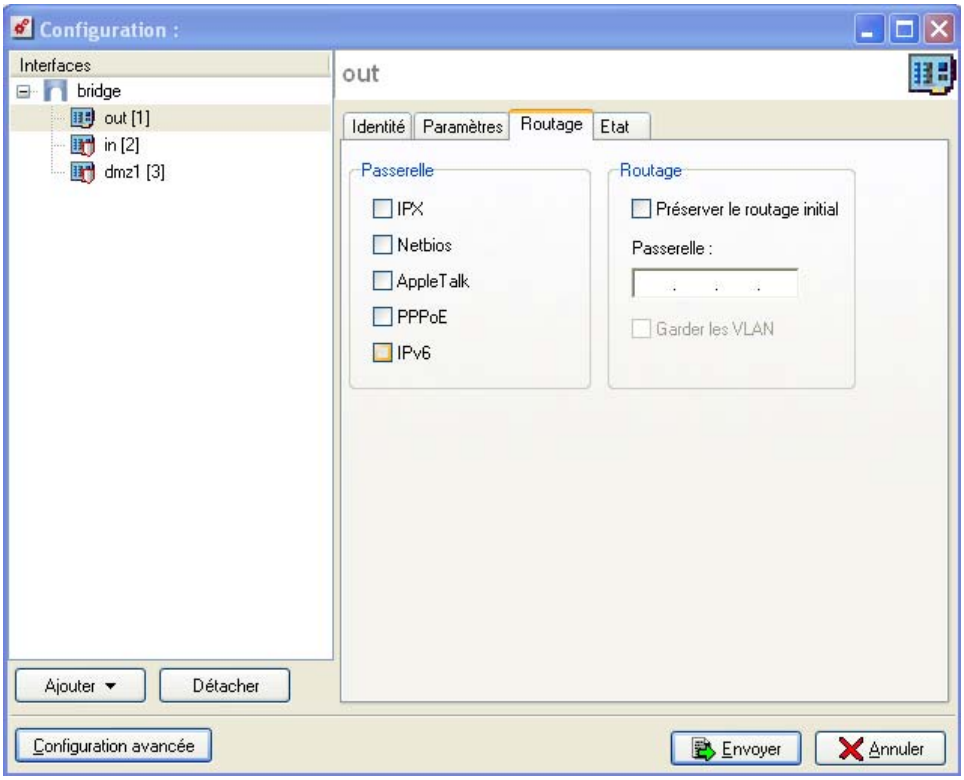


Figure 88 : Configuration - Interface Out – Routage

Passerelle	Permet de laisser passer les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoe ou IPv6 entre les interfaces du pont. Aucune analyse ou aucun filtrage de niveau supérieur n'est réalisé sur ces protocoles (le firewall bloque ou laisse passer).
Routage	Comme son nom l'indique, l'option **Préserver le routage initial** permet de préserver le routage initial des machines connectées sur cette interface. Ainsi vous pouvez spécifier

une passerelle par défaut pour certaines machines tout en spécifiant sur le firewall une passerelle pour celles qui n'en ont pas. Cette option facilite l'intégration du firewall dans une architecture composée de nombreuses passerelles différentes.
Le champ "Passerelle" sert au routage par interface. Tous les paquets arrivant sur cette interface seront routés via une passerelle.

L'option **Garder les VLAN** permet la transmission des trames taggées sans que le firewall soit terminaison du VLAN. Le tag VLAN de ces trames sont conservées ainsi le firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par le firewall. Le firewall agit de manière complètement transparente pour ce VLAN.

Onglet Etat

L'onglet **Etat** permet de visualiser en temps réel les points d'utilisation de l'interface et de tous les objets et groupes d'objets générés par l'interface (Network_xx, Firewall_xx) dans la configuration de l'Appliance UTM. Cet onglet peut s'avérer utile lors de changements éventuels sur cette interface.

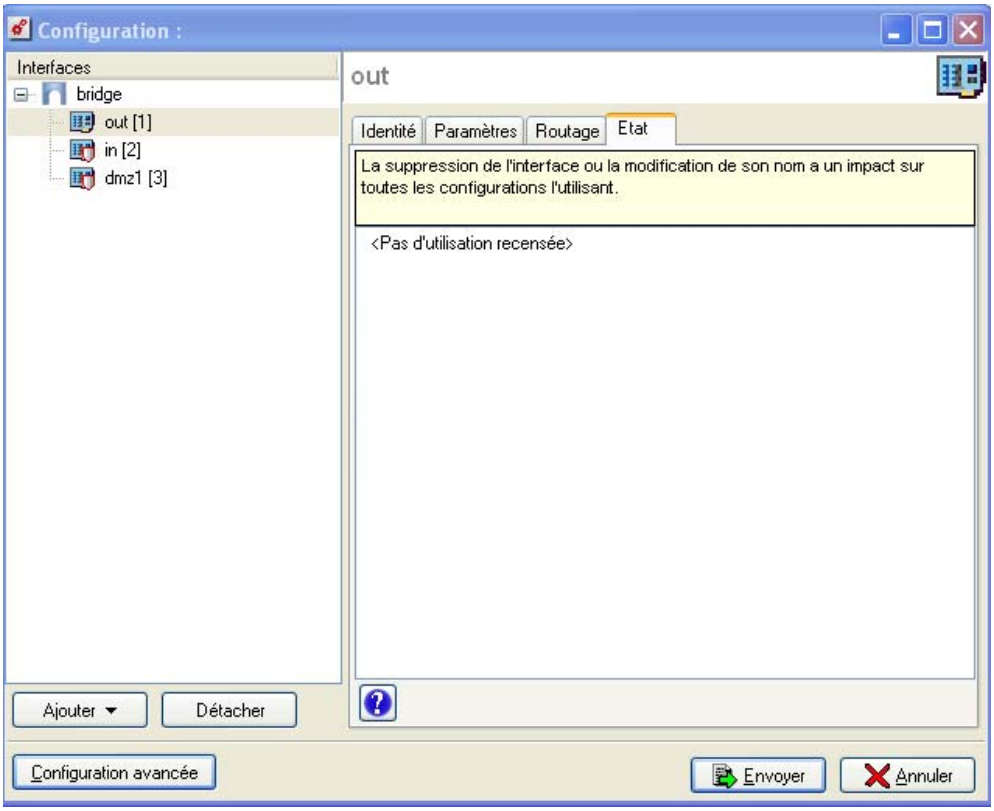


Figure 89 : Configuration - Interface out - Etat

De plus en cliquant sur le bouton , vous obtenez une visualisation plus précise de l'utilisation de l'interface, module par module, ligne par ligne.

AVERTISSEMENT
La suppression de l'interface ou la modification de son nom a un impact sur toutes les configurations l'utilisant.

5.2.2.4. Interface en mode avancé

Pour configurer une interface dans un réseau ne faisant pas partie d'un bridge, il suffit de la sortir de l'arborescence du bridge avec la souris ou en cliquant sur le bouton droit une fois l'interface sélectionnée et en sélectionnant **Détacher**. Vous pouvez ensuite configurer les paramètres de l'interface.

Lors du détachement, l'écran suivant s'affiche :

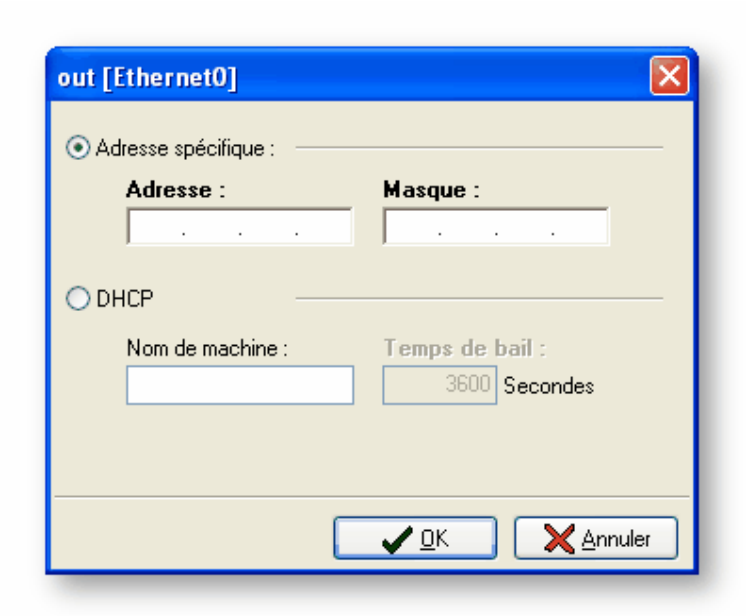


Figure 90 : Out (Ethernet)

Adresse spécifique	Indiquez une adresse IP à votre interface ainsi que le masque de sous-réseau.
DHCP	Indiquez un nom de machine, et un Temps de bail.

Onglet Identité

La fenêtre de configuration est identique à celle de l'interface en mode Bridge.

Onglet Paramètres

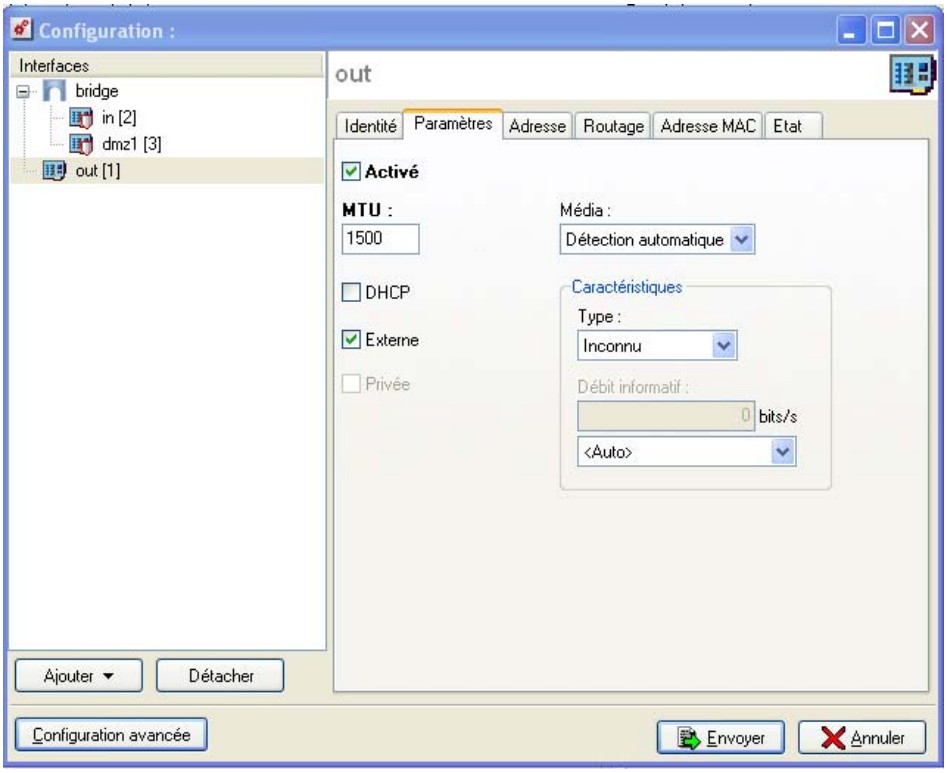


Figure 91 : Configuration - Paramètres

Activé	En cochant/décochant cette option on active/désactive l'interface. En désactivant une interface, on la rend inutilisable. En terme d'utilisation cela peut correspondre à une interface que l'on a prévu de déployer dans un futur proche ou éloigné mais qui n'est pas en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.
MTU	Longueur maximale des trames émises sur le support physique (Ethernet).
DHCP	L'adresse IP de l'interface est fournie par un serveur DHCP (utile pour les connexions Internet via le câble). (*Cf.* *Partie 11/Chapitre 1 : DHCP*).
Externe	Cochez cette option pour indiquer que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface (matérialisé par un bouclier) disparaît lorsque cette option est cochée. (Dans ce cas, le choix est grisé).
Privée	Cette option permet d'indiquer le caractère **Privée** de l'interface. Les adresses des interfaces **Privée** ne sont pas utilisables en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. **NOTE** On notera que **Privée** implique forcement d'être sur une interface protégée. Les options **Externe** et **Privée** sont donc incompatibles.
Média	Vitesse de liaison du réseau. Par défaut, le firewall le détecte automatiquement mais vous pouvez forcer l'utilisation d'un mode particulier. **AVERTISSEMENT** Si le firewall est directement connecté à un modem ADSL, NETASQ vous recommande de forcer le média que vous voulez utiliser sur l'interface en question.

Type	Cette option permet de définir quel type de machines est hébergé sur cette interface. **Machine** = machines de type hôte (utilisateurs), **Serveur** = machines de type serveur et **Inconnu** = type de machine non défini. Ainsi, dans les traces, vous verrez quels types de flux (machine à machine, machine à serveurs ...) transitent par le firewall.
Débit Informatif	En spécifiant le type de liaison Internet, il est possible de définir un débit maximal. Cette information n'est cependant pas utilisée pour réguler le trafic, ce n'est qu'une indication.

Onglet Adresse

NOTE

Disponible si l'option **DHCP** n'est pas sélectionnée.

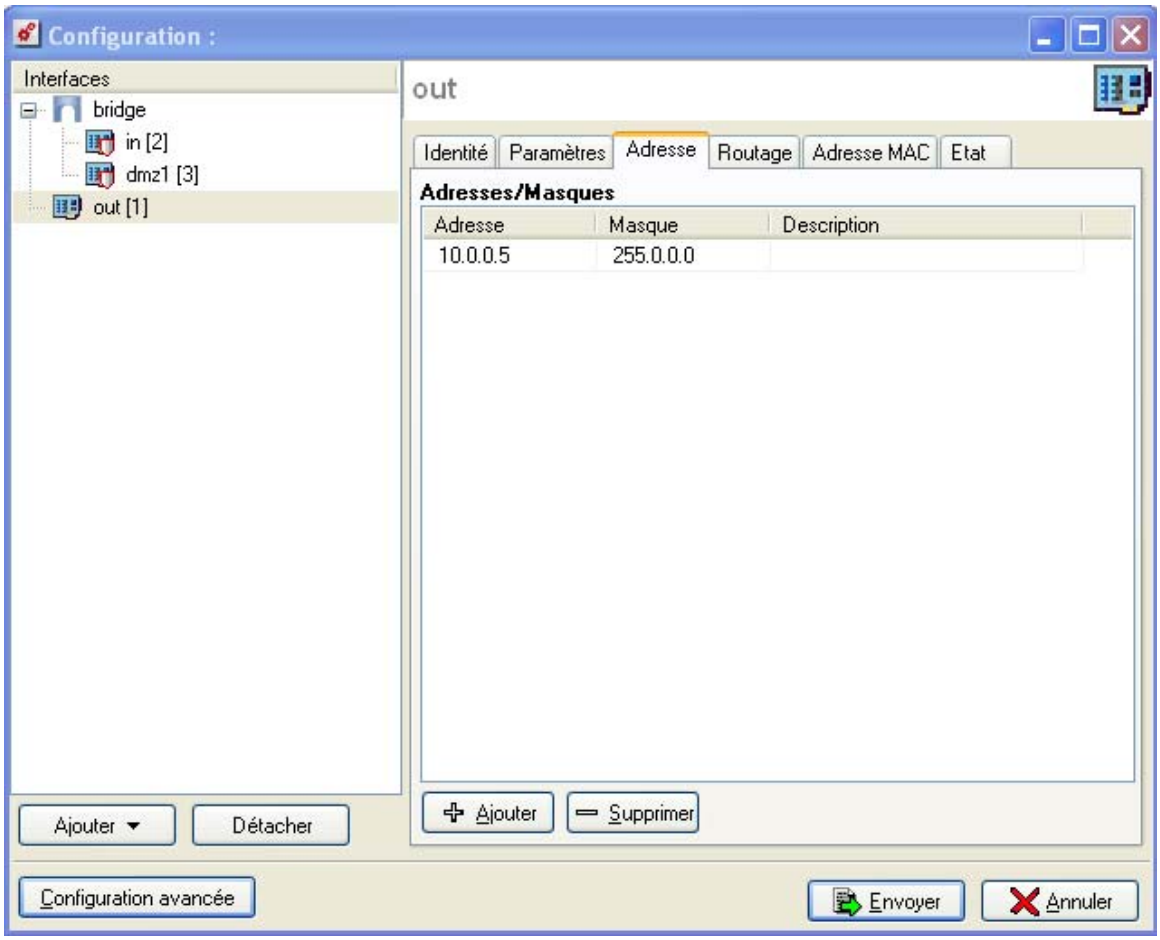


Figure 92 : Configuration - Adresse

Adresse	Adresse IP affectée à l'interface.
Masque	Masque de réseau du sous-réseau auquel appartient l'interface. Si l'option **DHCP** est sélectionnée, l'onglet **`Adresse`** est remplacé par un onglet **`DHCP`** (*Cf.* Partie 11/ Chapitre 1 : *DHCP*).
Description	Permet de spécifier un commentaire pour l'adressage du bridge.

Onglet DHCP

NOTE

Disponible si l'option **DHCP** est sélectionnée.

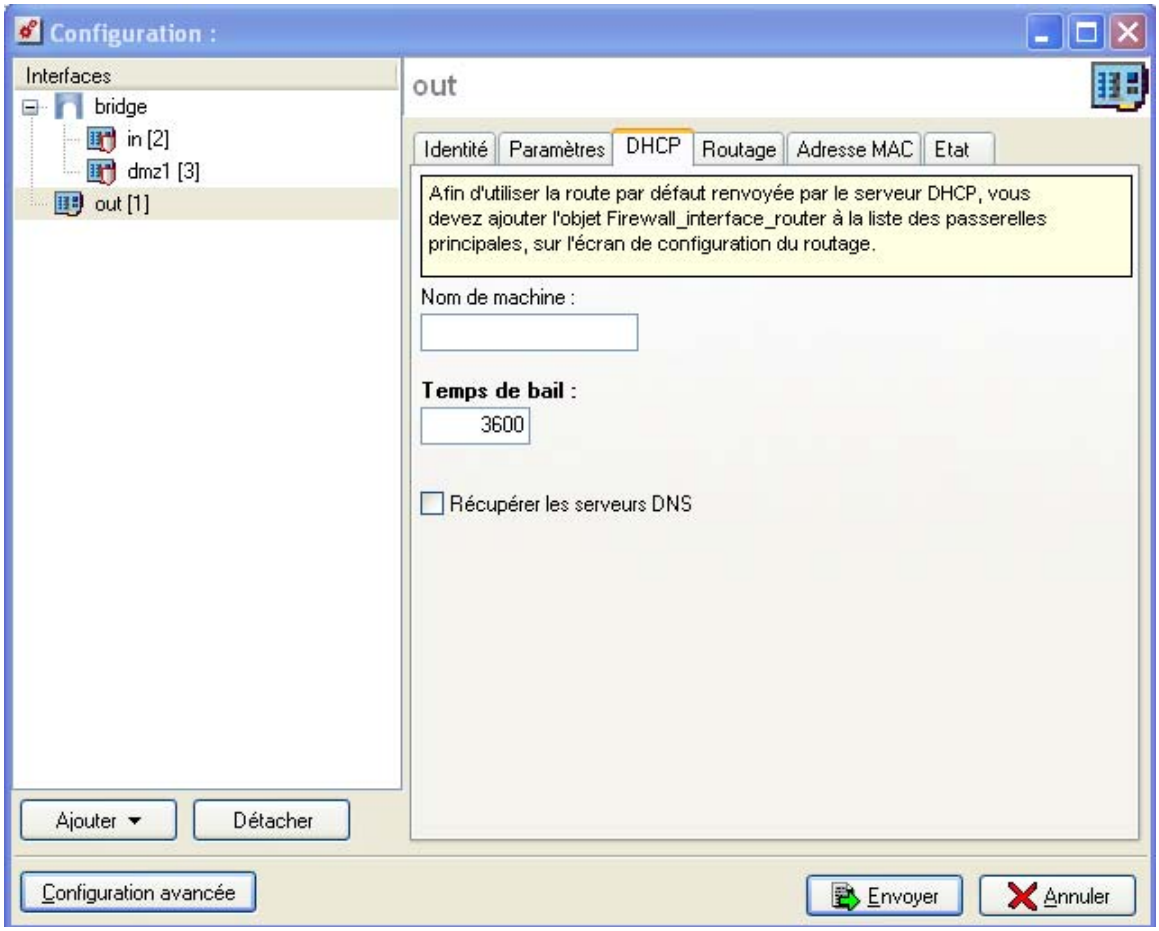


Figure 93 : Configuration - DHCP

Nom de machine	Nom d'utilisateur (FQDN) pour la connexion. Ce champ facultatif, n'identifie pas le serveur DHCP mais le firewall. Si le champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met à jour automatiquement le serveur DNS avec le nom fourni par le firewall et l'adresse IP qui lui a été fournie.
Temps de bail	Période de conservation de l'adresse IP avant renégociation.

Obtenir la route par défaut	Indique que l'interface en DHCP est connectée à la route par défaut du firewall. Si cette option est cochée, le firewall reçoit sa route par défaut auprès du serveur DHCP (fournisseur d'accès par exemple). Elle remplace alors la route par défaut déjà configurée. Il est tout de même indispensable de configurer une route par défaut manuellement dans le firewall pour préserver la stabilité de l'Appliance notamment dans la phase d'obtention de son adresse IP auprès du serveur DHCP. **REMARQUE** Pour utiliser la route par défaut renvoyée par le serveur DHCP, vous devez ajouter l'objet Firewall_interface_router à la liste des passerelles principales, sur l'écran de configuration du routage.
Récupérer les serveurs DNS	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qu'il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'objets : Firewall_<nom de l'interface>_dns1 et Firewall_<nom de l'interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.

ASTUCE

Afin d'utiliser la route par défaut renvoyée par le serveur DHCP, vous devez ajouter l'objet Firewall_<nomdelinterface>_router à la liste des passerelles principales, dans le menu `Routage, onglet Avancé` de l'arborescence de NETASQ UNIFIED MANAGER. Par exemple, si l'interface « out » est configurée en DHCP, l'objet qui correspond à la route par défaut s'appellera « Firewall_out_router ».

Onglet Routage

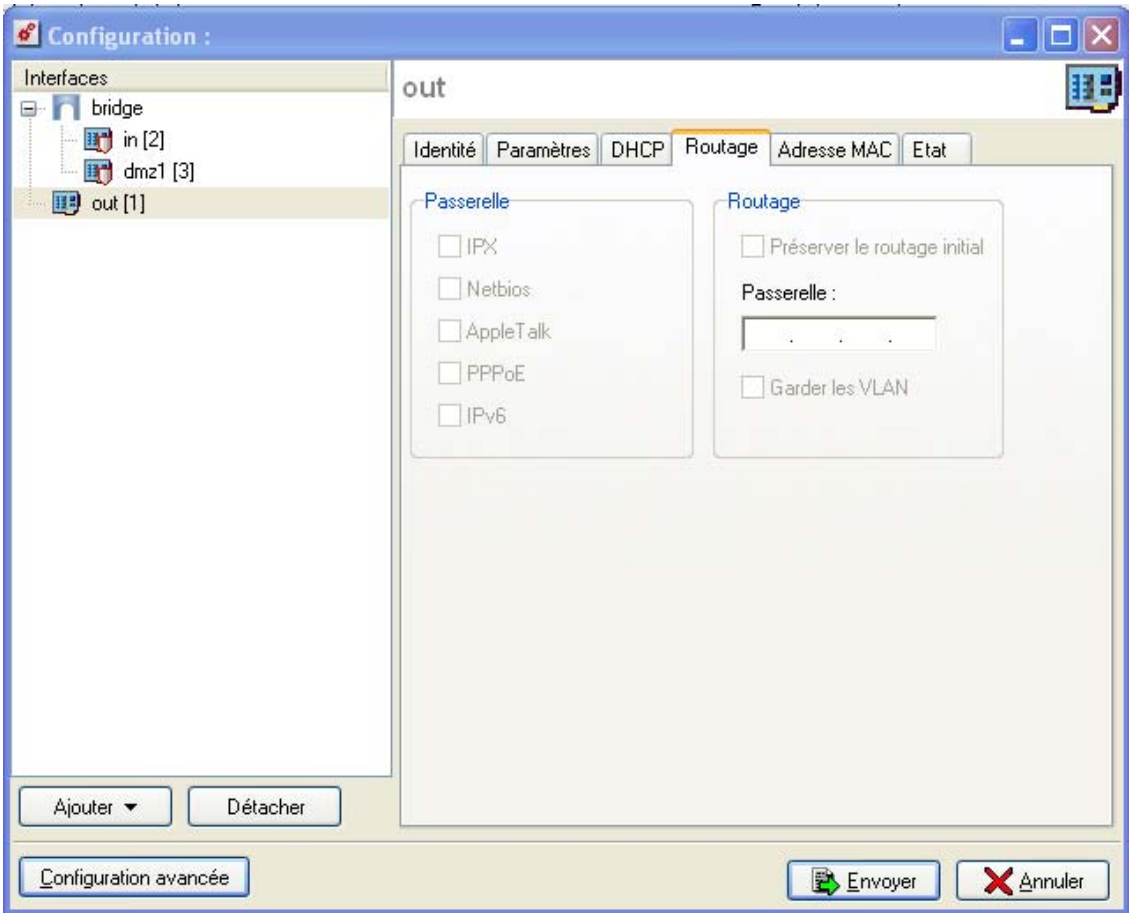


Figure 94 : Configuration Interfaces - Routage

Passerelle	Permet de laisser passer les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoe ou Ipv6 entre les interfaces du pont.
Routage	Comme son nom l'indique l'option **Préserver le routage initial** permet de préserver le routage initial. Le champ "Passerelle" sert au routage par interface.
Garder les VLAN	L'option **Garder les VLAN** permet la transmission des trames taggées sans que le firewall soit terminaison du VLAN. Le tag VLAN de ces trames sont conservées ainsi le firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par le firewall. Le firewall agit de manière complètement transparente pour ce VLAN.

Onglet Adresse MAC

Adresse MAC	Adresse MAC affectée au bridge. (Toutes les interfaces contenues dans le bridge possèdent la même adresse MAC). Pour éditer l'adresse MAC, cliquez sur le bouton  . L'écran ci-dessous s'affiche :

Figure 95 : Edition de l'adresse MAC

Réinitialiser	Remise à zéro du champ "Adresse MAC".

Onglet Etat

L'onglet **Etat** permet de visualiser les points d'utilisation de l'interface et de tous les objets et groupes d'objets générés par l'interface (Network_xx, Firewall_xx) dans la configuration de l'Appliance UTM.

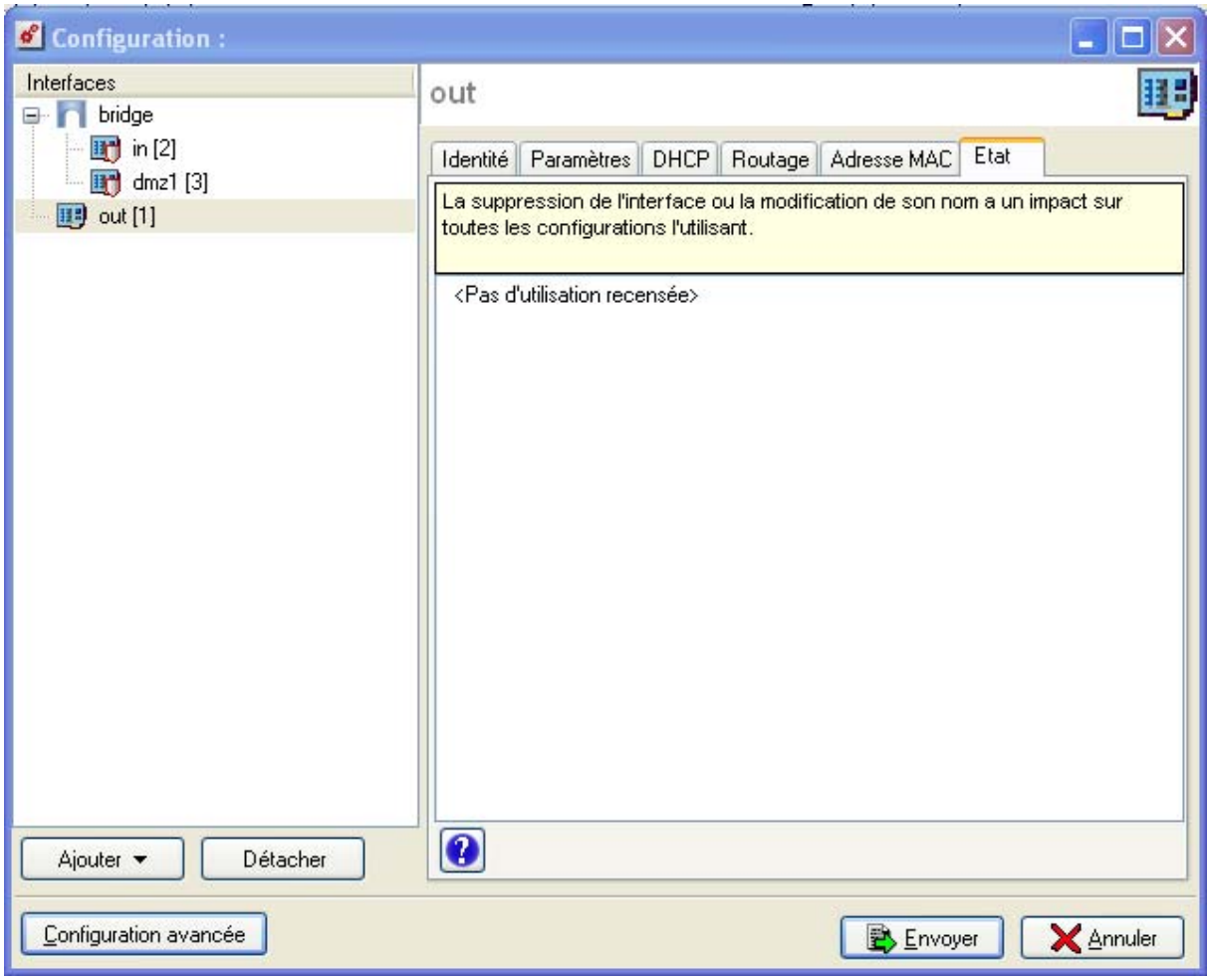


Figure 96 : Configuration - Interface Out - Etat

De plus en cliquant sur le bouton vous obtenez une visualisation plus précise de l'utilisation de l'interface, module par module, ligne par ligne.

AVERTISSEMENT

Afin d'utiliser la route par défaut renvoyée par le serveur DHCP, vous devez ajouter l'objet Firewall_interface_router à la liste des passerelles principales, dans le menu `Routage, onglet Avancé` de l'arborescence de NETASQ UNIFIED MANAGER.

5.2.3. Création d'un Bridge

La création d'un Bridge est réalisée au moyen d'un assistant vous permettant de créer de manière simple l'interface.

1 Sélectionnez le menu **`Réseau\Interfaces`** de l'interface de configuration.

2 Cliquez sur le bouton **Ajouter** puis sélectionnez "Bridge" ou effectuez un clic droit dans l'arborescence de configuration et sélectionnez "Nouveau bridge".
L'écran ci-dessous s'affiche :

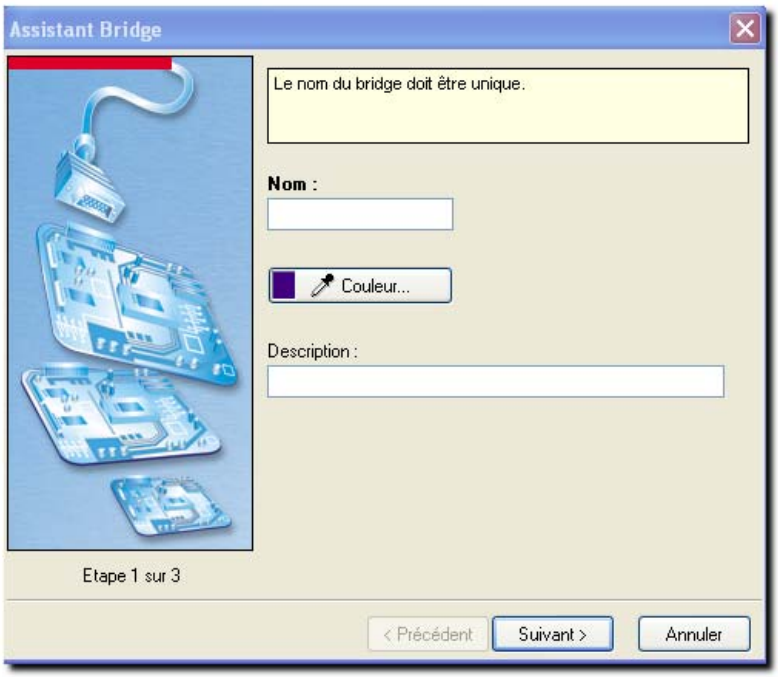


Figure 97 : Assistant Bridge - Etape 1

3 Saisissez un nom unique pour votre Bridge, définissez la couleur. Vous pouvez également donner une description. Cliquez sur le bouton **Suivant**. (Les champs indiqués en gras sont obligatoires).L'écran suivant s'affiche :

Figure 98 : Assistant Bridge - Etape 2

4 Si vous cochez "Adresse", indiquez l'adresse et le masque de sous-réseau du Bridge. Si vous cochez "DHCP", indiquez un nom de machine et le temps alloué (obligatoire). Cliquez ensuite sur le bouton Suivant. L'écran suivant s'affiche :

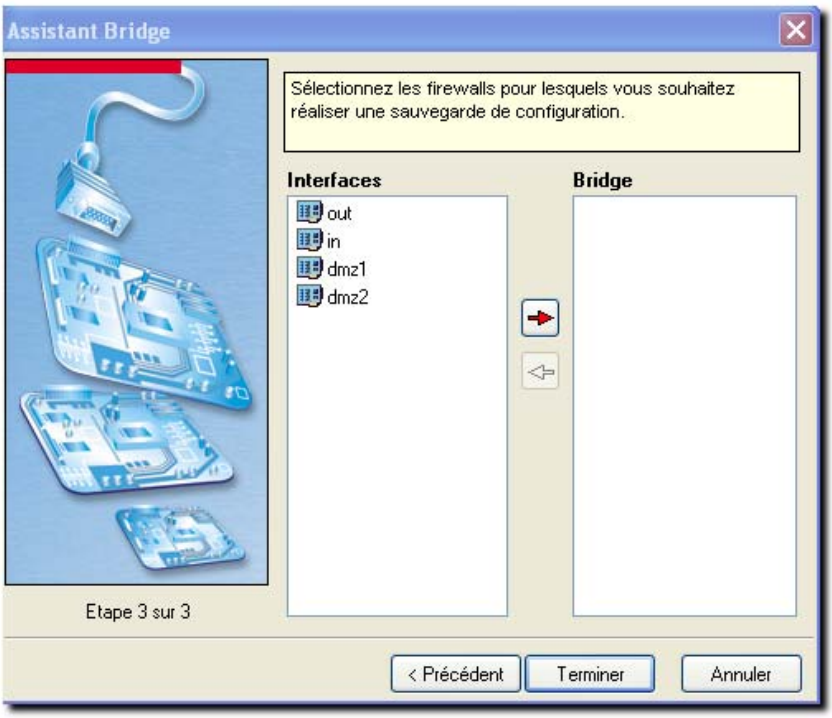


Figure 99 : Assistant Bridge - Etape 3

5 Sélectionnez les firewalls pour lesquels vous souhaitez réaliser une sauvegarde de configuration. La liste "Interfaces" recense les Ethernets et les vlan déjà présents dans la configuration. Il faut sélectionner au moins deux interfaces qui composeront le bridge, soit par l'intermédiaire des flèches, soit en effectuant un drag & drop entre les deux listes. Cliquez sur **Terminer** pour valider la création.

5.2.4. Création d'un VLAN

5.2.4.1. Présentation des VLAN

Un réseau local (LAN) est basé sur le principe de diffusion. Chaque information émise par un équipement connecté sur le LAN est reçue par tous les autres.
Avec l'augmentation du nombre d'équipements raccordés sur le LAN, on aboutit à des situations de saturation. En effet, plus il y a de stations, plus il y a de risques de collisions.

DEFINITION
Les réseaux virtuels (**VLAN** : ***Virtual Local Area Network***) permettent de réaliser des réseaux axés sur l'organisation de l'entreprise. En effet, ils introduisent la notion de segmentation virtuelle, qui permet de constituer des sous-réseaux logiques étanches au sein même d'une architecture réseau. Les VLAN sont donc des regroupements logiques d'utilisateurs ou de stations (qui peuvent représenter l'organisation fonctionnelle de l'entreprise). Tous les membres d'un VLAN sont habilités à communiquer ensemble et forment un domaine de diffusion.

Les VLAN sont définis en fonction d'une marque (tag) des trames Ethernet (norme 802.1q).On peut ainsi définir des domaines de diffusion (domaines de broadcast). Les échanges à l'intérieur d'un domaine sont automatiquement sécurisés par l'étanchéité entre VLAN, et les communications inter domaines peuvent être contrôlées par une passerelle de niveau 3 comme un firewall.
Les UTM NETASQ peuvent se placer en terminaison de VLAN pour ajouter ou retirer un tag VLAN. Le firewall assure le filtrage entre VLAN et assure les communications entre les VLAN et les réseaux connectés aux autres interfaces du firewall.
Les VLAN sont perçus par le firewall comme appartenant à des interfaces virtuelles, ce qui permet leur totale intégration au sein du système de sécurité de l'entreprise.

5.2.4.2. Avantage d'un VLAN

Le VLAN permet :

- Une augmentation des performances en limitant les domaines de diffusion tout en augmentant le nombre.
- A un utilisateur qui déménage de retrouver les mêmes droits d'accès aux ressources LAN sans que l'exploitant n'ait eu à intervenir.

5.2.4.3. Définition des VLAN

Grâce à un firewall NETASQ, il est possible de réaliser du VLAN de ports ou du bridge IP de VLAN.

AVERTISSEMENT
Pour utiliser des interfaces VLAN sur le firewall vous devez obligatoirement posséder des équipements gérant les VLAN sur votre réseau (switchs ou commutateurs).

La configuration d'un VLAN est réalisée au moyen d'un assistant vous permettant de créer de manière simple l'interface.

1. Sélectionnez le menu **`Réseau\Interfaces`** de l'interface de configuration.
2. Sélectionnez l'interface ou le bridge auquel vous désirez associer un VLAN.

3 Cliquez sur le bouton **Ajouter** et sélectionnez **`vlan sur…`**ou cliquez avec le bouton droit de la souris et sélectionnez **`Nouveau VLAN`** dans le menu contextuel.

4 L'écran ci-dessous s'affiche :

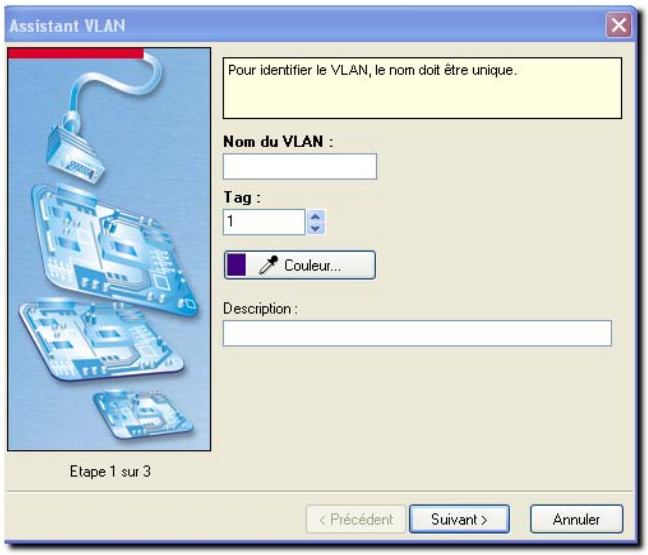


Figure 100 : Assistant VLAN - Etape 1

1 Etape 1

Saisissez un nom unique pour votre VLAN, sélectionnez un numéro de tag (ce numéro doit être unique pour chaque VLAN ayant pour support physique la même Ethernet), définissez la couleur. Vous pouvez également donner une description. Cliquez sur le bouton **Suivant**. (Les champs indiqués en gras sont obligatoires).

Figure 101 : Assistant VLAN - Etape 2

2 Etape 2

Cochez l'une des deux options suivantes pour donner une adresse au VLAN (soit manuellement, soit par DHCP). Cliquez sur le bouton **Suivant**.

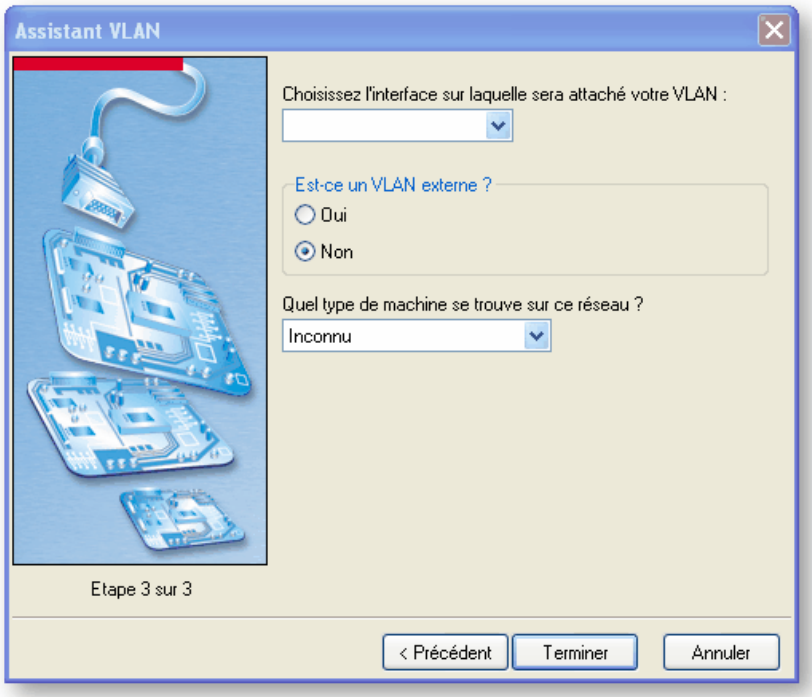


Figure 102 : Assistant VLAN - Etape 3

REMARQUE
Cette seconde étape peut être inexistante si le VLAN est créé avec un bridge prédéterminé (via le menu de création de l'arborescence des interfaces avec un bridge comme interface courante.

Etape 3
Sélectionnez l'interface sur laquelle sera attaché le VLAN. Puis cochez entre l'option **Oui** ou **Non** pour déterminer si vous souhaitez une interface externe ou pas. Enfin, définissez quel type de machine se trouve sur le réseau parmi les options proposées **Inconnu**, **Machine**, et **Serveur**.

REMARQUE
Lorsqu'on développe le bouton **Ajouter**, l'interface sur laquelle on va insérer un VLAN est rappelée.

Onglet Identité

Les informations à spécifier dans l'assistant sont décrites dans les tableaux suivants.

Nom	Nom que vous affectez au VLAN. *(Cf. Annexe M : Noms interdits)*.
Couleur	Couleur attribuée au VLAN. Ces couleurs seront très utiles pour vous aider lors de la mise en place des règles de filtrage, des translations... En effet, chaque objet créé prendra une couleur en fonction de la zone à laquelle l'adresse IP appartient.
Description	Commentaire associé au VLAN.
Client DNS dynamique	Lorsque votre firewall ne possède d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc.). Il est possible d'associer via un fournisseur de services DNS (dyndns.org par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter ce firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique vous avez préalablement configuré. La configuration des clients DNS

	dynamique est expliquée dans la suite du document (Cf. Partie 5/Chapitre 2 : *Client DNS dynamique*).

Onglet Paramètres

Activé	En cochant/décochant cette option on active/désactive l'interface. En désactivant une interface, on la rend inutilisable. En terme d'utilisation cela peut correspondre à une interface que l'on a prévu de déployer dans un futur proche ou éloigné mais qui n'est pas en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.
Tag	Ce champ permet de spécifier quelle sera la valeur associée au VLAN dans les paquets transitant sur le réseau. Ce tag identifie le VLAN et est utilisé au niveau Ethernet.
MTU	Longueur maximale des trames émises sur le support physique (Ethernet). Ce choix n'est pas disponible pour une interface contenue dans un bridge hormis dans le cas des interfaces VLAN.
DHCP	L'adresse IP du VLAN est fournie par un serveur DHCP (utile pour les connexions Internet via le câble). (cf. configuration de l'interface par DHCP). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Externe	Cochez cette option pour indiquer que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface (matérialisé par un bouclier) disparaît lorsque cette option est cochée.
Privée	Cette option permet d'indiquer le caractère privée de l'interface. Les adresses des interfaces "Privée" ne sont pas utilisables en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. **NOTE** On notera que **Privée** implique forcement d'être sur une interface protégée. Les options **Externe** et **Privée** sont donc incompatibles.
Média	Ce champ permet de définir physiquement quelle est l'interface de terminaison du VLAN.
Type	Cette option permet de définir quel type de machines est hébergé sur ce VLAN. **Machine** = machines de type hôte (utilisateurs), **Serveur** = machines de type **serveur et inconnu** = type de machine non défini. Ainsi, dans les traces, vous verrez quels types de flux (machine à machine, machine à serveurs ...) transitent par le firewall.
Débit informatif	En spécifiant le type de liaison Internet, il est possible de définir un débit maximal. Cette information n'est cependant pas utilisée pour réguler le trafic, ce n'est qu'une indication.

Onglet Adresse

Adresse	Adresse IP affectée à l'interface VLAN.
Masque	Masque de réseau du sous-réseau auquel appartient l'interface. Si l'option **DHCP** est sélectionnée, l'onglet **Adresse** est remplacé par un onglet **DHCP** (*Cf.* Partie 11/Chapitre 1 : DHCP).
Description	Permet de spécifier un commentaire pour l'adressage du bridge.

Cet onglet n'est bien sûr pas disponible pour un VLAN sur un bridge.

Onglet Routage

Passerelle	Permet de laisser passer les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoe ou Ipv6 entre les interfaces du pont.
Routage	Comme son nom l'indique l'option **Préserver le routage initial** permet de préserver le routage initial. Le champ "Passerelle" sert au routage par interface. L'option **Garder les VLAN** permet la transmission des trames taguées sans que le firewall soit terminaison du VLAN. Le tag VLAN de ces trames sont conservées ainsi le firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par le firewall. Le firewall agit de manière complètement transparente pour ce VLAN.

L'UTM NETASQ réalise un filtrage au niveau IP, il faut donc associer à chaque VLAN, une adresse IP différente (le firewall maintient une table de correspondance entre un tag Ethernet et une adresse IP. Lorsqu'un paquet provenant d'un VLAN arrive au firewall, le tag Ethernet du VLAN sert à retrouver l'adresse IP qui sera utilisée dans les règles de filtrage).

Onglet Etat

L'onglet **`Etat`** permet de visualiser les points d'utilisation de l'interface et de tous les objets et groupes d'objets générés par l'interface (Network_xx, Firewall_xx) dans la configuration du firewall.

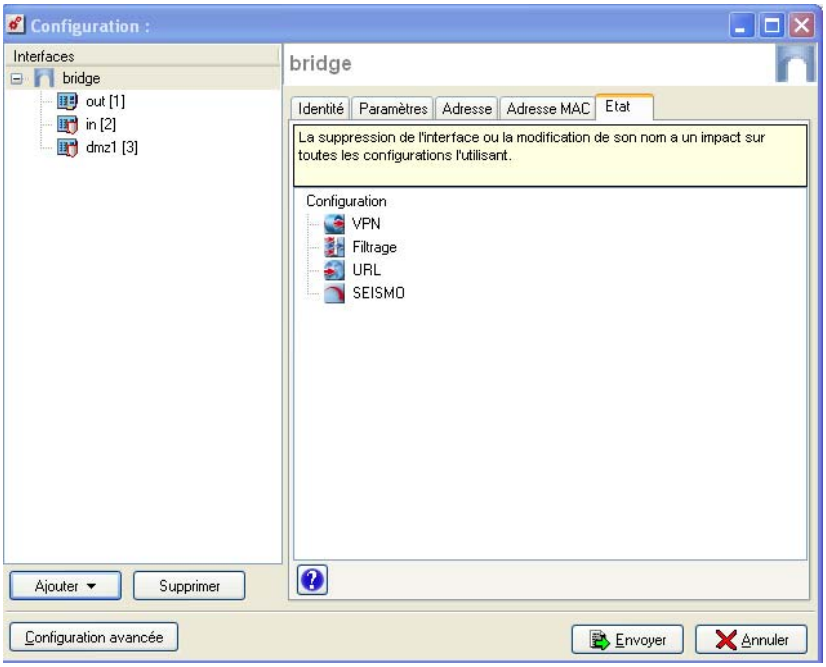


Figure 103 : Configuration interface - Bridge - Etat

De plus en cliquant sur le bouton , vous obtenez une visualisation plus précise de l'utilisation de l'interface, module par module, ligne par ligne.

5.2.4.4. VLAN dans un bridge

Dans la configuration des VLAN pour les bridges, il est possible d'utiliser le même tag pour deux interfaces VLAN associées à des interfaces physiques d'un même bridge. Ainsi le firewall apparaît de manière transparente sur le réseau. Cette méthode nécessite l'utilisation d'une interface VLAN par interface physique concernée.
Contrairement à l'option **Garder les VLAN** (qui rend le firewall complètement transparent par rapport au VLAN et qui empêche donc l'utilisation de fonctionnalités qui consisterait à couper le flux VLAN, par exemple les proxies), cette méthode de préservation du tag VLAN entre plusieurs interfaces d'un même bridge permet l'utilisation complète des fonctionnalités du firewall.

5.2.4.5. Paramètres avancés

Si vous souhaitez créer un nouveau VLAN et que vous êtes arrivé au maximum du nombre dynamique de VLAN possible, vous avez la possibilité d'en augmenter le nombre.
NETASQ UNIFIED MANAGER vous propose l'écran des paramètres avancés lorsque ce nombre est atteint. Cet écran vous permet de régler le nombre dynamique de VLAN possible.

L'ajout de VLAN s'effectue par tranche mais de manière complètement transparente pour l'utilisateur : par exemple, supposons que vous avez un boîtier U70. Dans ce cas, 32 VLAN maximum sont alloués en sortie d'usine mais 0 sont configurés. Supposons également que l'ajout de VLAN s'effectue par tranche de 8.
Vous souhaitez configurer votre premier VLAN :

- L'interface graphique de NETASQ UNIFIED MANAGER vous dirige vers l'écran des paramètres avancés pour augmenter le nombre de VLAN et vous avertit qu'il faut redémarrer le boîtier. Une tranche de 8 VLAN vous est allouée. Vous configurez le 1er VLAN. Mais vous pouvez en configurer 7 autres sans qu'il y ait nécessité de redémarrer le firewall.
- Vous souhaitez configurer un 9ème VLAN, une nouvelle tranche est alors nécessaire. Vous êtes averti que le firewall va redémarrer. Vous effectuerez ensuite la configuration du VLAN.

A la sortie d'usine de votre boîtier, un nombre de VLAN maximum est alloué selon le modèle. Le tableau ci-dessous vous indique le nombre de VLAN alloué maximum :

Modèles	Nbre VLAN max
U30, U70	32
U120, U250, U450	128
U1100, U1500	256
U6000	512

Au niveau du panneau de configuration des interfaces réseaux se trouve le bouton **Options avancées** qui vous permet d'augmenter votre nombre de VLAN.
Lorsque vous cliquez sur ce bouton, l'écran suivant s'affiche :

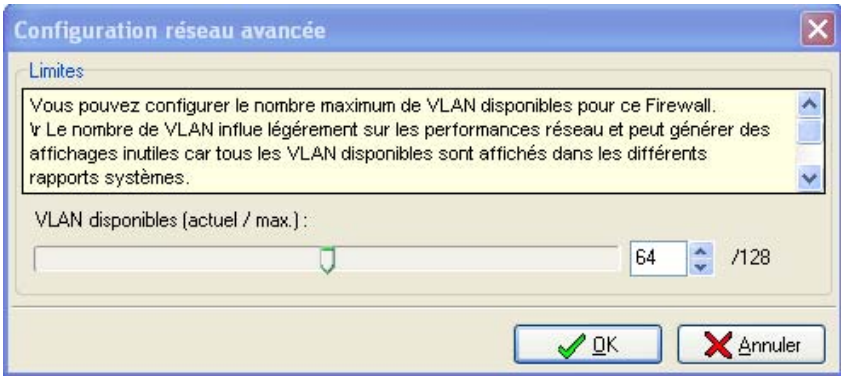


Figure 104 : Paramètres avancés

Cet écran vous permet de choisir le nombre de VLAN souhaité. Il suffit de glisser la jauge pour augmenter ou diminuer le nombre. Si le nombre de VLAN indiqué correspond à une nouvelle tranche, dans ce cas, le firewall devra redémarrer avant configuration (pour un ajout ou une suppression).

AVERTISSEMENT
Toute modification réalisée au niveau de la configuration réseau avant augmentation du nombre dynamique de VLAN sera perdue étant donné la fermeture de cet écran. Un message d'avertissement vous en informe.

5.2.5. Création d'une dialup

5.2.5.1. Création

Les interfaces dialup sont utilisées dans le cas de connexions distantes lorsque votre modem est branché directement sur le firewall (port série ou Ethernet). Le firewall accepte tout type de modem (ADSL, RNIS, RTC, ...).

La création de nouvelles interfaces dialup (par défaut, il existe déjà les interfaces "dialup" et "atldialup") se fait grâce à un assistant. Le nombre maximal de dialup disponibles sur votre firewall dépend du modèle.

1. Sélectionnez le menu **Réseau\Interfaces** de l'interface de configuration.
2. Cliquez sur le bouton **Ajouter** et sélectionnez **Dialup** ou cliquez avec le bouton droit de la souris et sélectionnez **Nouvelle dialup** dans le menu contextuel.

L'écran ci-dessous s'affiche :

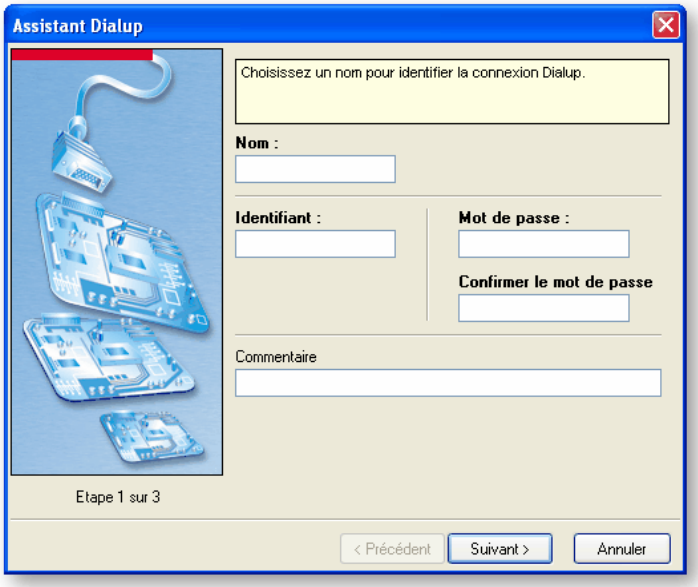


Figure 105 : Assistant dialup - Etape 1

4 Indiquez un nom (obligatoire), identifiant (obligatoire), mot de passe (obligatoire) et description pour identifier la connexion Dialup. Puis cliquez sur le bouton **Suivant**.

5 Choisissez le type de dialup entre PPPoe, PPTP, PPP ou L2TP. L'écran de configuration varie selon le type de dialup.

Si vous cochez **PPPoe**, l'écran suivant s'affiche :

Figure 106 : Assistant Dialup -PPPoE - Etape 2

Sélectionnez l'interface réseau utilisé pour le dialup.

Si vous cochez **PPTP**, l'écran suivant s'affiche :

Figure 107 : Assistant Dialup- PPTP - Etape 2

Saisissez l'adresse IP du modem.

Si vous cochez **PPP**, l'écran suivant s'affiche :

Figure 108 : Assistant Dialup - PPP - Etape 2

Indiquez le n° de téléphone utilisé pour le dialing.

Si vous cochez **L2TP**, l'écran suivant s'affiche :

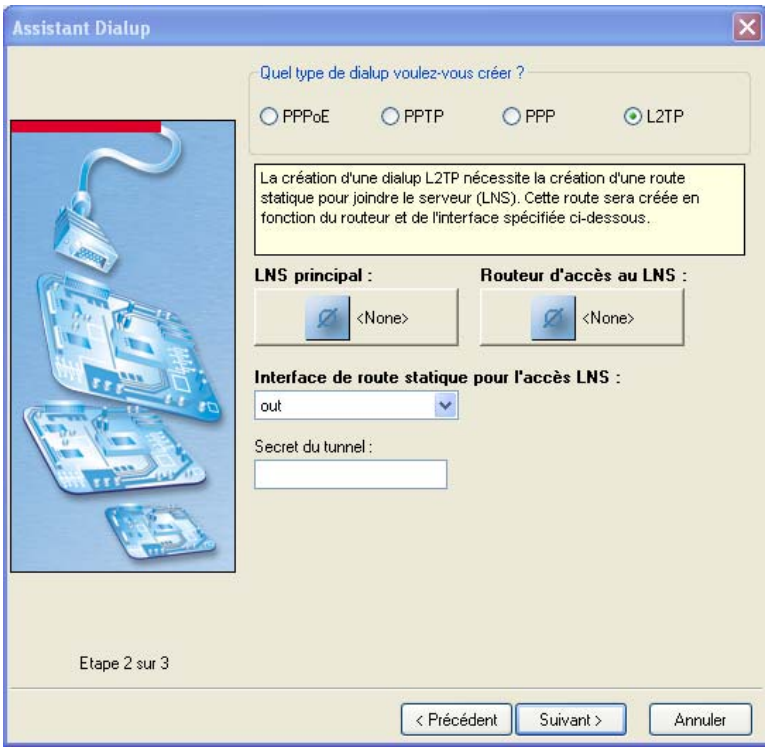


Figure 109 : Assistant Dialup - L2TP - Etape 2

Pour créer une dialup L2TP, définissez le LNS principal le routeur pour accéder au LNS principal et l'interface qui permettront la création de la route statique, utile pour joindre le serveur (LNS). Enfin, indiquez l'authentification du Peer du LNS (sous forme de clé).

6 Une fois l'étape 2 configurée, cliquez sur le bouton **Suivant**. L'écran suivant s'affiche :

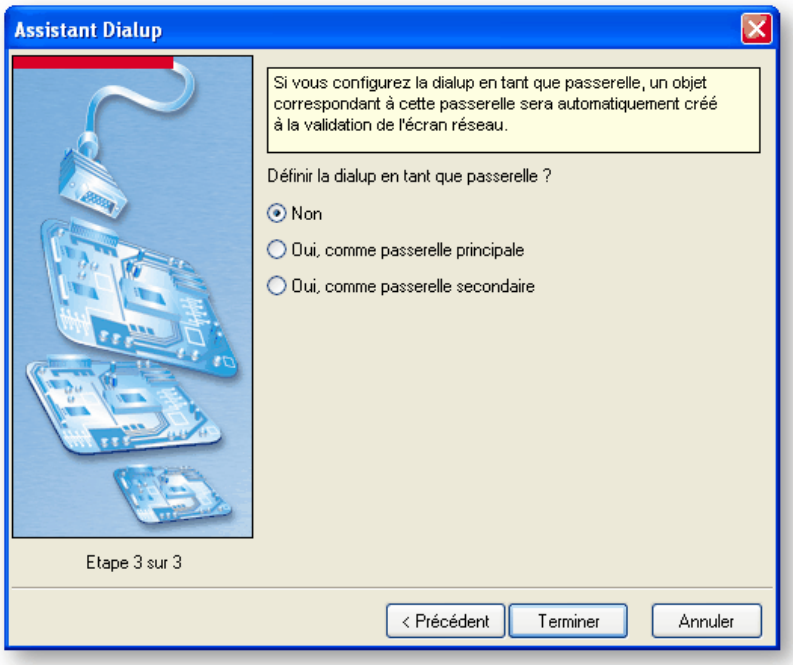


Figure 110 : Assistant Dialup - Etape 3

Choisissez si vous souhaitez définir la dialup en tant que passerelle.
Si oui : 2 options sont proposées : **Oui, comme passerelle principale** ou **Oui, comme passerelle secondaire.**
Cliquez sur **Terminer** pour valider la création de la dialup.

5.2.5.2. Configuration

Vous pouvez ensuite configurer les paramètres suivants de l'interface :

Onglet Identité

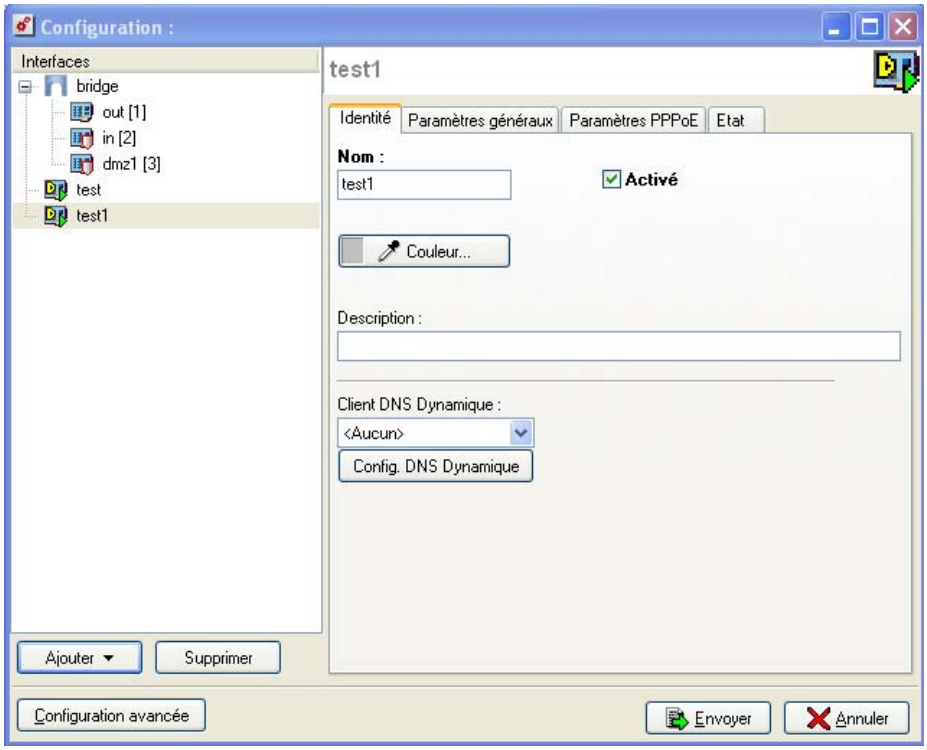


Figure 111 : Configuration - Dialup - Identité

Nom	Nom que vous affectez à la connexion distante. (*Cf. Remarques pour connaître les noms interdits*).
Activé	En cochant/décochant cette option on active/désactive l'interface. En désactivant une interface, on la rend inutilisable. En terme d'utilisation cela peut correspondre à une interface que l'on a prévu de déployer dans un futur proche ou éloigné mais qui n'est pas en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.
Couleur	Couleur attribuée à la connexion distante. Ces couleurs seront très utiles pour vous aider lors de la mise en place des règles de filtrage, des translations... En effet, chaque objet créé prendra une couleur en fonction de la zone à laquelle l'adresse IP appartient.
Description	Commentaire associé à la connexion distante.
Client DNS dynamique	Lorsque votre firewall ne possède d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès.). Il est possible d'associer via un fournisseur de services DNS (dyndns.org par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter ce firewall sans pour autant connaître son adresse IP.

	Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique vous avez préalablement configuré. La configuration des clients DNS dynamique est expliquée dans la suite du document (*Cf. Partie 5/Chapitre 2 : Clients DNS dynamique*).

Deux connexions dialup (ou plus) peuvent être actives en même temps. Cette configuration a l'avantage de permettre de répartir les connexions sortantes entre elles. (*Cf.Partie 5/Chapitre 3 : Interfaces\Routage*).

Onglet Paramètres Généraux

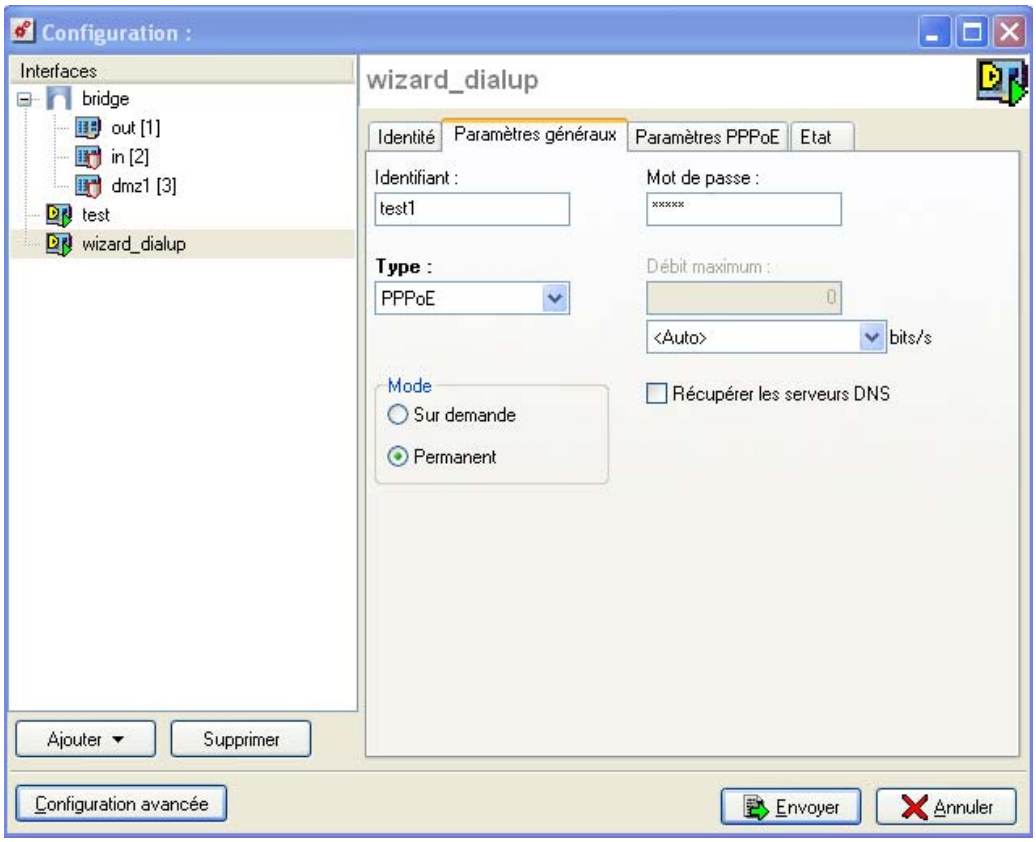


Figure 112 : Configuration - Dialup - Paramètres généraux

Identifiant	Identifiant chez le fournisseur d'accès.
Mot de passe	Mot de passe correspondant au login du fournisseur d'accès.
Type	Le type de connexion distante peut être PPP (RNIS, RTC), PPPoe (ADSL), PPTP (ADSL) ou L2TP. **REMARQUE** La sélection d'un type de dialup entraîne l'activation d'un onglet du même nom pour la configuration.
Débit Maximum	En spécifiant le type de liaison Internet, il est possible de définir un débit maximal. Cette information n'est cependant pas utilisée pour réguler le trafic, ce n'est qu'une indication.
Mode	Le mode **Sur demande** n'établit la connexion avec Internet que lorsqu'une demande de connexion émane du réseau interne (ce mode est plus économique dans le cas d'une liaison payante à la durée). Le mode **Permanent** conserve la

	connexion vers l'Internet active en permanence.
Récupérer les serveurs DNS	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qu'il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'objets : Firewall_<nom de l'interface>_dns1 et Firewall_<nom de l'interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.

Onglet Paramètres PPPoE

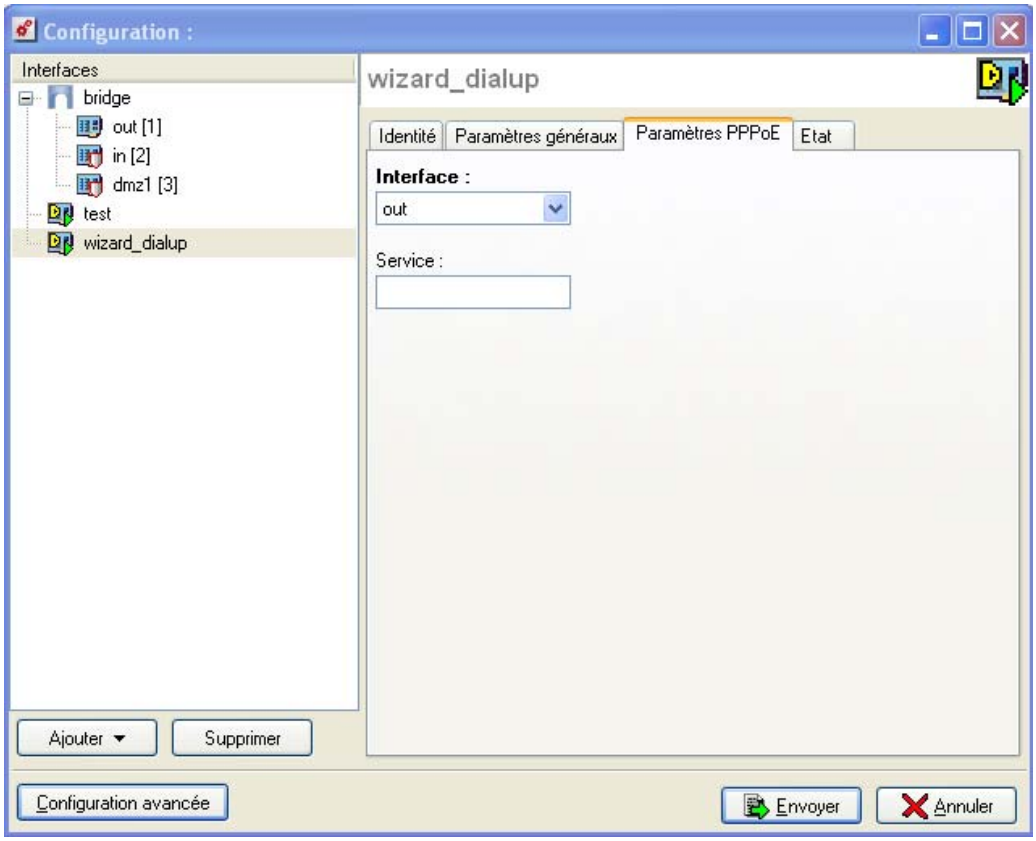


Figure 113 : Configuration - Dialup - Paramètres PPPoE

Interface	Indication des interfaces.
Service	Type de service PPPoe utilisé. Cette option permet de différencier plusieurs modems ADSL. Par défaut, laissez ce champ vide.

Onglet Paramètres PPP

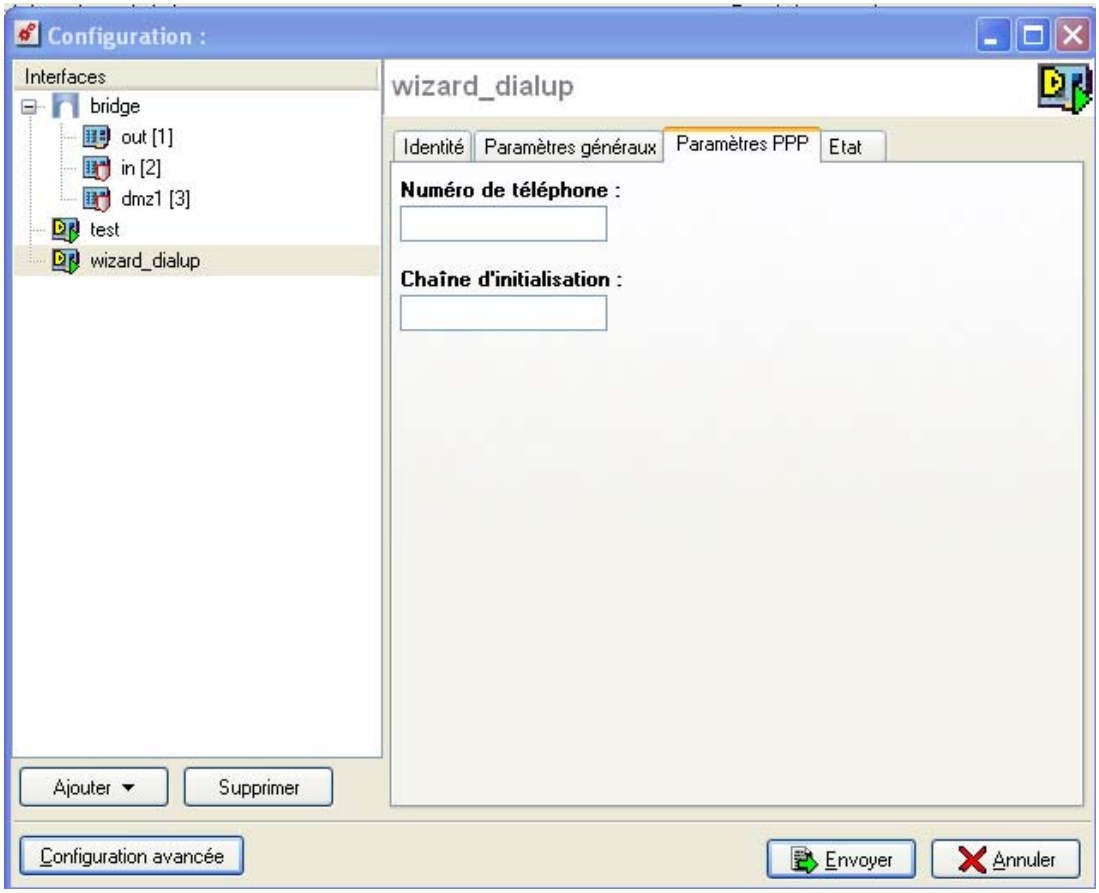


Figure 114 : Configuration - Dialup - Paramètres PPP

NOTE
Lorsque le type de connexion choisi est PPP.

Numéro de téléphone (obligatoire)	Numéro d'appel chez le fournisseur d'accès.
Chaîne d'initialisation (obligatoire)	Chaîne de caractères servant optionnellement à initialiser la connexion.

Onglet Paramètres PPTP

NOTE
Lorsque le type de connexion choisi est PPTP.

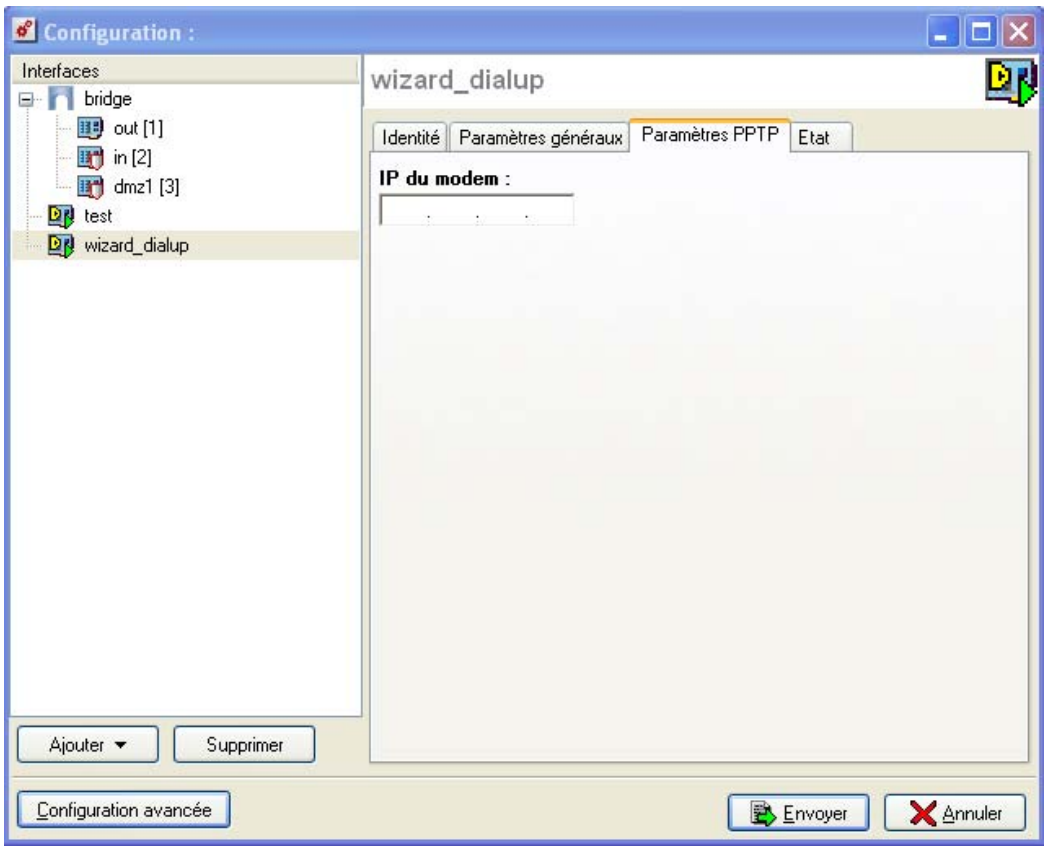


Figure 115 : Configuration - Dialup - Paramètres PPTP

IP du modem	Adresse IP interne du modem ADSL.

Onglet Paramètres L2TP

NOTE
Lorsque le type de connexion choisi est L2TP.

Les options de l'onglet **`Paramètres L2TP`** sont divisées en deux menus dont les paramètres sont expliqués ci-dessous.

Onglet Général

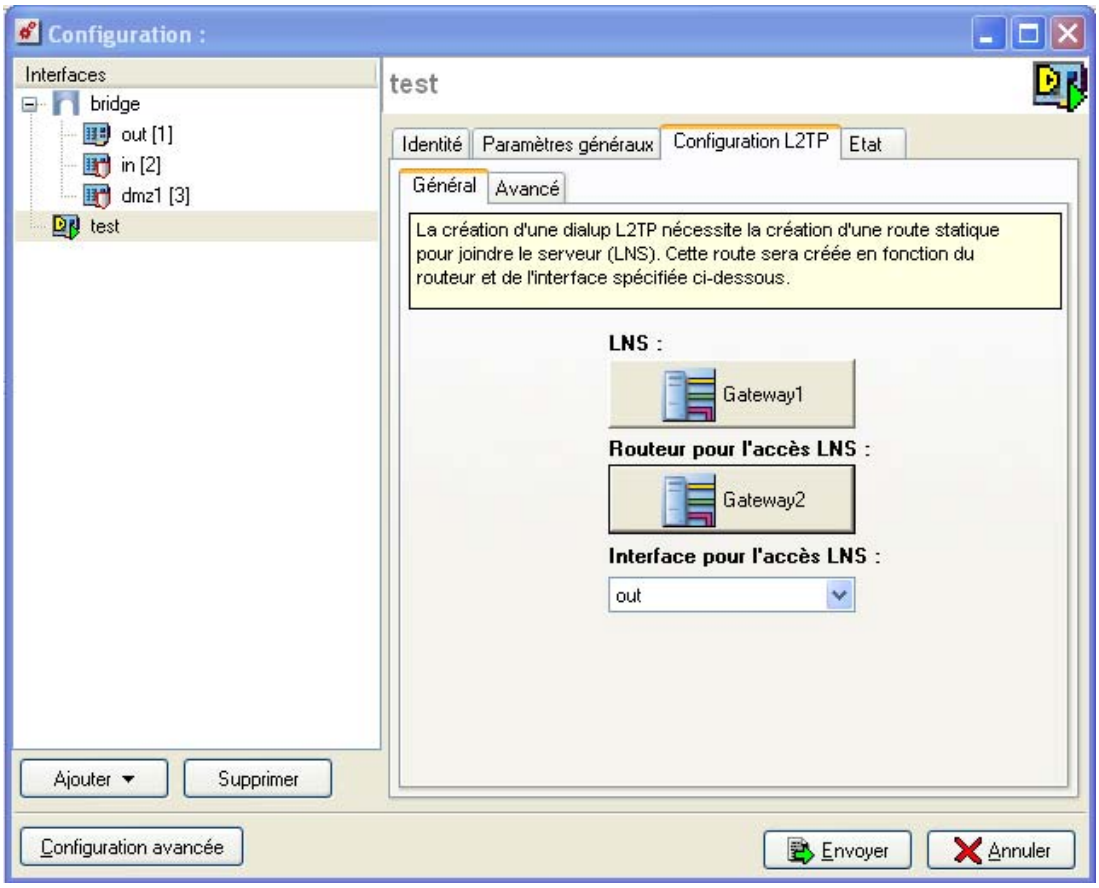


Figure 116 : Configuration - Dialup - Configuration L2TP

LNS	Adresse IP du serveur L2TP distant (LNS) utilisé pour la connexion L2TP.
Routeur pour l'accès LNS	La création d'une Dialup L2TP nécessite une route statique d'accès au serveur L2TP (LNS) définie par un routeur d'accès et l'interface à laquelle il est connecté. Cette option permet de définir le routeur d'accès.
Interface pour l'accès LNS	Nom de l'interface sur laquelle est relié le routeur LNS.

Onglet Avancé

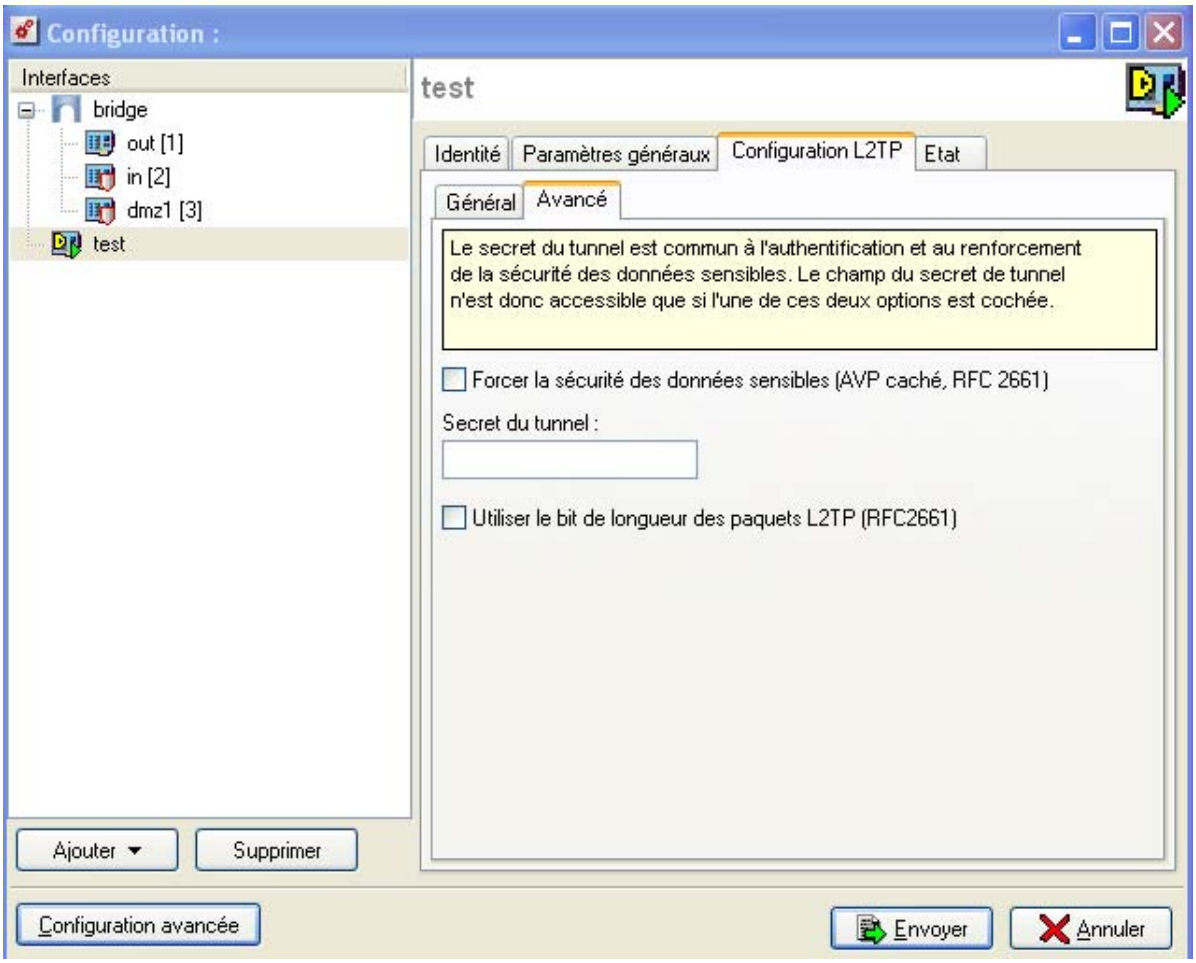


Figure 117 : Configuration - Dialup - Configuration L2TP

Forcer la sécurité des données sensibles (AVP caché, RFC 2661)	Certaines données sensibles transitant dans le tunnel L2TP peuvent être protégées (masquage de mots de passe par exemple) lors de l'échange.
Secret du tunnel	Champ utilisé pour la définition du secret partagé indispensable aux options Authentification du correspondant L2TP par secret partagé et Protection des données sensibles (Hidden AVP).
Utiliser le bit de longueur des paquets L2TP (RFC2661)	La RFC L2TP définit que l'utilisation de ce champ soit facultative. Par défaut ce champ n'est donc pas utilisé mais dans le cas où cela serait nécessaire (demande du serveur par exemple), cochez cette option.

5.2.5.3. Remarques générales sur la configuration de la dialup

- Le firewall négocie automatiquement l'ouverture de ligne et réinitialise la connexion en cas de coupure. Dans le cas où la connexion n'est pas possible (problème de ligne), le firewall envoie un message d'alarme.
- Le firewall crée un objet firewall_dialup représentant l'interface de connexion à Internet. Vous devez utiliser cet objet dans les règles de translation et de filtrage.
- Pour autoriser les connections PPTP, il faut aussi ajouter des règles de filtrage.

CHAPITRE 3 : ROUTAGE

5.3.1. Présentation du routage

L'acheminement des données est une tâche essentielle de tout équipement réseau. L'architecture réseau, devenant de plus en plus complexe, il est essentiel de définir des règles de routage optimales. Les firewalls NETASQ offrent différentes fonctionnalités comme le routage statique, le partage de charge (ou load balancing) ou encore de politique de routage (PBR : *Policy Based Routing*).

Plusieurs mécanismes de routage existent afin de délivrer ces paquets.

ROUTAGE STATIQUE

Basé sur la table de routage du boitier, le routage statique consiste à évaluer le paquet IP traité avec les différentes entrées de la table. Si l'adresse destination correspond à une entrée, identifiée par une adresse (machine ou réseau), le paquet est transmis à la passerelle définie pour cette entrée.

ROUTAGE PAR INTERFACE

Pour ce type de routage, le système d'exploitation des équipements NETASQ évalue la passerelle d'acheminement en fonction de l'interface source du paquet.

POLITIQUE DE ROUTAGE

Une politique de routage permet d'évaluer la passerelle d'acheminement en fonction de l'émetteur du paquet (machine, réseau ou groupe), de son destinataire (machine, réseau ou groupe) et du protocole utilisé pour véhiculer le paquet.

REPARTITION DE CHARGE

Le routage par répartition de charge permet de répartir la transmission de paquet vers plusieurs passerelles soit en fonction de la machine source soit en fonction des connections.

AVERTISSEMENT

Les différents types de routage mise en œuvre au sein des équipements NETASQ sont évalués dans un ordre bien précis qui est présenté ci-dessous :

1. Routage statique/Routage dynamique
2. Politique de routage
3. Routage par interface
4. Répartition de charges par connexions
5. Répartition de charges par source
6. Routage par défaut

NOTE

1) Une route par défaut est nécessaire dès que l'on définit une politique de routage, afin de véhiculer le trafic qui ne correspond pas à la politique de routage.
2) Il est tpossible de mettre en œuvre des politiques de routage sur du trafic IPSec.

Pour de plus amples informations au sujet du routage, veuillez vous référer à la note technique « Les types de routage v8.0 ».

5.3.2. Présentation des écrans et des grilles

Le fonctionnement du routage est segmenté en deux parties :

- Routage statique (onglet **Général**) : (routeur et routes statiques)
- Onglet **Avancé** : Cet onglet peut répondre à des besoins plus spécifiques.

Ces deux parties fonctionnent simultanément, le routage statique étant prioritaire sur tout le reste lors de l'acheminement d'un paquet sur le réseau.
Le routage statique représente un ensemble de règles définies par l'administrateur ainsi qu'une route par défaut. L'onglet **Avancé** peut être considéré comme une forme avancée de la route par défaut. Il propose une utilisation simultanée de plusieurs routes pour acheminer un paquet, suivant un algorithme paramétrable. L'onglet **Avancé** fonctionne avec un système de secours (backup).

Lorsque la Haute Disponibilité de liens est activée et en fonctionnement normal :

- Le premier lot (routes principales) contient les routes empruntées.
- Lorsque certaines de ces routes principales ne sont plus praticables (avec un nombre de routes valides inférieur à un seuil), alors le deuxième lot (les routes de secours) est activé et remplace le deuxième lot.

Chaque route est en réalité un objet de type "Machine" désignant son IP qui fait office de route.

La configuration du routage sur un firewall est effectuée à partir de l'arborescence des menus **Réseau\Routage**.

5.3.2.1. Onglet Général

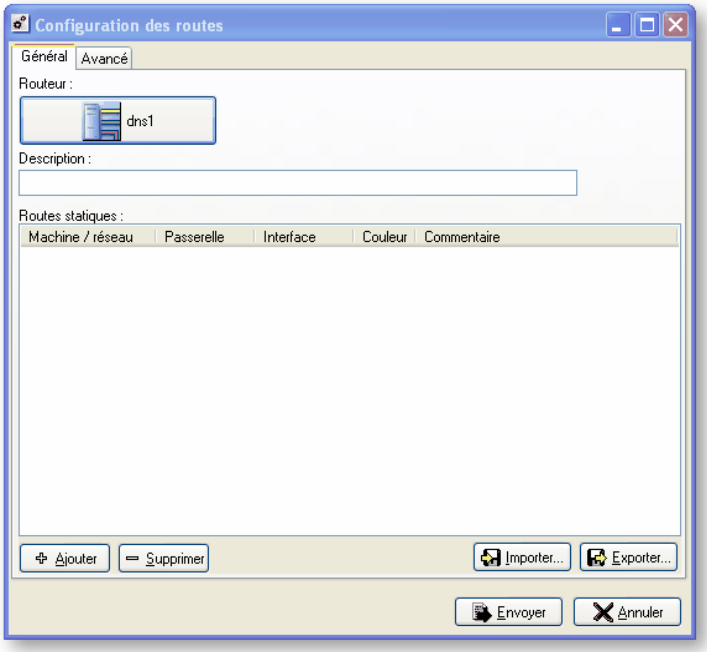


Figure 118 : Configuration des routes - Général

Présentation de l'écran

L'écran de cet onglet se compose de trois parties :

Routeur	Adresse IP du routeur par défaut. C'est à cette adresse que le firewall NETASQ envoie les paquets qui doivent sortir sur le réseau public. Bien souvent le routeur par défaut est connecté à l'Internet. Cliquer sur le bouton permet d'accéder à la base d'objets et de sélectionner une machine. Une fois la sélection faite, le nom de la machine réapparaît sur l'écran.
Description	Commentaire que vous pouvez saisir librement. (Texte simple).
Routes statiques	Si vous possédez plusieurs réseaux "derrière" un routeur, vous pouvez spécifier ici les différentes routes. Vous sélectionnez alors un réseau ou un groupe de machines puis la passerelle à utiliser pour atteindre ce réseau. Vous devez aussi préciser sur quelle interface est indirectement connectée cette passerelle. Vous pouvez également indiquer une couleur et une description. Vous pouvez ajouter ou retirer des routes statiques avec les boutons **Ajouter/Supprimer.**

Présentation de la grille

La grille présente cinq informations :

Machine/réseau	Un double-clic sur cette colonne ouvre la base d'objets afin de sélectionner une machine, un réseau ou encore un groupe.
Passerelle	Un double-clic sur cette colonne ouvre la base d'objets afin de sélectionner une machine (routeur).
Interface	Une liste déroulante permet de sélectionner une interface parmi Ethernet, Vlan, dialup.
Couleur	Une fenêtre s'affiche permettant de sélectionner une couleur d'interface.
Commentaire	Texte libre.

Le routeur par défaut est généralement l'équipement qui permet l'accès de votre réseau à Internet.
Si vous ne configurez pas le routeur par défaut, le firewall NETASQ ne sait pas laisser passer les paquets possédant une adresse de destination différente de celles directement reliées au firewall. Vous pourrez communiquer entre les machines sur les réseaux internes, externes ou DMZ, mais pas avec Internet.

Lignes de commandes

```
RESEAU , INTERFACE -> PASSERELLE , COULEUR # COMMENTAIRE
```

Les boutons d'actions

Six boutons sont disponibles au bas de la grille :

Ajouter	Ajoute une route statique "vide".
Supprimer	Supprime une route préalablement sélectionnée.
Importer	Importation de routes. Le contenu du fichier est du même format que celui reçu du firewall via la commande *network route show.*
Exporter	Exportation de routes. Les routes statiques sont exportées dans un fichier dans un

	format identique à l'importation.
Envoyer	Envoie la configuration des routes statiques.
Annuler	Annule la configuration des routes statiques.

REMARQUE
Au niveau de la grille, un clic droit permet d'afficher un menu contextuel afin d'effectuer les actions énoncées ci-dessus.

5.3.2.2. Onglet Avancé

Cet écran permet d'activer le mode "avancé" du routage. Il se substitue à la route par défaut de l'onglet **Général**.

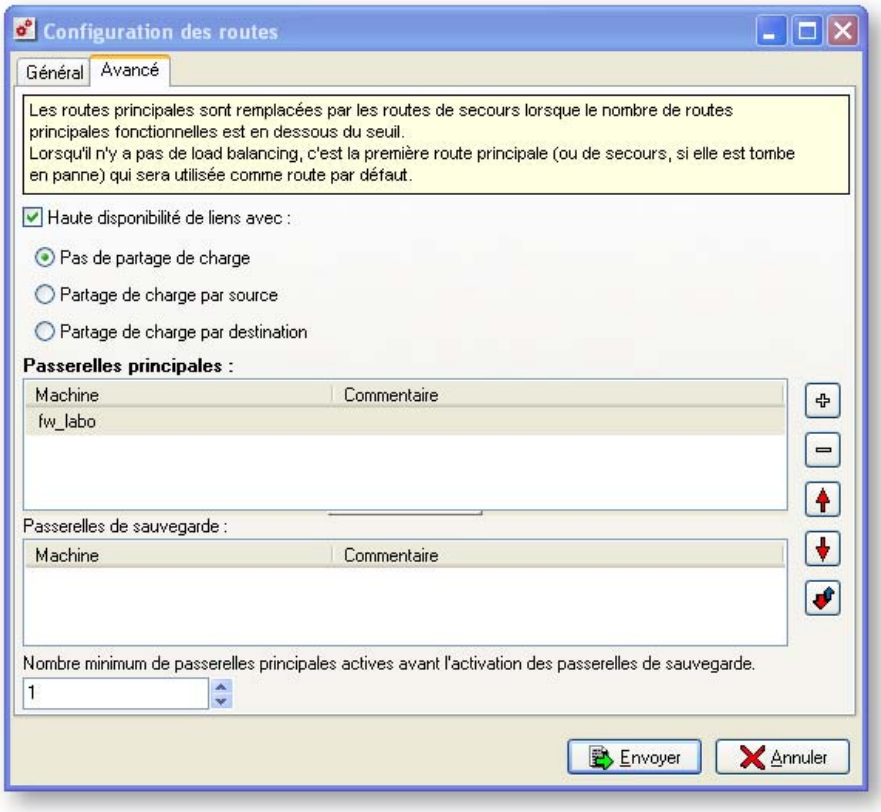


Figure 119 : Configuration des routes - Avancé

Partage de charge (ou Load Balancing)

Lorsque l'option **Haute Disponibilité de liens avec** permet d'activer ou non Gatemon. Lorsque cette option est activée, il est possible d'avoir plusieurs routes au lieu d'une seule (indiquée dans l'onglet **Général**).

Haute Disponibilité de liens avec	Lorsque vous activez cette option, la Haute Disponibilité des routes est activée. : 3 possibilités sont possibles :"Pas de partage de charge ", "Partage de charge par source", et "Partage de charge par destination". • **Pas de partage de charge** : La première route définie dans les grilles "Passerelles" principales" et "Passerelles de sauvegarde", est utilisée pour le routage tandis que les autres sont ignorées. Donc, si la route principale tombe en panne, la route de sauvegarde prend le relai (si elle existe). • **Partage de charge par source** : Toutes les routes définies dans la grille "Passerelles principales" sont utilisées. Un algorithme permet de répartir le routage en fonction de la source qui est à l'origine du trafic routé. Si trop de routes principales tombent en panne, le lot des routes de sauvegarde prend le relai. • **Partage de charge par destination** : Le partage est presque identique au partage de charge par source sauf que l'algorithme de partage se base non seulement sur la source mais aussi sur la destination du trafic. Le trafic est ainsi mieux réparti entre les différentes routes. Pour résumer, selon une machine définie, suivant ses connexions, les paquets ne passeront pas nécessairement par la même route. **REMARQUE** Les commandes sont passées en temps réel lors du choix du partage de charge. S'il y a échec, alors les boutons radio sont restaurés.
Nombre minimum de passerelles principales actives avant l'activation des passerelles de sauvegarde	Si on active la HA, alors, les passerelles de sauvegarde ne seront sollicitées que si le nombre de passerelles principales est inférieur au minimum de passerelles définies dans le champ **Nombre minimum de passerelles principales actives avant l'activation des passerelles de sauvegarde**. Ce nombre doit être au minimum de 1.

Les boutons d'action

Pour pouvoir ajouter ou supprimer des routes, cliquez sur le bouton ou le bouton. La base d'objets s'affiche afin de pouvoir sélectionner une machine qui permettra le routage.

(Ajouter)	Permet d'ajouter un routeur. En cliquant sur ce bouton, 2 options sont proposées : Ajouter une passerelle principale…ou Ajouter une passerelle de sauvegarde. La sélection d'une de ces options affiche la base d'objets afin de sélectionner la machine qui permettra le routage.
(Supprimer)	Permet de supprimer un routeur. Lorsque vous cliquez sur ce bouton, le message "Souhaitez-vous vraiment supprimer cet élément ?" s'affiche. Confirmez ou non la suppression.
(Basculer la catégorie)	Permet de basculer une route de la grille principale à la grille de sauvegarde.
(Haut)	Permet de faire remonter dans la grille la passerelle sélectionnée.
(Bas)	Permet de faire redescendre dans la grille la passerelle sélectionnée.

REMARQUE
L'action de ces boutons apparaît également lorsque l'on effectue un clic droit sur l'une des grilles.

Passerelles principales et de sauvegarde

Les grilles pour les passerelles principales et les passerelles de sauvegarde comportent les colonnes ci-dessous :

Machine	Objet permettant le routage. Cet objet peut être une machine quelconque, une passerelle de dialup (Firewall_<nom_interface_dialup>_peer), un routeur DHCP (Firewall_<nom_interface_DHCP>_router).
Description	Commentaire concernant cet objet.

REMARQUE
La création des passerelles principales et de sauvegarde est illimitée.

Envoi de la configuration

Les modifications effectuées sur cet écran sont validées à l'aide du bouton **Envoyer**. Lors de cette validation, des messages d'erreurs système peuvent s'afficher provoquant l'annulation de micro-actions. C'est pourquoi, l'envoi de configuration est effectué lors de l'activation du routage, de la configuration des routes avancées et de l'ASQ si le partage de charge a été modifié.

Une vérification de la cohérence des routes statiques est effectuée au préalable : si une route statique ne possède ni machine/réseau/ groupe, ni routeur, ni description, dans ce cas, l'envoi est annulé.

Si la configuration effectuée dans cet onglet présente deux passerelles principales ou une passerelle principale et une passerelle de secours, dans ce cas, le bouton de l'onglet **`Général`** "Routeur" est grisé.

5.3.3. Exemple de configuration par routage statique

5.3.3.1. Objectif

Cet exemple est basé sur une architecture réseau constituée d'un siège social et d'un site local (voir schéma ci-dessous), L'équipement UTM NETASQ du site local est ici configuré afin que tout le trafic à destination du siège social utilise la ligne spécialisée prévue à cet effet. Le trafic à destination d'Internet utilise le modem d'accès local.

5.3.3.2. Schéma

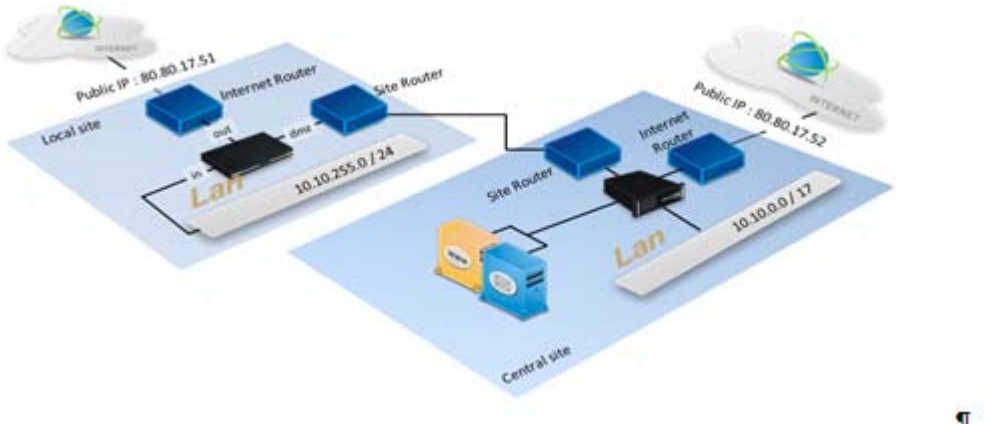


Figure 120 : Routage statique

5.3.3.3. Configuration

1. Il faudra au préalable effectuer de la translation d'adresses et créer les règles de filtrage.
2. Configurer la table de routage.

5.3.4. Exemple de configuration par politique de routage

5.3.4.1. Objectif

Cet exemple est basé sur une architecture réseau constituée d'un siège social et d'un site local (voir schéma ci-dessous), on souhaite configurer l'équipement UTM NETASQ du site local afin que tout le trafic à destination du siège social utilise la ligne spécialisée prévue à cet effet. Le trafic à destination d'Internet utilisera le modem d'accès local.

5.3.4.2. Schéma

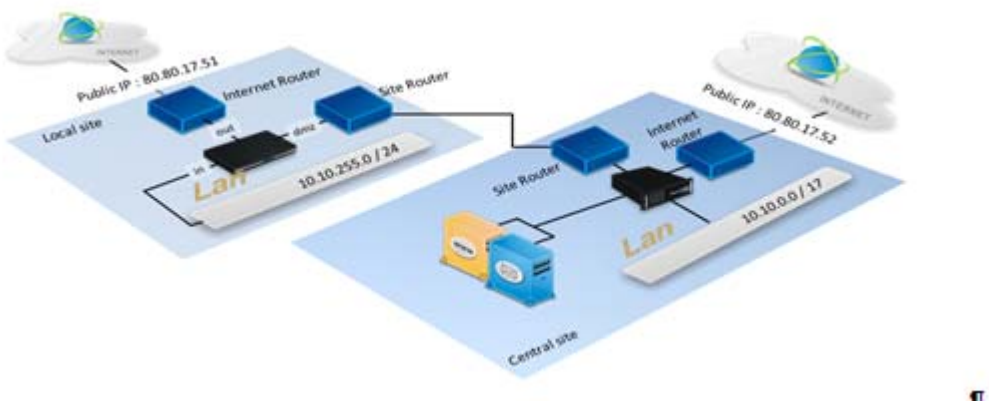


Figure 121 : Architecture réseau

5.3.4.3. Configuration

1. Il faudra au préalable effectuer de la translation d'adresses et créer les règles de filtrage.
2. Ajouter une passerelle par défaut.
3. Configurer le routage par politique.

Exemple de routage par politique

Figure 122 : Règles de filtrage

La première règle décrit que tout le trafic provenant de la source Network_in à destination de remote_network est routé vers leasedline_router.
Le trafic Web, quant à lui, provenant du réseau interne, est routé vers Internet_router.

5.3.5. Exemple de configuration de routage par interface

5.3.5.1. Objectif

Certaines structures doivent pouvoir disposer de plusieurs accès Internet avec des caractéristiques bien spécifiques.

Une société hébergeant des serveurs publics sur son réseau doit pouvoir offrir une qualité de service optimale pour l'accès à ces serveurs. Parallèlement, elle doit donner à ses utilisateurs internes la possibilité d'accéder à Internet sans diminuer la bande passante dédiée aux serveurs publics. La fonctionnalité de routage par interface va permettre de définir, au niveau du firewall, plusieurs accès Internet qui seront utilisés en fonction de l'interface sur laquelle arrive la demande de connexion. Il sera alors possible d'affecter un accès ADSL pour le réseau interne et une liaison spécialisée, avec garantie de service, pour l'accès à vos serveurs publics.

5.3.5.2. Configuration

1. Il faudra au préalable effectuer de la translation d'adresses et créer les règles de filtrage.
2. Configurer les VLAN.
3. Configurer le routage par interface.

Pour définir la configuration du routage par interface, veuillez vous référer à la procédure suivante :

1. Choisissez l'onglet **Interfaces** de la fenêtre de configuration réseau.
2. Choisissez l'interface désirée, puis l'onglet **Routage**.

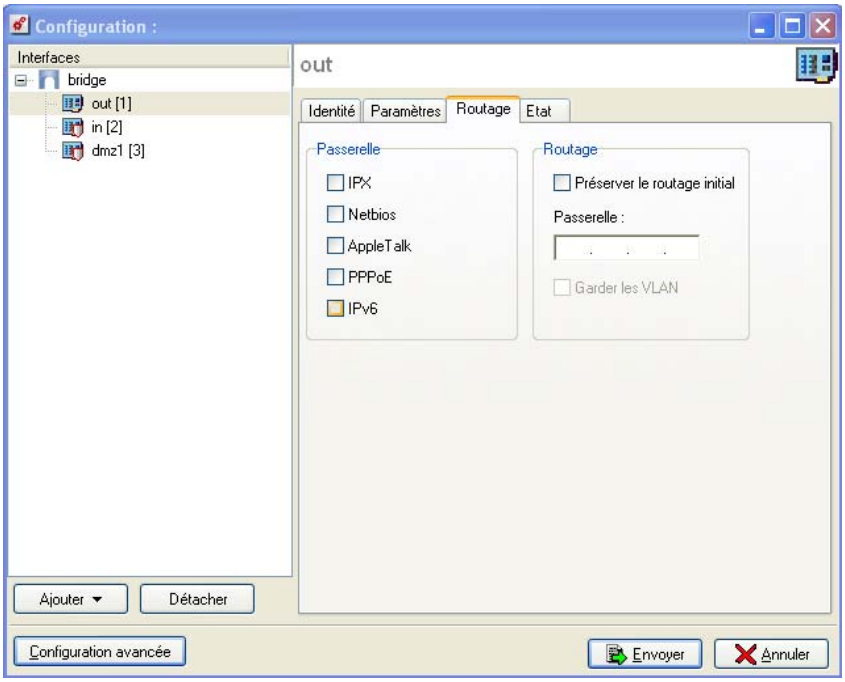


Figure 123 : Configuration out - Routage

Comme nous l'avons indiqué dans *la* *Partie 5/Chapitre 1 : Configuration des interfaces* pour chaque interface, un champ "Passerelle". Ce champ doit renseigner l'adresse IP de la passerelle par défaut (passerelle pour la sortie Internet) utilisée lorsqu'une demande de connexion à destination de l'Internet arrive sur cette interface. Ce champ peut être laissé vide. Dans ce cas, la passerelle par défaut utilisée sera celle définie dans l'onglet **Routage**.

5.3.5.3. Envoi des commandes

L'envoi des commandes s'effectue de manière "semi-temps réel". C'est-à-dire que les modifications effectuées sur une interface sont répercutées sous forme de commandes au moment où le panneau de configuration est remplacé par un autre.

Le programme se charge alors de faire la différence entre l'ancien état de l'interface et le nouveau, et d'en déduire les commandes adéquates.

5.3.6. Exemple de configuration par répartition de charge

5.3.6.1. Objectif

Cet exemple est basé sur une architecture réseau constituée d'un siège social et d'un site local (voir schéma ci-dessous), on souhaite configurer l'équipement UTM NETASQ du site local afin que tout le trafic à destination du siège social utilise la ligne spécialisée prévue à cet effet. Le trafic à destination d'Internet utilisera le modem d'accès local.

5.3.6.2. Schéma

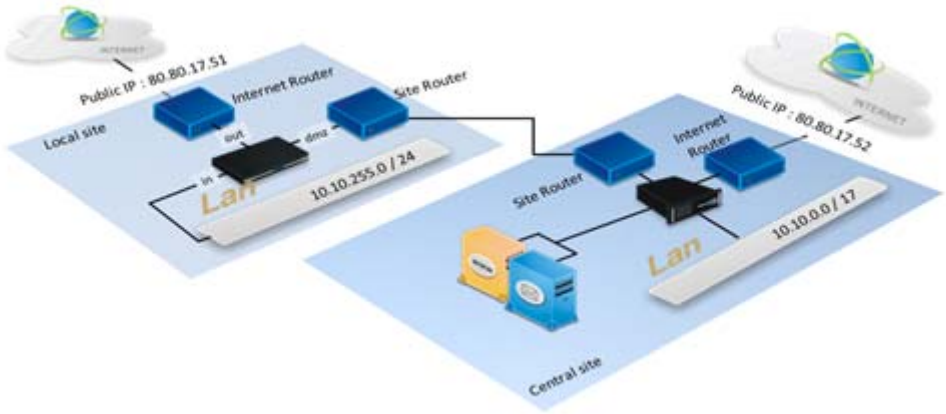


Figure 124 : Architecture réseau

5.3.6.3. Configuration

1. Il faudra au préalable effectuer de la translation d'adresses et créer les règles de filtrage.
2. Configurer la répartition par connexion.
3. Configurer la répartition par source.

CHAPITRE 4. REMARQUES GENERALES SUR LA CONFIGURATION RESEAU

REMARQUE
La modification des adresses IP interne et externe du firewall NETASQ peut nécessiter des modifications importantes de vos fichiers de configuration afin qu'ils conservent leur cohérence. Avant de redémarrer le firewall NETASQ, n'hésitez pas à vérifier la cohérence de vos données, notamment dans les sections *Partie 4 : Objets*, *Partie 6/Chapitre 4 : Translation d'adresses* et Partie 7/Chapitre 2 : *Filtrage*.
En aucun cas, une interface ne doit porter le nom **HD** ou un nom constitué de la façon suivante :

- "xx_peer" ou "firewall_yy".
- xx étant le nom d'une interface déjà existante.
- y étant une chaîne de caractères quelconque.

C'est à partir de cet écran qu'il est possible de configurer le load-balancing de dialups.
Il est possible d'effectuer un load-balancing de routeurs et de dialups. Le partage de charge de dialup est réalisé par le moteur ASQ.

PARTIE 6 : PREVENTION D'INTRUSION (ASQ)

CHAPITRE 1 : INTRODUCTION

6.1.1. Pour ce chapitre, vous devez avoir franchi les étapes :

- Partie 2 : Installation, pré-configuration, intégration.

6.1.2. Pour ce chapitre, vous devez connaître :

- Les actions à engager lors de la détection d'attaques.
- Les informations relatives à la configuration du stateful.
- Les ports que vous voulez surveiller.
- Les protocoles applicatifs que vous voulez analyser.

6.1.3. Utilité de ce chapitre

Ce chapitre vous permet de configurer le noyau ASQ, cœur d'un firewall NETASQ, notamment les actions à effectuer lorsque des attaques sont détectées. De plus la configuration du stateful, du routage, des sondes et des plugins complète la configuration du firewall avant la mise en place de politiques de filtrage, de translations, etc.

Les fonctions d'alarme du noyau ASQ permettent, suite à l'enregistrement d'un événement de sécurité possédant un niveau d'alarme, d'effectuer les actions suivantes :

- Allumer le voyant correspondant au niveau de l'alarme sur la face avant du firewall.
- Afficher l'alarme sur le NETASQ REAL-TIME MONITOR.
- Envoyer l'alarme par e-mail aux utilisateurs spécifiés.

6.1.4. Accéder à ce chapitre

➲ Accédez à la boîte de dialogue par le menu **`Prévention d'intrusion`** de l'arborescence des menus du NETASQ UNIFIED MANAGER.

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications.

AVERTISSEMENT
Avant d'effectuer toute modification importante sur votre firewall, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez revenir dans la configuration précédente.

CHAPITRE 2 : PRESENTATION

6.2.1. Description

L'ASQ, moteur de détection et de prévention d'intrusion, est intégré dans toute la gamme des firewalls NETASQ. Anticipant dès sa création l'évolution des technologies de sécurité Internet, les laboratoires de Recherche et Développement de NETASQ ont mis au point l'ASQ dès 1998. Ce moteur intelligent intègre :

- Un système de prévention d'intrusion (**IPS : *Intrusion Prevention System***) qui détecte et élimine tout comportement malicieux en temps réel.
- Un moteur de filtrage (STATEFUL FILTERING de type STATEFUL INSPECTION) avec optimisation des règles qui permettent d'appliquer la politique de contrôle du flux d'informations de manière sûre et efficace.
- Un moteur de détection d'attaques connues (STATEFUL PATTERN MATCHING) avec optimisation des recherches de signatures qui permettent une comparaison dans un contexte adéquat. Il existe donc moins de faux-positifs et moins de recherches inutiles.

L'ASQ intervient donc sur l'analyse IP, l'analyse des fragments, l'analyse globale, la politique de filtrage, l'analyse des protocoles applicatifs (via les plugins), la comparaison à une base d'attaques connues.

L'ASQ est donc véritablement le cœur de la sécurité fournie par le firewall NETASQ.

DEFINITION
IPS (*Intrusion Prevention System*) : Système permettant de détecter et de bloquer les tentatives d'intrusion, du niveau "réseau" jusqu'au niveau "applicatif" de la norme OSI.

Actuellement, les contre-mesures sont très compliquées à mettre en place et très ciblées vis-à-vis des d'attaques de type "déni de service" par exemple. En effet, d'un point de vue théorique, la plupart des attaques visant à créer des dénis de service sont basées sur des services ou protocoles standard sur Internet. S'en protéger reviendrait à couper les voies de communications normales avec Internet, alors que c'est la raison principale des machines concernées (serveurs web, de messagerie, etc...).

Pourtant, il faut tout de même agir pour garantir la sécurité des données de l'entreprise. Tout cela implique beaucoup de démarches : il faut monitorer le trafic (ce qui est loin d'être simple, du fait de la quantité de données qui transitent), établir des profils types de comportement et des écarts tolérables au-delà desquels on considérera que l'on fait l'objet d'une attaque; il faut également définir les types d'attaques contre lesquelles on souhaite se protéger (analyses de risques à l'appui) car il est impossible de toutes les prévoir. Il s'agit de mettre en place une protection intelligente et flexible.
L'ASQ répond à ces contraintes et, grâce à son analyse du trafic, prévient les grandes familles d'attaques en temps réel.

6.2.1.1. Interfaces réseaux

Le lien est réalisé à deux niveaux :

- Au niveau de l'Ethernet pour réaliser les fonctions de bridge.
- Au niveau IP pour assurer l'analyse du trafic du protocole IP et des protocoles supérieurs (TCP, UDP, HTTP,…).

6.2.1.2. Configuration et audit

La configuration du moteur qui va définir la réaction (passer ou bloquer) par rapport aux paquets est réalisée par une interface entre le noyau et les programmes utilisateurs. Cette interface sous FreeBSD utilise le mécanisme ioctl pour passer les paramètres de configuration et récupérer les journaux d'audit générés par l'ASQ.

Asqd

- Permet de récupérer les entrées permettant la création des fichiers d'audits.
- Permet de distribuer les informations d'alarmes aux différents modules comme serverd, snmp,…
- Permet de synchroniser l'état du moteur avec les fichiers de configuration.

Serverd

- Permet de fournir les informations temps réel sur l'état de l'ASQ, les statistiques et les alarmes (fonctions de monitoring).
- Permet de mettre à jour des fichiers de configuration de l'ASQ.

Sfctl

- Permet la configuration en mode administrateur (console) qui comprend l'accès distant en ssh et l'accès direct via le port série écran/clavier.
- Est utilisé par les scripts pour la modification de l'état de l'ASQ (routage load balancing des dialups,…)
- Est utilisé lors de la séquence de démarrage du firewall pour la configuration initiale du produit avant le chargement des divers services.

6.2.2. Ecran de configuration

Le menu de configuration propose cinq domaines d'intervention :

- Configuration du comportement du firewall vis-à-vis du trafic le traversant.
- Configuration des alarmes et signatures.
- Configuration de la quarantaine.
- Configuration des sondes.
- Configuration des plugins.

Le menu de configuration de l'ASQ est divisé en deux parties :

- A gauche un arbre présentant les diverses fonctionnalités du menu **`Prévention d'intrusion.`**
- A droite les options configurables.

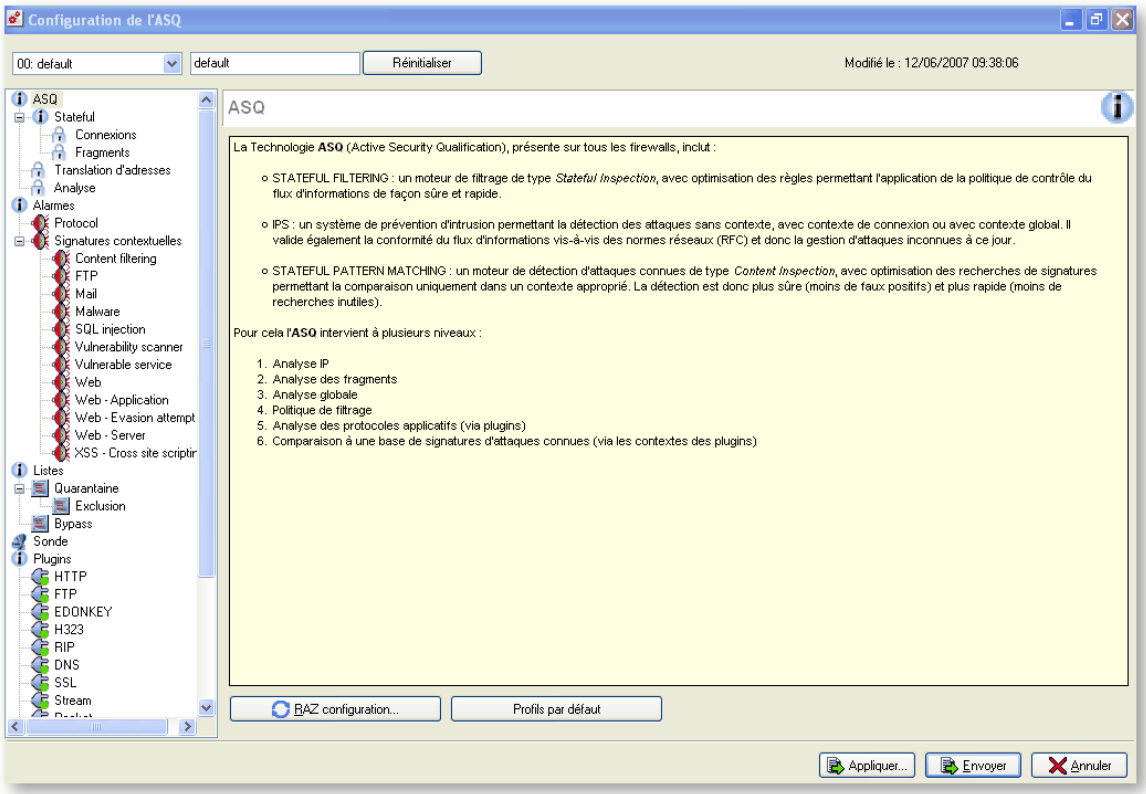


Figure 125 : Configuration de l'Asq - Asq

6.2.2.1. Multi-profil

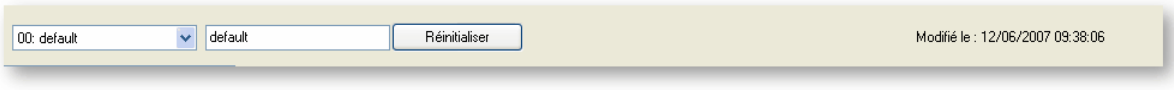


Figure 126 : Multi-profil

Il est possible de créer quatre profils de l'ASQ afin d'adapter l'analyse de l'ASQ en fonction des types de trafic ou du sens du trafic. Cela va permettre de désactiver certaines alarmes sur des trafics autorisés en sortie mais pas en entrée. (*Cf.* *Partie 7/Chapitre 2 : Edition d'une politique de filtrage*). La barre d'actions située en haut de l'écran vous indique quel profil de l'ASQ est actuellement affiché. De plus vous pouvez spécifier un nom pour chacun des quatre profils.
Les 4 profils par défaut sont :

- 00: default
- 01: Profile1
- 02: Profile2
- 03 : Profile3

Le bouton **Réinitialiser** vous permet de redéfinir les paramètres des profils ASQ dans leur configuration d'origine.

La date située à côté du bouton indique la date de la dernière modification de la configuration.

6.2.2.2. Application des changements

Le bouton **Appliquer…** situé dans la barre d'actions au bas de la fenêtre de configuration de l'ASQ vous permet d'appliquer les changements configurés sans avoir à fermer la fenêtre.

6.2.2.3. Configuration par défaut ASQ

Le bouton **RAZ configuration** affiche l'écran suivant :

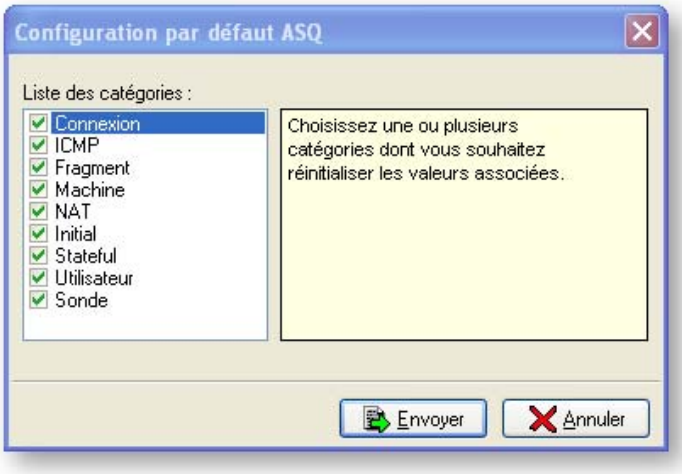


Figure 127 : Configuration par défaut ASQ

Cet écran vous permet de sélectionner par l'activation d'une coche les catégories pour lesquelles vous souhaitez effectuer une réinitialisation. Les valeurs par défaut associées à la catégorie seront restaurées.

6.2.2.4. Profils par défaut ASQ

Les profils ASQ doivent être reliés au trafic entrant ou sortant.
Le bouton **Profils par défaut ASQ,** affiche l'écran suivant :

Figure 128 : Profils par défaut - ASQ

Cet écran vous permet de sélectionner un profil par défaut pour le trafic entrant et pour le trafic sortant.
Par défaut : le profil 00 s'attache aux connexions entrantes, (provenant d'une interface non protégée) alors que le profil 01 s'attache aux connexions sortantes (provenant d'une interface protégée).

Il n'y a pas de migration de profils lorsque vous passez d'une version 6.3 à une version 7.0. Votre configuration n'est donc pas modifiée. Néanmoins, vous ne bénéficiez pas de cette différentiation entre profils pour connexions entrantes et sortantes.

Lorsque l'on effectue un Defaultconfig, la configuration est la suivante :

- "IncomingProfile=00" et "OutgoingProfile=01"
- 00 est basé sur le profil "Medium"
- 01 est bas sur le profil "Internet"

CHAPITRE 3 : STATEFUL

Ce module permet le suivi des données de connexion TCP.

Les paramètres de configuration du module **`Stateful`**, module permettant l'analyse dynamique des paquets, sont modifiables dans le menu **`Prévention d'intrusion\Stateful`**.

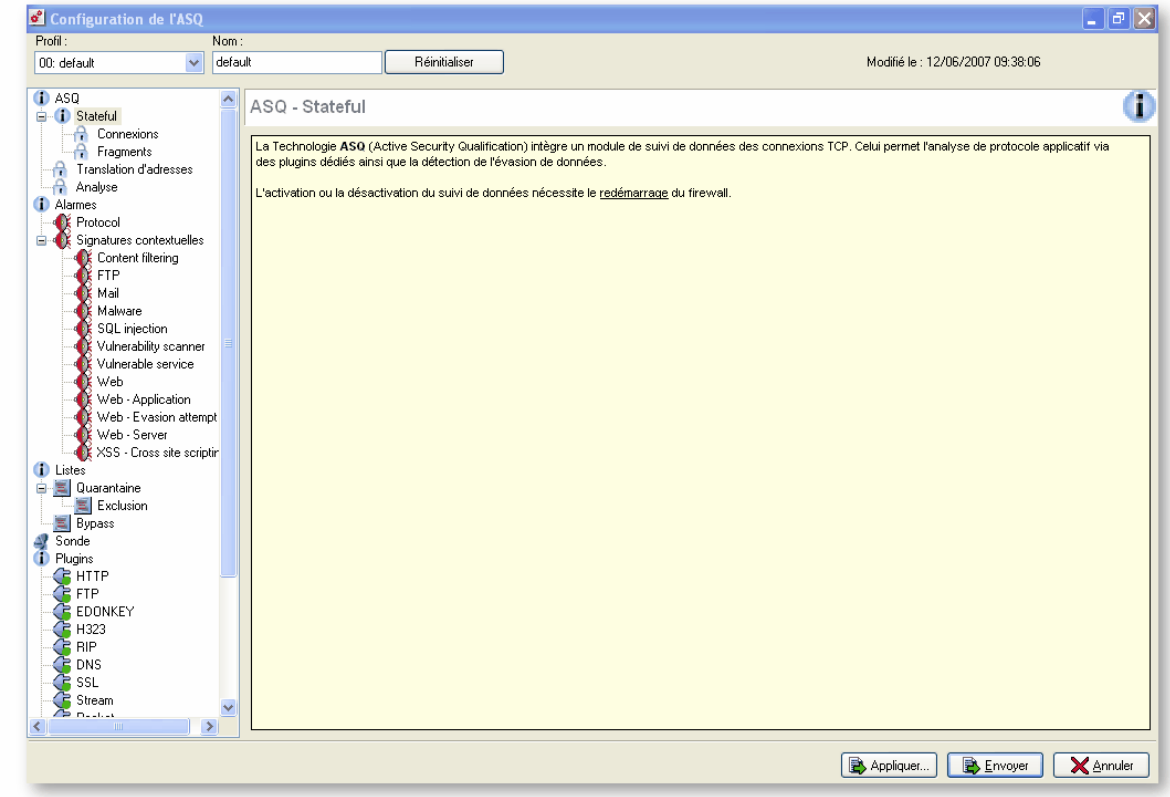


Figure 129 : Configuration de l'ASQ - Stateful

Ce module, intégré au module ASQ, conserve l'état des connexions et permet l'analyse des paquets pour la détection d'attaques. Le Stateful vous permet de ne définir, dans les règles de filtrage, que les règles "aller" (règle indiquant le sens de la connexion) sans avoir à préciser la règle "retour" (réponse de la machine contactée par l'émetteur de la connexion).

REMARQUE
Un redémarrage du firewall est nécessaire lorsque vous activez ou désactivez le suivi de données.

Le menu de configuration du moteur **`Stateful`** est divisé en deux sections : **`Connexions`** et **`Fragments`**. Les paramètres configurables dans ces sections sont expliqués dans les tableaux suivants.

6.3.1. Connexions

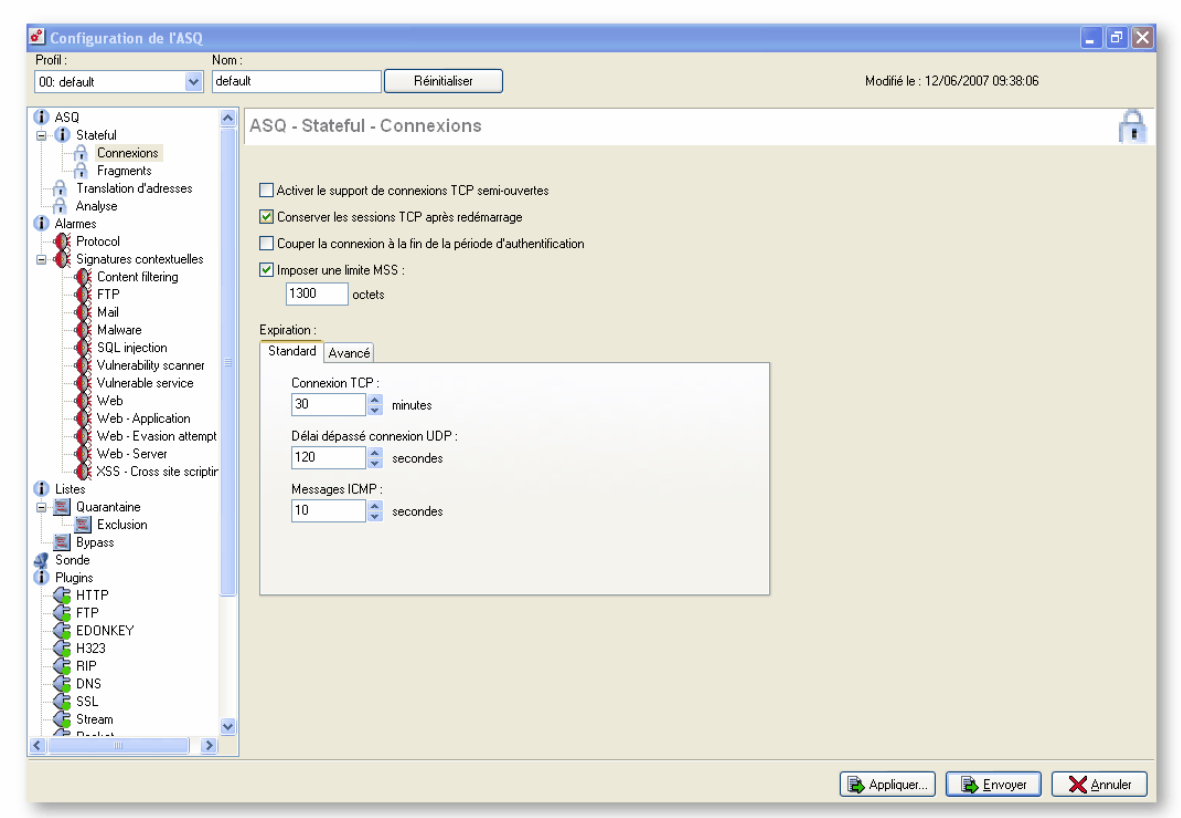


Figure 130 : Configuration de l'ASQ - Connexions

Activer le support de connexions TCP semi-ouvertes	Un des correspondants a clos sa connexion pourtant l'autre continue à émettre des paquets. La connexion est alors unidirectionnelle. Par défaut, cette option est désactivée.
Conserver les sessions TCP après redémarrage	Lorsque cette option est activée, le firewall garde en mémoire le contexte des connexions lorsqu'il redémarre et les connexions ne sont donc pas interrompues. Cette option doit être activée pour que le maintien des connexions soit réalisé lors d'un basculement de firewalls en Haute Disponibilité. Par défaut, cette option est activée.
Couper la connexion à la fin de la période d'authentification	Cette option permet la clôture des connexions actives à la fin de la période d'authentification. Par défaut, cette option est désactivée.
Imposer une limite MSS	Le firewall va redimensionner les paquets TCP (et pas UDP) à la taille indiquée dans le champ "Imposer une limite MSS". Cette fonctionnalité est utile pour des connexions de type PPPoe ou VPN car les paquets ne doivent pas dépasser une certaine taille (dans le cas contraire ils sont soit fragmentés, soit rejetés). La

	valeur conseillée est de 1300 octets.

AVERTISSEMENT

L'utilisation de l'option **Activer le support de connexions TCP semi-ouvertes** est déconseillée. En effet la sélection de cette option permet la transmission de paquets plus permissifs pour l'intégrité des ressources protégées par le firewall. Cette option est supportée pour des raisons de compatibilité avec le protocole TCP et n'est à utiliser qu'en connaissance de cause.

6.3.1.1. Délai d'expiration standard

Des délais d'expiration standards sont configurables sur le firewall. Ils sont expliqués dans le tableau suivant :

Connexion TCP	Temps au bout duquel les connexions TCP sont réinitialisées. Ce temps peut varier entre 10 et 10080 minutes. Par défaut, l'indication de l'expiration est indiquée à 30 minutes.
Connexion UDP	Temps au bout duquel les connexions UDP sont réinitialisées. Ce temps peut varier entre 30 et 3600 secondes. Par défaut, l'indication de l'expiration est indiquée à 120 secondes.
Messages ICMP	Temps de conservation des messages ICMP. Ce temps peut varier entre 2 et 60 secondes. Par défaut, l'indication de l'expiration est de 10 secondes.

6.3.1.2. Délai d'expiration avancé

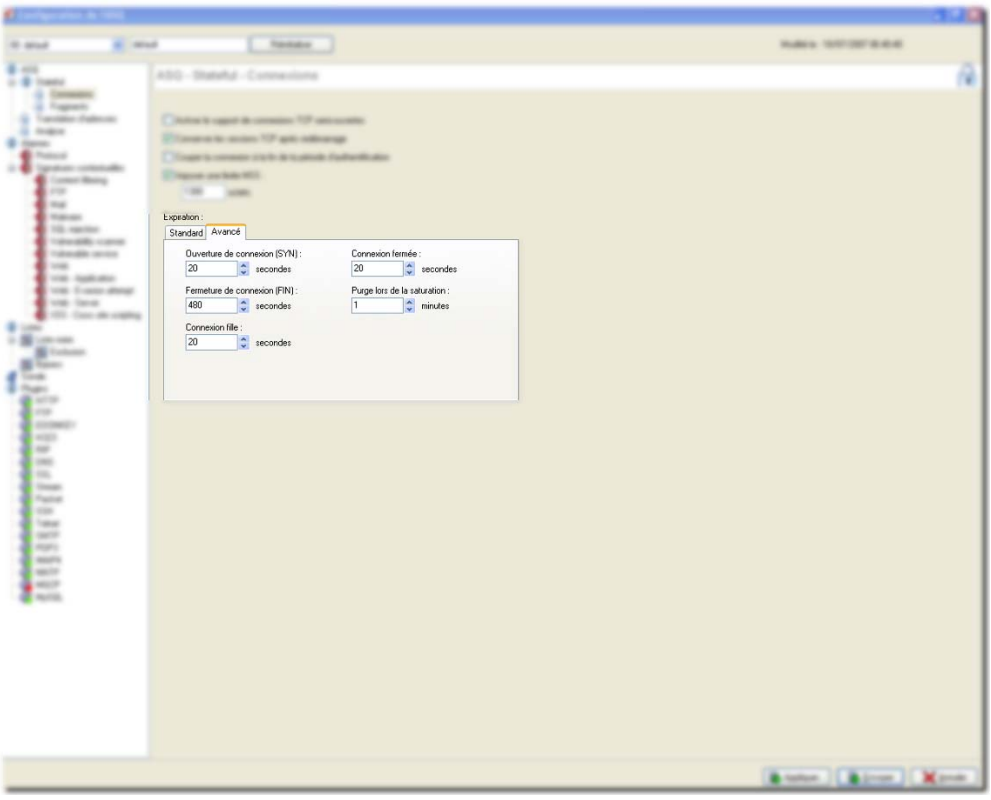


Figure 131 : Délai d'expiration - Avancé

Des délais d'expiration avancés sont configurables sur le firewall. Ils sont expliqués dans le tableau suivant :

Ouverture de connexion (SYN)	Temps maximum admis pour la phase d'ouverture d'une connexion TCP (SYN, SYN-ACK, ACK). Ce temps peut varier entre 10 et 60 secondes. Par défaut, le temps est indiqué à 20 secondes.
Fermeture de connexion (FIN)	Temps maximum admis pour la phase de fermeture d'une connexion TCP (FIN, FIN-ACK, FIN, FIN-ACK). Ce temps peut varier entre 10 et 3600 secondes. Par défaut, le temps est indiqué à 480 secondes.
Connexion fermée	Aucune connexion utilisant les mêmes adresses et ports, sources et destination ne peut débuter durant le délai de **Connexion fermée**. Ce temps peut varier entre 10 et 60 secondes. Par défaut, le temps est indiqué à 20 secondes.
Connexion fille	Temps durant lequel une tentative d'établissement d'une connexion fille est acceptée. Ce temps peut varier entre 10 et 60 secondes. Par défaut, le temps est indiqué à 20 secondes.
Purge lors de saturation	Lorsque la table des connexions de l'ASQ est pleine et qu'une nouvelle tentative de connexion arrive, l'ASQ tente de supprimer dans sa table certaines connexions (essentiellement les connexions en établissement) afin de libérer une place. Il réessaie dans l'intervalle défini par cette option. Cette purge peut varier entre 1 et 2880 minutes (par défaut : 1).

6.3.2. Fragments

La taille du redécoupage des paquets est désormais plus élevée. (Cf. Tableau ci-dessous pour obtenir des informations supplémentaires concernant la taille des fragments.

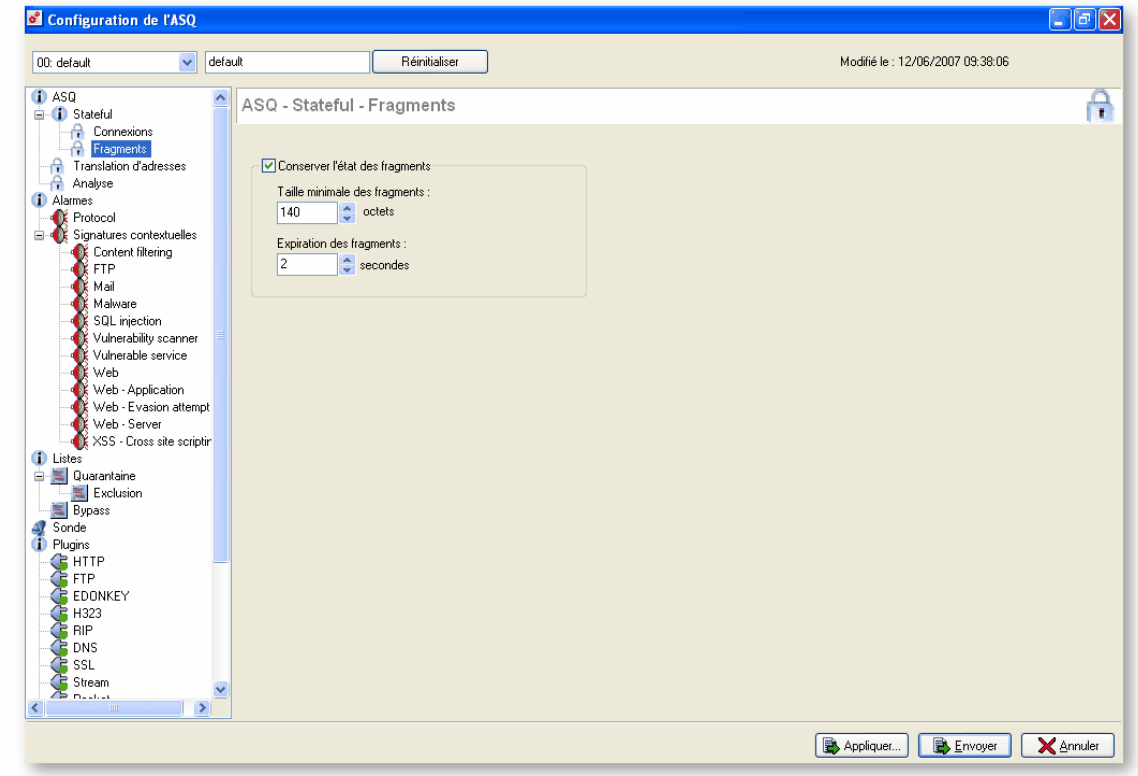


Figure 132 : Configuration de l'ASQ - Fragments

Conserver l'état des fragments	Si cette option a été sélectionnée, le firewall analyse les paquets IP fragmentés afin de déterminer les éventuelles attaques de type fragmentation de paquets

	IP. Si l'option n'est pas sélectionnée, le firewall ne laisse pas passer les paquets fragmentés.
Taille minimale des fragments	Taille minimale d'un fragment. Au minimum 140 octets. Au maximum, 32757 octets (par défaut : 140).
Expiration des fragments	Temps de conservation des fragments passant par le firewall variant entre 2 et 30 secondes (par défaut : 2).

CHAPITRE 4 : TRANSLATION D'ADRESSES

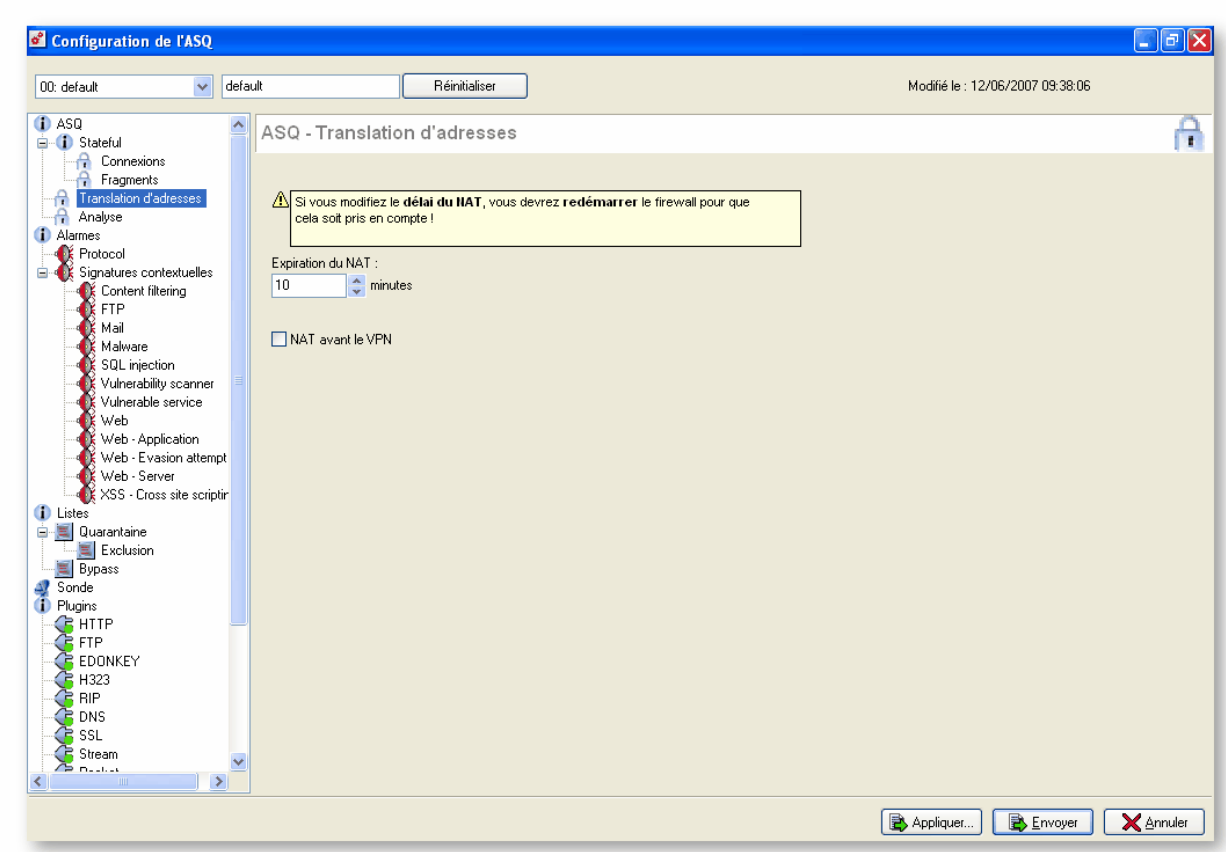


Figure 133 : Configuration de l'ASQ - Translation d'adresses

Une section de la configuration de l'ASQ est réservée à l'analyse de la translation d'adresses sur le firewall. En effet, l'ASQ influence la manière de gérer la translation d'adresses (NAT). Le tableau indique les paramètres configurables.

Expiration du NAT	Temps au bout duquel les connexions impliquant de la translation d'adresses sont réinitialisées. Ce temps peut varier entre 10 et 10080 minutes (par défaut : 10). **AVERTISSEMENT** La modification du délai d'expiration des sessions NAT nécessite le redémarrage du firewall pour une prise en compte.
NAT avant le VPN	Les fonctionnalités NAT et VPN ont parfois des incompatibilités. En effet le VPN IPSec utilise une fonction de hachage pour authentifier les différents paquets d'une connexion VPN. Cette fonction de hachage est basée sur les informations contenues dans l'entête du paquet. Or les fonctionnalités NAT modifient cet entête.

Ainsi l'entête et le hash VPN ne correspondent plus et le paquet associé est rejeté par le correspondant VPN distant.
Pour s'affranchir de cette incompatibilité cochez l'option **NAT avant le VPN** afin que les traitements NAT soient pris en compte avant le calcul du hash VPN.

CHAPITRE 5 : ANALYSE

L'analyse du trafic présente les paramètres permettant d'agir sur tous les plugins. Ces paramètres ont une influence majeure sur la sécurité offerte par le firewall.

Les paramètres de configuration du module **Analyse** sont modifiables dans le menu **`Prévention d'intrusion\Analyse`** de l'arborescence de l'ASQ.

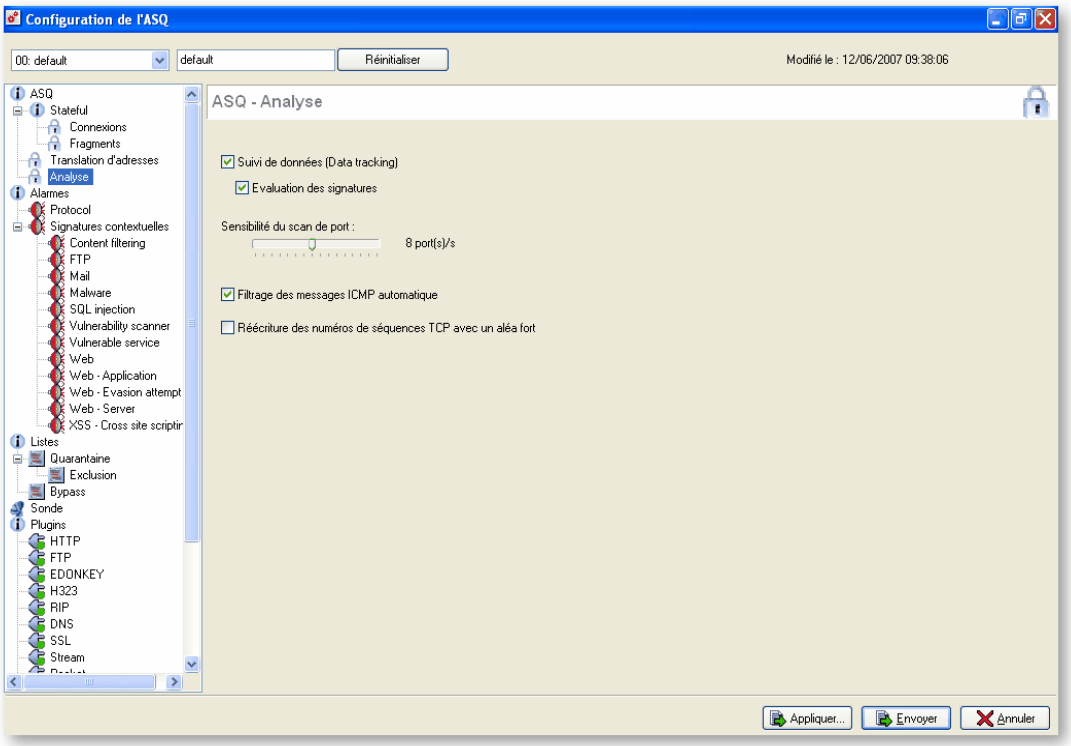


Figure 134 : Configuration de l'ASQ - Analyse

Suivi de données (Data tracking)	Le firewall analyse la cohérence entre les données contenues dans le paquet et son entête ainsi que la cohérence entre plusieurs paquets fragmentés (pour éviter l'évasion de données). - Désactiver cette option empêche l'ASQ d'utiliser les plugins. - Si l'option est activée (cochée par défaut), dans ce cas, il est possible ou non d'activer l'évaluation des signatures (cochée par défaut). **AVERTISSEMENT** L'activation ou la désactivation du Suivi de données (Data tracking) nécessite le redémarrage du firewall.
Evaluation des signatures	Cette option permet l'activation des analyses basées sur les signatures contextuelles.
Sensibilité du scan de port	Si cette option est sélectionnée, le firewall peut détecter les scans de ports y compris les scans furtifs (scans se basant sur les réponses des machines aux paquets FIN et pas aux paquets SYN. Ces scans sont, dans la majorité des cas,

	non tracés au niveau des machines scannées puisqu'aucun paquet SYN n'a été reçu). Il est possible de déterminer le nombre de ports pouvant être scannés avant le déclenchement de l'alarme. La sensibilité du scan de port peut varier entre 1 et 16 port(s) par seconde (par défaut : 8).
Filtrage des messages ICMP automatique	Cette option permet d'autoriser le passage de messages ICMP si ceux-ci sont cohérents dans une connexion TCP, UDP ou ICMP (filtrage intelligent des paquets ICMP). (Par défaut : activé).
Réécriture des numéros de séquences TCP avec un aléa fort	Afin de pallier aux systèmes générant des paquets avec des numéros de séquence peu aléatoires, il est possible d'activer cette option. Le firewall va réécrire les paquets avec un numéro de séquence beaucoup plus imprédictible. (Par défaut : désactivé).

CHAPITRE 6 : ALARMES

L'**ASQ** (***Active Security Qualification***) est une technologie unique de prévention d'intrusion en temps réel : Cette prévention d'intrusion analyse le trafic de la couche réseau jusqu'à la couche applicative et applique diverses méthodes pour identifier et bloquer tout le trafic malveillant.

Des familles d'attaques sont utilisées par l'ASQ afin de protéger le réseau contre les menaces les plus récentes. Le traitement préventif s'effectue en temps réel, les performances du système ne diminuent pas.

Il est possible de régler finement le comportement du firewall en fonction de chaque alarme susceptible d'être émise lors de la détection de trafic comportant des éléments malicieux.

Les paramètres de configuration du module **Alarmes** sont modifiables dans le menu **`Alarmes de l'arborescence de la configuration de l'ASQ.`**

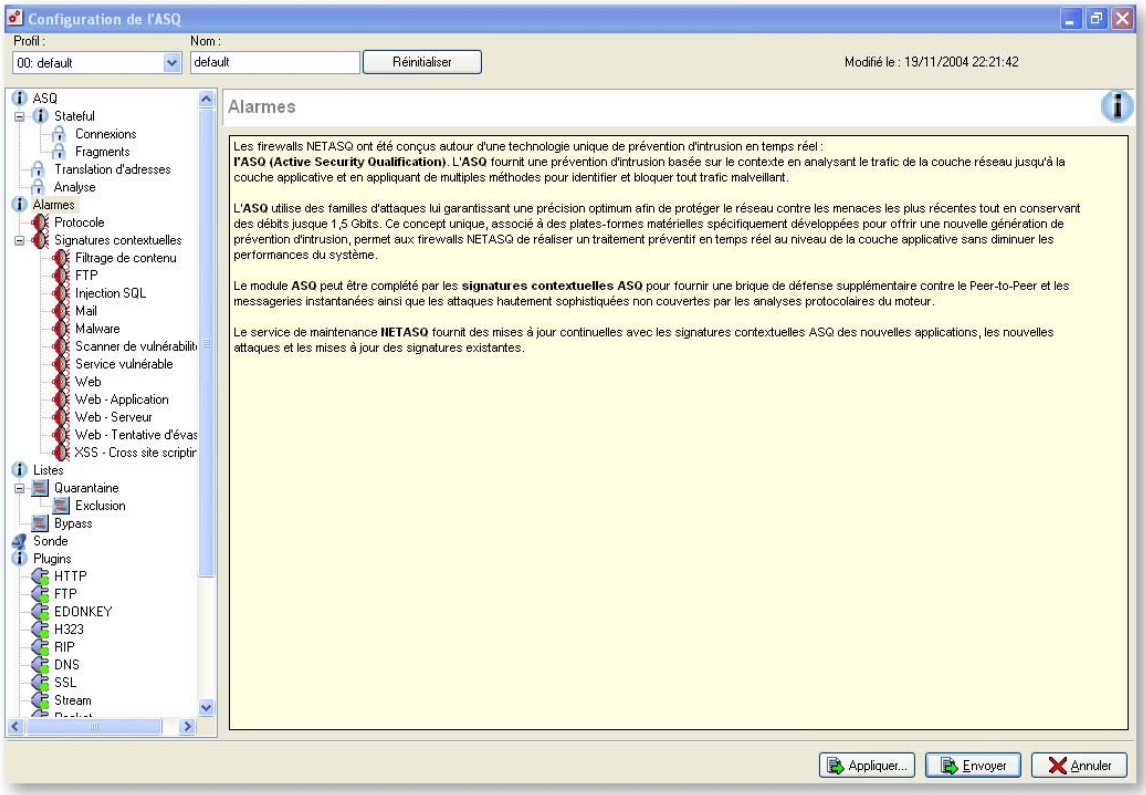


Figure 135 : Configuration de l'ASQ - Alarmes

Pour chacune des attaques gérées par les firewalls NETASQ, l'administrateur possédant les droits ***+M*** peut définir si les paquets incriminés doivent être transmis ou détruits et s'il y a lieu de générer un événement de sécurité possédant un niveau d'alarme, automatiquement enregistré dans le fichier de traces **Alarmes**.
La liste présentée dans cette fenêtre regroupe toutes les attaques et familles d'attaques gérées par les firewalls.

Les alarmes sont divisées en deux catégories :

- Les alarmes de catégorie **Protocole** : associées aux analyses protocolaires de l'ASQ.
- Les alarmes de catégorie **Signatures contextuelles** : associées aux analyses des signatures contextuelles. Il s'agit d'une liste d'alarmes émises lorsque l'ASQ détecte une séquence particulière dans le trafic réseau. Ces signatures sont classées par catégorie. Le firewall récupère ces catégories et effectue des mises à jour afin de contrer les menaces les plus récentes.

NOTE
Le module d'analyse par Signatures Contextuelles fait l'objet d'une licence supplémentaire payante.

6.6.1. Alarmes protocolaires

Les alarmes protocolaires disposent de presque toutes les propriétés des signatures contextuelles (sauf **Détail** et **Nouveau**).

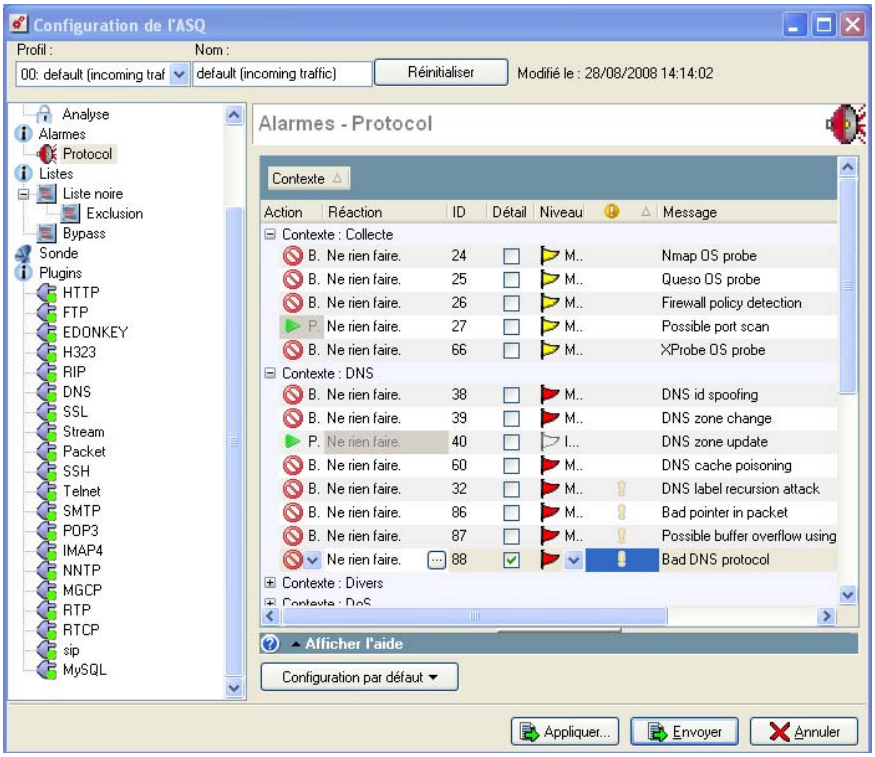


Figure 136 : Configuration de l'ASQ - Protocole

La grille se divise en six colonnes :

Contexte	les alarmes sont regroupées par catégorie qui sont : DNS, Divers, Dos, FTP, HTTP, ICMP, IGMP, IP, SMTP, Scan, TCP, UDP, MGCP et ssl.
Action	Lorsqu'une alarme est remontée le paquet qui a provoqué cette alarme subit l'action associée. Les actions sont "Bloquer" ou "Passer. Une case grisée indique qu'aucune modification de l'action n'est possible.
Réaction	En plus de l'action associée à l'alarme, il est possible de définir une réaction à la remontée d'une alarme parmi l'envoi d'un mail, la mise en quarantaine de la machine responsable ou **Aucune réaction supplémentaire**.

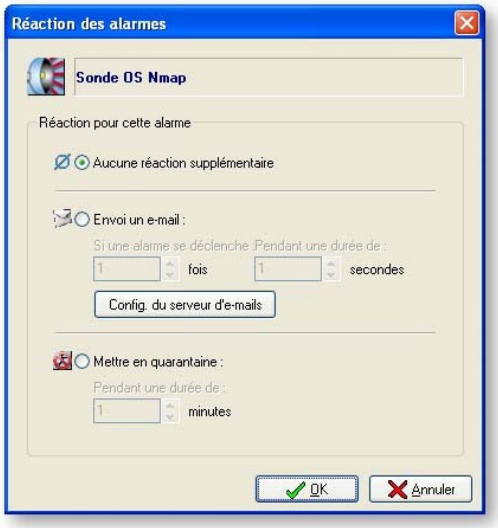


Figure 137 : Réaction des alarmes

1) **Envoi un e-mail :** lorsque le service d'envoi des mails est activé (Voir Partie 16/Chapitre 1 : Configuration du serveur d'e-mails) il est possible de définir l'envoi d'un mail lorsque deux facteurs sont réunis : le nombre de fois où l'alarme a été remontée et dans quel intervalle de temps.

2) **Mettre en quarantaine** : cette mise en quarantaine permet de bloquer l'ensemble des trafics en provenance de la machine responsable de la remontée d'alarme. Cette quarantaine dynamique est associée à une durée (en minutes) et ne résiste pas au redémarrage (la liste des machines en quarantaine est réinitialisée lors d'un redémarrage du firewall). La durée peut être comprise entre 1 et 7200 minutes (par défaut : 1).

ID	Indication de l'ID de l'alarme considérée comme sensible.
Détail	Cette option permet de sauvegarder le paquet responsable de la remontée d'alarme. La taille des informations sauvegardées dépend du modèle de votre firewall. Ce paquet est alors visualisable grâce au NETASQ REAL-TIME MONITOR. (*Cf. manuel NETASQ REAL-TIME MONITOR*).
Niveau	Trois niveaux d'alarmes sont disponibles, "Ignorer", "Mineure" et "Majeure".
	Indication par un indicateur pour savoir si l'alarme posera un poblème de sécurité lorsque l'on voudra la mettre à « Passer ». Dans un tel cas, le panneau d'aide afficherait un avertissement. Cette option est valable uniquement pour les alarmes protocolaires. L'icône apparaît grisée si l'action est à « Bloquer ». Pour plus d'informations, référez-vous à l'explication du Partie 6/Chapitre 9 : plugin Pass_detach.

Message	Cela correspond à l'intitulé de l'alarme. Des informations complémentaires sur l'alarme sont disponibles directement dans NETASQ UNIFIED MANAGER grâce aux liens présents dans cette colonne.

Un menu contextuel s'affiche lorsque l'on fait un clic droit sur une ligne. Ce menu contient les options : **Tout sélectionner**, **Aucune sélection**, **Inverser la sélection**, **Marquer**.

6.6.1.1. Profils de protection

Le bouton **Configuration par défaut** vous permet de redéfinir la configuration des alarmes selon quatre profils de protection disponibles :

- Sécurité faible…
- Sécurité moyenne…
- Sécurité forte…
- Sécurité Internet…

AVERTISSEMENT
L'application d'un profil de sécurité efface toutes les valeurs qui auraient pu être personnalisées pour chaque alarme.

6.6.1.2. Aide en ligne

Chaque alarme protocolaire est associée à une explication fournie par NETASQ au moyen d'une page HTML intégrée dans l'application NETASQ UNIFIED MANAGER. Pour afficher l'aide en ligne d'une alarme protocolaire, référez-vous à la procédure suivante :

1 Sélectionnez l'alarme protocolaire dont vous souhaitez l'explication.

2 Cliquez sur l'option **Afficher l'aide** (au dessus du bouton **Configuration par défaut**) pour afficher l'aide correspondante à l'alarme protocolaire sélectionnée. Un écran d'aide de ce type s'affiche :

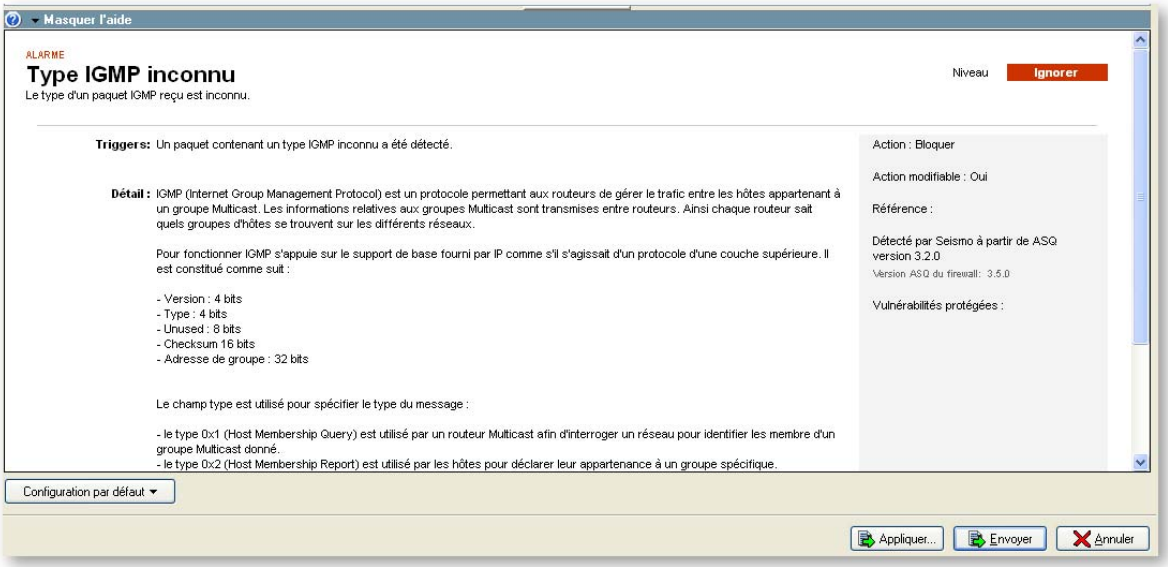


Figure 138 : Aide- Alarmes

6.6.2. Signatures contextuelles

6.6.2.1. Présentation

Les attaques visant à exploiter des erreurs d'implémentation locales clientes ou serveurs sont bloquées par le module de détection et de prévention d'intrusion par signatures contextuelles afin de fournir une défense supplémentaire contre les attaques, qu'elles soient standard ou plus sophistiquées non couvertes par les analyses protocolaires du moteur,ainsi que le Peer-to-Peer (Kasaa, Gnutella)et les messagerie instantanées (Yahoo, MSN, AOL Messenger). Cette base complémentaire aux autres analyses permet d'affiner l'analyse globale du trafic réalisé par le firewall NETASQ en gommant les inconvénients des systèmes des patterns matching habituels (comme les IDS) comme, par exemple, les faux positifs. De plus, grâce à la sauvegarde du contexte, le système NETASQ est plus efficace.

NOTE

Des mises à jour régulières sont disponibles pour les signatures contextuelles ASQ des nouvelles applications, les nouvelles attaques ou encore la mise à jour des signatures existantes grâce au menu Maintenance de NETASQ UNIFIED MANAGER.

L'analyse des plugins de l'ASQ permet la définition d'un contexte d'activation des signatures contextuelles. Ainsi, seules les signatures contextuelles qui correspondent au trafic détecté par les plugins sont utilisées lors de l'analyse.

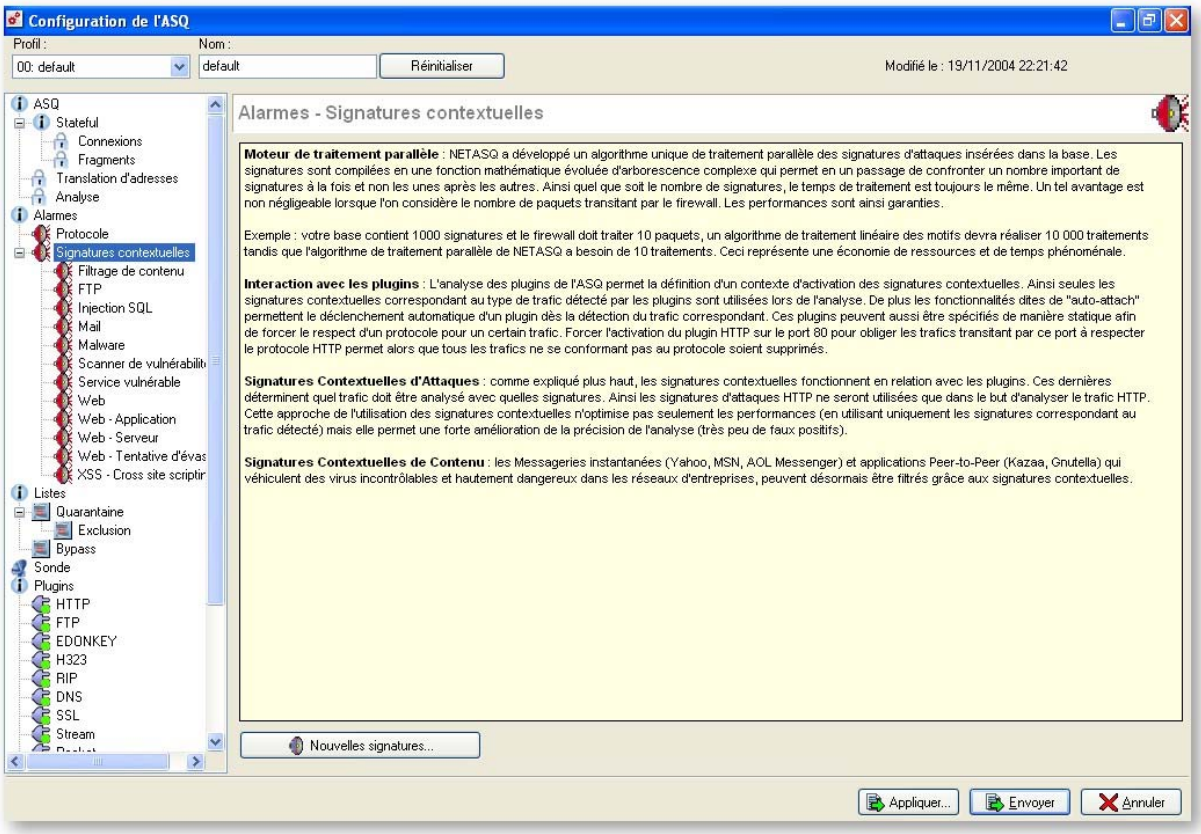


Figure 139 : Configuration de l'ASQ - Signatures contextuelles

6.6.2.2. Interface

Les signatures contextuelles de l'ASQ sont divisées dans l'interface graphique du NETASQ UNIFIED MANAGER selon les fonctions qu'elles réalisent, les attaques qu'elles préviennent ou les trafics qu'elles surveillent. Les signatures contextuelles sont divisées comme suit :

- Filtrage de contenu
- FTP
- Injection SQL
- Mail
- Malware
- Scanner de vulnérabilité
- SEISMO : l'intégration des signatures SEISMO permet un bénéfice de performance. La veille est mutualisée entre les attaques et les vulnérabilités.
- Service vulnérable
- Web
- Web-Application
- Web-Serveur
- Web-Tentative d'évasion
- XSS- Cross site Scripting

La grille des signatures contextuelles se divise en sept colonnes :

Contexte	Les alarmes sont regroupées par contexte. Ainsi les signatures ne s'appliquent que dans un certain contexte, ce qui permet de baisser le nombre de faux positifs et d'obtenir de meilleures performances.
Action	Lorsqu'une alarme est remontée, le paquet qui a provoqué cette alarme subit l'action associée. Les actions sont : "Bloquer" ou "Passer". Une case grisée indique qu'aucune modification de l'action n'est possible.
Réaction	En plus de l'action associée à l'alarme, il est possible de définir une réaction à la remontée d'une alarme parmi "Envoyer un e-mail", "Mettre en quarantaine" de la machine responsable ou "Aucune réaction supplémentaire". 1) **Envoyer un e-mail** : lorsque le service d'envoi des mails est activé (*Cf.* Serveur d'e-mails Il est possible de définir l'envoi d'un e-mail lorsque deux facteurs sont réunis : le nombre de fois où l'alarme a été remontée et dans quel intervalle de temps. 2) **Mettre en quarantaine** : cette mise en quarantaine permet de bloquer l'ensemble des trafics en provenance de la machine responsable de la remontée d'alarme. Cette quarantaine dynamique est associée à une durée (en minutes) et ne résiste pas au redémarrage (la liste des machines en quarantaine est réinitialisée lors d'un redémarrage du firewall).
Détail	Cette option permet de sauvegarder le paquet responsable de la remontée d'alarme. La taille des informations sauvegardées dépend du modèle de votre firewall. Si cette option est activée, un tampon de données binaire contenant le paquet suspect sera associé à l'alarme émise. Ce paquet est alors visualisable grâce au NETASQ REAL-TIME MONITOR ou au NETASQ EVENT REPORTER. (*Voir le manuel NETASQ REAL-TIME MONITOR et NETASQ EVENT REPORTER*). Ce paquet peut ensuite être ouvert avec un outil comme Wireshark ou Packetyzer afin d'en détailler le contenu.
Niveau	Trois niveaux d'alarmes sont disponibles :"Ignorer", "Mineure" et "Majeure"
Nouveau	Ce paramètre indique que la signature contextuelle est nouvelle dans la liste des signatures contextuelles téléchargée sur le site Web NETASQ. Cette signature contextuelle reste validée **Nouveau** tant que l'administrateur ne l'a pas décochée. Les options possibles sont : "Non vérifié", "Vérifié", "Non vérifié dans tous les profils", "Vérifié dans tous les profils".
Message	Cela correspond à l'intitulé de l'alarme. Des informations complémentaires sur l'alarme sont disponibles directement dans NETASQ UNIFIED MANAGER grâce aux liens présents dans cette colonne. Les nouveaux messages non vérifiés sont indiqués en caractères gras.

6.6.2.3. Profils de protection

Le bouton **Configuration par défaut** vous permet de redéfinir la configuration des alarmes selon quatre profils de protection disponibles :

- Sécurité faible…
- Sécurité moyenne…
- Sécurité forte…
- Sécurité Internet : Ce profil est notamment tout à fait adapté à la prévention des menaces en provenance d'Internet.

6.6.2.4. Nouvelles signatures

La bonne configuration des signatures contextuelles, notamment en terme d'actions (remontées d'alarmes, blocage des trafics associés…) garantit la pertinence de l'action du firewall sur les trafics surveillés par ces signatures et la sécurité des ressources que le firewall protège. Or ces signatures contextuelles sont régulièrement mises à jour par NETASQ et la gestion des actions entreprises par ces signatures est

fastidieuse pour l'administrateur car il doit vérifier régulièrement l'apparition de nouvelles signatures et configurer l'action de celles-ci.

Ainsi le bouton **Nouvelles signatures** du menu **`Signatures contextuelles`** permet une "pré-configuration" du comportement des futures signatures contextuelles qui seront téléchargées lors du processus de mise à jour de la base de signatures contextuelles. Cette pré-configuration s'effectue par catégorie. Toutes les signatures appartenant à une catégorie donnée seront configurées avec les paramètres définis par l'administrateur.

Figure 140 : Valeurs par défaut des signatures ASQ

Le tableau suivant indique les options du bouton **Nouvelles signatures** :

Classification des signatures	La pré-configuration du comportement des futures signatures s'effectue par catégorie. La liste présentée par le champ "Classification des signatures" désigne l'ensemble des catégories qui doivent être configurées. La catégorie "Nouvelles classifications" fait référence aux catégories de signatures contextuelles qui n'existent pas encore.
Modèle	Tel que pour les signatures déjà téléchargées, il est possible d'appliquer pour les futures signatures, un modèle ou profil de protection parmi Sécurité faible, Sécurité moyenne, Sécurité élevée, Internet ou Personnalisé. Pour le modèle personnalisé, l'administrateur doit définir les actions par défaut associées à ces nouvelles signatures contextuelles.
Valeurs par défaut	Disponibles uniquement lors de la définition d'un modèle personnalisé, ces options permettent la définition des actions par défaut (**Action par défaut** : "Bloquer" ou "Passer", **Niveau par défaut** : "Majeure", "Mineure" ou "Ignorer" et le dump du paquet) associées aux nouvelles signatures de la catégorie sélectionnée.

L'insertion des nouvelles signatures dans cette base est réalisée à intervalle régulier par le firewall (Cf. *Partie 18/Chapitre 1 : Active Update*).

6.6.2.5. Aide en ligne

Chaque signature contextuelle est associée à une explication fournie par NETASQ au moyen d'une page HTML intégrée dans l'application NETASQ UNIFIED MANAGER. Pour afficher l'aide en ligne d'une signature contextuelle, reportez-vous à la procédure suivante :

1 Sélectionnez la signature contextuelle dont vous souhaitez l'explication.

2 Cliquez sur l'option **Afficher l'aide** pour afficher l'aide correspondante à la signature contextuelle sélectionnée.

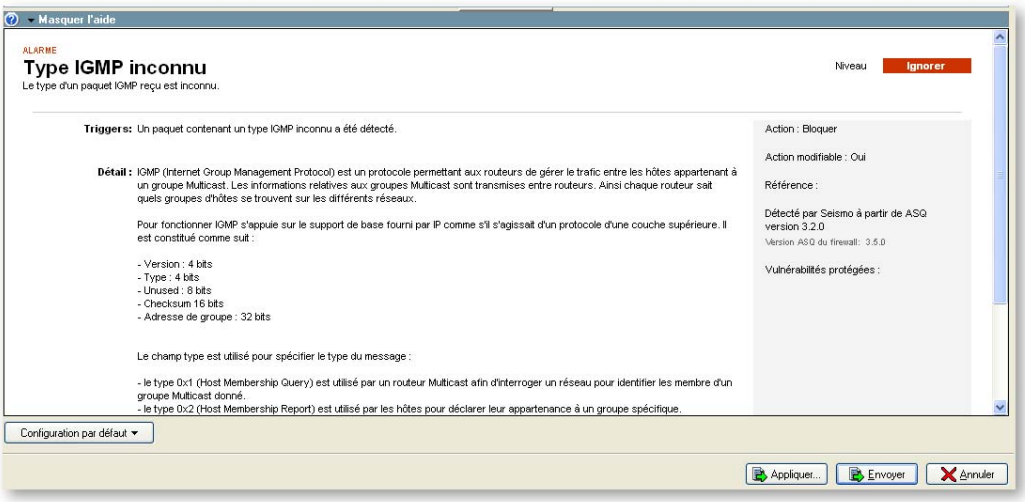


Figure 141 : Aide- Alarmes

L'aide affichée peut contenir des liens hypertextes vous permettant d'afficher une page HTML comportant des explications complémentaires.

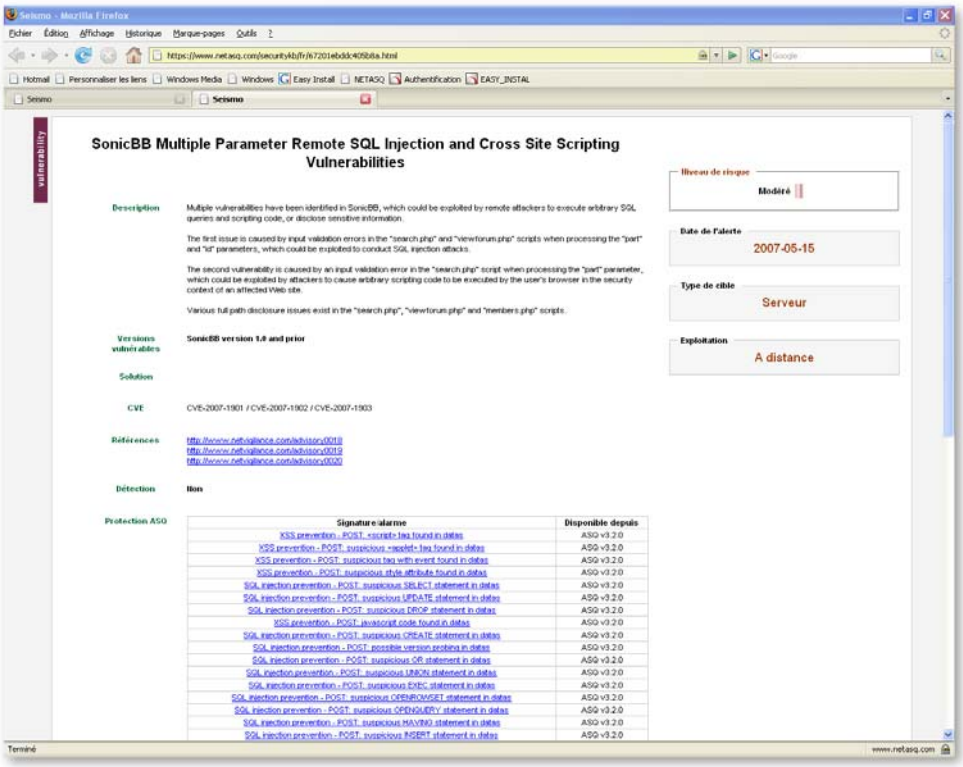


Figure 142 : Liens hypertextes

CHAPITRE 7 : LISTES

La liste noire de l'ASQ est une liste de machines permanentes dont le trafic est bloqué. Cette liste fonctionne de manière différente par rapport à la quarantaine. Cette liste peut être uniquement modifiée par l'écran de configuration de l'ASQ.
La quarantaine représente une liste temporaire de machines bloquées constituées par les alarmes sur lesquelles on a spécifié l'action "Mettre en quarantaine".

La liste blanche contient les machines qui ne seront jamais intégrées dans la liste noire, donc ne subiront pas l'analyse ASQ. Cette liste ne devrait contenir que des machines ne respectant pas les standards analysés par l'ASQ mais pour lesquelles l'administrateur décide de laisser passer le trafic de manière inconditionnelle. Cette liste permet au trafic d'entrer et de sortir. Les membres de cette liste sont donc accessibles de l'extérieur.

La liste noire contient un sous-menu **Exclusion**, permettant d'exclure par exemple, une machine d'un groupe de machines afin que celle-ci ne soit pas bloquée. Aussi, les machines incluses dans cette liste ne pourront jamais passer en quarantaine. Cette liste devrait contenir des machines de confiance dont la mise en quarantaine automatique (réaction d'alarme) n'est pas souhaitable.

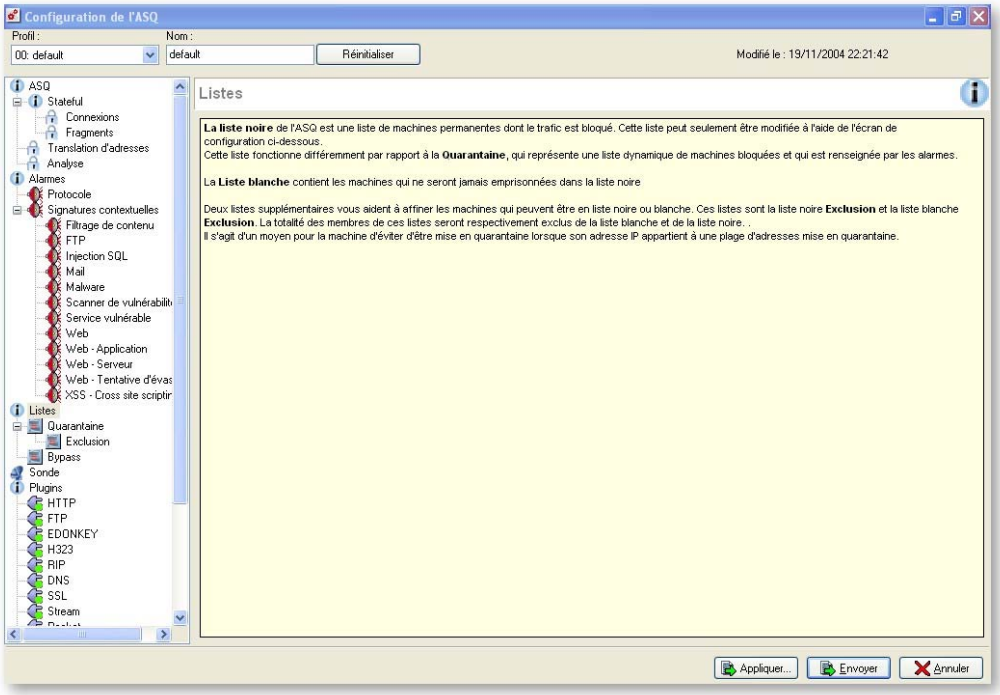


Figure 143 : Configuration de l'ASQ - Listes

Ce menu de la configuration de l'ASQ est divisé en deux parties : **Liste noire** et **By-pass**.

6.7.1. Liste noire

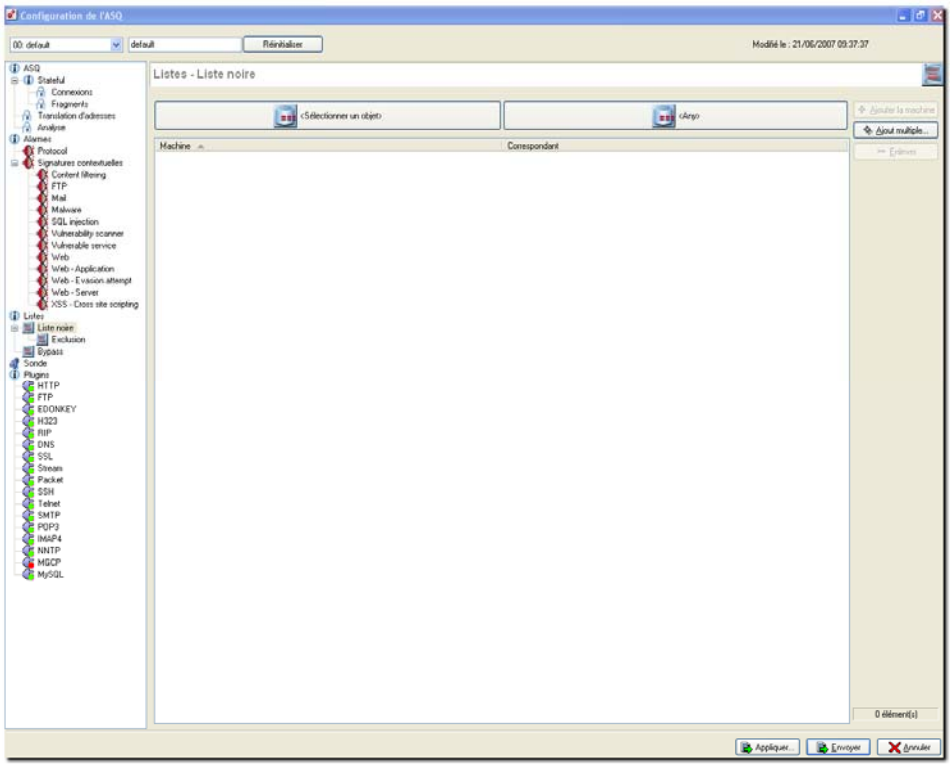


Figure 144 : Configuration de l'ASQ - Liste noire

Ce menu vous permet de configurer une quarantaine statique (cette quarantaine est différente de la quarantaine dynamique évoquée plus haut, (*Cf. Partie 6/Chapitre 6 : Alarmes protocolaires*). Cette quarantaine permet d'interdire tous les trafics en provenance d'une machine, à destination d'une machine ou entre deux machines.

Le menu de configuration des listes noires se présente sous la forme d'une grille représentant les machines et leur correspondant (si cela est nécessaire) actuellement en liste noire.

Pour ajouter une entrée dans cette grille, suivez la procédure suivante :

1. Sélectionnez la machine que vous désirez mettre en quarantaine statique grâce au bouton **Sélectionner un objet**.
2. Sélectionnez la machine correspondant pour la mise en quarantaine (tous les trafics, dans les deux sens, entre ces machines seront interdits). Si vous désirez interdire tous les trafics vers (ou en provenance) de n'importe quelle autre machine, veuillez laisser le champ "Correspondant" vide.
3. Ajoutez l'entrée en sélectionnant le bouton **Ajouter la machine**.

Le bouton **Enlever** vous permet de supprimer l'entrée sélectionnée.

Le bouton **Ajout multiple** vous permet de sélectionner simultanément plusieurs machines à placer en liste noire. Ce bouton ajoutera alors une entrée qui interdit les trafics entre la machine et toutes les autres machines.

6.7.1.1. Exclusion

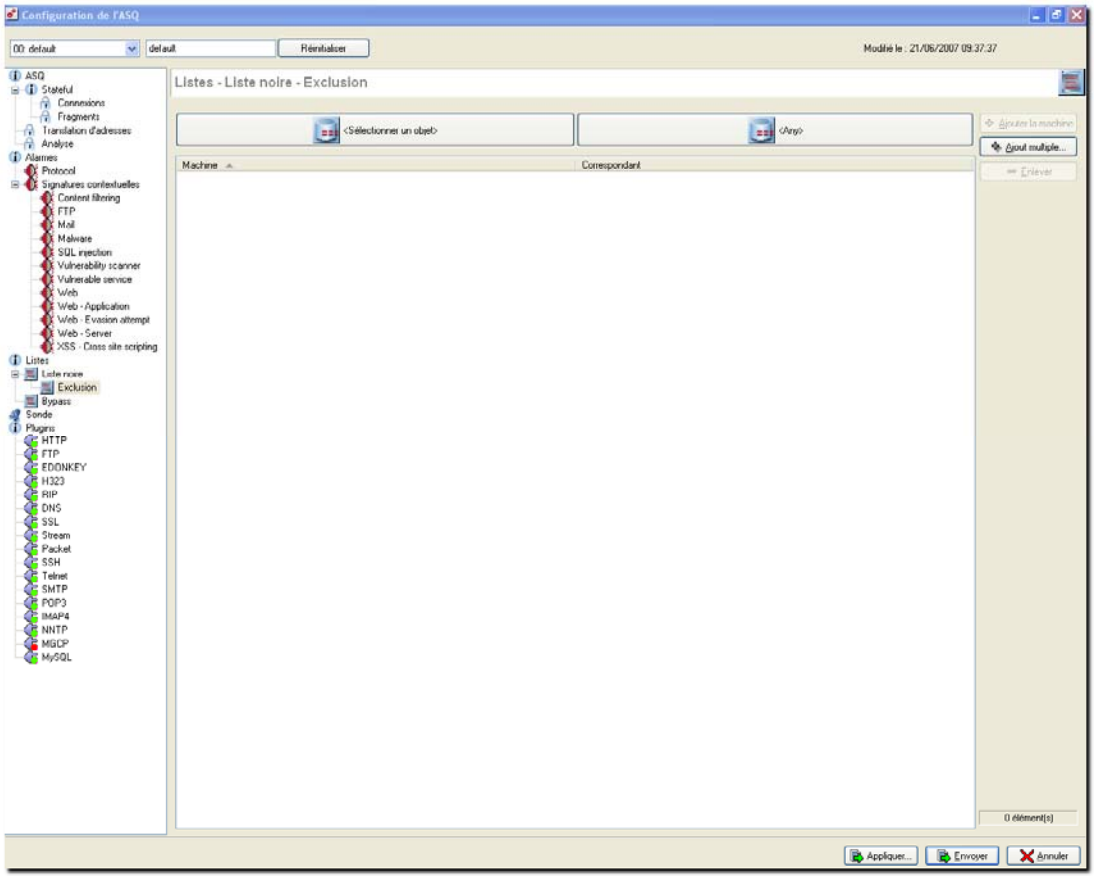


Figure 145 : Configuration de l'ASQ - Exclusion

Ce menu permet d'exclure une machine d'un groupe qui aurait été mise en quarantaine statique.

Le menu de configuration des exclusions de listes noires se présente sous la forme d'une grille représentant les machines et leur correspondant (si cela est nécessaire) actuellement en exclus de la liste noire.

Pour ajouter une entrée dans cette grille, suivez la procédure suivante :

1 Sélectionnez la machine que vous désirez exclure de la quarantaine statique en cliquant sur le bouton **Sélectionner un objet**.

2 Sélectionnez la machine correspondant pour l'exclusion de la quarantaine (tous les trafics, dans les deux sens, entre ces machines ne seront pas interdits). Si vous désirez ne pas interdire tous les trafics vers (ou en provenance) de n'importe quelle autre machine, veuillez laisser le champ "Correspondant" vide.

3 Ajoutez l'entrée en sélectionnant le bouton **Ajouter la machine**.

6.7.2. By-pass

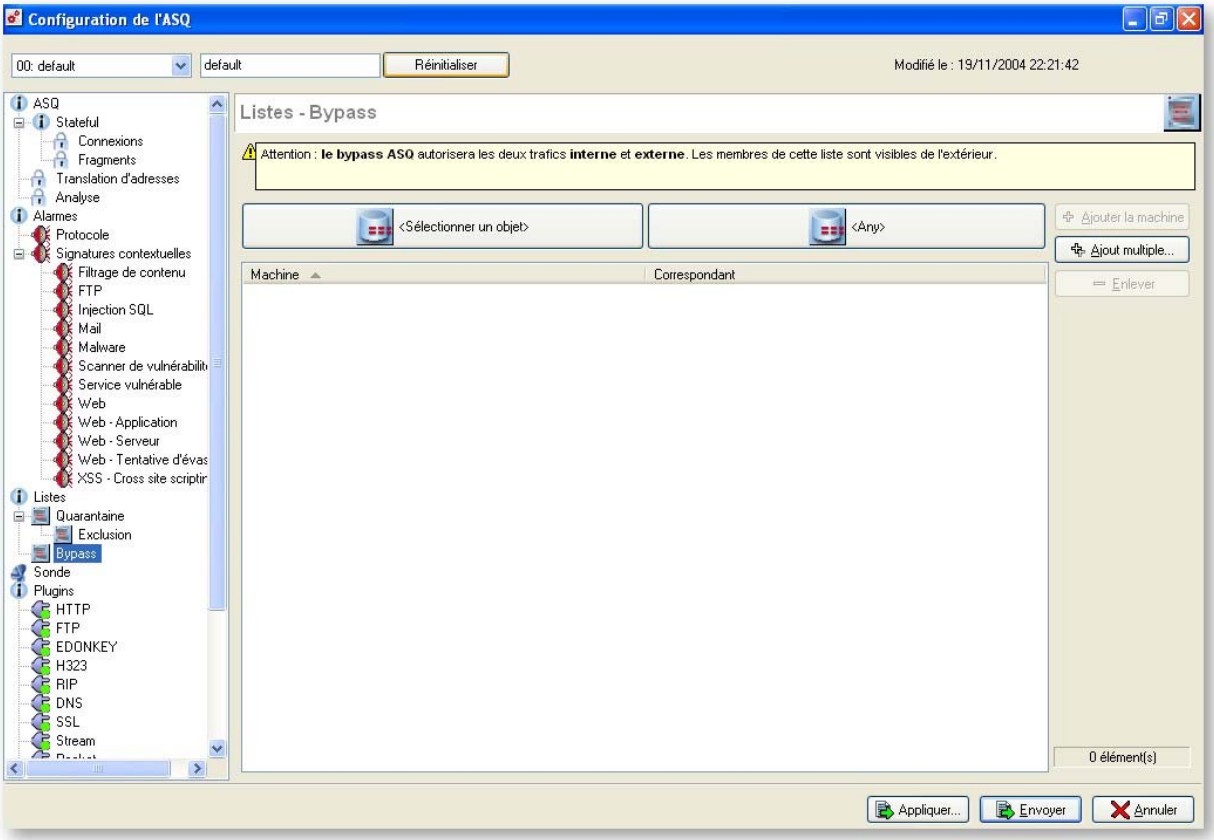


Figure 146 : Configuration de l'ASQ - Bypass

Ce menu vous permet de configurer une liste blanche de machines. Autrement appelée "By-pass", cette liste de contournement de l'ASQ permet de définir les trafics qui ne doivent pas être soumis à l'analyse de l'ASQ.

AVERTISSEMENT

La configuration d'une liste blanche de machines entraîne une très forte diminution de la sécurité des ressources et infrastructures protégées par le firewall. En effet, AUCUNE analyse ni politique de filtrage n'est appliquée au trafic concerné par la liste blanche (dans les deux sens).

Le menu de configuration des listes blanches se présente sous la forme d'une grille représentant les machines et leur correspondant (si cela est nécessaire) actuellement en liste blanche.

Pour ajouter une entrée dans cette grille, suivez la procédure suivante :

1. Sélectionnez la machine que vous désirez mettre en liste blanche en sélectionnant le bouton **Sélectionner un objet.**
2. Sélectionnez la machine correspondant pour la mise en liste blanche (tous les trafics, dans les deux sens, entre ces machines ne seront pas analysés par l'ASQ). Si vous désirez contourner l'analyse de l'ASQ pour tous les trafics vers (ou en provenance) de n'importe quelle autre machine, veuillez laisser le champ "Correspondant" vide.
3. Ajoutez l'entrée en sélectionnant le bouton **Ajouter la machine**.

6.7.2.1. Priorité en liste noire, liste blanche et filtrage

Un paquet (pas de notion de sens) est systématiquement refusé s'il correspond à une entrée de la liste noire, quelle que soit la liste blanche et la politique de filtrage.
La vérification de liste noire faite, un paquet absent (de la liste noire) est systématiquement autorisé s'il correspond à une entrée dans la liste blanche, quelle que soit la politique de filtrage, sans passer par les analyses de l'ASQ (protocolaires et signatures contextuelles).

CHAPITRE 8 : SONDE

Cet écran comprend une liste de services potentiellement dangereux détectés par l'alarme Sonde de port. Cette alarme est activée lorsqu'aucune règle de filtrage n'a traité le paquet.

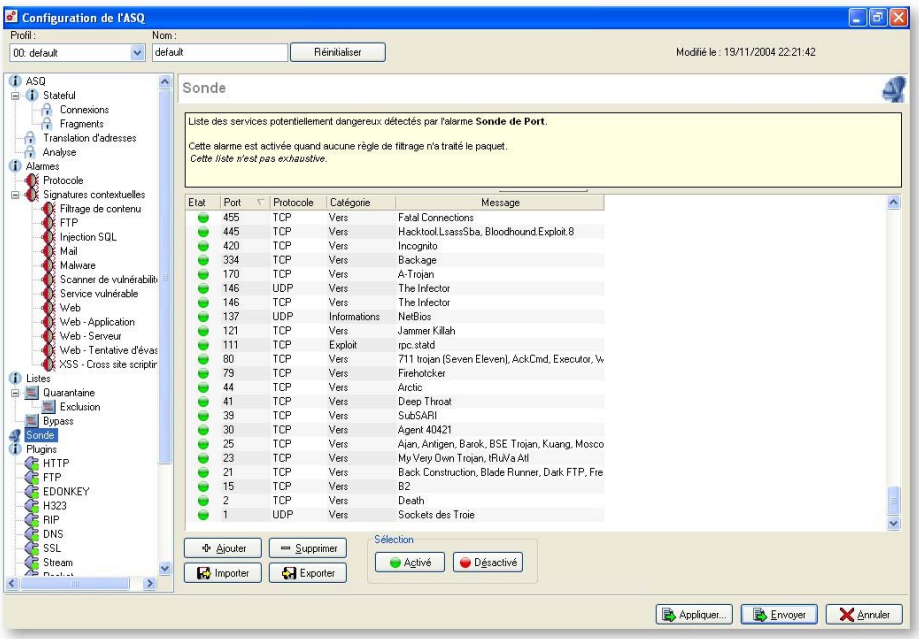


Figure 147 : Configuration de l'ASQ - Sonde

Ce menu présente une liste de services potentiellement dangereux utilisés fréquemment par des chevaux de Troie notamment ou des vers. Lorsqu'un de ces services est utilisé cela remonte l'alarme "Sonde de port" si et seulement si aucune règle de filtrage n'est associé au paquet en question.

Grâce aux boutons d'action au bas de la fenêtre vous pouvez modifier cette liste suivant les ports que vous désirez surveiller.

La grille se divise en cinq parties :

Etat	Pour désactiver, sans supprimer la sonde de ce port.
Port	Le numéro du port à surveiller. Ce numéro est compris entre 1 et 65535.
Protocole	Le protocole véhiculant des paquets malveillants. (TCP ou UDP).
Catégorie	Plusieurs catégories sont disponibles (Divers, Informations, Exploit, Vers, P2P, Relai).
Message	Un commentaire que vous pouvez indiquer librement. On peut y noter l'intitulé de la sonde de port.

Les boutons situés au bas de l'écran permettent de :

Ajouter	Ajoute un service. Une ligne supplémentaire s'affiche dans le tableau. Dans la colonne « Etat », activez ou désactivez ce service. Dans la colonne « Port », sélectionnez le n° de port. Dans la colonne « Protocole », sélectionnez TCP ou UDP. Dans la colonne « Catégorie », choisissez parmi les options Divers, Informations, Exploit, Vers, P2P, Relai. Dans la colonne « Message », donnez une description.
Supprimer	Supprime directement la ligne préalablement sélectionnée.

L'utilisateur peut modifier chacune de ces propriétés. Par contre, une contrainte interdit d'avoir deux sondes sur le même port et le même protocole.

> **Exemple**
> Une sonde sur le port 25/TCP et une autre sur le port 25/UDP peuvent coexister. Par contre, deux sondes ou plus sur le port 25/TCP sont refusées.

CHAPITRE 9 : PLUGINS

6.9.1. Présentation

La particularité de l'ASQ (*Active Security Qualification*) est son architecture optimisée à plugins protocolaires. Ces plugins réalisent une étude approfondie des données qui transitent dans les paquets, notamment en vérifiant leur cohérence par rapport aux entêtes, aux protocoles correspondants.

Les plugins vérifient la conformité aux RFC partiellement ou complètement afin de détecter toutes dérives et attaques (Buffer overflow sur URL, Encodage UTF-8 invalide…).

L'association d'un plugin avec le flux d'informations est réalisée soit :

- Manuellement via les objets *Services* ou le port par défaut configuré pour le plugin.
- Automatiquement, par détection du protocole applicatif.

La liste des plugins est la suivante :

- HTTP
- FTP
- EDONKEY
- H323
- RIP
- DNS
- SSL
- Stream
- Packet
- SSH
- Telnet
- SMTP
- POP3
- IMAP4
- NNTP
- MGCP
- RTP
- RTCP
- SIP
- MySQL

6.9.2. Attachement

Ces plugins sont rattachés à leur port standard.

Exemple
http sur port 80/tcp

Le plugin peut optionnellement détecter le protocole et s'attacher automatiquement à la connexion. Cela permet par exemple de capturer les sessions HTTP quelque soit le port dans une politique de filtrage ouverte. Il est aussi possible de configurer un plugin pour bloquer tout trafic se faisant sur un port non standard comme par exemple le trafic HTTP sur un port autre que le port TCP 80. Les plugins peuvent être configurés pour s'attacher sur toutes les connections utilisant un port réseau donné, par exemple le plugin DNS s'attachera sur le port UDP 53. Les plugins peuvent enfin être attachés depuis les règles de la politique de filtrage.

Les paramètres de configuration des plugins protocolaires sont modifiables dans l'onglet **Plugins** du menu **Prévention d'Intrusion** de l'arborescence.

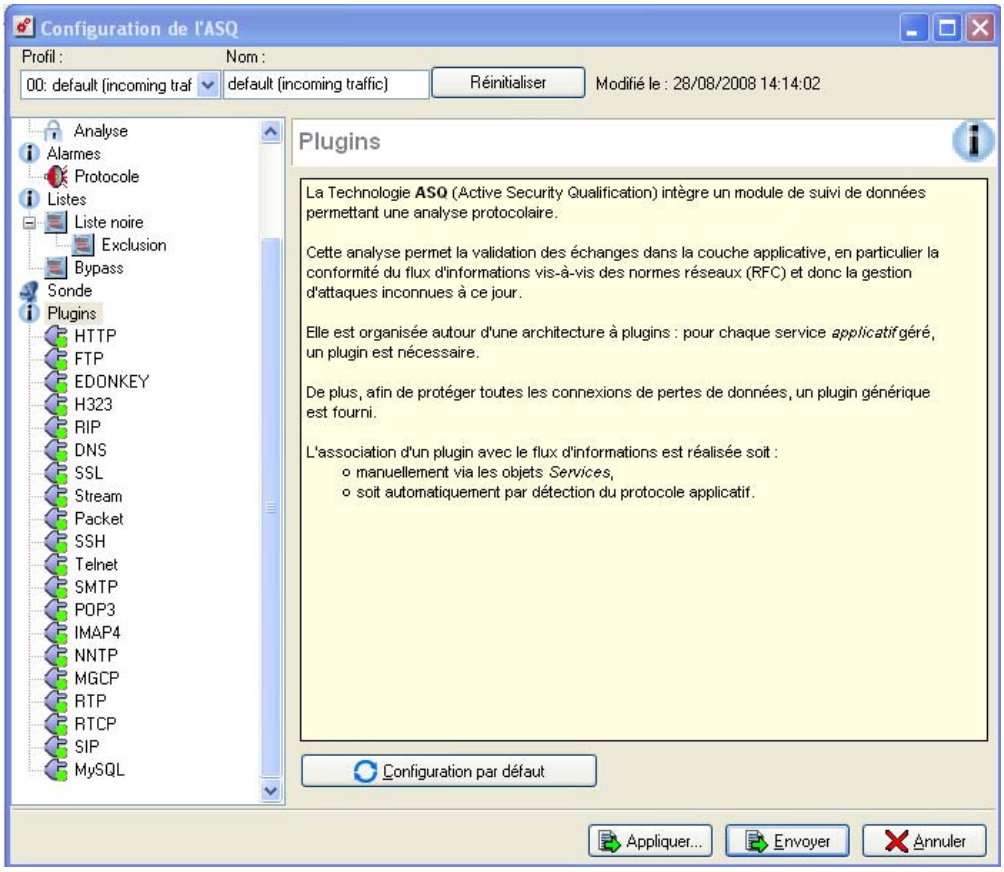


Figure 148 : Configuration de l'ASQ - Plugins

Les fonctionnalités disponibles pour les plugins actuels sont présentées dans le tableau suivant :

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.
Traces	Activation ou désactivation de la remontée des logs concernant le plugin.

Bloquer jusqu'à reconstitution des données	Cocher cette option permet l'analyse de certains flux potentiellement dangereux. Cette option est cochée par défaut. Ainsi, le plugin HTTP empêche le trafic de passer tant qu'il n'a pas reçu suffisamment de données pour être sûr que le flux est correct.
Support de Shout Cast	Support du Shout Cast. (HTTP uniquement).
Support de Webdav	Support du WebDav. (HTTP uniquement).
RFC 775	Respect et support des fonctionnalités de parcours des répertoires du protocole FTP. (FTP uniquement).
Authentification SSL	Activation du support de l'authentification SSL pour le protocole FTP. (FTP uniquement).
Pas de validation d'authentification	Cette option permet de rendre facultative la séquence d'authentification sur un serveur FTP.

6.9.3. Le plugin HTTP

L'activation de ce plugin permet la prévention de grandes familles d'attaques applicatives basées sur le protocole HTTP. Les différentes analyses effectuées par ce plugin (notamment la vérification de la conformité aux RFC), la validation de l'encodage utilisé dans l'URL ou la vérification de la taille de l'URL et du corps de la requête, vous permettent de stopper des attaques telles que Code RED, Code Blue, NIMDA, HTR, WebDav, Buffer Over flow ou encore Directory Traversal…
La gestion des débordements de tampons (ou Buffer Over flow) est primordiale chez NETASQ, c'est pourquoi la définition des tailles maximales permises pour les tampons dans le cadre du protocole HTTP est particulièrement développée.

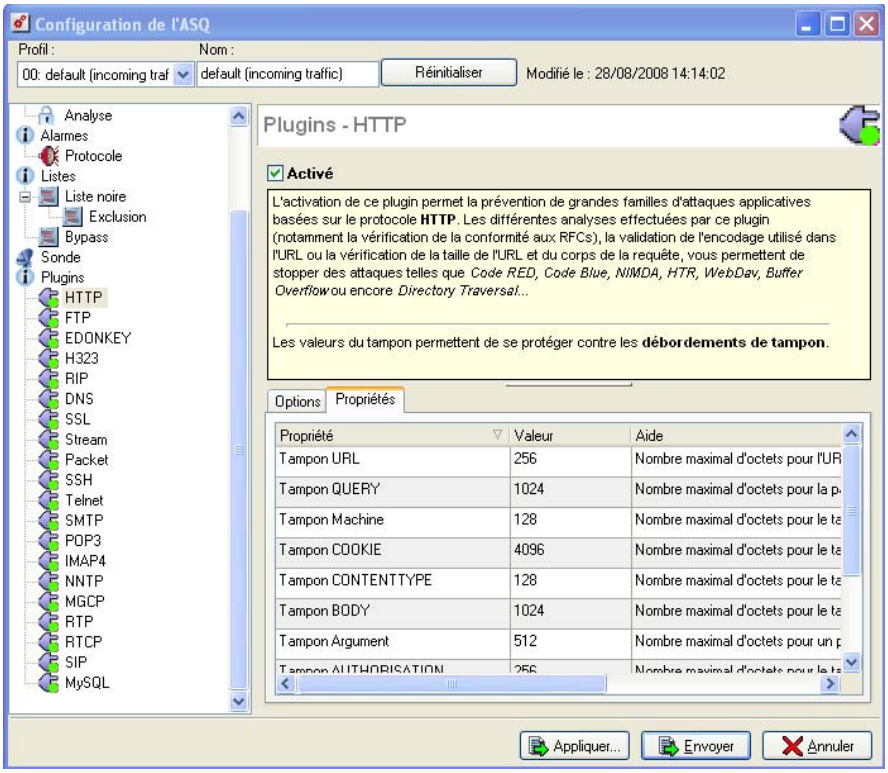


Figure 149 : Configuration de l'ASQ - HTTP

6.9.3.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.
Traces	Activation ou désactivation de la remontée des logs concernant le plugin.
Bloquer jusqu'à reconstitution des données	Cocher cette option permet l'analyse de certains flux potentiellement dangereux. Cette option est cochée par défaut. Ainsi, le plugin HTTP empêche le trafic de passer tant qu'il n'a pas reçu suffisamment de données pour être sûr que le flux est correct.
Support de Shout Cast	Support du Shout Cast. (HTTP uniquement).
Support de Webdav	Support du WebDav. (HTTP uniquement).

6.9.3.2. Détection des URL trop longues

Avec les sites multimédias récents, la longueur de l'URL devient de plus en plus importante. L'alarme "débordement de buffer dans l'URL" se déclenche de plus en plus souvent à tort. La détection des URL trop longues s'effectue de manière plus fine désormais à l'aide de 3 tampons :

- Tampon URL
- Tampon QUERY
- Tampon Argument

6.9.3.3. Détection double encodage et encodage invalide

Les URL sont de plus en plus souvent passées en paramètre (notamment les publicités), les doubles redirections sont de plus en plus fréquentes, entraînant un nombre croissant de faux positifs. De plus la détection d'attaque de double-encodage par signature n'est pas 100% efficace.
Lors de la détection d'un caractère % encodé, la remontée d'alarmes n'est donc plus une solution viable. En effet, de par son nombre élevé de faux positifs, cette alarme est désactivée. Il est désormais possible de contrer efficacement cette tentative d'évasion sans déclencher de faux positifs.

Lorsque cela est possible, lorsque l'encodage est invalide, mais que le décodage est possible, le caractère invalide peut désormais être décodé. (Cas d'un caractère qui ne devrait pas censé être encodé).

Cette détection s'effectue de manière automatique et permet une amélioration de détection plus fine des encodages.

Veuillez vous référer à l'Annexe T : Liste des alarmes relatives aux protocoles.

6.9.3.4. Onglet "Propriétés"

Opérations autorisées	Liste des commandes HTTP autorisées (au format CSV) séparées par des virgules. Longueur maximum de 128 caractères.
Opérations interdites	Liste des commandes HTTP interdites (au format CSV) séparées par des virgules. Longueur maximum de 128 caractères.
Port par défaut	Un ou plusieurs ports que le plugin va relier.
Tampon URL	Ce tampon concerne la totalité de l'URL. La syntaxe est la suivante : http://<URLBuffer>?<Querybuffer>. Nombre maximum d'octets pour l'URL incluant les attributs de formatage. La valeur indiquée par défaut est de 256.
Tampon BODY	Nombre maximum d'octets pour le champ BODY incluant les attributs de formatage.
Tampon COOKIE	Nombre maximum d'octets pour le champ COOKIE incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Tampon Machine	Nombre maximum d'octets pour le champ HOST incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Tampon CONTENTTYPE	Nombre maximum d'octets pour le champ CONTENTTYPE incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Tampon AUTHORIZATION	Nombre maximum d'octets pour le champ AUTHORIZATION incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Tampon QUERY	Le tampon Query inclut un ensemble d'arguments. Ces arguments sont séparés par le signe &. Nombre maximal d'octets pour la partie QUERY de cette URL. (Min : 128 ; Max : 4096). La valeur indiquée par défaut est d 1024.
Tampon Argument	La syntaxe est la suivante : "token=value"&. Nombre maximum d'octets pour un paramètre dans l'URL. (Min : 128 ; Max : 4096). La valeur indiquée par défaut est de 512.

6.9.4. Le plugin FTP

Le plugin FTP supporte la RFC principale [RFC959] ainsi que de nombreuses extensions.

L'activation de ce plugin permet de prévenir des grandes familles d'attaques applicatives basées sur le protocole FTP. Ce plugin effectue diverses analyses comme l'analyse de conformité aux RFC, la vérification de la taille des paramètres des commandes FTP ou les restrictions sur le protocole (SITE EXEC par exemple). Ces analyses, permettent ainsi de stopper les attaques comme FTP Bounce, FTP PASV DoS, Buffer overflow…Ce plugin est indispensable pour permettre au trafic FTP de traverser le firewall et de gérer dynamiquement les connexions de donnéesdu protocole FTP.

6.9.4.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a

connexion lors de l'attachement avec le plugin	déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.
Traces	Activation ou désactivation de la remontée des logs concernant le plugin.
RFC 775	Respect et support des fonctionnalités de parcours des répertoires du protocole FTP. (FTP uniquement).
Authentification SSL	Activation du support de l'authentification SSL pour le protocole FTP. (FTP uniquement).
Pas de validation d'authentification	Cette option permet de rendre facultative la séquence d'authentification sur un serveur FTP.

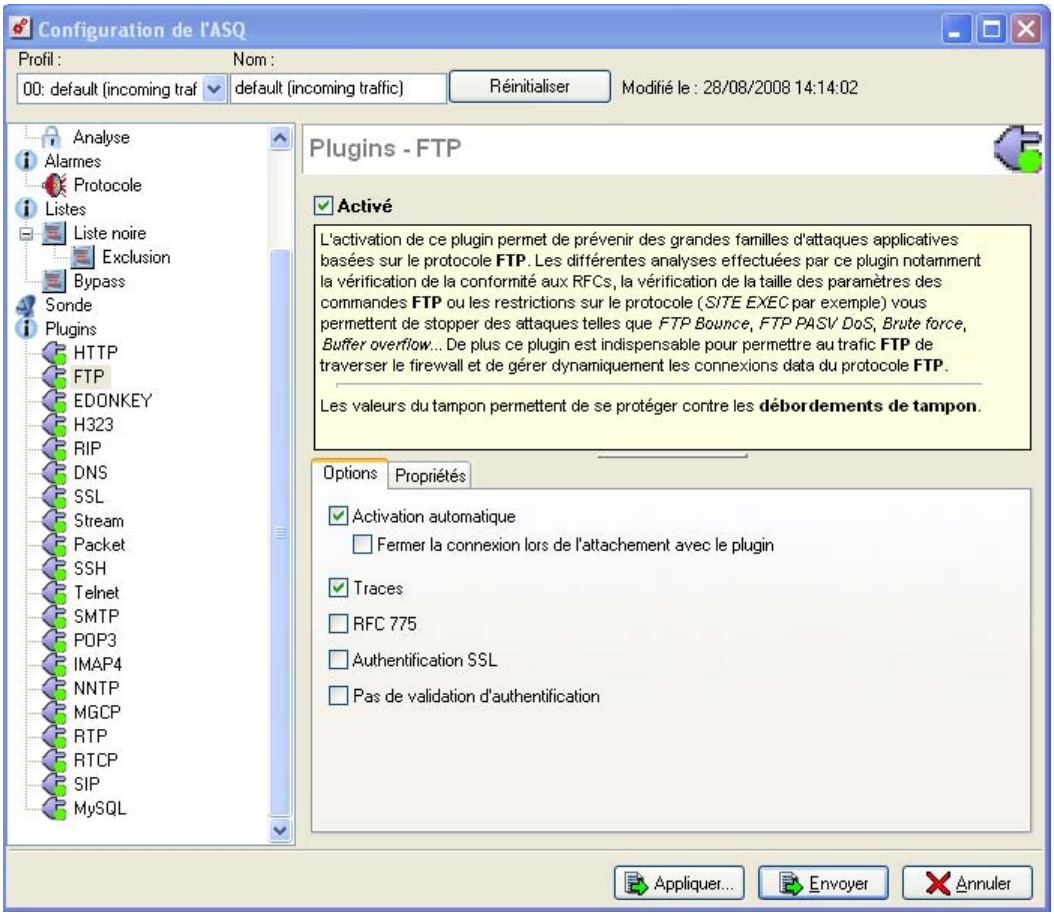


Figure 150 : Configuration de l'ASQ - FTP

6.9.4.2. Propriétés

Les différents tampons FTP pouvant être gérés sont indiqués dans le tableau suivant :

Port par défaut	Un ou plusieurs ports que le plugin va relier.
Tampon LIGNE	Nombre maximum d'octets pour une ligne FTP incluant les attributs de formatage. (Min : 128 ; Max : 2048).
Tampon PASS	Nombre maximum d'octets pour le mot de passe FTP incluant les attributs de formatage. (Min : 128 ; Max : 2048).
Tampon PATH	Nombre maximum d'octets pour le chemin FTP incluant les attributs de formatage. (Min : 128 ; Max : 2048).

Tampon SITE	Nombre maximum d'octets pour le Site String FTP incluant les attributs de formatage. (Min : 128 ; Max : 2048).
Tampon UTILISATEUR	Nombre maximum d'octets pour le nom d'utilisateur FTP incluant les attributs de formatage. (Min : 128 ; Max : 2048).
Opérations autorisées	Liste des commandes FTP autorisées (au format CSV), séparées par des virgules. Longueur maximum de 128 caractères.
Opérations interdites	Liste des commandes FTP interdites (au format CSV), séparées par des virgules. Longueur maximum de 128 caractères.

6.9.5. Le plugin EDONKEY

L'activation de ce plugin vous permet de supporter le protocole de ce logiciel. Grâce à ce plugin, vous pouvez récupérer des traces très complètes sur les fichiers échangés (nom du fichier par exemple).

Le plugin supporte l'attachement dynamique aux connexions et va donc pouvoir tracer le protocole sur des ports non standards.

6.9.5.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Traces	Activation ou désactivation de la remontée des logs concernant le plugin.

6.9.5.2. Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.6. Le plugin H323

L'activation de ce plugin vous permet de vérifier la conformité des paquets H323 reçus par rapport aux normes en vigueur pour ce protocole. Ce plugin est indispensable pour permettre au trafic H323 de traverser le firewall et de gérer dynamiquement les connexions datas du protocole H323.

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.7. Le plugin RIP

L'activation de ce plugin vous permet de vérifier la conformité des paquets RIP reçus par rapport aux RFC en vigueur pour ce protocole.

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.8. Les tampons du plugin DNS.

L'activation de ce plugin permet de prévenir des grandes familles d'attaques applicatives basées sur le protocole DNS.
Les différentes analyses effectuées par ce plugin, notamment la restriction sur les transferts de zones ou la conformité aux RFCs vous permettent de stopper des attaques telles que DNS ID spoofing, le DNS cache poisoning ou encore le DNS zone change et le DNS zone Update.
Les différents tampons DNS pouvant être gérés sont indiqués dans le tableau suivant :

Port par défaut	Un ou plusieurs ports que le plugin va relier.
Tampon NOM	Nombre maximum d'octets pour le champ NOM d'une requête DNS. (Min : 128 ; Max : 2048).

6.9.9. Les tampons du plugin SSL

Le plugin SSL a pour objectif de valider que le protocole SSL est correctement joué au travers du firewall. Certaines options permettent de renforçer la sécurité de ce protocole. Par exemple, il est possible d'interdire des négociations d'algorithmes cryptographiques considérés comme faibles, de détecter des logiciels utilisant le SSL pour passer outre les politiques de filtrage (SKYPE, proxy HTTPS,…).

6.9.9.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

6.9.9.2. Propriétés

Les différents tampons SSL pouvant être gérés sont indiqués dans le tableau suivant :

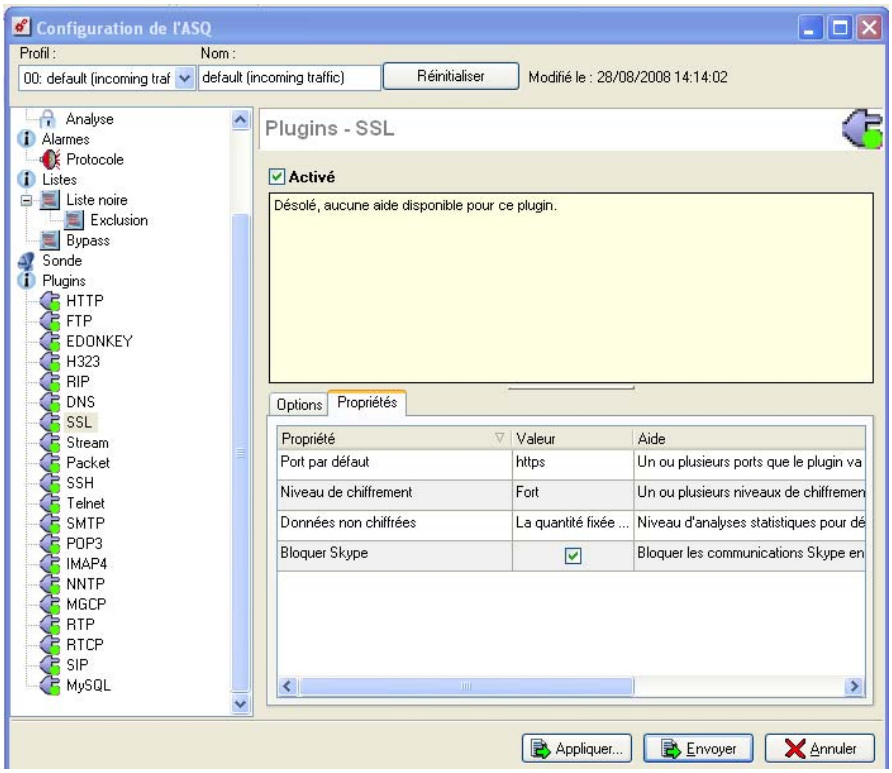


Figure 151 : Configuration de l'ASQ - SSL

Port par défaut	Un ou plusieurs ports que le plugin va relier.
Niveau de chiffrement	Une ou plusieurs puissances de chiffrement qui seront acceptées par le plugin. Les valeurs possibles sont "Chiffrement inconnu" (1), "Chiffrement NUL" (2), "Chiffrement faible (RC4-40, DES-40, etc.)" (4), Chiffrement commun (DES, RC4-64, etc.)" (8), "Chiffrement fort (AES-128, etc.)" (16). Le chiffrement fort AES est coché par défaut (niveau de chiffrement 16).
Données non chiffrées	Niveau d'analyses statistiques pour détecter les données chiffrées. Les options possibles sont "Pas d'analyses de données", "Toutes les données sont analysées", "La quantité fixée de données est analysée". Après négociation SSL, les communications avec Google talk, Hopster sont bloquées.
Bloquer Skype	L'application Skype utilise le port 443 et un protocole ressemblant à du SSL valide. Toutefois, plusieurs concurrents bloquent l'utilisation du Skype. Cette option permet de bloquer le trafic SKYPE sans pour autant bloquer tout le SSL. Il suffit de cocher cette option pour bloquer le trafic SKYPE.

6.9.10. Particularité des plugins "Stream" et "Packet"

Ces plugins permettent la vérification des données liées à aucun protocole en particulier. Cette option, une fois activée, n'est utilisée par le firewall que si aucun autre plugin ne s'active lors de l'analyse du paquet en question. Cette option est cochée par défaut pour vous offrir un maximum de sécurité, l'inconvénient est que les performances du firewall en sont réduites. Vous pouvez désactiver cette option, cela aura pour

conséquence de garantir de meilleures performances mais la sécurité de vos données sera moindre. Le plugin **Stream** est associé au protocole TCP et le plugin **Packet** à l'UDP.

6.9.10.1. Plugin Stream

Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.10.2. Plugin Packet

Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.11. Le plugin SSH

Le plugin SSH a pour objectif la détection des connexions entre deux machines utilisant le protocole sécurisé SSH. La détection s'effectue sur la bannière du client et du serveur. Le plugin n'effectue pas d'analyse du contenu du flux SSH. Il est utilisé par SEISMO pour détecter la version du client et/ou du serveur SSH utilisé afin de remonter d'éventuelles vulnérabilités.

6.9.11.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

6.9.11.2. Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.12. Le plugin Telnet

Le plugin TELNET a pour objectif de détecter les connexions entre deux machines utilisant le protocole TELNET. La détection est effectuée par analyse du préfixe commun à toutes les commandes TELNET. Le plugin n'effectue pas d'analyse de sécurité sur le contenu du flux TELNET.

6.9.12.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

6.9.12.2. Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.13. Le plugin SMTP

Le plugin SMTP a pour objectif de détecter les connexions entre un client et un serveur mail ou entre deux serveurs mails utilisant le protocole SMTP. La détection est effectuée en recherchant une réponse du serveur de type 220 (bannière du serveur SMTP). Le plugin n'effectue pas d'analyse du protocole SMTP. Il est utilisé par SEISMO pour détecter la version du client et/ou du serveur mail utilisé afin de remonter d'éventuelles vulnérabilités.

6.9.13.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

6.9.13.2. Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.14. Le plugin POP3

Le plugin POP3 a pour objectif de détecter les connexions entre un client et un serveur mail utilisant le protocole POP3. La détection se base sur le premier paquet du serveur devant contenir une ligne commençant par +OK. Le plugin n'effectue pas d'analyse du protocole POP3. Il est utilisé par SEISMO pour détecter la version du serveur mail utilisé en analysant la bannière du serveur afin de remonter d'éventuelles vulnérabilités.

6.9.14.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

6.9.14.1. Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.15. Le plugin IMAP4

Le plugin IMAP4 a pour objectif de détecter les connexions entre un client et un serveur mail utilisant le protocole IMAP4. La détection se base sur le premier paquet du serveur devant contenir une ligne commençant par *OK+. Le plugin n'effectue pas d'analyse du protocole IMAP4. Il est utilisé par SEISMO pour détecter la version du serveur mail utilisé en analysant la bannière du serveur afin de remonter d'éventuelles vulnérabilités.

6.9.15.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

6.9.15.2. Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.16. Le plugin NNTP

Le plugin NNTP a pour but de détecter les connexions entre deux machines utilisant le protocole de news NNTP. La détection se fait sur la bannière du serveur de news. Le plugin n'effectue pas d'analyse du contenu du flux NNTP. Il est utilisé par SEISMO pour détecter la version du serveur de news utilisé afin de remonter d'éventuelles vulnérabilités en analysant la bannière.

6.9.16.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

6.9.16.2. Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.17. Le plugin MGCP

Le plugin MGCP assure l'analyse protocolaire ainsi que l'autorisation dynamique des connexions secondaires.
L'analyse des connexions est réalisée ligne par ligne : la ligne doit être complète avant le lancement de l'analyse. Pour chaque ligne d'en-tête une vérification est réalisée en fonction de l'état de l'automate.

- Pour les requêtes et les réponses :
  - Vérification de la version MGCP et de la commande (pour les requêtes) ou du code de retour de la commande (pour les réponses), validation de l'identifiant de transaction, validation du nom de l'appelant, protection contre les attaques (encodage, format, débordement de tampons,…), validation des paramètres MGCP pour les requêtes.
  - Analyse et validation des données présentes dans le SDP (encodage, débordement de tampons, conformité à la RFC, présence et ordre des champs obligatoires, format des lignes…).
- Pour les réponses (en plus des vérifications précédentes) : cohérence générale de la réponse et par rapport à la requête.

6.9.17.1. Options

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a

connexion lors de l'attachement avec le plugin	déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

6.9.17.2. Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.18. Le plugin RTP

Le plugin RTP a pour objectif la validation des connexions de voix sur IP utilisant le protocole de transport RTP. Le plugin n'effectue pas de détection dynamique du protocole RTP. Il peut être attaché par une règle de filtrage ou par un autre plugin de voix sur IP (MGCP, SIP) sur une connexion fille. Le plugin RTP valide la conformité de l'entête des paquets RTP vis-à-vis de la RFC 3550. Il est possible d'interdire l'utilisation de certains codecs RTP.

Dans le cas où le plugin est attaché sur une connexion fille par le plugin SIP ou MGCP, la fonction d'audit est agrémentée d'un identifiant de groupe de session permettant de retrouver toutes les connexions d'une conversation, du nom de l'appelant et du type de média utilisé (audio, vidéo, application, donnée, contrôle…)

AllowCodec	A list of allowed RTP codecs, separated by coma. Maximum lengh is 128 chars.

6.9.19. Le plugin RTCP

Le plugin RTCP a pour objectif la validation des connexions de voix sur IP utilisant le protocole de contrôle RTCP. Le plugin n'effectue pas de détection dynamique du protocole RTCP. Il peut être attaché par une règle de filtrage ou par un autre plugin de voix sur IP (MGCP, SIP) sur une connexion fille. Le plugin RTCP valide la conformité de l'entête des paquets RTCP vis-à-vis de la RFC 3550, 3611, 2032. Un paquet UDP peut contenir plusieurs paquets RTCP (paquet composé). Il est possible d'interdire l'utilisation de certaines commandes RTCP.

Dans le cas où le plugin est attaché sur une connexion fille par le plugin SIP ou MGCP, la fonction d'audit est agrémentée d'un identifiant de groupe de session permettant de retrouver toutes les connexions d'une conversation, le nom de l'appelant et le type de média utilisé (audio, vidéo, application, donnée, contrôle ...).

Opérations interdites	A list of denied RTCP operations, separated by coma. Maximum lengh is 128 chars.
Opérations autorisées	A list of allowed RTCP operations, separated by coma. Maximum length is 128 chars.

6.9.20. Le plugin SIP

SIP (*Session Initiation Protocol*) est un protocole utilisé pour les télécommunications multimédia telles que la téléphonie par Internet (VoIP) ou encore la communication poste à poste.

Dans le cadre d'un échange poste à poste, une fois que la communication est établie, deux canaux (A vers B et Bvers A) sont utilisés pour véhiculer les données. Pour chaque canal le plugin SIP du moteur ASQ créée deux connexions : une pour véhiculer les données du protocole RTP et l'autre associée aux informations du protocole RTCP.

Le plugin SIP supporte la RFC principale RFC3261 ainsi que les extensions suivantes qui peuvent être activées ou bloquées au besoin :

- RFC3262 : PRACK
- RFC3265 : SUBSCRIBE, NOTIFY
- RFC2976 : INFO
- RFC3311 : UPDATE
- RFC3428 : MESSAGE
- RFC3515 : REFER
- RFC3903 : PUBLISH

Le plugin SIP assure l'analyse protocolaire ainsi que l'autorisation dynamique des connexions secondaires.L'analyse des connexions est réalisée ligne par ligne: la ligne doit être complète avant le lancement de l'analyse. Pour chaque ligne d'en-tête une vérification est réalisée en fonction de l'état de l'automate.

- Pour les requêtes et les réponses :

  - Vérification de la version SIP et de l'opération, validation de l'URI qui doit être encodée en UTF-8.
  - Analyse de l'en-tête ligne par ligne: validation des champs de l'en-tête et extraction d'information (nom de l'appelant et de l'appelé ...), protection contre les attaques (encodage, débordement de tampons, présence et ordre des champs obligatoires, format des lignes ...).
  - Analyse et validation des données présentes dans le SDP (encodage, débordement de tampons, conformité à la RFC, présence et ordre des champs obligatoires, format des lignes ...).

- Pour les réponses (en plus des vérifications précédentes): cohérence générale de la réponse et cohérence par rapport à la requête.

La fonction d'audit est agrémentée d'un identifiant de groupe de session permettant de retrouver toutes les connexions d'une conversation, les noms de l'appelant et de l'appelé et le type de média utilisé (audio, vidéo, application, donnée, contrôle ...).

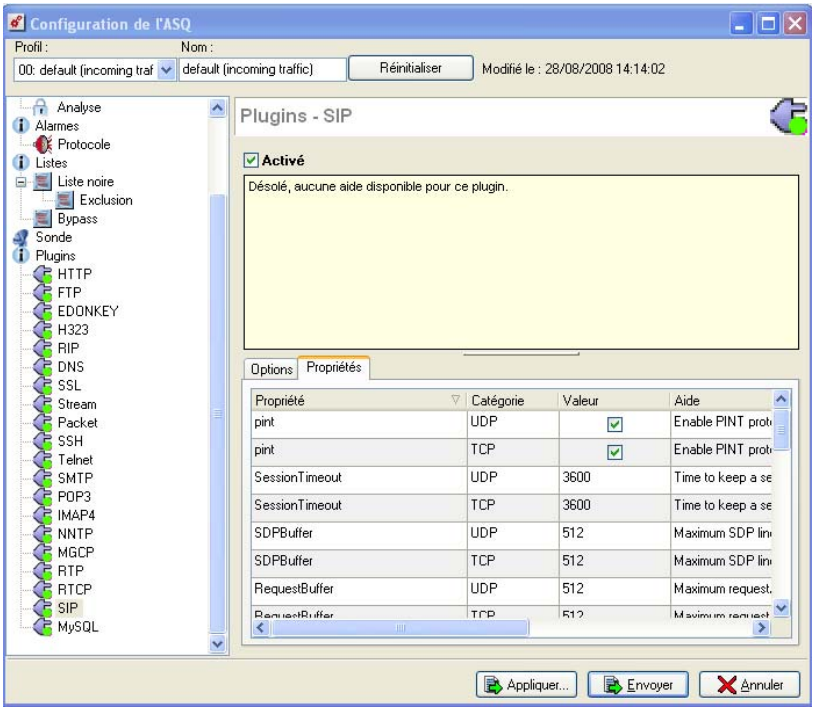


Figure 152 : Configuration de l'ASQ - SIP

Pour plus d'informations au sujet des alarmes liées au plugin SIP, veuillez vous référer à l'Annexe T : Liste des alarmes relatives aux protocoles.

6.9.20.1. Options

Les plugins SIP_UDP et SIP_TCP sont regroupés dans cet écran : ce qui permet de désactiver l'usage de ce protocole via UDP et/ou TCP.

Les options de l'onglet `Options` sont communes à ces deux plugins. C'est-à-dire que si vous cochez par exemple l'option « Activation automatique », les deux plugins seront activés.

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.
Traces	Activation ou désactivation de la remontée des logs concernant le plugin.

6.9.20.2. Propriétés

Les différents tampons SIP pouvant être gérés sont indiqués dans le tableau suivant :

Propriétés	Catégorie	Valeur	Aide
pint	UDP	Coche	Enable PINT protocol support

pint	TCP	Coche	Enable PINT protocol support
SessionTimeout	UDP	3600	Time to keep a session when there is no activity in its media.
Session Timeout	TCP	3600	Time to keep a session when there is no activity in its media.
SDPBuffer	UDP	512	Maximum SDP line size for buffer overflow protection.
SDPBuffer	TCP	512	Maximum SDP line size for buffer overflow protection.
RequestBuffer	UDP	512	Maximum request/response size for buffer overflow protection.
RequestBuffer	TCP	512	Maximum request/response size for buffer overflow protection.
RFC3903	UDP	Coche	Enable RFC3903 extensions : PUBLISH.
RFC3903	TCP	Coche	Enable RFC3903 extensions : PUBLISH.
RFC3515	UDP	Coche	Enable RFC3515 extensions : REFER.
RFC3515	TCP	Coche	Enable RFC3515 extensions : REFER.
RFC3428	UDP	Coche	Enable RFC3428 extensions : MESSAGE.
RFC3428	TCP	Coche	Enable RFC3428 extensions : MESSAGE.
RFC3311	UDP	Coche	Enable RFC3311 extensions : UPDATE.
RFC3311	TCP	Coche	Enable RFC3311 extensions : UPDATE.
RFC3265	UDP	Coche	Enable RFC3265 extensions : SUBSCRIBE, NOTIFY.
RFC3265	TCP	Coche	Enable RFC3265 extensions : SUBSCRIBE, NOTIFY.
RFC3262	UDP	Coche	Enable RFC3262 extensions : PRACK.
RFC3262	TCP	Coche	Enable RFC3262 extensions : PRACK.
RFC2976	UDP	Coche	Enable RFC2976 extensions : INFO.
RFC2976	TCP	Coche	Enable RFC2976 extensions : INFO.
Port par défaut	UDP	sip_udp	Un ou plusieurs ports que le plugin va relier.
Port par défaut	TCP	sip	Un ou plusieurs ports que le plugin va relier.
Opérations interdites	UDP		List of protocol command that must be refused.
Opérations interdites	TCP		List of protocol command that must be refused.
Opérations autorisées	UDP		Additionnal protocol command that need to be accepted.
Opérations autorisées	TCP		Additionnal protocol command that need to be accepted.
Messenger	UDP	Coche	Enable support for Windows Messenger.
Messenger	TCP	Coche	Enable support for Windows Messenger.
HeaderBuffer	UDP	512	Maximum header size for buffer overflow protection.
HeaderBuffer	TCP	512	Maximum header size for buffer overflow protection.

Les lignes sont doublées, du fait de nombreux paramètres similaires pour les deux plugins, ce qui donne la possibilité de configurer indifféremment l'un ou l'autre des plugins. Une colonne nommée « Catégorie » est en supplément (comparé aux autres plugins) pour faire la distinction entre le plugin SIP_TCP et SIP_UDP.

6.9.21. Le plugin MySQL

Le plugin MySQL a pour objectif de détecter les connexions à destination d'un serveur de base de données MySQL. La détection se fait sur le premier paquet qui contient la version du serveur. Le plugin n'effectue pas d'analyse du contenu du flux MySQL. Il est utilisé par SEISMO pour détecter la version du serveur MySQL utilisé afin de remonter d'éventuelles vulnérabilités.

6.9.21.1. Propriétés

Etat	Activation ou désactivation du plugin.
Activation automatique	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les plugins DNS, RIP, H323, RTP, RTCP.
Fermer la connexion lors de l'attachement avec le plugin	Lorsque le plugin s'active automatiquement sur un trafic, la connexion qui a déclenchée l'activation automatique du trafic est fermée. Les paquets sont alors bloqués. Par exemple, il est possible de bloquer tout trafic HTTP, indépendamment du port concerné. Les plugins DNS, RIP et H323, RTP et RTCP ne disposent pas de cette option.

6.9.21.2. Propriétés

Port par défaut	Un ou plusieurs ports que le plugin va relier.

6.9.22. Le plugin Pass_detach

Ce plugin permet de passer en mode IDS.
L'ASQ offre maintenant la possibilité de fonctionner en mode détection d'intrusion. Autrement dit, plutôt que de bloquer un flux suspect, il se contentera d'émettre une alarme.

Pour ce faire, il suffit de modifier la gestion liée aux alarmes protocolaires en indiquant une action « Pass ». Cette action, pouvant avoir un impact sur la sécurité du réseau, les alarmes sont représentées par l'icône  .

Pour une alarme dite « sensible », si vous modifiez son action et la configurez à «Passer», le flux suspect n'est pas bloqué et l'alarme se déclenche. Le moteur ASQ, quant à lui, détecte l'alarme sensible répondant aux critères associés à l'action « Passer » et détache le plugin impacté. Ce qui signifie, autrement dit, que l'analyse est désactivée sur le plugin impacté pour une connexion en cours seulement.

AVERTISSEMENT
Un plugin détaché signifie qu'il est désactivé. Cette désactivation comporte des risques pour les traitements suivants puisque le plugin n'est plus mis en œuvre pour une connexion donnée.

Exemple : Vous souhaitez laisser passer les paquets comportant une attaque de type « Invalid http protocol » au niveau du protocole HTTP. Dans ce cas, vous modifiez le comportement de cette alarme sensible en indiquant l'action « passer ».
Si l'ASQ repère un paquet contenant cette attaque, l'alarme se déclenche, le paquet passe et le plugin HTTP est détaché pour la connexion en cours.

Seulement, si un autre paquet au cours de la connexion, contient une attaque de type « Invalid %u encoding chair in URL » par exemple, le plugin étant détaché, votre réseau n'est plus protégé par cette attaque.

Pour connaître la liste des alarmes dont l'action « pass_detach » est possible, veuillez vous référer à l'Annexe S : Liste des alarmes sensibles.

6.9.23. Configuration par défaut

Il est possible de récupérer la configuration par défaut des plugins en cliquant sur le bouton **Configuration par défaut**. Toutes les valeurs personnalisées sont dans ce cas écrasées.

PARTIE 7 : POLITIQUE

CHAPITRE 1 : TRANSLATION D'ADRESSES (NAT)

7.1.1. Introduction

7.1.1.1 Pour ce chapitre, vous devez avoir franchi les étapes

- Partie 2 : Installation, pré-configuration, intégration.
- Partie 5 : Configuration réseau.
- Partie 4 : Objets

7.1.1.2. Pour ce chapitre, vous devez connaître

- Les machines dont vous souhaitez translater l'adresse IP.

7.1.1.3. Utilité de ce chapitre

Ce chapitre vous permet de définir les objets dont vous voulez translater l'adresse.

7.1.1.4. Accéder à ce chapitre

➲ Accédez à la boîte de dialogue par le menu **Politique\NAT** de l'arborescence de l'interface graphique.

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications.
Avant d'effectuer toute modification importante sur votre firewall NETASQ, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez vous retrouver dans l'état précédent.
Pour plus d'informations sur les sauvegardes, veuillez vous référer au chapitre Maintenance.

7.1.1.5. Introduction à ce chapitre

Les tables de translation d'adresses sont stockées sur le firewall dans des slots (fichiers de configuration numérotés de 01 à 10).

Chaque slot peut être programmé à une heure précise de la semaine, en écrasant la configuration du slot précédemment activé.

7.1.2. Présentation

DEFINITION : TRANSLATION D'ADRESSES (NAT)
Changement d'une adresse vers une autre. Par exemple, un assembleur traduirait des adresses symboliques en adresses de machine. Un système à mémoire virtuelle traduirait une adresse virtuelle en adresse réelle (la résolution d'adresses). Les règles qui composent une politique de translation d'adresses permettent de modifier certains éléments du trafic. Il est donc possible de créer du map, du bimap, de la redirection de ports…

Lorsque vous sélectionnez le menu **`Politique\NAT`** une boîte de dialogue s'affiche, elle vous permet de manipuler les slots associés à la translation d'adresses.

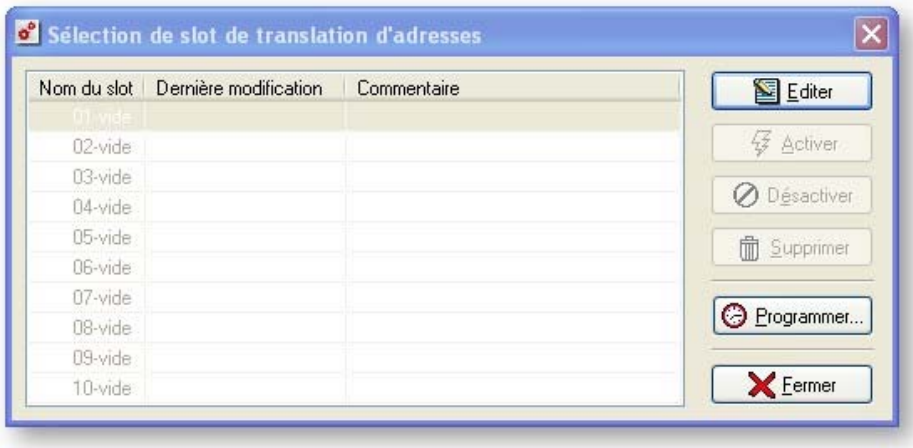


Figure 153 : Sélection d'une politique de NAT

Elle est découpée en deux zones :

Gauche	Liste des slots.
Droite	Actions sur le slot sélectionné.

7.1.2.1. Liste des politiques

Dans cette partie de la boite de dialogue se trouve la liste des slots. Il en existe 10, numérotés de 01 à 10.

Chaque politique possède un nom, une date/heure de mise en activité et la date de dernière modification effectuée sur cette politique. La programmation de l'activation de ces slots se fait grâce au programmateur horaire (*Cf.* *Partie 7/Chapitre 3 : Programmation horaire*).

La politique en cours d'activité est indiquée par une petite flèche verte à gauche de son nom. Une politique est dite "en activité" lorsque les paramètres qu'elle contient sont en service. Il ne peut y avoir plus d'une politique en activité car les paramètres de la dernière politique activée écrasent ceux de la politique activée précédemment.

Si vous modifiez une politique, vous devez le réactiver pour prendre en compte les modifications. Une politique modifiée mais non réactivée est notifiée par l'icône à la place de la flèche verte habituelle.

Il est possible qu'il n'y ait aucune politique en activité, cela implique qu'aucune translation d'adresses n'est active.

Chaque politique ne doit pas obligatoirement contenir des paramètres.

Une politique pour laquelle il n'existe pas de fichier de configuration sur le firewall NETASQ est affichée sous le nom "vide" dans la liste.
Une politique est dite sélectionnée quand vous faites un simple clic de la souris sur son nom. La sélection faite, vous pouvez l'éditer ou l'activer.

7.1.2.2. Actions sur la politique sélectionnée

Quand une politique est sélectionnée, vous pouvez réaliser différentes actions :

Editer	Modifier les règles de translation d'adresses associées à ce slot.
Activer	Activer immédiatement un slot : les paramètres enregistrés dans ce slot écrasent les paramètres en vigueur. Lorsqu'on sélectionne un slot déjà activé ce bouton ce transforme en un bouton **Désactiver** pour réaliser l'action de désactivation.
Désactiver	Désactive le slot actuellement activé. Aucune translation d'adresse n'est alors effectuée.
Supprimer	Efface le slot et toutes ses informations.
Programmer…	Donner l'heure et le ou les jours auxquels le fichier va s'activer automatiquement.
Fermer	Retour à l'écran principal.

7.1.3. Edition d'une politique de translation

Référez-vous à la procédure suivante pour éditer une politique de translation :

1. Sélectionnez une politique dans la liste des politiques de translation.
2. Cliquez sur le bouton **Editer** de la boite de dialogue contenant la liste des politiques de translation.

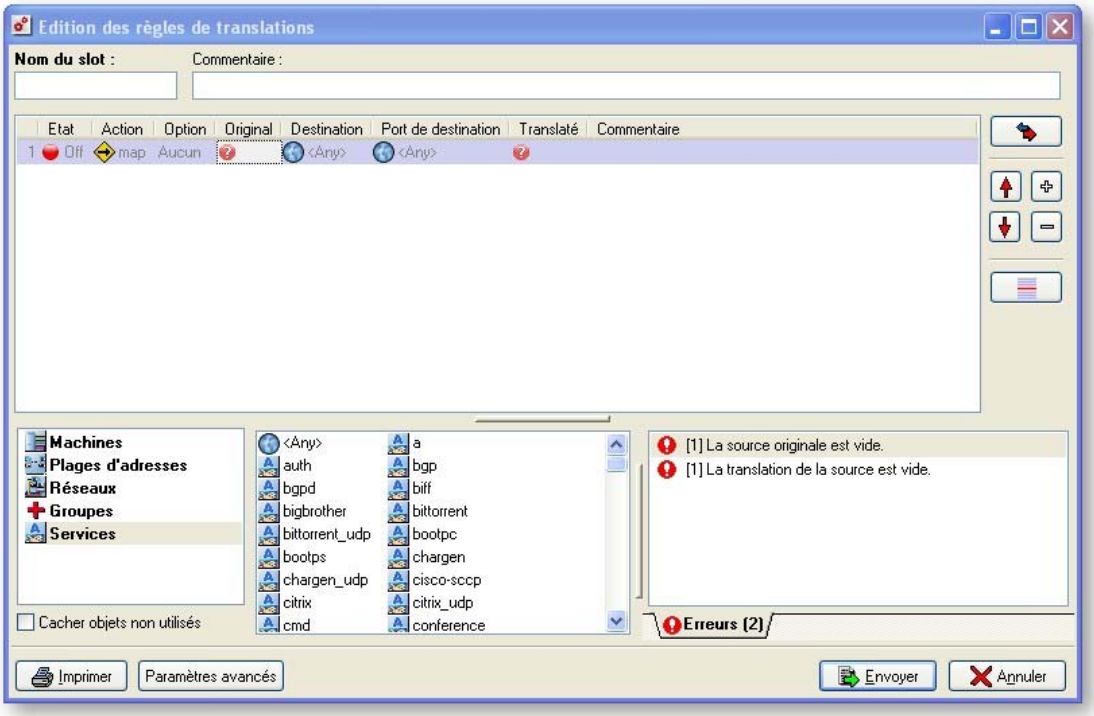


Figure 154 : Edition des règles de translation

La fenêtre d'édition d'une politique de translation apparaît. Elle est composée de plusieurs parties :

- Une zone comportant les règles de translation sous la forme d'un tableau.
- Un menu "Drag'n Drop".
- Un analyseur de cohérence et de conformité des règles.
- Une zone d'actions possibles.

7.1.3.1. Règles de translation

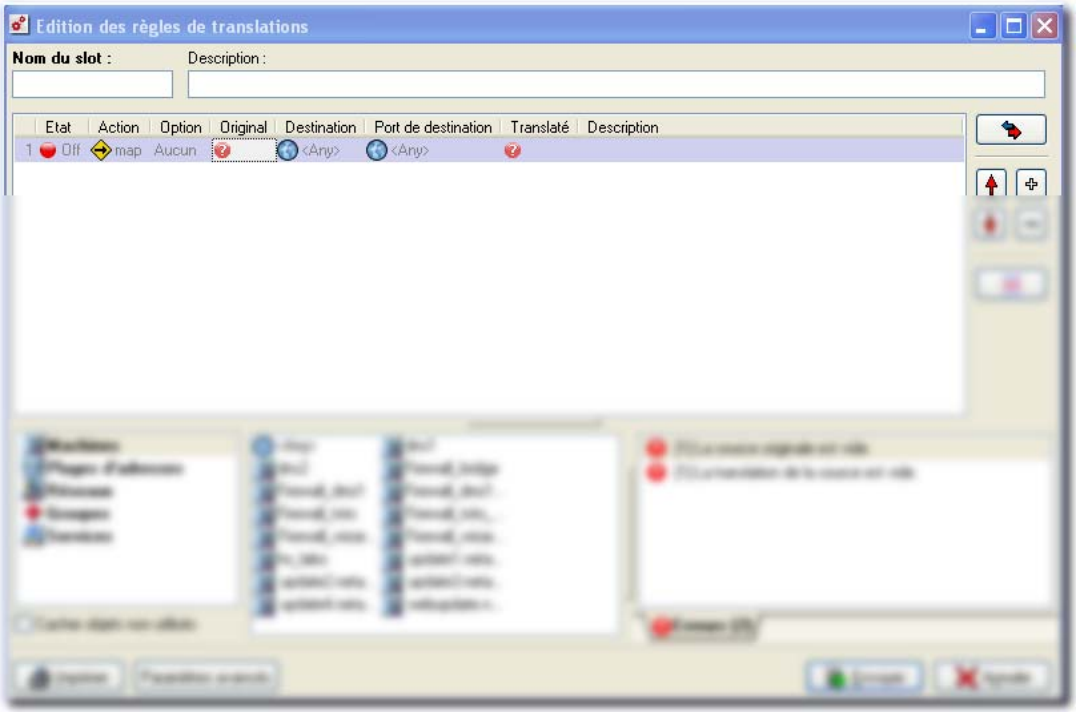


Figure 155 : Edition des règles de translation

ID	Numéro de la règle. Ce champ n'est pas éditable. Il indique l'emplacement de la règle dans la politique. L'ordre des règles est important.
Etat	(On)La règle est utilisée par le firewall NETASQ. (Off) La règle est désactivée. Il suffit de double-cliquer dans ce champ pour activer ou désactiver la règle. La ligne est grisée lorsque la règle est à l'état Off pour afficher clairement son inactivité.
Action	Définit le type de translation que vous désirez effectuer. La translation peut être Map, Map bidirectionnel, Redirection, Split, No map et s'effectuer entre toutes les interfaces du firewall. L'action choisie détermine le rôle des autres colonnes de la grille.
Option	Lors de l'utilisation des règles de translation d'adresses, seules les adresses IP contenues dans l'entête IP des paquets sont modifiées. Pourtant, certains protocoles référencent les adresses IP dans la couche de données. Les options de cette fenêtre permettent de modifier les adresses contenues dans les protocoles FTP, Real/Audio, H323 et NetBIOS pour que les paquets soient translatés correctement. Les options permettent d'ajouter 4 types de services particuliers :

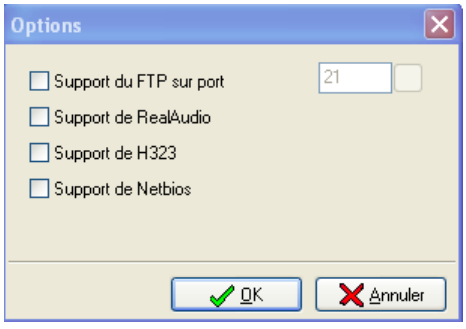


Figure 156 : Options

	● **Support du FTP sur port** : permet le support du FTP en mode actif (lorsque le serveur initie la connexion n des données. ● **Support de Real Audio (anciennes versions)** : qui font figurer les adresses sources dans les champs de données des paquets TCP/IP, ● **Support de H323** : permet de gérer partiellement le protocole H323 (traitement voix/vidéo sur IP). Dans ce cas, l'adresse source est remplacée. Notez que le NAT sur ce protocole n'est pas supporté lorsque les gatekeeper sont exploités. (Cf. Glossaire). ● **Support de NetBIOS** : permet de supporter les relations d'approbation entre serveurs Windows. Ces services nécessitent donc un traitement particulier lors de la translation d'adresses.
Original	Adresse IP non translatée. Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Destination	Destination du trafic qui nécessite une translation. Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Port de destination	Port de destination du trafic qui nécessite une translation. Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Translaté	Adresse IP translatée (modifiée par le firewall). Un double clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Description	Commentaire que vous pouvez associer à cette règle de translation.

Exemple

On peut indiquer que tout le trafic de l'"Original", à destination du port "Port de destination" de la machine "Destination", est redirigé vers la machine "Translaté".

AVERTISSEMENT

Lorsqu'une icône ressemblant à un point d'interrogation dans un cercle rouge apparaît dans un champ cela signifie que ce champ est obligatoire pour la règle de translation .

N'activez les options que si vous êtes sûrs de vouloir utiliser ces services. Ils ralentissent le traitement des paquets et peuvent être source de conflits.

7.1.3.2. Mode étendu

L'affichage détaillé permet d'accéder aux colonnes interfaces et port translaté. Pour obtenir l'affichage détaillé, cliquez sur le bouton  .

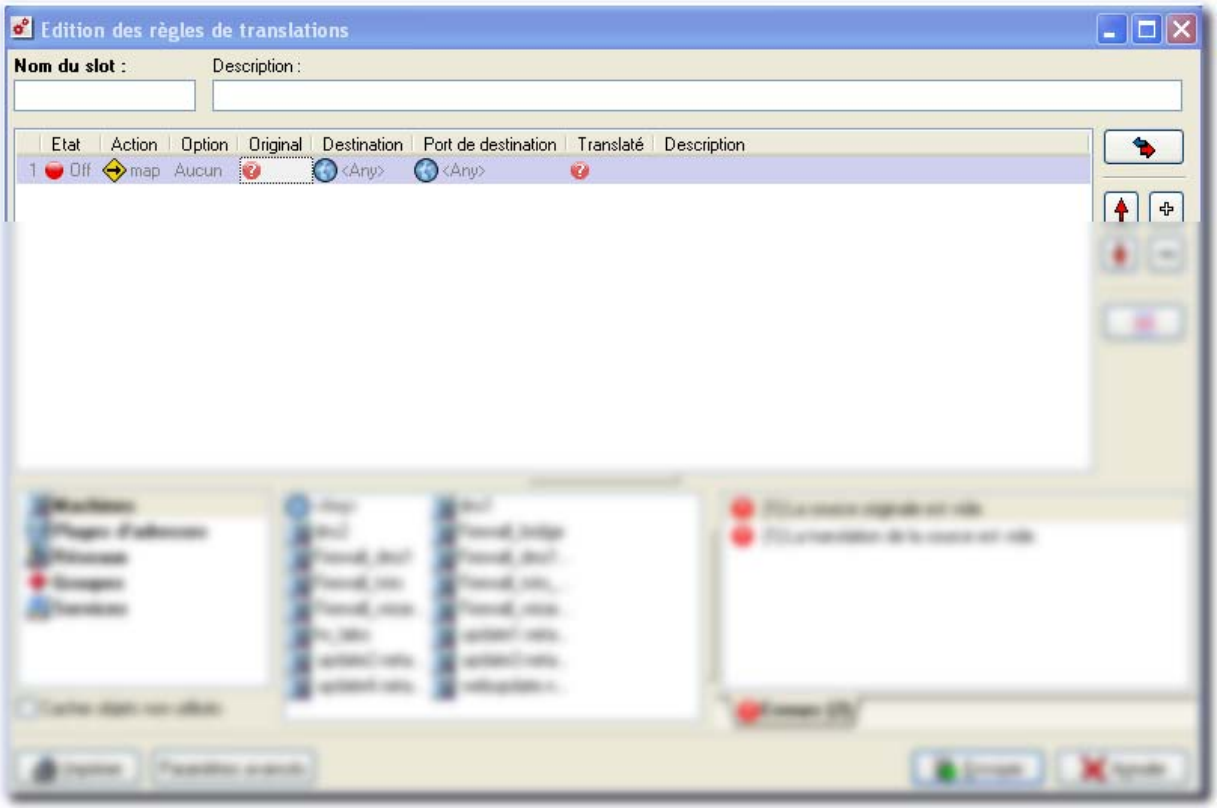


Figure 157 : Edition des règles de translation

Interface	Interface sur laquelle s'applique la règle de translation présentée sous forme de liste déroulante. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP source et destination. Il est possible de la modifier pour appliquer la règle sur une autre interface.
Port translaté	Port vers lequel est faite la translation. Surtout utilisé pour préciser une plage de ports vers laquelle s'effectue la translation d'adresses unidirectionnelle ou pour réaliser de la translation de port (pour rediriger une connexion demandée sur le port XX vers le port YY). Un double-clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.

7.1.3.3. Action

Cette zone de la boîte de dialogue contient une grille vous permettant de définir les translations d'adresses à appliquer. Les différentes possibilités sont :

Translation unidirectionnelle (map)

La translation d'adresses unidirectionnelle vous permet de convertir des adresses IP réelles de vos réseaux (interne, externe ou DMZ) en une adresse IP virtuelle sur un autre réseau (interne, externe ou DMZ) lors du passage par le firewall. L'adresse source est changée en adresse destination uniquement si la connexion provient de la machine source (unidirectionnelle).

La translation unidirectionnelle est généralement utilisée pour masquer les adresses IP en sortie du firewall.

Il faut préciser la plage de ports translatés en affichage détaillé pour éviter les conflits de ports.

Les plages d'adresse sont supportées par l'action **map**. Une fois que les ports de la première adresse sont tous utilisés, les ports de la seconde adresse sont utilisés…

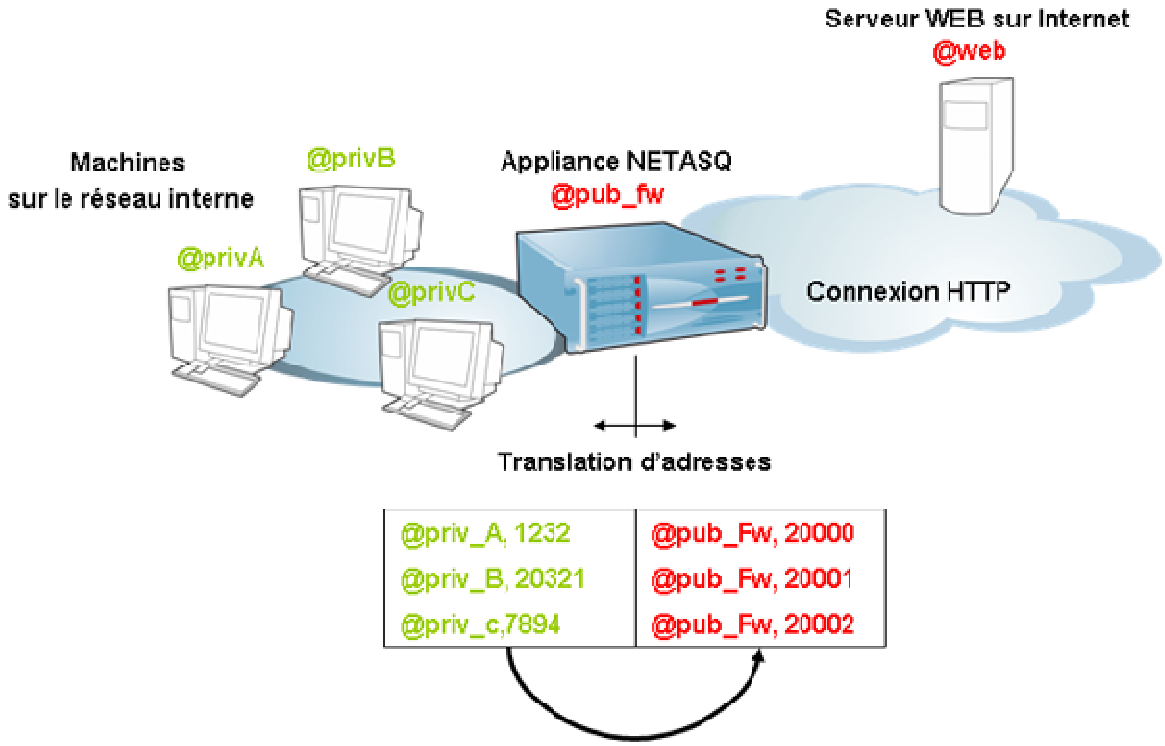


Figure 158 : Translation unidirectionnelle

Définition de la règle

Indiquez en origine l'adresse IP réelle (privée) de la machine ou du réseau, et en adresse translatée l'adresse IP virtuelle que vous désirez affecter.

No map

Il est possible de retirer une machine, comprise dans un réseau translaté, de l'opération de translation de type map.
L'adresse de cette machine ne sera alors pas translatée au travers du firewall.

Définition de la règle

L'origine est la machine qui ne doit pas être translatée. Choisissez l'option **no map** et n'indiquez rien dans la colonne **Translaté**.

Cette règle doit forcément être suivie d'une règle de type map.

> **AVERTISSEMENT**
> Pour une règle "no map", vous devez spécifier l'interface du firewall sur laquelle l'opération de no map sera effectuée (cette interface est la même que pour l'opération map associée).

Vous pouvez consulter les exemples de configurations de translation d'adresses en *Annexe E : Exemples de translations d'adresses* pour une meilleure compréhension de ces choix.

Translation bidirectionnelle (map bidirectionnel)

La translation d'adresses bidirectionnelle vous permet de convertir une adresse IP (ou N adresses IP) en une autre (ou en N adresses IP) lors du passage par le firewall, quelle que soit la provenance de la connexion.

> **AVERTISSEMENT**
> Pour une règle de bi-map de N vers N, les plages d'adresses, réseaux ou groupes de machines original et translaté doivent être de même taille.

La translation bidirectionnelle est généralement utilisée pour donner accès à un serveur depuis l'extérieur avec une adresse IP publique qui n'est pas l'adresse réelle de la machine.

Les plages d'adresses sont supportées par l'action map-bidirectionnel. Les adresses sources et translatées sont utilisées dans l'ordre : la plus "petite" adresse du champ source est translatée vers la plus "petite" adresse du champ translaté.

Définition de la règle

L'adresse IP origine correspond à l'adresse physique de la machine et l'adresse IP translatée à l'adresse IP virtuelle utilisée.

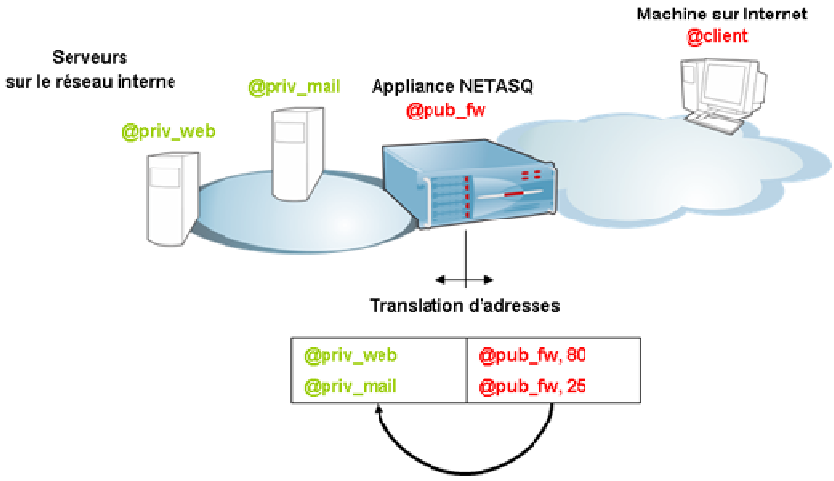


Figure 159 : Translation bidirectionnelle

Redirection de port (redirection)

La redirection de port permet de rediriger les paquets en provenance d'une ou plusieurs sources à destination d'une ou plusieurs adresses IP avec un port identique vers une autre adresse IP/N° de port.

Ceci permet de rediriger le flux vers la machine concernée, à partir d'une seule adresse IP publique, en fonction du numéro de port.

Les numéros de port sont accessibles en affichage détaillé.

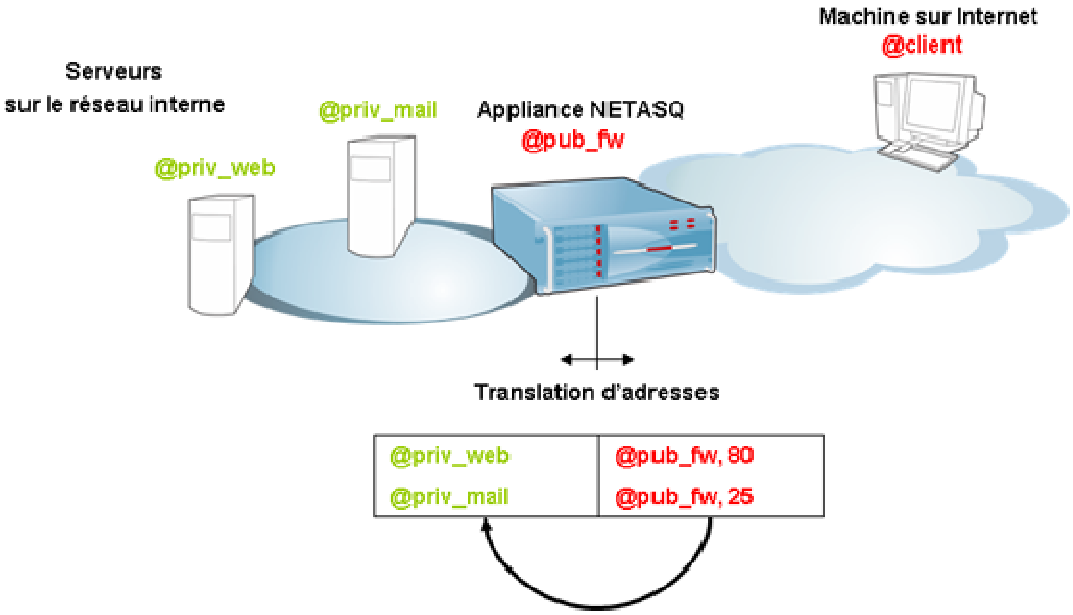


Figure 160 : Redirection de port

Définition de la règle

L'adresse IP publique utilisée correspond à l'adresse origine et l'adresse de redirection à l'adresse translatée.

Partage de charge (split)

Le partage de charge redirige les flux à destination d'une adresse IP vers plusieurs machines (groupe de machines). Il est possible de préciser les ports des adresses à rediriger en affichage détaillé.
Dans cette version, le partage est fait séquentiellement, sans vérifier l'accessibilité des machines.

Définition de la règle

Le pool d'adresses IP utilisé (groupe de machines) correspond à la partie translatée, l'origine étant l'adresse IP à contacter.

Vous pouvez consulter les exemples de configurations de translation d'adresses en *Annexe E : Exemples de translations d'adresses* pour une meilleure compréhension de ces choix.

7.1.3.4. Actions possibles

Nom du slot	Nom donné au fichier de configuration.
Description	Commentaire indicatif associé au slot de translation.
Mode étendu 	Affichage des paramètres de configuration avancés de la translation d'adresses.
Insérer une règle 	Insérer une ligne vierge après la ligne sélectionnée.
Supprimer une règle sélectionnée 	Supprimer la ligne sélectionnée.
Remonter une règle 	Placer la ligne sélectionnée avant la ligne directement au dessus
Descendre une règle 	Placer la ligne sélectionnée après la ligne directement en dessous.
Insérer un séparateur  .	Cette option permet d'insérer un séparateur au dessus de la ligne sélectionnée afin d'indiquer un commentaire sur une ligne de l'édition de la translation d'adresses. Pour définir un séparateur, il s'agit d'indiquer un commentaire et une couleur pour ce séparateur.
Imprimer	Ouvrir la boîte de dialogue d'Impression permettant d'imprimer vos règles de translation.
Paramètres avancés	En cliquant sur ce bouton, vous avez la possibilité de conserver actives les connexions TCP lors de l'activation du slot.
Envoyer	Envoyer le fichier de configuration au firewall NETASQ, et le programmer à l'heure d'activation spécifiée.
Annuler	Annuler les modifications depuis le dernier envoi au firewall NETASQ et revenir à la liste des slots.

Une ligne est dite sélectionnée quand un de ses éléments est sélectionné (en inverse-vidéo).

En plus de ces actions, vous pouvez utiliser pour chaque cellule du tableau les fonctionnalités de copier coller standard :

- Soit avec la souris (clic bouton droit).
- Soit avec les touches **CTRL-C** pour copier, **CTRL-V** pour coller.
- Soit avec les touches **CTRL-Insert** pour copier, **Shift-Insert** pour coller.

7.1.3.5. Menu contextuel

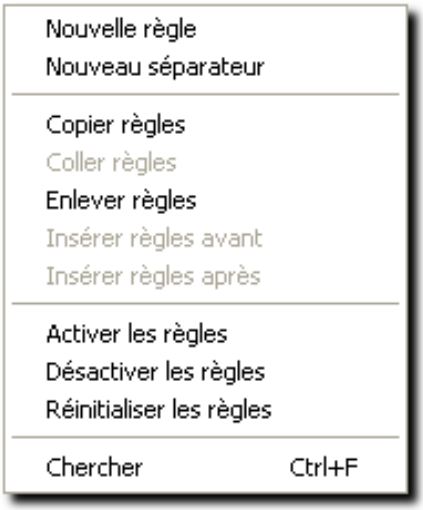


Figure 161 : Menu contextuel

Le menu contextuel est activable par un clic droit sur une ligne sélectionnée dans la grille. Les différentes actions proposées sont des raccourcis aux boutons équivalents situés dans la barre d'outils.

7.1.3.6. Menu Drag & Drop

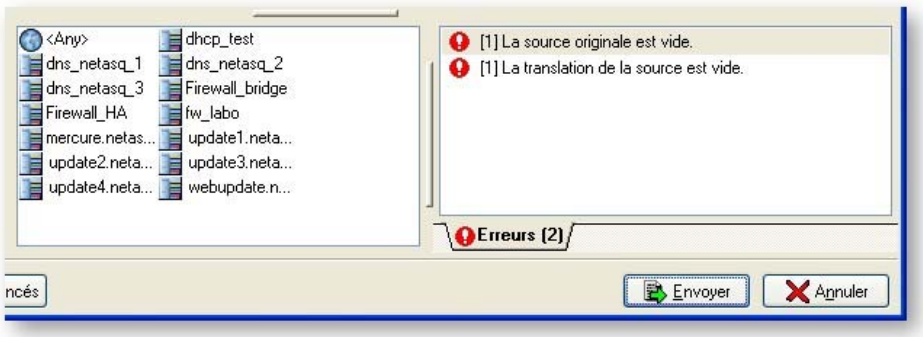


Figure 162 : Drag & Drop

Comme son l'indique le menu **Drag & Drop** permet en un Drag & Drop de positionner dans les règles de translation, les objets configurés dans le chapitre précédent. L'opération de Drag & Drop consiste à :

1. Sélectionner un objet.
2. Maintenir le bouton de souris enfoncé.
3. Réaliser un glissement de l'objet vers la grille de règles.
4. Enfin, y déposer l'objet.

Lorsque l'administrateur réalise une opération de Drag & Drop, les champs disponibles pour l'objet sélectionné apparaissent en surbrillance.

Le menu de sélection des types d'objet situé à gauche du menu **Drag & Drop** permet de sélectionner le type d'objet affiché dans la grille.

NOTE
Seuls les champs Original, Destination, Port de destination et Translaté sont autorisés dans les opérations de drag'n'drop puisqu'ils nécessitent la base d'objets.

Affichage de la grille

L'affichage des données contenues dans la grille peut être défini suivant les préférences de l'administrateur parmi les options d'affichage : grandes icônes, petites icônes, détaillé ou en liste.

Options d'affichage

Deux options d'affichage des données de la grille du menu **Drag & Drop** sont disponibles.

Cacher objets non utilisés

Comme son nom l'indique, cette option permet de cacher dans la grille les objets non utilisés dans les règles de translation.

Exemple
Firewall_pptpXX, Firewall_dialupXX, Firewall_ipsec…

Ces objets rendent la lecture générale difficile et sont cachés par défaut.

7.1.3.7. Analyseur de cohérence et de conformité des règles

La politique de translation d'un firewall est un des éléments les plus importants pour la sécurité des ressources que le firewall protège. Bien que cette politique évolue sans cesse, s'adapte aux nouveaux services, aux nouvelles menaces, aux nouvelles demandes des utilisateurs, elle doit conserver une cohérence parfaite afin que des failles n'apparaissent pas dans la protection que propose le firewall.
L'enjeu est d'éviter la création de règles qui en inhiberait une autre. Lorsque la politique de translation est conséquente, le travail de l'administrateur est d'autant plus fastidieux que ce risque s'accroît. De plus lors de la configuration avancée de certaines règles de translation très spécifiques, la multiplication des options pourrait entraîner la création d'une règle erronée, ne correspondant plus aux besoins de l'administrateur.
Pour éviter ces erreurs, l'écran d'édition des règles de translation des firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.

Divisé en deux onglets, cet analyseur regroupe les erreurs de création de règles dans l'onglet **`Erreurs`** et les erreurs de cohérence dans les règles dans l'onglet **`Avertissements`**.

CHAPITRE 2 : FILTRAGE

7.2.1. Introduction

7.2.1.1 Pour ce chapitre, vous devez avoir franchi les étapes

- Partie 2 : Installation, pré-configuration, intégration.
- Partie 5 : Configuration réseau.
- Partie 4 : Objets.
- Partie 7 : Translation d'adresses.

7.2.1.2. Pour ce chapitre, vous devez connaître

La politique de sécurité que vous voulez instaurer.

7.2.1.3. Utilité du chapitre

Ce chapitre vous permet de définir les règles de filtrage. C'est le "cœur" de votre politique de sécurité.
Vous définissez ici qui utilise quoi, quand et comment.
Vous pouvez aussi bien limiter l'accès de l'intérieur vers l'extérieur et/ou la DMZ que de l'extérieur vers l'intérieur et/ou la DMZ...
Vous pouvez aussi définir les règles d'authentification pour vos utilisateurs : services ou machines nécessitant une authentification.

7.2.1.4. Introduction à ce chapitre

La technologie ASQ inclut un moteur de filtrage dynamique des paquets (stateful inspection) avec optimisation des règles permettant l'application de la politique de filtrage de manière sûre et rapide. La mise en œuvre des fonctions de filtrage est basée sur la confrontation des attributs de chaque paquet IP reçu aux critères de chaque règle du slot de filtrage actif. Le filtrage porte sur tous les paquets sans exception. Les critères des règles de filtrage sont :

- L'interface de réception des paquets IP couverts par la règle.
- La ou les machines à l'origine des flux d'informations couverts par la règle.
- Le ou les protocoles IP, les services TCP/UDP ou les types de messages ICMP des flux d'information couverts par la règle, le DSCP afin de définir une différenciation des flux.
- La ou les machines destinataires des flux d'informations couverts par la règle.
- L'utilisateur ou le groupe d'utilisateurs autorisés par la règle.

Les attributs des paquets IP qui sont confrontés aux quatre premiers critères cités sont évidemment extraits des en-têtes Ethernet, IP, ICMP, UDP ou TCP des trames. En ce qui concerne l'utilisateur ou le groupe d'utilisateurs autorisés par la règle, à partir du moment où un utilisateur s'est identifié et authentifié avec succès à partir d'une machine donnée, le firewall note ce fait et attribue le nom de l'identifiant de cet utilisateur à tous les paquets IP présentant l'adresse de cette machine comme adresse IP source. En conséquence, les règles qui spécifient l'authentification des utilisateurs, même sans préciser de contraintes sur les utilisateurs autorisés, ne peuvent s'appliquer qu'à des paquets IP émis d'une machine à partir de

laquelle un utilisateur s'est préalablement authentifié. Chaque règle de filtrage peut spécifier une action de contrôle et une action de journalisation. Il y a quatre valeurs possibles pour l'action de contrôle :

- **Aucune** : le paquet est confronté aux règles suivantes (sert à spécifier une action de journalisation uniquement).
- **Passer** : le paquet est accepté et n'est pas confronté aux règles suivantes.
- **Bloquer** : le paquet est détruit silencieusement.
- **Réinitialiser** : le paquet est détruit et un signal TCP RST (cas TCP) ou ICMP unreachable (cas UDP) est envoyé à l'émetteur.
- : **Déléguer** : le paquet est confronté aux règles de filtrage de la politique locale. Cette action, disponible en politique globale du mode « Global Administration », sert à sortir de l'évaluation de la politique de filtrage globale pour permettre de déléguer un sous-ensemble de celle-ci à un administrateur local via la politique de filtrage locale.

Si aucune règle de filtrage n'est applicable au paquet, ou si les seules qui le sont ne spécifient "Aucune" action de contrôle, le paquet est détruit silencieusement.

Il convient de noter qu'à proprement parler, pour un ensemble de paquets IP liés à un même échange au niveau transport (connexion TCP, pseudo-connexion UDP ou ICMP), le firewall ne confronte que le paquet initial de l'échange aux règles du slot de filtrage courant. À la réception de tout paquet IP, préalablement à l'application des règles du slot de filtrage courant, le paquet est comparé aux connexions/pseudo-connexions actuellement établies. Si les attributs et les paramètres du paquet correspondent aux critères et à l'état d'une de ces connexions/pseudo-connexions, il est autorisé à passer sans être soumis aux règles de filtrage. Ce mécanisme permet notamment de gérer les échanges bidirectionnels (notamment les connexions TCP) sans avoir à définir une règle de filtrage dans les deux sens de traversée du firewall.

Des règles de filtrage implicites sont générées par le firewall en liaison avec la configuration d'autres fonctions de sécurité. Ce sont les règles correspondant à l'administration à distance du firewall, l'authentification des utilisateurs et l'établissement des VPN. Par ailleurs, des règles de filtrage dynamiques sont également générées pour les protocoles nécessitant des connexions filles.

À tout instant du fonctionnement d'un firewall, il y a une politique de filtrage actif.

Les tables de filtrage sont stockées sur le firewall NETASQ dans des politiques (fichiers de configuration numérotés de 01 à 10). Chaque politique peut être programmée à une heure précise de la semaine, en écrasant la configuration du slot précédemment activé.

Le principe est simple : quand un paquet arrive au firewall NETASQ (les règles de filtrage ne s'appliquant qu'en entrée d'interface, le firewall se fait confiance à lui-même pour les trafics qu'il génère comme par exemple RADIUS, LDAP, KERBEROS, etc.) , celui-ci fait descendre le paquet dans la liste de règles de filtrage. Si le paquet correspond aux critères de sélection d'une règle, il applique l'action associée à cette règle sinon le paquet est automatiquement supprimé. Une fois qu'une règle peut être appliquée au paquet, ce dernier n'est plus comparé aux règles suivantes. A moins qu'il n'y ait pas d'action sur le filtrage.

La façon dont vos règles de filtrage sont ordonnées est primordiale. La cohérence de cet ordre est la principale difficulté dans la configuration de votre firewall. (Cf. Annexe F : Exemples de règles de filtrage).

7.2.1.5. Accéder à ce chapitre

Accédez au filtrage par le menu **`Politique\Filtrage`** de l'arborescence.

7.2.2. Présentation

DEFINITION FILTRAGE

Opération qui consiste à utiliser un filtre. Il s'agit plus exactement d'un ensemble de règles qui acceptent ou bloquent certains trafics réseaux suivant des critères définis. (*Cf. Partie 10/Chapitre 4 : Règles de filtrage.*)

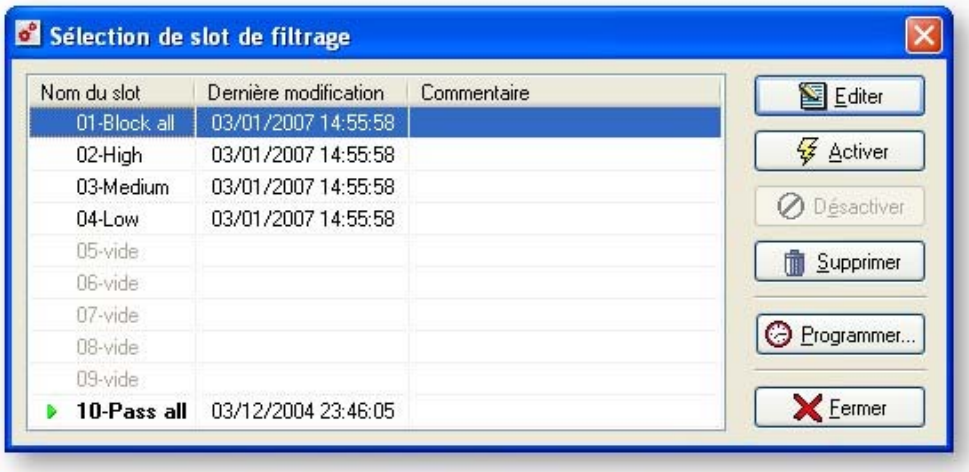


Figure 163 : Sélection d'une politique de filtrage

Lorsque vous sélectionnez le menu **Politique\Filtrage** une boîte de dialogue s'affiche, elle vous permet de manipuler les slots associés au filtrage de paquets.

Elle est découpée en deux zones :

Gauche	Liste des politiques.
Droite	Actions sur la politique sélectionnée.

7.2.2.1. Liste des slots

Dans cette partie de la boite de dialogue se trouve la liste des politiques (ou slots). Il en existe 10, numérotés de 01 à 10.
Chaque slot possède un nom, une date/heure de mise en activité et la date de dernière modification effectuée sur ce slot ainsi qu'une description. La programmation de l'activation de ces slots se fait grâce au programmateur horaire (Cf. Partie 7/Chapitre 3 : Programmation horaire).
Le slot en cours d'activité est indiqué par une petite flèche verte à gauche de son nom. Un slot est dit " en activité " lorsque les paramètres qu'il contient sont en service. Il ne peut y avoir plus d'un slot en activité car les paramètres du dernier slot activé écrasent ceux du slot activé précédemment.
Si vous modifiez un slot, vous devez le réactiver pour prendre en compte les modifications. Un slot modifié mais non réactivé est notifié par l'icône à la place de la flèche verte habituelle.
Il y a toujours forcément un slot de filtrage actif.

Par défaut, un fichier de configuration contient une seule règle bloquant tous les paquets. Chaque slot ne doit pas obligatoirement contenir des paramètres.
Un slot pour lequel il n'existe pas de fichier de configuration sur le firewall NETASQ est affiché sous le nom "vide" dans la liste.
Un slot est dit sélectionné quand vous faites un simple clic de la souris sur son nom. La sélection faite, vous pouvez l'éditer ou l'activer.

7.2.2.2. Actions sur la politique sélectionnée

Quand une politique est sélectionnée, vous pouvez réaliser différentes actions :

Editer	Modifie les règles de filtrage associées à ce slot.
Activer	Active immédiatement un slot : les paramètres enregistrés dans ce slot écrasent les paramètres en vigueur.
Activer	Permet de désactiver une politique au niveau du NAT ou du filtrage d'URL. Ce bouton est ici grisé car il n'est pas utilisé au niveau du filtrage qui a toujours une politique activée.
Supprimer	Efface le slot et toutes ses informations. Le slot courant est remplacé par un slot vide.
Programmer…	Donne l'heure et le ou les jours auxquels le fichier va s'activer automatiquement.
Fermer	Retourne à l'écran principal.

Un clic droit sur une politique fait apparaître un menu contextuel. Il est possible d'exporter dans un fichier .Txt le contenu d'un slot ou d'effectuer une importation.

La méthode du copier/coller permet de copier un slot et de le coller dans un autre slot. Dans ce cas, l'écran de configuration est appelé et pré-rempli. (Ce copier/coller n'utilise pas le presse-papier).

AVERTISSEMENT

- Il existe un slot préconfiguré, appelé "Pass all"**.** Ce slot laisse passer l'ensemble du trafic IP en provenance et à destination de tout le monde. Il est utile pour des phases de tests. Son utilisation dans un autre cadre pourrait se révéler dangereux pour la sécurité de vos ressources sensibles.
- Une règle implicite permet, au cas où la politique « Block all » est activée de se connecter au produit.

7.2.3. Remarques générales sur le filtrage

Lorsque vous utilisez la translation d'adresses, ne créez pas de règles de filtrage pour les adresses IP virtuelles, utilisez toujours le nom d'objet réel.

7.2.4. Edition d'une politique de filtrage

Référez-vous à la procédure suivante pour éditer une politique de filtrage :

1. Sélectionnez une politique dans la liste des politiques de filtrage.
2. Cliquez sur le bouton **Editer** de la boite de dialogue contenant la liste des slots de filtrage.

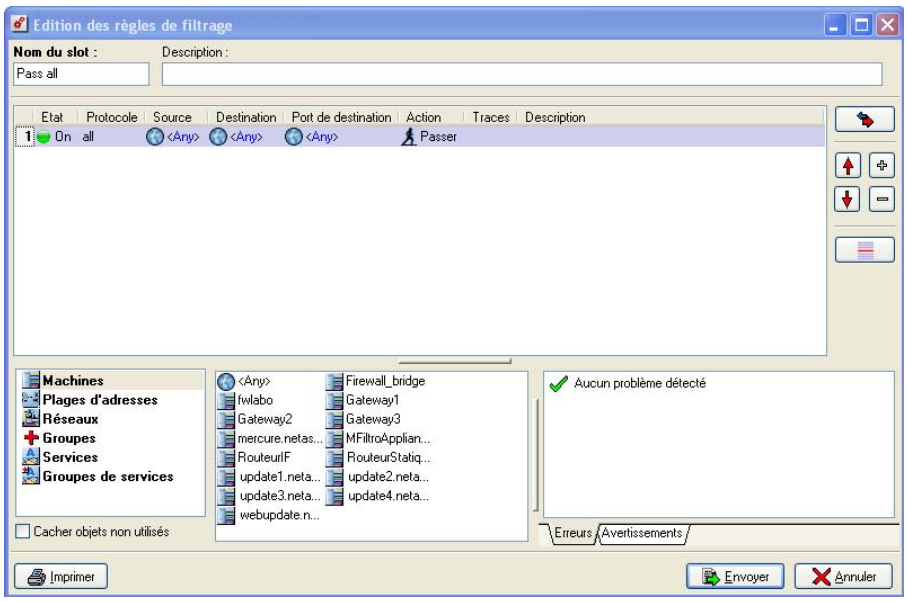


Figure 164 : Edition des règles de translation

La fenêtre d'édition d'une **politique** de filtrage apparaît.

- Une zone comportant les règles de filtrage sous la forme d'un tableau.
- Un menu **Drag'n Drop**.
- Un panneau comportant les objets.
- Un analyseur de cohérence et conformité des règles.
- Une zone d'actions possibles.

Une fonctionnalité permet de localiser des éléments textuels en fonction de ce que l'administrateur saisit au clavier. Aussi, lorsqu'il entre du texte, un panneau s'affiche sous la grille contenant le texte recherché. Les éléments de la grille contenant ce texte sont indiqués en surbrillance.

7.2.4.1. Règles de filtrage

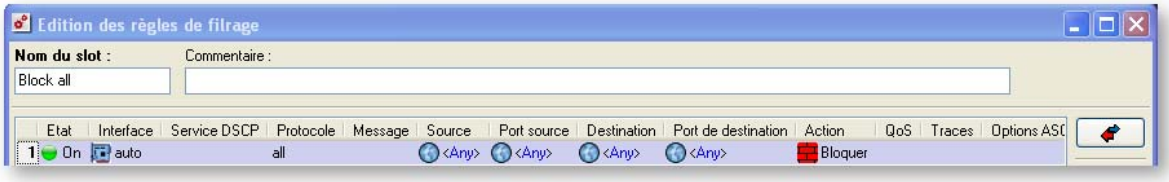


Figure 165 : Edition des règles de filtrage en mode étendu

Cette grille vous permet de définir les règles de filtrage à appliquer. Faites attention à bien ordonner vos règles de filtrage afin d'avoir un résultat cohérent. Le firewall exécute les règles dans l'ordre d'apparition à l'écran et s'arrête dès qu'une action s'applique au flux qui tente de le traverser. Il convient donc de définir les règles dans l'ordre du **plus détaillé au plus général.**

En mode simple, les informations suivantes s'affichent :

ID	Ce champ indique le numéro de la règle de filtrage dans la politique. Il existe autant de numéros qu'il y a de règles dans une politique.
Etat	Activation/désactivation d'une règle au sein d'une politique correspondant à ON ou OFF. Lorsque la règle est à l'état OFF, la ligne est grisée pour mettre en évidence l'inactivité de cette règle.

Protocole	Protocole sur lequel s'applique la règle de filtrage
Source	Objet source utilisé comme critère de sélection pour cette règle. Un double-clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Destination	Objet destination utilisé comme critère de sélection pour cette règle. Un double-clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Port de destination	Service ou groupe de service utilisé comme critère de sélection pour cette règle. Un double-clic sur cette zone permet de choisir l'objet associé. Le sélecteur d'objets n'affiche que les objets disponibles pour ce champ.
Action	Action appliquée sur le paquet remplissant les critères de sélection de cette règle de filtrage.
Traces	Type de trace générée.
Description	Commentaire que vous voulez associer à cette règle.

Au niveau de la colonne **Etat**, une lumière verte signifie que lors de l'activation du slot, cette règle sera appliquée, une lumière rouge signifie qu'elle ne sera pas appliquée. Ceci permet de définir des règles qui seront utilisées ultérieurement ou de désactiver temporairement certaines règles pour faire des tests.

AVERTISSEMENT
Par défaut les règles sont inactives (lumière rouge).

A la gauche des noms d'objets (Source et Destination) se trouve une icône d'état, indiquant la nature de l'objet (machine ou réseau). Le symbole **+** apparaît lorsqu'il s'agit d'un groupe d'objets.

Si une règle n'est pas ou plus valide, elle passe automatiquement à l'état **Off** et une icône avec un point d'exclamation apparaît dans la colonne posant problème.

7.2.4.2. Actions possibles sur les slots

Nom du slot	Nom donné au fichier de configuration.
Description	Commentaire indicatif associé à la politique de filtrage.
Mode normal/étendu 	Affichage des paramètres de configuration avancés du filtrage. Des colonnes supplémentaires s'affichent en mode avancé. Par défaut, la grille est en mode normal.
Insérer une règle 	Insérer une ligne vierge après la ligne sélectionnée.
Supprimer les règles sélectionnées 	Supprimer la ligne sélectionnée.
Remonter une règle 	Placer la ligne sélectionnée avant la ligne directement au dessus.
Redescendre une règle 	Placer la ligne sélectionnée après la ligne directement en dessous.
Insérer un	Cette option permet d'insérer un séparateur au dessus de la ligne sélectionnée afin

séparateur 	d'indiquer un commentaire sur une ligne de l'édition du filtrage. Pour définir un séparateur, il s'agit d'indiquer un intitulé et une couleur via une fenêtre de configuration. Une fois le séparateur inséré, un petit bouton s'affiche. Il est cliquable afin de déployer les règles. Si les règles au sein du séparateur ne sont pas affichées, le nombre de règles est indiqué à côté du libellé de ce séparateur.
Imprimer	Impression de la configuration du filtrage.

NOTES

1) Une ligne est sélectionnée quand l'un de ses éléments est sélectionné (en inverse-vidéo).
2) Certains boutons sont grisés lorsqu'ils sont susceptibles de ne pas être pertinents (par exemple, le bouton Mode normal/étendu est grisé pour le filtrage d'URL)

7.2.4.3. Menu contextuel

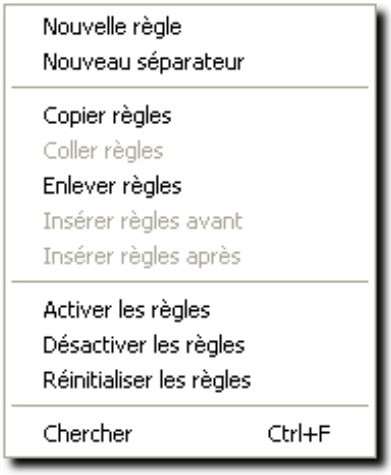


Figure 166 : Menu contextuel

Le menu contextuel est activable par un clic droit sur une ligne sélectionnée dans la grille. Les options de ce menu sont des raccourcis aux boutons équivalents situés dans la barre d'outils.

Vous pouvez accéder aux fonctionnalités du copier-coller grâce aux touches standards :

- **CTRL-C** pour copier, **CTRL-V** pour coller.
- **CTRL-D** pour supprimer la ligne.
- **Ins** pour insérer une ligne après la ligne en cours.
- **Maj+Ins** pour insérer une ligne avant la ligne en cours.

Vous pouvez supprimer une ligne en appuyant directement sur la touche **Suppr** du Clavier.

Vous pouvez déplacer une règle avec les touches **+** et **-** du clavier.

1. Sélectionner un objet.
2. Maintenir le bouton de souris enfoncé.
3. Réaliser un glissement de l'objet vers la grille de règles.
4. Enfin, y déposer l'objet.

Lorsque l'administrateur réalise une opération de Drag & Drop, les colonnes qui peuvent contenir l'objet sélectionné apparaissent en surbrillance. Une fois la manipulation effectuée, les colonnes qui étaient en surbrillance disparaissent.

Le menu de sélection des types d'objet situé à gauche du menu Drag & Drop permet de sélectionner le type d'objet affiché dans la grille.

Affichage de la grille

L'affichage des données contenues dans la grille peut être défini suivant les préférences de l'administrateur parmi les options d'affichage : grandes icônes, petites icônes, détaillé ou en liste.

Options d'affichage

Une option d'affichage des données de la grille du menu Drag & Drop sont disponibles.

Cacher objets non utilisés

Cette option permet de n'afficher dans la grille que les objets qui sont actuellement utilisés dans les règles de translation.

7.2.4.4. Analyseur de cohérence et de conformité des règles

La politique de filtrage d'un firewall est un des éléments les plus importants pour la sécurité des ressources que le firewall protège. Bien que cette politique évolue sans cesse, s'adapte aux nouveaux services, aux nouvelles menaces, aux nouvelles demandes des utilisateurs, elle doit converser une cohérence parfaite afin que des failles n'apparaissent pas dans la protection que propose le firewall.

L'enjeu est d'éviter la création de règles qui en inhiberait une autre. Lorsque la politique de filtrage est conséquente, le travail de l'administrateur est d'autant plus fastidieux que ce risque s'accroît. De plus lors de la configuration avancée de certaines règles de filtrage très spécifiques, la multiplication des options pourrait entraîner la création d'une règle erronée, ne correspondant plus aux besoins de l'administrateur.

Pour éviter cela, l'écran d'édition des règles de filtrage des firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.
Divisé en deux onglets, cet analyseur regroupe les erreurs de création de règles dans l'onglet **`Erreurs`** et les erreurs de cohérence dans les règles dans l'onglet **`Avertissements`**.

Figure 167 : Avertissements

Au niveau des intitulés des deux onglets s'affiche le nombre d'erreurs ou d'avertissements calculés dans la configuration des règles. Lorsque ce chiffre n'est plus à 0, le titre s'affiche en gras.

Lorsqu'il y a des erreurs ou avertissements, des lignes s'affichent dans ces onglets permettant d'indiquer par un commentaire le problème et la règle responsable du message.
Lorsqu'aucune erreur ou avertissement n'est rencontré, le message "Aucun problème détecté" reste affiché.

Le moteur de calcul fonctionne en arrière-plan et ne peut gêner l'administrateur lors de ses configurations.

7.2.5. Création des règles de filtrage

Cette section détaille la création de vos règles de filtrage. L'ordre de ces règles est important car le firewall les parcourt du haut vers le bas et s'arrête dès qu'il trouve une règle correspondant au paquet IP (sauf s'il exécute uniquement une option). Les règles d'authentification doivent être configurées dans cette section. Ces règles permettent de limiter à certains utilisateurs l'accès à certains services ou certaines machines.

7.2.5.1. Activation et désactivation d'une règle

On : La règle est utilisée pour le filtrage.
Off : La règle n'est pas utilisée pour le filtrage.

Figure 168 : Activation/Désactivation de règles

L'activation et la désactivation d'une règle de filtrage facilitent la mise au point de vos filtres. Une règle désactivée n'est pas prise en compte par le firewall NETASQ lorsque le slot est activé.

7.2.5.2. Objet source et objet destination

L'objet "Source" correspond à la source du paquet traité. Il peut s'agir d'une machine, d'un réseau, d'un groupe, d'un intervalle (range).

L'objet "Destination" correspond, quant à lui, à la destination du paquet traité.

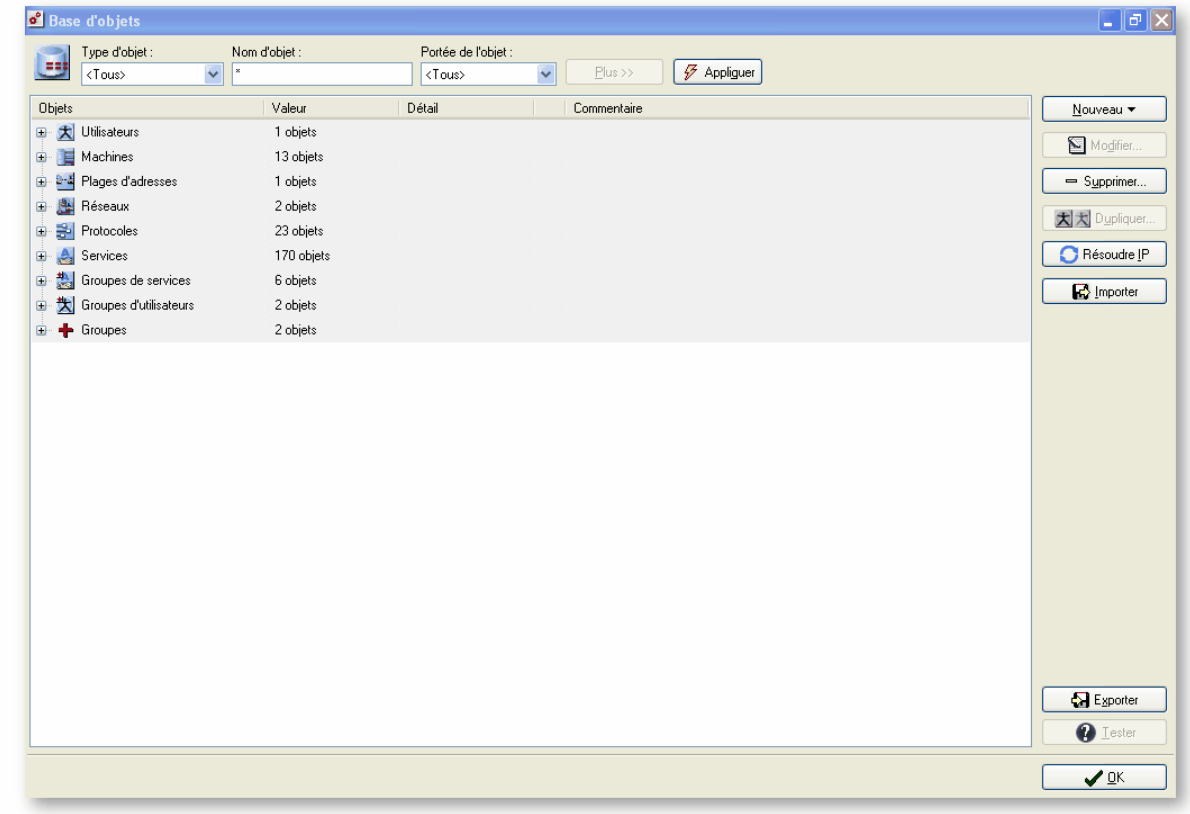


Figure 169 : Base d'objets

Un double-clic dans ces zones permet de choisir les objets concernés par la règle que vous voulez mettre en place, grâce à la boîte de dialogue de sélection des objets.

Choix de la source

Les sources des règles sont définies de la façon suivante : **<User>@<IP>**.

Pour préciser une source, vous devez donc choisir la partie <User> et la partie <IP>. La partie <User> peut être un utilisateur ou un groupe d'utilisateurs parmi ceux définis dans les objets du firewall. La partie <IP> peut être une machine, un groupe de machines, un réseau ou un groupe de réseaux définis dans les objets du firewall.

Différents cas de figure rencontrés :

- **<Any>@<Any>** : la règle s'applique à toute machine mais nécessite une authentification de l'utilisateur
- **<No Auth>@<Any>** : la règle s'applique à toute machine sans authentification
- **<No auth>@Object** : la règle s'applique à l'objet "Object" (Object peut être une machine, un groupe de machines, un réseau ou un groupe de réseaux) et ne nécessite pas d'authentification
- **<Any>@Object** : la règle s'applique à l'objet "Object" et nécessite une authentification de l'utilisateur
- **User@<Any>** : la règle s'applique à toute machine à condition que l'utilisateur soit authentifié sous le login User
- **User@Object** : la règle s'applique à l'objet "Object" et l'utilisateur doit être authentifié sous l'identifiant User.

Si une source possède une partie <user> différente de <No auth> alors une authentification sera nécessaire.

Choix de la destination

La destination est toujours une machine, un groupe de machines ou un réseau.

7.2.5.3. Le panneau des objets

Le panneau d'objets se compose en deux parties :

- Les catégories d'objets
- Les objets appartenant à la catégorie d'objet sélectionnée (que l'on sélectionne par Drag&drop). La liste des objets s'adapte donc en fonction de la catégorie choisie.

Chaque liste contient l'objet <Any> qui représente la totalité des objets.

7.2.5.4. Menu Drag & Drop

Comme son nom l'indique le menu Drag & Drop permet en un Drag & Drop de positionner les objets configurés dans le chapitre précédent dans les règles de filtrage. Il permet de copier un objet d'une cellule vers une autre ou d'accueillir des objets venant du panneau des objets. L'opération de Drag & Drop consiste à :

NOTE
L'objet **<Any>** correspond à TOUTES LES adresses IP possibles. Il faut bien comprendre que l'objet **<Any>** est un objet à part entière. Ce n'est pas un Joker qui remplace n'importe quel objet.

Les objets sont ceux que vous avez définis dans *Partie 4 : Objets*.

Le champ vide sous les onglets vous permet de faire une recherche rapide dans la liste (avec la première lettre de l'objet par exemple).

Sous les onglets, les boutons suivants apparaissent :

Opérateur	Signifie que l'objet concerné par la règle de filtrage est celui sélectionné. Signifie que l'objet concerné par la règle de filtrage est tout sauf celui sélectionné.
OK	Valide la sélection.
Annuler	Annule le choix et retourne à la fenêtre précédente.

AVERTISSEMENT
L'objet source correspond toujours à l'initiateur de la communication.

Si vous utilisez la translation d'adresses, utilisez toujours comme Source l'objet **Réel** (pas l'objet translaté) car le firewall NETASQ applique les règles sur les adresses réelles.

7.2.5.5. Port de destination

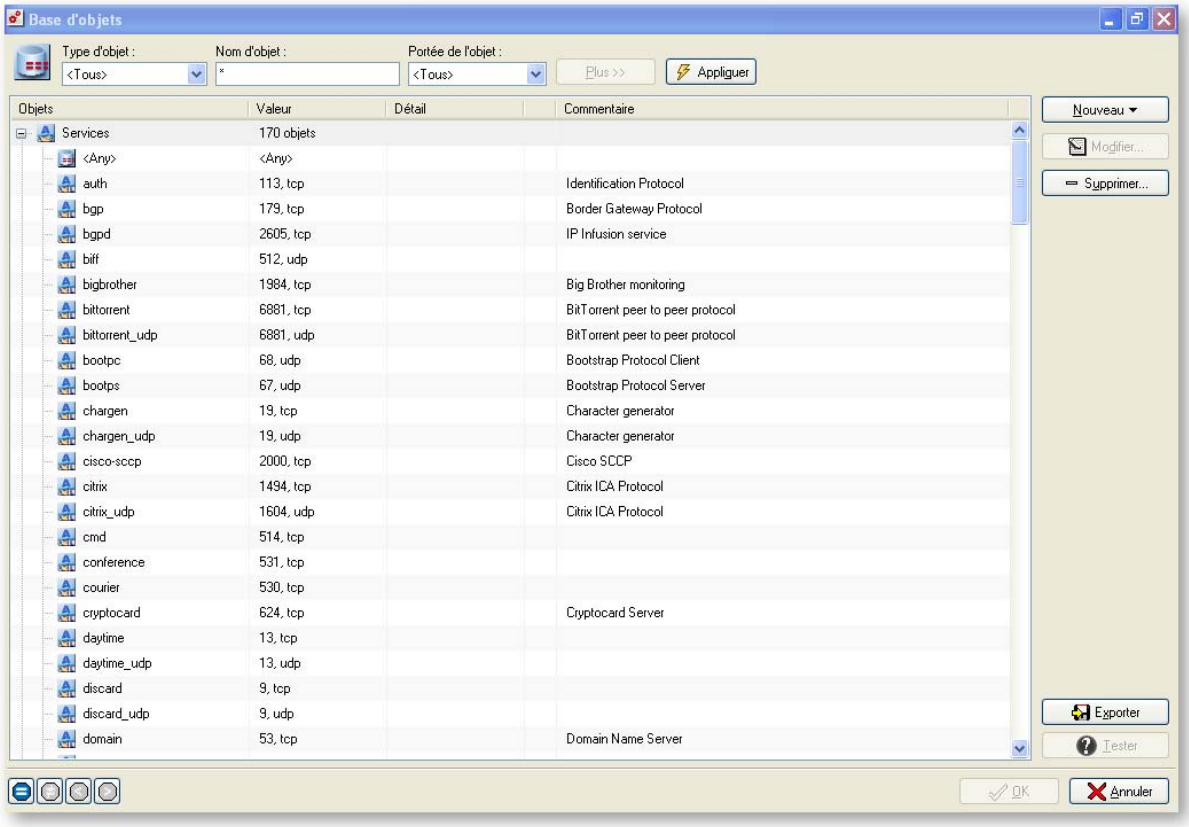


Figure 170 : Base d'objets

Un double-clic dans cette zone permet de choisir le service ou groupe de services concerné par la règle de filtrage, grâce à la boite de dialogue de sélection des services.

Vous pouvez choisir un service ou un groupe de services. Ces services sont ceux que vous avez définis dans Partie 4 : Objets.

En bas de cette fenêtre, les boutons suivants apparaissent :

Opération	Signifie que le service concerné par la règle de filtrage est celui sélectionné. Signifie que les services concernés par la règle de filtrage sont tout sauf celui sélectionné. Signifie que tous les services concernés sont ceux dont le numéro de port est inférieur et égal au numéro de port du service sélectionné. Signifie que tous les services concernés sont ceux dont le numéro de port est supérieur et égal au numéro de port du service sélectionné.
OK	Valide la sélection.
Annuler	Annule le choix et retourne à la fenêtre précédente.

Le service correspond par défaut au port destination de la machine de destination. Les ports sources sont gérés automatiquement par le module "Stateful".

Dans certains cas, vous pouvez avoir besoin de préciser les ports sources. Dans ce cas, il suffit de cliquer sur l'icône . Une colonne supplémentaire apparaît à côté de la colonne "Source". Elle est intitulée "Port Source". Vous pouvez, en double-cliquant sur cette colonne, choisir le service qui sera utilisé sur la machine source.

7.2.5.6. Action

A partir de la colonne "Action", un double-clic sur une action affiche l'écran suivant :

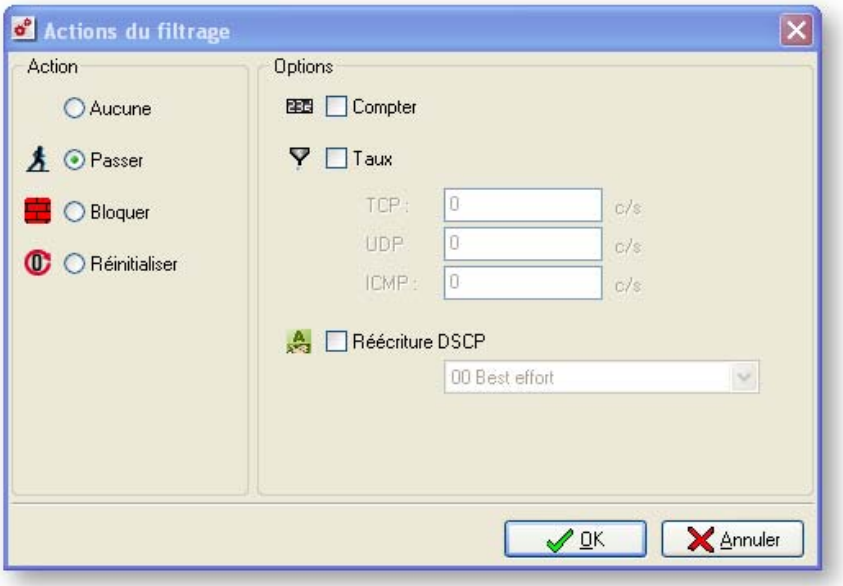


Figure 171 : Actions du filtrage

Un double-clic dans cette zone permet de choisir l'action associée à la règle de filtrage, grâce à la boîte de dialogue de sélection des actions.

La partie gauche de l'écran contient l'ensemble des actions que vous pouvez effectuer :

Aucune	Le firewall NETASQ n'effectue aucune action. Ceci est utile si vous voulez juste tracer certains flux sans appliquer d'action particulière.
Passer	Le firewall NETASQ laisse passer le paquet correspondant à cette règle de filtrage. Le paquet ne descend plus dans la liste de règles.
Bloquer	Le firewall NETASQ bloque silencieusement le paquet correspondant à cette règle de filtrage : le paquet est supprimé sans que l'émetteur ne le sache. Le paquet ne descend plus dans la liste des règles.
Réinitialiser	Le firewall NETASQ bloque explicitement le paquet correspondant à cette règle de filtrage : une réponse TCP/IP est envoyée par le firewall NETASQ à l'émetteur du paquet. Le paquet ne descend plus dans la liste des règles. Cette option n'est valable que pour certains services.

En complément de l'action **Passer**, vous pouvez ajouter les options suivantes :

Compter	Le firewall NETASQ compte le nombre de paquets correspondants à cette règle de filtrage et génère un rapport (dans les statistiques du compteur). Vous pouvez ainsi obtenir des informations de volumétrie sur les flux désirés.

Taux	Le firewall NETASQ peut limiter le nombre maximal de connexions acceptées par seconde pour une règle de filtrage. Définissez, pour le protocole correspondant à la règle (TCP, UDP, ICMP), le nombre désiré. **AVERTISSEMENT** La limitation ne s'appliquera qu'à la règle correspondante. **Exemple** Si vous créez une règle HTTP, seule la limitation TCP sera prise en compte. Cette option vous permet aussi d'éviter le déni de service que pourrait tenter d'éventuels pirates : vous pouvez limiter le nombre de requêtes adressées à vos serveurs. **REMARQUE** Si l'option est affectée à une règle contenant un groupe d'objets, la limitation s'applique au groupe dans son ensemble (nombre total de connexions).
Réécriture DSCP	Marquage du champ DSCP afin de définir une différenciation des flux. Le menu propose deux manières de définir le champ DSCP : selon les standards (la définition des classes fait l'objet d'une RFC) ou manuel (attention, cette option n'est pas compatible avec les équipements uniquement basés sur la qualification standard) Cette information peut être traitée par un équipement réalisant de la Qualité de Service (QoS). Cette option peut être associée au champ Service DSCP ou QoS de la configuration avancée du filtrage des firewalls NETASQ. Des exemples d'utilisation sont indiqués dans la section "DSCP et QoS" ci-dessous.

Certaines actions ou options ne sont disponibles qu'après avoir sélectionné le protocole ou service dans la règle de filtrage. Vous pouvez consulter les exemples de règles de filtrage en *Annexe F : Exemples de règles de filtrage* pour une meilleure compréhension de ces choix.

7.2.5.7. Traces

Figure 172 : Tracer

Un clic dans cette zone permet de définir la politique de traces pour la règle choisie.

Pas de traces	Aucune action de traces n'est affectée à la règle.
Tracer	Dès que cette règle de filtrage est appliquée à une connexion, une trace est ajoutée dans les fichiers de traces, dans la partie filtrage.
Mineure	Dès que cette règle de filtrage est appliquée à une connexion, une alarme mineure est générée. Cette alarme est reportée dans les logs (partie alarmes), est envoyée au moniteur temps réel et peut être envoyée par email (voir Chapitre VIII Gestion des traces).
Majeure	Dès que cette règle de filtrage est appliquée à une connexion, une alarme majeure est générée. Cette alarme est reportée dans les logs (partie alarmes), est envoyée au moniteur temps réel et peut être envoyée par email (voir Chapitre VIII Gestion des traces).

7.2.5.8. Description

Ce champ permet de donner une brève description de la règle.

7.2.5.9. Configuration avancée

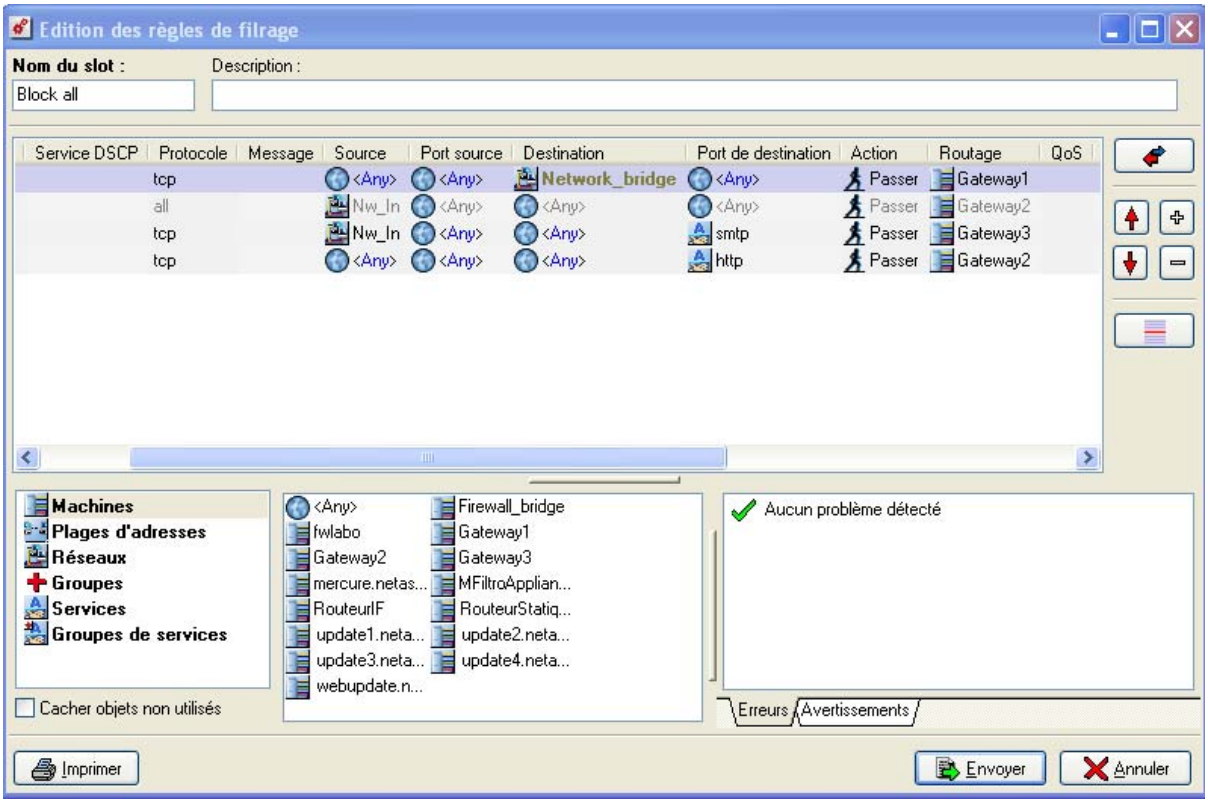


Figure 173 : Edition des règles de filtrage- Mode avancé

En cliquant sur le bouton  de nouvelles colonnes apparaissent. Ceci vous permet de paramétrer d'autres champs relatifs à vos règles de filtrage :

Interface	La colonne interface permet de choisir l'interface sur laquelle doit s'appliquer la règle. Par défaut, le firewall la détecte automatiquement d'après l'adresse IP de la machine source (auto).
Service DSCP	DSCP (pour *Differentiated Services Code Point*), permet comme son nom l'indique de déterminer grâce à un code préétabli, l'appartenance d'un trafic à un certain service plutôt qu'à un autre. Ce service DSCP, utilisé dans le cadre de la Qualité de Service, permet alors à l'administrateur d'appliquer des règles de QoS suivant la différenciation des services qu'il aura définis. Dans les règles de filtrage, lorsque l'administrateur spécifie un Service DSCP, il choisit de n'affecter la règle qu'aux trafics possédant le même DSCP. Ce champ peut être associé au champ QoS de la configuration avancée des règles de filtrage. Des exemples d'utilisation sont indiqués dans la section "*DSCP et QoS*" présente ci-dessous.
Message	Vous pouvez choisir les messages ICMP que vous désirez filtrer.
Port Source	La colonne "Port source" permet de préciser le port utilisé par la machine source, si c'est une valeur particulière. Par défaut, le module "Stateful"

	mémorise le port source utilisé et seul celui-ci est autorisé pour les paquets retour.
Routage	Cette colonne est utile pour spécifier un routeur particulier qui permettra de diriger le trafic correspondant à la règle vers le routeur défini. Elle permet de préciser la machine utilisée pou le routage. Le routage est ainsi configuré finement. **NOTE** Au moment du traitement du paquet, le moteur ASQ évalue les règles dans l'ordre où elles sont définies dans la grille. Par exemple, si l'on souhaite router le trafic HTTP vers un routeur particulier et restreindre l'accès http à un certain groupe d'utilisateurs, la règle de filtrage des utilisateurs devra être spécifiée avant la règle de routage.
QoS	Le champ QoS permet de définir la politique de Qualité de service associée au trafic. La configuration complète et l'utilisation de la QoS NETASQ sont indiquées dans *Partie 7/Chapitre 5 : Qualité de service*.
Options ASQ	Trois options ASQ sont disponibles dans le champ des options ASQ. • **N° du profil** : profil ASQ à appliquer au trafic. (*Cf. Partie 6 : Prévention d'intrusion (ASQ)*). • **N'attachez pas de plugin** : pour désactiver l'attachement automatique des plugins pour cette règle de filtrage. • **Pas de signatures contextuelles** : pour désactiver l'analyse par signatures contextuelles pour cette règle de filtrage.
Nom de règle	Permet d'indiquer un nom à la règle de filtrage sélectionnée. Cette option est utile dans le cadre des tris dans le Reporter.

AVERTISSEMENT
Ces options requièrent une très bonne connaissance du filtrage du firewall. Elles ne doivent être utilisées qu'en connaissance de cause.

Il n'est pas conseillé d'utiliser l'option de filtrage des messages ICMP sans une très bonne connaissance de la signification de ces derniers. L'option **Filtrage des messages ICMP automatique** (présente dans l'onglet **Analyse** du menu **Prévention d'intrusion\ASQ**) réalise déjà un filtrage ICMP en fonction du contexte des connexions.

7.2.5.10. DSCP et QoS

L'UTM NETASQ fait partie intégrante de la politique de Qualité de Service devant être mise en place au sein d'une entreprise. En effet la plupart des flux stratégiques de cette Qualité de Service vont notamment transiter au travers du firewall.

Ainsi l'administrateur d'un firewall NETASQ doit pouvoir configurer l'ensemble des services que l'on peut attendre d'un équipement effectuant une Qualité de Service. Pour cela il dispose de trois options :

- **Le champ Service DSCP** : situé dans la configuration avancée du filtrage des firewalls NETASQ, il permet la différenciation des trafics qui seront traités par le filtrage du firewall.
- **Le champ Réécriture DSCP** : situé dans le menu de configuration de l'action associée à une règle de filtrage. Cette option permet tout simplement la modification du champ DSCP.
- **Le champ QoS** : situé dans la configuration avancée du filtrage des firewalls NETASQ, cette option permet l'application de règles de QoS sur des trafics définis.

La combinaison de ces trois options permet la configuration complète d'une politique de QoS au niveau du firewall.

Exemple 1 : Réécriture DSCP

L'une des actions qui peut s'avérer très utile dans un premier temps est la réécriture du champ DSCP. Par exemple alors que sur Internet certains trafics ne sont pas différenciés, l'administrateur a mis en place une politique de QoS sur le réseau local qu'il souhaite pouvoir appliquer sur des trafics en provenance d'Internet. Dans ce cas, il est nécessaire de mettre en place un mécanisme de réécriture du champ DSCP qui marquera les trafics (jusqu'alors non différenciés) qui doivent être affectés par la politique de QoS.

La configuration de la politique de filtrage est alors la suivante :

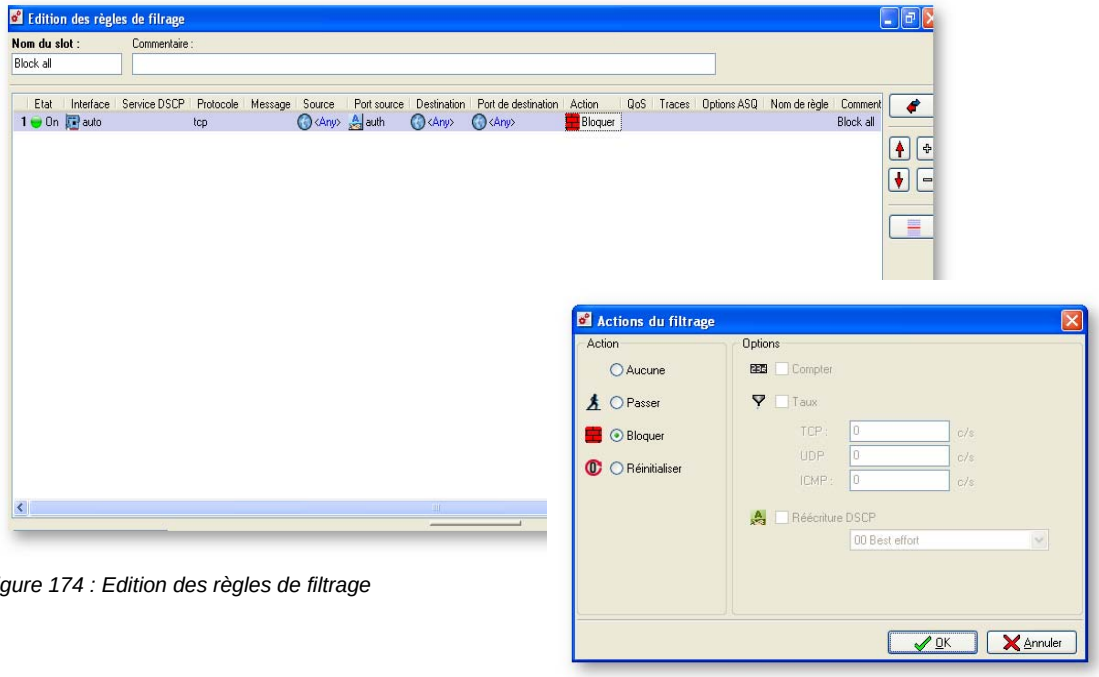


Figure 174 : Edition des règles de filtrage

Ici, tous les trafics non différenciés à destination du serveur Web voit leur champ DSCP réécrit.

Exemple 2 : Application d'une politique de QoS sur des trafics différenciés

L'autre utilisation principale des options de QoS expliquées plus haut est l'application d'une politique de QoS sur des trafics différenciés. En effet le firewall recevant des trafics différenciés grâce au champ "Service DSCP" peut alors appliquer la règle de QoS associée et définie par l'administrateur.

L'image suivante montre un exemple de configuration de la politique de filtrage :

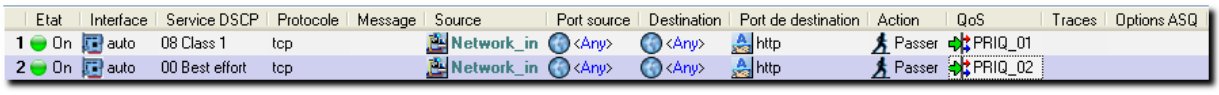


Figure 175 : Politique de QoS

Ici deux trafics quasiment identiques (trafic provenant du réseau local et à destination du Web) sont traités différemment à cause du champ DSCP.

CHAPITRE 3: PROGRAMMATION HORAIRE

7.3.1. Programmateur de slots

Les slots de filtrage et de chiffrement sont soumis à une programmation horaire. Pour chaque type de slot, l'administrateur possédant les droits "F+M" ou "V+M" (selon le type) utilise une grille horaire qui est construite comme un tableau interactif ; l'échelle horizontale représente les heures de la journée, et l'échelle verticale les jours de la semaine. En sélectionnant un des slots préalablement définis et en balayant avec la souris la surface correspondant à des plages horaires, on affecte ce slot à ces plages horaires.

Il doit toujours y avoir un slot de filtrage actif à un moment donné. Lorsque l'administrateur part d'une grille horaire de filtrage vierge pour définir ou modifier la programmation horaire du filtrage, le premier slot de filtrage que l'administrateur sélectionne est automatiquement affecté à toutes les heures de tous les jours de la semaine.

Vous pouvez configurer un slot pour qu'il ne s'active que lors des "heures de bureau", tout en programmant un blocage de tout trafic le reste du temps.

Pour programmer l'activation d'un slot vous avez deux possibilités :

- En sélectionnant le menu **`Programmateur de slots`** dans l'arborescence du Manager.
- En sélectionnant le bouton **Programmer...** présent dans chaque grille de slots.

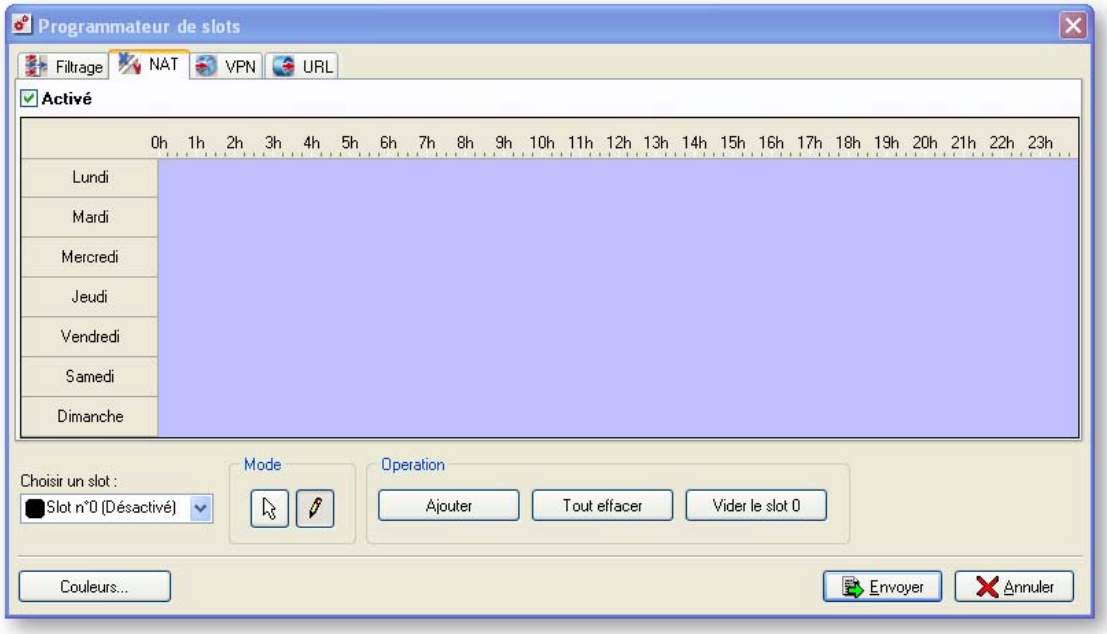


Figure 176 : Programmateur de slots - NAT

La fenêtre de programmation horaire se décompose en trois parties :

- Des onglets de sélection de type de slots.
- Une grille horaire.
- Des boutons d'action.

Les onglets de sélection de type de slots

Quatre types de choix de slots sont disponibles.

- **Filtrage** : Programmation des slots de filtrage.
- **NAT** : Programmation des slots de translation d'adresses.
- **VPN** : Programmation des slots de tunnels VPN.
- **URL** : Programmation des slots de filtrage d'URL.

Chacun des onglets fait apparaître une interface qui permet d'ajouter, supprimer ou modifier une programmation horaire hebdomadaire par bande et en manipulant la souris. L'utilisateur peut ainsi définir une plage horaire pour une politique donnée.

Activation/Désactivation de la programmation horaire

Il est possible désormais d'activer ou de désactiver la programmation horaire à l'aide de la case à cocher **Activé** (située sous les onglets). Cette possibilité de désactivation est particulièrement utile si vous souhaitez effectuer des tests sur vos politiques de filtrage.

La grille horaire

Cette zone est construite comme un tableau "interactif". L'échelle horizontale représente les heures, l'échelle verticale : les jours. Grâce aux boutons d'action vous pouvez programmer l'activation des slots en sélectionnant une surface avec la souris.

On peut noter qu'au moins un slot de filtrage doit toujours être programmé. Donc lorsque vous programmez le premier de ces slots de filtrage celui-ci est automatiquement programmé pour tous les jours à toutes les heures.

Les boutons d'action

Choisir un slot	Sélection du slot à programmer.
	Sélection d'une zone sur la grille.
	Modification d'une zone sur la grille.
Ajouter	Ajout d'un programmateur pour un slot. L'écran suivant s'affiche :

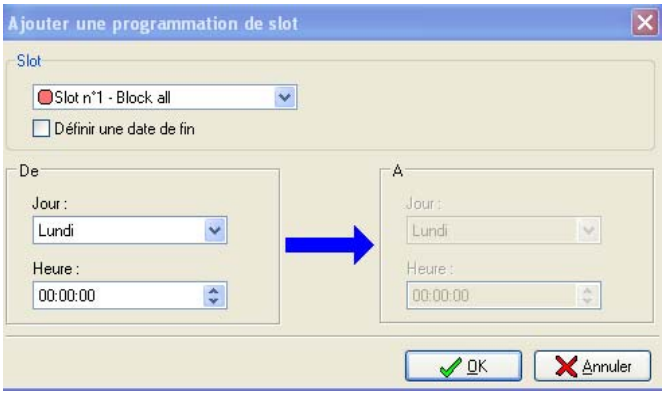


Figure 177 : Ajouter une programmation de slot

	Après avoir sélectionné un slot, il suffit de cocher l'option **Définir une date de fin** pour déterminer une période d'activation (Date et heure).
Tout effacer	Suppression de toutes les zones sur la grille.
Vider le slot x	Suppression de toutes les zones concernant un slot.
Couleurs…	Configuration des couleurs associées à chaque slot. Lorsque vous cliquez sur le bouton, l'écran ci-dessous s'affiche :

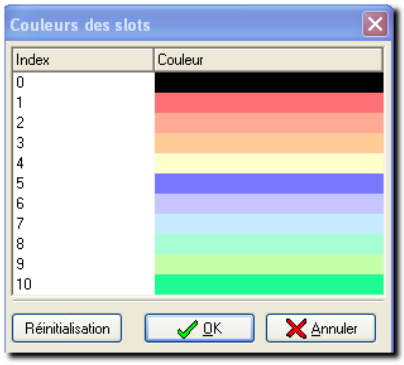


Figure 178 : Couleurs de slots

Envoyer	Un clic sur ce bouton fait parvenir au serveur les configurations modifiées et active ensuite la programmation horaire.

7.3.2. Calendriers

Les calendriers sont utilisés dans divers modules, notamment pour l'authentification des utilisateurs.

Chaque utilisateur est associé à un calendrier qui lui permet de s'authentifier auprès du firewall lorsque la politique de filtrage instaurée par l'administrateur l'y oblige. Ce calendrier peut être spécifique à l'utilisateur ou le même pour plusieurs utilisateurs. Il définit les zones où l'utilisateur doit s'authentifier et celles où il n'a aucun accès. Une fois les calendriers définis, ils peuvent être sélectionnés lors de la configuration de l'authentification des utilisateurs. Vous accédez à la configuration de ce calendrier en sélectionnant le menu **`Calendriers`** dans l'arborescence du Manager.

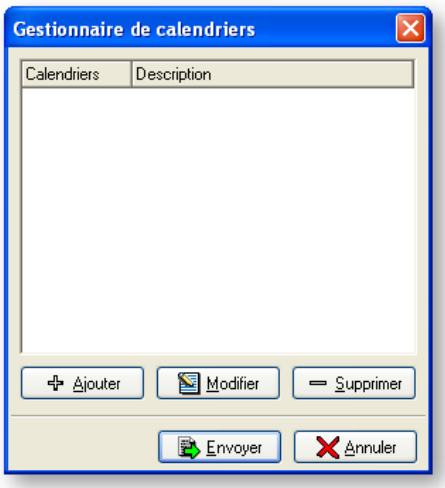


Figure 179 : Gestionnaire des calendriers

L'écran de sélection des calendriers se divise en trois parties :

- Une grille contenant les calendriers configurés.
- Des boutons d'action permettant l'ajout, la modification ou la suppression de calendriers
- Enfin en bas de la fenêtre les boutons de validation ou d'annulation des modifications effectuées.

Pour ajouter ou modifier un calendrier, vous avez plusieurs possibilités :

- En sélectionnant dans l'arborescence du Manager **Objets**, puis en double-cliquant sur un utilisateur. La fenêtre "Edition d'un utilisateur" s'affiche. Dans l'onglet **Authentification**, sélectionnez le bouton **Calendrier** puis **Création d'un calendrier**.
- En sélectionnant dans l'arborescence du Manager, le menu **Authentification\Portail captif** Dans les menus **Interfaces internes** et **Interfaces externes,** sélectionnez **Avancé.** Cliquez sur le bouton **Calendrier** puis sélectionnez **Création d'un calendrier.**
- En cliquant sur le bouton **Ajouter** ou **Modifier** de l'écran du menu **Calendriers**.

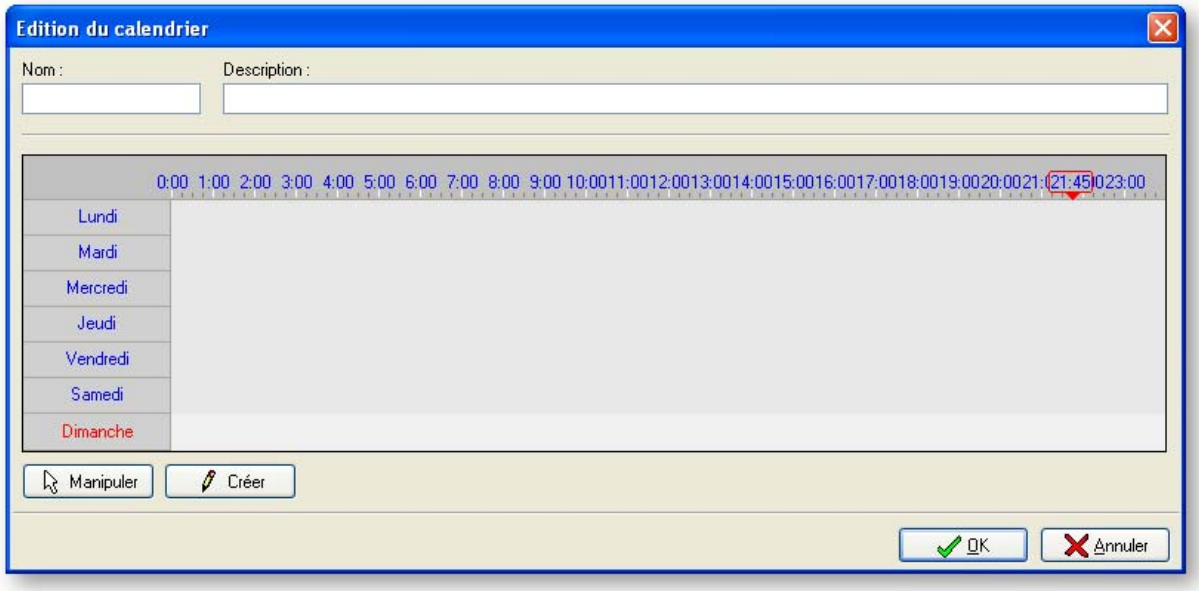


Figure 180 : Edition du calendrier

La fenêtre de configuration des calendriers se divise en trois parties :

- Le champ "Nom" : Nom défini pour le calendrier et "Description". La description d'un calendrier peut être éditée dans la grille, au contraire du nom.
- Une grille horaire étalée sur une semaine.
- Des boutons d'actions vous permettant de créer des plages d'horaires et de les manipuler ensuite.

REMARQUE
Le nombre de calendriers créés est illimité.

La grille horaire

Cette zone est construite comme un tableau "interactif". L'échelle horizontale représente les heures, l'échelle verticale : les jours. Vous pouvez programmer les zones pendant lesquelles l'authentification est permise en sélectionnant une surface avec la souris. En cliquant sur les titres de colonnes et de lignes vous inversez la sélection actuelle dans la colonne ou dans la ligne en question. En cliquant le coin haut gauche de la grille vous inversez la sélection entière.

CHAPITRE 4 : REGLES IMPLICITES

Les règles implicites représentent des règles de filtrage générées en fonction de plusieurs paramètres. Elles ne peuvent pas être modifiées comme les règles de filtrage.

Accédez aux règles implicites par le menu de l'arborescence **Politique**. L'écran de configuration des règles implicites s'affiche :

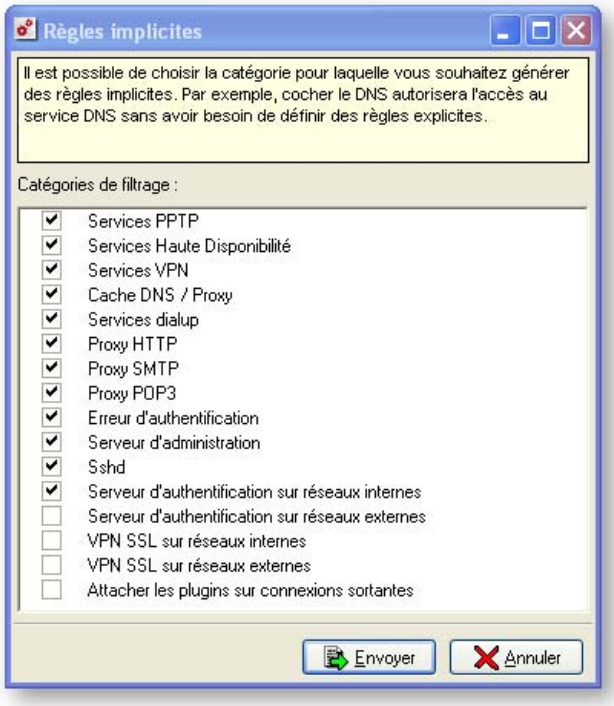


Figure 181 : Règles implicites

Dans cet écran on vous informe qu'il est possible de générer automatiquement certaines règles liées à l'utilisation des services du firewall. Si vous cochez un service, le firewall crée de lui-même les règles d'utilisation de ce service.

- **Services PPTP** : pour les tunnels sécurisés en PPTP.
- **Services Haute Disponibilité** : pour la Haute Disponibilité.
- **Services VPN** : pour les tunnels VPN.
- **Cache DNS/Proxy** : pour le cache DNS.
- **Services dialup** : pour les connexions distantes.
- **Proxy HTTP** : pour le proxy http.
- **Proxy SMTP** : pour le proxy SMTP.
- **Proxy POP3** : pour le proxy POP3.
- **Erreur d'authentification**
- **Serveur d'administration** : autorise l'accès avec l'interface graphique à partir d'une machine située sur les réseaux internes. Cette option crée une règle implicite au niveau du firewall. Si cette option est désélectionnée, il faudra créer une règle explicite, dans les règles de filtrage, pour autoriser la connexion au Firewall via NETASQ UNIFIED MANAGER (service Firewall_srv, port 1300).
- **Sshd** : permet d'ouvrir l'accès au firewall par SSH afin de pouvoir se connecter dessus en lignes de commande.
- **Serveur d'authentification sur réseaux internes** : autorise l'accès au service d'authentification pour les utilisateurs des réseaux internes. Ce service utilise les ports 443 (https)
- **Serveur d'authentification sur réseaux externes** : autorise l'accès au service d'authentification pour les utilisateurs des réseaux externes. Ce service utilise les ports 443 (https).

- **VPN SSL sur réseaux internes** : autorise l'accès au VPN SSL pour des utilisateurs des réseaux internes (les interfaces Ethernet et VLAN possédant l'attribut "protégée")
- **VPN SSL sur réseaux externes** : autorise l'accès au VPN SSL pour des utilisateurs des réseaux externes (les interfaces Ethernet et VLAN ne possédant pas l'attribut "protégée" et les interfaces de type Dialup).
- **Attacher les plugins sur connexions sortantes** : lorsque cette option est cochée, lors d'une connexion sortante, le plugin correspondant à cette connexion sera automatiquement attaché.

REMARQUE
Lors d'une mise à jour depuis la version 6.3, les règles implicites **VPN SSL sur réseaux internes** et **VPN SSL sur réseau externes** sont supprimées. Seule la règle implicite au serveur d'authentification demeure.

AVERTISSEMENT
Si l'utilisateur décoche la catégorie "Serveur d'administration" qui sert à générer les règles implicites qui autoriseront l'accès au serveur d'administration du firewall, un message d'avertissement s'affiche avant validation finale de l'écran.

CHAPITRE 5 : QUALITE DE SERVICE (QoS)

7.5.1. Présentation

7.5.1.1. Qu'est ce que la Qualité de Service, QoS (pour Quality of Service) ?

DEFINITION
Trois constats ont demandé le développement de la "Qualité de service" sur les réseaux IP :

- Premièrement, de plus en plus les stations de travail modernes contiennent des logiciels multimédia y compris codecs vidéo et audio, cela nécessite donc une certaine fiabilité des performances (vitesse) vidéo.

- Le développement de plus en plus courant du multicast d'IP.

- Enfin le développement de logiciels vidéo et audio hautement performants permettant la vidéoconférence par exemple.

Ce type d'application en temps réel ne pouvait se révéler fonctionnel sur l'Internet étant donné les délais de latence et pertes de paquets généralement rencontrés sur les réseaux IP. Les développements de la "Qualité de service" se sont donc avérés indispensables.

A un haut niveau d'abstraction, la "Qualité de service" fait référence à la capacité à fournir un service réseau en fonction de paramètres définis dans un contrat de niveau de service (SLA, "Service Level Agreement"). La "Qualité" du service est alors caractérisée par sa disponibilité, son taux de latence, ses fluctuations, son débit et son taux de paquets perdus.

Au niveau des ressources réseau, la "Qualité de service" fait référence à la capacité d'un équipement à fournir des services de prioritisation de trafic, un contrôle de la bande passante ainsi que de son temps de latence.

7.5.1.2. QoS sur les firewalls NETASQ

Le module "Stateful QoS" de l'ASQ permet une gestion efficace de la bande passante. Vous avez la possibilité d'associer une politique de QoS à chaque règle de filtrage en choisissant un algorithme d'ordonnancement des paquets.

Deux algorithmes sont proposés : **PRIQ** (Priority Queuing) et **CBQ** (Class-Based Queuing).

- **PRIQ** permet de rendre prioritaires les paquets associés à une règle de filtrage de façon qu'ils soient toujours traités en premier avant le reste du trafic.
- **CBQ** permet de traiter les paquets par classe de bande passante. Vous avez la possibilité de choisir une classe d'ordonnancement pour chaque règle de filtrage et de lui associer une garantie de bande passante aussi bien qu'une limite.

En cas d'utilisation simultanée de **CBQ** et **PRIQ**, les flux en **PRIQ** seront traités de façon prioritaire par rapport aux flux en **CBQ**.

7.5.2. Configuration

7.5.2.1. Menu de configuration de la QoS

La configuration de la QoS est accessible dans le menu **`Politique\Qualité de Service`** de l'arborescence ou lors de l'édition d'une politique de filtrage, en double-cliquant dans la colonne Qos d'une règle de filtrage. L'écran "Paramètres de Qos de la règle de filtrage" s'affiche.

Figure 182 : Paramètres de QoS de la règle de filtrage

Il suffit de cliquer sur le bouton **Configurer la QoS.**

Le menu de configuration de la QoS est divisé en deux parties :

- A gauche, un arbre présentant les diverses fonctionnalités du menu **`Qualité de service`**.
- A droite, les options configurables.

7.5.2.2. Général

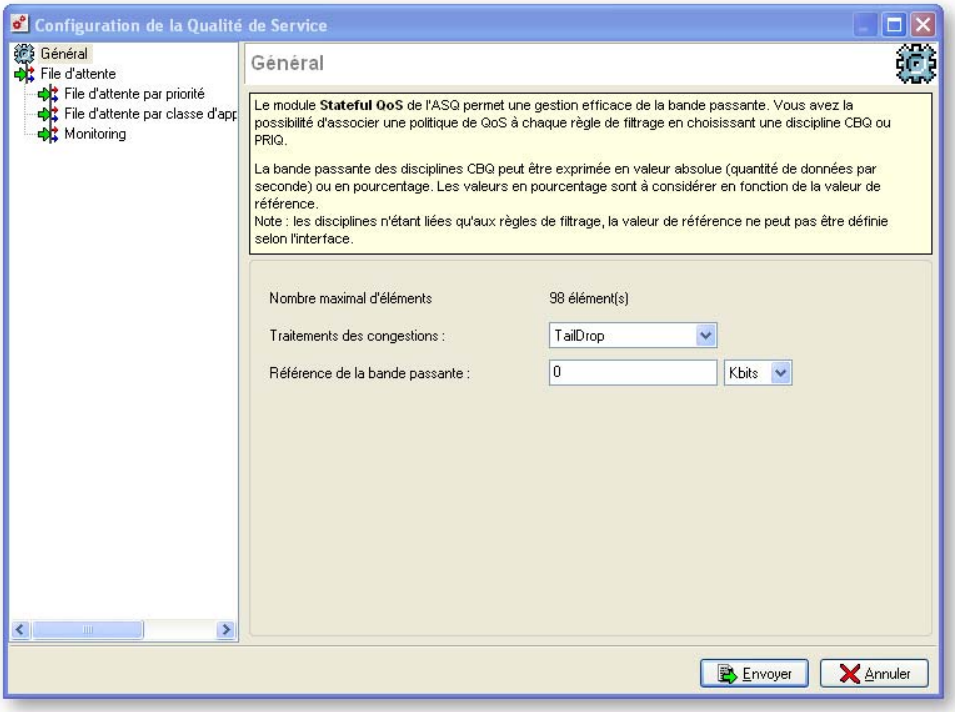


Figure 183 : Configuration de la qualité de service : Général

Les différentes options de la configuration générale sont présentées dans le tableau suivant :

Nombre maximal d'éléments	Donnée indicative présentée par NETASQ UNIFIED MANAGER, dépendante du modèle du firewall (20 pour les U30 et U70, 100 pour les U120, U250 et U450, 200 pour les U1100 et U1500, 255 pour le U6000, indiquant le nombre de file d'attente qui peuvent être créées.
Traitement des congestions	Cette option permet de définir l'algorithme de traitements des congestions qui sera utilisé lorsque le firewall n'est plus à même de gérer tout le trafic qu'il reçoit.
Référence de la bande passante	La valeur de référence en Kbits/s ou en Mbits/s permet d'indiquer une référence sur laquelle seront basées les limitations de bande passante indiquée en pourcentage dans la configuration des files d'attente.

Traitements des congestions

Un élément important dans la "Qualité de Service" est de résoudre le problème du niveau généralement très haut du taux de perte de paquets sur l'Internet. En effet lorsqu'un paquet est perdu avant d'atteindre sa destination, toutes les ressources mises en œuvre lors de son transit sont gâchées. Dans certain cas, cette situation peut même amener une situation de congestion grave qui parfois entraîne la paralysie totale des systèmes.

On est loin de la nécessité de stabilité et de "temps réel" des applications de vidéoconférence d'aujourd'hui. Le contrôle optimisé des situations de congestion et la gestion des queues de données deviennent un enjeu important de la "Qualité de Service".

Les firewalls NETASQ disposent de deux algorithmes pour leur traitement des congestions, l'algorithme **TailDrop** et l'algorithme **BLUE.** NETASQ recommande toutefois l'utilisation de l'algorithme BLUE comme algorithme de traitement des congestions.

TailDrop

Le principe de cet algorithme très basique est de supprimer les paquets arrivant dans la file d'attente lorsque celle-ci est pleine.

Blue

Cet algorithme très performant (de très loin devant la plupart des autres algorithmes) utilise un historique des paquets perdus et le taux d'utilisation des interfaces réseau pour gérer leur congestion.

Le principe général de cet algorithme est de définir une probabilité unique (P) qui est ensuite utilisée pour marquer (par l'option de congestion de trafic ECN) ou pour dropper des paquets de la file de données. Le taux de perte de paquets en file fait augmenter cette probabilité (P).

> **Exemple**
> Dans le cas d'un débordement de tampon (Buffer Overflow), la file de données perd continuellement des paquets de la file, la probabilité (P) est incrémentée, ce qui a pour effet d'augmenter artificiellement le nombre de paquets marqués (par ECN) ou le nombre de paquets droppés. Inversement lorsque le taux d'utilisation de l'interface réseau est faible voire nul, la probabilité (P) est alors diminuée.

Cette méthode a pour effet de stabiliser les flux réseaux, de réduire fortement le nombre de paquets finalement perdus, de maximiser les performances de chaque interface réseau et enfin de diminuer le temps de latence des paquets

Ces critères sont fondamentaux pour la SLA, "Service Level Agreement".

7.5.2.3. File d'attente

Le module de QoS, intégré à l'ASQ est associé au module de filtrage pour offrir les fonctionnalités de Qualité de Service. A l'arrivée d'un paquet, celui-ci est traité par une règle de filtrage puis l'ASQ affecte le paquet à la bonne file d'attente suivant la configuration du champ QoS de cette règle de filtrage. Il existe trois types de file d'attente sur le firewall. Deux sont directement associés aux algorithmes de QoS présentés ci- dessus : PRIQ (Priority Queuing) et CBQ (Class-Based Queuing), le troisième type permet le monitoring du trafic.

File d'attente par priorité

Il existe 8 niveaux de priorité. Les paquets seront traités en fonction des priorités paramétrées.

Il est possible d'associer une priorité élevée aux requêtes DNS en créant une règle de filtrage et en lui associant une queue PRIQ.

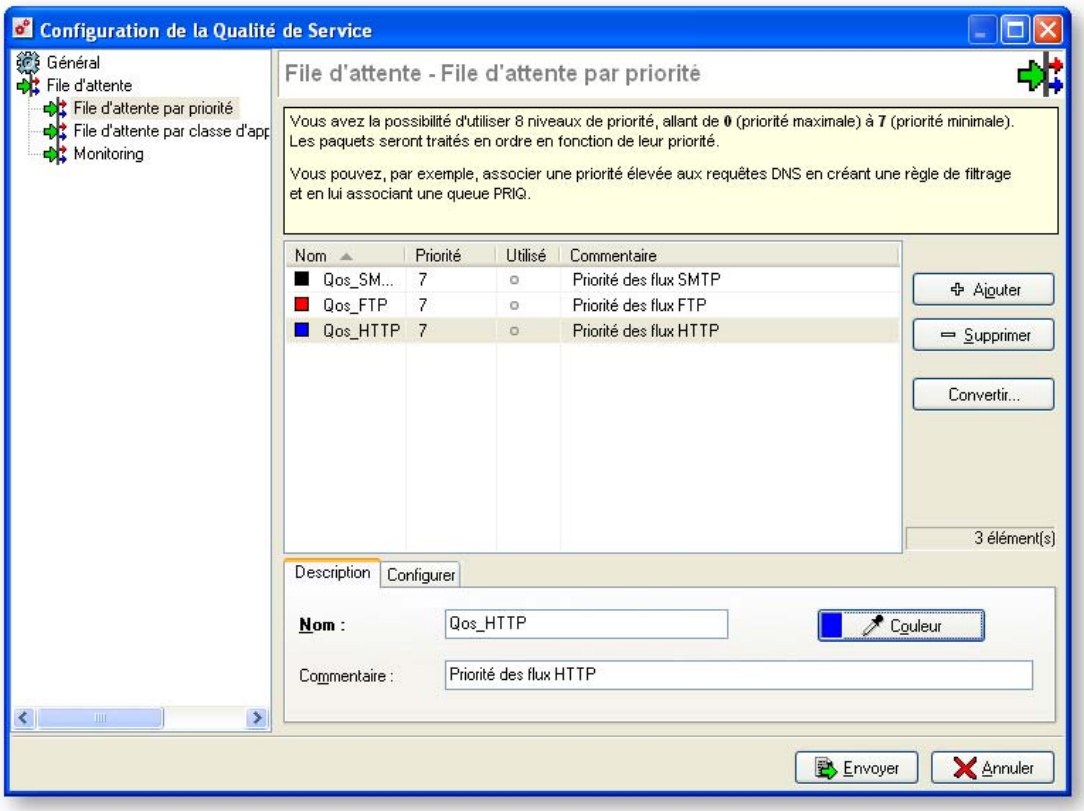


Figure 184 : Configuration de la QoS - File d'attente par priorité

Les files d'attente par priorité induisent une prioritisation des paquets dans leur traitement. Les paquets qui sont associés à une règle de filtrage avec une file d'attente du type **PRIQ** sont traités avant les autres.

Les priorités s'échelonnent entre 0 et 7. La priorité 0 correspond aux trafics les plus prioritaires parmi les files d'attente **PRIQ**. La priorité 7 correspond aux trafics les moins prioritaires parmi les files d'attente **PRIQ**. Les files d'attente **CBQ** et les flux sans règles de QoS sont associés à une priorité 8 "virtuelle" (elle n'est pas configurable) qui définit que quoi qu'il arrive, ces flux seront traités après toutes files d'attente du type **PRIQ**.

Les différentes options de la configuration d'une file d'attente du type PRIQ sont présentées dans le tableau suivant :

Ajouter	La grille du menu **Priority Queuing File d'attente par priorité** affiche les différentes files d'attente qui ont été configurées. Le bouton **Ajouter** permet l'ajout d'une nouvelle file d'attente.
Supprimer	La grille du menu **Priority Queuing File d'attente par priorité** affiche les différentes files d'attente qui ont été configurées. Le bouton **Supprimer** permet de supprimer la file d'attente sélectionnée.
Convertir	La conversion d'une file d'attente **PRIQ** en un autre type de file d'attente conserve le nom de la file d'attente et son commentaire.
xx élément(s)	Donnée cumulée présentée par NETASQ UNIFIED MANAGER indiquant le nombre de règles de QoS du type **PRIQ** qui ont été créées. Si le nombre total de règles de QoS (**PRIQ**, **CBQ** et **Monitoring**) est supérieur à la capacité maximum de gestion du firewall indiquée dans le menu **`Général`**, un message apparaît en bas à gauche de l'écran pour indiquer que le nombre maximum de règle de QoS a été dépassé.

Onglet Description

Nom	Nom de la file d'attente à configurer.
Commentaire	Commentaire associé.
Couleur	Couleur de différenciation de la file d'attente.

Onglet Configurer

Priorité	Priorité de la file d'attente configurée.

La grille du menu Priority Queuing affiche les différentes files d'attente qui ont été configurées. Lorsque ces règles de QoS sont effectivement utilisées dans la définition d'une règle de filtrage un bouton du type est affiché dans la liste. Un double clic sur le bouton permet d'affiche la liste des règles de filtrage dans lesquelles cette file d'attente est utilisée.

File d'attente par classe d'application ou d'affectation

Il est possible de choisir une classe d'ordonnancement pour chacune des règles de filtrage er de lui associer une garantie de bande passante ainsi qu'une limite.
Par exemple; vous pouvez associer une classe d'ordonnancement aux flux http en associant une queue CBQ à la règle de filtrage correspondante.

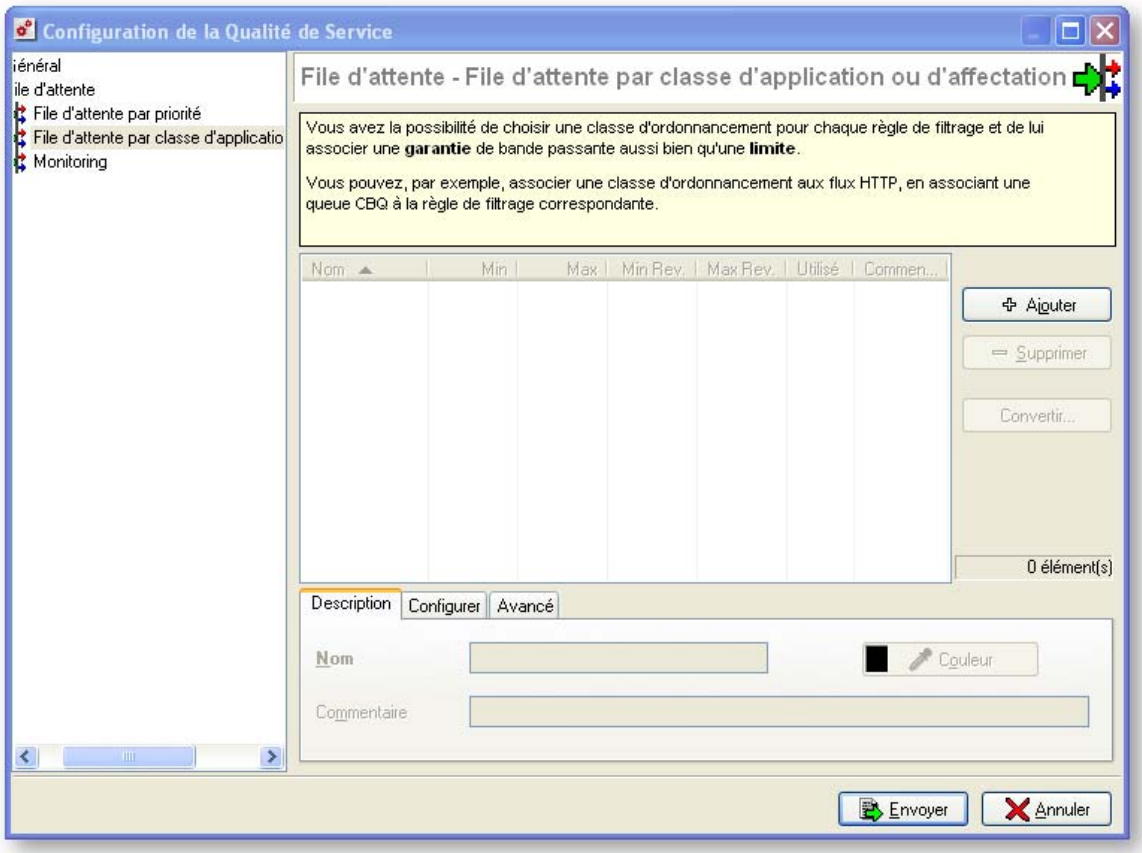


Figure 185 : Configuration de la QoS - File d'attente par classe d'application - Description

Les files d'attente par classe d'application ou d'affectation induisent la façon dont les trafics affectés par ces règles de QoS seront gérés sur le réseau. Les mécanismes de réservation et de limitation de la bande

passante de ce type de files d'attente permettent dans le premier cas, la garantie d'un service minimum et dans le deuxième cas, la préservation de la bande passante vis-à-vis d'applications coûteuses en ressources.

Les différentes options de la configuration d'une file d'attente du type CBQ sont identiques aux files d'attente par priorité.

Onglet Configurer

Max. autorisé bande passante	Agissant comme une limitation, cette option interdit le dépassement de bande passante pour le trafic affecté par ces files d'attente. Configurée en Kbits/s, en Mbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un maximum autorisé de 512Kbits/s alors la bande passante HTTP + la bande passante FTP ne doit pas dépasser 512Kbits/s.
Min. garanti bande passante	Agissant comme une garantie de service, cette option permet la garantie d'un débit donné et d'un délai maximal de transfert. Configurée en Kbits/s, en Mbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un minimum garanti de 10Kbits/s alors la bande passante HTTP + la bande passante FTP sera au minimum de 10Kbits/s. Cependant rien n'empêche que la bande passante HTTP soit de 9Kbits/s et la bande passante soit seulement de 1Kbit/s.
Bande passante illimitée	Cette option permet de ne pas définir de débit maximum autorisé. Dans ce cas c'est la valeur de la bande passante du lien affecté par la règle de QoS qui détermine le maximum disponible.

L'onglet **Configurer** permet la définition des paramètres de réservation et de limitation de la bande passante pour cette file d'attente. La configuration de ces paramètres peut être asymétrique, ce qui signifie que les paramètres de réservation et de limitation seront différents suivant le sens du trafic.

Par défaut l'onglet **Configurer** définit les réservations et limitation de la bande passante dans les deux sens. Mais lorsque des paramètres sont indiqués dans l'onglet **Avancé** (voir ci-dessous), l'onglet **Configurer** définit les paramètres des trafics allant dans le sens de la définition de la règle de filtrage soit "Source" vers "Destination".

La grille du menu **File d'attente par classe d'application ou d'affectation** affiche les différentes files d'attente qui ont été configurées. Lorsque ces règles de QoS sont effectivement utilisées dans la définition d'une règle de filtrage un bouton du type  est affiché dans la liste. Un double clic sur le bouton permet d'affiche la liste des règles de filtrage dans lesquelles cette file d'attente est utilisée.

Onglet Avancé

L'onglet **Avancé** permet la configuration des paramètres de réservations et limitation de la bande passante des trafics allant dans le sens inverse de la définition de la règle de filtrage soit "Destination" vers "Source".

Max. autorisé bande passante	Agissant comme une limitation, cette option interdit le dépassement de bande passante pour le trafic affecté par ces files d'attente. Configurée en Kbits/s, en Mbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un maximum autorisé de 512Kbits/s alors la bande passante HTTP + la bande passante FTP ne doit pas dépasser 512Kbits/s.
Min. garanti bande passante	Agissant comme une garantie de service, cette option permet la garantie d'un débit donné et d'un délai maximal de transfert. Configurée en Kbits/s, en Mbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un minimum garanti de 10Kbits/s alors la bande passante HTTP + la bande passante FTP sera au minimum de 10Kbits/s. Cependant rien n'empêche que la bande passante HTTP soit de 9Kbits/s et la bande passante soit seulement de 1Kbit/s.
bande passante illimitée	Cette option permet de ne pas définir de débit maximum autorisé. Dans ce cas c'est la valeur de la bande passante du lien affecté par la règle de QoS qui détermine le maximum disponible.

La grille du menu **File d'attente par classe d'application ou d'affectation** affiche les différentes files d'attente qui ont été configurées. Lorsque ces règles de QoS sont effectivement utilisées dans la définition d'une règle de filtrage un bouton du type ● est affiché dans la liste. Un double-clic sur le bouton permet d'affiche la liste des règles de filtrage dans lesquelles cette file d'attente est utilisée.

Monitoring

Les files d'attente de monitoring n'affectent pas la manière dont sont traités les trafics qui sont associés à ces règles de QoS. Elles permettent l'enregistrement d'informations de débit et de bande passante qui peuvent être visualisées au moyen de NETASQ UNIFIED MONITOR, dans l'onglet **Graphiques** du logiciel.

Les différentes options de la configuration d'une file d'attente du type Monitoring sont présentées dans le tableau suivant :

Ajouter	La grille du menu Monitoring affiche les différentes files d'attente qui ont été configurées. Le bouton **Ajouter** permet l'ajout d'une nouvelle file d'attente.
Supprimer	La grille du menu Monitoring affiche les différentes files d'attente qui ont été configurées. Le bouton **Supprimer** permet de supprimer la file d'attente sélectionnée.
Convertir	La conversion d'une file d'attente Monitoring en un autre type de file d'attente conserve le nom de la file d'attente et son commentaire.
xx élément(s)	Donnée cumulée présentée par NETASQ UNIFIED MANAGER indiquant le nombre de règles de QoS du type Monitoring qui ont été créées. Si le nombre total de règles de QoS (PRIQ, CBQ et Monitoring) est supérieur à la capacité maximum de gestion du firewall indiquée dans le menu **Général**, un message apparaît en bas à gauche de l'écran pour indiquer que le nombre maximum de règles de QoS a été dépassé.

Onglet Description

Nom	Nom de la file d'attente à configurer.
Commentaire	Commentaire associé.
Couleur	Couleur de différentiation de la file d'attente.

7.5.3. Utilisation de la QoS

7.5.3.1. Activation d'une file d'attente de QoS

C'est dans la configuration des politiques de filtrage que sont définies les règles de QoS qui seront utilisées pour traiter tel ou tel trafic. Le champ correspondant à la QoS n'est accessible qu'une fois le mode étendu de la définition des règles de filtrage activé.

Pour activer une file d'attente de QoS, référez-vous à la procédure suivante :

1. Sélectionnez le menu de configuration **`Politique\Filtrage.`**
2. Editez le slot de filtrage dont les règles doivent accueillir les options de QoS.
3. Sélectionnez le mode **étendu.**
4. Double-cliquez sur le champ **QoS** de la règle à modifier, la fenêtre suivante s'affiche :

Figure 186 : Paramètre de QoS de la règle de filtrage

5. Choisissez une file d'attente configurée (ou configurez-la d'abord).
6. Choisissez l'équité de traitement (si nécessaire, voir ci-dessous).
7. Cliquez sur **OK**, envoyez le slot configuré et activez la politique de filtrage.

Equité de traitement (Fairness)

AVERTISSEMENT

L'équité de traitement complexifie la gestion de la QoS telle qu'elle a déjà été évoquée dans cette documentation. Assurez-vous de maîtriser les aspects précédents de la configuration de la QoS avant d'activer cette option.

L'équité de traitement (Fairness) ajoute à chaque file d'attente QoS un système de pondération des paquets propre à chaque file. Ainsi il est possible de modifier le comportement du traitement des paquets appartenant à la même file d'attente.
Selon l'option Fairness NETASQ, les paquets appartenant à une même file d'attente seront traités :

- Par ordre d'arrivée, selon le mode FIFO (First In First Out, premier arrivé, premier parti) si AUCUNE option d'équité de traitement n'a été spécifiée.
- De façon à ce que le traitement soit équitable (égal) entre les paquets de chaque utilisateur présents dans la file d'attente si l'option d'équité de traitement est **Utilisateur**.
- De façon à ce que le traitement soit équitable (égal) entre les paquets de chaque machine présents dans la file d'attente si l'option d'équité de traitement est **Machine**.
- De façon à ce que le traitement soit équitable (égal) entre les paquets de chaque connexion présents dans la file d'attente si l'option d'équité de traitement est **Connexion**.

7.5.3.2. Cas d'application et recommandations d'utilisation

Exemple 1 : Prioritisation des flux DNS

Basées sur UDP, les requêtes DNS subissent de nombreuses pertes de paquets du fait de la définition même du protocole UDP, qui ne prévoit pas de mécanismes de gestion des erreurs de transmission et de l'écrasante présence des trafics TCP qui noient les trafics UDP dans la masse des paquets TCP.

Pour préserver ces trafics, et en particulier les flux DNS, il est recommandé de prévoir une règle de QoS de type "priorité" (PRIQ). Elle permettra de diminuer les trop fréquentes pertes de paquets et la latence qu'il pourrait y avoir sur ce type de trafic qui demande une réactivité importante (c'est d'ailleurs pour cette raison que les requêtes DNS sont réalisées sur UDP).

Définition de la règle de QoS pour le DNS

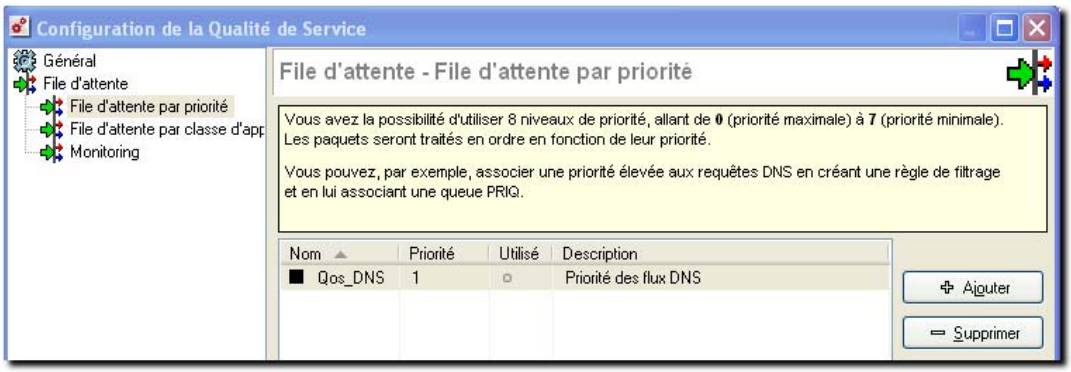


Figure 187 : Configuration de la QoS - File d'attente par priorité

Utilisation de la règle de QoS dans la politique de filtrage

Figure 188 : QoS dans la politique de filtrage

Effets sur le trafic

- Baisse des paquets perdus.
- Diminution de la latence.

Exemple 2 : Limitation du trafic HTTP

Parmi les trafics internet, les flux HTTP sont les plus gros consommateurs de la bande passante du lien Internet et du réseau local. Une utilisation importante de l'internet peut entraîner des problèmes de congestions du trafic réseau, les performances globales sont dégradées et l'utilisation du réseau devient fastidieuse.

Pour remédier à cet état de fait, il est recommandé de **limiter le trafic HTTP au moyen d'une règle de QoS de type "classe d'application ou d'affectation" (CBQ) définissant un débit maximum autorisé**. Elle permettra de préserver la bande passante du réseau et réduire l'impact de l'utilisation de l'internet sur les performances globales du réseau.

Définition de la règle de QoS pour le HTTP

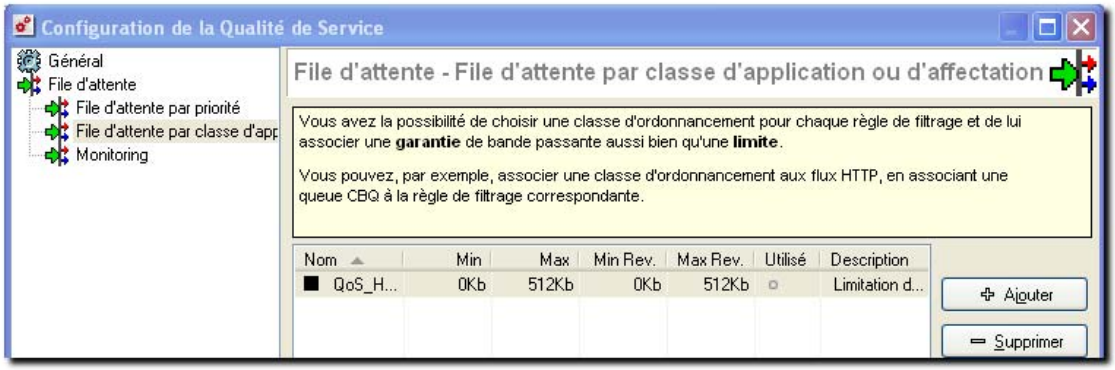


Figure 189 : QoS pour le HTTP

Utilisation de la règle de QoS dans la politique de filtrage

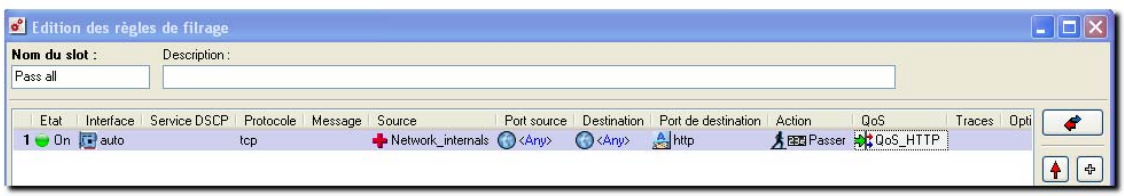


Figure 190 : Règle de QoS dans la politique de filtrage

Effets sur le trafic

- Diminution du risque de congestion du réseau.
- Réduction de l'impact du trafic sur les performances générales du réseau.

Exemple 3 : Garantie d'un niveau e service minimum

Certaines applications (VoIP par exemple) nécessitent un niveau de services avec la garantie que ce niveau de services sera respecté sous peine de disfonctionnement du service (impossibilité de suivre une conversation VoIP par exemple). Les autres applications et leur impact sur les performances générales du réseau peuvent perturber l'obtention du niveau de services requis.
Pour s'assurer que le niveau de services requis sera maintenu il est recommandé de créer une règle de QoS de type "classe d'application ou d'affectation" (CBQ) définissant un débit minimum garanti. Elle permettra de garantir un niveau de service pour un trafic donné indépendamment de l'impact des autres trafics sur les performances globales du réseau et sans définir de limitation de bande passante pour ces autres trafics.

Définition de la règle de QoS pour la VoIP

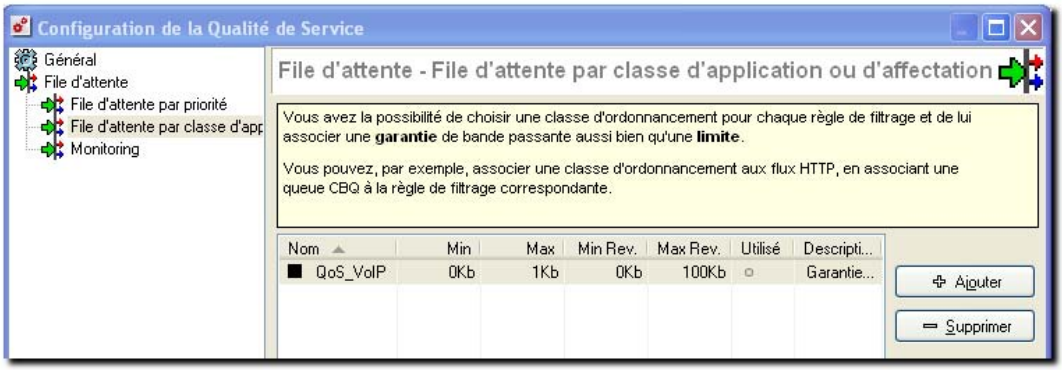


Figure 191 : Règle de QoS pour la VoIP

Utilisation de la règle de QoS dans la politique de filtrage

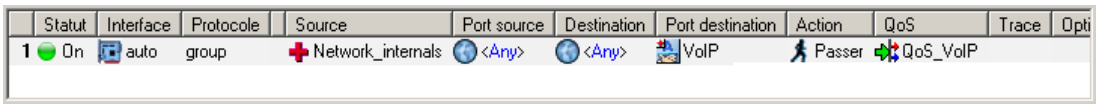


Figure 192 : QoS dans la politique de filtrage

Effets sur le trafic

- Garantie d'un niveau de service pour un trafic donné.
- Introduction d'un délai maximal de transfert des données du service.

PARTIE 8 : VPN

CHAPITRE 1. PRESENTATION

8.1.1. Qu'est ce que le VPN ?

DEFINITION

Les Réseaux Privés Virtuels ou RPV (*VPN : Virtual Private Network*) permettent la transmission sûre de données sensibles au travers d'un média non sûr tel que peut l'être l'Internet. Cette transmission sûre est assurée par des mécanismes de chiffrement et d'authentification de l'ensemble de la communication entre ce que l'on appelle les correspondants VPN.

8.1.2. Technologies VPN intégrées sur le firewall

Les firewalls NETASQ possèdent trois technologies pour assurer ses fonctionnalités VPN. Ces trois technologies correspondent à une utilisation spécifique du VPN :

- **Tunnels IPSec** : protocole standard, l'IPSEC permet la création de tunnels VPN entre le firewall et un autre firewall ou entre le firewall et des nomades sur lesquels seraient installés des clients VPN.
- **PPTP** : protocole propriétaire Microsoft, permet la création de tunnels VPN entre le firewall et des nomades sur lesquels existe un client PPTP intégré.
- **VPN SSL** : cette dernière technologie permet la création de tunnels VPN entre le firewall et des nomades ou encore le firewall et des postes fixes en interne (par exemple, afin de sécuriser des serveurs web ou des communications e-mail). Mais contrairement aux deux autres technologies, la technologie SSL permet la création de tunnels VPN sans nécessiter l'installation de client VPN sur la machine nomade.

8.1.2.1. Organisation de la section VPN

Pour faciliter la compréhension des fonctionnalités VPN et de leur technologie associée, la section VPN se divise en quatre parties (bien que la partie IPSec soit la plus importante) qui contiennent chacune une introduction à la technologie associée, sa configuration sur le firewall et enfin des exemples de configuration.

CHAPITRE 2 : CLES PRE-PARTAGEES

8.2.1. Introduction

La configuration des clés pré-partagées permet de définir le secret préalablement échangé entre deux correspondants du tunnel VPN IPSec. Chaque clé pré-partagée est définie en fonction d'un correspondant VPN distant et est obligatoire pour des tunnels VPN IPSec dynamiques par clés-pré-partagées.

REMARQUE
Les clés pré-partagées pour les clients mobiles peuvent aussi être indiquées directement dans les fiches LDAP des utilisateurs (*Cf.* *Partie 4/Chapitre 3 : Objets\Utilisateurs*). Dans ce cas, chaque utilisateur aura sa propre clé pré-partagée pour s'authentifier auprès du firewall lors d'un accès distant via VPN.

8.2.2. Présentation de l'interface

Il convient de configurer les clés pré-partagées.

Cette configuration est réalisée dans le menu **VPN\Clés pré-partagées** ou grâce au bouton **Configuration PSK** du menu général de configuration du VPN IPSec.

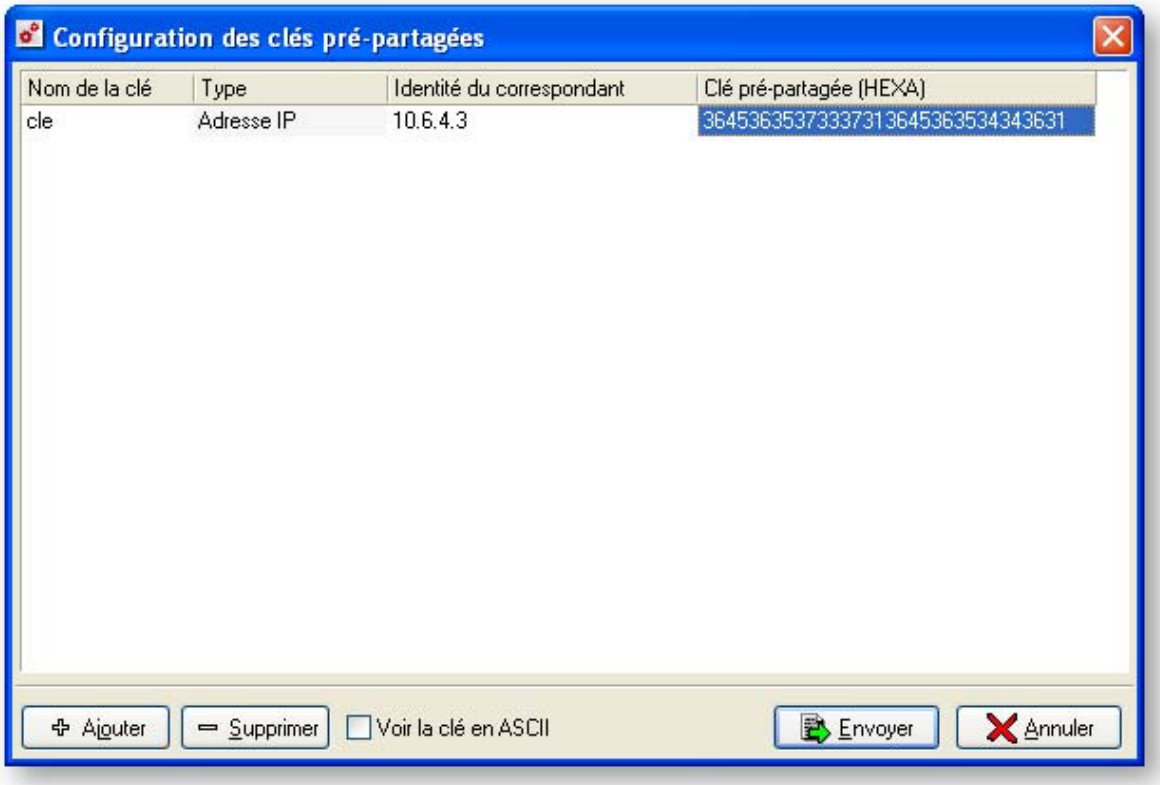


Figure 193 : Configuration des clés pré-partagées

Nom de la clé	Nom que vous affectez à cette clé. Valable pour l'utilisation interne du firewall et pour la gestion des clés de l'utilisateur. Ce nom est unique et sous forme de chaîne de caractères.
Type	Type d'identifiant de la machine distante. Les différentes possibilités sont : • **Nom de domaine non ambigu** : nom de domaine de la machine (ex : firewall.netasq.com) • **utilisateur@Fqdn** (e-mail) : nom de la machine sur un domaine. • **Adresse IP** : la machine distante est identifiée par son adresse IP Il n'y a pas de lien effectué avec un domaine. L'identifiant doit juste être le même sur la machine distante.
Identité du correspondant	Identifiant de la machine distante en fonction du type préalablement sélectionné.
Clé pré-partagée (HEXA)	Valeur de la clé en hexadécimal par défaut.

La création de clés pré-partagées est illimitée.

La suppression d'une clé pré-partagée appartenant à un tunnel VPN IPSec entraîne le dysfonctionnement de ce tunnel.

AVERTISSEMENT
Lors du mode principal la seule identité disponible pour ce tunnel est l'adresse IP.

Les clés ne sont pas liées à une machine (sauf avec l'identité de type adresse IP)* et peuvent être utilisées par plusieurs utilisateurs en même temps.

*Plusieurs machines peuvent avoir la même adresse IP (derrière un NAT par exemple). Cf. Partie 8/Chapitre 3 : Limitation de la fonctionnalité.

CHAPITRE 3 : TUNNELS IPSEC

8.3.1. Introduction

8.3.1.1. Caractéristiques principales d'IPSec

DEFINITION
Le terme IPSec (IP Security) désigne un ensemble de mécanismes de sécurité destiné à garantir une sécurité de haute qualité, basée sur la cryptographie, sans problème d'interopérabilité, pour le trafic au niveau d'IP (IPv4, IPv6). Les services proposés par IPSEC offre le contrôle d'accès, l'intégrité en mode non connecté, l'authentification de l'origine des données, la protection contre le rejeu, la confidentialité au niveau du chiffrement et sur le flux de trafic. Ces services sont offerts par IP ou par d'autres protocoles de couches supérieures. Ainsi IPSEC est indépendant des technologies de la couche Liaison de données (ATM, Frame Relay, Ethernet,...).

Le VPN IPSec permet d'établir un tunnel sécurisé (authentification du correspondant, chiffrement et/ou vérification del'intégrité des données) entre deux machines, entre une machine et un réseau, ou entre deux réseaux en utilisant des associations de négociation (Sas) et la politique de sécurité IPSec (SPD) par le noyau.

Le module VPN IPSec est assuré par une version modifiée de FAST_IPSec qui correspond au module IPSec natif de FreeBSD (http://www.freebsd.org). Il offre notamment un bon support des modules cryptographiques hardware.

Le module VPN doit assurer les fonctionnalités suivantes à partir de son fichier de configuration :

- Mise en place des politiques de sécurité, qui indiquent quels flux peuvent ou doivent être chiffrés.
- Chiffrement et/ou authentification des flux entrants concernés.
- Déchiffrement et/ou authentification des flux entrants concernés.
- Demande de négociation des Associations de sécurité (Security association, SA) quand cela est nécessaire via le protocole ISAKMP.

IPSec utilise deux protocoles pour assurer la sécurité du trafic : "Authentication Header (AH)" et "Encapsulating Security Payload (ESP)". Ces protocoles ont également été conçus pour être indépendants de tout algorithme. Cette modularité permet de sélectionner différents types d'algorithme sans affecter la partie implémentation.

> **Exemple**
> Des communautés différentes d'utilisateurs peuvent sélectionner (ou même créer) différents types d'algorithmes si nécessaire.

Chacun des protocoles ci-dessus supporte deux modes d'utilisation : le "mode transport" et le "mode tunnel". En mode transport, En mode «transport», IPSec protège le contenu du paquet IP. En mode «tunnel», le paquet IP est complètement encapsulé dans un nouveau paquet.

Basé sur la cryptographie, un certain nombre de paramètres de communication doivent être négociés préalablement à l'échange d'information. Ce contexte (algorithmes de chiffrement, clefs, mécanismes sélectionnés…) est réuni au sein d'une SA (Security Association). Le concept de SA fait partie intégrante d'IPSec.

L'IPSEC natif ne supporte pas la translation d'adresses. IPSEC ne permet pas d'établir un tunnel VPN si au moins une des deux extrémités du tunnel possède une adresse translatée (Cf. Partie 8/Chapitre 3 : Support de la fonctionnalité NAT-T).

8.3.1.2. Deux protocoles pour la sécurité du trafic

Authentication Header (AH)

L'entête d'authentification AH (Authentication Header) a été conçu pour assurer l'intégrité en mode non connecté, l'authentification de l'origine des données, et un service anti-rejeu optionnel. Le principe d'AH est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme.

Encapsulating Security Payload (ESP)

Le protocole ESP (Encapsulating Security Payload) a, lui, été conçu pour assurer la confidentialité des données. Mais il peut aussi apporter des services d'intégrité en mode non connecté, d'authentification de l'origine des données, et un service anti-rejeu optionnel. Le principe d'ESP est de déchiffrer (et éventuellement d'assurer l'intégrité) des données (y compris l'en-tête IP du paquet d'origine si on est en mode tunnel).

AVERTISSEMENT

Seul le protocole ESP en mode tunnel est supporté par le firewall NETASQ.

8.3.1.3. Modes d'utilisation

Pour chacun des mécanismes de sécurité d'IPSec, il existe deux modes : le "mode transport" et le "mode tunnel".

En "mode transport", seules les données en provenance du protocole de niveau supérieur et transportées par le datagramme IP sont protégées. Ce mode n'est utilisable que sur des équipements terminaux.

En "mode tunnel", l'en-tête IP est également protégé (authentification, intégrité et/ou confidentialité); l'ensemble du paquet est encapsulé dans un nouveau paquet IP (donc, avec un nouvel en-tête IP). Ce nouvel en-tête sert à transporter le paquet jusqu'à la fin du tunnel, où l'en-tête original est rétabli. Le mode tunnel est utilisable soit sur des équipements terminaux soit au niveau de passerelles de sécurité. Ce mode permet d'assurer une protection plus importante contre l'analyse du trafic.

Les exemples suivants montrent dans le cas de l'ESP (Encapsulating Security Payload) les différences entre les deux modes d'utilisation.

AVERTISSEMENT
Seul le protocole ESP en mode tunnel est supporté par le firewall NETASQ.

ESP "mode transport"

Protection de bout en bout (adresses sources et destination non modifiées)

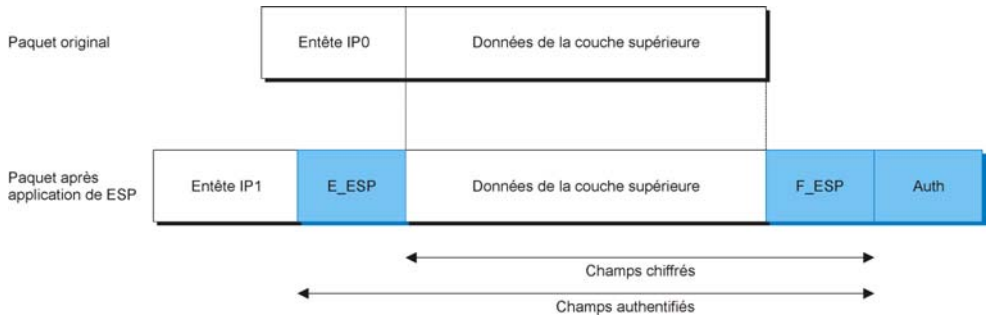


Figure 194 : ESP « mode transport »

ESP "mode tunnel"

A utiliser pour protéger le trafic entre deux éléments de coupure.

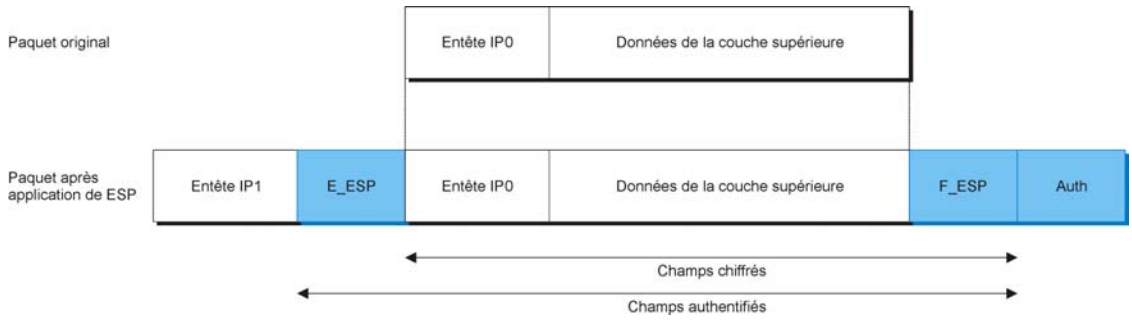


Figure 195 : ESP "mode tunnel"

8.3.1.4. Le choix de NETASQ

Comme indiqué ci-dessus, les fonctionnalités d'un firewall NETASQ implémentent uniquement le protocole ESP d'IPSec pour fournir des services d'authentification et de chiffrement des datagrammes échangés avec un correspondant VPN (qui peut être éventuellement un autre firewall), possédant des fonctionnalités homologuées.

De plus un firewall NETASQ met en œuvre le protocole ESP uniquement en "mode tunnel". Cela implique que les fonctions de chiffrement ne peuvent pas être mises en œuvre de bout en bout, mais uniquement sur une portion du réseau qui supporte le flux, physiquement délimitée par les correspondants VPN, typiquement le réseau dit "Untrusted" (non sûr). Sur cette portion les datagrammes IP à protéger sont intégralement chiffrés, signés et encapsulés dans des datagrammes ESP dont les adresses IP source et destination sont celles des correspondants VPN. Ainsi les adresses IP des machines réelles d'extrémité du flux sont inaccessibles à des attaquants à l'écoute sur le réseau non sûr. Les correspondants VPN sont appelés extrémités du tunnel, par opposition aux machines réelles d'extrémité du flux, situées "derrière" les correspondants VPN du point de vue réseau non sûr et qu'on appelle les extrémités de trafic.
Le fait d'avoir privilégié le protocole ESP en "mode tunnel" est basé sur deux constats.

Schématiquement on peut associer le "mode transport" à une utilisation dite "host to host" un trafic de bout en bout, d'une machine unique vers une machine unique. Tandis que le "mode tunnel" est plutôt utilisé dans un cadre dit "network to network" c'est à dire un groupe de machines vers un groupe de machines. Cette configuration correspond plus au type d'architecture rencontrée dans le cadre de l'utilisation d'un firewall, étant donné qu'un firewall est généralement utilisé pour protéger un réseau. Ainsi NETASQ privilégiera le "mode tunnel".

De plus on peut imaginer dans une certaine mesure que le "mode transport" soit en réalité un cas d'utilisation du "mode tunnel" (les extrémités de tunnel et de trafic sont confondues). Mais ce cas n'est pas supporté sur un firewall NETASQ.

Etant donné que NETASQ a choisi de n'implémenter que le mode tunnel sur son firewall, les développements sur l'**AH (Authentication Header**) ont été interrompu. En effet dans le cadre du mode tunnel seules trois informations "sensibles" nécessiterait le besoin d'une authentification : les adresses source et destination et l'index de sécurité (SPI : Security Policy Identifier) de la SA (Security Association) associée. Hors ces informations sont indispensables au fonctionnement de la politique VPN. La modification d'un de ces paramètres entraîne irrémédiablement le rejet du paquet par le correspondant. L'utilisation d'AH dans le cadre du mode tunnel devient alors inutile par rapport ESP.

8.3.1.5. Différentes phases

Dans le cadre d'ESP (AH aussi d'ailleurs mais seul ESP nous intéresse dans le cadre d'un firewall NETASQ), chaque datagramme échangé entre deux correspondants VPN donnés est rattaché à une connexion simplex ou unidirectionnelle (en fonction du point de vue elle est donc soit entrante soit sortante) mettant en œuvre des services de sécurité, appelée Association de Sécurité IPSec (SA : Security Association). Une SA IPSec spécifie les algorithmes de chiffrement et d'authentification à appliquer sur les datagrammes qu'elle couvre, ainsi que les clés secrètes associées.

Le déploiement et l'utilisation massive d'IPSec exige un protocole de gestion des SA standard sur Internet, extensible et automatisé. Par défaut, le protocole de gestion automatisée des clefs choisi pour IPSec est IKE. IKE est organisé autour de 2 phases de négociation.

La phase 1 du protocole IKE vise à établir un canal de communication chiffré et authentifié entre les deux correspondants VPN. Ce "canal" est appelé SA ISAKMP (différent de la SA IPSec). Deux modes de négociations sont possibles : le mode principal et le mode agressif.

La phase 2 du protocole IKE négocie de manière sécurisée (au moyen du canal de communication SA ISAKMP négocié dans la première phase) les paramètres des futures SA IPSec (une entrante et une sortante).

Phase 1 du protocole IKE

La phase 1 du protocole **IKE** concourt à trois objectifs :

- La négociation des paramètres SA ISAKMP (une entrante et une sortante).
- L'élaboration des clés secrètes d'authentification, de chiffrement et de dérivation de la SA ISAKMP.
- L'authentification mutuelle des correspondants VPN.

Dans le cadre d'un firewall NETASQ, les fonctions d'établissement de SA n'acceptent des négociations de SA ISAKMP qu'avec des correspondants VPN pour lesquels un tunnel est défini dans le slot de chiffrement courant et ce sur l'interface réseau spécifiée pour ce tunnel.

Le diagramme suivant représente les étapes de la négociation en mode principal par certificat x509.

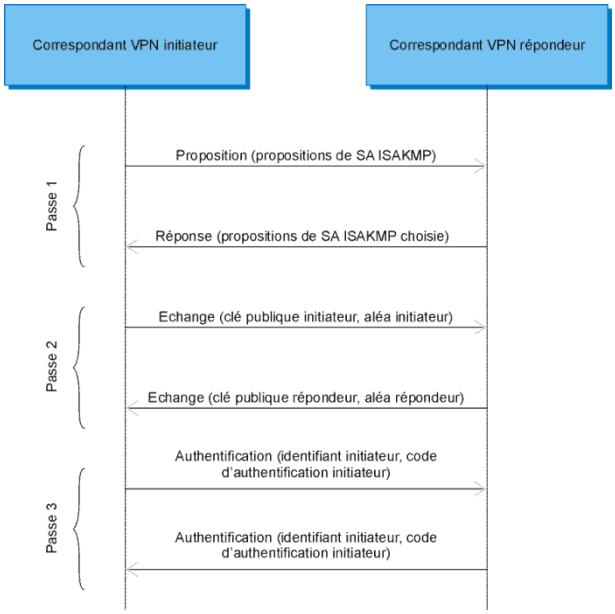


Figure 196 : Négociation en mode principal

La passe 1 correspond à la négociation de la SA ISAKMP. Chaque règle de chiffrement possède une liste de propositions de SA ISAKMP qui sont des quintuplés de la forme (durée de vie de la SA, algorithme d'authentification, taille de clé d'authentification, algorithme de chiffrement, taille de clé de chiffrement).

La passe 2 permet d'élaborer un secret partagé, dont on dérive la clé secrète d'authentification et la clé secrète de chiffrement de la SA ISAKMP, utilisables par les services négociés en passe 1.

La passe 3, protégée par les services d'authentification et de chiffrement, permet l'authentification mutuelle des correspondants VPN. Le code d'authentification de chaque correspondant VPN est généré à partir de la clé pré-partagée, du secret partagé, des aléas et de l'identifiant du correspondant VPN.

D'autres modes de négociation et méthodes d'authentification sont supportés par le firewall : mode agressif ou mode principal et authentification par clés pré-partagées ou par certificat X509.

Mode agressif

Le mode agressif s'effectue en trois étapes :

Etape 1
Cette étape combine la proposition, l'échange de clé initiateur et l'envoi de l'identification de l'initiateur.

Etape 2
Cette étape combine la réponse, l'échange de clé répondeur et l'authentification du répondeur.

Etape 3
Cette étape consiste pour l'initiateur à envoyer son code d'authentification.

Phase 2 du protocole IKE

L'établissement d'une paire de SA IPSec entre deux correspondants VPN nécessite une phase de négociation des paramètres et d'établissement des clés afin d'assurer que les deux extrémités du tunnel appliquent la règle de chiffrement associée à la SA IPSec de manière cohérente. La négociation des SA IPSec est basée sur la phase 2 (Quick mode) du protocole IKE. De manière simplifiée, les étapes de cette négociation peuvent être représentées par le diagramme de séquence suivant.

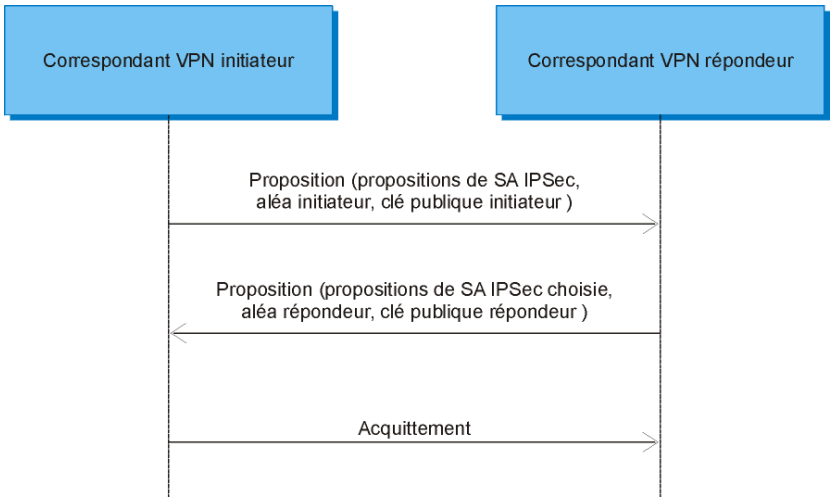


Figure 197 : Négociation - Phase 2

Tous les échanges sont chiffrés et authentifiés par les services fournis par la SA ISAKMP, négociée et établie entre les correspondants VPN préalablement à l'établissement des SA IPSec associées aux règles de chiffrement.

Chaque règle de chiffrement possède une liste de propositions de SA IPSec qui sont des quintuplés de la même forme que pour la négociation des SA ISAKMP.

Lors de la deuxième étape de la phase 2 du protocole IKE, le répondeur doit choisir et recopier dans sa réponse une des propositions qui lui a été soumise, sinon l'initiateur refuse la négociation. En situation de répondeur, le firewall NETASQ applique les règles suivantes pour sélectionner la réponse :

- La réponse choisie est la première qui correspond à la stratégie de négociation spécifiée au niveau du tunnel.
- La stratégie de négociation peut être "exacte", "stricte", "Claim" ou "Obey". En cas de stratégie exacte, une proposition de l'initiateur correspond à une proposition locale si elle lui est exactement égale. En cas de stratégie stricte, une proposition de l'initiateur correspond à une proposition locale si elle lui est égale ou supérieure. En cas de stratégie "Claim", une proposition de l'initiateur correspond à une proposition locale si elle lui est égale ou supérieure. Cependant si la durée de vie est plus courte, il est possible, via un message spécifique, d'imposer sa propre durée de vie). En cas de stratégie " Obey", la première proposition du correspondant est acceptée.

Une proposition de l'initiateur est égale ou supérieure à une proposition locale si les conditions du tableau ci-dessous sont réalisées :

Attrib. de la proposition initiateur	Relation	Attrib. de la proposition locale
Durée de vie	≤	Durée de vie
Algorithme d'authentification	=	Algorithme d'authentification
Taille de clé d'authentification	≥	Taille de clé d'authentification
Algorithme de chiffrement	=	Algorithme de chiffrement
Taille de clé de chiffrement	≥	Taille de clé de chiffrement
Perfect Forward Secrecy	≥	Perfect Forward Secrecy

En cas de stratégie stricte, il peut donc arriver que les attributs d'une SA soient différents de ceux des propositions locales associées à la règle de chiffrement utilisant la SA.

Suite à la réussite de la négociation, les clés d'authentification et de chiffrement sont élaborées à partir des clés publiques (secret partagé Diffie-Hellman), des aléas et des autres paramètres échangés lors de la phase 2, ainsi que d'une clé secrète de dérivation élaborée lors de la phase 1, hormis si le PFS est activé : dans ce cas, on regénère un secret partagé via Diffie Helmann.

8.3.1.6. Certificats X509

La solution du firewall NETASQ supporte et utilise deux méthodes d'authentification : les clés pré-partagées et les certificats X509. Les deux méthodes possèdent le même niveau de sécurité mais leur gestion est différente. Cette distinction est abordée dans la configuration des politiques VPN (*cf. Création d'un tunnel VPN*).

Cette section se focalise sur l'authentification des correspondants VPN par certificat.

Elle n'a pas pour vocation d'offrir une explication complète ou exhaustive des infrastructures à clé publique, mais d'expliquer la configuration ISAKMP par certificats dans un firewall NETASQ.

Génération des certificats

Un firewall NETASQ contient une infrastructure à clé publique interne qui vous permet de créer les certificats des utilisateurs de votre système d'information mais il peut aussi intégrer les fichiers générés par une PKI externe privée

> **Exemples**
> OpenSSL, CMS d'iPlanet, Baltimore,... ou officielle (ex: Thawte, Verisign, ...).

La procédure à suivre pour générer des certificats externes se déroule selon des formalités décrites dans les manuels des éditeurs de la solution PKI privée ou sur les sites web des CA officielles.

Les étapes pour la génération d'un certificat local et la configuration d'un firewall sont :

- Génération d'une paire de clés (appelée aussi biclé).
- Importation de la clé privée dans le firewall.
- Envoi d'une requête de demande de certificat (accompagné de la clé publique) à la CA.
- Récupération du certificat auprès de la CA après validation par celle-ci.
- Importation du certificat dans le firewall.
- Récupération et importation du certificat de la CA
- Récupération et importation des certificats des correspondants.

Donc, pour configurer le firewall, il faut importer différents fichiers (trois catégories de certificats, les clés privées et liste de révocation). Chaque fichier contient un des éléments cités ci-dessous.

Clé privée

De la paire de clés générée par la PKI, le firewall doit posséder l'exemplaire privé et public. Le firewall ne génère pas lui même la paire de clés, c'est la PKI qui le fait.

Cette clé privée permettra de signer les informations envoyées.

Cette clé est générée en même temps que la clé publique par l'administrateur en vue de la génération du certificat pour le firewall local.

Certificat de firewall local

Ce certificat est généré pour le firewall local. La clé publique qu'il contient permettra l'authentification avec les firewalls correspondants.

Ces certificats sont générés par l'administrateur pour le firewall local.

Certificats des correspondants

Ces certificats sont générés par les firewalls distants. La clé publique qu'il contient permettra l'authentification des firewalls correspondants.

Ces certificats sont fournis par l'administrateur des firewalls distants.

Certificats des CA

Ils sont générés par les **CA**. La clé publique qu'ils contiennent permettra de vérifier la validité des certificats des firewalls distants (certificats des correspondants) et ceux du firewall local.

Ces certificats sont le plus souvent récupérables, soit dans l'application PKI privée, soit sur le site de la CA officielle.

Liste de révocation

Chaque certificat peut être annulé (révoqué) lorsque des responsables (administrateurs, chefs de services ou d'entreprise, ... selon les cas) décident que tel ou tel certificat n'assure plus ou met en péril la sécurité des transactions. En effet, des certificats peuvent créer des failles de sécurité dans divers cas de figure tels que la perte ou vol de la clé privée, le départ de l'administrateur du firewall ou peuvent être associé à des personnes qui ne sont plus autorisées à accéder à ce système. Les PKI permettent de révoquer des certificats, générer, exporter et publier des listes contenant les certificats révoqués. Cette liste doit être mise à jour automatiquement et périodiquement consultée par le firewall, dans le cas contraire, certaines personnes ou ressources pourraient conserver des accès auxquels elles n'ont plus droit.

Formats reconnus par un firewall NETASQ

- **PEM** (Privacy Enhanced Mail). Il permet l'encodage des certificats X509 en base 64.
- **DER**, format binaire.
- **PKCS#12**.

Pour exemple, un certificat de type PEM se présente de la manière suivante :


```
-----BEGIN CERTIFICATE-----
MIIDdzCCAuCgAwIBAgIBBzANBgkqhkiG9w0BAQQFADCBpDELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAkdFMQ8wDQYD
VQQHEwZHZW5ldmExHTAbBgNVBAoTFFVuaXZlcnNpdHkgb2YgR2VuZXZhMSQwIgYDVQQLExtVTklHRSBDZXJ0aWZpY
2F0ZSBBdXRob3JpdHkxETAPBgNVBAMTCFVuaUdlIENBMR8wHQYJKoZIhvcNAQkBFhB1bmlnZWNhQHVuaWdlLmNoMB
4XDTk5MTAwNDE2MjI1N1oXDTAwMTAwMzE2MjI1N1owgbExCzAJBgNVBAYTAkNIMQswCQYDVQQIEwJHRTEPMA0GA1
UEBxMGR2VuZXZhMR0wGwYDVQQKExRVbml2ZXJzaXR5IG9mIEdlbmV2YTEeMBwGA1UECxMVRGl2aXNpb24gSW5mb
3JtYXRpcXVlMRowGAYDVQQDExFBbGFpbiBIdWdlbnRvYmxlcjEpMCcGCSqGSIb3DQEJARYaQWxhaW4uSHVnZW50b2J
sZXJAdW5pZ2UuY2gwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALIL5oX/FR9ioQHM0aXxfDELkhPKkw8jc6I7BtSY
Jk4sfqvQYqvOMt1uugQGkyIuGhP2djLj6Ju4+KyKKQVvDJIu/R1zFX1kkqOPt/A2pCLkisuH7nDsMbWbep0hDTVNELoKVoVIA
azwWMFIno2JuHJgUcs5hWskg/azqI4d9zy5AgMBAAGjgakwgaYwJQYDVR0RBB4wHIEaQWxhaW4uSHVnZW50b2JsZXJAd
W5pZ2UuY2gwDAYDVR0T200BAUwAwIBADBcBglghkgBhvhCAQ0ETxZNVU5JR0VDQSBjbGllbnQgY2VydGlmaWNhdGUsI
HNlZSBodHRwOi8vdW5pZ2VjYS51bmlnZS5jaCBmb3IgbW9yZSBpbmZvcm1hdGlvbnMwEQYJYIZIAYb4QgEBBAQDAgSwM
A0GCSqGSIb3DQEBBAUAA4GBACQ9Eo67A3UUa6QBBNJYbGhC7zSjXiWySvj6k4az2UqTOCT9mCNnmPR5I3Kxr1GpWT
oH68LvA30inskP9rkZAksPyaZzjT7aL//phV3ViJfreGbVs5tiT/cmigwFLeUWFRvNyT9VUPUov9hGVbCc9x+v05uY7t3UMeZejj8
zHHM+
-----END CERTIFICATE-----
```


Les balises "-----BEGIN CERTIFICATE-----" et "-----END CERTIFICATE-----" encadrent le bloc de "n" lignes de chacune 64 caractères de type [A-Za-z0-9/+].

C'est un format qui transite souvent par e-mail car celui-ci résiste très bien aux déformations des logiciels de messagerie.

Le fichier PEM est un fichier texte contenant ce type d'information.

De même le fichier CRL contient des chaînes de caractères codées en base 64 encadrées par des balises du type : "-----BEGIN X509 CRL-----" et "-----END X509 CRL-----".

Le fichier de clé privée, quant à lui, contient des chaînes de caractères codées en base 64 encadrées par des balises du type : "-----BEGIN RSA PRIVATE KEY-----" et "-----END RSA PRIVATE KEY-----".

8.3.2. Support de la fonctionnalité de NAT-T

Les incompatibilités connues entre la translation d'adresses (NAT : Network Address Translation) et les tunnels VPN (VPN : Virtual Private Network) IPsec entraînent des problèmes souvent bloquants lors de l'établissement de tunnel VPN IPsec au travers d'équipement effectuant des opérations de NAT.

Le NAT-T permet de supporter un trafic VPN transitant au travers de routeur réalisant de la translation d'adresses. Le nombre d'équipements réalisant une translation n'est pas une limite de la fonctionnalité chez NETASQ.

8.3.2.1. Incompatibilités connues entre la translation d'adresses (NAT) et l'IPSec

Ces incompatibilités entre le NAT et l'IPSec peuvent être divisées en trois catégories :

- Les problèmes intrinsèques au NAT. Ces incompatibilités dérivent directement des fonctionnalités de translation d'adresses. Ces incompatibilités seront donc présentes dans tous les équipements fournissant du NAT.
- Les faiblesses d'implémentation du NAT. Ces incompatibilités ne sont pas intrinsèques au NAT, mais sont présentes dans de nombreuses implémentations.
- Les solutions propriétaires. Ces incompatibilités sont présentes dans les équipements NAT qui tentent de fournir des fonctionnalités permettant le passage de l'IPSec au travers du NAT. Ces fonctionnalités créent encore plus d'incompatibilités, étant donné qu'elles ont été développées sur des technologies propriétaires.

Problèmes intrinsèques au NAT

Les incompatibilités entre l'AH IPSec et le NAT

Etant donné que l'entête AH intègre les adresses IP source et destination dans la vérification de l'intégrité des messages, les équipements NAT modifiant les champs d'adresses invalident la vérification de l'intégrité des messages. L'ESP IPSec n'intègre pas les adresses IP source et destination dans sa vérification optionnelle de l'intégrité chiffrée du message, ce problème ne se pose donc pas pour l'ESP.

Incompatibilité entre les sommes de contrôle et le NAT

Les sommes de contrôles TCP et UDP sont dépendantes des adresses IP source et destination par l'intégration de l'entête dans leur calcul. Ainsi, lorsque les sommes de contrôle sont calculées et vérifiées à la réception, ils sont invalidés lors d'un passage au travers d'un équipement NAT.

Ainsi seul, l'IPSec Encapsulating Security Payload (ESP) sera capable de passer au travers d'un équipement NAT si les protocoles TPC/UDP ne sont pas impliqués, ou si les sommes de contrôles ne sont pas calculées ou encore si l'on est en mode tunnel.

Incompatibilité entre les identifiants d'adresses IKE et le NAT

Lorsque les adresses IP sont utilisées comme identifiants dans la phase 1 du protocole **IKE** (Internet Key Exchange), la modification des adresses IP source et destination par le NAT résultera d'une erreur entre les identifiants et les adresses dans les entêtes IP.

Pour éviter d'utiliser les adresses IP comme identifiants de phase 1, les UserID et les FQDN peuvent être utilisés.

Les incompatibilités entre le port source fixé de l'IKE et le NAT

Lorsque de multiples machines derrière un équipement de NAT négocient des SA ISAKMP avec le même correspondant, un mécanisme est nécessaire pour permettre à l'équipement NAT de démultiplexer les paquets IKE entrants provenant du correspondant. Cela est typiquement réalisé par une translation du port source UDP IKE des paquets sortants de l'initiateur. Ainsi les correspondants doivent être capables d'accepter un trafic IKE provenant d'un port différent du port 500 et doivent répondre sur ce port. De plus il est important de faire attention à ce mécanisme pour éviter les comportements imprévisibles durant la renégociation des clés. Si le port source flottant n'est pas utilisé comme port destination pour la renégociation des clés, le NAT sera incapable d'envoyer les paquets renégociés vers la destination correcte.

Les incompatibilités entre la sélection des SPI IPSec et le NAT

Comme le trafic ESP IPSec est chiffré, il est donc opaque au NAT, le NAT est obligé d'utiliser des éléments des entêtes IP et IPSec pour démultiplexer les trafics IPSec entrants. La combinaison de l'adresse IP de destination, le protocole de sécurité (AH/ESP) et le SPI IPSec est typiquement utilisé dans ce but.

Cependant, comme les SPI entrantes et sortantes sont choisis indépendamment, il n'y a aucun moyen pour le NAT de déterminer quel SPI entrant correspond à quel machine de destination simplement en inspectant le trafic sortant. Ainsi lorsque deux machines derrière le NAT tentent de créer des SA IPSec avec la même destination simultanément, il est possible que le NAT délivre les paquets IPSec entrants vers la mauvaise destination.

Les incompatibilités entre les adresses IP embarquées et le NAT

Comme l'intégrité du payload est protégée, toutes les adresses IP incluses dans les paquets IPSec ne peuvent être translatées par un équipement de NAT. Ceci rend ineffective les passerelles de couche applicative (ALG : Application Layer Gateway) implémentées avec du NAT. Les protocoles qui utilisent des adresses IP embarquées incluent FTP, IRC, SNMP, LDAP, H323, SIP, SCTP (de façon optionnelle) et de nombreux jeux. Pour répondre à ce problème, il est nécessaire d'installer l'ALG sur une machine ou une passerelle de sécurité qui puisse traiter le trafic applicatif avant l'encapsulation IPSec et après la désencapsulation IPSec.

Directionnalité implicite du NAT

Les équipements de NAT requièrent souvent un paquet initial sortant pour les traverser dans le but de créer une table de mapping entrant. La directionnalité du protocole interdit l'établissement non sollicité de SA IPSec vers des machines situées derrière un équipement de NAT.

Faiblesses d'implémentation du NAT

L'incapacité à pouvoir traiter les trafics non UDP/TCP

Certaines implémentations du NAT suppriment les trafics non UDP/TCP ou réalisent uniquement une translation d'adresse lorsqu'un seul la machine se situe derrière l'équipement de NAT. De telles implémentations sont donc incapables d'accepter les trafics des protocoles ESP ou AH.

Les timeouts des "sessions" NAT

Les équipements de NAT ne sont pas homogènes dans leur gestion des durées de maintien des "sessions" UDP en l'absence de trafic. Ainsi, même lorsque les paquets IKE sont correctement translatés, les sessions de translation peuvent être prématurément supprimées.

Incapacité à traiter les fragments sortants

La plupart des équipements NAT peuvent fragmenter proprement les paquets IP sortants dans le cas où la taille des paquets IP dépasse le MTU de l'interface sortante. Cependant, une translation correcte des paquets sortants qui sont déjà fragmentés est difficile et la plupart des équipements NAT ne traitent pas correctement ces trafics. Lorsque deux machines génèrent des paquets fragmentés vers la même destination, les identifiants de fragments peuvent se recouvrir. Etant donné que la machine de destination se base sur les identifiants de fragmentation et le décalage des fragments pour le réassemblage, cela peut provoquer une corruption des données.

Incapacité à traiter les fragments entrants

De la même façon que pour les fragments sortants, le morcelage des adresses IP et des entêtes nécessaires à la translation peut nécessiter un réassemblage complet des fragments compliqué par une arrivée désordonnée des fragments.

Les solutions propriétaires

Vérification de l'entête des paquets ISAKMP

Certaines implémentations tentent d'utiliser les cookies **IKE** pour démultiplexer les trafics IKE entrants. Comme avec le démultiplexage basé sur le port source, le démultiplexage basé sur les cookies **IKE** subit les problèmes de la renégociation des clés, étant donné qu'une renégociation des clés en phase 1 n'utilisera typiquement pas les mêmes cookies que le trafic précédent.

Traitement spécifique sur le port 500

Etant donné que certaines implémentations d'IKE sont incapables d'utiliser des ports sources différents du port UDP 500, certains équipements de NAT ne translatent pas les paquets avec un port source UDP 500. Ceci signifie que ces équipements de NAT sont limités à un client IPSec par passerelle de destination, à moins qu'ils n'inspectent les détails de l'entête ISAKMP pour examiner les cookies qui créent le problème noté plus haut.

8.3.2.2. Fonctionnement du NAT-Traversal

La détection du support du NAT-Traversal et la détection du NAT sur le chemin entre deux correspondants IKE se situe dans la phase 1 IKE.

Le NAT-Traversal utilise plusieurs méthodes pour permettre le passage de l'IPSec au travers du NAT. Le changement de port (ou port floating) pour contourner les solutions propriétaires, l'encapsulation de l'ESP dans l'UDP pour permettre la différenciation des correspondants IPSec et de leur trafic et enfin l'envoi régulier de KEEPALIVE permettant la conservation de la session NAT.

Détection du support du NAT-Traversal

La capacité d'une machine à supporter le NAT-Traversal est déterminée par un échange de Payloads Vendor_ID. Les payloads Vendor_ID du NAT-T doivent être envoyés lors du premier échange de paquets de la phase 1 (et ils doivent être reçus par les deux correspondants) pour continuer à utiliser le NAT-T. Un payload pour chaque version du NAT-T supportée sera envoyé. Le contenu de ce payload est un hash MD5 de "RFC 3947", la valeur de ce payload est 4a131c81070358455c5728f20e95452f.

Détection de la présence du NAT

Le NAT-T ne détecte pas seulement la présence du NAT entre deux correspondants **IKE**, mais détecte aussi dans quel sens se trouve le NAT. Localiser l'équipement de NAT est important, étant donné que des "KEEPALIVE" doivent être initiés par le correspondant situé derrière le NAT.

Pour détecter du NAT entre les deux correspondants, il est nécessaire de détecter si l'adresse IP ou le port changent au cours du trajet (cela implique que les destinataires doivent être capables de traiter des paquets **IKE** dont le port source est différent du port 500 habituel).

Les correspondants envoient à leur vis à vis un hash des ports et adresses IP. Si lorsque chacun des correspondants recalculent le hash (à partir des ports et adresses IP qu'ils reçoivent), celui-ci correspond au hash envoyé par leur vis à vis alors il n'y a pas de **NAT** entre eux. Si les hashes ne correspondent pas, alors quelqu'un a translaté l'adresse ou le port. Ce qui signifie que du NAT-Traversal doit être fait pour que les paquets IPSec puissent traverser.

Les hashs sont envoyés comme une série de payloads NAT-D (NAT Discovery) inclus dans le troisième et quatrième paquet du mode principal et dans le second et le troisième paquet du mode agressif.

L'exemple suivant montre un échange de payloads NAT-D en mode principal :

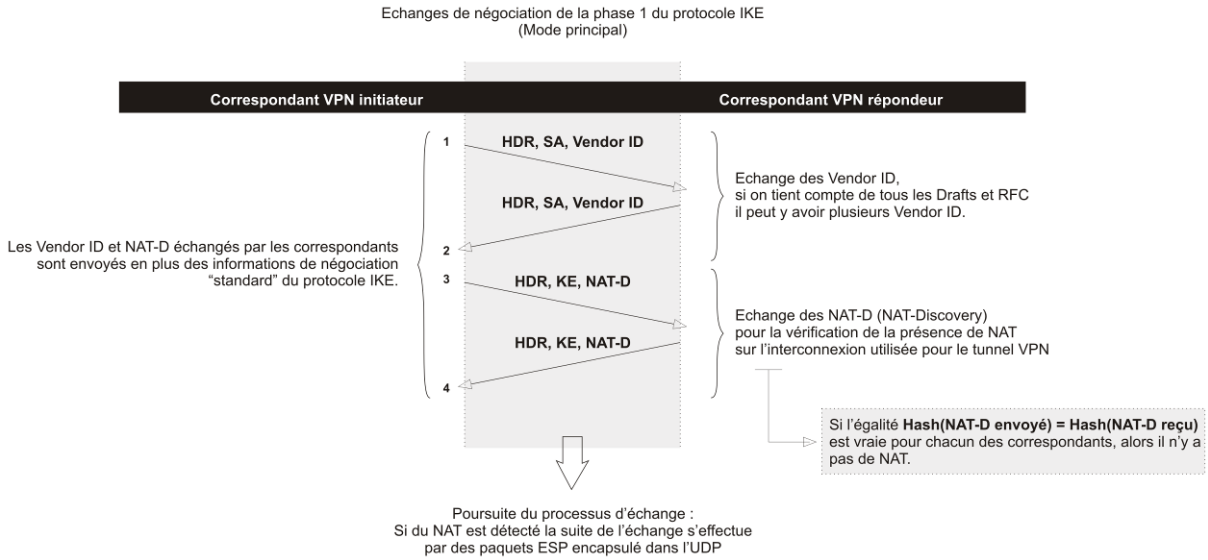


Figure 198 : Payloads NAT-D en mode principal

Le format d'un payload NAT-D est le suivant :

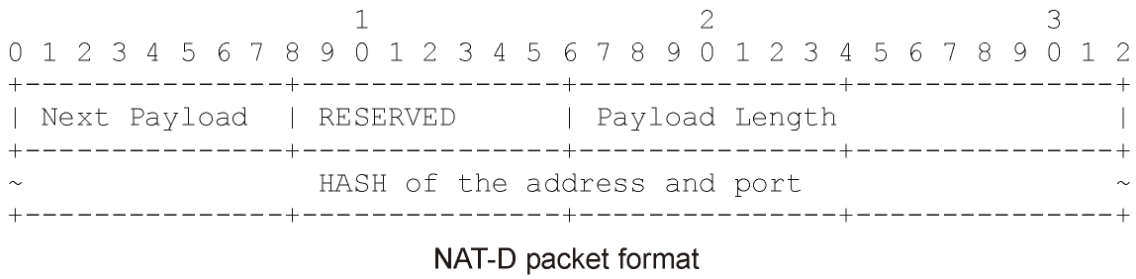


Figure 199 : Payload NAT-D

Le type du payload pour le payload du NAT-D (NAT Discovery) est 20.

Le hash est calculé de la manière suivante : HASH = HASH (CKY-I | CKY-R | IP | Port).

Ceci utilise l'algorithme de HASH précédemment négocié (les hashes sont envoyés dans le troisième et le quatrième paquet, les SA négociant les algorithmes de chiffrement et d'authentification sont envoyés dans le premier et le deuxième paquet). Le premier payload NAT-D contient l'adresse IP et le port de l'extrémité de tunnel distante (c'est-à-dire, l'adresse de destination des paquets UDP). Les payload NAT-D suivant contiennent les adresses IP et ports des différentes extrémités de tunnel locales possibles (c'est-à-dire toutes les sources possibles des paquets UDP).

S'il n'y a pas de NAT entre les correspondants, le premier payload NAT-D reçu par une machine doit correspondre au à un des payloads locaux (c'est-à-dire le payload NAT-D local qu'envoie cette machine à son correspondant), et un des autres payloads NAT-D doit correspondre à l'adresse IP et port du correspondant. Si la première vérification échoue (c'est-à-dire, que le premier des payload NAT-D ne correspond à aucune adresse IP et port local), cela signifie qu'il y a de la translation dynamique entre les correspondants et que cette extrémité de tunnel doit commencer à envoyer des KEEPALIVE (car cette extrémité se trouve derrière un équipement de NAT).

Le CKY-I et CKY-R sont les cookies de l'initiateur et du répondeur. Ils ont été ajoutés au hash pour protéger les adresses IP et port contre les attaques.

Changement vers un nouveau port

Les interactions IPSec et du NAT intelligent peuvent poser des problèmes. Certains équipements de NAT ne changeront pas le port source IKE (500) même s'il y a plusieurs clients derrière le NAT. Ils peuvent aussi utiliser les cookies IKE pour démultiplexer le trafic au lieu d'utiliser le port source. Les deux cas posent le problème de la transparence du NAT, qui engendre des problèmes pour la découverte par IKE des capacités de NAT des équipements traversés par le trafic. La meilleure approche consiste à simplement déplacer le trafic IKE vers un autre port que le 500 le plus vite possible pour éviter ces cas spéciaux de NAT intelligent.

Prenant en compte le cas le plus courant où l'initiateur se trouve derrière un équipement de NAT. L'initiateur doit rapidement changer vers le port UDP 4500 une fois que le NAT a été détecté pour minimiser la fenêtre des problèmes d'interactions IPSec et NAT intelligent.

Lorsque le répondeur reçoit ce paquet, le déchiffrement et les traitements habituels sont effectués sur les différents payloads. S'ils sont effectués avec succès, le répondeur doit mettre à jour sa table locale pour que tous les paquets suivants (les notifications d'informations incluses) à destination du correspondant utilisent le nouveau port et éventuellement la nouvelle adresse IP obtenues du paquet reçu. Le port sera généralement différent, ainsi le NAT effectuera un map UDP (500, 500) vers UDP(x, 500) et UDP (4500, 4500) vers UDP (y, 4500). L'adresse IP sera rarement différente de l'adresse IP précédente. Le répondeur renvoie tous les paquets IKE suivants vers son correspondant en utilisant UDP (4500, y).

De la même façon, si le répondeur doit renégocier la **SA** de phase 1, alors la négociation démarre en utilisant UDP (4500, y). Si une négociation démarre sur le port 4500, alors il n'est pas nécessaire de changer quoique ce soit dans le reste de l'échange.

Voici un exemple d'échange de phase 1 utilisant du NAT-Traversal en mode principal avec un changement de port :

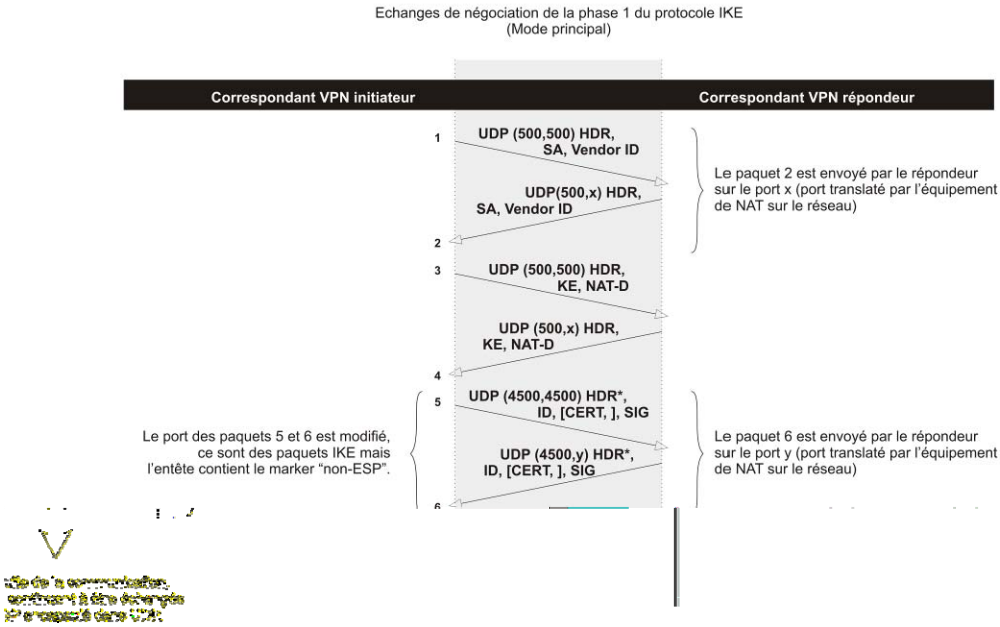


Figure 200 : NAT traversal - Mode principal

Encapsulation du trafic ESP dans l'UDP

Du fait des "incompatibilités entre la sélection des SPI IPSec et le NAT" (explications au début du document), il est indispensable de mettre en place un mécanisme permettant la distinction des différents trafics VPN. L'encapsulation du trafic ESP dans un protocole "plus classique" comme l'UDP permet de créer une certaine concordance entre les différents trafics VPN représentés par leur SPI et un élément de l'entête UDP que les équipements effectuant du NAT sauront traiter, en l'occurrence les ports.

Ainsi dès que la négociation VPN est terminée, l'ensemble du trafic ESP est encapsulé dans l'UDP comme le montrent les différents schémas suivants :

Désormais, plusieurs ports peuvent être utilisés, autres que le 4500 : ce qui permet à plusieurs clients d'une même entreprise de se connecter.

Encapsulation du trafic ESP en mode transport

Paquet avant encapsulation dans l'ESP et l'UDP.

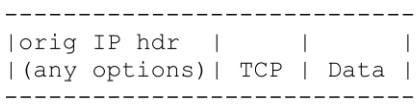


Figure 201 : Avant Encapsulation ESP en mode tranport

Paquet après encapsulation dans l'ESP et l'UDP.

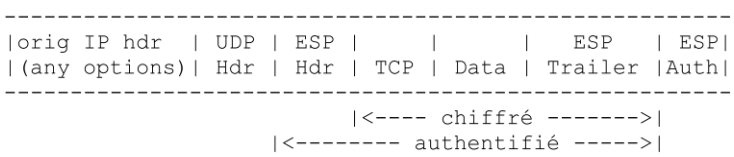


Figure 202 : Après encapsulation en mode transport

Encapsulation du trafic ESP en mode tunnel

Paquet avant encapsulation dans l'ESP et l'UDP.

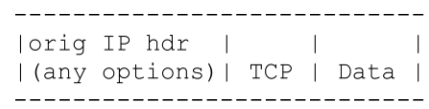


Figure 203 : Avant encapsulation en mode tunnel

Paquet après encapsulation dans l'ESP et l'UDP.

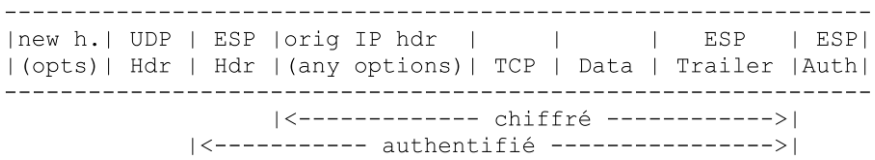
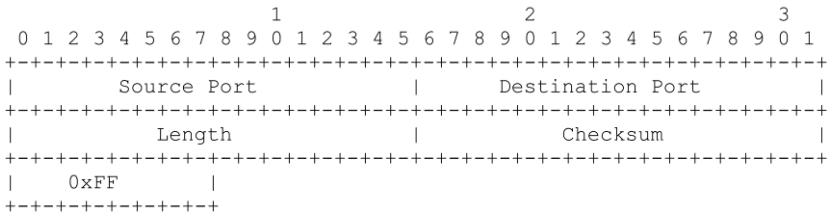


Figure 204 : Après encapulation en mode tunnel

Préservation de la pseudo-session NAT

La stabilité du tunnel VPN IPSec est garantie par la préservation de la session NAT, obtenue grâce à l'envoi régulier de KEEPALIVE entre les deux correspondants VPN. Ainsi la session de NAT est préservée et le port choisi pour la translation reste toujours le même. La renégociation d'un tunnel en fin de durée de vie peut ainsi être initiée par le répondeur sur le port translaté.

Le paquet UDP se présente de la façon suivante :



KEEPALIVE Header Format

Figure 205 : Keepalive

L'entête UDP ci-dessus correspond à un entête standard définit par la RFC 768. Il contient :

- Le port source et le port destination. Ces champs doivent être identiques à ceux utilisés pour l'encapsulation des flux ESP dans l'UDP.
- La somme de contrôle UDP doit être définie à 0.
- Le payload de ce paquet doit être défini à la valeur hexadécimale 0xFF par l'initiateur de la connexion VPN (seul des deux correspondants qui est censé envoyer des KEEPALIVE, bien que dans la pratique certaines solutions permettent au répondeur d'envoyer des KEEPALIVE).

8.3.2.3. Configuration du NAT-T sur l'Appliance UTM NETASQ

Cette fonctionnalité est activée de manière transparente sur les firewalls NETASQ. Si le correspondant VPN supporte la fonctionnalité de NAT-T alors elle sera mise en place si besoin est. Si le correspondant VPN ne supporte pas la fonctionnalité de NAT-T alors la fonctionnalité ne sera pas mise en place.

8.3.2.4. Limitation de la fonctionnalité

La fonctionnalité NAT-T NETASQ supporte désormais les architectures dans lesquelles on retrouve l'utilisation de plusieurs clients VPN mobile derrière une même adresse IP.
Cette fonctionnalité est par exemple utile lorsque plusieurs clients VPN sont utilisés pour contacter un site central depuis la même connexion Internet (dans un hôtel par exemple).

8.3.3. Configuration

Une politique de configuration VPN permet de définir des tunnels VPN.

8.3.3.1. VPN IPSec sur les produits UTM NETASQ

La configuration des tunnels VPN IPSec est accessible par le menu **VPN\Tunnels IPSec** de l'arborescence. La configuration d'un tunnel VPN IPSec s'effectue en trois étapes :

1. La sélection d'un slot de politique VPN
2. La réalisation des premières étapes de configuration grâce à un assistant
3. La fin de la configuration VPN dans le menu de configuration des tunnels VPN IPSec.

8.3.3.2. Sélection d'un slot de politique VPN

Lorsque vous sélectionnez le menu **VPN\Tunnels IPSec** une boîte de dialogue s'affiche, elle vous permet de manipuler les fichiers de configuration associés aux configurations VPN IPSec.

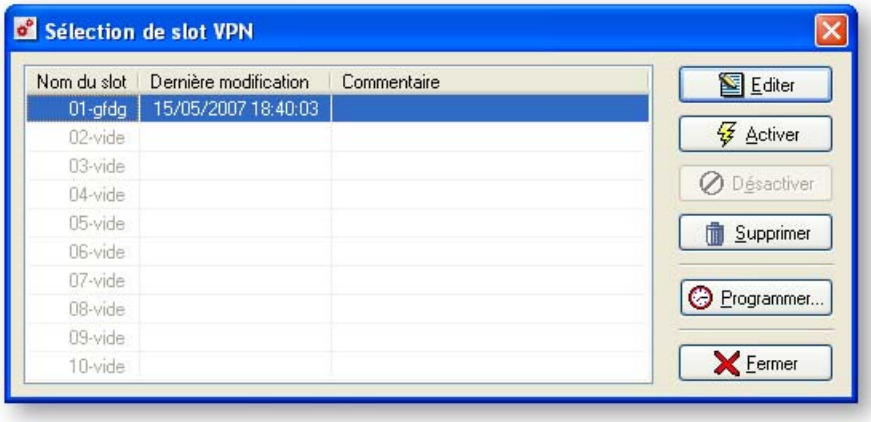


Figure 206 : Sélection de slot VPN

Elle est découpée en deux zones :

- **Gauche** : Liste des fichiers de configuration.
- **Droite** : Actions sur le fichier sélectionné.

> **NOTE**
> Le principe de fonctionnement de cet écran est identique au fonctionnement des écrans de NAT et de Filtrage.

Liste des fichiers de configuration

Dans cette partie de la boîte de dialogue se trouve la liste des fichiers de configuration. Il en existe 10, numérotés de 01 à 10.

Chaque fichier de configuration possède un nom, une date/heure de mise en activité et la date de dernière modification effectuée sur ce fichier de configuration.

L'activation contient l'heure et le/les jours d'activation du fichier. Les jours sont repérés par le numéro du jour dans la semaine (1=lundi). (Cf. Partie 7/Chapitre 3 : Programmateur de slots).

Le fichier de configuration en cours d'activité est indiqué par une petite flèche verte à gauche de son nom. Un fichier de configuration est dit "en activité" lorsque les paramètres qu'il contient sont en service. Il ne peut y avoir plus d'un fichier de configuration en activité car les paramètres du dernier fichier de configuration activé écrasent ceux du fichier de configuration activé précédemment.

Si vous modifiez un fichier de configuration, vous devez le réactiver pour prendre en compte les modifications. Un fichier de configuration modifié mais non réactivé est notifié par l'icône à la place de la flèche verte habituelle.

Il est possible qu'il n'y ait aucun fichier de configuration en activité, cela implique qu'aucun tunnel VPN n'est actif.

Chaque fichier de configuration ne doit pas obligatoirement contenir des paramètres.

Un fichier de configuration pour lequel il n'existe pas de fichier de configuration sur le firewall NETASQ est affiché sous le nom "vide" dans la liste.

Un fichier de configuration est dit sélectionné quand vous faites un simple clic de la souris sur son nom. La sélection faite, vous pouvez l'éditer ou l'activer.

Actions sur le fichier de configuration sélectionné

NOTE

Le principe de fonctionnement de ces boutons d'actions est identique au fonctionnement des boutons de NAT et de filtrage.

8.3.3.3. Assistant de configuration des tunnels VPN IPSec

Lorsque le slot de politique choisi est vide, les premières étapes de configuration d'un tunnel VPN IPSEC s'effectue grâce à un assistant de configuration en cinq étapes.

Etape 1 : Bienvenue

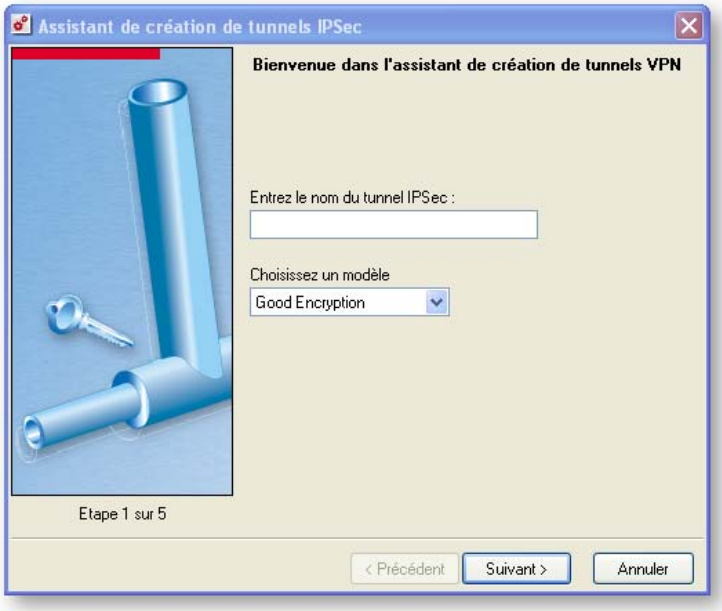


Figure 207 : Création de tunnels IPSec - Etape 1

L'étape 1 de la configuration permet de définir le nom qui sera associé à la politique VPN et le modèle de protection qui sera appliqué. Un modèle de type "Strong encryption (slow)" permettra la mise en place de tunnels VPN IPSec plus sécurisé mais cependant plus lent qu'un modèle de type "Fast encryption (weak)" (meilleurs algorithmes de chiffrement et d'authentification). Le modèle « Bypass » sert à gérer les exclusions IPSec, c'est-à-dire l'exclusion de toute machine ou réseau qu'on ne souhaite pas chiffrer vers une autre machine ou réseau distant.

Le modèle de protection définit des algorithmes de chiffrement et d'authentification qui peuvent être modifiés dans la suite de la configuration. NETASQ recommande donc de laisser cette option à sa valeur par défaut (à savoir "Good encryption") puis de modifier ce modèle si besoin est.

Etape 2 : Choix du type de tunnel

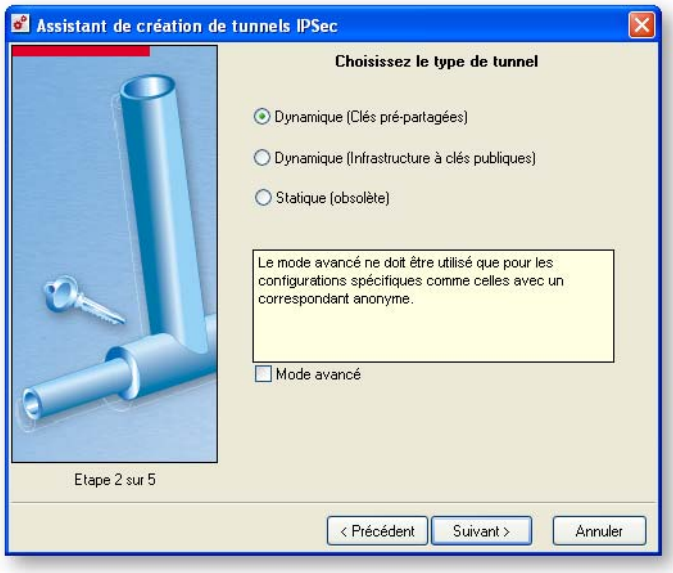


Figure 208 : Création de tunnels IPSec - Etape 2

L'étape 2 de l'assistant est consacrée à la définition du type de tunnel qui est configuré. Trois choix sont proposés. Deux types de tunnels sont basés sur une négociation dynamique des paramètres des tunnels VPN (clé de chiffrement) grâce au protocole IKE, ils diffèrent par le mode d'authentification (clés pré-partagées ou certificats). Notez que le mode "Statique (obsolète)" est obsolète et proposé que par souci d'interopérabilité avec des configurations existantes.
L'option "Mode avancé" est utilisée dans des cas de configuration avancée qui nécessitent l'utilisation de l'objet "any". Ce type de configuration nécessite une connaissance approfondie du fonctionnement des tunnels VPN IPSEC sur les firewalls NETASQ.

Etape 3 : Choix des extrémités du tunnel

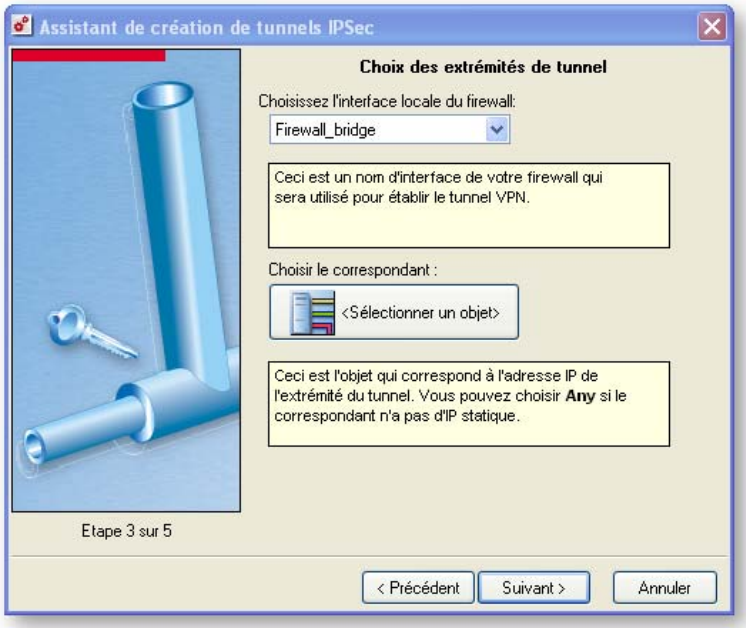


Figure 209 : Création de tunnels IPSec - Etape 3

L'étape 3 vous demande de définir les extrémités de tunnel. On nomme par extrémités de tunnel, les deux équipements entre lesquels le tunnel est créé et donc les communications chiffrées.

L'interface locale fait référence à l'interface concernée par le tunnel sur votre firewall. Par exemple "Firewall_out", interface externe du firewall ou "Firewall_dialup" si les connexions VPN parviennent au firewall via un modem configuré dans la partie dialup.

L'interface distante fait référence au correspondant VPN en vis-à-vis de votre firewall. Par exemple l'adresse IP publique connue de votre correspondant VPN. Pour les tunnels VPN nomade (l'adresse IP publique n'est pas connue) on choisira l'objet <any>, toutefois pour une information complète sur ce type de tunnel veuillez vous référer aux exemples de configuration.

Etape 4 : Choix des extrémités de trafic

Figure 210 : Création de tunnels IPSec - Etape 4

L'étape 4, quant à elle, vous demande de définir les extrémités de trafic. On nomme par extrémités de trafic, les deux correspondants réels qui vont communiquer au travers du tunnel VPN IPSEC.

La ou les machines locales font référence aux machines de votre réseau local qui souhaitent communiquer au travers du tunnel VPN. Par exemple "Network_in", votre réseau interne ou "Network_bridge" si vos interfaces internes sont définies en bridge.

La ou les machines distantes font référence aux machines du réseau de votre correspondant VPN. Par exemple l'adresse IP réseau. Pour les tunnels VPN nomade (l'adresse IP publique n'est pas connue) on choisira l'objet "any", toutefois pour une information complète sur ce type de tunnel veuillez-vous référer aux exemples de configuration.

Etape 5

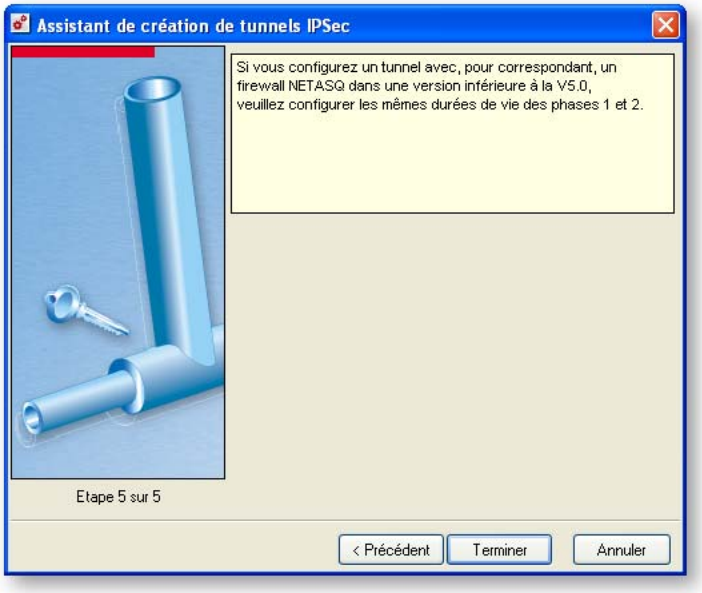


Figure 211 : Création de tunnels IPSec - Etape 5

L'étape 5 vous informe que les durées de vie doivent être compatibles entre la phase 1 et la phase 2 pour une version inférieure à la version 5.0. Sinon, ces durées sont complètement indépendantes.

AVERTISSEMENT

Les valeurs par défaut des durées de vie entre la version 5 et la version 6 on tété modifiées. Autrement dit, le tunnel ne fonctionnera pas avec un firewall en version 6 ou supérieure face à un firewall en version 5, si on se contente d'utiliser l'assistant.

Exemple de configuration en bypass

Pour retirer une machine (ou un réseau) de l'opération de chiffrement, utilisez l'opération « Bypass » (appelée aussi « No encryption »).
L'ordre de configuration des tunnels est important : le tunnel non chiffré doit être le 1er configuré.

AVERTISSEMENT

Pour un tunnel "bypass", vous devez spécifier la machine locale ou réseau qui sera utilisé comme source et qui sera exclu du chiffrement puis l'entité distante ou réseau qui sera utilisé comme destination.

L'exemple suivant montre comment retirer une machine de l'opération de chiffrement

Etape 1 : Bienvenue dans l'assistant de création de tunnels VPN

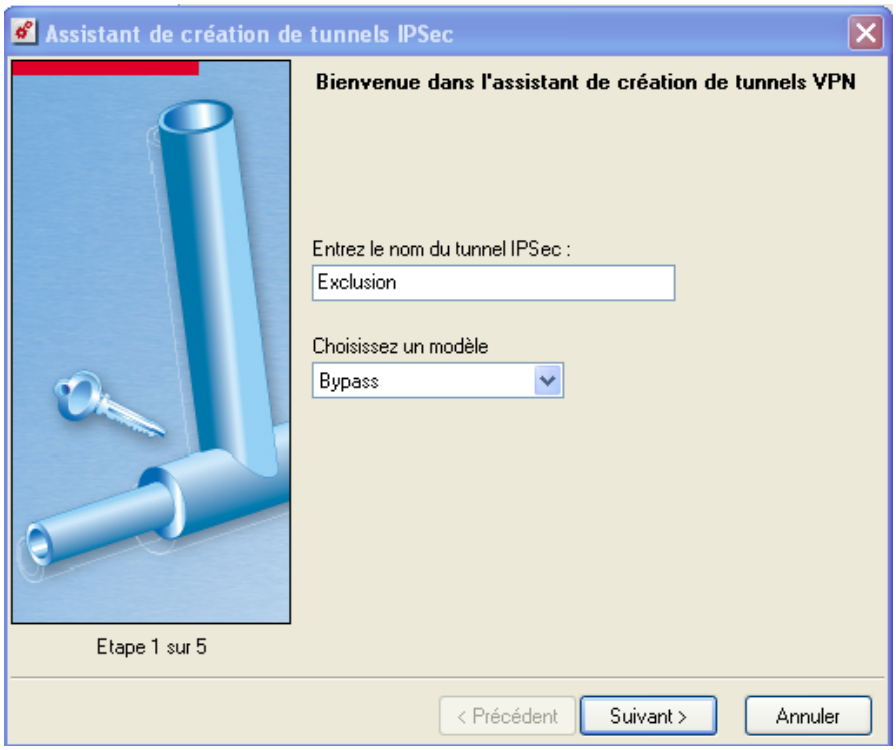


Figure 212 : Configuration IPSec - Etape 1

Donnez un nom au tunnel IPSec puis sélectionnez le modèle « Bypass ».

Etape 2 : Choix des extrêmités du tunnel

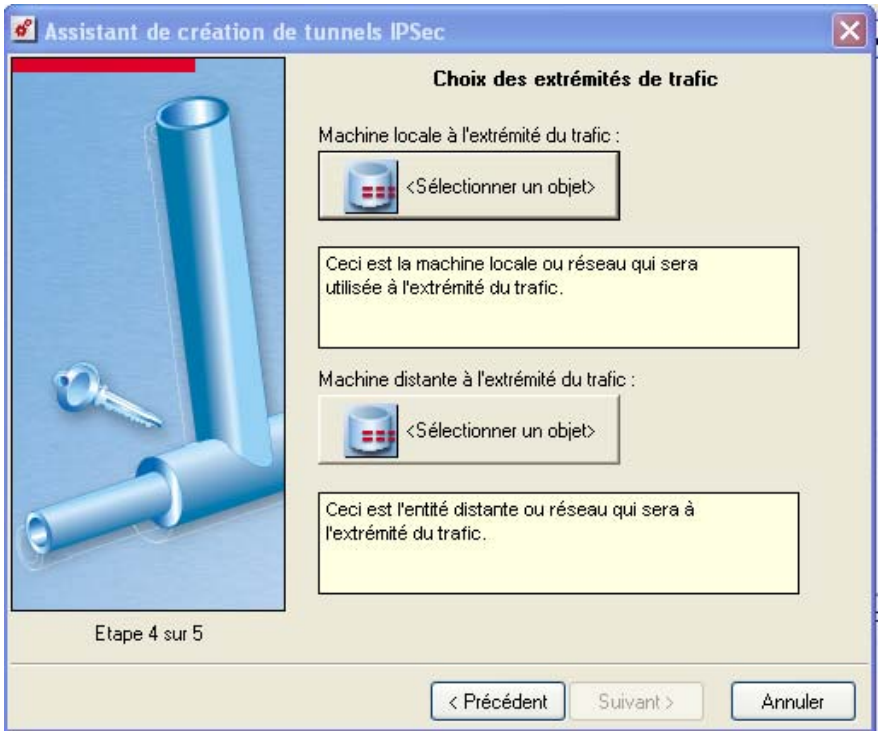


Figure 213 : Tunnel IPSec - Etape 4

Indiquez ici la machine locale ou réseau qui sera utilisée comme source puis l'entité distante ou réseau qui sera utilisée comme destination.

Etape 3 : Ordre des tunnels

Utilisez les flèches au bas de l'écran pour ordonner les tunnels. Les tunnels non chiffrés doivent se trouver en 1er.

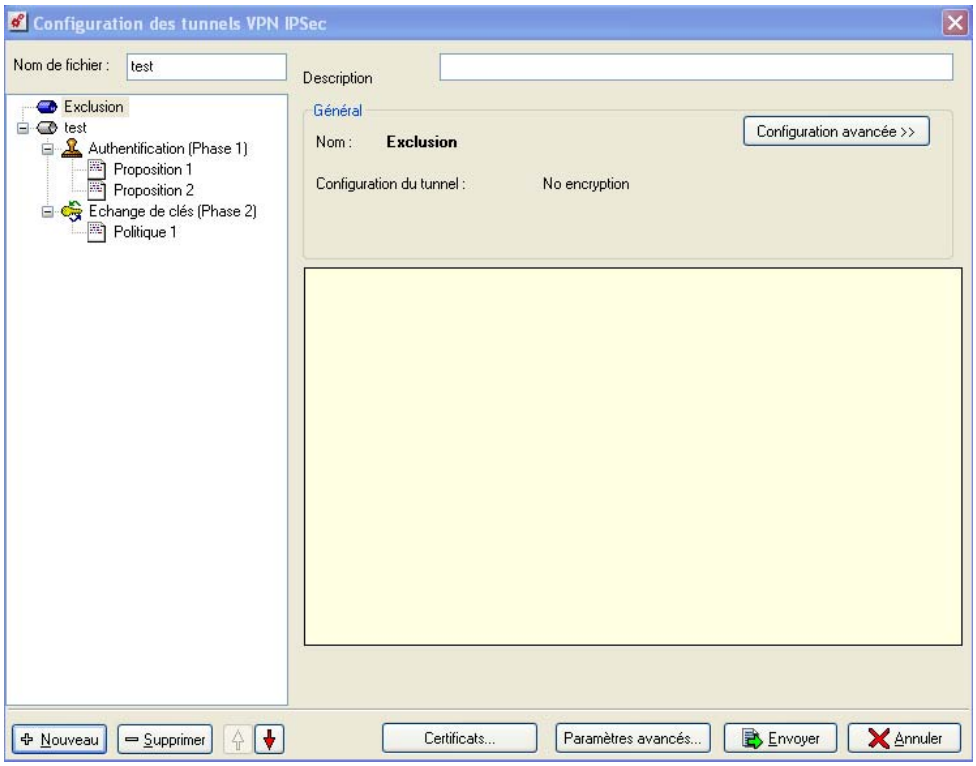


Figure 214 : Tunnel IPSec – Ordre

Menu de configuration des tunnels VPN

En validant la configuration réalisée grâce à l'assistant, le menu de configuration des tunnels VPN IPSec apparaît. Celui-ci regroupe l'ensemble des options nécessaires à la création et à la gestion des paramètres d'une politique VPN.

Notez que si vous sélectionnez un slot de VPN non vide, le menu de configuration des tunnels VPN apparaît automatiquement sans nécessiter de suivre une nouvelle fois les étapes de l'assistant. Pour recommencer l'assistant, sélectionnez un slot "vide" ou supprimez le slot sélectionné. Vous pouvez également sélectionner « Nouveau tunnel ».

Menu contextuel

Lorsque vous effectuez un clic droit sur l'un des tunnels dans l'arborescence, les options suivantes sont proposées :

Ajouter	Cette option vous permet d'ajouter un nouveau tunnel VPN IPSec.
Dupliquer	Cette option vous permet de dupliquer le tunnel VPN IPSec sélectionné.
Supprimer	Cette option vous permet de supprimer le tunnel VPN IPSec sélectionné.
Renommer	Cette option vous permet de renommer le tunnel VPN IPSec sélectionné.
Grouper/Déployer tout	Cette option vous permet de replier/déplier les tunnels IPSEC au niveau de l'arborescence.

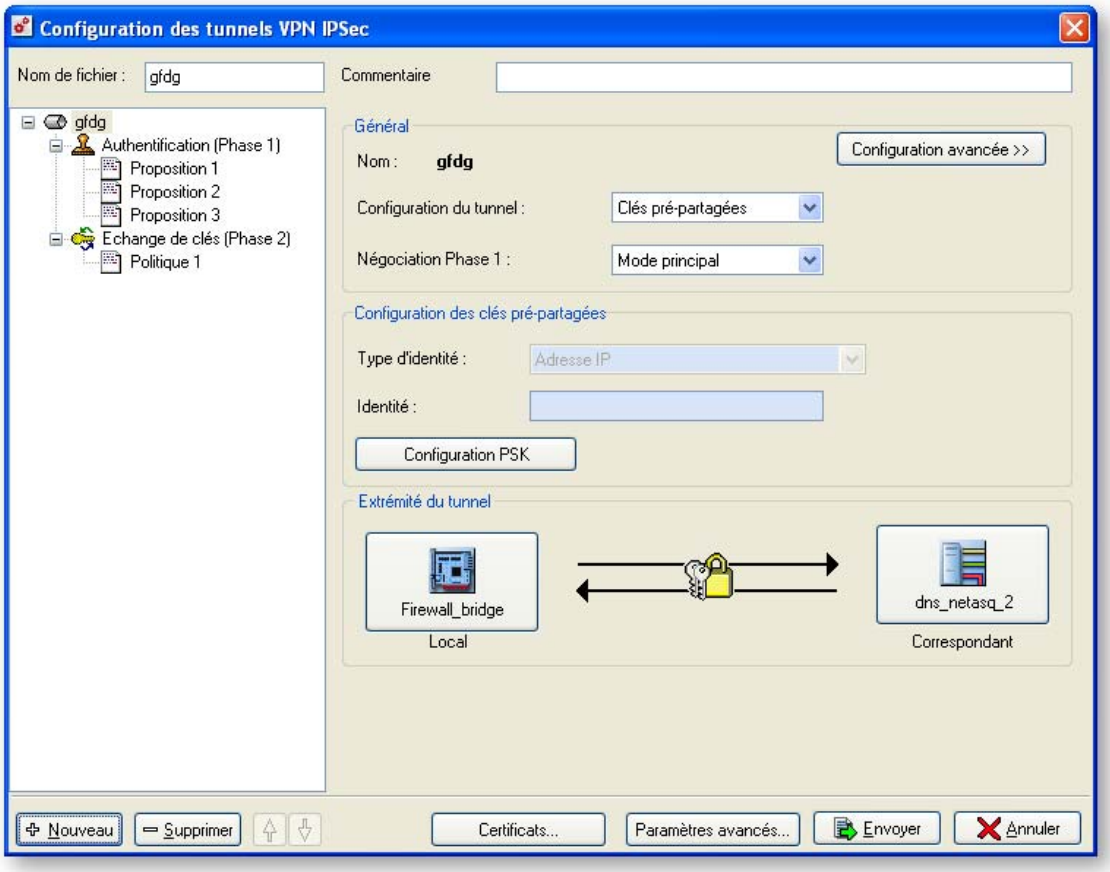


Figure 215 : Configuration des tunnels VPN IPSec

Référez-vous aux sections suivantes pour connaître la signification des différents champs et paramètres.

AVERTISSEMENT

Lorsqu'un slot de configuration VPN est modifié (ajout d'un nouveau tunnel, suppression ou modification d'un tunnel existant), seuls les tunnels directement concernés par les modifications effectuées sont rechargés lors de la réactivation du slot édité et modifié.

8.3.3.4. Menu de configuration des tunnels VPN IPSec

Une politique de tunnels VPN IPSec est définie par un nom (configuré dans l'assistant de configuration). Ce nom est indiqué en haut du menu de configuration des tunnels VPN IPSec. Une description peut aussi être ajoutée.

Paramètres généraux du tunnel VPN IPSEC

Chaque tunnel VPN IPSec dans une politique de tunnel VPN IPSec est aussi défini par son nom. Par défaut ce nom est identique à celui de la politique VPN IPSec. Cliquez sur le nom du tunnel dans l'arborescence des tunnels configurés pour accéder à l'ensemble des paramètres généraux de ce tunnel.

Général

Figure 216 : Configuration des tunnels VPN IPSec - Général

Nom	Le nom du tunnel que vous avez entré au moment de la création du tunnel. Ce nom peut être modifié en cliquant sur le bouton droit de la souris sur le nom du tunnel dans l'arborescence des tunnels configurés.
Configuration du tunnel	Comme dans l'étape 2 cette option définit le type de tunnel VPN IPSec configuré : par clés pré-partagées ou par certificats (PKI).
Négociation phase 1	**Mode principal** : dans ce mode, la phase 1 se déroule en 6 échanges. La machine distante ne peut être identifiée que par son adresse IP avec une authentification en clés pré-partagée. En mode PKI, l'identifiant est dans le certificat. Le mode principal assure l'anonymat. **Mode agressif** : dans ce mode, la phase 1 se déroule en 3 échanges entre le firewall et la machine distante. La machine distante peut être identifiée avec une adresse IP, FQDN ou une adresse mail mais pas avec un certificat par clé pré-partagée. Le mode agressif n'assure pas l'anonymat. **AVERTISSEMENT** L'utilisation du mode agressif + les clés pré-partagées (notamment pour les tunnels VPN à destination de nomades) peut se révéler moins sécuritaire que les autres modes du protocole IPSec. Ainsi NETASQ recommande l'utilisation du mode principal et en particulier du mode principal + certificats pour les tunnels à destination de nomades. En effet la PKI interne du firewall peut tout à fait fournir les certificats nécessaires à une telle utilisation. **REMARQUE** Ce paramètre n'est pas configurable pour les tunnels VPN IPSEC statiques.
Configuration avancée	Ce bouton permet l'accès aux options de configuration avancées.

Configuration des clés pré-partagées

La configuration des clés pré-partagées permet la définition du secret préalablement échangé entre les deux correspondants du tunnel VPN. Chaque clé pré-partagée est définie en fonction d'un correspondant VPN distant et est OBLIGATOIRE pour des tunnels VPN IPSEC dynamiques par clés pré-partagées.

Lorsque le type de tunnel VPN IPSEC sélectionné est dynamique par clés pré-partagées, une section de configuration spécifique apparaît. Cette section permet la définition de l'identité locale de votre firewall, l'identité du correspondant VPN et la clé partagée par les deux correspondants.

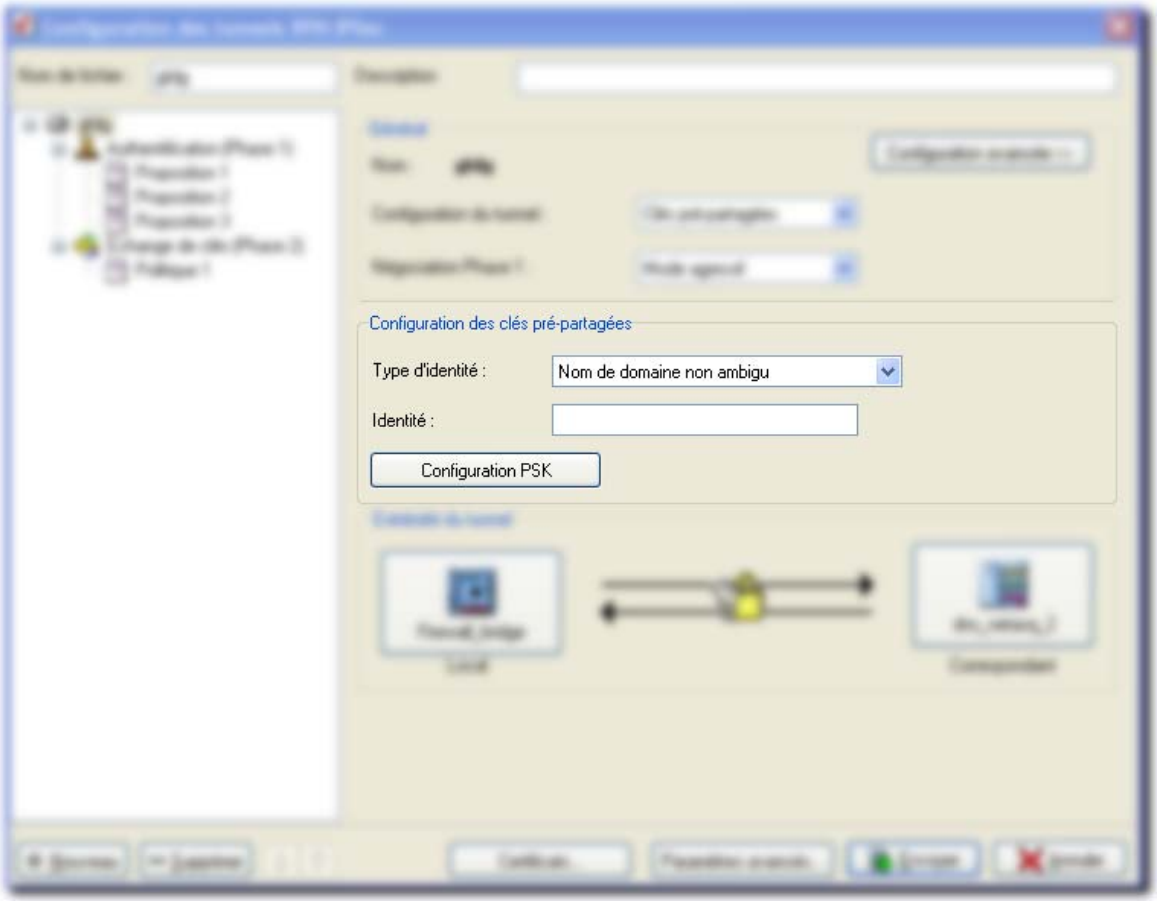


Figure 217 : Configuration des clés pré-partagées

Type d'identité	Le type d'identité permet définir de quelle façon sera identifié votre firewall. Il existe trois types d'identité sur un firewall NETASQ : l'adresse IP publique, le nom de domaine (FQDN : Full Qualified Domain Name) ou l'adresse e-mail (user@fqdn). Le mode principal sélectionne automatiquement le type d'identité "Adresse IP".
Identité	Le champ identité permet définir l'identité de votre firewall. Il s'agit de son identité locale. Par exemple firewall@netasq.com dans le cas d'une identité de type "e-mail". Le type d'identité "Adresse IP" ne nécessite pas de remplir le champ **Identité** car il est automatiquement défini grâce à l'objet choisi pour définir l'extrémité locale de tunnel.
Configuration PSK	Ce bouton permet l'accès aux options de configuration des clés pré-partagées (identité du correspondant distant et une clé unique pour les deux correspondants VPN).

Certificats PKI

Lorsque le type de tunnel VPN IPSec sélectionné est dynamique par certificats (PKI), une section de configuration spécifique apparaît. Cette section permet la définition de l'identité locale de votre firewall (sous la forme d'un certificat), l'identité du correspondant VPN (sous la forme d'un certificat).

Les certificats utilisés dans la configuration d'un tunnel VPN IPSEC avec authentification par certificat sont configurés dans un menu de configuration des certificats.

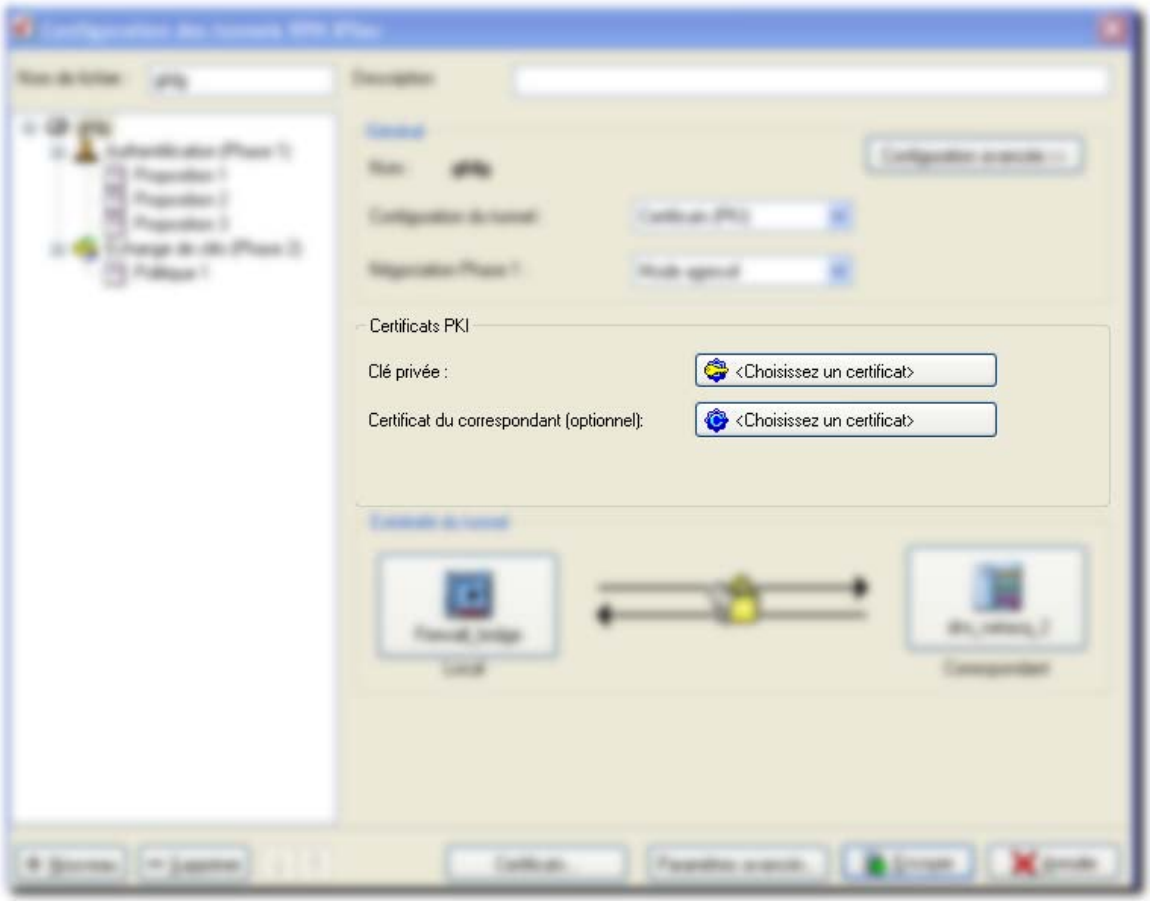


Figure 218 : Certificats PKI

Clé privée	Configuration du certificat du firewall local (une fenêtre s'ouvre sur la liste des certificats locaux disponibles). La clé privée permet de mettre en œuvre les algorithmes de signature électronique, de déchiffrement, d'authentification vis-à-vis d'un tiers.
Certificat du correspondant (optionnel)	Configuration optionnelle du certificat du firewall distant (une fenêtre s'ouvre sur la liste des certificats distants disponibles). **AVERTISSEMENT** Si on définit un certificat pour le correspondant, alors le module IPSec, lors de la phase d'authentification, vérifiera seulement si le certificat du correspondant est le même que celui qu'on a sélectionné, MAIS aucune vérification ne sera faite sur la validité du certificat (expiration, révocation, signature pas l'autorité). Donc la révocation du certificat par la CA n'aura aucun effet. Il est donc fortement déconseillé de spécifier un certificat pour le correspondant, sauf pour des besoins spécifiques.

Extrémités du tunnel

Cette section du menu rappelle les extrémités de tunnel configurées dans l'assistant de configuration. Ces extrémités de tunnel peuvent alors être modifiées en cliquant sur les objets représentant les extrémités locales et distantes (correspondants) du tunnel.

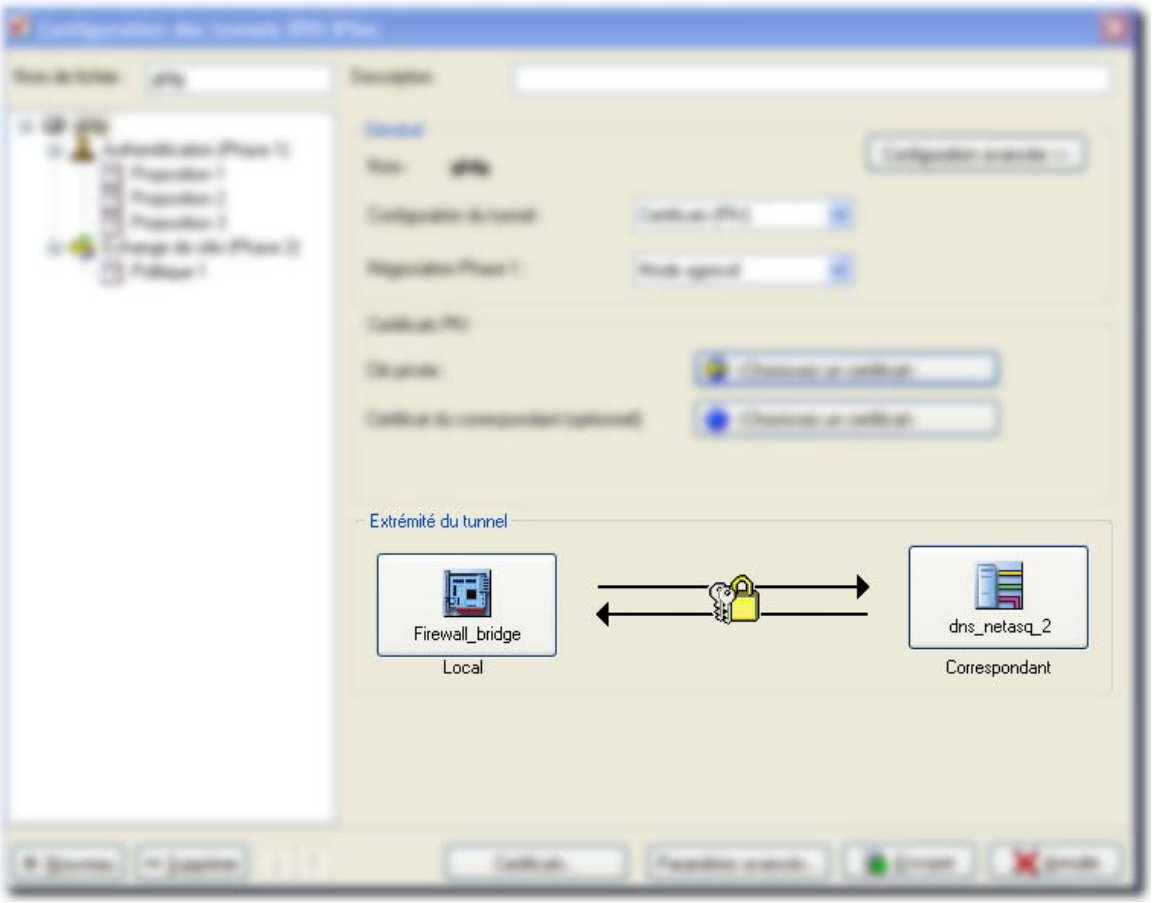


Figure 219 : Extrémité du tunnel

Local	Interface concernée par le tunnel VPN IPSec sur le firewall local.
Correspondant	Adresse IP publique du correspondant VPN distant. Rappel : si cette adresse IP n'est pas connue, l'objet "any" doit être utilisé. Référez-vous aux exemples de configuration avancée de tunnel VPN IPSec pour plus d'informations sur l'utilisation de l'objet "any".

8.3.3.5. Configuration avancée

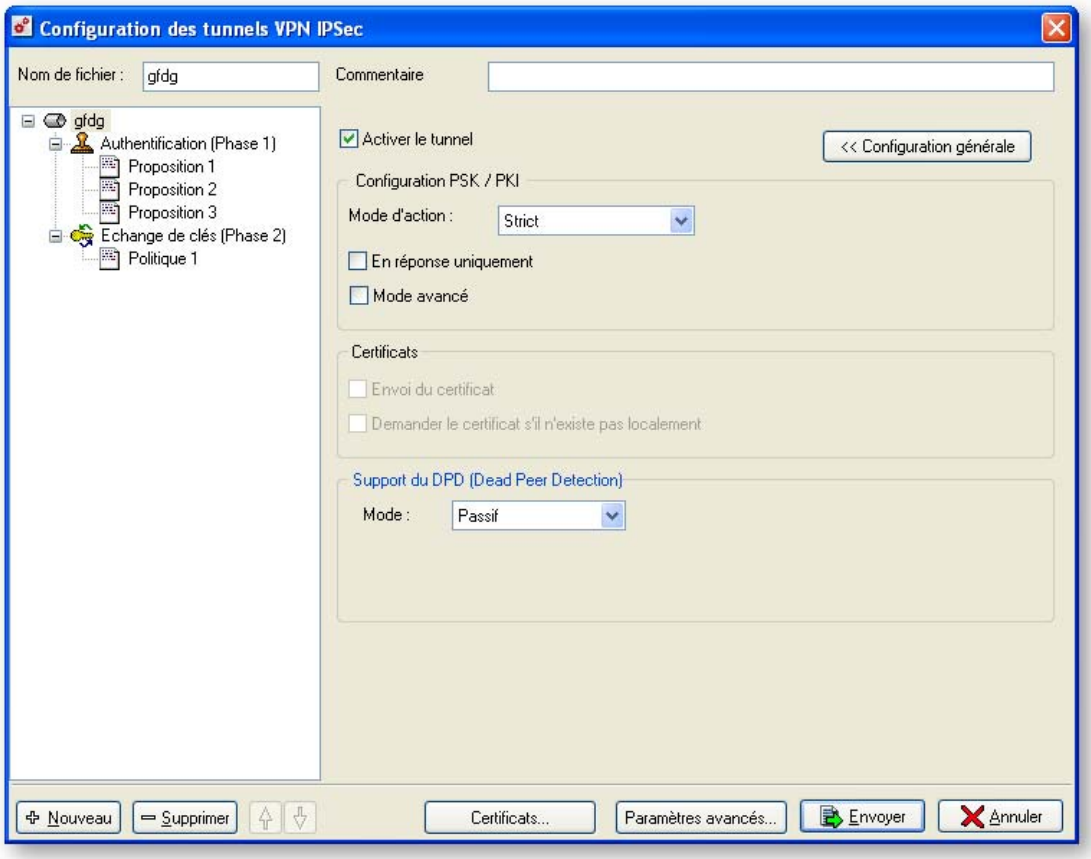


Figure 220 : Configuration des tunnels VPN IPSec - Configuration avancée

Un bouton en haut de la fenêtre, à droite permet de passer en **Configuration avancée**. En configuration avancée, il est possible de modifier :

- Le mode d'action.
- L'option "En réponse uniquement".
- L'option "Mode avancé".
- Options de la configuration VPN avec Certificats.

Mode d'action

Les modes d'action conditionnent le comportement du serveur IPSec en phase 1 lors de la négociation des options PFS (Perfect Forward Secrecy) et durée de vie de SA :

- **Strict** : n'accepte que les options égales ou plus strictes que les siennes (PFS plus élevée, durée de vie de SA plus courte).
- **Claim** : accepte que les options égales ou moins strictes que les siennes (PFS moins élevée, durée de vie de SA plus longue) mais choisit toujours les options les plus strictes.
- **Exact** : n'accepte que les options aussi strictes que les siennes (même niveau de PFS, durée de vie de SA strictement égale).
- **Obey** : accepte les options quelles qu'elles soient (niveau de PFS, durée de vie de SA).

AVERTISSEMENT
Les modes d'action "Obey" et "Claim" ne sont pas couverts par les Critères Communs.

En réponse uniquement

L'option "En réponse uniquement" met le serveur IPSec en attente. Il ne prendra pas l'initiative de négociation du tunnel. Cette option est utilisée dans le cas où le correspondant est un mobile.

Mode avancé

L'option "Mode avancé" permet quant à elle, de pouvoir spécifier <any> aux deux correspondants. Grâce à cette fonctionnalité vous pouvez réaliser un rebond sur un firewall NETASQ pour du Hub'n spoke par exemple.

AVERTISSEMENT
Cette fonction doit être utilisée avec prudence car elle permet la réalisation de configurations potentiellement "erronées".

Le Hub'n Spoke permet aux machines d'un LAN satellite disposant d'un VBox Agency ou d'un firewall NETASQ d'accéder aux LANs des autres sites satellites et/ou à l'extérieur, le tout au travers d'un tunnel avec le site central. Tout le trafic est alors analysé par le firewall NETASQ.

Certificats

Il est possible d'envoyer automatiquement le certificat local au correspondant par l'option "Envoi du Certificat".

Il est possible de récupérer le certificat du correspondant automatiquement s'il n'existe pas dans la base locale par l'option "Demander le certificat s'il n'existe pas localement".

Support du DPD (Dead Peer Detection)

Ce menu permet de configurer la fonctionnalité VPN dite de DPD (*Dead Peer Detection*). Quand le DPD est actif sur un correspondant, celui-ci envoie régulièrement des paquets à l'autre correspondant, auxquels ce dernier répond pour dire qu'il est toujours là. Ces échanges sont sécurisés via les SA ISAKMP (phase 1). Si on détecte qu'un correspondant ne répond plus, alors on détruit les SA (phases 1 et 2) négociées avec celui-ci, et le DPD purge tout.

AVERTISSEMENT
Cette fonctionnalité apporte une stabilité au service VPN sur les firewalls NETASQ, à la condition que le DPD soit correctement configuré.

Pour configurer l'option de **DPD**, quatre choix sont disponibles :

- **Passif** : Les requêtes DPD émises par le correspondant obtiennent une réponse du firewall. Par contre, le firewall n'en n'envoie pas.
- **Elevé et Faible** : Il s'agit de deux profils préconfigurés pour l'utilisation du DPD. Ils diffèrent par la fréquence d'envoi des paquets DPD et par le nombre d'échecs au-delà duquel on considère que le

correspondant est inactif. En « Elévé », la fréquence est élevée et le nombre d'échecs plus bas, en « Faible », la fréquence est faible, et le nombre d'échecs tolérés plus élevé.

- **Manuel** : il s'agit de configurer l'option DPD manuellement selon les paramètres suivants :

  - Le premier paramètre, **Délai** correspond à un délai d'attente avant la prochaine vérification de la présence du correspondant qui a répondu à une requête DPD.

  - Le deuxième paramètre « Réessayer » correspond au délai d'attente avant la prochaine vérification de la présence du correspondant qui n'a pas répondu à une requête DPD.

  - Le dernier paramètre « Echec max » correspond au nombre d'échecs de la vérification de la présence du correspondant au-delà duquel on considère qu'il n'y a plus de correspondant. Les SA sont effacées.

Paramètres généraux de l'authentification [phase 1 IKE]

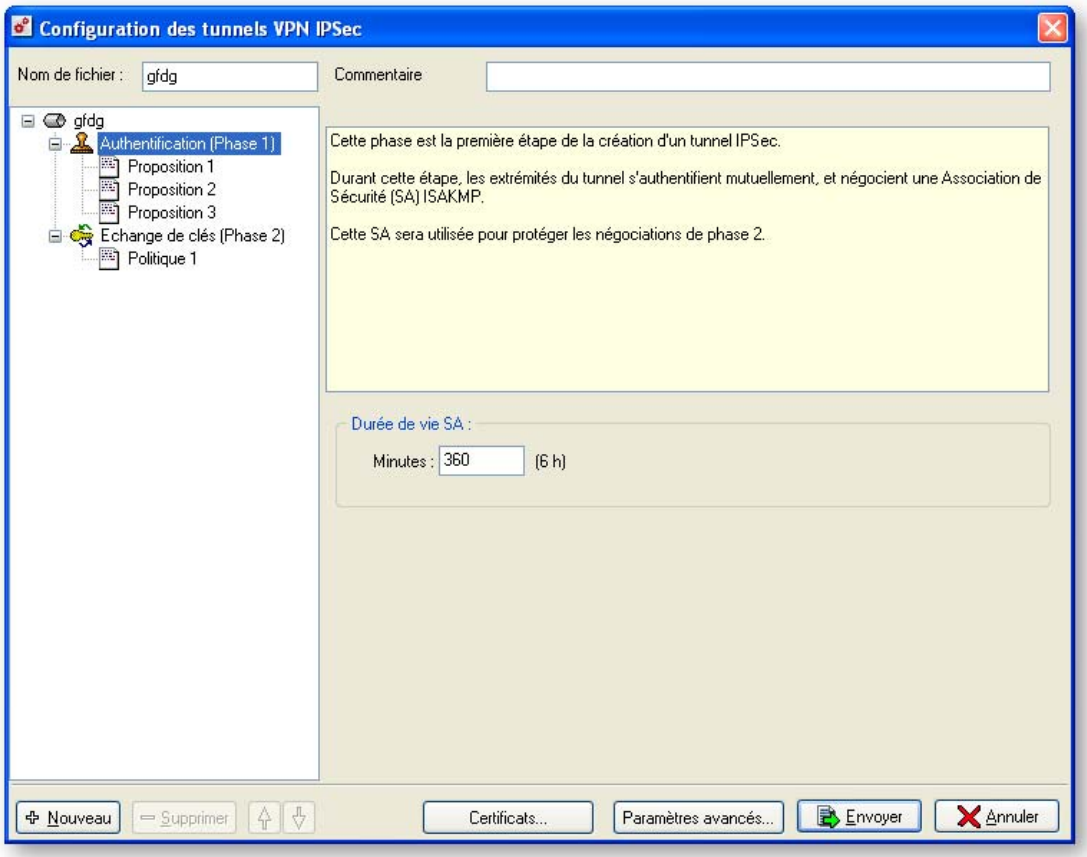


Figure 221 : Configuration des tunnels VPN IPSec - Durée de vie SA

Les paramètres généraux de la phase 1 sont :

Durée de vie SA	Période de temps au bout de laquelle les éléments de la phase 1 sont renégociés. Par défaut, le délai est de 360 minutes.

Algorithmes supportés pour la phase 1 de ce tunnel

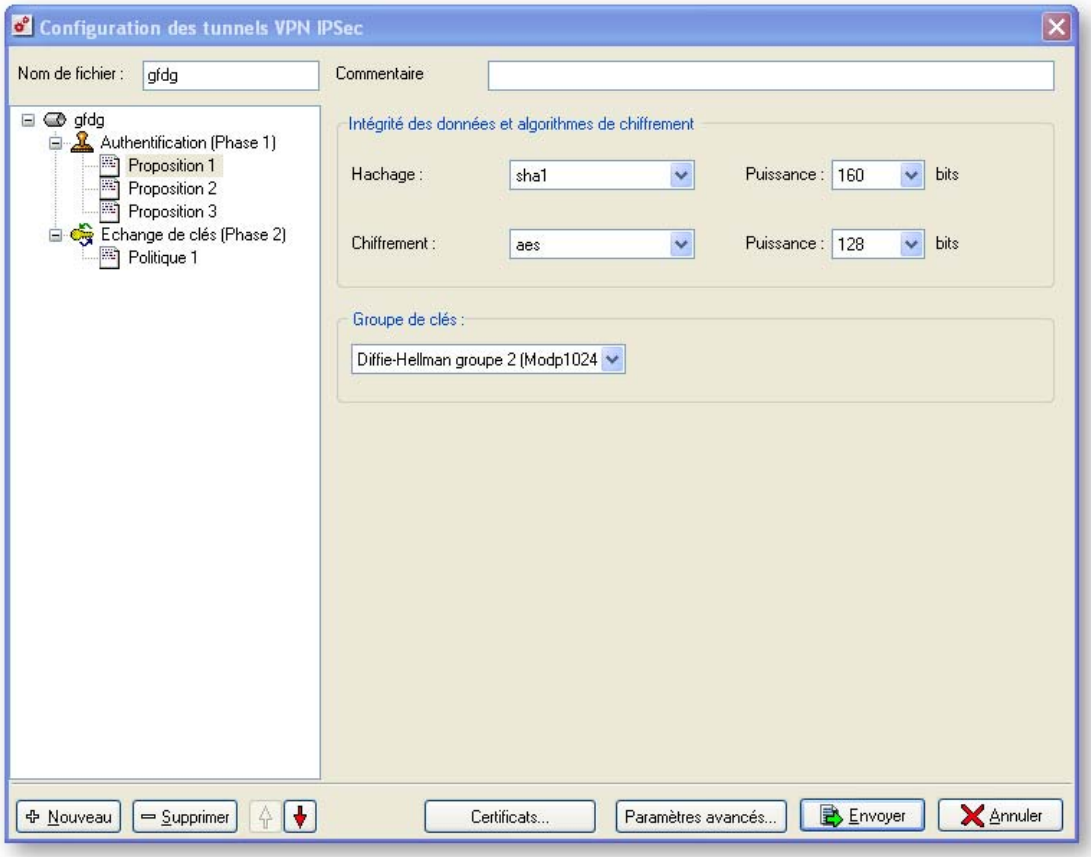


Figure 222 : Configuration des tunnels VPN IPSec - Algorithmes de la phase 1

Les propositions correspondent aux différents algorithmes d'authentification et de chiffrement supportés dans la phase 1 par le firewall pour ce tunnel. Pour qu'une machine distante puisse établir la phase 1 du protocole IPSec, il faut qu'au moins une des propositions soit commune avec le firewall.

Vous pouvez établir plusieurs propositions pour un même tunnel.

Les paramètres de la proposition sont :

Hachage	Algorithme utilisé pour garantir l'intégrité des données. Les firewalls NETASQ supportent les fonctions de hachage : • SHA1 (160 bits) • MD5 (128 bits) • Sha2_256 • Sha2_384 • Sha2_512

Chiffrement	Algorithme utilisé pour chiffrer les données. Les firewalls NETASQ proposent les algorithmes suivants : • DES • 3DES • BLOWFISH • CAST128 • AES **AVERTISSEMENT** NETASQ recommande vivement l'utilisation de l'AES car c'est l'algorithme le plus performant en termes de débit et aussi le plus sécuritaire. IL FAUT bien comprendre que les algorithmes présentés plus haut ne sont pas égaux en termes de performances et de débit. L'AES est actuellement le meilleur algorithme de chiffrement.
Groupe de clés	Méthode utilisée pour le calcul des clés. En mode agressif, cette méthode est commune à toutes les propositions et est choisie dans les paramètres généraux de la phase 1. • Diffie-Hellman groupe 1 (Modp768) • Diffie-Hellman groupe 2 (Modp 1024) • Diffie-Hellman groupe 5 (Modp 1536)

Paramètres généraux de l'échange des clés [phase 2 IKE]

Dans cette phase, les échanges sont authentifiés et chiffrés avec des clés secrètes symétriques, négociées en phase 1 (ISAKMP SA).

3 objectifs :

1) **Négociation des paramètres de sécurité** : les correspondants se mettent d'accord sur les valeurs de certains paramètres concernant le tunnel IPSec. Les extrémités du traffic sont vérifiées.
2) **Génération des clés pour IPSec** : en utilisant la SA négociée dans la phase 1, les correspondants se mettent d'accord sur les clés qui seront utilisées dans le tunnel IPSec.
3) **Protection contre le rejeu :** Le rejeu de spaquets IPSec est protégé. Cette protoection est configurée aau niveau de la phase 2 de la négociation.

Onglet Général

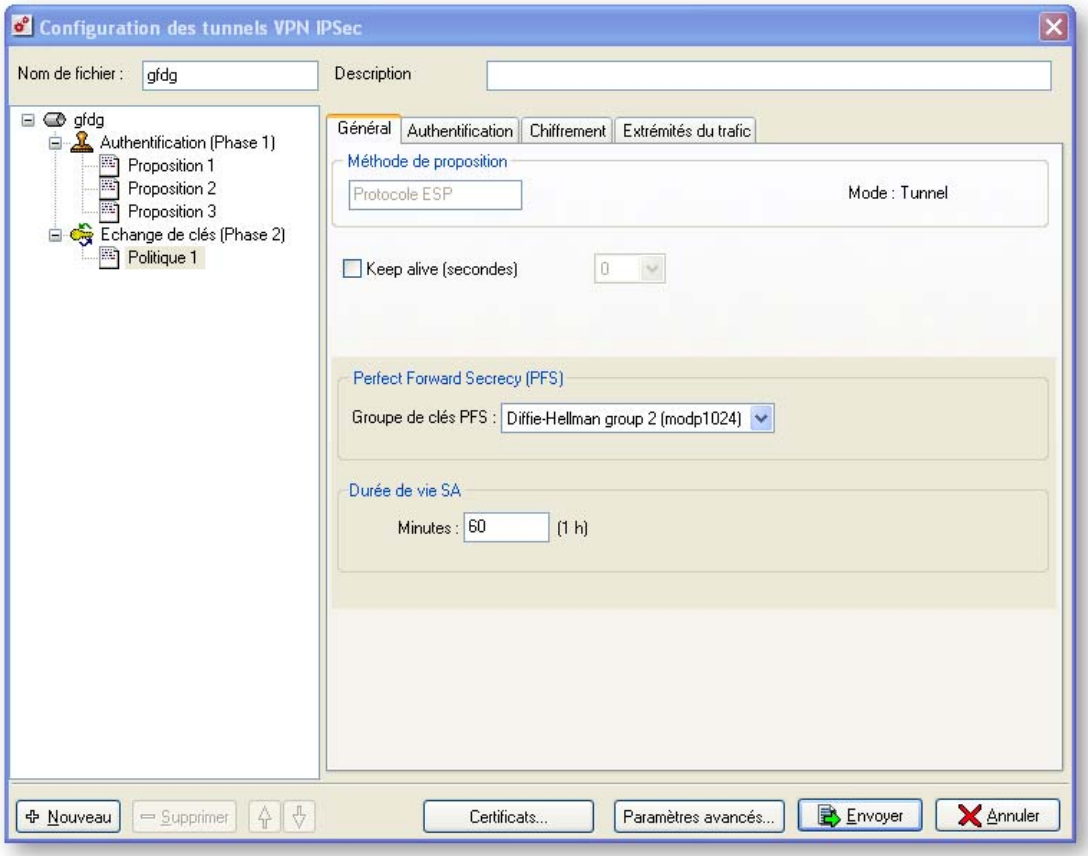


Figure 223 : Configuration des tunnels VPN IPSec - Général

Méthode de proposition	Sélection des protocoles IPSec utilisés dans le tunnel : • Protocole ESP (chiffrage)
Keep alive (secondes)	Temps écoulé, en secondes, entre deux paquets envoyés au travers d'un tunnel VPN pour assurer le maintien de ce tunnel. Les paquets envoyés sont uniquement utilisés pour le maintien de connexion.
Perfect Forward Secrecy	Permet de garantir qu'il n'y a aucun lien entre les différentes clés de chaque session. Les clés sont recalculées par l'algorithme de Diffie-Hellman sélectionné. Plus le chiffre est élevé (aucune, 1, 2 ou 5), plus la sécurité est importante. 2 est le niveau de PFS le plus couramment utilisé.
Durée de vie SA	Période de temps au bout de laquelle les clés sont renégociées. La période est par défaut de 60 minutes.

Onglet Authentification

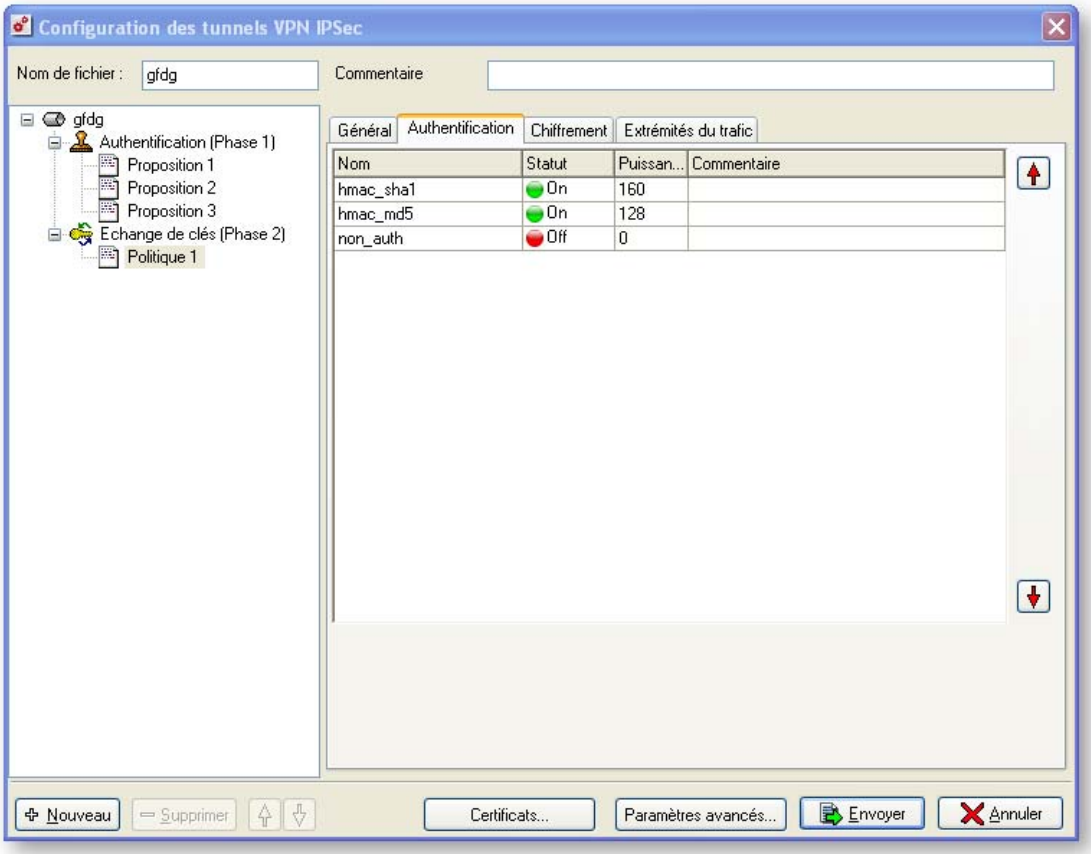


Figure 224 : Configuration des tunnels VPN IPSec - Authentification

L'onglet **Authentification** vous permet de sélectionner les algorithmes d'authentification acceptés par cette proposition.

Le firewall supporte les algorithmes suivants :

- Pas d'authentification
- HMAC-SHA1
- HMAC-MD5

Onglet Chiffrement

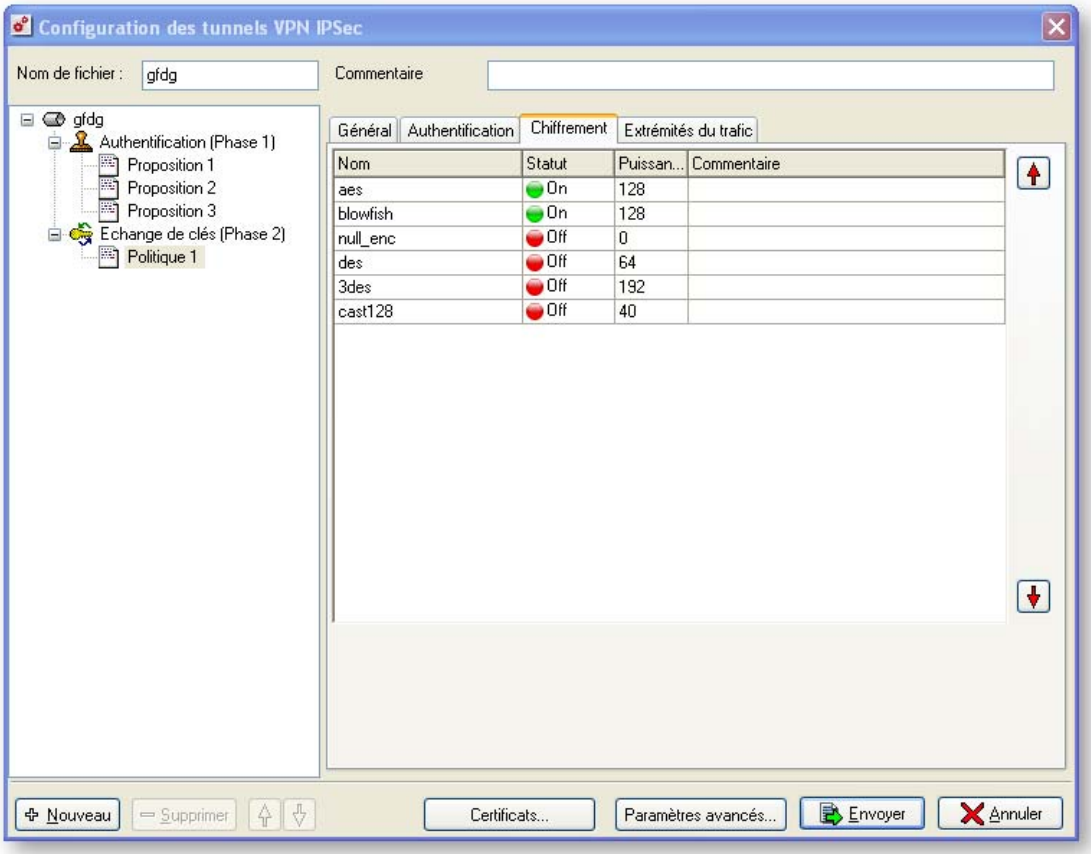


Figure 225 : Configuration des tunnels VPN IPSec – Chiffrement

L'onglet **`Chiffrement`** vous permet de sélectionner les algorithmes de chiffrement acceptés par cette proposition.

Le firewall supporte les algorithmes suivants :

- Null_enc
- DES
- 3DES
- BLOWFISH
- CAST128
- AES

Onglet Extrémités du trafic

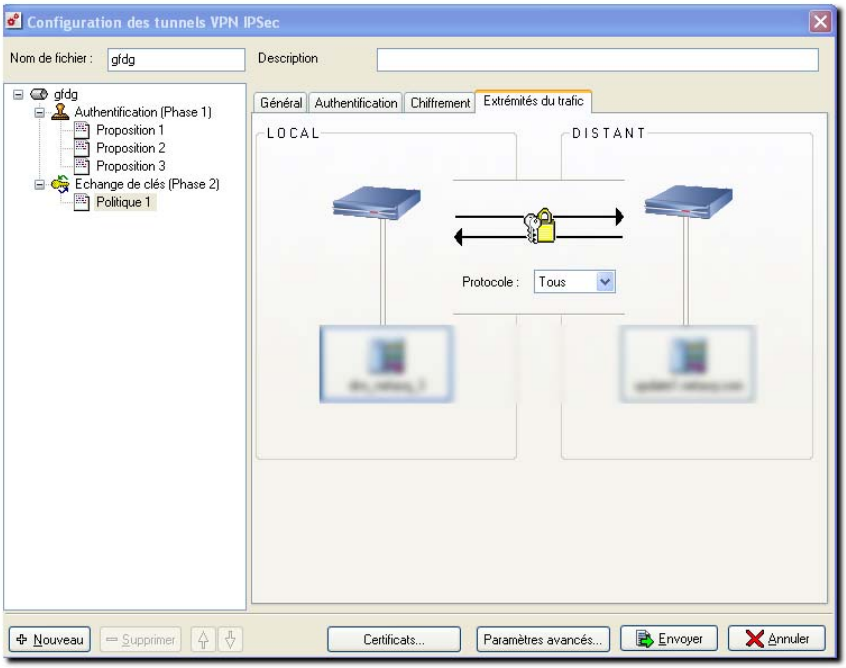


Figure 226 : Configuration des tunnels VPN IPSec - Extrémités du trafic

Cette section vous permet de définir quels utilisateurs locaux utilisent le tunnel et éventuellement pour quels protocoles.

Vous sélectionnez les machines ou réseaux distante dans la liste des objets déclarés puis éventuellement un protocole particulier à chiffrer.

Paramètres avancés

- Pour accéder aux paramètres avancés, cliquez sur le bouton **Paramètres avancés** :

Figure 227 : Propriétés du slot VPN

Ce menu vous permet de gérer des paramètres supplémentaires pour un tunnel IPSec. Il est disponible autant pour les tunnels statiques que pour les tunnels dynamiques.

C'est ici que l'on va mettre en place le comportement général du tunnel sélectionné.

Considérer les correspondants IPSec comme internes	En cochant cette option, les interfaces IPSec sont considérées comme interfaces internes. Donc cela leur confère un caractère "protégé" comme toutes interfaces internes. Cette option est notamment nécessaire pour la configuration du Hub'n spoke.
Utiliser la SA la plus ancienne	Lorsqu'on renouvelle des SA, les anciennes et nouvelles SA coexistent pendant quelques temps. Par défaut, un correspondant IPSec doit utiliser la SA la plus récente (celle nouvellement négociée). En cochant l'option « Utiliser la SA la plus ancienne » la SA la plus ancienne est utilisée jusqu'à ce qu'elle expire. Cette option sert à se rendre interopérable avec des implémentations qui utilisent les SA jusqu'à expiration. **AVERTISSEMENT** Cette fonction ne doit être utilisée qu'en cas de stricte nécessité.
Faire confiance à la PKI interne	Lorsque vous utilisez un tunnel VPN utilisant des certificats numériques et que vous cochez cette option, celle-ci permet de confronter les certificats des correspondants IPSec à la PKI interne du firewall.
Tester la CRL interne	Cochez cette option afin de paramétrer la fréquence de mise à jour de la liste de révocation des certificats (CRL). Il est possible de faire des vérifications régulières, pour cela, paramétrez la base de temps (en minutes, heures, jours ou mois). Plus le délai est court, plus le firewall devra vérifier sa CRL lorsque ce tunnel est actif. Donc il vaut mieux ne pas définir un temps trop court (baisse de performances), ni trop long (risque d'utiliser une CRL obsolète). Le temps doit être cohérent avec la fréquence d'émission de la CRL.

Certificats

- Pour accéder aux certificats, cliquez sur le bouton **Certificats** :

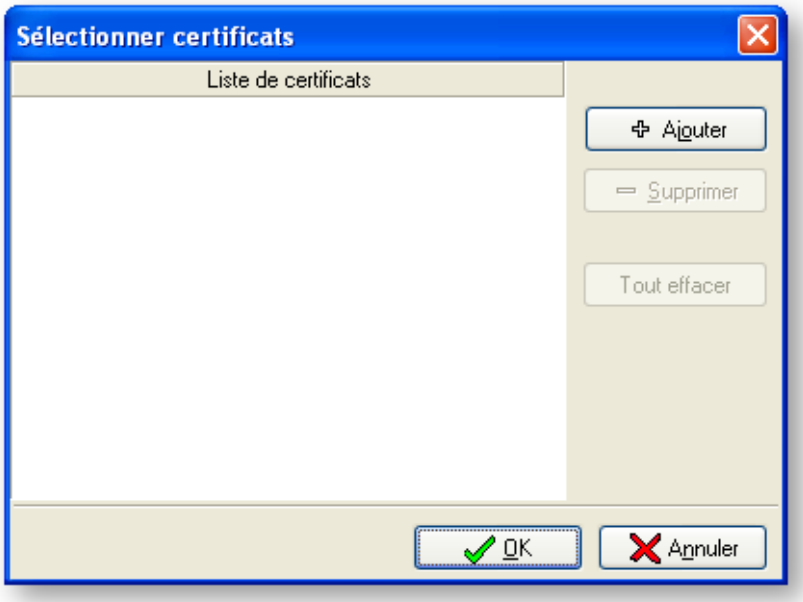


Figure 228 : Sélection des certificats

Lorsque des certificats d'autorité de certification externe sont insérés dans la liste des certificats, tous les certificats utilisateurs signés par ces autorités de certification sont automatiquement reconnus par le firewall comme certificat valide à l'authentification de leur détenteur.

Pour utiliser ces autorités de certification reconnues, dans la configuration des politiques VPN, il faut spécifier dans le bouton **Certificats** (du panneau de configuration générale des tunnels VPN), la liste des autorités de certification qui doivent être validées pour ce slot de configuration VPN. Cette liste d'autorité de certification est spécifique au slot configuré bien que l'on retrouve la liste globale de toutes les autorités de certification autorisées par l'administrateur dans un seul et même endroit.
Pour ajouter une autorité de certification dans la liste des autorités reconnues pour le slot VPN configuré, référez-vous à la procédure suivante :

1. Cliquez sur le bouton **Certificats…** du panneau de configuration générale des tunnels VPN.
2. Cliquez sur le bouton **Ajouter** du panneau de configuration des certificats. L'écran suivant s'affiche :

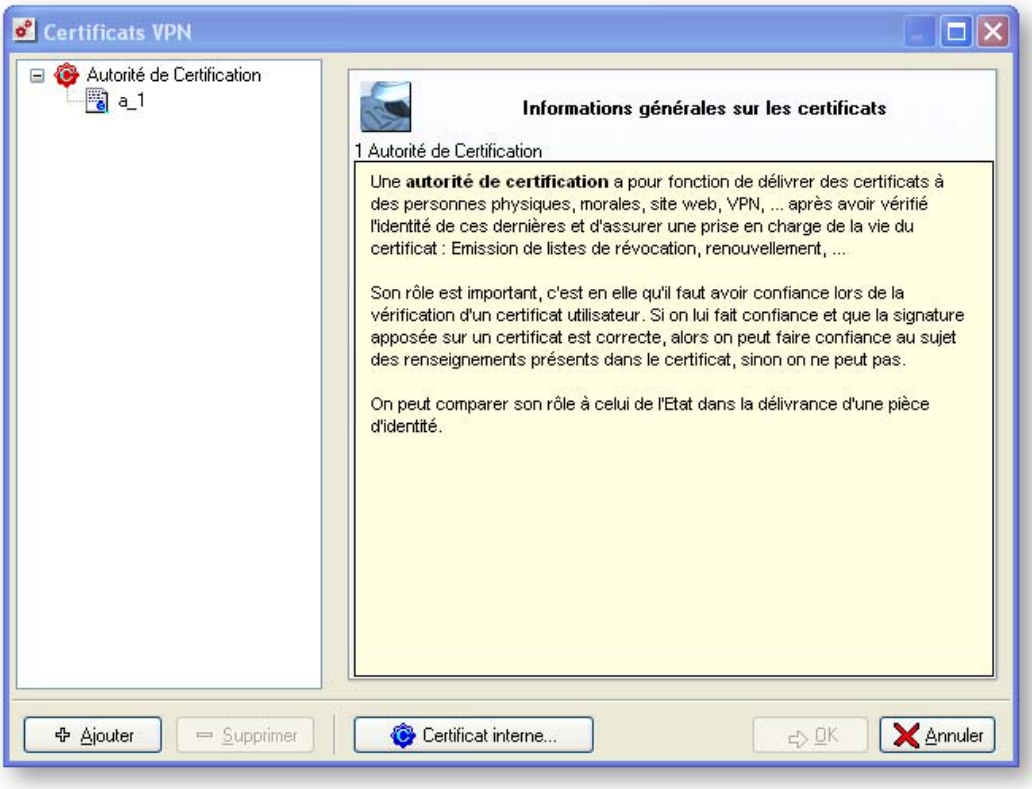


Figure 229 : Certificats VPN

3 Cliquez sur le bouton **Ajouter**. L'écran suivant s'affiche :

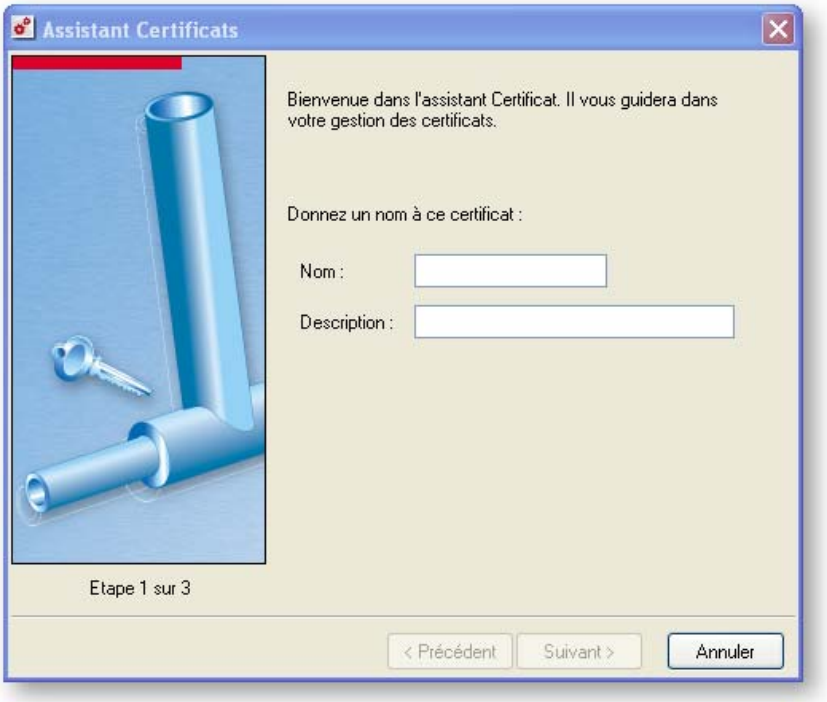


Figure 230 : Assistant Certificats - Etape 1

Donnez un nom au certificat puis une description.

3 Cliquez sur le bouton **Suivant**. L'écran suivant s'affiche :

Figure 231 : Assistant Certificats - Etape 2

4 Choisissez le type de certificat puis cliquez sur **Suivant**. L'écran suivant s'affiche :

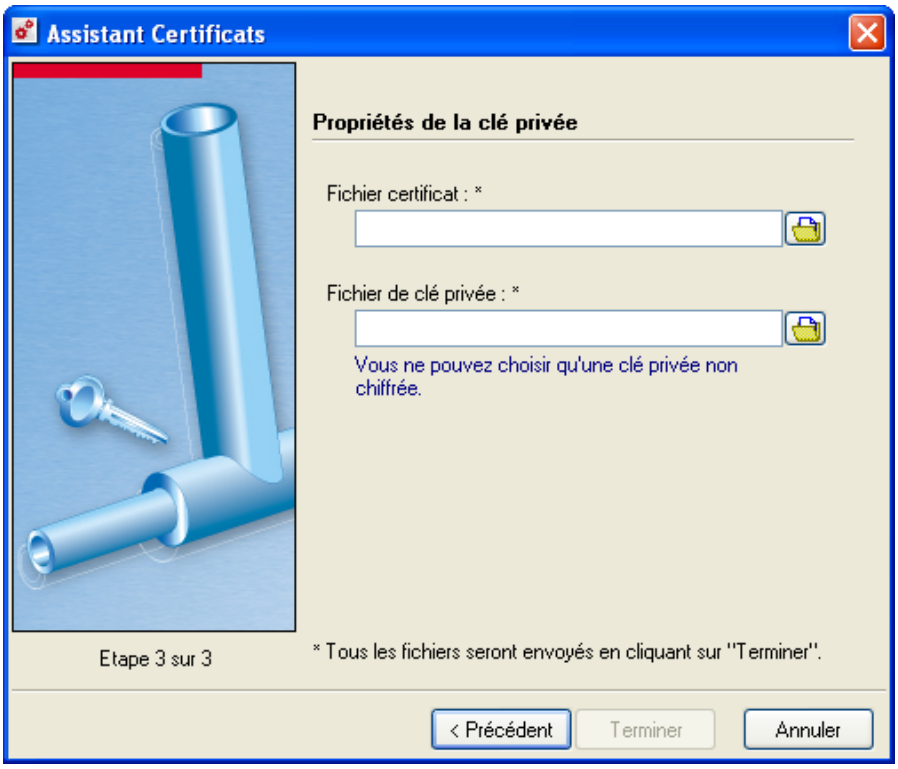


Figure 232 : Assistant Certificats - Etape 3

5 Sélectionnez les fichiers.

6 Validez enfin l'ajout de ces certificats en envoyant la configuration du slot VPN.

8.3.4. Règle de filtrage

Après la configuration du ou des tunnels VPN, il faut définir un ensemble de règles de filtrage permettant l'établissement du ou des tunnels et la transmission des informations chiffrées. Pour cela, deux actions doivent être réalisées :

- Activation des règles implicites VPN.
- Edition des règles de filtrage pour autoriser le trafic au travers d'un tunnel IPSec.

8.3.4.1. Activation des règles implicites VPN

Les firewalls NETASQ peuvent générer de façon automatique des règles de filtrage pour l'établissement des tunnels VPN. Ces règles n'ont donc pas besoin d'être définies de façon explicite par l'administrateur au niveau de l'édition des slots de filtrage.

➔ L'activation des règles implicites se fait au moyen du menu de l'arborescence **`Politique\Règles implicites`**.

Activez la case **Services VPN** puis cliquez sur **OK.**

AVERTISSEMENT
Les règles implicites ne sont générées que pour les tunnels IPSec Gateway to Gateway. Pour le tunnel anonyme, il faut obligatoirement définir explicitement des règles au niveau des slots de filtrage.

Pour un tunnel anonyme, les règles à définir sont du type :

Etat	Protocole	Source	Destination	Port de destination	Action
On	UDP	Any	Firewall_out	isakmp	Passer
On	Vpn-esp	Any	Firewall_out		Passer
On	Vpn-esp	Firewall_out	Any		Passer

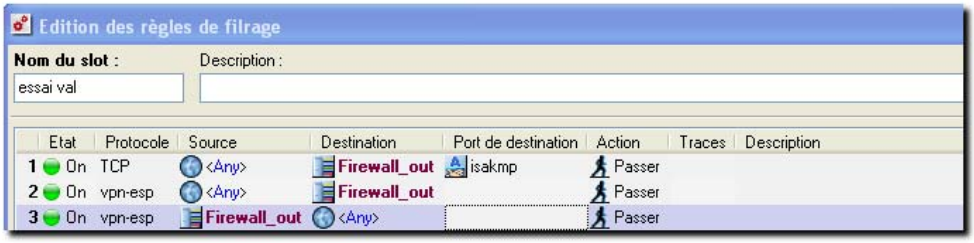


Figure 233: Edition des règles de filtrage

Dans cet exemple, on ne connaît pas la plage d'adresses utilisée par les clients VPN nomades (on utilise donc l'objet "ANY"). Si la plage d'adresses utilisée par les clients nomades est connue (plage d'adresses du fournisseur d'accès, par exemple), alors il est conseillé de restreindre les règles à cette plage d'adresses.

8.3.4.2. Edition des règles de filtrage

Sans règles de filtrage explicites pour le trafic transitant au travers du tunnel IPSec, aucune donnée ne sera autorisée au travers de ce tunnel (même si le tunnel est déjà actif). Pour autoriser des données à transiter au travers du firewall, il faut rajouter des règles de filtrage comme dans l'exemple suivant :

Figure 234 : Edition des règles de filtrage

Exemple
Les machines du réseau distant (Netwk_SatelliteA) ont accès aux machines du réseau interne (Network_Bridge) pour les services WEB. Les machines du réseau interne (Network_Bridge) ont accès à toutes les machines du réseau distant (Netwk_SatelliteA) pour tous les services.

AVERTISSEMENT
Les règles de filtrage s'appliquant au trafic venant du réseau distant doivent avoir l'interface "IPSec" sélectionnée. Les règles de filtrage s'appliquant au trafic en direction du réseau distant doivent avoir l'interface "Auto" sélectionnée.

8.3.5. Tunnels VPN passerelle par passerelle

Dans cette section, plusieurs configurations basiques de tunnels VPN sont abordées. Elle décrit en particulier :

- La création d'un tunnel G2G avec clés pré partagées.
- La création d'un tunnel G2G avec certificats.
- La création d'un tunnel G2G VPN statique (ce type de configuration, aujourd'hui obsolète, est uniquement supporté pour des raisons de compatibilités).

8.3.5.1. Tunnel VPN IPSEC avec clés pré partagées

L'exemple suivant explique la configuration nécessaire à la réalisation d'un tunnel VPN passerelle à passerelle (gateway to gateway avec clés pré-partagées.

Définition
On appelle **Tunnel VPN passerelle à passerelle** un tunnel VPN réalisé entre deux éléments réseaux compatibles VPN qui jouent le rôle d'extrémités de tunnel, d'une passerelle (essentiellement firewall à firewall).

Cette architecture est représentée par le schéma suivant :

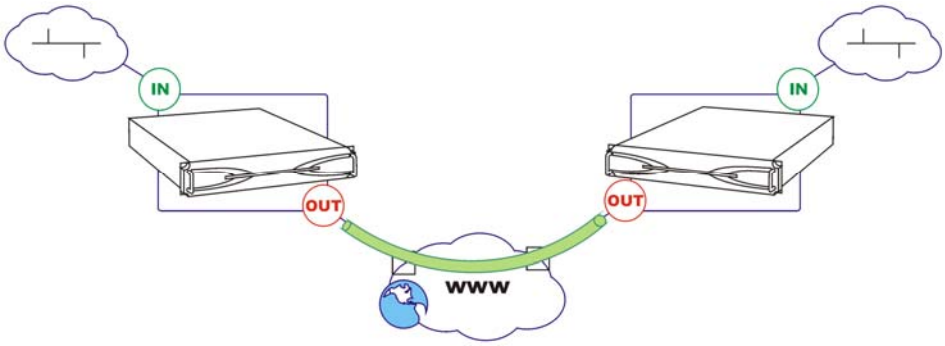


Figure 235 : Tunnel VPN IPSec avec Clés pré-partagées

Configuration du tunnel

Afin de réaliser la configuration du tunnel, sélectionnez le slot VPN dans lequel vous désirez réaliser le tunnel. L'assistant VPN vous aiguille alors dans la configuration VPN.

Cette configuration est à réaliser sur chacun des firewalls participant au tunnel VPN. Pensez toutefois à inverser les extrémités de trafic et de tunnel.

Le premier écran de l'assistant VPN apparaît. Choisissez le nom que vous désirez attribuer à ce tunnel (le nom du slot sera automatiquement attribué avec cette valeur mais vous pouvez la modifier ensuite). Cliquez sur le bouton **Suivant** pour continuer la configuration.

A l'étape 2 de l'assistant VPN, choisissez le type de tunnel que vous désirez réaliser (ici "Dynamique (Clés pré-partagées) pour l'exemple). Cliquez sur le bouton **Suivant**.

Les étapes 3 et 4 permettent de spécifier dans un premier temps les différents éléments réseaux aux extrémités du tunnel puis les extrémités du trafic transitant à l'intérieur du tunnel VPN.

AVERTISSEMENT

Dans l'exemple l'interface Firewall_out est utilisée comme extrémité de tunnel. Si votre firewall est directement relié à un modem vous devez utiliser l'interface Dialup qui correspond à votre connexion Internet active.

Lorsque les extrémités sont définies, cliquez sur le bouton **Suivant** pour terminer la configuration du tunnel. Un écran général rappelle la configuration définie dans l'assistant. Vous pouvez contrôler cette configuration avant d'envoyer la configuration VPN spécifiée au firewall.

AVERTISSEMENT

Pour qu'un tunnel VPN soit négocié il est nécessaire qu'il possède une passerelle par défaut valide (même lors d'une phase de test).

Pensez à effectuer le filtrage nécessaire au passage du trafic VPN sur les firewalls participant au tunnel.

Configuration des clés pré partagées

Pour de plus amples informations au sujet de la configuration des clés-pré-partagées, veuillez vous référer au chapitre Partie 8/Chapitre 2 : Clés pré-partagées.

8.3.5.2. Tunnel VPN IPSec avec certificats

Configuration du tunnel

Afin de réaliser la configuration du tunnel, sélectionnez le slot VPN dans lequel vous désirez réaliser le tunnel. L'assistant VPN vous aiguille alors dans la configuration VPN.

Cette configuration est à réaliser sur chacun des firewalls participant au tunnel VPN. Pensez toutefois à inverser les extrémités de trafic et de tunnel.

Etape 1

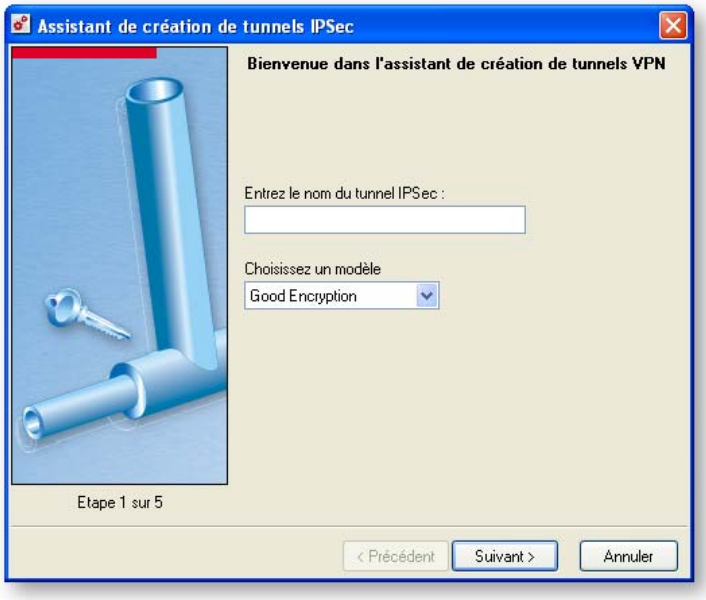


Figure 236 : Création de tunnels IPSec - Etape 1

La première étape dans la création du tunnel est de choisir le nom que vous désirez attribuer à ce tunnel (le nom du slot sera automatiquement attribué avec cette valeur mais vous pouvez la modifier ensuite). Cliquez sur **Suivant** pour continuer la configuration.

Etape 2

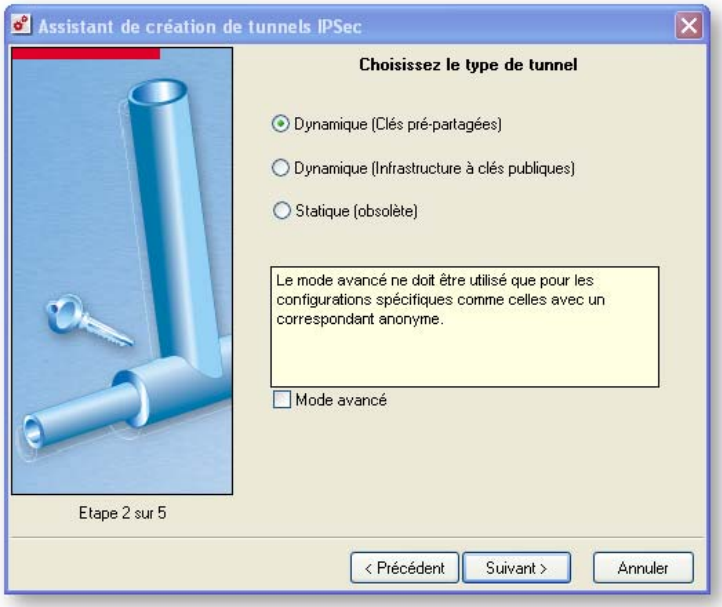


Figure 237 : Création de tunnels IPSec - Etape 2

A l'étape 2 de l'assistant VPN, choisissez le type de tunnel que vous désirez réaliser (ici dynamique avec certificats pour l'exemple). Cliquez sur **Suivant**.

Etape 3

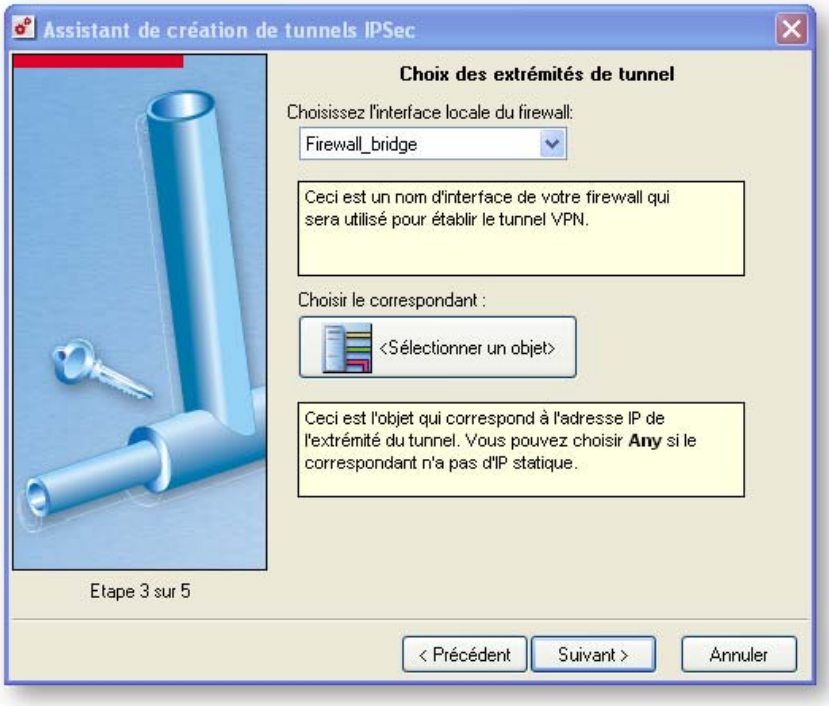


Figure 238 : Création de tunnels IPSec - Etape 3

Etape 4

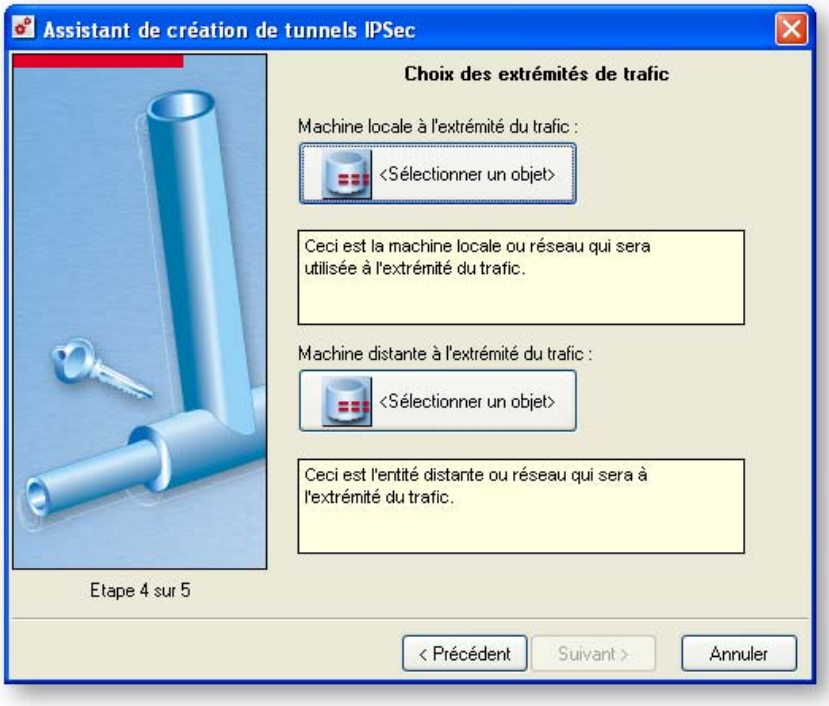


Figure 239 : Création de tunnels IPSec - Etape 4

Les étapes 3 et 4 permettent de spécifier dans un premier temps les différents éléments réseaux aux extrêmités du tunnel puis les extrémités du trafic transitant à l'intérieur du tunnel VPN.

AVERTISSEMENT
Dans l'exemple l'interface Firewall_out est utilisée comme extrémité de tunnel. Si votre firewall est directement relié à un modem vous devez utiliser l'interface Dialup qui correspond à votre connexion Internet active.

Etape 5

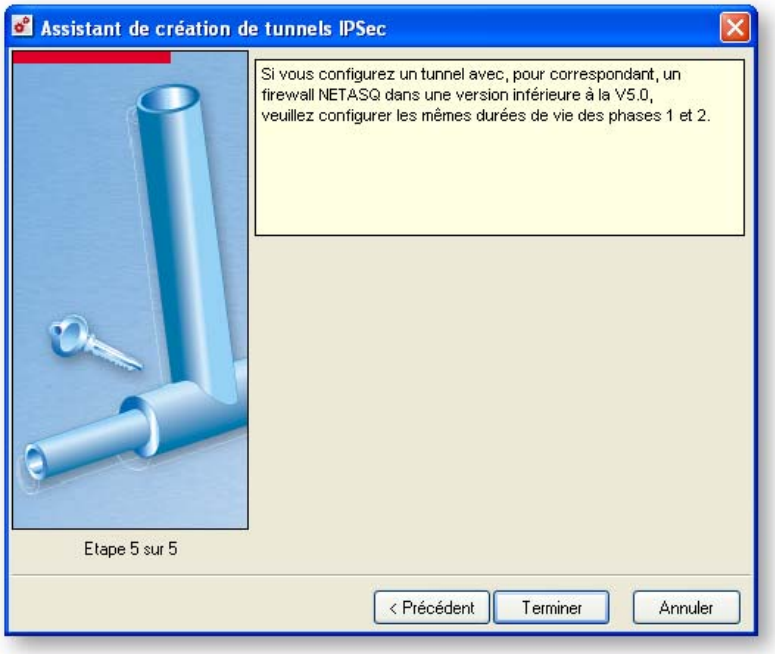


Figure 240 : Création de tunnels IPSec - Etape 5

Lorsque les extrémités sont définies, cliquez sur le bouton **Suivant** pour terminer la configuration du tunnel. Un écran général rappelle la configuration définie dans l'assistant.

AVERTISSEMENT
Pour qu'un tunnel VPN soit négocié il est nécessaire qu'il possède une passerelle par défaut valide (même lors d'une phase de test).

Pensez à effectuer le filtrage nécessaire au passage du trafic VPN sur les firewalls participant au tunnel.

Configuration des certificats

Suite à la configuration du tunnel, il convient de configurer les certificats. Dans le cadre "Certificats PKI" de l'écran de configuration globale des tunnels VPN, cliquez sur le bouton **Choisissez un certificat**
Vous pouvez alors générer un certificat numérique pour le firewall. Pour cela, cliquez sur le bouton **Certificat interne** puis sur le bouton **Créer un certificat VPN…** indiquez le mot de passe de l'autorité de certification du firewall. Une fois généré, le certificat apparaît dans la partie "Clé privée".

Un seul certificat peut être généré.

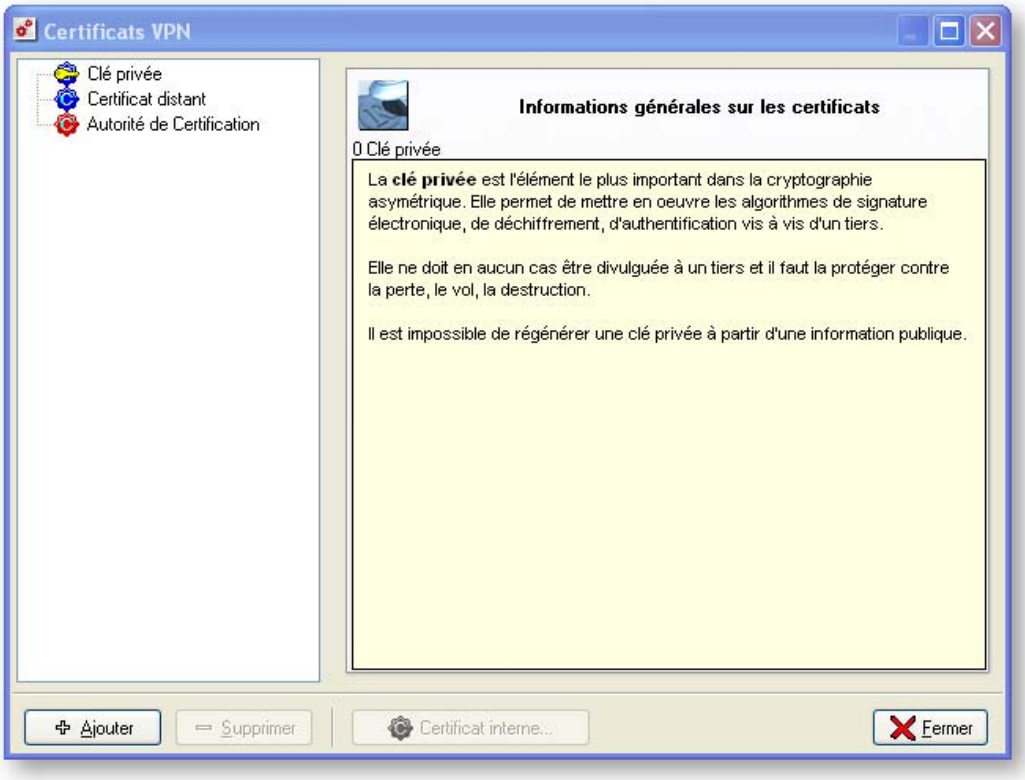


Figure 241 : Certificats VPN

AVERTISSEMENT
La génération de certificats n'est disponible que dans le cas où le service PKI interne est configuré et actif sur le firewall.

Configuration avancée avec les certificats

Si le correspondant est un client mobile, vous pouvez définir son certificat dans la fiche de l'utilisateur utilisant le client IPSec. (*Cf.* *Partie 4/Chapitre 3 : Objets\Utilisateurs*).

Si le correspondant est une autre passerelle VPN :

- Vous pouvez exporter votre autorité de certification interne dans l'autre firewall (*Cf.* *Partie 12 : Authentification*) et importer l'autorité de certification du firewall distant dans la partie "Autorité de certification" (de façon croisée).
- Vous pouvez définir le firewall distant comme un utilisateur. Dans ce cas, vous devez ajouter une fiche utilisateur (*Cf.* *Partie 4/Chapitre 3 : Objets/Utilisateurs*) pour le firewall distant et générer le certificat. Vous devez sauvegarder ce certificat et l'importer dans la partie "Clés privées et certificats" du firewall distant.

Intégration de l'architecture VPN dans une PKI externe

Le firewall NETASQ peut intégrer les certificats provenant d'une PKI externe. Les certificats doivent alors être importés au niveau du firewall. Dans la fenêtre Certificats VPN, avant l'importation, la fenêtre ne contient que le certificat du firewall.

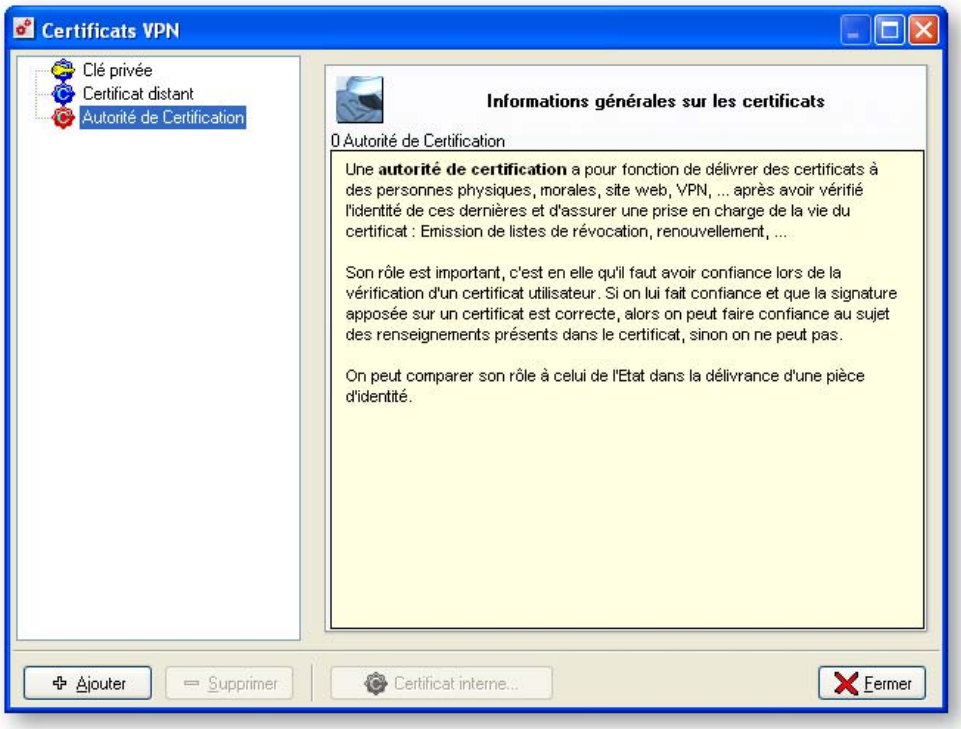


Figure 242 : Certificats VPN - Autorité de certification

La colonne de gauche affiche trois types de certificats. Lorsque vous sélectionnez un type de certificat une explication sur le type de clé sélectionné apparaît.

Pour ajouter un certificat provenant d'une PKI externe, référez-vous à la procédure suivante :

1 Cliquez sur le bouton **Ajouter**, un assistant d'intégration des certificats apparaît. La première étape permet de saisir le nom du certificat.

Figure 243 : Assistant Certificats - Etape 1

2 La deuxième étape permet de choisir le type de certificat.

Figure 244 : Assistant certificats - Etape 2

La troisième étape permet de sélectionner le fichier certificat que l'on désire insérer.

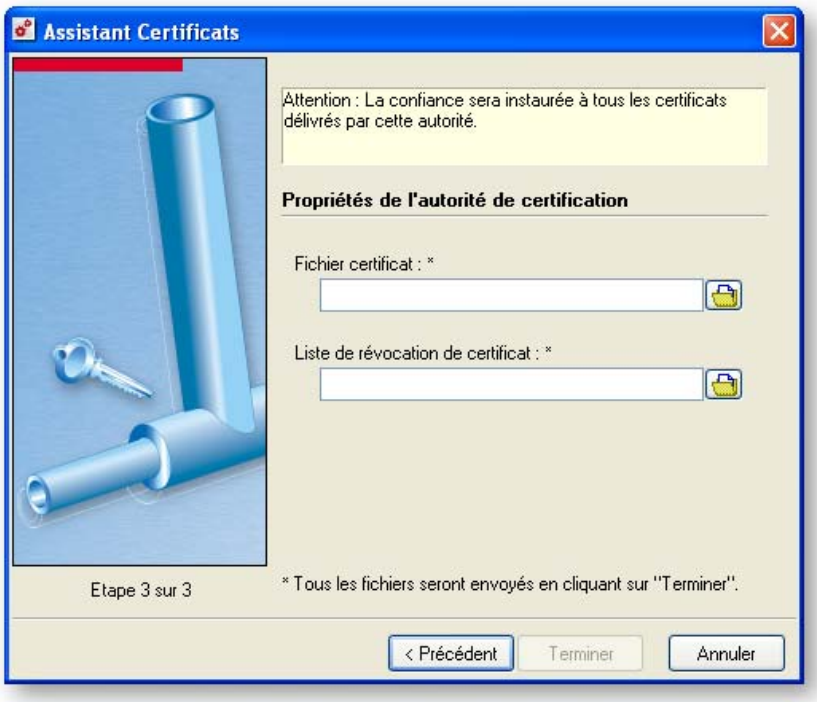


Figure 245 : Assistant Certificats - Etape 3

Suivant le type de certificat, l'assistant d'intégration des certificats requiert des fichiers différents à la troisième étape.

- Le choix **Clé privée** donne la possibilité de charger le certificat (au format *.cer, *.der ou *.pem) et la clé privée (au format *.key ou *.pem non chiffré c'est à dire texte clair) dans deux fichiers différents.
Le firewall teste si le certificat correspond bien à la clé privée.

- Le choix **Certificat distant** donne la possibilité de charger le certificat (au format *.cer, *.der ou *.pem)
- Le choix **Autorité de Certification** donne la possibilité de charger le certificat (au format *.cer, *.der ou *.pem) ainsi que la liste de révocation des certificats (au format *.crl ou *.pem) :

La liste de révocation des certificats est une option. Toutefois une fois un premier fichier configuré, il faut mettre à jour la liste dès que celle-ci est périmée. Dans le cas contraire, l'autorité de certification sera inutilisable.

- Le choix **Container PKCS12** donne la possibilité de charger un fichier PKCS#12. Un container PKCS#12 contient une clé privée, une clé publique et un certificat. Toutes ces informations sont chiffrées en utilisant un mot de passe qu'il faut préciser.

Le contenu et le détail du certificat peut être visualisé dans la partie droite de la fenêtre grâce aux onglets **`Certificat`** et **`Détails du certificat`**.

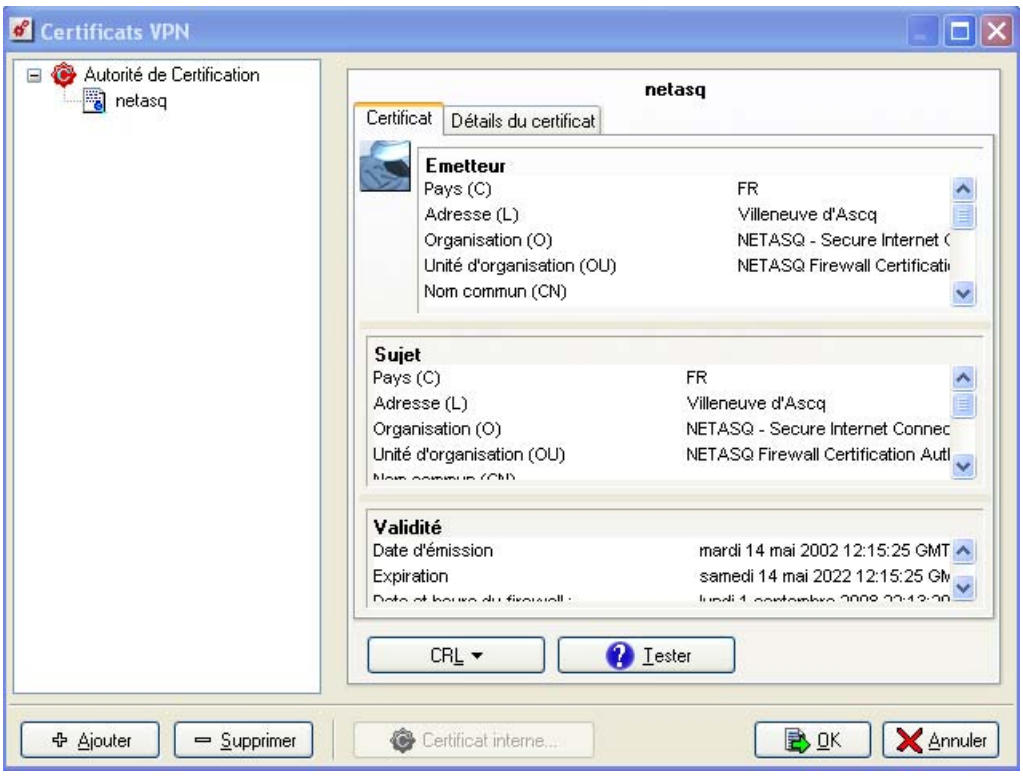


Figure 246 : Certificats VPN - Certificat

REMARQUE

On y retrouve entre autres le propriétaire du certificat, l'autorité de certification qui a signé le certificat, la période de validité du certificat. Le certificat devient grisé s'il n'est plus valide.

Lorsqu'une autorité de certification externe est insérée dans le menu certificat, tous les certificats signés par cette autorité de certification sont automatiquement reconnus comme certificats valides à l'authentification de leur détenteur.

Le bouton **Tester** vous permet d'accéder à l'écran suivant :

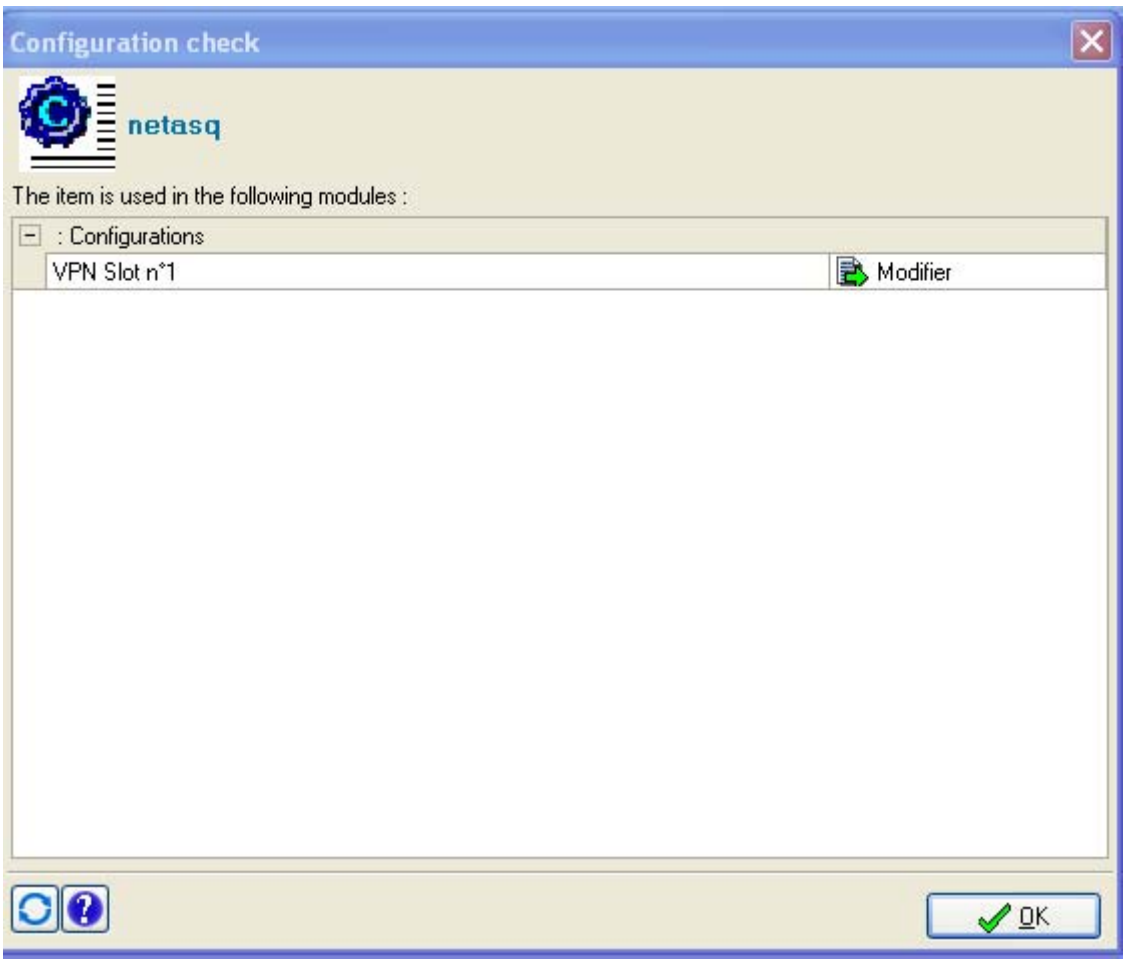


Figure 247 : Configuration check

Il s'agit d'un écran de recherche qui vous permet de connaître dans quelle politique l'autorité de certification est utilisée.
En cliquant sur **Modifier**, vous accédez aux écrans de configuration du tunnel IPSec.

8.3.5.3. Tunnel VPN IPSEC statique

L'exemple suivant explique la configuration nécessaire à la réalisation d'un tunnel VPN passerelle à passerelle (gateway to gateway avec clés pré partagées).

DEFINITION
On appelle "tunnel VPN passerelle à passerelle" un tunnel VPN réalisé entre deux éléments réseaux compatibles VPN qui jouent le rôle d'extrémités de tunnel, d'une passerelle (essentiellement firewall à firewall).

Cette architecture est représentée par le schéma suivant :

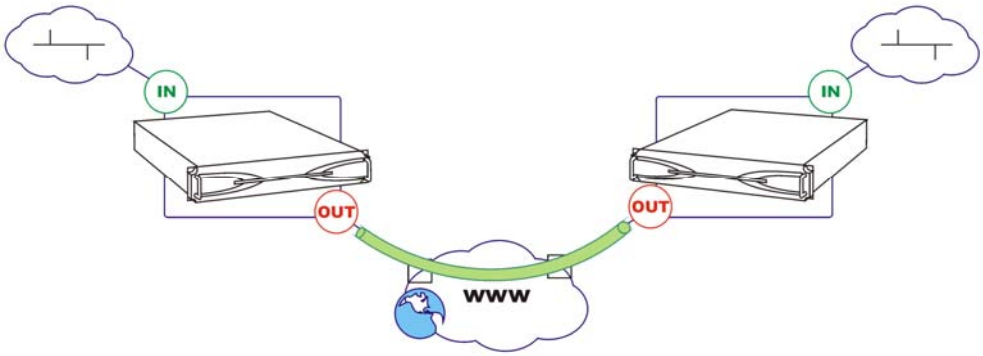


Figure 248 : Tunnel VPN IPSec statique

Configuration du tunnel

Afin de réaliser la configuration du tunnel, sélectionner le slot VPN dans lequel vous désirez réaliser le tunnel. L'assistant VPN vous aiguille alors dans la configuration VPN.

Cette configuration est à réaliser sur chacun des firewalls participant au tunnel VPN. Pensez toutefois à inverser les extrémités de trafic et de tunnel.

Les premières étapes de l'assistant de création des tunnels VPN est de choisir le nom que vous désirez attribuer à ce tunnel (le nom du slot sera automatiquement attribué avec cette valeur mais vous pouvez la modifier ensuite). Cliquez sur **Suivant** pour continuer la configuration.

A l'étape 2 de l'assistant VPN, choisissez le type de tunnel que vous désirez réaliser (ici Statique (obsolète). Le message suivant s'affiche :

> "Les tunnels manuels sont obsolètes. Souhaitez-vous vraiment créer un tunnel manuel ?"

Cliquez sur **Oui** puis sur **Suivant**.

Les étapes 3 et 4 permettent de spécifier dans un premier temps les différents éléments réseaux aux extrémités du tunnel puis les extrémités du trafic transitant à l'intérieur du tunnel VPN.

> **AVERTISSEMENT**
> Dans l'exemple l'interface Firewall_out est utilisée comme extrémité de tunnel. Si votre firewall est directement relié à un modem vous devez utiliser l'interface Dialup qui correspond à votre connexion Internet active.

Lorsque les extrémités sont définies, cliquez sur **Suivant** pour terminer la configuration du tunnel. Un écran général rappelle la configuration définie dans l'assistant.

> **AVERTISSEMENT**
> Pour qu'un tunnel VPN soit négocié il est nécessaire qu'il possède une passerelle par défaut valide (même lors d'une phase de test).
>
> Pensez à effectuer le filtrage nécessaire au passage du trafic VPN sur les firewalls participant au tunnel.

Configuration des clés manuelles

Afin de compléter la configuration des tunnels VPN Statique, sélectionner la politique 1 dans l'arborescence pour accéder au menu de configuration des clés manuelles.

Dans la partie générale de la configuration, vous configurez les paramètres suivants :

Méthode de proposition	Cette option non modifiable indique que le protocole utilisé pour ce tunnel est le protocole ESP en mode tunnel.
Authentification	Algorithme utilisé pour garantir l'intégrité des données. Les firewalls NETASQ supportent les fonctions de hachage : • non_auth (pas d'authentification) • HMAC-SHA1 • HMAC-MD5 Vous configurez la clé statique correspondante en cliquant sur l'icône en forme de clé.
Chiffrement	Algorithme utilisé pour chiffrer les données. Les firewalls NETASQ proposent les algorithmes suivants : • null_enc • DES • 3-DES • BLOWFISH • CAST128 • AES **AVERTISSEMENT** NETASQ recommande vivement l'utilisation de l'AES car c'est l'algorithme le plus performant en termes de débit et aussi le plus sécuritaire. IL FAUT bien comprendre que les algorithmes présentés plus haut ne sont pas égaux en termes de performances et de débit. L'AES est actuellement le meilleur algorithme de chiffrement. Vous configurez la clé statique correspondante en cliquant sur l'icône en forme de clé.
SPI (données entrantes)	Identifiant du tunnel entrant. Valeur unique calculée par défaut par le-firewall.
SPI (données sortantes)	Identifiant du tunnel sortant. Valeur unique calculée par défaut par le firewall.
Keep alive (secondes)	Temps écoulé, en secondes, entre deux paquets envoyés au travers d'un tunnel VPN pour assurer le maintien de ce tunnel. Les paquets envoyés sont uniquement utilisés pour le maintien de connexion.

AVERTISSEMENT
Les valeurs des SPI doivent être inversées (entrant et sortant) dans la configuration du tunnel.

La clé manuelle est définie grâce à une fenêtre de saisie.

Dans l'onglet **`Extrémités du trafic`**, vous précisez quelles machines vont utiliser ce tunnel et éventuellement pour quel type de connexions.

Vous sélectionnez les machines ou réseaux locaux en cliquant sur la machine de gauche et les machines ou réseaux distants en cliquant sur la machine de droite.

AVERTISSEMENT
Dans un tunnel statique il est interdit d'avoir "Any" en correspondant.

CHAPITRE 4 : PPTP

8.4.1. Introduction

8.4.1.1. Principe

Le protocole **PPTP** permet de se connecter à distance sur le réseau local de manière sécurisée. Le poste client dispose d'un client **PPTP** (disponible sous Windows en standard ou MAC OSX) qui vient se connecter au firewall et identifier l'utilisateur.

L'utilisateur s'identifie par identifiant/mot de passe. Ces profils sont stockés sur le firewall, dans la base LDAP contenant les fiches des utilisateurs internes.

AVERTISSEMENT
L'utilisation d'IPSEC est préférable par rapport au PPTP car le niveau de sécurité est plus élevé.

8.4.2. Configuration

8.4.2.1. Mise en place

La mise en place est très simple et rapide. Elle se déroule en trois étapes :

Ce menu permet la configuration des paramètres suivants :

- Le pool d'adresses.
- Les paramètres de chiffrement.
- Le Serveur DNS et la résolution NetBIOS.

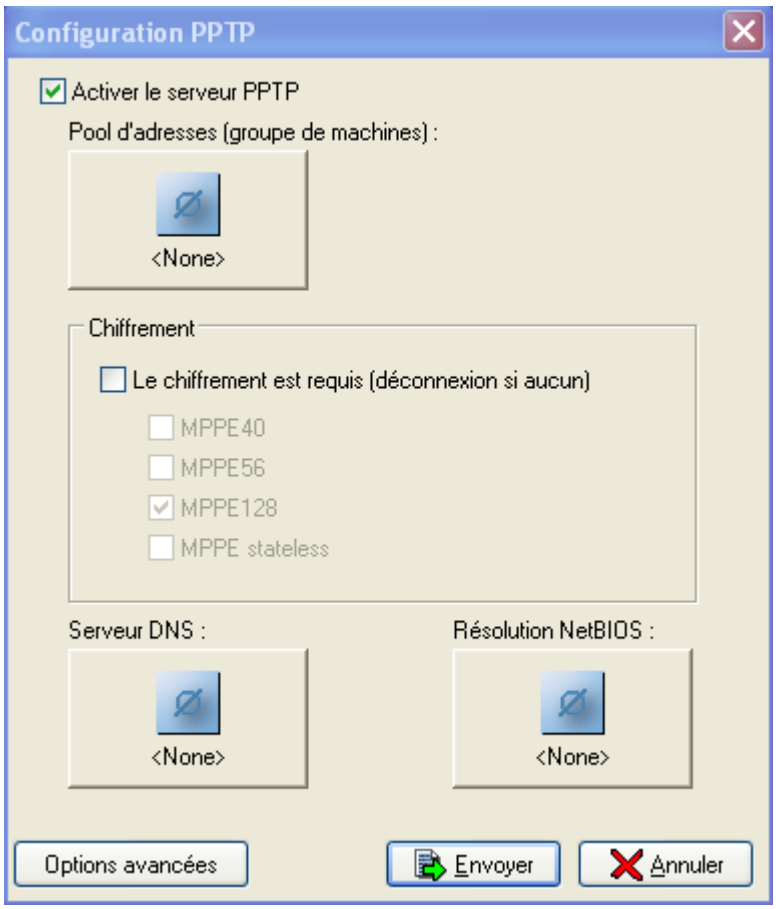


Figure 249 : Configuration PPTP

Etape 1 : Activation du serveur

Activation/Configuration du serveur **PPTP** sur le firewall. Cela est réalisé dans le menu **VPN \PPTP** en cochant Activer le serveur PPTP.

Etape 2 : Pool d'adresses

Une fois le serveur PPTP activé, il faut obligatoirement créer un pool d'adresses IP privées. Le firewall affecte au client qui vient se connecter en **PPTP** une adresse IP disponible dans le pool. Il faut créer un groupe de machines contenant les adresses réservées. (*Cf.* Assistant), ou une plage d'adresses provenant de la base objets.

Le pool d'adresses est un groupe de machines contenant les adresses IP réservées ou une plage d'adresses pour la connexion en **PPTP** (cf. *Etape 1*).

Etape 3 : Chiffrement (facultatif)

Activer un chiffrement permet d'établir une connexion entre les clients et le serveur.

Les paramètres de chiffrement possibles sont :

Le chiffrement est requis (déconnexion si aucun)	Autorise la connexion uniquement si le client chiffre les données.
MPPE40	Autorise l'utilisation du protocole de chiffrement MPPE 40 bits.
MPPE56	Autorise l'utilisation du protocole de chiffrement MPPE 56 bits.
MPPE128	Autorise l'utilisation du protocole de chiffrement MPPE 128 bits.
MPPE stateless	Permet de supprimer la conservation d'état du tunnel. Cela accélère un peu le chiffrement mais devient plus lent à reprendre en cas de perte de paquets.

Etape 4 : Le serveur DNS et la résolution NetBIOS

Le champ **Serveur DNS** permet d'envoyer l'adresse IP du serveur DNS au client.

Le champ **Résolution NetBIOS** permet d'envoyer au client l'adresse IP du serveur WINS du site.

Etape 5 : Profils utilisateurs

Création des profils utilisateurs. La connexion en PPTP est authentifiée par identifiant/mot de passe. Vous pouvez définir les mots de passe des utilisateurs PPTP dans les fiches utilisateur (*Cf.* *Partie 4/Chapitre 3 : Objets\Utilisateurs*.)

Etape 6 : Options avancées

Si vous souhaitez créer un nouveau serveur PPTP et que vous êtes arrivé au maximum du nombre dynamique de PPTP possible, vous avez la possibilité d'en augmenter le nombre.
NETASQ UNIFIED MANAGER vous propose l'écran des paramètres avancés lorsque ce nombre est atteint. Cet écran vous permet de régler le nombre dynamique de serveurs PPTP possible.

L'ajout d'un serveur PPTP s'effectue par tranche mais de manière complètement transparente pour l'utilisateur : par exemple, supposons que vous avez un boîtier U70. Dans ce cas, 48 serveurs PPTP maximum sont alloués en sortie d'usine mais 0 sont configurés. Supposons également que l'ajout des serveurs s'effectue par tranche de 8.
Vous souhaitez configurer un serveur :

- L'interface graphique de NETASQ UNIFIED MANAGER vous dirige vers l'écran des paramètres avancés pour augmenter le nombre de serveurs PPTP etvous avertit qu'il faut redémarrer le boîtier. Une tranche de 8 serveurs PPTP vous est allouée. Vous configurez le 1er serveur. Mais vous pouvez en configurer 7 autres sans qu'il y ait nécessité de redémarrer le firewall.
- Vous souhaitez configurer un 9éme serveur, une nouvelle tranche est alors nécessaire. Vous êtes averti que le firewall va redémarrer. Vous effectuerez ensuite la configuration du serveur.

A la sortie d'usine de votre boîtier, un nombre de serveurs maximum est alloué selon le modèle. Le tableau ci-dessous vous indique le nombre de serveurs alloué maximum :

Modèles	Nbre VLAN max
U30, U70	48
U120, U250, U450	96
U1100, U1500	192
U6000	192

Au niveau du panneau de configuration des interfaces réseaux se trouve le bouton **Options avancées** qui vous permet d'augmenter le nombre de serveurs.
Lorsque vous cliquez sur ce bouton, l'écran suivant s'affiche :

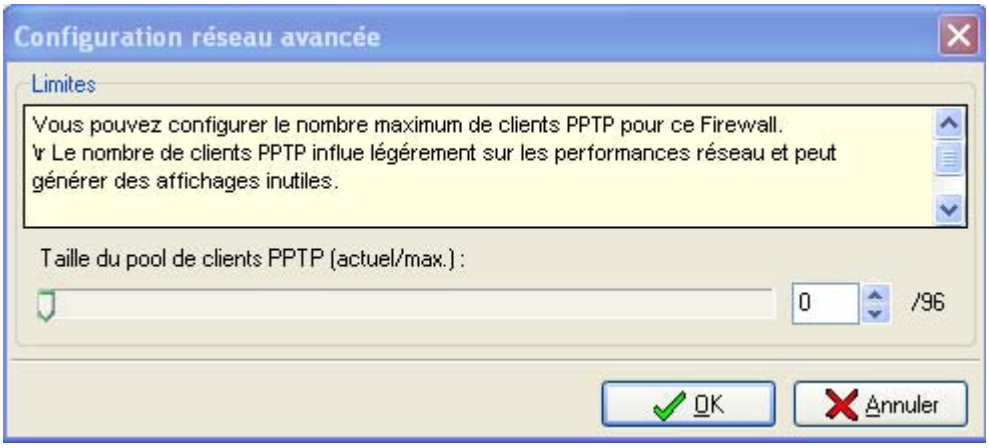


Figure 250 : paramètres avancés

Cet écran vous permet de choisir le nombre de VLAN souhaité. Il suffit de glisser la jauge pour augmenter ou diminuer le nombre. Si le nombre de VLAN indiqué correspond à une nouvelle tranche, dans ce cas, le firewall devra redémarrer avant configuration (pour un ajout ou une suppression).

AVERTISSEMENT
Toute modification réalisée au niveau de la configuration avant augmentation du nombre dynamique de serveurs PPTP sera perdue étant donné la fermeture de cet écran. Un message d'avertissement vous en informe.

CHAPITRE 5 : VPN SSL

8.5.1. Introduction

L'utilisation de la technologie IPSec nécessite l'intervention d'un administrateur sur les postes client par l'installation d'un logiciel de gestion de tunnels VPN. Cela est contraignant lorsque le nombre des postes client à équiper (installation, configuration et maintenance) est important, difficile lorsqu'on cherche à se procurer un tel client pour des périphériques tels que des PDA et coûteux car il nécessite l'achat de licences pour chaque station concernée.

Grâce à la technologie VPN SSL NETASQ et à un simple navigateur Web, l'utilisateur accède au portail d'authentification NETASQ qui lui permet de justifier son identité avant d'atteindre les ressources autorisées par l'administrateur. Les communications sont alors chiffrées en SSL, la confidentialité est assurée.

➲ La configuration de cette fonctionnalité est disponible grâce au menu **VPN\VPN SSL** de l'arborescence du Manager.

Le port utilisé est le port TCP 443. Les accès Web et les accès par l'applet Java utilisent le protocole SSL. La connexion s'effectue par le port 443. Cette modification a un impact sur les liens au sein des pages Web, accessibles depuis le VPN SSL. En effet, les liens sont modifiés au niveau de la partie « Host » (qui se trouve rarement dans les liens) et de la partie « Chemin ».

8.5.1.1. Utilisation du VPN SSL avec le firewall NETASQ

Cette fonctionnalité peut vous permettre d'accéder aux ressources protégées (par le firewall) de votre entreprise et cela sans installation d'un logiciel client sur le poste d'utilisation. Le cas d'utilisation le plus évident est celui d'un utilisateur nomade qui voudrait pouvoir récupérer ses mails alors qu'il est en déplacement. Cela est déjà possible grâce au VPN IPSEC mais nécessite l'installation d'un logiciel client qui pénalise l'utilisateur nomade. Grâce à la technologie VPN SSL, l'utilisateur nomade va désormais récupérer ses mails (ou visiter le site intranet de l'entreprise, accéder à un serveur privé, etc.) de manière sécurisée (les flux sont chiffrés) tout en ne nécessitant pas d'installation de logiciel client. L'utilisateur peut donc tout à fait se connecter depuis un cybercafé, un ordinateur qui ne lui appartient pas, etc.

8.5.1.2. Fonctionnement

La technologie VPN SSL est divisée en deux fonctionnalités suivant le type d'accès que vous désirez réaliser : un accès à des ressources de type Web (Intranet, Internet, etc.) ou d'autres accès (serveur mail, serveurs d'applications privées).

L'écran de configuration du VPN SSL se décompose en deux parties :

- A gauche un arbre présentant les diverses fonctionnalités du menu VPN SSL.
- A droite les options configurables.

8.5.2. Configuration

8.5.2.1. Global

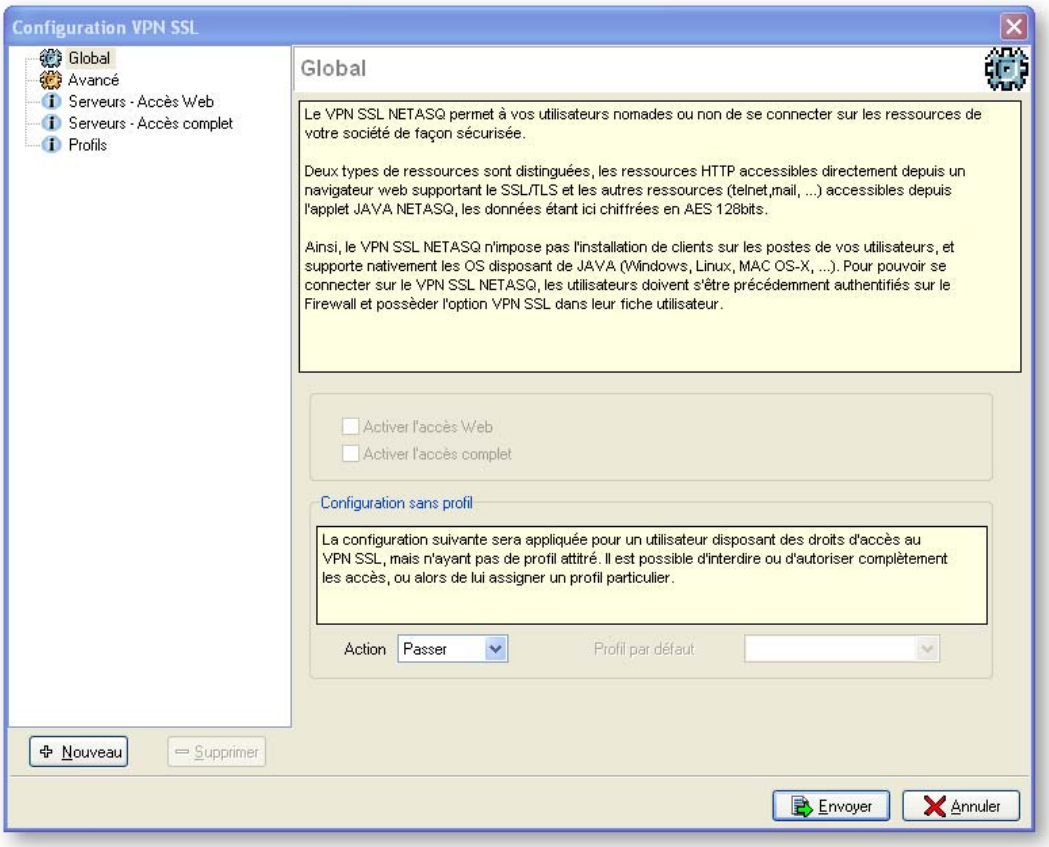


Figure 251 : Configuration VPN SSL – Global

Activation du VPN SSL

Activer l'accès Web	Utilisation du module de VPN SSL pour l'accès aux ressources de type Web.
Activer l'accès complet	Utilisation du module de VPN SSL pour l'accès aux ressources de type flux TCP.

La différence entre les deux technologies réside dans l'utilisation d'une applet JAVA pour l'accès aux ressources autre que le Web. Cette applet JAVA insérée dans les pages du portail Web NETASQ permet la redirection des flux vers les serveurs autorisés.

Configuration sans profil

Les options de la "Configuration sans profil" permettent de déterminer les différents accès aux fonctionnalités de VPN SSL des firewalls si l'utilisateur ne possède pas de profil spécifique défini dans sa fiche utilisateur (Cf. *Partie 4 : Objets*). Ces accès sont expliqués dans le tableau suivant :

Passer	Si l'action de la "Configuration sans profil" est "Passer" alors tous les serveurs configurés par l'administrateur seront vu par un utilisateur sans profil spécifique.
Bloquer	Si l'action de la "Configuration sans profil" est "Bloquer" alors aucun serveur configuré par l'administrateur ne sera vu par un utilisateur sans profil spécifique.
Défaut	Si l'action de la "Configuration sans profil" est "Défaut" alors les serveurs configurés par l'administrateur et faisant partie du "profil par défaut" seront vus par un utilisateur sans profil spécifique.

8.5.2.2. Avancé

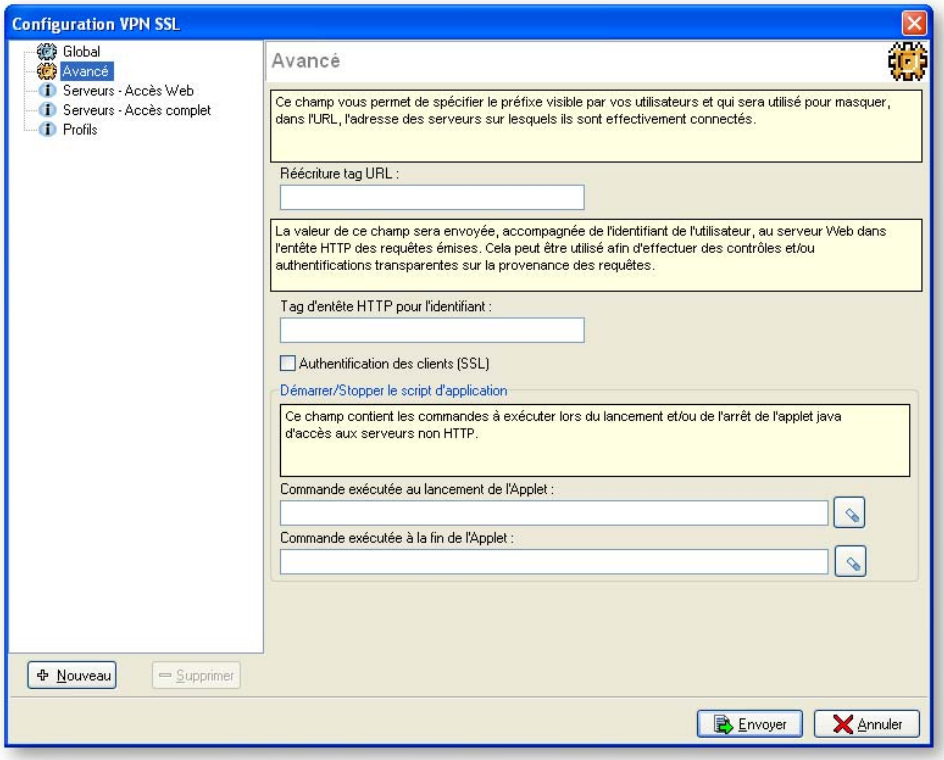


Figure 252 : Configuration VPN SSL - Avancé

Réécriture tag URL

La technologie VPN SSL NETASQ permet de masquer l'adresse réelle des serveurs vers lesquels les utilisateurs sont redirigés en réécrivant l'ensemble des URL contenues dans les pages HTTP rencontrées. Ces URL sont remplacées par un préfixe suivi de 4 chiffres. Ce champ permet de définir le préfixe qui sera utilisé.

Tag d'entête HTTP pour l'identifiant

La valeur de ce champ sera envoyée, accompagnée de l'identifiant de l'utilisateur, au serveur Web dans l'entête HTTP des requêtes émises. Cette valeur peut être utilisée afin d'effectuer des contrôles et/ou authentification transparentes sur la provenance des requêtes.

Dans le cas où le serveur vers lequel les flux HTTP sont redirigés demande une authentification, il est possible de spécifier un login dans l'entête du paquet HTTP. Ce login pourrait servir par exemple à indiquer que ces flux arrivant au serveur proviennent du firewall et peuvent être accepté par le serveur sans authentification.

Authentification des clients (SSL)

Si l'option **Authentification des clients (SSL)** est cochée, chaque requête transitant par le module de VPN SSL des firewalls NETASQ nécessite une authentification par certificat de l'utilisateur émetteur de la requête.

Commande exécutée au lancement de l'Applet

Exécutée au lancement de l'applet, cette commande permet à l'administrateur de définir des actions préalables à l'affichage de l'applet. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui modifierait les paramètres du compte de messagerie de l'utilisateur de telle façon que lorsque l'applet est lancée, les flux SMTP ou POP soit automatiquement redirigé, sans intervention de l'utilisateur.

Lorsque vous cliquez sur le bouton  , un assistant de configuration s'affiche :

Etape 1

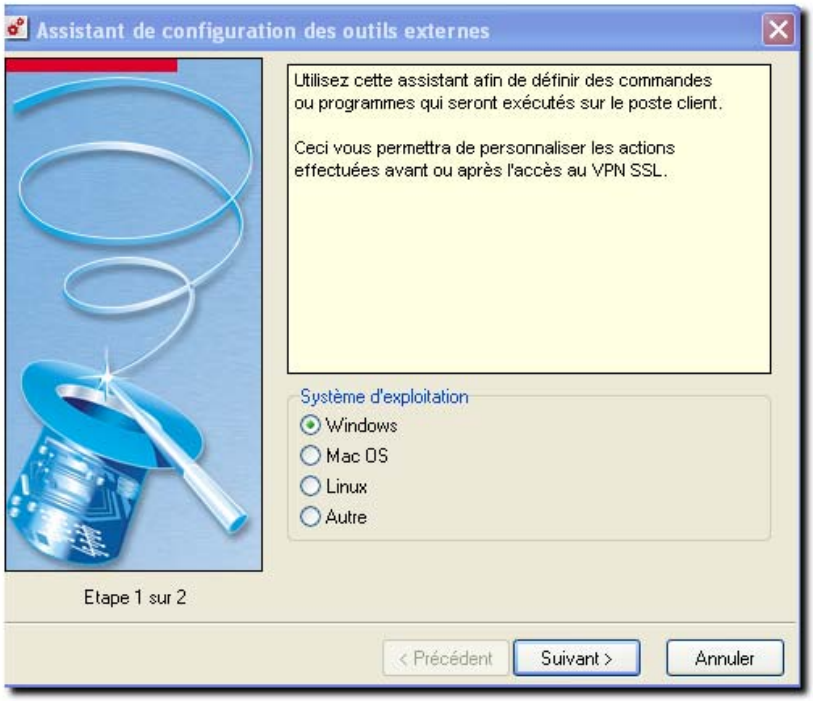


Figure 253 : Assistant de configuration des outils externes - Etape 1

Sélectionnez le système d'exploitation parmi les quatre choix possibles puis cliquez sur le bouton **Suivant**.

Etape 2

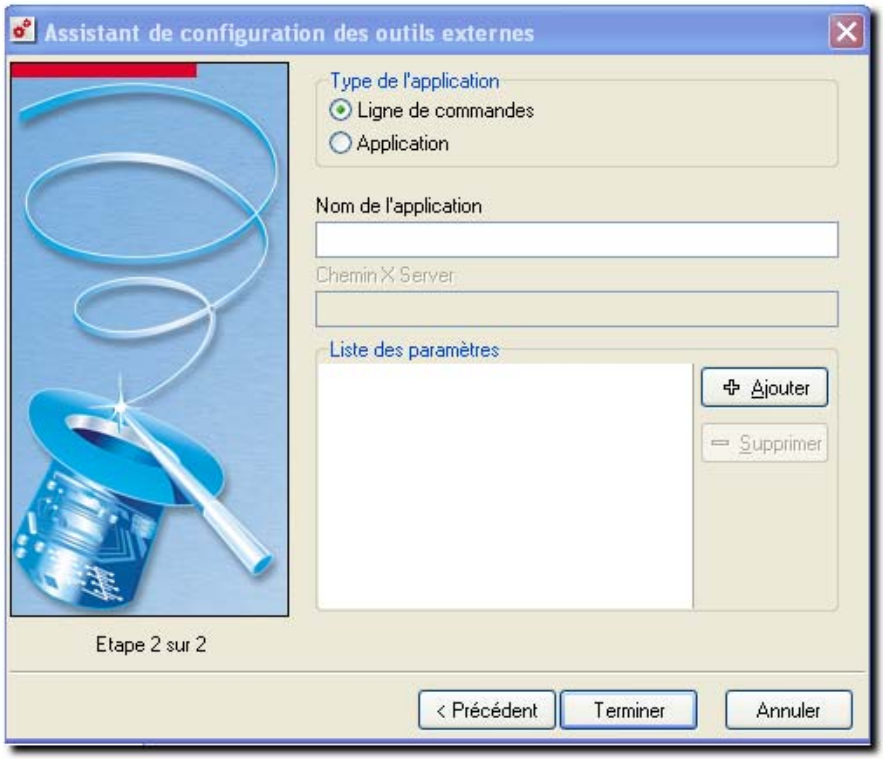


Figure 254 : Assistant de configuration - Etape 2

Déterminez le type de l'application entre **Ligne de commandes** et **Application**. Indiquez un nom pour l'application puis ajoutez une valeur pour le paramètre.

Commande exécutée à la fin de l'Applet

Exécutée à la fermeture de l'applet, cette commande permet à l'administrateur de définir des actions préalables à la fermeture de l'applet. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui modifierait les paramètres du compte de messagerie de l'utilisateur de telle façon que lorsque l'applet est fermée, les flux SMTP ou POP ne sont plus automatiquement redirigé et encore une fois sans intervention de l'utilisateur.

8.5.2.3. Serveurs-Accès Web

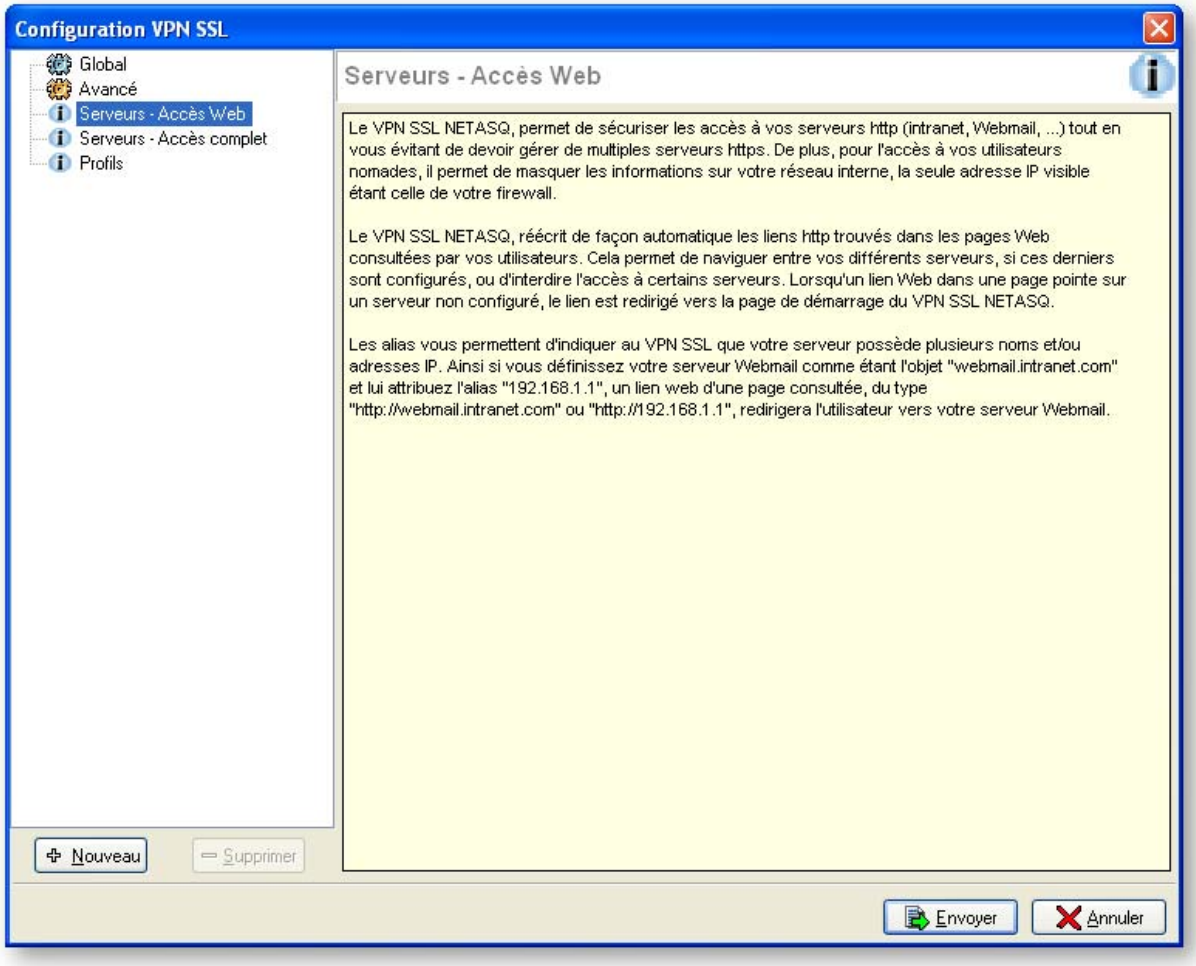


Figure 255 : Configuration VPN SSL - Serveurs- Accès Web

Cette section rassemble les serveurs configurés pour les accès aux ressources de type Web.

VPN SSL sert à la sécurisation de vos serveurs HTTP. Il évite aussi la gestion de plusieurs serveurs HTTPS. Il permet également de centraliser l'authentification de plusieurs serveurs. Il sert également aux utilisateurs nomades qui souhaitent accéder au réseau de l'entreprise à distance en masquant les informations du réseau interne.

Les liens HTTP sont réécrits de manière automatique. Ce qui permet de naviguer entre différents serveurs, s'ils sont configurés, ou d'interdire l'accès à certains serveurs. Si le lien pointe sur un serveur non configuré, dans ce cas, ce lien est redirigé vers la paged'erreur de type « Ce lien n'est pas autorisé par votre administrateur ».

Les alias permettent d'indiquer au VPN SSL que votre serveur possède plusieurs noms et/ou adresses IP.

Le nombre de serveurs Web configurables varie selon les modèles de boîtiers :

Modèle	Nbre max. serveurs HTTP	Nbre max. serveurs Autres
U30, U70	64	32
U120, U250, U450	128	64
U1100, U1500	256	128
U6000	512	256

Ajouter un serveur d'accès Web

Pour ajouter un serveur d'accès Web, suivez la procédure suivante :

1 Cliquez sur le bouton **Nouveau** situé en bas de la fenêtre de configuration du VPN SSL, puis sélectionnez **`Serveur HTTP`**. L'écran suivant s'affiche :

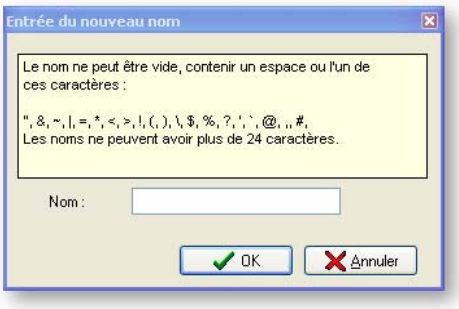


Figure 256 : Entrée du nouveau nom

2 Indiquez un nom pour ce serveur.
3 La configuration de ce serveur apparaît alors, les explications des différents paramètres sont données dans le tableau ci-dessous.

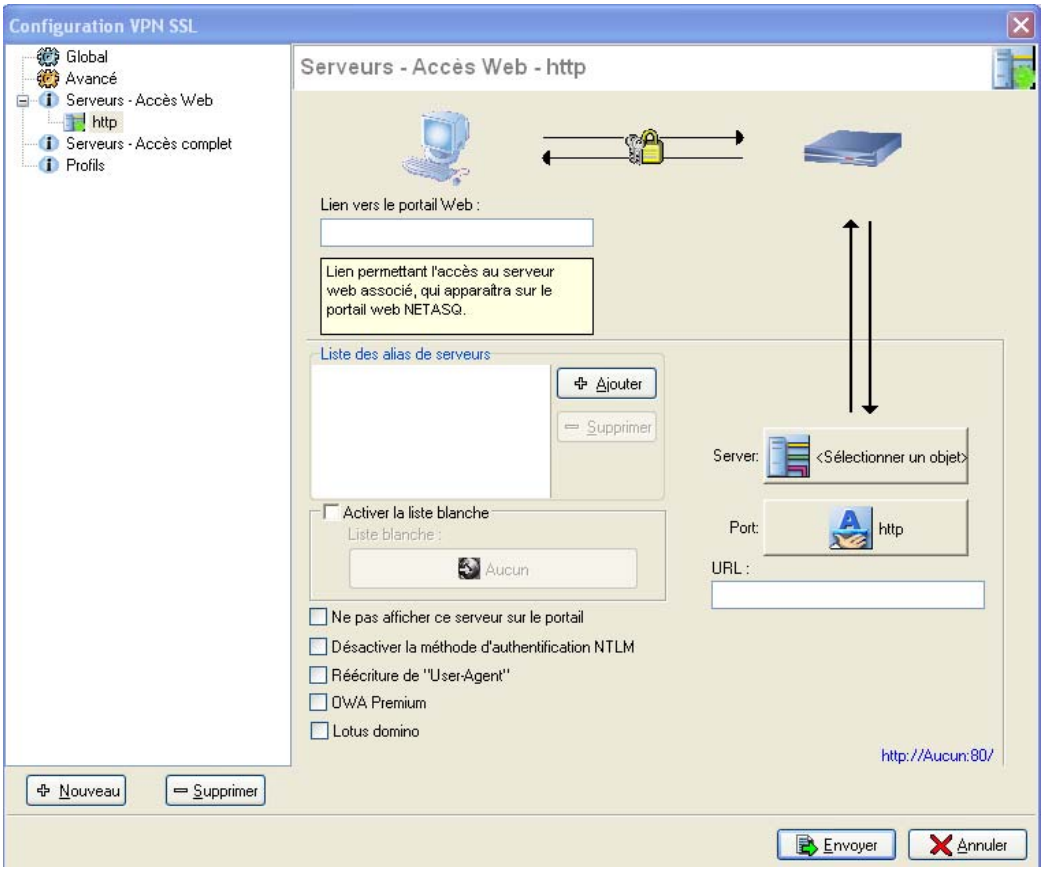


Figure 257 : Configuration VPN SSL - Serveurs- Accès web - HTTP

Lien vers le portail Web	Le lien défini apparaît sur le portail Web NETASQ. Lorsque l'utilisateur clique sur ce lien, il est redirigé vers le serveur correspondant.

Serveur	Le champ permet de spécifier l'objet correspondant au serveur auquel l'utilisateur pourra accéder. **AVERTISSEMENT** Veillez à utiliser un objet dont le nom est identique au nom **FQDN** du serveur auquel il fait référence. Si cela n'est pas le cas (nom de l'objet : webmail, nom FQDN : www.webmail.com par exemple), il est possible que les requêtes du firewall auprès de ce serveur soient refusées.
Port	Champ permettant de spécifier le port du serveur auquel l'utilisateur veut accéder. Le port défini est 80 pour http.
URL	Cette URL permet d'arriver directement sur la page spécifiée.
Liste des alias de serveurs	Les alias permettent d'indiquer au module VPN SSL que le serveur possède plusieurs noms et/ou adresses IP. Si un serveur de mails est défini comme l'objet « webmail.intranet.com » auquel on assigne l'alias "192.168.1.1", lorsque le lien visité sera « http://webmail.intranet.com » ou "http://192.168.1.1" l'utilisateur sera redirigé vers le serveur de mails. En cliquant sur le bouton **Ajouter**, l'écran qui s'affiche vous permet d'ajouter un nouvel alias.

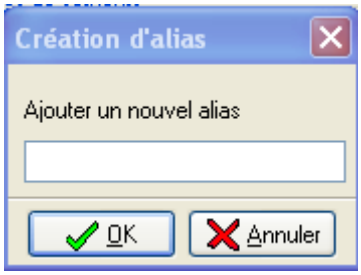


Figure 258 : Création d'alias

Activer la liste blanche	Seuls les liens réécrits par le module VPN SSL sont accessibles au travers du VPN SSL. S'il existe sur un site autorisé un lien vers un site Web extérieur (dont le serveur n'est pas défini dans la configuration VPN SSL), celui-ci sera inaccessible par le VPN SSL. Lorsque la liste blanche est activée, elle permet l'accès à des URL qui ne seraient pas réécrites. Par exemple, pour un accès vpnssl webmail, si l'on souhaite autoriser les utilisateurs à quitter le vpnssl en cliquant sur les liens contenus dans leurs mails, dans ce cas il faut ajouter une liste blanche contenant « * ». En cliquant sur le bouton **Liste blanche**, l'écran ci-dessous s'affiche :

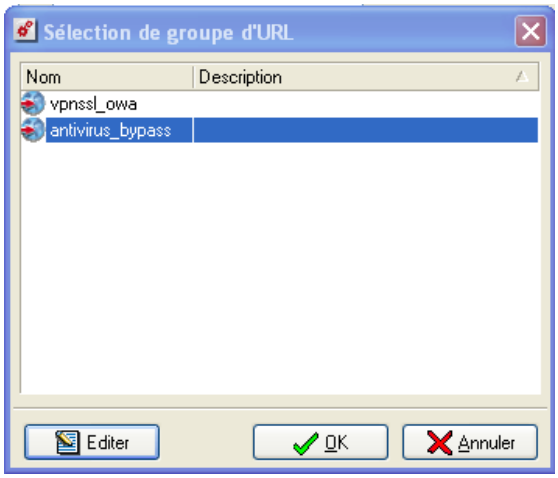


Figure 259 : Sélection de groupe d'URL

	Le bouton **Editer** de l'écran de sélection de groupe d'URL vous permet d'accéder à l'écran d'édition des Groupes d'URL. **AVERTISSEMENT** Lorsqu'un lien de cette liste blanche est cliqué par un utilisateur, celui-ci n'est plus protégé par le module de VPN SSL NETASQ.
Ne pas afficher ce serveur sur le portail	Tous les serveurs configurés dans la configuration du VPN SSL sont par défaut indiqués sur le portail d'authentification NETASQ. Toutefois il pourrait être nécessaire qu'un de ces serveurs ne soit accessible que par l'intermédiaire d'un autre serveur, alors, dans ce cas, il faudrait cocher l'option « Ne pas afficher ce serveur sur le portail ». En effet lorsque cette option est cochée dans la configuration d'un serveur, ce serveur est accessible par le VPN SSL mais n'est pas présent dans la liste d'accès direct. Il faut un lien sur un serveur vers ce serveur pour y accéder. Une application peut utiliser plusieurs serveurs mais n'avoir qu'un seul point d'entrée, donc un seul lien dans le menu du portail.
Désactiver la méthode d'authentification NTLM	Certains serveurs Web peuvent demander une authentification préalable au transfert de flux entre le serveur et l'utilisateur. Ne supportant pas cette méthode d'authentification pour les trafics traversant le firewall, celle-ci peut être désactivée. Ainsi l'utilisateur ne peut jamais choisir cette méthode pour son authentification sur le serveur Web distant.
Réécriture du "User Agent"	Le champ "User-Agent" de l'entête d'une requête HTTP contient l'identifiant de navigateur Web utilisé par l'utilisateur. Pour Internet Explorer par exemple : Mozilla/4.0 (compatible; MSIE 6.0 ...). La réécriture du "User-Agent" permet donc de modifier la requête HTTP de telle façon que l'on pense qu'elle provient d'un autre type de navigateur qu'en réalité. Cette option est notamment utile dans une utilisation dégradée d'Outlook **Web Access** (OWA). En effet, **Outlook Web Access** (OWA) en mode premium, mode très évolué d'Outlook **Web Access** fait appel au Webdav, une extension du protocole HTTP. Ces extensions n'étant pas supportées par tous les équipements réseau (le mode premium d'OWA est supporté par le module VPN SSL des firewalls NETASQ), le transit de ces trafics pourrait poser des problèmes de compatibilité en particulier sur Internet. Plutôt que de devoir dégrader l'utilisation d'OWA pour tous les utilisateurs (interne et externe), l'option **Réécriture du User-Agent** permet une utilisation "premium" de OWA en interne (compatibilité avec le mode premium facile à obtenir) et une utilisation "dégradée" en passant par le VPN SSL (utilisé par les utilisateurs nomades, via Internet). En effet les "vieux" navigateurs Web ne supportent pas ces extensions, OWA fonctionne donc automatiquement en mode dégradé lorsqu'il rencontre le "User-Agent" de ces navigateurs.
OWA Premium	En cochant cette option, vous activez les règles spécifiques de réécriture permettant de supporter Outlook Web Access en mode premium.
Lotus domino	En cochant cette option, vous activez les règles spécifiques de réécriture permettant de supporter les applications Web de Lotus domino.

Ajouter un serveur HTTP-OWA

Le module **VPN SSL** des firewalls NETASQ supporte les serveurs OWA ("Outlook Web Access").

DEFINITION OWA
(Outlook Web Access) permet aux utilisateurs d'utiliser leurs boîtes de messagerie professionnelle à distance par le biais d'une interface accessible sur un navigateur web. C'est un équivalent web du client mail Outlook.

Le mode « Premium » est utilisable sous Windows avec Internet Explorer 5 ou + uniquement. Il est basé sur les technologies web comme html, css, javascript mais également sur des technologies propriétaires Microsoft comme htc, xml, activeX.

En Exchange 2003, les liens sont des liens absolus que ce soit dans les pages HTML, les scripts javascripts, dans les données XML, dans les feuilles XSL. C'est-à-dire de type http://www.netasq.com/index.htm.

Il est donc possible d'ajouter dans la liste des serveurs d'accès Web, un serveur HTTP avec certaines options spécifiquement pré remplies pour une parfaite compatibilité avec OWA.

Pour ajouter un serveur HTTP-OWA, suivez la procédure suivante :

1 Cliquez sur le bouton **Nouveau** situé en bas de la fenêtre de configuration du VPN SSL, le menu contextuel ci-dessous s'affiche :

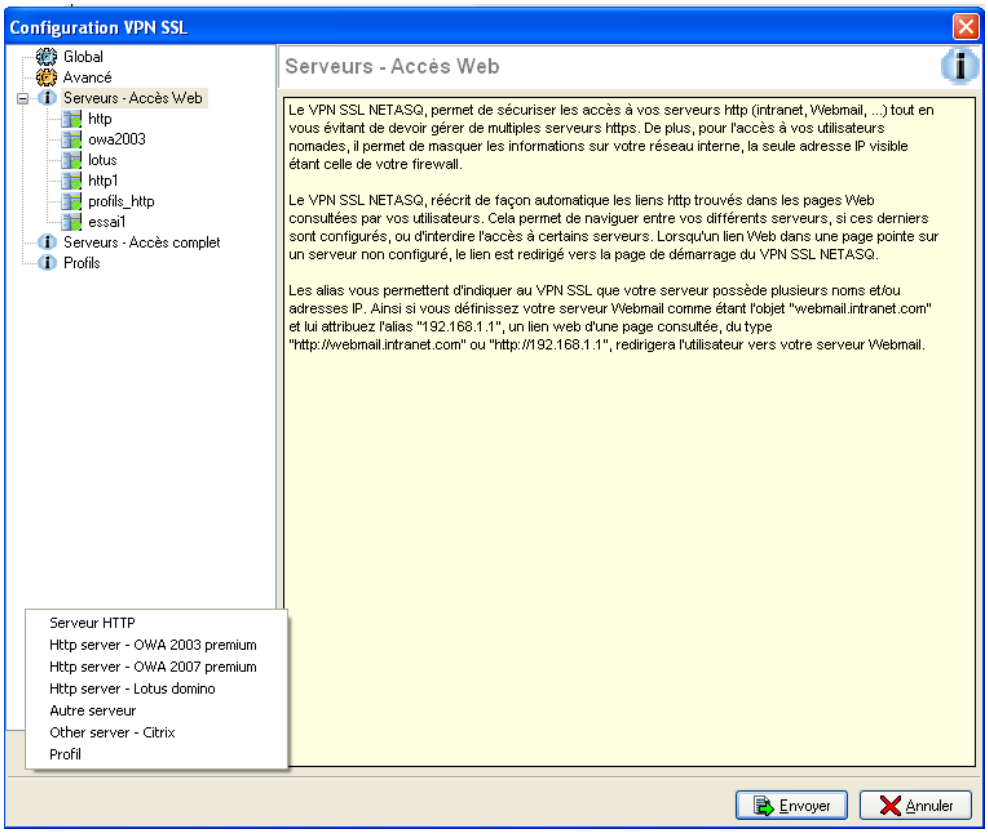


Figure 260 : Configuration VPN SSL - Serveurs - Accès Web

Sélectionnez **`Http server – OWA 2003`** ou **`Http server premium– OWA 2007 premium.`** L'écran suivant s'affiche :

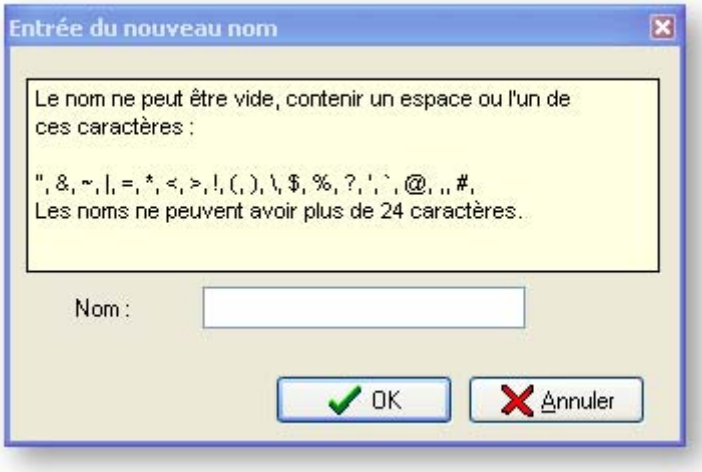


Figure 261 : Entrée du nouveau nom

2 Indiquez un nom pour ce serveur.

3 Les options pré-remplies pour un serveur OWA 2003 premium sont **Activer la liste blanche** avec l'indication du groupe d'URL « vpnssl_owa », le port « http », le champ URL avec l'indication "exchange", le champ **OWA Premium**. Pour un serveur OWA 2007, les champs préremplis sont **Activer la liste blanche** avec l'indication du groupe d'URL « vpnssl_owa », le port HTTP, l'URL avec l'indication "owa" et le champ « OWA Premium ».
Les autres options non remplies doivent être configurées de la même manière que pour un serveur d'accès Web "normal".

Ajouter un serveur HTTP-Lotus domino

Le module **VPN SSL** des firewalls NETASQ supporte les serveurs Lotus domino.

DEFINITION LOTUS DOMINO
Serveur applicatif d'IBM de Lotus.

Il est possible d'ajouter dans la liste des serveurs d'accès Web, un serveur HTTP avec certaines options spécifiquement pré remplies pour une parfaite compatibilité avec LOTUS DOMINO.

Pour ajouter un serveur HTTP-Lotus domino, suivez la procédure suivante :

1 Cliquez sur le bouton **Nouveau** situé en bas de la fenêtre de configuration du VPN SSL, le menu contextuel ci-dessous s'affiche :

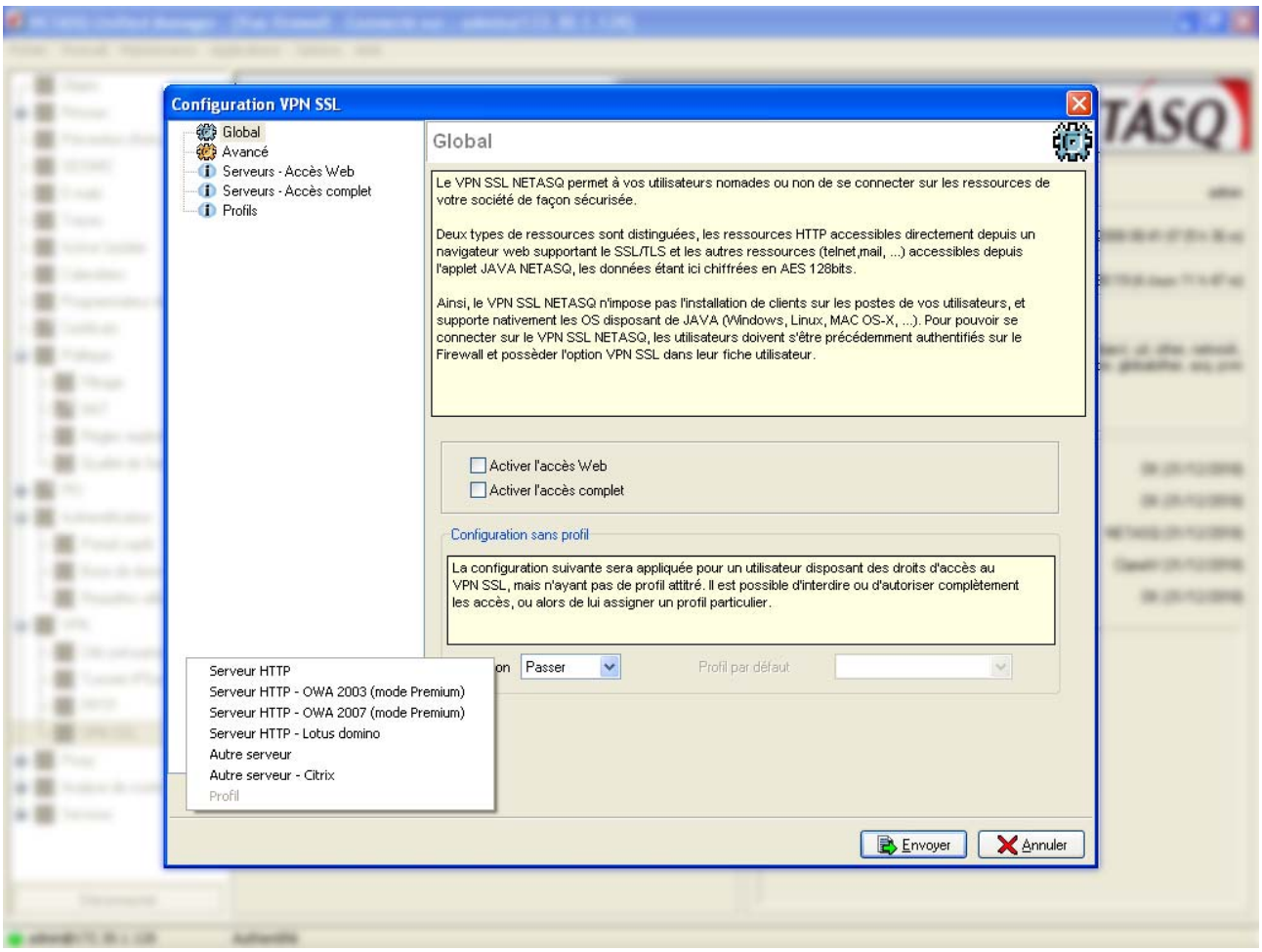


Figure 262 : Configuration VPN SSL - Serveurs - Accès Web

Sélectionnez **`Http serveur-Lotus domino.`** L'écran suivant s'affiche :

Figure 263 : Entrée du nouveau nom

2 Indiquez un nom pour ce serveur.

3 Les options pré-remplies pour un serveur Lotus domino sont le champ « Lotus domino », coché par défaut.

8.5.2.4. Accès complet

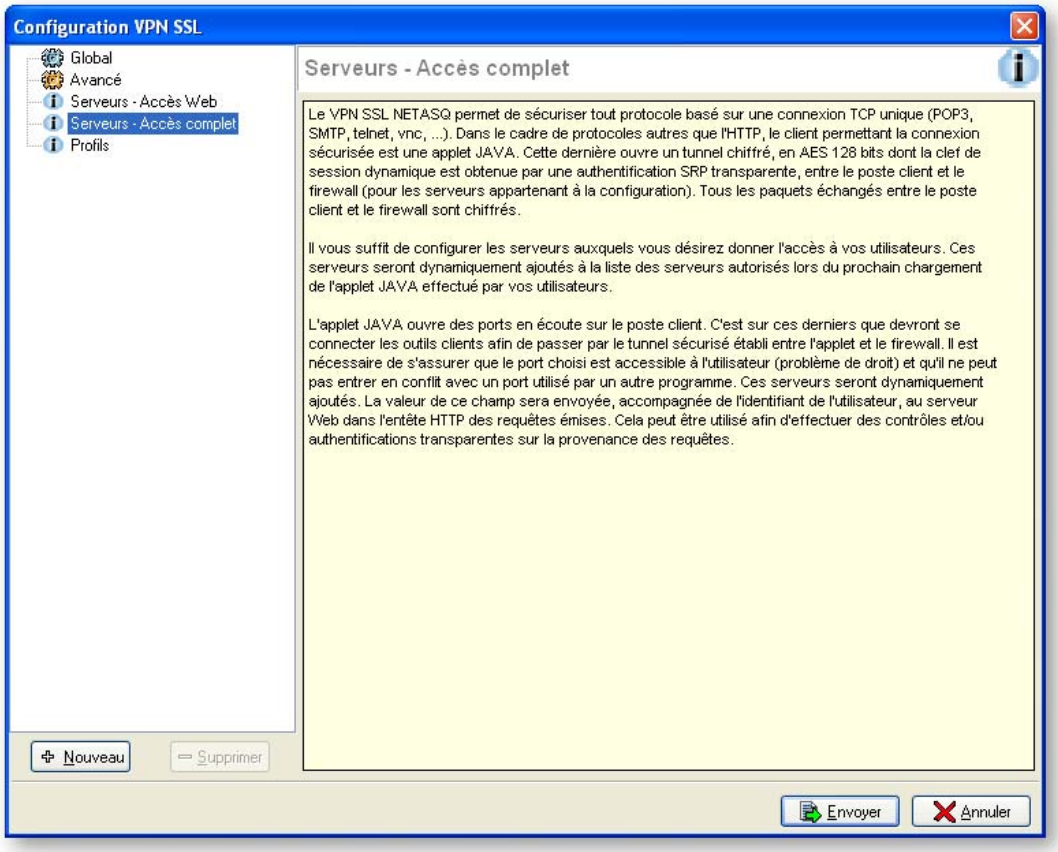


Figure 264 : Configuration VPN SSL - Accès complet

Le VPN SSL NETASQ permet de sécuriser tout protocole basé sur une connexion TCP unique (POP3, SMTP, telnet, accès distant, ...). Dans le cadre de protocoles autres que l'HTTP, le client permettant la connexion sécurisée est une applet JAVA. Cette dernière ouvre un tunnel chiffré. Tous les paquets échangés entre le poste client et le firewall sont chiffrés.

Il vous suffit de configurer les serveurs auxquels vous désirez donner l'accès à vos utilisateurs. Ces serveurs seront dynamiquement ajoutés à la liste des serveurs autorisés lors du prochain chargement de l'applet JAVA effectué par vos utilisateurs.

L'applet JAVA ouvre des ports en écoute sur le poste client. C'est sur ces derniers que devront se connecter les outils clients afin de passer par le tunnel sécurisé établi entre l'applet et le firewall. Il est nécessaire de s'assurer que le port choisi est accessible à l'utilisateur (problème de droit) et qu'il ne peut pas entrer en conflit avec un port utilisé par un autre programme. Ces serveurs seront dynamiquement ajoutés. La valeur de ce champ sera envoyée, accompagnée de l'identifiant de l'utilisateur, au serveur Web dans l'entête HTTP des requêtes émises. Cela peut être utilisé afin d'effectuer des contrôles et/ou authentifications transparentes sur la provenance des requêtes.

Cette section rassemble les serveurs configurés pour les accès aux ressources autres que le type Web.

Ajouter un serveur d'accès aux ressources autres que le type Web

Pour ajouter un serveur d'accès aux ressources autres que le type Web, suivez la procédure suivante :

1 Cliquez sur le bouton **Nouveau** situé en bas de la fenêtre de configuration du VPN SSL, puis sélectionnez **`Autre Serveur.`** L'écran suivant s'affiche :

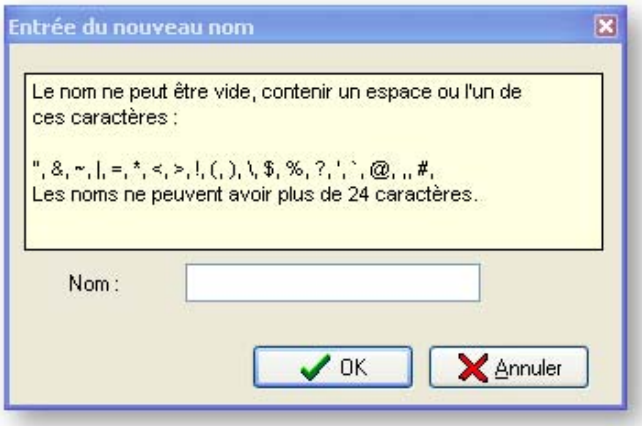


Figure 265 : Entrée du nouveau nom

2 Indiquez un nom pour ce serveur.

3 La configuration de ce serveur apparaît alors, les explications des différents paramètres sont données dans le tableau ci-dessous.

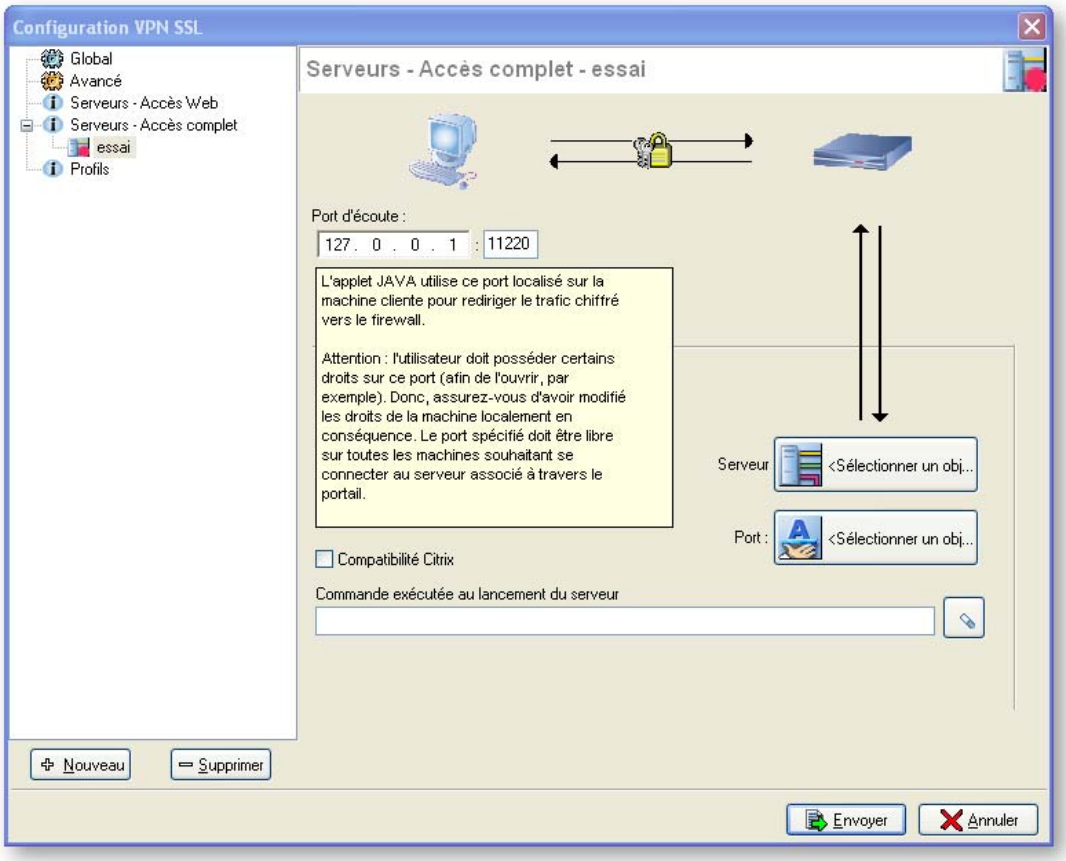


Figure 266 : Configuration VPN SSL - Serveurs - Accès complet

Port d'écoute	Ce port situé sur la station distante est utilisé par l'applet JAVA pour la redirection des flux chiffrés à destination du firewall NETASQ. Notez que l'utilisateur doit posséder certains droits sur ce port (pour l'ouverture par exemple), veillez donc à modifier les droits locaux d'administration de la machine en conséquence. De plus, le port spécifié doit être libre d'utilisation sur toutes les machines désirant se connecter

	au serveur associé via le portail.
Serveur	Ce champ permet de spécifier l'objet correspondant au serveur auquel l'utilisateur pourra accéder.
Compatibilité Citrix	Permet d'activer la compatibilité avec le portail Web d'authentification Citrix et l'accès via navigateur Web. Cette option est inutile si le client lourd Citrix est utilisé.
Port	Ce champ permet de spécifier le port sur le serveur auquel l'utilisateur pourra accéder.
Commande exécutée au lancement du serveur	Exécutée au lancement de l'applet, cette commande permet à l'administrateur de définir des actions préalables à l'affichage du serveur. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui vérifierait l'activité de l'antivirus présent sur la machine de l'utilisateur avant de lui donner accès au serveur.

Exemple de configuration avec un serveur Citrix

DEFINITION

Citrix Presentation Server est un produit conçu par la société Citrix systems.

Ce logiciel serveur permet de déployer des programmes sur un réseau afin d'y accéder à distance à partir de clients légers (accès via le navigateur web) ou clients lourd (application installée).

Son principe de fonctionnement est le suivant :

- Installation et lancement d'une application sur le serveur. Cette application utilise donc les ressources du serveur.
- Par le réseau local, le poste client reçoit l'affichage et les outils de cette application pour pouvoir y travailler via un portail Web et après s'être connecté.

L'avantage est donc de rendre disponibles des programmes sans avoir à les installer sur chaque poste client où moins de ressources sont utilisées.

Citrix peut fonctionner selon deux modes :

- En mode client léger (portail Web Citrix)
- En mode client lourd (application installée sur le poste client)

Etape 1 : Création d'un objet pour le serveur Citrix

Accédez à la base d'objets afin de créer une machine puis sélectionnez une machine.

Etape 2 : Configuration d'un Serveur-Accès complet

Accédez au menu de l'arborescence du Manager **VPN\VPN SSL**. Sélectionnez **Serveurs-Accès complet.** L'écran ci-dessous s'affiche :

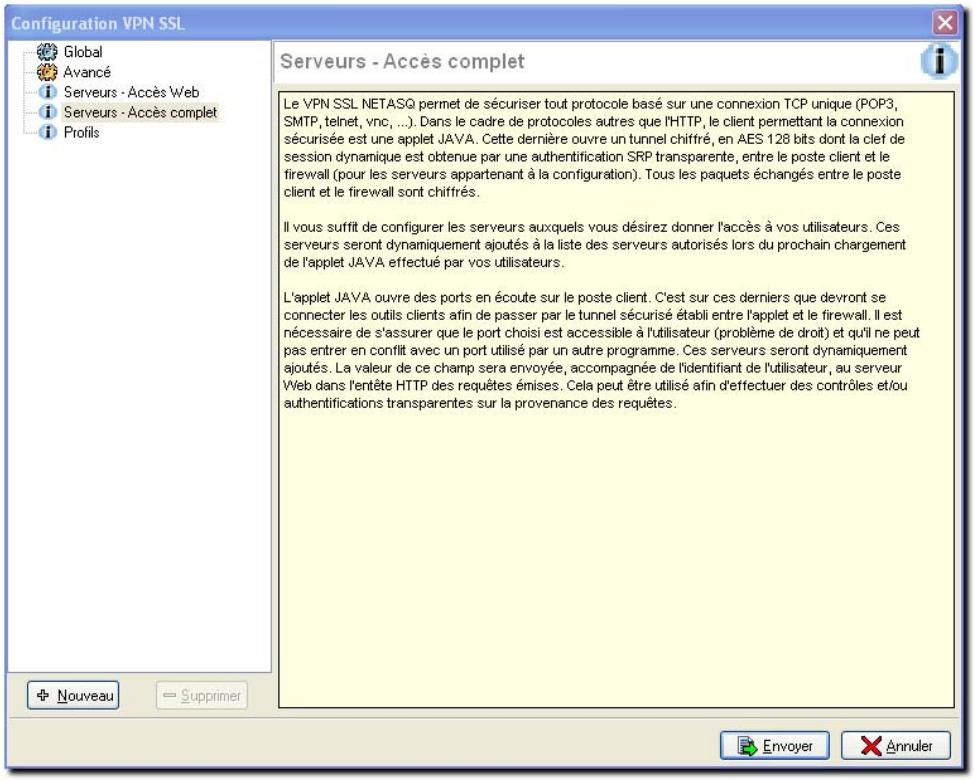


Figure 267 : Configuration VPN SSL - Serveurs - Accès complet

Cliquez sur le bouton **Nouveau** puis sélectionnez "Autre serveur-Citrix". Donnez un nom à votre serveur. L'écran de configuration du serveur Citrix s'affiche :

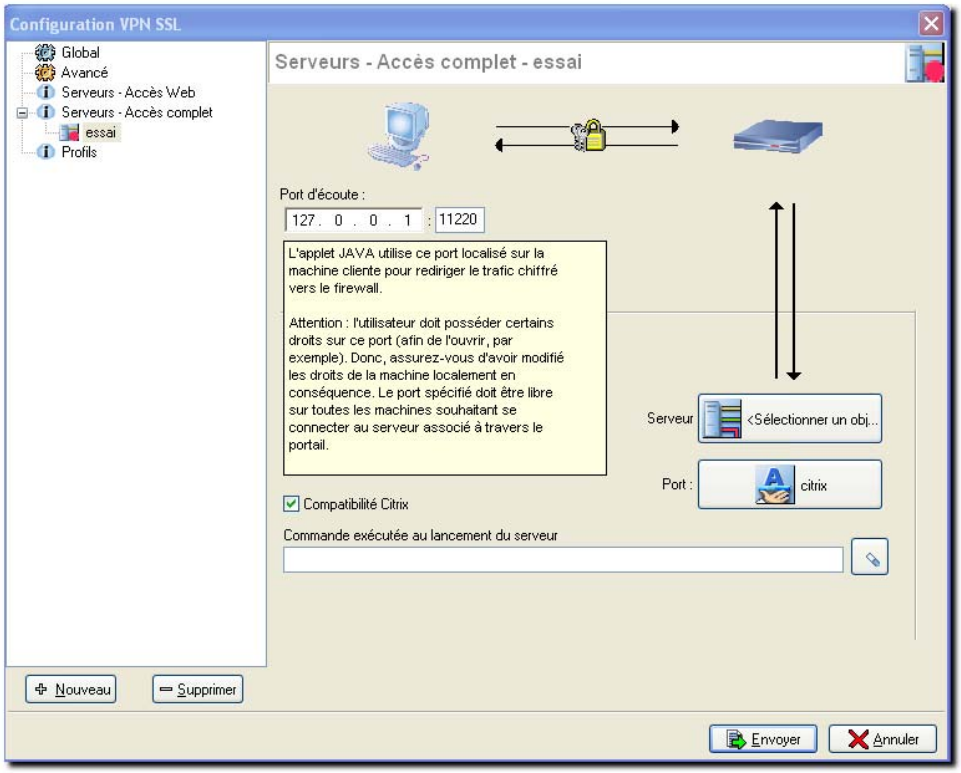


Figure 268 : Configuration VPN SSL - Serveurs - Accès complet

Sélectionnez le serveur Citrix créé précédemment dans la base d'objets.

Etape 3 : Configuration d'un Serveur-Accès Web

Sélectionnez dans l'arborescence de la configuration "VPN SSL" **Serveurs-Accès Web**. L'écran ci-dessous s'affiche :

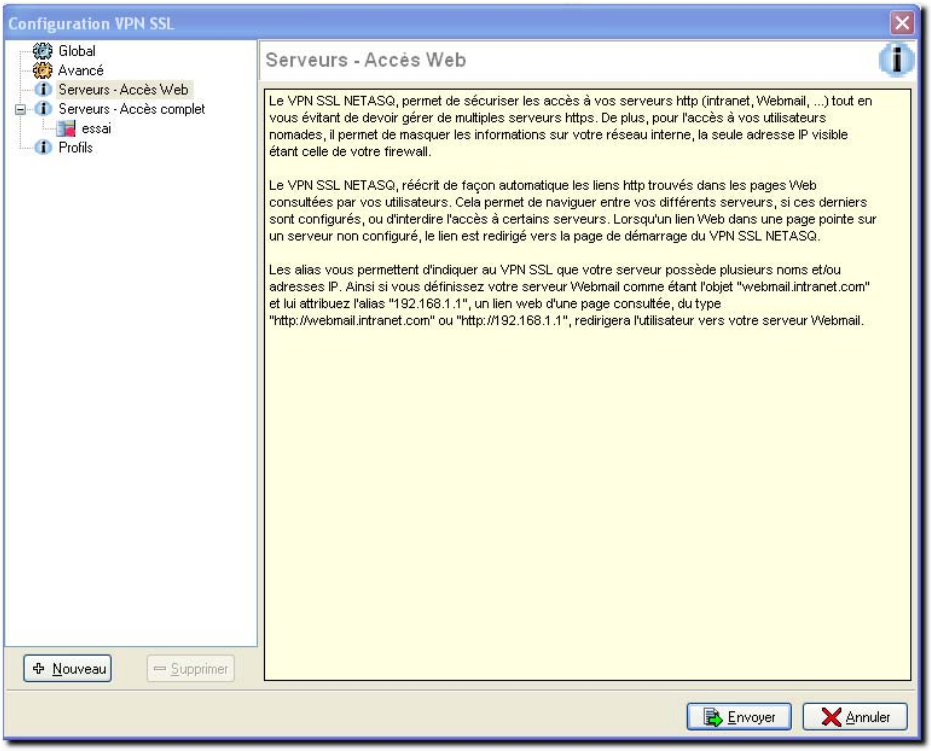


Figure 269 : Configuration VPN SSL - Serveurs - Accès Web

Cliquez sur le bouton **Nouveau** puis sélectionnez "Serveur HTTP". Donnez un nom à votre serveur. L'écran de configuration du serveur Web s'affiche :

A l'aide du bouton **Serveur**, sélectionnez votre serveur Web. Au niveau de l'URL, indiquez CitrixAccess/auth/login.aspx (s'il s'agit de la version Presentation Server 4.0).

4 Envoi de la configuration

Cliquez sur le bouton **Envoyer**.

5 Accès au portail Web

Ouvrez un navigateur Web puis identifiez –vous (https://adresse IP de votre firewall ou son nom).
Allez dans "Accès sécurisé" puis sélectionnez dans la liste déroulante "Ouvrir l'accès sécurisé dans un pop-up".

AVERTISSEMENT
Il est important que l'applet VPNSSL NETASQ fonctionne en tache de fond.

Sélectionnez ensuite **Accès portail\Portail** puis saisissez votre nom d'utilisateur, votre mot de passe et le domaine.

NOTE
A partir du portail Citrix, les applications de la Suite d'Administration sont disponibles par un simple clic sur des icônes.

8.5.2.5. Retirer un serveur

Pour supprimer un serveur, suivez la procédure suivante :

1. Sélectionnez le serveur à supprimer.
2. Cliquez sur le bouton **Supprimer**. Le message suivant s'affiche :

   "Supprimer ce serveur ?"

3. Cliquez sur **Oui** pour confirmer la suppression.

AVERTISSEMENT
Lorsqu'un serveur est retiré de la liste des serveurs VPN SSL configurés, il est automatiquement retiré des profils auxquels il faisait partie.

8.5.2.6. Profils

Si vous souhaitez restreindre l'accès aux serveurs définis dans la configuration du VPN SSL, vous devez définir des profils contenant la liste des serveurs autorisés, puis de les attribuer aux autilisateurs.

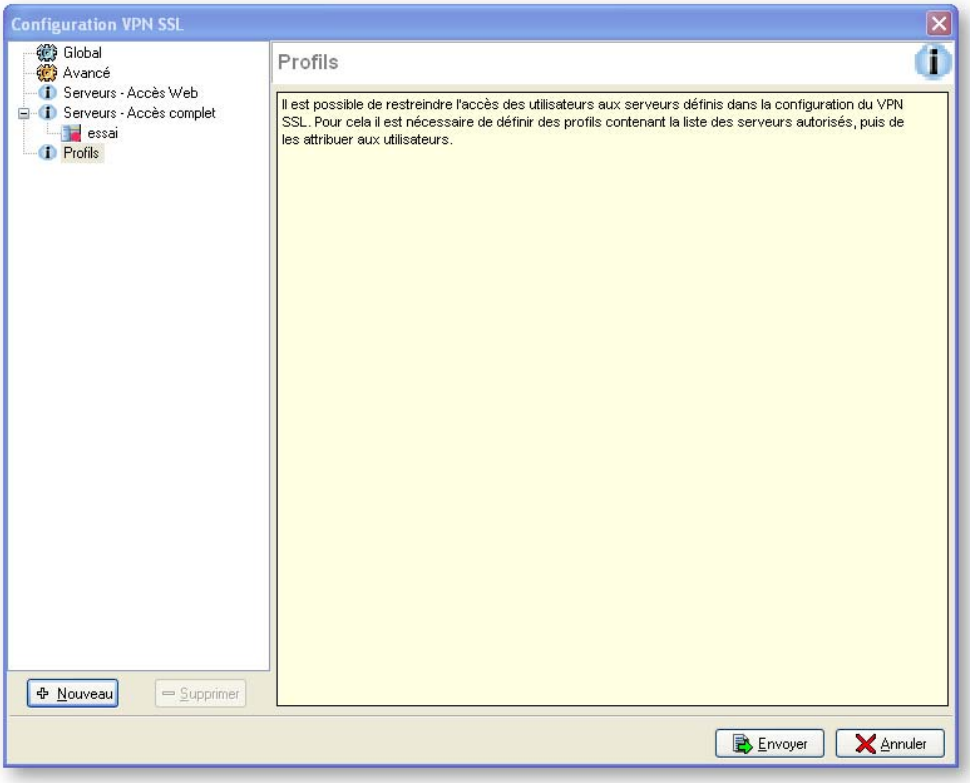


Figure 270 : Configuration VPN SSL – Profils

Principe de fonctionnement

Par défaut tous les serveurs configurés dans le module VPN SSL sont affichés sur le portail d'authentification. Ainsi tous les utilisateurs ayant droit aux fonctionnalités de VPN SSL offertes au firewall ont accès à tous les serveurs configurés par l'administrateur. La notion de profil permet de déterminer quels utilisateurs auront accès à quels serveurs configurés dans le VPN SSL.

Configurer un profil

Ajouter un profil

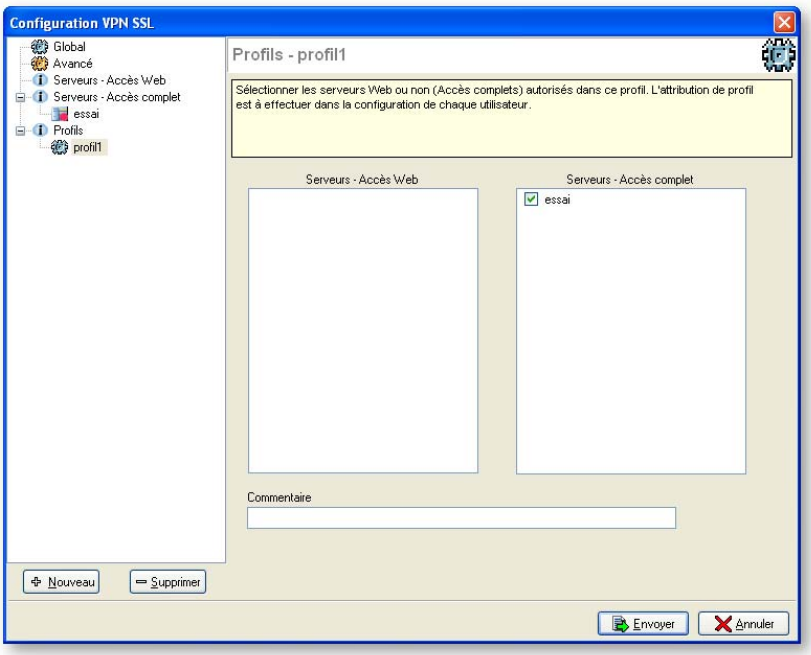


Figure 271 : Configuration VPN SSL - Profils

Pour ajouter un profil dans la liste des profils VPN SSL disponibles, référez-vous à la procédure suivante :

1. Cliquez sur le bouton **Nouveau** situé en bas de la fenêtre de configuration du VPN SSL, puis spécifiez le nom du profil en accord avec les recommandations indiquées par la fenêtre de définition du nom du profil.
2. Sélectionnez dans les listes de serveurs d'accès Web et d'accès complet, les serveurs qui seront accessibles aux utilisateurs appartenant à ce profil.
3. Cliquez sur **Envoyer** pour activer la configuration.

AVERTISSEMENT
Il est impossible de créer un profil s'il n'existe pas au minimum 1 serveur VPN SSL configuré.

Supprimer un profil

Pour supprimer un profil, référez-vous à la procédure suivante :

1. Sélectionnez le profil à supprimer.
2. Cliquez sur le bouton **Supprimer**.

Utiliser un profil

Un profil peut être utilisé de 2 manières différentes. Soit il est utilisé comme profil par défaut dans la configuration du VPN SSL, soit il est assigné à un ou plusieurs utilisateurs comme profil spécifique de ces utilisateurs.

Utiliser un profil comme profil par défaut

Pour utiliser un profil comme profil par défaut de la configuration VPN SSL (tous les utilisateurs n'utilisant pas de profil spécifique seront affectés par ce profil par défaut), référez-vous à la procédure suivante :

1. Définissez le profil qui sera utilisé comme profil par défaut (nom du profil et serveurs associés) dans le menu de configuration des profils.
2. Dans le menu **Global** de la configuration VPN SSL, sélectionnez l'action **Défaut** de la configuration sans profil.
3. Indiquez le profil, que vous avez préalablement défini, dans l'option **Profil par défaut**, puis cliquez sur **Envoyer** pour appliquer les modifications.

Utiliser un profil comme profil spécifique d'un ou plusieurs utilisateurs.

Pour utiliser un profil comme profil spécifique d'un ou plusieurs utilisateurs (quelle que soit la liste des serveurs définis par le profil par défaut, ces utilisateurs posséderont une liste de serveurs spécifiques), référez-vous à la procédure suivante :

1. Définissez le profil qui sera utilisé comme profil par défaut (nom du profil et serveurs associés) dans le menu de configuration des profils puis appliquez les modifications en cliquant sur **Envoyer**.
2. Sélectionnez, dans la liste des utilisateurs du menu **Objets** de l'arborescence des menus du NETASQ UNIFIED MANAGER, l'utilisateur auquel vous désirez associer le profil préalablement défini.
3. Sélectionnez l'onglet **Accès** de sa fiche utilisateur et cochez l'option **Par VPN SSL** (si cela n'est pas déjà fait).
4. Cochez l'option **Utiliser un profil spécifique** et indiquez le profil que vous désirez associer à cet utilisateur, puis cliquez sur **Envoyer** pour appliquer les modifications.

8.5.2.7. Services VPN SSL sur le portail Web NETASQ

Lorsque l'authentification sur le firewall est activée (Cf. Partie 12 : Authentification) ASQ permet aux utilisateurs d'accéder aux fonctionnalités du VPN SSL NETASQ.

Pour accéder aux fonctionnalités du **VPN SSL**, suivez la procédure suivante :

1. Ouvrir un navigateur Web.
2. Indiquer dans la barre d'adresse, l'URL : https://Adresse_Firewall.
3. La page d'authentification sur le firewall apparaît, l'utilisateur doit se connecter.
4. Si l'utilisateur possède des droits sur l'utilisation des fonctionnalités VPN le menu **Accès sécurisé** apparaît, il permet d'accéder aux fonctionnalités VPN SSL.

Ce menu présente les sites Web configurés par l'administrateur et auxquels les utilisateurs peuvent accéder.

Les autres accès sécurisés sont ici permet d'accéder au menu des autres sites sécurisés configurés par l'administrateur.

Accédez aux ressources de votre entreprise par un tunnel SSL

Ce menu présente les autres serveurs configurés par l'administrateur et auxquels les utilisateurs peuvent accéder.

> **AVERTISSEMENT**
> Sur cette page aucun lien n'est disponible. Il est pourtant indispensable que cette fenêtre reste ouverte pendant toute la durée de la connexion (elle peut être minimisée). La fermeture de la fenêtre entraîne la coupure de la connexion.

Pour accéder aux ressources configurées par l'administrateur, il s'agit d'indiquer au logiciel client, un client de messagerie par exemple, que le serveur auquel il doit se connecter pour récupérer les mails n'est plus le serveur mail habituel mais il faut lui indiquer une adresse du type "127.0.0.1:Port_Ecoute" où "Port_Ecoute" est le port spécifié dans la configuration du serveur.

Le port d'écoute pour chacun des serveurs configurés est rappelé dans la page du portail Web NETASQ.

PARTIE 9 : CONFIGURATION DES PROXIES

CHAPITRE 1. PRESENTATION

Le proxy est un système qui a pour fonction de relayer des connexions qu'il intercepte ou qui lui sont adressées. Ainsi le proxy se substitue à l'initiateur de la connexion et recrée intégralement une nouvelle connexion vers la destination initiale. Les systèmes proxy peuvent notamment être utilisés pour réaliser de l'analyse antivirus ou du filtrage des connexions.

Le module « Proxy » disponible sur les firewalls NETASQ permet la configuration des proxies HTTP, SMTP POP3 et FTP.

- Le proxy HTTP est lié aux sites visités et aux pages web demandées. A l'aide de ce module, il est possible d'effectuer de l'antivirus mais aussi du filtrage d'URL.
- Le proxy SMTP est lié à l'envoi de mails. Il est possible d'effectuer de l'antivirus et de l'antispam.
- Le proxy POP3 est lié à la réception des mails. Il est possible d'effectuer de l'antivirus et de l'antispam.
- Le proxy FTP est lié au transfert de fichiers. Il est possiple d'effectuer de l'antivirus.

9.1.1. Pour cette partie, vous devez avoir franchi les étapes

- Partie 2 : Installation, pré-configuration, intégration
- Partie 4 : Objets

9.1.2. Utilité de cette partie

Cette partie vous permet d'activer les proxies HTTP, SMTP, FTP, de rediriger les flux HTTP vers des serveurs proxies externes et de filtrer les flux SMTP et POP3.

9.1.3. Accéder à cette partie

➲ Accédez au menu **Proxy** depuis l'arborescence des menus de NETASQ UNIFIED MANAGER.

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications.

Avant d'effectuer toute modification importante sur votre firewall NETASQ, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez vous retrouver dans l'état précédent. Pour plus d'informations sur les sauvegardes, veuillez vous référer au chapitre Sauvegarde.

9.1.4. Introduction à cette partie

Les tables de filtrage URL sont stockées sur le firewall NETASQ dans des slots (fichiers de configuration numérotés de 01 à 10).

Chaque slot peut être programmé à une heure précise de la semaine, en écrasant la configuration du slot précédemment activée. (*Cf.* Partie 7/Chapitre 3 : *Programmateur de slots*)

9.1.5. L'écran des proxies

Cet écran est divisé en deux parties :

- A gauche un arbre présentant les diverses fonctionnalités des divers proxies.
- A droite les options configurables.

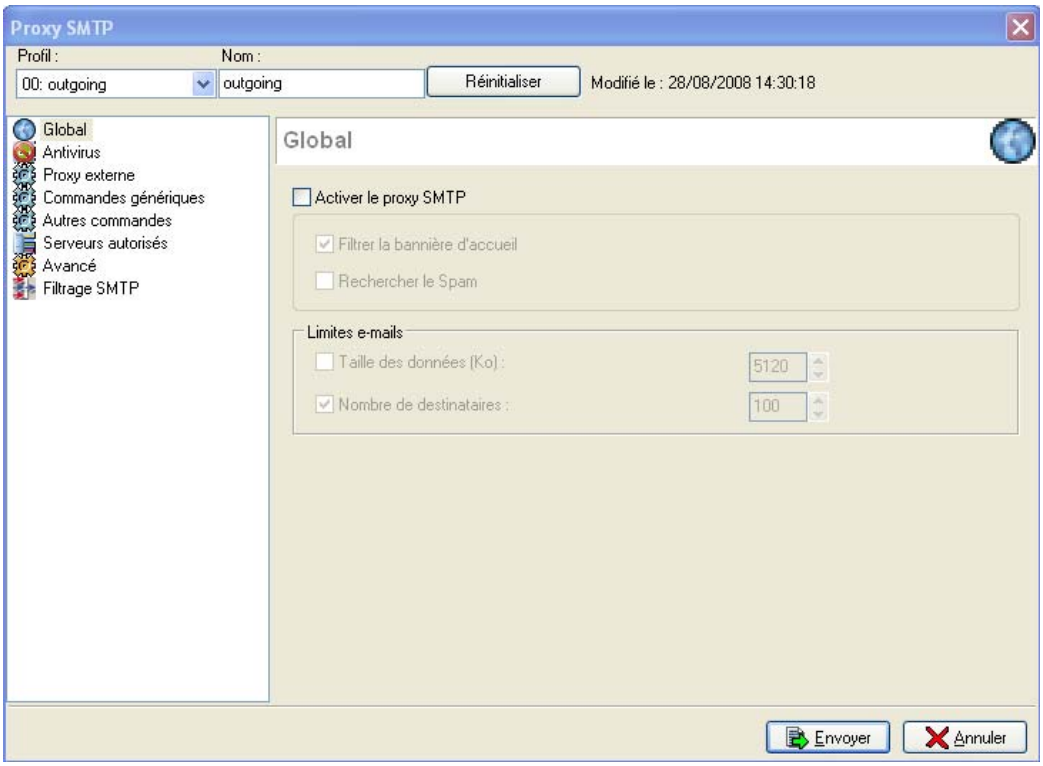


Figure 272 : Exemple d'écran de configuration d'un proxy

Il est possible de créer quatre profils pour le proxy afin d'adapter l'analyse du proxy de l'interface de provenance du trafic. Cela va permettre de désactiver certaines fonctionnalités sur les trafics autorisés en sortie mais pas en entrée.
Ces profils sont :

- 00:default
- 01: default 01
- 02: default 02
- 03 : default 03

La barre d'actions située en haut de l'écran vous indique quel profil du proxy HTTP est actuellement affiché. De plus vous pouvez spécifier un nom pour chacun des quatre profils dans le champ **Nom**.

Le bouton **Réinitialiser** vous permet de redéfinir les paramètres des profils du proxy HTTP dans leur configuration d'origine.

La date située à côté du bouton **Réinitialiser** indique la date de la dernière modification de la configuration.

CHAPITRE 2. REDIRECTION DES FLUX VERS LES PROXIES (MENU « GENERAL »)

Vous avez la possibilité de choisir sur quels ports et interfaces les proxies vont agir. Lorsqu'une connexion provient de l'interface indiquée et demande le service configuré dans cette partie, le proxy intercepte et gère la connexion.

➔ On accède à cette configuration dans le menu **`Proxy\Général`**.

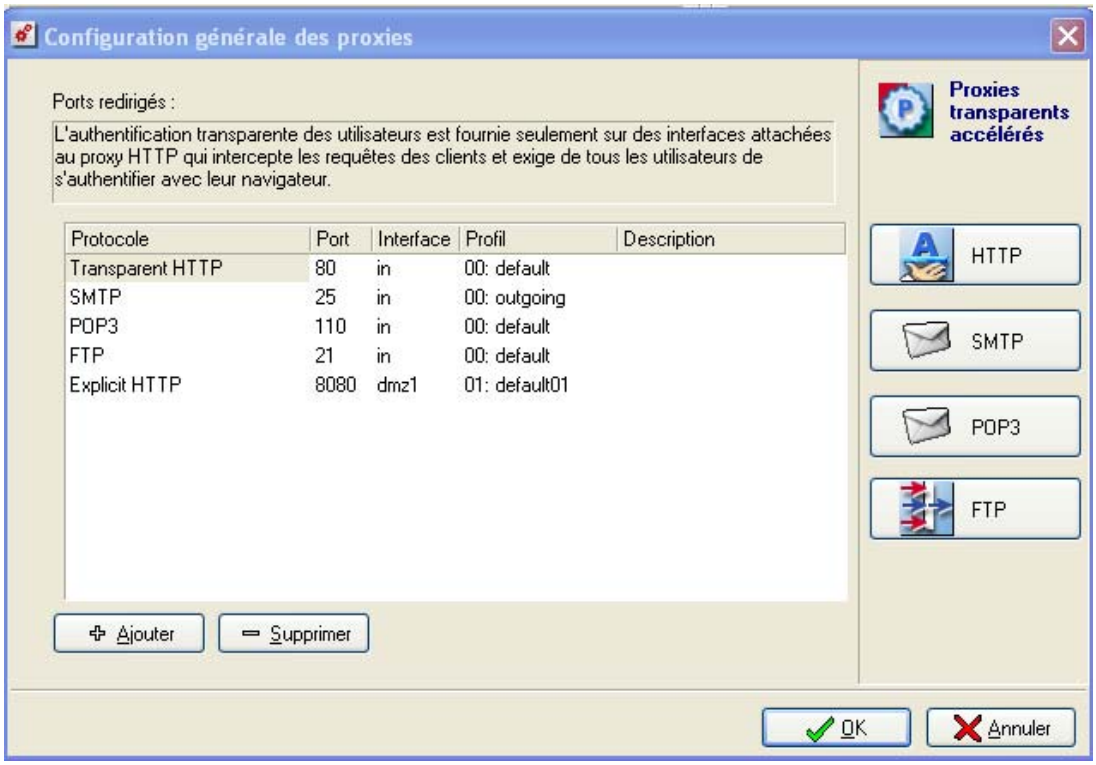


Figure 273 : Configuration générale des proxies

La redirection des flux vers les proxies nécessite la définition des paramètres suivants :

Protocole	Protocole géré par le proxy.
Port	Port sur lequel le proxy doit écouter
Interface	Interface sur laquelle le proxy écoute.
Profil	Permet d'associer un profil Proxy à l'analyse réalisée par les proxies. Pour permettre des configurations différentes suivant les interfaces par exemple.
Description	Commentaire associé à cette ligne.

On ajoute un port ou interface à filtrer avec les boutons **Ajouter**/**Supprimer**. Par défaut, le filtrage URL (proxy HTTP) s'applique sur le port 80 pour les machines du réseau interne uniquement, le filtrage URL

(proxy HTTP) s'applique sur le port 8080, le filtrage SMTP s'applique sur le port 25 pour les machines du réseau interne, le filtrage POP3 s'applique sur le port 110 pour les machines du réseau interne aussi et le filtrage FTP sur le port 21. Les ports d'écoute sont modifiables sauf pour le proxy explicite (8080).

Les boutons situés à droite du tableau (**HTTP**, **SMTP**, **POP3** et **FTP**) permettent d'accéder directement aux écrans de configuration de chaque proxy.

Le filtrage URL entre en application lorsqu'un fichier de règles est activé (Cf. Partie 10/Chapitre 4 : Filtrage d'URL).

AVERTISSEMENT
Les règles implicites sont créées pour les flux interceptés par les proxies. Vous appliquez donc les règles d'accès Internet uniquement au niveau du filtrage URL. Si vous activez un slot de filtrage d'URL, le proxy sera automatiquement activé.

REMARQUE
L'authentification transparente (la page d'authentification est automatiquement proposée à l'utilisateur lorsqu'il désire se connecter à Internet) est fournie seulement aux interfaces liées au proxy HTTP qui intercepte les requêtes clientes. Le filtrage URL ne s'applique pas sur les requêtes HTTPS.

CHAPITRE 3. PROXY HTTP

9.3.1. Description

Le proxy HTTP sert à filtrer les accès à certains sites web, c'est-à-dire à déterminer quelles seront les pages Web autorisées ou bloquées à travers le firewall.

Le proxy HTTP peut fonctionner à partir de 2 modes : « mode transparent » et « mode explicite ».

9.3.1.1. Mode transparent

En mode transparent, une règle de translation permet de rediriger le trafic vers le port d'écoute du proxy. Le proxy transparent s'appuie sur la translation d'adresses pour identifier la destination réelle du serveur que le client souhaite interroger.
Le proxy explicite permet de référencer le proxy dans un navigateur et de lui transmettre directement les requêtes http.

En mode transparent, voici comment se passe l'acheminement d'une page Web : L'utilisateur interne effectue une demande de page web (par exemple http://www.Webserver.com/index.html). Le firewall intercepte la requête et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Le serveur Web répond à la requête de l'utilisateur interne et lui retourne la page web demandée. Le firewall intercepte la réponse du serveur et effectue une analyse antivirale de contenu puis relaie la page à l'utilisateur.

9.3.1.2. Mode explicite

En mode explicite, votre ordinateur se connecte au proxy référencé dans le navigateur web au niveau des paramètres réseaux.
Ce mode offre les deux avantages suivants :

- Si vous souhaitez identifier plusieurs utilisateurs qui utilisent la même adresse IP.

En mode explicite, l'utilisateur interne effectue une demande de page web en tapant son adresse (exemple http://www.Webserver.com/index.html). Le navigateur transmet la requête au proxy explicite. Après avoir vérifié la conformité de la demande avec les règles de filtrage URL, le firewall résout le nom de domaine www.Webserver.com en envoyant une requête DNS. Puis il émet la requête au serveur web pour demander la page index.html. Sur réception de la page de réponse, le firewall effectue l'analyse antivirale du contenu puis renvoie la page à l'utilisateur.

Pour que les navigateurs web puissent savoir quel proxy explicite ils devront utiliser pour joindre une URL donnée, il existe plusieurs modes de configuration possible :

- Détection automatique (l'information sera fournie par DHCP via un fichier PAC)
- Définition de l'URL du fichier de configuration.
- Configuration manuelle (via le navigateur Web).

Pour une détection automatique, 3 étapes sont nécessaires au niveau de la configuration du firewall :

1. Sélection d'un fichier PAC dans le menu Partie 12 : Authentification\Portail web.
2. Autorisation de publier le fichier PAC dans le menu Partie 12 : Authentification\Interfaces internes.
3. Configuration du Partie 11/Chapitre 1 : Service DHCP afin de délivrer le fichier PAC.

DEFINITION

Le fichier PAC permet de rediriger toutes les requêtes HTTP et HTTPS sur le proxy explicite, avec pour exceptions, les requêtes sur le portail d'authentification du firewall et les requêtes sur d'autres protocoles.
Ce fichier doit contenir :

```
Function FindProxyForURL(url, host)
{
// Exclusion du proxy pour le portail
if (host == "NUM_SERIE") {
return "DIRECT";
} else {
// Pour toutes les urls (http|https)
if (shExpMatch(url, "http:*") || shExpMatch(url, "https:*"))
return "PROXY NUM_SERIE:8080" ;
return "DIRECT";
}
}
```

La valeur NUM_SERIE est à remplacer soit par le numéro de série du boitier NETASQ soit par un nom de domaine. L'utilisation d'un nom de domaine nécessite l'insertion d'un certificat spécifique dans le portail, afin de remplacer le certificat par défaut qui correspond au numero de serie.

Pour plus d'informations au sujet du proxy explicite, veuillez vous référer à la note technique Configuration HTTP-V1.

9.3.2. Pour utiliser cette fonctionnalité, vous devez avoir franchi les étapes

9.3.2.1. Pour le proxy transparent :

- Partie 5 : Configuration réseau
- Partie 4/Chapitre 3 : Utilisateurs
- Partie 12 : Authentification
- Partie 7/Chapitre 2 : Filtrage
- Partie 10/Chapitre 3 : Antivirus
- Partie 10/Chapitre 4 : Filtrage d'URL

9.3.2.2. Pour le proxy explicite :

- Partie 5 : Configuration réseau
- Partie 4/Chapitre 3 : Utilisateurs
- Partie 7/Chapitre 2 : Filtrage
- Partie 10/Chapitre 3 : Antivirus
- Partie 10/Chapitre 4 : Filtrage d'URL

9.3.3. Les étapes après configuration du proxy HTTP explicite

- Partie 11/Chapitre 1 : DHCP (Optionnel)
- Configuration du service cache DNS
- Modification de la configuration du Partie 12/Chapitre 1 : Portail captif
- Configuration des postes clients. (Cf. *Voir Note technique de configuration HTTP.)*

9.3.4. Accéder à cette fonctionnalité

➔ Accédez au menu **Proxy** HTTP depuis l'arborescence des menus de NETASQ UNIFIED MANAGER.

9.3.5. Description des écrans de configuration

9.3.5.1. Global

➔ Pour utiliser le proxy HTTP, celui-ci doit être activé. L'activation du proxy est réalisée dans **Proxy\Proxy HTTP.** L'écran ci-dessous s'affiche :

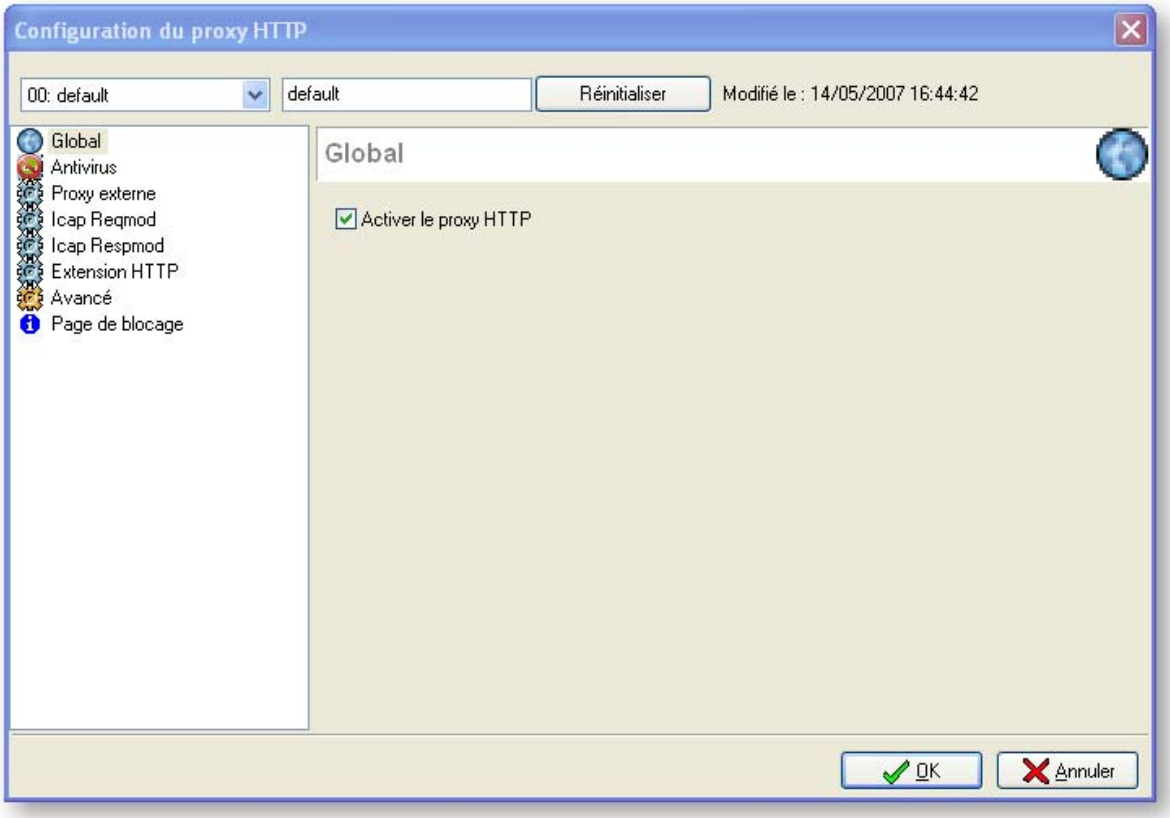


Figure 274 : Configuration du proxy HTTP

Activer le proxy HTTP	Active le proxy HTTP et effectue les analyses spécifiées dans les menus suivants.

9.3.5.2. Antivirus

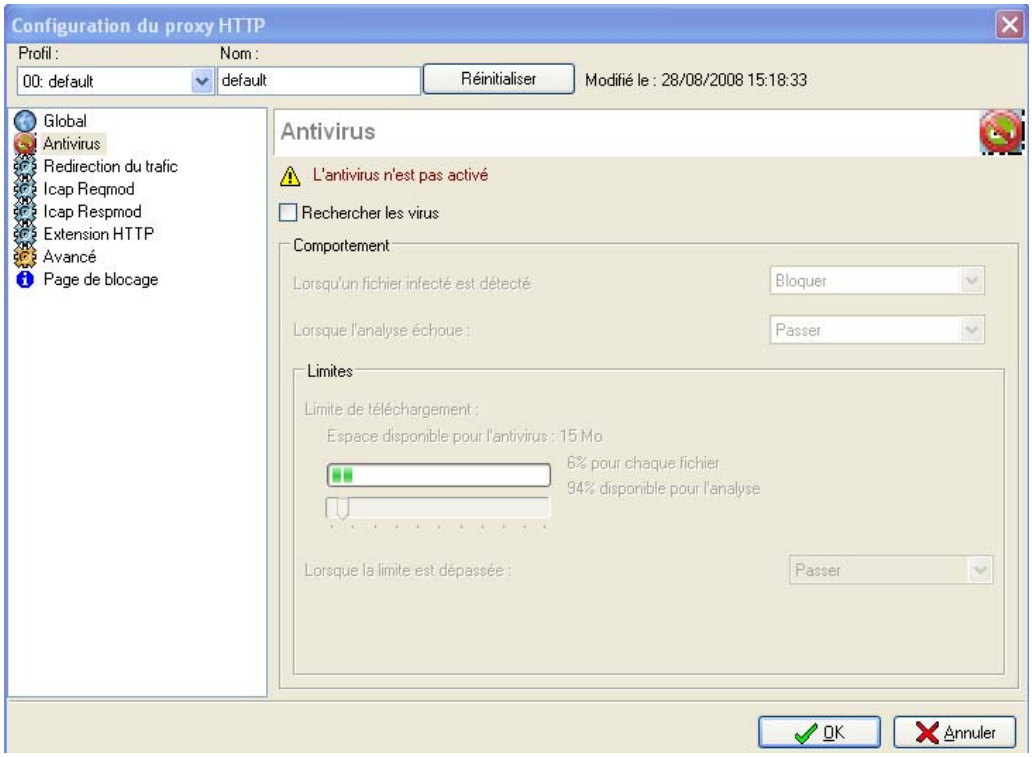


Figure 275 : Configuration du proxy HTTP - Antivirus

L'activation du proxy HTTP permet notamment l'activation de la recherche des virus dans les trafics HTTP (uniquement sur les requêtes GET). Pour activer la recherche des virus référez-vous à la procédure suivante :

Rechercher les virus	Activer la recherche des virus en cochant l'option **Rechercher les virus** dans le menu **`Antivirus.`**
Comportement	La section **Comportement** décrit le comportement de l'antivirus face à certains événements. L'option Sur **detection d'un fichier infecté** contient 2 options : « Passer » et « Bloquer ». En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », l'antivirus transmet le fichier en cours d'analyse. L'option **Lorsque l'analyse échoue** définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue. **Exemple** Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer** est spécifié, le fichier en cours d'analyse est transmis.
Limites	L'option **Limite de téléchargement** est fonction des capacités matérielles de chaque modèle de firewall mais elle peut être adaptée selon les besoins de l'entreprise. Pour cela, déplacez la réglette. **AVERTISSEMENT** Lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total, représenté par la réglette correspond à un espace commun pour l'ensemble des

	ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur HTTP est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps. L'option **Lorsque la limite est dépassée** définit le comportement de l'antivirus si la taille du fichier d'analyse qu'il est en train de scanner dépasse la limite autorisée. Si « Bloquer » est spécifié, le fichier en cours d'analyse n'est pas transmis. Si « Passer » est spécifié, le fichier en cours d'analyse est transmis.

9.3.5.3. Proxy externe

Le proxy HTTP sert pour le filtrage d'URL Section Partie 10/Chapitre 4 : Filtrage d'URL) mais il permet aussi de rediriger les requêtes HTTP provenant des utilisateurs du réseau interne vers des proxies externes.

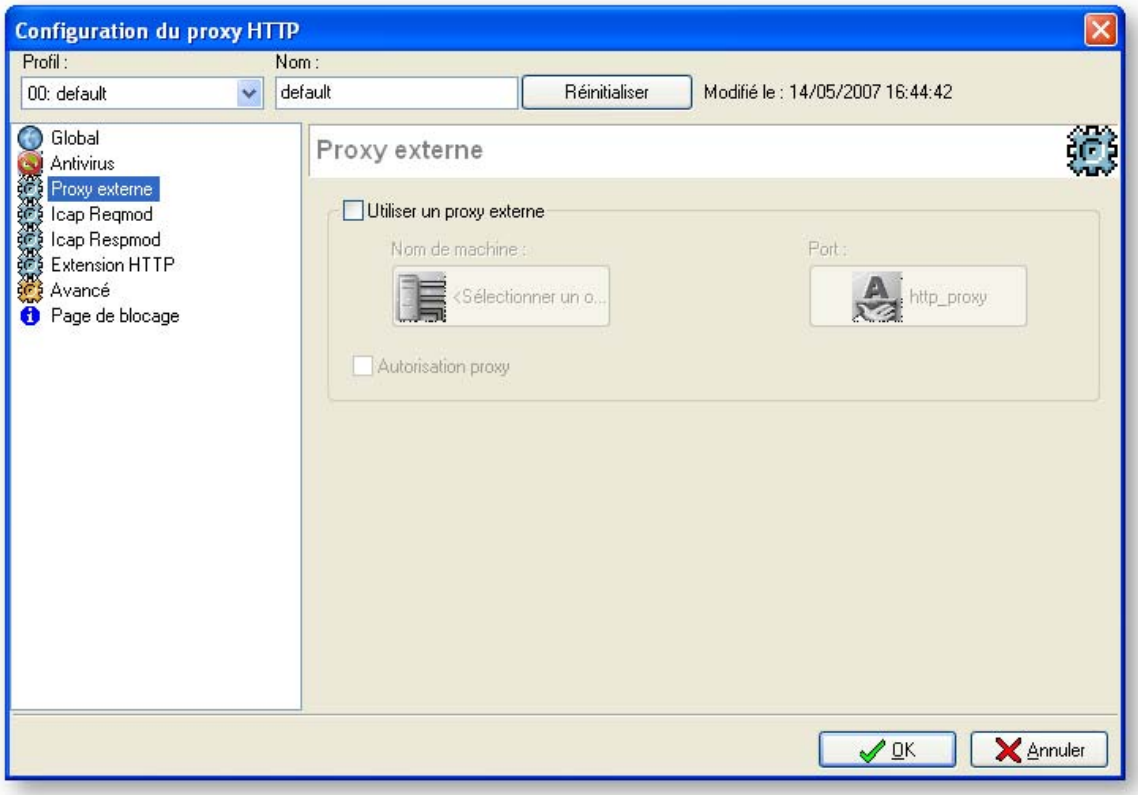


Figure 276 : Configuration du proxy HTTP - Proxy externe

Utiliser un proxy externe	Pour activer cette redirection, cochez la case correspondante puis précisez l'adresse IP du serveur ainsi que le port sur lequel il reçoit les requêtes. Si l'administrateur spécifie un groupe de serveurs dans l'option **Nom de machine**, le firewall effectuera un partage de charge entre les différentes proxies externes du groupe en fonction de la machine source (une machine source donnée utilisera toujours le même proxy externe).
Autorisation proxy	Si le proxy HTTP externe nécessite une authentification des utilisateurs, l'administrateur peut cocher l'option **Autorisation proxy** présente dans le menu **Proxy externe** pour envoyer au proxy externe les informations concernant l'utilisateur recueilli par le module d'authentification du firewall.

9.3.5.4. ICAP Reqmod

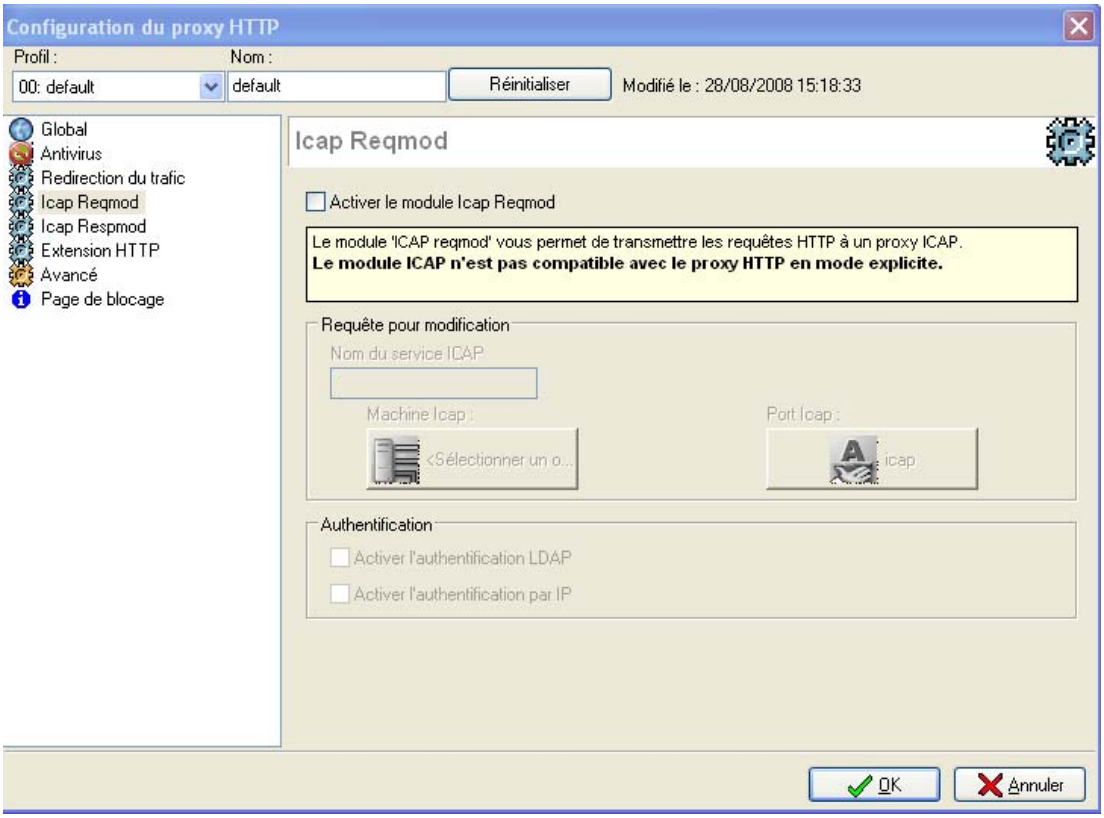


Figure 277 : Configuration du proxy HTTP - Icap Reqmod

DEFINITION

ICAP (ou ***Internet Content Application Protocol***) est un protocole d'adaptation de contenu. Il assure une interopérabilité avec des solutions d'analyse et de traitement de contenu comme WebWasher et permet des services de filtrage d'URL ou de filtrage de contenu. Il fonctionne selon deux modes : le **Reqmod** et le **Respmod**.

Le **Reqmod** (***Request for Modification***) fonctionne selon le principe suivant :

- Un client HTTP envoie une requête HTTP
- Celle-ci
- Le serveur ICAP renvoie une réponse au firewall qui la transmet au serveur Web concerné

Le **Respmod** fonctionne dans le sens inverse.

Le firewall NETASQ supporte les deux modes : **Icap Reqmod** et **Icap Respmod**.

Activer le module Icap Reqmod	Active le module Icap Reqmod et effectue les analyses spécifiées dans les menus suivants.
Requête pour modification	Indication du nom du service à mettre en place. Cette information est différente suivant la solution utilisée, le serveur ICAP ainsi que le port utilisé.
Authentification	On peut utiliser les informations disponibles sur le firewall pour réaliser des services ICAP. **Exemple** Il est possible de définir dans un serveur ICAP que tel ou tel site n'est destiné qu'à telle ou telle personne. Dans ce cas, vous pouvez filtrer selon un identifiant LDAP ou une adresse IP.

	L'option **Activer l'authentification LDAP** permet de se servir des informations relatives à la base LDAP (notamment l'identifiant d'un utilisateur authentifié). L'option **Activer l'authentication par IP** permet de se servir des adresses IP des clients HTTP effectuant la requête à Adapter.

9.3.5.5. ICAP Respmod

Activer le module Icap Respmod	Active le module Icap Respmod et effectue les analyses spécifiées dans les menus suivants.
Requête pour modification	Indication du nom du service à mettre en place. Cette information est différente suivant la solution utilisée, le serveur ICAP ainsi que le port utilisé.
Authentification	On peut utiliser les informations disponibles sur le firewall pour réaliser des services ICAP. **Exemple** Il est possible de définir dans un serveur ICAP que tel ou tel site n'est destiné qu'à telle ou telle personne. Dans ce cas, vous pouvez filtrer selon un identifiant LDAP ou une adresse IP. L'option **Activer l'authentification LDAP** permet de se servir des informations relatives à la base LDAP (notamment l'identifiant d'un utilisateur authentifié). L'option **Activer l'authentication par IP** permet de se servir des adresses IP des clients HTTP effectuant la requête à Adapter.

AVERTISSEMENT
Il est impossible d'utiliser le respmod ICAP lorsque la recherche de virus sur HTTP est activée. Le message suivant s'affiche : « impossible d'activer simultanément les fonctionnalités ICAP RESMOD et antivirus sur http. ».

9.3.5.6. Extension http

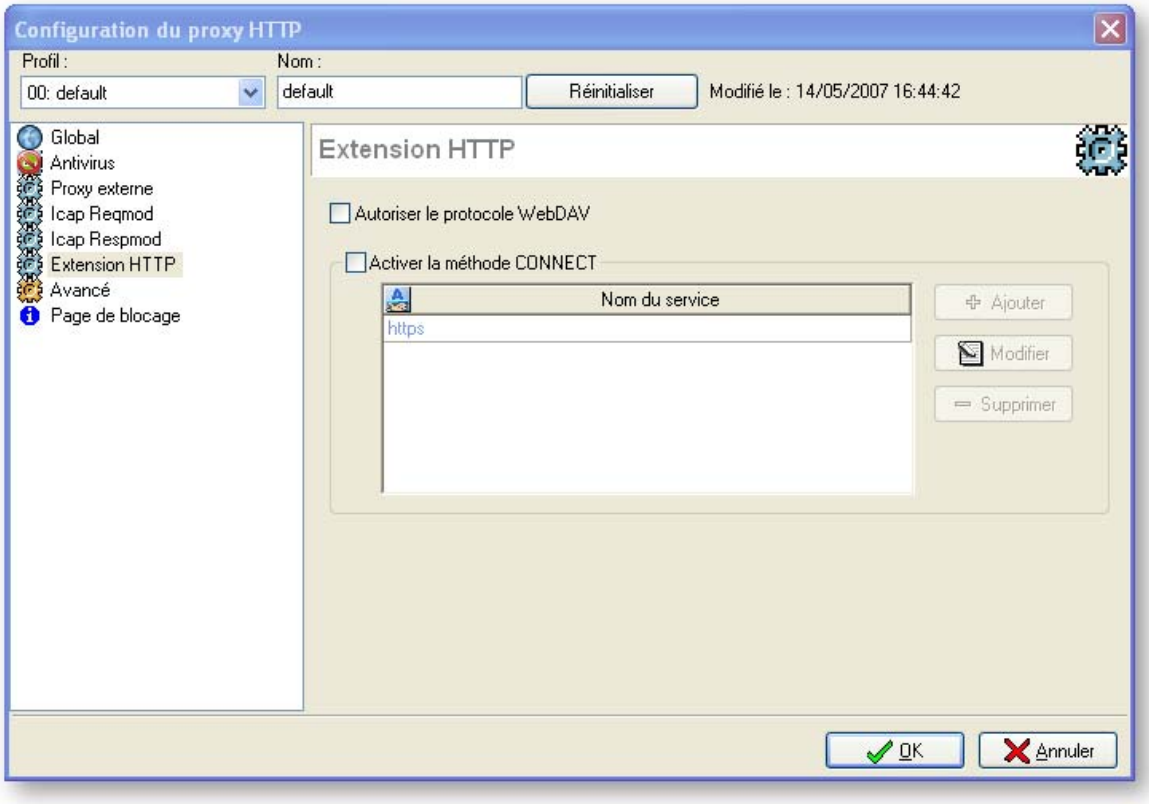


Figure 278 : Configuration du proxy HTTP - Extension HTTP

Le menu **Extension HTTP** permet de configurer les paramètres suivants :

Autoriser le protocole WebDAV	WebDAV est un ensemble d'extensions au protocole HTTP concernant l'édition et la gestion collaborative de documents. Si cette option est cochée, le protocole WebDav est autorisé au travers du firewall NETASQ.
Activer la méthode CONNECT	La **méthode CONNECT** permet de réaliser des tunnels sécurisés au travers de serveurs proxies. La zone "Nom du service" sert à spécifier quels types de service peuvent utiliser une telle méthode. Si cette option est cochée la méthode **CONNECT** est autorisée au travers du firewall NETASQ. Le bouton **Ajouter** vous permet d'ajouter des services via la base d'objets. Le bouton **Modifier** vous permet de remplacer un service préalablement sélectionné par un autre. Le bouton **Supprimer** vous permet de supprimer le service sélectionné. Un message de type « Supprimer le service… » s'affiche pour confirmer ou non la suppression.

9.3.5.7. Avancé

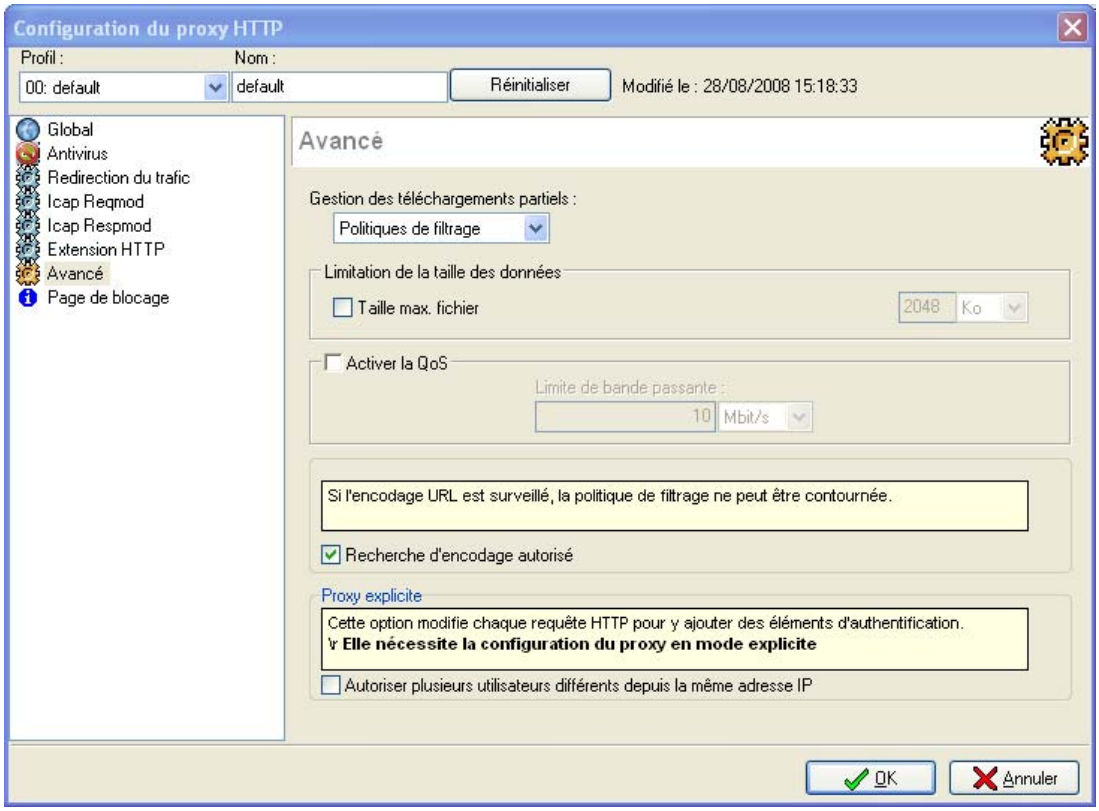


Figure 279 : Configuration du proxy HTTP - Avancé

Le menu **Avancé** permet de configurer les paramètres suivants :

Gestion des téléchargements partiels	Par exemple lorsqu'on télécharge un fichier via FTP si le téléchargement ne s'effectue pas jusqu'au bout (erreur de connexion par exemple), il est possible de relancer le téléchargement à partir de là où a surgi l'erreur plutôt que de devoir tout télécharger de nouveau. Il s'agit dans ce cas d'un téléchargement partiel (le téléchargement ne correspond pas à un fichier complet). L'option **Gestion des téléchargements partiels** permet de définir le comportement du proxy HTTP du firewall vis-à-vis de ce type de téléchargement. • **Bloquer** : le téléchargement partiel est interdit • **Politiques de filtrage** : le téléchargement partiel est autorisé et le trafic est filtré par l'antivirus. • **Passer** : le téléchargement partiel est autorisé mais il n'y a pas d'analyse antivirale effectuée.
Limitation de la taille des données	Lorsque les fichiers téléchargés sur l'Internet, via HTTP sont trop imposants, ils peuvent dégrader la bande passante du lien Internet et cela pour une durée parfois très longue. Pour éviter cela, cochez l'option **Taille max. fichier** et indiquez la taille maximum en Ko pouvant être téléchargée par le protocole HTTP.
Activer la QoS	Régulation du trafic HTTP. Cette option vous permet de définir un débit maximum pour ce type de trafic. Un calcul de dérivée de la courbe du trafic permet de déterminer si des paquets doivent être supprimés silencieusement afin de ne pas dépasser le débit limite.

Recherche d'encodage autorisé	En cochant cette option, la politique de filtrage ne peut être contournée.
Autoriser plusieurs utilisateurs different depuis la même adresse IP	En cochant cette option, vous activez la méthode d'authentification http « basic ». Plusieurs utilisateurs peuvent se trouver derrière la même adresse IP source. Cette option est à utiliser avec le proxy explicite. *Pour plus d'informations au sujet de l'authentification multiple, veuillez vous référer à la note technique « Authentification multiple d'utilisateurs »*.

Cas de l'authentification multiple d'utilisateurs

Il est possible d'authentifier des utilisateurs partageant la même adresse IP. Dans ce cas, l'activation du proxy http explicite est nécessaire. La configuration à mettre en place pour bénéficier de l'authentification multiple d'utilisateurs s'effectue en 5 étapes.

1. Configuration du proxy HTTP explicite nécessaire pour l'authentification multiple.
2. Configuration du service cache DNS.
3. Configuration des règles de filtrage d'URL
4. Configuration de l'authentification et du portail (Partie 12).

La mise en place d'une authentification multiple pour des utilisateurs ayant la même adresse IP nécessite la création préalable d'une base LDAP ainsi que de l'insertion des utilisateurs devant être authentifiés.

Pour plus d'informations au sujet de l'authentification multiple, veuillez vous référer à la note technique « Authentification multiple d'utilisateurs ».

9.3.5.8. Page de blocage

➲ Sélectionnez le menu **Page de blocage**. La fenêtre suivante s'affiche :

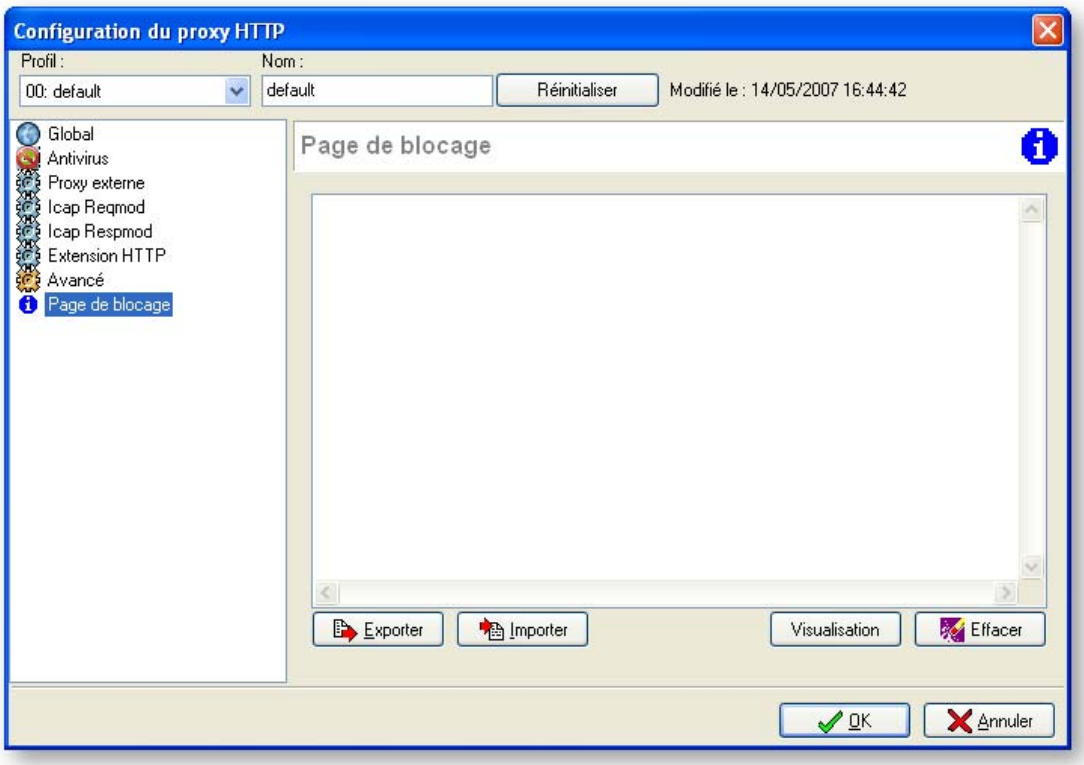


Figure 280 : Configuration du proxy HTTP - Page de blocage

La page de blocage est affichée lorsque la requête HTTP d'un utilisateur est rejetée par le proxy HTTP (URL non autorisée).

Cette page s'affiche dans le navigateur de l'utilisateur à la place de la page Web demandée.

Par défaut, une page NETASQ s'affiche, informant l'utilisateur que sa demande ne peut pas être acceptée, avec la règle de filtrage appliquée et l'URL demandée.

Vous pouvez remplacer cette page par défaut par votre propre page en entrant dans cette fenêtre le code HTML de la page à afficher.

Vous pouvez ajouter les informations suivantes dans cette page :

- $rule: nom de la catégorie
- $host : le nom du destinataire HTTP (ex : www.google.com)
- $url : URL qui est bloquée

Exemple
/search?hl=fr&q=test&btng=rechercher&meta=

REMARQUE
Pour créer vos propres messages de blocage, utilisez un éditeur HTML puis enregistrez le document au format HTML. Vous pouvez ensuite importer ce document avec le bouton **Importer**.

Toute page éditée dans le menu **Page de blocage** peut ensuite être enregistrée pour être importée sur un autre firewall avec le bouton **Exporter**.

Vous avez la possibilité de visualiser le rendu de la page HTML éditée, en cliquant sur le bouton **Visualisation**. Cette action ouvre automatiquement le navigateur par défaut de votre machine.

Enfin si la page que vous avez configurée ne vous convient plus le bouton **Effacer** vous permet de la supprimer pour revenir à la page par défaut de NETASQ.

9.3.5.9. Optimisation du délai d'affichage des pages Web

Une modification au niveau du pipelining et du chunking a été effectuée ; ce qui permet une amélioration sensible des pages Web dans le navigateur.

CHAPITRE 4. PROXY SMTP

9.4.1. Description

9.4.1.1. Définition

Ces dernières années, la messagerie électronique est devenue un outil de communication largement utilisé par les entreprises et les administrations. La transmission rapide et performante des informations permet une amélioration notable de la compétitivité et une baisse des coûts.

Cependant, sans une gestion adéquate du trafic, l'usage de cet outil peut s'avérer désastreux pour la productivité.

Les courriers de masse non sollicités (tels que la publicité, les newsletters…) peuvent avoir des conséquences sur la disponibilité de votre bande passante. De plus, les messages infectés provenant de l'Internet sont autant de failles dans votre sécurité.

Ces écueils sont généralement imputables à une utilisation de l'outil de messagerie à des fins personnelles.

DEFINITION
C'est le protocole **SMTP** (*Simple Mail Transfer Protocol*), protocole de communication TCP-IP, qui est utilisé pour les échanges de courrier électronique dans Internet.

Il s'agit d'un protocole fonctionnant en mode connecté, encapsulé dans une trame TCP/IP. Le courrier est remis directement au serveur de courrier du destinataire. Le protocole **SMTP** fonctionne grâce à des commandes textuelles envoyées au serveur **SMTP** (par défaut sur le port 25). Chacune des commandes envoyées par le client (validée par la chaîne de caractères ASCII CR/LF, équivalent à un appui sur la touche entrée) est suivie d'une réponse du serveur **SMTP** composée d'un numéro et d'un message descriptif.

Il est ainsi possible d'envoyer un courrier grâce à un simple Telnet sur le port 25 du serveur **SMTP**.

9.4.1.2. Différentes utilisations possibles du proxy SMTP

Le proxy SMTP peut être utilisé pour filtrer différents types de flux :

Flux entre les utilisateurs du réseau interne et la passerelle de messagerie

La passerelle doit être placée dans la DMZ. Dans ce cas, les mails envoyés par les clients de messagerie du réseau interne à destination de la passerelle interne pourront être filtrés.

Conséquences

Le serveur de messagerie peut être déchargé des e-mails trop volumineux (un message d'erreur est envoyé au client de messagerie en cas de rejet d'un message), les utilisateurs internes ne peuvent pas utiliser le serveur pour faire du relaying **SMTP**. Votre serveur peut être protégé des Hawks en bloquant les messages envoyés à plusieurs destinataires simultanément.

DEFINITION
HAWK : Méthode utilisée par certains virus pour se propager avec les contacts du carnet d'adresses OUTLOOK.

Configuration

Activer la redirection **SMTP** sur le port 25 et l'interface interne.

Flux SMTP venant de la passerelle de messagerie vers l'Internet

Le firewall est placé entre la passerelle interne et l'Internet. Les e-mails envoyés par la passerelle interne vers l'Internet sont filtrés.

Conséquences

Impossible de faire du relaying SMTP en se servant de la passerelle interne. Possibilité de limiter les envois de pièces jointes vers l'extérieur (permet d'éviter la fuite d'informations et de documents confidentiels, par exemple.

AVERTISSEMENT
Les messages sont alors complètement détruits. Supprime la bannière de bienvenue du serveur SMTP.

Configuration

Activer la redirection **SMTP** sur le port 25 et sur l'interface sur laquelle se trouve le serveur de messagerie.

Flux SMTP venant de l'Internet vers la passerelle interne.

Le firewall est placé entre la passerelle interne et l'Internet. Les e-mails reçus par la passerelle sont filtrés.

Conséquences

Il est possible de limiter la taille des e-mails entrants pour éviter une surcharge du serveur. Vous pouvez éviter le spam d'e-mails. Vous pouvez interdire les e-mails provenant de certains expéditeurs.

Configuration

Activer la redirection **SMTP** sur le port 25 et sur l'interface OUT.

9.4.2. Pour utiliser cette fonctionnalité, vous devez avoir franchi les étapes

- Les noms de domaines autorisés à sortir de votre réseau en SMTP.
- La politique de filtrage d'e-mails que vous voulez mettre en place.

9.4.3. Accéder à cette fonctionnalité

Pour utiliser le proxy SMTP, celui-ci doit être activé. L'activation du proxy est réalisée via le menu **Proxy\Proxy SMTP.**

Pour gérer du by-pass proxy, un profil par défaut est possible désormais.

La barre d'actions située en haut de l'écran vous indique quel profil du proxy SMTP est actuellement affiché. De plus vous pouvez spécifier un nom pour chacun des quatre profils.

9.4.4. Description des écrans de configuration

9.4.4.1. Global

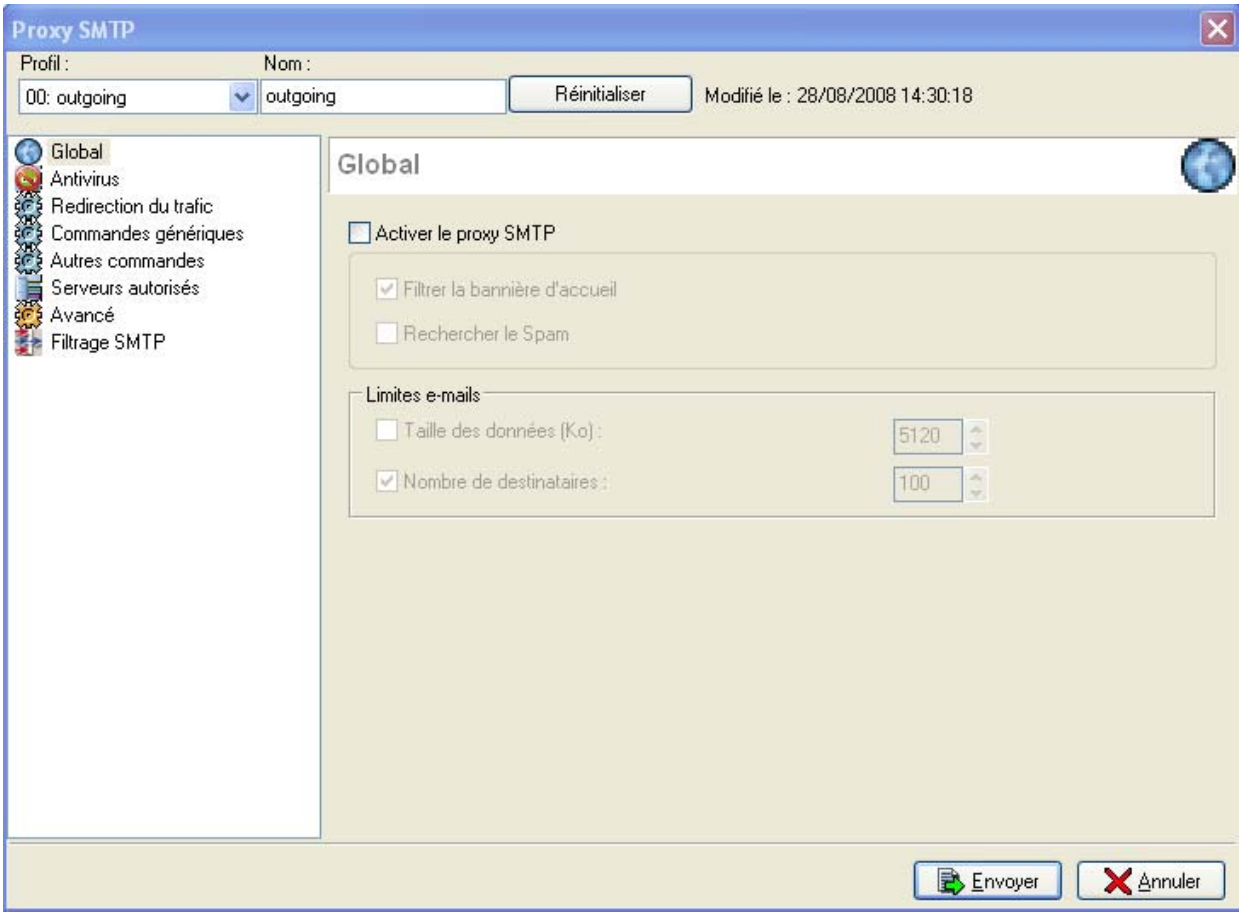


Figure 281 : Proxy SMTP - Global

Le menu **Global** permet de configurer les paramètres suivants :

Activer le proxy SMTP	Active le proxy SMTP et effectue les analyses spécifiées dans les menus suivants. L'activation du proxy SMTP permet notamment l'activation de la recherche des virus dans les trafics SMTP.
Filtrer la bannière d'accueil	Lorsque cette option est cochée, la bannière de votre serveur de messagerie n'est plus envoyée lors d'une connexion SMTP. En effet, cette bannière contient des informations qui peuvent être exploitées par certains pirates (type de serveur, version logicielle ...).
Rechercher le Spam	Activation des fonctionnalités du proxy SMTP pour la rechercher de spam.
Taille des données (Ko)	Indiquez la taille maximale en Ko que peut prendre un message passant par le firewall NETASQ. Les messages dont la taille est excessive seront supprimés par le firewall (un message d'erreur est envoyé à l'expéditeur). Si la ligne dépasse 2048 octets, une trace est conservée.
Nombre de destinataires	Indiquez le nombre maximum de destinataires que peut contenir un message. Les messages dont le nombre de destinataires est excessif seront supprimés par le firewall (un message d'erreur est envoyé à l'expéditeur). Permet de limiter le spam d'e-mails.

9.4.4.2. Antivirus

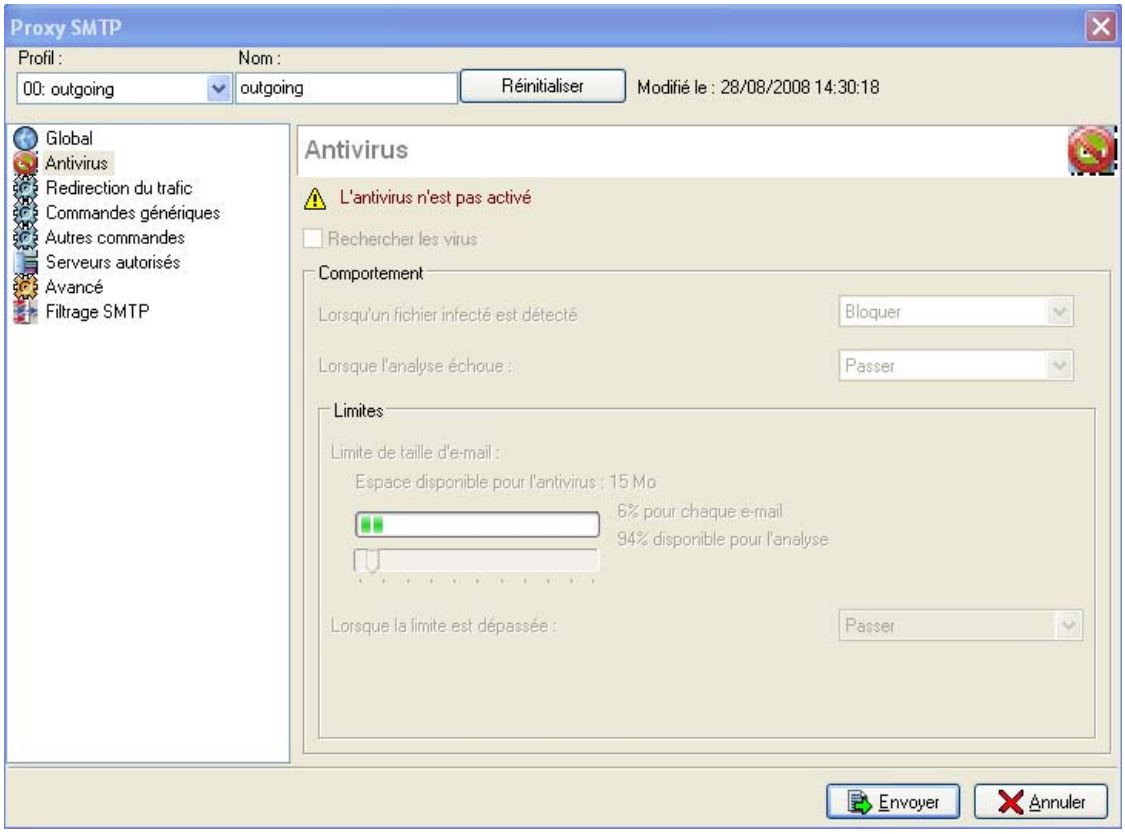


Figure 282 : Proxy SMTP - Antivirus

Rechercher les virus	Active la recherche des virus en cochant d'abord l'option **Activer le proxy SMTP** du menu **`Global`**.
Comportement	La zone "Comportement" décrit le comportement de l'antivirus face à certains événements. L'option **Sur détection d'un fichier infecté** contient 2 options : « Passer » et « Bloquer ». En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », l'antivirus transmet le fichier même s'il est détecté comme infecté. L'option **Lorsque l'analyse échoue** définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue **Exemple** Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer** est spécifié, le fichier en cours d'analyse est transmis.
Limites	L'option **Espace disponible pour l'antivirus** est fonction des capacités matérielles de chaque modèle de firewall mais elle peut être adaptée selon les besoins de l'entreprise. Pour cela, déplacez la réglette. L'option **Lorsque la limite est dépassée** définit le comportement de l'antivirus si la taille du fichier d'analyse qu'il est en train de scanner dépasse la limite autorisée. Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer** est spécifié, le fichier en cours d'analyse est transmis.

AVERTISSEMENT

Lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total, représenté par la réglette correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur SMTP est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps.

9.4.4.3. Redirection du trafic

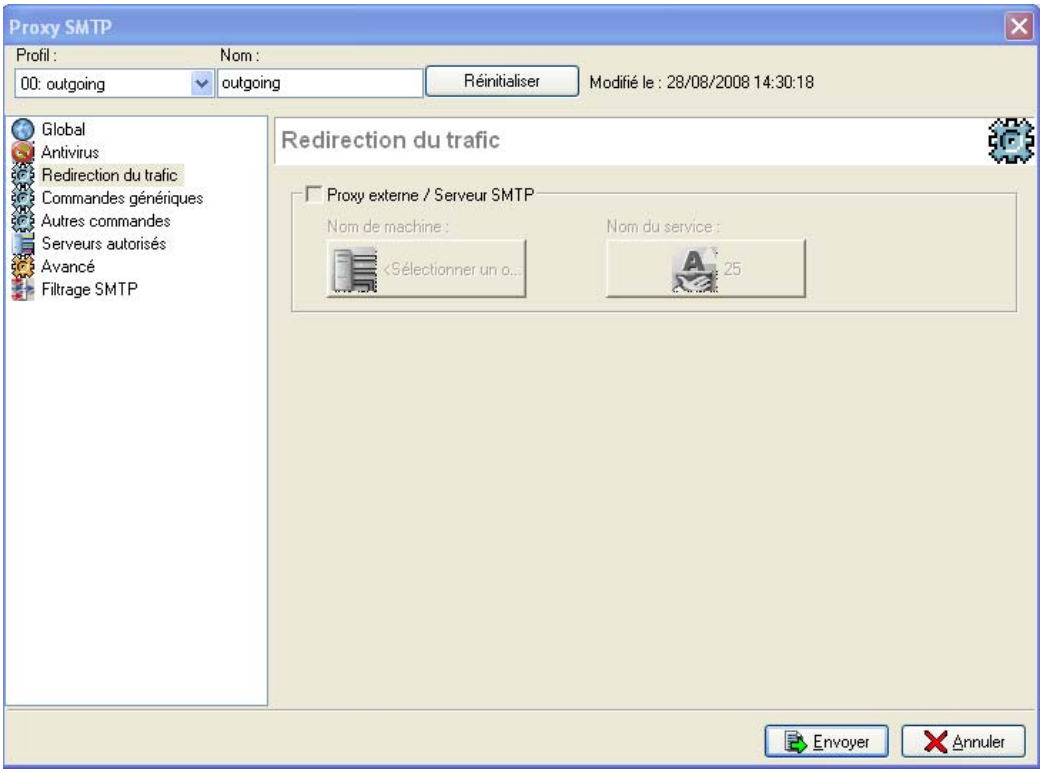


Figure 283 : Proxy SMTP - Proxy externe

Le proxy SMTP permet de rediriger les requêtes SMTP provenant des utilisateurs du réseau interne vers des proxies externes.

Pour activer cette redirection, cochez la case **Proxy externe** puis précisez l'adresse IP du serveur ainsi que le service sur lequel il reçoit les requêtes. Si l'administrateur spécifie un groupe de serveurs dans l'option **Nom de machine**, le firewall effectuera un partage de charge entre les différentes proxies externes du groupe en fonction de la machine source (une machine source donnée utilisera toujours le même proxy externe).

9.4.4.4. Commandes génériques

Figure 284 : Proxy SMTP - Commandes génériques

Ce menu vous permet d'autoriser ou de rejeter les commandes SMTP définies dans les RFC. Vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

9.4.4.5. Autres commandes

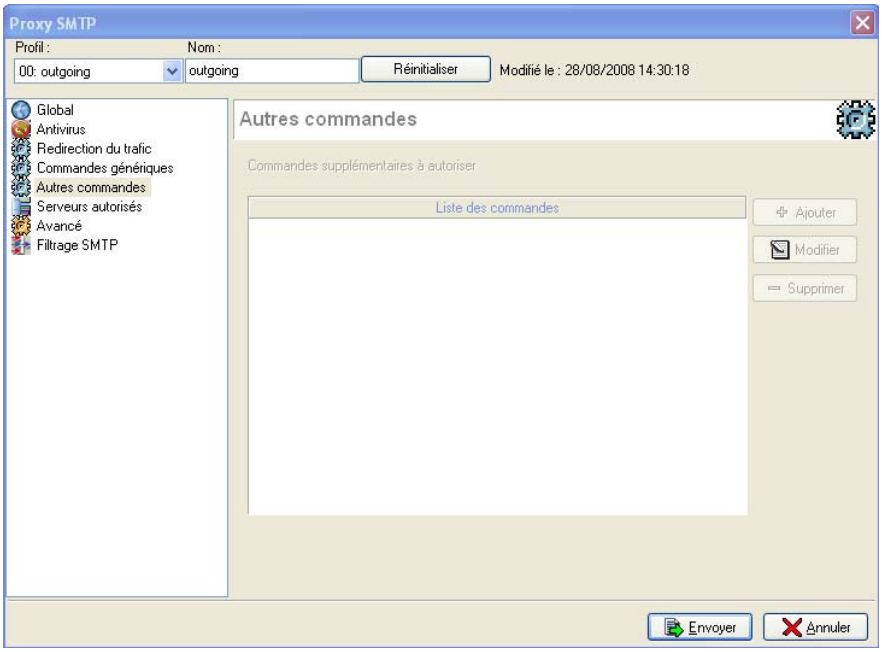


Figure 285 : Proxy SMTP - Autres commandes

Par défaut, toutes les commandes non définies dans les RFC sont interdites. Cependant, certains systèmes de messagerie utilisent des commandes supplémentaires non standardisées. Vous pouvez donc ajouter ces commandes afin de les laisser passer au travers du firewall.

Les boutons d'actions **Ajouter**, **Modifier** et **Supprimer** permettent d'agir sur la liste de commandes.

9.4.4.6. Serveurs autorisés

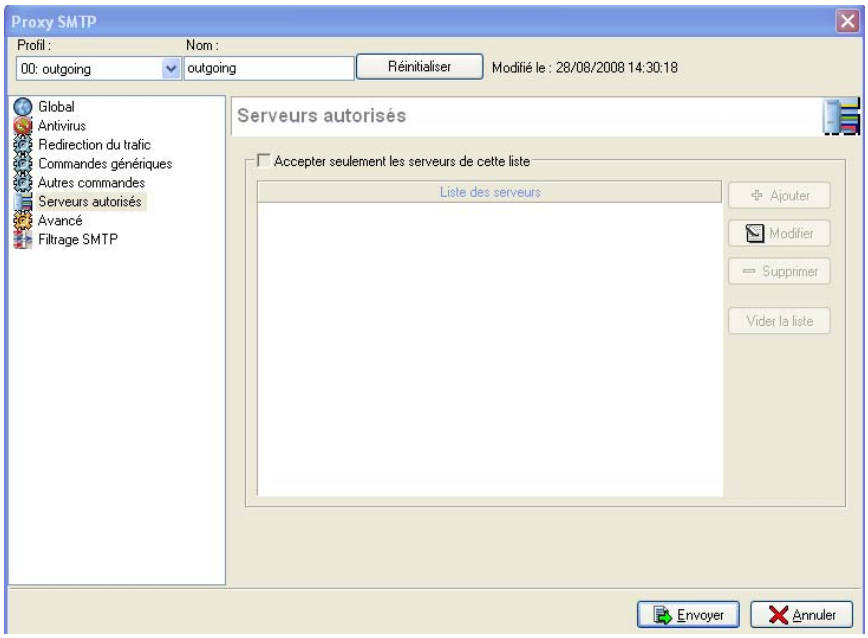


Figure 286 : Proxy SMTP - Serveurs autorisés

En sélectionnant l'option **Accepter seulement les serveurs de cette liste** vous n'autorisez le trafic SMTP qu'à destination des serveurs spécifiés dans la liste.

Les boutons d'action sur la droite de la fenêtre vous permettent de sélectionner vos serveurs autorisés dans la liste de vos objets. Les messages à destination d'un serveur ne faisant pas partie de la liste seront supprimés par le firewall. Si cette case n'est pas cochée, tous les e-mails sont autorisés.

9.4.4.7. Avancé

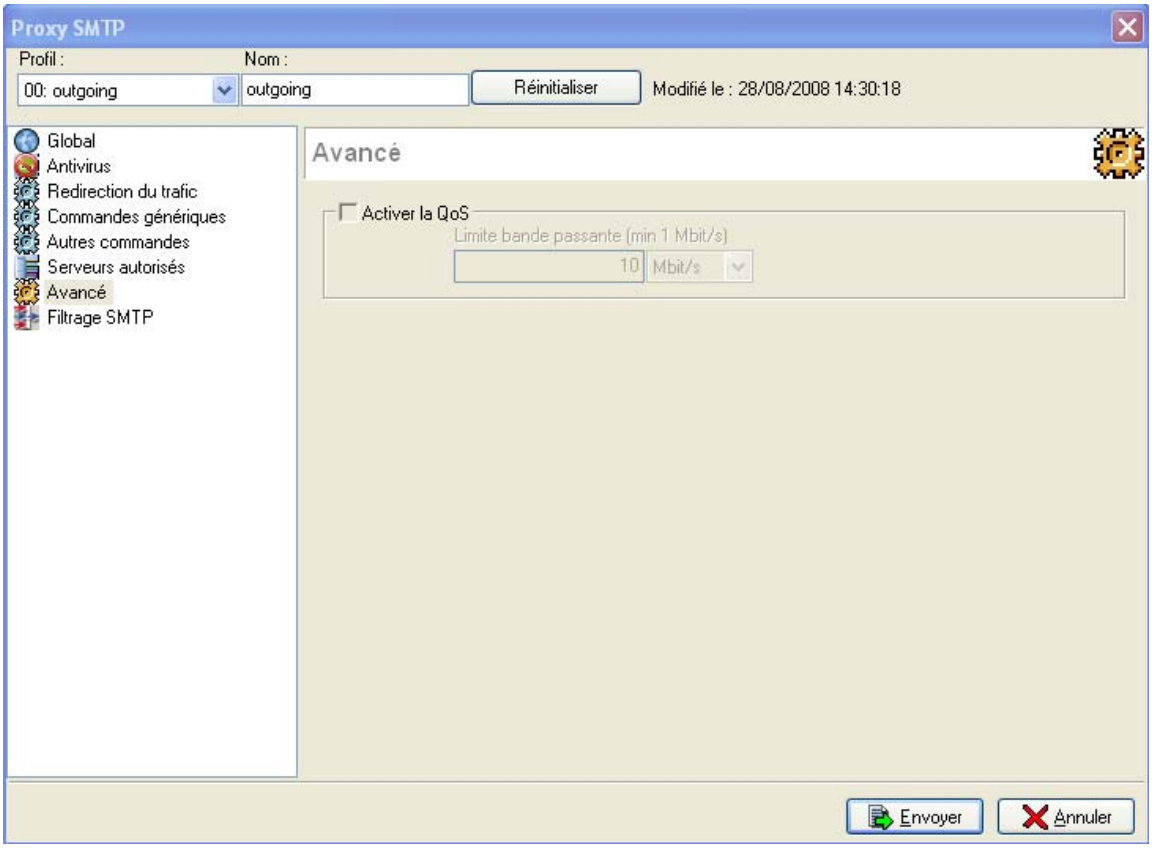


Figure 287 : Proxy SMTP - Avancé

Le menu **Avancé** permet de configurer le paramètre suivant :

Activer la QoS	Régulation du trafic SMTP. Un calcul de dérivée de la courbe du trafic permet de déterminer si des paquets doivent être supprimés silencieusement afin de ne pas dépasser le débit limite.

9.4.4.8. Filtrage SMTP

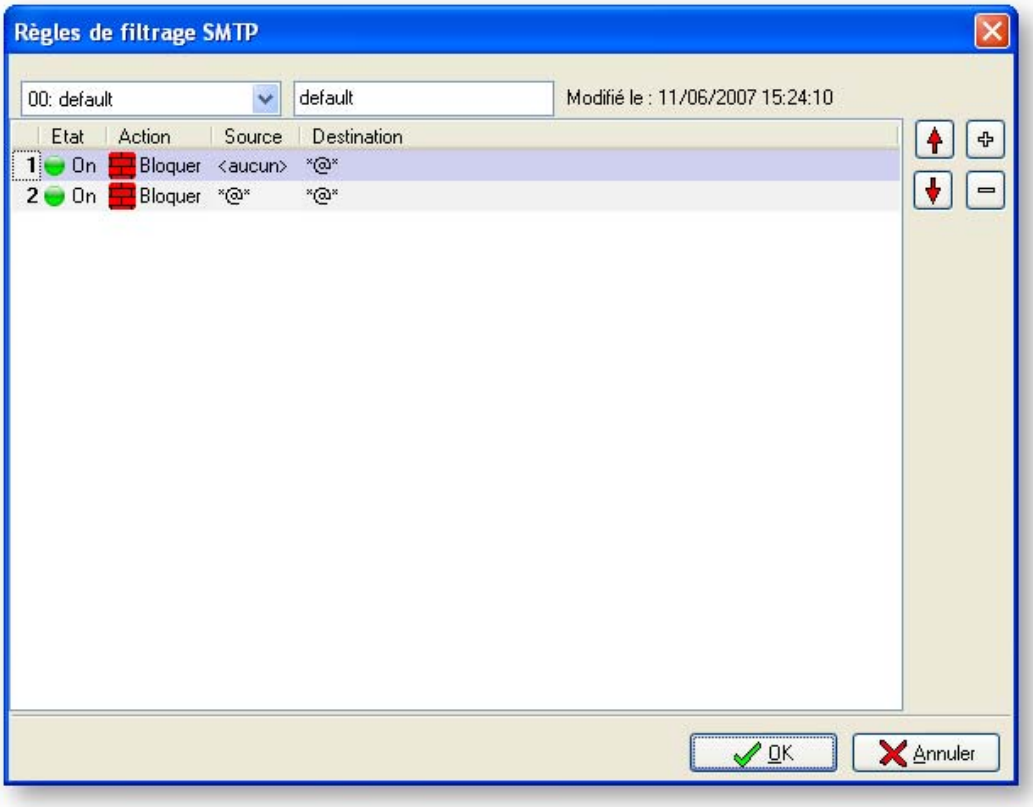


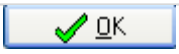
Figure 288 : Règles de filtrage par défaut

Ce menu vous permet de réaliser un véritable filtrage sur les e-mails que vous envoyez ou que vous recevez. En cliquant sur le menu **`Filtrage SMTP`** le menu de configuration apparaît. Ce menu se divise en deux parties :

- Une grille de définition des règles de filtrage d'e-mails.
- Des boutons d'actions.

Boutons d'actions

Les actions réalisées par les boutons d'actions sont expliquées dans le tableau ci-dessous.

	Placer la ligne sélectionnée avant la ligne directement au dessus.
	Placer la ligne sélectionnée après la ligne directement en dessous.
	Insérer une ligne vierge après la ligne sélectionnée.
	Supprimer la ligne sélectionnée.
	Accepter les modifications apportées.
	Annuler les modifications apportées.

Création d'une règle de filtrage d'e-mails

La grille de définition vous permet de réaliser une véritable politique de filtrage d'e-mails, les colonnes de la grille représentent :

Etat	**ON** : La règle est utilisée pour le filtrage. **OFF** : La règle n'est pas utilisée pour le filtrage.
Action	Action réalisée par la règle de filtrage d'e-mails sélectionnée. Choisir parmi **Passer** ou **Bloquer**.
Source	Définition de l'émetteur du mail.
Destination	Définition du destinataire du mail.

La saisie d'un masque d'e-mails peut comporter la syntaxe suivante :

- * : Remplace une séquence de caractères quelconque.

Exemple
*@netasq.com permet de définir l'ensemble des emails domaine Internet de la société NETASQ.

Exemple
commerce ?@netasq.com est équivalent à commerce1@netasq.com ou de commercea@netasq.com mais pas à commerce12@netasq.com

- ? : Remplace un caractère.
- [a-z] : Remplace un intervalle de caractère.

Exemple
commerce[1-2]@netasq.com est équivalent à commerce1@netasq.com et à commerce2@netasq.com.

- <aucun> : Cette valeur ne peut être obtenue que lorsque le champ **Source** est vide. Elle n'est utilisée que pour le cas des "Mailer Deamon".

En effet, lorsqu'un mail ne trouve pas de destinataire sur le serveur mail distant, un message d'erreur est renvoyé par le serveur mail distant, indiquant qu'il y a erreur sur le destinataire. Dans ce cas, le champ **Source** de ce message d'erreur est vide.

Fonctionnement des filtres SMTP et constat initial de configuration

Les filtres SMTP fonctionnent par défaut en mode "White List" (ce qui n'est pas explicitement autorisé est interdit). Par défaut la configuration des filtres SMTP se compose de deux règles de filtrage SMTP.

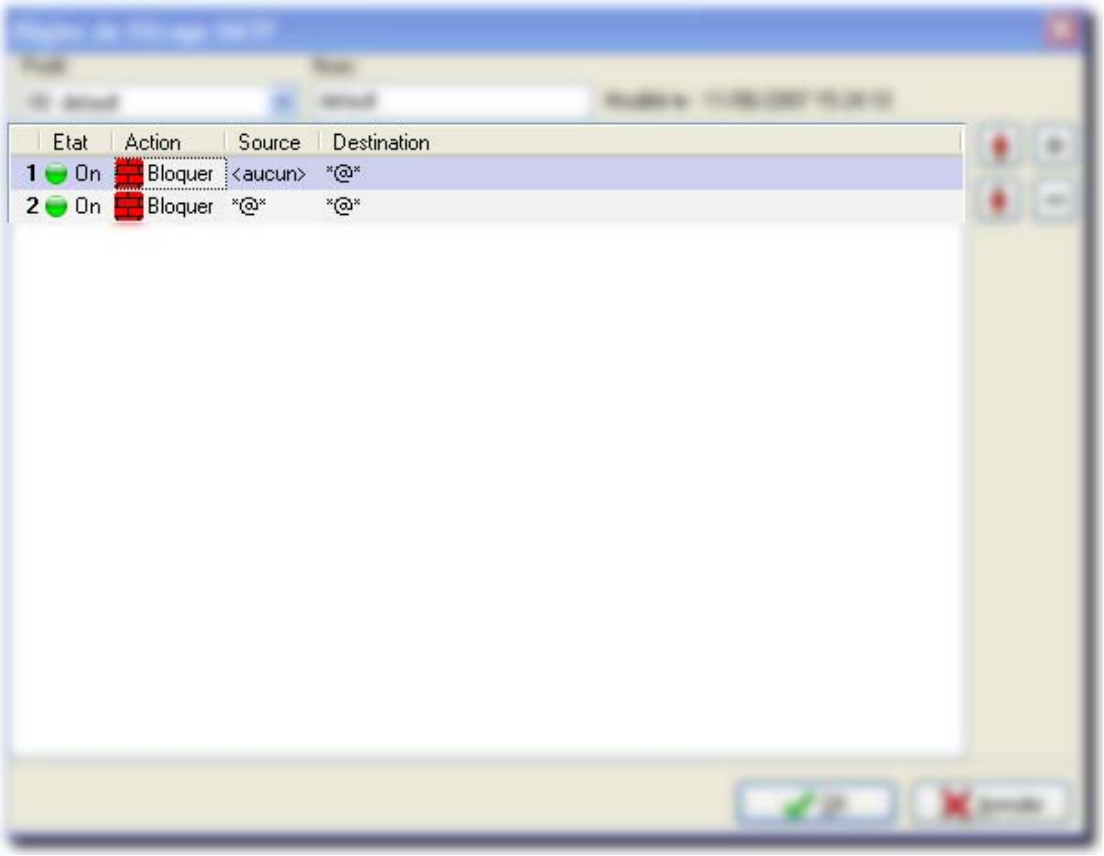


Figure 289 : Fonctionnement des filtres

La règle 1 bloque par défaut les messages des mailers démon. En effet, lorsqu'un mail ne trouve pas de destinataire sur le serveur mail distant, un message d'erreur est renvoyé par le serveur mail distant, indiquant qu'il y a erreur sur le destinataire. Dans ce cas, le champ "Source" de ce message d'erreur est vide. La règle 1 est une transposition explicite d'une règle existante précédemment sous une forme implicite.

La règle 2 autorise par défaut la transmission des messages provenant de tous les expéditeurs possibles à tous les destinataires possibles. Lorsque la règle 2 est supprimée et que le proxy SMTP est activé, les messages en provenance d'expéditeurs et à destination de destinataires non autorisés sont bloqués.

CHAPITRE 5. PROXY POP3

9.5.1. Description

La section précédente décrit le fonctionnement et les avantages du proxy SMTP NETASQ. Comme indiqué, ce proxy est mis en place dans le cadre d'une architecture dans laquelle le firewall va protéger un serveur de mail interne (ou placé en DMZ) en analysant les flux SMTP et immuniser votre réseau contre la menace antivirale grâce à l'antivirus KASPERSKY intégré au firewall.

Le trafic Mail n'est pas seulement basé sur le protocole SMTP mais aussi sur POP3. Ce protocole va permettre à l'utilisateur d'un logiciel de messagerie, de récupérer sur son poste, des mails, stockés sur un serveur distant. Ce serveur de mail distant pouvant être situé à l'extérieur du réseau local ou sur une interface distincte, le flux POP3 transite au travers du firewall lui permettant de réaliser son analyse.

9.5.2. Pour utiliser cette fonctionnalité, vous devez connaître

- Les noms de domaines autorisés à sortir de votre réseau en SMTP et POP3.
- La politique de filtrage d'e-mails que vous voulez mettre en place.

9.5.3. Accéder à cette fonctionnalité

Pour utiliser le proxy POP3, celui-ci doit être activé. L'activation du proxy est réalisée dans le menu **Proxy\Proxy POP3**.

9.5.4. Description des écrans de configuration

9.5.4.1. Global

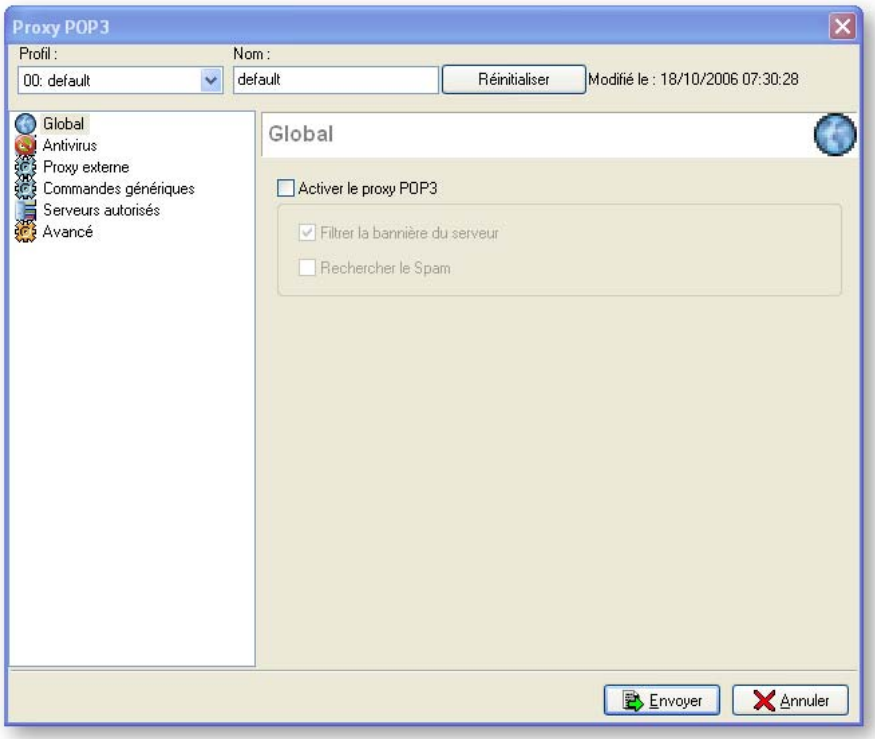


Figure 290 : Proxy POP3 - Global

Le menu **Global** permet de configurer les paramètres suivants

Activer le proxy POP3	Active le proxy **POP3** et effectuez les analyses spécifiées dans les menus suivants.
Filtrer la bannière d'accueil	Lorsque cette option est cochée, la bannière de votre serveur de messagerie n'est plus envoyée lors d'une connexion POP3. En effet, cette bannière contient des informations qui peuvent être exploitées par certains pirates (type de serveur, version logicielle ...).

Rechercher le Spam	Activation des fonctionnalités du proxy POP3 pour la rechercher de spam.

9.5.4.2. Antivirus

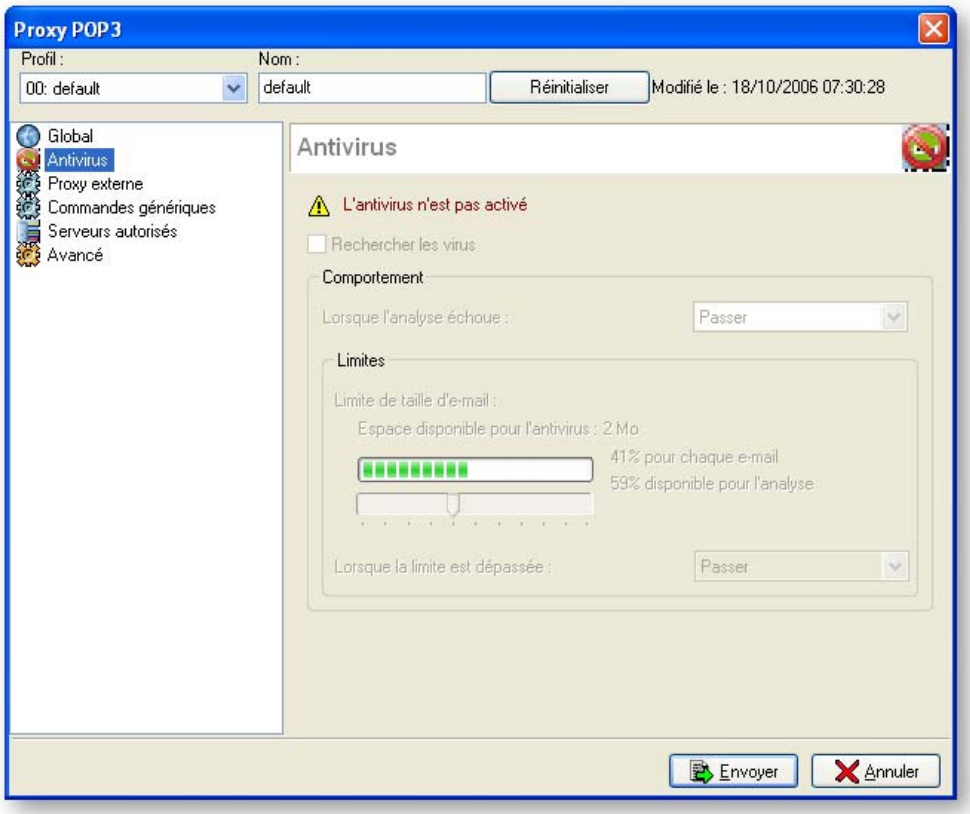


Figure 291 : Proxy POP3 - Antivirus

L'activation du proxy POP3 permet notamment l'activation de la recherche des virus dans les trafics POP3. Pour activer la recherche des virus référez-vous à la procédure suivante :

Rechercher les virus	Active la recherche des virus en cochant d'abord l'option **Activer le proxy SMTP** du menu **`Global`**.
Comportement	La zone "Comportement" décrit le comportement de l'antivirus face à certains événements. L'option **Lorsque l'analyse échoue** définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue **Exemple** Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer** est spécifié, le fichier en cours d'analyse est transmis.
Limites	La **limite de taille d'e-mail** est fonction des capacités matérielle chaque modèle de firewall mais elle peut être adaptée selon les besoins de l'entreprise. Pour cela, déplacez la réglette. **AVERTISSEMENT** Lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total,

représenté par la réglette correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur SMTP est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps.

L'option **Lorsque la limite est dépassée** définit le comportement de l'antivirus si la taille du fichier d'analyse qu'il est en train de scanner dépasse la limite autorisée.

Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis.
Si **Passer** est spécifié, le fichier en cours d'analyse est transmis.

9.5.4.3. Proxy externe

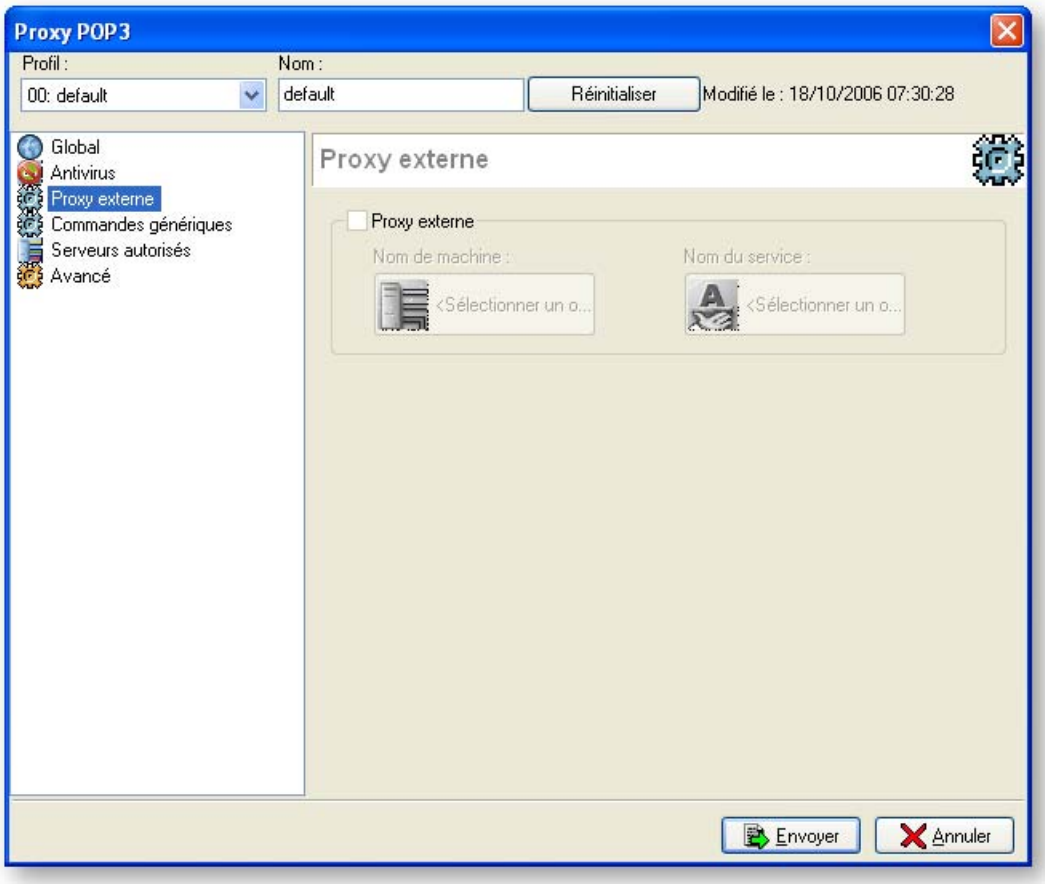


Figure 292 : Proxy POP3 - Proxy externe

Le proxy POP3 permet de rediriger les requêtes POP3 provenant des utilisateurs du réseau interne vers des proxies externes.

Pour activer cette redirection, cochez la case correspondante puis précisez l'adresse IP du serveur ainsi que le port sur lequel il reçoit les requêtes.

9.5.4.4. Commandes génériques

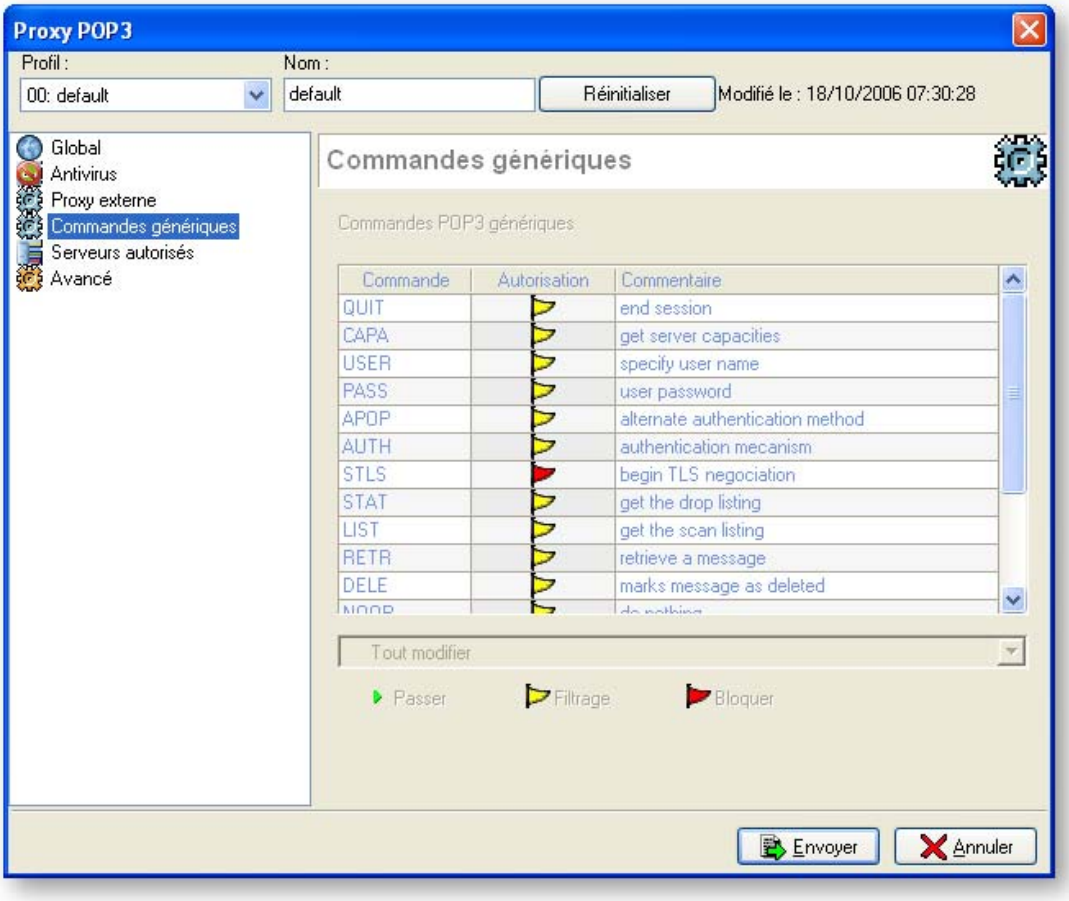


Figure 293 : Proxy POP3 - Commandes génériques

Ce menu vous permet d'autoriser ou de rejeter les commandes POP3 définies dans les RFC. Vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

DEFINITION : RFC
Une série de documents qui communiquent des informations sur l'Internet. N'importe qui peut soumettre un commentaire, mais seul l'Internent Engineering Task Force (IETF) décide si les standards deviennent des RFC. Un n° est assigné à chaque RFC, et il ne peut être modifié une fois publié.

9.5.4.5. Serveurs autorisés

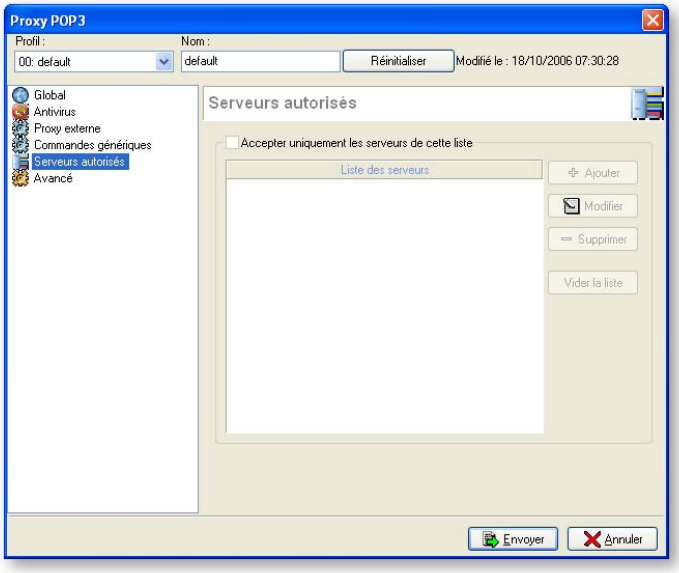


Figure 294 : Proxy POP3 - Serveurs autorisés

En sélectionnant l'option **Accepter uniquement les serveurs de cette liste** vous n'autorisez le trafic POP3 qu'à destination des serveurs spécifiés dans la liste.
Les boutons d'action sur la droite de la fenêtre vous permettent de sélectionner vos serveurs autorisés dans la liste de vos objets. Les messages à destination d'un serveur ne faisant pas partie de la liste seront supprimés par le firewall. Si cette case n'est pas cochée, tous les mails sont autorisés.

9.5.4.6. Avancé

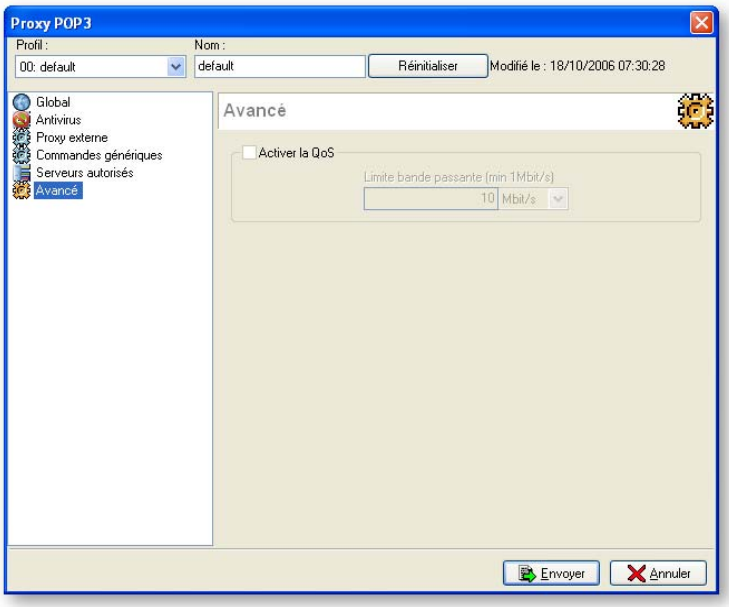


Figure 295 : Proxy POP3 - Avancé

Le menu **Avancé** permet de configurer le paramètre suivant :

Activer la Qos	Régulation du trafic POP3. Un calcul de dérivée de la courbe du trafic permet de déterminer si des paquets doivent être supprimés silencieusement afin de ne pas dépasser le débit limite.

CHAPITRE 6. PROXY FTP

9.6.1. Description

FTP (*File transfert Protocol*)
Il s'agit d'un protocole qui permet l'échange de fichiers sur un réseau TCP/IP. Il permet la copie de fichiers d'un ordinateur à un autre du réseau.
Le fonctionnement est le suivant : le client envoie des requêtes auxquelles le serveur répond.

Le protocole FTP permet de télécharger des fichiers depuis un serveur vers le client (Download). Il permet également de télécharger des fichiers depuis le client vers un serveur (Upload), par exemple, pour la mise à jour de pages web personnelles.

Le proxy est utilisé pour vérifier les commandes du protocole FTP et pour effectuer une analyse antivirale sur les fichiers transférés (upload et download). Seuls les transferts de fichiers sont soumis à l'analyse antivirale. L'analyse protocolaire étant réalisée par le moteur ASQ, le proxy FTP analyse plus particulièrement le nombre et la nature des arguments des commandes en proposant 3 niveaux de vérifications :

- Blocage inconditionnel de la commande.
- Vérification de la validité de la commande.
- Acceptation inconditionnelle de la commande.

Le protocole peut s'utiliser de deux manières différentes lorsque le firewall NETASQ est utilisé pour filtrer les paquets.

- En mode actif : le client FTP détermine le port de connexion à utiliser pour autoriser le transfert des données.
- En mode passif : le serveur FTP détermine lui-même le port de connexion à utiliser pour permettre le transfert des données et le communique au client.

L'implémentation de la fonctionnalité de proxy FTP sert avant tout à permettre une analyse antivirale des données qui transitent par FTP.

NOTE
Le proxy FTP est conforme à la RFC et à diverses extensions.

9.6.2. Etapes avant configuration du proxy FTP

- Partie 5 : Configuration réseau.

9.6.3. Etapes après configuration du proxy FTP

- Partie 10/Chapitre 3 : Activation de l'antivirus.

9.6.4. Accéder à cette fonctionnalité

Pour utiliser le proxy FTP, celui-ci doit être activé. L'activation du proxy est réalisée dans le menu **Proxy\Proxy FTP**.

9.6.5. Description des écrans de configuration

9.6.5.1. Global

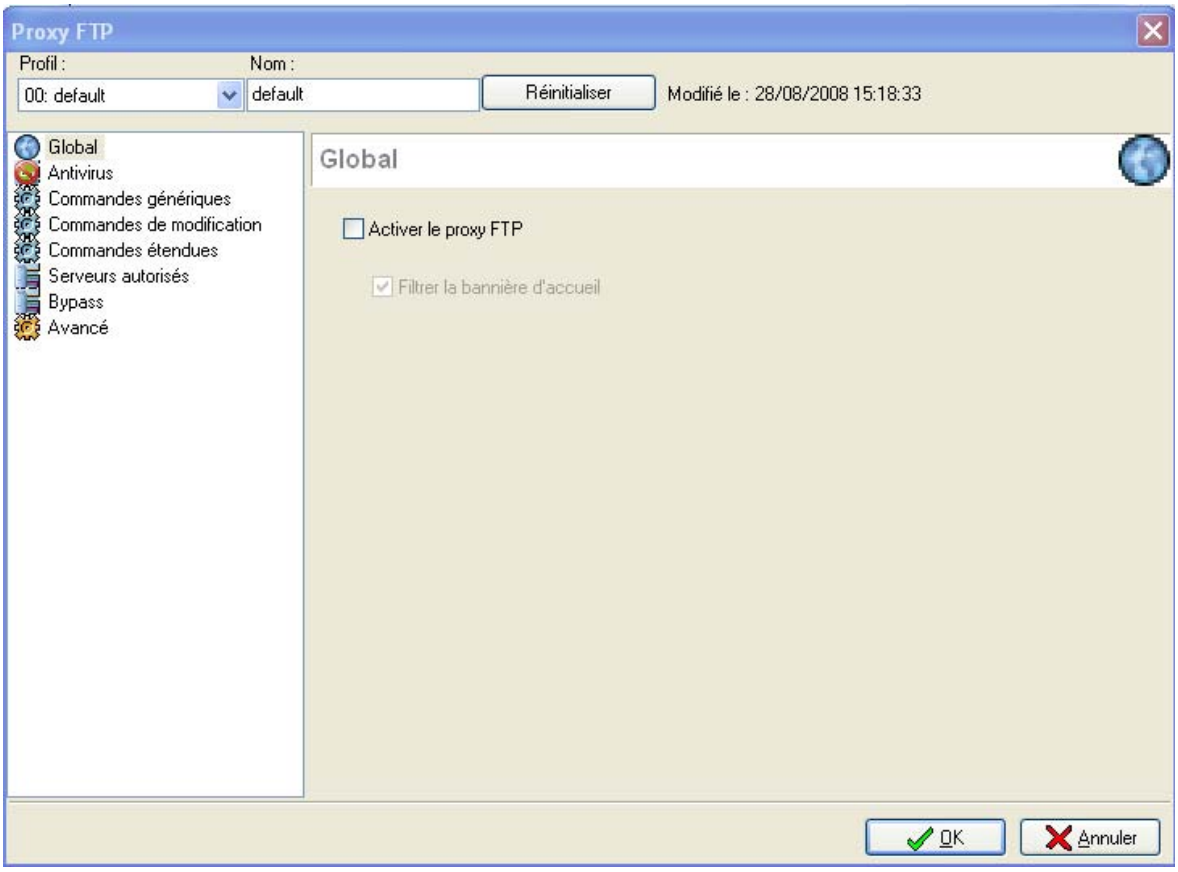


Figure 296 : Proxy FTP - Global

Le menu **Global** permet de configurer les paramètres suivants :

Activer le proxy FTP	Active le proxy **FTP** et effectuez les analyses spécifiées dans les menus suivants.
Filtrer la bannière d'accueil	Permet de filtrer le message d'accueil.

9.6.5.2. Antivirus

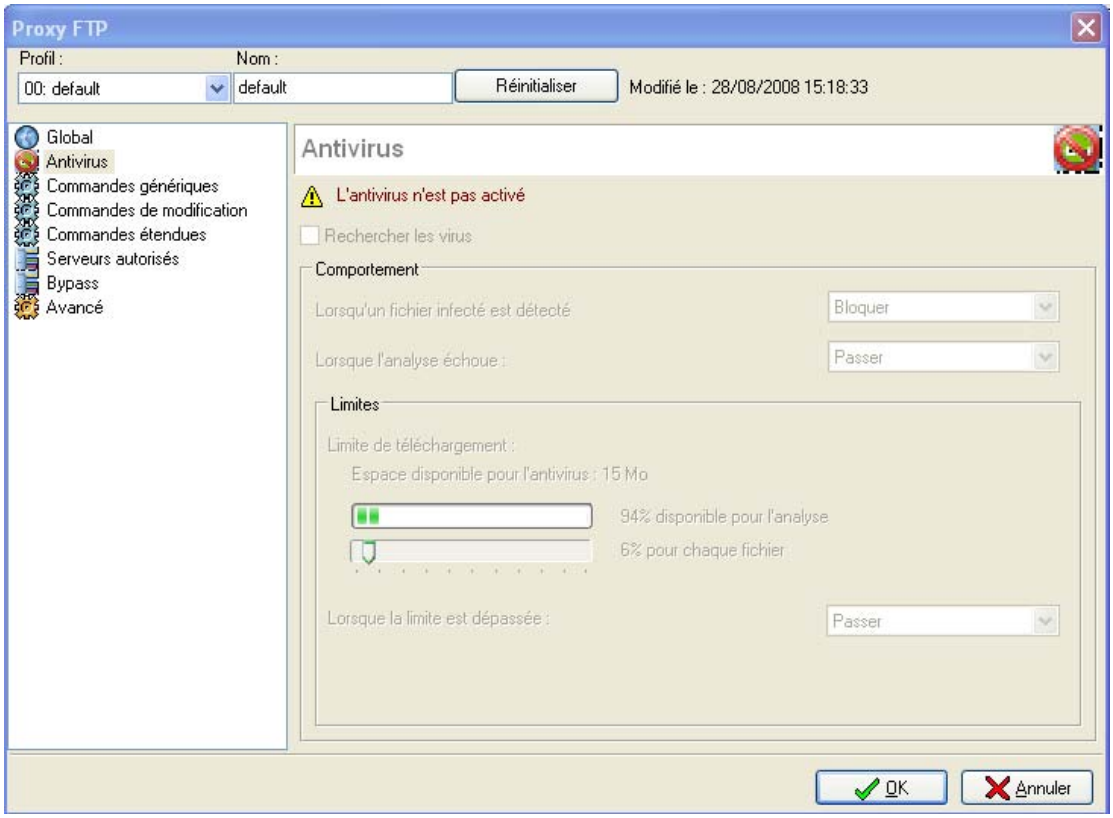


Figure 297 : Proxy FTP - Antivirus

L'activation du proxy FTP permet la configuration de l'antivirus.

Le message « Le moteur Antivirus n'est pas activé » vous indique qu'il faut activer l'antivirus. Cependant la configuration de l'antivirus au sein de du proxy n'est pas bloquante.

Rechercher les virus	Active la recherche des virus en cochant d'abord l'option **Activer le proxy FTP** du menu **`Global`**.
Comportement	La zone "Comportement" décrit l'état de l'antivirus face à certains événements. L'option Sur **detection d'un fichier infecté** contient 2 options : « Passer » et « Bloquer ». En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », l'antivirus transmet le fichier en cours d'analyse. L'option **Lorsque l'analyse échoue** définit l'état de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue **Exemple** Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer** est spécifié, le fichier en cours d'analyse est transmis.
Limites	Il est possible ici de déterminer la taille maximale utilisée pour l'analyse des fichiers. Pour cela, déplacez la réglette. Vous pouvez également configurer l'action à entreprendre si le fichier est supérieur à la taille autorisée. **AVERTISSEMENT** Lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total,

représenté par la réglette correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur SMTP est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps.

L'option **Lorsque la limite est dépassée** définit le comportement de l'antivirus si la taille du fichier d'analyse qu'il est en train de scanner dépasse la limite autorisée.

Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis.
Si **Passer** est spécifié, le fichier en cours d'analyse est transmis.

9.6.5.3. Commandes génériques

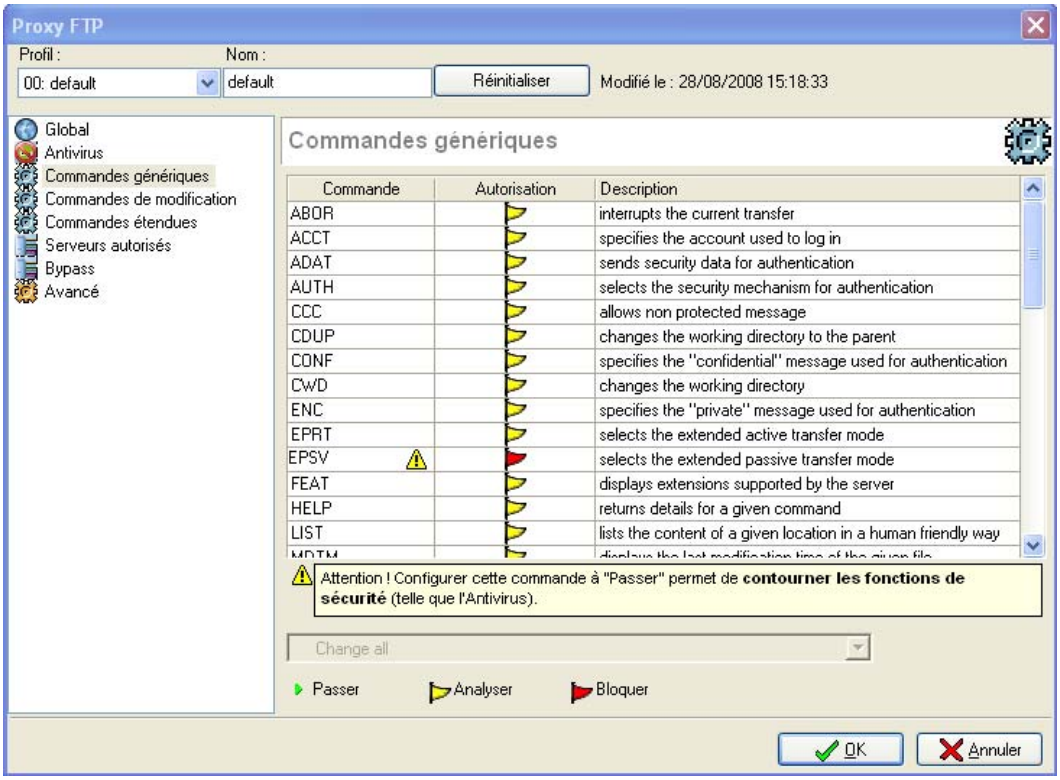


Figure 298 : Proxy FTP - Commandes génériques

Ce menu vous permet d'autoriser ou de rejeter les commandes FTP dites « génériques » définies dans les RFC. Vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

Cf. Annexe Q : Liste des commandes FTP génériques et détail du filtrage.

Commande	Nom de la commande. L'icône d'avertissement (qui est affichée pour certaines commandes) indique que vous pouvez modifier l'état de la dite commande mais pas sans risque. Ces commandes sont bloquées par défaut.
Autorisation	3 autorisations possibles entre « Passer », « Analyser » et « Bloquer ».
Description	Description de la commande.

9.6.5.4. Commandes de modification

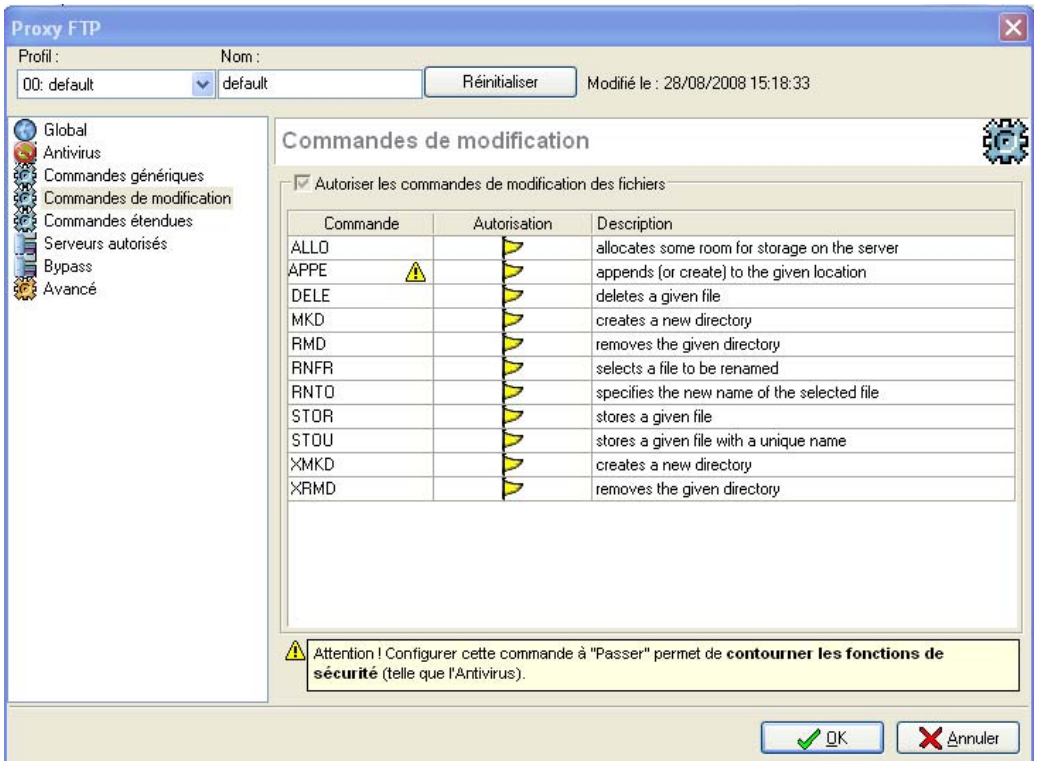


Figure 299 : Proxy FTP - Modification de commandes

Ce menu vous permet d'autoriser ou de rejeter les commandes FTP dites « de modification» définies dans les RFC. Il s'agit de commandes pouvant entraîner des modifications au niveau du serveur comme, par exemple, la suppression de données ou encore la création de répertoires. Le fonctionnement de ces commandes est identique aux commandes dites « génériques » : en effet, vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

Activer les commandes de modification	Cette option permet de passer le serveur en « lecture seule » : 3) Si vous cochez cette option, vous pouvez définir pour chaque commande une action parmi « Bloquer », « Analyser » et « Passer ». Par défaut, toutes les commandes sont à « Analyser ». 4) S vous décochez cette option, les commandes de modification sont à l'état « Bloquer ». Dans ce cas, il n'est pas possible de modifier l'état d'une commande.
Commande	Nom de la commande. L'icône d'avertissement (qui est affichée pour certaines commandes) indique que vous pouvez modifier l'état de la dite commande mais pas sans risque.
Autorisation	3 autorisations possibles entre « Passer », « Analyser » et « Bloquer ».
Description	Description de la commande.

Cf. Annexe R : Liste des commandes de modification FTP et détail du filtrage.

9.6.5.5. Commandes étendues

Ce menu vous permet de spécifier une liste de commandes qui seront autorisées à passer le proxy FTP. Si des commandesnon standard sont passées mais ne se trouvent pas dans cette liste, elles seront dans ce cas, bloquées par le firewall.

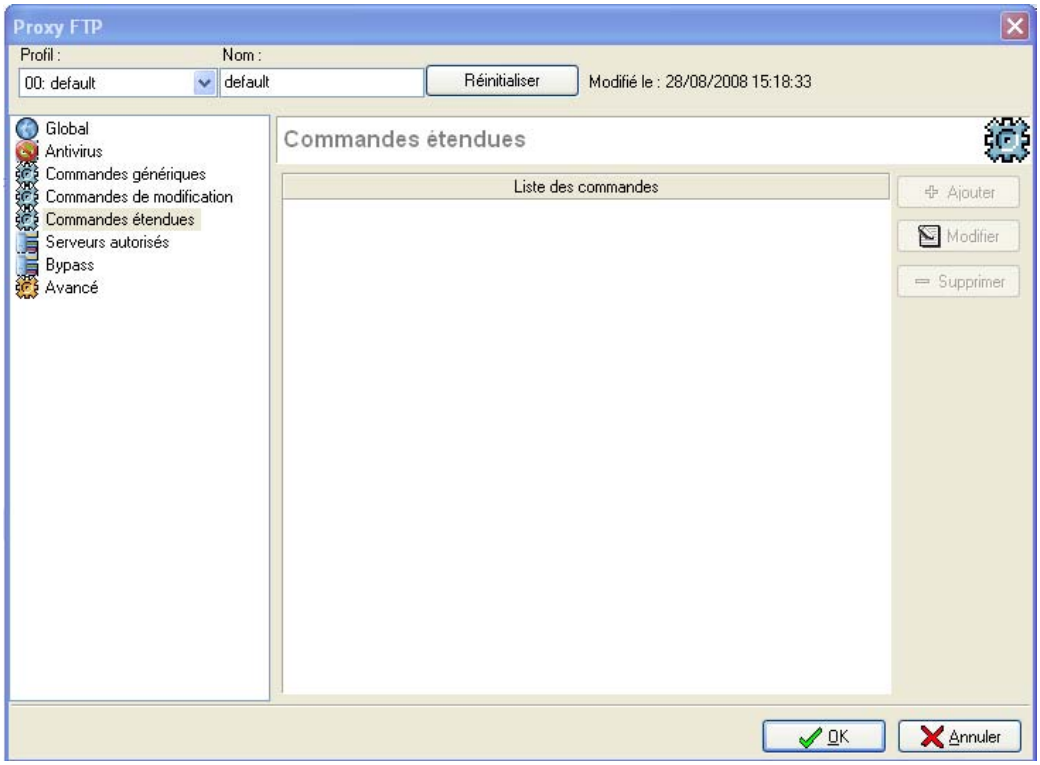


Figure 300 : Proxy FTP - Commandes extras

Ajouter	En cliquant sur le bouton **Ajouter**, l'écran suivant s'affiche, vous permettant de saisir le nom d'une nouvelle commande.

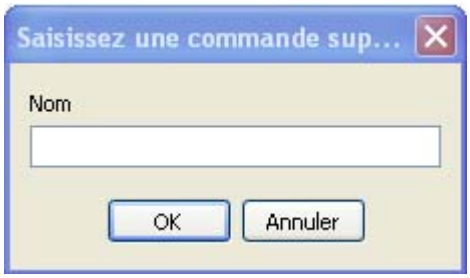


Figure 301 : Saisie d'une commande

Modifier	En cliquant sur ce bouton, vous pouvez modifier le nom de la commande.
Supprimer	Une fois la commande sélectionnée, en cliquant sur ce bouton, le message : « Supprimer la commande X ? » s'affiche. Confirmez ou non la suppression.

9.6.5.6. Serveurs autorisés

Ce menu permet de définir une liste de serveurs qui seront habilités à passer. Autrement dit, seuls les serveurs FTP de cette liste seront autorisés à passer.

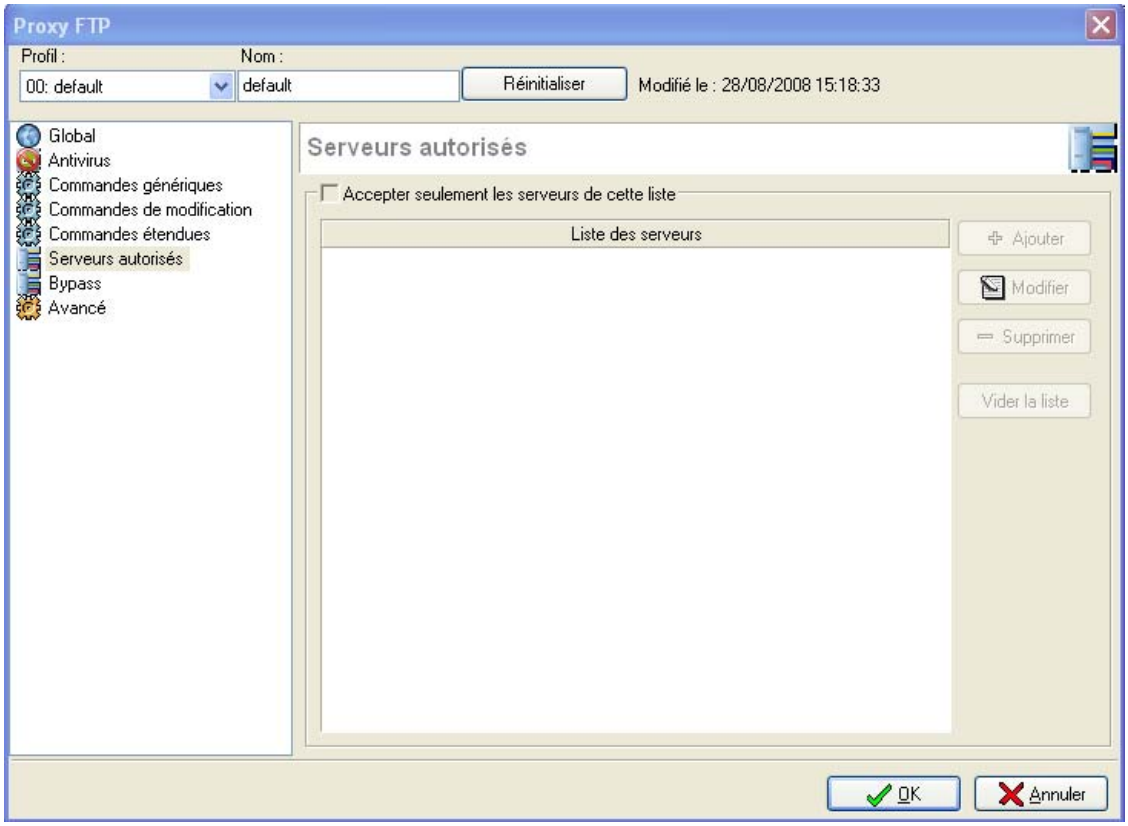


Figure 302 : Proxy FTP - Serveur autorisé

Accepter uniquement les serveurs de cette liste	Cette option permet aux utilisateurs de définir une liste de serveurs (sous forme d'objet de type HOST) abilités à passer. A partir de cette activation, tout trafic FTP qui n'est pas à destination de ces machines est bloqué. Cette option n'est pas activée par défaut afin de ne pas bloquer le trafic FTP.
Ajouter	En cliquant sur le bouton **Ajouter**, La base d'objets « Machines » s'affiche afin de sélectionner le/les serveurs.
Modifier	En cliquant sur ce bouton, vous pouvez remplacer le serveur préalablement sélectionné par un autre dans la base d'objets « Machines ».
Supprimer	Une fois le serveur sélectionné, en cliquant sur ce bouton, le message : « Supprimer la machine X ? » s'affiche. Confirmez ou non la suppression.
Vider la liste	Cette option supprime tous les serveurs indiqués dans la liste.

9.6.5.7. Bypass

Ce menu permet de lister les serveurs pour lesquels aucune analyse ne sera effectuée (vérification des commandes, analyse antivirus).
Ces traitements sont les suivants :

- La vérification des commandes.
- L'analyse antivirale.

Cette liste peut contenir juqu'à 128 serveurs.

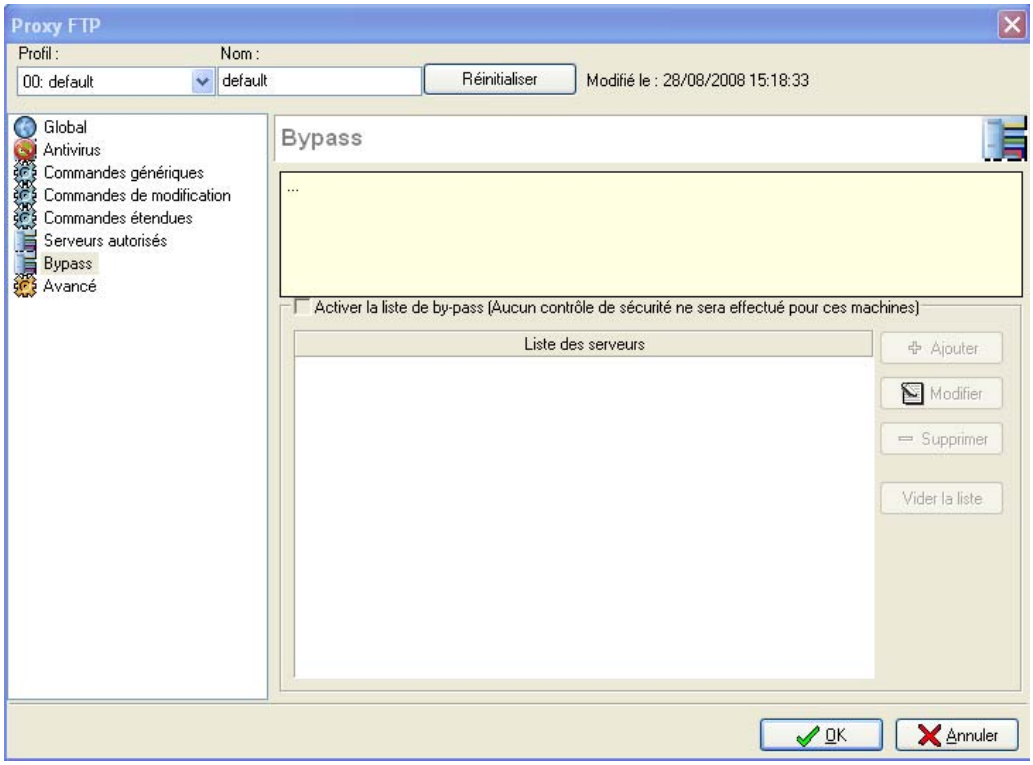


Figure 303 : Proxy FTP - Bypass

Le menu **Bypass** permet de configurer les paramètres suivants :

Activer la liste Bypass (Aucun contrôle de sécurité ne sera effectué pour ces machines)	Cette commande permet d'autoriser une liste de serveurs à passer le proxy FTP sans que les commandes soient analysées et sans que l'analyse antivirale soit faite.
Ajouter	En cliquant sur le bouton **Ajouter**, La base d'objets « Machines » s'affiche afin de sélectionner le/les serveurs.
Modifier	En cliquant sur ce bouton, vous pouvez remplacer le serveur préalablement sélectionné par un autre dans la base d'objets « Machines ».
Supprimer	Une fois le serveur sélectionné, en cliquant sur ce bouton, le message : « Supprimer la machine X ? » s'affiche. Confirmez ou non la suppression.
Vider la liste	Cette option supprime tous les serveurs indiqués dans la liste.

9.6.5.8. Avancé

Le menu Avancé permet de régler les modes de transferts entre le client et le proxy ainsi qu'entre le proxy et le serveur. Le mode de transfert permet de savoir quelles sont les entités qui initient les connexions :

Le proxy ftp permet également de régler finement les modes de transfert (any / actif / passif). Par défaut, le mode de transfert utilisé pour les connexions client-proxy et proxy-serveur est celui spécifié par le client.
En définissant un mode particulier pour les connexions serveurs, ce mode de transfert sera utilisé quelque soit le mode choisi par le client. Par contre, en définissant un mode particulier pour les connexions client, cela peut aboutir à l'émission d'une erreur FTP indiquant au client que le mode de transfert choisi n'est pas autorisé.

- En mode passif : le client indique qu'il veut utiliser le mode passif. Le serveur lui indique les paramètres de connexions (IP, port). Le client se connecte alors à l'adresse et au port indiqué.

- En mode actif, le client indique qu'il veut utiliser le mode actif en envoyant des paramètres de connexion (IP, port). Le serveur FTP se connecte ensuite à l'adresse et aux ports indiqués.

Lorsque le mode de transfert est établi, alors le transfert de données peut avoir lieu (Upload ou Download).

Le transfert de données s'effectue en deux temps, lorsque l'on souhaite faire de l'analyse antivirale avec le proxy FTP :

- Lors d'un download, le proxy commence le transfert du fichier dès la connexion, ceci afin d'éviter que le client (ou le serveur) se déconnecte, ne voyant pas de données arriver.
- Lors d'un upload, le proxy récupère les données du client FTP et effectue l'analyse avant d'envoyer les données au serveur.

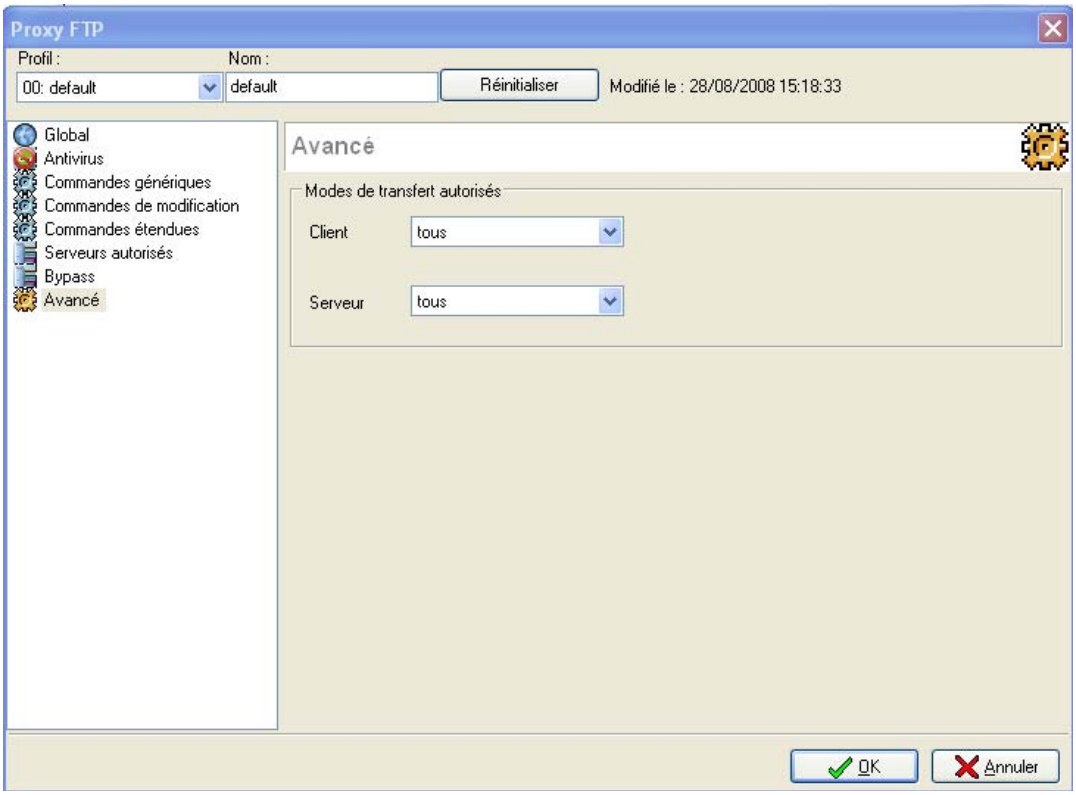


Figure 304 : Proxy FTP - Avancé

- Par défaut, les deux paramètres sont réglés sur « Any » :

Dans ce cas, le mode utilisé entre le proxy et le serveur FTP est le même que celui utilisé par le client. Par exemple, si le client demande un transfert en mode passif, dans ce cas, le proxy utilisera le mode passif avec le serveur FTP.

- Le client est sur n'importe quel mode/Le serveur est sur le mode actif ou passif :

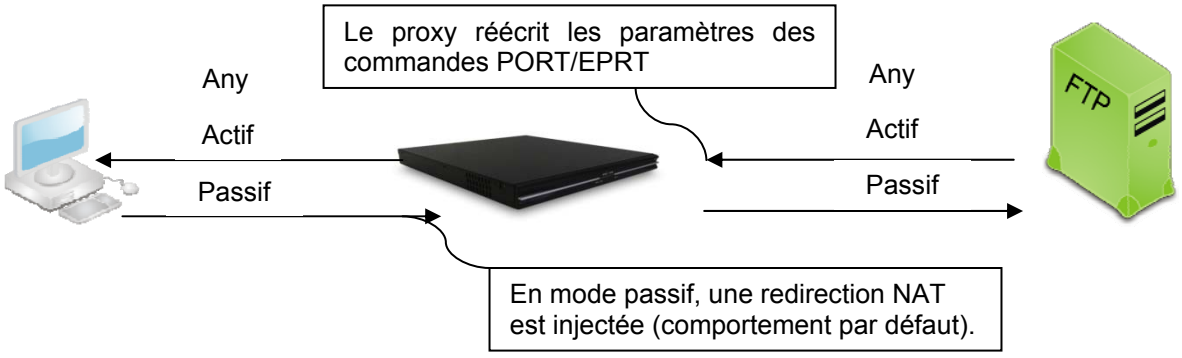
Gestion des connexions au serveur.

- Le client est sur le mode actif ou passif/ Le serveur est sur n'iporte quel mode :

Dans ce cas, le mode autorisé est géré du point de vue client.

Si les modes spécifiés sont différents, le proxy convertit automatiquement la commande spécifiant le mode utilisé. Dans le cas où le client FTP demande un mode passif et que la configuration force l'utilisation d'un mode actif entre le proxy et le serveur, le proxy n'initie aucune connexion (le client et le serveur se connectent tous les deux sur le proxy).

L'interception du trafic se fait de la manière suivante :



9.6.5.9. Postprocessing FTP

Flux de données soumis à l'antivirus

Seuls les transferts concernant l'envoi ou la réception de fichiers sont soumis à l'analyse antivirale.

Post-processing

Le post-processing du proxy FTP est capable de manipuler un bon nombre de types de transferts. Il gère, en effet, les modes passif et actif à la fois pour la réception et l'envoi de fichiers.
Le proxy FTP n'envoie que le strict minimum pour garder la connexion ouverte. Les clients FTP téléchargent le fichier directement à l'endroit définitif. Pour éviter qu'un fichier partiellement téléchargé ne contienne un virus, le proxy en envoie le moins possible. En conséquence, le débit temps réel en début de transfert sera quasi nul alors qu'il sera au maximum à la fin du transfert.

9.6.5.10. Regroupement de commandes

La liste des commandes FTP est conséquente. Il existe un groupe de commandes FTP qui agit en écriture. Ce qui permet de protégér u serveur en n'autorisant que la lecture seule aux clients.

Les commandes regroupées dans MODIFY sont :

- STOR
- STOU
- APPE
- ALLO
- RNFR
- DELE
- RMD
- MKD
- XRMD
- XMKD

PARTIE 10 : ANALYSE DE CONTENU

CHAPITRE 1. INTRODUCTION

10.1.1 Pour cette partie, vous devez avoir franchi les étapes :

- Partie 2 : Installation, pré-configuration, intégration.
- Définition des interfaces, des objets et de la configuration du noyau.
- Proxies HTTP, SMTP et POP3.

10.1.2. Pour cette partie, vous devez connaître :

- La politique de filtrage URL de l'entreprise.
- Les adresses des différents proxies.

10.1.3. Utilité de la partie

Cette partie vous permet de définir les règles de filtrage URL que vous allez appliquer aux postes.

10.1.4. Accéder à cette partie

➲ Accédez au filtrage de contenu en cliquant sur **`Analyse de contenu`** dans l'arborescence des menus de NETASQ UNIFIED MANAGER.

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications. Avant d'effectuer toute modification importante sur votre firewall NETASQ, nous vous conseillons d'effectuer une sauvegarde. Ainsi, en cas de mauvaise manipulation vous pourrez vous retrouver dans l'état précédent. Pour plus d'informations sur les sauvegardes, veuillez vous référer au chapitre adéquat. (Cf. Partie 18 : Maintenance).

10.1.5. Introduction à cette partie

Vous pouvez imposer l'authentification pour le filtrage d'URL. Lorsqu'un utilisateur voudra accéder au Web ou à certains sites Web, il devra alors s'authentifier. Lorsque le filtrage d'URL est actif et que l'utilisateur doit s'authentifier, une page d'authentification est proposée à ce dernier lors de la consultation d'un site Web.

Les tables de filtrage URL sont stockées sur le firewall NETASQ dans des slots (fichiers de configuration numérotés de 01 à 10). Chaque slot peut être programmé à une heure précise de la semaine, en écrasant la configuration du slot précédemment activée. (Cf. Partie 7/Chapitre 3 : Programmateur de slots).

CHAPITRE 2. ANTISPAM

10.2.1. Introduction

Le développement exceptionnel d'Internet et la banalisation de l'utilisation de l'e-mail ont favorisé l'émergement de ce qu'on appelle "le spam". Ces courriers électroniques indésirables, vantant les mérites de produits ou services, polluent encore et toujours les boîtes aux lettres électroniques des utilisateurs de messageries Web.

De plus, en recherche constante de nouvelles techniques de spams, les spammeurs déjouent une à une les contre-mesures mises en place par les administrateurs pour protéger les boîtes aux lettres de leurs utilisateurs. Ainsi les nouvelles contre-mesures se doivent de multiplier les méthodes d'analyse pour gérer des spams aussi variés et variables que possibles.

Le module Antispam intégré par NETASQ dans ses Appliance UTM est basé sur 4 méthodes d'analyse complémentaires: une analyse par liste noire DNS, une analyse heuristique, un filtrage par liste noire de domaines et un filtrage par liste blanche de domaines.

10.2.1.1. L'analyse par liste noire DNS (ou RBL DNS)

L'analyse par liste noire DNS ou **RBL** (***Real time Blackhole List)*** permet la qualification d'un message en spam par l'intermédiaire de serveurs RBL. Ces serveurs RBL contiennent des listes d'adresses IP identifiant les spammeurs et tous les serveurs qui relayent le spam sans le combattre.

Pour chaque message à analyser, l'appliance UTM demande auprès de ces serveurs **RBL** si l'expéditeur ou les relais de messagerie par lesquels le message a transité est considéré comme un spammeur. Puis l'Appliance UTM se base sur leur réponse pour qualifier le message comme un spam.

REMARQUE
Cette analyse nécessite la licence "NETASQ Antispam module" pour fonctionner.

10.2.1.2. L'analyse heuristique (ou bayésienne)

L'analyse heuristique est basée sur l'antispam Vade Retro de GOTO Software. Cet antispam utilise de 7 méthodes d'analyse pour évaluer la légitimité d'un mail analysé.

REMARQUE
Cette analyse heuristique requiert l'option de licence "OEM Antispam module".

Analyse par règles empiriques

L'analyse par règles empiriques est basée sur l'utilisation de règles, non prédictibles, déduites à partir de l'analyse approfondie de tous les composants du message (champs d'entête, texte du sujet, corps du texte, html, pièces jointes,...). Ces règles, déterminées par les experts Vade retro, définissent un ensemble de caractéristiques originales, communes à certains types de messages

> **Exemple**
> les messages envoyés par des robots.

Elles permettent ainsi de repérer de futurs messages qui posséderaient les mêmes caractéristiques.

Analyse sémantique

L'analyse sémantique consiste à comparer le contenu textuel du message à un dictionnaire prédéfini de mots et locutions caractéristiques des spams ou des messages légitimes. La technologie de recherche de locution de Vade Retro est aussi originale dans son approche, puisqu'elle permet de rechercher des combinaisons logiques de mots mais aussi de détecter des mots avec une orthographe approchante.

Recherche de contre-mesures

Les filtres de ce type constituent sans doute la partie le plus originale et la plus efficace du moteur de filtrage Vade Retro. Ils consistent à détecter, dans les messages, les techniques qu'emploient les spammeurs pour déjouer les solutions anti-spams utilisant les méthodes de filtrage "classiques".

Analyse du code HTML intégré

Lorsque le message contient une partie HTML, une "empreinte" de ce code est établie par l'antispam. Cette empreinte est alors comparée à une liste "d'empreintes" couramment utilisées par les spammeurs. Cette méthode, associée à une technique de statistiques sur les tailles d'images, permet d'identifier, entre autres, certains messages indésirables qui ne contiennent pas de texte, mais seulement une ou plusieurs images.

Recherche de langues étrangères non latines

L'apparition de plus en plus courante de spams en provenance de l'Asie ou des pays de l'Est rend désormais indispensable l'identification des jeux de caractères non latin. Cela soit lors de la déclaration du jeu de caractères soit lors de son utilisation effective.

Analyse Anti-Scams

Les scams sont des escroqueries qui reposent le plus souvent sur des propositions de participation à une opération financière internationale très alléchante. Initialement pratiqués par courrier traditionnel ou par fax, les scams ont aujourd'hui leur déclinaison par e-mail sous forme de spams qui ne ressemblent pas aux autres messages publicitaires habituellement filtrés. La technologie Vade Retro inclut un module spécifique de détection des messages de ce type.

Détection des notifications d'antivirus et de non remise

Les serveurs de messagerie sont actuellement engorgés par les messages de notification induits par la prolifération des virus par e-mail. En effet, ce type de virus exploitent les carnets d'adresses des machines infectées et envoient des messages en falsifiant l'adresse de l'émetteur. Le filtrage de Vade Retro comporte un module spécifique d'identification des divers messages de notification émis par les serveurs SMTP lors de la détection d'un virus ou de la non remise d'un message à une adresse e-mail inexistante.

10.2.1.3. Domaines en liste noire

Les deux premières analyses très évoluées du module Antispam NETASQ sont complétées par des filtres basiques de domaines. Le filtrage par liste noire de domaines contient la liste des domaines qui doivent être systématiquement considéré comme spammeurs.

10.2.1.4. Domaine en liste blanche

Le filtrage par liste blanche de domaines définit ce que contient la liste des domaines qui doivent être systématiquement considéré comme légitimes.

10.2.2. Utilisation possible de l'antispam des produits UTM NETASQ

L'antispam permet de marquer les e-mails lorsqu'ils correspondent à du spam. Ainsi il est alors possible de classer automatiquement ces mails grâce aux fonctions de "rangement" de votre client de messagerie. NETASQ conseille de réaliser des filtres de vos mails et de placer un filtre spécial correspondant au spam à la toute fin de vos filtres. Ainsi si un de vos mails valide est tout de même marqué comme du spam, il est rangé par vos filtres personnels avant d'être traité par le filtre du spam.

NOTE
Le module **Antispam** détermine un niveau de confiance (de 1 à 3) qui définit un niveau de certitude qu'a le module Antispam d'avoir détecté un spam (1 pour peu confiant, 3 pour très confiant). Ce niveau de confiance se retrouve dans la configuration notamment des serveurs RBL.

10.2.3. Fonctionnement

Le module Antispam nécessite une activation dans les menus Proxy SMTP et POP3. En effet, l'analyse Antispam ne fonctionne que par un proxy.

Lorsqu'elles sont disponibles, il est possible d'activer ou non ces analyses.
Aussi, pour fonctionner, l'antispam dépend de la licence, des proxies SMTP/POP3 et de la configuration DNS du boîtier.

Pour utiliser l'antispam des firewalls NETASQ, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu **Analyse de contenu\Antispam** de l'arborescence.

AVERTISSEMENT
Le proxy DNS doit être activé pour le fonctionnement de l'antispam.

L'écran de configuration du service Antispam se décompose en deux parties :

- A gauche un arbre présentant les diverses fonctionnalités du menu **`Antispam.`**
- A droite les options configurables.

La configuration de ce module n'est pas dépendante d'autres modules.

Les boutons **Envoyer** et **Annuler** situés dans le coin inférieur droit permettent respectivement l'application des modifications effectuées sur la configuration et l'annulation des modifications.

10.2.3.1. Général

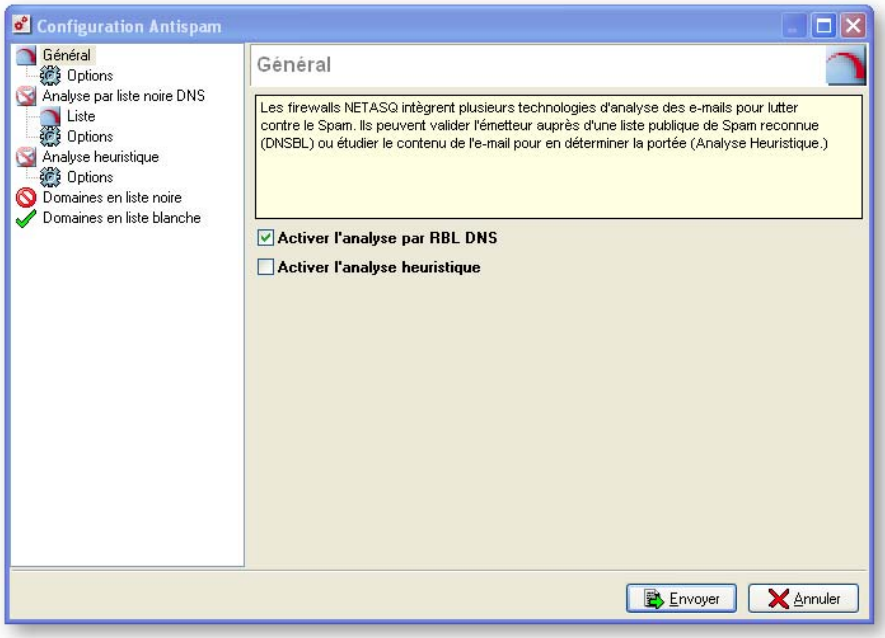


Figure 305 : Ecran Général de l'Antispam

L'activation de l'antispam s'effectue en déterminant qu'elles seront les analyses activées. Deux choix sont disponibles sur le firewall : Le premier, permet de valider lémetteur auprès d'une liste publique de Spams reconnue (DNSBL). Le 2ème, permet d'étudier le contenu du mail pour en déterminer la portée.

Activer l'analyse par RBL DNS	Permet d'activer l'analyse par liste noire DNS.
Activer l'analyse heuristique	Permet d'activer le module Antispam Vade Retro.

Options

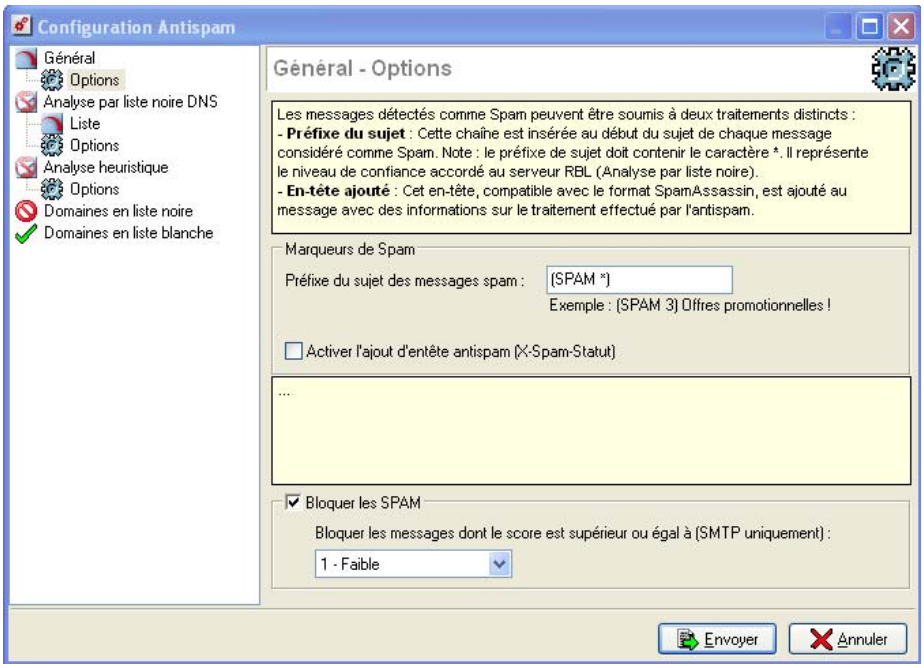


Figure 306 : Ecran Options de l'antispam

Les messages identifiés comme spam ne sont pas supprimés par le module AntiSpam du boîtier UTM NETASQ. Cependant il effectue des actions de modifications du message détecté comme spam de façon à permettre un traitement futur par le client de messagerie Web par exemple. Deux actions de marquage sont disponibles :

Préfixe du sujet des messages spam	Le sujet des messages identifiés comme spam sont préfixés par la chaine de caractères définis. Par défaut cette chaîne est **(SPAM *)** où ***** représente le niveau de confiance accordé. Ce score peut varier de 1 à 3. Plus ce score est élevé, plus il est probable que le courrier soit du pourriel. Quelle que soit la chaîne de caractères utilisée, il est indispensable de prévoir l'insertion du niveau de confiance dans cette chaîne en utilisant ***.** Cet * sera ensuite remplacé par le score. La longueur maximale du préfixe peut être de 128 caractères. Les courriers identifiés comme spam sont acheminés et non supprimés. **AVERTISSEMENT** Les caractères "guillemets doubles, guillemets simples et dièse ne sont pas autorisés).
Activer l'ajout d'entête antispam (X-Spam-Statut)	En cochant cette option, le module Antispam ajoute au message identifié comme spam, un entête synthétisant le résultat de son analyse pour ce message. Cet entête antispam, au format "spam assassin" peut ensuite être utilisé par le client de messagerie Web pour effectuer les traitements adéquats sur le message marqué.
Bloquer les SPAM	En cochant cette option, le proxy SMTP répond au serveur SMTP distant en indiquant un rejet pour cause de spam. L'option **Bloquer les messages dont le score est supérieur ou égal à (SMTP uniquement)** permet de definir à partir de quel seuil de confiance un mail sera rejeté. Les seuils sont : « 1 – Faible », « 2 – Modéré », « 3 – Elevé ». Pour exemple : si vous configurez au niveau de l'analyse heuristique un seuil de 500, les mails seront considérés comme spam à partir de 500. De 500 à 1000, le

niveau de confiance sera faible, de 1000 à 1500, il sera modéré, de 1500 à 2000, il sera élevé. Si vous avez indiqué au niveau de cette option un seuil de confiance modéré, tous les mails de niveau modéré et élevé (donc de 1000 à 2000) seront rejetés alors que ceux de 500 à 1000 seront gardés.

REMARQUE
Lorsque plusieurs méthodes d'analyse sont utilisées simultanément, le plus haut niveau de score est attribué.

10.2.3.2. Analyse par liste noire DNS

L'analyse par liste noire DNS ou **RBL** (*Real time Blackhole List*) permet la qualification d'un message en spam par l'intermédiaire de serveurs RBL. Les menus suivant permettent de configurer la liste des serveurs RBL qui seront utilisés pour cette analyse ainsi que le niveau de confiance accordé à chacun des serveurs.

Liste

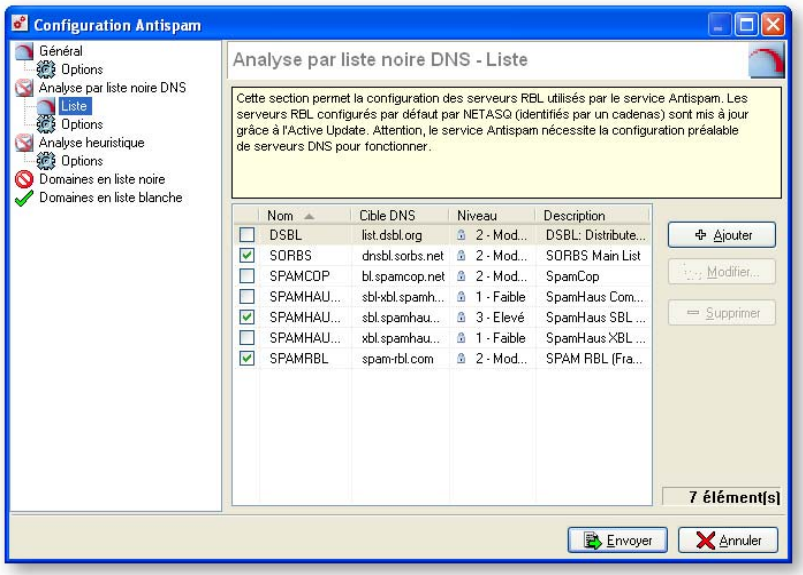


Figure 307 : Analyse par liste noire - Liste

Dans cette section, une grille affiche une liste des serveurs RBL auxquels le boîtier UTM envoie ses requêtes pour vérifier qu'un e-mail n'est pas un spam. Cette liste est actualisée par l'Active Update. Elle n'est pas modifiable mais vous pouvez toutefois désactiver certains serveurs en cliquant sur la case présente au début de chaque ligne.

Le niveau spécifié dans les colonnes de la grille indique le niveau de confiance accordé à ce serveur.

Vous pouvez aussi configurer vos propres serveurs RBL auxquels vous souhaitez que l'Appliance se connecte. Pour ajouter un serveur, cliquez sur le bouton **Ajouter.** L'écran suivant s'affiche :

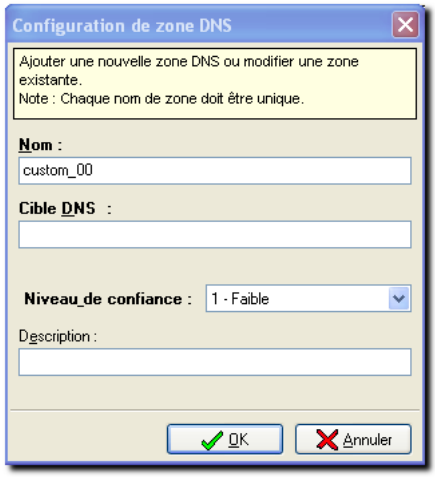


Figure 308 : Configuration de zone DNS

Spécifiez un nom pour ce serveur (unique pour la liste des serveurs RBL), une cible DNS (nom DNS uniquement. Cela doit être un nom de domaine valide), un niveau de confiance (Faible, Modéré, Elevé) et enfin une description. L'indication de la description est facultative. Puis cliquez sur **OK.**

Pour supprimer ou modifier un serveur configuré, cliquez respectivement sur les boutons **Supprimer** et **Modifier**.

NOTE
Le proxy DNS doit être activé pour le fonctionnement de l'antispam.

Notez que la différenciation entre les serveurs RBL nativement configurés par NETASQ et les serveurs configurés de manière personnalisée s'effectue grâce au cadenas qui indique les serveurs **RBL** nativement configurés par NETASQ.

Rappel : seule la liste de ces serveurs est mise à jour par **Active Update**.

Options

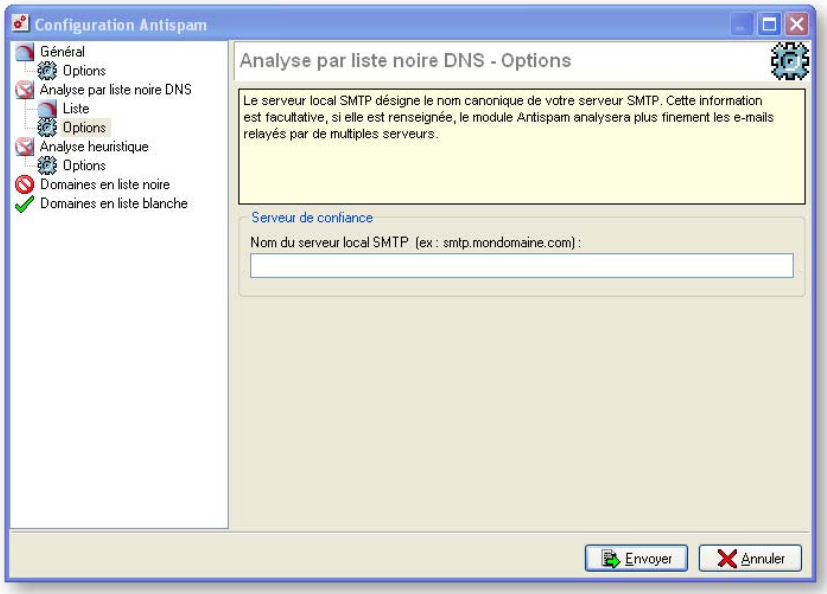


Figure 309 : Analyse par liste noire DNS - Options

Le serveur de confiance concerne le serveur SMTP. En renseignant ce champ, qui est facultatif, les e-mails seront analysés de manière plus fine par le module Antispam.

Nom du serveur local SMTP (ex. : smtp.mondomaine.com	Le serveur local **SMTP** désigne le nom canonique de votre serveur SMTP. Cette information est facultative, si elle est renseignée, le module AntiSpam analysera plus finement les e-mails relayés par de multiples serveurs.

10.2.3.3. Analyse heuristique

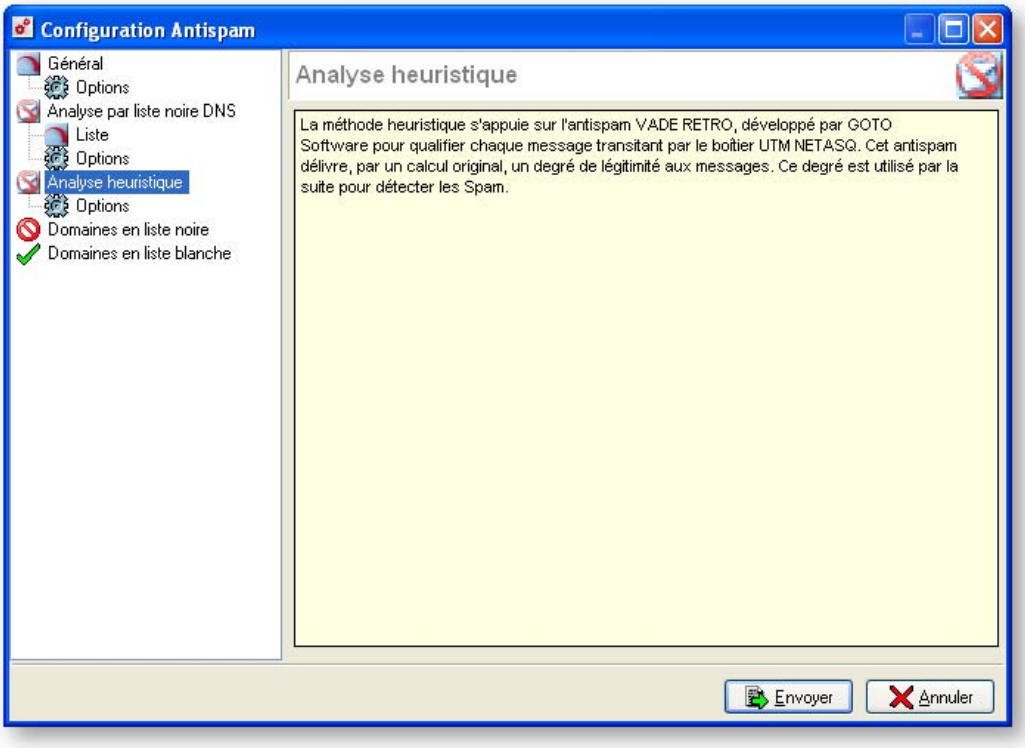


Figure 310 : Analyse heuristique

L'analyse heuristique est basée sur l'Antispam Vade Retro de GOTO Software. Cet antispam délivre, par un calcul original, un degré de légitimité aux messages. La configuration de l'analyse effectuée par Vade Retro s'effectue dans le menu **Options** du menu de l'analyse heuristique.

Options

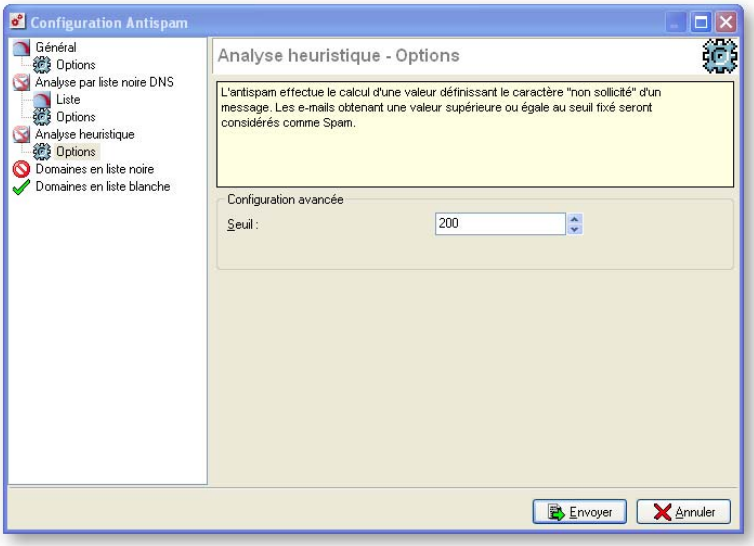


Figure 311 : Analyse heuristique - Options

Seuil L'analyse heuristique effectuée par le module Antispam effectue le calcul d'une valeur définissant le caractère "non-sollicité" d'un message. Les e-mails obtenant une valeur supérieure ou égale au seuil fixé seront considérés comme spams. Cette section permet de définir le seuil à appliquer, par défaut NETASQ choisit "200".

De plus, plus cette valeur calculée est élevée plus le niveau de confiance accordé par l'antispam à l'analyse sera élevé. Les seuils de franchissement des niveaux de confiance ne sont pas configurables dans NETASQ UNIFIED MANAGER.

10.2.3.4. Domaines en liste noire

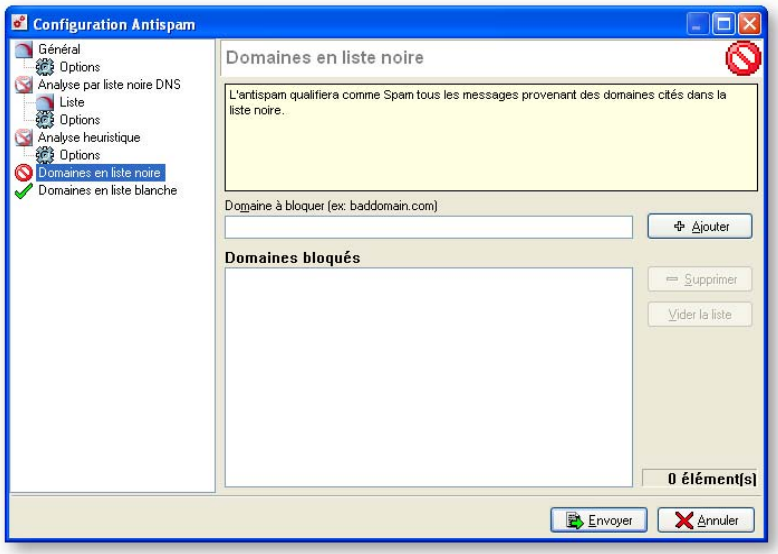


Figure 312 : Domaines en liste noire

Cette section permet de définir les domaines en provenance desquels les messages analysés seront systématiquement définis comme spam. Pour ajouter un domaine à bloquer, référez-vous à la procédure suivante :

Domaine à bloquer (ex.baddomain.com)	Permet de spécifier le domaine à bloquer. Cliquer sur **Ajouter**. Le domaine ainsi ajouté apparaît alors dans la liste des domaines bloqués. Chaque message identifié comme spam du fait de ces domaines en liste noire seront associés au niveau de confiance le plus élevé (à savoir 3). Pour supprimer un domaine donné ou la liste complète des domaines, cliquez respectivement sur **Supprimer** et **Vider la liste**.

10.2.3.5. Domaines en liste blanche

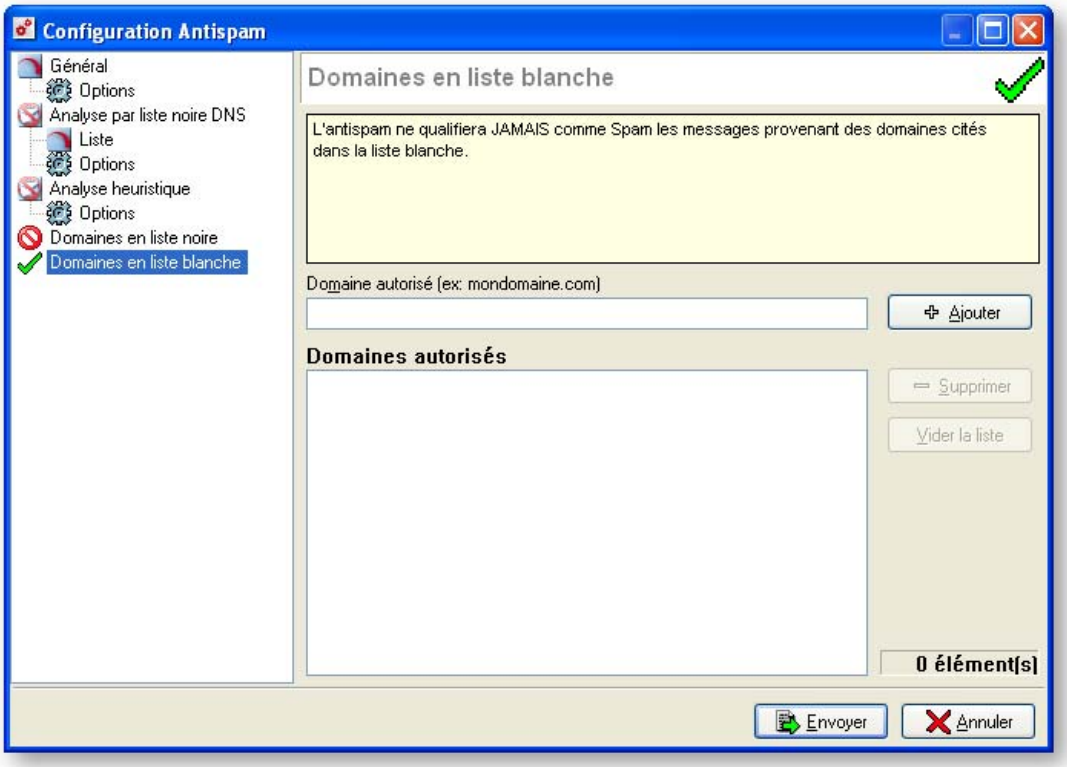


Figure 313 : Domaines en liste blanche

Cette section permet de définir les domaines en provenance desquels les messages analysés seront systématiquement définis comme **légitimes**. Pour ajouter un domaine à autoriser, référez-vous à la procédure suivante :

Domaine autorisé (ex: mondomaine.com)	Permet de spécifier le domaine à autoriser. Cliquer sur **Ajouter**. Le domaine ainsi ajouté apparaît alors dans la liste des domaines en liste blanche. Pour supprimer un domaine donné ou la liste complète des domaines, cliquez respectivement sur **Supprimer** et **Vider la liste**.

10.2.3.6. Remarques sur les domaines en liste noire et en liste blanche

Le filtrage par liste blanche et liste noire prévaut sur les méthodes d'analyses par liste noire DNS et analyse heuristique. Le nom de domaine de l'expéditeur est successivement comparé aux domaines en liste noire et liste blanche.

Pour chacune des listes, il est possible de définir jusqu'à 50 domaines. Il n'est pas possible d'avoir dans une liste le même domaine. Par contre, ce domaine peut être présent en liste blanche et en liste noire. Cependant, la liste noire est prioritaire.

Un nom de domaine peut contenir des caractères alphanumériques, "_", "-" et ".". Les caractères "Wildcard" "*" et "?" sont également autorisés. La longueur du nom de domaine ne peut excéder 128 caractères.

CHAPITRE 3. ANTIVIRUS

De part sa position centrale sur votre réseau, le produit UTM NETASQ est un élément important de la politique de sécurité de votre entreprise. En tant que passerelle indispensable en direction et vers l'Internet, votre firewall vous protège contre les intrusions grâce notamment à son moteur de prévention et de détection d'intrusion l'ASQ.

Cette protection contre les intrusions est associée à un service Antivirus permettant le filtrage du contenu des trafics transitant au travers du firewall à la recherche de virus, portes dérobées (backdoor), chevaux de Troie (Trajan) ou autres malwares que l'on rencontrer sur Internet.

L'offre de service Antivirus sur les firewalls NETASQ se compose de deux solutions.

10.3.1. Le service antivirus ClamAV

Le projet "Open-source" de l'antivirus **ClamAV** est intégré gratuitement et par défaut dans les produits firewalls NETASQ. Il offre ainsi une protection contre les virus et complète l'offre de protection tout en un des firewalls NETASQ.

Démon multi-threadé (il peut effectuer plusieurs tâches simultanément) rapide, flexible et extensible, il est une solution performante aux problèmes causés par les virus circulant sur Internet. Disposant d'une base d'environ 36 000 signatures de virus, vers et Chevaux de Troie, il offre une bonne protection qui se complète de jour en jour.

10.3.2. Le service antivirus Kaspersky

Kaspersky Labs est un éditeur international de logiciels antivirus, anti-hacker et contre le spamming fondé en 1997.

Grâce à un dur travail et à une profonde implication, Kaspersky Labs est devenu un leader en matière de développement de systèmes de défense antivirus. Kaspersky Labs a été le premier à développer de nombreux standards de technologie dans l'industrie de l'antivirus, y compris des solutions de grande envergure pour Linux, Unix et NetWare, un analyseur heuristique de seconde génération conçu pour détecter les virus encore inconnus, un système de défense efficace contre les virus polymorphes et géants,

une base de données antivirus mise à jour régulièrement **(elle dispose actuellement de plus de 120 000 signatures)** et la capacité de rechercher des virus dans les fichiers d'archive.

Le service antivirus Kaspersky est désormais intégré au sein de la Suite d'Administration de NETASQ.
Il suffit juste d'installer une licence compatible puis de sélectionner ce service dans NETASQ UNIFIED MANAGER.

AVERTISSEMENTS

1) La mise en place du service Antivirus du firewall NETASQ n'apporte pas une solution globale aux problèmes que posent les virus.
2) Il est INDISPENSABLE de mettre en place une solution qui analyse les postes de travail et serveurs pour protéger vos ressources réseau contre l'insertion de virus par des voies telles que les systèmes physiques de transport de données (disquettes, …).

10.3.3. Utilisation possible du service Antivirus du firewall NETASQ

En complément du filtrage effectué par les proxies **SMTP**, **POP3** et **HTTP** (Activation préalable des proxies pour l'utilisation du service Antivirus), le service Antivirus vous protège des virus se cachant dans le flux de données SMTP, POP3 et HTTP.

AVERTISSEMENT

Le service antivirus ne fonctionne que sur les interfaces sur lesquelles les proxies **SMTP**, **POP3** et **HTTP** ont été activés. Dans le cas où vous désirez protéger votre réseau contre les virus provenant d'un trafic SMTP externe, il est nécessaire d'activer le proxy SMTP en ce sens (Cf. Partie 9 : Proxies HTTP, SMTP et POP3).

10.3.4. Fonctionnement

Pour utiliser le service Antivirus, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu **Analyse de contenu\Antivirus** de l'arborescence.

L'écran de configuration du service Antivirus se décompose en deux parties :

- A gauche un arbre présentant les diverses fonctionnalités du menu **Antivirus.**
- A droite les options configurables.

L'activation du service Antivirus d'un firewall NETASQ nécessite certaines opérations préalables :

1. Activation des proxies des menus **Proxy SMTP**, **Proxy POP3** et **Proxy HTTP.**
2. Activation de l'antivirus du menu **Analyse de contenu\Antivirus**.

10.3.5. Général

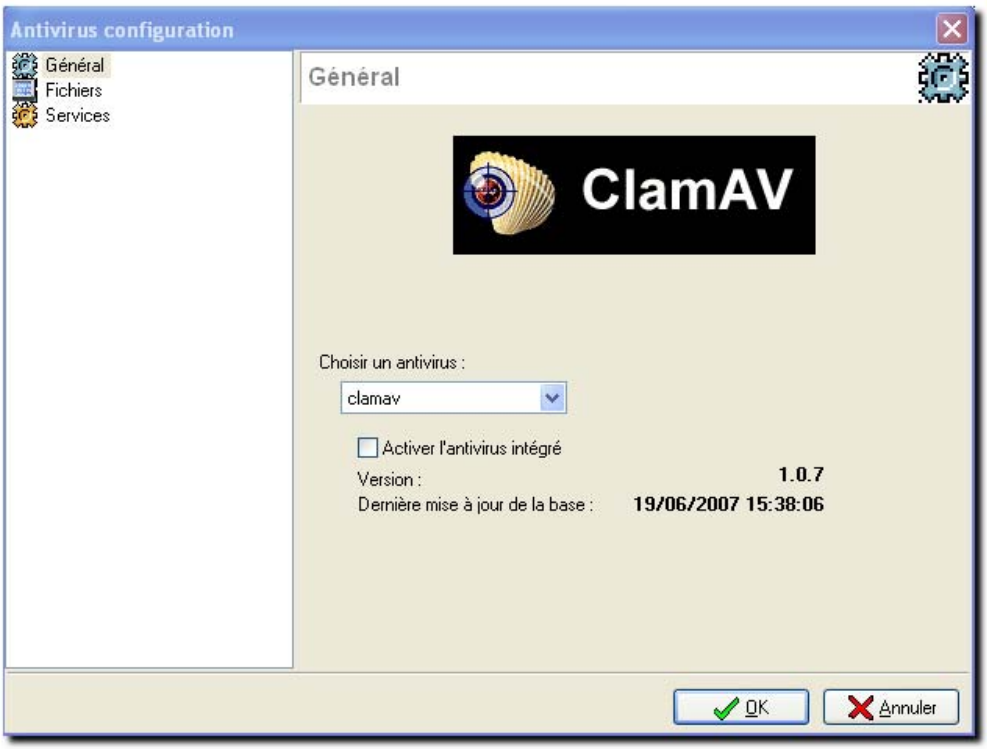


Figure 314 : Antivirus configuration - Général

L'activation du service permet d'analyser les trafics **SMTP**, **POP3** ou **HTTP** (suivant la configuration des proxies réalisée préalablement. (Cf. Partie 9 : Proxy SMTP, Proxy POP3 et Proxy HTTP).
Le menu de configuration général du service antivirus des firewalls NETASQ est constitué de plusieurs options expliquées dans le tableau suivant :

Figure 315 : Choisir un antivirus

Choisir un antivirus	A partir du menu déroulant, sélectionnez l'antivirus de votre choix : 2 antivirus sont disponibles : Clamav et Kaspersky.
Activer l'antivirus intégré	Cochez l'option pour activer la protection contre les virus. Par défaut l'antivirus **ClamAV** est utilisé pour fournir cette protection mais il est possible de bénéficier du service antivirus Kaspersky, pour cela contactez votre partenaire.
Version	Donnée informative indiquant la version du moteur antiviral intégrée dans ses produits firewalls NETASQ.
Dernière mise à jour de la base	Donnée informative indiquant la date de la dernière mise à jour réussie de la base antivirale de l'antivirus. La mise à jour de la base antivirale est un élément important dans la garantie d'un service antivirus performant et efficace. En effet lorsqu'un nouveau virus apparaît, il est important de bénéficier au plus vite de sa signature pour s'en protéger. Les modalités de mise à jour automatique de la base antivirale sont définies dans l'**Active Update**.

10.3.6. Fichiers

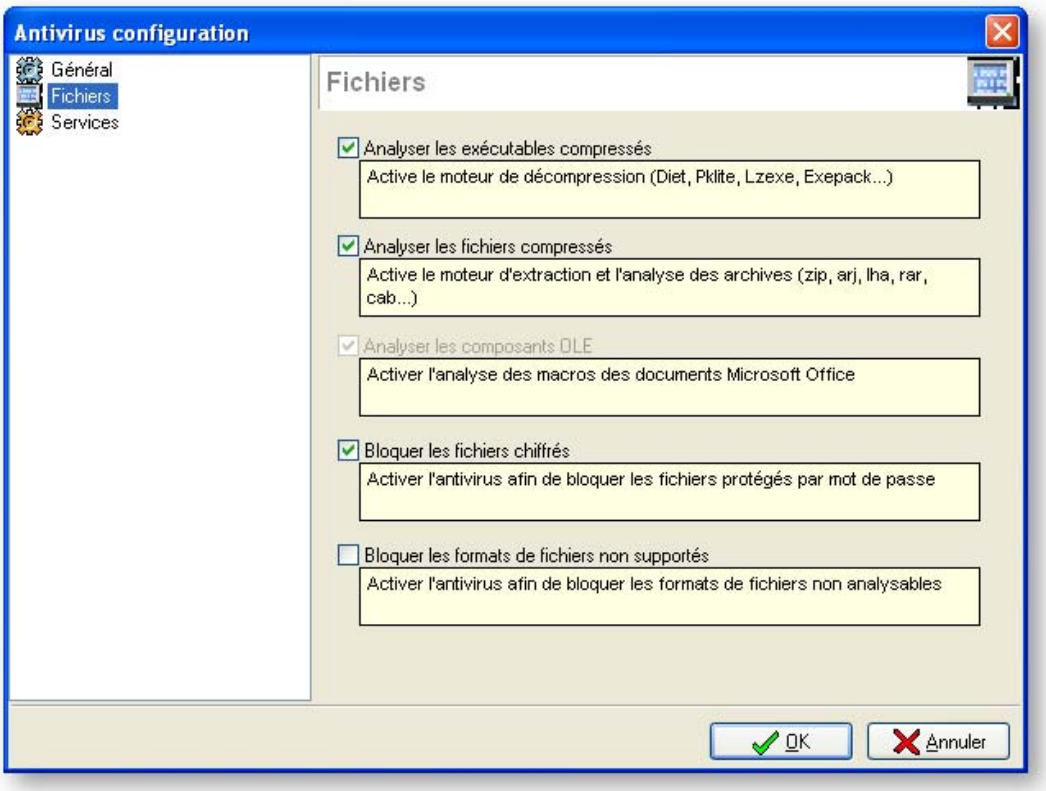


Figure 316 : Antivirus configuration - Fichiers

Dans ce menu, vous configurez les types de fichiers qui doivent être analysés par le service Antivirus du firewall NETASQ.

Analyer les exécutables compressés	Cette option permet d'activer le moteur de décompression.
Analyser les fichiers compressés	Cette option permet d'activer le moteur d'extraction et d'analyser les archives.
Analyser les composants OLE	Cette option permet d'activer l'analyse des macros des documents Microsoft Office.
Bloquer les fichiers chiffrés	Cette option permet d'activer l'antivirus afin bloquer les fichiers protégés par mot de passe.
Bloquer les formats de fichiers non supportés	Cette option permet d'activer l'antivirus afin de bloquer les formats de fichiers non analysables.

10.3.7. Services

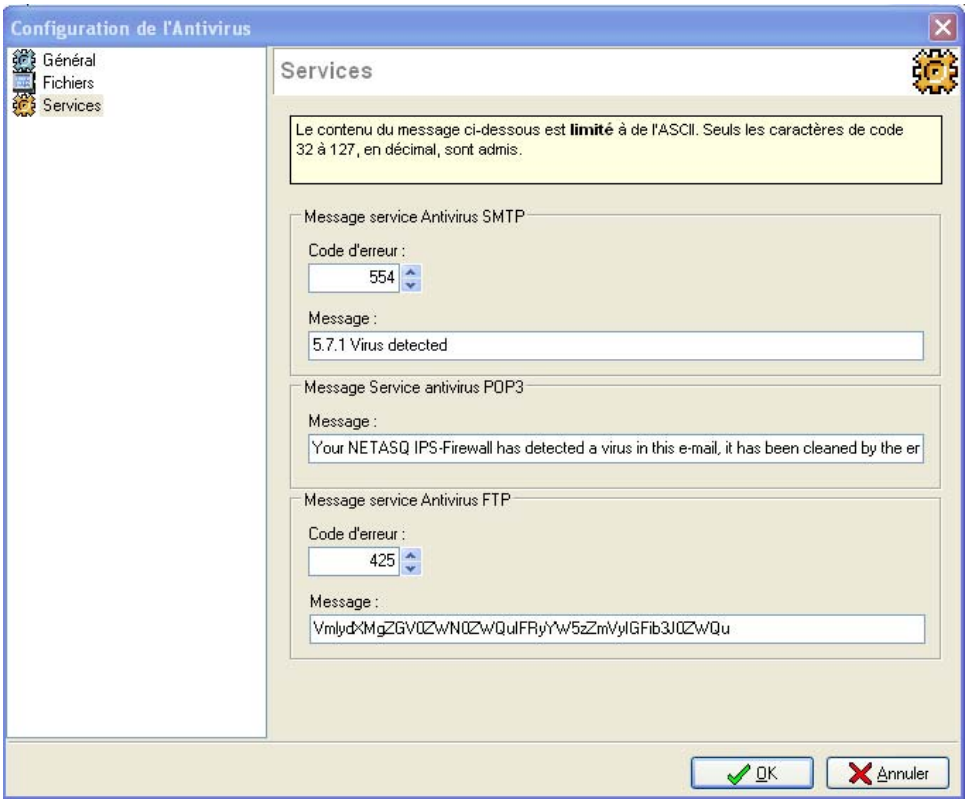


Figure 317 : Antivirus configuration - Services

La configuration avancée de l'antivirus **Kaspersky** intégré permet de personnaliser les réponses envoyées aux utilisateurs lorsqu'un mail contient un virus. Le tableau suivant explique les différents paramètres.

Code d'erreur	Code d'erreur SMTP renvoyé à l'expéditeur lors de la découverte d'un virus dans un trafic SMTP.
Message	Message associé au code d'erreur SMTP.
Message Service antivirus POP3	Lors de la découverte d'un virus sur un trafic POP3, un e-mail est créé par le firewall NETASQ. Il contient le message indiqué dans ce champ et une partie de l'e-mail original (expéditeur, destinataire et sujet principalement). Cet e-mail est alors envoyé par le firewall à l'émetteur de la requête POP3 sur laquelle a été découvert le virus.
Message service Antivirus FTP	Lors de la découverte d'un virus sur un trafic FTP, un e-mail est créé par le firewall NETASQ. Il contient un code d'erreur et le message indiqué dans le champ **Message** et une partie de l'e-mail original (expéditeur, destinataire et sujet principalement). Cet e-mail est alors envoyé par le firewall à l'émetteur de la requête FTP sur laquelle a été découvert le virus.

CHAPITRE 4. FILTRAGE D'URL

Définir une politique de filtrage d'URL consiste à créer des règles afin de déterminer quelles seront les pages Web autorisées ou bloquées à travers le firewall. Ce filtrage sert donc exclusivement au trafic http et permet de bloquer l'accès à certains sites selon des critères définis.

Lorsque vous sélectionnez le menu **`Analyse de contenu\Filtrage d'URL\Règles de filtrage`** une boîte de dialogue s'affiche, elle vous permet de manipuler les slots associés au filtrage URL.

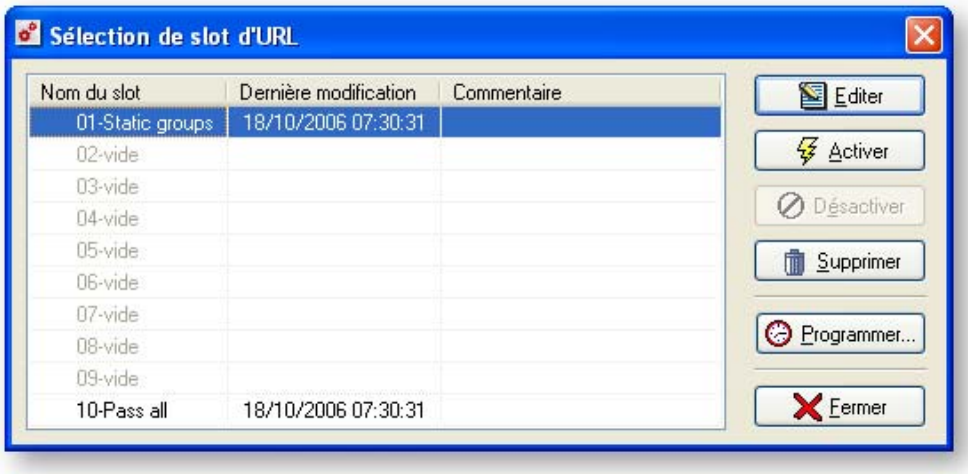


Figure 318 : Sélection de slot d'URL

AVERTISSEMENT
Le filtrage d'URL est actif si un des profils du proxy http est actif.

Elle est découpée en deux zones :

Gauche	Liste des politiques ou slots.
Droite	Actions sur le slot sélectionné.

10.4.1. Liste des slots

Dans cette partie de la boite de dialogue se trouve la liste des slots. Il en existe 10, numérotés de 01 à 10.

Chaque politique possède un nom, une date/heure de mise en activité et la date de dernière modification effectuée sur ce slot. La programmation de l'activation de ces slots se fait grâce au programmateur horaire (Cf. Partie 7/Chapitre 3 : Programmation horaire).

Le slot en cours d'activité est indiqué par une petite flèche verte à gauche de son nom. Un slot est dit "en activité" lorsque les paramètres qu'il contient sont en service. Il ne peut y avoir plus d'un slot en activité car les paramètres du dernier slot activé écrasent ceux du slot activé précédemment.

Si vous modifiez un slot, vous devez le réactiver pour prendre en compte les modifications. Un slot modifié mais non réactivé est notifié par l'icône à la place de la flèche verte habituelle.

Il est possible qu'il n'y ait aucun slot en activité, cela implique que tous les sites web sont bloqués (action par défaut) sauf si une règle autorisant le **HTTP** est ajoutée dans les règles de filtrage.

Chaque slot ne doit pas obligatoirement contenir des paramètres.
Un slot pour lequel il n'existe pas de fichier de configuration sur le firewall NETASQ est affiché sous le nom "vide" dans la liste.

Un slot est dit sélectionné quand vous faites un simple clic de la souris sur son nom. La sélection faite, vous pouvez l'éditer ou l'activer.

10.4.2. Actions sur le slot sélectionné

Par défaut un slot de filtrage d'URL a été configuré. Ce slot n'est pas actif mais peut l'être. Il est un exemple des possibilités offertes par le filtrage d'URL NETASQ.

10.4.3. Groupes d'URL

La création de groupes d'URL va accélérer la saisie des règles de filtrage. Chaque groupe contient une liste de masques d'URL et permet par exemple de représenter les besoins de chaque service au sein d'une entreprise.

La création des groupes d'URL est accessible via le menu **Analyse de contenu\Filtrage d'URL\Groupes d'URL**.

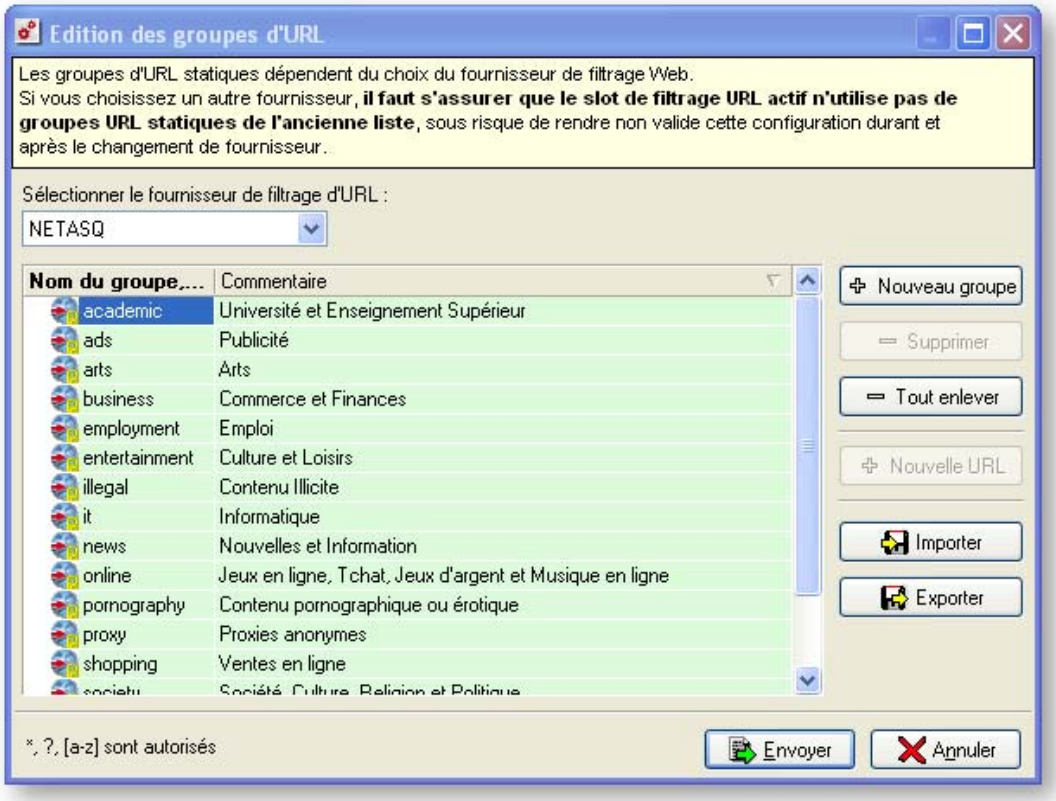


Figure 319 : Edition des groupes d'URL

Vous pouvez, au niveau de la configuration des groupes, effectuer les actions suivantes :

Nouveau groupe	Crée un nouveau groupe.
Supprimer	Supprime un groupe ou une URL existant. Sélectionnez la ligne à supprimer puis

	cliquez sur ce bouton.
Tout enlever	Permet de supprimer la totalité des groupes d'URL.
Nouvelle URL	Ajoute une URL à un groupe. Sélectionnez d'abord le groupe dans lequel vous voulez ajouter une URL puis cliquez sur ce bouton.
Importer	Permet d'importer une liste d'URL contenue dans un fichier.Txt. Vous devez d'abord créer un nouveau groupe et lui affecter un nom. Cliquez ensuite sur le bouton **Importer** et choisissez le fichier concerné. Les URL contenues dans le fichier seront alors intégrées au groupe. **AVERTISSEMENT** Si ce groupe contenait déjà des URL, celles-ci seront écrasées.
Exporter	Permet d'exporter une liste d'URL contenue dans un groupe. Choisissez le groupe dont vous voulez exporter la liste, puis cliquez sur le bouton **Exporter**. La liste sera enregistrée dans un fichier texte.
Sélectionner le fournisseur de filtrage d'URL	Il existe deux types de groupes d'URL : des groupes d'URL statiques (entrés manuellement par l'administrateur) et des groupes d'URL dynamiques (Cf. Filtrage d'URL dynamique ci-dessous). Le fournisseur demandé est le fournisseur des groupes d'URL dynamiques, par défaut NETASQ.

10.4.3.1. Format du fichier d'URL

Les fichiers texte pour l'import ou l'export d'URL doivent être formatés de la façon suivante :

URL1
URL2
URL3
...

Vous pouvez éditer vos listes dans un éditeur de texte et les importer ensuite au niveau du firewall.

La saisie d'un masque d'URL peut comporter la syntaxe suivante :

*****	Remplace une séquence de caractères quelconque. **Exemple** *.netasq.com/permet de définir le domaine Internet de la société NETASQ.
?	Remplace un caractère. **Exemple** ???.netasq.com est équivalent à www.netasq.com ou de ftp.netasq.com mais pas à www1.netasq.com.
[a-z]	Remplace un intervalle de caractère. **Exemple** ftp [1-2].netasq.com est équivalent à ftp1.netasq.com et à ftp2.netasq.com.

Un masque d'URL peut contenir une URL complète (**exemple** : www.netasq.com*) ou des mots-clés contenus dans l'URL (**exemple** : *mail*).

Il est aussi possible de filtrer des extensions de fichiers :

> **Exemple**
> le masque d'URL '*.exe' peut servir à filtrer les fichiers exécutables.

Vous pouvez afficher ou masquer le contenu de chaque groupe d'URL en cliquant sur les icônes "+" ou "-".

10.4.3.2. Filtrage d'URL dynamique

Le filtrage d'URL dynamique disponible sur les boîtiers UTM NETASQ vous permet de réaliser du filtrage d'URL au moyen de listes d'URL renseignées et actualisées dynamiquement grâce à la fonctionnalité d'**Active Update** (Cf. Partie 18 : Active Update).

Ces URL sont classées par catégories. Chacune des catégories contient une liste d'URL répertoriées que vous pouvez autoriser ou interdire.

Il est impossible de visualiser les URL contenues dans ces groupes car ils sont compressés et optimisés pour leur traitement par le firewall, elles ne sont donc pas modifiables. Un cadenas jaune  apparaît sur les groupes d'URL dynamique.

10.4.3.3. Fournisseur des listes d'URL

Suivant le type de service de maintenance souscrit (***Voir la politique tarifaire NETASQ en cours***), les listes d'URL disponibles sont mises à jour dynamiquement par des fournisseurs différents (parmi NETASQ ou OPTENET). Aujourd'hui, NETASQ a catégorisé deux types de fournisseurs : NETASQ en lui-même et OPTENET. Par défaut lorsqu'un service de maintenance "standard" est souscrit, ce sont les listes d'URL NETASQ qui sont proposées.

Lorsque vous souscrirez au service de maintenance incluant OPTENET, pour activer la fonctionnalité de filtrage d'URL sur les listes d'URL OPTENET, sélectionnez dans la liste des fournisseurs proposés : OPTENET. A la fermeture du menu des groupes d'URL, l'Appliance prendra en compte la demande et effectuera le téléchargement des nouvelles listes d'URL grâce au module **Active Update**.

> **AVERTISSEMENT**
> Lorsque vous modifiez le fournisseur des groupes d'URL, assurez-vous que le slot de filtrage d'URL actif ne sera pas affecté par la perte des anciens groupes d'URL. Si le slot actif est impacté, désactivez-le.

10.4.3.4. Requête d'ajout d'URL

NETASQ a mis en place sur son site Web, un formulaire vous permettant de demander l'ajout d'une URL qui serait inconnue dans les groupes d'URL dynamique. Ce formulaire est disponible à l'adresse suivante : **http://www.netasq.com/updates/url_fr.php**. NETASQ se réserve le droit de ne pas donner suite à cette requête (pour une raison de validité de la demande, l'adresse ne correspond à aucune catégorie déjà définie…).

NOTE
Il est toujours possible de rajouter manuellement cette adresse dans un groupe d'URL "statique" et de l'ajouter au filtrage.

10.4.4. Règles de filtrage

Référez-vous à la procédure suivante pour éditer un slot de filtrage d'URL :

1. Sélectionnez un slot dans la liste des slots de filtrage d'URL.
2. Cliquez sur le bouton **Editer** de la boite de dialogue contenant la liste des slots de filtrage d'URL.

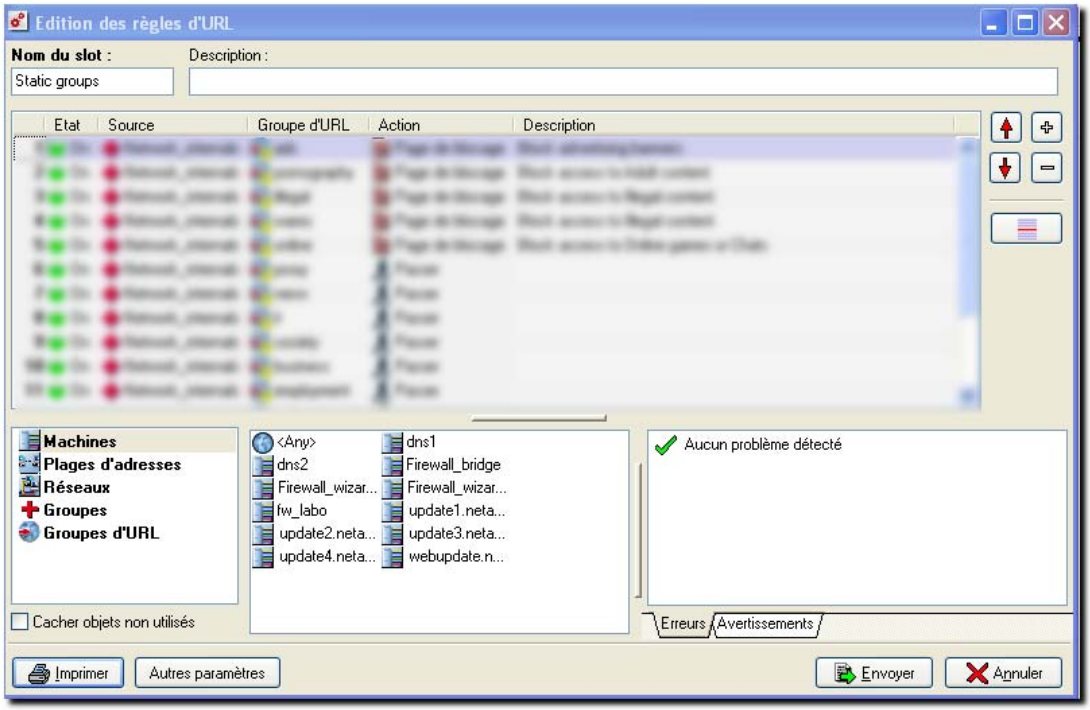


Figure 320 : Edition des règles d'URL

La fenêtre d'édition d'un slot de filtrage d'URL apparaît. Elle est composée de plusieurs parties :

- Une grille contenant les règles de filtrage.
- Un menu Drag'n Drop.
- Un analyseur de cohérence et de conformité des règles.
- Une zone d'actions possibles.

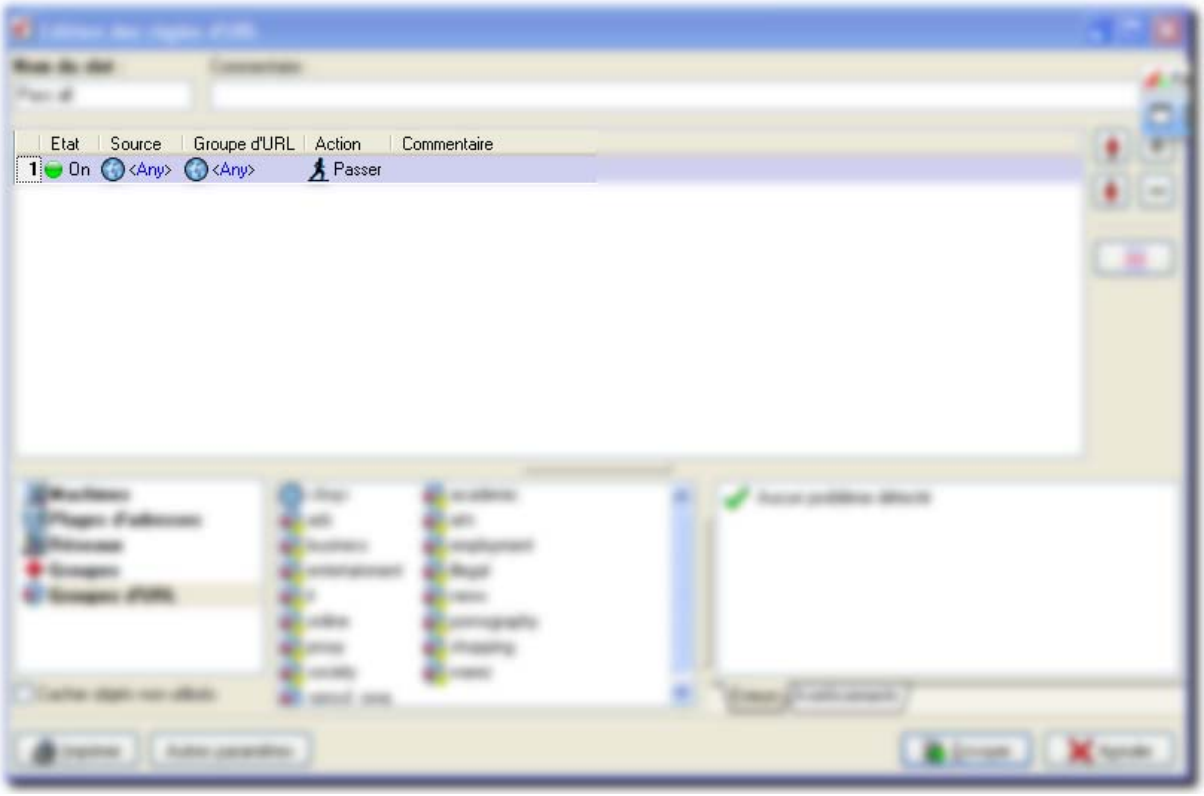


Figure 321 : Grille de règles

Cette zone de la boîte de dialogue contient une grille vous permettant de définir les règles de filtrage URL à appliquer. Pour éditer les règles, il suffit de double cliquer sur la zone à modifier.

ID Il s'agit du numéro de règle dans la politique. Il peut y avoir autant de numéros qu'il y a de règles dans une politique de filtrage d'URL. Ce champ ne peut être édité puisqu'il correspond à l'ordre de la règle.

Etat Etat de la règle :

ON, la règle sera active lorsque ce slot de filtrage sera actif.

OFF, la règle ne sera pas active lorsque ce slot sera actif. Lorsque la règle est à **Off**, la ligne est grisée afin de refléter la désactivation.

Le firewall va évaluer les règles une à une en partant du haut. Dés qu'il rencontre une règle qui correspond à la demande, il effectue l'action spécifiée et ne descend plus dans les règles. Si aucune règle n'est valable, le firewall utilisera le paramétrage par défaut. (Autorisation ou blocage selon la sélection ou non de l'option "Autoriser l'accès si aucune règle ne correspond" présente dans la fenêtre accessible via le bouton **Autres paramètres**).

Figure 322 : Options des règles de filtrage URL

Source Ce champ indique à quel utilisateur, machine, plage d'adresses, groupe d'utilisateurs, groupe ou réseau s'applique la règle. Lorsque la source est un utilisateur ou un groupe

	d'utilisateurs, cela nécessite d'avoir un groupe en complément pour obtenir l'objet user@host.
Groupe d'URL	Un nom de groupe d'URL précédemment créé. En double-cliquant sur le champ, une boîte de dialogue vous invite à choisir un groupe d'URL.

Figure 323 : Sélection de groupe d'URL

	Le groupe <Any> correspond à toutes les URL.
Action	Permet de spécifier le résultat de la règle, **Passer** pour autoriser le site, **Bloquer** pour interdire l'accès sans message de blocage, **Page de blocage** pour interdire l'accès et afficher la page de blocage.
Description	Commentaire associé à la règle.

Au niveau de la source, vous pouvez définir les utilisateurs ou groupes d'utilisateurs qui doivent s'authentifier pour accéder à certains sites (vous pouvez autoriser certains sites uniquement pour certains utilisateurs). L'utilisateur devant s'authentifier verra une page d'authentification apparaître dans son navigateur lorsqu'il essaiera de se connecter à un site Web.

10.4.4.1. Actions possibles

Nom du slot	Nom donné au fichier de configuration.
Commentaire	Commentaire indicatif associé au slot de filtrage
Insérer 	Insérer une ligne vierge après la ligne sélectionnée.
Effacer 	Supprimer la ligne sélectionnée.
	Placer la ligne sélectionnée avant la ligne directement au dessus.
	Placer la ligne sélectionnée après la ligne directement en dessous.
Insérer un séparateur 	Cette option permet d'insérer un séparateur au dessus de la ligne sélectionnée afin d'indiquer un commentaire sur une ligne de l'édition du filtrage. Pour définir un séparateur, il s'agit d'indiquer un commentaire et une couleur pour ce séparateur.
Imprimer	Impression de la configuration du filtrage d'URL.
Autres Paramètres	Permet de spécifier le fonctionnement du filtrage d'URL. Cochez l'option **Autoriser l'accès si aucune règle ne correspond** pour un fonctionnement de type "Liste noire d'URL".

REMARQUE
Le drag & Drop ne s'applique ici que sur les champs Source et Groupe d'URL puisqu'ils font appel à la base d'objets.

10.4.4.2. Affichage de la grille

L'affichage des données contenues dans la grille peut être défini suivant les préférences de l'administrateur parmi les options d'affichage : grandes icônes, petites icônes, détaillé ou en liste.

10.4.4.3. Options d'affichage

Deux options d'affichage des données de la grille du menu Drag'n Drop sont disponibles.

Cacher objets non utilisés

Comme son nom l'indique, cette option permet d'afficher dans la grille que les objets qui sont actuellement utilisés dans les règles de translation.

10.4.5. Analyseur de cohérence et de conformité des règles

De la même façon que pour l'édition des règles de filtrage et de translation, l'écran d'édition des règles de filtrage d'URL des firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.

Divisé en deux onglets, cet analyseur regroupe les erreurs de création de règles dans l'onglet **`Erreurs`** et les erreurs de cohérence dans les règles dans l'onglet **`Avertissements`**.

10.4.6. Envoi des modifications au firewall NETASQ

Cliquez sur le bouton **Envoyer** pour stocker le fichier sous le nom défini dans la zone de saisie "Nom".

Lors de l'envoi du slot au firewall NETASQ, le logiciel de configuration vérifie le nom que vous avez attribué au slot. En aucun cas le nom de fichier ne peut valoir "vide" ou avoir pour valeur un nom de slot existant. Si tel est le cas, le logiciel affiche une boîte de dialogue vous invitant à modifier le nom du slot ("Nom").

Après avoir cliqué **OK**, vous êtes libre de modifier le champ **Nom**, ainsi que tous les autres paramètres.

AVERTISSEMENT
La modification d'un slot de filtrage URL n'est pas dynamique. Les modifications ne seront effectives qu'à la prochaine activation du slot sur le firewall NETASQ.

PARTIE 11 : SERVICES

CHAPITRE 1. DHCP

11.1.1. Introduction

Le DHCP fournit des paramètres de configuration pour des machines Internet. Il est constitué de 2 parties : Un protocole pour la livraison de paramètres de configuration de machines spécifiques à partir d'un serveur DHCP et un mécanisme d'allocation d'adresses réseau à des machines.

DHCP est bâti sur le modèle client-serveur.

DEFINITION
Le terme **serveur** se réfère à une machine fournissant des paramètres d'initialisation au travers du DHCP, et le terme **client** se réfère à une machine qui utilise DHCP pour obtenir des paramètres de configuration telle qu'une adresse réseau.

11.1.2. Utilisation du service DHCP du firewall NETASQ

DEFINITION
Le service DHCP de NETASQ est un serveur qui peut vous permettre d'allouer des adresses réseau et de délivrer des paramètres de configuration à des machines configurées dynamiquement.

11.1.3. Fonctionnement

Pour utiliser le service DHCP, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu **Services\DHCP**.

L'écran de configuration du service DHCP se décompose en deux parties :

- A gauche un arbre présentant les diverses fonctionnalités du menu **DHCP**.
- A droite les options configurables.

11.1.4. Global

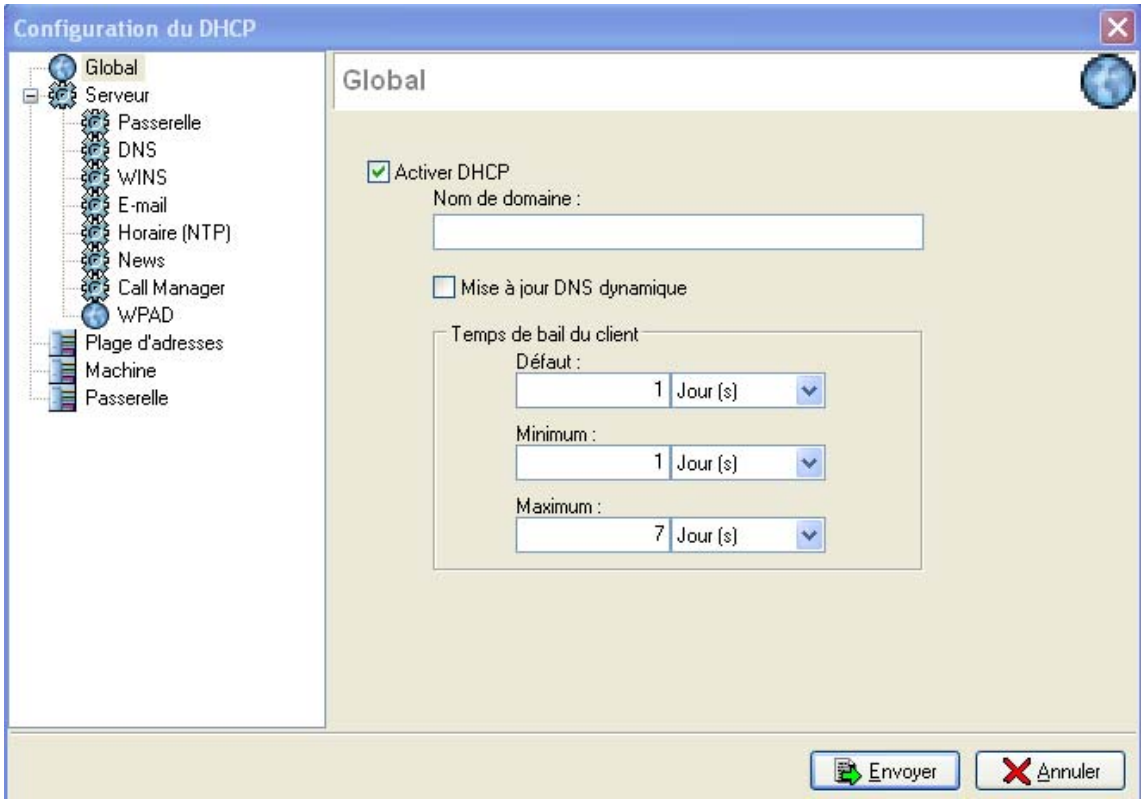


Figure 324 : Configuration du DHCP : Global

Nom de domaine	Nom de domaine utilisé pour la définition des utilisateurs.
Mise à jour DNS dynamique	Mise à jour dynamique du DNS. Lorsque les informations contenues par le serveur DHCP sont modifiées, le serveur DNS 1 (configuré dans le menu serveur DNS) est dynamiquement mis à jour).
Temps de bail du client	Temps pendant lequel les stations garderont la même adresse IP. Une valeur par défaut, au minimum et au maximum.

11.1.5. Serveur

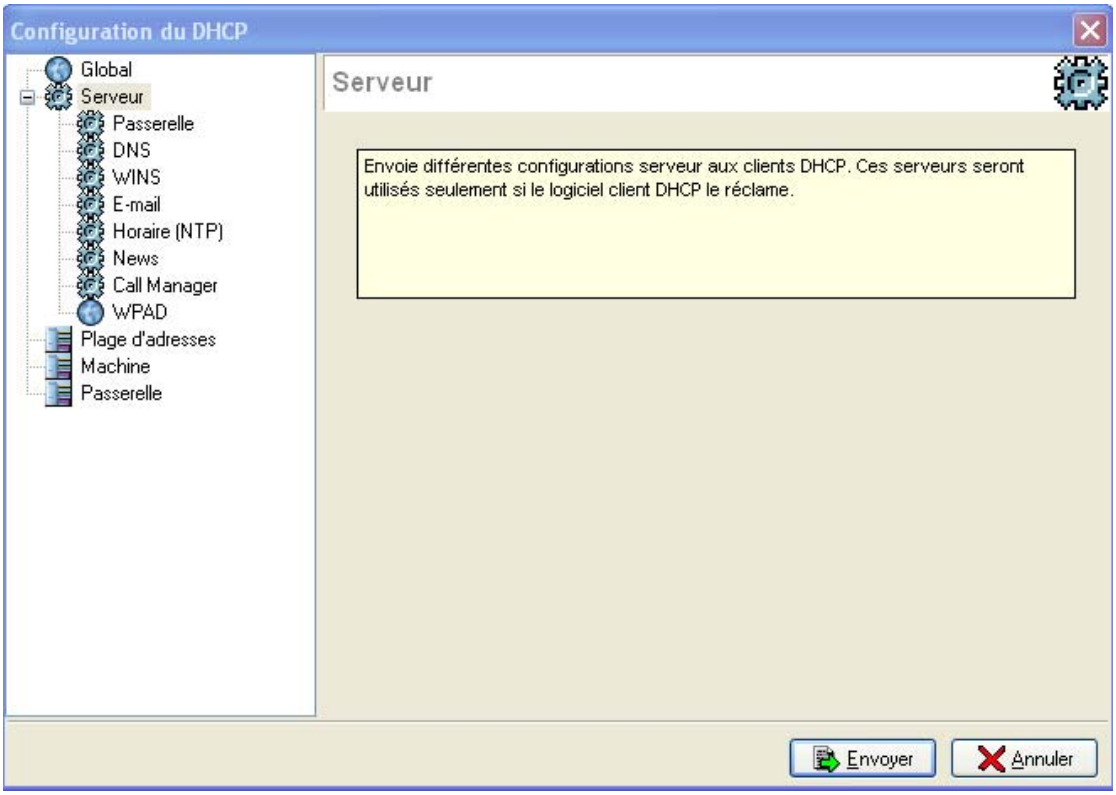


Figure 325 : Configuration du DHCP - Serveur

Ce menu est réservé à la configuration des adresses des différents serveurs : "Passerelle", "DNS", "WINS", "E-mail" (**SMTP** et **POP**), "Horaire" (**NTP**), News et Call Manager. Ces adresses seront automatiquement envoyées aux stations pour qu'elles puissent contacter les serveurs correspondants.

Deux modes d'attribution sont possibles :

- Par plage
- Par machine

Par plage vous spécifiez un groupe d'adresses destinées à être allouée aux utilisateurs. L'adresse allouée l'est alors pour temps déterminé dans la configuration globale. Dans la configuration **DHCP** par machine, l'adresse allouée par le service est toujours la même : celle indiquée dans le menu **Machine**. Il s'agit en réalité d'un adressage "statique" mais qui permet de "libérer" le poste client de sa configuration réseau.

11.1.5.1. Passerelle

La passerelle globale par défaut est la route par défaut utilisée si aucune autre n'a été spécifiée pour l'adresse du client ou du réseau.

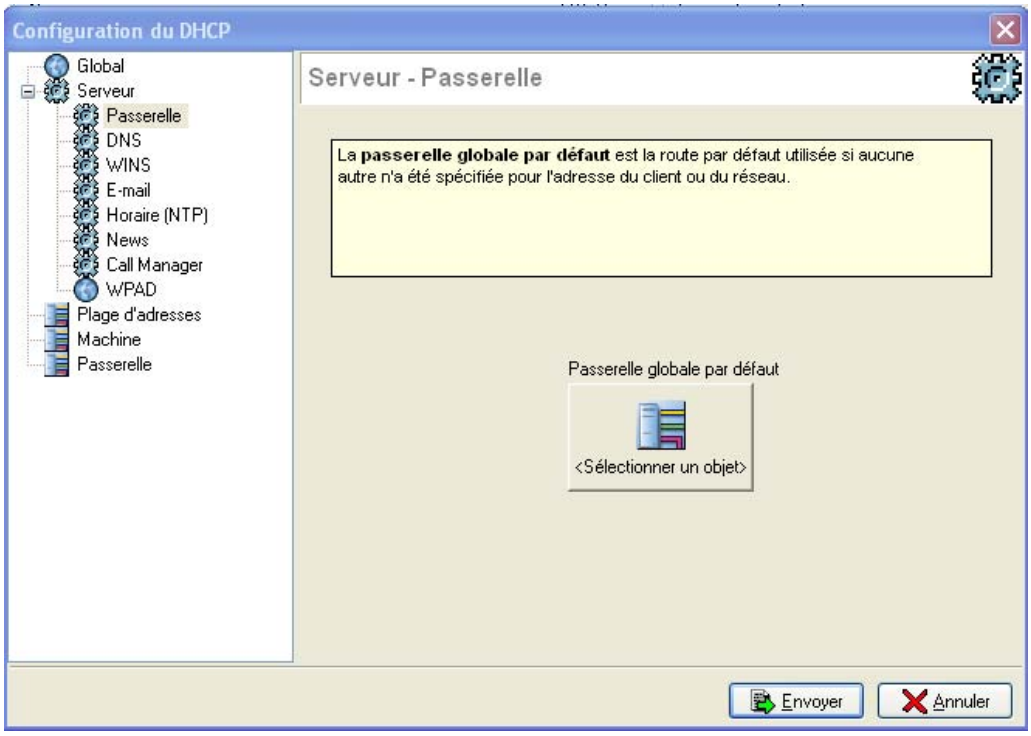


Figure 326 : Configuration du DHCP - Serveur - Passerelle

11.1.5.2. Rappel pour les Serveurs DNS

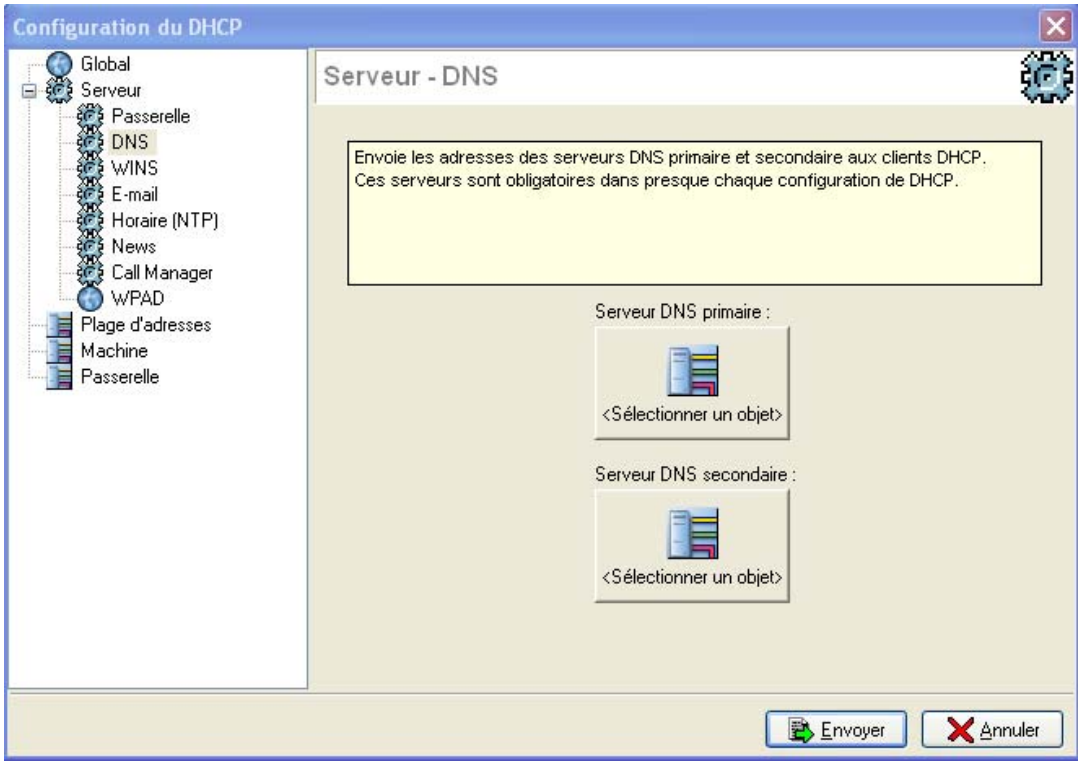


Figure 327 : Configuration du DHCP - Serveur - DNS

Si le firewall obtient l'adresse IP d'une des interfaces par DHCP et que l'option "Requêtes DNS" est configurée, alors il est possible de définir dans la configuration du service DHCP, les serveurs DNS obtenus

par le firewall auprès du fournisseur d'accès. Ces serveurs sont identifiés dans la configuration des objets par les machines "Firewall_<nom de l'interface>_dns1" et "Firewall_<nom de l'interface>_dns2".

11.1.5.3. WINS

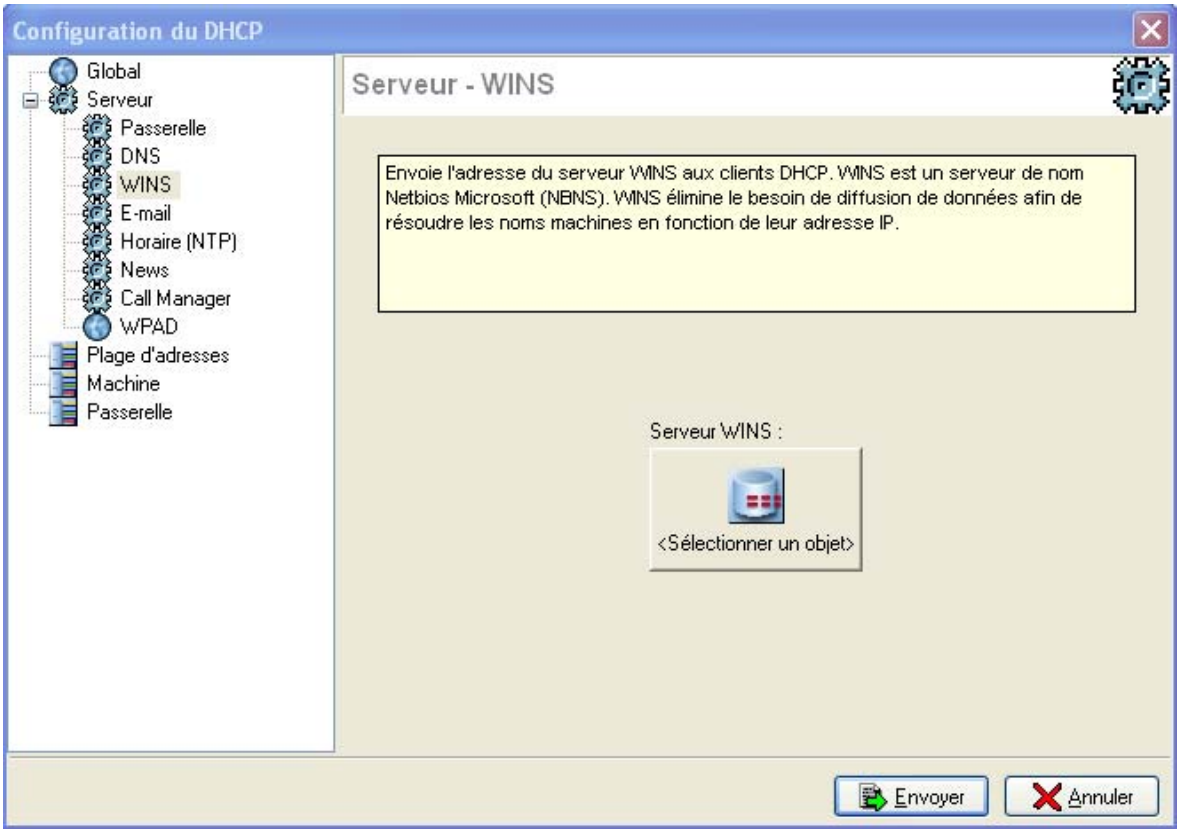


Figure 328 : Configuration du DHCP - Serveur - WINS

Définition : WINS *(Windows Internet Naming Service)*
Il s'agit d'un serveur de noms et services pour les machines qui utilisent NetBIOS.

Il s'agit d'une base de données à laquelle un client, voulant contacter un ordinateur peut envoyer des requêtes pour trouver l'adresse IP à joindre, plutôt que d'envoyer une requête globale (broadcaste) pour demander l'adresse à contacter. Le système réduit alors le trafic sur le réseau.

11.1.5.4. E-mail

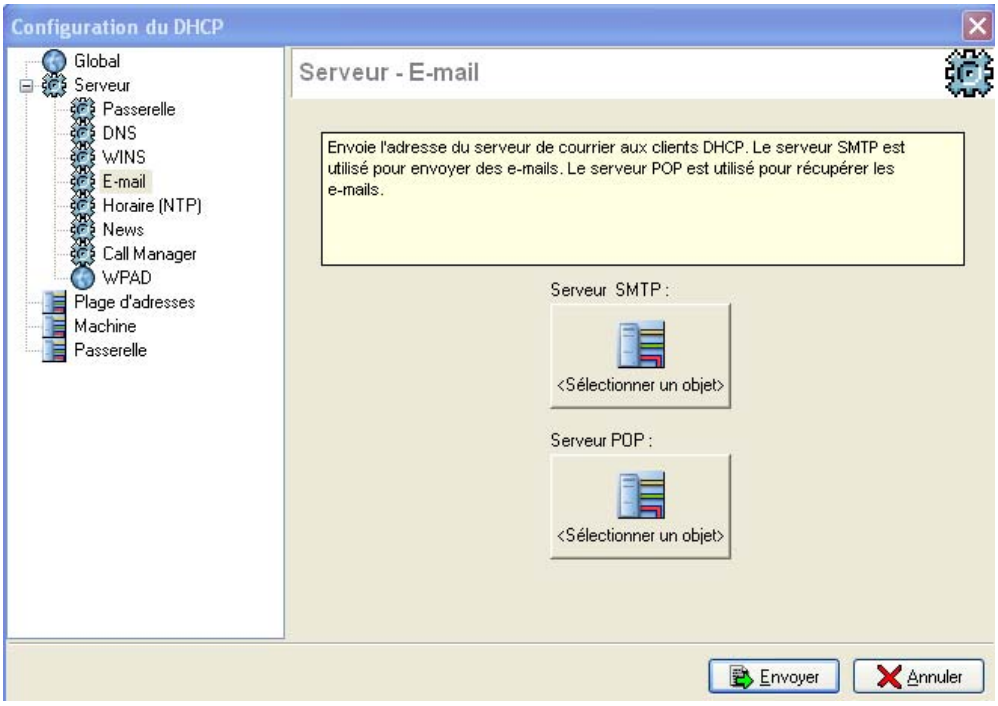


Figure 329 : Configuration du DHCP - Serveur - E-mail

Cet écran permet d'envoyer l'adresse du serveur de courrier aux clients DHCP. Le serveur SMTP est utilisé pour envoyer des e-mails alors que le serveur POP est utilisé pour en recevoir. Un clic sur les boutons permet de sélectionner un objet.

11.1.5.5. Horaire (NTP)

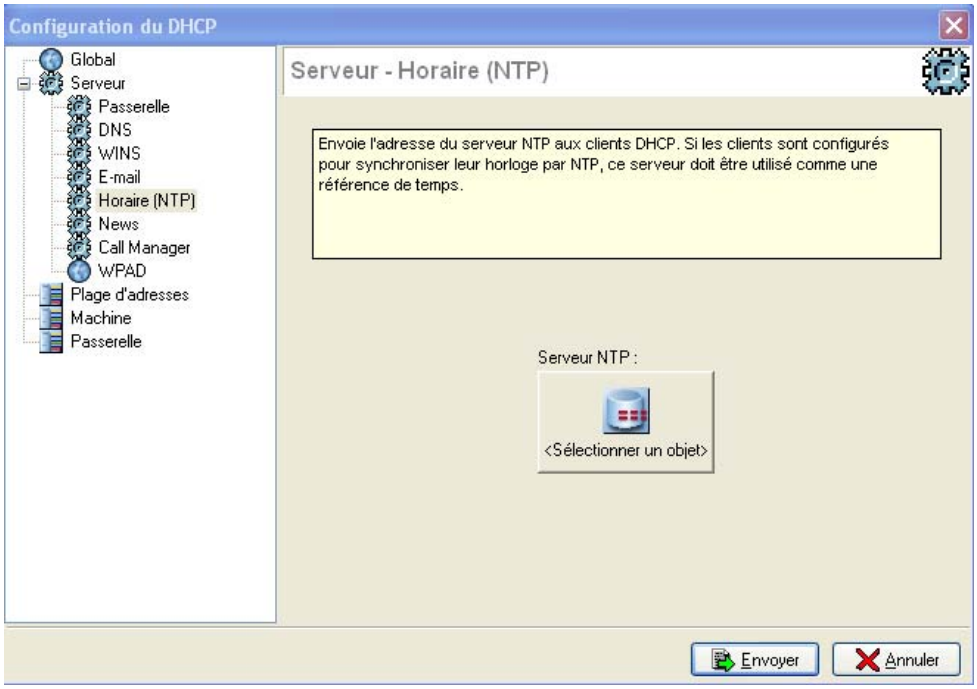


Figure 330 : Configuration du DHCP - Serveur - Horaire (NTP)

Cet écran permet d'envoyer l'adresse du serveur NTP aux clients DHCP. Si les clients sont configurés pour synchroniser leur horloge NTP, ce serveur doit être utilisé comme une référence de temps.

11.1.5.6. News

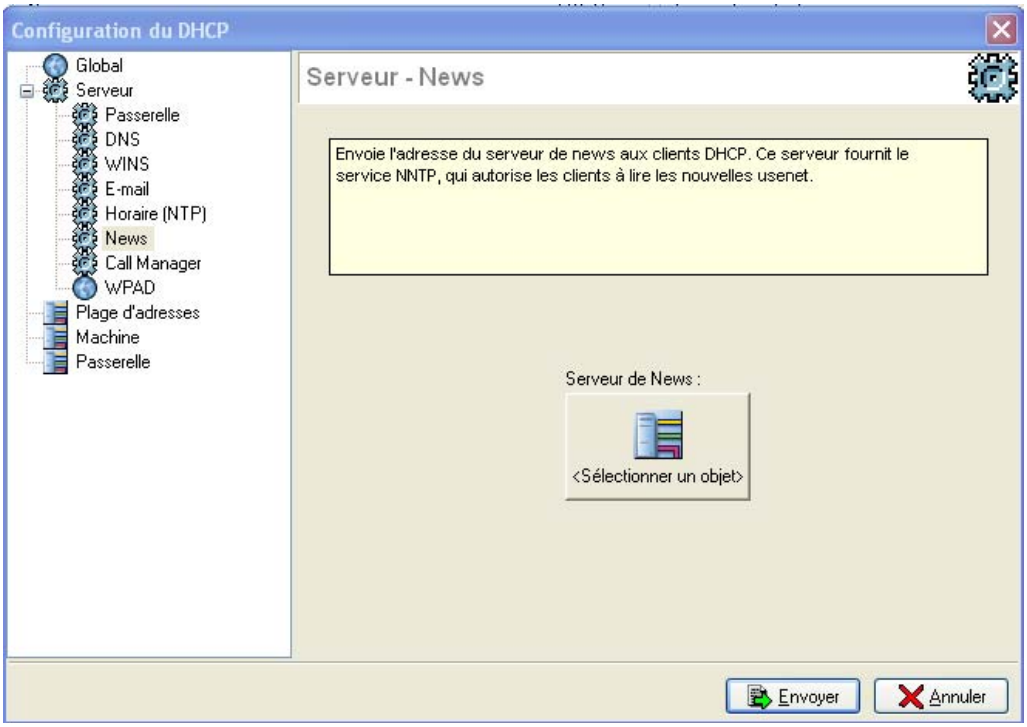


Figure 331 : Configuration du DHCP - Serveur - News

Cet écran permet d'envoyer l'adresse du serveur de news aux clients DHCP. Ce serveur fournit le service NNTP, qui autorise les clients à lire les nouvelles Usenet.

11.1.5.7. Call Manager

AVERTISSEMENTS

1) Deux plages ne peuvent se chevaucher. Une plage d'adresses appartient à un unique bridge/interface. Une machine ne peut être définie dans une plage. La passerelle définie pour un réseau appartient à ce réseau.
2) Seuls les objets de type "plage d'adresses" sont autorisés dans cette configuration.

La grille affiche le réseau, le masque et la passerelle.

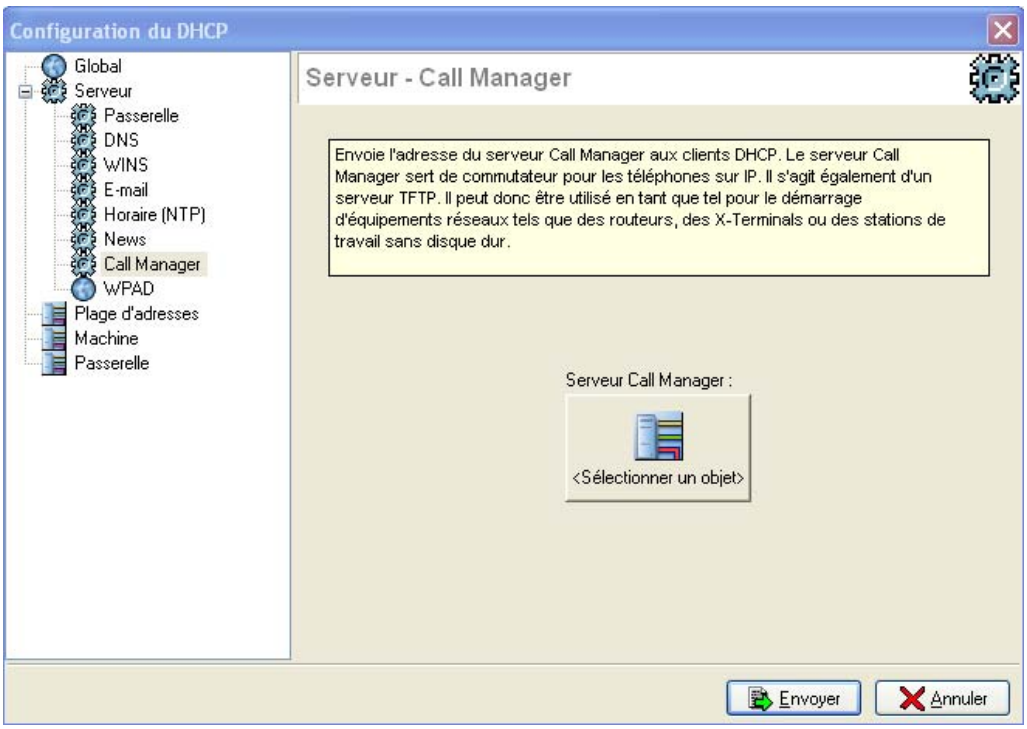


Figure 332 : Serveur-Call Manager

11.1.5.8. WPAD

DEFINITION

WPAD (Web Proxy Auto-Discovery), est un protocole qui permet d'effectuer automatiquement le paramétrage d'accès à l'Internet de son navigateur.

En sélectionnant le menu **WPAD**, l'écran suivant s'affiche :

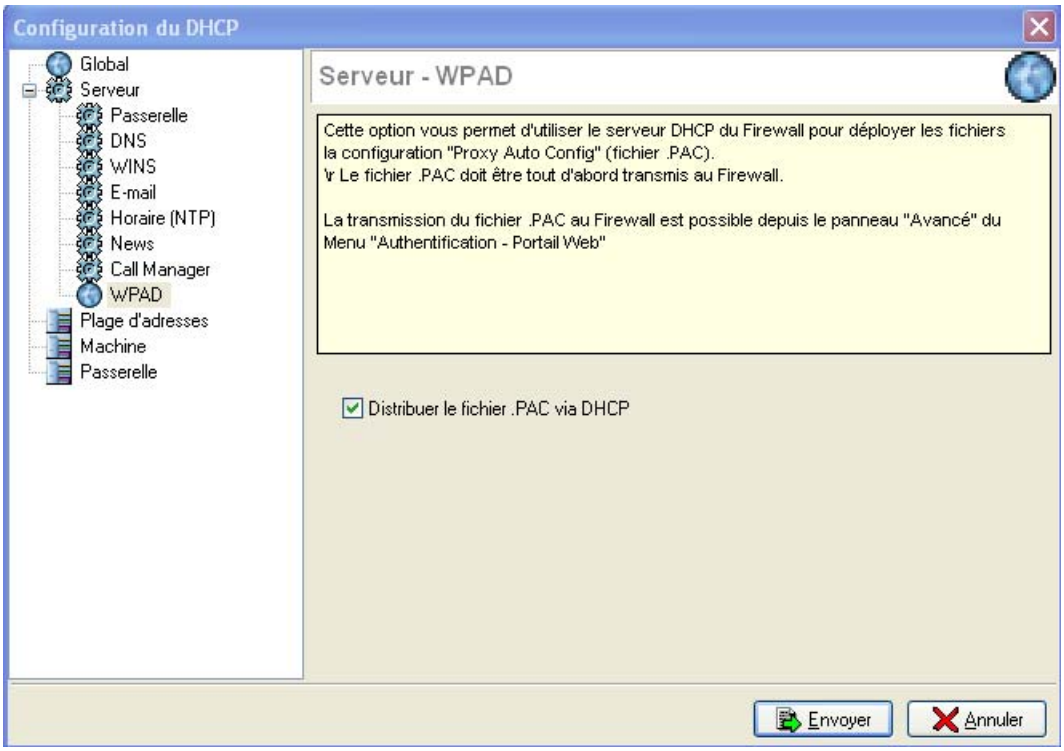


Figure 333 : Configuration du DHCP - Serveur- WPAD

L'option **Distribuer le fichier .PAC via DHCP** permet au serveur de distribuer aux clients DHCP qui demandent une adresse, la configuration du proxy à travers le fichier PAC.

Le fichier .PAC est transmis dans la réponse DHCP (champ option 252 :WPAD-URL).

En cochant cette option, l'utilisateur sera informé qu'il devra activer le partage sur les interfaces internes et/ou externes dans l'écran d'authentification. Cf. Partie 12 : Authentification.

11.1.6. Machine

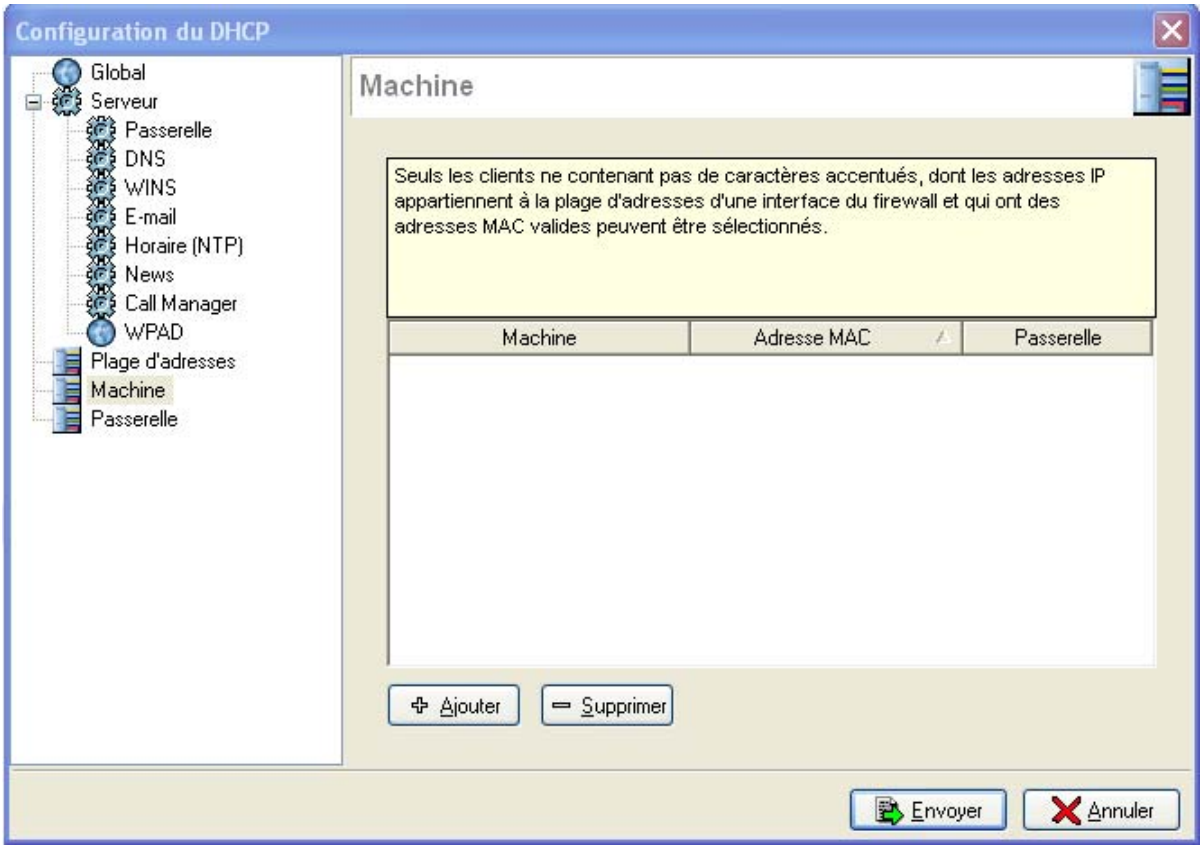


Figure 334 : Configuration du DHCP - Machine

Dans le menu **Machine**, il est possible de définir une adresse IP et une passerelle par défaut spécifique pour un poste client possédant une adresse MAC donnée. Cette configuration se rapproche d'un adressage statique mais rien n'est indiqué sur le poste client ainsi la gestion des adresses allouées et de la configuration des postes clients est simplifiée.

La grille affiche la machine, l'adresse MAC et la passerelle.

11.1.7. Passerelle

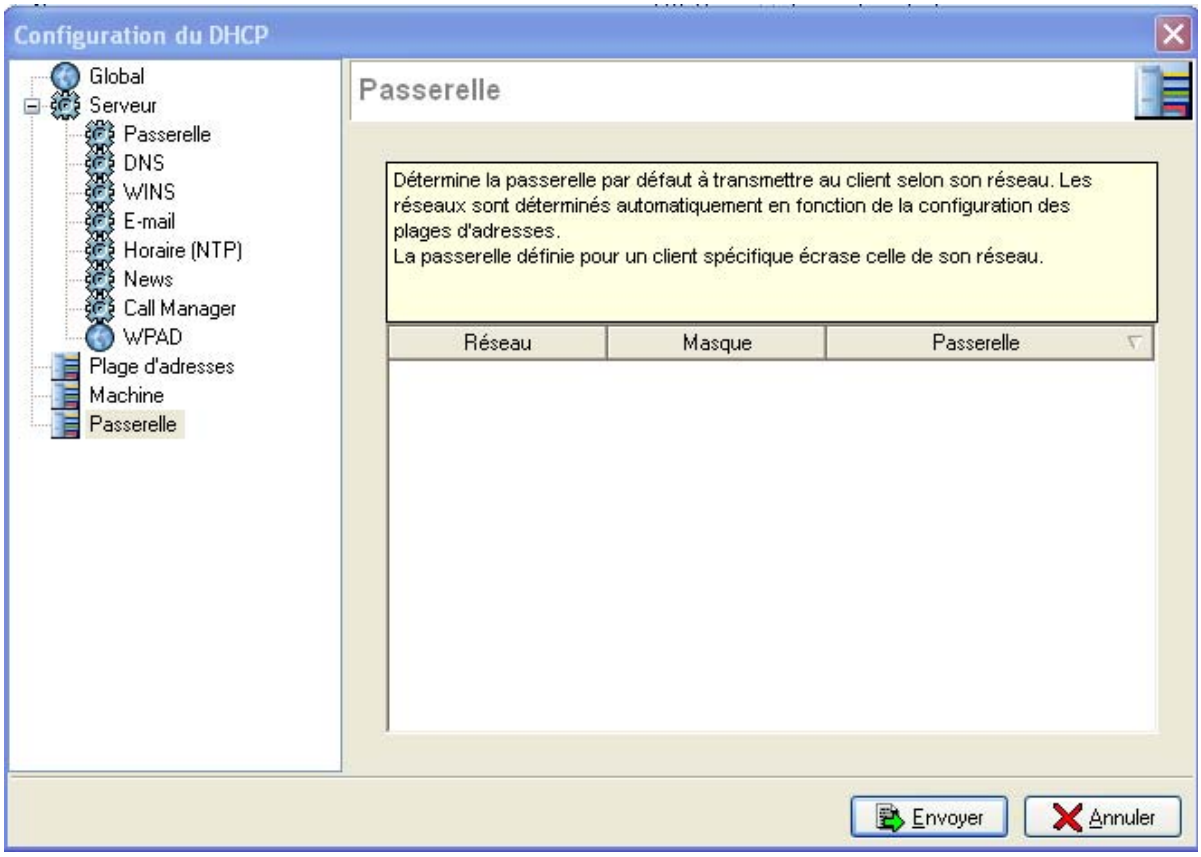


Figure 335 : Configuration du DHCP - Passerelle

Cet écran détermine la passerelle par défaut à transmettre au client selon son réseau. Les réseaux sont déterminés automatiquement en fonction de la configuration des plages d'adresses. La passerelle définie pour un client spécifique écrase celle de son réseau.

CHAPITRE 2. DNS

11.2.1. Introduction

Ici nous voulons rappeler une partie du fonctionnement du DNS.

Le fonctionnement du DNS est de type client-serveur. La partie client s'appelle le *resolver*, c'est une bibliothèque. La partie serveur s'appelle le *name server*.

Il existe trois types de name server :

- **Primaire** : possède les tables à jour d'un domaine.
- **Secondaire** : possède les tables à jour provenant d'un autre serveur.
- **Cache** : possède des tables construites à partir des informations traitées.

11.2.2. Utilisation possible du service DNS du produit UTM NETASQ

Le service DNS de NETASQ est un cache. Lorsqu'une requête DNS est envoyée au travers du firewall, celui-ci garde en mémoire (dans le cache **DNS**) la réponse et cela pour garantir un meilleur temps de réponse lors d'une prochaine requête DNS similaire. De plus, le firewall intercepte et reçoit la requête assurant ainsi un niveau de sécurité optimum.

11.2.3. Fonctionnement

Pour utiliser le service DNS, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu **Services\DNS**.

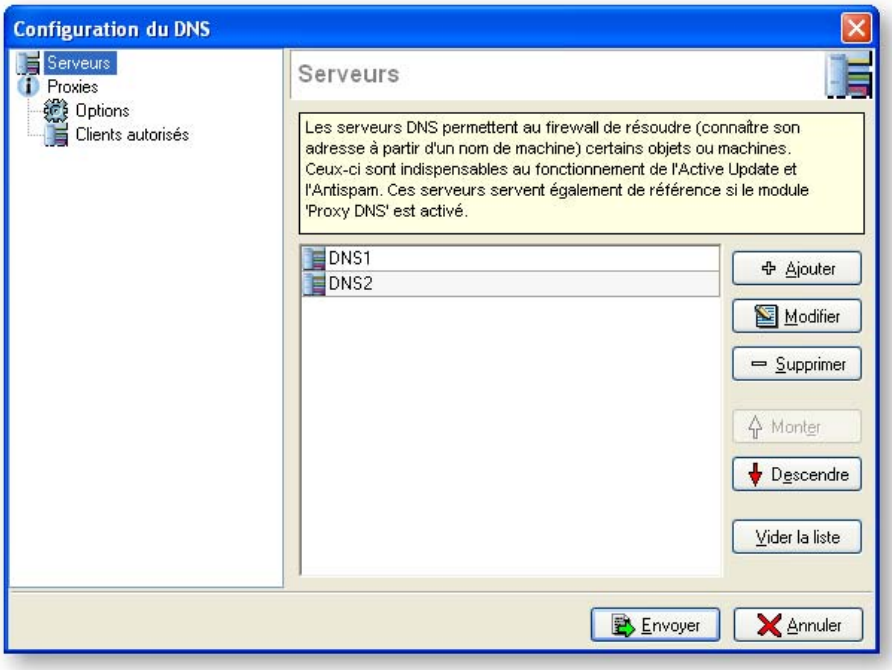


Figure 336 : Configuration du DNS - Serveurs

L'écran de configuration du service **DNS** se décompose en deux parties :

- A gauche, un arbre présentant les diverses fonctionnalités du menu **DNS**
- A droite, les options configurables

Le service **DNS** proposé par le firewall NETASQ est un cache **DNS**. Celui-ci vise à garder en mémoire des réponses **DNS** contenant les correspondances entre noms de domaine et adresses IP.

11.2.4. Serveurs

Les serveurs permettent au firewall de résoudre (connaître l'adresse IP d'une machine à partir de son nom) certains objets ou machines. Ceux-ci sont indispensables au fonctionnement de l'Active Update et l'Antispam. Ces serveurs serviront également de référence si le proxy DNS est activé.
Lorsque des serveurs sont configurés, les modules d'Antispam, d'Antivirus et de résolution des objets effectuent leur requête vers ces serveurs sans que le proxy DNS du firewall (cache DNS) soit nécessairement activé. Dans ce cas, si un utilisateur envoie une requête DNS sur un serveur non configuré, la requête est transmise par le firewall au dit serveur et un utilisateur envoyant une requête DNS au firewall voit sa requête refusée.

Si l'option **Activer le DNS** du menu **Proxies** est activée, les modules d'Antispam, d'Antivirus et de résolution des objets effectuent leur requête vers les serveurs configurés sans toutefois faire appel au cache DNS. Si un utilisateur envoie une requête DNS sur un serveur non configuré, la requête est transmise par firewall au dit serveur. Et lorsqu'un utilisateur envoie une requête DNS au firewall, sa requête est alors traitée par le cache DNS.

Enfin si le proxy DNS est activé et le mode transparent configuré (Voir la configuration du mode transparent ci-dessous), les modules d'Antispam, d'Antivirus et de résolution des objets effectuent leur requête vers les serveurs configurés en utilisant le cache DNS. Si un utilisateur envoie une requête DNS sur un serveur non configuré, la requête est redirigée de manière transparente par le firewall vers les serveurs configurés dans ce module. Et lorsqu'un utilisateur envoie une requête DNS au firewall, sa requête est alors traitée par le cache DNS.

11.2.4.1. Barre d'actions

Ajouter	Ajout d'un serveur DNS. La base d'objets s'affiche afin de sélectionner parmi Machines, Plages d'adresses et Groupes.
Modifier	Modifier le serveur DNS sélectionné.
Supprimer	Supprimer le serveur DNS sélectionné.
Monter	Placer la ligne sélectionnée avant la ligne directement au dessus.
Descendre	Placer la ligne sélectionnée après la ligne directement en dessous.
Vider la liste	Suppression de la liste complète des serveurs.

11.2.5. Proxies

Le module de DNS offre des fonctions de proxy transparent et de cache. Une fois activé, les requêtes DNS, provenant de clients autorisés et passant au travers du firewall seront résolues par ce dernier en utilisant les serveurs configurés.

En mode transparent toutes les requêtes sont interceptées, même si celles-ci sont à destination d'autres serveurs DNS que le firewall. Les réponses sont gardées un certain temps en mémoire pour éviter de retransmettre des demandes déjà connues.

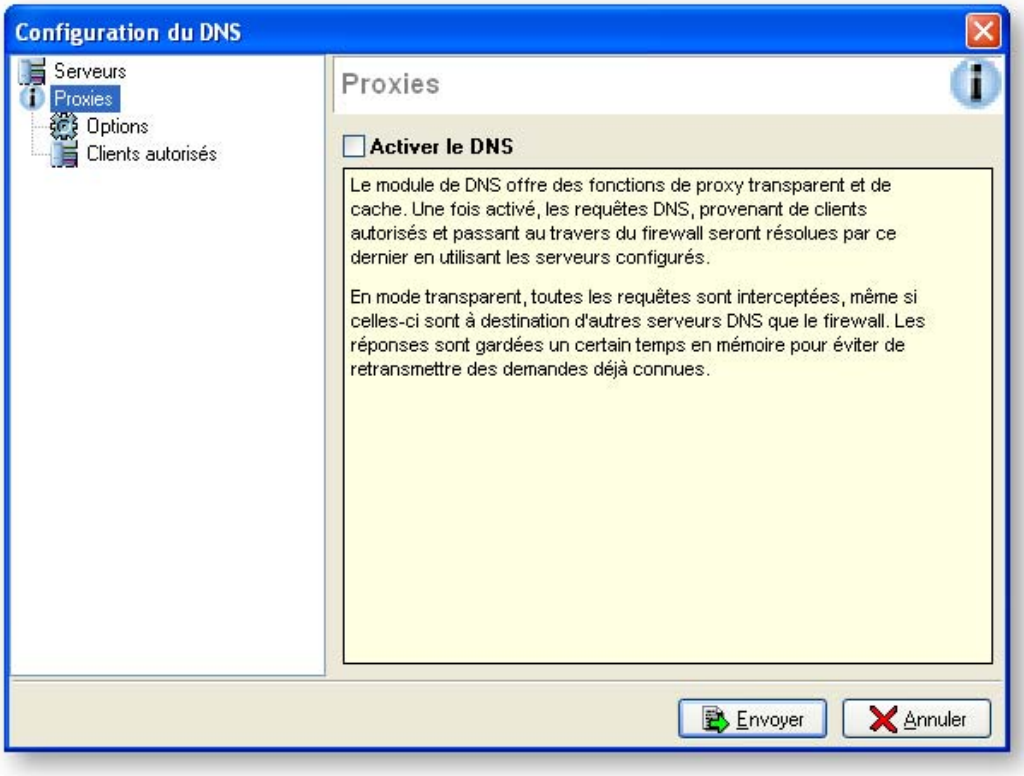


Figure 337 : Configuration du DNS - Proxies

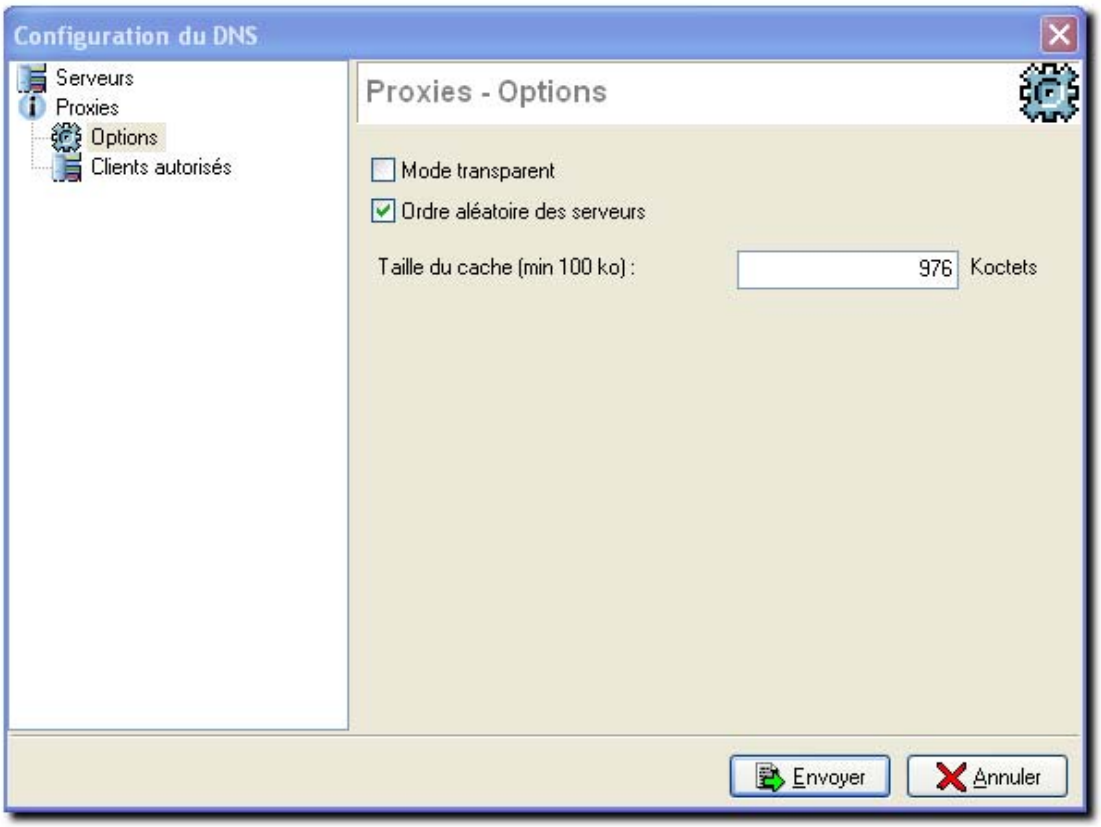


Figure 338 : Configuration du DNS - Proxies - Options

11.2.5.1. Options

Mode transparent	Comme son nom l'indique cette option vise à rendre transparent le service DNS du firewall NETASQ. Ainsi lorsque cette option est activée la redirection des flux DNS vers le cache DNS est invisible aux utilisateurs qui pensent accéder à leur serveur DNS.
Ordre aléatoire des serveurs	En cochant cette option, le firewall va sélectionner au hasard le serveur DNS dans la liste.
Taille du cache (min 100 ko)	Taille allouée au cache DNS.

11.2.5.2. Clients autorisés

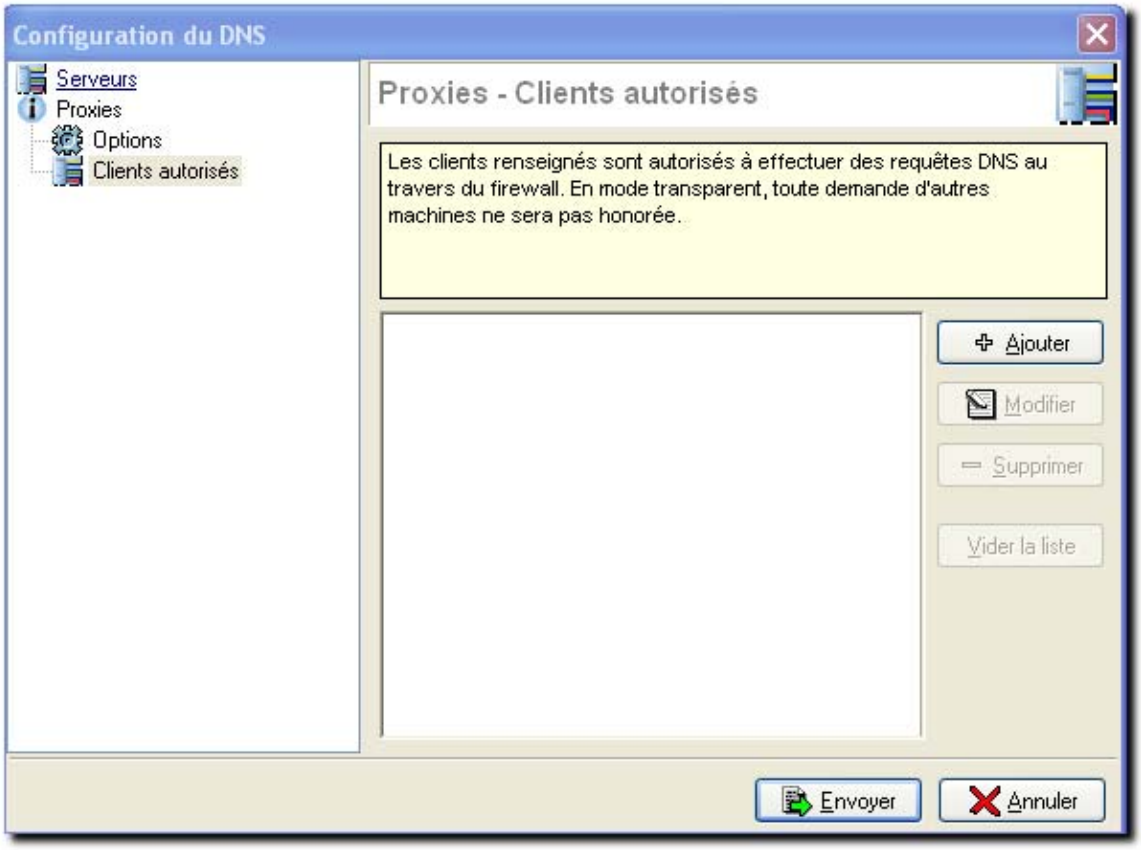


Figure 339 : Configuration du DNS - Clients autorisés

Clients autorisés : Liste des clients autorisés à émettre une requête DNS. Cette liste peut contenir des réseaux. En mode transparent, toute demande d'autres machines ne sera pas honorée.

CHAPITRE 3. NTP

11.3.1. Introduction

Ce protocole permet la synchronisation des horloges réseau de clients et serveurs répartis. NTP est construit sur le protocole UDP, ce qui en fait un protocole du type non connecté. C'est en réalité une version évoluée des mécanismes Time Protocol et ICMP Timestamp message et un remplaçant tout à fait approprié. NTP fournit des mécanismes de synchronisation du temps avec une précision de l'ordre de la nanoseconde, tout en préservant une date non-ambiguë. Ce protocole inclut la possibilité de spécifier des informations sur la précision et l'erreur estimée de l'horloge locale ainsi que des indications sur l'horloge de référence auprès de laquelle elle peut se synchroniser.

11.3.2. Utilisation possible du service NTP du firewall NETASQ

Le protocole NTP se base sur une structure arborescente dans laquelle le firewall n'est qu'un client.

11.3.3. Fonctionnement

Pour utiliser le service NTP, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu **Services\NTP**.

> **REMARQUE**
> L'état de la case à cocher d'activation du NTP grise ou dégrise l'ensemble des autres éléments de l'écran.

L'écran de configuration du service NTP se décompose en deux parties :

- L'onglet **Serveurs** : liste des serveurs NTP publics ou privés.
- L'onglet **Clés** : liste des clés d'authentification.

> **REMARQUE**
> Une modification de la configuration entraîne l'ajout d'une étoile au titre de l'écran afin de spécifier à l'utilisateur que les données ont probablement été modifiées.

11.3.4. Serveurs

Cet écran permet d'ajouter, modifier ou supprimer des serveurs NTP et de leur affecter éventuellement une clé.

Il se décompose en 3 colonnes : le nom de l'objet, le type (machine, plage d'adresses et groupe) et la clé éventuellement associée (avec, pour indication, "aucun" ou un chiffre allant de 1 à 15 ou encore une indication d'invalidité si la clé associée n'existe plus).

Il est possible à partir de cet écran de sélectionner une clé d'authentification ou de la supprimer en sélectionnant dans la liste déroulante "Aucun".

Il n'est pas possible d'avoir la même clé pour deux entrées du tableau.

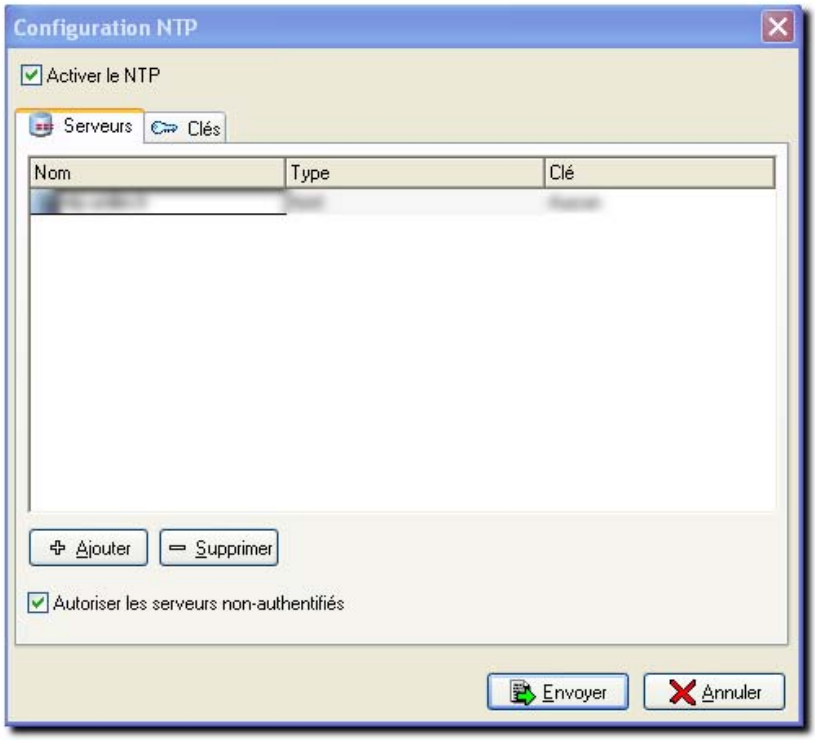


Figure 340 : Configuration du NTP - Serveurs

Serveurs	Liste des serveurs NTP publics ou privés auxquels le firewall pourra se connecter pour se synchroniser.
Ajouter	Permet d'accéder à la base d'objets afin de sélectionner le/les serveur(s).
Supprimer	Permet de supprimer un serveur après l'avoir sélectionné dans la grille.
Autoriser les serveurs non-authentifiés	Cette option vous permet d'autoriser l'utilisation de serveurs ne demandant aucune authentification (donc, pas de clé associée).

11.3.5. Clés

Cet onglet vous permet de configurer des clés pour l'authentification auprès de serveurs NTP. Cette clé est apparente si vous vous connectez avec les droits de modifications. Sinon elle est cachée.

Les clés sont définies par un numéro unique allant de 1 à 15. (La tentative d'ajout d'une seizième clé entraîne un message d'erreur).

Il est possible de modifier directement dans le tableau une clé. Un message d'erreur s'affiche si la clé est plus longue que 8 caractères. Il est possible également de modifier le numéro de la clé. Dans ce cas, seuls les numéros non encore attribué seront proposés.

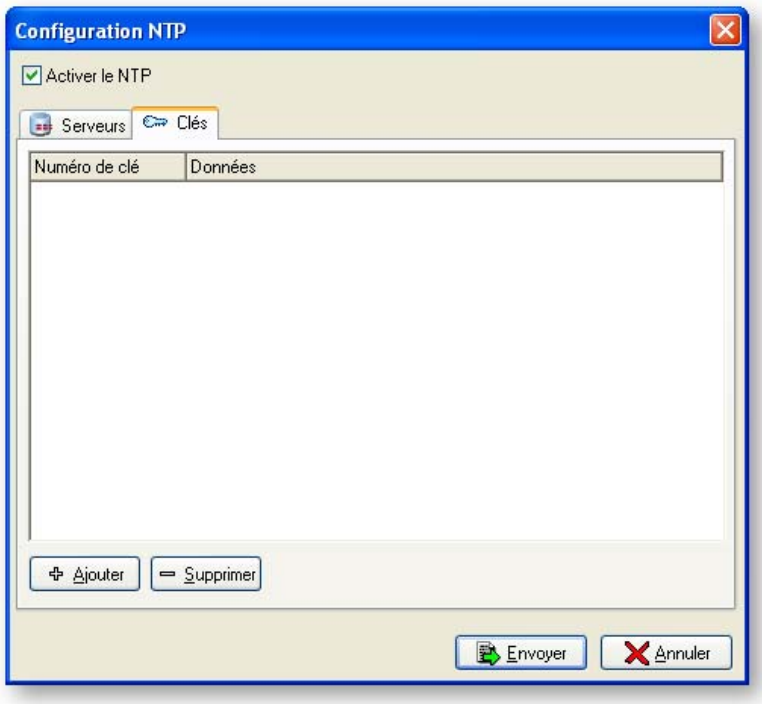


Figure 341 : Configuration du NTP - Clés

Ajouter Lorsque vous cliquez sur ce bouton, l'écran ci-dessous s'affiche :

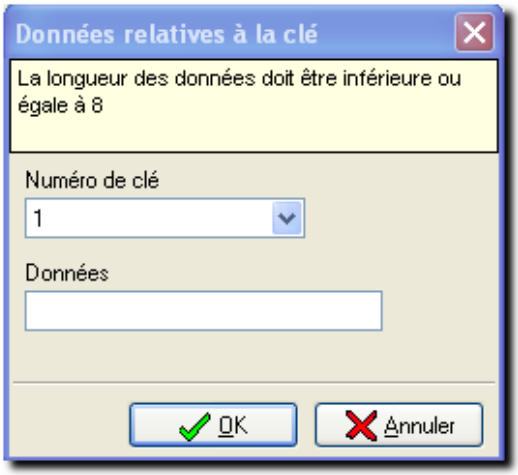


Figure 342 : Données relatives à la clé

Indiquez un n° pour la clé puis indiquez une valeur dans le champ "Données".

REMARQUE
La longueur des données doit être inférieure ou égale à 8.

Supprimer Permet de supprimer une clé après l'avoir sélectionnée dans la grille.

11.3.5.1. Envoi

En cliquant sur le bouton **Envoyer**, les données sont vérifiées et envoyées.
L'étape de vérification permet de voir si les clés associées à chaque serveur existent réellement. Si ce n'est pas le cas, un message d'erreur s'affiche et l'envoi est annulé.

Si l'option "Autoriser les serveurs non authentifiés" n'est pas cochée, un message d'erreur s'affiche s'il existe des serveurs sans clé associée.

D'autre part, il n'est pas possible d'envoyer une configuration NTP activée sans indication de serveurs.

Si la procédure de vérification s'est correctement déroulée, dans ce cas, l'envoi est possible.

CHAPITRE 4. SNMP

11.4.1. Introduction

La gestion du réseau est assurée par des applications qui supervisent et contrôlent l'état des différents éléments d'un réseau. Ces éléments peuvent être des stations de travail, des serveurs, des passerelles qui contiennent les agents de gestion requis par ces applications de gestion du réseau. Les agents remontent des informations de gestion qui sont exploitées par les applications. Le SNMP est utilisé pour la communication entre les agents et les applications.

SNMP utilise le protocole UDP par conséquent les paquets échangés entre la station de gestion (client) et l'agent (serveur) présent sur l'élément de réseau sont des datagrammes sans garantie d'arrivée.

Il existe deux types d'échanges entre le client et le serveur :

- Soit le client envoie une requête et le serveur répond.
- Soit c'est le serveur qui prend l'initiative en envoyant des messages (traps) à la station de gestion pour lui indiquer qu'un événement important est survenu.

L'agent (serveur) écoute sur le port UDP 161 et la station de gestion écoute les traps (alarmes) sur le port 162.

11.4.2. Utilisation du service SNMP du firewall NETASQ

Le service SNMP du firewall NETASQ est un serveur qui peut vous permettre de superviser l'état du firewall. Le firewall peut donc être intégré dans une solution de gestion de réseau tel Tivoli ou HP OpenView.

11.4.3. Fonctionnement

➲ Pour utiliser le service SNMP, celui-ci doit être activé. L'activation du service est réalisée au niveau du menu **Services\SNMP**.

L'écran de configuration du service SNMP se décompose en deux parties :

- L'onglet **Global** : cet écran vous permet de spécifier la version du protocole SNMP utilisée et les informations relatives à chaque version.
- L'onglet **Evénements** : dans cet onglet vous spécifiez vers quelles machines doivent être envoyées les informations remontées par le firewall.
- L'onglet Alarmes (Traps) : permet de définir le type (Système/ASQ) d'alarmes supervisées en fonction de leur sévérité.

11.4.4. Global

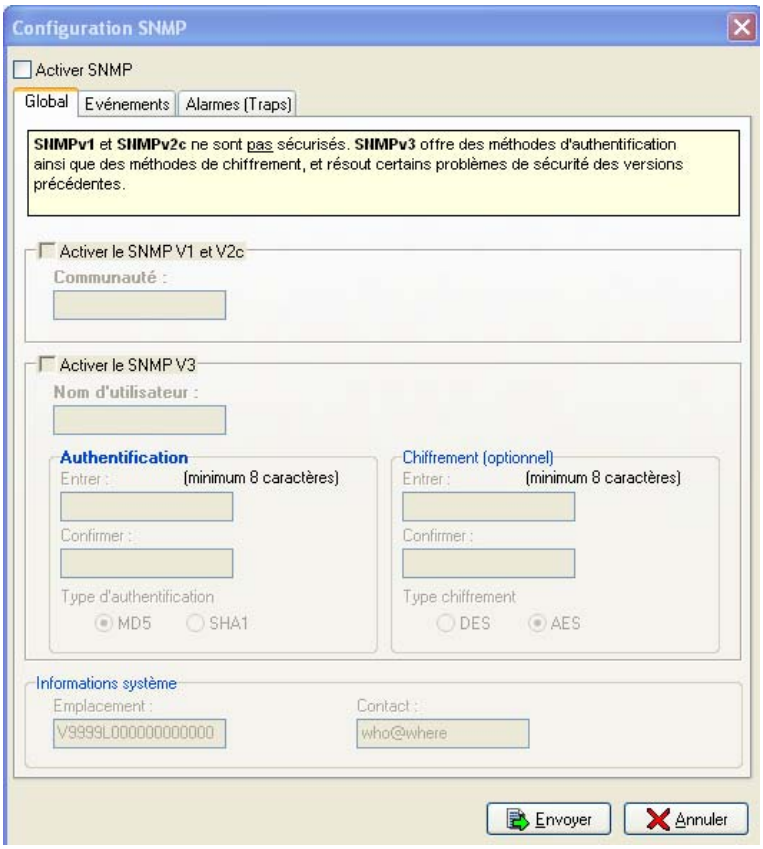


Figure 343 : Configuration du SNMP - Global

Le protocole SNMP fonctionne selon ce qu'on pourrait appeler deux "modes". Soit une station de gestion vient chercher les informations auprès de l'élément du réseau, soit c'est l'élément de réseau qui remonte ces informations de gestion auprès d'une station qui lui est spécifiée.
Dans cet onglet, vous configurez les informations nécessaires à l'établissement d'une connexion entre le firewall et la station de gestion lorsque celle-ci cherche à obtenir des données de gestion.

AVERTISSEMENT
SNMPv1 et SNMPv2c ne sont pas sécurisés.

11.4.4.1. Activer le SNMP V1 et V2c

Les premières versions du protocole **SNMP** ne sont pas sécurisées. Le seul champ nécessaire est le nom de la communauté. Par défaut la RFC propose le nom "public".

AVERTISSEMENT
Nous vous conseillons toutefois de ne pas l'utiliser pour des raisons de sécurité.

Si vous souhaitez indiquer plusieurs communautés, séparez-les par des virgules comme montré ci-dessous :

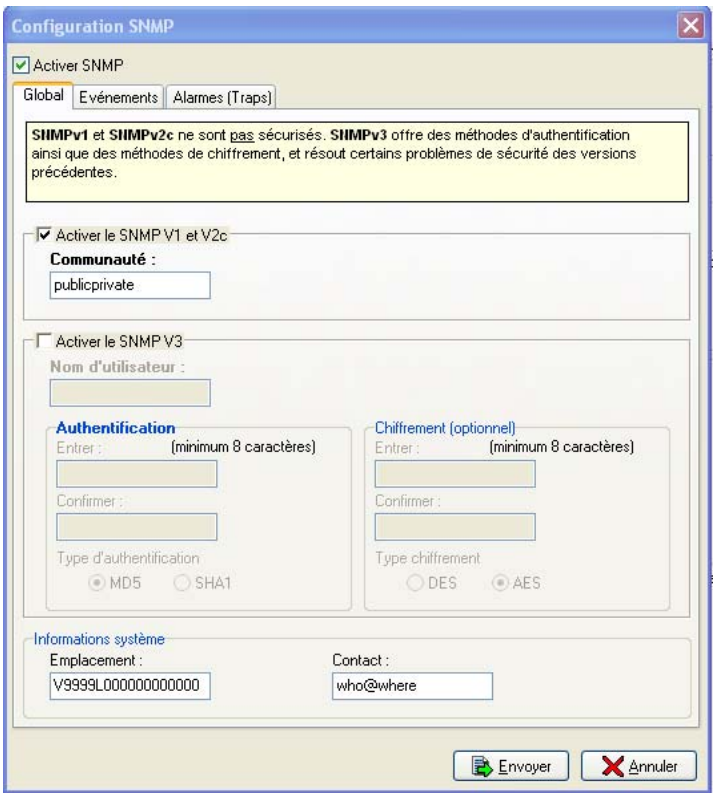


Figure 344 : Configuration du SNMP - Global

11.4.4.2. Activer le SNMP V3

Depuis décembre 2002, un nouveau standard existe pour le protocole SNMP, il apporte une avancée significative en matière de sécurité. La configuration requiert les paramètres suivants :

SNMPv3 offre des méthodes d'authentification ainsi que des méthodes de chiffrement, et résout certains problèmes de sécurité des versions précédentes.

Nom d'utilisateur	Nom d'utilisateur utilisé pour la connexion.
Type d'authentification	Deux types d'authentification sont disponibles, le MD5 (algorithme de hachage qui calcule un condensé de 128 bits) et le SHA1 (algorithme de hachage qui calcule un condensé de 160 bits).
Authentification	Mot de passe de l'utilisateur.
Chiffrement (optionnel)	Les paquets SNMP sont chiffrés en DES ou AES, une clé de chiffrement peut être définie. Par défaut c'est la clé d'authentification qui est utilisée.

AVERTISSEMENT
Il est vivement recommandé d'utiliser une clef spécifique**.**

DEFINITION : CHIFFREMENT
Il existe deux types de chiffrement : le chiffrement symétrique et asymétrique.
- Un système de chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer.
- Un système de chiffrement asymétrique utilise des clés différentes. Une clé publique pour chiffrer et une clé privée pour déchiffrer.

Les méthodes de chiffrement les plus connues sont le DES et l'AES.

Le **DES** : est une méthode de chiffrement utilisant des clés de 56 bits. Lorsqu'il est utilisé, c'est généralement en triple DES.
L'AES est un algorithme de chiffrement symétrique. La clé peut faire 128, 192 ou 26 bits.

11.4.4.3. Informations système

Emplacement	Information de lieu sur l'élément surveillé.
Contact	Adresse e-mail de la personne à contacter en cas de problème.

11.4.5. Evénements

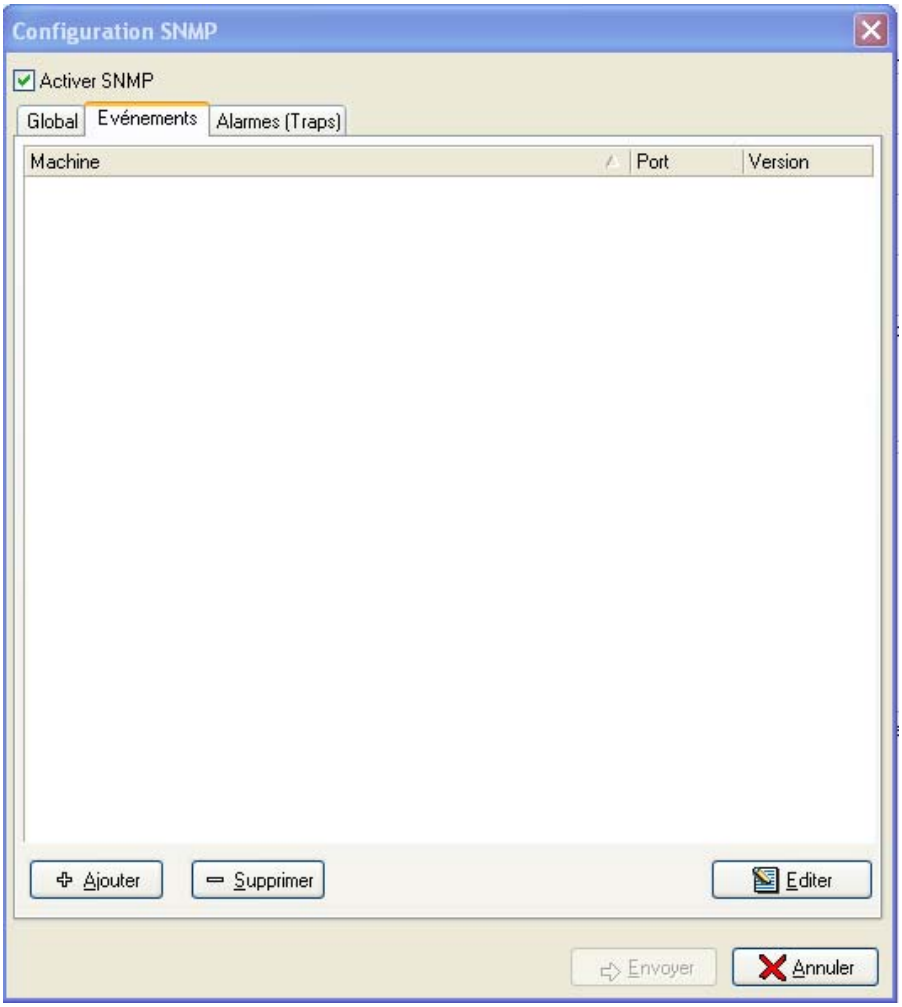


Figure 345 : Configuration du SNMP - Evènements

Dans cet onglet, vous configurez les stations que doit contacter le firewall lorsqu'il veut envoyer une Trap SNMP (événement). Si aucune station (machine) n'est spécifiée, le firewall n'envoie pas de messages.

En activant l'option **Activer les événements d'erreur d'authentification** vous pourrez recevoir les informations concernant les erreurs d'authentification.

Un assistant vous guide dans la configuration des machines.

La configuration d'une machine dans l'assistant se déroule comme pour l'onglet global. La sélection d'une version du protocole SNMP détermine le type de configuration à effectuer.

Le bouton d'action **Editer** permet de modifier les informations concernant une machine une fois que celle-ci a été créée.

Etape 1

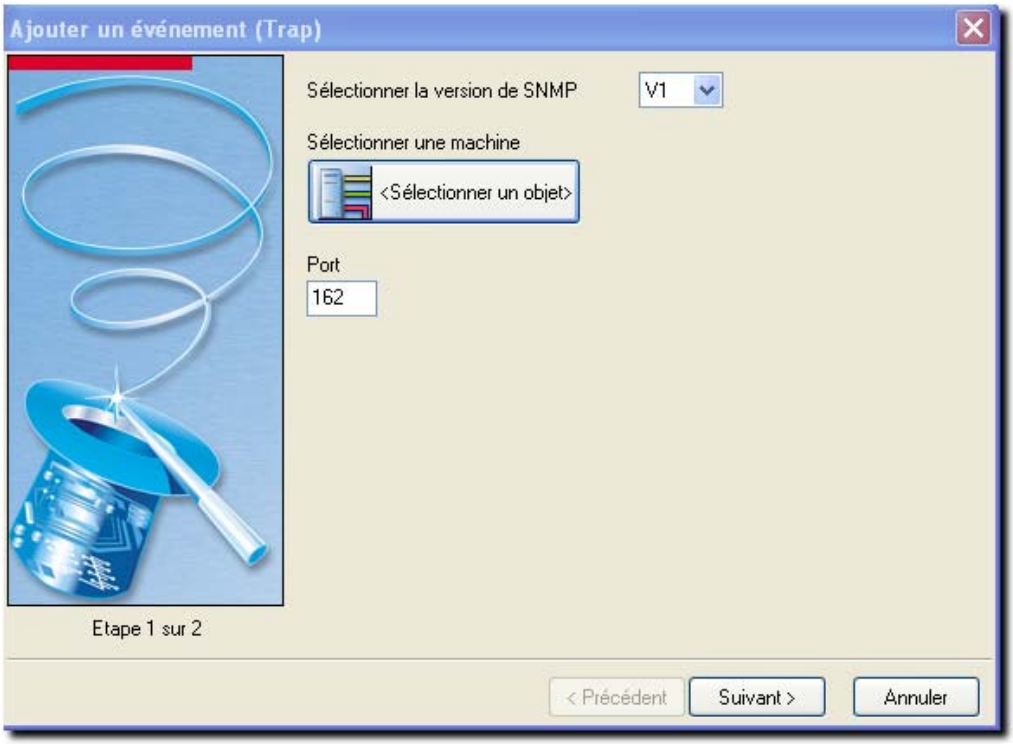


Figure 346 : Ajouter un événement (Trap) - Etape 1

Sélectionnez la version de SNMP : 3 choix possibles V1, V2c et V3.
En cliquant sur le bouton **Sélectionner une machine**, la base d'objets s'affiche vous permettant de sélectionner une machine.

Etape 2

- En sélectionnant SNMP V1 ou V2c

Dans ce cas, seul un nom de communauté est nécessaire.

- En sélectionnant SNMP V3 :

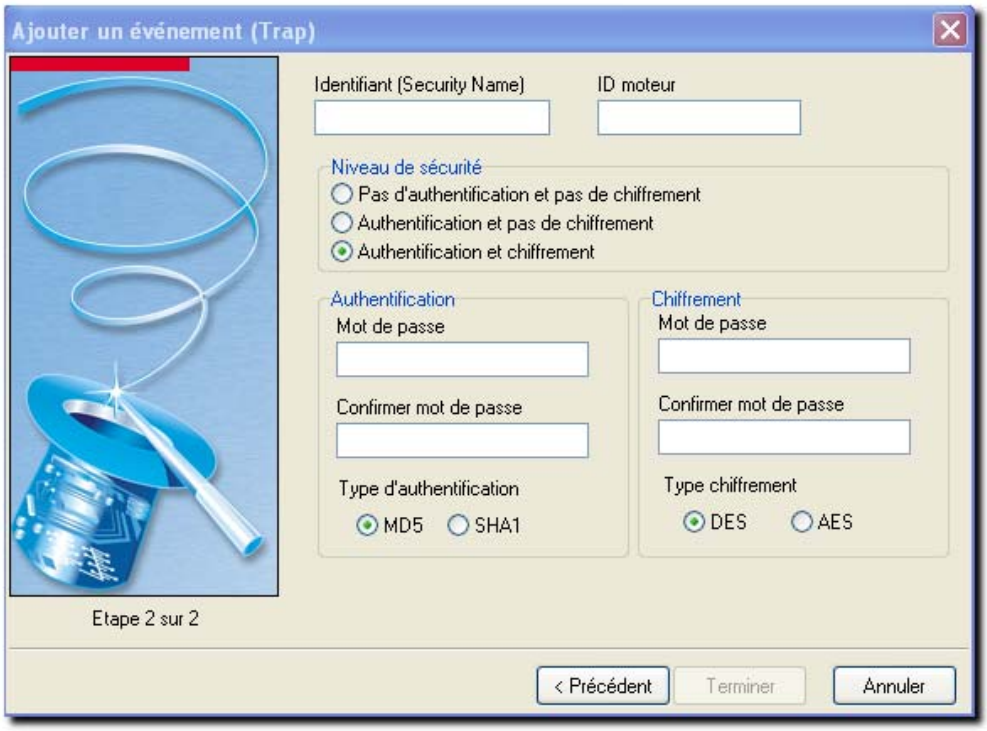


Figure 347 : Ajouter un événement (Trap) - Etape 2

Les paramètres de la configuration des événements de type SNMP V3 sont les suivants :

Identifiant (Security Name)	Nom de l'utilisateur autorisé à envoyer une trap sur la station de gestion.
ID moteur	Chaîne en hexadécimal créé par la station de gestion pour identifier l'utilisateur de manière unique de type 0x0011223344 (avec ou sans le 0x devant). Le moteur ID, à partir de la version 8.0, doit être composé au minimum de 5 octets et au maximum de 32 octets.
Niveau de sécurité	Différents niveaux de sécurité sont disponibles pour la version du protocole SNMP : • **Pas d'authentification et de chiffrement** : aucune sécurité • **Authentification et pas de chiffrement** : authentification sans chiffrement des traps • **Authentification et chiffrement** : si le mot de passe chiffrement reste vide on utilise le mot de passe authentification pour le chiffrement.
Mot de passe authentification	Mot de passe de l'utilisateur.
Mot de passe chiffrement	Les paquets SNMP sont chiffrés en DES, une clé de chiffrement peut être définie. Par défaut c'est la clef d'authentification qui est utilisée. **AVERTISSEMENT** Il est vivement recommandé d'utiliser une clé spécifique.
Type d'authentification	Deux types d'authentification sont disponibles, le MD5 et le SHA1.
Type chiffrement	Les deux types de chiffrement possibles sont DES et AES.

11.4.6. Alarmes (Traps)

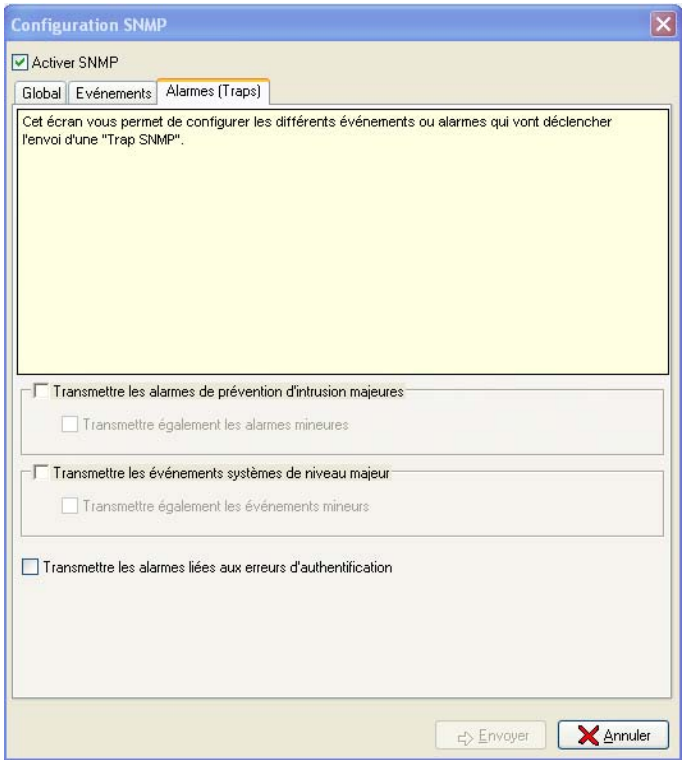


Figure 348 : Configuration SNMP - Alarmes

Transmettre les alarmes de prévention d'intrusion majeures	En cochant cette option, vous pourrez recevoir les alarmes ASQ majeures. En cochant l'option **Transmettre également les alarmes mineures**, les alarmes mineures ASQ seront également émises (via les traps et/ou consultation de la MIB).
Transmettre les événements systèmes de niveau majeur	En cochant cette option, vous pourrez recevoir les alarmes Système majeures. En cochant l'option **Transmettre également les événements mineurs**, les alarmes Système mineures seront également émises (via les traps et/ou consultation de la MIB).
Transmettre les alarmes liées aux erreurs d'authentification	Cette option autorise le système à envoyer des traps en cas d'échec d'authentification (tentative d'accès au service SNMP avec mauvaise communauté (V1/V2c/mauvaise authentification en V3).

PARTIE 12 : AUTHENTIFICATION

12.1.1. Introduction

Les fonctions d'identification/authentification permettent à l'utilisateur de déclarer son login (identification) et de vérifier que cet utilisateur est bien la personne qu'il prétend être, par la fourniture d'éléments qu'il est censé être le seul à pouvoir fournir (authentification).Une fois l'authentification réussie, le login de l'utilisateur est attribué, à travers la table des utilisateurs authentifiés, à la machine à partir de laquelle celui-ci s'est identifié et à tous les paquets IP qui en proviennent, et ce pour une durée spécifiée par l'utilisateur. L'utilisateur peut également se retirer manuellement de la table des utilisateurs authentifiés avant cette échéance.

12.1.1.1 Pour cette partie, vous devez avoir franchi les étapes

- Partie 2 : Installation, pré-configuration, intégration.
- Définition des interfaces, des objets et de la configuration du noyau.

12.1.1.2 Pour cette partie vous devez connaître

- Les données des utilisateurs (nom, prénom, adresse e-mail ...).

12.1.1.3 Utilité de la partie

Cette partie vous permettra de configurer la base de données des utilisateurs, de générer l'autorité de certification servant à créer les certificats numériques et de choisir la méthode d'authentification qu'utiliseront les utilisateurs internes.

L'authentification utilise une base de données **LDAP** (***Lightweight Directory Access Protocol***) stockant des fiches utilisateurs et, éventuellement, le certificat numérique x509 de l'utilisateur. Chaque firewall NETASQ embarque une base de données LDAP mais vous avez aussi la possibilité d'utiliser une base LDAP externe. Ainsi, vous pourrez centraliser vos fiches utilisateurs sur une base LDAP externe et plusieurs firewalls pourront utiliser la même base. Les firewalls NETASQ supportent aussi l'authentification via un serveur RADIUS, un serveur Kerberos ou un serveur NTLM externe.

NETASQ supporte aussi l'utilisation du protocole SRP pour l'authentification des utilisateurs. Ce protocole sans divulgation de mot de passe est résistant aussi bien aux attaques d'écoute passive qu'aux attaques actives basées sur la modification ou l'insertion de paquets dans la séquence d'authentification. Il utilise un mot de passe réutilisable fourni par l'utilisateur, et conserve ses propriétés de résistance aux attaques même lorsque l'entropie du mot de passe est basse.

Concrètement, le firewall fournit, à travers des capacités de type "serveur HTTP", des formulaires Web qui permettent de s'identifier, de s'authentifier en spécifiant la durée de la session, et de fermer la session manuellement. Il n'est pas nécessaire que la session HTTP persiste pour que la session reste active. Les étapes du protocole SRP sont effectuées par une applet Java téléchargée depuis le firewall sur le poste de l'utilisateur. Cette applet se sert du mot de passe fourni par l'utilisateur pour mener les étapes du protocole SRP. Grâce à cet enrôlement Web, la tâche de l'administrateur est simplifiée car ce sont les utilisateurs qui demandent la création de leur compte d'accès (à l'Internet, au serveur mail, à tous les services qui

nécessitent selon votre politique de filtrage une authentification) en renseignant eux-mêmes les informations les concernant.

12.1.2. Portail captif

Avant d'activer l'authentification, vous devez avoir configuré la base de données LDAP (Cf. *Configuration de la base LDAP*). L'activation de l'authentification est accessible par le menu **`Authentification\Portail captif.`**

L'écran de configuration de l'authentification se décompose en trois parties :

- A gauche, un arbre présentant les diverses fonctionnalités du menu configuration de l'authentification.
- A droite, les options disponibles.
- Des boutons d'action au bas de l'écran.

12.1.2.1. Boutons d'action

Bouton "Assistant de configuration de l'authentification"

Etape 1 : Bienvenue

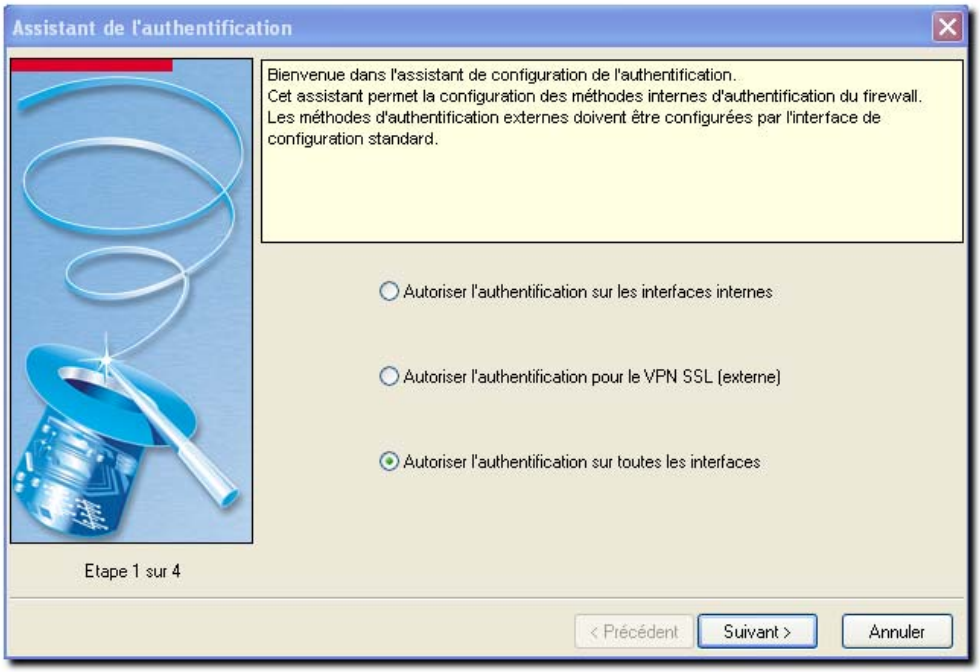


Figure 349 : Assistant de l'authentification - Etape 1

Il existe deux interfaces pour les méthodes d'authentification : cette interface permet la configuration interne du firewall.

2 Méthodes d'authentification

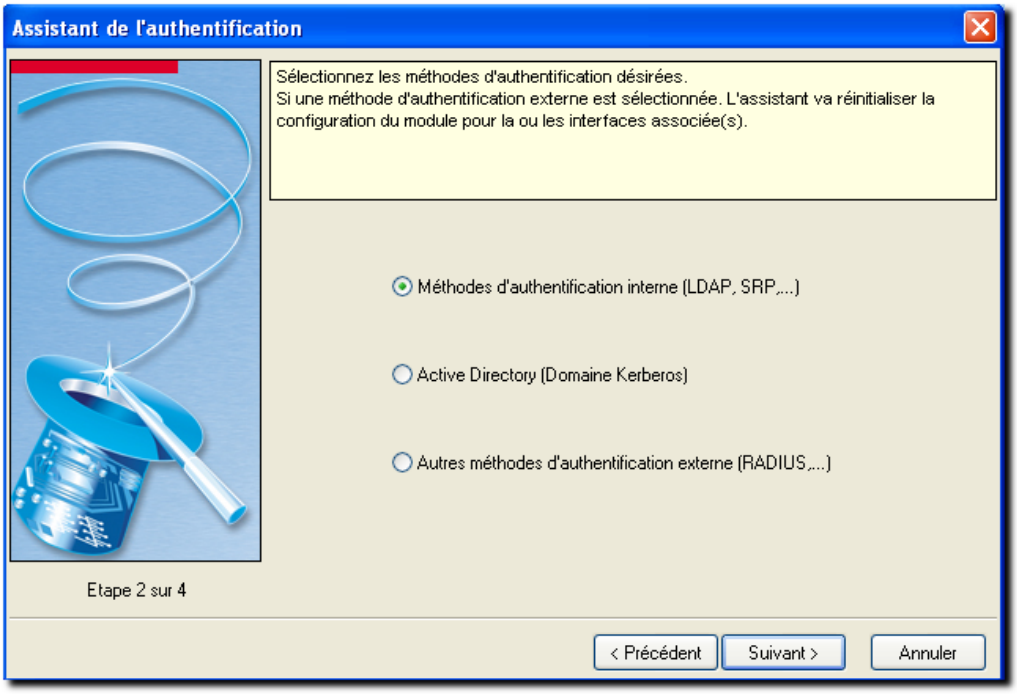


Figure 350 : Assistant de l'authentification - Etape 2

Cet écran permet de sélectionner une méthode d'authentification parmi :

- Méthodes d'authentification interne (LDAP, SRP,…).
- Active Directory (Domaine Kerberos).
- Autres méthodes d'authentification externe (RADIUS,…).

3 Enrôlement

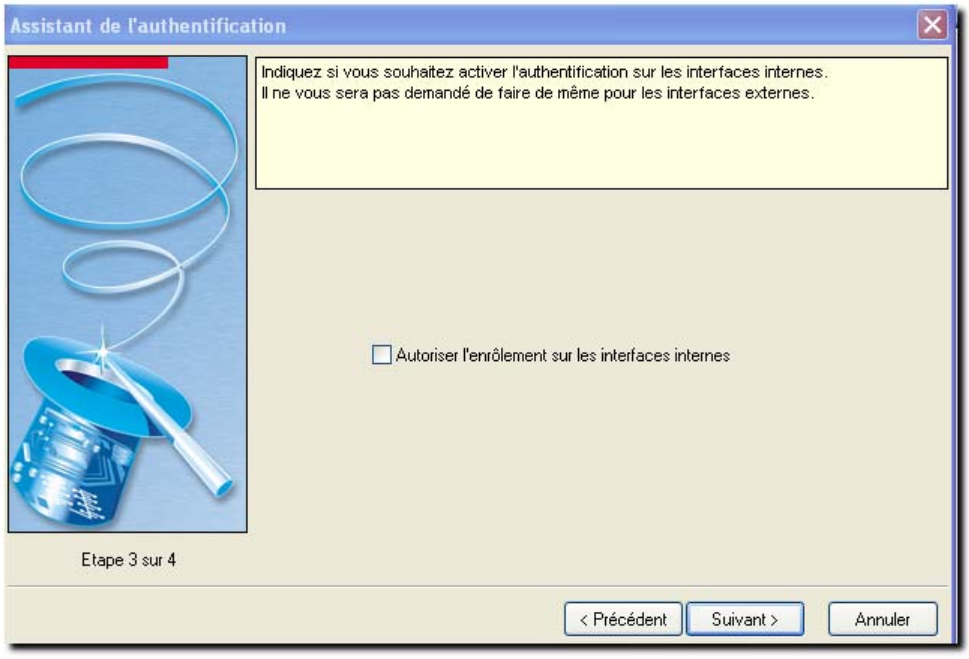


Figure 351 : Assistant de l'authentification - Etape 4

En cochant l'option **Autoriser l'enrôlement sur les interfaces internes** vous activez l'authentification sur les interfaces internes.

4 Mots de passe

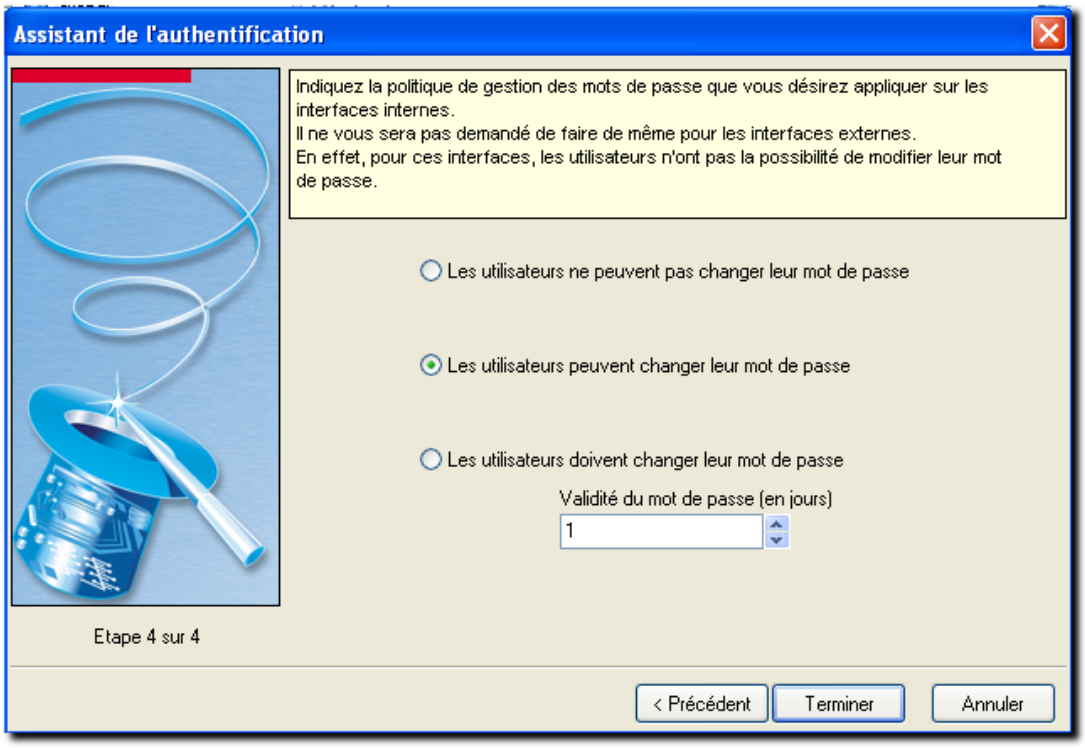


Figure 352 : Assistant de l'authentification - Etape 4

Sur les interfaces internes, il est possible de modifier les mots de passe. Cet écran vous permet d'indiquer votre politique de gestion de mots de passe entre les options Les utilisateurs ne peuvent pas changer leur mot de passe, Les utilisateurs peuvent changer leur mot de passe, les utilisateurs doivent changer leur mot de passe. Pour cette dernière option, indiquez le nombre de jours de validité du mot de passe.

Boutons "Envoyer et "Annuler"

Envoyer	Activation de la configuration de l'authentification.
Annuler	Annule le paramétrage modifié de l'écran d'authentification

12.1.2.2. Global

Deux méthodes d'authentification sont possibles pour l'authentification des utilisateurs :

- Pour les utilisateurs du réseau interne (interfaces internes).
- Pour les utilisateurs connectés au réseau par une interface externe.

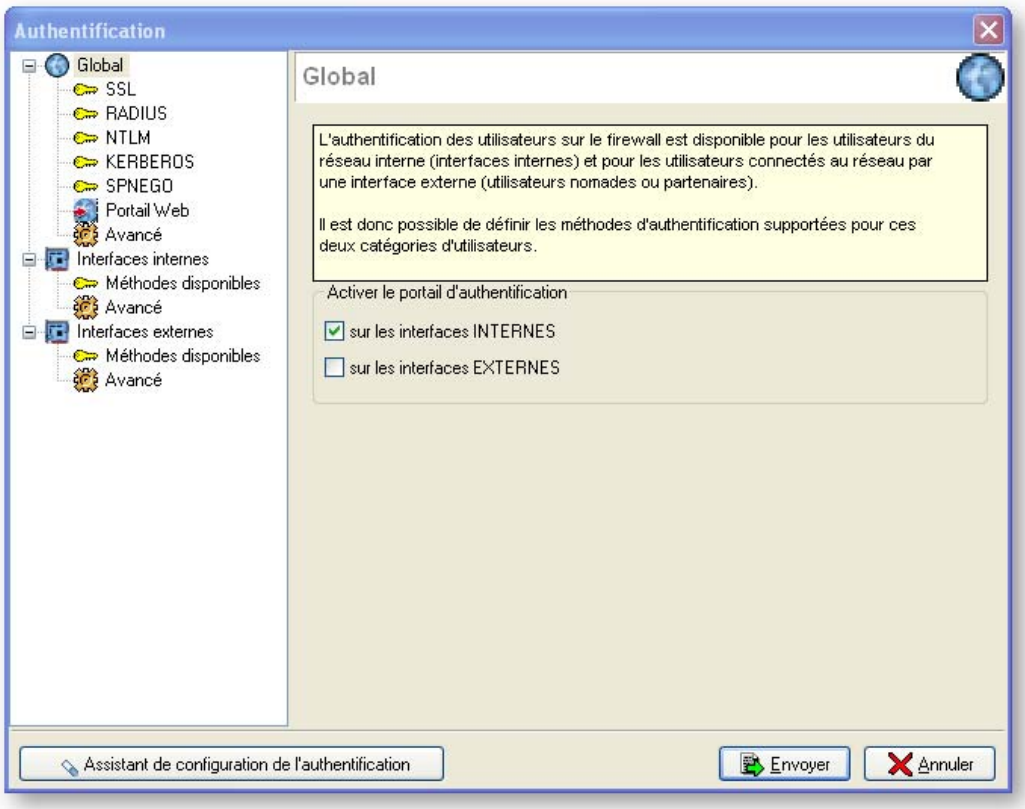


Figure 353 : Authentification - Global

L'authentification sur les firewalls est différenciée par les interfaces sur lesquelles arrivent les flux de trafic. En effet il est possible d'activer l'authentification uniquement sur les interfaces internes, uniquement sur les interfaces externes ou sur les deux types d'interfaces.

Pour activer l'authentification sur un type d'interface, cochez l'option sur les interfaces INTERNES et/ou sur les interfaces EXTERNES correspondant au type d'interface.

SSL

La liste de révocation des certificats (CRL) est régulièrement mise à jour. Ces mises à jour sont nécessaires pour l'authentification par certificat SSL. De plus, il faut indiquer l'identifiant de l'utilisateur pour ce type de PKI.

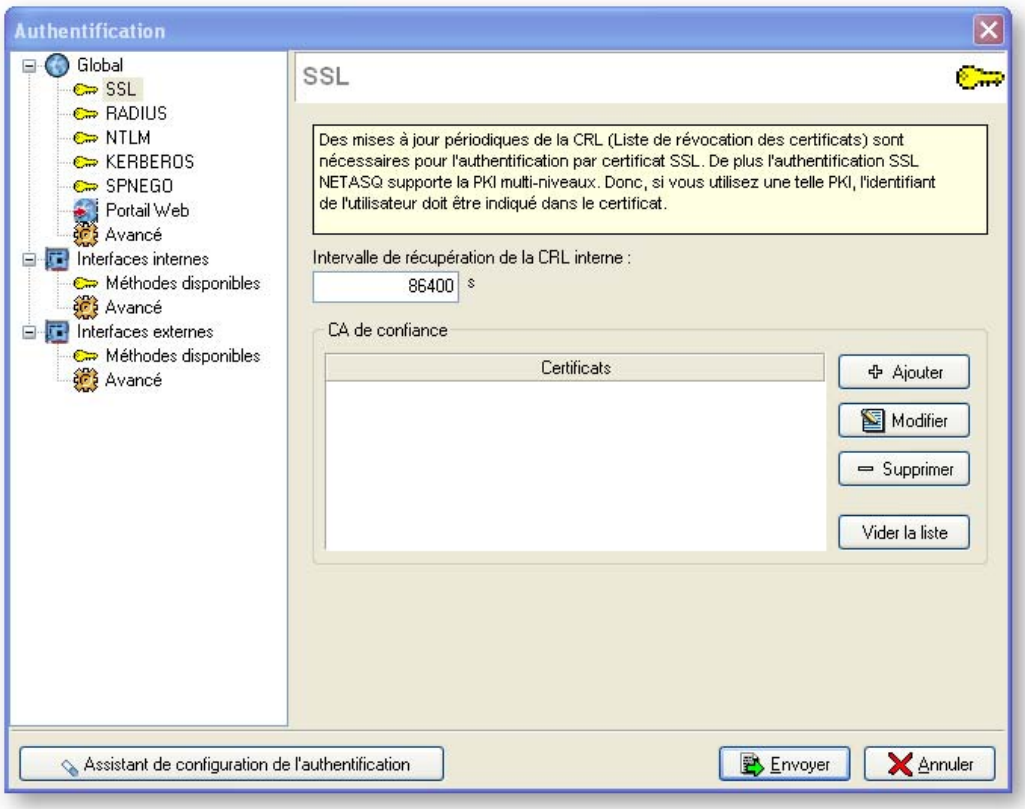


Figure 354 : Authentification - SSL

Lorsque la méthode SSL est sélectionnée, l'authentification SSL est activée. Les options de configuration de la méthode SSL sont indiquées dans le tableau ci-dessous :

Intervalle de récupération de la CRL interne	Temps en secondes au bout duquel il faut récupérer la **CRL** servant à vérifier la validité des certificats numériques créés par la **PKI** interne du firewall.
CA de confiance	La méthode d'authentification SSL peut accepter l'utilisation de certificats signés par une autorité de certification externe au firewall. Pour cela il est nécessaire d'ajouter cette autorité de certification dans la configuration du firewall de façon à ce que celui accepte tous les certificats effectivement signés par cette autorité. Si l'autorité de certification est elle-même signée par une autre autorité de certification. Il est possible de rajouter cette autorité dans la liste des CA de confiance pour ainsi créer une "Chaîne de confiance". Lorsqu'une CA de confiance ou une chaîne de CA de confiance est spécifiée dans la configuration de la méthode d'authentification SSL, elle s'ajoute à la CA interne du firewall implicitement vérifiée dès qu'il existe une PKI interne valide sur le firewall.

Les boutons d'action

Ajouter	L'ajout d'une autorité de certification dans la liste des autorités de certification de confiance permet d'accepter cette autorité comme autorité reconnue et de valider tous les certificats signés par cette autorité de certification. En cliquant sur le bouton **Ajouter** on accède à la fenêtre des certificats externes. (Cf. *Certificats*). Si l'autorité de certification à laquelle vous désirez faire confiance ne fait pas partie de la liste des certificats externes, cliquez sur le bouton **Ajouter** de la fenêtre des certificats externes pour ajouter cette autorité de certification dans la liste. Les firewalls supportent les PKI multi niveaux. Ainsi si le certificat de l'utilisateur à authentifier est signé par une autorité de certification, elle-même signée par une autorité de certification supérieure, vous pouvez insérer toute la chaine de certification créée par cette PKI multi niveaux. Pour que toute la chaîne soit correctement prise en compte, il est important d'insérer l'ensemble de la chaîne des autorités entre l'autorité la plus haute que vous avez inséré et l'autorité directement supérieure au certificat utilisateur.
Modifier	Permet la modification d'une autorité de certification. Par exemple, chaque CA est obligatoirement associée à une CRL. Cette CRL a une durée de vie limitée (pour prendre en compte régulièrement les nouveaux certificats révoqués) mais elle n'est pas modifiée automatiquement, il faut donc le faire manuellement.
Supprimer	Supprime l'autorité de certification sélectionnée.
Vider la liste	Supprime la liste complète des certificats configurés.

AVERTISSEMENTS

1) L'ajout d'une autorité de certification de confiance nécessite obligatoirement d'associer à cette CA, une liste de révocation des certificats. L'assistant d'ajout d'autorité de certification demande obligatoirement cet ajout. Toutefois cette CRL n'est pas récupérée automatiquement comme dans le cas de la CRL interne de la PKI des firewalls NETASQ.
2) L'utilisation d'une autorité de certification externe nécessite que l'email spécifié dans le certificat utilisateur qui sera utilisé pour l'authentification soit identique à celui précisé dans la fiche utilisateur de la base d'utilisateur du firewall. Afin que celui-ci puisse effectuer une correspondance stricte entre le certificat qui lui proposé et un identifiant d'utilisateur présent dans sa base d'utilisateurs.

RADIUS

Introduction

RADIUS est un protocole d'authentification qui fonctionne en mode client-serveur. Le firewall NETASQ peut se comporter comme un client RADIUS. Il peut alors adresser, à un serveur RADIUS externe, des demandes d'authentification pour les utilisateurs désirant traverser le firewall. L'utilisateur ne sera authentifié sur le firewall que si le RADIUS accepte la demande d'authentification envoyée par le firewall.

Toutes les transactions RADIUS (communications entre le firewall et le serveur RADIUS) sont elles-mêmes authentifiées par l'utilisation d'un secret pré-partagé, qui n'est jamais transmis sur le réseau. Ce même secret sera utilisé pour chiffrer le mot de passe de l'utilisateur, qui transitera entre le firewall et le serveur RADIUS. L'authentification RADIUS utilise le protocole UDP sur le port 1812.

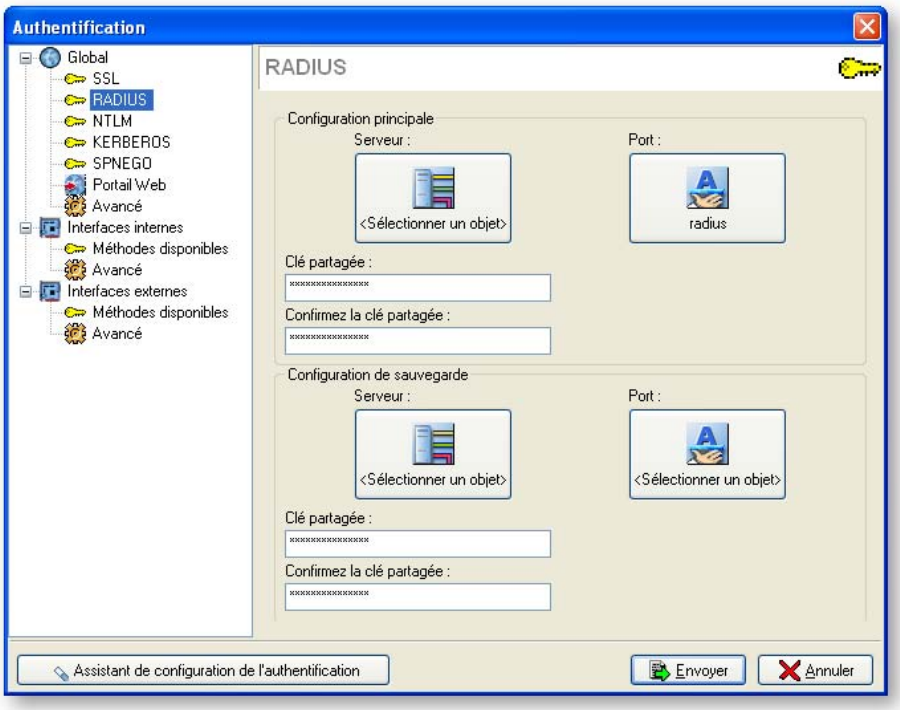


Figure 355 : Authentification - RADIUS

Fonctionnement

Lorsque la méthode RADIUS est sélectionnée, l'authentification RADIUS est activée. Ce menu vous permet de préciser les informations relatives au serveur RADIUS externe utilisé et d'un éventuel serveur RADIUS de sauvegarde. Pour chacun la configuration nécessite de renseigner les informations présentées dans le tableau suivant :

Serveur	Adresse IP du serveur RADIUS.
Port	Port utilisé par le serveur RADIUS.
Clé partagée	Clef utilisée pour le chiffrement des échanges entre le firewall et le serveur RADIUS.
Confirmez la clé partagée	Saisissez à nouveau la clé pour confirmation.

Processus de basculement entre le serveur principal et le serveur de sauvegarde

Le firewall tente de se connecter 2 fois au serveur RADIUS "principal", en cas d'échec il tente de se connecter 2 fois au serveur RADIUS "backup". Si le serveur RADIUS "backup" répond, il bascule en tant que serveur RADIUS "principal". Au bout de 600 secondes, un nouveau basculement s'opère, l'ancien serveur RADIUS "principal" redevient "principal".

NTLM

Introduction

NTLM sert de protocole d'authentification pour les transactions entre deux ordinateurs d'un même domaine, où l'un des deux ordinateurs, ou les deux, exécutent Windows NT 4.0 ou une version précédente.

Le protocole de NTLM authentifie des utilisateurs et des ordinateurs basés sur un mécanisme de challenge/réponse. Toutes les fois qu'une nouvelle marque d'accès est nécessaire, le firewall entre en contact avec un service d'authentification sur le contrôleur de domaine pour vérifier l'identité de l'utilisateur.

L'utilisateur ne sera authentifié sur le firewall que si le service d'authentification NTLM accepte lademande d'authentification envoyée par le firewall.

Le firewall est donc compatible avec l'authentification NT.

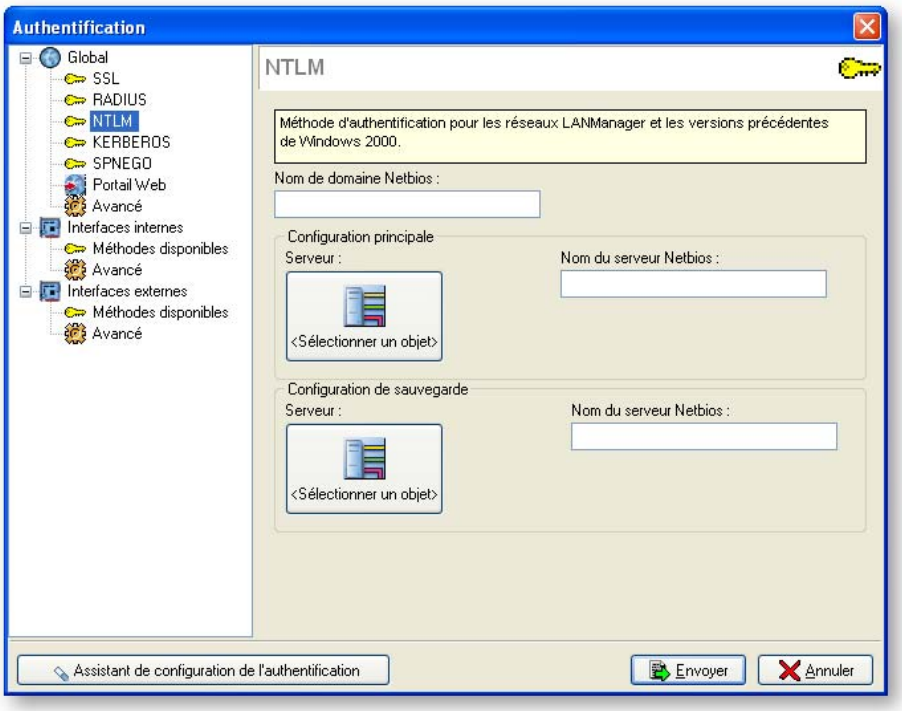


Figure 356 : Authentification - NTLM

Fonctionnement

Lorsque la méthode NTLM est sélectionnée, l'authentification NTLM est activée. Ce menu vous permet de préciser les informations relatives au serveur NTLM externe utilisé et d'un éventuel serveur NTLM de sauvegarde. Pour chacun la configuration nécessite de renseigner les informations présentées dans le tableau suivant :

Nom de domaine NetBIOS	Nom de domaine sur lequel est utilisé le serveur NTLM.
Serveur	Adresse IP du serveur NTLM. En cliquant sur le bouton, la base d'objets s'affiche vous permettant de sélectionner une machine.
Nom du serveur NetBIOS	Nom utilisé par le serveur NTLM.

Processus de basculement entre le serveur principal et le serveur de sauvegarde

Le firewall tente de se connecter 2 fois au serveur NTLM "principal", en cas d'échec il tente de se connecter 2 fois au serveur NTLM "backup". Si le serveur NTLM "backup" réponde, il bascule en tant que serveur NTLM "principal". Au bout de 600 secondes, un nouveau basculement s'opère, l'ancien serveur NTLM "principal" redevient "principal".

KERBEROS

Introduction

Kerberos est différent des autres méthodes d'authentification. Plutôt que de laisser l'authentification avoir lieu entre chaque machine cliente et chaque serveur, Kerberos utilise un cryptage symétrique et un programme fiable, le Centre distributeur de tickets (KDC, Key Distribution Center) afin d'authentifier les utilisateurs sur un réseau.

Le protocole UDP est utilisé dans un cas standard mais nécessite tout de même le protocole TCP en cas de requêtes trop longues. Lorsqu'une requête trop longue est détectée, le serveur bascule donc de l'UDP vers le TCP.

Une fois l'authentification effectuée, Kerberos stocke un ticket spécifique à cette session sur l'ordinateur de l'utilisateur et les services "kerberisés" rechercheront ce ticket au lieu de demander à l'utilisateur de s'authentifier à l'aide d'un mot de passe.

Dans ce processus d'authentification le boîtier agit comme un client qui se substitue à l'utilisateur pour demander une authentification. Cela signifie que même si l'utilisateur est déjà authentifié sur le KDC pour son ouverture de session Windows par exemple, il faut tout de même se ré-authentifier auprès de ce serveur même si les informations de connexion sont identiques, pour traverser le firewall.
Toutefois l'intérêt de cette méthode est qu'il n'y a qu'une base d'authentification à tenir à jour. Kerberos est utilisé par les environnements Windows 2000 et XP, ce qui rend le firewall compatible avec l'authentification de ces systèmes.

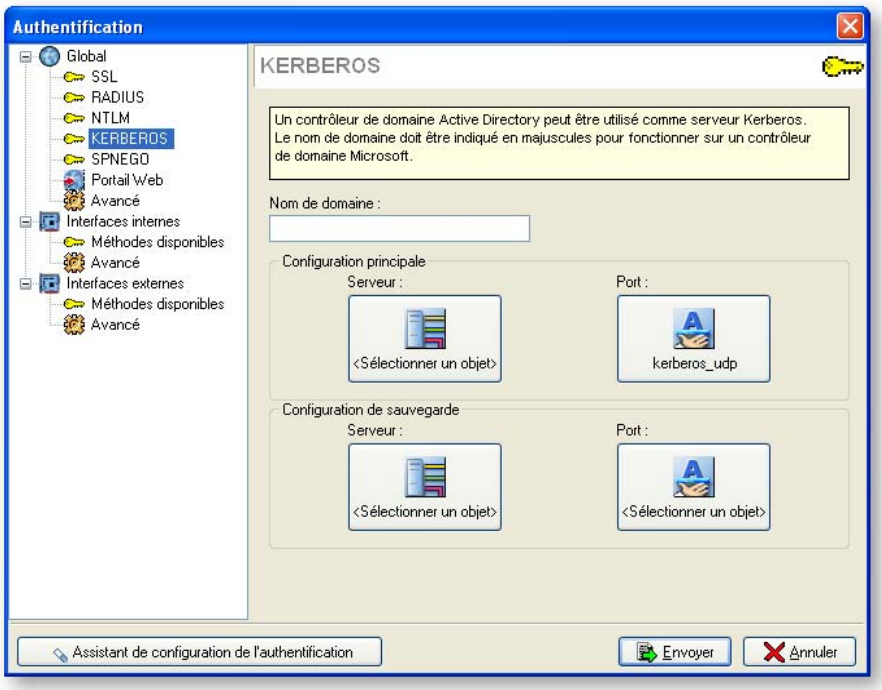


Figure 357 : Authentification - KERBEROS

Fonctionnement

Lorsque la méthode Kerberos est sélectionnée, l'authentification Kerberos est activée. Ce menu vous permet de préciser les informations relatives au serveur Kerberos externe utilisé et d'un éventuel serveur Kerberos de sauvegarde. Pour chacun la configuration nécessite de renseigner les informations présentées dans le tableau suivant :

Nom de domaine	Nom de domaine sur lequel est utilisé le serveur Kerberos.
Serveur	Adresse IP du serveur Kerberos. En cliquant sur le bouton, la base d'objets s'affiche vous permettant de sélectionner une machine.
Port	Port utilisé par le serveur Kerberos. Mais parfois les requêtes sont trop longues. Le port est donc basculé automatiquement vers le protocole TCP.

Processus de basculement entre le serveur principal et le serveur de sauvegarde

Le firewall tente de se connecter 2 fois au serveur Kerberos "principal", en cas d'échec il tente de se connecter 2 fois au serveur Kerberos "backup". Si le serveur Kerberos "backup" répond, il bascule en tant que serveur Kerberos "principal". Au bout de 600 secondes, un nouveau basculement s'opère, l'ancien serveur Kerberos "principal" redevient "principal".

SPNEGO

Introduction

La méthode SPNEGO permet le fonctionnement du "Single Sign On" pour l'authentification Web avec un serveur d'authentification externe Kerberos. Cela signifie qu'un utilisateur se connectant à son domaine par une solution basée sur un serveur Kerberos serait automatiquement authentifié sur un firewall NETASQ dans le cas d'un accès à l'Internet (nécessitant une authentification dans la politique de filtrage sur le firewall) grâce à un navigateur Web (Internet Explorer, Firefox, Mozilla).

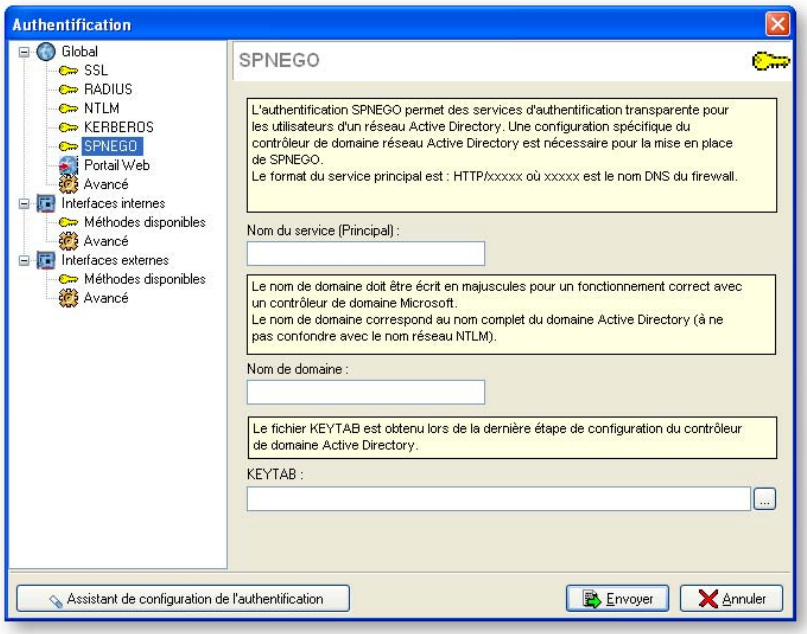


Figure 358: Authentification - SPNEGO

Pré requis

La solution NETASQ s'intègre dans le cadre d'une solution de "Single Sign On" complète, il s'agit donc d'installer certains composants sur le serveur Kerberos. Pour cela suivez la procédure suivante :

1. Installation d'un "Nom du service (Principal)" (SPN) sur le serveur SPNEGO afin de permettre le chiffrement des échanges entre le serveur SPNEGO, l'utilisateur et le firewall.
2. Exécution du script SPNEGO livré par NETASQ dans le CD-ROM de l'Administration Suite.
3. Récupération de la "KEYTAB" générée par le script.

Fonctionnement

La configuration de SPNEGO sur le firewall est réalisée grâce aux options expliquées dans le tableau suivant :

Nom du service (Principal)	Nom ou adresse du firewall utilisé pour l'authentification. Ce nom correspond au nom indiqué dans le script NETASQ (voir ci-dessus). Il sera précédé de la mention **HTTP/xxxxx ou xxxxx.** **Exemple** HTTP/U70XXAZ0899020
Nom de domaine	Nom de domaine du serveur Kerberos. Ce nom de domaine correspond au nom de domaine indiqué dans le script. Il correspond au nom complet du domaine Active Directory. Il doit être écrit en majuscules.
KEYTAB domaine	Récupérer la "KEYTAB" générée par le script NETASQ (voir ci-dessus).

Pour réaliser une redirection transparente de l'authentification, activez le proxy **HTTP** (Cf. Partie 9/Chapitre 3 : Configuration du proxy HTTP).

NOTE
L'authentification Web ne s'active que si une règle d'authentification a été définie dans la politique de filtrage (Cf. Partie 7/Chapitre 2 : Filtrage).

Portail Web

Le serveur d'authentification peut utiliser des certificats que vous aurez préalablement configurés.

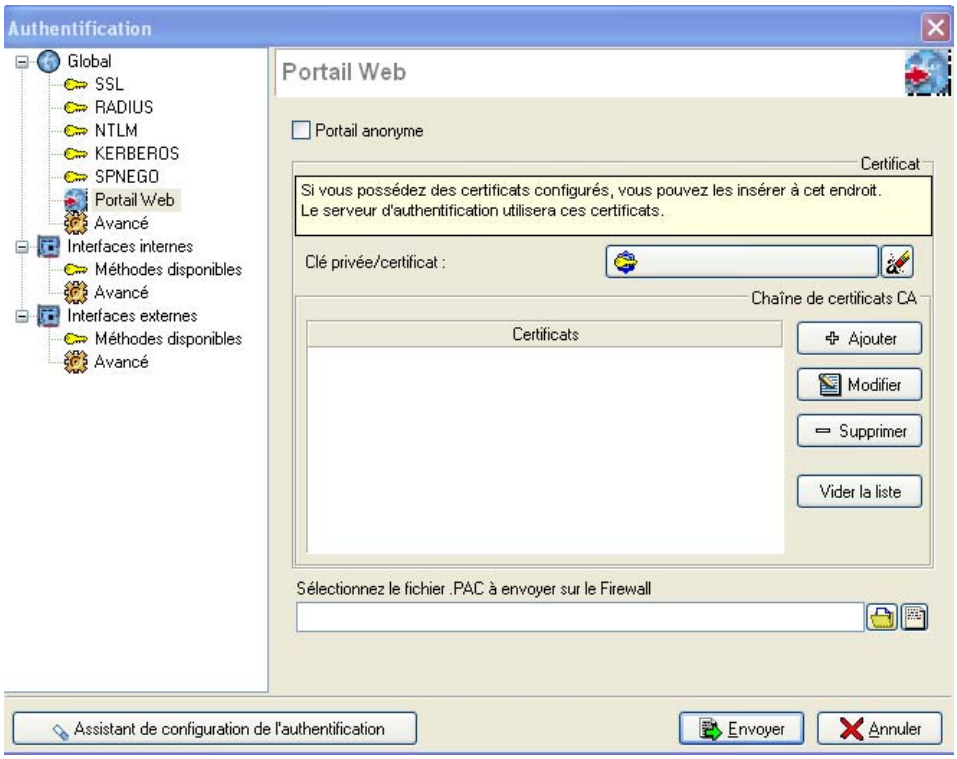


Figure 359 : Authentification - Portail Web

Portail anonyme	Lorsque cette option est activée, le logo NETASQ du portail d'authentification est masqué.
Clé privée/certificat	Par défaut le certificat utilisé par le module d'authentification du firewall est le certificat propre du firewall, le nom associé à ce certificat est le numéro de série du produit. Ainsi lorsqu'un utilisateur essaie de contacter le firewall différemment que par son numéro de série, il reçoit un message d'avertissement indiquant une incohérence entre ce que l'utilisateur essaie de contacter et le certificat qu'il reçoit. Pour éviter ce message, le module d'authentification des firewalls offre la possibilité de spécifier un certificat « serveur » (impossible de spécifier un certificat utilisateur pour cette fonctionnalité) dont le nom serait beaucoup plus facile à retenir. **Exemple** www.netasq.com. Pour obtenir ce type de certificat, vous devez contacter des organismes du type Verisign ou Thawte. En cliquant sur le bouton Clef privée/certificat l'écran de configuration des certificats s'affiche (ici pour la clé privée).
Sélectionnez le fichier .PAC à envoyer sur le Firewall	Ce champ permet d'envoyer au firewall le fichier .PAC à distribuer. L'utilisateur peut récupérer un fichier PAC ou alors vérifier son contenu à l'aide des deux boutons situés à droite du champ. L'utilisateur peut pécifier dans son navigateur web, le script de configuration automatique qui se situe dans https://if_firewall>/config/wpad.dat.

Chaîne de certificat CA

Cette chaîne de certificat CA certifie la clé privée utilisée dans la configuration du portail d'authentification. Pour cela il est nécessaire d'ajouter cette autorité de certification dans la configuration du firewall de façon à ce que celui accepte tous les certificats effectivement signés par cette autorité (et la clé privée spécifiée plus haut plus particulièrement. Si l'autorité de certification est elle-même signée par une autre autorité de certification. Il est possible de rajouter cette autorité dans la liste des CA de confiance pour ainsi créer une « Chaîne de confiance ».

Ajouter	L'ajout d'une autorité de certification dans la liste des autorités de certification de confiance permet d'accepter cette autorité comme autorité reconnue et de valider tous les certificats signés par cette autorité de certification. En cliquant sur le bouton **Ajouter** on accède à la fenêtre des certificats externes. Si l'autorité de certification à laquelle vous désirez faire confiance ne fait pas partie de la liste des certificats externes, cliquez sur le bouton **Ajouter** de la fenêtre des certificats externes pour ajouter cette autorité de certification dans la liste. Les firewalls supportent les PKI multi niveaux. Ainsi si le certificat de l'utilisateur à authentifier est signé par une autorité de certification, elle-même signée par une autorité de certification supérieure, vous pouvez insérer toute la chaine de certification créée par cette PKI multi niveaux. Pour que toute la chaîne soit correctement prise en compte, il est important d'insérer l'ensemble de la chaîne des autorités entre l'autorité la plus haute que vous avez inséré et l'autorité directement supérieure au certificat utilisateur.
Modifier	Permet la modification d'une autorité de certification. **Exemple** Par exemple, chaque CA est obligatoirement associée à une CRL. Cette CRL a une durée de vie limitée (pour prendre en compte régulièrement les nouveaux certificats révoqués) mais elle n'est pas modifiée automatiquement, il faut donc le faire manuellement.
Supprimer	Supprime l'autorité de certification sélectionnée.
Vider la liste	Supprime la liste complète des certificats configurés.

AVERTISSEMENT
L'ajout d'une autorité de certification de confiance nécessite obligatoirement d'associer à cette CA, une liste de révocation des certificats. L'assistant d'ajout d'autorité de certification demande obligatoirement cet ajout. Toutefois cette CRL n'est pas récupérée automatiquement comme dans le cas de la CRL interne de la PKI des firewalls NETASQ.

Avancé

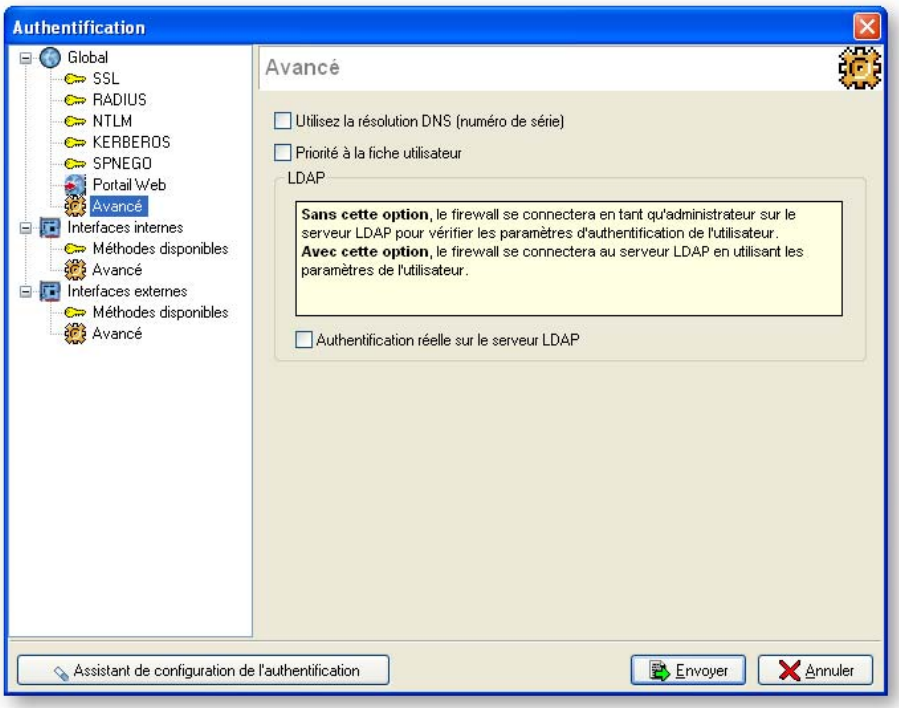


Figure 360 : Authentification - Avancé

Utilisez la résolution DNS (numéro de série)	Lorsque l'authentification transparente est activée (utilisation du proxy URL), l'utilisateur désirant se connecter à un site Web doit d'abord s'authentifier en HTTPS sur le Firewall. Pour cela, le navigateur de l'utilisateur vérifie le certificat du firewall. Un message d'erreur s'affiche dans le navigateur puisque le certificat correspond au numéro de série du firewall et pas à son adresse IP. L'utilisation de la résolution DNS permet de faire la correspondance entre le numéro de série du firewall et son adresse IP. **AVERTISSEMENT** Il faut, dans ce cas, que le numéro de série du firewall soit indiqué au niveau du serveur DNS. (Correspondance entre le numéro de série du firewall et son adresse IP).
Priorité à la fiche utilisateur	Lorsque cette option est cochée, quel que soit le résultat de la méthode d'authentification SPNEGO, le firewall tentera une authentification grâce à la méthode indiquée dans la fiche de l'utilisateur.
Authentification réelle sur le serveur LDAP	Lorsque cette option est décochée, le firewall réalise une connexion en temps qu'administrateur sur le serveur LDAP pour valider l'authentification de l'utilisateur. Lorsque cette option est cochée, le firewall tente réellement de s'authentifier sur le serveur LDAP avec les paramètres de l'utilisateur. Si l'authentification du firewall sur le serveur LDAP échoue, l'authentification est alors refusée à l'utilisateur.

12.1.2.3. Interface interne et interface externe

Pour chaque type d'interface, l'activation de l'authentification nécessite la définition de paramètres d'utilisation. Ces paramètres d'utilisation sont les mêmes pour les interfaces dites internes (**ne possédant pas** l'attribut "Externe" dans la configuration réseau) et pour les interfaces dites externes (possédant l'attribut "Externe" dans la configuration réseau).

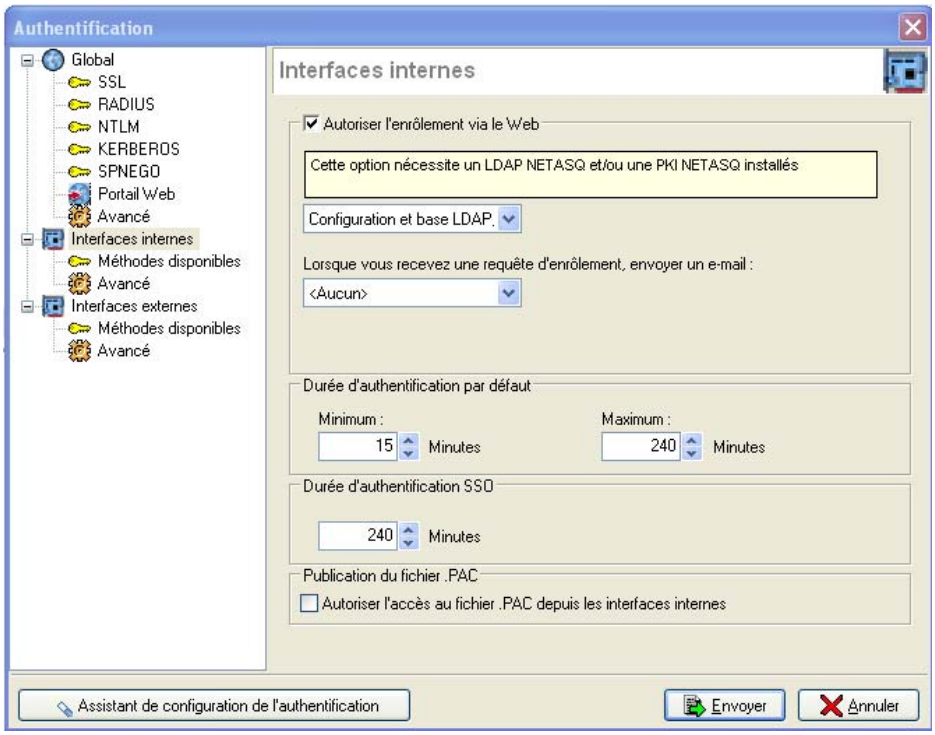


Figure 361 : Authentification - Interfaces internes

Autoriser l'enrôlement via le Web

NETASQ vous propose l'enrôlement d'utilisateurs par le web. Si l'utilisateur qui tente de se connecter n'existe pas dans la base des utilisateurs, il a la possibilité de demander la création de son compte par un enrôlement Web.

Autoriser l'enrôlement via le Web	Un LDAP NETASQ ou une PKI NETASQ doivent être installés pour que cette option soit fonctionnelle. Vous pouvez spécifier deux types d'enrôlement disponible à partir du Web : • **LDAP** : création d'un compte utilisateur. • **LDAP/PKI** : création d'un compte utilisateur et d'un certificat.
Lorsque vous recevez une requête d'enrôlement, envoyer un e-mail	Lorsqu'un utilisateur demande la création d'un compte par l'enrôlement Web, cette requête est indiquée dans NETASQ UNIFIED MANAGER. L'administrateur peut aussi être prévenu de cette requête par mail si l'option **Envoi des requêtes par e-mail** est cochée. Dans ce cas le firewall NETASQ utilise l'adresse e-mail indiquée dans la configuration des traces (Cf. Partie 17 : Gestion des traces).

Durée d'authentification par défaut	**Minimum** : Temps minimum durant lequel l'utilisateur est authentifié. **Maximum** : Temps maximum durant lequel l'utilisateur est authentifié. Au bout de ce délai, l'authentification expire et l'utilisateur doit se ré-authentifier. Les deux précédentes valeurs permettent de définir une plage de choix pour l'authentification (l'utilisateur pourra choisir une durée d'authentification comprise dans cette plage). **AVERTISSEMENT** Afin d'éviter le détournement de session d'authentification, il est conseillé de ne pas définir un temps maximum trop élevé (4 heures maximum) mais cela implique que l'utilisateur devra se ré-authentifier souvent.
Durée d'authentification SSO	Lorsqu'une méthode d'authentification basée sur SSO (Single Sign On), l'authentification unique, cette période permet de définir la durée pendant laquelle aucune réauthentification transparente n'est de demandée par le firewall.
Publication du fichier .PAC	En cochant l'option **Autoriser l'accès au fichier .PAC depuis les interfaces internes**, vous autorisez la publication du fichier .PAC sur les interfaces internes. La publication du fichier .PAC est également possible pour les interfaces externes.

Méthodes disponibles

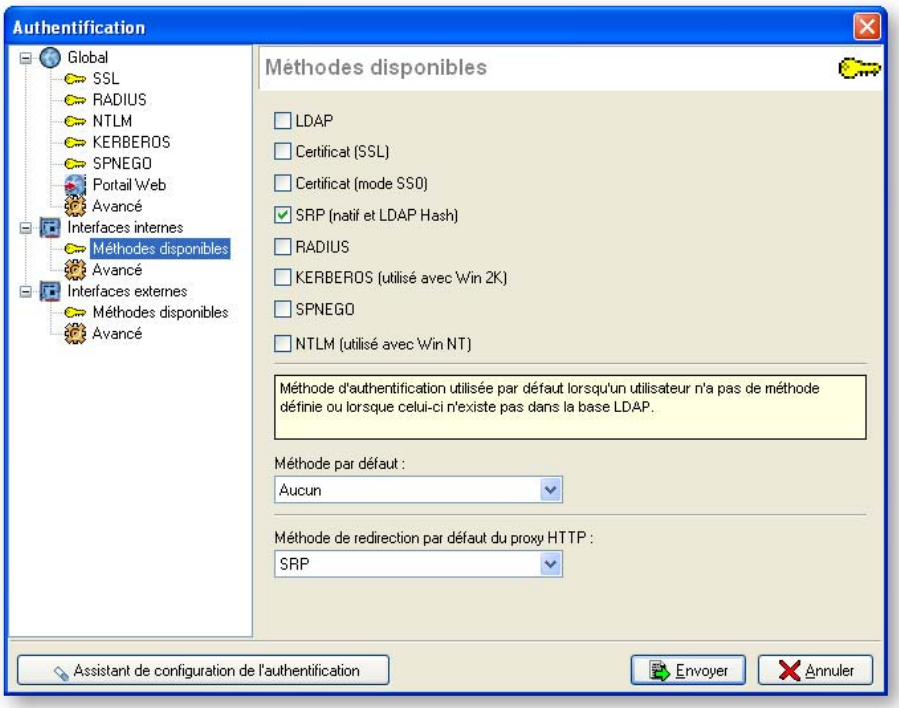


Figure 362 : Authentification - Méthodes disponibles

Choisissez la ou les méthodes autorisées sur le firewall NETASQ. Il s'agit de méthodes d'authentification par défaut et elles correspondent à des mécanismes d'authentification différents. Chaque utilisateur peut avoir une méthode d'authentification différente mais elle doit avoir été sélectionnée dans cette fenêtre pour être utilisable.

LDAP	L'utilisateur doit saisir un couple identifiant/mot de passe. Ces informations transitent en SSL (si l'utilisateur se connecte au firewall en https avec son navigateur Internet). Cette méthode utilise le port 443. **AVERTISSEMENT** Cette méthode est la moins sécurisée car il est désormais possible d'accéder (frauduleusement) aux informations contenues dans un trafic SSL. Toutefois cela ne s'applique à la méthode SSL+Certificat.
Certificat (SSL)	L'utilisateur n'a pas besoin de saisir de couple identifiant/mot de passe mais un certificat numérique généré par la PKI interne du firewall doit être installé sur le poste utilisateur. Les informations sont chiffrées en SSL. L'utilisateur doit, pour s'authentifier, se connecter au firewall en https avec son navigateur Internet. Cette méthode utilise le port 443.
Certificat (Mode SSO)	Basée sur une utilisation de la méthode SSL dans un mode **SSO** (***Single Sign On***) permet la simplification des étapes d'authentification par la méthode SSL. En effet, le firewall reconnaît automatiquement la méthode d'authentification qui sera utilisée pour l'authentification de l'utilisateur.
SRP (natif et LDAP Hash)	Cette méthode utilise le protocole **SRP** (***Secure Remote Password***) pour lequel le mot de passe n'est jamais émis. L'utilisateur doit se connecter au firewall en https et saisir un couple identifiant/mot de passe. Cette méthode utilise le port 443 (port utilisé par l'applet Java SRP). Cette méthode inclue le SRP natif et le SRP_Hash.
RADIUS	Cette méthode est utilisée si l'authentification est relayée à un serveur RADIUS externe.
KERBEROS (utilisé avec Win 2k)	Cette méthode est utilisée si l'authentification est relayée à un serveur Kerberos externe.
SPNEGO	Cette méthode utilise le principe d'authentification unique permettant dans certaines conditions que lorsque l'utilisateur est authentifié sur un domaine grâce à l'ouverture de sa session, il soit aussi authentifié auprès du firewall.
NTLM (utilisé avec Win NT)	Cette méthode est utilisée si l'authentification est relayée à un serveur NTLM externe.

Méthode par défaut

Cette méthode est utilisée lorsqu'un utilisateur désirant s'authentifier n'est pas présent dans l'annuaire LDAP interne ou externe. Cette option vous permet, par exemple, d'avoir certaines fiches utilisateurs sur la base LDAP et d'autres sur un serveur RADIUS, Kerberos ou NTLM (dans ce cas, sélectionnez les options correspondantes).

Exemple

Si on sélectionne RADIUS, lorsqu'un utilisateur n'est spécifié dans la base LDAP, le firewall interrogera le serveur RADIUS.

Méthode de redirection par défaut du proxy HTTP

Lorsqu'une méthode de redirection par défaut du proxy HTTP est activé (SRP, Certificat ou SPNEGO), le mode SSO de cette méthode est activé. Par exemple dans le cas de la méthode d'authentification SRP en mode SSO, l'applet SRP du portail d'authentification présente le login et le mot de passe sur la page. En effet car quelles que soit les méthodes d'authentification c'est la méthode SRP en mode SSO qui sera utilisée.

Avancé

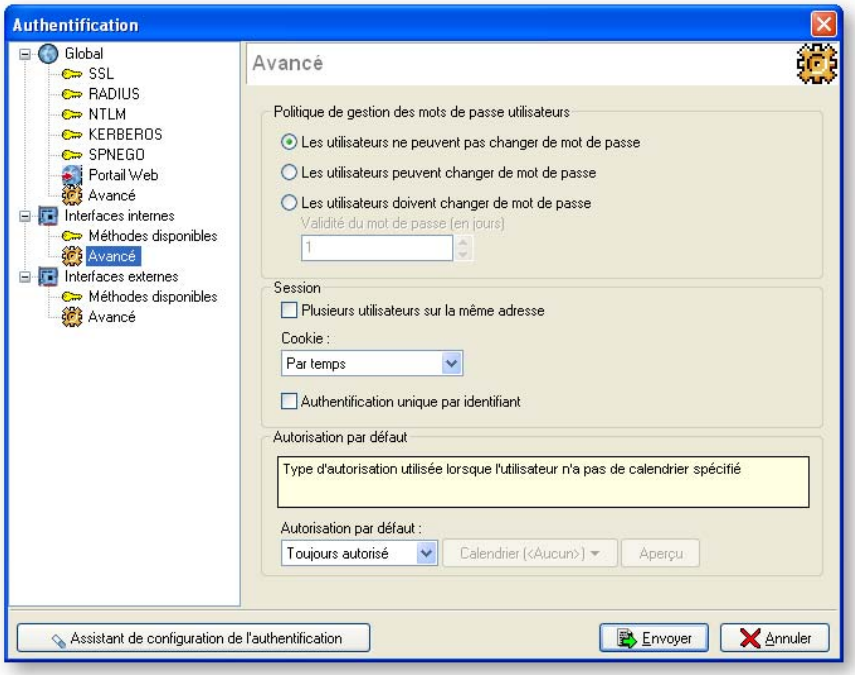


Figure 363 : Authentification - Avancé

Politique de gestion des mots de passe utilisateurs

Il existe trois possibilités de gestion des mots de passe utilisateurs sur les firewalls NETASQ.

- **Les utilisateurs ne peuvent pas changer de mot de passe** : en sélectionnant cette option, il sera impossible aux utilisateurs de modifier leur mot de passe d'authentification sur le firewall NETASQ.
- **Les utilisateurs peuvent changer de mot de passe** : en sélectionnant cette option, les utilisateurs peuvent modifier leur mot de passe d'authentification sans contrainte de temps et de validité.
- **Les utilisateurs doivent changer de mot de passe** : en sélectionnant cette option, les utilisateurs doivent changer leur mot de passe d'authentification à leur première connexion sur le portail d'authentification du firewall puis à chaque fois que la durée de validité du mot de passe est expiré. Cette durée est spécifiée en jours sans précision d'heure. Cela signifie que par exemple si la durée de validité du mot de passe de l'utilisateur est de 1 jour et que le mot de passe de l'utilisateur est initialisé une première fois le 27 juillet 2005 14:00, ce mot de passe doit être modifié dès le 28 juillet 2005 00:00 et non 24 heures plus tard.

Session

La section "Session" de la configuration de l'authentification est composé de trois options expliquées dans le tableau suivant :

- **Plusieurs utilisateurs sur la même adresse** : L'authentification NETASQ est basée sur l'enregistrement dans une table de l'ASQ d'une entrée qui associe un nom d'utilisateur à une adresse IP. Par défaut, il est impossible d'enregistrer plusieurs logins sur la même adresse IP. En cochant cette option, il est possible d'enregistrer plusieurs logins sur la même adresse IP permettant ainsi l'authentification d'utilisateurs différents situés derrière un équipement de NAT qui masquerait l'adresse réelle des utilisateurs par une adresse IP unique.
- **Cookie** : La gestion des cookies pour l'authentification des utilisateurs sur les

	firewalls permet une sécurisation de l'authentification prévenant par exemple les attaques par rejeu étant donné qu'il est indispensable de posséder le cookie de connexion pour être considéré comme authentifié. Par défaut les cookies sont définis "par Temps", ce qui signifie que les cookies ne sont négociés qu'une seule fois pour toute la durée d'authentification. Mais il est aussi possible de configurer les cookies "par Session", ce qui signifie que les cookies sont négociés à chaque instance du navigateur Web. Enfin il est possible de ne pas utiliser les cookies, mais cette option n'est pas recommandée car elle dégrade la sécurité de l'authentification. Les cookies sont indispensables pour le fonctionnement de l'option **Plusieurs logins sur la même adresse IP.** Les cookies sont négociés par navigateur Web. Ainsi si une authentification est réalisée avec Internet Explorer, elle ne sera pas effective avec Firefox ou d'autres navigateurs Web. • **Authentification unique par identifiant** : En cochant cette option, il est impossible pour un utilisateur de s'authentifier deux fois sur deux machines différentes.
Autorisation par défaut	Lorsqu'un utilisateur est créé ou lorsque des règles d'authentification le concernant sont mises en place, on associe à cet utilisateur un calendrier Ce dernier spécifie les zones horaires où l'utilisateur a le droit de s'authentifier. Pour toutes les autres zones, la connexion est refusée. Dans le cas où aucun calendrier ne correspond à un utilisateur, vous pouvez configurer plusieurs actions : • Toujours autorisé : L'utilisateur peut se connecter à toutes les heures, tous les jours définis par les règles de filtrage. • Toujours interdit : Quel que soit le résultat de l'authentification, la connexion est refusée. • Personnalisé : Vous avez la possibilité de spécifier un calendrier par défaut

12.1.3. Base de données LDAP

12.1.3.1. Introduction

DEFINITION

LDAP (***Lightweight Directory Access Protocol)*** est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP.

Le protocole LDAP définit la méthode d'accès aux données sur le serveur au niveau du client, et non la manière selon laquelle les informations sont stockées. Il présente les informations sous forme d'une arborescence d'informations hiérarchique appelée **DIT** (**Directory Information Tree**), dans laquelle les informations, appelées entrées (ou encore DSE, Directory Service Entry), sont représentées sous forme de branches.

Une branche située à la racine d'une ramification est appelée racine ou suffixe (en anglais root entry).

Chaque entrée de l'annuaire LDAP correspond à un objet abstrait ou réel

Exemple
Une personne, un objet matériel, des paramètres

Chaque entrée est constituée d'un ensemble de paires clés/valeurs appelées attributs.

12.1.3.2. Utilisation de LDAP dans les firewalls NETASQ

L'annuaire LDAP contient divers éléments de la configuration du firewall comme les utilisateurs, les groupes d'utilisateurs ou encore les profils du XVPN.
Les firewalls NETASQ embarquent, deux types d'annuaires LDAP : une base LDAP (Lightweight Directory Access Protocol) interne. Cette base permet de stocker les informations relatives aux utilisateurs devant s'authentifier pour passer au travers du firewall, une base LDAP externe qui se trouve sur une machine distante.

12.1.3.3. Assistant d'initialisation LDAP

L'assistant LDAP vous permettra de configurer facilement votre base de données LDAP.

Etape 1

Cette première étape de l'assistant de configuration de la base LDAP est accessible dans **`Authentification\Base de données LDAP`** lorsque la base LDAP n'est pas initialisée ou par un bouton sur l'écran de la configuration générale lorsque la Base LDAP est déjà initialisée.

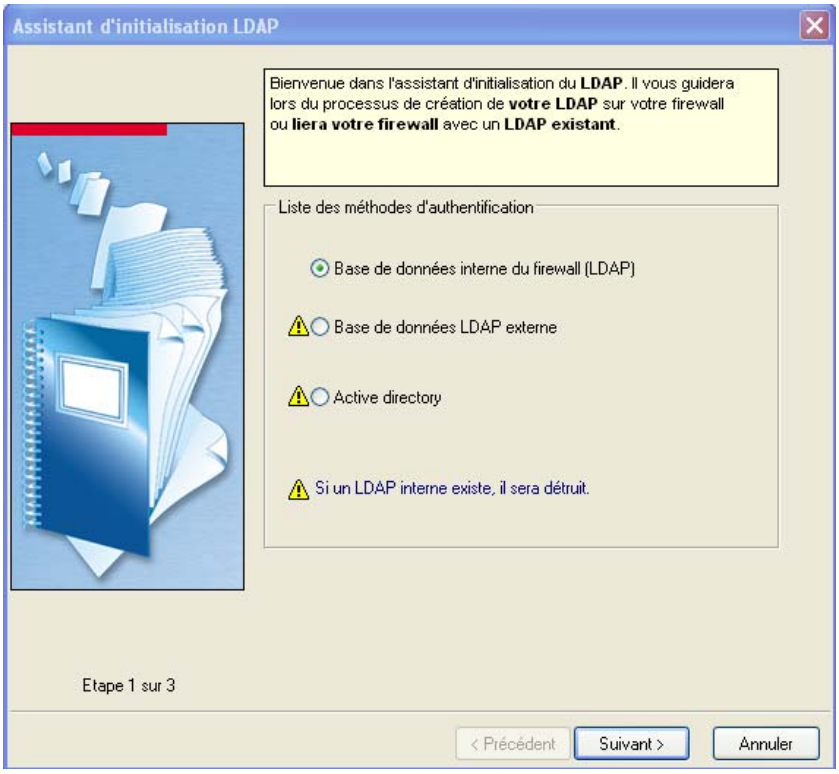


Figure 364 : Assistant lDAP - Etape 1

Lors de cette première étape, vous devez choisir si vous désirez créer un annuaire LDAP interne au firewall ou alors indiquer au firewall d'utiliser un annuaire externe que vous possédez déjà.

En fonction de votre choix, l'étape suivante est variable, la configuration d'un LDAP externe réclamant plus de renseignements.

Etape 2 : Annuaire interne

Lors de cette seconde étape, vous devez renseigner les informations générales concernant la base LDAP que vous désirez créer. Les informations saisies se retrouveront dans le schéma de l'annuaire LDAP de votre firewall.

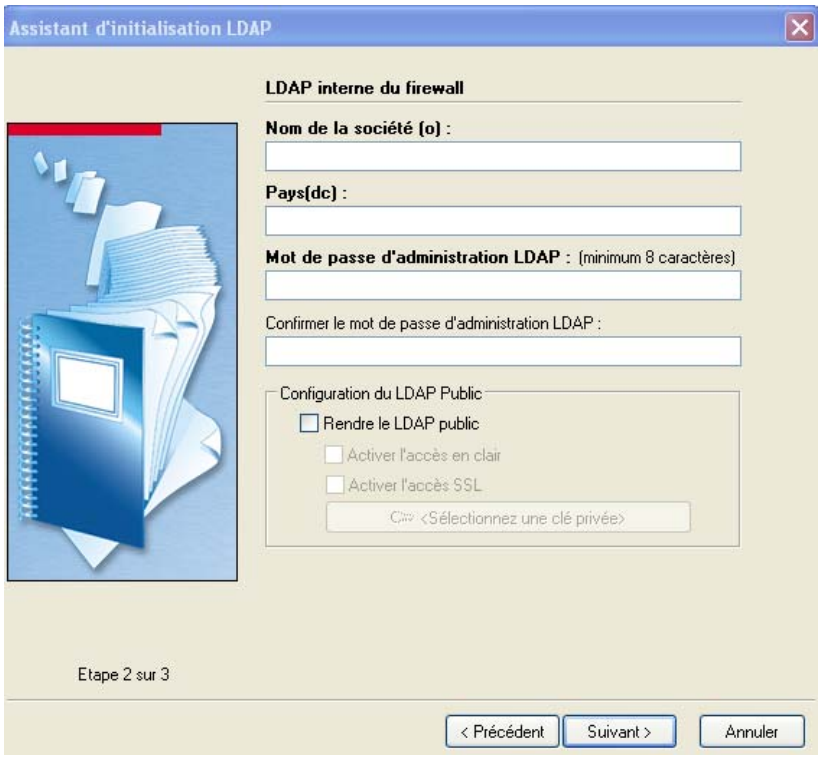


Figure 365 : Assistant d'initialisation LDAP - Etape 2

Nom de la société (o)	le nom de votre société (ex : NETASQ).
Pays (dc)	le domaine de votre société (ex : com).
Mot de passe d'administration LDAP	un mot de passe permettant au firewall de se connecter sur l'annuaire LDAP.
Confirmer le mot de passe d'administration LDAP	Confirmation du mot de passe d'administration LDAP
Rendre le LDAP public	Il est possible d'accéder de l'extérieur à l'annuaire LDAP. Deux méthodes sont disponibles : soit un accès en clair, soit un accès au moyen d'une authentification par Certificat (SSL). Il faut alors dans ce cas choisir le certificat désiré.

NOTE
Seul le mot de passe sera modifiable par la suite.

AVERTISSEMENT

Si l'accès externe n'est pas nécessaire, il est vivement conseillé de ne pas activer l'option **Rendre le LDAP public**.

Etape 2 : Annuaire externe

Dans certaines architectures, l'utilisation d'une base d'utilisateurs exploitable uniquement par le firewall peut devenir très rapidement trop contraignante. En effet, cela nécessite la gestion de multiples bases et une duplication manuelle des informations entre chacune des bases, les comptes utilisateurs ne sont pas centralisés. Ensuite, avec une base hermétique, il n'est pas possible de réutiliser les comptes utilisateurs déjà configurés sur d'autres bases.

Afin de remédier à cette limitation, les firewalls NETASQ offrent la possibilité de s'interfacer à des bases LDAP externes pour une intégration complète au sein du système d'information.

Lors de cette seconde étape, vous devez renseigner les informations générales concernant la base LDAP que vous possédez et que le firewall va consulter.

Cet assistant est décomposé en trois zones :

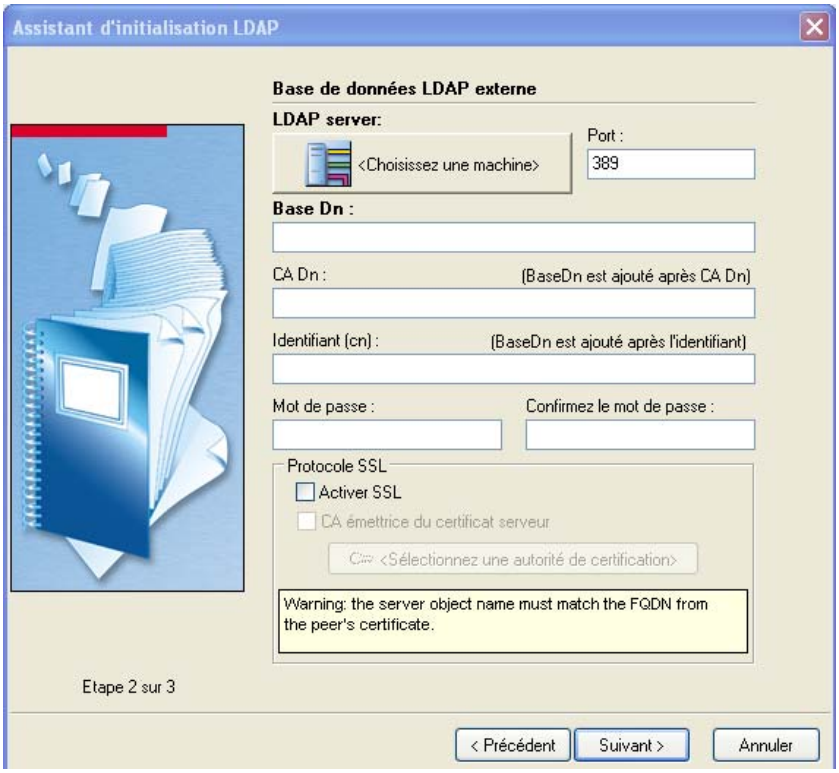


Figure 366 : Assistant d'initialisation LDAP - Etape 2

Configuration réseau du serveur LDAP externe

Vous devez choisir un objet correspondant à votre serveur LDAP. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur LDAP. Le choix du nom de l'objet doit correspondre au Common

Name du certificat de votre serveur LDAP dans le cas de l'utilisation du protocole SSL, sinon, le nom de l'objet a peu d'importance.

Vous devez renseigner le port d'écoute de votre serveur LDAP. Les ports par défaut sont :

- 389 pour une authentification en clair,
- 636 pour une authentification en SSL.

NOTE
Pour que le firewall NETASQ puisse utiliser un annuaire LDAP externe, il faut que cet annuaire intègre le schéma LDAP NETASQ. Pour intégrer ce schéma, contactez le support technique de NETASQ.

Configuration de la sécurité des communications

Si votre serveur LDAP est configuré pour supporter le SSL et que vous désirez que le firewall communique via SSL avec votre serveur vous devez cocher la case "Activer le SSL". Vous pouvez en option (en cochant la case "Envoyer un certificat au firewall" et en choisissant un fichier contenant le certificat de l'autorité) envoyer au firewall le Certificat de l'autorité ayant émis le certificat de votre serveur. Cela permet de vérifier la validité du certificat présenté par le serveur LDAP.

Configuration de la base LDAP

Base Dn	Vous devez renseigner le DN de la racine de votre annuaire (ex : o=NETASQ, dc=COM).
CA Dn	Ce champ est optionnel est sera uniquement utilisé si vous activez la PKI sur le firewall. Dans ce cas, le certificat et la CRL de l'autorité qui sera créée seront mis dans cette « fiche » LDAP. (ex : cn=Autorite Interne,ou=Autoritees de Certification).
Identifiant (cn)	Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des lectures/écritures sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. (ex : cn=Admin Firewall NETASQ).
Mot de passe	Le mot de passe pour permettre à l'utilisateur créé sur le firewall de se connecter sur le serveur LDAP.
Confirmez le mot de passe	Confirmation du mot de passe d'administration LDAP.
Protocole SSL	En cochant cette option, l'accès public au LDAP est protégé avec le protocole SSL. Si cette option n'est pas cochée, l'accès est non chiffré.

Etape 2 : Active directory (base Windows 2000 ou XP)

Lors de cette seconde étape, vous devez renseigner les informations générales concernant la Base Active Directory que vous possédez et que le firewall va consulter.

Cet assistant est décomposé en trois zones :

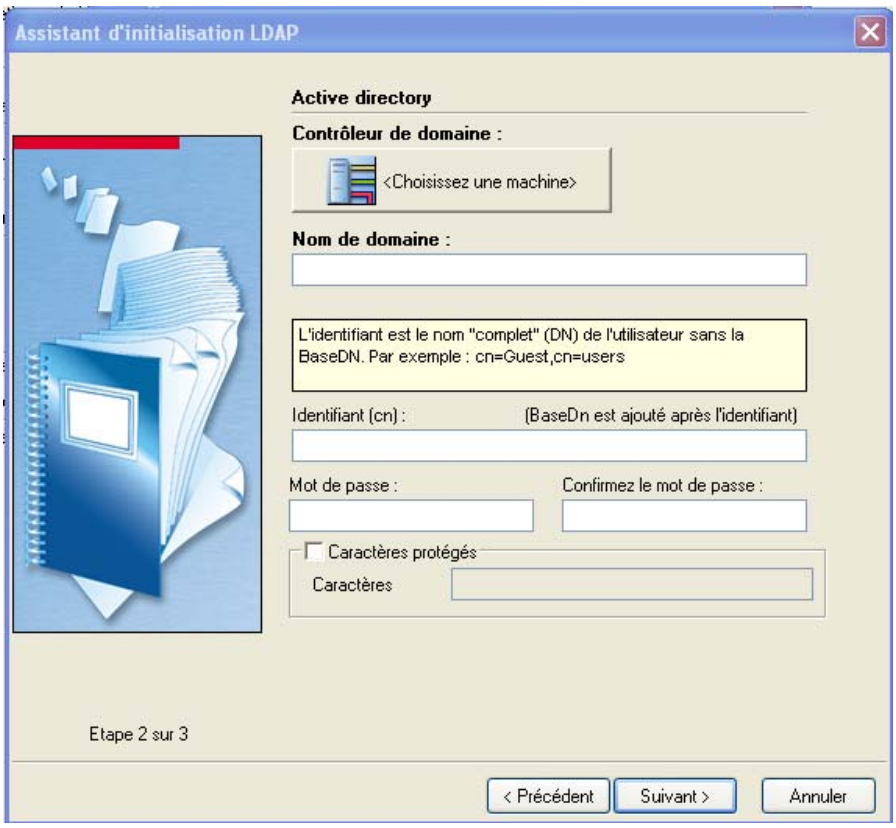


Figure 367 : Assistant d'initialisation LDAP - Etape 2

Contrôleur de domaine	Vous devez choisir un objet correspondant à votre serveur Active Directory. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur.
Nom de domaine	Vous devez renseigner le nom de domaine correspondant à la base Active Directory.
Identifiant (cn)	Un compte administrateur permettant au firewall de se connecter sur votre serveur Active Directory et d'effectuer des lectures/écritures sur certains champs. Nous vous recommandons de créer un compte spécifique sur la base Active Directory pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. (ex : cn=Admin Firewall NETASQ).
Mot de passe	Le mot de passe pour permettre à l'utilisateur créé sur le firewall de se connecter sur le serveur Active Directory.
Confirmez le mot de passe	Confirmation du mot de passe d'administration LDAP.
Caractères protégés	Pour certains serveurs externes, il est nécessaire d'ajouter un \ pour que les requêtes LDAP soient comprises.

Une fois l'assistant utilisé, vous pouvez accèder à chacun des écrans de configuration

12.1.3.3 Configuration de la base LDAP interne

L'écran de configuration de la base LDAP interne est accessible dans **Authentification\Annuaire LDAP**. Il vous permet de visualiser et de configurer votre base LDAP interne.

Onglet "LDAP interne"

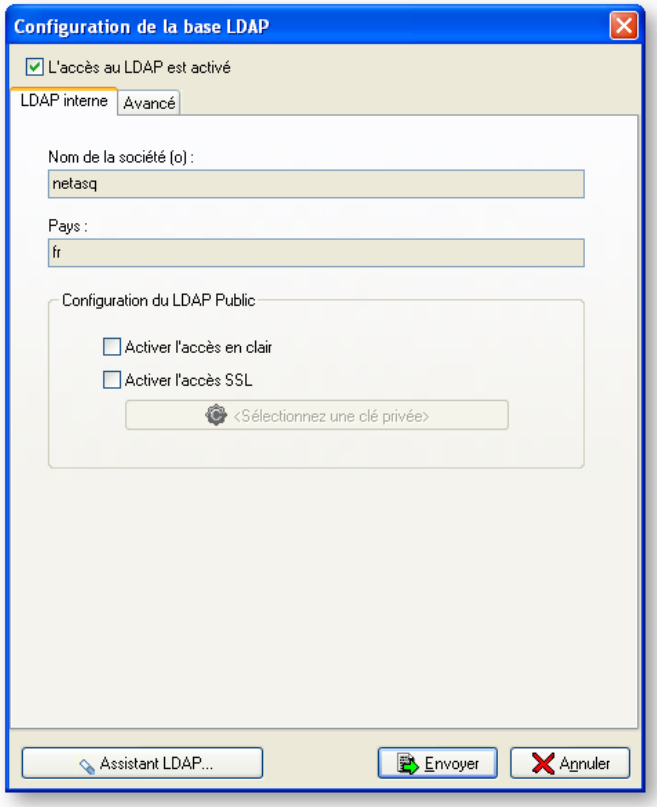


Figure 368 : Configuration de la base LDAP - LDAP interne

Il se décompose en trois parties :

- Une case à cocher indiquant le statut actuel de l'accès à l'annuaire LDAP. Si la case est cochée l'accès est actuellement actif, sinon, vous pouvez cocher cette case pour l'activer. Cela permet d'activer et de désactiver l'accès à l'annuaire LDAP sans pour autant détruire la configuration.
- Une zone d'onglet et la fenêtre correspondant à l'onglet choisi. Les onglets disponibles vous permettent respectivement de visualiser la configuration actuelle de la base LDAP et de visualiser et modifier les paramètres avancés de votre configuration.
- Une zone en bas à droite avec trois boutons vous permettant d'initialiser votre annuaire LDAP, d'envoyer vos modifications au firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

Nom de la société (o)	Le nom de votre société (ex : NETASQ).
Pays	Le domaine de votre société (ex : com).
Configuration du LDAP Public	Il est possible d'accéder de l'extérieur à l'annuaire LDAP. Deux méthodes sont disponibles : soit un accès en clair, soit un accès au moyen d'une authentification par Certificat (SSL). Il faut alors dans ce cas choisir le certificat désiré.

NOTE
Seul le mot de passe sera modifiable par la suite.

AVERTISSEMENT
Si l'accès externe n'est pas nécessaire, il est vivement conseillé de ne pas activer l'option "Configuration du LDAP public".

Onglet "Avancé"

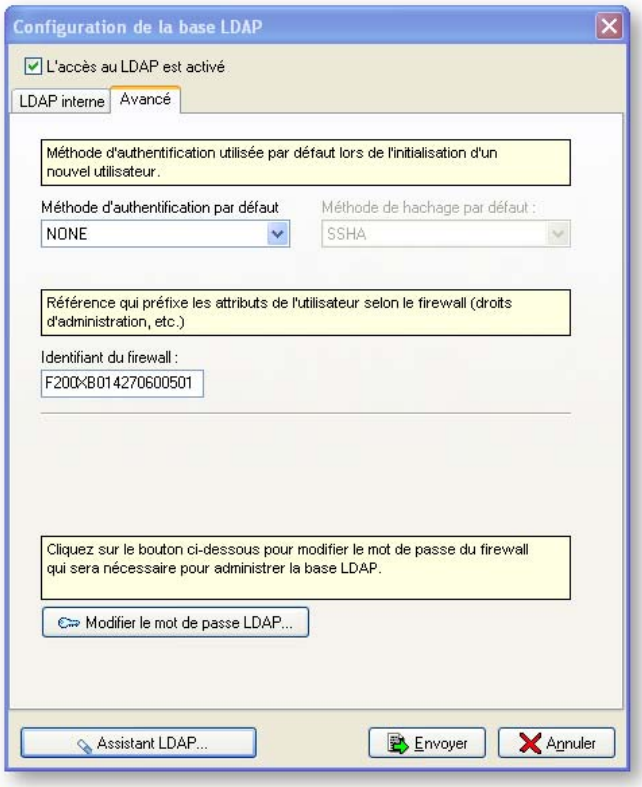


Figure 369 : Configuration de la base LDAP - Avancé

Cet onglet permet de configurer les paramètres d'authentification des utilisateurs qui seront créés par la suite et de modifier le mot de passe de l'administrateur de la base LDAP.

Méthode d'authentification par défaut

Les différentes méthodes d'authentification disponibles sont les suivantes :

- **NONE** : les utilisateurs ne pourront pas s'authentifier.
- **LDAP** : l'authentification sera effectuée par transmission au firewall du mot de passe de l'utilisateur via un tunnel protégé (HTTPS) ou directement (HTTP).
- **SSL** : les utilisateurs devront présenter au firewall un certificat valide pour s'authentifier.
- **SRP** : cette méthode permet la non transmission du mot de passe utilisateur au firewall, elle est basée sur un protocole de défi-réponse. Désormais, lorsque cette méthode est utilisée, le nom DNS est utilisé plutôt que l'adresse IP du firewall.
- **SRP_LDAP** : cette méthode est identique à la précédente, à ceci près qu'elle utilise le mot de passe LDAP existant de l'utilisateur pour générer une clé éphémère SRP et permettre l'authentification SRP
- **RADIUS** : cette méthode permet d'authentifier les utilisateurs sur un serveur RADIUS. Le mot de passe est transmis au firewall de la même manière que pour la méthode LDAP
- **KERBEROS** : cette méthode permet d'authentifier les utilisateurs sur un serveur Kerberos
- **NTLM** : cette méthode permet d'authentifier les utilisateurs sur un serveur NTLM.

AVERTISSEMENT

La méthode d'authentification SRP est l'une des plus sécurisées, nous vous en recommandons l'utilisation. La méthode d'authentification SRP_LDAP est très intéressante lorsque l'annuaire LDAP est externe et que les utilisateurs possèdent déjà un mot de passe. Dans ce cas, elle permet d'obtenir une grande sécurité sans modifier l'existant.

Méthode de hachage par défaut

Certaines méthodes d'authentification **(SRP_LDAP, LDAP)** doivent stocker le mot de passe utilisateur sous la forme d'un hash (résultat d'une fonction de hachage appliquée au mot de passe) qui évite le stockage en clair de ce mot de passe. Dans ce cas, vous devez choisir la méthode de hash désirée :

- **NONE** : pas de hash, le mot de passe est stocké en clair (Peu recommandé).
- **MD5** : le mot de passe est hashé avec l'algorithme MD5.
- **SMD5** : le mot de passe est hashé avec l'algorithme Salt MD5. Cette variante du MD5 utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes.
- **SHA** : le mot de passe est hashé avec l'algorithme SHA-1.
- **SSHA** : le mot de passe est hashé avec l'algorithme Salt SHA-1. Cette variante du SHA-1 utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes.
- **CRYPT** : le mot de passe est protégé par l'algorithme CRYPT. Il s'agit ici de la méthode native de CRYPT qui est dérivée de l'algorithme DES. A ne pas confondre avec le CRYPT UNIX qui permet l'utilisation de divers algorithmes en fonction de l'OS.

AVERTISSEMENT

La méthode de hash la plus sécurisée est **SSHA**. Nous vous en recommandons l'utilisation. La méthode **SRP** stocke également des informations pour authentifier les utilisateurs, mais ces informations sont sous la forme d'une clé Diffie-Hellman et d'une graine aléatoire. Ces deux informations sont stockées dans des champs du schéma LDAP NETASQ.

Identifiant du

Tous les utilisateurs de la base LDAP sont préfixés du numéro de série du firewall sur lequel la base LDAP a été créée (préfixe par défaut). Mais lorsque le firewall est

firewall	remplacé ou lorsque la configuration de la base LDAP est sauvegardée puis restaurée sur un autre firewall, le préfixe par défaut n'est alors plus valide. Cette option permet de spécifier un préfixe non attaché au firewall.
Modifier le mot de passe LDAP…	Cette option permet de modifier le mot de passe de configuration de la base LDAP.

Assistant LDAP interne

L'assistant LDAP vous permettra de configurer facilement votre base de données LDAP.

Etape 1
Cette première étape de l'assistant de configuration de la base LDAP est accessible dans **`Authentification\Annuaire LDAP`** lorsque la base LDAP n'est pas initialisée ou par un bouton sur l'écran de la configuration générale lorsque la Base LDAP est déjà initialisée.

Lors de cette première étape, vous devez choisir si vous désirez créer un annuaire LDAP interne au firewall ou alors indiquer au firewall d'utiliser un annuaire externe que vous possédez déjà.

En fonction de votre choix, l'étape suivante est variable, la configuration d'un LDAP externe réclamant plus de renseignements.

Etape 2 : Annuaire interne
Lors de cette seconde étape, vous devez renseigner les informations générales concernant la base LDAP que vous désirez créer. Les informations saisies se retrouveront dans le schéma de l'annuaire LDAP de votre firewall.

12.1.3.4. Configuration de la base LDAP externe

Onglet "LDAP externe" (pour un LDAP externe ou Active Directory)

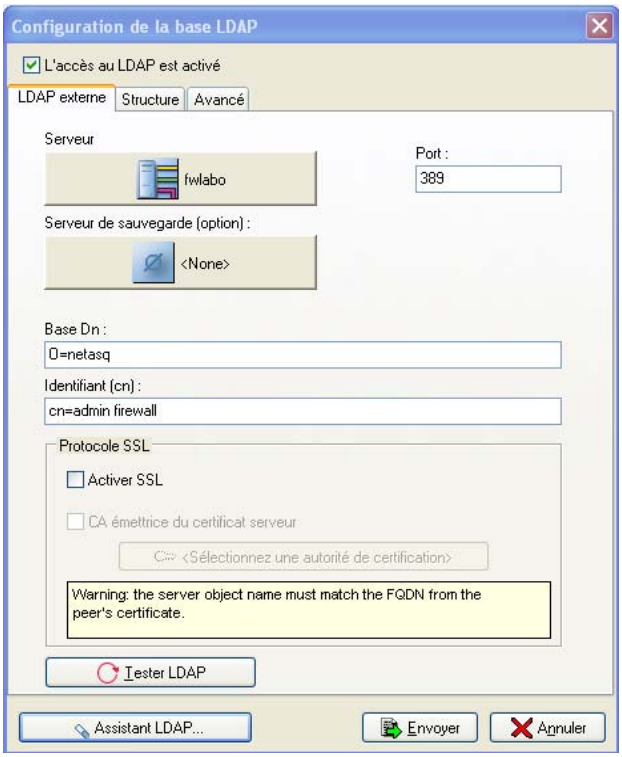


Figure 370 : Configuration de la base LDAP - LDAP externe

Configuration réseau du serveur LDAP externe

Vous devez choisir un objet correspondant à votre serveur LDAP. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur LDAP. Le choix du nom de l'objet doit correspondre au Common Name du certificat de votre serveur LDAP dans le cas de l'utilisation du protocole SSL, sinon, le nom de l'objet a peu d'importance.

Vous devez renseigner le port d'écoute de votre serveur LDAP. Les ports par défaut sont :

- 389 pour une authentification en clair,
- 636 pour une authentification en SSL.

Il est possible de configurer un serveur de Backup externe. La configuration de serveur de backup est soumise aux mêmes exigences de configuration que le serveur LDAP externe « principal ».

Configuration de la sécurité des communications

Si votre serveur LDAP est configuré pour supporter le SSL et que vous désirez que le firewall communique via SSL avec votre serveur vous devez cocher la case "Activer SSL". Vous pouvez en option (en cochant la case "CA émettrice du certificat serveur" et en choisissant un fichier contenant le certificat de l'autorité) envoyer au firewall le Certificat de l'autorité ayant émis le certificat de votre serveur. Cela permet de vérifier la validité du certificat présenté par le serveur LDAP.

Configuration de la base LDAP

Base Dn	Vous devez renseigner le DN de la racine de votre annuaire (ex : o=NETASQ, dc=COM).
Identifiant (cn)	Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des lectures/écritures sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. (ex : cn=Admin Firewall NETASQ).

Le bouton **Tester LDAP** permet de vérifier que le LDAP externe est bien accessible.

Onglet "Structure"

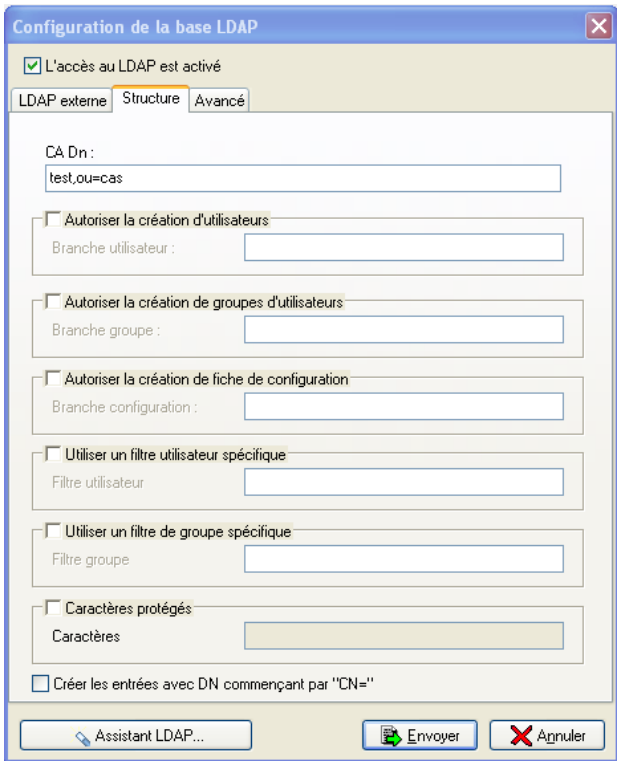


Figure 371 : Configuration de la base IDAP - Structure

Cet onglet est ajouté lorsqu'une base LDAP externe ou Active Directory est utilisée.

Les options de cet onglet vous permettent d'ajouter, dans la base LDAP externe ou Active Directory, les fiches utilisateurs créées dans la configuration des objets. Les utilisateurs et les groupes seront chacun stockés dans une branche spécifique de l'annuaire LDAP ou Active Directory.

CA Dn	Ce champ définit l'emplacement de l'autorité de certification présente dans la base LDAP externe ou Active Directory. Cet emplacement est notamment utilisé lors de la recherche de la CA utilisé pour la méthode d'authentification SSL. Il n'est pas indispensable de configurer ce champ mais dans ce cas, pour que la méthode d'authentification SSL fonctionne, il faut spécifier la CA dans la liste des CA de confiance dans la configuration de la méthode SSL (Voir «Méthode d'authentification SSL»).
Autoriser la création d'utilisateurs	Donnez le nom de la branche LDAP pour stocker les utilisateurs. Exemple : ou=users.
Autoriser la création de groupes d'utilisateurs	Donnez le nom de la branche LDAP pour stocker les groupes d'utilisateurs. Exemple : ou=groups.
Autoriser la création de fiche de configuration	Donnez le nom de la branche LDAP pour stocker les configurations. Exemple : ou=configuration.
Utiliser un filtre utilisateur spécifique	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à ObjectClass = InetOrgPerson.
Utiliser un filtre de groupe spécifique	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à ObjectClass = GroupOfNames.
Caractères protégés	Pour certains serveurs externes, il est nécessaire d'ajouter un \ pour que les requêtes LDAP soient comprises.
Créer les entrées avec DN commençant par « CN= »	…

Onglet "Avancé"

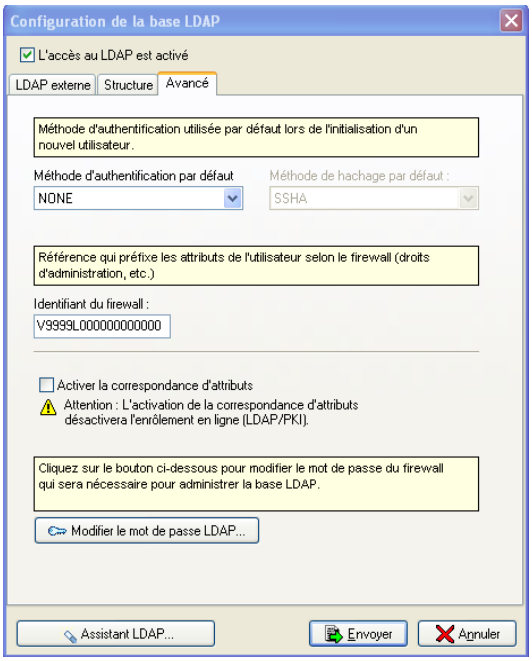


Figure 372 : Configuration de la base LDAP - Avancé

L'onglet `Avancé` pour une configuration de base externe possède une option supplémentaire : **Activer la correspondance d'attributs**. Cette option permet d'activer le mapping (ou correspondance) entre les objets du schéma LDAP NETASQ, utilisés par le firewall, et les objets d'un autre annuaire. Lorsque cette option est cochée, un nouvel onglet (onglet `Correspondance d'attributs`) apparaît.

Onglet "Correspondance d'attributs"

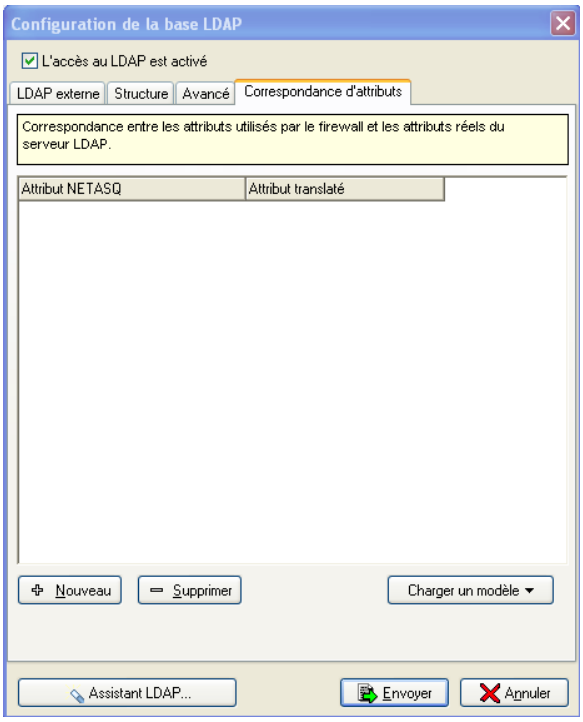


Figure 373 : Configuration de la base LDAP - Correspondance d'attibuts

Cet onglet est ajouté lorsqu'une base LDAP externe ou Active Directory est utilisée et que l'option **Activer la correspondance d'attributs** de l'onglet `Avancé` est cochée (par défaut).

Les options de cet onglet vous permettent d'indiquer la correspondance entre les attributs utilisés par NETASQ et ceux utilisés dans la base externe.

Par exemple : le NETASQ attribute <uid> = l'Active Directory attribute <sAMAccountName>

Vous pouvez ajouter ou supprimer des correspondances d'attributs grâce aux boutons **Nouveau** et **Supprimer**.

Charger un template

Ce bouton vous permet de spécifier une liste de correspondance, déjà définie par NETASQ, avec des produits du marché (Active Directory, OpenDirectory…).

PARTIE 13 : PKI

CHAPITRE 1. PRESENTATION

13.1.1. Qu'est-ce que c'est ?

DEFINITION

La PKI ou Public Key Infrastructure (infrastructure à clé publique) est un système cryptographique (basé sur la cryptographie asymétrique). Elle utilise des mécanismes de signature et certifie des clés publiques (en associant une clé à un utilisateur) qui permettent de chiffrer et de signer des messages ainsi que des flux de données, afin d'assurer confidentialité, authentification, intégrité et non-répudiation.

Ces quatre notions (confidentialité, authentification, intégrité et non-répudiation) sont les bases de toutes solutions de sécurité. Toutefois, elles ne sont pas développées dans la suite de ce document. Si vous sentez le besoin d'approfondir vos connaissances sur ces concepts, un ouvrage générique sur la sécurité vous apportera les bases nécessaires à leur compréhension.

13.1.2. Principe

La PKI est un système basé sur une autorité de confiance (votre firewall NETASQ par exemple) qui signe et délivre des certificats contenant une bi-clé associée à des informations propriétaires à un utilisateur.

Ces certificats sont de véritables passeports électroniques qui servent à l'authentification des utilisateurs. De plus, ils contiennent les clés de chiffrement et déchiffrement qui garantissent la confidentialité des données.

13.1.3. Intérêt de la PKI

Une infrastructure à clé publique est une couche de sécurité supplémentaire par rapport à un système d'authentification "simplement" basé sur un annuaire LDAP. La bi-clé, le certificat, l'autorité de confiance sont utilisés pour sécuriser les échanges sur l'Internet.

Le certificat est une alternative "sympathique" aux systèmes de log on car l'utilisateur n'a plus à retenir de mot de passe. En effet la portabilité du certificat lui permet d'être intégré dans des solutions du type clé USB par exemple.

De la même façon le certificat peut être utilisé pour les tunnels VPN. Il n'est plus nécessaire de partager un secret qu'il est difficile de s'échanger à l'abri des regards indiscrets du monde du web.

13.1.4. Général

Les produits NETASQ possèdent une PKI interne (sauf les modèles U30 et U70), vous permettant de créer des certificats numériques pour vos utilisateurs. Ces certificats peuvent être utilisés pour l'authentification des utilisateurs au travers du firewall, pour l'authentification VPN. Ils peuvent aussi être utilisés par des applications de votre système d'information.

Cette fenêtre est accessible dans **PKI\Général**. Elle vous permet de visualiser et de configurer votre PKI après l'avoir initialisée.

Elle se décompose en deux parties :

- Une zone d'onglets et la fenêtre correspondant à l'onglet choisi. Les onglets disponibles vous permettent respectivement de visualiser les informations de votre configuration, de modifier certaines options, de visualiser les informations de votre PKI
- Une zone en bas à droite avec deux boutons vous permettant d'envoyer vos modifications au firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

Si vous accédez à cette section pour la première fois, vous devrez configurer la PKI en utilisant l'assistant PKI.

CHAPITRE 2. ASSISTANT PKI

Cet assistant se lance automatiquement lors du premier accès au menu **PKI\Général** ou lorsque vous cliquez sur le bouton **Assistant de création de PKI** sur l'écran de configuration générale.

Etape 1 : Bienvenue

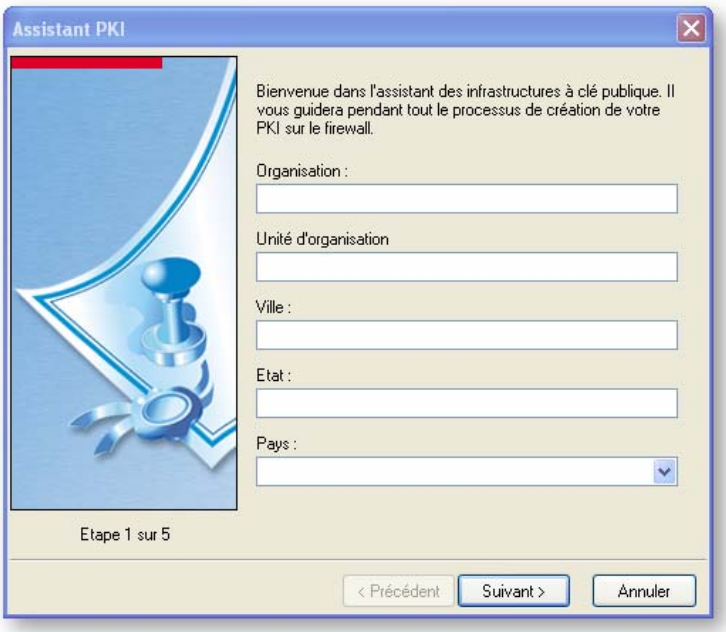


Figure 374 : Assistant PKI - Etape 1

Lors de cette première étape, vous devez renseigner les informations générales concernant la PKI que vous voulez mettre en œuvre. Les informations saisies se retrouveront dans le certificat de votre autorité de certification et dans les certificats de vos utilisateurs.

Organisation	Nom de votre société (ex : NETASQ).
Unité d'organisation	"branche" de votre société (ex : INTERNE).
Localité	Ville de votre société (ex : Villeneuve d'Ascq).
Département	Département géographique de votre société (ex : Nord).
Pays	Choisissez dans la liste le pays de la société (ex : France).

Etape 2 : Mot de passe

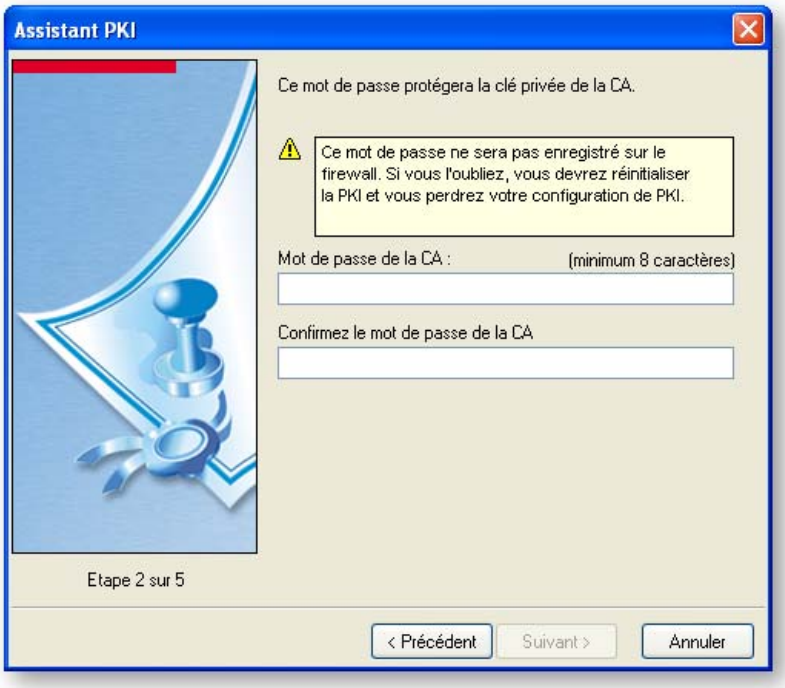


Figure 375: Assistant PKI - Etape 2

Dans cette seconde étape du wizard de configuration de la PKI, vous devez renseigner un mot de passe (au minimum huit caractères) qui va permettre la protection de la clé privée de votre autorité de certification.
Le compte Admin peut supprimer la PKI existante sans avoir à fournir de mot de passe. Par contre, les autres comptes d'administration devront fournir ce mot de passe. Ceci permet de recréer une PKI en cas de perte de mot de passe.

AVERTISSEMENT
Le choix d'un mot de passe trop simple est déconseillé. Nous vous recommandons de mélanger les lettres minuscules, majuscules, les chiffres, les caractères spéciaux.

L'initialisation de la PKI prend un certain temps afin de générer l'autorité de certfication interne.

Etape 3 : Autorité de certification, utilisateur, taille de clé

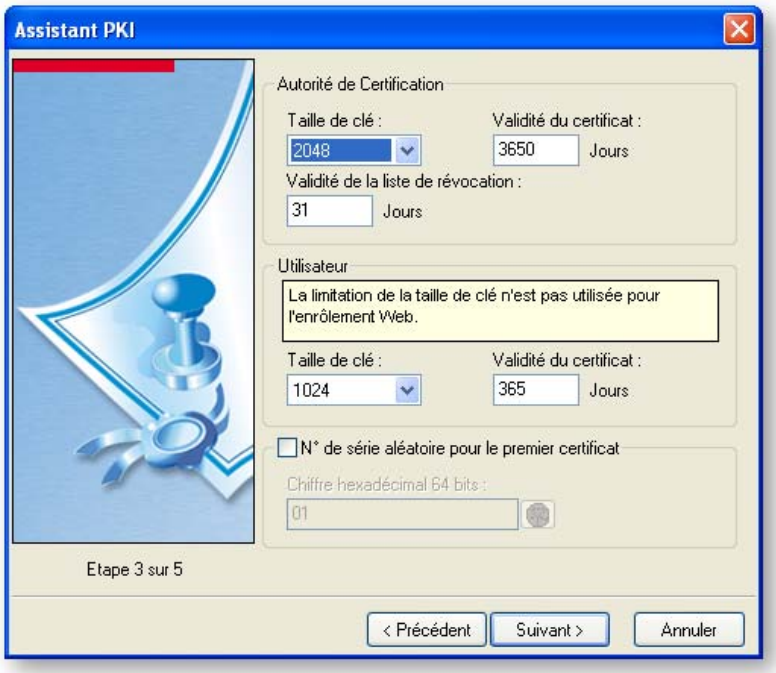


Figure 376 : Assistant PKI - Etape 3

Dans la troisième étape du wizard de configuration de la PKI, vous devez renseigner la configuration concernant le matériel cryptographique de votre PKI.

Cette étape est décomposée en deux :

- Configuration du matériel cryptographique pour l'autorité de certification.
- Configuration du matériel cryptographique pour les utilisateurs.

Matériel cryptographique pour l'autorité de certification :

Taille de clé : taille de la clé de votre autorité exprimée en bits. Cette valeur ne sera pas modifiable par la suite. Plus la taille est grande, plus la sécurité est importante.

Validité du certificat : le nombre de jours durant lesquels votre certificat d'autorité et par conséquent votre PKI seront valide. Cette date influe sur tous les aspects de votre PKI, en effet, une fois ce certificat expiré, tous les certificats utilisateurs le seront également. Cette valeur ne sera pas modifiable par la suite.

Validité de la liste de révocation : le nombre de jours durant lesquels votre CRL sera valide.

AVERTISSEMENT
Il est normal de mettre à jour régulièrement votre CRL et donc de ne pas mettre une date trop importante pour la validité de votre CRL. Cette valeur sera modifiable par la suite.

Matériel cryptographique pour les utilisateurs :

Taille de clé : taille de la clé pour vos utilisateurs exprimée en bits. Cette valeur sera modifiable par la suite.

Validité du certificat : le nombre de jours durant lesquels les certificats utilisateurs seront valides. Cette valeur sera modifiable par la suite.

Numéro de série aléatoire pour le premier certificat

Cette fonctionnalité permet de définir manuellement ou de façon aléatoire le premier numéro de certificat généré par la PKI. Ainsi le nombre de certificats générés par la PKI est invisible à une tierce personne.

> **Exemple**
> Si le premier numéro est 10245 et que l'administrateur génère 15 certificats, le quinzième certificat porte donc le numéro 10259 et il est impossible de savoir s'il y a eu 10259 certificats effectivement générés.

Le champ **Chiffre hexadécimal 64 bits** permet de spécifier le numéro du premier certificat généré sous la forme d'un nombre hexadécimal de 64 bits. Le bouton représentant un dé génère ce nombre de façon aléatoire.

Etape 4 : CRL

Figure 377 : Assistant PKI - Etape 4

Dans cette étape de l'assistant de configuration de la PKI, vous devez renseigner la configuration concernant la distribution de la CRL. Cette information sera intégrée aux certificats générés et permettra aux applications utilisant le certificat de récupérer automatiquement la CRL afin de vérifier la validité du certificat.

Dans le cas de l'utilisation de la PKI interne, il est fortement recommandé d'exporter la CA et la CRL NETASQ sur un serveur Web (voir onglet ***Autorité***) et de spécifier ici l'URL de ces deux fichiers stockés sur le serveur Web. Cette opération doit être réalisée régulièrement afin que la CRL à disposition sur le serveur Web soit la plus à jour possible. Une fois les champs **Protocole** et **URL** renseignés, il faut cliquer sur le bouton **Ajouter** pour créer le point de distribution.

Protocole protocole utilisé pour la diffusion de la CRL.

URL	adresse du lieu de distribution de la CRL.
Liste des points de distribution	liste de tous les points de distribution configurés avec les deux champs précédents.

Etape 5 : Enrôlement des utilisateurs

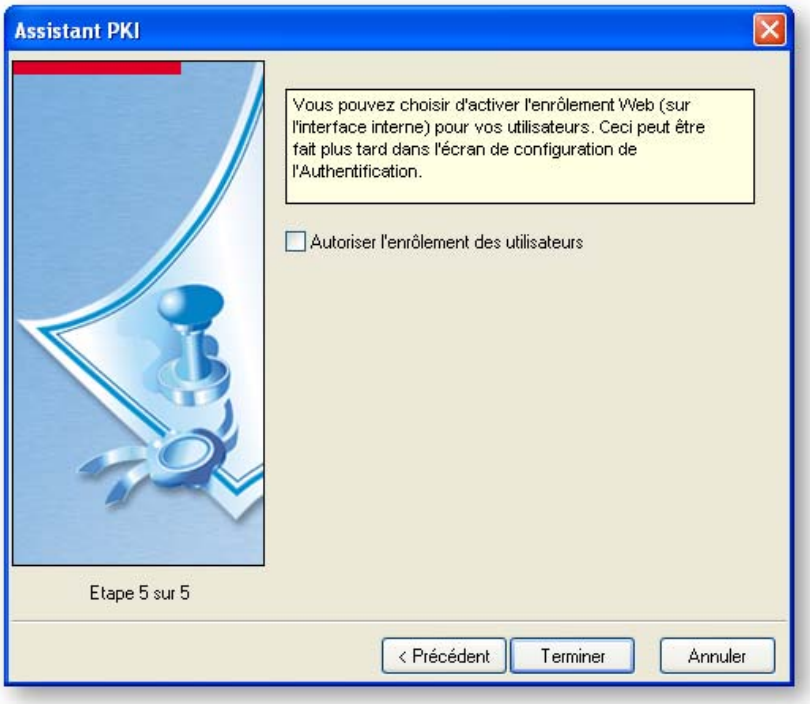


Figure 378 : Assistant PKI - Etape 5

Dans cette dernière étape de la configuration de la PKI NETASQ, il s'agit de spécifier si l'enrôlement des utilisateurs est autorisé en sélectionnant l'option **Autoriser l'enrôlement des utilisateurs**.

CHAPITRE 3. CONFIGURATION DE LA PKI

13.3.1. Onglet Global

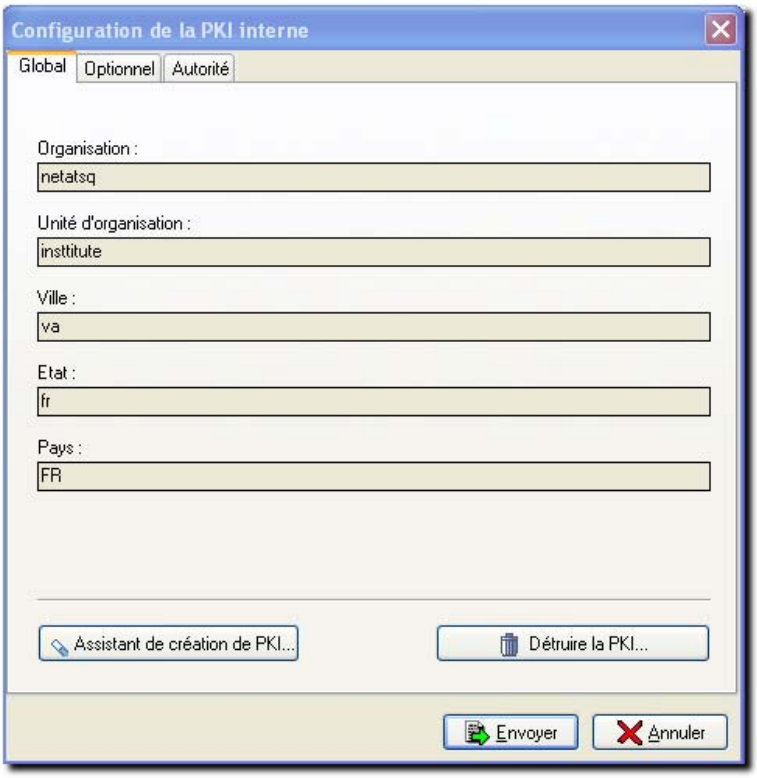


Figure 379 : Configuration de la PKI interne - Global

Cet écran est décomposé en trois parties :

- Une zone informative sur la configuration actuelle de la PKI. Les informations affichées sont celles renseignées durant la première étape du Wizard d'initialisation de la PKI.
- Une zone contenant deux boutons permettant d'initialiser une nouvelle PKI (détruit la PKI actuelle), de détruire la PKI actuelle.
- Une zone en bas à droite avec deux boutons vous permettant d'envoyer vos modifications au firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

AVERTISSEMENT

Le compte "admin" vous permet de détruire une PKI sans indiquer le mot de passe de l'autorité de certification. Cette fonctionnalité permet à l'administrateur de détruire une PKI même s'il oublie ce mot de passe.

13.3.2. Onglet Optionnel

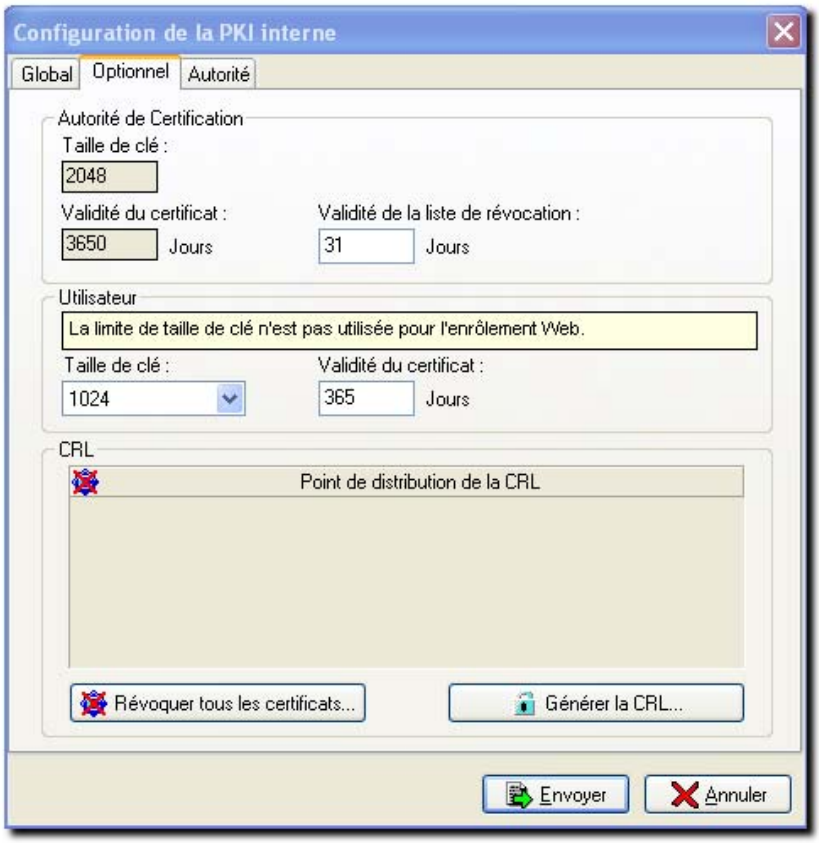


Figure 380 : Configuration de la PKI interne - Optionnel

Cet onglet est décomposé en cinq parties :

- Une zone informative sur la configuration du matériel cryptographique pour l'autorité de certification. Les informations affichées sont celles renseignées durant la seconde étape du Wizard d'initialisation de la PKI. La validité de la CRL peut être modifiée.
- Une zone informative sur la configuration du matériel cryptographique pour les utilisateurs. Les informations affichées sont celles renseignées durant la seconde étape du Wizard d'initialisation de la PKI. Les champs de cette zone peuvent être modifiés.
- Une zone informative sur les points de distribution de CRL.
- Une zone contenant deux boutons permettant de révoquer tous les certificats utilisateurs. Dans ce cas, les certificats utilisateurs deviennent inutilisables, et de générer une nouvelle CRL.
- Une zone en bas à droite avec deux boutons vous permettant d'envoyer vos modifications au firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

13.3.3. Onglet Autorité

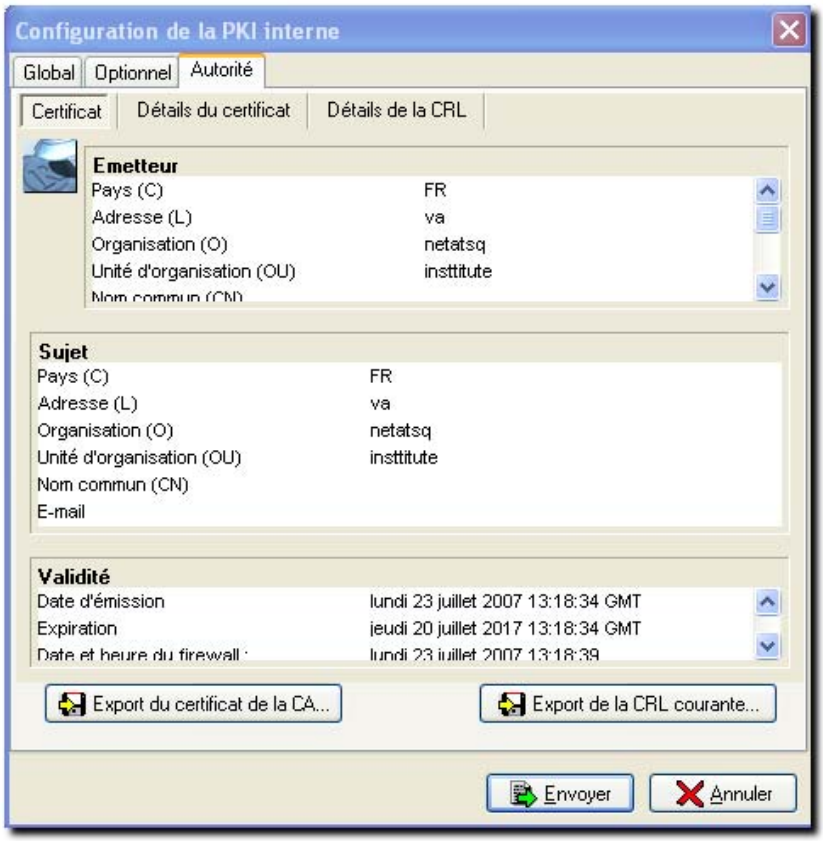


Figure 381 : Configuration de la PKI interne - Autorité

Cet onglet est décomposé en trois parties :

- Une zone contenant trois onglets permettant d'obtenir : Une vision générale du contenu du certificat (Onglet **Certificat).** Le contenu complet du certificat (Onglet **Détails du certificat**).Le contenu complet de la CRL (Onglet **Détails de la CRL**). Vous pouvez voir les certificats qui ont été révoqués.
- Une zone contenant deux boutons permettant d'exporter le certificat de l'autorité de certification au format .**DER** et d'exporter la CRL de l'autorité de certification au format **.CRL**.
- Une zone en bas à droite avec deux boutons vous permettant d'envoyer vos modifications au firewall ou de quitter cette fenêtre sans prendre en compte les modifications.

CHAPITRE 4. LISTE DES REQUETES UTILISATEURS

Lorsque l'authentification est activée, l'utilisateur doit passer par une phase de reconnaissance avant de pouvoir tenter une connexion au travers du firewall. Deux cas peuvent se présenter :

13.4.1. Le filtrage d'URL est activé sur le firewall

Lorsque le filtrage d'URL et l'authentification sont activés au niveau du firewall, l'utilisateur n'a pas besoin de se connecter au firewall pour s'authentifier. La page d'authentification lui sera automatiquement envoyée lorsqu'il voudra se connecter à un site Web. L'utilisateur sera alors authentifié pour tous les services auquel il est autorisé et pendant toute la période d'authentification.

13.4.2. Le filtrage d'URL n'est pas activé au niveau du firewall

Dans ce cas, l'utilisateur doit s'authentifier sur le firewall avant de tenter une connexion nécessitant l'authentification. L'utilisateur doit se connecter au firewall via son navigateur Internet, l'URL à utiliser est la suivante : https://<adresse IP du firewall>.

> **Exemple**
>
> https://10.0.0.254

13.4.3. Missions de l'administrateur

L'administrateur est le garant du bon usage des fonctionnalités d'authentification offertes par les équipements de son réseau et en particulier par son UTM NETASQ. Dans ce cadre, NETASQ rappelle que la sensibilisation des utilisateurs à l'utilisation des pages d'authentification permet d'éviter leur mauvais usage.

Cette sensibilisation comprend :

- Une aide à la définition de mots de passe ayant une entropie élevée (Cf. Partie 13/Chapitre 6 : Sensibilisation des utilisateurs).
- Une formation à l'utilisation des fonctionnalités des pages d'authentification.
- Une sensibilisation aux enjeux de la sécurité des ressources, des biens et des personnes.

13.4.4. Login

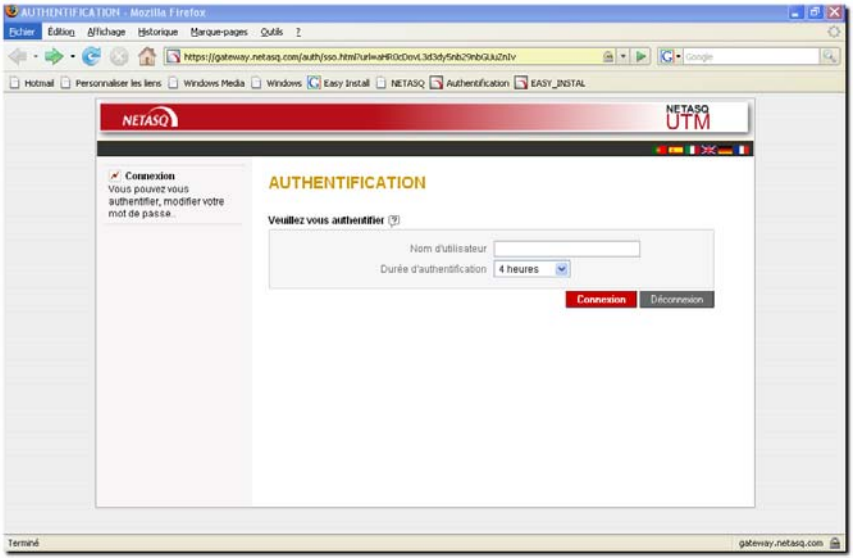


Figure 382 : Identifiant portail

Dans les deux cas, pour s'authentifier, l'utilisateur doit saisir son login et la durée pendant laquelle il souhaite être authentifié, puis cliquez sur **Connexion**. Lorsque cette période est écoulée, l'utilisateur doit se ré-authentifier.

> **AVERTISSEMENT**
> Ne pas mettre une durée trop longue pour des raisons de sécurité (l'utilisateur pourrait quitter son poste de travail sans le verrouiller et se faire intercepter sa session).

Selon la méthode choisie pour l'utilisateur, ce dernier doit ensuite, soit saisir son mot de passe, soit choisir un certificat numérique.

- **Pour la méthode LDAP** : saisie du mot de passe.
- **Pour la méthode certificat (SSL)** : choix d'un certificat (ce certificat doit au préalable avoir été installé sur le poste de l'utilisateur).
- **Pour la méthode SRP** : saisie du mot de passe (une applet Java est lancée et permet d'utiliser le nom DNS plutôt que l'adresse IP du firewall. L'authentification est donc désormais possible même lorsque l'adresse IP de l'UTM NETASQ est différente de l'adresse IP vue par le navigateur.

> **AVERTISSEMENT**
> L'utilisation de SRP implique l'installation d'une JVM (*Java Virtual Machine*) sur le poste utilisateur (la plupart des navigateurs Web intègrent cette machine virtuelle). La JVM de SUN (version 1.4) est fortement conseillée.

13.4.5. Logout

Pour se délogger, il faut se connecter au firewall en https (voir précédemment), saisir le login de l'utilisateur désirant se délogger puis cliquer sur le bouton **Déconnexion**. L'utilisateur doit à nouveau saisir son mot de passe pour être déloggé (évite qu'un utilisateur ne s'amuse à délogger d'autres utilisateurs).

AVERTISSEMENT
Lorsqu'un utilisateur quitte son poste de travail avant la fin de la période d'authentification, il faut qu'il fasse un logout pour ne pas se faire intercepter sa session d'authentification.

13.4.6. Changement du mot de passe

L'utilisateur peut modifier son mot de passe d'authentification à distance. Pour cela, il suffit de saisir le login et de cliquer sur **Changez votre mot de passe**.

L'utilisateur n'a plus qu'à modifier son mot de passe.

NOTE
Le changement de mot de passe ne fonctionne pas pour l'authentification en SSL avec certificats ou pour une authentification avec un serveur RADIUS externe.

CHAPITRE 5. ENROLEMENT DES UTILISATEURS

Lorsqu'un service d'authentification est mis en place, il faut définir chaque utilisateur autorisé en créant un objet "utilisateur" (cf.*Partie 4 : Objets*) Plus la société est importante plus cette tâche est fastidieuse. Le service d'enrôlement Web de NETASQ permet de faciliter cette tâche. Désormais c'est l'utilisateur "inconnu" qui demande la création de son compte et de son certificat (si une PKI a été définie par l'administrateur).

13.5.1. Requêtes des utilisateurs

Lorsque l'administrateur a spécifié dans la configuration générale de l'authentification, l'option "Autoriser l'enrôlement via le web" (Voir la "*Partie 12 : Authentification*"), le service d'enrôlement est activé. Le portail d'authentification Web comporte désormais un bouton "Nouvel utilisateur" en plus.

En sélectionnant le bouton **Nouvel utilisateur**, l'utilisateur accède au menu d'enrôlement et peut alors émettre sa requête d'enrôlement.

Suivant la méthode d'enrôlement (LDAP ou LDAP et PKI), différents champs sont à remplir :

Nom	Nom de l'utilisateur (ce champ est obligatoire).
Prénom	Prénom de l'utilisateur (ce champ est obligatoire).
Adresse e-mail	Adresse électronique (ce champ est obligatoire).
Description	Description succincte concernant l'utilisateur.
Numéro de téléphone	Champ réservé au téléphone.
Mot de passe	Mot de passe utilisateur utilisé pour l'authentification.
Confirmez votre mot de passe	Confirmation du mot de passe.
Cryptographic Service Providers	Taille de la clef privée de l'utilisateur (uniquement dans le cas d'un enrôlement LDAP et PKI).

13.5.2. Gestion des requêtes

Lorsqu'un utilisateur a envoyé une requête, l'administrateur peut gérer ces requêtes en attente. Deux menus sont utilisés pour la gestion des requêtes :

- **Liste des requêtes utilisateurs** : gestion des requêtes de création des comptes utilisateurs, cette liste est accessible par le menu **Authentification\Liste des requêtes d'utilisateurs**.
- **Liste des requêtes de certificats** : gestion des requêtes de création de certificats, cette liste est accessible par le menu **PKI\Liste des requêtes de certificats**.

Les options de configurations de ces deux menus sont relativement identiques.

13.5.2.1. Validation et rejet des requêtes

Lorsque vous accédez au menu **Liste des requêtes d'utilisateurs** (ou au menu **Liste des requêtes de certificats**), l'écran de gestion des requêtes s'affiche :

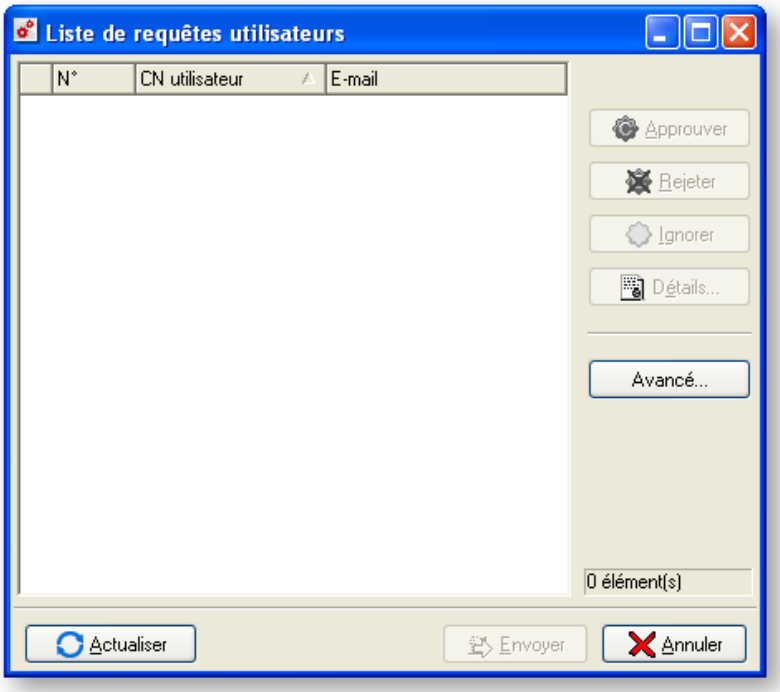


Figure 383 : Liste des requêtes utilisateurs

Cet écran se divise en deux :

- A gauche : la liste des requêtes en attente.
- A droite : les actions réalisables.

Approuver	Ce bouton vous permet d'approuver la requête de l'utilisateur.
Rejeter	Ce bouton vous permet de rejeter la requête de l'utilisateur.
Ignorer	Ce bouton vous permet d'ignorer la requête de l'utilisateur.
Détails	Ce bouton vous permet d'accéder à une visualisation des détails de la requête de l'utilisateur.
Avancé	Ce bouton vous permet d'accéder aux options de l'enrôlement WEB.

Toute action de cet écran n'est validée que lorsque vous appuyez sur le bouton **Envoyer**. Si vous validez (ou rejetez) par mégarde une requête vous pouvez utiliser le bouton **Ignorer** pour remettre en attente la requête d'un utilisateur.

13.5.2.2. Options des requêtes

Appuyez sur le bouton **Avancé** du menu **`Liste des requêtes d'utilisateurs`** (ou au menu **`Liste des requêtes de certificats`**) vous permet d'accéder au menu de configuration des options des requêtes. Cet écran se divise en trois onglets :

- **Options** : configuration des options générales de l'enrôlement :

  DEFINITION
  1) Chaîne de format : la configuration de cette chaîne est explicitée dans l'application.
  2) Approuver automatiquement les requêtes de certificats : (uniquement pour le menu `Liste des requêtes d'utilisateurs`) cette option vous permet la validation automatique des requêtes de certificats. Lorsque l'administrateur valide la requête de création de compte utilisateur, l'application validera automatiquement la création du certificat associé à cet utilisateur.

- **Service d'e-mails** : activation de l'envoi automatique des réponses aux requêtes. Vous ne pouvez démarrer ce service que si vous avez au préalable activé l'envoi des notifications d'alarmes dans le menu **ASQ**. Cette option permet l'envoi d'un email à l'utilisateur pour lui préciser que sa requête a été validée ou non et qu'il peut s'authentifier ou retirer son certificat.

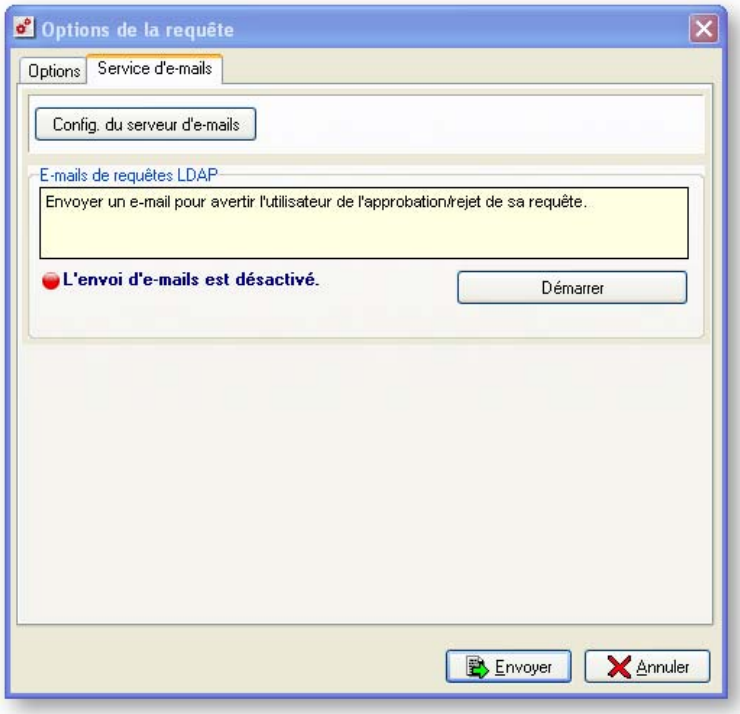


Figure 384 : Options de la requête

Lorsque la requête de l'utilisateur est validée par l'administrateur. Il peut désormais s'authentifier sur le firewall pour bénéficier des services auxquels il a accès. Il est mis au courant de cette validation par mail, si le service de mail a été activé.

Lorsque la requête de création d'un certificat est validée l'utilisateur peut retirer ce certificat :

- Soit par défaut sur le firewall, à l'adresse **https:\\<adresse du firewall>**, en cliquant sur le bouton **Certificats** de la page.
- Soit à l'adresse spécifiée par l'administrateur sur un poste externe au firewall.

CHAPITRE 6. SENSIBILISATION DES UTILISATEURS

L'administrateur du firewall est responsable de la formation des utilisateurs quant à la sécurité du réseau, des équipements qui le composent et des informations qui y transitent.

En effet, la plupart des utilisateurs d'un réseau sont néophytes en informatique et à fortiori en sécurité des réseaux. Il incombe donc à l'administrateur ou au responsable de la sécurité du réseau de mettre en place des sessions de formation ou tout du moins des campagnes de sensibilisation à la sécurité des réseaux.

Lors de ces sessions, il est important d'insister sur la gestion des mots de passe de l'utilisateur et de son environnement de travail et la gestion de leurs accès aux ressources de l'entreprise.

13.6.1. Gestion des mots de passe de l'utilisateur

Au cours de l'évolution des technologies de l'information, de nombreux mécanismes d'authentification ont été inventés et mis en place afin de garantir une meilleure sécurité des systèmes d'information des entreprises. Cette multiplication des mécanismes a entraîné une complexité qui contribue aujourd'hui à détériorer la sécurité des réseaux d'entreprises.

Les utilisateurs (néophytes et non formés) choisissent des mots de passe "simplistes", tirés généralement de leur vie courante et la plupart du temps correspondant à un mot contenu dans un dictionnaire. Ces comportements entraînent, bien entendu, une dégradation notable de sécurité du système d'information.

Il faut prendre conscience que l'attaque par dictionnaire est un "outil" plus que performant. Une étude de 1993 montre déjà cet état de fait. La référence de cette étude est la suivante : (**http://www.klein.com/dvk/publications/**). Ce qui est le plus frappant dans cette étude est sûrement le tableau présenté ci-dessous (basé sur un mot de passe de 8 caractères) :

Type de mot de passe	Nombre de caractères	Nombre de mots de passe	Temps de Cracking
Lexique anglais 8 caract. et +	spécial	250000	< 1 seconde
casse minuscule uniquement	26	208827064576	9 heures
casse minuscule + 1 majuscule	26/spécial	1670616516608	3 jours
minuscules et majuscules	52	53459728531456	96 jours
Lettres + chiffres	62	218340105584896	1 an
Caractères imprimables	95	6634204312890620	30 ans
Jeu de caractères ASCII 7 bits	128	72057594037927900	350 ans

On peut citer aussi un état de fait qui tend à se résorber mais qui est encore d'actualité : les fameux post-its collés à l'arrière des claviers.

L'administrateur doit mettre en place des actions (formation, sensibilisation, …) dans le but de modifier et de corriger ces "habitudes".

Exemple

- Incitez vos utilisateurs à choisir des mots de passe de longueur supérieure à 7 caractères.
- Demandez-leur d'utiliser des chiffres et des majuscules.
- De changer souvent de mots de passe.
- Et surtout de ne noter en aucun cas le mot de passe qu'ils auront finalement choisi.

L'une des méthodes classiques pour trouver un bon mot de passe est de choisir une phrase que l'on connaît par cœur (vers d'une poésie, parole d'une chanson) et d'en tirer les premières lettres de chaque mot. Cette suite de caractères peut alors être utilisée comme mot de passe. Par exemple :

- " **N**ETASQ, **1**er **c**onstructeur **f**rançais **d**e **b**oîtiers **F**IREWALL **e**t **V**PN…"

Le mot de passe pourrait être le suivant : **N1cfdbFeV**.

13.6.2. Environnement de travail

L'espace de travail est souvent un lieu de passage, un croisement pour de nombreuses personnes internes et extérieures à l'entreprise. Il s'agit donc de sensibiliser les utilisateurs au fait que certaines personnes (fournisseurs, clients, ouvriers, …) peuvent accéder à leur espace de travail et de ce fait recueillir des informations sur l'activité de l'entreprise.

Il est important de faire prendre conscience à l'utilisateur qu'il ne faut pas qu'il divulgue son mot de passe aussi bien par téléphone que par Email (social engineering) et qu'il faut qu'il tape son mot de passe à l'abri des regards indiscrets.

13.6.3. Gestion des accès d'utilisateurs

Pour compléter ce chapitre sur la sensibilisation des utilisateurs à la sécurité des réseaux, l'administrateur doit aborder la gestion des accès utilisateur. En effet le mécanisme d'authentification d'un firewall NETASQ (comme beaucoup d'autres systèmes) basé sur un système de login/mot de passe n'implique pas forcément de délogage à fermeture de l'application à l'origine de cette authentification (crédit de temps d'authentification). Cet état de fait n'est pas forcément évident pour l'utilisateur néophyte. Ainsi malgré avoir fermé l'application en question, l'utilisateur (qui pense ne plus être connecté) reste authentifié. S'il quitte son poste une personne malintentionnée peut alors usurper son identité et accéder aux informations contenues dans l'application.

Enfin incitez les utilisateurs à verrouiller leurs sessions lorsqu'ils se déplacent et laissent leur poste de travail sans surveillance. Cette tâche qui se révèle parfois fastidieuse peut être facilitée par des mécanismes d'authentification qui automatise le verrouillage (token USB par exemple).

PARTIE 14 : DISPONIBILITE DES FIREWALLS

Il existe deux fonctions permettant d'assurer une meilleure disponibilité des firewalls :

- Le Watchdog
- La Haute Disponibilité

CHAPITRE 1. LE WATCHDOG

14.1.1. Pour ce point, vous devez avoir franchi les étapes

- Partie 2 : Installation, pré-installation, intégration.

14.1.2. Utilité de ce point

Cette section vous permet de configurer le Watch dog, élément hardware qui teste régulièrement le firewall afin de détecter une éventuelle inactivité de celui-ci. Le Watch dog peut commander un redémarrage du firewall en cas de freeze de ce dernier.

14.1.3. Accéder à ce point

- Accédez à la boîte de dialogue par le menu **`Firewall\Haute Disponibilité.`**

14.1.4. Important

AVERTISSEMENT
Seuls les firewalls sortis de production ou revenus en SAV depuis octobre 2001 peuvent avoir les fonctionnalités Watch dog et Haute Disponibilité. Si votre Firewall est plus ancien, vous pouvez également bénéficier de ces fonctionnalités. Dans ce cas, le Firewall devra néanmoins subir une modification matérielle, et donc revenir chez NETASQ pour intervention.

La fonctionnalité Watch dog va vous permettre d'automatiser le reboot du firewall en cas de "gel". Le principe est très simple : le Watch dog est un composant hardware qui réalise à intervalles réguliers des tests d'activité sur le firewall. Au bout d'un certain temps (paramétrable) sans réponse, l'arrêt et le démarrage du Firewall ont lieu.

La configuration est très simple. Il suffit dans le menu Haute Disponibilité (onglet **Firewall**) de cocher "Watch dog est actif" dans l'onglet **Watchdog** et de déterminer le temps d'inactivité maximale. Les connexions actives sont récupérées après redémarrage.

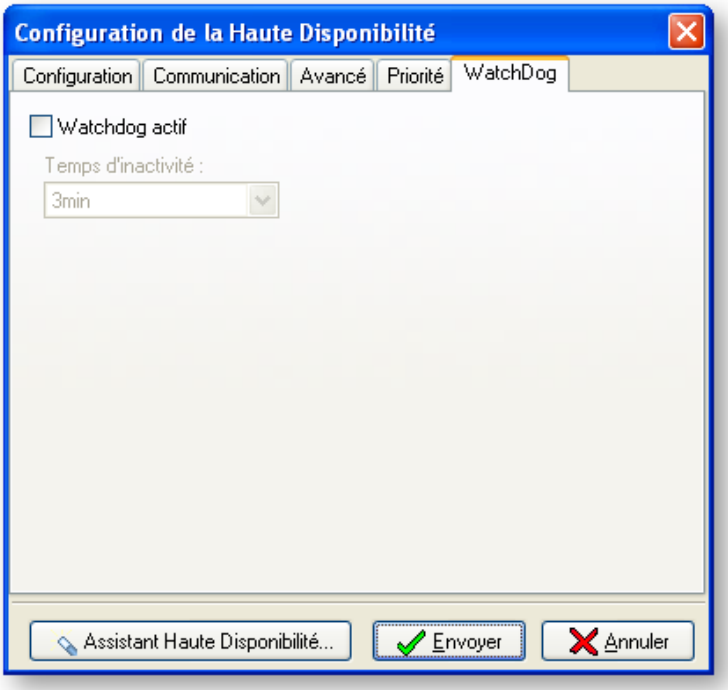


Figure 385 : Configuration du WatchDog

AVERTISSEMENT
Ne mettez pas une valeur de temps limite d'inactivité trop court (inférieur à 1 minute), vous risqueriez de faire rebooter le firewall fréquemment alors que ce n'est pas nécessaire. En effet, il peut arriver que le firewall ne réponde plus durant quelques secondes et reprenne une activité normale aussitôt après, sans que cela ne nécessite un reboot.

Cette fonctionnalité est accessible indépendamment de la haute disponibilité.

CHAPITRE 2. LA HAUTE DISPONIBILITE

14.2.1. Introduction

14.2.1.1. Pour cette partie, vous devez avoir franchi les étapes

- Partie 2 : Installation, pré-configuration, intégration.
- Demande de clés d'activation pour la haute disponibilité auprès de NETASQ.

14.2.1.2. Pour cette partie, vous devez connaître

- La politique de sécurité de l'entreprise.
- Le mot de passe de l'utilisateur "HA".
- L'adresse IP du lien de gestion de la Haute Disponibilité.

14.2.1.3. Utilité de la partie

Cette partie vous permet de configurer la fonctionnalité de haute disponibilité. Cette fonctionnalité n'est utilisable que si vous avez deux firewalls en votre possession.

Le principe sera de basculer toutes les connexions du firewall actif vers le second (firewall passif) en cas de dysfonctionnement du firewall actif.

14.2.1.4. Accéder à cette partie

➲ Accédez à la boîte de dialogue par le menu **`Firewall\Haute Disponibilité`**.

Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications et posséder deux firewalls.

14.2.2. Licences

Pour utiliser la fonctionnalité de haute disponibilité, vous devez avoir deux firewalls en votre possession.

Deux clés d'activation particulières doivent être demandées auprès de NETASQ (une pour chaque firewall) et installées via l'interface graphique (*Cf.* Partie 19/Chapitre 1 : Actions diverses\Licence).

14.2.2.1. Notion de principal/secondaire

Un des deux firewalls sera considéré comme principal et le second comme secondaire (le statut de chaque firewall sera déterminé par la clé d'activation installée).

La différenciation principale et secondaire sert dans les cas suivants :

- Si les deux firewalls démarrent simultanément.
- Si les deux firewalls se retrouvent dans le même état (suite à une perte de communication par l'interface Ethernet par exemple)
- Pour différencier les adresses IP affectées de chaque côté de la liaison haute disponibilité.

> **AVERTISSEMENT**
> Seuls les firewalls sortis de production ou revenus en SAV depuis octobre 2001 peuvent avoir les fonctionnalités Watch dog et Haute Disponibilité. Si votre Firewall est plus ancien, vous pouvez également bénéficier de ces fonctionnalités. Dans ce cas, le Firewall devra néanmoins subir une modification matérielle, et donc revenir chez NETASQ pour intervention.

14.2.3. Fonctionnement

Aucun élément réseau n'étant à l'abri d'une panne, la fonctionnalité de haute disponibilité (ou de tolérance de pannes) proposée sur les firewalls NETASQ permet d'assurer une continuité de service même en cas de dysfonctionnement.

Cette fonctionnalité nécessite l'utilisation de deux firewalls qui seront considérés par le réseau comme une seule entité. Ces deux firewalls possèdent la même configuration mais un seul firewall sera actif à un instant donné (un seul firewall prendra en charge les connexions). Le second firewall ne deviendra actif que lorsque le premier ne sera plus dans un mode de fonctionnement normal d'un firewall (les connexions actives sont récupérées lors du basculement).

Les interfaces réseau du firewall passif sont désactivées et ne sont réactivées automatiquement que lorsque le firewall redevient actif.

Les flux pour la haute disponibilité (tests d'activité, transfert des configurations ...) peuvent être acheminés via un câble Ethernet. Il faut donc affecter une ou deux interfaces réseau sur chaque boîtier et relier ces deux interfaces via des liaisons Ethernet. Vous pouvez soit dédier ces interfaces au fonctionnement de la Haute disponibilité ou soit réaliser la configuration de la haute disponibilité basée sur un VLAN.

La liaison Ethernet

NETASQ a choisi de ne plus supporter la haute disponibilité sur lien série car le débit sur un lien série n'était plus suffisant pour la base d'informations à répliquer entre les deux firewalls. Dans le cas de la liaison Ethernet, le débit est beaucoup plus important, les transferts de configuration et la mise à jour de la base LDAP sont alors considérablement accélérés.

NOTE
Avec la fonctionnalité de haute disponibilité, il est préférable d'utiliser une base externe afin d'éviter la réplication de la base LDAP interne entre les deux firewalls.

Il est possible de placer les deux boîtiers à des distances plus importantes l'un de l'autre.

Haute Disponibilité sur VLAN

La haute disponibilité sur VLAN permet d'utiliser la liaison Ethernet comme liaison de contrôle entre les deux firewalls en haute disponibilité sans toutefois dédier cette interface. En effet grâce au support de la haute disponibilité sur VLAN, l'interface de contrôle peut alors être utilisée pour réaliser une DMZ par exemple.

14.2.3.1. Test de fonctionnement du firewall

Le firewall passif teste grâce à des pings (envoyés sur la liaison Ethernet reliant les deux firewalls) si le firewall actif fonctionne. Ces tests sont réalisés de manière ponctuelle toutes les T secondes (T étant défini grâce NETASQ UNIFIED MANAGER, voir section "Mise en place"). Un bout d'un certain nombre de pings sans réponse (nombre paramétrable grâce au NETASQ UNIFIED MANAGER), le firewall est considéré comme "freezé", c'est-à-dire ne répondant plus. Dans ce cas, le firewall passif devient actif et prend en charge les connexions.

En plus du Ping, les firewalls se testent de manière croisée :

- Chacun demande de manière régulière l'état de l'autre (actif ou passif) pour détecter le cas où deux firewalls seraient actifs (cas où le câble série ou Ethernet dédié ont été débranchés). Dans ce cas, le firewall principal reste actif et le secondaire devient passif.
- Si le firewall actif a moins de cartes Ethernet en fonctionnement que le firewall passif (dysfonctionnement d'une carte), il sera basculé en mode passif alors que le passif deviendra actif.

- Si le firewall passif ne répond pas, une alarme du type "HA : défaillance du firewall" sera envoyée.
- Si deux liaisons de contrôle ont été configurées, les firewalls vérifient d'abord leur connectivité par l'intermédiaire du premier lien de contrôle. Si cette liaison est rompue, la connectivité est testée sur le deuxième lien de contrôle avant qu'il y ait un basculement effectif.

14.2.3.2. Haute disponibilité sur deux liens de contrôle

La configuration de haute disponibilité NETASQ n'est viable que si à aucun moment, les deux Appliance participant au cluster de haute disponibilité ne sont actifs simultanément. En effet dans le cas où les deux Appliance serait actifs au même moment, cela poserait d'importants problèmes réseau car chaque Appliance possède les mêmes adresses IP et les mêmes adresses MAC que son correspondant de haute disponibilité.

Pour parer à ce problème réseau, il est possible de configurer deux liens de contrôle. Ainsi si la connectivité entre les deux correspondants de haute disponibilité ne peut être établie sur le premier lien de contrôle (perte d'une interface, perte du lien…), elle est testée sur le deuxième lien de contrôle avant activation du firewall passif.

Spécificité de la deuxième liaison de contrôle

La première liaison de contrôle est chargée non seulement de la vérification de la connectivité entre les deux Appliance participant à la haute disponibilité mais aussi de la synchronisation des informations entre l'Appliance actif et l'Appliance passif (synchronisation de la configuration, échange des tables de fonctionnement, etc.). Tandis que le deuxième lien de contrôle permet uniquement la vérification de la connectivité entre les deux Appliance. Elle permet donc d'empêcher un basculement inutile (passif vers actif) de l'Appliance passif.

14.2.4. Mise en place

Avant de lire ce chapitre, vous devez avoir pris connaissance du titre **Licences** et avoir installé les deux clés d'activation.

14.2.4.1. Installation

Pour installer l'architecture de haute disponibilité, veuillez suivre la procédure suivante :

1. Les deux firewalls doivent être déconnectés du réseau local (dans le cas contraire, des problèmes de conflits d'adresses pourraient survenir) mais sous tension.
2. Connectez-vous au firewall secondaire en changeant l'adresse IP du bridge (prenez par exemple l'adresse 10.0.0.253). Cette adresse doit absolument être différente de celle du firewall principal. Le firewall doit rebooter.
3. Reliez les deux firewalls avec un câble Ethernet.
4. Connectez-vous au firewall principal, Un assistant vous permet de configurer simplement la fonctionnalité de haute disponibilité. (bouton Assistant d'initialisation de la HA...).

1 **Etape 1**

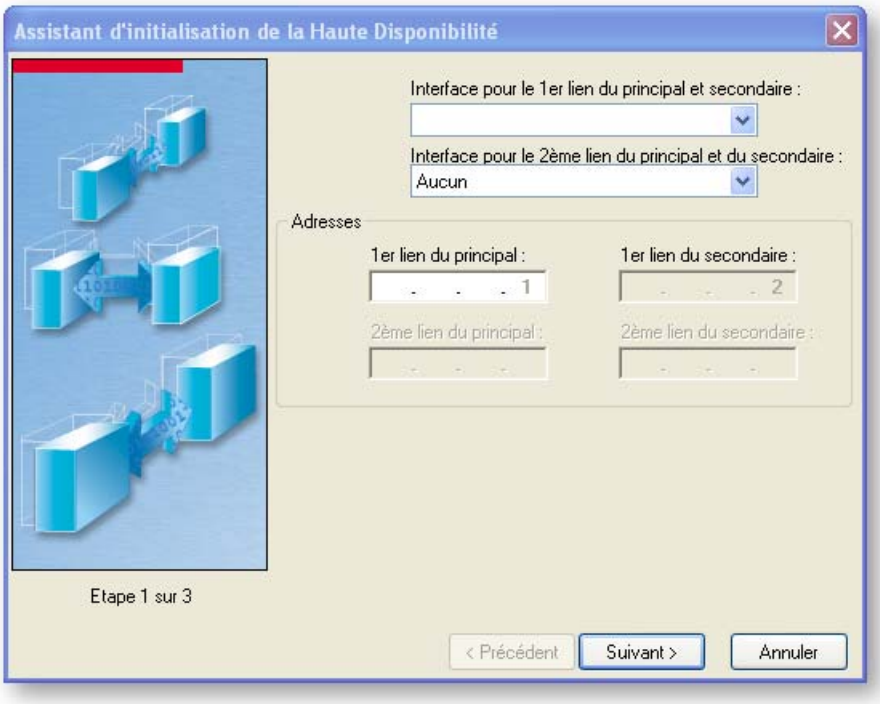


Figure 386 : Assistant HA - Etape 1

Choisissez la ou les interfaces utilisées pour la haute disponibilité (pour le principal et pour le secondaire) et l'adresse IP du principal (l'adresse IP secondaire = adresse IP principal +1). Si une interface VLAN est configurée, il est possible d'utiliser cette interface pour la haute disponibilité.

Dans ce cas l'interface Ethernet à laquelle l'interface VLAN est rattachée n'est plus dédiée à la haute disponibilité.

Deuxième lien de contrôle

Notez qu'il est possible de configurer deux liens de contrôle grâce à l'assistant de configuration de la haute disponibilité. Ce deuxième lien de contrôle n'est utilisé que pour tester la connectivité existante entre les deux Appliance participant au cluster de haute disponibilité.

Adressage des interfaces de haute disponibilité

Dans l'étape 1, vous définissez aussi le plan d'adressage utilisé par les interfaces des Appliance participant aux liaisons de contrôle. L'assistant vous permet de définir l'adresse réseau et c'est lui-même qui attribue des adresses pour chacune des interfaces.

Notez qu'il est possible de définir à priori, n'importe quel plan d'adressage. Toutefois attention si vous définissez un plan d'adressage "public", l'accès aux sites Web utilisant ce plan d'adressage sera impossible. Il est recommandé d'utiliser un plan d'adressage privé (différent de plus de celui utilisé par les autres interfaces).

Etape 2

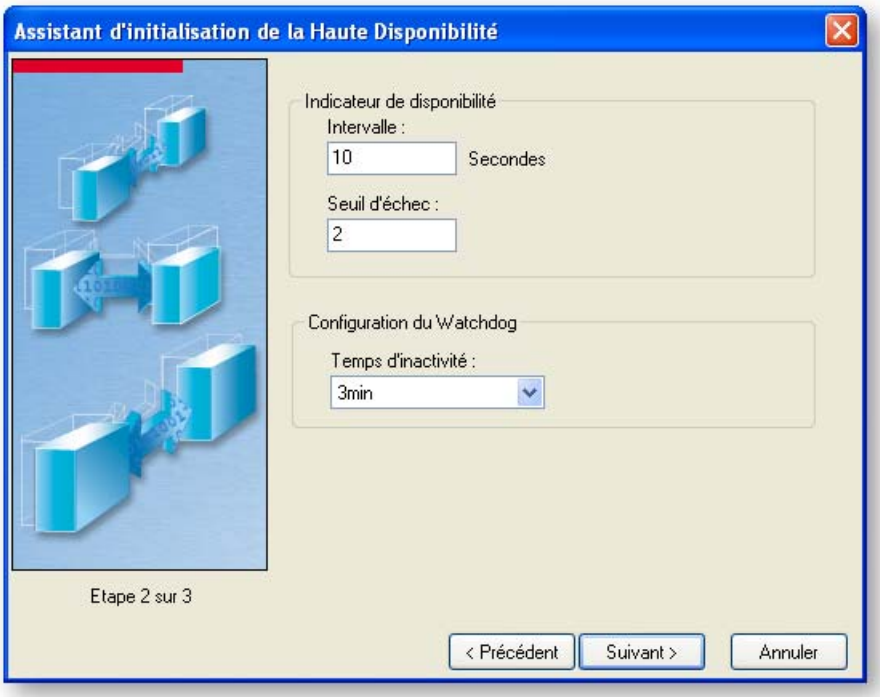


Figure 387 : Assistant HA - Etape 2

Indiquez le temps entre deux pings dans le champ "intervalle" ainsi que le nombre de pings sans réponse accepté (seuil d'échec) avant un basculement du firewall actif vers le firewall passif.

Le seuil d'échec ne peut pas être inférieur à 2 et il est fortement déconseillé de mettre un intervalle de temps inférieur à 5 secondes.

AVERTISSEMENT
Un intervalle de 15 secondes et un seuil d'échec de 2 sont conseillés

La partie **Configuration du Watch dog** vous permet de définir le temps d'inactivité acceptable avant un reboot forcé du firewall.

Etape 3

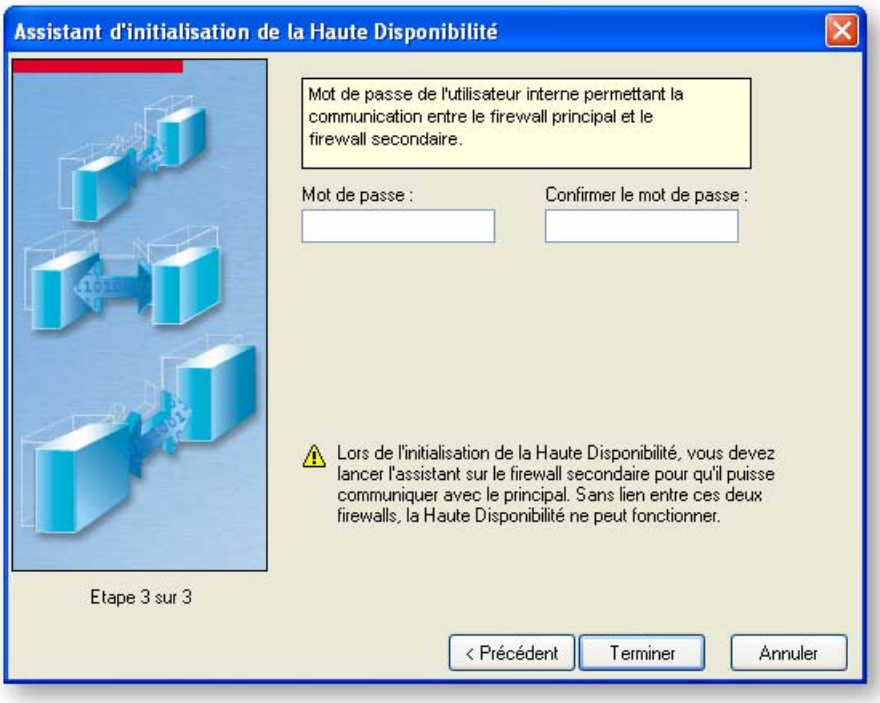


Figure 388 : Assistant HA - Etape 3

Enfin, indiquez le mot de passe utilisé pour chiffrer les communications entre les deux firewalls. Les firewalls communiquent entre eux sur le port 1300 et les données sont chiffrées en AES.

Tous les paramètres saisis dans cet assistant peuvent être modifiés par la suite.

1 Connectez-vous à l'autre firewall (firewall secondaire) et relancez l'assistant.

AVERTISSEMENT
Les interfaces, adresses IP et mots de passe doivent être identiques au firewall principal.

2 Une fois l'assistant réalisé sur les deux firewalls, vous devez vous connecter sur le MASTER (dans le cas où seul le SLAVE répond, faites une permutation manuelle) et faites une synchronisation des deux

firewalls (voir plus bas). Il faut absolument que la première synchronisation soit faite du firewall MASTER vers le firewall SLAVE, pour une réplication des adresses MAC sur les deux boîtiers.

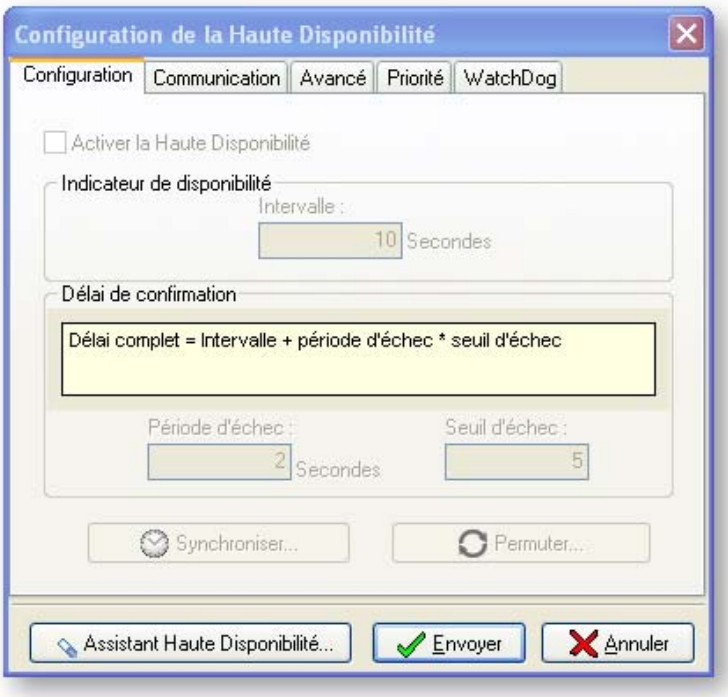


Figure 389 : Configuration de la HA - Configuration

14.2.4.2. Onglet Communication

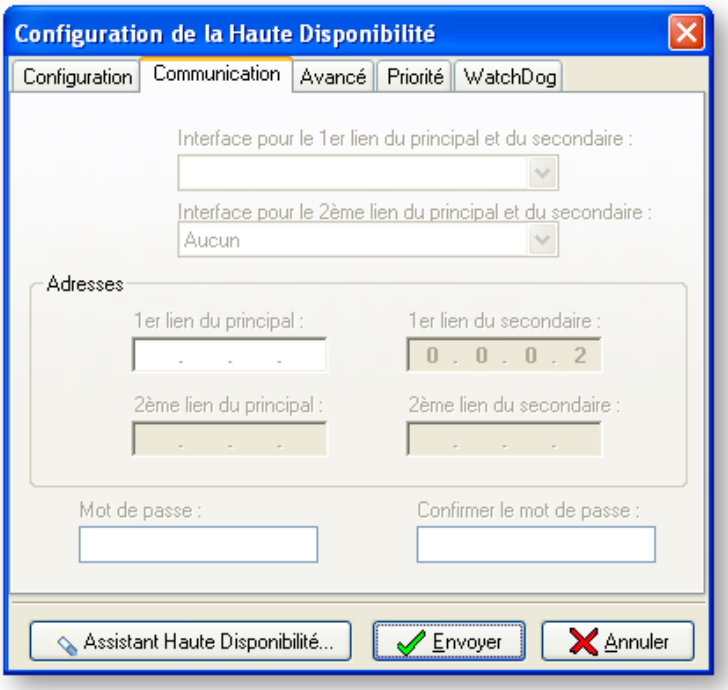


Figure 390 : Configuration de la HA - Communication

Dans ce menu vous pouvez modifier les paramètres définis dans l'assistant.

Interface pour le 1er lien du principal et du secondaire	Interface principale utilisée pour relier les deux firewalls constituant le cluster.
Interface pour le 2ème lien du principal et du secondaire	Interface secondaire utilisée pour relier les deux firewalls constituant le cluster.
Adresses	Adresses IP attribuées aux différents firewalls.
Mot de passe	Mot de passe utilisé pour chiffrer les communications entre les deux firewalls.

14.2.4.3. Onglet Avancé

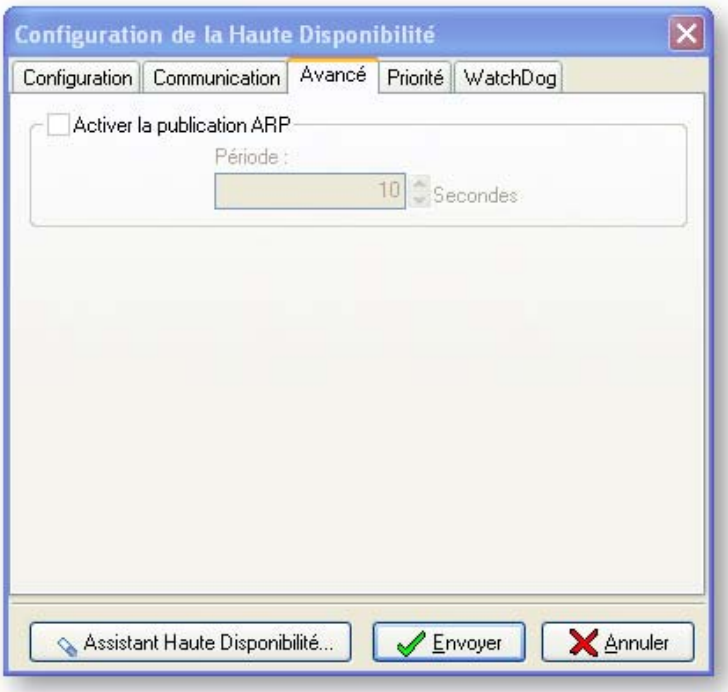


Figure 391 : Configuration de la HA - Avancé

Ce menu vous permet d'activer l'envoi de paquets du type "Gracious ARP". C'est-à-dire que le firewall publie régulièrement, sur le réseau, ses adresses IP et MAC.

Période	Intervalle de temps entre les différents envois de paquets

14.2.4.4. Onglet Priorité

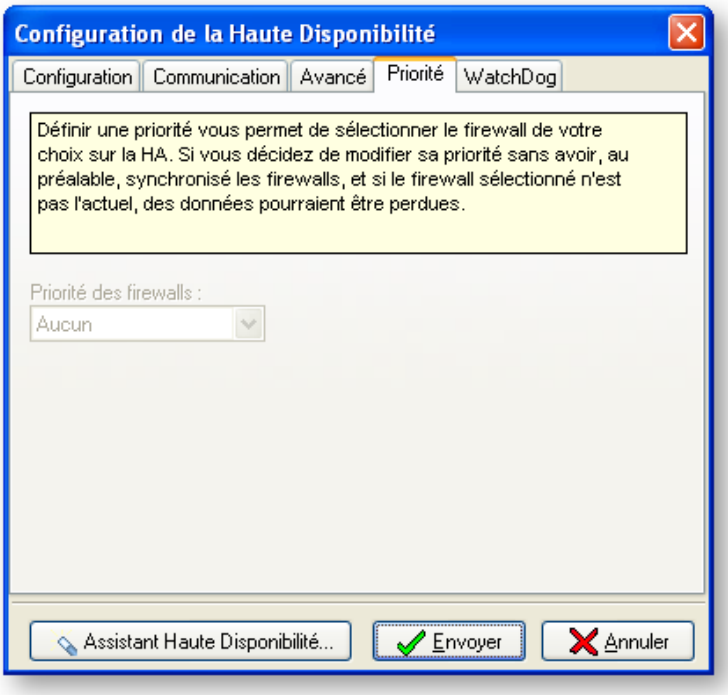


Figure 392 : Configuration de la HA - Priorité

Dans le cas où les deux firewalls se retrouvent dans l'état actif ou démarrent en même temps, l'option priorité permet de spécifier quel firewall va prendre la main et quel firewall reprendra l'état passif.

Priorité des firewalls	Choix du firewall prioritaire.

14.2.4.5. Onglet Priorité

Cf. Chapitre 1. Le Watchdog.

14.2.4.6. Synchronisation des firewalls

La synchronisation des firewalls permet la réplication de la configuration du firewall actif sur le firewall passif. Cette synchronisation est effectuée sur la configuration complète, les mots de passe, les changements de dates. La synchronisation peut être soit forcée en cliquant sur le bouton **Synchroniser** de l'onglet **`Configuration`**, soit demandée par le firewall lorsqu'on quitte celui-ci.

AVERTISSEMENT
Si vous faites une synchronisation manuelle, les firewalls seront indiqués comme non synchronisés, alors que la synchronisation a bien eu lieu. Pour vérifier la synchronisation, utilisez le moniteur temps réel qui vous donnera l'état de synchronisation des deux firewalls.

14.2.4.7. Permutation des firewalls

Si vous désirez rendre actif le firewall passif, cliquez sur le bouton **Permuter** de l'Onglet **Configuration**.

14.2.5. Exemple d'architecture

Schéma de mise en place de la Haute Disponibilité avec deux firewalls U450/4 et 3 Hubs 10/100Mbits de 4 ports avec les 3 interfaces des firewalls disponibles (la quatrième est utilisée pour la haute disponibilité).

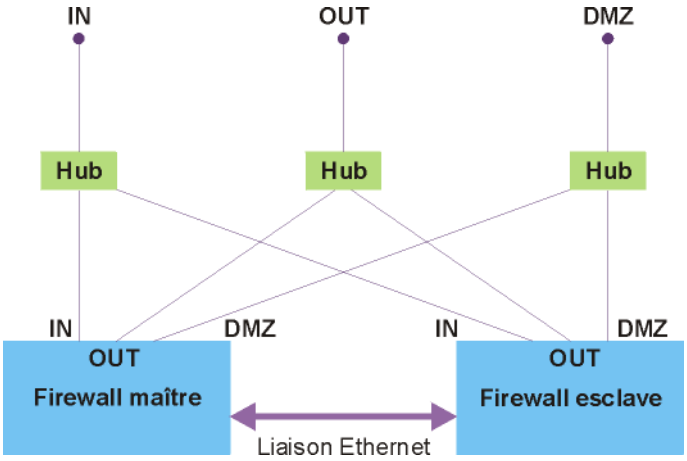


Figure 393 : HA

Utiliser une liaison Ethernet vous permet de séparer physiquement les deux boîtiers, en effet, vous pouvez placer chacun des firewalls dans une pièce différente. Par contre, vous perdez une interface Ethernet par boîtier (utilisées pour la haute disponibilité).

NOTE
L'utilisation de switchs à la place des hubs est possible mais fortement déconseillée, à cause du caractère "intelligent" de ces derniers. De plus, les hubs représentent un surcoût beaucoup moins important que les switchs.

14.2.6. Arrêt de la Haute Disponibilité

Si vous désirez ne plus utiliser la fonctionnalité de haute disponibilité, veuillez suivre la procédure suivante :

1. Arrêter l'un des deux firewalls.
2. Arrêter l'option haute disponibilité sur le firewall en marche, puis arrêter ce firewall.
3. Démarrer le premier firewall, puis arrêter l'option haute disponibilité sur ce firewall. (éventuellement changer ses IP).

> **AVERTISSEMENT**
> Arrêter la haute disponibilité sur un seul firewall risque de causer des problèmes de conflit d'utilisation d'adresses IP et Mac.

14.2.7. Remarques

Lorsque vous tentez de vous connecter au cluster (ensemble des deux firewalls) via NETASQ UNIFIED MANAGER ou NETASQ REAL-TIME MONITOR, la connexion est forcément établie avec le firewall actif. Pour se connecter au firewall passif, il faut rendre ce dernier actif (en utilisant le bouton **Permuter** de l'onglet **`Configuration`**).

La synchronisation des firewalls après une modification de la configuration du firewall actif entraîne un redémarrage du firewall passif.

Les fichiers de traces ne sont pas communs. Vous ne verrez dans un fichier que les traces récupérées lorsque le firewall était actif. Pour centraliser les logs des deux firewalls, il faut les rediriger vers un serveur SYSLOG externe identique, vers le serveur NETASQ SYSLOG.
Une sauvegarde du système complet (sur la partition de sauvegarde ne sera réalisée que sur le firewall actif.

Pour tester la Haute Disponibilité, vous pouvez débrancher une interface réseau du firewall actif, le second firewall doit, au bout d'un temps donné, basculer en actif.

Processus de mise à jour

Pour mettre à jour vos firewalls en haute disponibilité, il y a deux possibilités :

- La mise à jour par le firewall actif.
- La mise à jour par le firewall passif (réalisable que pour une mise à jour mineure à partir de la version 5).

La mise à jour par le firewall actif

Lorsqu'une mise à jour logicielle du firewall actif est réalisée, il n'y a pas de permutation lors du redémarrage du firewall actif.

Une fois que le firewall actif a été mis à jour, vous devez réaliser une permutation manuelle des deux firewalls en cliquant sur le bouton **Permuter** de l'onglet **`Configuration`**.

Déconnectez puis reconnectez-vous (vous serez alors connecté sur l'autre firewall).

Réalisez à nouveau la mise à jour logicielle. Le redémarrage consécutif entraînera une permutation des firewalls pour se retrouver dans la configuration précédant la mise à jour.

Cette procédure permet de récupérer au moins un firewall dans l'ancienne version logicielle, si la mise à jour ne s'est pas déroulée correctement.

La mise à jour par le firewall passif

L'option **Mise à jour du passif** de l'assistant de mise à jour du firewall vous permet de mettre à jour le firewall passif avant le firewall actif. Dans ce cas vous mettez à jour le firewall passif à partir du firewall actif.

Puis une fois le firewall passif redémarré vous pouvez pratiquer une permutation manuelle pour réitérer l'opération (mise à jour du passif).

Puis une fois le deuxième firewall redémarré vous pouvez permuter manuellement les firewalls pour retrouver dans la configuration précédant la mise à jour.

Cette procédure permet de récupérer au moins un firewall dans l'ancienne version logicielle, si la mise à jour ne s'est pas déroulée correctement sans altérer la continuité des services.

PARTIE 15 : SEISMO

15.1.1. Introduction

15.1.1.1. Introduction à cette partie

Comment fonctionne NETASQ SEISMO ?

NETASQ SEISMO est un module qui permet à l'administrateur réseau de collecter en temps réel des informations et de les analyser afin de découvrir d'éventuelles vulnérabilités susceptibles de compromettre son réseau. Il permet, entre autres, de remonter les alertes venant de l'ASQ et de maintenir ainsi une politique de sécurité optimale.
NETASQ SEISMO collecte et archive les informations liées, notamment, au système d'exploitation, aux divers services activés ainsi qu'aux différentes applications installées. Il existe deux types d'application :

- Les produits qui correspondent à des applications clientes installées sur une machine (exemple : Firefox 1.5)
- Les services qui correspondent à des applications serveurs attachées à un port (exemple : openSSH 3.5)

Au niveau des applications détectées, il est possible de les regrouper par famille. En couplant ces informations avec sa base de vulnérabilités, NETASQ SEISMO propose les failles probables de sécurité liées à ces applications.

Cette collecte permet la création de notices descriptives des éléments du réseau.

NETASQ SEISMO a pour objectifs :

- De configurer la politique de sécurité de votre réseau d'entreprise.
- D'analyser l'état de risque.
- D'optimiser le niveau de sécurité.
- De reporter les évènements de sécurité.

Le procédé est le suivant :

1. Le moteur de prévention d'intrusion de NETASQ (ASQ) extrait en temps réel des données à l'aide de protocoles réseaux qu'il connaît.
2. SEISMO combine et pondère ces données.
3. La vulnérabilité trouvée peut ensuite être traîtée grâce à des bases de données indexées dynamiquement. Une fois ces informations collectées, elles sont exploitées dans le Monitor afin de pouvoir corriger les failles sur le réseau, détecter des logiciels interdits par la politique de sécurité, ou obtenir en temps réel le véritable risque lié à une attaque.
4. La fiche d'informations est alors complétée.
5. Une ou plusieurs solutions peuvent être alors envisagées.

> **Exemple**
> Une entreprise possède un site Web public qu'elle met à jour 2 fois par mois en utilisant le protocole FTP. Au moment de l'établissement des connexions, à une date et heure précises, une vulnérabilité qui affecte éventuellement les serveurs FTP est remontée et est donc intégrée immédiatement dans le Monitor, ce qui permet sa détection par l'administrateur réseau de manière quasi-simultanée.
> Cette vulnérabilité est représentée par une ligne qui indique le nombre de machines affectées et s'il y a une

solution ou non.
En déployant cette ligne, le détail des machines concernées s'affiche ainsi que le service touché par la vulnérabilité. Une aide, constituée entre autres de liens, peut être proposée pour corriger la faille détectée.

Une fois que l'administrateur réseau a pris connaissance de la vulnérabilité, il peut à tout moment corriger la vulnérabilité, mettre en quarantaine la/les machine(s) affectée(s) et générer un rapport.

NETASQ SEISMO peut également effectuer un rapport hebdomadaire, mensuel ou annuel à l'aide de l'application **NETASQ EVENT REPORTER** (Autoreport). (*Cf. Voir le manuel d'utilisation **NETASQ EVENT REPORTER***.)

A Quoi sert la configuration de profils ?

La technologie ASQ inclut un moteur de filtrage dynamique des paquets (stateful inspection) avec optimisation des règles permettant l'application du profil de vulnérabilité de manière sûre et rapide. La mise en œuvre des fonctions de profils est basée sur la confrontation des attributs de chaque paquet IP reçu aux critères de chaque règle du profil de vulnérabilité créé.

Dans le module NETASQ SEISMO, des profils sont créés par défaut. Il en existe 4. Par ailleurs, vous pouvez créer autant de profils que vous le souhaitez.

Les règles de vulnérabilités sont stockées sur le firewall NETASQ dans des profils.

Le principe est simple : quand un paquet arrive au produit UTM NETASQ, celui-ci fait descendre le paquet dans la liste de règles de vulnérabilités. Si le paquet correspond aux critères de sélection d'une règle, il applique l'action associée à cette règle sinon le paquet est automatiquement supprimé. Une fois qu'une règle peut être appliquée au paquet, ce dernier n'est plus comparé aux règles suivantes.

La façon dont vos règles de vulnérabilités sont ordonnées est primordiale. La cohérence de cet ordre est la principale difficulté dans la configuration de votre firewall.

15.1.1.2. Pour cette partie, vous devez connaître

Les profils que vous voulez instaurer.

15.1.1.3. Utilité de la partie

Cette partie vous permet de définir les profils de vulnérabilités et les règles qui y sont associées.

15.1.1.4. Accéder à cette partie

Pour accéder à la configuration du module SEISMO, sélectionnez **SEISMO** dans l'arborescence des menus de NETASQ UNIFIED MANAGER.

15.1.2. Présentation

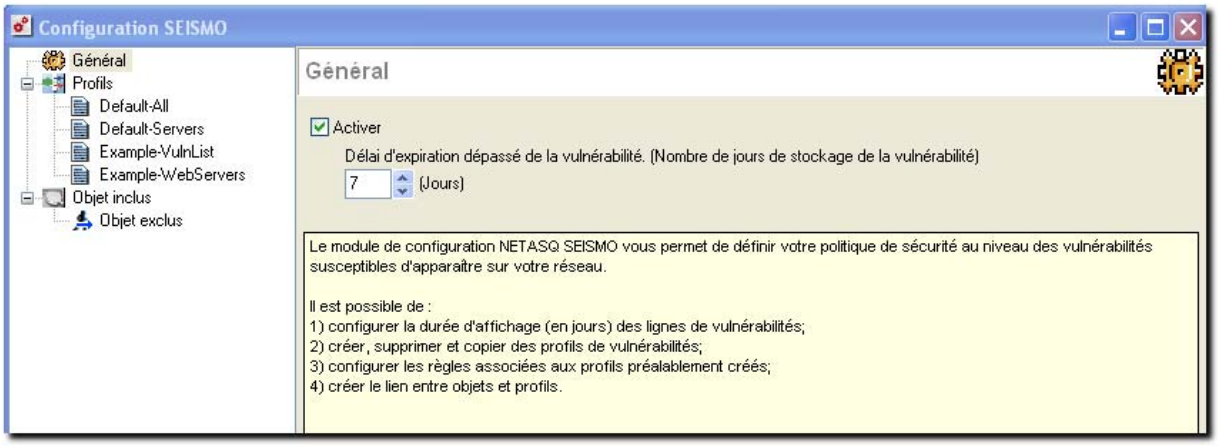


Figure 394 : Configuration SEISMO - Général

Cette section vous permet de définir les profils et les règles qui y sont associées. C'est ici que vous gérez votre politique de sécurité concernant les vulnérabilités.

Ce menu de configuration vous permet de configurer votre politique de sécurité au niveau des vulnérabilités susceptibles d'apparaitre sur votre réseau.

La configuration consiste à :

- Configurer la durée d'affichage des lignes de vulnérabilités
- Créer, supprimer, et copier des profils de vulnérabilité (en dehors du profil Default-all)
- Configurer les règles associées aux profils préalablement créés
- Effectuer le lien entre objets et profils

L'écran se divise en deux zones distinctes :

- Une zone affichant une arborescence permettant de passer d'un écran à un autre dans la configuration de NETASQ SEISMO.
- Une zone permettant les différentes configurations

Cette configuration lors de la visualisation des traces SEISMO dans NETASQ REAL-TIME MONITOR et NETASQ EVENT REPORTER.

15.1.3. Général

- Le menu **Général** est accessible à partir de l'arborescence de la configuration SEISMO :

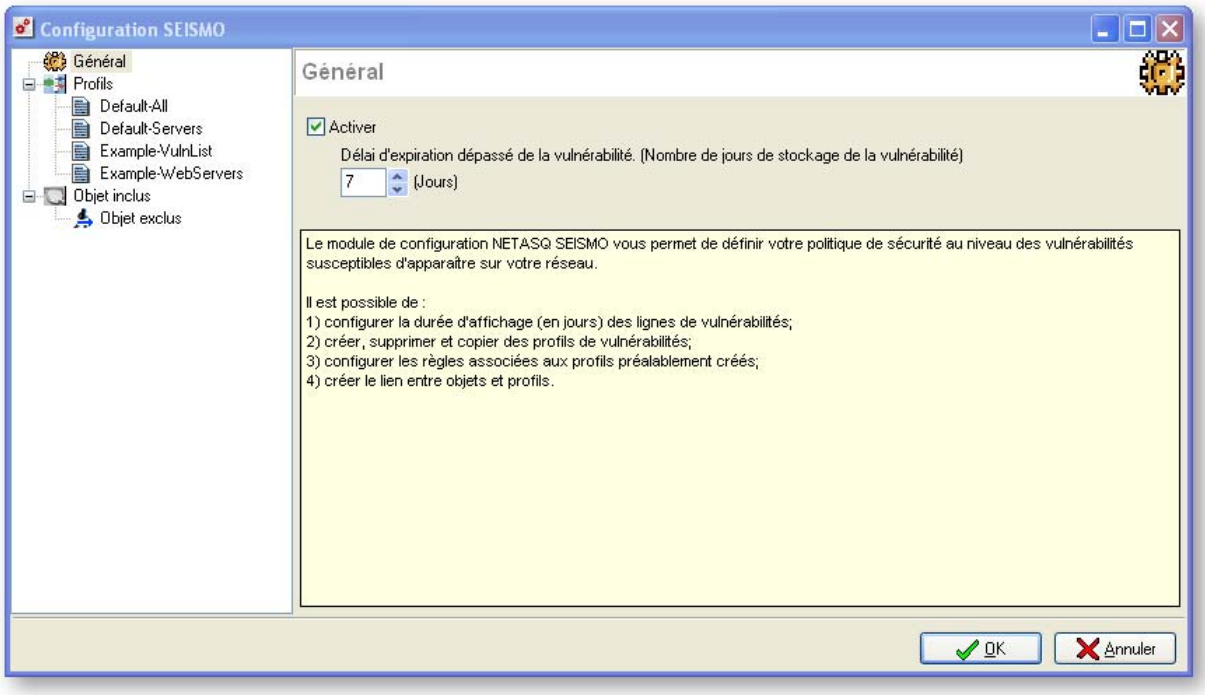


Figure 395 : Configuration SEISMO - Général

Activer	Cocher l'option **Activer** permet d'afficher les informations liées au module NETASQ SEISMO. Il est possible alors, lorsque l'option **Activer** est cochée de déterminer un nombre de jours d'affichage pour les lignes de vulnérabilités au sein du Monitor et Reporter. Les informations ne seront pas visibles si vous ne cochez pas cette option. **Remarque** Lors de la mise à jour (et si vous avez acquis la licence), le module NETASQ SEISMO sera activé par défaut. La remontée d'alertes se fera en fonction de la configuration existante.
Délai d'expiration dépassé de la vulnérabilité (Nombre de jours de stockage de la vulnérabilité)	Cette option permet de déterminer le nombre maximal de jours de visibilité des lignes de vulnérabilités une fois celles-ci apparues.

15.1.4. Profils

Le menu **`Profils`** est accessible à partir de l'arborescence de la configuration SEISMO.
La fenêtre suivante s'affiche :

Cette fenêtre présente la liste de 4 profils configurés par défaut. Vous pouvez, créer vos propres profils.

REMARQUE
Le profil que vous créez est automatiquement ajouté à la liste des profils dans l'arborescence.

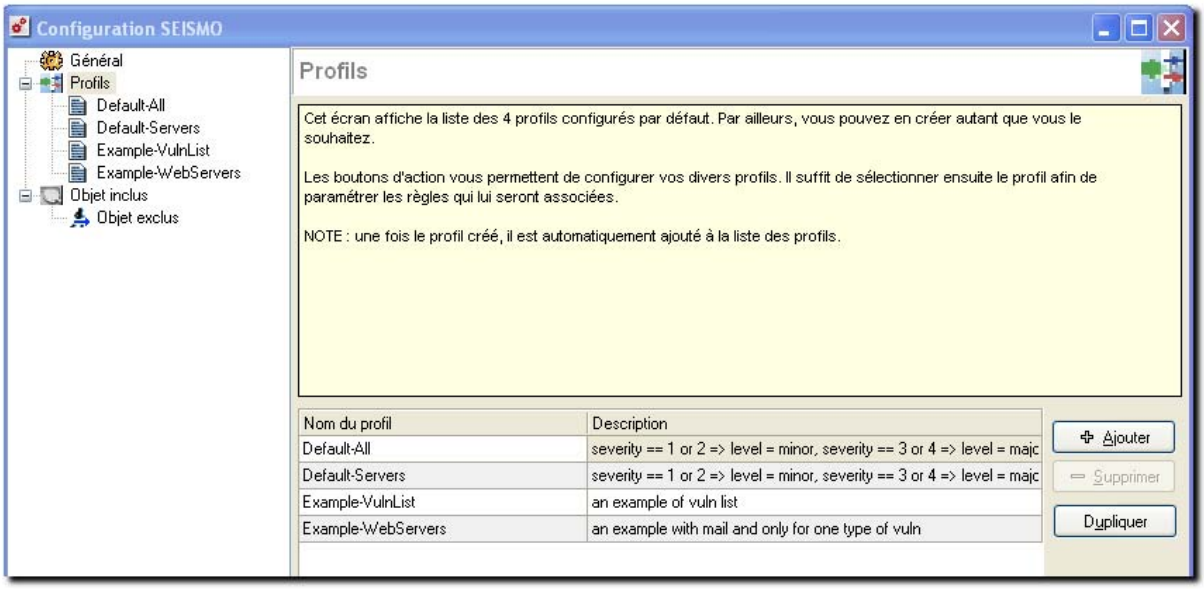


Figure 396 : Configuration SEISMO - Profils

La fenêtre présente deux zones spécifiques :

A gauche	Liste des profils créés.
A droite	Boutons d'action sur le profil sélectionné.

Le tableau d'indication des différents types de profils créés affiche les données suivantes :

Nom du profil	Indique le nom donné au profil.
Description	descriptif du profil. Il peut être utile d'indiquer ici le niveau de sévérité. **Exemple** severity==1or2=>level=minor, severity==3or 4=>level=major

15.1.4.1. Liste des profils

Dans cette partie de la boite de dialogue se trouve la liste des profils. Il en existe 4 par défaut.
Chaque profil possède un nom et une description.

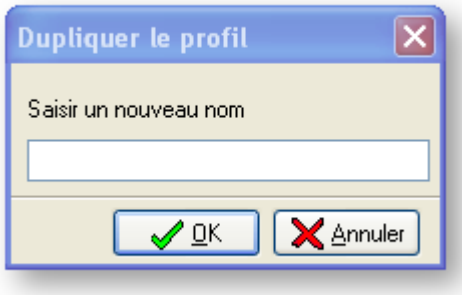
Le profil créé devra ensuite être associé à un objet.

AVERTISSEMENT
Il ne peut y avoir qu'un seul profil associé à un objet.

Un profil est dit sélectionné quand vous faites un simple clic de la souris sur son nom. La sélection faite, vous pouvez le supprimer ou le dupliquer.

15.1.4.2. Actions possibles

Vous pouvez réaliser différentes actions à partir de cet écran :

Ajouter	Ce bouton permet d'ajouter un profil au tableau. **NOTE** Le profil créé est automatiquement ajouté dans l'arborescence de la configuration de SEISMO.
Supprimer	Sélectionnez le profil à supprimer puis cliquez sur le bouton. Le profil Default-All ne peut pas être supprimé. **AVERTISSEMENT** Aucun message ne vous demande de confirmer la suppression du profil. **Cette suppression est donc instantanée.**
Dupliquer	Sélectionnez le profil que vous souhaitez dupliquer. L'écran suivant s'affiche :  *Figure 397 : Dupliquer le profil* Entrez un nom pour ce profil et cliquez sur **OK**. Le nouveau profil s'affiche dans le tableau et dans l'arborescence des menus de SEISMO. Les règles de ce nouveau profil sont celles du profil préalablement dupliqué.

15.1.4.3. Edition d'un profil

Référez-vous à la procédure suivante pour éditer un profil :

1. Sélectionnez un profil dans le menu de l'arborescence **`Profils`**. La boîte de dialogue des règles du profil sélectionné s'affiche.

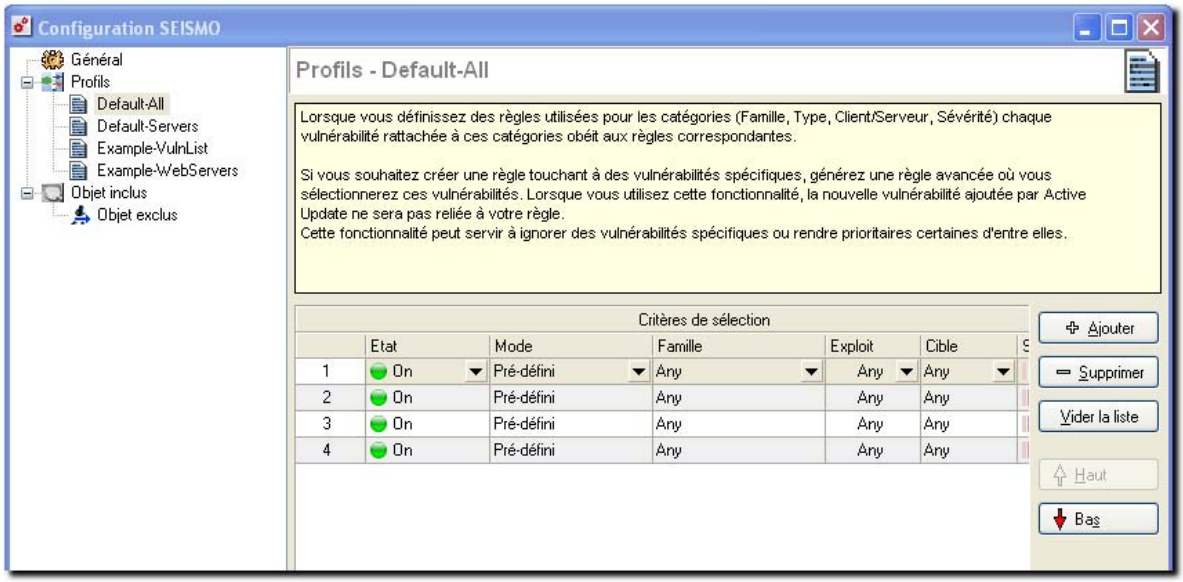


Figure 398 : Configuration SEISMO - Profils

Cette fenêtre est composée de deux zones :

- Une zone comportant les règles de vulnérabilités sous la forme d'un tableau.
- Une zone d'actions possibles.

Règles de vulnérabilités

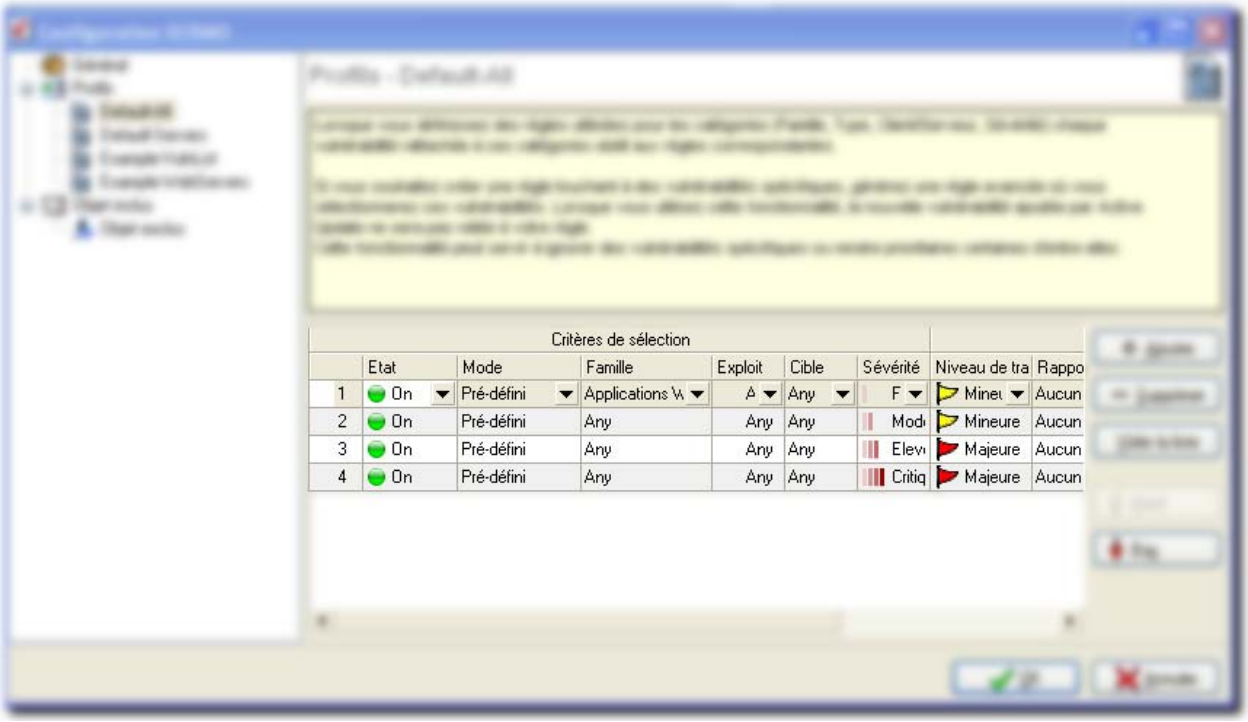


Figure 399 : Critères de sélection

Cette grille vous permet de définir les règles utilisées pour chaque profil de vulnérabilités à appliquer. Faites attention à bien ordonner vos règles afin d'avoir un résultat cohérent. En effet, le firewall exécute les règles dans l'ordre d'apparition à l'écran et s'arrête dès qu'une action s'applique au flux qui tente de le traverser. Il convient donc de définir les règles dans l'ordre du **plus détaillé au plus général.**

ID	N° de la règle.
Etat	2 états possibles : **On** et **Off**. Une lumière verte signifie que cette règle sera appliquée, une lumière rouge signifie qu'elle ne sera pas appliquée. Ceci permet de définir des règles qui seront utilisées ultérieurement ou de désactiver temporairement certaines règles pour faire des tests.
Mode	2 modes possibles : **Prédéfini** et **Personnalisé**. En mode prédéfini, la règle s'applique à une famille de vulnérabilités (par exemple, la famille Peer to Peer) alors qu'en mode Personnalisé le choix est affiné : vous pouvez choisir les vulnérabilités d'une famille pour lesquelles sera appliquée la règle. (Par exemple, vous pouvez ne choisir que 2 vulnérabilités de la famille Client FTP). Ici, chaque vulnérabilité contient une sévérité propre.
Famille	Famille à laquelle appartient la vulnérabilité. Le contenu est dynamique. (*Cf. Annexe*). **Exemple** • Serveur DNS • Client FTP
Exploit	L'accès à la vulnérabilité peut s'effectuer en local ou à distance (par le réseau) ou les deux. Il permet d'exploiter la vulnérabilité.
Cible	On détermine ici quelle est la cible liée à la règle. 3 modes possibles : **Any**, **Client** et **Serveur**.
Sévérité	Niveau de sévérité de la vulnérabilité : il en existe 6 : Any, Informations, Faible, Modéré, Elevé, Critique.
Niveau de traces	3 niveaux de logs : Ignorer, Mineure et Majeure.
Rapport détaillé	Il est possible d'effectuer des envois des listes de vulnérabilités aux personnes susceptibles d'administrer et d'analyser les logs. Il faut avoir, au préalable créé les groupes de personnes pour l'envoi du rapport par e-mail. Cette configuration est générée à partir du menu E-mails de l'arborescence de NETASQ UNIFIED MANAGER.
Rapport simplifié	Possibilité d'envoyer un rapport simplifié des listes de vulnérabilités à un autre groupe de destinataires. Il faut avoir, au préalable créé les groupes de personnes pour l'envoi du rapport par e-mail. Cette configuration est générée à partir du menu E-mails de l'arborescence de NETASQ UNIFIED MANAGER.
Description	Descriptif associé à la règle.

Actions possibles sur les règles

Ajouter	Ajoute une règle au profil sélectionné.
Supprimer	Supprime une règle préalablement sélectionnée.
Vider lakiste	Supprime la liste des règles du profil.
Haut	Remonte ligne à ligne la règle préalablement sélectionnée.
Bas	Descend ligne à ligne la règle préalablement sélectionnée.

Une ligne est sélectionnée quand l'un de ses éléments est sélectionné (en inverse vidéo).

15.1.4.4. Création des règles de vulnérabilité

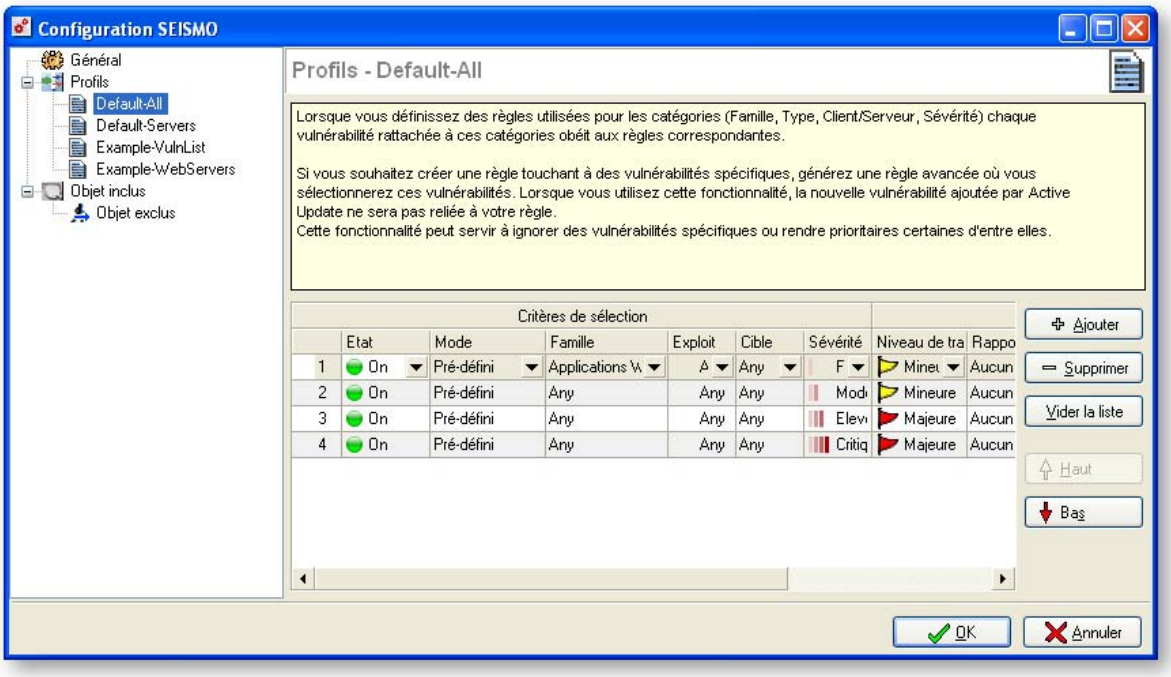


Figure 400 : Configuration SEISMO - Profils

Cette section détaille la création de vos règles de vulnérabilités. L'ordre de ces règles est important car le firewall les parcourt du haut vers le bas et s'arrête dès qu'il trouve une règle correspondant au paquet IP (sauf s'il exécute uniquement une option).

Activation et désactivation d'une règle

On : La règle est activée pour filtrer les vulnérabilités.
Off : La règle n'est pas activée pour filtrer les vulnérabilités.

L'activation et la désactivation d'une règle facilitent la mise au point de vos filtres. Une règle désactivée n'est pas prise en compte par le firewall NETASQ lors de l'utilisation du profil.

15.1.5. Objet inclus et exclus

Une fois les profils créés, vous pouvez leur associer les objets concernés. L'objet sera ainsi analysé par le moteur NETASQ SEISMO qui se basera sur les règles créées dans un profil.

Le choix des objets concernés par le profil que vous voulez mettre en place s'effectue à partir du menu de l'arborescence **`Seismo\Objets inclus`**. La fenêtre suivante s'affiche :

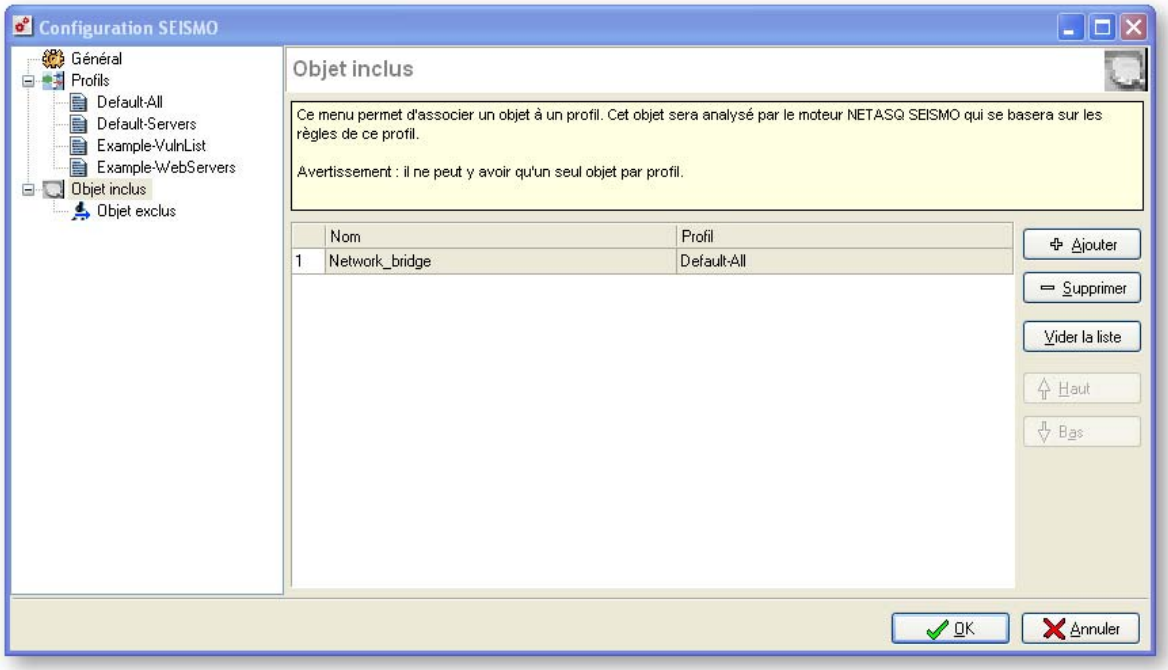


Figure 401 : Configuration SEISMO - Objet inclus

Cette fenêtre est composée de deux zones :

- Une zone affichant les objets inclus.
- Une zone d'actions possibles pour ajouter, supprimer des objets.

15.1.5.1. Choix de l'objet

L'objet lié à la règle est toujours une machine, un groupe de machines ou un réseau.

Pour ajouter un objet :

1. Cliquez sur le bouton **Ajouter** puis sélectionnez un objet dans la base d'objets. L'écran suivant s'affiche :

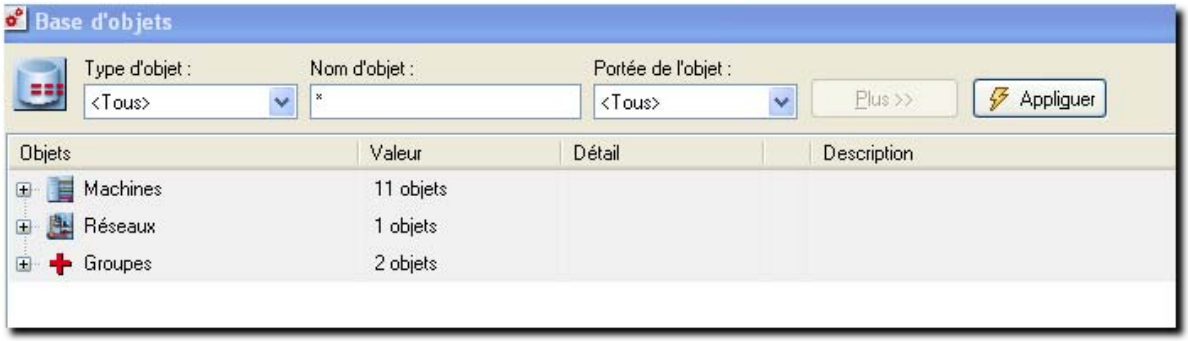


Figure 402 : Base d'objets

2. Sélectionnez l'objet puis cliquez sur **OK**.

15.1.5.2. Choix du profil

Pour choisir le profil :

1. Cliquez sur le triangle qui apparaît lorsque vous êtes dans la colonne "Profil" afin de choisir le profil lié à l'objet.
2. Cliquez sur **OK** pour valider la liste des objets inclus.

15.1.5.3. Objet exclus

Une fois les objets associés à un profil, il est possible d'exclure ou plusieurs objet(s) de l'analyse de NETASQ SEISMO.

➔ Le choix des objets à exclure s'effectue à partir du menu de l'arborescence **`Seismo\Objets exclus`**. La fenêtre suivante s'affiche :

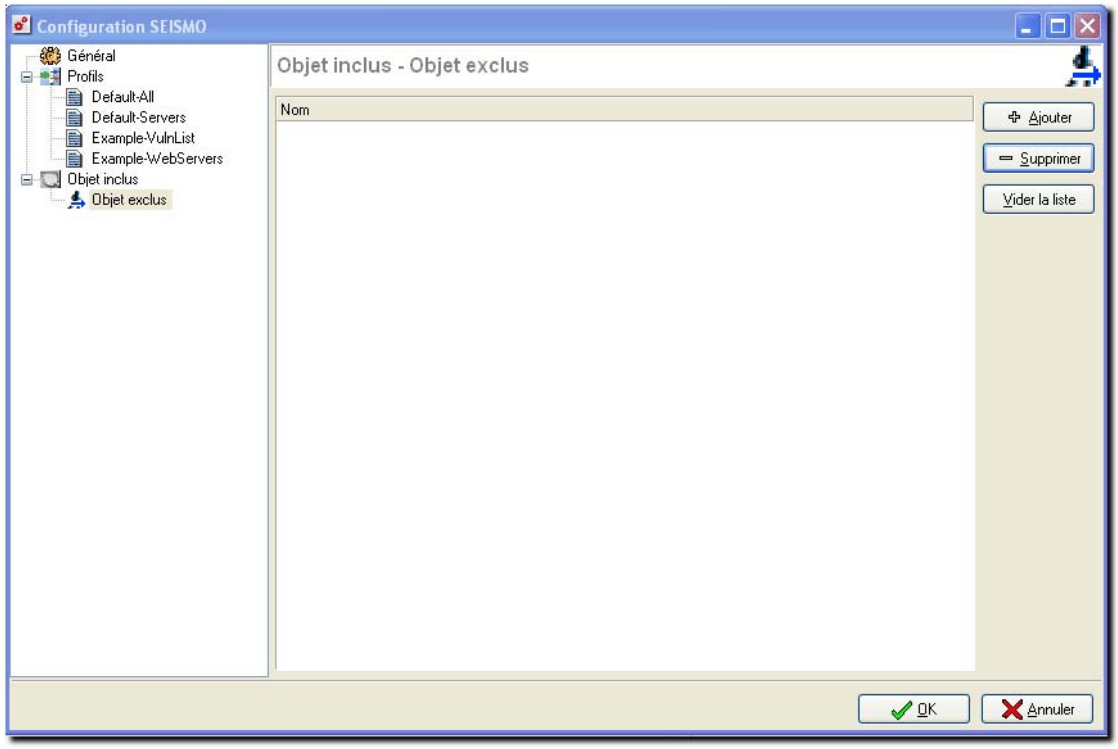


Figure 403 : Configuration SEISMO - Objet exclus

Pour exclure un objet :

1. Cliquez sur le bouton Ajouter afin de sélectionner l'objet à exclure dans la base d'objets.
2. Cliquez sur **OK** pour valider votre choix. L'écran des objets exclus s'affiche.
3. Cliquez sur **OK** pour valider la configuration.

PARTIE 16 : CONFIGURATION DES MAILS

16.1.1. Introduction

16.1.1.1. Pour cette partie, vous devez connaître

Les paramètres de configuration du server e-mail et les groupes que vous voulez instaurer.

16.1.1.2. Utilité de la partie

Cette partie vous permet de définir la configuration du système d'e-mail afin de permettre au firewall NETASQ d'envoyer des e-mails lorsque certains événements surviennent. Elle permet d'administrer les groupes pour les envois de mails. Vous pouvez également configurer l'envoi des alarmes à un groupe mail. Enfin, il existe des modèles d'e-mail préconfigurés.

NOTE
NETASQ SEISMO bénéficie de son propre écran de configuration pour l'envoyer des rapports simplifiés et détaillés concernant les vulnérabilités.

16.1.1.3. Introduction à cette partie

La gestion de la messagerie utilisée dans les différentes applications est désormais centralisée dans NETASQ UNIFIED MANAGER.

A partir de cet écran, vous pouvez :

- Effectuer la configuration de l'accès à un serveur de mail.
- Définir les groupes de destinataires.
- Définir le groupe de destinataires pour l'envoi des alarmes de prévention d'intrusion (ASQ) et pour les évènements système.
- Modifier les modèles de mails préconfigurés.

16.1.1.4. Accéder à cette partie

Accédez à la boîte de dialogue par le menu de l'arborescence **E-mails.**

15.1.2. Configuration du serveur d'e-mails

Cet écran regroupe tous les paramètres nécessaires à la configuration de l'accès du firewall à un serveur d'e-mails.
L'écran de configuration comporte les champs suivants :

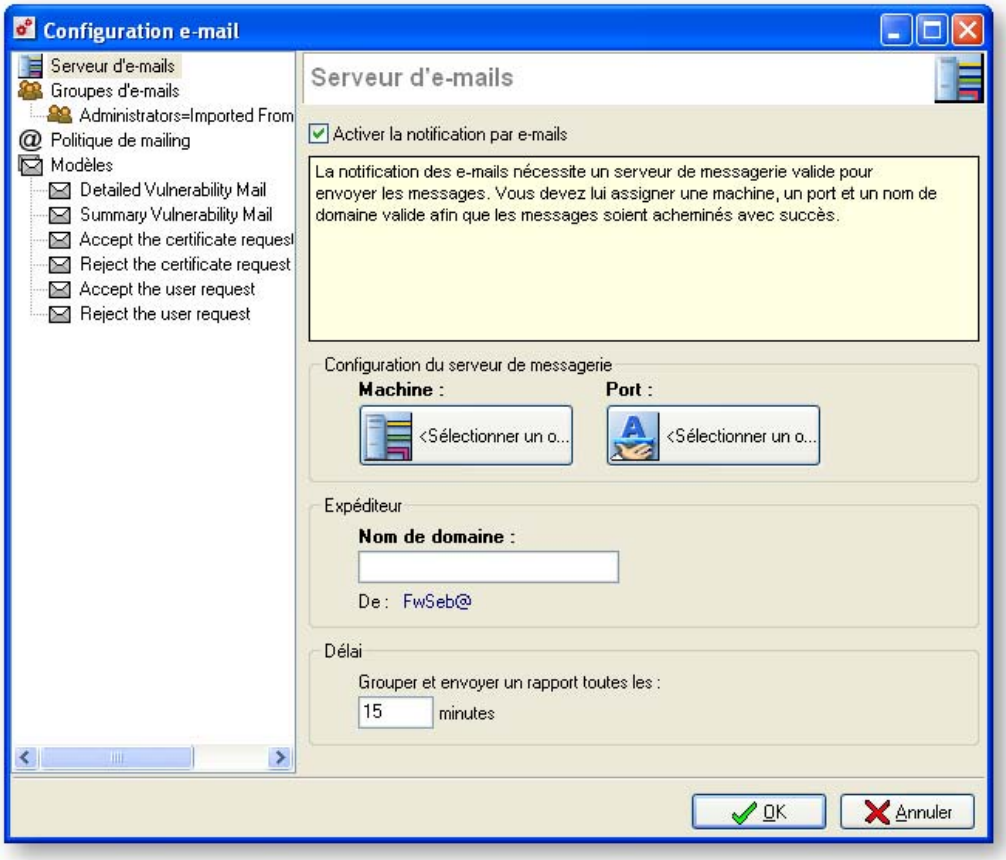


Figure 404 : Configuration e-mail - Serveur d'e-mails

Activer la notification par e-mails	Active l'envoi des messages. En cas de désactivation, aucun élément de configuration ne sera accessible car le firewall n'enverra pas de mail. **REMARQUE** La notification des e-mails nécessite un serveur de messagerie capable de recevoir les e-mails provenant du firewall.
Machine (*)	Indication de la machine (serveur SMTP) à qui le firewall va envoyer les mails en la sélectionnant dans la base d'objets.
Port (*)	Port du serveur SMTP où seront envoyés les e-mails.
Nom de domaine (*)	Utile pour indiquer le nom de l'émetteur des e-mails. L'adresse e-mail de l'émetteur sera alors indiquée comme suit : <nom_du_firewall>@<nom_de_domaine>.
Grouper et envoyer un rapport toutes les	Cette option vous permet de spécifier la fréquence d'envoi des rapports. Un rapport contient toutes les alarmes détectées depuis le rapport précédent. Ainsi, la réception du mail s'effectue par tranche horaire et non par alarme déclenchée.

16.1.3. Groupes d'e-mails

Un groupe rassemble un certain nombre d'adresses e-mail.
Il est possible de créer jusqu'à 50 groupes.
Il n'existe aucun groupe préconfiguré. Vous pouvez ajouter de nouveaux groupes, modifier leurs noms et descriptions, ou encore les supprimer.
Un groupe doit contenir au moins une adresse e-mail. Le nombre d'adresse e-mails dans un groupe est indéfini.

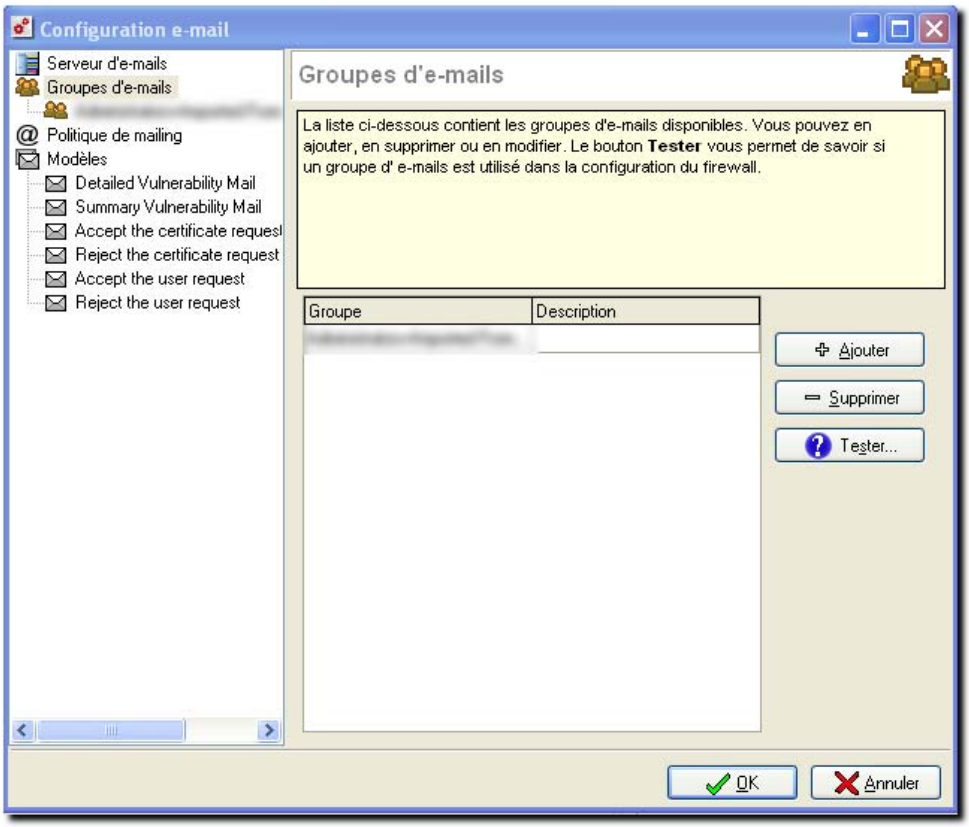


Figure 405 : Groupes d'e-mails

La liste ci-dessus affiche les groupes d'e-mails créés. Vous pouvez créer des groupes ou en supprimer.
Il sera possible ensuite de choisir un groupe pour l'envoi des rapports détaillés ou simplifiés dans le menu SEISMO.

Créer un groupe

1 Cliquez sur le bouton **Ajouter.** Une ligne supplémentaire s'affiche dans la liste et dans l'arborescence de la configuration des e-mails.
2 Modifiez le nom du groupe si nécessaire (ce nom est unique). Vous pouvez également attribuer une description à ce groupe.

Une fois le groupe créé, il apparaît dans l'arborescence de la configuration d'e-mails.

La saisie de l'adresse e-mail est libre mais le format de l'adresse est vérifié. Il est possible également d'ajouter un utilisateur de la base d'objets plutôt qu'un e-mail.

Supprimer un groupe

1 Sélectionnez la ligne à supprimer. Celle-ci apparaît en inverse-vidéo.
2 Cliquez sur le bouton **Supprimer**. Le groupe est supprimé de la liste et de l'arborescence de l'écran de configuration e-mail sans message de confirmation.

REMARQUE
La suppression d'un groupe ne peut être réalisée que si le groupe n'est pas utilisé dans une autre configuration du firewall.

Tester

Le bouton **Tester** permet de vérifier si un groupe d'e-mails est utilisé dans les différents modules de configuration du firewall afin de pouvoir le supprimer en toute sécurité ensuite.

1 Sélectionnez la ligne à tester.
2 Cliquez sur le bouton **Tester** afin d'effectuer la vérification.

16.1.4. Configuration de la politique de mailing

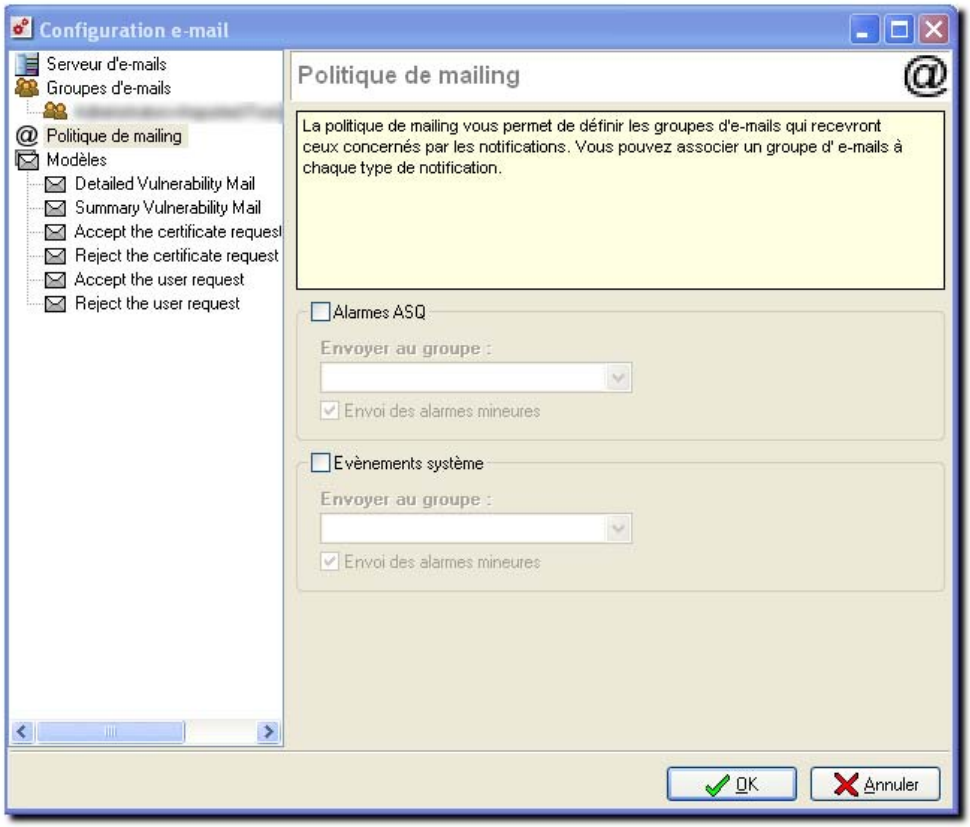


Figure 406 : Politique de mailing

La politique de mailing vous permet de notifier un groupe qui recevra les alarmes ASQ et un groupe (qui peut être différent) pour la réception des évènements système.
La liste des alarmes ainsi que les événements système sont envoyés dans le corps de l'e-mail au groupe spécifié.
Le délai d'envoi du rapport des alarmes et des évènements système se modifie dans le champ "Délai" du menu **`Serveur d'e-mails`**.

> **Exemple**
> Si vous spécifiez un envoi toutes les 15 minutes dans le champ "Délai", vous serez averti par e-mail toutes les 15 minutes des alarmes et événements système produits durant ce laps de temps sur le firewall.

En cochant l'option **Envoi des alarmes mineures**, le groupe recevra également la liste des alarmes mineures. (Les alarmes majeures sont systématiquement envoyées).

Le groupe spécifié pour recevoir les événements système obtiendra la liste des traces Système contenant la date de l'évènement ainsi que le service et le message de l'événement.

> **Exemple**
> 07:17:39 sysevent Active Update : update successful Kaspersky.

> **AVERTISSEMENT**
> Les envois d'e-mails par la levée d'une alarme se configure, alarme par alarme, dans le menu *Partie 6 : Prévention d'intrusion (ASQ).*

16.1.5. Modèles

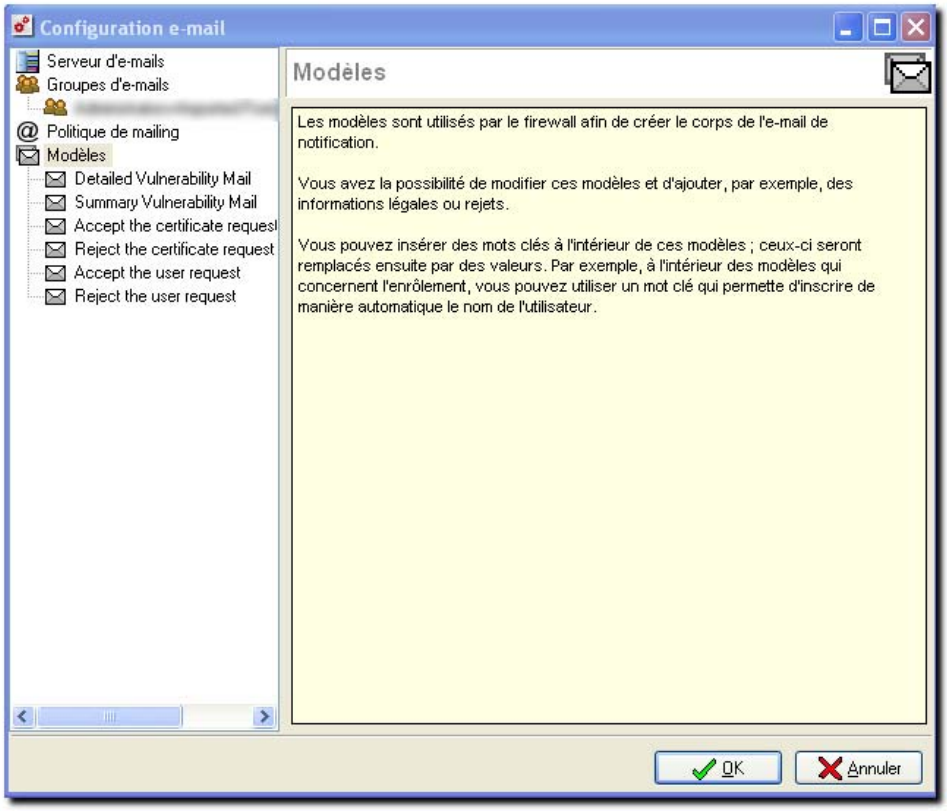


Figure 407 : Modèles

Liste

Les modèles d'e-mails servent au firewall pour créer des e-mail émis vers le serveur d'e-mails. Six modèles d'e-mails sont disponibles, contenant chacun, un corps qui diffère selon le message que l'on veut envoyer :

- E-mail de détail d'une vulnérabilité.
- E-mail de résumé d'une vulnérabilité.
- E-mail pour une requête d'enrôlement utilisateur acceptée (a).
- E-mail pour une requête d'enrôlement utilisateur refusée (a).
- E-mail pour une requête de certificat utilisateur acceptée (a).
- E-mail pour une requête de certificat utilisateur refusée (a).

(a) Ces modèles sont utilisés dans les l'enrôlement des utilisateurs.

Contenu

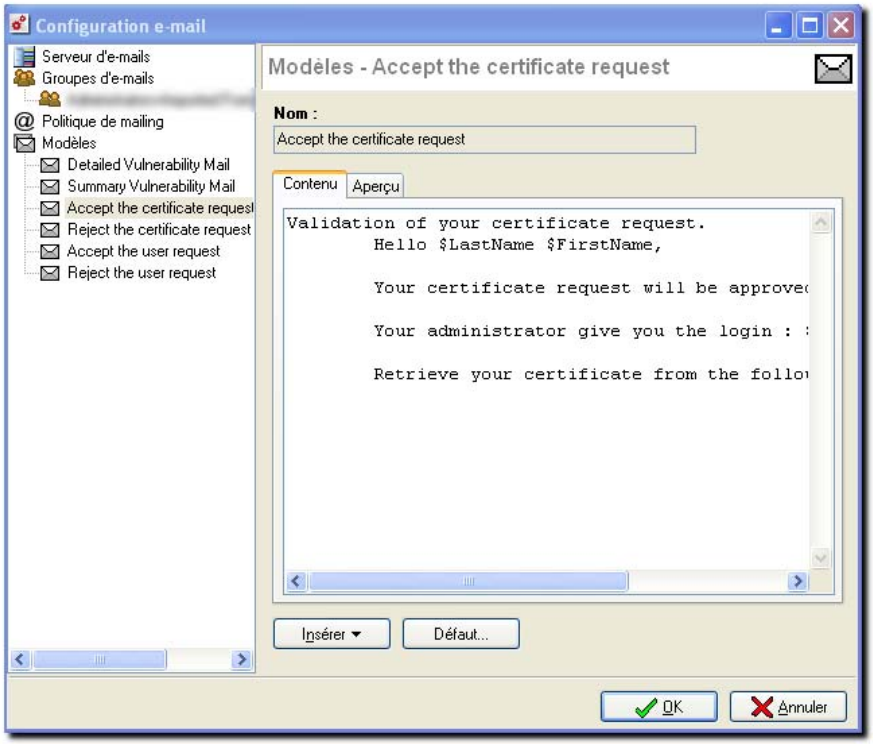


Figure 408 : Configuration e-mail - Contenu

Chaque modèle comporte du contenu appelé "body" (comme pour une page HTML). Ce contenu est un texte au format libre qui peut contenir des balises HTML simples afin de finaliser la mise en forme.

Ces modèles sont modifiables. Ils peuvent contenir des mot-clés qui seront remplaçés ensuite par des valeurs. Par exemple, un mot-clé peut afficher de manière automatique le nom de l'utilisateur.

2 boutons vous permettent de modifier le corps du message :

Insérer	Ce bouton vous permet de sélectionner des mots-clés qui seront ensuite remplacés par des valeurs réelles lors de l'envoi du message.
Défaut...	Permet de réinitialiser le modèle à sa présentation initiale. Lorsque vous cliquez sur ce bouton, le message suivant s'affiche : "Confirmer la réinitialisation du modèle "Nom du modèle" ?"

Liste des champs spéciaux

Modèles "Detailed Vulnerability Mail" et "Summay Vulnerability Mail" :

- $Title : Sujet de l'e-mail
- $SubTitle : Sous-tutre de l'e-mail
- $MailSummary : Résumé de l'e-mail
- $VulnSummary : Résumé des vulnérabilités
- $HostsByVuln : Liste des machines affectées par les vulnérabilités
- $VulnByProduct : Liste des vulnérabilités par produit
- $Footer : Pied de page de l'e-mail

Modèles pour l'enrôlement Web (user/certificate request)

- $LastName : Nom de famille de la personne enrôlée
- $FirstName : Prénom de la personne enrôlée
- $Date : Date de la demande d'enrôlement
- $UID : Identifiant (login) de la personne
- $URL : URL du site d'enrôlement pour télécharger son certificat (en cas d'approbation)

Aperçu

Cet écran vous permet d'obtenir un aperçu du modèle d'e-mail.

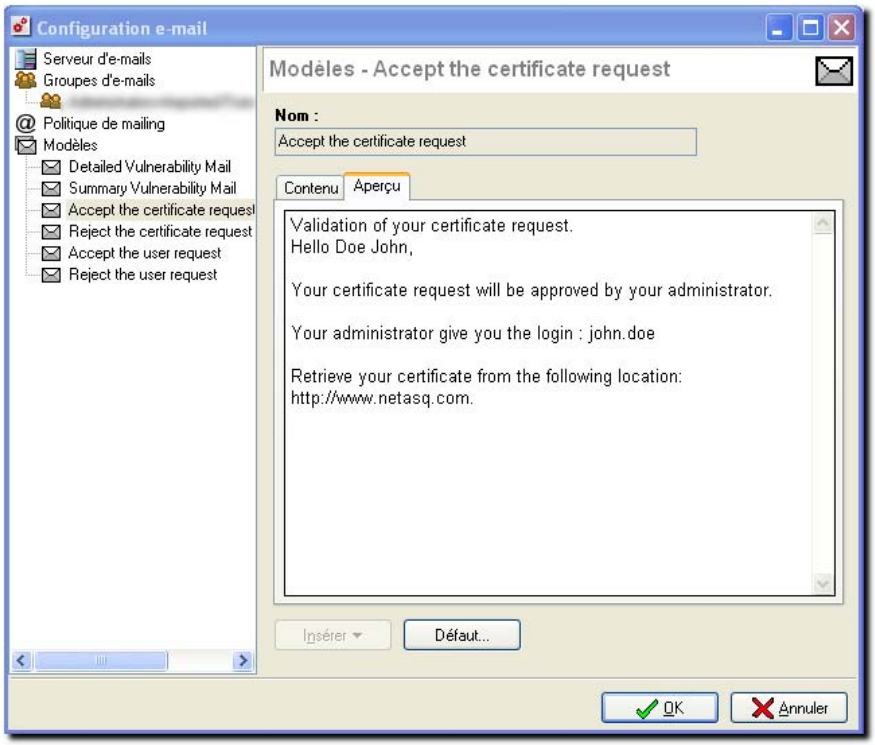


Figure 409 : Configuration e-mail - Aperçu

Exemple de rapport reçu par e-mail pour les alarmes

Type	minor
Action	pass
Date	2006-03-02 12:47:20
Interface	in
Protocol	tcp
Source	192.168.6.1:2756 (peer_192_168_6_1:2756)
Destination	10.2.0.110:80 (PPTP_DNS:http)
Description	Suite de slash dansl'URL

PARTIE 17 : GESTION DES TRACES

CHAPITRE 1. CONFIGURATION DES TRACES

17.1.1. Introduction

17.1.1.1. Pour cette partie, vous devez avoir franchi les étapes

- Partie 2/Chapitre 1 : Interface graphique.
- Partie 2 : Installation, intégration et pré-configuration.
- Définition des interfaces, des objets et de la configuration du noyau.
- Mise en place des politiques (translations, filtrage, VPN).
- Partie 9 : Configuration des proxies.
- Configuration de l'authentification.
- Partie 14 : Haute Disponibilité.

17.1.1.2. Pour cette partie, vous devez connaître

- La façon dont vous voulez être informé des alarmes.
- Les statistiques dont vous avez besoin.

17.1.1.3. Utilité de la partie

Cette partie vous permet de configurer la gestion des différents fichiers de traces et de configurer les statistiques. Elle vous permet aussi de rediriger les traces vers un serveur SYSLOG externe.

17.1.1.4. Introduction à cette partie

Le firewall gère un certain nombre de fichiers de traces destinés à recueillir les événements détectés par les fonctions de journalisation. Les fichiers concernés par les événements de sécurité sont :

- **Politiques de Filtrage** : événements liés à l'application des fonctions de filtrage.
- **Serveur :** événements liés au serveur d'administration des firewalls : "serverd".
- **Alarmes** : événements liés à l'application des fonctions de prévention des intrusions.
- **Web :** événements liés au trafic Web.
- **SMTP :** événements liés pour le trafic SMTP.
- **VPN** : événements liés à l'établissement des SA.
- **Connexion :** événements liés aux connexions à travers et à destination du firewall.
- **Authentification** : événements liés à l'authentification des utilisateurs.
- **Evénements Système** : arrêt/démarrage des fonctions de journalisation. Plus généralement : c'est dans ce journal que sont enregistrés les événements liés directement au système : arrêt/démarrage du firewall,

erreur système, etc. L'arrêt et démarrage des fonctions de journalisation correspondent à l'arrêt et au démarrage des « démons » qui génèrent les traces.

- **Plugins :** événements liés au traitement des plugins de l'ASQ.
- **VPN SSL :** événements liés à l'établissement du VPN SSL.
- **POP3 :** événements lié à l'envoi des messages.
- **Monitor :** événements lié au monitoring temps réel.
- **SEISMO :** événements liés à l'application de consultation des vulnérabilités sur le réseau NETASQ SEISMO.

Les fichiers partagent un espace global de stockage avec d'autres fichiers de traces. L'administrateur possédant les droits "*+M " peut spécifier le pourcentage maximum que chacun des fichiers de traces peut occuper dans cet espace total.

Lorsque le seuil maximum est atteint, le firewall entreprend une action paramétrée, pour chaque fichier, parmi les trois suivantes :

- **Assurer la Rotation des fichiers** : les traces les plus récentes effacent les traces les plus anciennes.
- **Stopper l'écriture des fichiers** : les traces ne sont plus mémorisées sur le firewall.
- **Arrêter le firewall** : le firewall ne s'arrête pas réellement mais il bloque l'ensemble des flux excepté les connexions du firewall depuis le réseau interne.

Les fichiers "Authentification" ont chacun un espace alloué fixe et sont protégés par des actions de rotation en cas de saturation.

17.1.1.5. Accéder à cette partie

Accédez à la boîte de dialogue par le menu **Traces** de l'arborescence.

17.1.2. Log

En sélectionnant le menu **Traces** de l'arborescence de l'interface graphique de configuration NETASQ, l'écran de configuration des traces apparaît.

La configuration des traces permet d'allouer de l'espace disque pour chaque type de traces du firewall. Ce menu permet également la modification du comportement du firewall lors de l'enregistrement et l'envoi de ces traces.

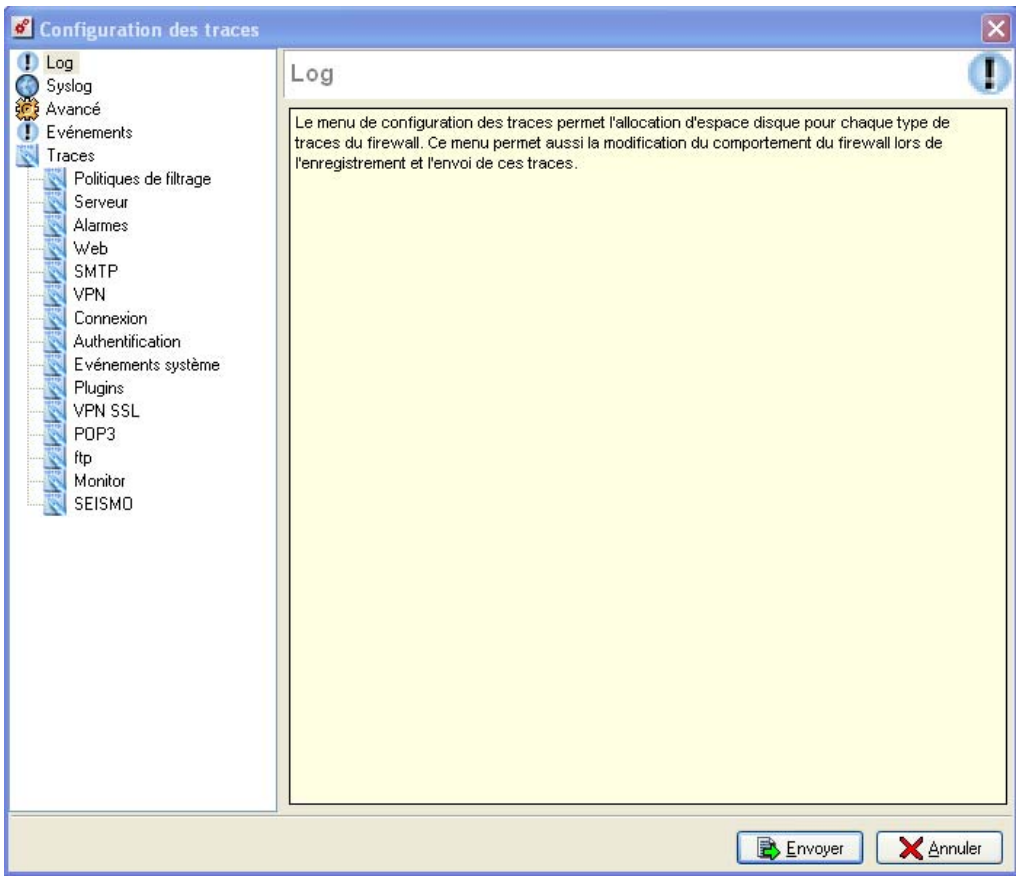


Figure 410 : Configuration des traces - Log

Cet écran est divisé en deux parties :

- A gauche : un arbre présentant les diverses fonctionnalités du menu **Traces.**
- A droite : les options configurables.

17.1.3. Syslog

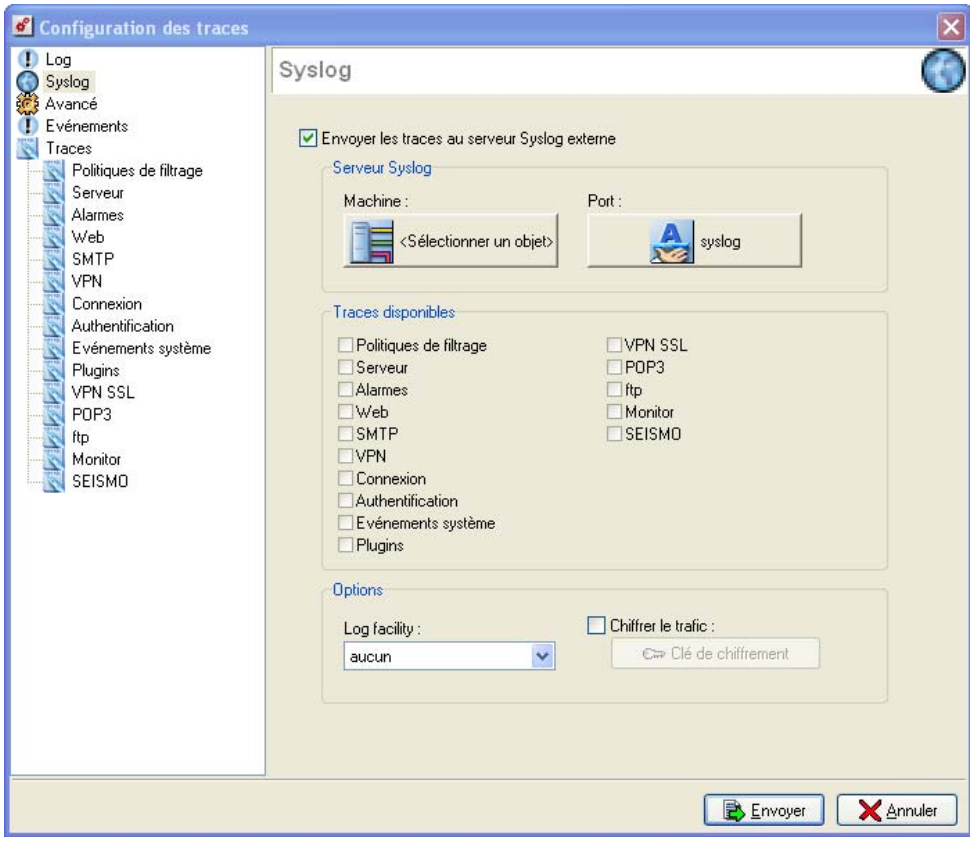


Figure 411 : Configuration des traces - Syslog

17.1.3.1. Envoyer les traces au serveur Syslog externe

Le firewall NETASQ vous permet d'envoyer automatiquement les traces vers un serveur dédié. Les traces sont envoyées au format WELF. Ce serveur peut être un serveur SYSLOG ou le NETASQ SYSLOG. Les traces peuvent aussi être récupérées par le NETASQ LOG ANALYZER.
Pour envoyer les traces, il suffit de cocher la case **Envoyer les messages au serveur Syslog externe** puis de donner l'adresse IP du serveur ainsi que le port de communication associé au serveur.

Vous pouvez aussi sélectionner le log facility (c'est un aiguillage vers différents fichiers afin de trier les informations) sur lequel sont envoyées les traces ainsi que les catégories de fichiers à envoyer (Alarme, connexion, Web, filtrage…).

17.1.3.2. Envoi des traces vers le NETASQ SYSLOG ou le NETASQ LOG ANALYZER

Le NETASQ SYSLOG est un utilitaire installé sur une machine d'administration qui offre un service SYSLOG pour la récupération et la gestion de traces. Cet utilitaire est particulièrement intéressant pour les firewalls U30 et U70 qui ne peuvent pas stocker les traces sur le firewall. Les traces sont alors stockées en local sur la machine d'administration.

Le NETASQ LOG ANALYZER est un outil plus évolué développé par NETASQ et disponible en option. Il peut récupérer les logs de différents firewalls et les stocker dans une base SQL, apportant plus de performance dans les traitements de données.

Les traces peuvent être envoyées au NETASQ SYSLOG en indiquant l'adresse IP de la machine sur laquelle est installé l'outil ainsi que le port utilisé.

Les communications entre le firewall et le NETASQ SYSLOG peuvent être chiffrées en AES à partir du firewall. Pour cela, activez l'option **Chiffrer le trafic** et indiquez la clé de chiffrement utilisée en cliquant sur le bouton **Clé de chiffrement.**

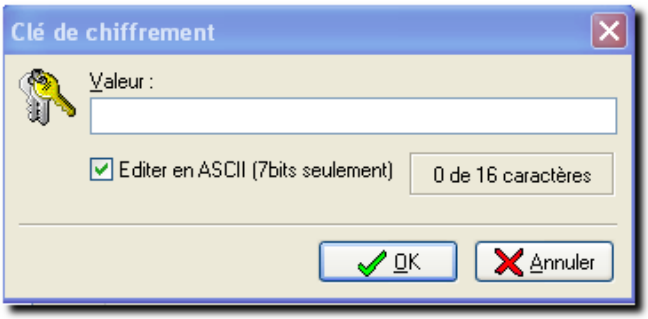


Figure 412 : Clé de chiffrement

Il suffit de spécifier la clé de chiffrement dans la zone Valeur.

> **AVERTISSEMENT**
> Le chiffrement n'est utilisable que pour une redirection des logs vers le NETASQ SYSLOG et pas pour un serveur SYSLOG quelconque. L'option Chiffrer le trafic doit donc être désactivée pour un serveur Syslog quelconque. Par contre il est fortement conseillé d'activer le chiffrement pour le Syslog NETASQ. Les communications entre les firewalls et le Log Analyzer sont, elles, toujours chiffrées.

Les traces peuvent aussi être conservées sur le firewall (sauf modèles U30 et U70).

Pour configurer le NETASQ SYSLOG :

1. Activez l'option **Envoyer les traces au serveur SYSLOG externe.**
2. Indiquez la machine d'administration sur laquelle est installé le NETASQ SYSLOG à l'aide du bouton **Sélectionner un objet** puis cliquez sur le bouton **Syslog** et vérifiez que le port de connexion est à la valeur 514.
3. Spécifiez les types de traces qui seront envoyées du firewall au NETASQ SYSLOG (Politiques de filtrage, Serveur, Alarmes, Web, SMTP, VPN, Connexion, Authentification, Evénements système, Plugins, VPN SSL, POP3, Monitor, SEISMO).
4. Le Log facility doit être sélectionné sur **aucun.**
5. **Chiffrer le trafic** : Le flux transitant entre le firewall et le NETASQ SYSLOG peut être chiffré en AES. Pour activer le chiffrement, sélectionnez l'option **Chiffrer le trafic** puis cliquez sur le bouton **Clé de chiffrement**. Saisissez alors la clef de chiffrement utilisée (la même valeur de clef sera configurée sur le NETASQ SYSLOG). **Le chiffrement doit alors obligatoirement être activé sur le NETASQ SYSLOG.**

17.1.4. Avancé

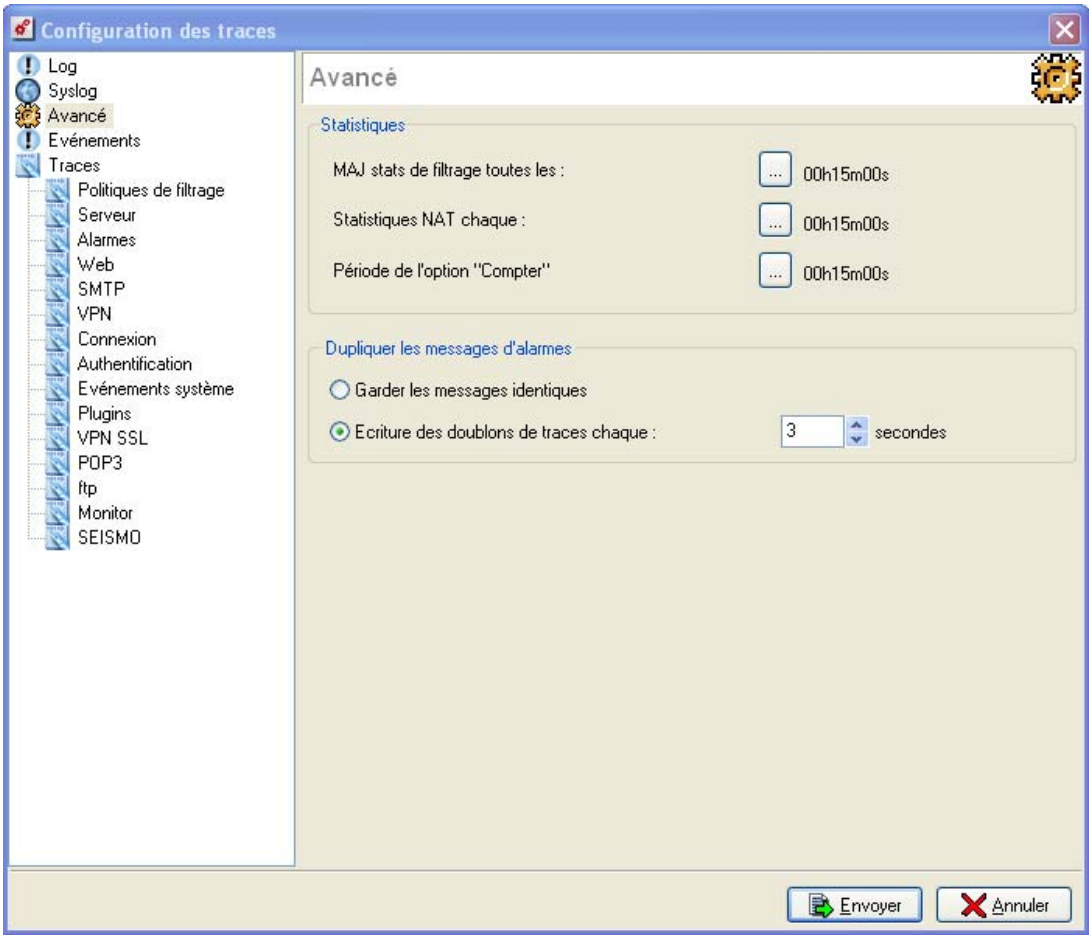


Figure 413 : Configuration des traces - Avancé

17.1.4.1. Statistiques

Ce menu vous permet de configurer plusieurs types de statistiques :

- Indication de la durée pour la mise à jour des statistiques du filtrage.
- Indication de la durée pour les statistiques NAT.
- Taux de rafraîchissement des règles de filtrage contenant l'option "Compter".

Pour chaque partie il vous suffit de sélectionner la fréquence du calcul des statistiques.

Un rapport sera généré pour chaque période que vous configurez.

Une fois vos choix effectués, appuyez sur le bouton **Envoyer** pour envoyer les informations au Firewall NETASQ.

Nous vous conseillons de n'utiliser les granularités inférieures à une journée que sur une courte durée afin d'éviter de saturer le disque du firewall NETASQ.

17.1.4.2. Dupliquer les messages d'alarmes

Deux options dans la zone "Dupliquer les messages d'alarmes" sont disponibles dans le menu avancé :

- **Garder les messages identiques** : dans ce cas toutes les alarmes sont inscrites dans les logs (même si elles sont identiques).
- **Ecriture des doublons de traces chaque** : ici vous sélectionnez une fenêtre de temps dans laquelle même si une alarme est remontée plusieurs fois, elle n'est inscrite qu'une seule fois dans les logs.

17.1.5. Evénements

Ce menu vous permet de modifier les actions par défaut à entreprendre lors de la remontée de certains types d'événements. Ceux-ci sont indépendants des conditions de trafic. La liste présentée dans cette fenêtre regroupe tous les événements que peut générer un firewall.

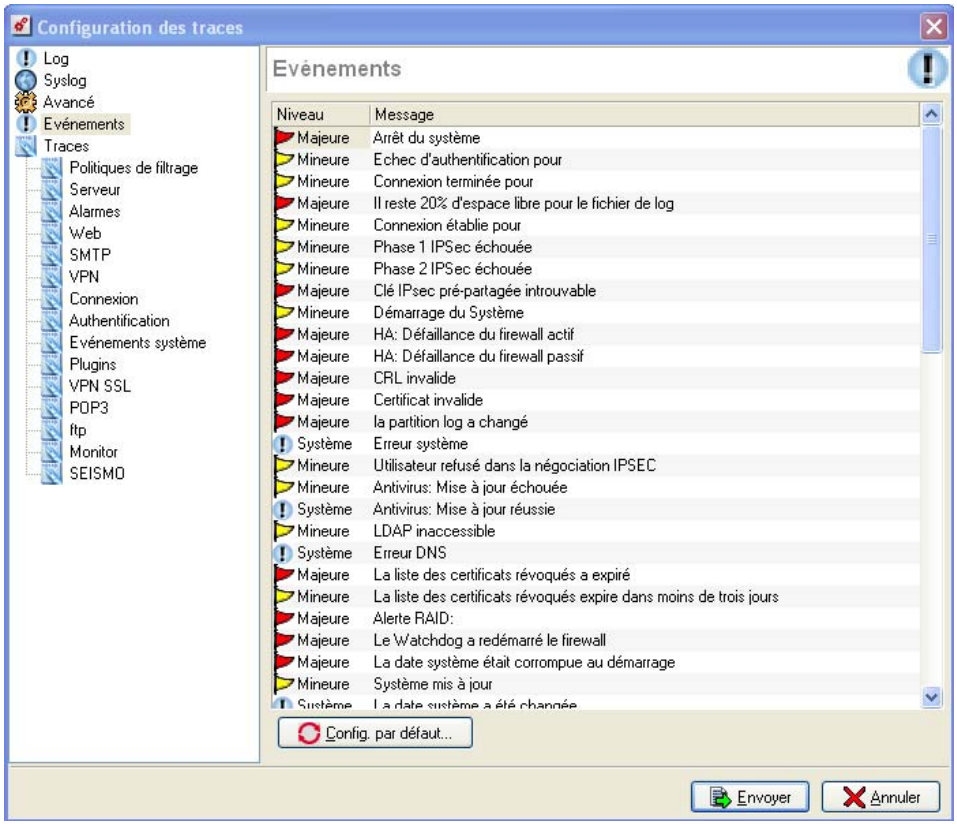


Figure 414 : Configuration des traces - Evénements

La grille se divise en deux :

- A gauche figurent les actions à entreprendre lors de la remontée d'un événement.
- A droite figure le type d'événement.

Les différentes actions possibles dans la colonne "Niveau" sont :

Ignorer	Aucune notification.
Mineure	Génère une alarme mineure.
Majeure	Génère une alarme majeure.

Système	Génère une entrée dans le journal d'audit système.

Le bouton **Config. par défaut** vous permet de redéfinir les paramètres d'événements dans leur configuration d'origine. Lorsque vous cliquez sur ce bouton, le message suivant s'affiche :

"La configuration par défaut va être appliquée au firewall. Continuer ?"

Une fois vos modifications effectuées, vous devez les envoyer au firewall NETASQ avec le bouton **Envoyer**.

17.1.6. Traces

Ce menu vous donne la possibilité de configurer plusieurs paramètres liés aux traces: leur taille, l'action à entreprendre lorsque le seuil est atteint, etc. Lorsque vous sélectionnez ce menu, la fenêtre principale du menu vous présente un aperçu graphique de la répartition actuelle de l'espace réservé pour chacun des fichiers de traces.

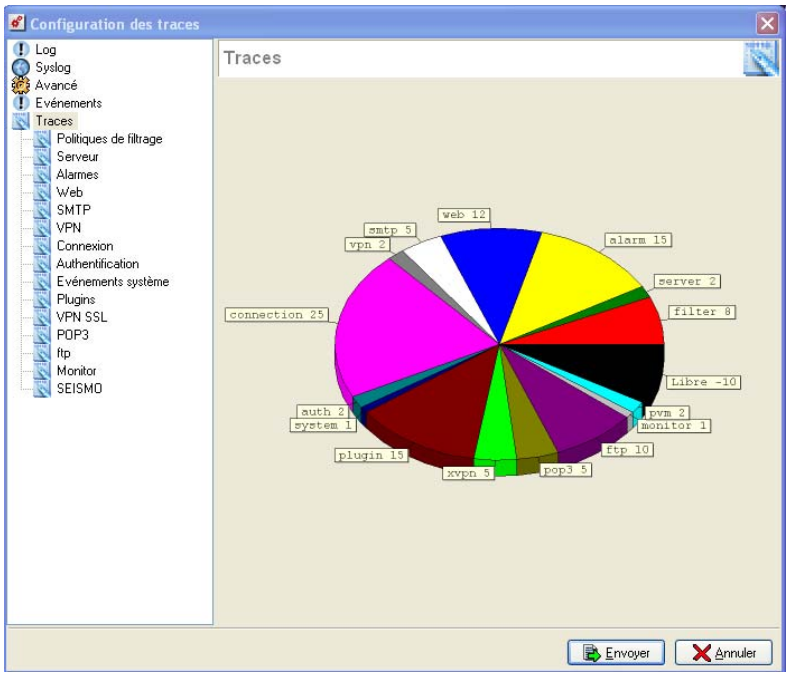


Figure 415 : Configuration des traces - Traces

17.1.6.1. Gestion des fichiers de traces

Pour chaque menu de traces (filter, server, alarm, WEB, SMTP, VPN, connection, auth, system, plugin, xvpn, pop3 et monitor), vous pouvez limiter la taille du fichier de traces du filtrage en sélectionnant la taille du fichier en pourcentage de l'espace réservé pour les fichiers de logs.

Vous avez aussi la possibilité de choisir l'action à entreprendre une fois que ce seuil est atteint. Les différentes possibilités sont :

- **Rotation des fichiers** : les traces les plus récentes effacent les traces les plus anciennes.
- **Stopper l'écriture des fichiers** : les traces ne sont plus mémorisées sur le firewall.
- **Arrêter le firewall** : le firewall ne s'arrête pas réellement mais il bloque l'ensemble des flux excepté les connexions du **NETASQ UNIFIED MANAGER** depuis le réseau interne.

Enfin un graphique représente le taux d'occupation actuel en pourcentage.

17.1.6.2. Politiques de Filtrage

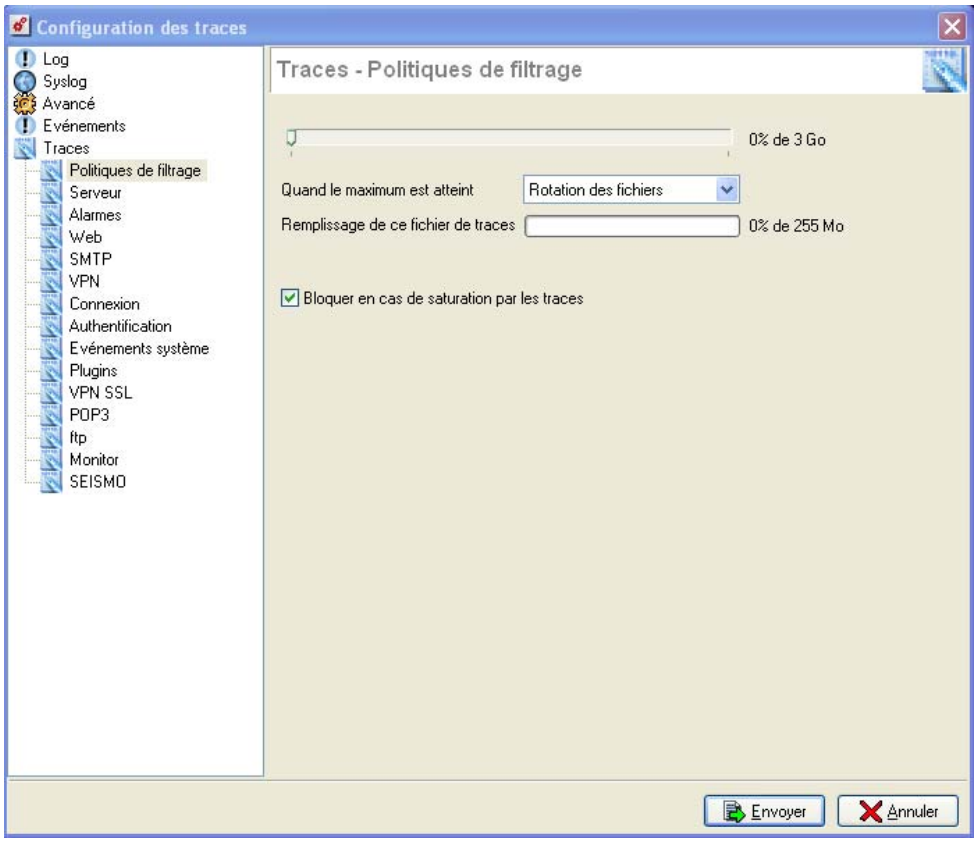


Figure 416 : Configuration des traces - Politique de filtrage

L'option **Bloquer en cas de saturation par les traces**, présente dans les menus **`Politiques de filtrage`** et **`Alarmes`** définit qu'un trafic autorisé par le filtrage à traverser l'Appliance sera tout de même bloqué si l'enregistrement dans les traces est impossible (espace réservé plein ou surcharge de l'Appliance par exemple). Cette condition ne s'applique que sur les trafics passants avec l'option **Tracer** appliquée à la règle.

En décochant cette option, vous permettez que les trafics passants (ET dont l'option **Tracer** est spécifiée) soient autorisés même si l'enregistrement des traces (logging) est impossible.

17.1.6.3. Connexion

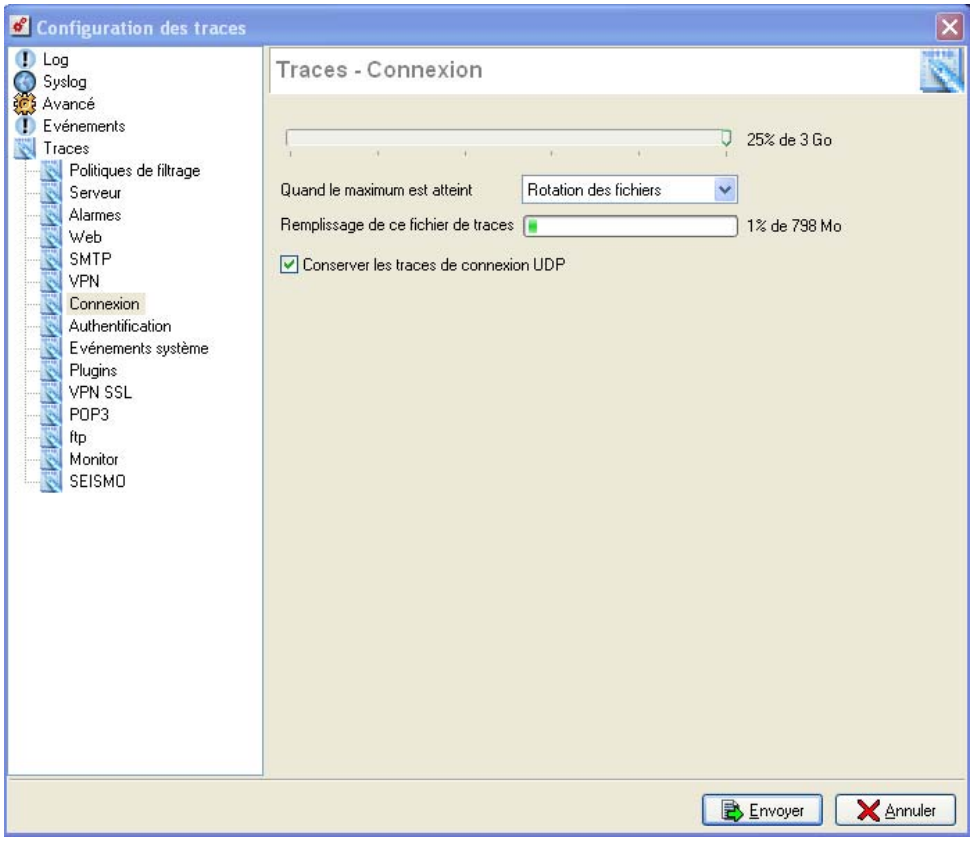


Figure 417 : Configuration des traces - Connexion

L'option **Conserver les traces de connexion UDP**, présente dans le menu **`Connexion`** permet de tracer aussi les datagrammes UDP.

AVERTISSEMENT
De part la nature de ce type de flux (un envoi datagramme = 1 connexion), les traces peuvent être plus rapidement engorgées.

CHAPITRE 2. RECEPTION DES ALARMES ET DES TRACES

17.2.1. Introduction

Le firewall NETASQ différencie deux types d'alarmes :

- Les alarmes majeures.
- Les alarmes mineures.

Les alarmes mineures sont déclenchées par les paquets arrivant au firewall NETASQ et correspondant à une règle de filtrage ou à un événement pour laquelle ou lequel vous avez spécifié l'action "Alarme mineure".

Les alarmes majeures sont déclenchées automatiquement par le firewall NETASQ lorsqu'un paquet ou une action lui semble réellement suspect.

> **Exemple**
> Par exemple : une attaque par SYN Flooding.

Plusieurs moyens permettent d'être informé des alarmes émises par le firewall :

- L'alarme est envoyée aux moniteurs temps réel connectés (Application NETASQ REAL-TIME MONITOR). Pour recevoir les alarmes sur un poste distant, il faut lancer le moniteur temps réel et ouvrir une connexion vers le firewall à surveiller
- Par e-mail. Pour cela, il faut remplir le champ **Serveur SMTP** avec l'adresse IP du serveur SMTP. Vous pouvez ensuite préciser l'adresse e-mail de réception des messages d'alarmes.

17.2.2. Présentation de NETASQ REAL-TIME MONITOR

Dans le répertoire où se trouve le logiciel de configuration depuis Windows C:\Program Files\Netasq\Administration Suite x.x par défaut vous trouverez l'application "monitor.exe" ou tout simplement à partir du raccourci Applications\Launch RealtimeMoniteur dans la barre de menus.

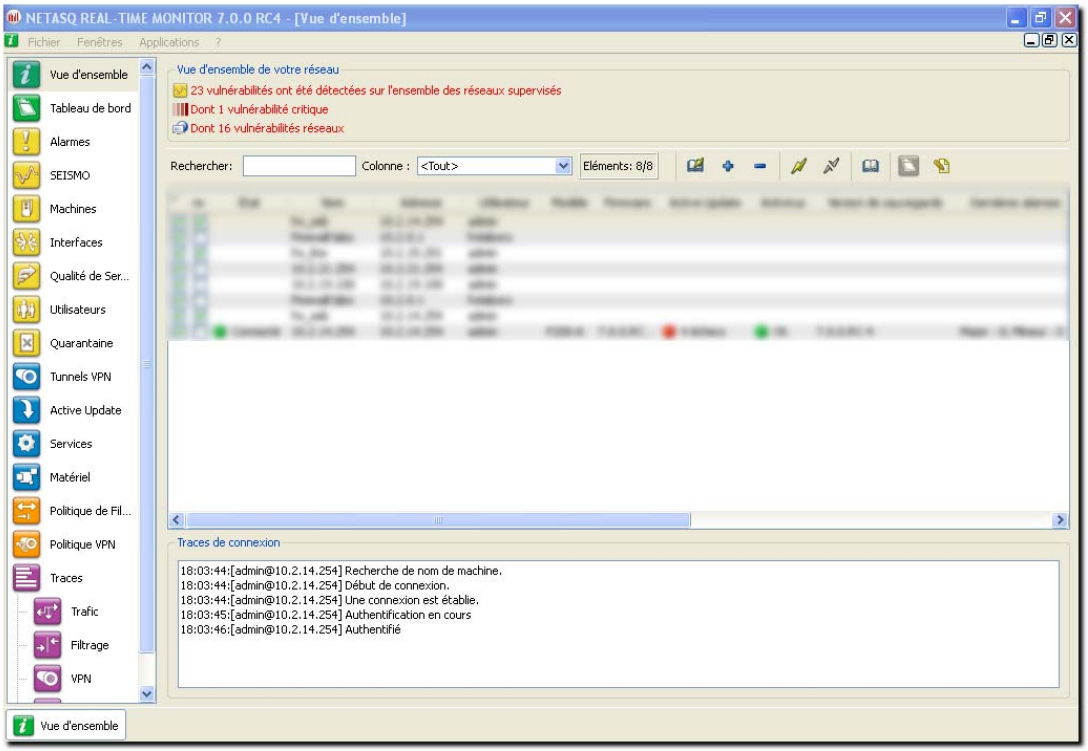


Figure 418 : Vue d'ensemble

Le moniteur d'alarmes temps réel vous permet de visualiser simplement les connexions transitant par le firewall et les alarmes qu'il a déclenchées.

Lorsqu'il est connecté, le moniteur reçoit les informations du firewall. Vous pouvez ensuite le réduire avec le bouton de réduction de la fenêtre Windows. Le moniteur tourne alors en arrière plan. Pour le faire réapparaître à l'écran, double cliquez sur l'icône figurant au niveau de la barre des tâches (à côté de l'horloge).

Par défaut, ce moniteur ne peut être exécuté que sur une machine connectée au réseau interne et doit être lancé en permanence pour ne pas perdre d'alarmes. Vous pouvez l'utiliser de façon distante (au travers d'Internet) mais il faut alors explicitement autoriser le service (Firewall_srv), dans les règles de filtrage.

REMARQUES

1) A la réception d'une alarme, la fenêtre du NETASQ REAL-TIME MONITOR peut passer en avant-plan et un son est éventuellement émis.
2) Dans le cas où une alarme ne parvient pas au moniteur, celle-ci est tout de même tracée et le voyant "minor" située en face avant du Firewall NETASQ est allumé brièvement. De plus, si vous avez précisé une adresse mail où envoyer les alarmes, les messages d'alertes seront envoyés par mail.
3) La génération d'alarmes est très pratique pour pister d'éventuels abus. Il suffit, pour cela, d'ajouter, dans les règles de filtrage, l'option "alarme mineure" sur la règle dont vous voulez pister l'utilisation. Cependant une utilisation excessive de cette fonctionnalité la rendra très rapidement inutilisable de part la taille des fichiers de traces générées, le nombre d'alarmes affichées sur votre moniteur et le passage en avant-plan de la fenêtre du moniteur.

PARTIE 18 : MAINTENANCE

18.1.1. Introduction

18.1.1.1. Pour cette partie, vous devez avoir franchi les étapes

- Partie 2/Chapitre 1 : Interface graphique.
- Partie 2 : Installation, intégration et pré-configuration.

18.1.1.2. Pour cette partie, vous devez connaître

- L'adresse IP du firewall NETASQ sur le réseau interne.

18.1.1.3. Utilité de la partie

Cette partie vous permet de sauvegarder/restaurer toutes les informations spécifiques à votre firewall.

L'administrateur possédant le droit **maintenance** peut sauvegarder dans un fichier sur la station d'administration :

- La configuration complète.
- La configuration réseau du firewall (adresses du firewall, passerelles, etc.).
- Les objets (machines, réseaux, services et chacun des groupes).
- Les règles de filtrage.
- La base LDAP (base locale des utilisateurs).

Il est possible de chiffrer et signer le fichier avec un mot de passe.

La restauration de la configuration à partir d'un fichier de sauvegarde nécessite les droits de maintenance.

Enfin, cette section explique la méthode de mise à jour des boîtiers.

18.1.1.4. Accéder à cette partie

➔ Accédez aux boîtes de dialogue par les sous-menus **Maintenance\Sauvegarder…**, **Maintenance\Restaurer…**, **Maintenance\Rechercher Firmware** et **Maintenance\Mettre à jour le firmware**.

> **REMARQUE**
> Vous devez être connecté avec les privilèges de modification pour pouvoir effectuer ces modifications.

18.1.2. Sauvegarde

Lorsque vous apportez des modifications à votre firewall, pour des raisons de sécurité, aucune information n'est enregistrée sur l'ordinateur où est installé le NETASQ UNIFIED MANAGER.

Ceci présente en outre un autre avantage : vous pouvez consulter et configurer le firewall à partir de n'importe quel poste du réseau interne équipé de l'interface graphique.

Toutefois, il est important de constater que ceci présente un inconvénient : en cas d'erreur lors de la configuration, de problème hardware ou, si vous voulez configurer plusieurs firewalls de manière presque identique vous êtes plus ou moins bloqué.

C'est pourquoi le NETASQ UNIFIED MANAGER est équipé d'une fonctionnalité permettant de sauvegarder/restaurer l'ensemble ou une partie des fichiers de configuration de votre firewall. La sauvegarde réalisée peut être chiffrée et signée pour des raisons de confidentialité et d'intégrité de la configuration.

18.1.2.1. Sauvegarde de la configuration

Pour sauvegarder la configuration de l'UTM NETASQ, sélectionnez le menu **`Maintenance\Sauvegarder…`** de la barre de menus située en haut de l'interface NETASQ UNIFIED MANAGER. Un assistant vous guide pas à pas dans les fonctionnalités de sauvegarde des produits NETASQ.

Etape 1

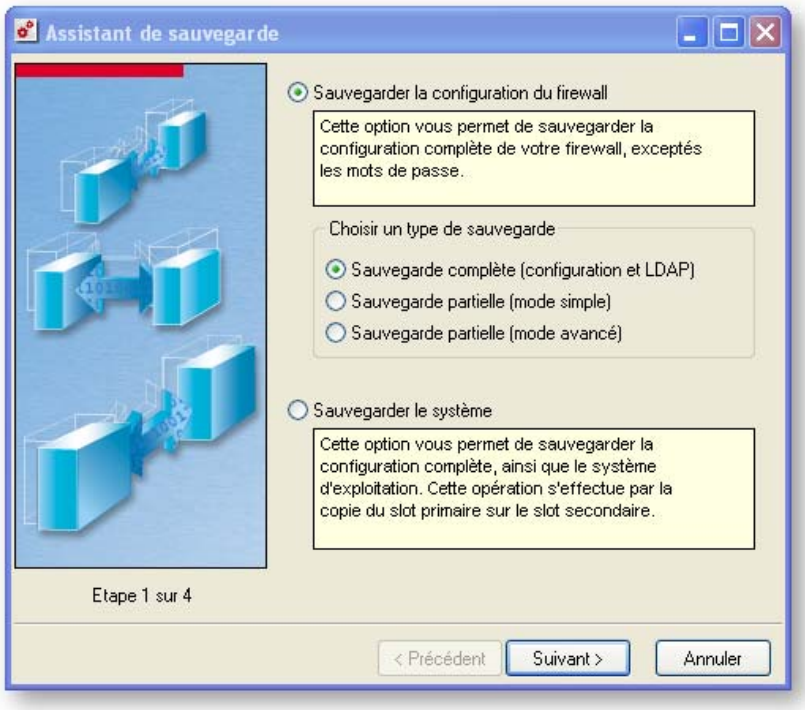


Figure 419 : Assistant de sauvegarde - Etape 1

La première étape permet de définir ce qui doit être sauvegardé : la configuration ou le système. Comme indiqué dans l'interface, la sauvegarde de la configuration consiste à enregistrer sur la station d'administration un fichier chiffré contenant la configuration de l'Appliance (totale ou partielle selon les options choisies). La sauvegarde du système consiste à enregistrer sur l'Appliance directement, dans une

partition de sauvegarde, l'ensemble du système et de la configuration. Seuls les mots de passe ne sont pas sauvegardés.

Type de sauvegarde de configuration

Il existe trois types de sauvegarde de la configuration :

- **Sauvegarde complète (configuration et LDAP)** : ce choix permet la sauvegarde de la configuration de l'Appliance et de l'ensemble des informations stockées dans la base LDAP (fiches utilisateurs), sans option, cette configuration enregistre tout.
- **Sauvegarde partielle (mode simple)** : ce choix permet la sauvegarde de la configuration de l'Appliance selon des choix effectués par l'administrateur. Ce type de configuration partielle permet par exemple l'enregistrement de la base d'objets pour que celle-ci soit ensuite restaurée sur un autre produit et ainsi faciliter le travail de l'administrateur.
- **Sauvegarde partielle (mode avancé)** : ce choix, plus granulaire que l'option « simple » permet la sélection la plus spécifique en termes de sauvegarde.

Les écrans de configuration de sauvegarde de l'étape 2 varient en fonction du type de sauvegarde sélectionné.

Etape 2

Sauvegarde partielle (mode simple)

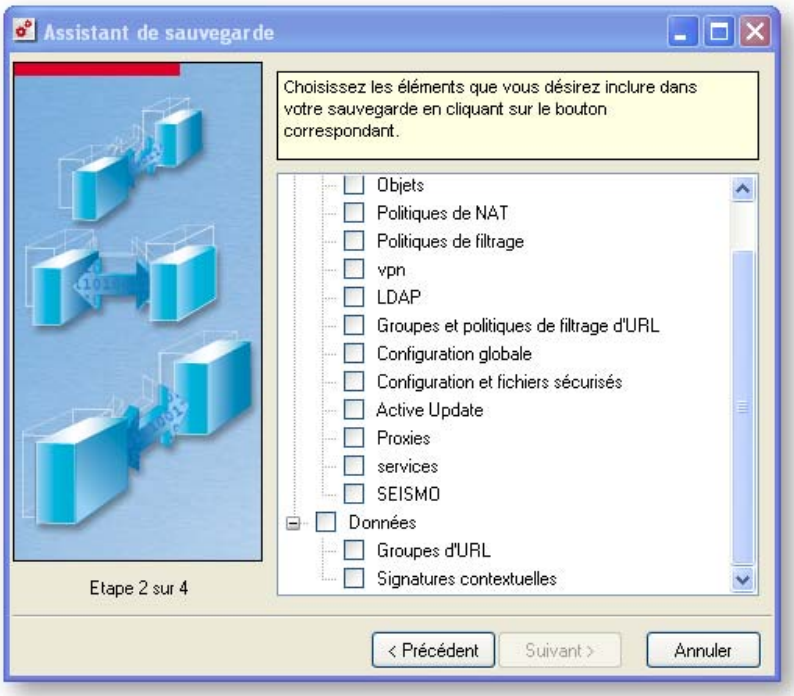


Figure 420 : Assistant de sauvegarde - Etape 2

Lorsque la sauvegarde simple est sélectionnée, les options de sauvegarde sont les suivantes :

- **Configuration** : sélectionne tous les éléments situés sous ce choix.
- **Interface et routage statique** : configuration réseau de l'Appliance, la configuration des interfaces, la passerelle par défaut et les routes statiques.
- **Objets** : la base des objets, sauf les utilisateurs.
- **Politique de NAT** : tous les slots de la configuration de la translation d'adresses.
- **Politiques de filtrage** : tous les slots de la configuration du filtrage.
- **Vpn** : tous les slots de la configuration des tunnels VPN IPSec, les clés pré partagées et les certificats stockés dans le menu **`Certificats`**.
- **LDAP** : configuration de la base LDAP de l'Appliance, ainsi que les éléments stockés dans la base (utilisateurs) et configuration de la PKI.
- **Groupes et politiques de filtrage d'URL** : tous les slots de la configuration du filtrage d'URL ainsi que les groupes d'URL statiques (créés par l'administrateur).
- **Configuration globale** : tous les slots de la configuration globale ainsi que les objets globaux.
- **Configuration et fichiers sécurisés** : configuration sécurisée et fichiers chiffrés et sécurisés par la configuration sécurisée.
- **Active Update** : configuration du module de mise à jour automatique du firewall.
- **Proxies** : configuration des proxies HTTP, SMTP et POP3.
- **Services** : configuration des services de l'Appliance, DHCP, DNS, NTP et SNMP.
- **SEISMO** : configuration du module de détection des vulnérabilités liées au réseau.
- **Données** : sélectionne tous les éléments situés sous ce choix.
- **Groupes d'URL** : tous les groupes d'URL dynamiques, obtenus par Active Update.
- **Signatures contextuelles** : signatures ASQ obtenues par Active Update.

Sélectionnez, en les cochant, les éléments que vous souhaitez inclure dans votre sauvegarde.

Sauvegarde partielle (mode avancé)

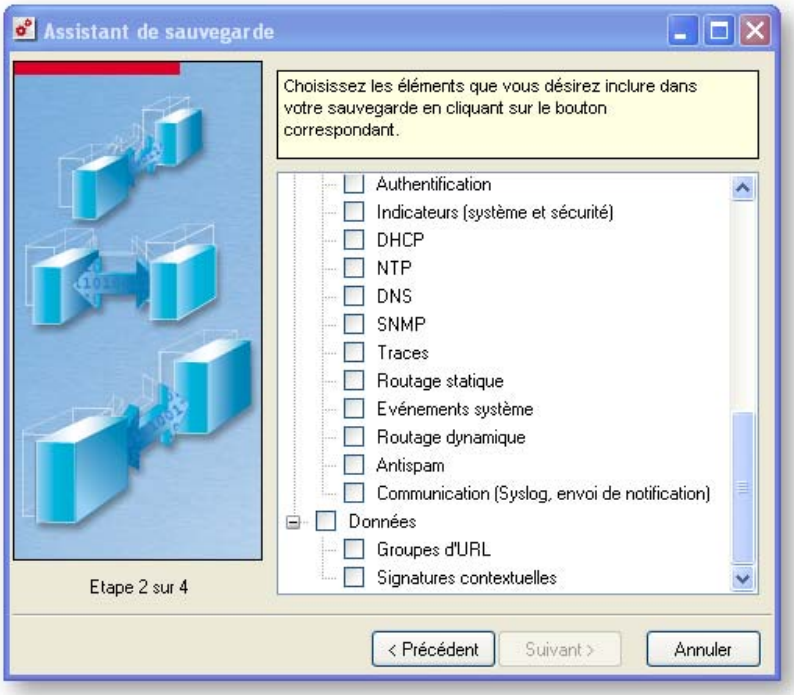


Figure 421 : Assistant de sauvegarde - Etape 2

Lorsque la sauvegarde avancée est sélectionnée, les options de sauvegarde sont les suivantes :

- **Configuration** : sélectionne tous les éléments situés sous ce choix.
- **Interfaces et routage statique** : configuration réseau de l'Appliance, la configuration des interfaces, la passerelle par défaut et les routes statiques.
- **Objets** : la base des objets, sauf les utilisateurs.
- **Politique de NAT** : tous les slots de la configuration de la translation d'adresses.
- **Politiques de filtrage** : tous les slots de la configuration du filtrage.
- **LDAP**: configuration de la base LDAP de l'Appliance, ainsi que les éléments stockés dans la base (utilisateurs) et configuration de la PKI.
- **Groupes et politiques de filtrage d'URL** : tous les slots de la configuration du filtrage d'URL ainsi que les groupes d'URL statiques (créés par l'administrateur).
- **Configuration globale** : tous les slots de la configuration globale ainsi que les objets globaux.
- **Configuration et fichiers sécurisés** : configuration sécurisée et fichiers chiffrés et sécurisés par la configuration sécurisée.
- **Active Update** : configuration du module de mise à jour automatique de l'Appliance.
- **Proxies** : configuration des proxies HTTP, SMTP et POP3.
- **SEISMO** : configuration du module de détection des vulnérabilités liées au réseau.
- **Certificats et clés-pré-partagées** : certificats stockés dans le menu « Certificats » et clés pré partagées configurées.
- **Prévention d'intrusion (ASQ)** : configuration du moteur de prévention de l'Appliance, l'ASQ.
- **Configuration du module VPN SSL** : configuration du module VPN SSL.
- **Configuration des tunnels PPTP** : configuration du serveur PPTP.
- **Politiques de tunnels VPN IPSec** : configuration des tunnels VPN IPSec uniquement.
- **Programmation horaire** : programmation horaire définie pour les slots.
- **Règles événementielles** : règles de filtrage événementielles configurées manuellement par l'administrateur.
- **QoS** : configuration des politiques de Qualité de Service.
- **Authentification** : configuration de l'authentification.
- **Indicateurs (système et sécurité)** : indicateurs que l'on retrouve dans l'Administration globale.
- **DHCP** : service DHCP de l'Appliance.
- **NTP** : service NTP de l'Appliance.
- **DNS** : service DNS de l'Appliance.
- **SNMP** : service SNMP de l'Appliance.
- **Traces** : configuration des traces uniquement.
- **Routage statique** : passerelle par défaut et routes statiques configurées.
- **Evénements système** : configuration des événements système.
- Routage dynamique : configuration de la plateforme de routage dynamique.
- **Antispam** : configuration du module Antispam.
- **Communication (Syslog, envoi de notification)** : module de communication de l'Appliance, notamment envoi des traces auprès des serveurs Syslog et envoi des notifications d'alarmes aux administrateurs.
- **Données** : sélectionne tous les éléments situés sous ce choix.
- **Groupes d'URL** : tous les groupes d'URL dynamiques, obtenus par Active Update.
- **Signatures contextuelles** : signatures ASQ obtenues par Active Update.

Sélectionnez, en les cochant, les éléments que vous souhaitez inclure dans votre sauvegarde.

Etape 3

L'écran suivant s'affiche :

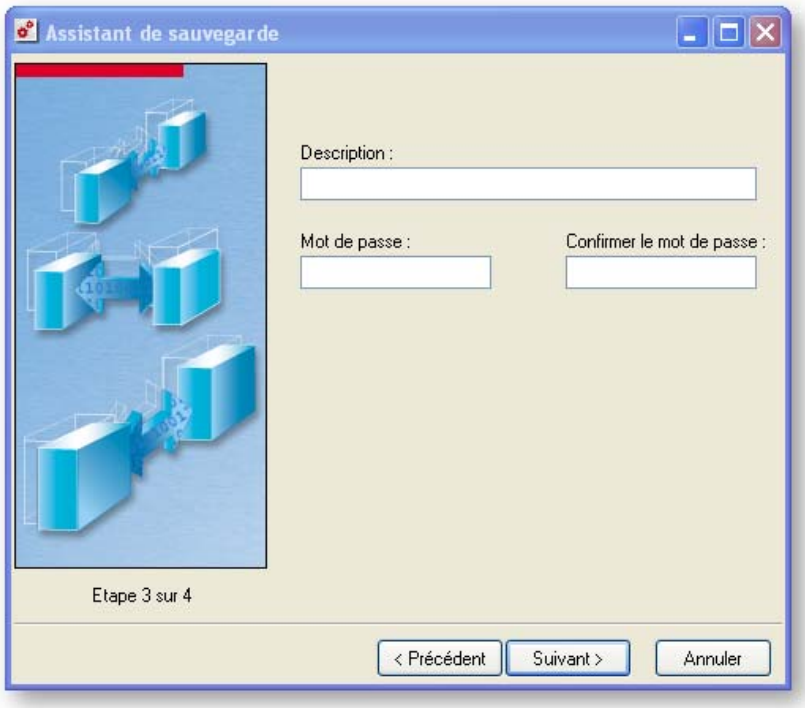


Figure 422 : Assistant de sauvegarde - Etape 3

Vous donnez le nom de votre sauvegarde et choisissez son emplacement.

- **Description** : Cette description sera affichée lors de la restauration de la configuration. Ainsi, vous pouvez réaliser plusieurs sauvegardes et distinguer chacune d'entre elles.
- **Mot de passe et Confirmer le mot de passe** : Vous avez aussi la possibilité de chiffrer la sauvegarde afin qu'elle ne puisse pas être restaurée sur un autre firewall ou pour qu'elle ne puisse pas être visualisée. Pour cela, indiquez un mot de passe qui servira pour le chiffrement.

> **AVERTISSEMENT**
> Si la sauvegarde n'est pas stockée sur des supports fiables et sécurisés, il est vivement conseillé d'activer le chiffrement.

Etape 4

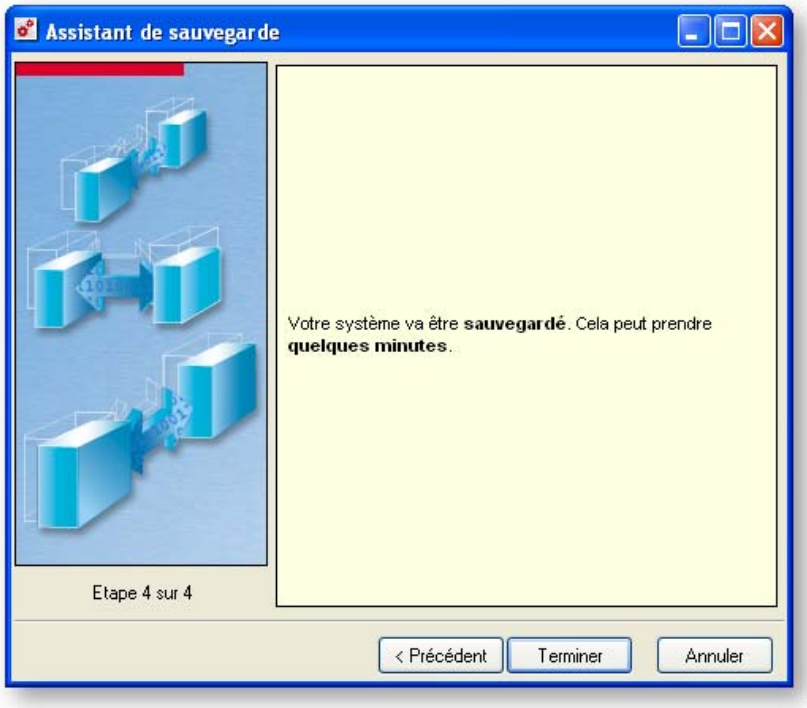


Figure 423 : Assistant de sauvegarde - Etape 4

Cliquez sur **Terminer** pour effectuer la sauvegarde.

18.1.3. Restauration

Pour restaurer une configuration sur un Appliance NETASQ, sélectionnez le menu **Maintenance\Restaurer…** de la barre de menu située en haut de l'interface NETASQ UNIFIED MANAGER. Un assistant vous guide pas à pas dans les fonctionnalités de restauration des produits NETASQ.

Etape 1 : restauration du firewall et du système

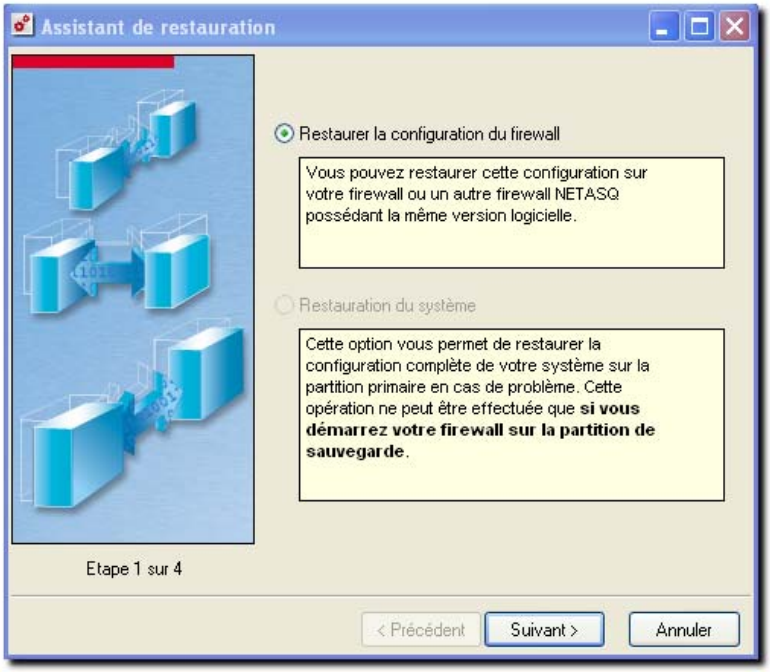


Figure 424 : Assistant de restauration - Etape 1

Dans la première étape de l'assistant, la restauration du système est disponible Cliquez sur **Suivant** pour continuer.

REMARQUE
Vous pouvez restaurer cette configuration sur votre firewall ou un autre firewall NETASQ possédant la même version logicielle.

Etape 2 : Fichier de restauration

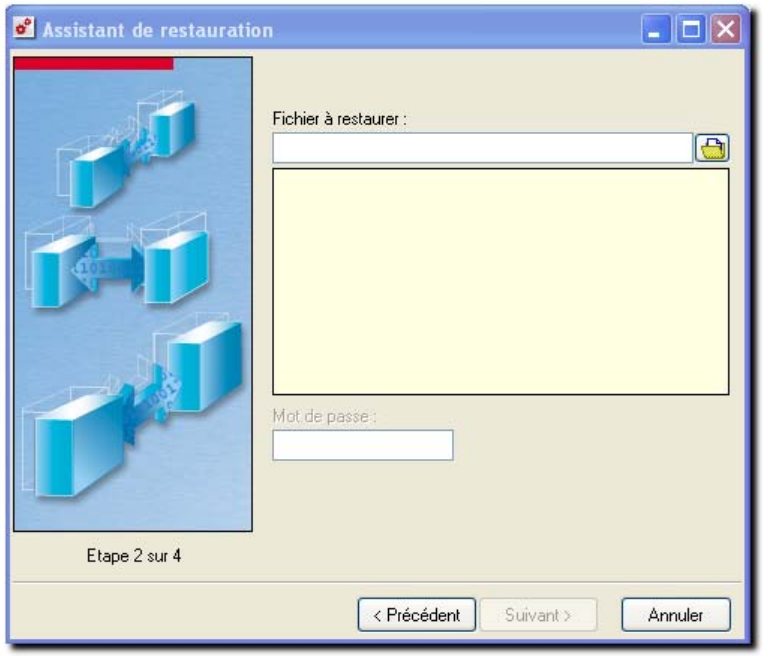


Figure 425 : Assistant de restauration - Etape 2

Indiquez le fichier de sauvegarde que vous voulez restaurer. Une description de la sauvegarde s'affiche et vous permet de distinguer les différentes sauvegardes.

Etape 3 : Eléments de restauration

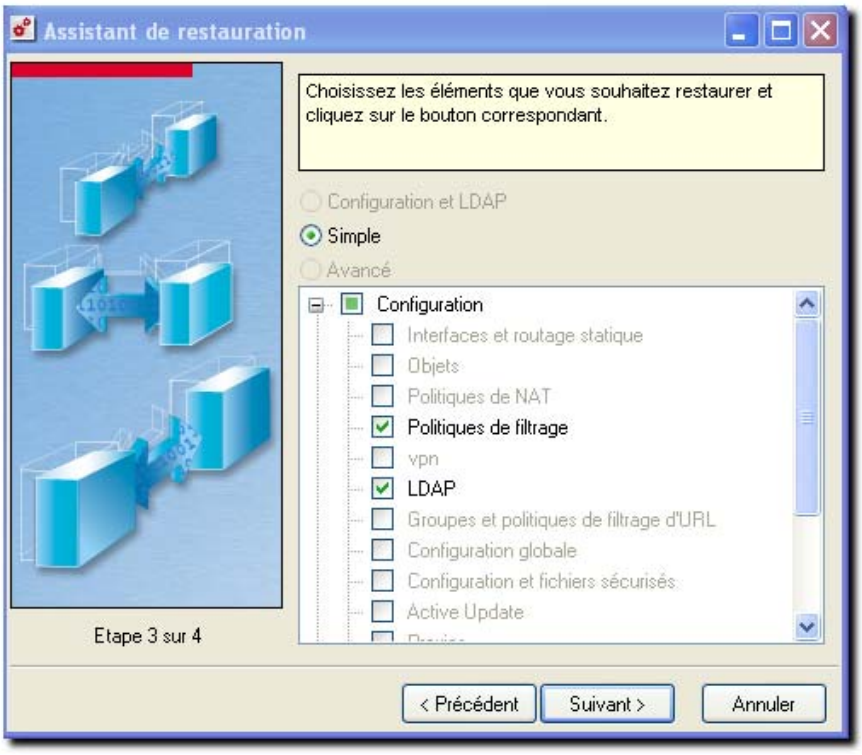


Figure 426 : Assistant de restauration - Etape 3

Puis les options de restauration apparaissent. De la même façon que pour la sauvegarde de configuration, il existe trois types de restauration, ces trois types font référence aux trois types de sauvegarde. Référez-vous à la section "Sauvegarde de la configuration" pour plus d'informations.

AVERTISSEMENT
Il vous est conseillé d'effectuer une sauvegarde des fichiers de configuration à chaque modification importante.

Si vous ne désirez sauvegarder qu'un slot, vous pouvez utiliser la fonctionnalité **Copier**/**Coller**.

AVERTISSEMENT
Les mots de passe ne sont pas sauvegardés. Ils restent les mêmes après une sauvegarde ou une restitution.

Etape 4 : Mise à jour

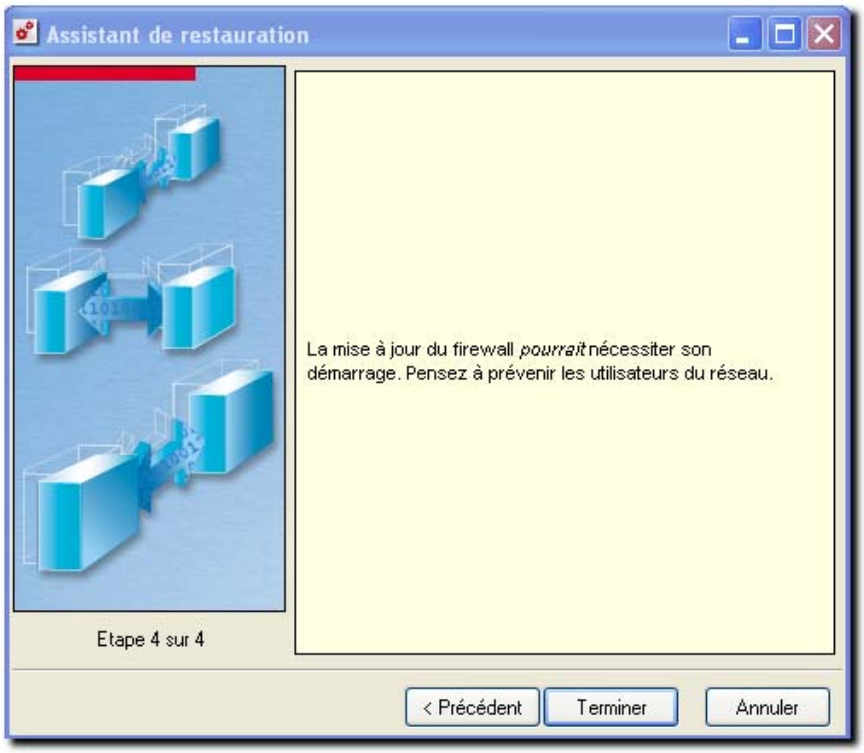


Figure 427 : Assistant de restauration - Etape 4

Un message s'affiche pour vous prévenir que la mise à jour du firewall pourrait nécessiter son démarrage. Cliquez sur **Terminer** pour effectuer la restauration.

18.1.4. Avertissement sur les sauvegardes du système

Cette fonctionnalité vous permet de sauvegarder l'ensemble de la configuration et le système d'exploitation du firewall (image disque). Cela permet de basculer sur cette sauvegarde lors du non-fonctionnement du système principal (problème sur le disque dur, mise à jour infructueuse...).

Une fois que votre configuration est en production sans problème, vous pouvez faire une sauvegarde du système.

> **AVERTISSEMENT**
> La sauvegarde du système peut entraîner une baisse des performances du firewall pendant le temps de la sauvegarde (environ 1 minute).

En cas de problème, vous rebootez et démarrez sur le système de sauvegarde.

Pour cela, il suffit d'être connecté en mode console (clavier + écran) au moment du redémarrage. Lorsque vous voyez apparaître le menu de démarrage, tapez 2 pour démarrer sur la sauvegarde.

Une fois le firewall démarré, vous pouvez vous y connecter avec l'interface graphique pour rétablir le système de sauvegarde sur le système principal.

Il est également possible de redémarrer sur la partition de votre choix via le menu **`Maintenance\Partition de démarrage`** s'il en existe une sur le firewall.

18.1.5. Mise à jour

Chaque mise à jour est décomposée en paquets indépendants. Pour une mise à jour majeure, l'ensemble des paquets est installé alors que pour une mise à jour mineure, seuls les paquets modifiés sont installés.

Deux types de mise à jour peuvent être faites :

- Mise à jour du logiciel firewall.
- Mise à jour de l'interface graphique de configuration (NETASQ UNIFIED MANAGER et NETASQ REAL-TIME MONITOR).

La mise à jour de fonctionnalités logicielles du firewall NETASQ est une opération de maintenance. Vous comprendrez que la mise à jour des fichiers système sur le firewall NETASQ soit une opération délicate et entraîne une coupure du service pour les utilisateurs.

AVERTISSEMENT
Vous devez toujours réaliser la mise à jour dans l'ordre suivant :

1. Mise à jour du logiciel firewall à partir de l'ancienne interface graphique
2. Désinstallation de l'ancienne interface graphique de configuration si vous ne désirez pas la conserver. Installation de la nouvelle interface graphique de configuration.
3. Dans le cas des mises à jour majeures, il est important de suivre l'ordre des mises à jour logicielles, le passage d'une version ancienne à une version beaucoup plus récente sans passer par les mises à jour intermédiaires sera bloqué par le firewall.

18.1.5.1. Mise à jour de l'interface graphique

Cette mise à jour consiste en une simple réinstallation du logiciel.

Il vous suffit d'avoir préalablement récupéré l'installation sur le poste où vous désirez l'effectuer et de l'exécuter.

18.1.5.2. Mise à jour du firewall

La mise à jour du firewall par l'interface graphique est très simple. On y accède par le menu **`Maintenance\Mettre à jour le firmware`**.

Etape 1 : Bienvenue

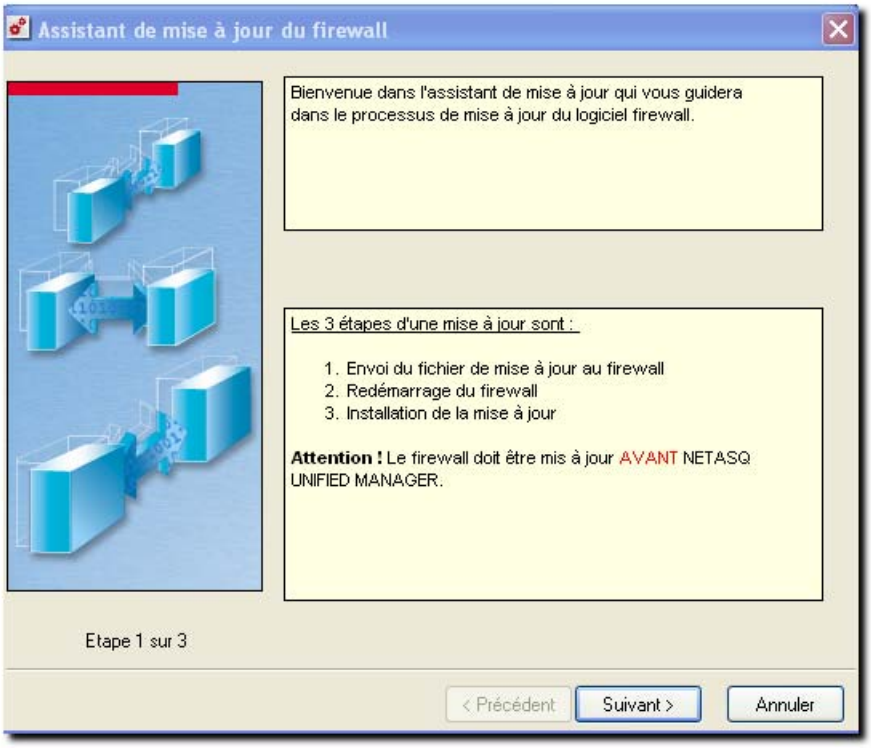


Figure 428 : Assistant de mise à jour du firewall - Etape 1

Le premier écran vous informe des 3 étapes de la mise à jour.

Etape 2 : Sélection du fichier de mise à jour

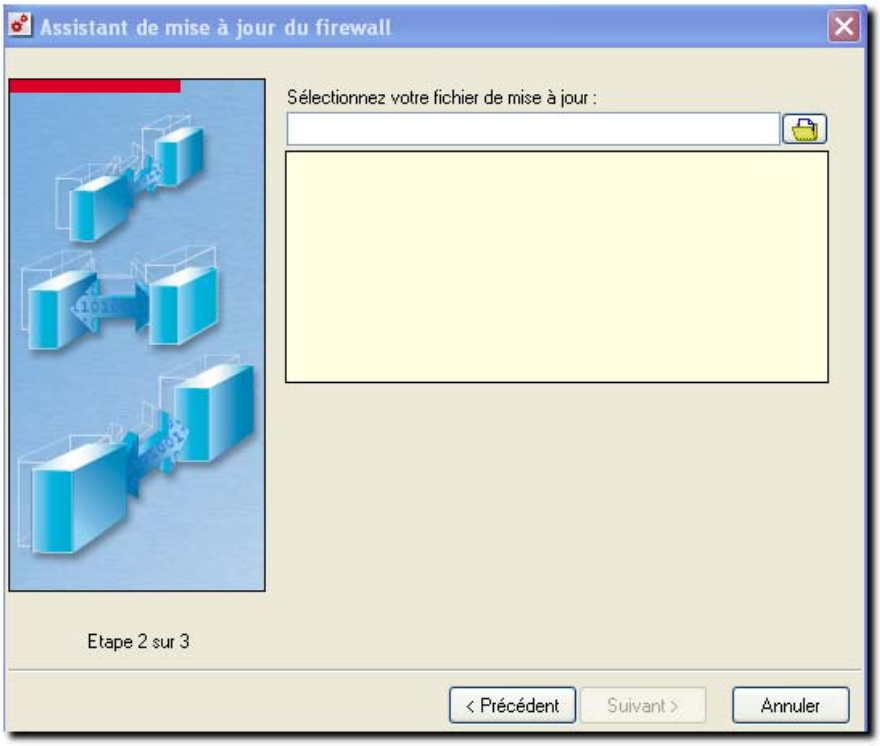


Figure 429 : Assistant de mise à jour du firewall - Etape 2

Sélectionnez le fichier de fichier de mise à jour. Vous devez télécharger ce fichier, portant l'extension **.maj.** à partir du site Web de NETASQ (www.netasq.com).

Vérifiez les informations de la mise à jour affichées lors de l'insertion du fichier MAJ dans l'assistant.

Etape 3 : Message

Vous avez ensuite le message d'avertissement qui vous rappelle que cette mise à jour nécessite de redémarrer le firewall et donc de couper momentanément les connexions qui le traversent.

Vous voyez aussi, à ce niveau, quelle est la version minimale à avoir pour pouvoir réaliser cette mise à jour.

Pendant la mise à jour, une fenêtre de progression s'affiche vous indiquant que la mise à jour est en train de se dérouler.

A la fin de l'envoi du fichier, le message vous indique que le fichier a été transféré et le firewall redémarre.

A la prochaine connexion, vous aurez un message vous indiquant le résultat du changement de version.

Haute Disponibilité

Si vous possédez deux firewalls en Haute Disponibilité, il vous est possible mettre à jour le firewall passif avant le firewall actif. (Cf. Partie 14 : Haute Disponibilité).

Mise à jour certifiée

Pour vérifier si une version ou une mise à jour a bien été certifiée, il faut se connecter sur le site Web de NETASQ (www.netasq.com), puis se logger sur son compte à partir de l'espace client. Ensuite, dans la partie "Téléchargements", cliquez sur le lien **Télécharger la dernière version** pour vérifier si la dernière version a été certifiée ou sur le lien **Télécharger les versions précédentes** pour vérifier les versions certifiées parmi la liste des anciennes mises à jour. Une mention sera alors indiquée pour chaque version certifiée.]

Downgrade vers une version inférieure

Il n'est pas possible de gérer de mise à jour inversée. Pour plus d'informations à ce sujet, veuillez contacter votre revendeur certifié ou le support NETASQ.

18.1.5.3. Remarques

REMARQUES

1) La procédure de mise à jour n'altère pas vos fichiers de configuration : ceux-ci sont stockés sur le firewall NETASQ. Les fichiers de configuration sont mis à jour en même temps que le firewall.
2) La mise à jour de fichiers système sur le firewall NETASQ n'implique pas systématiquement une mise à jour du logiciel de configuration à distance. Si c'est le cas, cela sera stipulé au moment du téléchargement de la nouvelle version.
3) Inversement, la mise à jour du logiciel de configuration à distance n'implique pas systématiquement une mise à jour des fichiers système du firewall NETASQ. Si c'est le cas, cela sera stipulé au moment du téléchargement de la nouvelle version.

AVERTISSEMENT

Il n'est pas possible d'installer une mise à jour modifiée (erronée, altérée, compromise,…) car le fichier de mise à jour est chiffré et nécessite donc de la part du logiciel de configuration à distance et du firewall des mécanismes et des clés de déchiffrement pour réaliser l'opération de mise à jour.

18.1.6. Mise à jour Web

Le firewall NETASQ est un produit de sécurité qui évolue pour protéger le réseau, de menaces toujours plus évoluées. Des mises à jour régulières sont nécessaires pour prendre en compte ces différentes évolutions. De plus les logiciels de la Suite d'Administration doivent être mis à jour pour gérer ces nouvelles fonctionnalités.

La recherche des mises à jour du firmware ou de la Suite d'Administration peut être effectuée automatiquement par des mécanismes de programmation expliqués dans le menu **Options\Préférences\Accès au site Internet** ou manuellement.

Cette section décrit les menus permettant la recherche manuelle de mises à jour. Pour accéder à ces menus sélectionnez dans les menus du NETASQ UNIFIED MANAGER :

- **Options\Préférences\Accès au site Internet** : pour déclencher manuellement une recherche des mises à jour concernant la Suite d'Administration des produits firewalls NETASQ.
- **Maintenance\Rechercher firmware** : pour déclencher manuellement une recherche des mises à jour concernant les firmwares des produits NETASQ.

18.1.6.1. Mises à jour de l'Administration Suite et du firmware

Cette mise à jour est accessible via le menu **Maintenance\Rechercher firmware**.

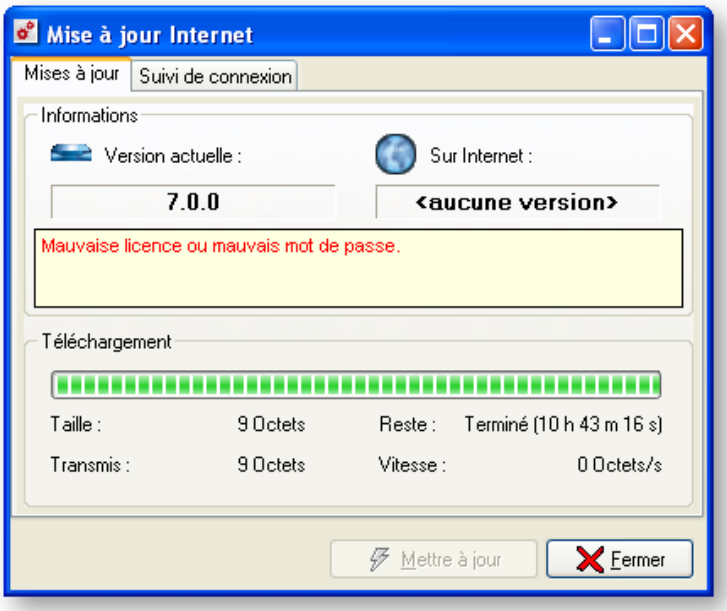


Figure 430 : Mise à jour Internet - Mises à jour

La mise à jour de l'Administration Suite et du firmware permet le support des nouvelles fonctionnalités disponibles sur le firewall, intégrées par NETASQ pour assurer la protection la plus adaptée aux menaces circulant sur l'Internet.

Informations de mises à jour

De nombreuses informations sur le téléchargement des mises à jour sont affichées par le menu de mises à jour Web. Ces différentes informations sont décrites dans le tableau suivant :

Onglet Mise à jour

Version actuelle	Donnée informative indiquant la version actuellement installée sur le poste de travail.
Sur Internet	Donnée informative indiquant la version actuellement disponible sur le site Web NETASQ.
Taille	Taille du fichier à télécharger. La taille d'une mise à jour de la Suite d'Administration oscille autour de 60 Mo Une mise à jour du Firmware des firewalls NETASQ oscille quant à elle autour de 11 Mo.
Transmis	Données en octets déjà téléchargées.
Reste	Temps restant estimé pour la réception complète du fichier.
Vitesse	Débit informatif de téléchargement de la mise à jour.

Onglet Suivi de la connexion

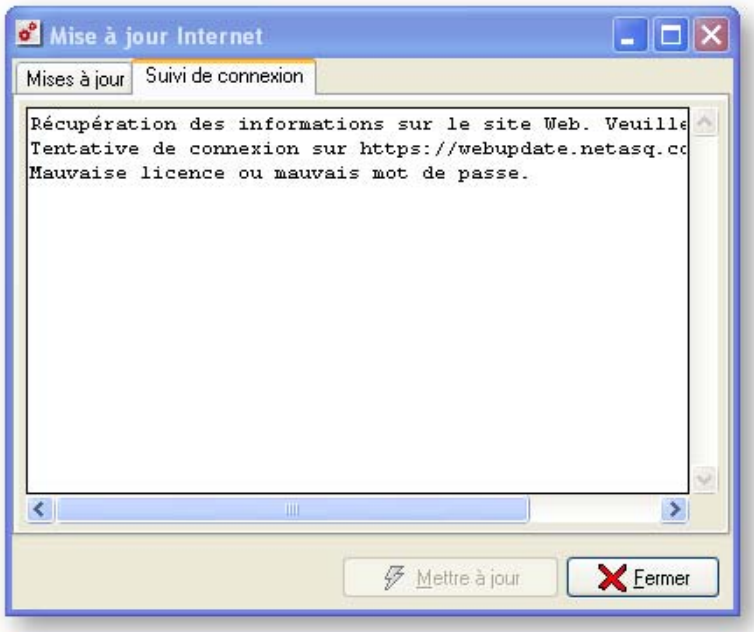


Figure 431 : Mise à jour Internet - Suivi de connexion

Le suivi de la connexion de la mise à jour affiche les différents événements survenus lors de la récupération des informations sur le site Web NETASQ et cela dans toutes les étapes du téléchargement de la mise à jour (identifiant, mot de passe, connexion, téléchargement).

Procédure de mise à jour de la Suite d'Administration

Pour effectuer une mise à jour de l'Administration Suite, référez-vous à la procédure suivante :

1 Renseignez les informations nécessaires à la connexion de NETASQ UNIFIED MANAGER au site Web NETASQ (Cf. le menu **Options\Préférences\Accès au site Internet**).

2 Sélectionnez le menu **Maintenance\Rechercher le firmware.**

3 Lorsque le menu apparaît il vous indique s'il existe une version plus récente de la Suite d'Administration actuellement sur le site Web NETASQ.

4 Cliquez sur le bouton **Mettre à jour,** un dossier de téléchargement est demandé si celui-ci n'a pas été spécifié dans les préférences du Web Update (Cf. menu **Options\Préférences\Accès** au site Internet) puis la nouvelle Suite d'Administration est installée.

> **AVERTISSEMENT**
> Si la mise à jour de la Suite d'Administration est une mise à jour mineure, la nouvelle Suite d'Administration sera installée sur la précédente.
>
> Veillez à la compatibilité de connexion entre la nouvelle Suite d'Administration et le firewall. En effet NETASQ ne garantit pas la compatibilité entre version majeure.

Procédure de mise à jour du firmware UTM NETASQ

Pour effectuer une mise à jour du firmware UTM NETASQ, référez-vous à la procédure suivante :

1 Renseignez les informations nécessaires à la connexion de **NETASQ UNIFIED MANAGER** au site Web NETASQ (Cf. le menu **Options\Préférences\Accès au site Internet**)

2 Sélectionnez le menu **Maintenance\Rechercher firmware\Mises à jour.**

3 Lorsque le menu apparaît il vous indique s'il existe une version plus récente du firmware actuellement sur le site Web NETASQ.

4 Cliquez sur le bouton **Mettre à jour.** Un dossier de téléchargement est demandé si celui-ci n'a pas été spécifié dans les préférences du Web Update (Cf. menu **Options\Préférences\Accès** au site Internet). Puis le menu de mise à jour des firewalls apparaît. Le fichier à renseigner pour la mise à jour du firmware est alors déjà indiqué.

> **AVERTISSEMENT**
> Veillez à la compatibilité de connexion entre la nouvelle Suite d'Administration et le firewall. En effet, NETASQ ne garantit pas la compatibilité entre versions majeures.

18.1.7. Redémarrage du firewall

Pour redémarrer le firewall NETASQ :

1. Sélectionnez le menu **`Maintenance\Redémarrer...`** Le message suivant s'affiche :

   "Redémarrer le firewall NETASQ ?"

2. Cliquez sur le bouton **Oui** et le NETASQ UNIFIED MANAGER redémarre à distance.

Le redémarrage d'un firewall NETASQ implique le blocage systématique de tout paquet et donc de toute communication transitant par le NETASQ UNIFIED MANAGER, ainsi qu'une déconnexion du logiciel de configuration sous Windows (Ceci est visible dans l'écran principal par le passage à la couleur rouge du voyant d'état).

Vous devrez vous connecter à nouveau pour pouvoir continuer la configuration de votre firewall.

Une fois que le firewall a redémarré (une minute après l'envoi de la commande), celui-ci réactive les règles de sécurité et de traces en vigueur avant son redémarrage.

18.1.8. Arrêt du Firewall

Pour arrêter le firewall :

1. Sélectionnez le menu **`Maintenance\ Arrêter...`**Le message suivant s'affiche :

   "Arrêt du firewall NETASQ ?

2. Cliquez sur le bouton **Oui** et NETASQ UNIFIED MANAGER s'arrête à distance.

L'arrêt du firewall implique le blocage systématique de tout paquet transitant par le firewall, ainsi qu'une déconnexion du logiciel de configuration sous Windows (Ceci est visible dans l'écran principal par le passage à la couleur rouge du voyant d'état). Vous devez vous connecter à nouveau pour pouvoir continuer la configuration de NETASQ UNIFIED MANAGER. Ceci arrête le firewall NETASQ à distance. Le firewall est arrêté une fois que le voyant "Power" est éteint. Les voyants d'activité des cartes réseaux (IN, OUT et DMZ) restent en fonctionnement. Vous pouvez aussi, sur certains modèles, éteindre le boîtier grâce au bouton prévu à cet effet en façade du produit.

> **AVERTISSEMENT**
> Il est fortement conseillé d'attendre l'extinction du voyant "Power" après une demande d'arrêt manuelle ou à distance, avant de couper l'alimentation du firewall.
> Une coupure trop rapide peut entraîner des problèmes d'écriture sur le disque du firewall et provoquer des erreurs matérielles.

Cas de la Haute Disponibilité

Lorsque votre firewall fait partie d'un "cluster" (Haute Disponibilité avec un deuxième firewall), une boîte de dialogue s'affiche. Grâce à cet écran vous pouvez choisir de stopper le firewall actif, le firewall passif ou les deux.

Figure 432 : Arrêt de la HA

18.1.9. Active Update

18.1.9.1. Introduction

Le module Active Update, présent sur tous les boîtiers permet au firewall le téléchargement automatique des mises à jour des listes Antispam, des bases URL, des bases antivirus, des signatures contextuelles et de la base de vulnérabilités et ce, depuis une liste d'URL fournie. Il se compose de sous-systèmes qui correspondent chacun à une fonction du produit.

Les signatures contextuelles ASQ sont intégrées à la procédure de mise à jour automatique. Il s'agit de :

- Content Filtering
- FTP
- Malware
- SQL injection
- Vulnerability scanner
- Vulnerability service
- Web – Application
- Web – Evasion attempt
- Web – Server
- XSS – Cross Site Scripting

Le module **Active Update** est accessible à partir de l'arborescence de NETASQ UNIFIED MANAGER.

AVERTISSEMENT
Pour fonctionner correctement, ce module nécessite la configuration du service DNS (Cf. Partie 11/Chapitre 2 :Services\DNS).

NOTE
Un retour arrière automatique est effectué en cas d'échec de la mise à jour.

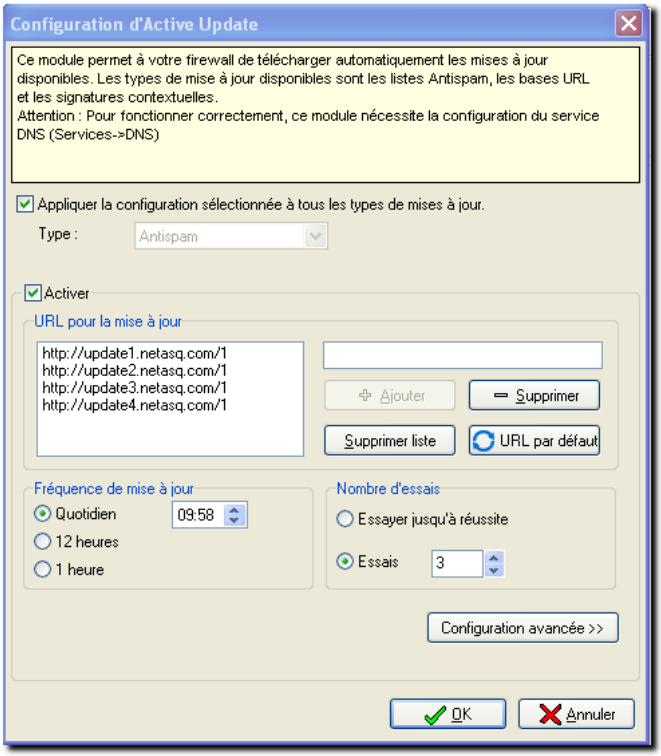


Figure 433 : Configuration Active Update

18.1.9.2. Fonctionnement

Il est nécessaire de configurer les paramètres expliqués dans le tableau suivant :

Appliquer la configuration sélectionnée à tous les types de mises à jour	En cochant cette option, les mises à jour sont effectuées de manière globale (c'est-à-dire pour tous les types de mises à jour possibles) En décochant cette option, les mises à jour s'effectuent de manière individuelle pour chaque type ceci afin de permettre une configuration plus fine (par exemple, au cas où certains fichiers seraient sur un autre serveur). Si l'option est décochée, sélectionnez un type de mise à jour parmi : "Antispam", "URLFiltering", "Patterns, "Vaderetro", "Pvm".
Activer	Activation de la mise à jour via l'Active Update pour le type de mise à jour sélectionné.
URL pour la mise à jour	Les fichiers de mise à jour sont récupérés sur un ou des serveurs définis par l'utilisateur. 4 URL sont définies par défaut. Pour ajouter une URL, indiquez son adresse URL dans la zone blanche puis cliquez sur **Ajouter**. Pour supprimer une URL de la liste, sélectionnez-là puis cliquez sur **Supprimer**. Pour supprimer la liste entière des URL, cliquez sur **Supprimer liste**. Pour réinitialiser la liste des serveurs, cliquez sur **URL par défaut**.
Fréquence de mises à jour	Choix de la fréquence des mises à jour des listes d'URL dynamique, des signatures contextuelles ASQ et de la configuration de l'antispam. Choisir la fréquence parmi : "Quotidien", "12 heures", "1 heure".
Nombre d'essais	Le champ « Essayer jusqu'à réussite » vous permet de spécifier que l'Active Update essaiera de réaliser la mise à jour jusqu'à sa réussite. Le champ "Essais" permet de spécifier un nombre de tentatives avant l'abandon de la mise à jour.
Configuration	Ce bouton permet d'accéder à l'écran d'activation du proxy. (*Cf. Explication ci-*

avancée	*dessous*).

Activation du proxy

Lorsque le firewall n'est pas directement connecté à Internet mais par l'intermédiaire d'un proxy, il faut configurer ce proxy pour que la mise à jour puisse être effectuée automatiquement. Cette configuration est disponible via le bouton **Configuration avancée.**

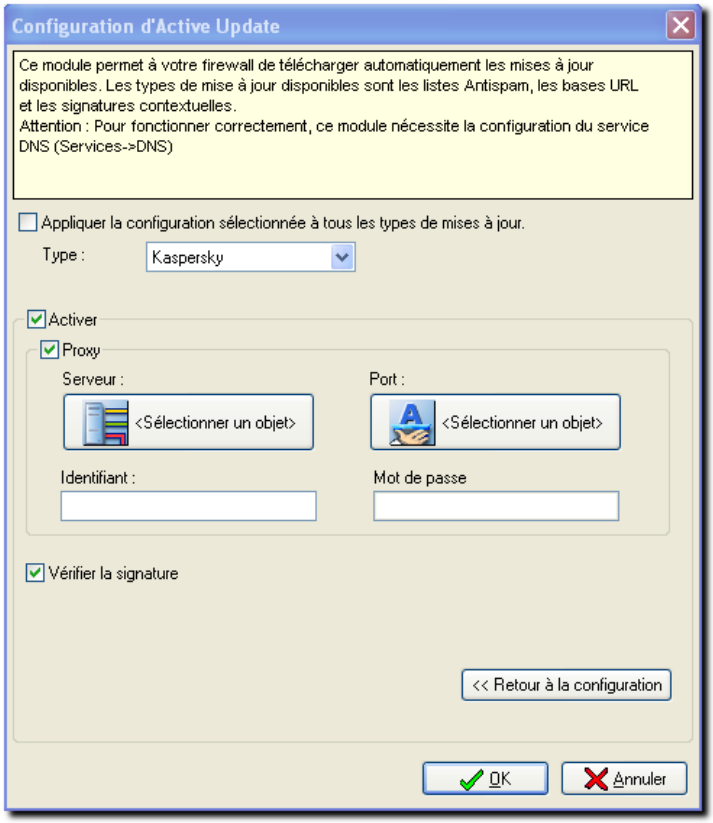


Figure 434 : Configuration Active Update - Configuration avancée

Appliquer la configuration sélectionnée à tous les types de mises à jour	Cette option vous permet de rechercher dans une liste déroulante un type de mise à jour (par exemple : Kaspersky).
Activer	Permet l'activation automatique des mises à jour.
Proxy	En activant cette option, permet la sélection d'un serveur et d'un port à partir de la base d'objets.
Identifiant	Indication d'un identifiant pour effectuer les mises à jour automatiques.
Mot de passe	Indication d'un mot de passe pour effectuer les mises à jour automatiques.
Vérifier la signature	Permet d'indiquer que les mises à jour téléchargées par Active Update sont signées numériquement par l'autorité de certification NETASQ. Le firewall vérifie donc l'intégrité etl'origine des mises à jour. En décochant cette option, vous pouvez télécharger des mises à jour depuis un serveur privé. Dans ce cas, l'origine et l'intégrité de la mise à jour n'est pas vérifiée.
Retour à la configuration	Permet de revenir à l'écran de configuration général de l'Active update.

18.1.9.3 Interface avec les autres modules

L'état des mises à jour des sous-systèmes « Active Update » est visible dans le menu `Active Update` de NETASQ REALTIME MONITOR.

PARTIE 19 : ACTIONS DIVERSES

19.1.1. Introduction

19.1.1.1. Pour cette partie, vous devez avoir franchi les étapes

- Partie 2/Chapitre 1 : Interface graphique.
- Partie 2 : Installation, intégration et pré-configuration.

19.1.1.2. Utilité de cette partie

Cette partie vous permet de modifier des paramètres divers et généraux de la configuration du firewall.

19.1.2. Options

Les options de gestion de l'application NETASQ UNIFIED MANAGER sont disponibles dans le menu **Options\Préférences.** En cliquant sur ce menu, l'écran de configuration des options de l'interface NETASQ UNIFIED MANAGER s'affiche.

Le menu de configuration des options d'affichage de l'interface est divisé en deux parties :

- A gauche un arbre présentant les diverses fonctionnalités du menu **Préférences.**
- A droite les options configurables.

Toute personne ayant accès au poste où se trouve l'interface graphique du firewall NETASQ, peut accéder à ces fonctionnalités.

19.1.2.1. Général

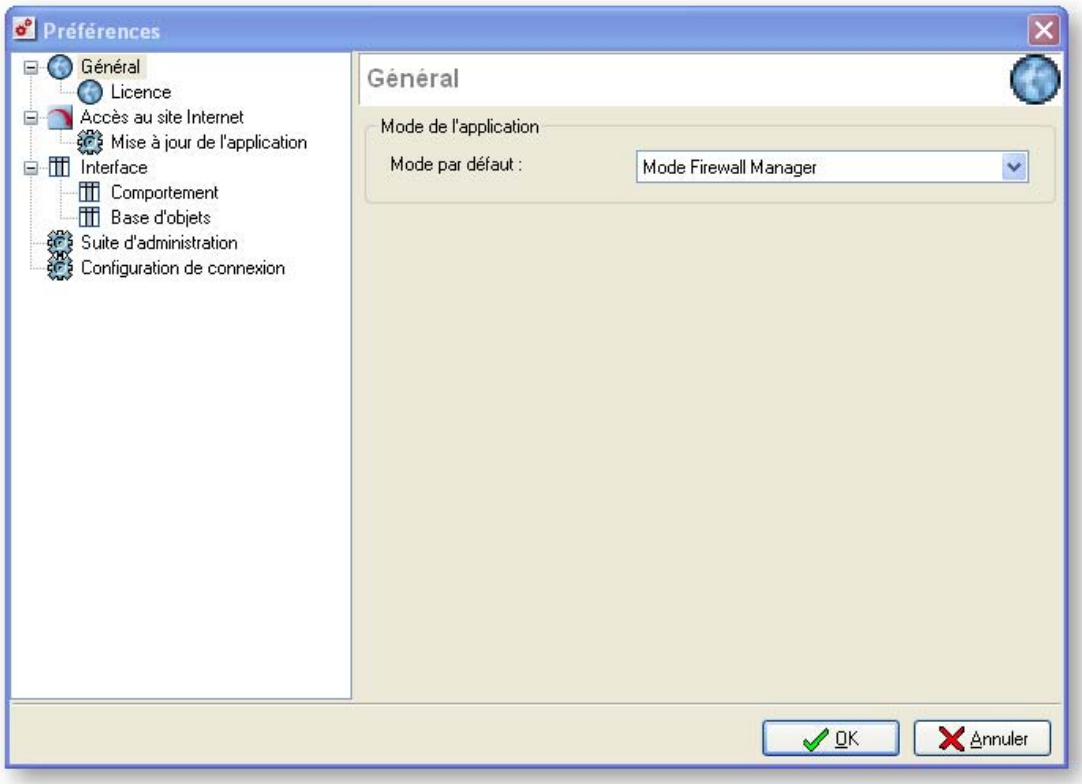


Figure 435 : Préférences - Général

Mode par défaut	Cette option vous permet de sélectionner le mode de l'application de NETASQ UNIFIED MANAGER. Les deux options possibles sont " Mode Global Administration" et "Mode Firewall Manager". Le premier mode permet de configurer un parc de firewalls alors que le second gère la configuration d'un firewall.

Licence

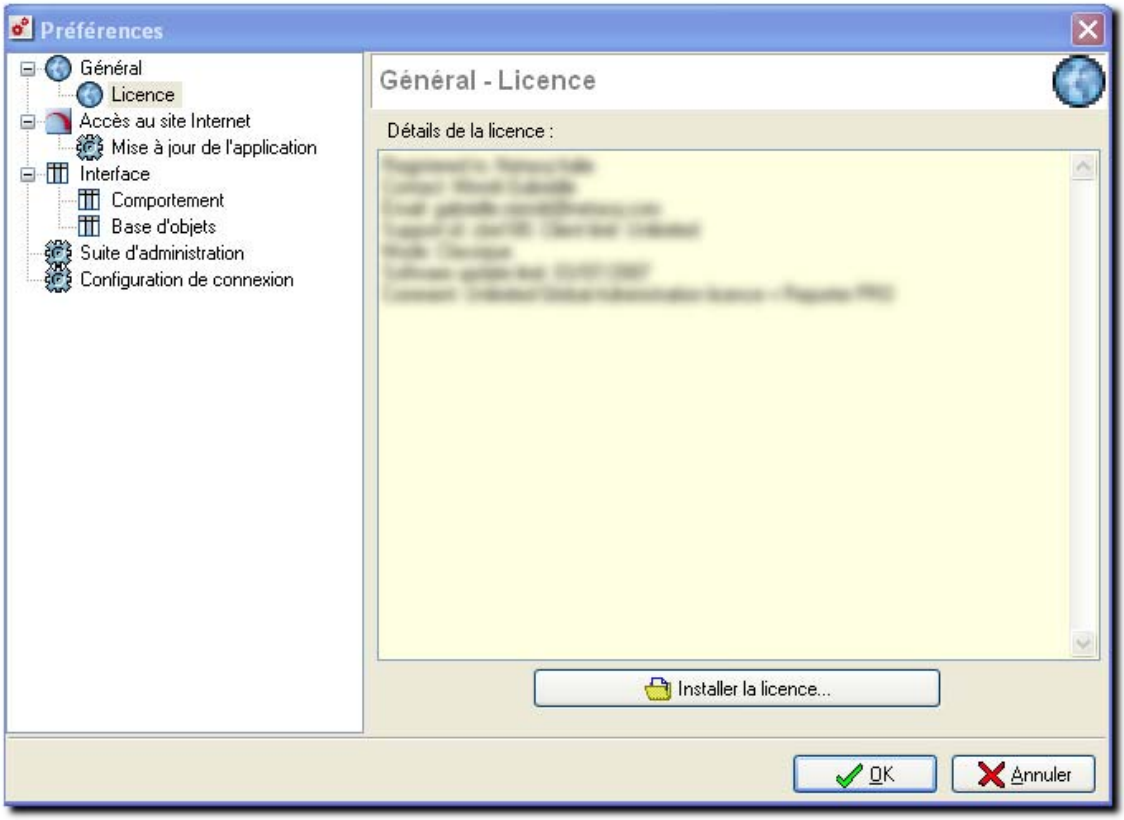


Figure 436 : Préférences - Licence

Cet vue affiche le détail des licences pour chaque application.

Attribuée à :	Nom de la société – client final
Contact :	Nom du contact dans la société
Email :	Email du contact
Support id :	Numéro de support de la société
Mode	
Limite de mise à jour du Software	Indication de la date limite de mise à jour.
Nombre limite de clients :	Nombre maximum de clients (appliances NETASQ) pouvant être gérés par l'ADMINISTRATION GLOBALE NETASQ
Commentaire	Indication du type de licence…

Le bouton **Installer la licence** vous permet de récupérer une licence plus récente préalablement téléchargée sur votre poste de travail.

19.1.2.2. Accès au site Internet

Le firewall NETASQ est un produit de sécurité qui évolue pour protéger le réseau, de menaces toujours plus évoluées. Des mises à jour régulières sont nécessaires pour prendre en compte ces différentes évolutions.

De plus les logiciels de la Suite d'Administration doivent être mis à jour pour gérer ces nouvelles fonctionnalités.

Accès pour mise à jour

Pour effectuer la recherche des mises à jour sur le site Web NETASQ, il est nécessaire de spécifier les différentes options suivantes :

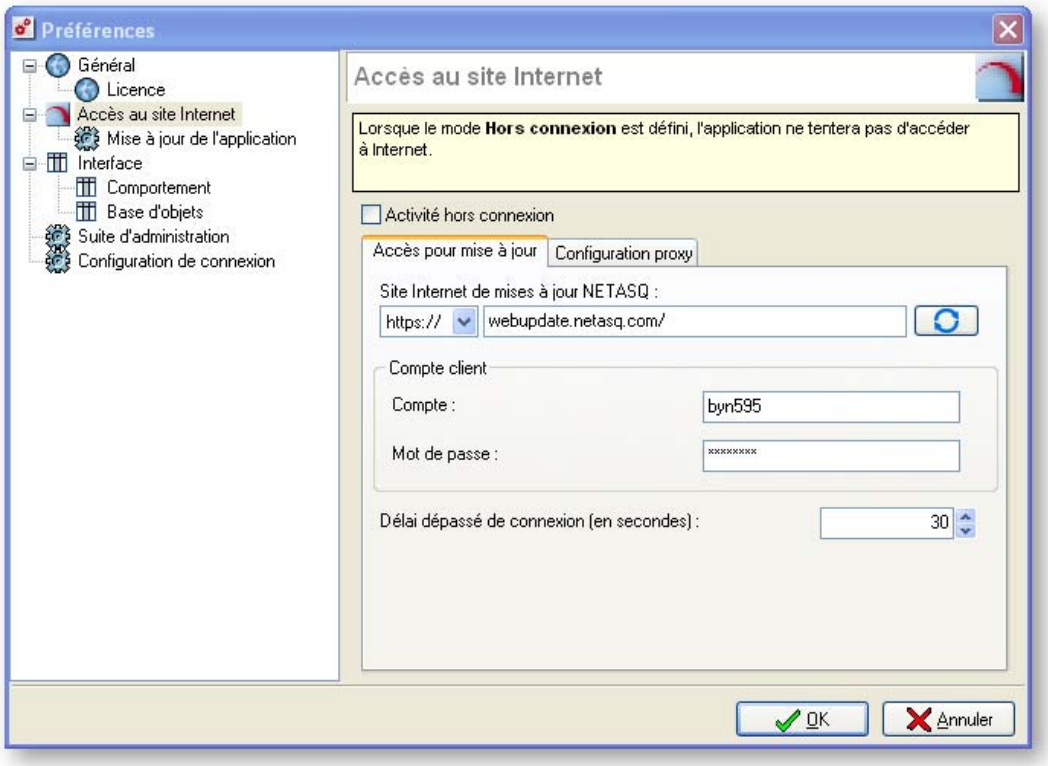


Figure 437 : Préférences - Accès au site Internet

Activité hors connexion	En cochant cette option, l'application ne tente pas d'accéder à Internet.
Site Internet de mises à jour NETASQ	URL en HTTP ou HTTPS permettant de contacter la section du site Web permettant la recherche des mises à jour. Le bouton permet de rappeler l'adresse URL du site qui est spécifiée par défaut.
Compte	Login d'accès au site WEB NETASQ permettant à l'Administration Globale NETASQ de récupérer les mises à jour des produits. Il s'agit d'un compte d'accès à l'espace client ou à l'espace partenaire.
Mot de passe	Mot de passe associé au compte support spécifié ci-avant. Par défaut ce mot de passe est le code d'activation indiqué sur l'étiquette située sous le produit NETASQ.
Délai dépassé de connexion (en secondes)	L'Administration Globale NETASQ tente de se connecter au site Web NETASQ durant le délai indiqué. En cas d'échec de connexion, les informations relatives au site WEB ne sont pas mises à jour.

Configuration Proxy

L'onglet **Configuration proxy** permet d'accéder à la configuration d'un proxy pour l'accès de l'application à Internet.

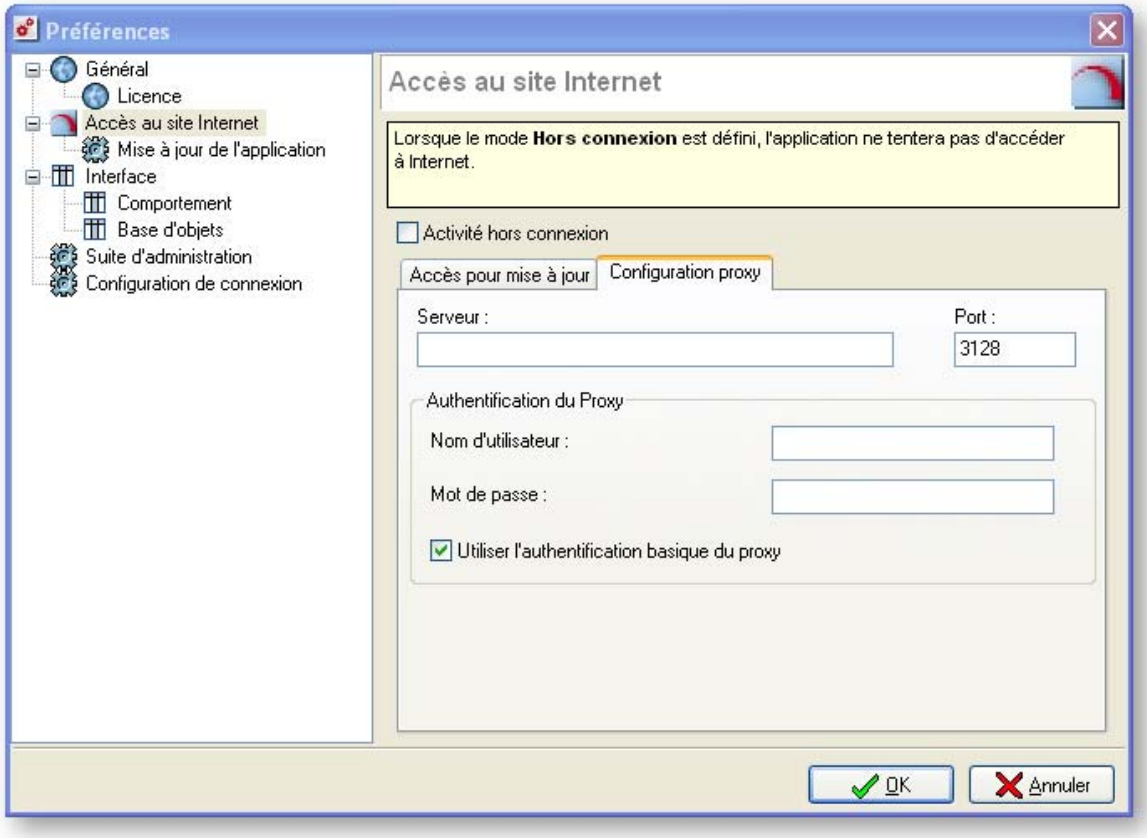


Figure 438 : Préférences - Accès au site Internet

S'il existe un proxy pour l'accès à Internet sur le réseau, il est indispensable de remplir la configuration du proxy. Sans cette configuration, il sera alors impossible au NETASQ UNIFIED MANAGER de vérifier la présence d'une mise à jour sur le site Web NETASQ. Les différentes options sont les suivantes :

Serveur	Adresse IP ou nom de machine du proxy par lequel la station d'administration doit se connecter pour accéder à Internet.
Port	Port à utiliser pour contacter le proxy, par défaut ce port est 3128.
Nom d'utilisateur	Login de la station d'administration si une authentification est n'est nécessaire pour accéder au proxy.
Mot de passe	Mot de passe de connexion au proxy associé au login.
Utiliser l'authentification basique du proxy	Définit que l'authentification est effective. Si la case n'est plus cochée, il n'y a pas d'authentification même si le proxy la demande.

Mise à jour de l'application

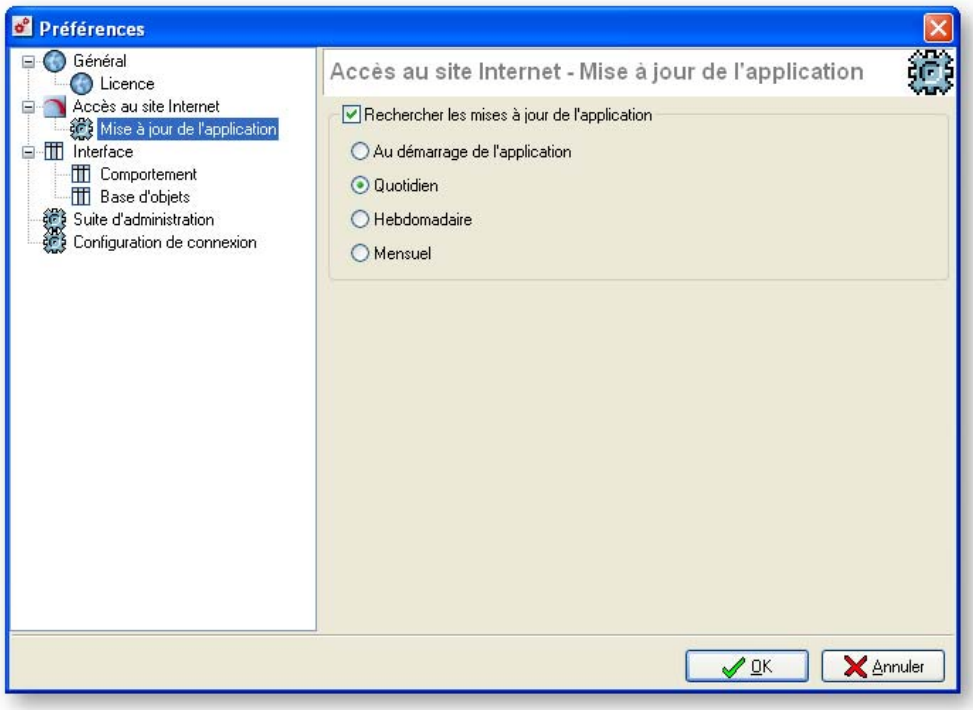


Figure 439 : Préférences - Mise à jour de l'application

L'intervalle de mise à jour peut être important car lorsque NETASQ publie une nouvelle mise à jour critique, il est préférable que cette mise à jour soit vite repérée. Par défaut, cette fréquence de recherche des mises à jour est disposée à **Quotidien** mais il est possible de modifier cet intervalle parmi : **Au démarrage de l'application**, **Hebdomadaire** et **Mensuel**.

Par défaut Active Update effectue une recherche de mise à jour de la Suite d'Administration selon la fréquence sélectionnée. Si l'option **Rechercher les mises à jour de l'application** est cochée, une recherche automatique de firmware firewall est effectuée. Sinon il n'y a pas de recherche automatique de firmware.

Lorsque la période de référence sélectionnée est écoulée, NETASQ UNIFIED MANAGER effectue une recherche de mises à jour lors de son démarrage. Si une mise à jour du firmware ou de la Suite d'Administration est trouvée sur le site Web NETASQ, une indication est présente sur la page principale de NETASQ UNIFIED MANAGER.

19.1.2.3. Interface

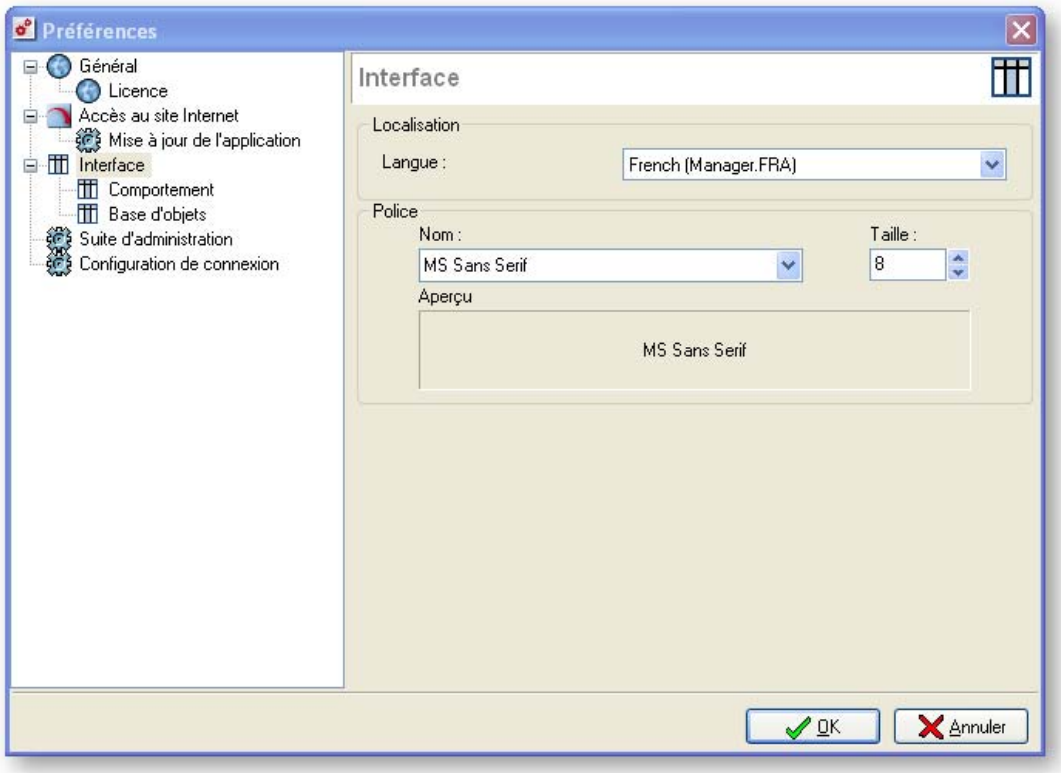


Figure 440 : Préférences - Interface

Les différentes options de l'interface sont présentées dans le tableau suivant :

Langue	Cette option vous permet de choisir la langue dans laquelle apparaissent les menus de l'interface graphique. **AVERTISSEMENT** Une fois la langue choisie, vous devez redémarrer l'interface pour prendre en compte la modification. Le choix **<Détection automatique>** permet d'utiliser la langue utilisée par le système d'exploitation "Windows".
Police	Police et taille des informations qui seront affichées dans les grilles de configuration de NETASQ UNIFIED MANAGER (Exemple : règles de filtrage).

Comportement

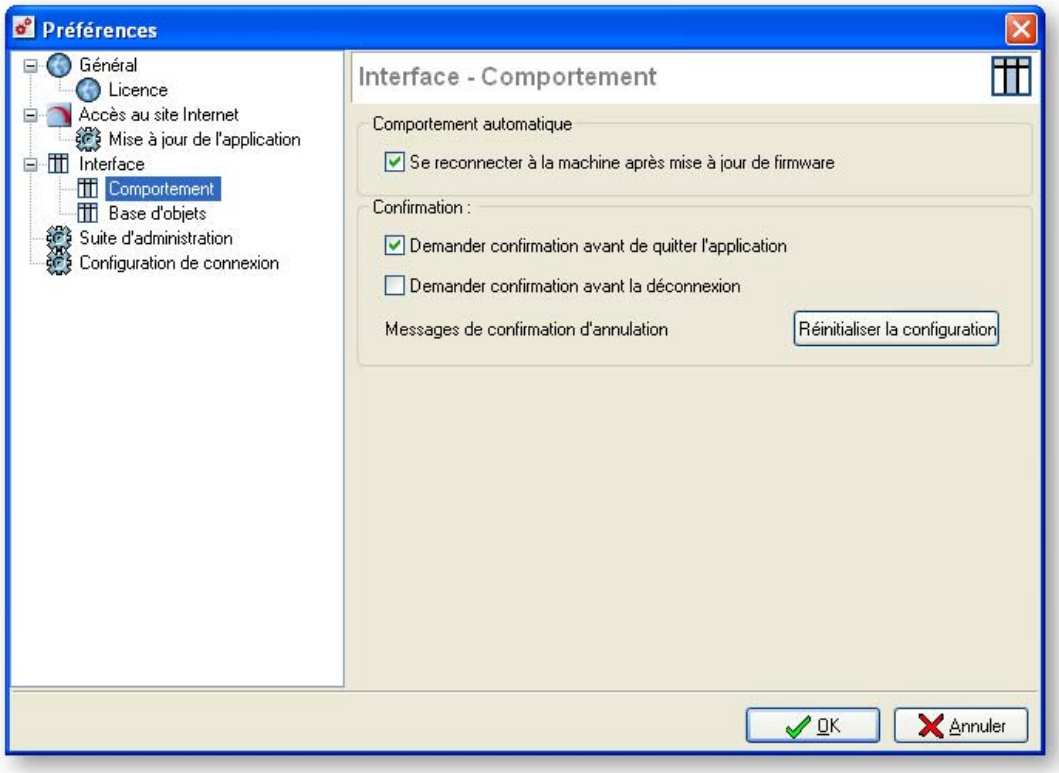


Figure 441 : Préférences - Comportement

Les options de confirmations déterminent la façon dont est terminée l'application NETASQ UNIFIED MANAGER. Il existe deux options de confirmations :

Se reconnecter à la machine après mise à jour de firmware	Lors du redémarrage d'un boîtier UTM, il est possible de configurer le NETASQ UNIFIED MANAGER pour que celui-ci se reconnecte automatiquement à l'appliance sans avoir à surveiller son redémarrage effectif. (Cf. Partie 18/Chapitre 1 : Redémarrage du firewall).
Demander confirmation avant de quitter l'application	Un message de confirmation apparaît avant la fermeture de l'application NETASQ UNIFIED MANAGER.
Demander confirmation avant la déconnexion	Un message de confirmation apparaît avant que la connexion entre NETASQ UNIFIED MANAGER et le firewall ne soit coupée.
Messages de confirmation d'annulation	Certains menus de configuration demandent la confirmation de l'abandon des modifications avant de quitter un menu. Ces messages peuvent être masqués. Le bouton **Réinitialiser la configuration** permet la remise à zéro des messages de confirmation masqués.

Base d'objets

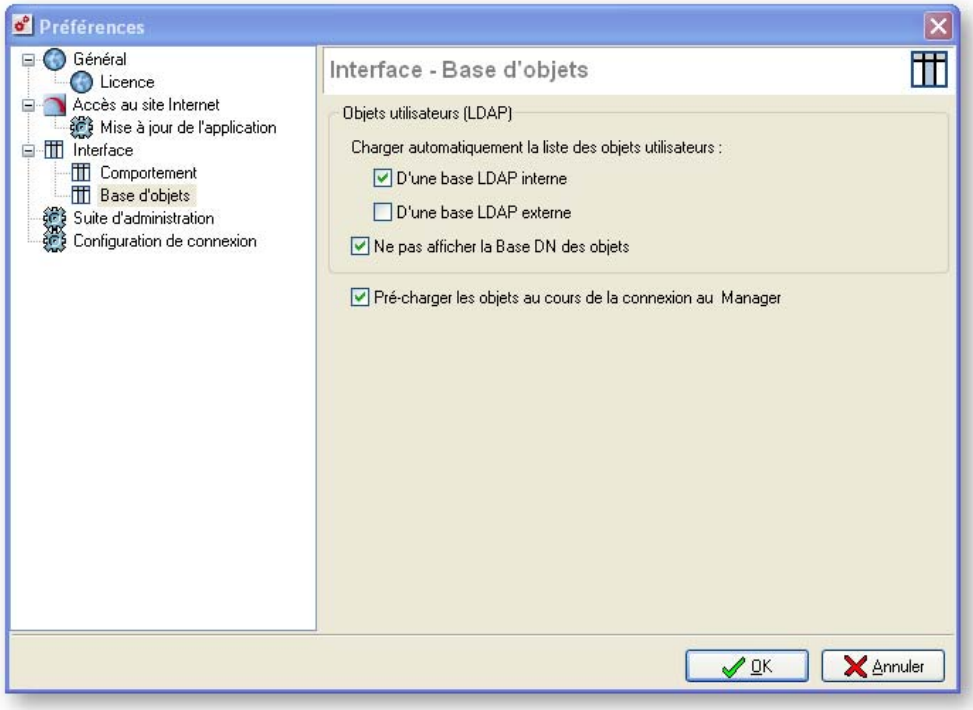


Figure 442 : Préférences - Base d'objets

Les différentes options de traitement des objets sont présentées dans le tableau suivant :

Charger automatiquement la liste des objets utilisateurs	Par défaut, lorsque la base LDAP est chargée entièrement dans la configuration des objets, NETASQ UNIFIED MANAGER affiche un message d'avertissement, car dans certains cas, la base LDAP peut s'avérer conséquente et le chargement est alors très long. En cochant l'option **D'une base LDAP interne**, ce message d'avertissement est masqué dans le cas d'une base LDAP interne. En cochant l'option **D'une base LDAP externe**, ce message d'avertissement est masqué dans le cas d'une base LDAP externe.
Ne pas afficher le BaseDN des objets	Les utilisateurs stockés dans les bases d'utilisateurs utilisées par les boîtiers UTM NETASQ (internes ou externes) sont identifiés par leur nom (appelé CN ou Common Name) et l'organisation à laquelle ils appartiennent (appelée Base DN). Cette Base DN est identique à tous les utilisateurs de la base et reprend les champs O (Nom de la société) et DC (Pays) demandés dans la construction des bases LDAP. Cocher l'option **Ne pas afficher le Base DN des objets** simplifie l'affichage des objets utilisateurs et groupes d'utilisateurs en masquant la partie **Organisation**.
Pré-charger les objets au cours de la connexion au Manager	Cette option permet un chargement anticipé de certaines informations nécessaires à la réalisation de tâches basiques.

19.1.2.4. Suite d'administration

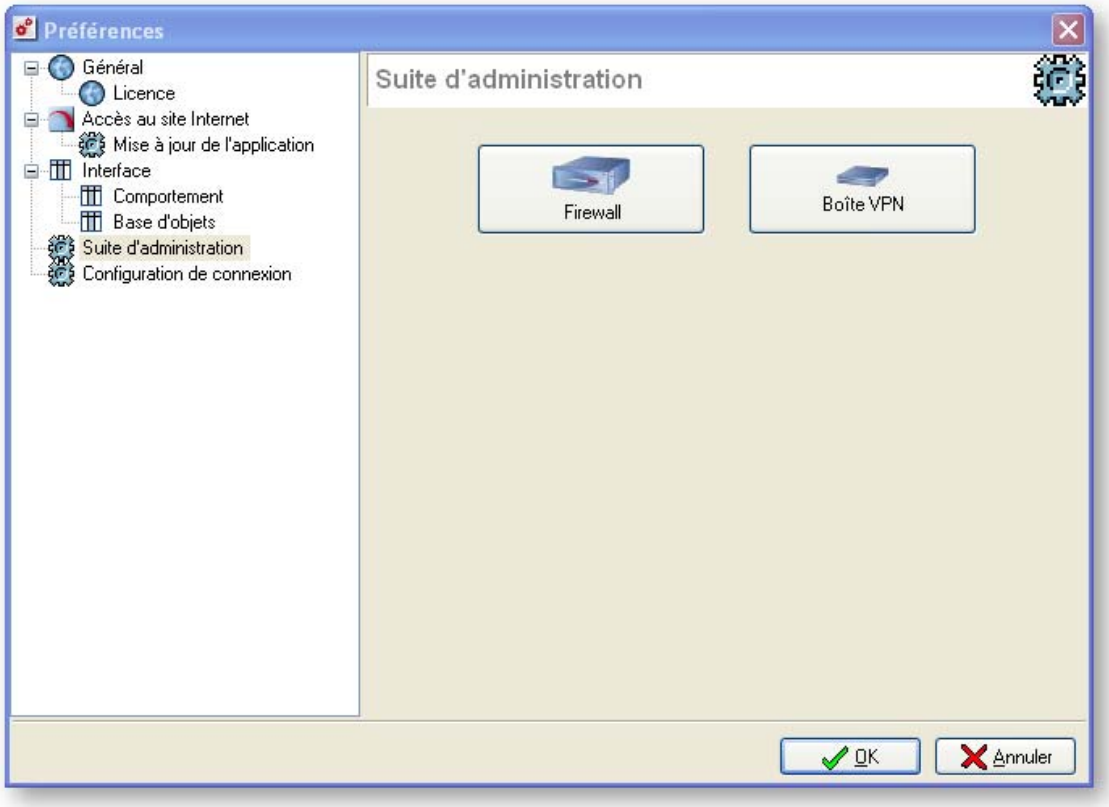


Figure 443 : Préférences - Suite d'administration

Ce menu permet de définir les chemins d'accès vers les différents applicatifs NETASQ utilisés par l'Administration Globale NETASQ.

Pour chaque type d'Appliance (Firewall, Boîte VPN), cliquez sur le bouton correspondant.

Firewall	Pour les firewalls.
Boîte VPN	Pour les VBOX.

Dans la fenêtre qui s'affiche, choisissez pour chaque application le chemin correspondant à chaque version logicielle (si votre parc d'appliances contient des produits dans des versions logicielles différentes, il est possible de spécifier ici les logiciels à utiliser dans chacune des versions). Ainsi, l'Administration globale NETASQ lancera automatiquement le logiciel adéquat en fonction du type d'Appliance et de la version logicielle.

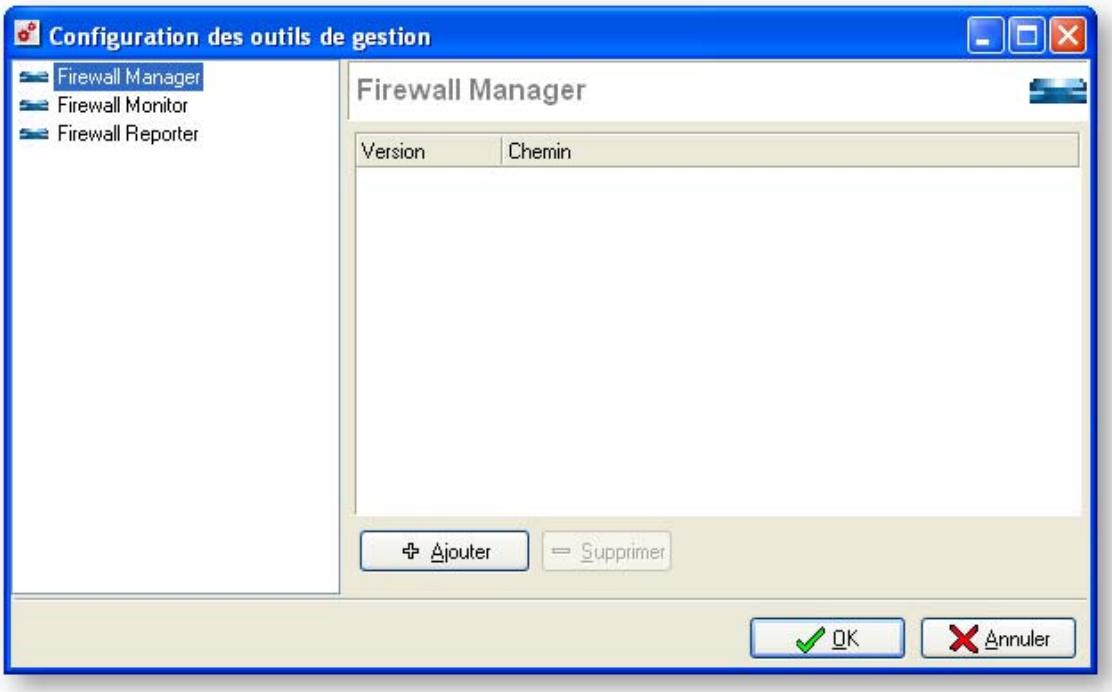


Figure 444 : Configuration des outils de gestion - Firewall Manager

Pour ajouter une version et le chemin du logiciel qui correspond, cliquez sur le bouton **Ajouter.** Indiquez le numéro de version dans la colonne "Version" et choisissez le logiciel associé en cliquant sur le bouton dans la colonne "Chemin".

Pour retirer une version, sélectionnez celle-ci et cliquez sur le bouton **Supprimer**.

Cliquez sur **OK** une fois la configuration des applications terminée.

19.1.2.5. Configuration de connexion

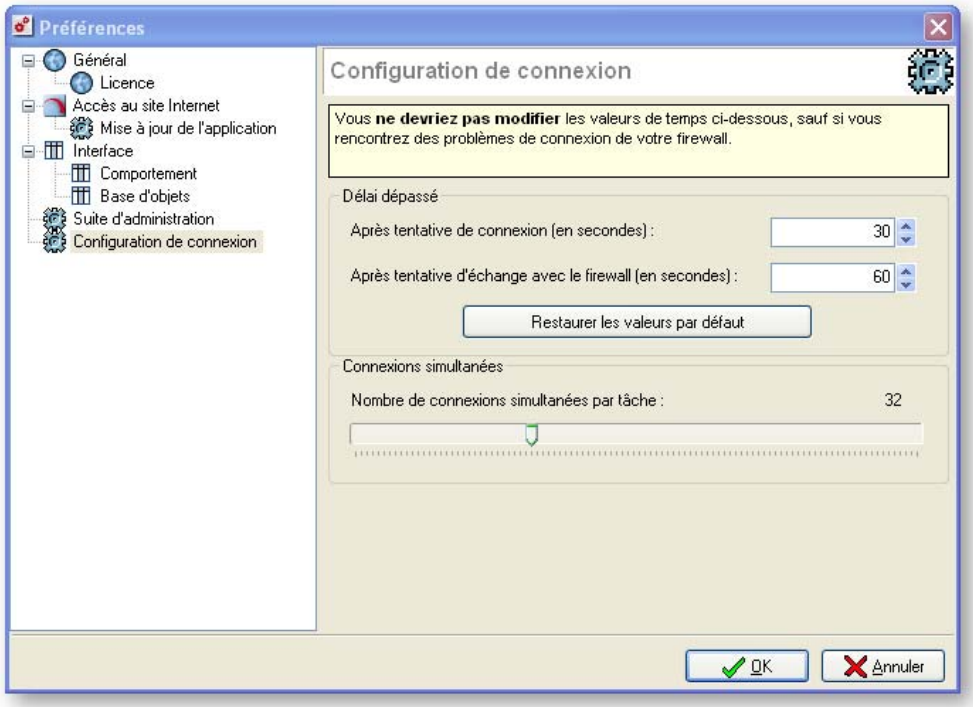


Figure 445 : Préférences - Configuration de connexion

Après tentative de connexion (en secondes)	Indication du délai de connexion. En cas d'échec, la connexion n'est pas établie.
Après tentative d'échange avec le firewall (en secondes)	Indication du délai limite après tentative d'échange avec le firewall.
Restaurer les valeurs par défaut	En cliquant sur ce bouton, vous restaurez les délais d'origine. Vos modifications sont effacées.
Nombre de connexions simultanées par tâche	Indication du nombre de connexions simultanées par tâche. Déplacez le curseur pour baisser ou augmenter ce nombre.

19.1.3. Applications

19.1.3.1. Lancer le Monitor et le Reporter

Le menu **Applications** que l'on trouve depuis l'interface d'accueil de NETASQ UNIFIED MANAGER se décompose en deux sous-menus :

- Lancer NETASQ REAL-TIME MONITOR
- Lancer NETASQ EVENT REPORTER

Figure 446 : Monitor et Reporter

Ces deux sous-menus permettent l'ouverture des logiciels NETASQ REAL-TIME MONITOR et NETASQ EVENT REPORTER de la Suite d'Administration NETASQ au moyen de NETASQ UNIFIED MANAGER. Utiliser les deux raccourcis procurent l'avantage de ne pas devoir se ré-authentifier sur les deux applications. L'authentification réalisée sur NETASQ UNIFIED MANAGER est réalisée par les deux applications.

19.1.4. Licence

Chaque firewall possède une licence qui définit l'ensemble des fonctionnalités disponibles pour votre firewall. Cette clé vous permet d'activer certaines options du firewall (filtrage d'URL, chiffrement VPN fort, mises à jour ...). Cette clé peut être récupérée sur le site Web NETASQ (www.netasq.com).

19.1.4.1. Première connexion

Lors de votre première connexion, le firewall ne contient aucune licence. Sans elle, il est inutilisable. L'écran de configuration de la licence apparaît alors.

> **AVERTISSEMENT**
> Si, à la réception de votre firewall, aucun message concernant la licence n'apparaît, c'est que NETASQ a installé une licence temporaire dans votre produit. Cette licence correspond à la licence minimale du produit NETASQ (aucune option n'est activée). De plus si un incident survient alors que la licence temporaire est toujours installée sur votre produit, vous ne serez pas couvert par la garantie. Ainsi même si votre firewall fonctionne temporairement, NETASQ vous conseille de télécharger au plus vite votre licence définitive avant l'expiration de cette licence temporaire.

Le bouton **Licence** vous permet d'insérer votre licence préalablement récupérée sur le site web NETASQ et ainsi activer la configuration de votre firewall.

19.1.4.2. La licence de votre firewall et sa mise à jour

NETASQ UNIFIED MANAGER est livré avec une licence pour 5 boîtiers UTM. Ce qui permet à l'administrateur d'importer le carnet d'adresses quelque soit sa taille.

Ces renseignements sont accessibles par le menu **`Firewall\Licences`** depuis l'interface principale de NETASQ UNIFIED MANAGER.

L'écran de configuration de la licence vous donne la version de votre firewall, des informations sur le matériel et les différentes options avec leur date d'expiration s'il y en a une.

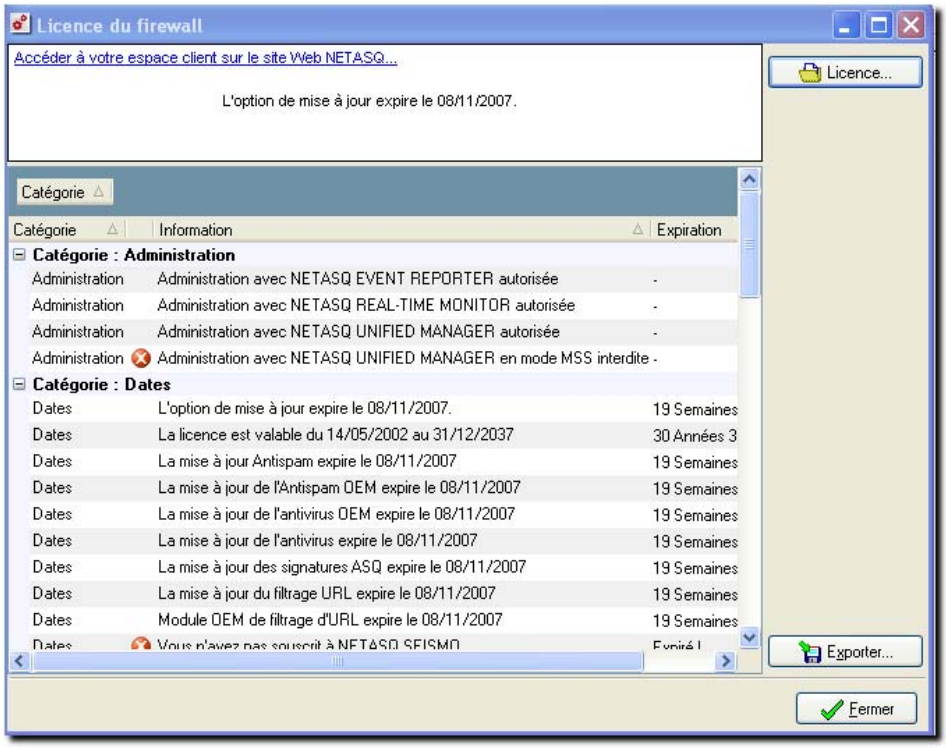


Figure 447 : Licence du firewall

Le firewall NETASQ est livré par défaut avec l'ensemble de ses fonctionnalités. Cependant, certaines fonctionnalités (filtrage URL, Haute Disponibilité...) sont optionnelles et ne sont pas activées. D'autre part certaines options, comme la mise à jour, sont limitées dans le temps. Si la date d'expiration est dépassée, certaines options sont désactivées sur le firewall.

Si vous choisissez d'utiliser de nouvelles fonctionnalités ou renouveler certaines options, veuillez contacter votre revendeur. Une nouvelle clé sera alors disponible sur le site Web de NETASQ. Entrez cette clé avec le bouton "Mettre à jour la licence" situé en bas à gauche puis validez en envoyant au firewall. Les informations concernant votre firewall sont modifiées et les nouvelles options sont activées sur le firewall.

19.1.5. Configurer les paramètres système

Pour modifier les paramètres du firewall NETASQ allez dans le sous-menu **Firewall\Configuration du Système**. L'écran de configuration système est divisé en deux onglets :

- L'onglet **Système.**
- L'onglet **Fuseau horaire.**

19.1.5.1. Onglet Système

Figure 448 : Configuration du firewall - Système

L'onglet Système permet la modification des paramètres suivants :

- Nom du firewall (ce nom est utilisé dans les mails d'alarmes envoyés à l'administrateur et est affiché sur la fenêtre principale du firewall. Ce nom peut-être quelconque.
- Date. Choisissez la date sur le calendrier.
- Heure.
- Langue du firewall (type de clavier supporté par le firewall).

La date et l'heure auxquelles votre firewall NETASQ est réglé sont importantes : elles vous permettent de situer dans le temps un événement enregistré dans le fichier log. Elles servent également à la programmation horaire des configurations.

A chaque ouverture de cette boîte de dialogue, le logiciel de configuration à distance vous indique l'heure et la date actuellement paramétrées sur le Firewall NETASQ.

19.1.5.2. Onglet Fuseau horaire

AVERTISSEMENT
Un changement de fuseau horaire entraîne un redémarrage du firewall.

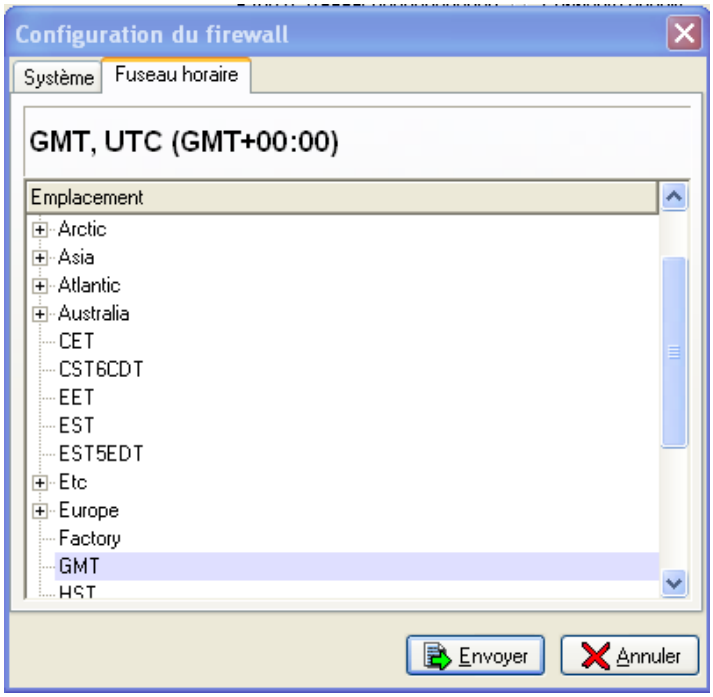


Figure 449 : Fuseau horaire

19.1.6. Sécurité

Pour modifier les paramètres de sécurité du firewall NETASQ allez dans le menu **Firewall\Sécurité**.

Ce menu est constitué de deux onglets :

- **Mot de passe Admin** : Permet la modification du mot de passe du compte super-administrateur, le compte « admin ».
- **Accès SSH** : Configuration de l'accès à l'Appliance NETASQ via un client SSH en mode console.

Mot de passe Admin

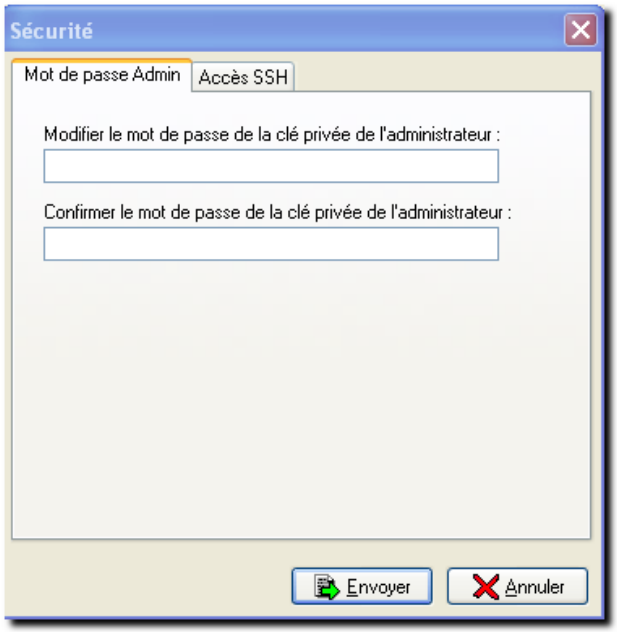


Figure 450 : Sécurité - Mot de passe Admin

Les champs **Modifier le mot de passe de la clé privée de l'administrateur** et Confirmer le mot de passe de la clé privée de l'administrateur vous permettent de modifier le mot de passe utilisé pour vous connecter en SSH au firewall. Ce mot de passe correspond au mot de passe du compte "admin". Si vous changez le mot de passe, vous devrez aussi utiliser ce nouveau mot de passe pour vous connecter via l'interface graphique, sous le compte "admin".

Accès SSH

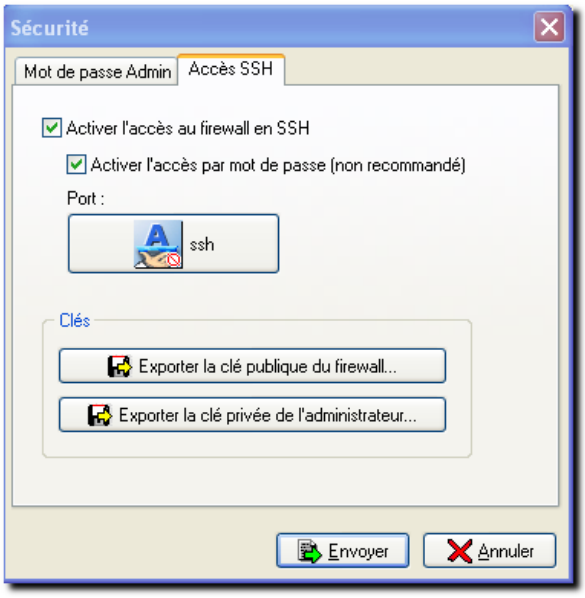


Figure 451 : Sécurité - Accès SSH

Le firewall possède un serveur SSH (version 2) intégré. Ce serveur vous permet, via un client SSH, d'accéder au firewall en mode console de façon totalement sécurisée. La configuration du serveur peut se réaliser à partir de cet onglet. Les communications entre un client et un serveur SSH sont chiffrées et authentifiées afin d'assurer un maximum de sécurité durant la configuration. Pour activer le serveur, cochez la case "Activer l'accès SSH au firewall". Si cette case n'est pas cochée, il sera impossible de vous connecter à distance en mode console.
Vous pouvez exporter la clé publique du firewall et la clé privée de l'administrateur, afin de les installer sur la machine intégrant le client SSH, grâce aux boutons appropriés. Le format d'export de la clé privée de l'admin est celui d'OpenSSH, incompatible avec SSH.COM.

L'onglet **Fuseau horaire** vous permet de configurer la plage horaire de votre firewall.

> **AVERTISSEMENT**
> SSH fonctionne avec certificats. Toutefois vous pouvez toujours activer l'option Activer l'accès par mot de passe pour utiliser un accès login/password mais cette option n'est pas recommandée.

Par défaut, le filtrage du firewall bloque la connexion sur le port 22 (SSH) du Firewall. Il est donc nécessaire de mettre en place une règle de filtrage pour autoriser cette communication.

19.1.7. Configuration sécurisée

19.1.7.1. Introduction

La configuration du firewall contient des informations très sensibles. Ces informations révèlent l'activité du réseau et la manière de contourner les mécanismes de protection de ce réseau. Pour protéger ces données sensibles, il est possible d'utiliser les fonctionnalités de chiffrement des firewalls sur les fichiers de configuration du firewall lui-même.

Les fichiers de configuration chiffrés ne pouvant être déchiffrés qu'au moyen d'un secret détenu par le firewall et l'administrateur, ce dernier se protège contre le vol et l'utilisation illicite de son firewall. En effet sans déchiffrement des fichiers, le firewall est inutilisable.

19.1.7.2. Principe de fonctionnement

Pour mettre en place cette technologie, NETASQ propose l'utilisation de clés USB qui contiendront les secrets échangés. Sans cette clé, il est impossible de démarrer le firewall. Une fois la configuration chargée en mémoire, la clé USB peut être retirée pour préserver la confidentialité des fichiers de configuration. Au prochain démarrage, la clé est de nouveau indispensable.

> **AVERTISSEMENT**
> NETASQ a qualifié des clés USB compatibles avec cette fonctionnalité. Seules les clés USB qualifiées et distribuées par NETASQ sont donc supportées pour cette fonctionnalité.
> Cette fonctionnalité n'est disponible que pour les produits possédant un port USB effectivement fonctionnel.

19.1.7.3. Configuration sécurisée

L'activation des fonctionnalités de configuration sécurisée est réalisée dans le menu **Firewall \Configuration sécurisée** de la barre de menu de l'interface graphique NETASQ UNIFIED MANAGER

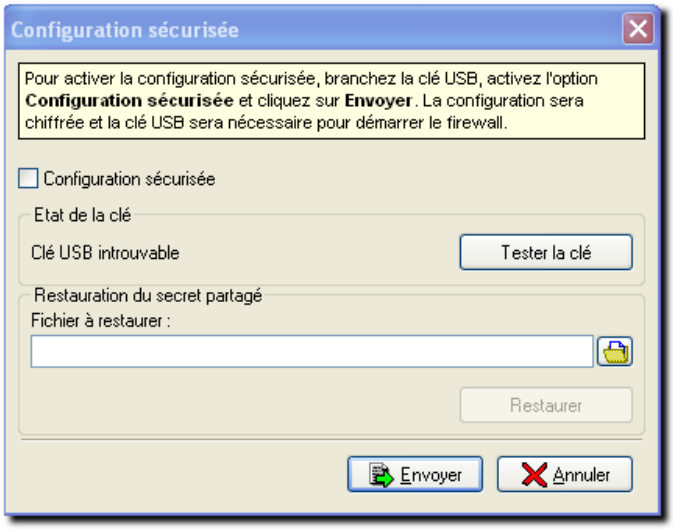


Figure 452 : Configuration sécurisée

Les différentes options de la configuration sécurisée sont présentées dans le tableau suivant :

Configuration sécurisée	Bouton d'activation de la configuration sécurisée. Une fois activée, les fichiers de configuration du firewall sont chiffrés. Il est alors indispensable de posséder la clé USB contenant le secret échangé avec le firewall pour déchiffrer sa configuration.
Etat de la clé	Valeur informative remontée par le firewall indiquant l'état actuel de la clé qui servira à stocker le secret de déchiffrement. Il existe trois états différents : • **Clé USB non trouvée** : la clé n'est pas insérée dans le port USB du firewall ou pas formaté selon son format de fichiers. • **Clé USB non initialisée** : la clé est détectée mais elle ne contient pas de secret de déchiffrement de la configuration du firewall. • **Clé USB initialisée** : la clé est détectée et elle contient un secret de déchiffrement de la configuration du firewall.
Tester la clé	Avant l'affichage du menu **Configuration sécurisée,** NETASQ UNIFIED MANAGER vérifie l'état de la clé. Le bouton **Tester la clé** permet l'actualisation des informations affichées. Si une clé USB est insérée après l'affichage du menu **Configuration sécurisée**, cliquez sur le bouton **Tester la clé** pour actualiser les informations d'état de la clé.
Restauration du secret partagé.	Si le secret contenu par la clé ou la clé elle-même est défectueuse, il est alors possible de restaurer cette sauvegarde sur la même clé ou sur une autre clé vierge.
Envoyer	Activation de la configuration sécurisée. Avant la fermeture du menu, il est demandé de spécifier un chemin pour la sauvegarde de la clé de déchiffrement insérée dans la clé USB.
Annuler	Annule le paramétrage modifié de la configuration sécurisée.

Les fichiers de configuration chiffrés

Afin de faciliter la configuration, l'activation et l'utilisation de cette fonctionnalité, le firewall ne permet pas le choix des fichiers de la configuration qui seront chiffrés. Par défaut les fichiers chiffrés par la configuration sécurisée sont :

- Les clés pré-partagées de la configuration VPN.
- La configuration de l'annuaire LDAP.
- La configuration de l'authentification.
- Le fichier Key tab de la configuration SPNEGO.
- La clé privée de l'autorité de certification de la PKI.
- La configuration de la PKI.
- Les certificats signés par l'autorité de certification de la PKI.

19.1.7.4. Utilisation

L'utilisation de la fonctionnalité de chiffrement de la configuration n'est possible qu'avec les produits possédant un port USB et l'administrateur doit posséder d'une clé USB compatible. Contactez votre partenaire pour obtenir cette clé USB.

Une fois la configuration sécurisée activée, la clé USB contenant le secret est indispensable au démarrage du produit. L'administrateur retire cette clé après le démarrage du firewall ainsi la configuration de l'Appliance est sécurisée.

Pour activer la configuration sécurisée, reportez-vous à la procédure suivante :

1. Sélectionnez le menu de configuration **`Firewall\Configuration Sécurisée`**, l'écran de la configuration sécurisée apparaît.
2. Connectez la clé USB.
3. Cliquez sur **Tester la clé**, l'état de la clé doit être alors "Clé USB non initialisée".
4. Cochez l'option **Configuration sécurisée**
5. Cliquez sur **Envoyer** pour activer la configuration sécurisée.
6. La clé est initialisée, les fichiers de configuration du firewall sont chiffrés et un chemin de copie du fichier de sauvegarde est demandé.

Restaurer une clé défectueuse ou tester une clé de sauvegarde

Lors de la génération de l'initialisation de la clé USB contenant le secret partagé avec le firewall, le firewall effectue une sauvegarde de ce secret. Il est ainsi possible de réaliser des opérations de sauvegarde sur les clés USB.

Pour restaurer une clé USB, référez-vous à la procédure suivante :

1. Sélectionnez le menu de configuration **Firewall\Configuration Sécurisée**, l'écran de la configuration sécurisée apparaît.
2. Connectez la clé USB.
3. L'état de la clé peut être "Clé non initialisée" ou "Clé initialisée suivant la dégradation de la clé.
4. L'option Configuration sécurisée est normalement déjà cochée.
5. Sélectionnez le fichier de sauvegarde à restaurer en cliquant sur l'icône .
6. Cliquez sur **Restaurer** pour restaurer la clé USB.
7. Cliquez sur **Envoyer** pour terminer la restauration.

Pour créer une clé USB de sauvegarde, référez-vous à la procédure suivante :

1. Sélectionnez le menu de configuration **Firewall\Configuration Sécurisée**, l'écran de la configuration sécurisée apparaît.
2. Connectez la clé USB vierge.
3. Cliquez sur **Tester la clé**, l'état de la clé doit être alors "Clé USB non initialisée".
4. L'option **Configuration sécurisée** est normalement déjà cochée.
5. Sélectionnez le fichier de sauvegarde à restaurer en cliquant sur l'icône .
6. Cliquez sur **Restaurer** pour restaurer la clé USB.
7. Cliquez sur **Envoyer** pour terminer la création de la clé USB de sauvegarde.

19.1.8. Importer un carnet d'adresses

Il est possible d'importer un carnet d'adresses (au format .gap) en accédant au menu `Fichier\Importer un carnet d'adresses`.

Pour plus d'informations au sujet du carnet d'adresses, veuillez vous référer à la section "Partie 3/Chapitre 2 : Configuration du carnet d'adresses".

PARTIE 20 : MODE GLOBAL ADMINISTRATION

CHAPITRE 1 : PRESENTATION

20.1.1. Description

La gestion d'un parc d'équipements de sécurité est souvent une tâche complexe et très coûteuse en temps de part les nombreuses opérations à réaliser sur chaque produit afin de maintenir un niveau de sécurité optimal. Un produit de sécurité se doit notamment d'être mis à jour fréquemment pour s'adapter aux nouvelles menaces informatiques qui apparaissent quotidiennement. Ces mises à jour, lorsqu'elles sont réalisées de façon manuelle sur chaque produit, mobilisent des ressources humaines importantes.

L'Administration Globale NETASQ permet de gérer facilement et à moindre coût depuis un point central unique certaines actions d'administration sur l'ensemble d'un parc de produits NETASQ :

- Mise à jour automatique et centralisée des firmwares NETASQ.
- Mise à jour automatique et centralisée des licences.
- Déploiement de politiques de sécurité et de bases d'objets.
- Sauvegarde et restauration des configurations et des politiques de sécurité.
- Sauvegarde des partitions système.
- Exécution d'outils d'administration.
- Lancement des outils NETASQ : NETASQ UNIFIED MANAGER, NETASQ REAL-TIME MONITOR, NETASQ EVENT REPORTER pour l'administration, le monitoring et l'analyse des traces de chaque firewall du parc.

L'Administration Globale NETASQ est capable de se connecter automatiquement au site Web NETASQ afin de récupérer les mises à jour et les licences des boîtiers UTM, il peut ensuite se connecter de façon tout aussi automatique aux Appliance gérés pour mettre à jour ces derniers, ce qui réduit considérablement le temps d'administration du parc.

L'autre fonction de l'Administration Globale NETASQ est d'apporter des outils pour le monitoring et la supervision du parc d'équipements NETASQ :

- Indicateur d'état du produit NETASQ ou d'une machine sur le réseau (en ligne, inaccessible ou arrêté, version logicielle actuelle, version de la licence…).
- Indicateur d'état système de chaque produit.
- Indicateur d'état de la sécurité.

Les informations peuvent être visualisées sous forme tabulaire ou sous forme graphique de type topologique afin d'offrir la plus grande simplicité de lecture des informations et une administration la plus intuitive et la plus ergonomique.

Cette partie décrit les différents éléments et fonctionnalités composant l'Administration Globale NETASQ afin de guider l'administrateur dans sa tâche de configuration et d'utilisation du produit.

20.1.2. Accès

➲ Pour utiliser l'Administration Globale NETASQ, lancez l'application à partir du menu Démarrer de Windows, par le chemin suivant : **`Démarrer\Programmes\Netasq\Administration Suite 7.0\NETASQ UNIFIED MANAGER.`**

AVERTISSEMENT
Le mode Global Administration doit être indiqué dans le menu **`Options\Préférences\Général.`**

20.1.3. Création/ouverture d'un projet

L'Administration globale NETASQ fonctionne en mode projet. Il est donc possible de réaliser plusieurs configurations (projets), correspondant chacune à un ensemble de produits NETASQ pouvant être administrés.

➲ Lorsque vous lancez l'Administration Globale NETASQ

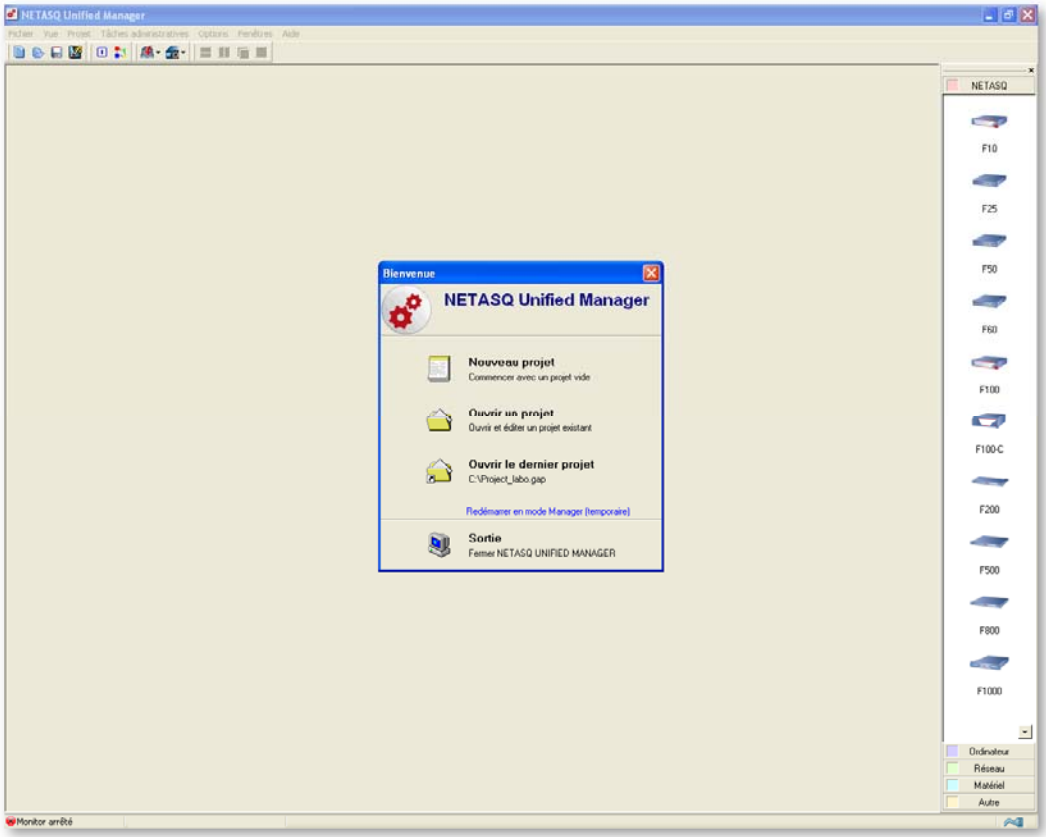


Figure 453 : Lancement de Global Administration

Plusieurs choix vous sont proposés :

- **Nouveau projet** : permet de créer un nouveau projet, soit une nouvelle configuration d'administration.
- **Ouvrir un projet** : permet d'ouvrir un projet déjà existant. Une fenêtre s'ouvre alors afin de permettre le choix du fichier de projet correspondant.
- **Ouvrir le dernier projet** : permet d'ouvrir le dernier projet qui a été ouvert ou créé par l'Administration Globale NETASQ.

- **Redémarrer en mode Manager (temporaire)** : permet d'ouvrir NETASQ UNIFIED MANAGER en mode Firewall Manager. Dans ce cas, un message s'affiche et vous demande si vous souhaitez modifier de manière permanente le mode application en "Mode Firewall Manager".
- **Sortie**: permet de quitter l'application immédiatement.

Un seul projet peut être ouvert par instance de l'Administration Globale NETASQ.

Lors de la première utilisation de l'Administration Globale NETASQ, il faut choisir l'option **Nouveau projet**.

CHAPITRE 2 : PRISE EN MAIN

20.2.1. Présentation de l'interface

20.2.1.1. Fenêtre principale

La fenêtre générale, lors de la création d'un nouveau projet, se présente de la manière suivante :

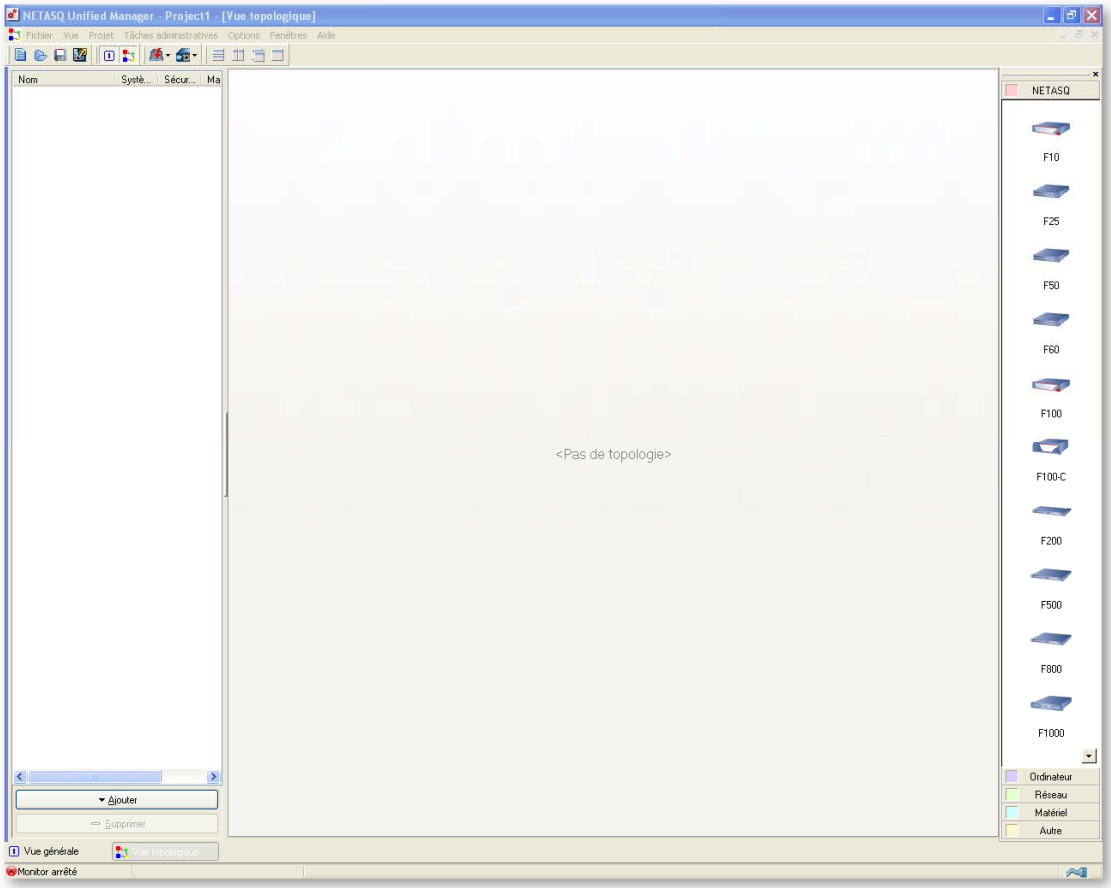


Figure 454 : Fenêtre principale

Cette fenêtre est décomposée en plusieurs parties :

- Une barre de menus.
- Une barre d'icônes de raccourcis.

- Une barre d'objets.
- La vue globale (tableau listant les firewalls du projet).
- Une barre pour la permutation des vues.

20.2.1.2. Barre des menus

Cette barre contient les menus suivants :

- **Fichier**
- **Vue**
- **Projet**
- **Tâches administratives**
- **Options**
- **Fenêtres**
- **Aide**

20.2.1.3. Barre d'icônes de raccourcis

La barre suivante contient des raccourcis vers certaines opérations :

Figure 455 : Icônes de raccourci

	Permet de créer un nouveau projet (correspond au menu **Fichier\ Nouveau)**.
	Permet d'ouvrir un projet déjà existant (correspond au menu **Fichier\Ouvrir**).
	Permet d'enregistrer le projet en cours (correspond au menu **Fichier\Enregistrer**).
	Permet de définir ou de modifier les préférences de l'Administration Globale NETASQ (correspond au menu **Options\Préférences**).
	Permet d'afficher ou de masquer la vue générale (correspond au menu **Vue\Vue générale**).
	Permet d'afficher ou de masquer la vue topologique (correspond au menu **Vue\Vue topologique**).
	Menu d'accès aux fonctionnalités de configuration (Sauvegarde et Restauration) de l'Administration Globale. (Cf. menu **Tâches d'administratives.**)
	Menu d'accès aux fonctionnalités de mise à jour, de sauvegarde de partition et de Scripting de l'Administration globale (correspond au menu **Tâches administratives**).
	Permet d'organiser la disposition des fenêtres du projet en cours avec une disposition horizontale (correspond au menu **Fenêtres\Disposition horizontale**).
	Permet d'organiser la disposition des fenêtres du projet en cours avec une disposition verticale (correspond au menu **Fenêtres\Disposition verticale).**
	Permet d'arranger les fenêtres du projet en cours. (correspond au menu **Fenêtres\Cascade**).
	Permet d'afficher les fenêtres du projet en cours en cascade (correspond au menu **Fenêtres\Arranger**).

20.2.1.4. Barre d'objets

La barre d'objets se présente de la façon suivante :

Figure 456 : Barre d'objets

Elle contient tous les objets pouvant être utilisés dans la vue principale pour construire une vue graphique de type topologique du réseau ou du sous-réseau administré. Ces objets sont répartis en 5 catégories :

- NETASQ
- Ordinateur
- Réseau
- Matériel
- Autre

Description des catégories

NETASQ	Cette catégorie regroupe tous les équipements NETASQ pouvant être gérés par l'Administration Globale NETASQ.
Ordinateur	Cette catégorie regroupe deux sous-ensembles : les stations de travail sur lesquelles sont installée l'Administration Globale NETASQ et les autres stations de travail du réseau (ordinateurs fixes, portables et serveurs).
Réseau	Cette catégorie regroupe les équipements de connexion réseau (réseau Internet, modem, hub, switch, scanner intranode).
Matériel	Cette catégorie regroupe certains équipements comme les imprimantes ou les firewalls d'autres marques que NETASQ.
Autre	Cette catégorie contient un objet permettant d'ajouter une note sur un schéma topologique et un objet permettant de représenter une autre topologie existante.

20.2.1.5. Barre de permutation de vues

La barre située au bas de l'écran de l'Administration Globale NETASQ indique les vues ouvertes (Vue générale et vue topologique). La vue affichée est celle dont la case est enfoncée. Pour basculer sur une autre vue ouverte, il suffit de cliquer sur le nom de celle-ci.

Figure 457 : Permutation de vues

Par défaut, deux cases sont présentes : "Vue topologique" et "Vue générale". En choisissant de masquer dans la barre d'icônes de raccourcis ou dans le menu **Vues** l'une ou l'autre des vues, vous masquez la case correspondante.

REMARQUE
D'autres cases peuvent apparaître lorsque vous configurez certaines fonctionnalités de l'Administration Globale NETASQ **`Configuration`**, **`Sauvegarder la partition`** et **`Déploiement`**).

20.2.1.6. Moniteur et Mode Web

Sous la barre de changement de vue, une barre contenant deux informations est visible. Ces informations sont relatives à l'état du moniteur et à l'état du mode Web.

Figure 458 : Monitor et mode Web

Le fonctionnement du moniteur est décrit dans la Partie 20/Chapitre 3 : Monitoring et supervision. L'état du mode Web est représenté par une prise de courant branchée (mode Web activé) ou débranchée (mode Web désactivé). Cette option détermine si l'Administration Globale NETASQ peut se connecter sur le site Web NETASQ pour récupérer les informations de mise à jour sur les firewalls. Pour modifier l'état du mode, réalisez un double clic sur l'icône représentant la prise ou définissez l'option du projet relative au site Web, **Activité hors connexion** du menu **`Options\Préférences\Accès au site Internet`**.

20.2.1.7. Vue Topologique

Cette vue est la première vue s'affichant lors de la création d'un nouveau projet :

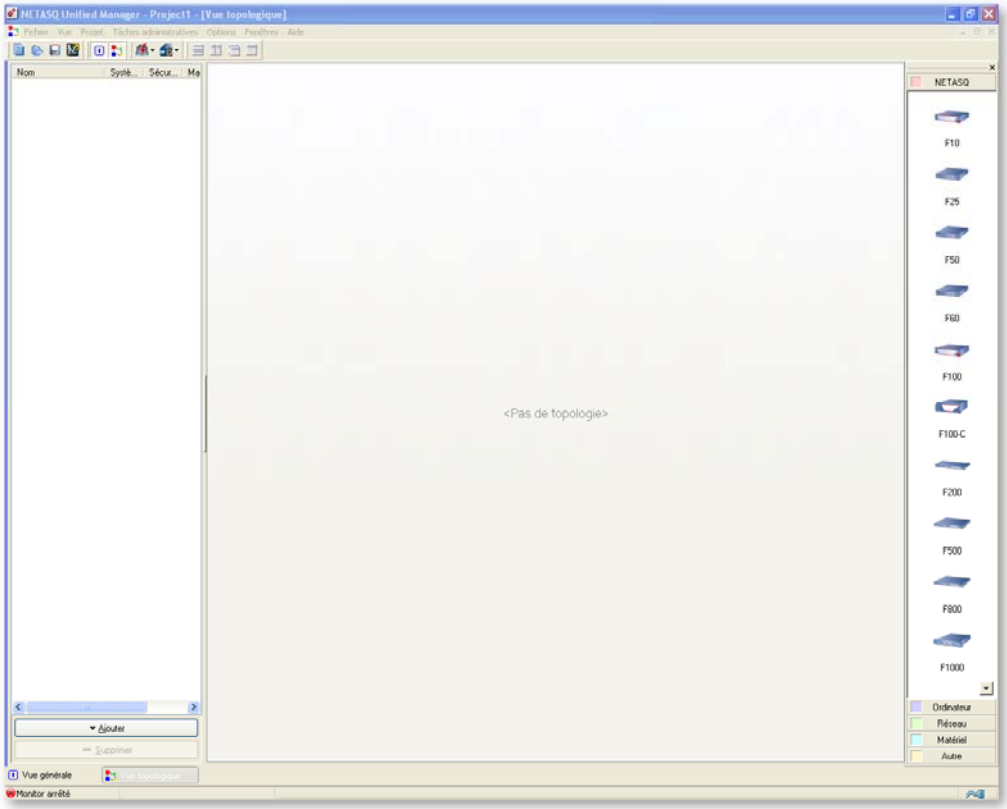


Figure 459 : Vue topologique

Des explications supplémentaires sur cette vue seront données dans la suite du manuel.

20.2.2. Présentation des menus

20.2.2.1. Fichier

Nouveau projet	Permet de créer un nouveau projet.
Ouvrir	Permet d'ouvrir un projet existant.
Enregistrer	Permet d'enregistrer les modifications réalisées sur le projet en cours.
Enregistrer sous	Permet d'enregistrer le projet sous un autre nom.

Importer le carnet d'adresses	Permet de récupérer un carnet d'adresses existant au format **.gap**
Importation de fichier firewall	Permet d'importer un fichier au format **.csv** contenant une liste d'équipements NETASQ.
Exportation de fichier firewall	Permet d'exporter un fichier au format **.csv** contenant une liste d'équipements NETASQ.
Quitter	Permet de quitter l'application.

20.2.2.2. Vue

Vue Générale	Permet d'ouvrir ou de fermer la vue générale.
Vue topologique	Permet d'ouvrir ou de fermer la vue topologique.
Barres d'outils topologiques	Permet d'afficher ou de masquer la barre d'objets.

20.2.2.3. Projet

Modifiez votre mot de passe	Permet de modifier le mot de passe protégeant le projet en cours.
Options	Permet de définir les options du projet en cours

20.2.2.4. Tâches administratives

Configuration	Permet d'ouvrir l'écran de sauvegarde ou de restauration de configuration.
Mettre à jour le firmware…	Permet d'ouvrir l'écran de mise à jour de firewalls
Mettre à jour la licence…	Permet d'ouvrir l'écran de mise à jour des licences
Sauvegarder la partition…	Permet d'ouvrir l'écran de sauvegarde de la partition système.
Scripts…	Ce menu permet l'exécution de scripts NETASQ sur les boîtiers UTM ciblés.
Déploiement	Permet d'ouvrir le menu relatif à la définition des options de déploiement des politiques de sécurité et/ou des bases d'objets.

20.2.2.5. Options

Préférences…	Permet de définir les options de l'Administration Globale NETASQ.

20.2.2.6. Fenêtres

Disposition horizontale	Permet d'organiser la disposition des fenêtres du projet en cours avec une disposition horizontale.
Disposition verticale	Permet d'organiser la disposition des fenêtres du projet en cours avec une disposition verticale.
Arranger	Permet d'arranger les fenêtres du projet en cours.
Cascade	Permet d'afficher les fenêtres du projet en cours en cascade.

20.2.2.7. Aide

Aide	Permet d'afficher le fichier d'aide en ligne.
Mise à jour de NETASQ UNIFIED MANAGER	Permet d'afficher des informations sur les versions installées.
A propos…	Permet d'afficher une fenêtre indiquant les informations relatives à l'Administration globale NETASQ.

20.2.3. Projet

Plusieurs options propres à chaque projet sont disponibles. Pour accéder à la configuration de ces options, sélectionnez le menu **`Projet\Options`**.

20.2.3.1. Monitoring des clients

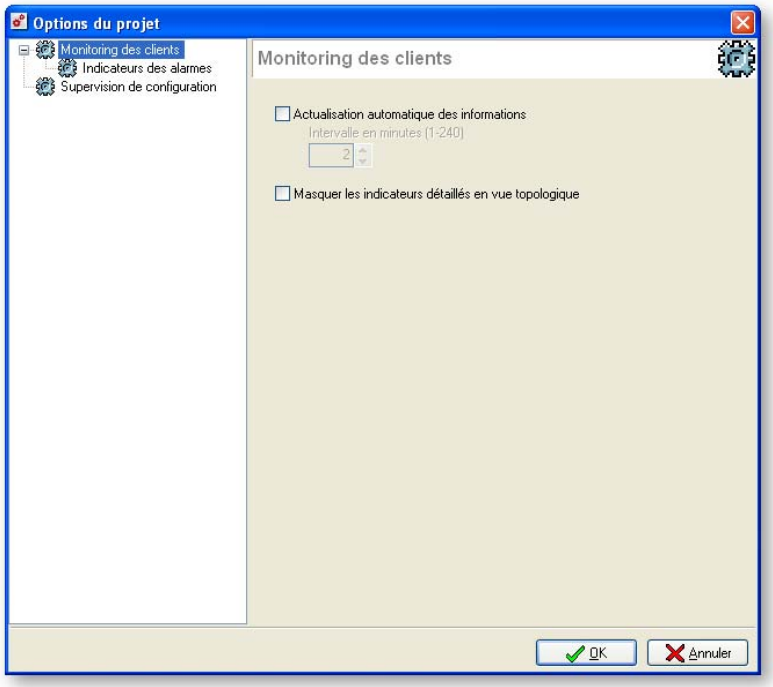


Figure 460 : Options du projet - Monitoring des clients

Si la case **Actualisation automatique des informations** n'est pas cochée, aucun rafraîchissement automatique des données (version, attributs…) et des alarmes (systèmes et sécurité) ne sera effectué. Si la case est cochée, indiquez la valeur en minutes du délai entre chaque rafraîchissement.

Il est possible également de masquer les indicateurs détaillés (Niveaux de problèmes système, Niveau de problèmes de sécurité, Etat des alarmes) lorsque vous vous trouvez en vue topologique.

Indicateurs des alarmes

L'écran "Indicateurs des alarmes" vous permet de définir l'affichage du statut des alarmes dans la vue topologique. Les différentes options vous permettent de visualiser le cumul des statuts d'alarmes, les statuts d'alarmes en temps réel ou les deux.

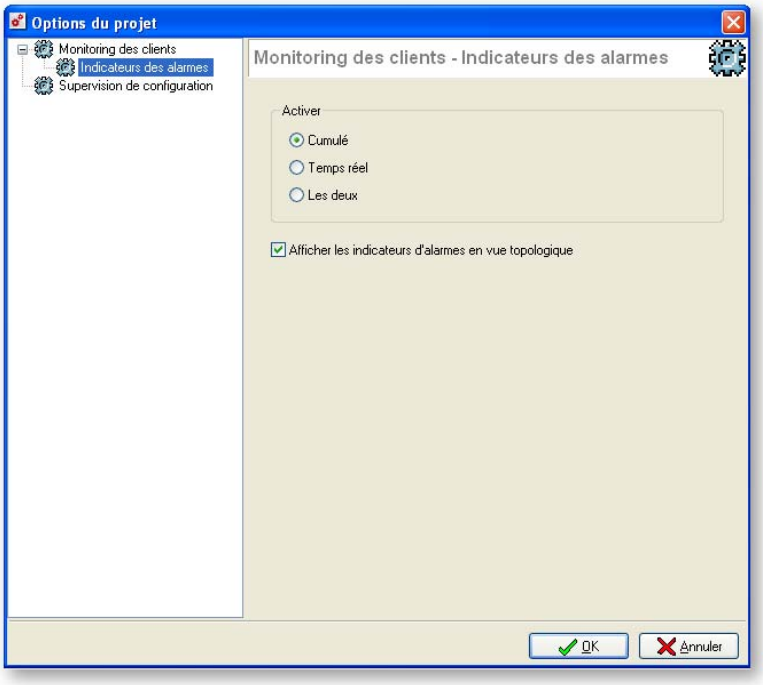


Figure 461 : Options du projet - Indicateurs des alarmes

20.2.3.2. Supervision de la configuration

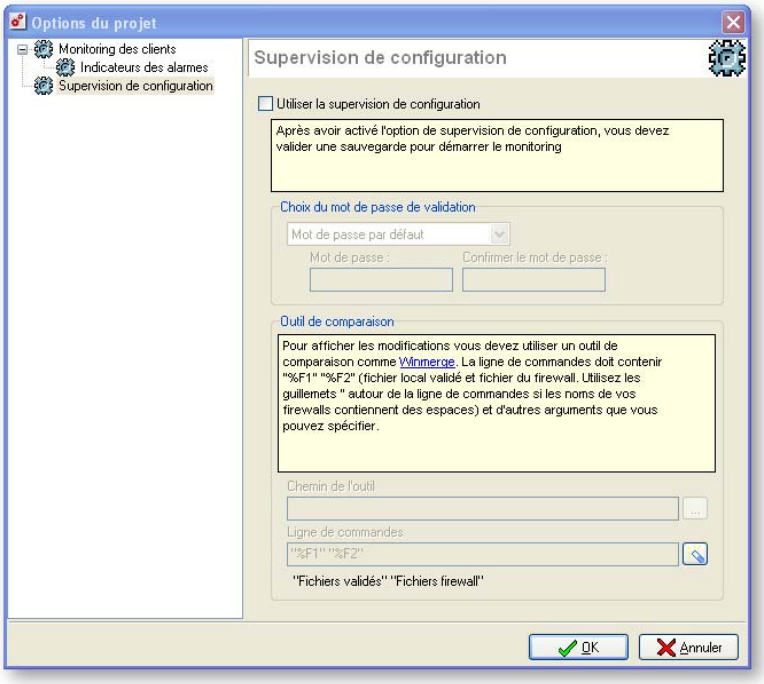


Figure 462 : Options du projet - Supervision de configuration

Le menu **`Supervision de la configuration`** permet l'activation du contrôle des modifications effectuées dans la configuration des Appliances gérés par l'Administration Globale (Fonctionnalités disponibles uniquement pour les boîtiers UTM NETASQ à partir de la version 6.3).

Activer la	Option d'activation du monitoring des configurations. Cette fonctionnalité nécessite

supervision de configuration	la sauvegarde et la validation des configurations des boîtiers UTM surveillés pour débuter le monitoring.
Choix du mot de passe de validation	Par défaut la validation d'une configuration ne nécessite pas de mot de passe. Pourtant il est possible dans définir un : soit unique et identique à tous les Appliances managés, soit spécifique pour chacun d'entre eux. Cette option permet de définir le mode de gestion des mots de passe de validation : • **Mot de passe par défaut** : mode de gestion par défaut. • **Un seul mot de passe pour tous** : un mot de passe unique doit être spécifié. Il est identique pour tous les appliances gérés. Dans ce cas, indiquez un mot de passe et confirmez-le. • **Un mot de passe par firewall** : le mot de passe de validation est défini différemment pour chaque Appliance.
Outil de comparaison	Pour visualiser les modifications apportées aux configurations monitorées, vous spécifiez un outil de comparaison externe au logiciel d'Administration globale (tel que **Winmerge**). Pour définir cet outil, spécifiez dans un premier temps l'application de comparaison de fichier en indiquant le chemin de l'outil. Puis sélectionnez les lignes de commandes qui seront utilisés au lancement de l'application. Par défaut on retrouve deux arguments : "%F1" et "%F2", qui représentent respectivement les fichiers locaux de configuration "validés" et les fichiers du firewall. **REMARQUE** Les guillemets doivent être utilisés dans la ligne de commandes si les noms de vos firewalls contiennent des espaces ou d'autres arguments que vous pouvez spécifier.

20.2.4. Options

Ce menu est expliqué dans la Partie 19 : Actions diverses. Cependant, en mode Global Administration, certaines fenêtres diffèrent.

20.2.4.1 Comportement

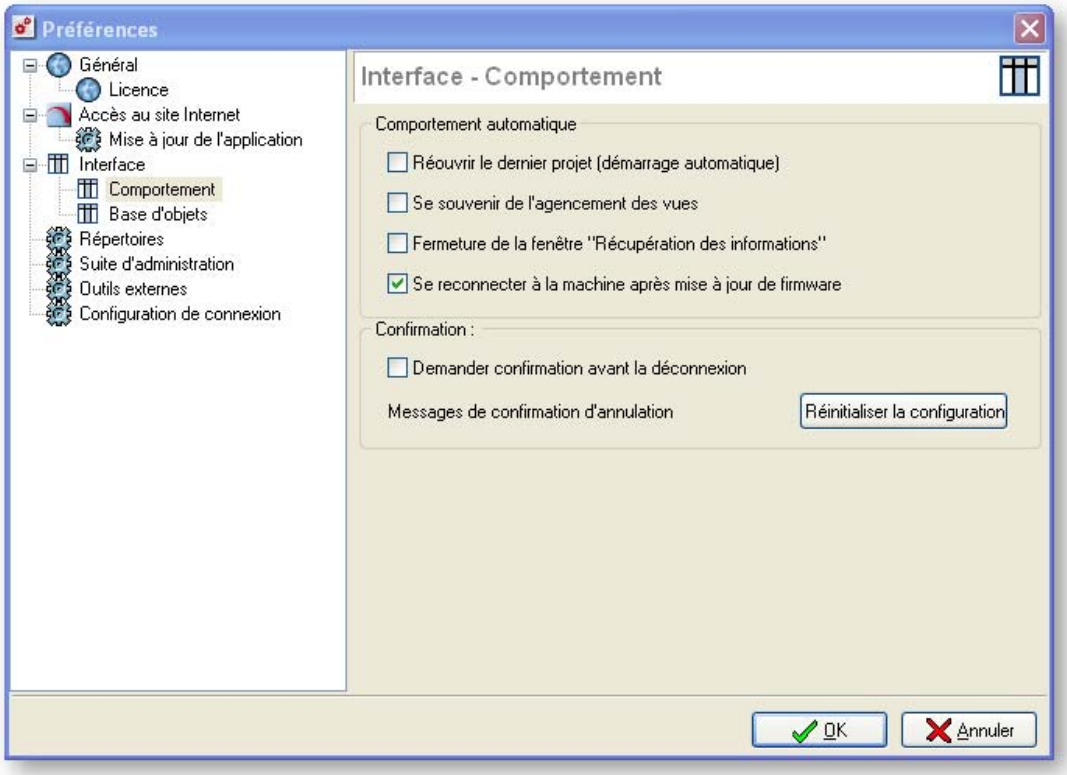


Figure 463 : Interface - Comportement

Rouvrir le dernier projet (démarrage automatique)	Lorsque cette case est cochée, le dernier projet édité est ouvert automatiquement lors du lancement de l'application d'Administration Globale NETASQ.
Se souvenir de l'agencement des vues	Lorsque cette case est cochée, le projet s'ouvre avec la même disposition des fenêtres que lors de la précédente utilisation.
Fermeture de la fenêtre "Récupération des informations"	Permet la fermeture automatique de cette fenêtre.
Se reconnecter à la machine après mise à jour de firmware	Permet la réouverture automatique du produit une fois la mise à jour effectuée.
Demander confirmation avant la déconnexion	Permet d'affiche un message de confirmation avant de se déconnecter du firewall.
Réinitialiser la configuration	Permet de revenir à la configuration par défaut.

20.2.4.2. Répertoires

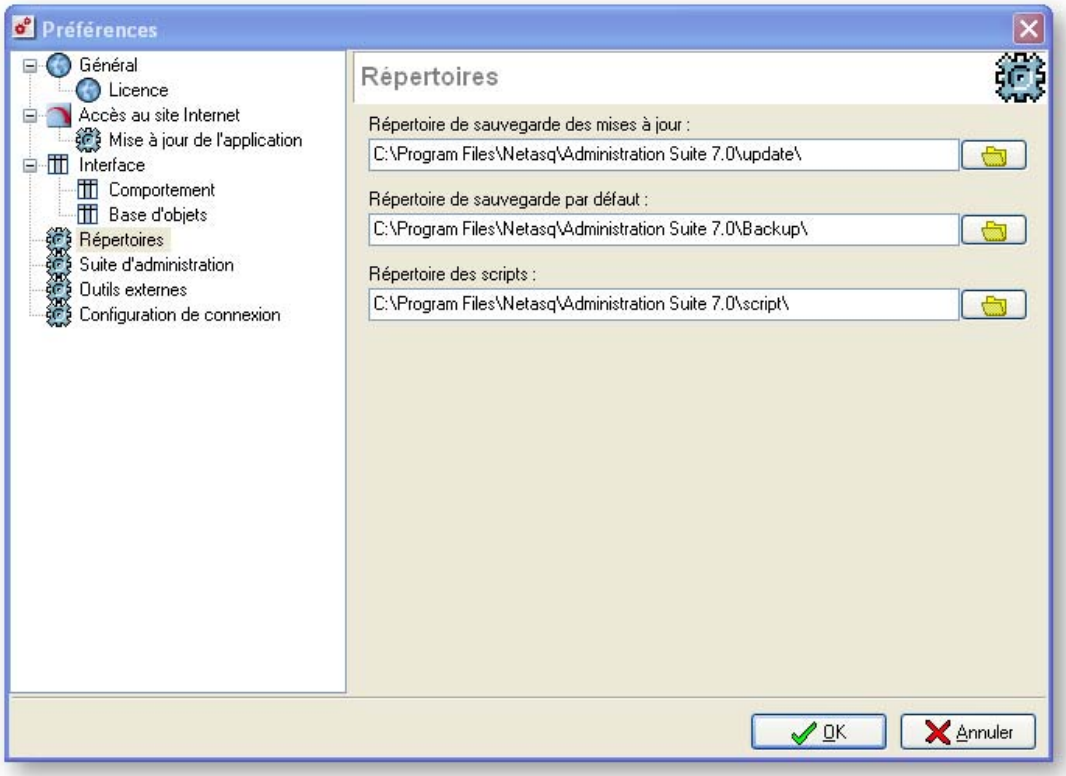


Figure 464 : Préférences - Répertoires

Répertoire de stockage des mises à jour	Indiquez dans ce champ le répertoire dans lequel seront stockées les mises à jour. En effet, lorsque l'Administration Globale NETASQ récupère une mise à jour de firmware sur le site Web de NETASQ, le fichier est stocké dans ce répertoire avant d'être distribué et installé sur les boîtiers UTM. Par défaut ce répertoire est le suivant : `%Répertoire d'installation de l'Administration Suite 7.0\Update\`
Répertoire de sauvegarde par défaut	Indiquez dans ce champ le répertoire dans lequel seront stockées les sauvegardes de configuration. En effet, lorsque l'Administration Globale NETASQ effectue une sauvegarde de la configuration d'un firewall celle-ci est stockée dans ce répertoire. Par défaut ce répertoire est le suivant : `%Répertoire d'installation de l'Administration Suite 7.0\Backup\`
Répertoire des scripts	Indiquez dans ce champ le répertoire dans lequel seront stockés les scripts. Par défaut ce répertoire est le suivant : `%Répertoire d'installation de l'Administration Suite 7.0\script\`

20.2.4.3. Outils externes

Cet onglet permet de configurer les outils externes (max. 12), tels que SSH ou Telnet, qui peuvent être lancés pour un Appliance (ou pour tout autre équipement pour lequel les champs "adresse IP", "login" et "mot de passe" ont été renseignés dans la fiche d'informations).

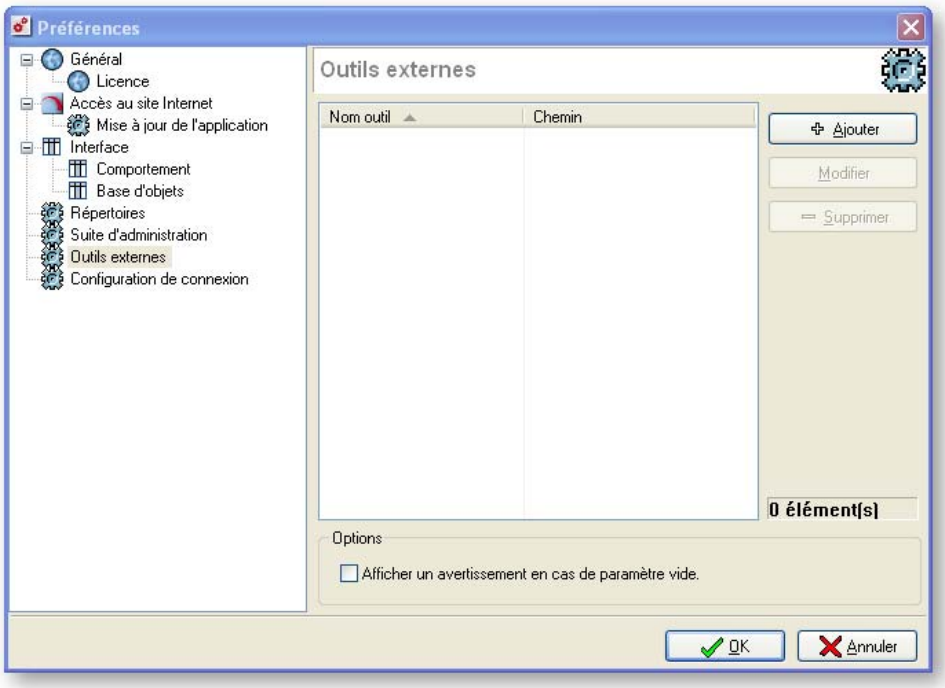


Figure 465 : Préférences - Outils externes

Pour ajouter un outil externe, cliquez sur le bouton **Ajouter**.

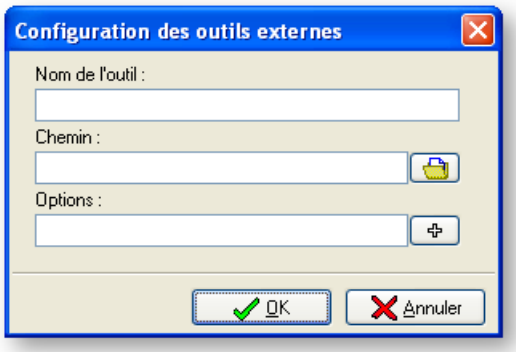


Figure 466 : Configuration des outils externes

Dans la fenêtre qui s'affiche, indiquez les informations qui suivent :

Nom de l'outil	Indiquez le nom choisi pour désigner l'outil.
Chemin	En cliquant sur le bouton associé, choisissez le fichier exécutable de l'outil externe.
Options	Dans ce champ, vous pouvez spécifier une chaîne d'options qui sera passée en paramètre de ligne de commande lors du lancement de l'outil externe. Dans cette chaîne, il est possible d'insérer dynamiquement, lors du lancement de l'outil, des informations

présentes dans la fiche de l'objet et qui sont propres à cet objet

Exemple
Login de connexion, adresse IP, mot de passe, email …). Pour ajouter une information dynamique dans la chaîne d'options, cliquez sur le bouton associé et choisissez l'information dans la liste qui s'affiche.

Cliquez ensuite sur **OK**.

Vous pouvez ajouter autant d'outils que vous le désirez. Pour retrouver facilement un outil dans la liste, vous pouvez la trier en cliquant sur le titre de la colonne " Nom Outil" ou filtrer les noms d'outils en cliquant sur la petite flèche noire dans le titre de la colonne "Nom Outil".

Pour supprimer un outil externe de la liste, sélectionnez celui-ci et cliquez sur le bouton **Supprimer**. Pour modifier la configuration du lancement d'un outil externe, sélectionnez celui-ci et cliquez sur le bouton **Modifier**.

En bas de la fenêtre, la case à cocher **Afficher un avertissement en cas de paramètre vide** permet, lorsqu'elle est cochée, d'avertir l'administrateur de l'Administration Globale NETASQ qu'un des champs qui doit être passé dans la chaîne d'options est vide (le champ n'est pas rempli dans la fiche d'informations de l'objet). Cet avertissement est donné au lancement de l'outil.

Exemple

Utilisation du logiciel **PUTTY** pour se connecter en ligne de commande SSH sur un Appliance.

Dans la fenêtre de création d'un outil, indiquez les informations suivantes :
Nom : SSH
Chemin : <chemin vers l'exécutable putty.exe>
Options : -ssh -2 -pw $PASSWORD$ $LOGIN$@$ADRESSE$

Ainsi lorsque l'outil sera lancé, il se connectera directement au boîtier désiré et vous n'aurez pas besoin de saisir ni login, ni mot de passe.

CHAPITRE 3 : UTILISATION DE L'ADMINISTRATION GLOBALE

20.3.1. Généralités

20.3.1.1. Présentation

L'Administration Globale NETASQ fonctionne en mode projet. Les projets correspondent à des configurations d'administration de réseaux ou de sous réseaux. Tous les projets sont protégés par mot de passe.

20.3.1.2. Création de projet

Un projet peut être créé en utilisant le menu **Fichier\Nouveau Projet** ou en utilisant le raccourci correspondant dans la barre de raccourcis.

20.3.1.3. Ouverture et fermeture de projet

L'ouverture d'un projet peut être réalisée au lancement de l'Administration Globale NETASQ (Cf. Partie 20/Chapitre 1 : Création/Ouverture d'un projet) ou grâce au menu **Fichier\Ouvrir**. Une fenêtre s'affiche vous invitant à choisir le fichier de projet à ouvrir. Les fichiers projet portent l'extension .**gap**. L'ouverture d'un fichier peut aussi être réalisée en cliquant sur le raccourci correspondant dans la barre de raccourcis. Un seul projet à la fois peut être ouvert. Si vous ouvrez un projet alors qu'un autre projet est déjà en cours d'utilisation, ce dernier sera automatiquement fermé. A l'ouverture d'un projet, le mot de passe protégeant celui-ci doit être indiqué.

Figure 467 : Mot de passe

- La fermeture d'un projet est réalisée soit lorsque vous quittez l'application au moyen du menu **Fichier\Quitter** soit lorsque vous ouvrez un autre projet.

20.3.1.4. Enregistrement de projet

Un projet peut être enregistré soit en utilisant le menu **Fichier\Enregistrer**, soit en utilisant le raccourci correspondant dans la barre de raccourcis, soit en utilisant le raccourci clavier **CTRL+S**. Toutes les modifications seront alors enregistrées dans le projet en cours.

Il est aussi possible d'enregistrer un projet sous un autre nom ou dans un autre emplacement. Pour cela, il est possible d'utiliser le menu **Fichier\Enregistrer sous…**ou le raccourci correspondant dans la barre de raccourcis.

Lorsqu'un projet est sauvegardé pour la première fois ou lorsque l'opération **Enregistrer sous…** est réalisée, une fenêtre demande de renseigner et de confirmer un mot de passe pour protéger le projet.

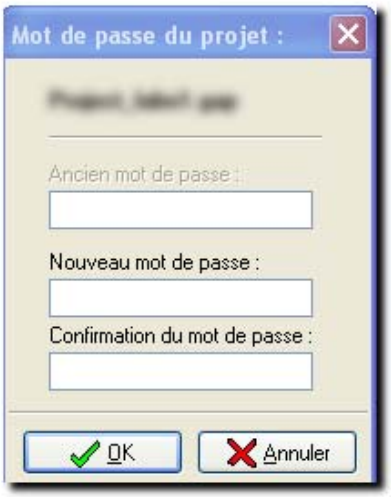


Figure 468 : Mot de passe du projet

20.3.1.5. Importation d'équipements UTM NETASQ dans un projet

Il est possible d'importer une base d'objets firewall dans un projet. Pour cela, il faut utiliser le menu **Fichier\Importation de fichier firewall…**. Une fenêtre s'affiche vous invitant à choisir un fichier d'objets firewalls. Ce fichier doit être au format **csv**.

Ce fichier peut contenir les informations suivantes :

- Nom du firewall.
- Adresse IP du firewall.
- Nom du compte d'administration.
- Mot de passe du compte d'administration.

> **AVERTISSEMENT**
> Par mesure de sécurité il est très largement recommandé de ne pas renseigner ce champ).

- Description du firewall (texte d'explication).
- Nom du contact du firewall.
- Prénom du contact du firewall.
- Entreprise du contact du firewall.
- Ville où est installé le firewall.
- Adresse où est installé le firewall.

- Code postal de la ville où est installé le firewall.
- Pays où est installé le firewall.

Chaque ligne du fichier doit correspondre à un firewall. Les informations doivent être séparées soit par des virgules, soit par des points-virgules, soit par un caractère de votre choix.

AVERTISSEMENT

Ce caractère ne doit pas être un caractère usuel afin qu'il ne risque pas d'être utilisé dans les champs d'information). Aucun champ n'est obligatoire donc il n'est pas nécessaire de renseigner toutes les informations ci-dessus (il est fortement conseillé de ne pas renseigner le mot de passe dans le fichier CSV, qui est un fichier non chiffré). L'ordre des champs dans le fichier n'a pas d'importance.

Exemple

FW_1,10.0.0.1,admin,FRANCE,jean.dupont@netasq.com
FW_2,10.0.0.2,admin,ITALIE
FW_3,10.0.0.3,BELGIQUE

Dans cet exemple, la première information correspond au champ Nom du firewall, la deuxième à l'adresse IP du firewall, la troisième au nom du compte d'administration, la quatrième à le pays où est installé le firewall et enfin la dernière à l'adresse mail du contact.

REMARQUES

1) Un champ peut être vide pour certains boîtiers UTM alors qu'il est renseigné pour les autres (cas FW_3), il faut alors dans ce cas laisser les caractères de séparation.
2) N'indiquez dans le fichier que les champs que vous désirez renseigner.

Une fois le fichier choisi, l'écran suivant s'affiche :

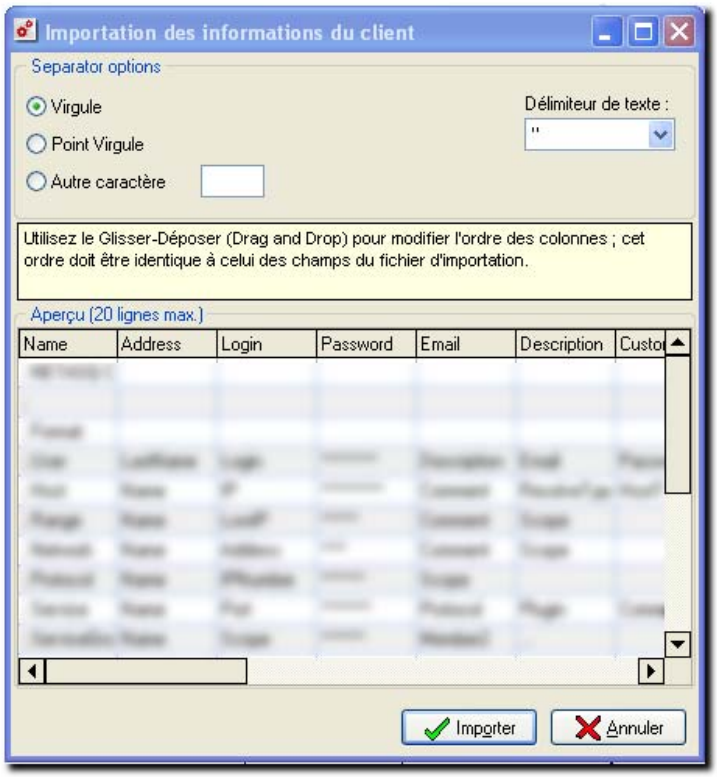


Figure 469 : Importation des informations du client

Vous allez alors pouvoir définir les règles d'importation des informations. Tout d'abord, vous devez spécifier le type de séparateur entre les informations (virgule, point-virgule ou caractère particulier qu'il faut préciser) et le type de délimiteur pour les zones de texte.

Vous pouvez alors déplacer les colonnes de la zone de prévisualisation grâce à un mécanisme de "glisser déposer" (drag&drop) afin que les informations du fichier correspondent avec la disposition des colonnes de la prévisualisation. Cette disposition sera alors appliquée au fichier lors de l'import des informations.

Dans notre exemple précédent, il faut choisir le séparateur **virgule** et indiquer la chaîne suivante dans la zone de saisie **Disposition des champs** :

Name,Address,Login,Country,Email

Dans la zone "Aperçu", le contenu du fichier est alors affiché. Si une information présente dans le fichier n'apparaît pas, vérifiez que les champs du fichier sont bien séparés par le bon séparateur.

L'importation d'un fichier permet d'ajouter les informations du fichier dans la vue globale. Toutes les informations de firewalls déjà contenues dans la vue globale sont conservées après importation.

20.3.1.6. Exportation de firewalls dans un projet

Il est aussi possible d'exporter tous les appliances de la vue générale ou une sélection de ceux-ci vers un fichier .CSV ou .TXT.

Ce fichier pourra contenir les informations suivantes pour chaque Appliance :

- Nom du firewall.
- Adresse IP du firewall.
- Nom du compte d'administration.
- Mot de passe du compte d'administration.

> **AVERTISSEMENT**
> Par mesure de sécurité il est très largement recommandé de ne pas exporter ce champ car les mots de passe sont affichés en clair).

- Email du compte d'administration
- Description du firewall (texte d'explication).
- Custom1
- Custom2
- Custom3
- Zip Code
- Ville où est installé le firewall.
- Pays où est installé le firewall.
- Entreprise du contact du firewall.
- Nom du contact du firewall.
- Prénom du contact du firewall.
- Code postal de la ville où est installé le firewall
- SuperviseGenerationPassword
- SuperviseFirewallValidBackup
- Monitoring On

➲ Pour exporter les informations des appliances vers un fichier, sélectionnez le menu **`Fichier\Exportation de fichier firewall…`**La fenêtre suivante s'affiche :

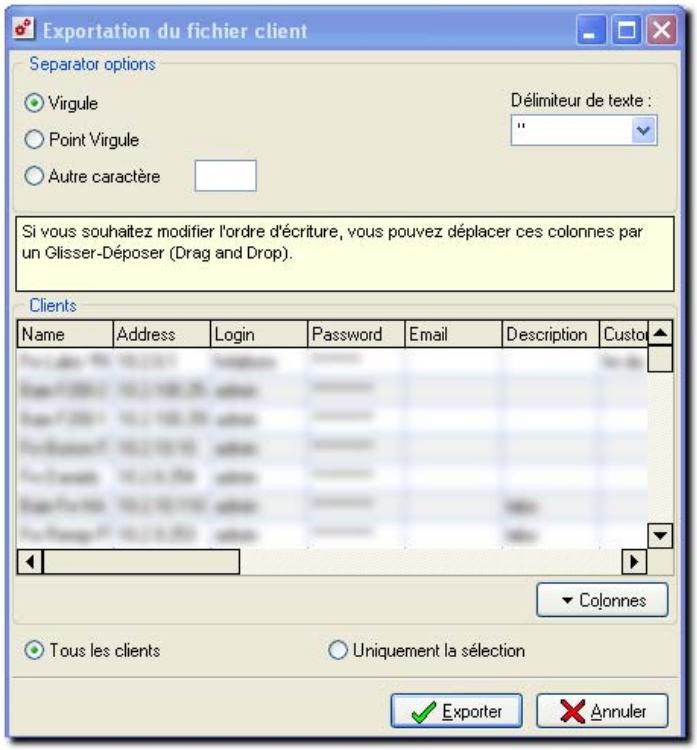


Figure 470 : Exportation du fichier client

Choisissez tout d'abord le type de séparateur qui sera utilisé entre chaque champ du fichier. Indiquez aussi le délimiteur de texte.
Choisissez ensuite les colonnes que vous souhaitez exporter. Pour cela, cliquez sur le bouton **Colonnes** puis **Personnaliser**.

Une fenêtre similaire à la fenêtre suivante s'affiche :

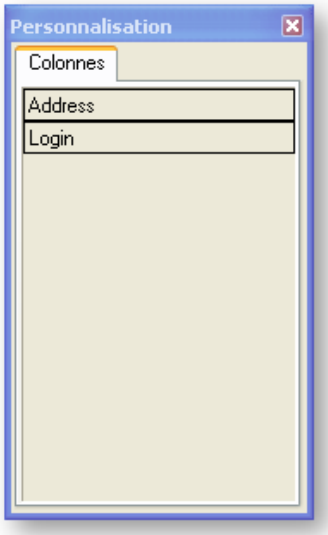


Figure 471 : Personnalisation - Colonnes

Dans cette fenêtre, on trouve le nom des colonnes qui ne sont pas affichées mais qu'il est possible de rendre visibles. Pour afficher une colonne, sélectionnez avec le bouton gauche de la souris le nom de cette colonne et maintenez le bouton de la souris enfoncé. Ensuite, déplacez l'intitulé de la colonne jusqu'à l'endroit où vous désirez l'insérer dans la prévisualisation puis relâchez le bouton de la souris.

Pour masquer une colonne, faîtes l'opération inverse : sélectionnez dans la barre des titres de colonne, le nom de la colonne qu'il faut masquer, avec le bouton gauche de la souris. Maintenez le bouton gauche appuyé et déplacez le nom de la colonne jusqu'à la fenêtre "Personnalisation" puis relâchez le bouton.

La disposition des colonnes affichées peut être modifiée en utilisant le même mécanisme de "drag and drop". Il suffit de sélectionner une colonne et de la déplacer à l'endroit voulu.

Pour revenir à la disposition d'origine des colonnes, cliquez sur le bouton **Colonnes** puis **Réinitialiser**.

Enfin, si vous souhaitez exporter tous les appliances du projet, cochez la case **Tous les clients**. Si vous souhaitez n'exporter que la sélection qui a précédemment été réalisée, cochez la case **Uniquement la sélection**.

Cliquez sur le bouton **Exporter,** choisissez le nom et l'emplacement du fichier. Les informations seront alors insérées dans le fichier sous un format particulier : une ligne par Appliance et chaque champ délimité par le séparateur choisi précédemment.

20.3.1.7. Modification de mot de passe projet

Il est possible de modifier le mot de passe protégeant le projet en cours.

Sélectionnez le menu **`Projet\Modifiez votre mot de passe`**. La fenêtre suivante s'affiche :

Figure 472 : Mot de passe du projet

Saisissez l'ancien mot de passe du projet puis saisissez et confirmez le nouveau mot de passe.

20.3.2. Gestion des firewalls par la vue générale

20.3.2.1. Vue générale

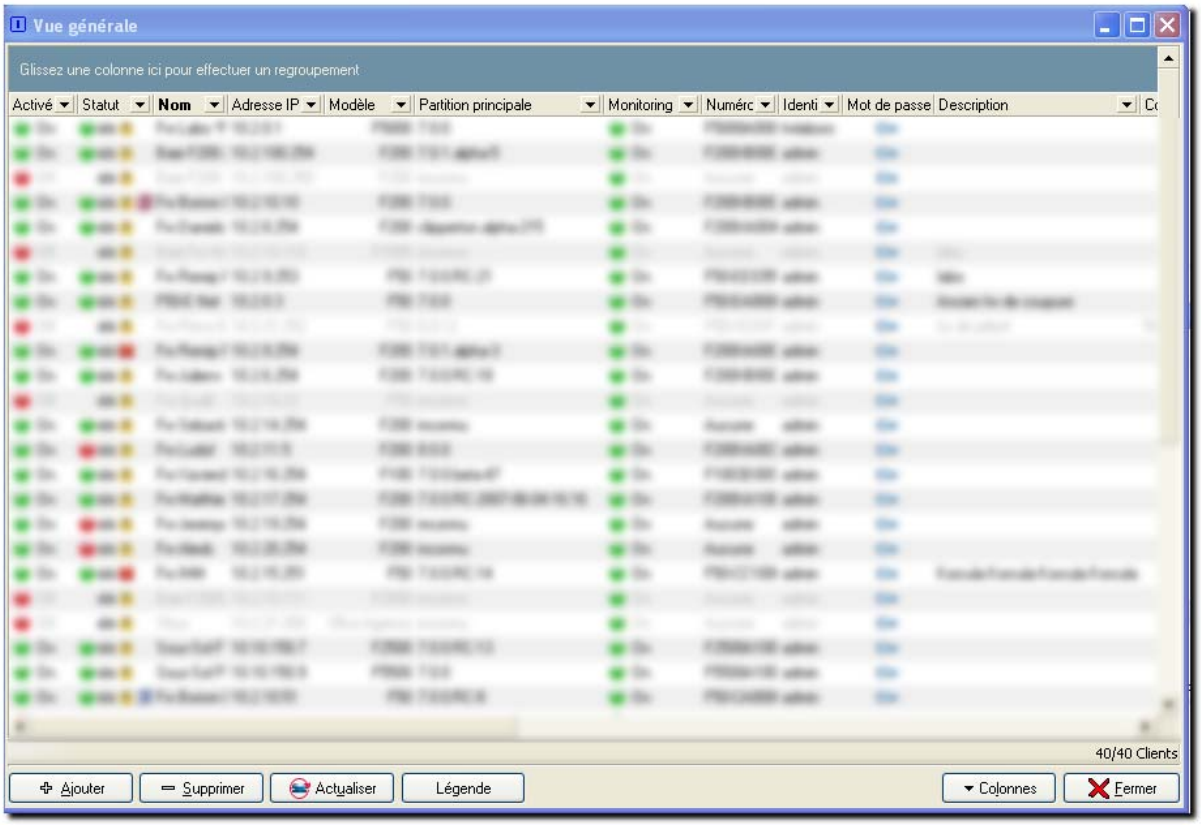


Figure 473 : Vue générale

La première vue qui apparaît lorsque vous ouvrez un nouveau projet est la vue générale. Cette vue contient la liste de tous les équipements NETASQ qui ont été ajoutés dans le projet (qu'ils aient été ajoutés à partir de la vue générale ou à partir de la vue topologique).
Cette liste se présente sous la forme d'un tableau affichant des informations concernant chacun des appliances.

En bas de la vue se trouve une barre de boutons d'action :

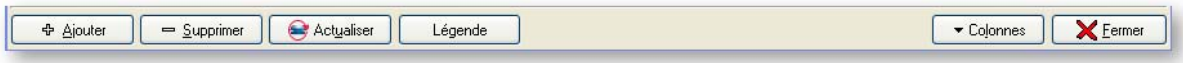


Figure 474 : Boutons d'action

Ajouter	Permet d'ajouter un Appliance dans le tableau.
Supprimer	Permet de supprimer un Appliance dans le tableau.
Actualiser	Permet de rafraîchir manuellement les informations concernant les appliances.
Légende	Permet d'afficher une fenêtre d'informations au sujet de la dernière connexion, la HA, le suivi de configuration, la connexion.
Colonnes	Permet d'afficher ou de masquer certaines colonnes du tableau.
Fermer	Permet de fermer la vue.

20.3.2.2. Gestion des firewalls dans un tableau

Ajouter un Appliance dans le tableau

Pour ajouter un Appliance dans la vue générale, trois moyens peuvent être utilisés :

- En utilisant le bouton d'action **Ajouter** situé en bas de la vue.
- En utilisant la barre d'objets à droite de la vue, si celle-ci est affichée. Si la barre n'est pas affichée, sélectionnez le menu **`Vue\Barre d'outils topologique`** pour afficher celle-ci. Ensuite, pour ajouter un produit UTM NETASQ, il suffit de choisir, dans la catégorie NETASQ, le modèle d'Appliance souhaité puis de cliquer avec le bouton gauche de la souris dans la vue générale. Les objets des autres catégories ne peuvent pas être utilisés dans la vue générale.
- En utilisant le menu contextuel, pour cela, cliquez avec le bouton droit de la souris dans la vue générale. Choisissez l'option "Ajouter".

Dans les trois cas, la fenêtre suivante s'ouvre, vous invitant à renseigner les informations relatives au nouveau firewall :

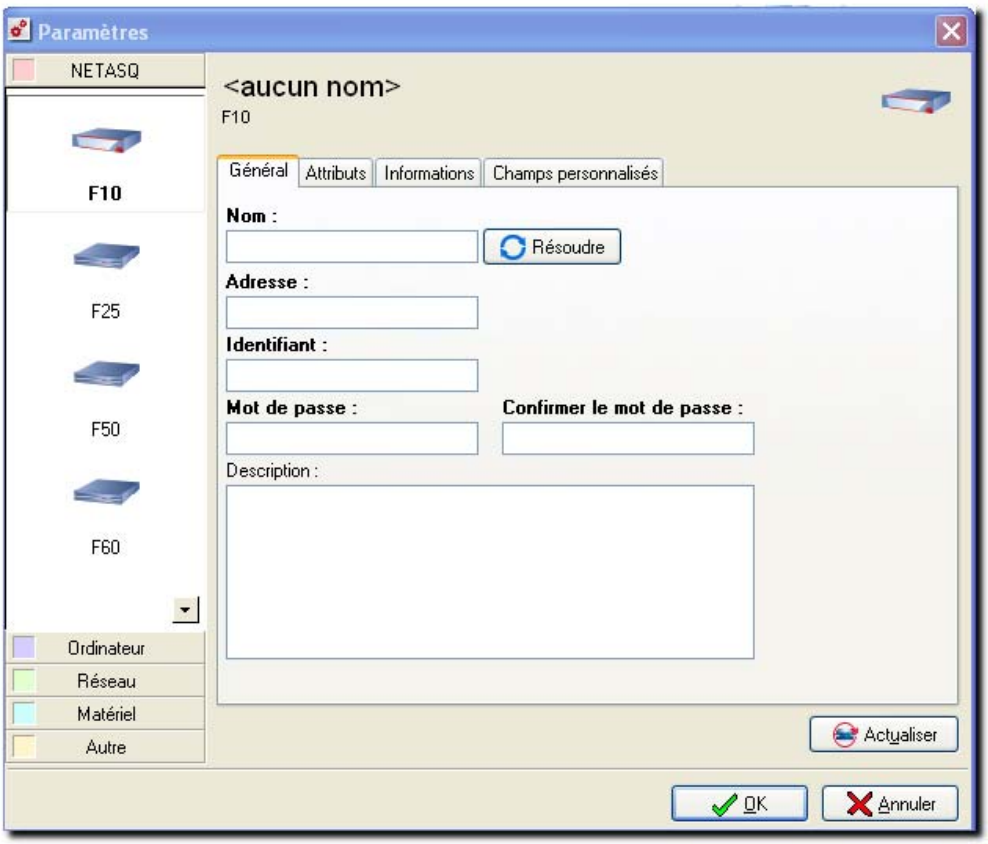


Figure 475 : Paramètres - Général

Onglet "Général"

Les informations demandées dans l'onglet **Général** sont nécessaires pour insérer le firewall dans l'Administration Globale NETASQ.

Nom	Indiquez le nom choisi pour le firewall. Ce nom sera utilisé pour distinguer le firewall des autres équipements. Le bouton **Résoudre** effectue la résolution des adresses IP, des machines de type "manuelle".
Adresse	Indiquez l'adresse IP de l'Appliance que peut contacter la machine sur laquelle est installée l'Administration Globale NETASQ.
Identifiant	Indiquez le login du compte d'administration sur le produit.
Mot de passe	Indiquez le mot de passe du compte d'administration sur le firewall.
Confirmer le mot de passe	Confirmez le mot de passe du compte d'administration.
Description	Indiquez un commentaire libre concernant le firewall.

REMARQUE
Les champs en gras doivent être obligatoirement renseignés.

Onglet "Attributs"

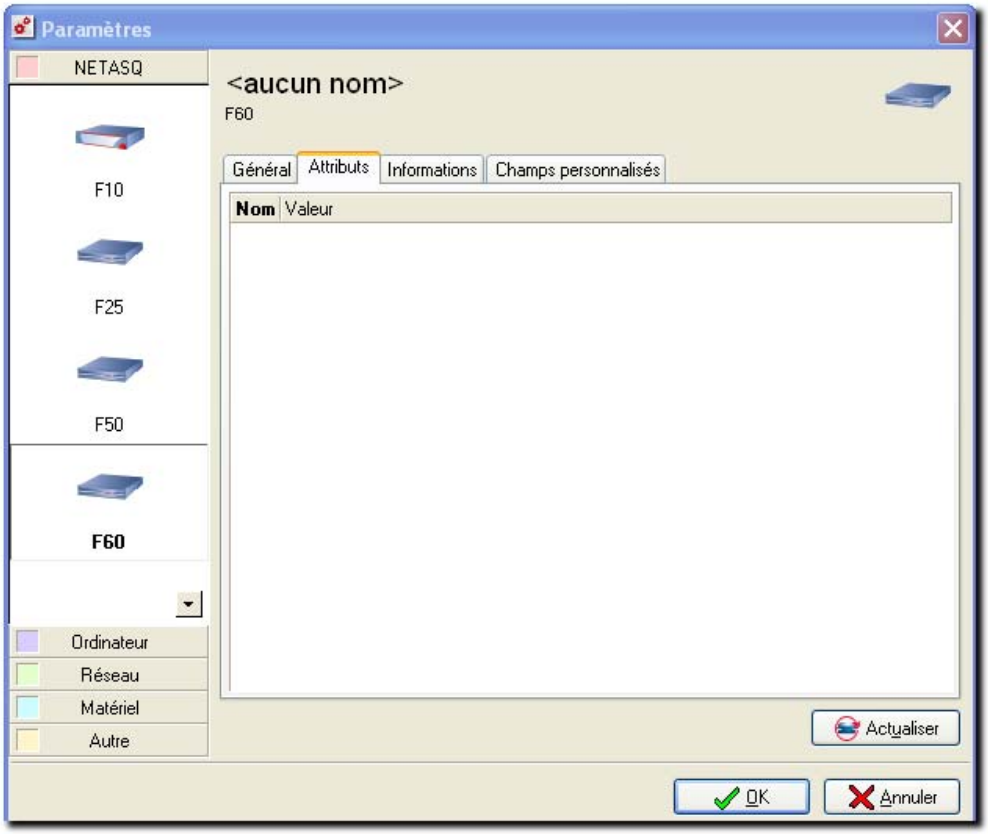


Figure 476 : Paramètres - Attributs

Cette zone n'affiche des données que lorsque les informations pour l'Appliance ont été mises à jour une première fois. Les données affichées alors sont :

Série	Numéro de série du produit UTM NETASQ.
Firmware	Version du firmware du firewall.
OEM	Marque sous laquelle est vendu le produit.
GMTDate	Date du firewall au format GMT.
GMTOffset	Ecart de l'heure locale avec l'heure GMT.
HA	Etat de la haute disponibilité.
Partition Active	Partition active (principale ou backup).
Version de la partition de backup	Version de la partition qui n'est pas active
LastSaveToOtherPartition	Dernière sauvegarde de la partition active vers l'autre partition.
Options du Global Admin	Option de la licence permettant au firewall d'être administré en mode "service". Contactez votre revendeur ou le service commercial de NETASQ pour de plus amples renseignements concernant ce mode.

Pour rafraîchir les données de ce tableau, cliquez sur le bouton **Actualiser** en bas de la fenêtre.

Onglet "Informations"

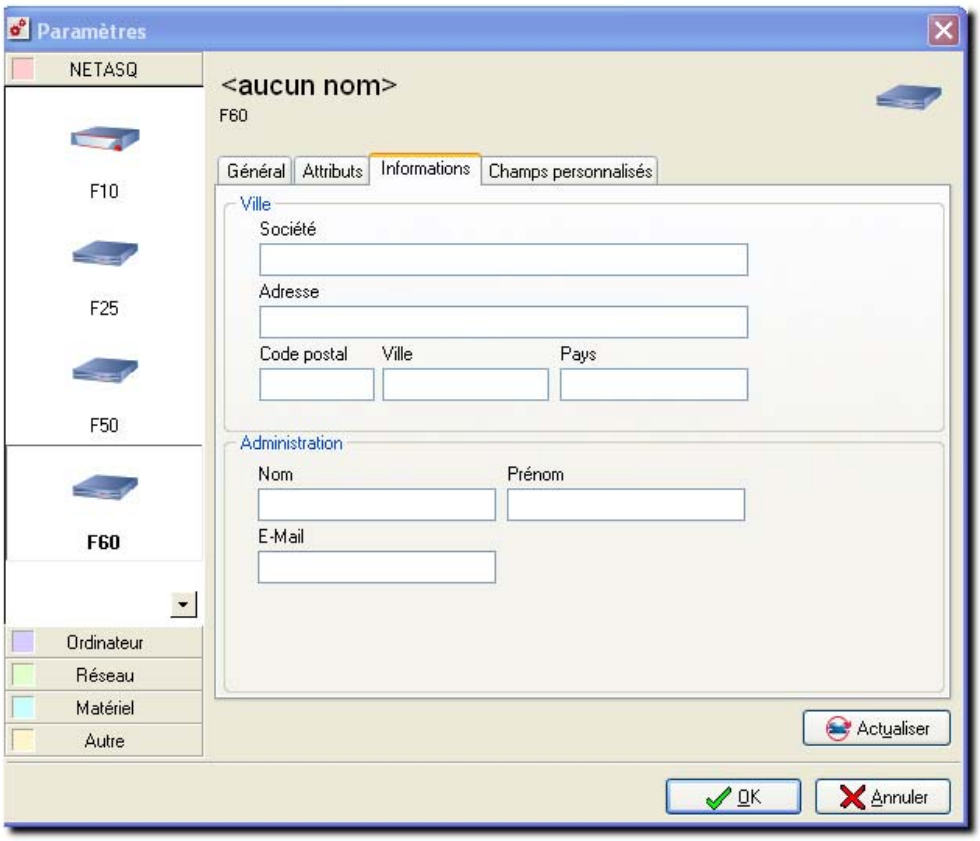


Figure 477 : Paramètres - Informations

Les informations demandées dans cet onglet sont facultatives et servent à identifier l'Appliance.

Société	Indiquez le nom de l'entreprise (ou la filiale, le service…) où est installé l'Appliance.
Adresse	Indiquez l'adresse où est installé l'Appliance.
Code postal	Indiquez le code postal de la ville où est installé l'Appliance.
Pays	Indiquez le pays où est installé l'Appliance.
Ville	Indiquez la ville où est installé le produit UTM.
Nom	Indiquez le nom du contact qui gère localement l'Appliance.
Prénom	Indiquez le prénom du contact.
E-mail	Indiquez l'adresse e-mail du contact.

Onglet "Champs personnalisés"

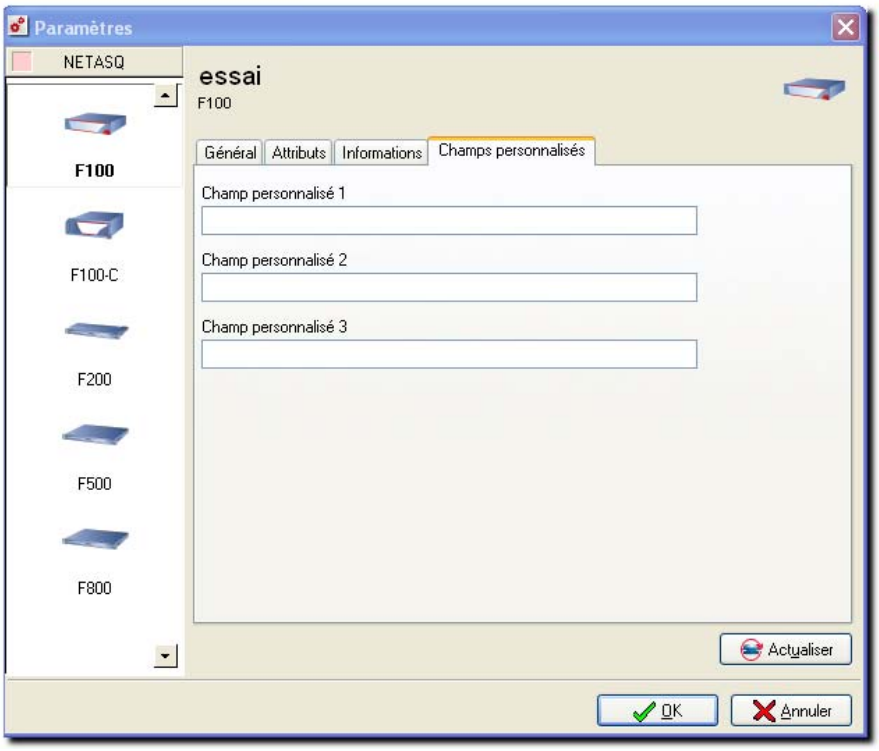


Figure 478 : Paramètres - Champs personnalisés

Cet onglet vous permet de donner des informations supplémentaires au sujet du firewall.

Onglet "Supervision de configuration"

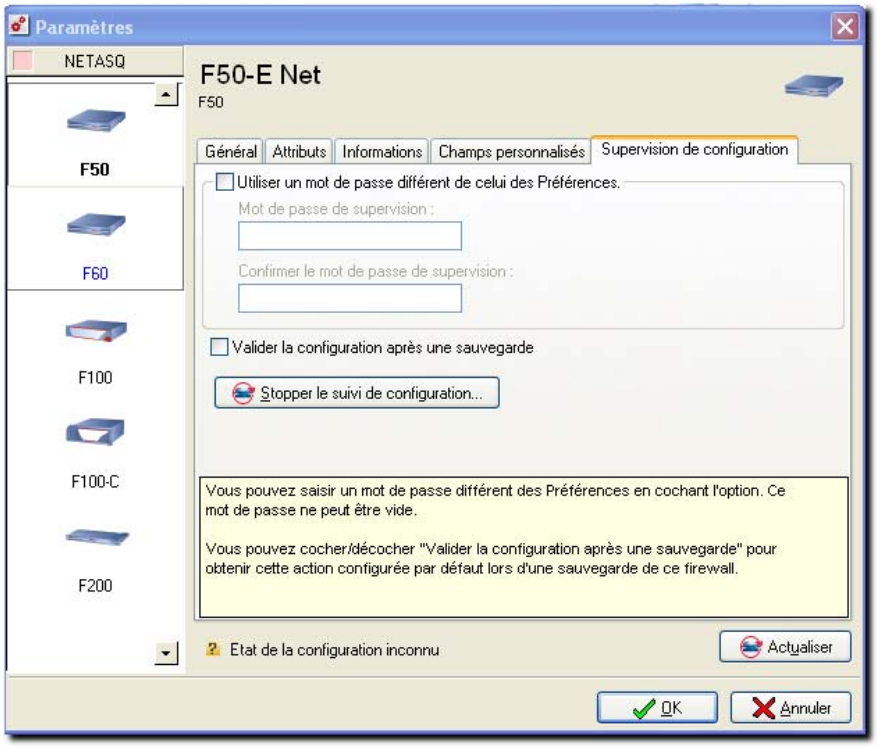


Figure 479 : Paramètres - Supervision de configuration

Cet onglet n'apparaît que si les fonctions de monitoring de la configuration sont activées dans l'Administration Globale (Cf. Partie 20/Chapitre 2 : Projet) et que si l'Appliance supporte cette fonctionnalité (UTM NETASQ en version 6.3 ou plus). Les options de cet onglet permettent de définir le mode monitoring choisi par l'administrateur.

Utiliser un mot de passe différent de celui des préférences	Pour monitorer la configuration de l'Appliance, l'Administration Globale base sa comparaison sur une sauvegarde de configuration "validée". Cette sauvegarde est validée par défaut par le mot de passe. Cette option permet de définir un mot de passe spécifique de monitoring.
Mot de passé de supervision	Champ d'insertion du mot de passe (indispensable si l'option **Utiliser un mot de passe différent de celui des préférences** est cochée).
Confirmer le mot de passe de supervision	Champ de confirmation du mot de passe de monitoring.
Valider la configuration après une sauvegarde	Pour monitorer la configuration du produit, l'Administration Globale base sa comparaison sur une sauvegarde de configuration "validée". Lors de l'étape de sauvegarde, la case à cocher **Valider la configuration après une sauvegarde** est automatiquement cochée. Assurant ainsi que chaque sauvegarde est automatiquement "validée".
Stopper le suivi de configuration	Le bouton **Stopper le suivi de configuration** réinitialise les informations connues sur la configuration du firewall. L'Administration Globale n'indique plus si la configuration a été modifiée, jusqu'à la prochaine "Actualisation".

Il est aussi possible de changer le modèle de firewall choisi, pour cela, il suffit de sélectionner un nouveau modèle dans la barre de gauche de la fenêtre.

Cliquez sur **OK** une fois les informations saisies. Le firewall est alors ajouté dans la liste de la vue générale. Ajoutez alors tous les firewalls que vous désirez gérer dans le projet en cours.

Supprimer un firewall dans le tableau

Pour supprimer un firewall, il faut tout d'abord sélectionner celui-ci dans le tableau puis soit cliquer sur le bouton **Supprimer** , soit appuyer sur la touche **Suppr**, soit cliquer avec le bouton droit de la souris et choisir l'option "Supprimer". L'Appliance est alors retiré de la liste et toutes les informations le concernant sont supprimées.

Désactiver un firewall du tableau

Si un produit UTM NETASQ n'est plus actif (suite à une panne matérielle, une désinstallation…) il est possible de le considérer comme désactivé dans l'Administration Globale NETASQ. Pour cela, cliquez sur le firewall avec le bouton droit de la souris, puis choisissez l'option "Désactiver". Le firewall n'est alors plus géré par l'Administration Globale NETASQ, son état passe à **OFF** et il apparaît grisé dans les différentes vues. Pour réactiver celui-ci, cliquez avec le bouton droit de la souris puis choisissez l'option "Activer".

Multi-Sélection

Il est possible d'effectuer les mêmes actions sur plusieurs firewalls du tableau simultanément. Utilisez les touches **Shift** et **Ctrl** pour sélectionner plusieurs firewalls.

Menu contextuel de la vue générale

Le menu contextuel de la vue générale est obtenu en réalisant un clic droit de la souris dans la vue générale. Les fonctionnalités accessibles par le menu contextuel lorsqu'on sélectionne un objet ou lorsqu'on pointe le vide sont différentes. Toutefois les fonctionnalités accessibles par le menu contextuel lorsqu'on sélectionne un objet intègrent les fonctionnalités accessibles lorsqu'on pointe le vide donc nous n'évoquerons que ce menu.

Le menu contextuel de la vue générale donne accès aux sous menus suivants :

Figure 480 : Menu contextuel

Ajouter	Ajouter un firewall dans la vue générale.
Configurer	Accéder à la configuration d'un firewall. Rappel : un double-clic sur l'objet vous permet aussi d'accéder à la configuration.
Désactiver	Désactiver la prise en compte d'un firewall de la vue générale. Cette option permet notamment de verrouiller le firewall envers toutes les actions possibles dans l'Administration Globale sans retirer le firewall.
Désactiver le monitoring	Il est désormais possible d'activer ou de désactiver le monitoring par firewall. Le monitoring est activé par défaut tant que les limitations de la licence ne sont pas atteintes.
Supprimer	Retirer un firewall de la vue générale.
Firewall Manager	Ouverture de NETASQ UNIFIED MANAGER. Dans ce cas, le mode « Firewall Manager » est affiché avec, au niveau de son arborescence, un menu supplémentaire « Politique globale ».
Outils	Accès aux outils de configuration NETASQ et externes.
Configuration directe	Accès à la configuration directe (cf. *Partie 20/Chapitre 3 : Configuration directe*).
Maintenance	Accès aux actions de maintenance de l'Administration Globale.
Déploiement	Déployer des configurations dans l'Administration Globale.
Scripts…	Ce menu permet l'exécution de scripts NETASQ sur les Appliance ciblés.
Disponibilité (Ping)	Test de disponibilité (tentative de connexion au serverd).
Vérification de l'état	Actualisation manuelle de l'état du firewall.

20.3.2.3. Informations présentées dans le tableau

Le tableau présente un certain nombre d'informations relatives à chaque produit.

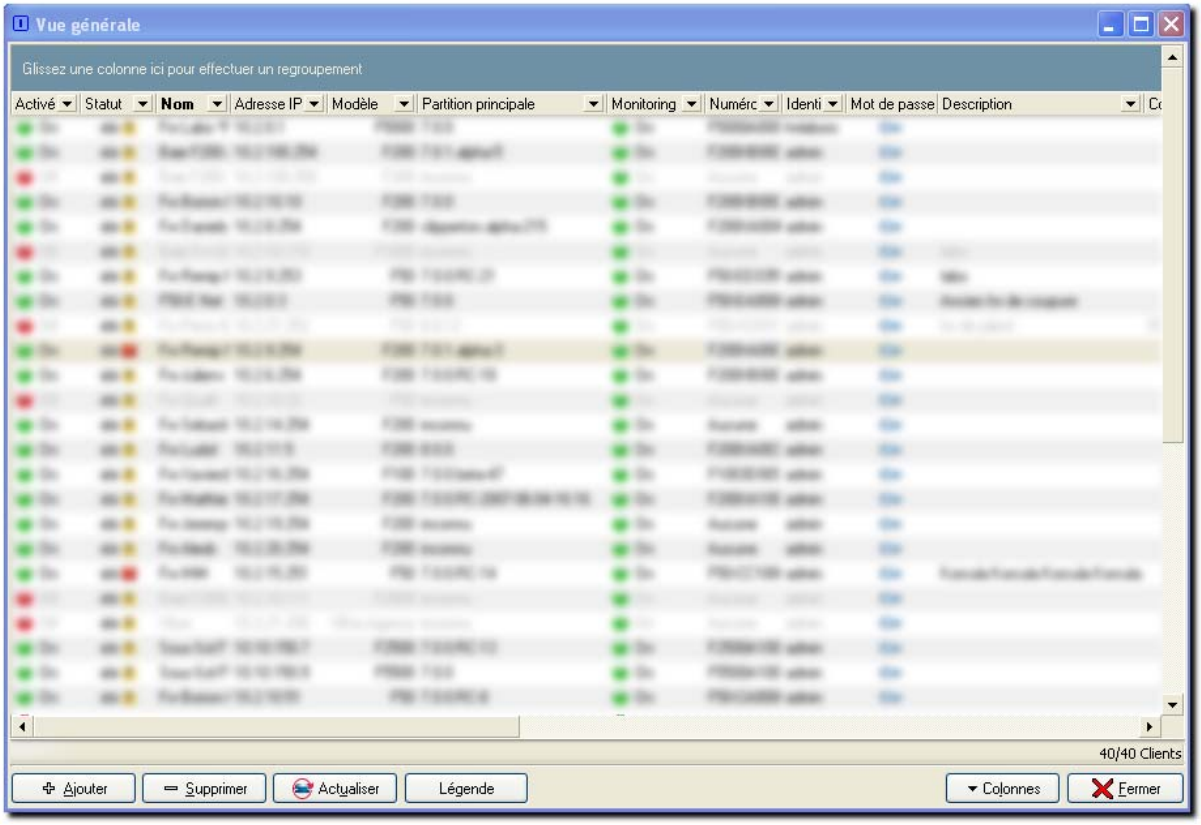


Figure 481 : Vue générale

Les informations présentées sont :

Activé	Ce champ permet de définir si vous voulez ou non que le firewall soit géré par l'Administration Globale NETASQ. Si l'état est sur **ON**, le firewall sera géré par l'Administration Globale NETASQ, si l'état est sur **OFF**, le firewall ne sera plus géré par l'Administration Globale NETASQ (mais les informations seront conservées dans le projet).
Nom	Nom choisi pour le firewall.
Adresse IP	Adresse IP du firewall sur lequel l'Administration Globale NETASQ peut se connecter.
Identifiant	Login du compte d'administration du firewall.
Mot de passe	Mot de passe du compte d'administration du firewall.
Partition	Version logicielle actuelle du firmware du firewall.
Modèle	Modèle du firewall.
Monitoring	L'état de configuration monitoring est visible dans la vue générale.
Description	Commentaire associé au firewall.
Société	Entreprise (ou filiale, ou service…) où est installé le firewall.
Pays	Pays où est installé le firewall.
E-mail de l'Admin	E-mail du contact local gérant le firewall.
Prénom de l'Admin	Prénom du contact gérant le firewall.
Nom de l'Admin	Nom du contact gérant le firewall.
Adresse	Adresse où est installé le firewall.
Code postal	Code postal de la ville où est installé le firewall.
Statut	Etat du firewall. Cette information est actualisée grâce à la fonction "Vérification de l'état".

Numéro de série	N° de série du firewall
Champ personnalisé 1	Premier champ personnalisé contenant des informations supplémentaires.

L'information "Partition" est récupérée directement sur chaque firewall. Toutes les autres informations ont été saisies lors de l'ajout des firewalls. Le champ "Mot de passe" n'apparaît pas en clair pour des raisons évidentes de sécurité.

Pour modifier les informations contenues dans le tableau, il suffit de double-cliquer sur le firewall que vous voulez éditer ou de sélectionner le firewall puis de cliquer avec le bouton droit de la souris et de choisir **`Configurer`**. Vous pourrez alors modifier les informations concernant le firewall dans la fenêtre qui s'ouvre.

20.3.2.4. Modification de l'affichage des informations

Pour des raisons de lisibilité et d'accès plus facile à l'information, il est possible de modifier l'affichage des informations.

Choix des colonnes à afficher

Certaines informations affichées ne vous sont pas forcément nécessaires et inversement, vous voulez peut-être afficher des informations qui vous sont utiles. Il est possible de masquer et d'afficher certaines colonnes du tableau. Pour cela, cliquez sur le bouton **Colonnes\Personnaliser**. Une fenêtre similaire à la fenêtre suivante s'affiche :

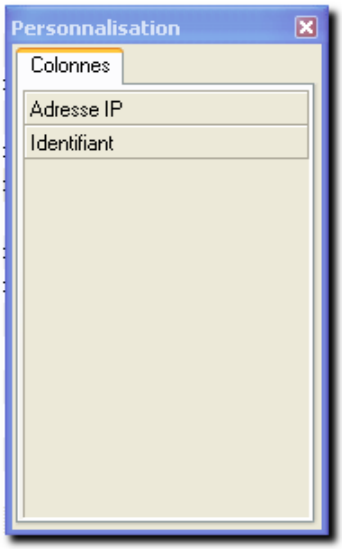


Figure 482 : Personnalisation - Colonnes

Dans cette fenêtre, on trouve le nom des colonnes qui ne sont pas affichées mais qu'il est possible de rendre visibles. Pour afficher une colonne, sélectionnez avec le bouton gauche de la souris le nom de cette colonne et maintenez le bouton de la souris enfoncée. Ensuite, déplacez l'intitulé de la colonne jusqu'à l'endroit où vous désirez l'insérer dans la barre des titres de colonne puis relâchez le bouton de la souris.

Pour masquer une colonne, faîtes l'opération inverse : sélectionnez, dans la barre des titres de colonne, le nom de la colonne qu'il faut masquer, avec le bouton gauche de la souris. Maintenez le bouton gauche appuyé et déplacez le nom de la colonne jusqu'à la fenêtre "Personnalisation" puis relâchez le bouton.

La disposition des colonnes affichées peut être modifiée en utilisant le même mécanisme de "drag and drop". Il suffit de sélectionner une colonne et de la déplacer à l'endroit voulu.

Pour fermer la fenêtre "Personnalisation", cliquez sur la croix blanche en haut à droite de la fenêtre.

Il est possible de rétablir l'affichage initial des colonnes en cliquant sur le bouton "Colonnes\Réinitialiser".

Vue arborescente

Le tableau peut être visualisé sous une forme arborescente, ce qui facilite grandement la lecture des informations. Cette visualisation arborescente est possible en créant des regroupements d'information.

Une zone de "drop" est placée au dessus du tableau, vous pouvez y lire "Glisser une colonne ici pour effectuer un regroupement". Pour regrouper les informations d'une colonne, sélectionnez le titre de la colonne et déplacez-le dans cette zone. Le tableau change alors d'aspect. La colonne ainsi groupée apparaît dans la zone de drop et le tableau affiche les valeurs résultant du groupage sous forme de nœuds. Un signe + apparaît devant les valeurs des groupes permettant de déplier les nœuds et d'afficher les lignes qui ont été regroupées. Il est ainsi possible d'effectuer des regroupements à l'intérieur des groupes sans aucune limite.

> **Exemple**
> Il est possible de faire un regroupement par Partition principale puis par modèle afin de voir l'état des mises à jour sur le parc par type de boîtier.

Tris et filtres sur les informations

Deux outils supplémentaires permettent de gérer l'affichage des informations.

Le tri

Les lignes du tableau peuvent être triées en fonction de la valeur d'une des colonnes, il suffit pour cela de cliquer sur le titre de la colonne pour laquelle vous désirez trier les informations. Un petit triangle gris apparaît alors à côté du titre de la colonne . Le sens du tri dépend du sens du triangle. Pour changer de sens, il suffit de cliquer à nouveau sur le titre de la colonne.

Les filtres

Il est possible de n'afficher que les lignes du tableau pour lesquels certains champs répondent à des critères particuliers. En effet, au niveau de chaque titre de colonne, on trouve le petit symbole suivant : 

En cliquant sur ce symbole, une liste déroulante apparaît. Cette liste comporte toutes les valeurs rencontrées dans la colonne plus deux valeurs "All" et "Custom".

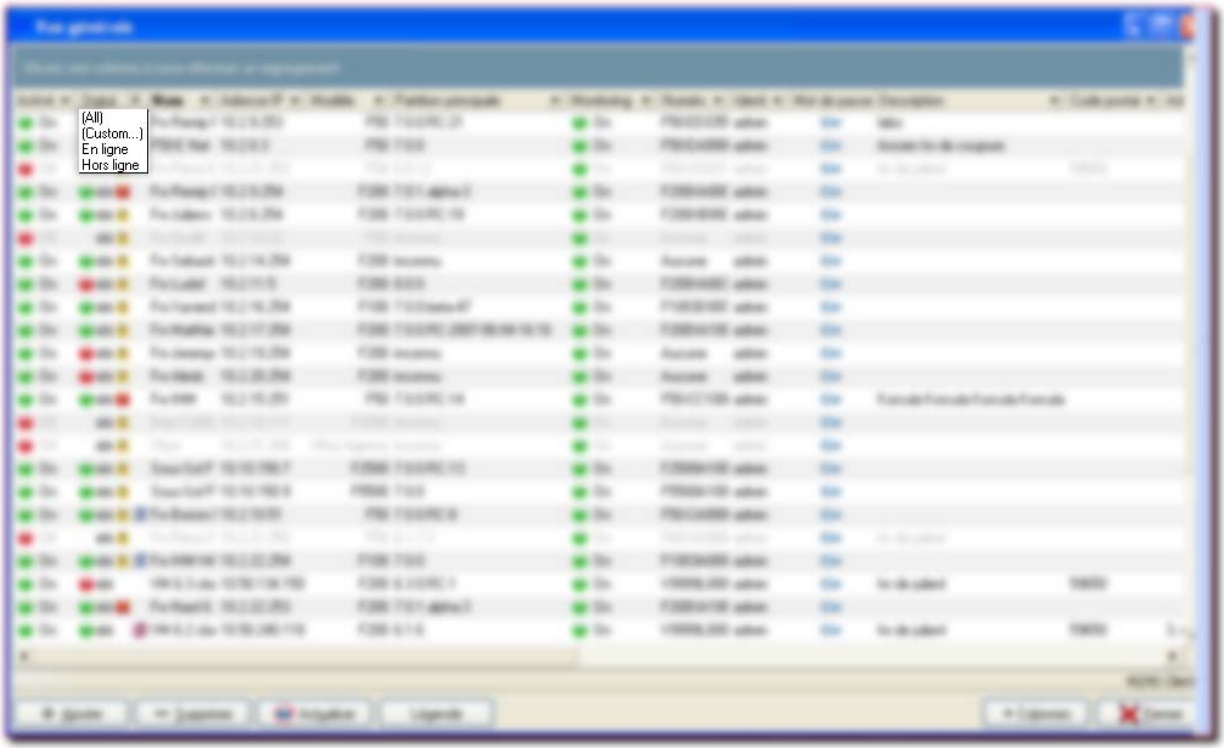


Figure 483 : Liste déroulante

En choisissant une valeur de la liste, seules les lignes dont la valeur de la colonne est égale à la valeur choisie seront affichées.

En choisissant "All" toutes les lignes sont affichées.

En choisissant "Custom", la fenêtre suivante s'affiche :

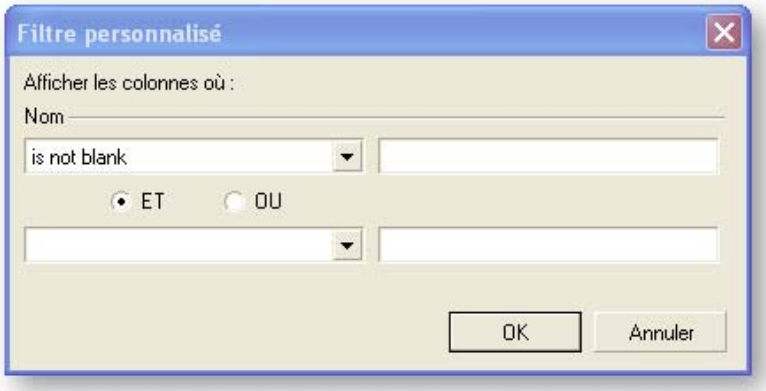


Figure 484 : Filtre personnalisé

Cette fenêtre vous permet de définir un filtre personnalisé. Vous avez la possibilité de définir deux critères liés entre eux par un lien logique "ET" ou "OU".

Lorsqu'un ou plusieurs filtres sont appliqués, une nouvelle barre apparaît en bas du tableau. Cette barre affiche l'ensemble des critères qui sont appliqués pour filtrer le tableau. La case à cocher dans cette barre permet d'affecter ou de retirer le filtre. La case contenant une croix permet de supprimer le filtre.

Figure 485 : Barre de filtres

Le bouton **Personnaliser…** présent dans cette même barre permet d'afficher un constructeur de filtres pour réaliser des filtres plus fins.

Figure 486 : Constructeur de filtres

Le constructeur de filtres se présente sous forme arborescente et représente les différentes conditions du filtre. Les filtres peuvent être sauvegardés pour être utilisés dans d'autres projets, grâce au bouton **Enregistrer…**. Il suffit alors d'utiliser le bouton **Ouvrir…** pour rechercher et charger un filtre précédemment enregistré.

Exemple de filtre :
Ce filtre signifie que les lignes sélectionnées seront celles pour lesquelles le firewall est activé.

20.3.2.5. Mettre à jour les informations

La mise à jour des informations concernant chaque Appliance peut être automatique – **`Options/Préférences)`** ou manuelle. Pour réaliser une mise à jour manuelle des informations, cliquez sur le bouton **Actualiser**, seuls les firewalls dont la colonne **Etat** a la valeur **ON** seront pris en compte. La fenêtre suivante s'affiche alors :

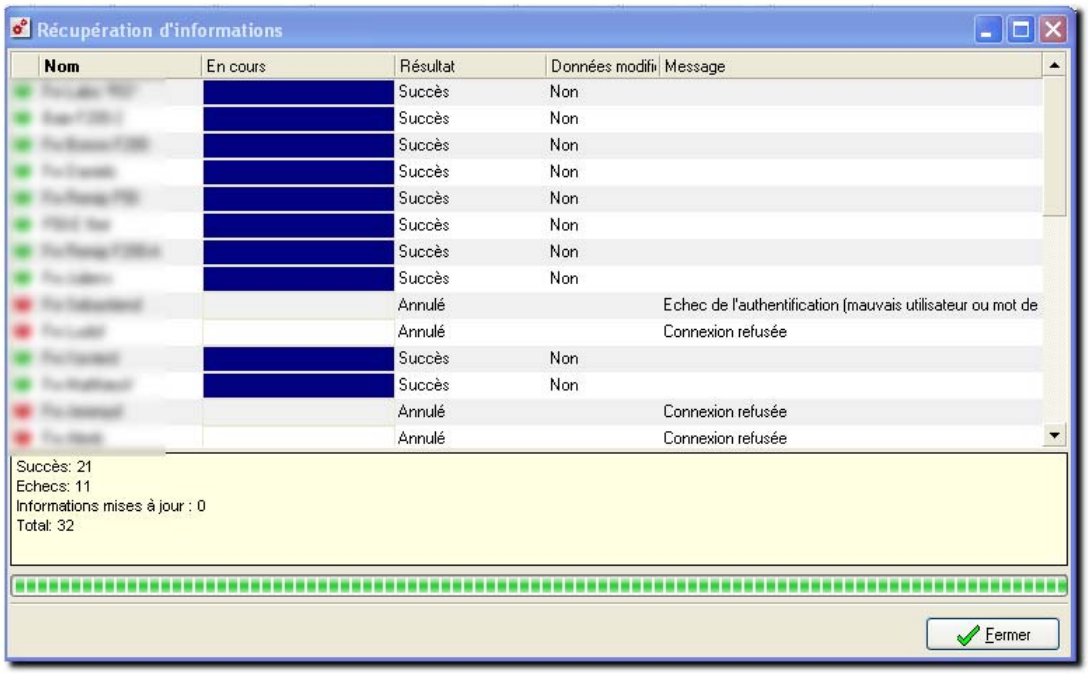


Figure 487 : Récupération d'informations

Tous les firewalls concernant apparaissent dans cette fenêtre, une barre indique la progression de la mise à jour des informations et un voyant indique l'état de la mise à jour :

	La mise à jour des informations est en cours.
	La mise à jour des informations a échoué.
	La mise à jour des informations a réussi.

Description des différents champs présents dans cette fenêtre

Nom	Nom du firewall dont les informations doivent être mises à jour.
En cours	Jauge de progression de la mise à jour.
Résultat	Résultat de la mise à jour des informations.
Données modifiées	Indique si des informations ont été modifiées depuis la dernière mise à jour des informations.
Message	Message d'explication par rapport à l'opération.

Au bas de la fenêtre, 4 informations sont données : le nombre de mises à jour des informations réussies, le nombre de mises à jour des informations ayant échoué, le nombre de mises à jour des informations ayant apporté des modifications, le total des succès, échecs et nombre de mise à jour des informations ayant apporté des informations.

Le panneau de mise à jour suivant s'affichera aussi pour indiquer l'avancement de la mise à jour des informations par rapport au site Web de NETASQ :

Une fois la mise à jour des informations réalisées, cliquez sur le bouton **Fermer**. Les informations de la vue générale et des attributs de firewalls, comme le numéro de version logicielle, sont maintenant complètement à jour.

20.3.3. Gestion des firewalls par la vue topologique

20.3.3.1. Vue topologique

La première vue qui apparaît lorsque vous ouvrez un nouveau projet est la vue topologique.

Cette vue, plus intuitive que la vue générale, permet en effet de représenter les équipements du projet sous une forme graphique, en dessinant la topographie du réseau ou du sous réseau. Plusieurs topologies peuvent être éditées avec les mêmes objets.

Cette vue peut être affichée en sélectionnant le menu **`Vues\Vue topologique`**. Si la vue est déjà ouverte, il suffira de cliquer sur le bouton **Vue topologique** en bas de l'écran dans la barre de changement de vue pour y accéder.

La vue topologique se présente de la façon suivante :

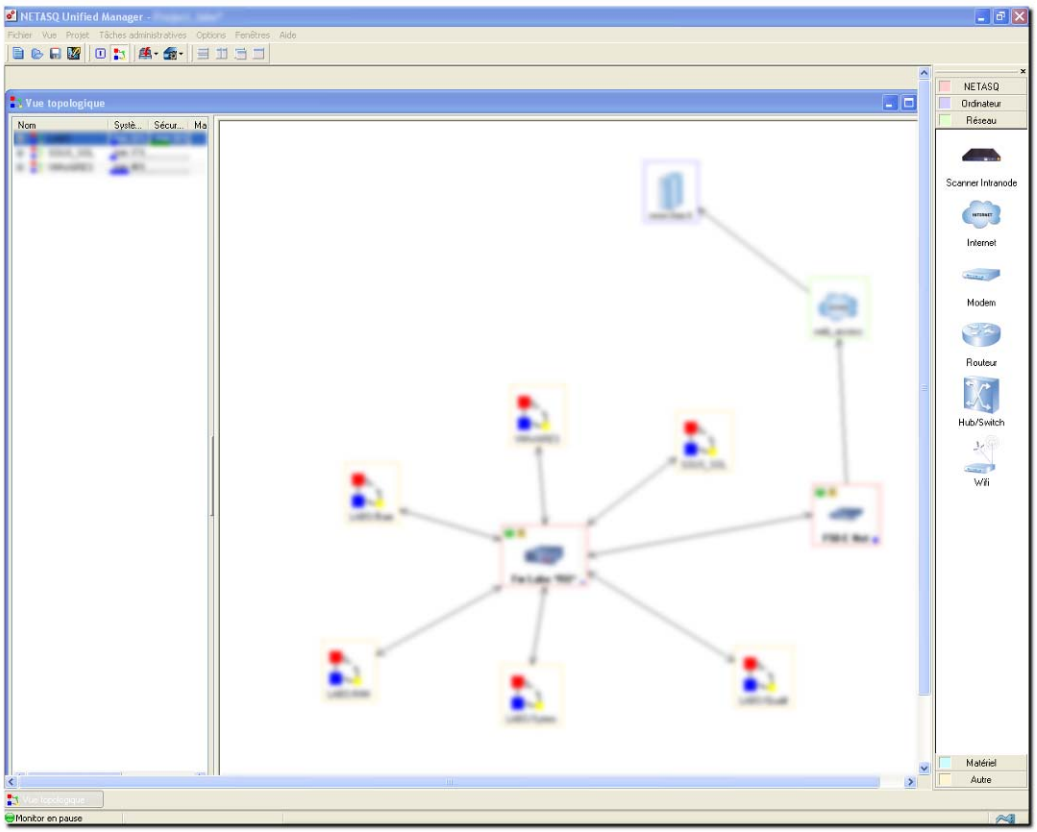


Figure 488 : Vue topologique

La fenêtre est segmentée en trois parties :

- Une zone de classement des topographies (à gauche de l'écran).
- Une zone de visualisation de la topographie d'un réseau ou d'un sous réseau (au centre).
- La barre d'objets (à droite de l'écran).

20.3.3.2. Zone de classement des topologies

Cette zone permet de définir des ensembles de topologies sous une forme arborescente. Ainsi l'administration de sous réseaux sera facilité en réalisant un découpage du réseau en plusieurs topologies (correspondant chacune à un sous réseau).

Pour créer l'arborescence des topologies qui seront utilisées dans le projet, créez autant de niveaux et de sous niveaux que vous le désirez afin d'organiser votre projet au mieux.

Pour créer un nouveau regroupement au niveau de la racine de l'arborescence, cliquez sur le bouton **Ajouter** puis "Sur la racine…". Une fenêtre vous demande de saisir le nom du regroupement.

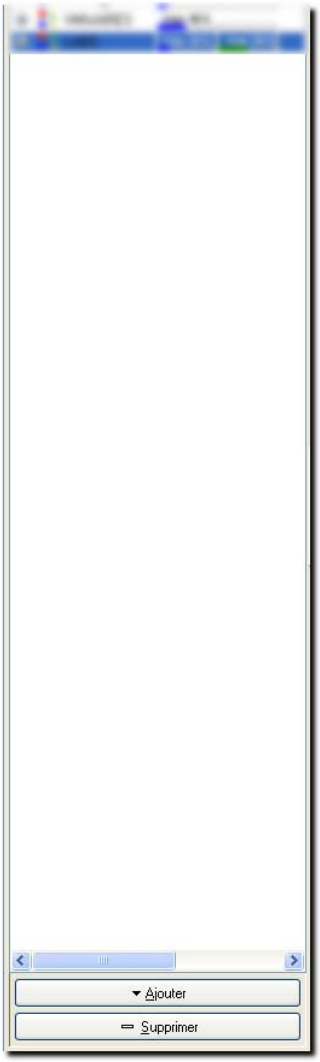


Figure 489 : Classement des topologies

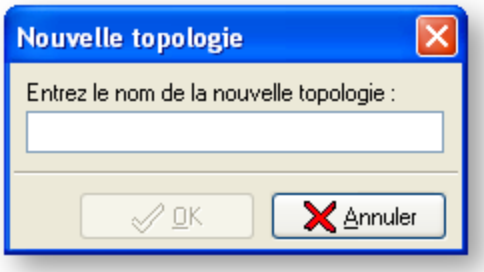


Figure 490 : Nouvelle topologie

Le nom apparaît alors au niveau de la racine de l'arborescence.

Pour créer un sous niveau dans un regroupement, il faut sélectionner le regroupement pour lequel vous désirez créer le sous niveau et cliquer sur le bouton **Ajouter** puis Sur **`Nom du regroupement`** ou en cliquant avec le bouton droit de la souris et en sélectionnant **Ajouter** sur "Nom du regroupement".

Un menu contextuel est aussi disponible en cliquant avec le bouton droit de la souris sur un niveau pour renommer ou supprimer celui-ci, ou pour ajouter un sous niveau.

Il est possible de créer autant de regroupements et de sous niveaux que vous le désirez.

Les sous niveaux dans un regroupement peuvent être affichés ou masqués. Lorsque les sous niveaux sont affichés, le symbole suivant apparaît devant le nom du regroupement. Il suffit alors de cliquer sur ce symbole pour masquer les sous niveaux du regroupement. Lorsque les sous niveaux sont masqués, le symbole suivant apparaît devant le nom du regroupement. Il suffit alors de cliquer sur le symbole pour afficher les sous niveaux du regroupement.

Visualisation rapide des indicateurs

En plus des différentes topologies et des objets présents dans ces topologies, la zone de classement des topologies permet une visualisation rapide des indicateurs système et sécurité, ainsi que des cumuls d'alarmes présents sur chaque firewall. Une explication plus avancée des indicateurs est donnée dans la suite du document.

20.3.3.3. Zone de visualisation de la topologie

Figure 491 : Zone de visualisation de la topologie

Cette zone permet de créer et de gérer la vue topologique de chaque élément de l'arborescence de la zone de classement. Pour cela, sélectionnez l'élément de l'arborescence que vous désirez éditer puis construisez de manière graphique votre vue topologique. Un même objet peut être utilisé dans plusieurs topologies mais ne peut pas être utilisé plusieurs fois dans la même topologie.

Sous la zone de visualisation de la topologie, la barre d'actions vous permet de :

- **Vérifier tous** : ce bouton vous permet de vérifier l'état de tous les clients présents dans la zone.
- **Légende** : Permet d'afficher une fenêtre d'informations au sujet de la dernière connexion, la HA, le suivi de configuration, la connexion.
- **Zoom +** : un zoom intérieur est réalisé sur la zone de visualisation.
- **Zoom -** : un zoom extérieur est réalisé sur la zone de visualisation.
- **Zoom par défaut** : ce bouton vous permet de réinitialiser le zoom de la zone de visualisation.

Ajouter, éditer et supprimer un objet dans la vue

Ajouter un objet

Deux moyens permettent d'ajouter un objet dans la vue :

- En utilisant la barre d'objets à droite de l'écran, si celle-ci est affichée. Si la barre n'est pas affichée, sélectionnez le menu **Vues\Barre d'outils topologique** pour afficher celle-ci. Ensuite, pour ajouter un objet, il suffit de choisir, dans la catégorie voulue l'objet souhaité puis de cliquer avec le bouton gauche de la souris dans la vue générale.
- En utilisant le menu contextuel, pour cela, cliquez avec le bouton droit de la souris dans la zone de visualisation de la vue. Choisissez le type d'objet.

AVERTISSEMENT
Tous les objets ne peuvent pas être ajoutés par ce moyen.

Dans les deux cas, une fenêtre s'ouvre, vous invitant à renseigner les informations relatives à l'objet.

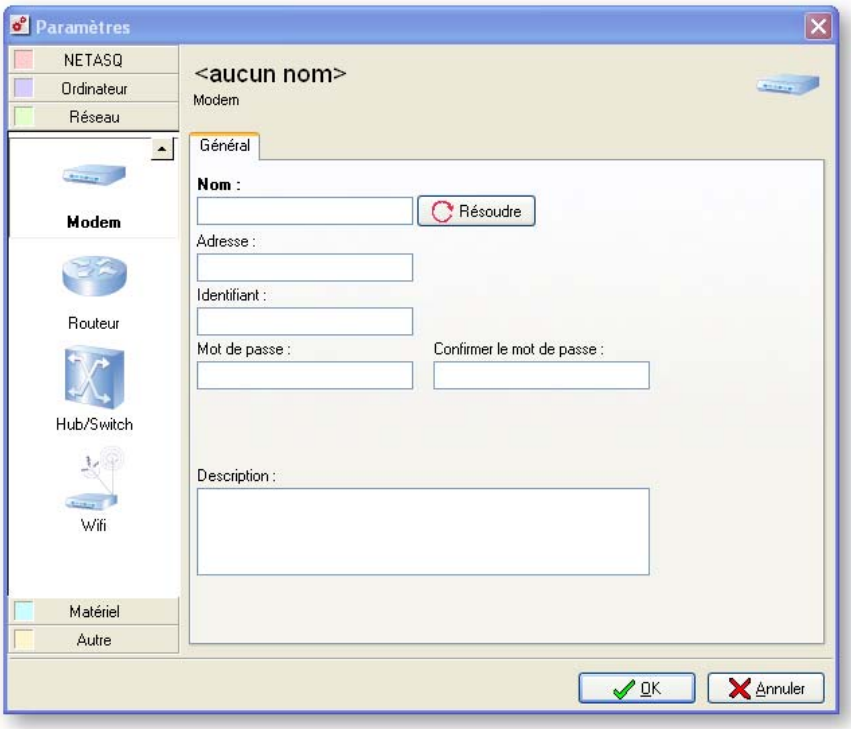


Figure 492 : Paramètres - Général

(*Cf. Pour connaître la signification de chacune des catégories d'objets de la barre d'objets, référez-vous à la Partie 20/Chapitre 2 : Présentation de l'interface.*)

Editer un objet

Pour modifier les propriétés d'un objet, il suffit de double-cliquer sur celui-ci avec le bouton gauche de la souris ou de cliquer avec le bouton droit de la souris sur l'objet et de choisir l'option "Configurer" dans le menu contextuel qui s'affiche.

Supprimer un objet

Pour supprimer un objet existant, sélectionnez celui-ci avec le bouton gauche de la souris et appuyez sur la touche **Suppr**.

Mettre à jour les informations d'un objet

Pour mettre à jour les attributs d'un produit UTM NETASQ (version logicielle, état de la Haute Disponibilité…), double-cliquez sur l'objet représentant le firewall avec le bouton gauche de la souris et cliquez sur le bouton **Actualiser** présent dans la nouvelle fenêtre.

Dans le cas d'un objet de la catégorie "NETASQ"

La première fenêtre qui s'affiche est la suivante :

Figure 493 : Choisir un client

Si le firewall a déjà été défini dans la vue globale, cliquez sur le bouton **Choisir un client** et choisissez le firewall désiré, celui-ci est alors ajouté à la zone de visualisation. Si vous souhaitez créer un nouveau firewall, cliquez sur le bouton **Nouveau client** et la fenêtre suivante s'affiche :

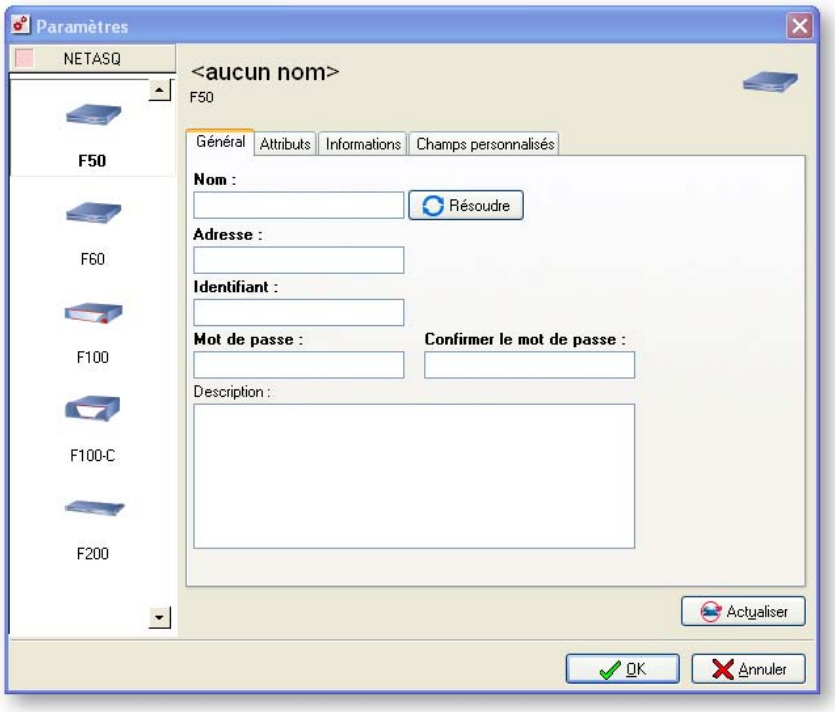


Figure 494 : Paramètres - Général

Des informations sont alors demandées sous plusieurs onglets :

Onglet Général

Les informations demandées dans l'onglet **Général** sont nécessaires pour insérer le firewall dans le mode NETASQ UNIFIED MANAGER.

Nom	Indiquez le nom choisi pour le firewall. Ce nom sera utilisé pour distinguer l'Appliance des autres équipements.
Adresse	Indiquez l'adresse IP de l'Appliance que peut contacter la machine sur laquelle est installée l'Administration Globale NETASQ.
Identifiant	Indiquez le login du compte d'administration sur le firewall.
Mot de passe	Indiquez le mot de passe du compte d'administration sur le firewall.
Confirmation du mot de passe	Confirmez le mot de passe du compte d'administration.
Commentaire	Indiquez un commentaire libre concernant le firewall.

Les champs en gras doivent être obligatoirement renseignés.

Onglet Attributs

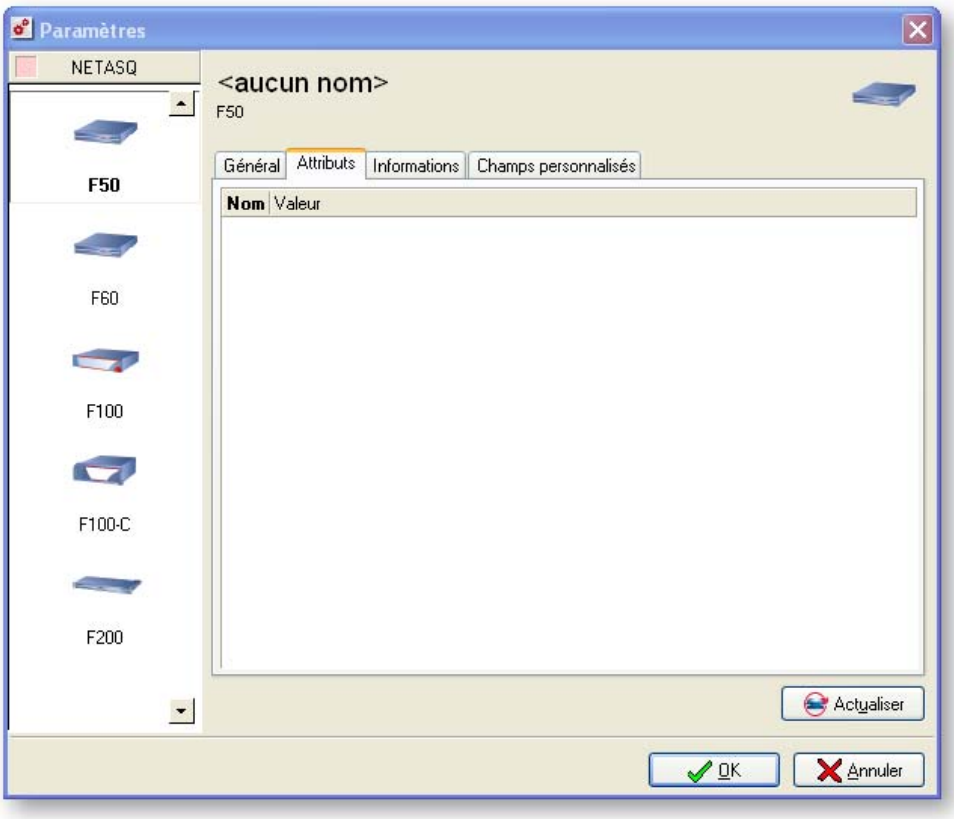


Figure 495 : Paramètres - Attributs

Cette zone n'affiche des données que lorsque les informations pour le produit ont été mises à jour une première fois. Les données affichées alors sont :

Numéro de série	Numéro de série du firewall.
Firmware	Version du firmware du firewall.
OEM	Marque sous laquelle est vendu le produit.
GMTDate	Date du firewall au format GMT
GMTOffset	Ecart de l'heure locale avec l'heure GMT.
HA	Etat de la haute disponibilité.
Current Partition	Partition active (principale ou backup).
OtherPartitionVersion	Version de la partition qui n'est pas active.
LastSaveToOtherPartition	Dernière sauvegarde de la partition active vers l'autre partition.
GlobalAdminOption	Option de la licence permettant au firewall d'être administré en mode "service". Contactez votre revendeur ou le service commercial de NETASQ pour de plus amples renseignements concernant ce mode.

Pour rafraîchir les données de ce tableau, cliquez sur le bouton **Actualiser** au bas de la fenêtre.

Onglet Informations

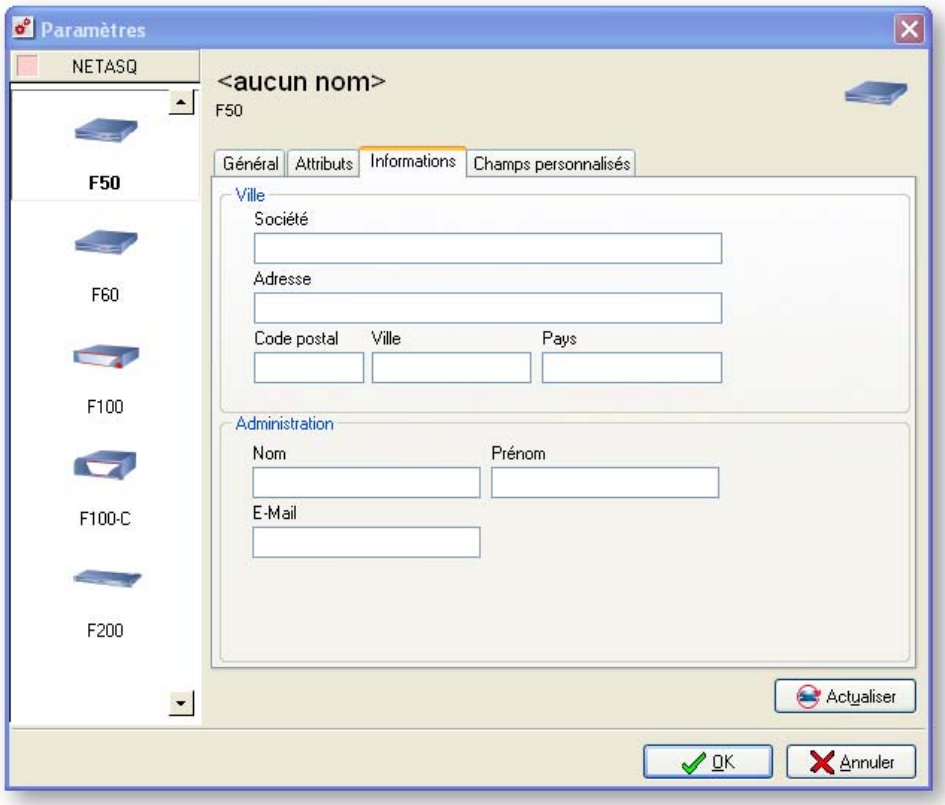


Figure 496 : Paramètres - Informations

Les informations demandées dans cet onglet sont facultatives et servent à identifier le produit.

Société	Indiquez le nom de l'entreprise (ou la filiale, le service…) où est installé le firewall.
Adresse	Indiquez l'adresse où est installé le firewall.
Code postal	Indiquez le code postal de la ville où est installé le firewall.
Ville	Indiquez la ville où est installé le firewall.
Pays	Indiquez le pays où est installé le firewall.
Nom	Indiquez le nom du contact qui gère localement l'Appliance.
Prénom	Indiquez le prénom du contact.
E-mail	Indiquez l'adresse e-mail du contact.

Il est aussi possible de changer le modèle d'Appliance choisi, pour cela, il suffit de sélectionner un nouveau modèle dans la barre de gauche de la fenêtre.

L'objet apparaît alors dans la zone de visualisation. U**n point d'interrogation** est visible en haut à gauche du cadre de l'objet si les informations concernant l'Appliance n'ont pas encore été récupérées. Cet icône disparaît dès que les informations concernant l'Appliance sont mises à jour.

Dans le cas d'un objet de la catégorie « Ordinateurs »

La fenêtre suivante s'affiche :

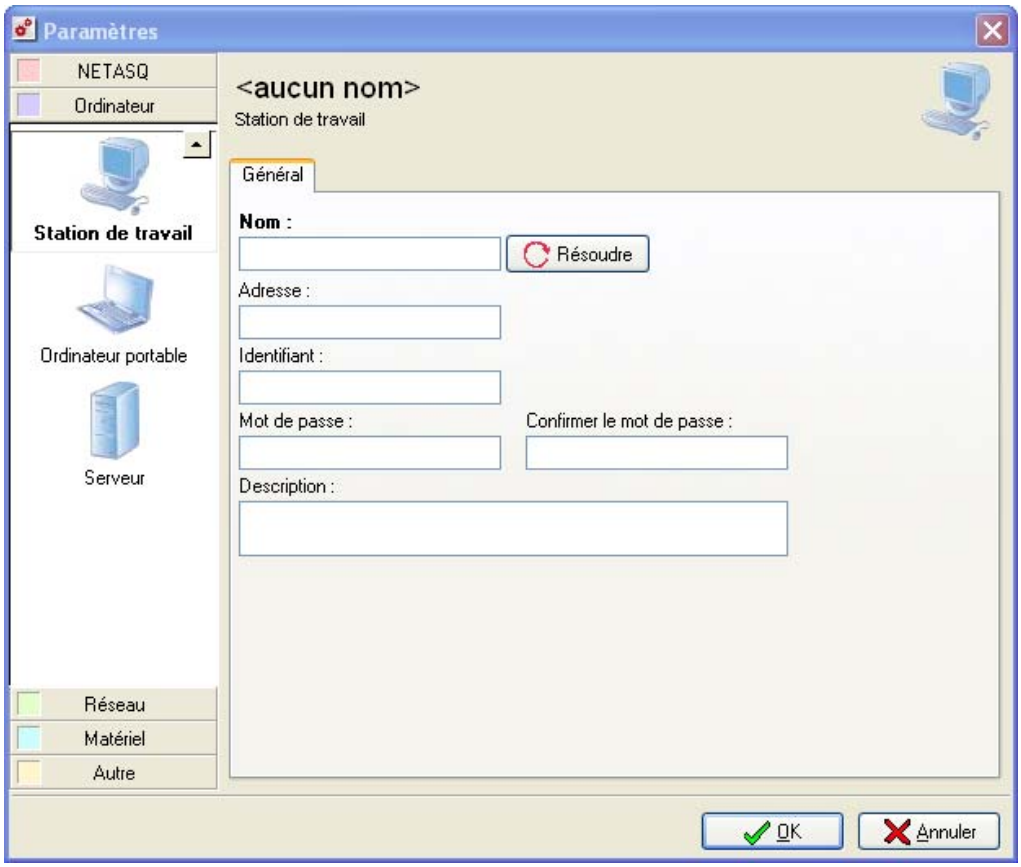


Figure 497 : Paramètres - Général

Les informations suivantes sont alors demandées :

Nom	Indiquez le nom choisi pour le firewall. Ce nom sera utilisé pour distinguer l'Appliance des autres équipements.
Adresse	Indiquez l'adresse IP du firewall que peut contacter la machine sur laquelle est installée l'Administration Globale NETASQ.
Identifiant	Indiquez le login du compte d'administration sur l'Appliance.
Mot de passe	Indiquez le mot de passe du compte d'administration sur le firewall.
Confirmer le mot de passe	Confirmez le mot de passe du compte d'administration.
Description	Indiquez un commentaire libre concernant le firewall.

Les champs en gras doivent être obligatoirement renseignés.

Le mode NETASQ UNIFIED MANAGER peut lancer des outils externes d'administration pour certains équipements, il utilisera alors les informations de connexions données ici.

Cliquez sur **OK**. L'objet est alors ajouté dans la zone de visualisation.

Dans le cas d'un objet de la catégorie « Réseau »

Par exemple, pour un modem la fenêtre suivante s'affiche :

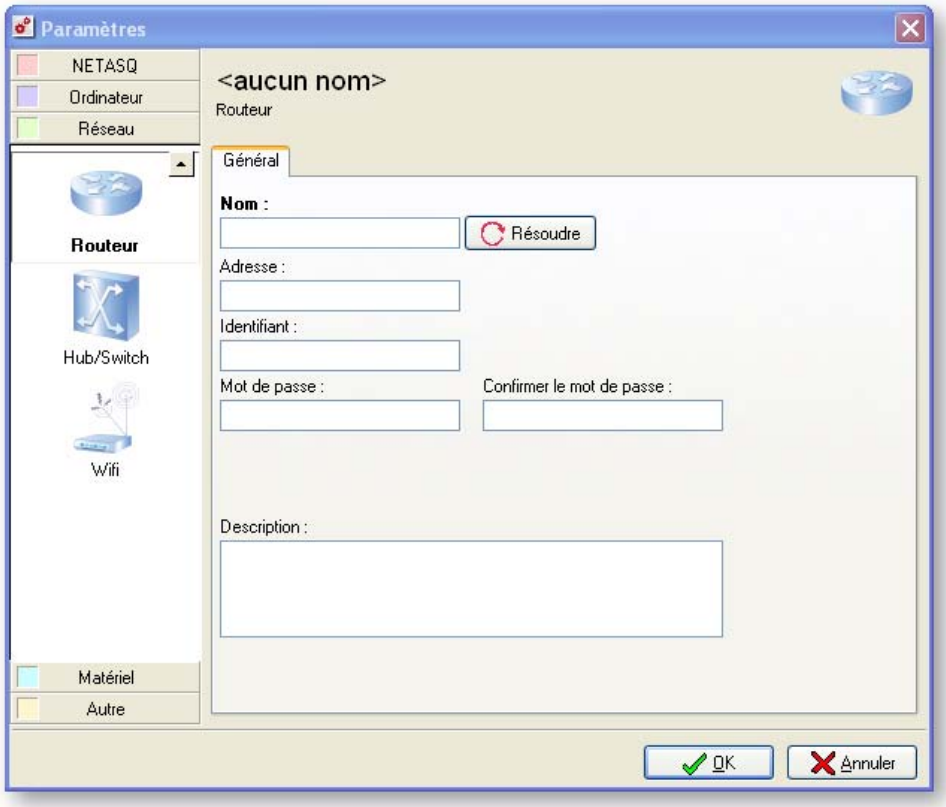


Figure 498 : Paramètres - Général

Les informations suivantes sont alors demandées :

Nom	Indiquez le nom choisi pour le firewall. Ce nom sera utilisé pour distinguer l'Appliance des autres équipements.
Adresse	Indiquez l'adresse IP du firewall que peut contacter la machine sur laquelle est installée l'Administration globale NETASQ.
Identifiant	Indiquez le login du compte d'administration sur le firewall.
Mot de passe	Indiquez le mot de passe du compte d'administration sur le firewall.
Confirmer le mot de passe	Confirmez le mot de passe du compte d'administration.
Description	Indiquez un commentaire libre concernant le firewall.

Les champs en gras doivent être obligatoirement renseignés.
Le mode NETASQ UNIFIED MANAGER peut lancer des outils externes d'administration pour certains équipements, il utilisera alors les informations de connexions données ici.

Cliquez sur **OK**. L'objet est alors ajouté dans la zone de visualisation.

Dans le cas d'un objet de la catégorie « Matériel »

La fenêtre suivante s'affiche :

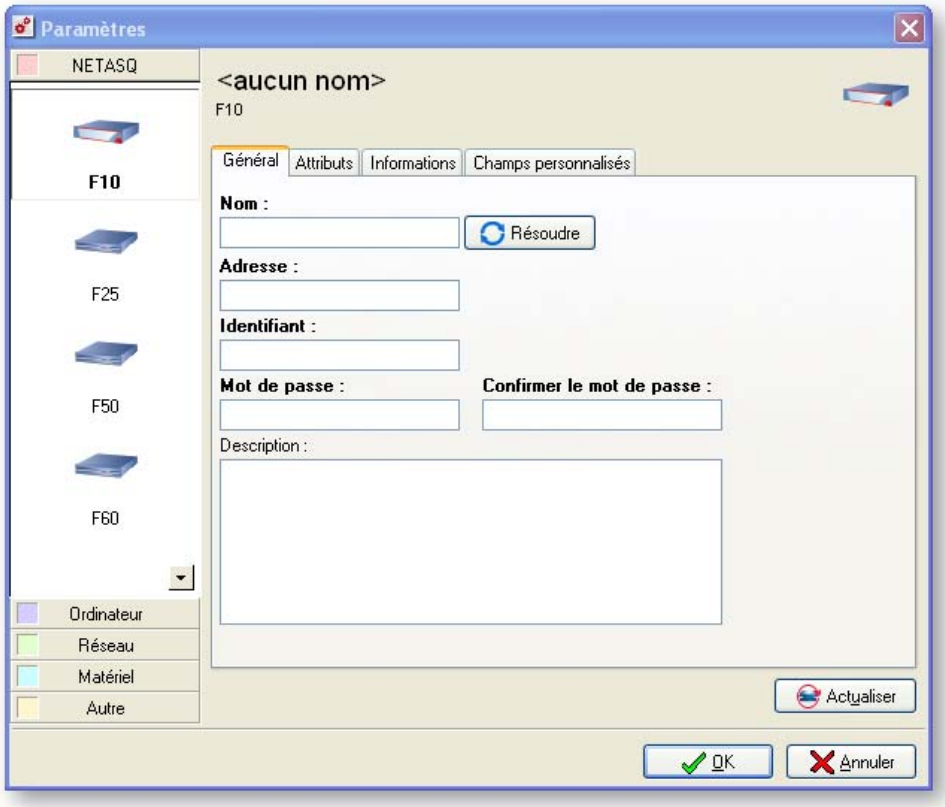


Figure 499 : Paramètres - Général

Les informations suivantes sont alors demandées :

Nom	Indiquez le nom choisi pour le firewall. Ce nom sera utilisé pour distinguer l'Appliance des autres équipements.
Adresse	Indiquez l'adresse IP du firewall que peut contacter la machine sur laquelle est installée l'Administration globale NETASQ.
Identifiant	Indiquez le login du compte d'administration sur le firewall.
Mot de passe	Indiquez le mot de passe du compte d'administration sur le firewall.
Confirmer le mot de passe	Confirmez le mot de passe du compte d'administration.
Description	Indiquez un commentaire libre concernant le firewall.

Les champs en gras doivent être obligatoirement renseignés.

Le mode NETASQ UNIFIED MANAGER peut lancer des outils externes d'administration pour certains équipements, il utilisera alors les informations de connexions données ici.

Cliquez sur **OK**. L'objet est alors ajouté dans la zone de visualisation.

Dans le cas d'un objet de la catégorie « Autres »

La fenêtre suivante s'affiche :

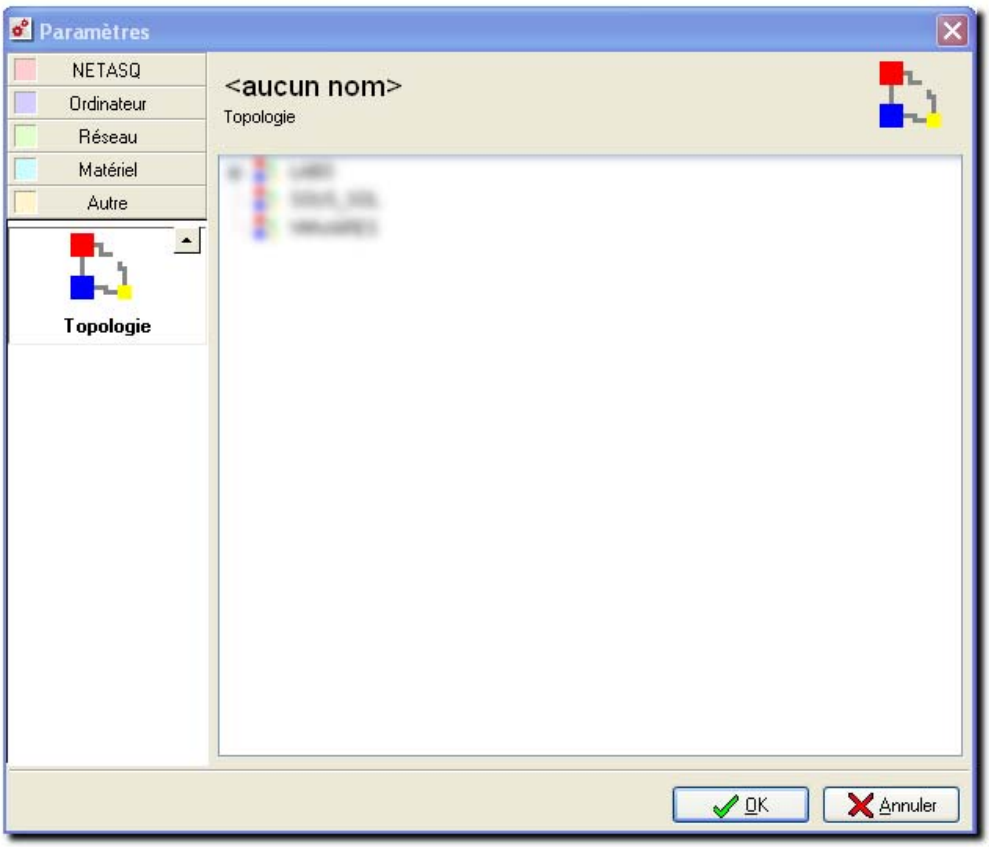


Figure 500 : Paramètres - Autres

Cette catégorie ne contient que les objets « Note » et « Topologie ». L'objet « Note » permet de définir sur la zone de visualisation, une zone de couleur sur laquelle il est possible d'apposer du texte. Cet objet est toujours placé en arrière plan par rapport aux autres objets.
L'objet « Topologie » permet de définir, sur la zone de visualisation, une zone représentant une autre topologie déjà définie, un clic sur l'objet permet d'accéder directement à la visualisation de la topologie correspondante.

Pour les deux objets, indiquez le texte que vous désirez voir apparaître.

Cliquez sur **OK**. L'objet est alors ajouté dans la zone de visualisation.

Menu contextuel de la vue topologique

Le menu contextuel de la vue topologique est obtenu en réalisant un clic droit de la souris dans la vue topologique. Les fonctionnalités accessibles par le menu contextuel lorsqu'on sélectionne un objet ou lorsqu'on pointe le vide sont différentes. Contrairement à la vue générale, elles sont complémentaires, nous évoquerons les deux menus.

Menu contextuel sur un objet de la vue topologique

Ce menu contextuel de la vue topologique donne accès aux sous menus suivants :

Configurer	Accéder à la configuration d'un firewall. Rappel : un double-clic sur l'objet vous permet aussi d'accéder à la configuration.
Désactiver	Désactiver la prise en compte d'un firewall de la vue générale. Cette option permet notamment de verrouiller le firewall envers toutes les actions possibles dans l'Administration Globale sans retirer le firewall.
Désactiver le monitoring	Il est désormais possible d'activer ou de désactiver le monitoring par firewall. Le monitoring est activé par défaut tant que les limitations de la licence ne sont pas atteintes.
Supprimer	Retirer un firewall de la vue générale.
Firewall Manager	Ouverture de NETASQ UNIFIED MANAGER.
Outils	Accès aux outils de configuration NETASQ et externes.
Configuration directe	Accès à la configuration directe (cf. Partie 20/Chapitre 3 : *Configuration directe*).
Maintenance	Accès aux actions de maintenance de l'Administration Globale.
Déploiement	Déployer des configurations dans l'Administration Globale.
Scripts…	Ce menu permet l'exécution de scripts NETASQ sur les Appliance ciblés.
Disponibilité (Ping)	Test de disponibilité (tentative de connexion au serverd).
Vérification de l'état	Actualisation manuelle de l'état du firewall.
Réinitialiser les alarmes	Permet de remettre par défaut l'état des alarmes.

Menu contextuel hors d'un objet de la vue topologique

Ce menu contextuel de la vue topologique donne accès aux sous-menus d'ajout des objets configurables dans le mode « Firewal Manager » :

- UTM NETASQ.
- Machine : stations de travail du mode »Firewall Manager », serveurs, autres.
- Objet réseau : switch, modem, autres.
- Objet matériel.
- Notes.
- Topologies.

20.3.3.4. Ajouter, éditer et supprimer un lien entre 2 objets

Ajouter un lien

Lorsque plusieurs objets ont été créés et ajoutés à la zone de visualisation topologique, il est possible de représenter les liens physiques qui existent entre eux (liaison Ethernet, Dialup, Personnalisé…).

Pour cela, il suffit d'utiliser le bouton droit de la souris. Cliquez avec le bouton droit sur le premier objet que vous désirez inclure dans la liaison. Maintenez le bouton appuyé et déplacer le pointeur de la souris jusqu'à l'objet constituant la seconde extrémité de la liaison, relâchez alors le bouton. Un trait a été dessiné entre les deux objets et la fenêtre suivante s'affiche :

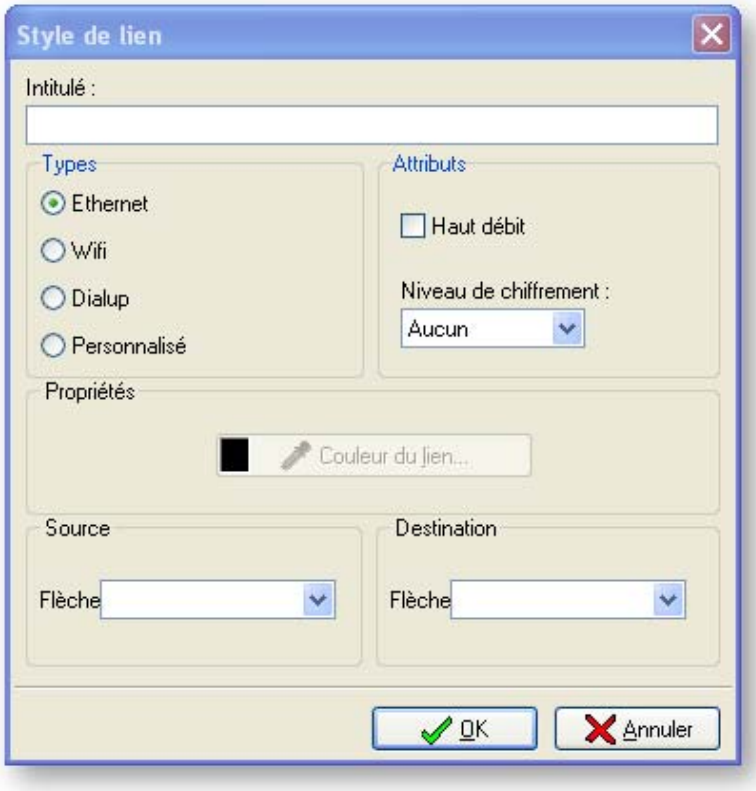


Figure 501 : Style de lien

Dans cette fenêtre indiquez les informations suivantes :

Intitulé	Indiquez ici un nom pour désigner le lien. Ce nom sera affiché au dessus du lien, dans la zone de visualisation.
Types	Type de lien : Ethernet, Dialup ou Personnalisé. Chaque type de lien a une couleur différente à l'affichage. Le type « Personnalisé » permet de définir un type de lien personnalisé.
Attributs	Attributs du lien : Haut débit (lien 100M ou Gigabit par exemple), [SUPPR : bas débit, sécurité haute (lien chiffré et authentifié), sécurité basse (lien normal)], Niveau de chiffrement (Aucun, Faible, Elevé).
Couleur du lien	Pour le type de lien « Personnalisé », il est possible de définir une couleur personnalisée dans la palette des couleurs.
Source	La liste déroulante permet de définir si l'objet source (premier objet sélectionné lors de la création du lien) doit être pointé par une flèche.

Destination	La liste déroulante permet de définir si l'objet destination (second objet sélectionné lors de la création du lien) doit être pointé par une flèche.

Le lien est alors complètement créé et relie les deux objets. Il est possible de relier un objet topologie à d'autres objets.

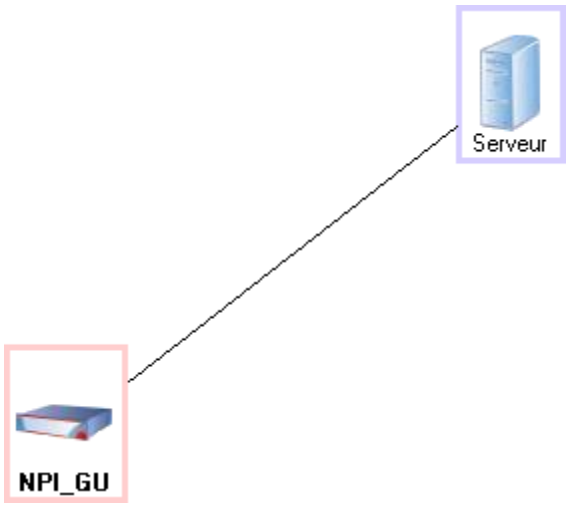


Figure 502 : Lien

Le lien sera représenté de façon différente selon le paramétrage réalisé dans la fenêtre précédente : une couleur différente selon le type de lien, un trait plus épais si la case **Haut débit** a été cochée, une clef sur le lien si un niveau de chiffrement a été choisi.

Modifier un lien

Pour modifier les propriétés du lien, double-cliquez sur celui-ci avec le bouton gauche de la souris et la fenêtre décrite précédemment s'ouvre.

Si pour des raisons de disposition et de présentation des objets, vous souhaitez courber les lignes représentant les liens, il est possible de modifier la forme des liens. Pour cela, cliquez avec le bouton gauche de la souris sur l'endroit que vous désirez courber puis déplacer le lien en maintenant le bouton de la souris appuyé. Relâchez le bouton lorsque la forme du lien vous convient.

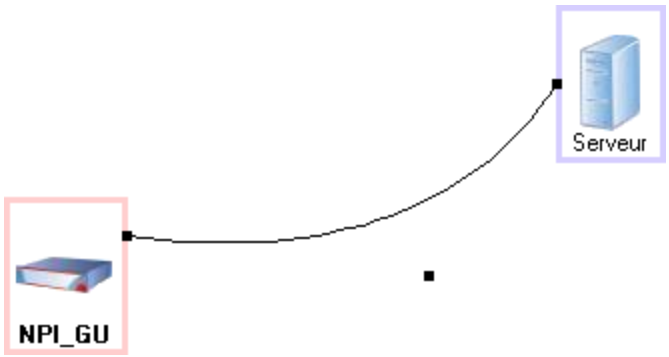


Figure 503 : Lien

Supprimer un lien

Pour supprimer le lien, cliquez sur celui-ci avec le bouton gauche de la souris et appuyez sur le bouton **Suppr** de votre clavier.

Déplacer un ou plusieurs objets

Sélectionnez le ou les objets que vous désirez déplacer puis, en maintenant le bouton gauche de la souris appuyé déplacez la sélection jusqu'à l'emplacement voulu.

20.3.4. Indicateurs système et sécurité

Pour les objets NETASQ de la vue topologique, le mode Global Administration permet un monitoring des événements système et sécurité très performant. En effet, pour chaque boîtier UTM NETASQ, le mode Global Administration offre une fenêtre d'indicateurs pouvant être mis à jour par le moniteur du mode Global Administration ou de façon manuelle par la fonction « Vérification de l'état ».

Ces indicateurs sont classés en deux catégories. Les indicateurs système, sont attachés à la surveillance des événements relatifs aux interfaces Ethernet, à la charge du processeur du firewall… Et les indicateurs sécurité sont attachés à la surveillance des alarmes et des événements relatifs au noyau ASQ.

Fenêtre d'indicateurs de la vue topologique

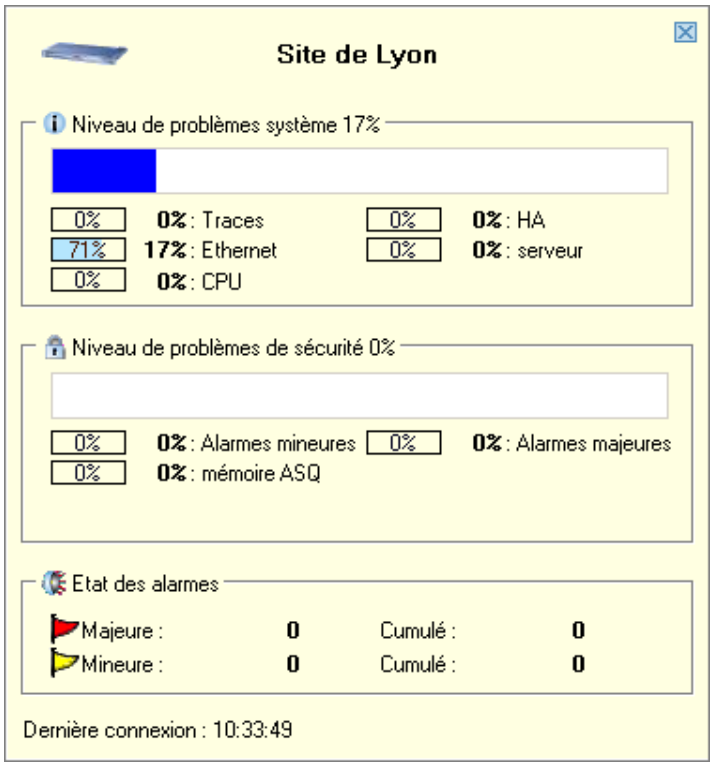


Figure 504 : Indicateurs

La fenêtre d'indicateurs regroupe plusieurs informations concernant le firewall monitoré :

- Le nom du firewall.
- Le niveau de problèmes système.
- Le niveau de problèmes sécurité.
- L'état des alarmes.
- L'heure de la dernière connexion du moniteur du mode « Globale Administration » NETASQ à ce firewall.

Les indicateurs système

La première section de la fenêtre d'indicateurs regroupe les indicateurs système. Ces indicateurs concernent :

- Les traces : indicateurs relatifs au remplissage de l'espace alloué aux traces.
- Ethernet : indicateurs relatifs à la connectivité des interfaces.
- CPU : indicateurs relatifs à la charge du processeur du firewall.
- HA : indicateurs relatifs au dispositif de Haute Disponibilité, si celui-ci est présent sur le firewall
- Serveur : indicateurs relatifs à certains serveurs critiques du firewall.

L'affichage de ces indicateurs est basé sur la pondération des événements système les uns par rapport aux autres afin de présenter un état cohérent du firewall. Chaque indicateur est présenté de la façon suivante :

> [pourcentage] pourcentage : nom de l'indicateur

Pour expliquer les informations présentées, nous nous baserons sur l'exemple suivant :

> **Exemple**
> [75%] 17% : Ethernet

Le premier pourcentage fait référence au niveau de problème Ethernet. Par exemple dans notre cas, 3 des 4 interfaces du firewall ne sont pas connectées alors que l'administrateur les a définies comme actives dans NETASQ UNIFIED MANAGER, il y a sûrement un problème sur ces interfaces.

Le deuxième pourcentage fait référence à l'incidence globale de ces problèmes sur le firewall. Vous comprenez ici que chacun des événements système est pondéré avec un seuil maximum de poids sur l'état général du firewall.

Les indicateurs de sécurité

La deuxième section de la fenêtre d'indicateurs regroupe les indicateurs système. Ces indicateurs concernent :

- Alarmes mineures : indicateurs relatifs au nombre d'alarmes mineures.
- Alarmes majeures : indicateurs relatifs au nombre d'alarmes majeures.
- Mémoire ASQ : indicateurs relatifs au taux de remplissage de la mémoire ASQ.

L'affichage de ces indicateurs est basé sur la pondération des événements sécurité les uns par rapport aux autres afin de présenter un état cohérent du firewall (les alarmes majeures auront plus de poids que les alarmes mineures). Chaque indicateur est présenté de la façon suivante :

> **Exemple**
> [pourcentage] pourcentage : nom de l'indicateur

Référez-vous à la section "indicateurs système" » pour obtenir une explication complète des informations présentées.

Etat des alarmes

Nous présentons l'état des alarmes dans la section "indicateurs de sécurité" » car ils sont fortement liés. Les informations présentées dans cette section sont paramétrées dans les options du projet (Cf. *Partie 20/Chapitre 2 : Projets*).

Par type d'alarmes (majeure ou mineure) est présenté le nombre d'alarmes survenues entre deux actualisations de NETASQ REAL-TIME MONITOR et un cumul des alarmes depuis le démarrage de l'application d'ADMINISTRATION GLOBALE NETASQ.

20.3.5. Tâches administratives

20.3.5.1. Présentation

La fonction première de l'Administration globale NETASQ est de faciliter l'administration d'un parc d'équipements UTM NETASQ au moyen de divers outils intégrés au produit.

L'Administration globale NETASQ est capable de se connecter au site Web NETASQ afin de récupérer de façon automatique les mises à jour de firmwares, les licences des Appliance et de les installer de façon tout aussi automatique sur les différents Appliance gérés.

AVERTISSEMENT
Lors des opérations d'administration, il est vivement conseillé de désactiver le moniteur de l'Administration globale NETASQ (voir section Monitoring et supervision).

Le menu Tâches administratives est le principal outil d'administration de l'Administration globale NETASQ, il permet en effet de mettre à jour les appliances et de mettre à jour les licences, de déployer les politiques de sécurité, de créer des scripts…

Configuration	Pour sauvegarder ou restaurer les configurations des appliances.
Mettre à jour le firmware	Pour mettre à jour les firmwares des appliances.
Mettre à jour la licence	Pour mettre à jour les licences des appliances.
Sauvegarder la partition	Pour sauvegarder les partitions principales sur les partitions secondaires (partitions de backup).
Scripts	Ce menu permet l'exécution de scripts NETASQ sur les appliances ciblés.
Déploiement	Ce menu permet le déploiement des politiques de sécurité et les bases d'objets.

20.3.5.2. Configuration

Le mode Global Administration vous permet la sauvegarde ou la restauration des configurations des boîtiers UTM sélectionnés. Ces fonctionnalités sont accessibles grâce à plusieurs menus du mode Global Administration :

- Le menu **Tâches administratives\Configuration.**
- Le menu contextuel de la vue générale dans la section "Maintenance"
- Le menu contextuel de la vue topologique dans la section **Maintenance\Sauvegarder ou Restaurer.**

Sauvegarde de configuration

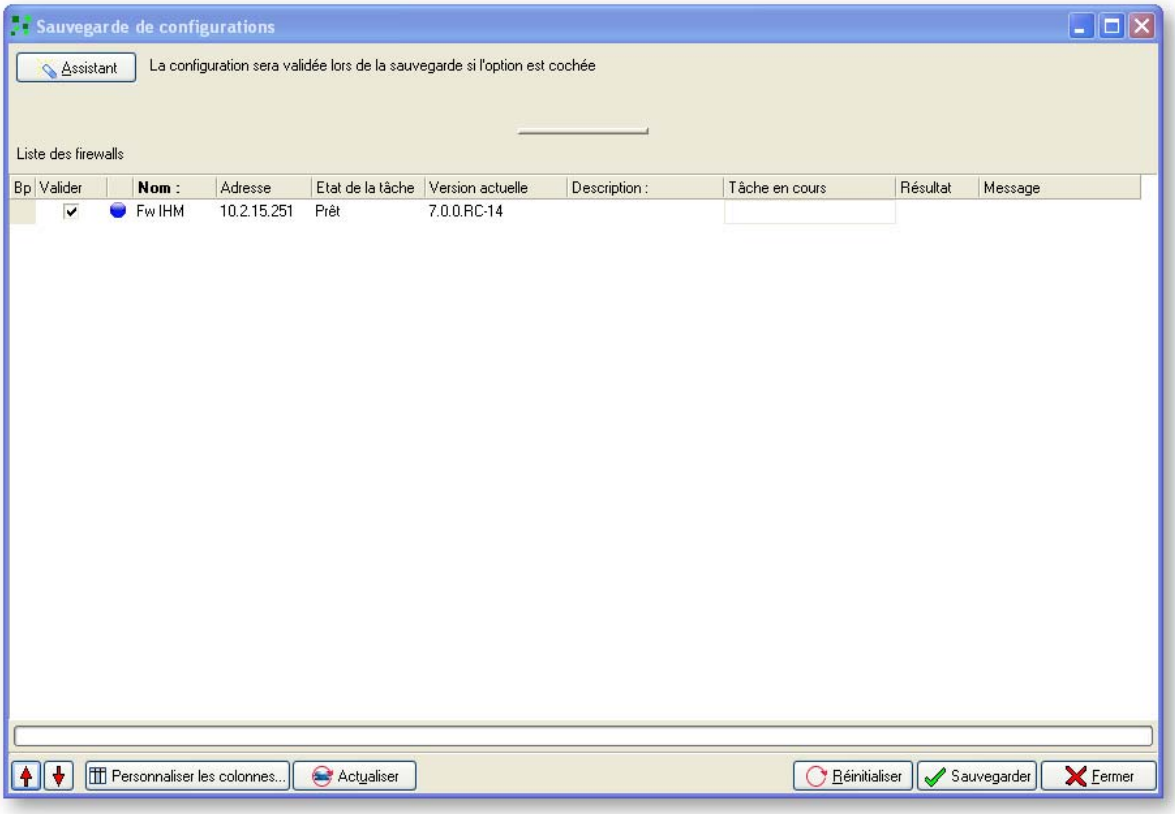


Figure 505 : Sauvegarde de configuration

Pour réaliser la sauvegarde de la configuration d'un ou de plusieurs boîtiers UTM, sélectionnez le bouton **Assistant** au haut de l'écran. La sauvegarde de la configuration des appliances s'effectue en deux étapes.

Etape 1

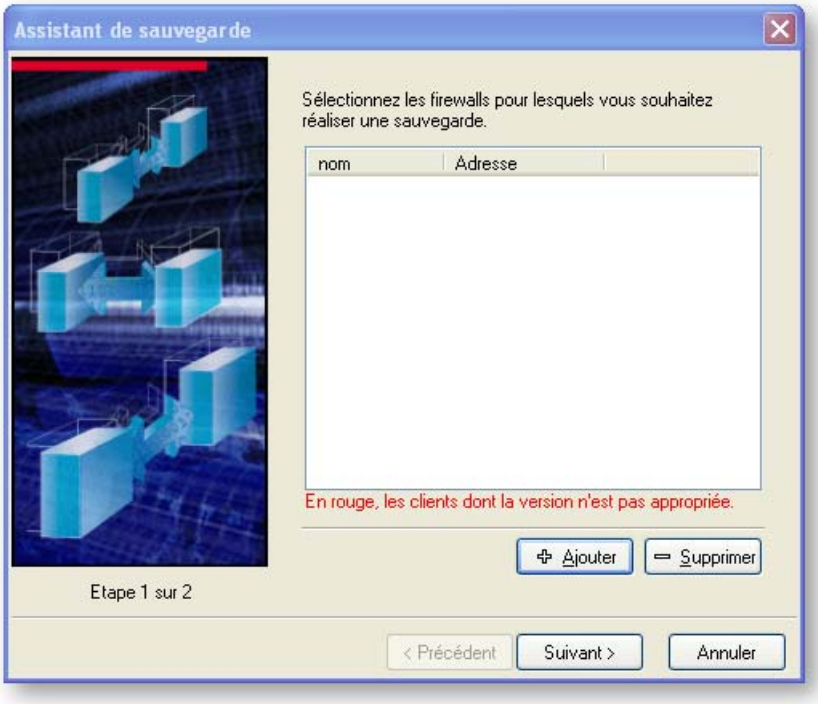


Figure 506 : Assistant de sauvegarde - Etape 1

Choisissez les firewalls dont vous désirez effectuer la sauvegarde de la configuration.
Cliquez sur **Ajouter**, l'écran suivant s'affiche :

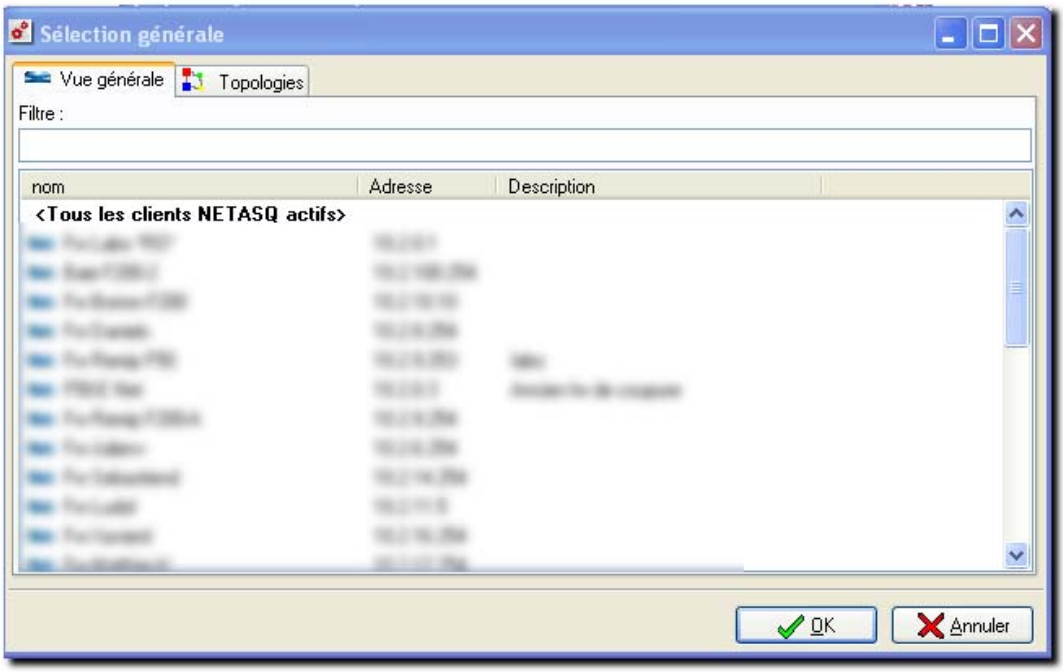


Figure 507 : Sélection générale - Vue générale

Sélectionnez le/les firewalls à ajouter puis cliquez sur **Suivant** pour continuer.

Etape 2

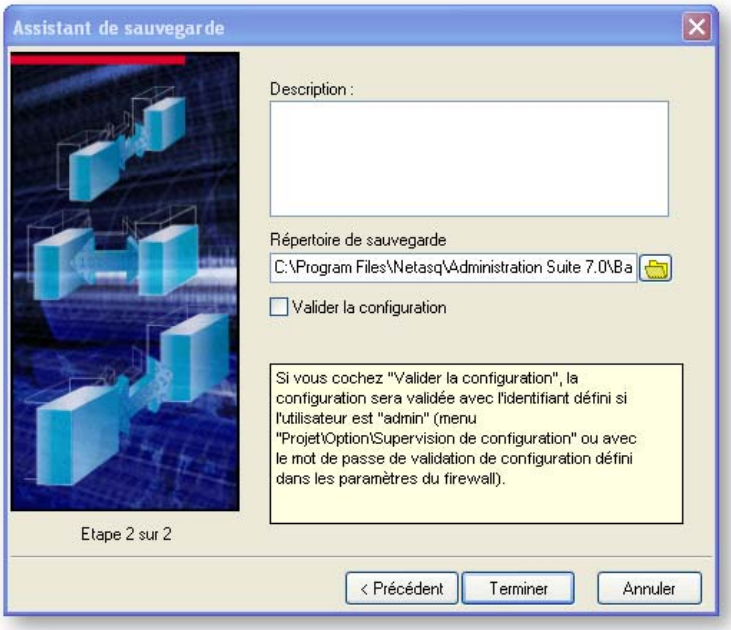


Figure 508 : Assistant de sauvegarde - Etape 2

Cet écran vous permet d'ajouter une description à la sauvegarde et de spécifier le répertoire de sauvegarde dans lequel vous désirez stocker les sauvegardes. Par défaut, le répertoire de sauvegarde est celui défini dans les préférences du Mode "Global Administration". »Cliquez sur **Terminer** pour effectuer la sauvegarde des configurations.

La fenêtre du gestionnaire des sauvegardes de configurations apparaît. Elle récapitule les paramètres définis dans l'assistant de sauvegarde de configurations. Dans cet écran vous pouvez modifier les paramètres définis.

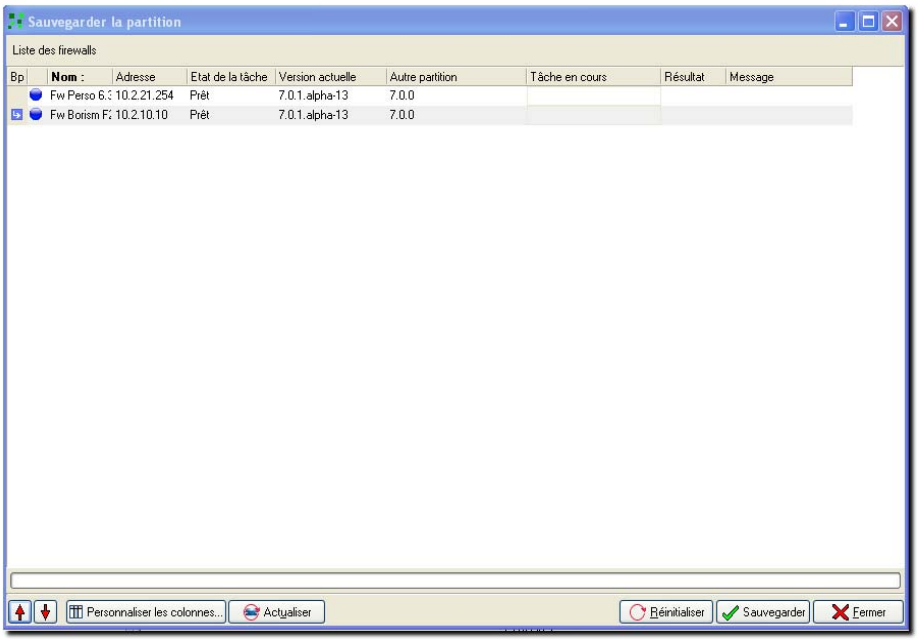


Figure 509 : Sauvegarde de la partition

Par défaut la première colonne, intitulée "B« ", »permet de spécifier des points d'arrêts dans l'exécution de la tâche configurée. Le principe est le suivant : en spécifiant un point d'arrêt sur une ligne, la tâche configurée sera d'abord réalisée sur tous les appliances situés au dessus et sur ce point d'arrêt dans le tableau puis si toutes les tâches sont un succès, le mode Global Administration NETASQ effectuera les tâches pour les appliances qui suivent. Pour spécifier un point d'arrêt, faites un double-clic sur la ligne voulue. Pour retirer le point d'arrêt, faites un double-clic sur le point d'arrêt

Par défaut, dans la deuxième colonne du tableau est affiché un voyant lumineux. La couleur donnée au voyant dépend de l'état de l'action :

	En attente.
	Action commencée.
	Action annulée ou non réalisée.
	Action terminée avec success.

Ensuite, le tableau est composé des colonnes suivantes :

Nom	Nom choisi pour l'appliance.
Adresse	Adresse IP de l'appliance.
Etat de la tâche	Etat de l'action (en attente, commencée, terminée…).
Version actuelle	Version du firmware de la partition active de l'Appliance.
Description	Commentaire associés à la sauvegarde.

Ajouter des appliances

Ajouter dans le tableau les appliances que vous désirez sauvegarder en cliquant avec le bouton droit de la souris et en choisissant **Ajouter** dans le menu contextuel qui s'affiche.

Choisissez ensuite **`firewalls`** si vous voulez choisir les Appliances à sauvegarder ou **`Tous les firewalls actifs`** si vous voulez sauvegarder tous les Appliances actifs (ceux dont l'état est à ON dans la vue générale).

Pour retirer un Appliance de la liste, sélectionnez celui-ci et cliquez avec le bouton droit de la souris, choisissez alors l'option **Supprimer**.

Le bouton **Réinitialiser**, réinitialise les tâches de sauvegarde de configuration.

AVERTISSEMENT
Pour que les sauvegardes de configuration puissent être effectuées, il faut que les informations concernant les Appliances choisis aient été mises à jour (au moyen du bouton **Actualisation** de la vue globale).

Sauvegarder les configurations

Cliquez sur le bouton **Tout MAJ.** Le voyant lumineux passe alors en orange sur les Appliances en cours de sauvegarde et vous pouvez voir la barre de progression avancer. Toutes les configurations sont alors sauvegardées simultanément.

Restauration de configuration

Pour réaliser la restauration de la configuration d'un ou de plusieurs Appliances, sélectionnez le menu **`Tâches administratives\Configuration\Restaurer`**. La restauration de la configuration des Appliances s'effectue en quatre étapes.

Etape 1

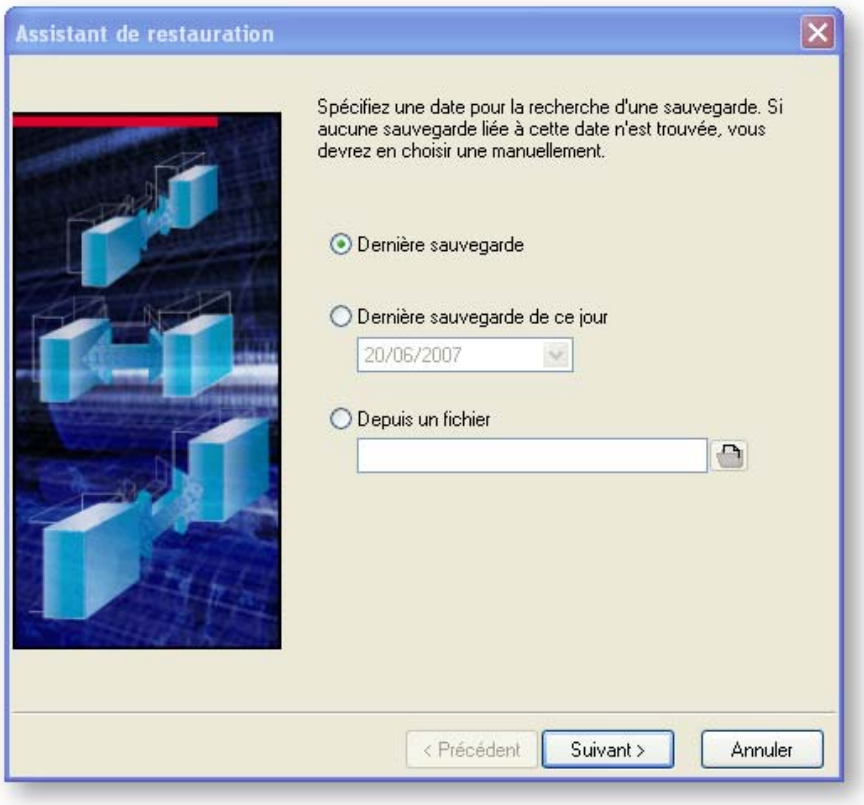


Figure 510 : Assistant de restauration

Les étapes 1 et 2 consistent à définir quelle sauvegarde doit être utilisée pour la restauration en définissant la date de la sauvegarde et la provenance.

Dernière sauvegarde : Cette option permet de spécifier la dernière sauvegarde située dans le répertoire des sauvegardes de configuration.

Dernière sauvegarde de ce jour : Cette option permet de spécifier la dernière sauvegarde à la date indiquée située dans le répertoire des sauvegardes de configuration. Vous définissez la date de recherche grâce à un mini calendrier.

Depuis un fichier : Spécifiez directement le fichier de sauvegarde que vous souhaitez restaurer. Si vous choisissez ce paramètre l'étape 2 de l'assistant (expliquée ci-dessous) n'apparaît pas.

Etape 2

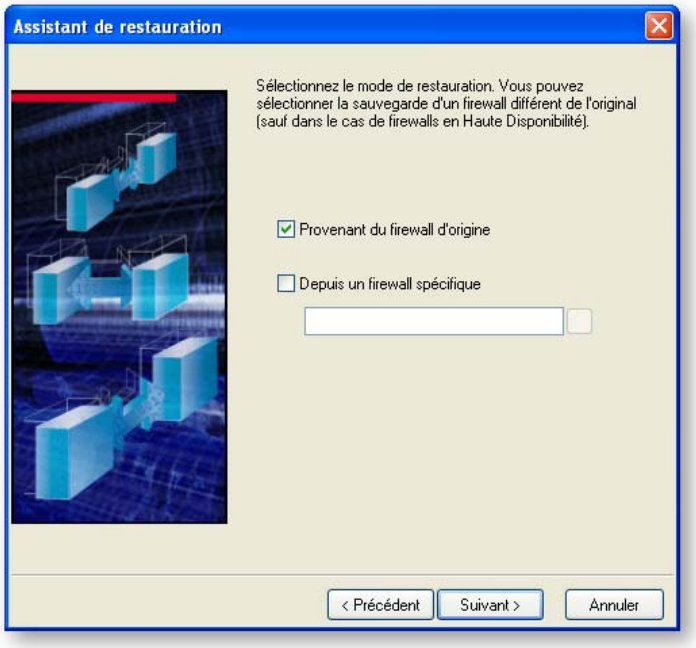


Figure 511 : Assistant de restauration

Provenant du firewall d'origine : Cette option permet de spécifier une sauvegarde située dans le répertoire des sauvegardes de configuration réalisée à partir du firewall sur lequel sera effectuée la restauration.

Depuis un firewall spécifique : Cette option permet de spécifier une sauvegarde située dans le répertoire des sauvegardes de configuration réalisée à partir du firewall sélectionné.

Etape 3

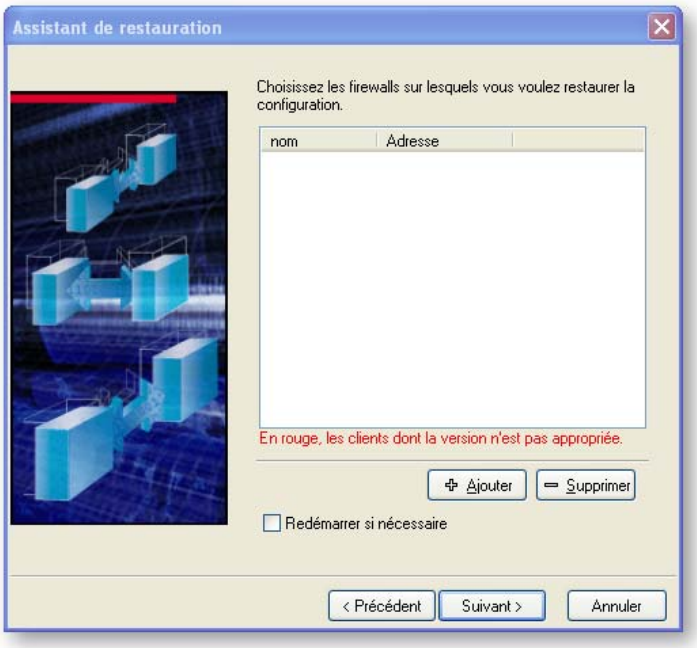


Figure 512 : Assistant de restauration

L'étape 3 consiste à définir les firewalls sur lesquels une restauration doit être effectuée.

Notez l'option **Redémarrer si nécessaire** permettant d'indiquer que s'il y a lieu l'Appliance redémarrera pour prendre en compte la modification des fichiers du fait de la restauration.

Etape 4

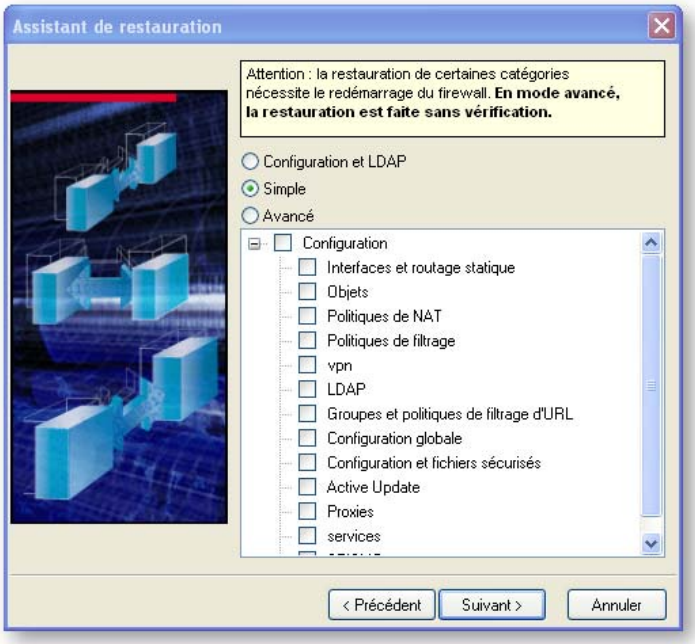


Figure 513 : Assistant de restauration - Simple

Enfin si dans vos choix précédents, vous avez sélectionné une des options suivantes : "Provenant du firewall d'origine" puis «un firewall spécifique» l'assistant de restauration vous permet de séléctionner trois types de restauration :

- Configuration et LDAP (Restauration complète) : ce choix permet la restauration de la configuration de l'Appliance et de l'ensemble des informations stockées dans la base LDAP (fiches utilisateurs), sans option, cette configuration restaure tout.
- Simple (Restauration partielle) : ce choix permet la restauration de la configuration de l'Appliance selon des choix effectués par l'administration. Ce type de configuration partielle permet par exemple la restauration de la base d'objets et ainsi faciliter le travail de l'administrateur.
- Avancé (Restauration partielle) : ce choix, plus granulaire que l'option "simple" permet la sélection la plus spécifique en terme de restauration. Mais attention, ce type de restauration doit être manipulé avec précaution car elle permet la restauration de configurations incomplète (les tunnels VPN IPsec sans leurs clés par exemple).

Les options de restauration sont les suivantes :

- Configuration : sélectionne tous les éléments situés sous ce choix.
- Interfaces et routage statique : configuration réseau de l'appliance, la configuration des interfaces, la passerelle par défaut et les routes statiques.
- Objets : la base des objets, sauf les utilisateurs.
- Politiques de NAT : tous les slots de la configuration de la translation d'adresses.
- Politiques de filtrage : tous les slots de la configuration du filtrage.
- Configuration et base LDAP, PKI : configuration de la base LDAP de l'appliance, ainsi que les élements stockés dans la base (utilisateurs) et configuration de la PKI.

- Groupes et politiques de filtrage d'URL : tous les slots de la configuration du filtrage d'URL ainsi que les groupes d'URL statiques (créés par l'administrateur).
- Configuration globale : tous les slots de la configuration globale ainsi que les objets globaux.
- Configuration sécurisée et fichiers sécurisés : configuration sécurisée et fichiers chiffrés et sécurisés par la configuration sécurisée.
- Active Update : configuration du module de mise à jour automatique de l'appliance.
- Proxies : configuration des proxies HThttpSMTP et POP3.
- Certificats et clés pré partagées : certificats stockés dans le menu « Certificats » et clés pré partagées configurées.
- Prévention d'intrusion (ASQ) : configuration du moteur de prévention de l'appliance, l'ASQ
- Configuration du module VPN SSL : configuration du module VPN SSL.
- Configuration des tunnels PPTP : configuration du serveur PPTP.
- Tunnels VPN IPsec : configuration des tunnels VPN IPsec uniquement.
- Programmation horaire : programmation horaire définie pour les slots.
- Règles événementielles : règles de filtrage événementielles configurées manuellement par l'administrateur.
- QoS : configuration des politiques de Qualité de Service.
- Authentification : configuration de l'authentification.
- Indicateurs (système et sécurité) : indicateurs que l'on retrouve dans l'Administration globale.
- Serveur DHCP : service DHCP de l'appliance.
- Client NTP : service NTP de l'appliance.
- Proxy DNS : service DNS de l'appliance.
- Agent SNMP : service SNMP de l'appliance.
- Traces : configuration des traces uniquement.
- Routage statique : passerelle par défaut et routes statiques configurées.
- Evénements système : configuration des événements système.
- Routage dynamique : configuration de la plateforme de routage dynamique.
- Antispam : module Antispam.
- Communication (syslog, envoi de notification) : module de communication de l'appliance, notamment envoi des traces auprès des serveurs syslog et envoi des notifications d'alarmes aux administrateurs.
- Données : sélectionne tous les éléments situés sous ce choix.
- Groupes d'URL dynamiques : tous les groupes d'URL dynamiques, obtenus par Active Update.
- Signatures contextuelles : signatures ASQ obtenues par Active Update.

Etape 5

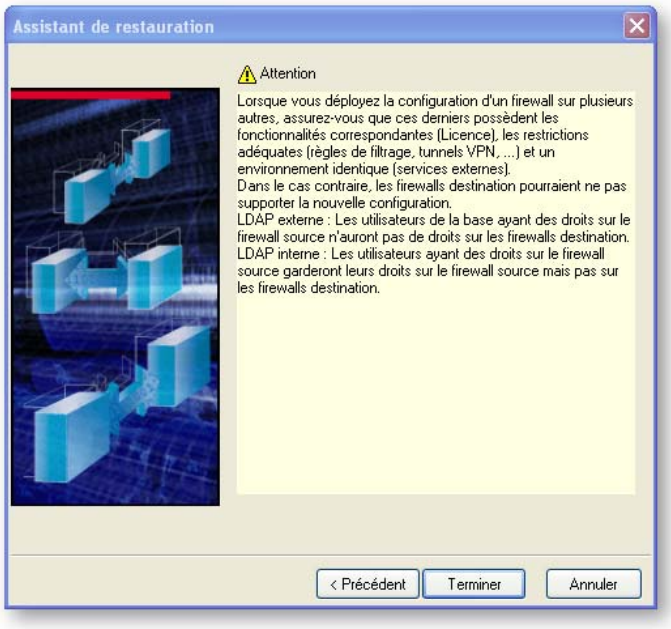


Figure 514 : Assistant de restauration

Gestionnaire de restauration de configurations

Lorsque l'ensemble des paramètres a été défini, cliquez sur **Terminer** pour effectuer la restauration des configurations. La fenêtre du gestionnaire des restaurations de configurations apparaît. Elle récapitule les paramètres définis dans l'assistant de restauration de configuration. Dans cet écran vous pouvez modifier les paramètres définis.

Pour de plus amples informations concernant cette fenêtre, veuillez-vous référer aux pages précédentes.

20.3.5.3. Mise à jour du produit

En sélectionnant le menu `Tâches administratives\Mettre à jour le firmware`, la fenêtre suivante s'affiche :

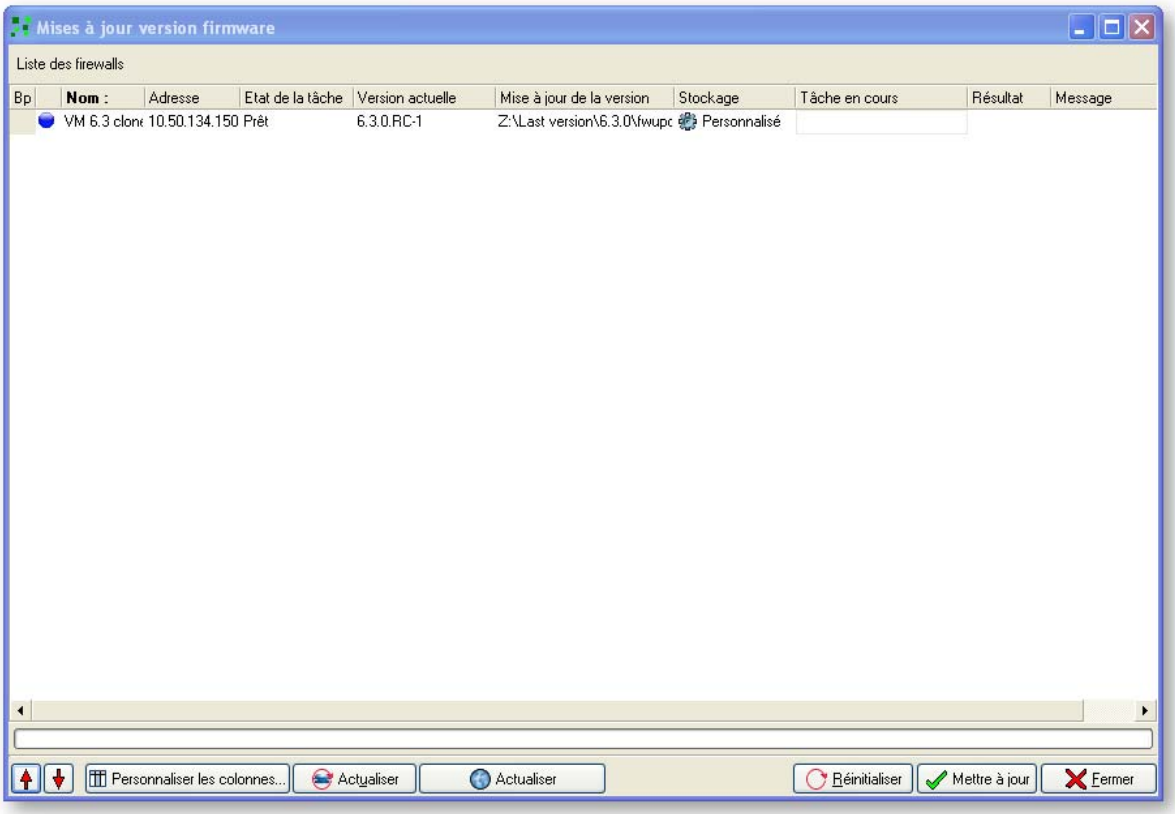


Figure 515 : Mise à jour firmware

Par défaut la première colonne, intitulée "B« ", »permet de spécifier des points d'a'rêt dans l'exécution de la tâche configurée. Le principe est le suivant : en spécifiant un point d'a'rêt sur une ligne, la tâche configurée sera d'abord réalisée sur tous les boîtiers UTM NETASQ situés au-dessus et sur ce point d'a'rêt dans le tableau puis si toutes les tâches sont un succès, le mode "Global Administration" NETASQ effectuera les tâches pour les appliances qui suivent. Pour spécifier un point d'a'rêt, faites un double clic sur la ligne voulue. Pour retirer le point d'a'rêt, faites un double-clic sur le point d'arrêt.

Par défaut, dans la deuxième colonne du tableau est affiché un voyant lumineux. La couleur donnée au voyant dépend de l'état de l'action :

	En attente
	Action commencée
	Action annulée ou non réalisée
	Action terminée avec succès

Ensuite, le tableau est composé des colonnes suivantes :

Nom	Nom choisi pour l'appliance
Adresse	Adresse IP de l'appliance
Etat de la tâche	Etat de l'action (en attente, commencée, terminée…)
Version actuelle	Version du firmware de l'appliance
Mise à jour de la version	Versions de mise à jour disponibles pour cet appliance. Il est possible de choisir l'option "Personnaliser" dans la liste déroulante. Cette option permet de choisir un fichier de mise à jour qui serait stocké en local sur la machine d'administration.
Stockage	Emplacement de la mise à jour (Web, si elle est sur le site Web NETASQ, Personnaliser, si elle se trouve en local).

Tâche en cours	Progression de la tâche.
Résultat	Résultat de la tâche de mise à jour.
Message	Message d'explication en relation avec le champ "Résultat"

Certaines informations affichées ne vous sont pas forcément nécessaires et inversement, vous voulez peut-être afficher des informations qui vous sont utiles. Il est possible de masquer et d'afficher certaines colonnes du tableau. Pour cela, cliquez sur le bouton **Personnaliser les colonnes…**.

Choisir les boîtiers UTM à mettre à jour

Ajouter dans le tableau les firewalls que vous désirez mettre à jour en cliquant avec le bouton droit de la souris et en choisissant **`Ajouter`** dans le menu contextuel qui s'affiche.

Choisissez ensuite **`Firewalls`** si vous voulez choisir les appliances à mettre à jour ou **`Tous les firewalls actifs`** si vous voulez mettre à jour tous les appliances actifs (ceux dont l'état est à ON dans la vue générale).

Pour retirer un appliance de la liste, sélectionnez celui-ci et cliquez avec le bouton droit de la souris, choisissez alors l'option **Supprimer**.

> **AVERTISSEMENT**
> Pour que les mises à jour puissent être effectuées, il faut que les informations concernant les appliances choisis aient été mises à jour (au moyen du bouton **Mettre à jour les informations de la vue globale**).

Mettre à jour les produits UTM NETASQ

Choisissez pour chaque firewall la version de mise à jour à installer (dans la colonne "Mise à jour de la version", puis cliquez sur le bouton **Mettre à jour**. Le voyant lumineux passe alors en orange sur les appliances en cours de mise à jour et vous pouvez voir la barre de progression avancer. Tous les appliances seront alors mis à jour les uns après les autres.

> **AVERTISSEMENT**
> Il est fortement recommandé d'effectuer une sauvegarde de partition après chaque mise à jour du firmware (Cf. "Partie 20/Chapitre 3 : Sauvegarder la partition").

20.3.5.4. Mettre à jour la licence

- En sélectionnant le menu **`Tâches administratives\Mettre à jour la licence`**, la fenêtre suivante s'affiche :

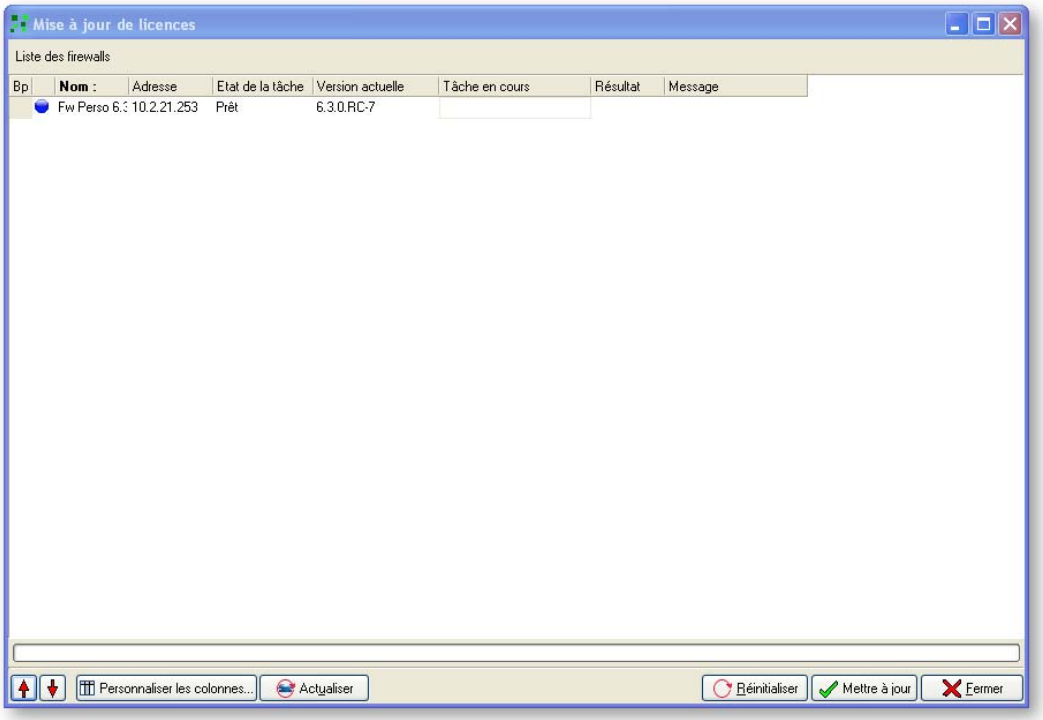


Figure 516 : Mise à jour de licences

Par défaut la première colonne, intitulée "Bp", permet de spécifier des points d'arrêts dans l'exécution de la tâche configurée. Le principe est le suivant : en spécifiant un point d'arrêt sur une ligne, la tâche configurée sera d'abord réalisée sur tous les appliances situés au dessus et sur ce point d'arrêt dans le tableau puis si toutes les tâches sont un succès, le mode Global administration NETASQ effectuera les tâches pour les appliances qui suivent. Pour spécifier un point d'arrêt, faites un double-clic sur la ligne voulue. Pour retirer le point d'arrêt, faites un double-clic sur le point d'arrêt.

Par défaut, dans la deuxième colonne du tableau est affiché un voyant lumineux. La couleur donnée au voyant dépend de l'état de l'action :

	En attente.
	Action commencée.
	Action annulée ou non réalisée.
	Action terminée avec succès.

Ensuite, le tableau est composé des colonnes suivantes :

Nom	Nom choisi pour l'appliance.
Adresse	Adresse IP de l'appliance.
Etat de la tâche	Etat de l'action (en attente, commencée, terminée…).
Version actuelle	Version du firmware actuel de l'appliance.
Version de licence	Version actuelle de la licence.
Tâche en cours	Progression de la tâche.
Résultat	Résultat de la tâche de mise à jour.
Message	Message d'explication en relation avec le champ résultat.

AVERTISSEMENT

Le numéro de version de la licence n'a pas de lien de correspondance avec le numéro de version du firmware. Ces deux numérotations sont totalement indépendantes.

Choisir les équipements UTM NETASQ pour lesquels les licences doivent être mises à jour

Ajoutez dans le tableau les appliances que vous désirez mettre à jour en cliquant avec le bouton droit de la souris et en choisissant **Ajouter** dans le menu contextuel qui s'affiche.

Choisissez ensuite **Firewalls** si vous voulez choisir les appliances dont les licences doivent être mises à jour ou **Tous les firewalls activés** si vous voulez mettre à jour les licences de tous les appliances actifs (ceux dont l'état est à ON dans la vue générale).

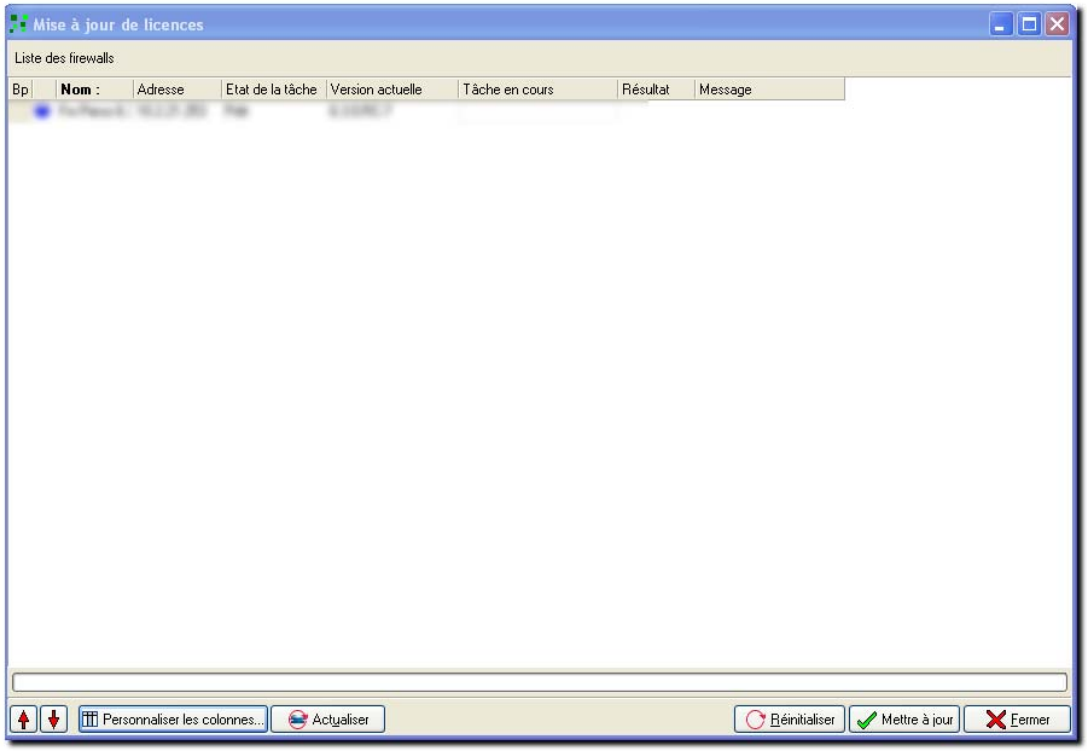


Figure 517 : Mise à jour de licences

Pour retirer un appliance de la liste, sélectionnez celui-ci et cliquez avec le bouton droit de la souris, choisissez alors l'option "Supprimer".

AVERTISSEMENT

Pour que les mises à jour de licences puissent être effectuées, il faut que les informations concernant les boîtiers UTM NETASQ choisis aient été mises à jour (au moyen du bouton **Mettre à jour les informations** de la vue générale).

Mettre à jour les licences des appliances

Cliquez sur le bouton **Mettre à jour.** Le voyant lumineux passe alors en orange sur les appliances en cours de mise à jour de licence et vous pouvez voir la barre de progression avancer. Les licences de tous les appliances seront alors mises à jour les unes après les autres.

20.3.5.5. Sauvegarder la partition

Cette fonctionnalité permet de réaliser à distance une sauvegarde du système complet, à partir de la partition principale (partition active) sur la partition de backup. Ainsi, en cas de problème, sur la partition active, il sera possible de démarrer le système en utilisant une partition de backup à jour. Il est fortement recommandé d'effectuer une sauvegarde après chaque mise à jour du firmware.

En sélectionnant le menu **`Tâches administratives\Sauvegarder la partition`**, la fenêtre suivante s'affiche :

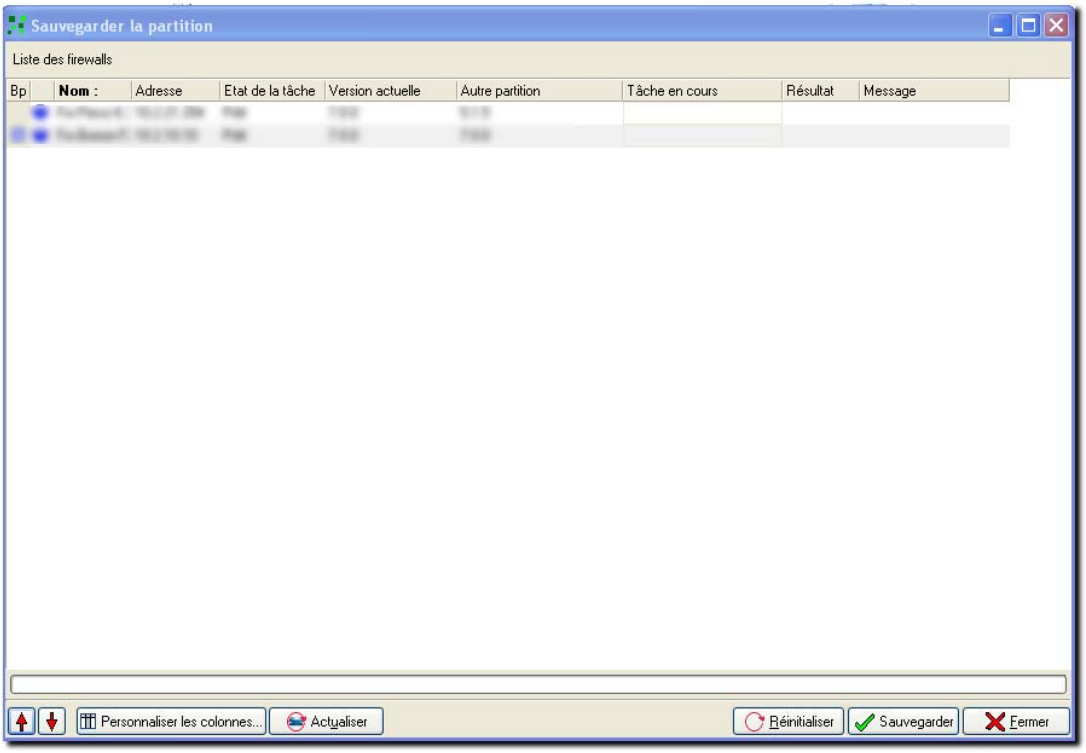


Figure 518 : Sauvegarde de la partition

Par défaut la première colonne, intitulée "Bp", permet de spécifier des points d'arrêt dans l'exécution de la tâche configurée. Le principe est le suivant : en spécifiant un point d'arrêt sur une ligne, la tâche configurée sera d'abord réalisée sur tous les appliances situés au dessus et sur ce point d'arrêt dans le tableau puis si toutes les tâches sont un succès, le mode Global Administration NETASQ effectuera les tâches pour les appliances qui suivent. Pour spécifier un point d'arrêt, faites un double clic sur la ligne voulue. Pour retirer le point d'arrêt, faites un double clic sur le point d'arrêt.

Par défaut, dans la deuxième colonne du tableau est affiché un voyant lumineux. La couleur donnée au voyant dépend de l'état de l'action :

	En attente
	Action commencée
	Action annulée ou non réalisée
	Action terminée avec succès

Ensuite, le tableau est composé des colonnes suivantes :

Nom	Nom choisi pour l'appliance.
Adresse	Adresse IP de l'appliance.
Etat de la tâche	Etat de l'action (en attente, commencée, terminée…).
Version actuelle	Version du firmware de la partition active de l'appliance.
Autre partition	Versions du firmware de la partition de backup de l'appliance.
Tâche en cours	Progression de la tâche.
Résultat	Résultat de la tâche de sauvegarde.
Message	Message d'explication en relation avec le champ "Résultat".

20.3.6. Scripts

Le "mode Global Administration" permet le déploiement et l'exécution de scripts formatés selon le mode de configuration NSRPC. Ce mode permet la configuration complète des appliances NETASQ. Ainsi les scripts offrent une solution de déploiement d'une configuration d'un parc complet de boîtiers UTM NETASQ pour des fonctionnalités non prévues dans les menus de déploiement du "mode Global Administration".

En sélectionnant le menu **`Tâches administratives\Scripts`**, la fenêtre suivante s'affiche :

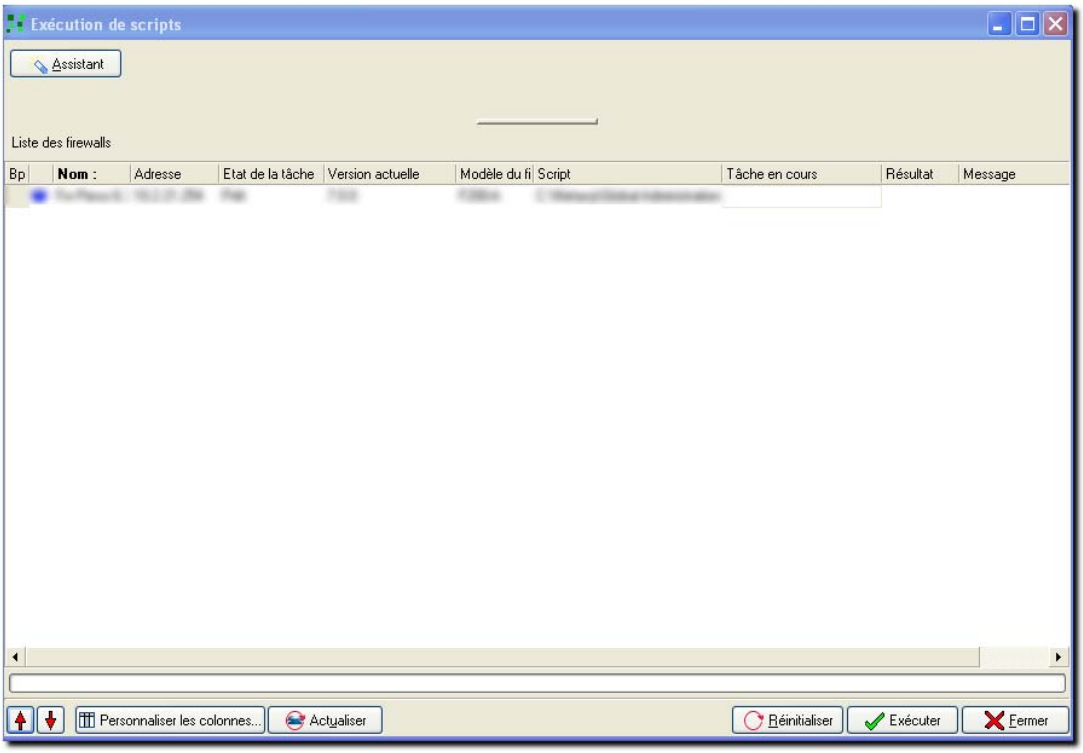


Figure 519 : Exécution de scripts

Etape 1

Figure 520 : Assistant de script - Etape 1

La première étape de l'assistant de déploiement des scripts nécessite de définir le script qui doit être déployé puis exécuté. Choisissez donc le script à exécuter sur les firewalls puis cliquez sur **Suivant**.

Etape 2

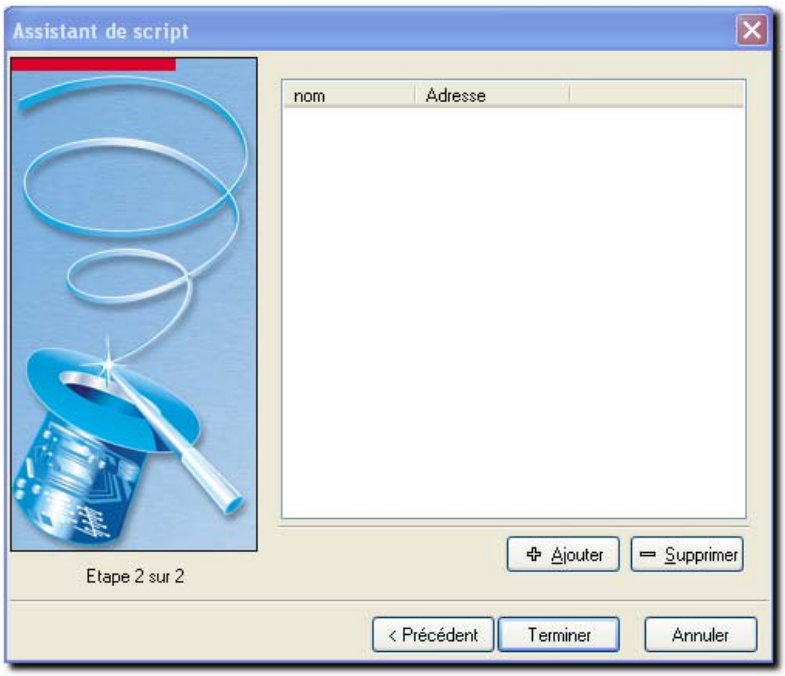


Figure 521 : Assistant de script - Etape 2

La deuxième étape de l'assistant de déploiement des scripts nécessite de définir les appliances concernés par ce déploiement. Pour cela cliquez sur **Ajouter** pour faire la fenêtre des appliances disponibles. Enfin cliquez sur **Terminer**, la fenêtre de déploiement et d'exécution des scripts apparaît

20.3.6.1. Exécuter le script sur les firewalls

Cliquez sur le bouton **Exécuter**. Le voyant lumineux passe alors en orange sur les appliances en cours de sauvegarde et vous pouvez voir la barre de progression avancer. Toutes les partitions principales seront alors sauvegardées les unes après les autres.

20.3.6.2. Construire un script

Les scripts sont formatés sous la forme de commandes NSRPC regroupées au sein d'un fichier qui sera spécifié lors de l'assistant de déploiement des scripts. Référez-vous à la documentation associée disponible sur le site Web NETASQ pour plus d'informations sur ce mode de configuration NSRPC.

> **AVERTISSEMENT**
> Toute commande ayant un résultat négatif interrompt l'exécution du script.

Les commandes NSRPC peuvent être associées à des MACROS ou variables qui vont faciliter le déploiement massif des scripts définis.

Les commentaires

Il est possible d'insérer des commentaires entre les différentes lignes de script. Les commentaires sont commencés par le caractère #.

Les macros

Les macros représentent des variables associées à l'appliance sur lequel le script est déployé. Pour être interprétée, la MACRO doit être encadrée par le caractère %, exemple %MACRO%.

Les MACROS pouvant être utilisées dans les scripts sont les suivantes.

> **AVERTISSEMENT**
> Les MACROS sont sensibles à la casse.

- **APP_PAT** : Chemin complet du dossier l'application "path delimiter" inclus.
- **FW_ADDRESS** : Champ adresse IP du firewall.
- **FW_COMPANY** : Champ société du firewall.
- **FW_COUNTRY** : Champ pays du firewall.
- **FW_DESCRIPTION** : Champ description du firewall.
- **FW_LOCATION** : Champ société du firewall.
- **FW_MODEL** : Modèle de firewall.
- **FW_NAME** : Nom du firewall.
- **FW_SERIAL** : Numéro de série du firewall.
- **FW_VERSION** : Nom de la version du firewall.
- **FW_ZIP_CODE** : Champs pays du firewall.
- **FW_CITY** : Champ ville du firewall.
- **FW_CUSTOM1** : Champ personnalisé numéro 1.
- **FW_CUSTOM2** : Champ personnalisé numéro 2.
- **FW_CUSTOM3** : Champ personnalisé numéro 3.
- **NOW** : Date complète au format local.

- **NOW_AS_DATE** : Date au format local.
- **NOW_AS_TIME** : Heure au format local.
- **SCRIPT_PATH** : Chemin complet du dossier de script "path delimiter" inclus.
- **ADMIN_LASTNAME** : Nom de famille de l'administrateur.
- **ADMIN_FIRSTNAME** : Prénom de l'administrateur.
- **ADMIN_EMAIL** : Adresse mail de l'administrateur.

Les fonctions

Certaines fonctions non définies dans les commandes NSRPC doivent être utilisées pour les actions de sauvegardes et restauration par exemple. Ces fonctions commencent par le caractère $ et sont sensibles à la casse :

La syntaxe d'utilisation de ces fonctions est alors la suivante : $FONCTION(« chemin_du_fichier »). Notez que les guillemets derrière la parenthèse ouvrante et devant la parenthèse fermante sont obligatoires.

Les fonctions sont les suivantes :

- **SAVE_TO_DATA_FILE** : Sauvegarde d'un fichier sans traitement Unicode.
- **SAVE_TO_TEXT_FILE** : Sauvegarde d'un fichier avec traitement Unicode.
- **FROM_DATA_FILE** : Lecture d'un fichier sans traitement Unicode.
- **FROM_TEXT_FILE** : Lecture d'un fichier avec traitement Unicode.

Les fonctions *_DATA_FILE seront plutôt utilisés pour des fichiers du type *.na tandis que les fonctions *_TEXT_FILE seront utilisés pour les fichiers de slot par exemple.

> **AVERTISSEMENT**
> Les noms des fichiers doivent respecter les contraintes de l'O.S. Sous Windows, un nom de fichier ne peut contenir /, :, *, ?, ", <, >, |.

Exemple

Confirmation
Ci-dessous sont présentés quelques exemples de script :

```
#Sauvegarde de la configuration
CONFIG BACKUP list=all $SAVE_TO_DATA_FILE("%APP_PATH%%FW_NAME%\all.na")

#Restauration des règles de filtrage du 16/12/2005
CONFIG RESTORE list=filter $FROM_DATA_FILE("%APP_PATH%16_12_2005\all.na")

#Activation des règles de filtrage 05
CONFIG SLOT ACTIVATE type=filter config=5
```

20.3.7. Déploiement

Grâce à ce menu on accède à tous les écrans permettant le déploiement des politiques de sécurité et des bases d'objets. Le mode Global Administration NETASQ permet le déploiement des politiques et bases suivantes :

Objets	Déploiement de la configuration des objets.
Prévention d'intrusion	Déploiement de la configuration du noyau ASQ.
QoS	Déploiement des règles de QoS.
Translation d'adresses (NAT)…	Déploiement de la configuration des politiques de translation.
Filtrage…	Déploiement de la configuration des politiques de filtrage.
Filtrage global…	Déploiement de la configuration des politiques de filtrage global. Il est similaire au filtrage classique sauf qu'il est prioritaire sur ce dernier dans le déroulement exécutif du filtrage. Un paquet réseau qui passera par le firewall appliquera les règles établies d'abord dans le filtrage global plutôt que d'appliquer éventuellement celles du filtrage local.
Filtrage d'URL…	Déploiement de la configuration des politiques de filtrage d'URL.

Pour obtenir la description des fonctionnalités de déploiement du mode "Global Administration" NETASQ, *référez-vous à la section Partie 20/Chapitre 3 : Déploiement*.

20.3.8. Monitoring et supervision

Le mode "Global Administration" de NETASQ offre aussi des outils de monitoring et de supervision de votre parc d'appliances permettant d'avoir une vision globale de l'état de fonctionnement des équipements installés. Pour monitorer et superviser votre parc, utilisez la vue topologique et sa zone de visualisation de topologies.

20.3.8.1. Moniteur

Le mode "Global Administration" NETASQ offre un petit outil assurant le monitoring des appliances en tâche de fond. Lorsque cet outil est actif, l'icône suivante est visible dans le coin en bas à gauche de la fenêtre principale . Le moniteur permet de mettre à jour de façon automatique les informations, les indicateurs et les états de fonctionnement (représentés par un voyant dans le cadre de l'objet pour la vue topologique) relatifs aux appliances. L'outil est actif par défaut.

AVERTISSEMENT
Lors des opérations d'administration, il est vivement conseillé de désactiver le moniteur du mode "Global Administration" NETASQ.

Pour le désactiver ou le réactiver, cliquez avec le bouton droit de la souris sur l'icône .

20.3.8.2. Vérification de l'état de fonctionnement des équipements

Vérification globale

La vue topologique permet de vérifier l'état de fonctionnement de tous les équipements de la zone de visualisation. Pour lancer cet outil, cliquez sur le bouton **Vérifier tous**. Un témoin d'état (voyant coloré) apparaît alors dans le coin haut et gauche de certains objets de la vue (tous les objets pour lesquels une adresse IP a été définie).

Ce voyant peut prendre les couleurs et formes suivantes :

	En cours de vérification de l'état de l'équipement
	Vérification terminée – équipement en fonctionnement
	Vérification terminée – équipement non fonctionnel ou non accessible

Le mode "Global Administration" NETASQ réalise un ping sur tous les équipements de la vue pour lesquels une adresse IP a été définie.

> **AVERTISSEMENT**
> Si certains équipements se trouvent derrière un équipement filtrant, il est possible que ceux-ci soient vus par le mode "Global Administration" NETASQ comme non fonctionnels alors qu'ils fonctionnent tout à fait correctement. De même si l'équipement ne répond pas aux commandes ICMP, il sera vu comme non fonctionnel. Pour une utilisation efficace du mode "Global Administration" NETASQ, assurez-vous qu'aucun équipement ne filtre les requêtes ICMP provenant de la station d'administration du mode "Global Administration" NETASQ et que les équipements sont bien configurés pour répondre aux requêtes ICMP.

Le rafraîchissement des témoins d'état des appliances est réalisé de façon automatique lorsque le moniteur du mode "Global Administration" NETASQ est actif.

Vérification individuelle

Il est aussi possible de vérifier l'état de fonctionnement de chaque appliance ou équipement de manière individuelle. Cette opération peut se réaliser sur les vues générale et topologique pour les appliances et uniquement sur la vue topologique pour les autres équipements.

Pour cela, sélectionnez le ou les équipements désirés et cliquez avec le bouton droit de la souris. Choisissez l'option "Disponibilité (ping)" dans le menu contextuel qui s'affiche et la fenêtre suivante s'ouvre (pour les appliances l'Administration globale NETASQ réalise une tentative de connexion au serverd et pour les autres objets un ping) :

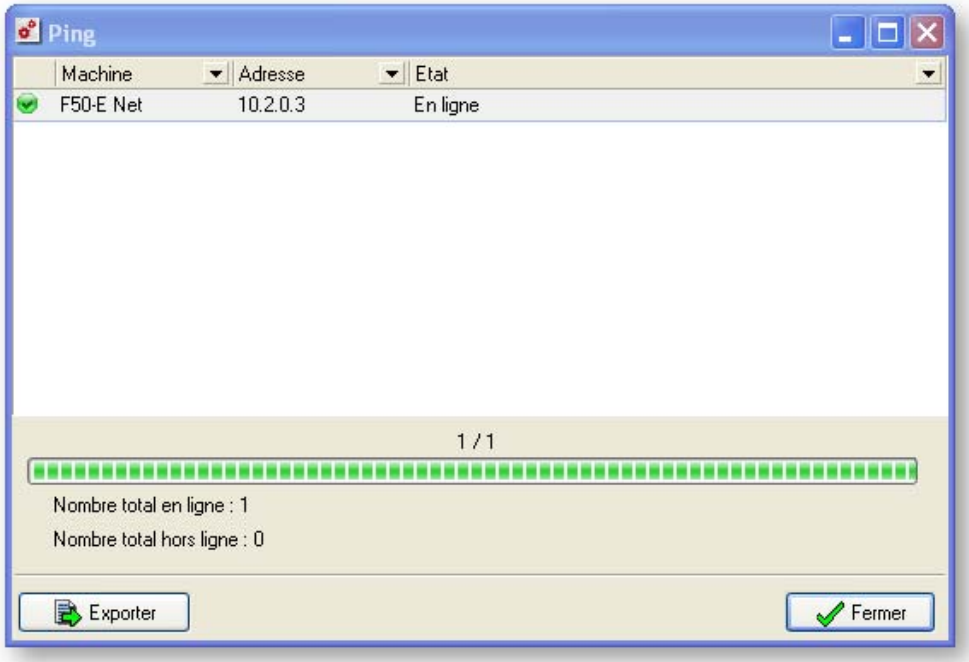


Figure 522 : Ping

Plusieurs informations sont alors visibles :

Voyant – témoin d'état	Le voyant change de couleur en fonction de l'état de l'opération : Bleu pour opération en cours, vert pour opération réussie, orange pour opération échouée.
Machine	Nom attribué à l'équipement testé.
Adresse	Adresse de l'équipement testé.
Etat	Message d'explication de l'état de fonctionnement.
Barre de progression	Barre de progression de l'opération.
Nombre total en ligne	Nombre total d'équipements fonctionnels.
Nombre total hors ligne	Nombre total d'équipements non fonctionnels ou inaccessibles.
Exporter	Exporter le tableau de résultat au format .txt.

Les informations du tableau peuvent être triées en cliquant sur le titre de la colonne que vous souhaitez utiliser pour faire le tri. Il est aussi possible de filtrer les lignes en cliquant sur la petite flèche noire à droite du titre de la colonne sur laquelle vous souhaitez placer le filtre et en choisissant le critère de filtre dans la liste déroulante qui s'affiche.

AVERTISSEMENT

Si certains équipements se trouvent derrière un équipement filtrant, il est possible que ceux-ci soient vus par le mode "Global Administration" NETASQ comme non fonctionnels alors qu'ils fonctionnent tout à fait correctement. De même si l'équipement ne répond pas aux commandes ICMP, il sera vu comme non fonctionnel. Pour une utilisation efficace du mode "Global Administration" NETASQ, assurez-vous qu'aucun équipement ne filtre les requêtes ICMP provenant de la station d'administration du mode "Global Administration" NETASQ et que les équipements sont bien configurés pour répondre aux requêtes ICMP.

20.3.8.3. Affichage des indicateurs

Pour afficher les indicateurs d'un firewall, placez le curseur de la souris au-dessus du celui-ci dans la zone de visualisation de la vue topologique.

Une fenêtre similaire s'affiche alors :

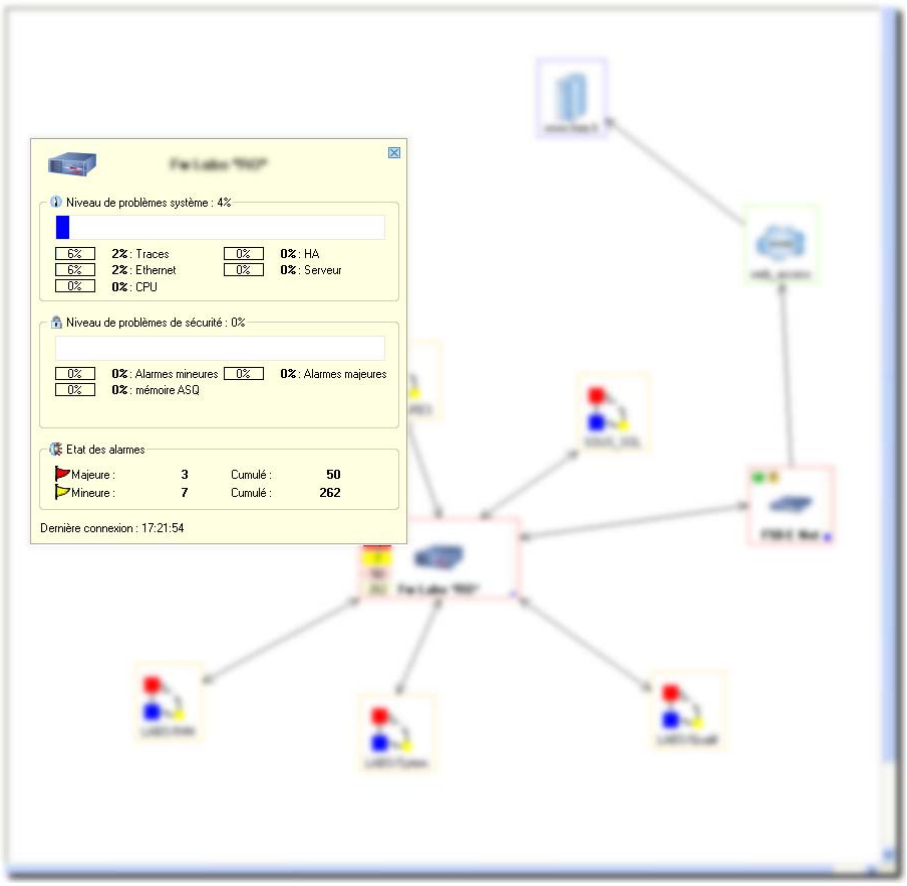


Figure 523 : Indicateurs

Cette fenêtre présente les informations suivantes :

- Une représentation graphique du type firewall, le nom du firewall concerné.
- Deux jauges qui représentent les indicateurs. La jauge Système représente l'indicateur Système. La jauge Sécurité représente l'indicateur Sécurité. Plus la jauge a une valeur élevée, plus la situation est critique pour ce firewall.
- Les valeurs des informations utilisées pour calculer les deux indicateurs.

20.3.8.4. Administration Suite

Les logiciels de la Suite d'Administration NETASQ peuvent être utilisés pour faciliter la supervision et le monitoring du parc d'appliances. Ainsi, il est possible de se connecter directement avec un de ces logiciels sur l'appliance voulu.

Les outils de la Suite d'Administration ont les fonctions suivantes :

NETASQ UNIFIED MANAGER	Permet l'administration et la définition des politiques de sécurité.
NETASQ REAL-TIME MONITOR	Permet la supervision en temps réel.
NETASQ EVENT-REPORTER	Permet l'analyse des traces.

Lancer NETASQ REAL-TIME MONITOR et NETASQ EVENT REPORTER

Pour superviser et monitorer le parc d'appliances, les outils NETASQ REAL-TIME MONITOR et NETASQ EVENT REPORTER sont indispensables. NETASQ REAL-TIME MONITOR permet en effet de superviser en temps réel l'activité des appliances (débit, connexions, utilisateurs authentifiés, tunnels VPN, utilisation des ressources système, remontées d'alarmes…). NETASQ EVENT REPORTER permet de visualiser les traces remontées par l'appliance et de réaliser des analyses sur ceux-ci (analyses graphiques, édition de filtres, regroupements arborescents…).

Pour lancer NETASQ-REAL-TIME, sélectionnez le firewall que vous désirez superviser dans la vue générale ou la vue topologique puis réalisez un clic avec le bouton droit de la souris et choisissez l'option **Outils\Exécuter NETASQ REAL-TIME MONITOR** dans le menu contextuel qui s'affiche. Le lien sera grisé si NETASQ REAL-TIME MONITOR n'a pas été lancé au moins une fois auparavant.

Si le chemin vers NETASQ REAL-TIME MONITOR n'a pas été défini pour la version logicielle de l'appliance ou si la version logicielle est inconnue, une aide vous permet de choisir le Monitor adéquat.

La connexion au logiciel se réalise de manière automatique (aucun besoin de saisir un mot de passe, une adresse IP ou un login). Vous pouvez alors monitorer le firewall. Plusieurs fenêtres du NETASQ REAL-TIME MONITOR peuvent être ouvertes, connectées sur des firewalls différents.

Pour lancer le NETASQ EVENT REPORTER, sélectionnez l'appliance que vous désirez consulter dans la vue générale ou la vue topologique puis réalisez un clic avec le bouton droit de la souris et choisissez l'option Outils\Exécuter NETASQ EVENT REPORTER dans le menu contextuel qui s'affiche. Le lien sera grisé si le firewall n'a pas été lancé au moins une fois auparavant ou si l'appliance concerné est un U30, U70 ou un Vbox Agency.

Si le chemin vers NETASQ EVENT REPORTER n'a pas été défini pour la version logicielle de l'appliance ou si la version logicielle est inconnue, une aide vous permet de choisir le Reporter adéquat.

La connexion au logiciel se réalise de manière automatique (aucun besoin de saisir un mot de passe, une adresse IP ou un login). Vous pouvez alors consulter les traces du firewall. Plusieurs fenêtres du NETASQ EVENT REPORTER peuvent être ouvertes, connectées sur des firewalls différents.

AVERTISSEMENT

Le NETASQ EVENT REPORTER n'est jamais accessible via le mode "Global Administration" NETASQ pour les appliances U30, U70 et Vbox Agency. Le lien est donc toujours grisé pour ces appliances.

20.3.9. Monitoring de la configuration

La modification de la configuration d'un appliance de sécurité est une des tâches d'administration les plus sensibles. En effet, l'appliance, situé au cœur de l'infrastructure, agit comme une clef de voûte pour l'ensemble de l'architecture réseau. Chaque modification peut engendrer des erreurs qui se révèlent parfois catastrophiques pour la stabilité du réseau et à fortiori pour la productivité de l'entreprise. Ainsi les différentes étapes de cette modification sont mesurées, action par action, option par option.

La **version 6.3 des appliances NETASQ** fournit un outil de différenciation de configurations. Grâce à cette fonctionnalité, l'administrateur peut qualifier une configuration qu'il utilisera comme point de comparaison lors de chaque modification.

20.3.9.1. Principe de fonctionnement

Le mode Global Administration va établir un modèle de comparaison de configuration à partir d'une sauvegarde de configuration dite "validée". Cette configuration validée est alors constamment comparée à la configuration effective sur l'appliance surveillé. Dès qu'une différence est détectée entre les deux configurations, le mode Global administration l'indique par l'intermédiaire d'identifiants visuels. Dès lors que l'administrateur est averti de cette modification, il peut visualiser les différences apportées grâce aux menus du mode Global Administration en association avec un logiciel de comparaison de fichiers.

20.3.9.2. Mise en place du monitoring de configuration

Etape 1 : Activation du monitoring de configuration

Activez le monitoring de la configuration en cochant l'option **Utiliser la supervision de configuration**. (Cf. *Partie 20/Chapitre 3 : Supervision de configuration* pour plus d'informations sur les paramètres disponibles dans ce menu).

Etape 2 : Mise en fonction du Moniteur

Activer le moniteur du mode Global Administration NETASQ pour permettre une surveillance constante des appliances pour lesquels est mis en place le monitoring de configuration. *(Cf. Partie 20/Chapitre 3 :Supervision de configuration).*

Etape 3 : Sauvegarde et validation d'une configuration

La troisième étape de la mise en place du monitoring de configuration est la sauvegarde d'une configuration qui sera qualifiée de "validée". *(Cf. Projets Référez-vous à la section Administration puis Configuration du chapitre Manipulation des projets pour effectuer une sauvegarde de configuration)*. Lors de cette sauvegarde, l'option **Valider la configuration** doit être cochée.

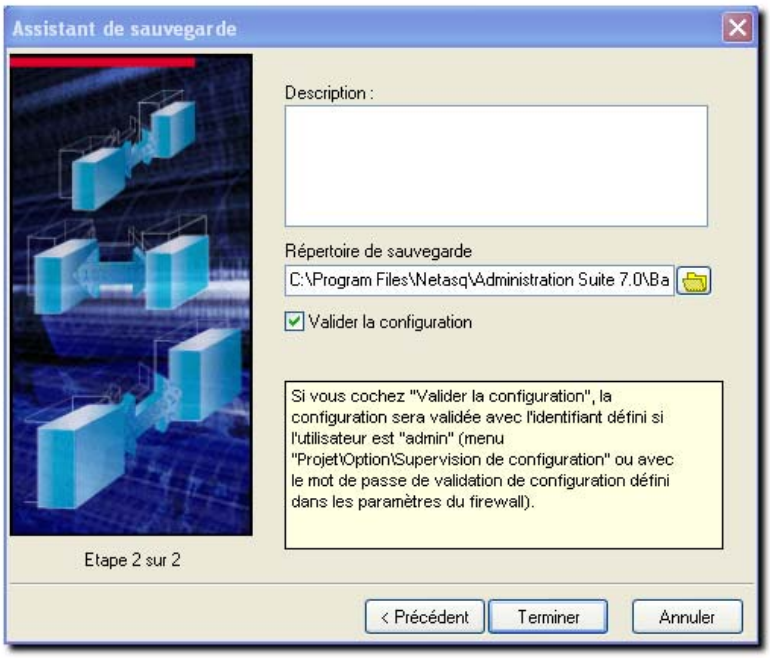


Figure 524 : Assistant de sauvegarde - Etape 2

Lorsque la sauvegarde de la configuration est effectuée, le monitoring de la configuration sauvegardée et validée est activé. Dès lors l'Administration globale vérifie les modifications apportées à cette configuration et prévient l'administrateur de tout changement apparu.

20.3.9.3. Détection de modifications sur une configuration surveillée

Indicateur de modification de la configuration "validée"

Dès qu'une modification est apportée sur une configuration surveillée par le monitoring de configuration, l'icône apparaît dans la vue topologique ou générale.

En cliquant sur le bouton droit de la souris sur l'appliance dont la configuration a été modifiée, le menu **`Voir les modifications`** apparaît. Cliquez sur ce menu pour visualiser les modifications apportées.

Voir les modifications

L'écran de modification affiche les modifications existantes entre les fichiers "Validés" et les fichiers présents sur l'appliance. Les modifications se présentent sous la forme de trois types, "Différences", "Ajout", "Suppression". "Différences" indique qu'un fichier présent dans les fichiers "Validés" et les fichiers présents sur l'appliance présente des différences. "Ajout" indique qu'un fichier qui n'existe pas dans les fichiers "Validés" a été ajouté. "Suppression" indique qu'un fichier qui existe dans les fichiers validés a été supprimé.

Comme évoqué plus avant, le monitoring de configuration se base sur une sauvegarde "Validée" pour prévenir l'administrateur des éventuelles modifications apportées à la configuration. Par défaut il s'agit de la sauvegarde la plus récente. Dans l'écran de comparaison, vous pouvez sélectionner une sauvegarde plus ancienne. De plus, il est possible de restaurer la configuration "Validée" si les modifications apportées ne conviennent pas à l'administrateur surveillant la configuration. Pour cela cliquez sur le bouton **Rétablir cette configuration** L'assistant de restauration démarre alors.

Outil de comparaison des fichiers

Pour visualiser le détail des modifications d'un fichier de configuration donné, sélectionnez la ligne indiquant la modification et cliquez ensuite sur le bouton  situé à droite de la sélection. L'outil de comparaison configuré est alors lancé, affichant les modifications les différences identifiées dans les fichiers.

20.3.10. Quitter le mode Global Administration

Pour quitter l'application du mode Global Administration NETASQ, sélectionnez le menu **`Fichier\Quitter`** ou cliquez sur le bouton de fermeture de la fenêtre (dans le coin haut-droit de la fenêtre du mode Global Administration NETASQ).

Si le projet en cours n'a pas été sauvegardé, une fenêtre de confirmation s'affichera vous demandant si vous désirez sauvegarder votre projet.

20.3.11. Configuration directe

20.3.11.1. Configuration directe

Les menus de "Configuration directe" du mode Global Administration NETASQ permettent l'accès rapide et direct à la configuration des firewalls sélectionnés (il n'est pas nécessaire de se réauthentifier sur le firewall sélectionné pour faire apparaître le menu de configuration).

Ces sections de configuration (**Prévention d'intrusion…**, **Réseau, Objets…, Qos…, Traces…, Translation d'adresses (NAT), Filtrage, Filtrage Global…, Filtrage URL…, VPN…**) sont spécifiques au firewall sélectionné dans le mode Global Administration NETASQ et en particulier la version du firmware installé.

L'accès à chacun des menus de "Configuration directe" s'effectue via les menus contextuels des vues générale et topologique :

1. Sélectionnez un appliance NETASQ.
2. Cliquez sur le bouton droit de la souris pour faire apparaître le menu contextuel associé à ce produit.
3. Sélectionnez la section "Configuration directe" de votre choix

20.3.12. Déploiement des configurations

20.3.12.1. Accès

La clé de voûte de la sécurité d'un système d'information est la politique de sécurité imaginée, conçue et mise en place par les administrateurs et responsables de la sécurité (confidentialité, intégrité et authenticité) des données et des ressources du système.

La politique de sécurité définie sur un modèle de fonctionnement théorique (et donc idéal) est fragilisée par le déséquilibre des versions des éléments réseau constituant le système d'information. S'assurer de l'homogénéité des systèmes se révèle être une brique indispensable pour réussir l'utilisation d'une politique de sécurité performante et efficace

Chaque jour, des outils d'administration centralisés aident les administrateurs à repérer les faiblesses (voire les failles) du système et à combattre leurs effets. Le mode Global Administration NETASQ va plus loin que ses concurrents en facilitant le déploiement des configurations homogènes sur toute la gamme des produits NETASQ.

S'appuyant sur le principe d'un modèle client/serveur, le mode Global Administration NETASQ permet de déployer les configurations (objets, noyau ASQ, Règles de QoS) ou slots (filtrage, filtrage global, translation, filtrage URL) sur tous les appliances NETASQ ("les clients") se trouvant sur le réseau à partir d'un firewall source ("le serveur").

Les fonctionnalités de déploiement sont accessibles de deux façons :

- Le menu contextuel dans les vues générale et topologique.
- Le menu **`Tâches administratives\Déploiement`** dans la fenêtre principale.

Menu contextuel

Cliquez sur un objet firewall NETASQ avec le bouton droit de la souris pour visualiser le menu contextuel des vues générale et topologique :

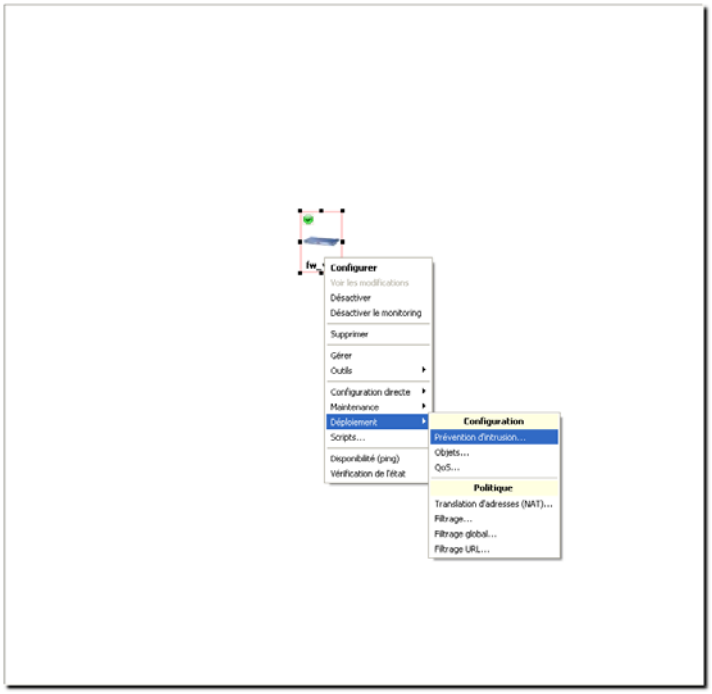


Figure 525 : Menu contextuel

20.3.12.2. Présentation générale des interfaces de déploiement

Les interfaces présentent à quelques exceptions près la même interface de configuration. La différence entre interface réside au niveau des options de déploiement.
L'interface de déploiement comporte 4 sections distinctes.

- Le firewall source ("le serveur")
- Le ou les firewall(s) destination ("les clients")
- La barre d'actions de l'écran de déploiement d'une base d'objets.
- Les options de déploiement.

Le firewall "Source"

Il s'agit d'abord de sélectionner un firewall. Pour ce faire, cliquez sur le bouton **Source.**

> **AVERTISSEMENT**
> Le message "Pas de client sélectionné" apparaît en rouge sous l'icône du bouton si aucun déploiement n'a encore été effectué à partir du projet actuellement ouvert. Sinon c'est le firewall sélectionné lors du dernier déploiement réalisé à partir du projet actuellement ouvert qui est indiqué par défaut.

Dans un premier temps, lorsque la fenêtre de sélection générale apparaît, sélectionnez le firewall depuis lequel vous désirez effectuer le déploiement (sa base d'objets sera déployée sur tous les firewalls destination sélectionnés) à l'aide du bouton situé dans la zone "Source".

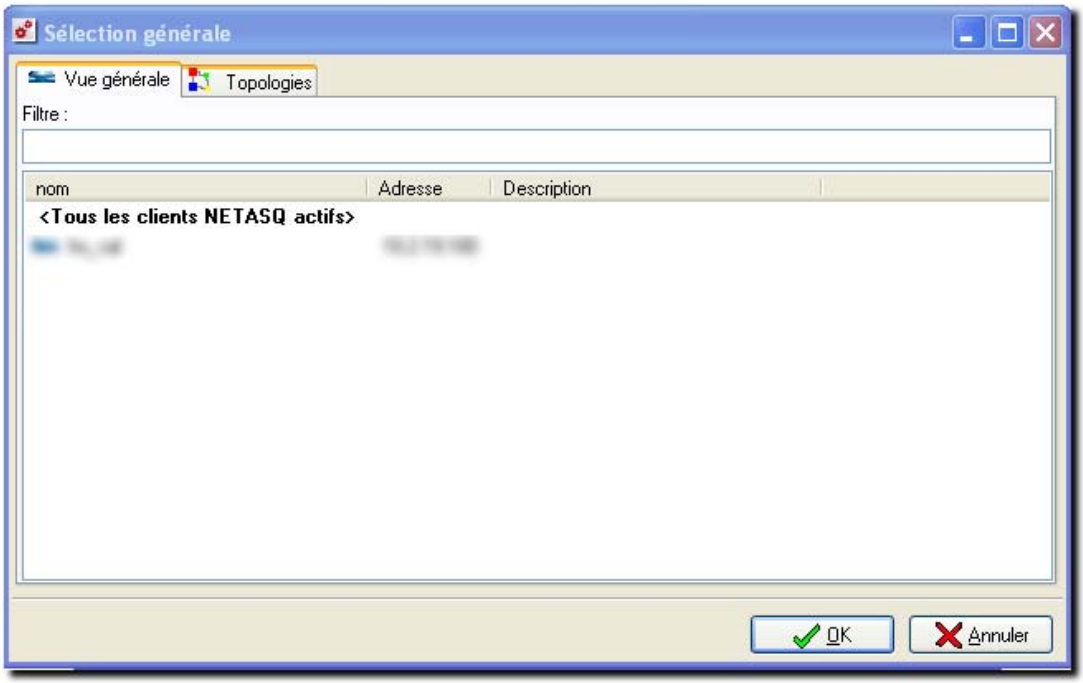


Figure 526 : Sélection générale - Vue générale

2 onglets permettent de rechercher un firewall : par Vue générale et par Topologies.
Il est également possible d'effectuer un filtre de recherche sur la colonne "Nom" pour retrouver facilement un firewall.

Les firewalls "Destination"

Les firewalls sélectionnés pour recevoir les bases d'objets du firewall source se présentent sous la forme d'une liste dans laquelle il est possible :

- D'ajouter un nouveau firewall : cliquez sur le bouton **Ajouter** et sélectionnez-le (maintenez la touche **Ctrl** appuyée et sélectionnez les firewalls désirés) ou tous les firewalls dans la liste des firewalls de l'écran de sélection générale. La sélection des firewalls destination est présentée selon le modèle de la vue générale dans l'onglet **Vue générale** (vous pouvez réaliser un filtre de recherche sur la colonne "Nom") ou selon le modèle de la vue topologique dans l'onglet **Topologies** (l'onglet **Topologies** n'apparaît que si des firewalls ont été définis dans une topologie).

De retirer un firewall de la liste des firewalls destination : sélectionnez-le (maintenez la touche **Ctrl** appuyée et sélectionnez les firewalls désirés) ou tous les firewalls dans la liste des firewalls destination et cliquez sur **Supprimer**.

> **AVERTISSEMENT**
> Le firewall sélectionné apparaît en rouge dans la liste des firewalls lorsque la version de celui-ci n'est pas approprié au firewall source (Il est impossible de réaliser un déploiement de configuration d'un firewall en version 7 vers un firewall version 6 ou inversement).

La barre d'actions

La barre d'actions du menu de déploiement des objets est constituée de deux boutons :

OK	Déployer la configuration des objets.
Annuler	Annuler les modifications.

Lorsque vous cliquez sur le bouton **OK** le déploiement des objets continue, et la fenêtre suivante apparaît :

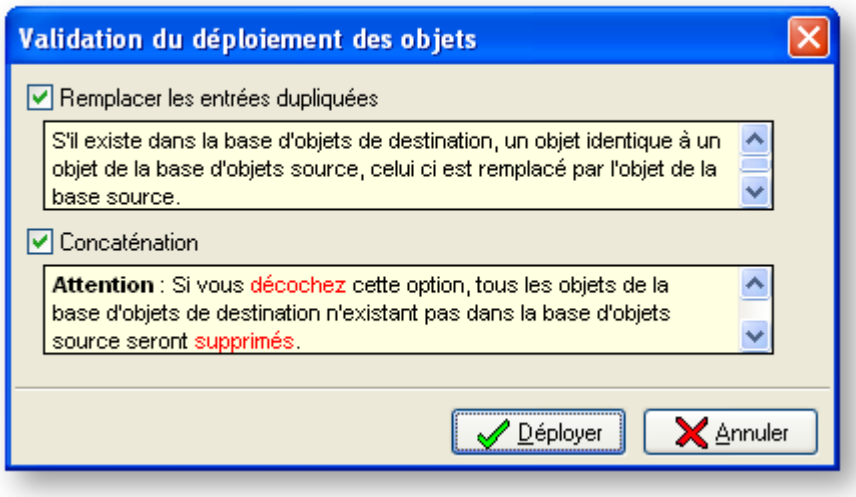


Figure 527 : Validation du déploiement des objets

Comme l'indique cet écran, il s'agit de définir deux options avant de continuer le déploiement du slot de filtrage du firewall source :

Remplacer les entrées dupliquées	Lorsque cette option est cochée, s'il existe dans la base d'objets de destination, un objet portant le même nom qu'un objet de la base d'objets source, la valeur de l'objet de la base de destination est remplacée par celle de l'objet de la base source.
Concaténation	**AVERTISSEMENT** Si vous décochez cette option, tous les objets de la base d'objets de destination n'existant pas dans la base d'objets source sont supprimés. Attention, cette option peut entraîner des disfonctionnements des règles utilisant les objets supprimés.
Déployer	En cliquant sur ce bouton, le mode Global Administration NETASQ entame le chargement de la base d'objets puis vous demande si vous désirez l'éditer avant de l'envoyer. Enfin un écran de déploiement apparaît vous permettant de lancer le déploiement.

20.3.12.3. Particularités des écrans de déploiement

Catégories d'objets

Les catégories sont utilisées dans le déploiement d'objets.

- Sélectionnez "Objets" si vous désirez déployer une base d'objets. La fenêtre suivante s'affiche :

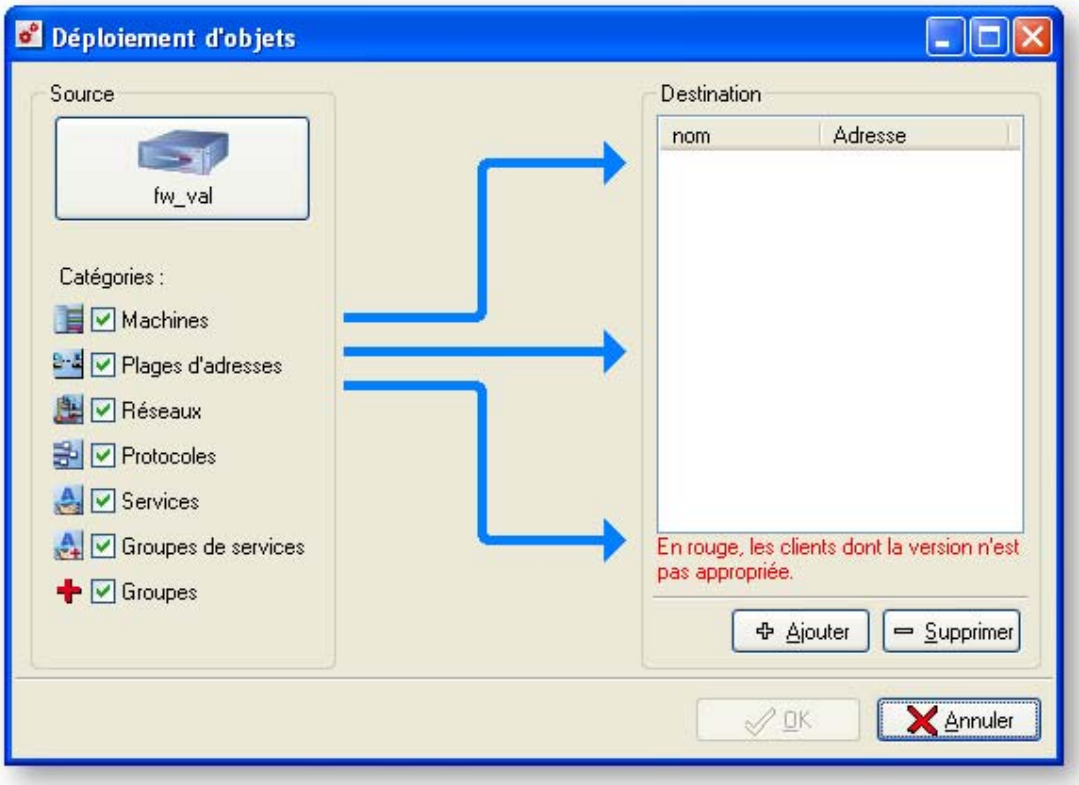


Figure 528 : Déploiement d'objets

Deux paramètres permettent la définition des options de données de source dans le menu de déploiement de configuration. Dans un premier temps, le choix de la source, dans un deuxième temps, sélectionnez les catégories qui seront envoyées aux firewalls destination. On trouve parmi ces catégories configurables : **Machines, Plages d'adresses, Réseaux, Protocoles, Services, Groupes de services, Groupes.**

Choix du profil pour la prévention d'intrusion

Le profil est utilisé au sein de la prévention d'intrusion (ASQ)

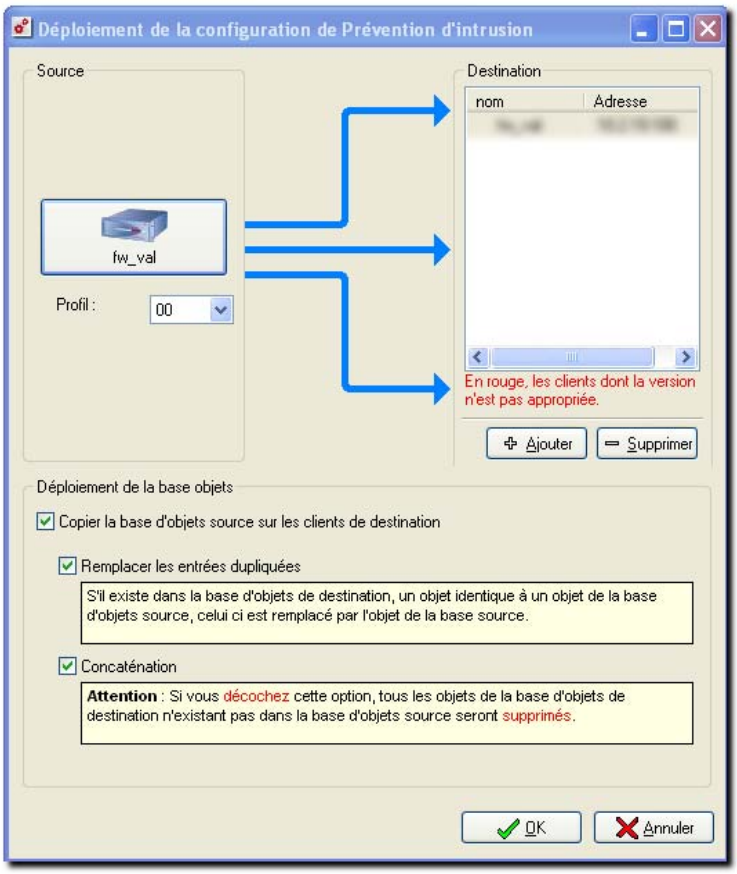


Figure 529 : Déploiement de la configuration de Prévention d'intrusion

Choisissez "Prévention d'intrusion", si vous désirez effectuer un déploiement de la configuration du noyau ASQ. L'écran suivant apparaît :

La liste déroulante vous permet de choisir un profil. Ce profil a été préalablement configuré en mode "Firewall Manager" dans le menu Prévention d'ntrusion.

Pour rappel, un profil contient tous les paramètres définis dans l'arborescence du menu **`Prévention d'intrusion`**.

Liste des éléments de la QoS

La liste est, pour ce déploiement, limitée à 253 éléments. En effet, si l'on sélectionne une nouvelle source, les nouvelles configurations de cette source remplacent les anciennes. Ce qui peut rendre la configuration du filtrage obsolète.

La liste est réduite afin de ne pas dépasser la capacité des firewalls.

20.3.12.4. Déploiement de la base objets

Copier la base objets source sur les clients de destination	Cette option active les options de déploiement de la base d'objets décrite ci-dessous. (Cette option s'applique pour les écrans de déploiement de prévention d'intrusion, Translation d'adresses (NAT)…, Filtrage, Filtrage global, Filtrage d'URL).
Remplacer les entrées dupliquées	Lorsque cette option est cochée, s'il existe dans la base d'objets de destination, un objet portant le même nom qu'un objet de la base d'objets source, la valeur de l'objet de la base de destination est remplacée par celle de l'objet de la base source. (Cette option s'applique pour les écrans de déploiement de prévention d'intrusion, Translation d'adresses (NAT)…, Filtrage, Filtrage global, Filtrage URL).
Concaténation	**AVERTISSEMENT** Si vous décochez cette option, tous les objets de la base d'objets de destination n'existant pas dans la base d'objets source sont supprimés. Attention, cette option peut entraîner des disfonctionnements des règles utilisant les objets supprimés. (Cette option s'applique pour les écrans de déploiement de la Prévention d'intrusion, Translation d'adresses (NAT), Filtrage, Filtrage global, Filtrage URL).
Uniquement les éléments utilisés	Lorsque cette option est cochée, seules les règles de QoS utilisées dans la politique de filtrage active sur le firewall source seront envoyées aux firewalls destination.

Lorsque vous cliquez sur le bouton **OK** pendant que le déploiement de la politique de filtrage continue, le mode "Global Administration" filtrage du firewall source et la fenêtre suivante apparaît :

20.3.12.5. Fenêtre de déploiement

Suite à la définition d'un déploiement (Objets, ASQ, Filtrage…) le mode "Global Administration" NETASQ affiche une fenêtre de déploiement. Cette fenêtre rappelle les firewalls sur lesquels le déploiement configuré va être effectué.

Un onglet correspondant à la fenêtre de déploiement actuellement ouverte apparaît dans le bas de l'écran.

En fonction du type de déploiement effectué, le titre de cet onglet change.

Grille de données

Dans la deuxième colonne du tableau (par défaut) est affiché un voyant lumineux. La couleur donnée au voyant dépend de l'état de l'action :

	En attente
	Action commencée
	Action annulée ou non réalisée
	Action terminée avec succès

Ensuite, le tableau est composé des colonnes suivantes :

BP	(*Breakpoint*) Point d'arrêt : les firewalls situés au-dessus de ce point d'arrêt sont mis à jour (le firewall situé sur la ligne de ce point d'arrêt est inclus dans ce groupe) avant les firewalls situés en dessous. Il faut que les résultats des opérations effectuées sur le premier groupe soit tous un succès pour entamer le deuxième groupe.
Nom	Nom choisi pour le firewall.
Adresse	Adresse IP du firewall.
Etat actuel	Etat de l'action (en attente, commencée, terminée…).
Version actuelle	Version du firmware du firewall.
Tâche en cours	Progression de la tâche.
Résultat	Résultat de la tâche de mise à jour.
Message	Message d'explication en relation avec le champ "résultat".

Certaines informations affichées ne vous sont pas forcément nécessaires et inversement, vous voulez peut-être afficher des informations qui vous sont utiles. Il est possible de masquer et d'afficher certaines colonnes du tableau. Pour cela, cliquez sur le bouton **Personnaliser les colonnes.** Une fenêtre similaire à la fenêtre suivante s'affiche :

Dans cette fenêtre, on trouve le nom des colonnes qui ne sont pas affichées mais qu'il est possible de rendre visibles. Pour afficher une colonne, sélectionnez avec le bouton gauche de la souris le nom de cette colonne et maintenez le bouton de la souris enfoncé. Ensuite, déplacez l'intitulé de la colonne jusqu'à l'endroit où vous désirez l'insérer dans la barre des titres de colonne puis relâchez le bouton de la souris.

Pour masquer une colonne, faîtes l'opération inverse : sélectionnez, dans la barre des titres de colonne, le nom de la colonne qu'il faut masquer, avec le bouton gauche de la souris. Maintenez le bouton gauche appuyé et déplacez le nom de la colonne jusqu'à la fenêtre "Personnalisation" puis relâchez le bouton.

La disposition des colonnes affichées peut être modifiée en utilisant le même mécanisme de "drag and drop". Il suffit de sélectionner une colonne et de la déplacer à l'endroit voulu.

Pour fermer la fenêtre "Personnalisation", cliquez sur la croix blanche en haut à droite de la fenêtre.

Déploiement des configurations sur les boîtiers UTM de destination

Trois boutons vous permettent de gérer le déploiement :

Reset	Retirez tous les firewalls destination du déploiement configuré.
Update All	Démarrez le déploiement.
Fermer	Fermez la fenêtre de déploiement. Cette action annule le déploiement.

AVERTISSEMENT
Le déploiement nécessite que les informations sur les firewalls destination soient mises à jour. Si cette mise à jour est annulée le déploiement n'est pas effectué sur le firewall non mis à jour.

ANNEXES

Annexe A : Droits de la session et droits des utilisateurs

Droits de la session :

- Base (B) : administration minimum, tous les accès indispensables à l'administration.
- Other (*) : gestion autre (actions diverses).
- Log (L) : accès aux fichiers de traces et à la function d'audit.
- Filter (F) : accès aux slots de filtrage.
- Vpn (V) : accès aux slots VPN, clés pré-partagées, certificat (VPN-Firewall).
- Url : accès aux politiques de filtrage d'URL.
- Pki : gestion de la PKI interne (émission, révocation…).
- Object (O) : ajout et suppression d'objets (de configuration du réseau).
- User (U) : gestion des utilisateurs.
- Admin (A) : super-administrateur (login "admin")
- Network (N) : gestion de la configuration réseau (interfaces, bridges, dialups, VLAN…)
- Route (R) : gestion du routage (route par défaut, routes statiques, réseaux de confiance).
- Maintenance (Ma) : accès aux opérations de maintenance.
- Asq (As) : consultation de la configuration du moteur stateful ASQ.
- Globalobject (GO) : ajout et suppression d'objets de la configuration globale.
- Globalfilter (GO) : accès aux slots de filtrage de la configuration globale.
- Globalother (G*) : gestion autre (actions diverses) de la configuration globale.
- SEISMO : gestion des vulnérabilités (consultation, modification).
- Ha : haute disponibilité (interne, interdit aux utilisateurs).

Droits de l'utilisateur :

- Modify (M) : modification des données de sécurité incluant la configuration.
- Base (B) : administration minimum, tous les accès indispensables à l'administration.
- Other (*) : gestion autre (actions diverses).
- Log (L) : accès aux fichiers de traces et à la function d'audit.
- Filter (F) : accès aux slots de filtrage.
- Vpn (V) : accès aux slots VPN, clés pré-partagées, certificat (VPN-Firewall).
- Url accès aux politiques de filtrage d'URL.
- Pki :gestion de la PKI interne (émission, révocation…).
- Object (O) : ajout et suppression d'objets (de configuration du réseau).
- User (U) : gestion des utilisateurs.
- Admin (A) : super-administrateur (login "admin")
- Network (N) : gestion de la configuration réseau (interfaces, bridges, dialups, VLAN…)
- Route (R) : gestion du routage (route par défaut, routes statiques, réseaux de confiance).
- Maintenance (Ma) : accès aux opérations de maintenance.
- Asq (As) : consultation de la configuration du moteur stateful ASQ.
- Globalobject (GO) : ajout et suppression d'objets de la configuration globale.
- Globalfilter (GO) : accès aux slots de filtrage de la configuration globale.
- Globalother (G*) : gestion autre (actions diverses) de la configuration globale.
- SEISMO : gestion des vulnérabilités (consultation, modification).
- Ha : haute disponibilité (interne, interdit aux utilisateurs).
- MW pour "Mon_Write" droits de modification sur le Moniteur uniquement.

Annexe B : Services TCP/IP

Dans cette annexe vous trouverez la liste de services TCP et UDP couramment utilisés tels que : FTP, Telnet, www, SMTP,...

Cette annexe vous est présentée sous la forme d'une liste composée de quatre colonnes :

- Une colonne contenant le nom du service.
- Une colonne contenant le numéro de port associé au service.
- Une colonne indiquant le protocole utilisé (TCP et/ou UDP).
- Une colonne contenant une description du service.

Nous vous conseillons de ne pas saisir tous ces services lorsque vous définissez la liste des objets, afin de ne pas surcharger votre affichage et de gagner en visibilité.

Service	Port	Protocole	Description
echo	7	TCP/UDP	Echo
discard	9	TCP	Discard
systat	11	TCP/UDP	Systat
daytime	13	TCP/UDP	Daytime
qotd	17	TCP/UDP	Quote of tThe Day
chargen	19	TCP/UDP	Character generator
ftp-data	20	TCP	File Transfer (Default Data)
ftp	21	TCP	File Transfer (Control)
telnet	23	TCP	Telnet
smtp	25	TCP	Simple Mail Transfer
time	37	TCP/UDP	
rip	39	UDP	Ressource Locator Protocol
nameserver	42	TCP/UDP	Host Name Server
nicname	43	TCP	
login	49	TCP/UDP	
domain	53	TCP/UDP	Domain Name Server (DNS)
Sql-net	66	TCP/UDP	Oracle SQL Net
bootps	67	UDP	Bootstrap Protocol Server
bootpc	68	UDP	Bootstrap Protocol Client
tftp	69	TCP/UDP	Trivial File Transfer
gopher	70	TCP	Gopher
finger	79	TCP	Finger
www	80	TCP	World Wide Web
kerberos	88	TCP/UDP	Kerberos
npp	92	TCP/UDP	Network Printng Protocol
hostname	101	TCP	NIC Host Name Server
Uucp-path	117	TCP	ISO-TSAP Class 0
sqlserv	118	TCP/UDP	SQL Services
nntp	119	TCP	Network News Trasfer Protocol
ntp	123	UDP	Network Time Protocol
epmap	135	TCP/UDP	Netbios Net Service
netbios-ns	137	TCP/UDP	DCE edpoint resolution
netbios-dgm	138	UDP	Netbios Datagram Service
netbios-ssn	139	TCP	Netbios session service
Imap2	143	TCP	Interim Mail Access Protocol version 2

sql-net	150	TCP/UDP	SQL-NET
snmp	161	UDP	Simple Network Management Protocol
snmptrap	162	UDP	SNMP trap
print-srv	170	TCP	
bgp	179	TCP	Border Gateway Protocol
irc	194	TCP	Internet Relay Chat Protocol
ipx	213	UDP	IPX over IP
imap3	220	TCP / UDP	Internet Message Access Protocol 3
ldap	389	TCP	Lightweight Directory Access Protocol
netware-ip	396	TCP / UDP	Novell Netware over IP
ups	401	TCP / UDP	Uninterruptible power Supply
smtpe	420	TCP / UDP	SMPTE
https	443	TCP / UDP	Https Mcom
microsoft ds	445	TCP / UDP	
kpasswd	464	TCP / UDP	Kerberos (v5)
isakmp	500	UDP	Internet Key Exchange
exec	512	TCP / UDP	Remote process execution
biff	512	TCP / UDP	Notify user of new mail received
login	513	TCP / UDP	Remote login
who	513	TCP / UDP	Who's logged in to machines
cmd	514	TCP / UDP	Remote exec
syslog	514	TCP / UDP	
printer	515	TCP	Spooler
talk	517	UDP	
ntalk	518	UDP	
router	520	TCP / UDP	Extended File Name Server
timed	525	UDP	Timeserver
tempo	526	TCP	
courier	530	TCP	
conference	531	TCP	
uucp	540	TCP	
klogin	543	TCP	Kerberos login
kshell	544	TCP	Kerberos remote shell
remotefs	556	TCP	Remote login using Kerberos
rmonitor	560	UDP	
rmonitor	561	UDP	
whoami	565	TCP / UDP	
ldaps	636	UDP	LDAP over TLS/SSL
Kerberos-adm	749	TCP / UDP	Kerberos administration
Kerberos-iv	750	UDP	Kerberos version IV

Annexe C : Contrôle des saisies

Durant la configuration du firewall, vous êtes amené à saisir au clavier, différents types de données :

- Adresse IP.
- Commentaires.
- Nom de fichier.
- Nom d'objets (machine, réseau, service).

Chacun de ces types de données accepte un ensemble précis de caractères, ces caractères sont filtrés durant la saisie du paramètre.

Adresse IP

Les chiffres de 0 à 9 et le "." sont les seuls caractères gérés. Pour effacer un caractère, vous pouvez utiliser la touche **Backspace** ou **Suppr**.

Commentaires

Vous pouvez utiliser les moyens classiques de mouvement du curseur durant l'édition d'un commentaire (souris, flèches au clavier).

Nom de fichier

Vous pouvez utiliser les moyens classiques de mouvement du curseur durant l'édition d'un commentaire (souris, flèches au clavier).

Nom d'objets

Certains caractères comme les accents et les espaces ne sont pas gérés dans les noms d'objets. Durant l'édition d'un nom d'objet, quand un caractère accentué est saisi au clavier, le logiciel de configuration insère le caractère non accentué correspondant. Un caractère non géré n'est pas validé et n'apparaît pas à l'écran.

Vous pouvez utiliser les moyens classiques de mouvement du curseur durant l'édition d'un commentaire (souris, flèches au clavier).

Annexe D : Codes ICMP

Type	Code	Description	Requête	Erreur
0	0	echo reply	x	
3		Destination unreachable		x
	0	network unreachable		x
	1	host unreachable		x
	2	protocol unreachable		x
	3	port unreachable		x
	4	fragmentation needed but don't fragment bit set		x
	5	source route failed		x
	6	destination network unknown		x
	7	destination host unknown		x
	8	source host isolated (obsolete)		x
	9	destination network administratively prohibited		x
	10	destination host administratively prohibited		x
	11	network unreachable for TOS		x

	12	host unreachable for TOS		x
	1	communication administratively prohibited by filtering		x
	14	host precedence violation		x
	15	precedence cutoff in effect		x
4	0	source quench	x	
5		redirect :		
	0	redirect for network		x
	1	redirect for host		x
	2	redirect for type of service and network		x
	3	redirect for type of service and host		x
8	0	echo request	x	
9	0	routeur advertisement		x
10	0	routeur solicitation		x
11		time excedeed !		
	0	time tolive equals 0 during transit		x
	1	time to live equals 0 during reassembly		x
12		parameter problem :		
	0	IP header bad		x
	1	required option missing		x
13	0	timestamp request	x	
14	0	timestamp reply	x	
15	0	information request (obsolete)	x	
16	0	information reply (obsolete)	x	
17	0	address mask request	x	
18	0	address mask reply	x	

Annexe E : Exemples de translations d'adresses

Les exemples ci-dessous illustrent différentes configurations utilisant la translation d'adresses. Ils utilisent les différentes possibilités offertes suivant les besoins et l'architecture réseau, dans des cas volontairement simplifiés.

- Translation unidirectionnelle du réseau interne pour accès à l'Internet.
- Configuration avec un serveur Web dans la DMZ.
- Configuration avec un serveur web dans la DMZ qui doit être accessible du réseau interne et externe avec son adresse officielle.
- Connexion par modem sur le port série du firewall de l'accès Internet.
- Redirection de port : utilisation d'une seule adresse IP pour contacter plusieurs serveurs.
- Partage de charge : distribution des connexions sur un pool de serveurs.

Exemple 1 : translation unidirectionnelle d'une classe d'adresses

Le schéma ci-dessous donne un exemple de configuration de translation d'adresses unidirectionnelle de l'ensemble du réseau interne vers une adresse virtuelle sur le réseau externe.

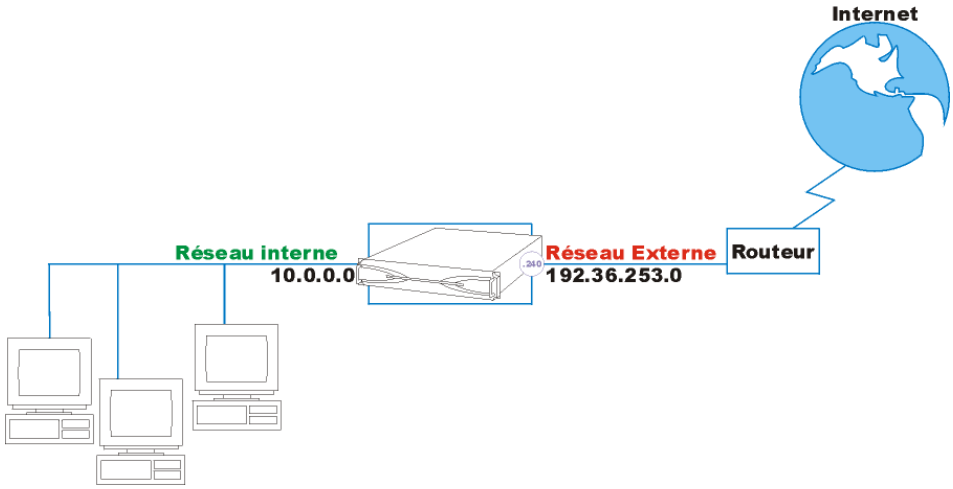


Figure 530 : Transaction unidirectionnelle

Au niveau du firewall, la configuration de la translation d'adresses correspondante est :

Statut	Action	Option	Original	Destination	Port destination	Translaté	Description
On	Map	Aucun	Ntwk_in	<Any>	<Any>	Firewall_out	

Typiquement, cette configuration permet à l'ensemble des postes se situant sur le réseau interne d'accéder à Internet.

Les machines sortent du réseau avec l'adresse virtuelle 192.36.253.240 et peuvent recevoir les réponses à leurs requêtes.

Il faut bien entendu que l'adresse virtuelle sur le réseau externe soit routable sur Internet (adresse officielle).

Cependant, les machines internes ne sont pas joignables de l'extérieur (unidirectionnelle); si une demande de connexion vers l'adresse 192.36.253.240 arrive au firewall, aucune translation d'adresses n'est effectuée vers une adresse d'une machine du réseau interne.

En passant en configuration avancée (bouton ), on remarque que cette règle translate les ports destination sur une plage appelée ephemeral_fw (port 20000 à 59999). Cela signifie que non seulement l'adresse source est translatée mais aussi le port source. Le firewall utilise un port disponible pour la translation dans cette plage, ce qui évite les conflits si deux machines du réseau interne utilisent le même port source.

Si vous désirez retirer une machine de l'opération de map (l'adresse IP de cette machine ne sera pas translatée), utilisez l'opération "no map".

L'exemple suivant montre comment retirer une machine de l'opération de map (les adresses IP spécifiées ne correspondent plus à l'exemple précédent) :

Statut	Action	Option	Original	Destination	Port destination	Translaté	Description
On	No map	Aucun	Client	<Any>	<Any>		
On	Map	Aucun	Network_bridge	<Any>	<Any>	Firewall_out	

Ici la machine "Client" ne sera pas mappée.

Exemple 2 : translation bidirectionnelle

L'exemple ci-dessous illustre une configuration dans laquelle figure un serveur Web dans la DMZ.

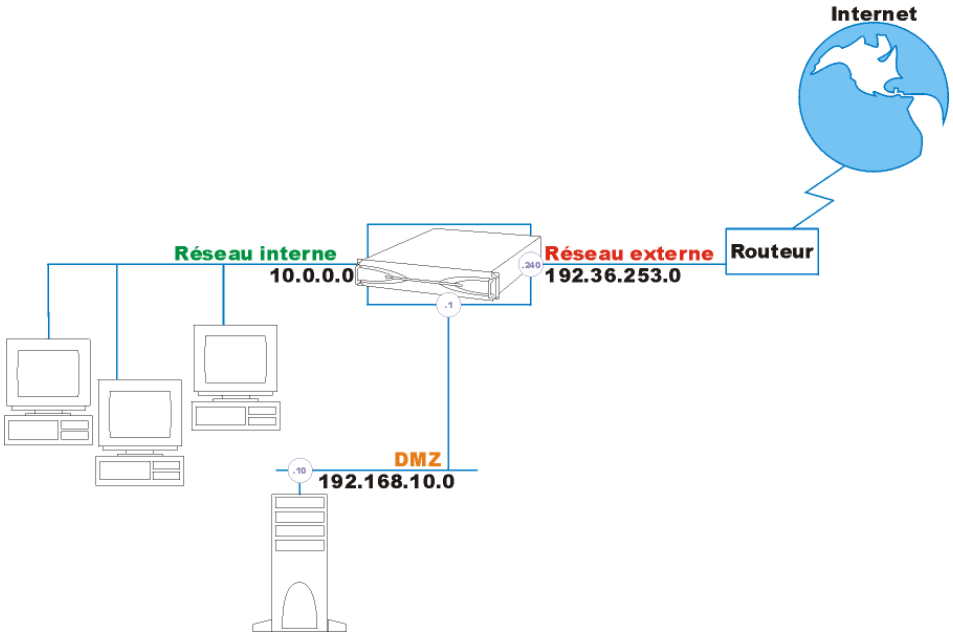


Figure 531 : Transaction bidirectionnelle

La configuration de la translation d'adresses sur le firewall doit être la suivante :

Statut	Action	Option	Original	Destination	Port destination	Translaté	Description
On	Map bidirectionnel	Aucun	Serveur_web_privé1	<Any>	<Any>	Serveur_web_public	

Avec la translation d'adresses bidirectionnelle, le serveur est accessible de l'extérieur. L'adresse utilisée à l'extérieur est l'adresse virtuelle, routable sur l'Internet.

Ainsi les requêtes provenant de l'extérieur (direction OUT) avec adresse de destination 192.36.253.10 sont changées en 192.168.10.10 et routées par le firewall vers la DMZ.

Exemple 3 : Accès à un serveur Web en DMZ

L'exemple ci-dessous illustre une configuration avec trois sous-réseaux (interne, externe et DMZ) et un serveur web dans la DMZ. On veut que le serveur web soit accessible de l'extérieur mais aussi à partir du réseau interne, avec son adresse officielle (virtuelle).

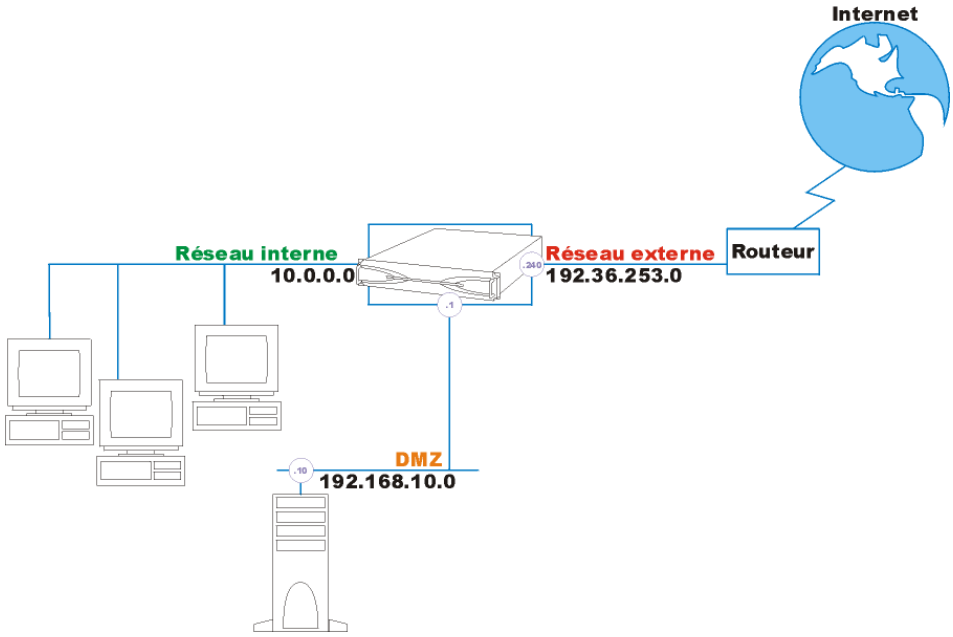


Figure 532 : Serveur Web en DMZ

Si un poste sur le réseau interne veut se connecter au serveur Web via son URL, la première chose effectuée est la résolution DNS.

Dans le cas où le serveur DNS est externe, il va renvoyer l'adresse virtuelle du serveur Web connu sur Internet (192.36.253.10). La machine envoie donc sa requête avec cette adresse en destination. La machine visée n'existant pas sur le réseau externe, la requête est envoyée sur l'Internet et se perd ou renvoie une erreur. Elle peut aussi être renvoyée par le routeur.

Il faut donc translater sur l'interface interne du firewall cette adresse virtuelle en l'adresse réelle du serveur dans la DMZ. On veut aussi que le serveur soit accessible depuis le réseau externe avec cette adresse virtuelle.

On a donc deux fois la même règle mais qui s'applique sur des interfaces différentes. Le choix de l'interface se fait en mode avancé (bouton ) Par défaut, le firewall choisit l'interface où se trouve l'adresse IP virtuelle (OUT dans l'exemple).

Statut	Interface	Action	Option	Original	Destination	Port destination	Translaté	Port translaté	Description
On	Out	Map bidirectionnel	Aucun	Serveur_web_privé1	<Any>	<Any>		Serveur_web_public	
On	in	Map bidirectionnel	Aucun	Serveur_web_privé1	<Any>	<Any>	Firewall_out	Serveur_web_public	

Ainsi les requêtes provenant de l'extérieur (Interface OUT) et du réseau interne (Interface IN) avec l'adresse de destination 192.36.253.10 sont changées en 192.168.10.10 et routées directement par le firewall vers la DMZ.

REMARQUES

1) L'ordre des règles est ici important. Il faut pour ce cas mettre en premier lieu la règle avec l'adresse IP virtuelle et l'interface réseau (direction) appartenant au même réseau. Dans notre exemple, l'adresse virtuelle appartient au réseau externe (OUT). Il faut donc mettre la règle avec comme direction l'interface OUT en premier.
2) Il n'est pas possible de contacter le serveur avec son adresse virtuelle si le client et le serveur sont réellement sur le même réseau. En effet, le message arrivera bien au serveur mais celui-ci

va répondre directement au client (car ils sont sur le même réseau) avec son adresse réelle. Le client reçoit alors la réponse avec une adresse différente de sa requête initiale et rejette le paquet.

Exemple 4 : connexion Internet par modem

Dans le cas d'une connexion modem, sur le port série ou l'interface externe du firewall NETASQ, il faut translater les adresses des machines internes voulant utiliser le modem.

On doit translater les adresses vers l'adresse firewall_dialup. Cette interface possède l'adresse IP (fixe ou non) négociée avec le provider lors de la demande de connexion.

Dans cet exemple, on veut donner accès au réseau interne à Internet via le modem installé sur le port série du boîtier :

Statut	Action	Option	Original	Destination	Port destination	Translaté	Description
On	Map	Aucun	Ntwk_in	<Any>	<Any>	Fwall_dialup	

Si vous fonctionnez en mode transparent vous devez mettre cette règle en place (en remplaçant l'objet *Network_in* par *Network ou Bridge*) pour pouvoir accéder à Internet avec votre modem.

Exemple 5 : Redirection de port

Dans le cas où on ne possède qu'une seule adresse IP publique et plusieurs serveurs publics, la redirection de port permet de rediriger les flux à destination de ces serveurs en fonction uniquement du numéro de port.

Exemple

L'entreprise A possède l'adresse IP publique 192.36.253.240. Elle héberge un serveur Web et un serveur Mail dans la DMZ.

Le firewall va rediriger le flux vers le bon serveur en fonction du numéro de port visé. Si la demande de connexion concerne le port 80 (HTTP), le firewall redirige vers le serveur Web. Si la demande de connexion est faite sur le port 25 (SMTP), le firewall redirige le flux vers le serveur mail.

Statut	Interface	Action	Option	Original	Destination	Port destination	Translaté	Port translaté
On	out	redirect	none	<Any>	Firewall_out	http	Web_Server	http
On	out	redirect	none	<Any>	Firewall_out	smtp	Mail_Server	smtp

REMARQUE
Il est possible de rediriger le flux vers un autre port de la machine destination.

Exemple 6 : Partage de charge

Certains serveurs sont physiquement répliqués sur plusieurs machines pour pouvoir répondre plus efficacement au nombre important de connexions arrivant sur ces serveurs.
Avec le firewall NETASQ, il est possible que ces serveurs soient accessibles avec une seule adresse IP. Le firewall va rediriger vers les serveurs les demandes de connexions à destination de l'adresse IP publique.

Une entreprise A possède par exemple un serveur web (www.netasq.com), installé physiquement sur plusieurs machines dans la DMZ. La résolution DNS renvoie pour le site www.netasq.com, l'adresse IP 192.36.253.10.

On va créer un groupe de machines avec les adresses IP physiques des serveurs et donner une règle de translation au firewall.

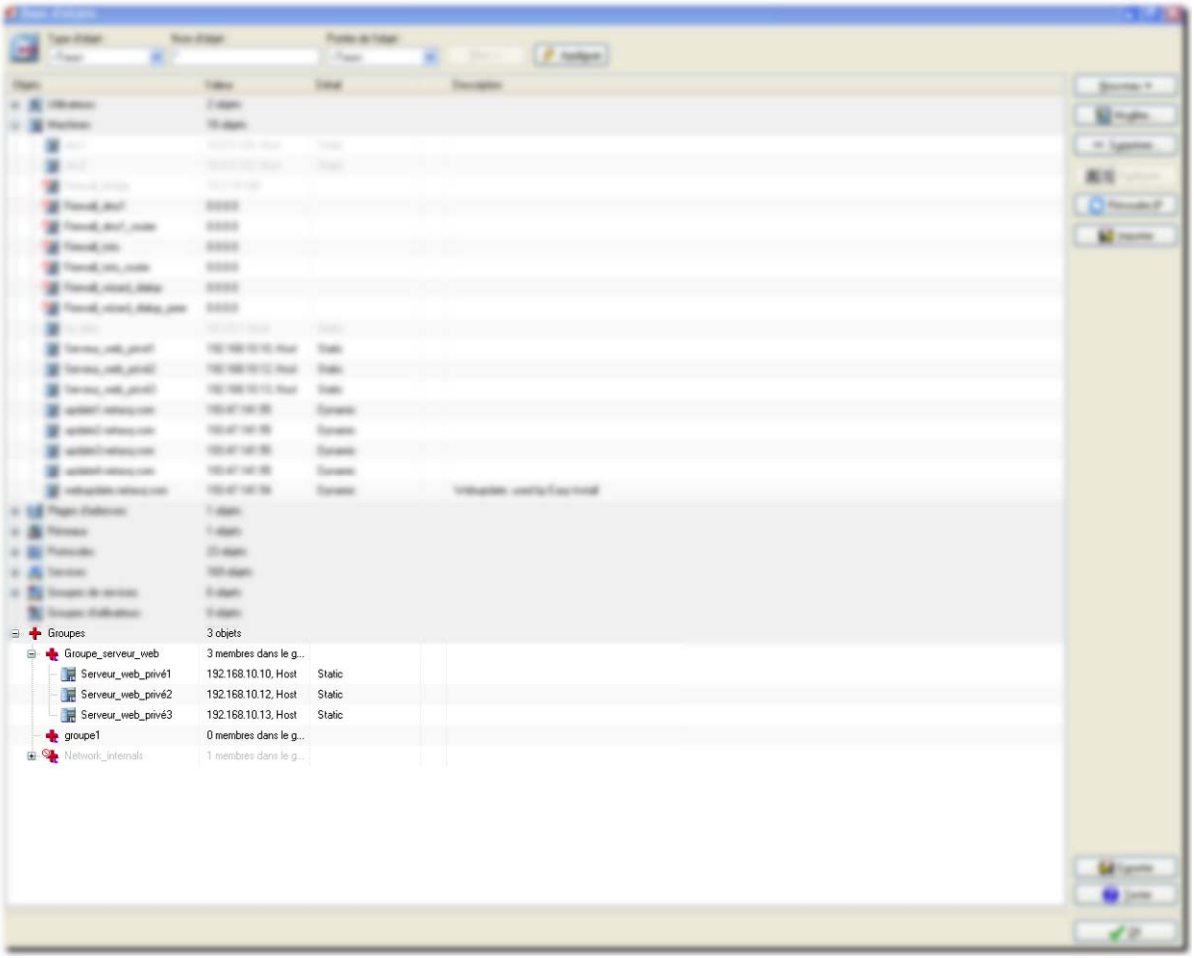


Figure 533 : Groupes

Le flux à destination de l'adresse IP publique 192.36.253.10 est partagé équitablement et séquentiellement entre les différentes machines du groupe de serveurs web.

Statut	Action	Option	Original	Destination	Port destination	Translaté	Description
On	split	Aucun	Serveur_web_public	<Any>	<Any>	Grpue_serveur_web	

REMARQUE
Il est possible de préciser les ports sources des machines source et destination en affichage détaillé. Cela revient à combiner partage de charge et redirection de ports.
Le partage se fait, dans cette version, de façon équitable, sans prise en compte de la charge respective des machines et/ou la disponibilité de ces machines.

Annexe F : Exemples de règles de filtrage

Dans cette annexe, nous vous indiquons concrètement comment configurer certaines règles de bases telles que :

- Accès au DNS
- Accès à ICMP
- Accès au Telnet
- Accès au FTP
- Accès à un serveur Web interne depuis l'extérieur et depuis le réseau interne
- Accès à l'internet avec ou sans le filtrage URL
- Accès des postes clients au serveur mail
- Configuration d'un serveur de messagerie
- Régulation de bande passante
- Vérification des règles de filtrage
- Authentification

AVERTISSEMENT
Certaines configurations peuvent s'avérer inutiles si les règles implicites correspondantes ont été activées. (Cf. Règles implicites).

Accès à ICMP

Dans cet exemple nous allons ajouter l'accès du réseau interne au protocole ICMP, permettant notamment d'utiliser le programme "ping".

Pour ajouter ICMP, il suffit, dans la sélection de services, de sélectionner "ICMP".

Figure 534 : Accès à ICMP

Vous pouvez, si vous le désirez n'autoriser que certains codes ICMP. Dans cet exemple, seul le ping (equo request) est autorisé.

Accès à Internet

Pour donner accès à l'Internet au réseau interne en passant par le firewall, il suffit de mettre une règle qui autorise le réseau interne à contacter tout le monde en utilisant le protocole "http" et le protocole "domain_udp" pour la résolution DNS. Ces protocoles sont inclus au groupe de services "Web".Cela donne :

Figure 535 : Accès à Internet

Si vous utilisez le filtrage URL, vous allez passer indirectement par un proxy web situé sur le firewall.

Vous ne vous connectez donc plus directement au serveur web mais au proxy web puis le proxy se connecte au serveur web. Ces différentes phases sont implicites dans les règles de filtrage.

Vous pouvez, au niveau des postes de travail, configurer votre navigateur pour vous connecter sur un serveur proxy distant. Dans ce cas, pour accéder à Internet, le poste n'utilise plus le protocole "http" sur le port 80 mais sur le port 8080.

Si vous avez implicitement laissé passer ce dernier protocole au niveau du firewall, vos utilisateurs peuvent accéder à l'Internet sans passer par le filtrage d'URL que vous avez mis en place.

Pour éviter cela, vous pouvez rediriger toutes les requêtes utilisant un service particulier (8080 par exemple) vers le filtrage d'URL :

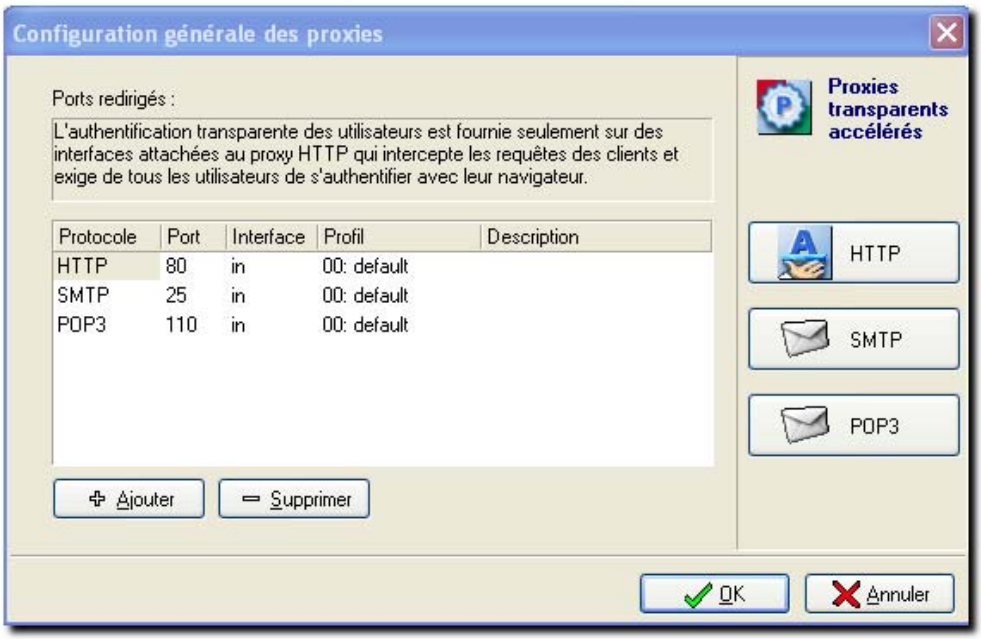


Figure 536 : Configuration générale des proxies

Accès à un serveur Web

Dans cet exemple, on suppose que votre serveur Web est disposé dans la DMZ.

Il doit être accessible depuis le réseau externe (depuis Internet) et depuis le réseau interne soit tout le monde.

La configuration du filtrage est alors assez simple : la machine source est "any", la machine destination est "Serveur_Web_prive1", le service "http" et l'action à appliquer est de "Passer" :

Figure 537 : Edition des règles de filtrage

AVERTISSEMENT

Si vous faîtes de la translation d'adresses pour ce serveur web, vous devez configurer une règle de translation supplémentaire pour y accéder de votre réseau interne avec son nom de domaine. Référez-vous à l'exemple sur la translation d'adresses traitant ce cas pour plus de renseignements.

Accès au DNS

Nous allons donner au réseau interne un accès au service DNS pour pouvoir utiliser les noms de domaine au lieu des adresses IP.

La règle suivante permet d'autoriser le réseau interne à accéder aux serveurs DNS (internes et externes). Il n'est pas nécessaire d'établir cette règle si vous avez choisi le groupe de services WEB, mais ce type de règle peut être intéressant si vous souhaitez filtrer les serveurs DNS accessibles.

Figure 538 : Edition des règles de filtrage

Accès au FTP

Le protocole FTP est un peu particulier. Il utilise deux types de connexion :

- Une connexion de commande pour envoyer et recevoir les commandes FTP.
- Une connexion data pour le transit des flux de données.

De plus le FTP peut être utilisé en deux modes différents :

- Le FTP actif (sous DOS par exemple) pour lequel la connexion pour le transfert de données se fait par le port FTP-data du serveur. Cette connexion est à l'initiative du serveur. En FTP actif, l'adresse IP privée du client est envoyée, via la connexion de commande, au serveur afin que ce dernier puisse établir la seconde connexion. Si l'adresse privée du client est translatée, il faut donc cocher l'option "FTP actif" dans la configuration de la translation d'adresse, afin que le firewall modifie automatiquement l'adresse envoyée dans les commandes FTP.
- Le FTP passif (avec un Browser Web par exemple), pour lequel la machine source effectue les deux connexions elle-même sur le serveur FTP. Cependant, le transfert de données ne se fait pas sur le port FTP-data mais sur un port éphémère du serveur.

Règle générale

Le firewall NETASQ intègre un plugin FTP qui va gérer automatiquement la seconde connexion (connexion data), vous permettant de ne définir qu'une seule règle de filtrage (celle pour autoriser la connexion de commande du client vers le serveur). La seule règle à définir est la suivante :

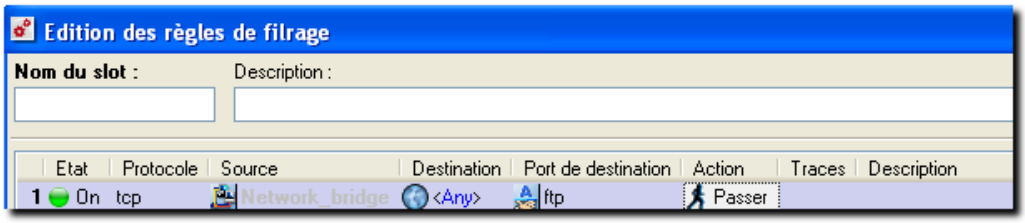


Figure 539 : Edition des règles de filtrage

Cette règle permet à une machine du réseau interne (Network_Bridge) d'accéder aux serveurs FTP sur Internet.

Accès au serveur de messagerie placé en DMZ

Pour pouvoir envoyer et recevoir des e-mails sur un poste client, il faut autoriser les services SMTP et POP3 du poste client vers le serveur de messagerie.

Le serveur de messagerie peut être un hébergé en interne ou à l'extérieur du réseau (chez le provider par exemple). Il faut donc déclarer, dans la configuration des objets, le serveur de messagerie (avec son adresse IP).

Vous pouvez ensuite créer un groupe de services appelé "Messagerie" dans lequel vous mettez les services POP3 et SMTP. Ceci vous évitera de mettre deux lignes possédant les mêmes propriétés dans les règles de filtrage.

Vous créez ensuite la règle de filtrage du réseau interne (où sont placés les postes clients) vers le serveur de Messagerie avec le groupe de Service "Messagerie" et l'action **Passer**. Cela donne :

Accès au telnet

Le service telnet permet l'ouverture d'un shell sur une machine distante (généralement une machine UNIX).

Dans cet exemple, nous allons autoriser la machine "ma_machine" à se connecter au "mon_serveur_web" pour en assurer l'administration.

Figure 540 : Edition des règles de filtrage

Seule la machine " Client " pourra faire un telnet sur le serveur Web, situé dans la DMZ.

Connexions IPSec

Après avoir paramétré le VPN IPsec sur le firewall, il faut mettre des règles de filtrage pour autoriser ces protocoles sur le firewall (sauf si les règles implicites sont activées pour ce type de trafic).

La première phase du protocole IKE se négocie sur le port UDP 500 (ISAKMP). Il faut donc autoriser les connexions sur ce port sur l'interface du firewall concernée par le tunnel.

Dans le cas d'une connexion IPsec sortante, il faut accepter une connexion sur un firewall distant sur le port ISAKMP.

En fonction des protocoles sélectionnés dans la configuration du VPN (ESP), il faut autoriser ces protocoles à atteindre le firewall. Ces règles ne sont pas prises en compte par le module Stateful Inspection et doivent donc être positionnées dans les deux sens de communications.

Les 3 premières règles de l'écran suivant permettent d'établir le tunnel VPN entre le firewall local et le firewall distant (ces 3 règles doivent être indiquées sur les deux firewalls réalisant le VPN). Pour un tunnel anonyme, l'objet "FW_correspondant" doit être remplacé par "ANY".

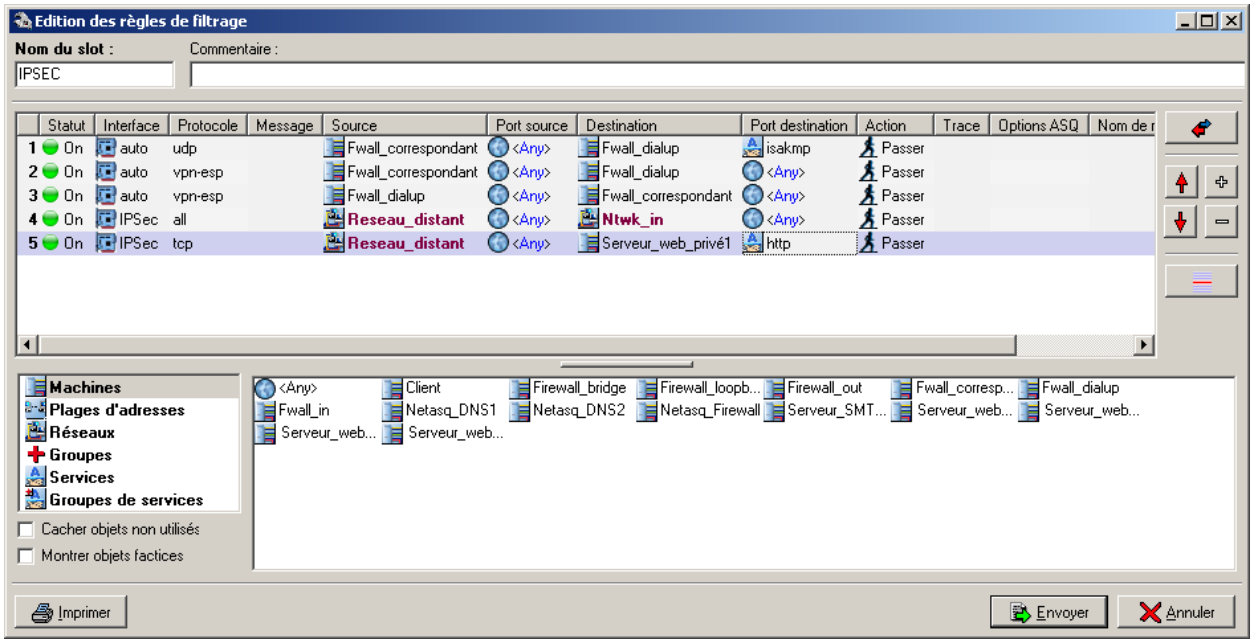


Figure 541 : Edition des règles de filtrage

Une fois les 3 premières règles en place, le tunnel peut être créé.

Vous pouvez ensuite filtrer les accès VPN aux machines internes. Pour filtrer les paquets arrivant au firewall au travers du tunnel, vous devez spécifier l'interface IPSEC (en affichage détaillé) pour définir les règles de filtrage. Pour filtrer les paquets sortant de votre firewall vers le tunnel VPN, vous n'avez pas besoin de définir l'interface (laissez l'interface sur auto) si les objets sources et destination sont bien précisés.

Les deux dernières règles indiquent comment filtrer les flux venant du réseau distant et passant par le VPN.

Connexions PPTP

Après avoir configuré le serveur PPTP sur le firewall, il faut mettre des règles de filtrage associées (sauf si les règles implicites sont activées pour ce type de trafic).

Vous avez besoin de rajouter trois règles :

- La première autorisant les clients PPTP à se connecter avec le protocole PPTP (TCP port 1723) sur l'interface du firewall utilisée pour le PPTP,
- Deux autres autorisant le protocole GRE (protocole d'encapsulation) du client vers le firewall et la règle inverse.

Exemple

On considère qu'un client se connecte sur Internet chez un provider A. Généralement, ce provider fournit des adresses IP dans une plage particulière qu'il est possible de repérer.

On crée donc un objet réseau Plage_IP_Provider avec ces adresses. Si vous ne connaissez pas cette plage, vous pouvez laisser l'objet "any" à la place.

On considère que la connexion Internet est reliée à l'interface Out du firewall et les postes nomades arrivent sur cette interface pour se connecter en PPTP.

Les règles de filtrage sont donc, dans ce cas, les suivantes :

Figure 542 : Edition des règles de filtrage

Contrôle de bande passante

Le firewall NETASQ vous donne la possibilité de faire de la régulation de bande passante. Ceci se fait en autorisant le passage d'un nombre limité d'octets pendant une période de 1 seconde.

Le niveau peut être assez fin puisque vous pouvez limiter chacun des services du protocole IP, pour chaque machine différente.

Ceci se paramètre au niveau du filtrage par l'action "Limiter à". Au lieu de bloquer ou laisser passer les paquets, ils vont être autorisés jusqu'au seuil fixé puis se verront rejetés si le seuil est atteint dans la période donnée.

L'exemple ci-dessous illustre comment limiter le téléchargement de fichiers en FTP à partir du réseau interne.

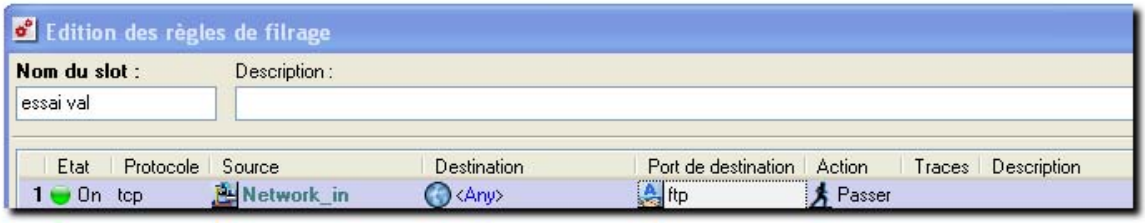


Figure 543 : Edition des règles de filtrage

Contrôle du filtrage

Après avoir configuré les règles les plus simples, il se peut que vous vous demandiez s'il n'en manque pas pour assurer le bon fonctionnement des flux réseaux.

Il se peut aussi qu'un serveur applicatif utilise un protocole particulier que vous ne connaissez pas.

Si vous n'utilisez pas de règles explicitement bloquantes pour ces machines ou protocoles, un moyen simple est de placer temporairement une règle de traçage en fin de filtrage. Cette règle va logger tout ce qui est bloqué par le firewall.

Ainsi, le flux que vous n'avez pas explicitement autorisé passe toutes les règles puis arrive en fin de tableau où il subit la règle par défaut (bloquer). Si vous placez une règle qui trace tout juste avant la règle par défaut (qui n'apparaît pas dans la liste des règles de filtrage), le flux sera inscrit dans les fichiers de traces que vous pourrez consulter ensuite.

Vous verrez notamment apparaître, dans le fichier de traces, le numéro de port destination, ce qui est utile si vous ne le connaissiez pas.

Vous pouvez aussi analyser tout ce qui a été bloqué et voir si certains flux doivent réellement être bloqués.

Accès au serveur de messagerie

Si vous possédez votre propre serveur de messagerie, il faut, au niveau du filtrage, lui autoriser l'envoi et la réception des courriers. Pour cela, il suffit d'autoriser l'envoi et la réception au travers du service SMTP.

Ceci n'est bien entendu utile que si votre serveur de messagerie communique avec l'extérieur. S'il sert uniquement pour la messagerie interne, ces règles sont inutiles.

Le serveur de messagerie envoie ou reçoit des courriers de différents serveurs de messagerie, qui ne sont pas identifiables. Ils seront donc représentés par la machine "any".

Les deux règles (une pour l'émission l'autre pour la réception) sont les suivantes :

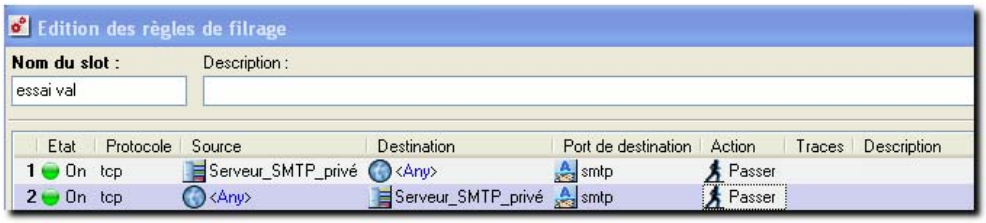


Figure 544 : Edition des règles de filtrage

REMARQUE
Si votre serveur de messagerie est juste un relais avec le serveur de messagerie de votre provider Internet, l'échange se fait uniquement du port 25 (SMTP) vers le port 25 de votre serveur.

Authentification

L'authentification peut être demandée pour l'accès à certains services ou à certaines machines. Pour cela, il faut avoir défini les fiches des utilisateurs qui peuvent s'authentifier au travers du firewall. Par exemple, l'accès au Web pour les utilisateurs authentifiés, appartenant au réseau interne, pourra être autorisé avec la règle suivante :

Figure 545 : Edition des règles de filtrage

Vous pouvez aussi donner des accès particuliers à certains utilisateurs authentifiés. Par exemple, la politique suivante autorise l'utilisateur DUPONT à faire du FTP (où qu'il se trouve), les utilisateurs authentifiés du réseau Network_bridge peuvent faire du Web et tous les utilisateurs du réseau Network_bridge, même non authentifiés, ont accès à la messagerie :

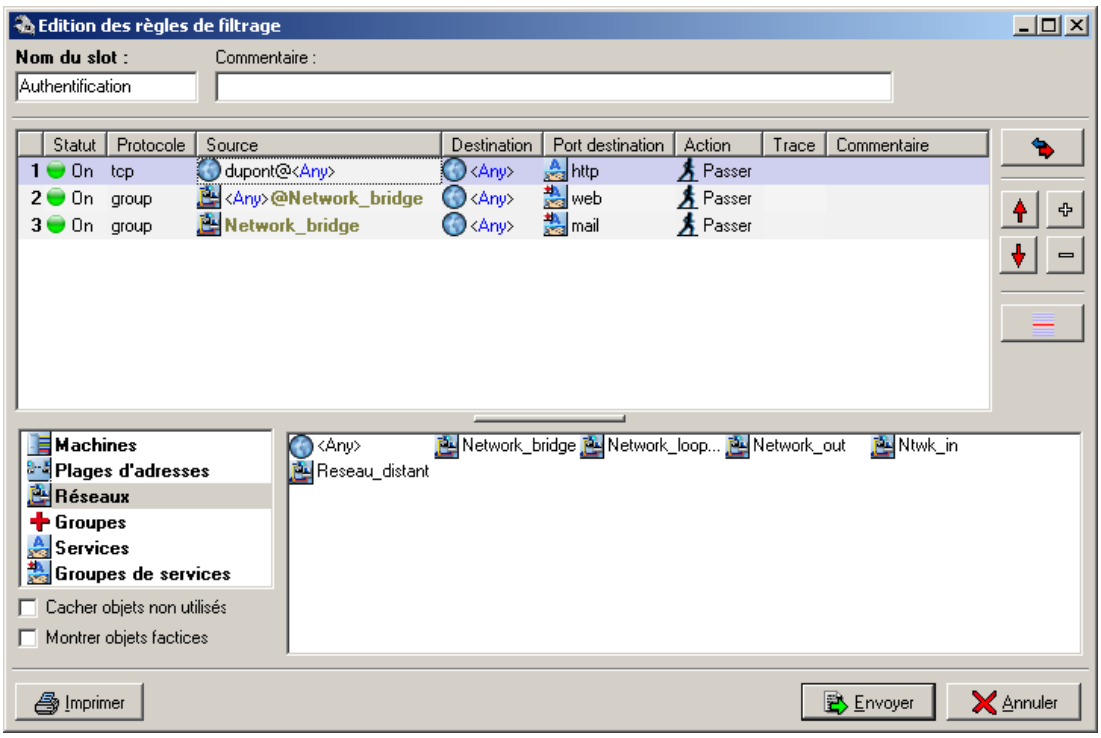


Figure 546 : Edition des règles de filtrage

Il est aussi possible d'authentifier les utilisateurs pour des connexions entrantes (provenant de l'Internet).

Ainsi, vous pouvez autoriser l'accès à certains services hébergés sur votre réseau interne à certains utilisateurs de l'Internet (il faut bien entendu que les informations de connexion aient été, au préalable, fournies à ces utilisateurs). L'exemple suivant montre comment autoriser le groupe d'utilisateur Partenaire à accéder à un serveur Web particulier (pour un Extranet, par exemple) :

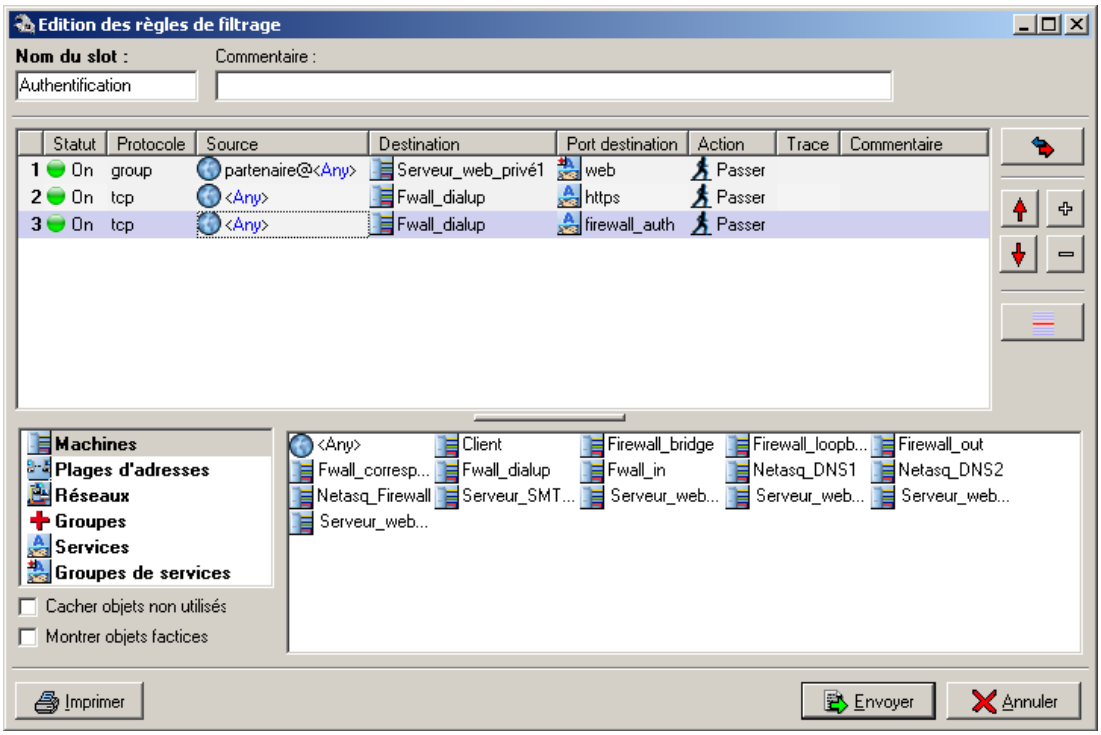


Figure 547 : Edition des règles de filtrage

Si vous souhaitez authentifier des utilisateurs situés à l'extérieur du périmètre de sécurité du firewall, il faut autoriser les services nécessaires à l'authentification, à savoir le service HTTPS et le service

d'authentification propriétaire NETASQ via SRP (port1200). Attention, le port 1200 ne doit être ouvert que si vous utilisez l'authentification via SRP, dans les autres cas seul le HTTPS est nécessaire.

Annexe G : Evénements

Voici une liste non exhaustive des notifications d'événements déclenchés par le firewall NETASQ.

Notification d'événements

Certains événements sont logués par le firewall sans être pour autant des attaques. Ces événements sont visualisable à partir de NETASQ UNIFIED MANAGER (Menu **`Configuration\Traces`**)

Notification	Description
Arrêt du firewall	Indique un arrêt du firewall
Authentification échouée pour + nom d'utilisateur	L'authentification du protocole PPTP a échoué (le login ou le mot de passe PPTP sont incorrects).
Connexion terminée pour + nom d'utilisateur	La connexion PPTP ou dialup est terminée.
Il reste 20% d'espace libre pour le fichier de logs	Le fichier de logs a dépassé les 80% de remplissage (seulement en mode shutdown ou sécurisation, ce qui signifie que dans ce cas le firewall agit comme un "block all").
Connexion établie pour	La connexion PPTP ou dialup est correctement établie.
Phase 1 IPsec échouée	La phase 1 du protocole IKE n'a pas pu s'établir correctement.
Phase 2 IPsec échouée	La phase 2 du protocole IKE n'a pas pu s'établir correctement.
La clé IPsec est introuvable pour + identifiant VPN	Aucune clé pré-partagée ne correspond à cet identifiant VPN. La clé correspondant à l'identifiant n'a pas été définie dans le gestionnaire des clés pré-partagées.
Démarrage du firewall	Indique un démarrage du firewall.
HA : Défaillance du firewall actif	Indique une panne du firewall actif. Le firewall passif devient alors actif. (Cet événement ne peut-être détecté que si vous possédez deux firewalls configurés en haute disponibilité).
HA : Défaillance du firewall passif	Indique une panne du firewall passif (Cet événement ne peut-être détecté que si vous possédez deux firewalls configurés en haute disponibilité).
CRL invalide pour le tunnel VPN	La liste de révocation de certificats (CRL) utilisée pour un tunnel VPN n'est pas valide.
Certificat invalide pour le tunnel VPN	Le certificat de l'équipement VPN distant n'est pas valide.
La partition de log a changé	La partition disque contenant les logs n'est plus détectée sur le même disque qu'au précédent reboot. Deux causes sont possibles : une intervention matérielle (un disque a été rajouté dans le firewall pour contenir la partition de log), un problème disque (la partition de log n'est plus correctement détectée).

Annexe H : Commandes

L'accès au firewall en mode console (connexion par SSH, par port série ou avec un écran-clavier) permet la maintenance du firewall au moyen d'un jeu de commandes.

Cette annexe présente les principales commandes utilisées (attention à bien respecter la casse) :

Lancement du serveur de commandes

- **nsrpc user@127.0.0.1** : permet de lancer, de façon locale, le serveur de commande du firewall avec le user admin.

Visualisation d'informations de configuration

- **ifinfo :** affiche la correspondance entre les noms des interfaces définies dans la configuration réseau (avec NETASQ UNIFIED MANAGER) et les noms utilisés par le système.
- **ifconfig** : affiche les informations relatives à la configuration réseau du firewall.
- **ipnat -l :** donne les règles de translation d'adresses actives.
- **sfctl -s filter** : donnes les règles de filtrage actives.

Vous avez la possibilité de visualiser le contenu des fichiers de configuration avec un éditeur tel que vi.

Les fichiers de configuration se trouvent dans le répertoire /Firewall/ConfigFiles.

Activation/Désactivation de slot ou de fonctionnalité

Désactivation

- **ennat 00 :** désactive les translations d'adresses.
- **envpn 00** : désactive le tunnel VPN actif.
- **enurl 00 :** désactive le filtrage d'URL.

Activation

- **ennat xx :** active le slot de translation d'adresses portant le numéro xx.
- **envpn xx :** active le slot vpn portant le numéro xx.
- **enurl xx :** active le slot de filtrage d'URL portant le numéro xx.
- **enfilter xx :** active le slot de filtrage portant le numéro xx.
- **enfilter 10 :** active le slot 10 (pass_all dans la configuration par défaut, le firewall laisse passer tous les paquets).
- **endialup :** relance une connexion avec un modem.
- **ennetwork :** recharge une configuration réseau.
- **engui :** réactive l'autorisation de connexion de NETASQ UNIFIED MANAGER sur les réseaux internes.

Activité du firewall

- **sfctl -s stat :** donne les statistiques du firewall.
- **sfctl –T :** affiche des informations "temps réel" sur le moteur stateful du firewall.
- **dstat :** donne la liste des services actifs.
- **top -u :** donne l'activité du processeur et des processus ainsi que l'occupation de la mémoire.
- **tcpdump -i <nom de l'interface> <filtre> :** affiche en temps réels les paquets qui transitent par une interface du firewall.
- <*nom de l'interface*> correspond au nom de l'interface utilisé par le système (ce nom peut être récupéré grâce à la commande ifinfo).
- <*filtre*> permet de filtrer les protocoles ou services affichés.

Le filtre d'un service doit être précédé du mot "port". Les services peuvent être indiqués par leur numéro de port ou par leur nom (si le service fait partie des services courants).

Exemple de filtres

- tcpdump -i fxp0 not port 23 (pour ne pas afficher les flux telnet),
- tcpdump -i fxp0 udp OR port HTTP (pour n'afficher que les flux UDP et HTTP),
- tcpdump -i fxp0 tcp AND port 53(pour n'afficher que les flux DNS TCP),
- tcpdump –s0 –w /tmp/dump –i fxp0 (écriture du trafic dans un fichier donné),
- tcpdump –s0 –i fxp0 ESP OR port isakmp (visualisation du trafic chiffré ESP ou des phases de négociation VPN).

Commandes VPN

- **showSPD :** Affichage de la SPD (Security Policy Database) contenant toutes les informations relatives aux tunnels définis (actifs ou non).
- **showSAD :** Affichage de la SAD (Security Association Database) contenant les informations relatives aux tunnels actifs.

Divers

- **getversion :** affiche la version logicielle du firewall.

AVERTISSEMENTS

1) Utilisez cette commande dès la réception de votre firewall pour vérifier que la version livrée correspond bien à la version attendue.
2) La manipulation des fichiers et l'utilisation de certaines commandes doivent être réalisées avec précaution, en effet certaines opérations peuvent avoir des conséquences sur le fonctionnement du firewall.

Support technique et "sysinfo"

Enfin la commande "sysinfo" permet la visualisation de la configuration complète d'un appliance UTM NETASQ. Indispensables à la bonne compréhension de votre problème, les informations fournies par cette commande vous sont systématiquement demandées par le support technique lors de la résolution d'un incident.

Pour information, le résultat de cette commande peut être obtenu par l'intermédiaire du menu **Firewall\Support technique** NETASQ de NETASQ UNIFIED MANAGER. Ce menu permet notamment l'enregistrement du résultat pour envoi au support par exemple.

Ci-dessous, est présenté un exemple (partiel) du résultat de la commande sysinfo.

```
##############################
#   Software information     #
##############################
current date :  2006-07-18 18:42:42
Serial       :  U70XXA0Z0899020
Model        :  U70
Software     :  Netasq Firewall software version 6.2.1
Branch/Build :  EUROPE / M
Partitions   :  Active=Main BackupVersion="6.2.1" BackupBranch=" EUROPE "
Date="2006-07-11 14:42:39" Boot=Main
Uptime       :  36 days 3:52, hours
##############################

##############################
#   Slot information         #
##############################
Filtering : slot_filter_01
NAT       : slot_nat
VPN       : slot_vpn
URL       :
##############################

##############################
#   Memory information       #
##############################
Stateful
--------

host                                    0 %
fragment                                0 %
ICMP                                    0 %
connection                              0 %
data tracking                           0 %

mbuf
----
1012/1056/7798 mbufs in use (current/peak/max):
        1012 mbufs allocated to data
261/272/5199 mbuf clusters in use (current/peak/max)
808 Kbytes allocated to network (6% of mb_map in use)
0 requests for memory denied
0 requests for memory delayed
0 calls to protocol drain routines
```

Annexe I : Foire aux questions

1) Que signifie le message “Impossible de localiser la machine en x.x.x.x” ?

Ce message signifie que la machine sur laquelle vous êtes connecté ne peut pas joindre le firewall avec l'adresse IP que vous avez précisée dans la fenêtre de connexion. Le problème peut être dû à plusieurs choses.

Vérifiez:

- Que l'adresse IP que vous avez spécifiée dans la fenêtre de connexion est bien celle du firewall (celle de l'interface interne en mode avancé).
- Que votre machine possède bien une adresse IP différente du firewall mais dans le même sous-réseau.
- Que les branchements sont corrects (utilisez un câble croisé uniquement si vous branchez le firewall directement à une machine ou un routeur). Saisissez "**arp -a**" dans une fenêtre DOS sous Windows pour voir si le PC connaît l'adresse physique (Ethernet) du firewall NETASQ. Si ce n'est pas le cas, vérifier vos câbles, les connexions physiques à votre hub.
- Que vous n'avez pas changé de mode de fonctionnement du firewall (transparent ou avancé).
- Que l'adresse IP est bien prise en compte au niveau du firewall (cf. *Comment vérifier l'adresse IP affectée au firewall*).
- Que le serveur d'accès à l'interface graphique n'a pas été désactivé sur le firewall.

2) Comment vérifier l'(les) adresse(s) IP réellement affectée(s) au firewall ?

Afin de vérifier la(les) adresse(s) IP affectée(s) au firewall ainsi que le mode de fonctionnement, il suffit de se connecter en mode console au firewall. Pour cela, vous pouvez soit faire un SSH sur le firewall (si le SSH est activé et autorisé), soit vous connecter directement sur le boîtier par le port série ou en branchant un écran et un clavier sur le boîtier.

Une fois connecté en mode console (avec le login admin), saisissez la commande "**ifinfo**". Le résultat vous donne la configuration des cartes réseau et le mode de fonctionnement actuel.

3) Que signifie le message "Vous avez perdu le privilège MODIFY" ?

Il ne peut y avoir qu'un seul utilisateur ayant les droits de modification connecté au firewall. Ce message signifie qu'une session est ouverte par un utilisateur ayant le droit de modification.

Pour forcer la fermeture de cette session, il suffit de se connecter en ajoutant un point d'exclamation devant le nom d'utilisateur (!admin).

AVERTISSEMENT
Si une session avec le droit MODIFY est ouverte sur une autre machine, elle sera fermée.

4) Que signifie le message "L'opération a dépassé le temps imparti" ?

Par mesure de sécurité, toute connexion, aboutie ou non, entre le firewall et l'interface graphique est stoppée au bout d'un certain temps. Cela évite notamment d'attendre indéfiniment la connexion dans le cas où le firewall n'est pas joignable sur le réseau.

5) Comment arrêter le voyant d'alarme majeure sur le firewall ?

La led d'alarme majeure s'allume dès qu'une alarme majeure est reçue et reste allumée tant que personne ne valide la visualisation de l'alarme.

Pour arrêter la led, il suffit de valider l'option **Eteindre les voyants d'alarme** dans le menu Firewall de NETASQ UNIFIED MANAGER.

6) Comment suis-je au courant d'une tentative d'intrusion ?

Chaque tentative d'intrusion peut être configurée pour déclencher une alarme majeure ou mineure suivant son importance. Vous êtes informés de ces alarmes par quatre moyens différents :

- Premièrement, les leds sur la face avant du boîtier s'allument (rouge) ou clignotent (jaune) pour vous signaler l'alarme.
- Ensuite, les alarmes sont tracées dans un fichier spécifique consultable à partir de l'interface graphique (NETASQ REAL-TIME MONITOR ou NETASQ EVENT REPORTER).
- Vous pouvez recevoir un rapport d'alarmes à une fréquence régulière (cf. *réception des alarmes*) via l'application NETASQ UNIFIED MANAGER. Celui-ci peut-être configuré pour que la levée d'une alarme entraîne l'envoi d'un mail. Lorsque plusieurs alarmes sont levées dans un laps de temps très courts, elles sont regroupées au sein d'un mail commun.
- Enfin, NETASQ REAL-TIME MONITOR affiche à l'écran, en temps réel, les alarmes reçues.

7) Que se passe-t-il lorsqu'une alarme est déclenchée par le firewall ?

Toute tentative d'intrusion ou attaque détectée est automatiquement stoppée. Suivant la configuration, soit le paquet qui déclenche l'alarme est bloqué, soit la connexion est réinitialisée (voir si c'est toujours le terme employé au niveau du filtrage). De plus, une réaction peut être ajoutée : envoi d'un mail ou mise en quarantaine du responsable de la levée de l'alarme.

La mise en quarantaine consiste à bloquer, sans autre forme de procès, tout paquet provenant de la machine en question.

En cas d'attaque franche, il convient de surveiller de près les connexions entrantes à l'aide de NETASQ REAL-TIME MONITOR ou NETASQ EVENT REPORTER ou d'autres outils d'analyse réseau.

8) Est-il possible de laisser passer d'autres protocoles qu'IP ?

Le firewall ne peut analyser (cohérence avec l'alarme "protocole IP non-analysé") que les protocoles s'appuyant sur IP (modèle OSI=architecture en couches). Tout protocole qui n'est pas analysé par le firewall est considéré comme suspect et se retrouve bloqué.

Cependant, avec le mode de fonctionnement transparent, il est possible de laisser passer d'autres protocoles bien qu'ils ne soient pas analysés. Ces protocoles sont "IPX" de Novell, "IPv6", "PPPoE", "Appletalk" et "NetBIOS".

Annexe J : Rôle de la DMZ

Le but habituel d'une DMZ (De-Militarized Zone) est d'isoler de votre réseau interne les machines qui doivent recevoir des connexions du monde extérieur.

Ainsi, vous isolez complètement l'accès direct du réseau externe vers votre réseau interne. Les accès possibles de l'extérieur se font uniquement dans la DMZ qui est physiquement séparée du réseau interne.

Vous bénéficiez ainsi d'une protection efficace sur le réseau interne. Les machines de la DMZ, qui sont exposées à un risque plus important (puisque joignables de l'extérieur), ne peuvent pas permettre de rebondir directement sur l'ensemble du réseau.

Il faut ensuite bien définir les relations entre la DMZ et le réseau interne pour ne pas compromettre le niveau de sécurité atteint.

Exemple de mise en place d'une DMZ

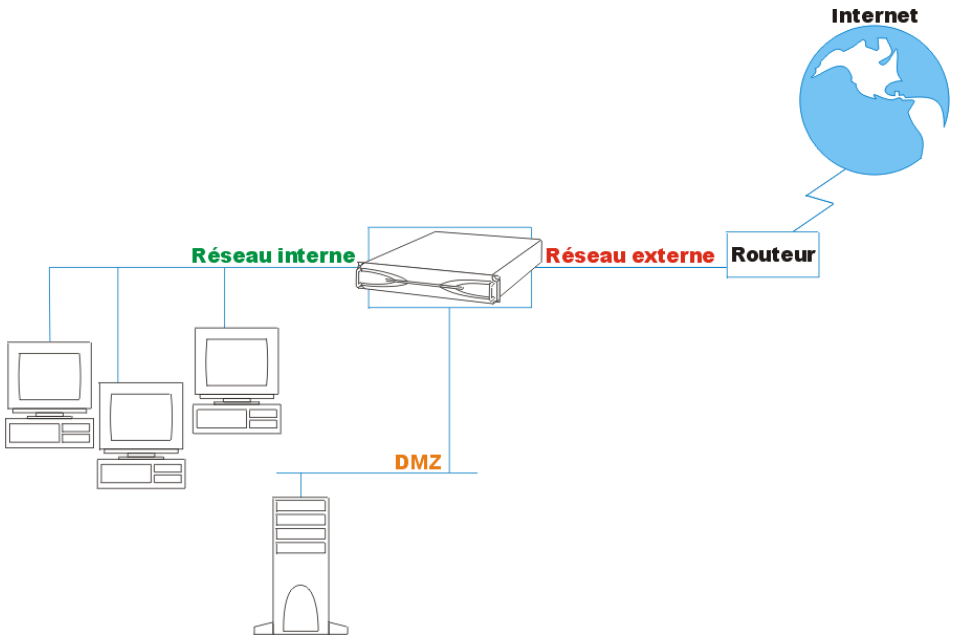


Figure 548 : Mise en place d'une DMZ

La DMZ peut aussi être utilisée à d'autres fins (séparation de branches d'une entreprise,...).

Annexe K : Connexion au serveur SSH

Le firewall NETASQ intègre un serveur SSH. La connexion à ce serveur peut servir à la configuration du firewall en mode console (en ligne de commande).

Définition de Secure Shell

Secure Shell est un protocole de communication sécurisé permettant l'accès distant au firewall afin d'y exécuter des programmes. SSH permet de pallier les faiblesses de sécurité des accès distants tels que telnet en fournissant les services de sécurité essentiels : authentification du serveur et du client, confidentialité des flux (notamment des mots de passe).
SSH repose sur la technique de cryptographie asymétrique RSA pour l'authentification et utilise l'algorithme symétrique IDEA pour la confidentialité des flux.

Activation du serveur SSH sur le firewall

Le service est désactivé par défaut sur le firewall, il faut donc l'activer par l'intermédiaire du menu **`Firewall\Sécurité`**.

La clé privée de l'utilisateur admin sera nécessaire pour l'authentification lors de la connexion. Il est donc nécessaire de la sauvegarder et de la stocker dans un répertoire sur la machine depuis laquelle la connexion en SSH sera lancée.

Par défaut le filtrage du firewall bloque la connexion sur le port 22 (SSH) du firewall. Il est donc nécessaire de mettre en place une règle de filtrage pour autoriser cette communication.

Configuration de la partie cliente

> **AVERTISSEMENT**
> Un logiciel ssh supportant la version 2 de ce protocole est nécessaire pour l'utilisation avec le firewall.

La configuration de la partie cliente dépend du logiciel client utilisé.

Annexe L : Réinitialisation du firewall

Il est possible de restaurer la configuration usine d'un firewall NETASQ. Cette opération ramène alors le produit dans l'état où il était à la livraison.

> **AVERTISSEMENTS**
> La réinitialisation d'un firewall détruit toute la configuration réalisée sur le produit, elle est irréversible, attention donc à ne réaliser cette opération que si elle est absolument nécessaire.

Cas du U30, U70, U120, U250 et U450

Pour réinitialiser le U30, U70, U120, U250 ou U450, munissez-vous d'une pointe (stylo bille par exemple). Un petit interrupteur est placé sur la façade du boîtier (entre le port USB et le port VGA) et est accessible par un trou réalisé dans le capot. Maintenez l'interrupteur appuyé au moyen de la pointe pendant plusieurs secondes (environ 15 secondes) jusqu'à entendre un signal sonore. La procédure de réinitialisation du firewall se lancera alors automatiquement et après quelques instants le firewall aura retrouvé sa configuration d'usine et rebootera. Ce reboot peut durer 5 minutes, veuillez donc attendre la fin du reboot

(nouveau signal sonore) pour vous reconnecter au firewall Attention, cette opération réinitialise aussi le mot de passe.

Pour tous les autres produits

Pour les autres produits, la réinitialisation du boîtier se fait en mode console. Plusieurs méthodes permettent d'accéder au produit UTM NETASQ en mode console, la plus simple est réalisée avec la liaison série. Pour cela, utilisez le câble série livré avec le firewall pour connecter l'appliance et un PC via leur port série respectif.

Lancez ensuite une application du type HyperTerminal (accessible via le menu **`Démarrer\Programmes\Accessoires\Communication`**).

Choisissez alors une communication sur le port COM, puis spécifiez les paramètres du port suivants :

- Bits par seconde : 9600
- Bits de données : 8
- Parité : Aucun
- Bits d'arrêt : 1
- Contrôle de flux : Matériel

L'invite suivante apparaît alors :

FreeBSD (U70XXA0Z0899020) (ttyd0)
login :

Renseignez alors le login « admin » puis le mot de passe correspondant au login "admin" que vous utilisez d'habitude pour vous connecter au firewall. Vous êtes maintenant connecté au firewall. Saisissez alors la commande : "defaultconfig" –f et appuyez sur entrée.

FreeBSD (U70XXA0Z0899020) (ttyd0)
login: admin
SSH Passphrase:
Copyright (c) 1980, 1983, 1986,1988, 1990, 1991, 1993, 1994
The Regents of the University of California. All rights reserved

U70XXA0Z0899020>defaultconfig -f

Un bip d'avertissement doit retentir et votre firewall doit redémarrer. Le firewall est alors réinitialisé.

Annexe M : Noms interdits

Voici une liste des noms d'objets (à l'exception des objets « utilisateur ») interdits sur le firewall NETASQ. :

Caractères interdits

Ces caractères ne peuvent être utilisés dans les noms d'objets :

- « »
- \
- #

- @
- [
-]
- =
- <tab>
- <espace>

Caractères interdits en première position

Les noms d'objets ne peuvent commencer par les chiffres (0, 1, 2, 3, 4, 5, 6, 7, 8, 9).

Préfixes interdits

Ces préfixes, non sensibles à la casse, ne peuvent être utilisés en début d'un nom d'objet :

- Firewall_
- Network_
- ephemeral_
- Global_

Noms interdits

Les noms suivants, non sensibles à la casse, ne peuvent pas être utilisés dans la création d'objets sur le firewall :

- any
- anonymous
- broadcast

Annexe N : Configuration des autres équipements

Pour un fonctionnement optimal de l'Administration globale NETASQ, plusieurs opérations doivent être réalisées sur vos appliances NETASQ et sur les équipements filtrants de votre réseau (firewall central par exemple).

Configuration des appliances NETASQ

Certaines manipulations doivent être réalisées sur les produits UTM NETASQ gérées par le mode Global Administration en fonction des opérations d'administration et de supervision que vous désirez réaliser.

Si le mode Global Administration NETASQ accède à au firewall par son interface interne (ou une autre interface protégée).

Si le mode Global Administration NETASQ accède à l'appliance par son interface.

En principe, aucune opération n'est nécessaire (excepté pour utiliser l'outil de vérification de fonctionnement et les outils externes). Il faut juste vérifier que les règles implicites pour le serveur d'administration sont bien actives.

Pour un firewall en version 5 et 6, connectez-vous à l'appliance avec le NETASQ UNIFIED MANAGER correspondant, puis sélectionnez le menu Configuration\Règles implicites. La case "Serveur d'administration" doit être cochée. Si vous souhaitez utiliser l'EZAdmin à partir du mode "Global Administration" de NETASQ, vérifiez aussi que la case "serveur d'authentification est cochée".

Pour un firewall en version 4, connectez-vous à l'appliance avec NETASQ UNIFIED MANAGER correspondant, puis sélectionnez le menu **`Configuration\Filtrage\Editez le slot actif,`** cliquez sur le bouton **Paramètres avancés**.

Les cases "Accès au NETASQ UNIFIED MANAGER sur les réseaux internes" et "Accès aux services d'authentification sur les réseaux internes" doivent être cochées.

Si le mode Global Administration NETASQ accède à au firewall par son interface externe (ou une autre interface non protégée).

Dans ce cas, il faut obligatoirement créer une règle de filtrage spécifique au niveau de la politique de sécurité de l'appliance.
Sélectionnez le menu **`Configuration\Filtrage Editez le slot actif.`**

Créez d'abord une machine en cliquant sur le bouton **Editer les objets**. Cette machine représente la station d'administration de l'Administration Globale NETASQ et possède donc l'adresse IP de la station.

> **AVERTISSEMENTS**
> Attention aux cas de translation d'adresses : si un équipement réalise de la translation d'adresses entre la station et l'appliance, il faut utiliser l'adresse translatée).

Créez ensuite une règle indiquant que les connexions de type "firewall_srv" provenant de la station d'administration de l'Administration globale NETASQ sont autorisées sur l'appliance.

Si le mode Global Administration NETASQ accède à l'appliance via un tunnel VPN

Si le mode Global Administration NETASQ accède à l'appliance via un tunnel VPN, il ne faut pas oublier d'autoriser le port TCP 1300 à transiter au travers du tunnel. Sur un firewall NETASQ, il suffit d'ajouter, dans les règles de filtrage, la règle autorisant les connexions firewall_srv provenant de l'interface IPSec à se connecter sur l'appliance.

Ensuite, sélectionnez le menu **`Configuration\VPN\Tunnels IPSEC\Editer le slot actif,`** cliquez sur le bouton **Paramètres avancés.** La case "Considérer les correspondants IPSEC comme internes" doit absolument être cochée.

Pour utiliser l'outil de vérification de fonctionnement

L'outil de vérification de fonctionnement des appliances et les témoins d'état utilisent le protocole ICMP (commande ping). Pour utiliser cette fonctionnalité, il est donc nécessaire d'autoriser ce type de flux sur l'appliance. Pour cela, ajoutez dans les règles de filtrage un règle autorisant le protocole ICMP (et plus particulièrement la commande PING) à destination de l'appliance.

Pour utiliser un outil externe

L'utilisation d'un outil externe pour se connecter en SSH sur une appliance nécessite d'activer le service SSH. Sélectionnez le menu **`Firewall\Sécurité`**. Activez les cases "Activer l'accès SSH au firewall". Si vous souhaitez réaliser une connexion SSH avec certificats, ne cochez pas la case "Activer l'accès par mot de passe" mais exportez les clés (certificats) dans l'outil externe. Si vous souhaitez réaliser une connexion SSH par mot de passe, cochez la case "Activer l'accès par mot de passe". Dans ce cas, le login **Admin** et le mot de passe correspondant seront utilisés.

Ensuite, il faut créer la règle de filtrage autorisant la connexion SSH sur l'appliance :

Configuration des équipements filtrants

Certains équipements sur votre réseau peuvent empêcher le bon fonctionnement de l'application. Il est donc important d'identifier tous les éléments qui seraient susceptibles de filtrer des flux nécessaires à le mode Global Administration NETASQ et de modifier leur configuration en conséquence.

Règles pour autoriser les flux entre la station d'administration du mode Global Administration NETASQ et le site Web NETASQ.

La station d'administration du mode Global Administration NETASQ et le site Web de NETASQ communique via les protocoles HTTP (port TCP/80) et HTTPS (port TCP/443), il est donc important que ces flux ne soient pas bloqués entre ces deux extrémités. De plus, il faut que la station d'administration du mode Global Administration NETASQ puisse réaliser des résolutions DNS, ce service doit donc lui être autorisé et accessible.

Enfin, il est préférable de ne pas demander d'authentification pour les flux HTTP et HTTPS transitant entre la station d'administration et le site Web de NETASQ, car cela risquerait de perturber le fonctionnement de l'application.

Règles pour autoriser les flux entre la station d'administration du mode Global Administration NETASQ et les appliances NETASQ.

La station d'administration du mode Global administration NETASQ et les appliances NETASQ utilisent plusieurs types de flux selon les fonctionnalités utilisées :

Fonctionnalités	Types de flux utilisés
Mode Global Administration NETASQ	Port TCP/1300
Outil de vérification de fonctionnement des appliances et témoins d'état	ICMP (commande PING)
NETASQ UNIFIED MANAGER, NETASQ REAL-TIME MONITOR, NETASQ EVENT REPORTER, VPN Manager	Port TCP/1300
Outil externe pour connexion SSH	Port TCP/22
Autre outil externe	Dépendant de l'outil

Pour utiliser correctement une fonctionnalité, il faut s'assurer qu'aucun filtrage sur les flux nécessaires n'est réalisé entre la station d'administration de l'Administration globale NETASQ et les appliances. Il convient donc d'ajouter des règles de filtrage autorisant ces flux.

Enfin, il est préférable de ne pas demander d'authentification pour les flux nécessaires transitant entre la station d'administration et les appliances, car cela risquerait de perturber le fonctionnement de l'application.

Annexe O : Famille de vulnérabilités

Il existe actuellement 15 familles de vulnérabilités :

- Any
- Base de données
- Serveur DNS
- Serveur FTP
- Peer to Peer
- Messagerie instantanée
- Applications Web
- SSH
- Serveur Web
- Client Web
- Client FTP
- Divers
- Serveur d'e-mails
- E-mail client
- Media Player

Annexe P : Liste des alarmes protocolaires

Alarmes Collecte

- Sonde OS Nmap
- Sonde OS Queso
- Détection de la politique de filtrage
- Possible scan de ports
- Sonde OS XProbe

Alarmes DNS

- Récursion de label DNS
- DNS id spoofing
- DNS zone change
- DNS zone update
- Empoisonnement du cache DNS
- Mauvais pointeur
- Débordement possible avec une chaîne DNS
- Protocole DNS invalide

Alarmes Divers

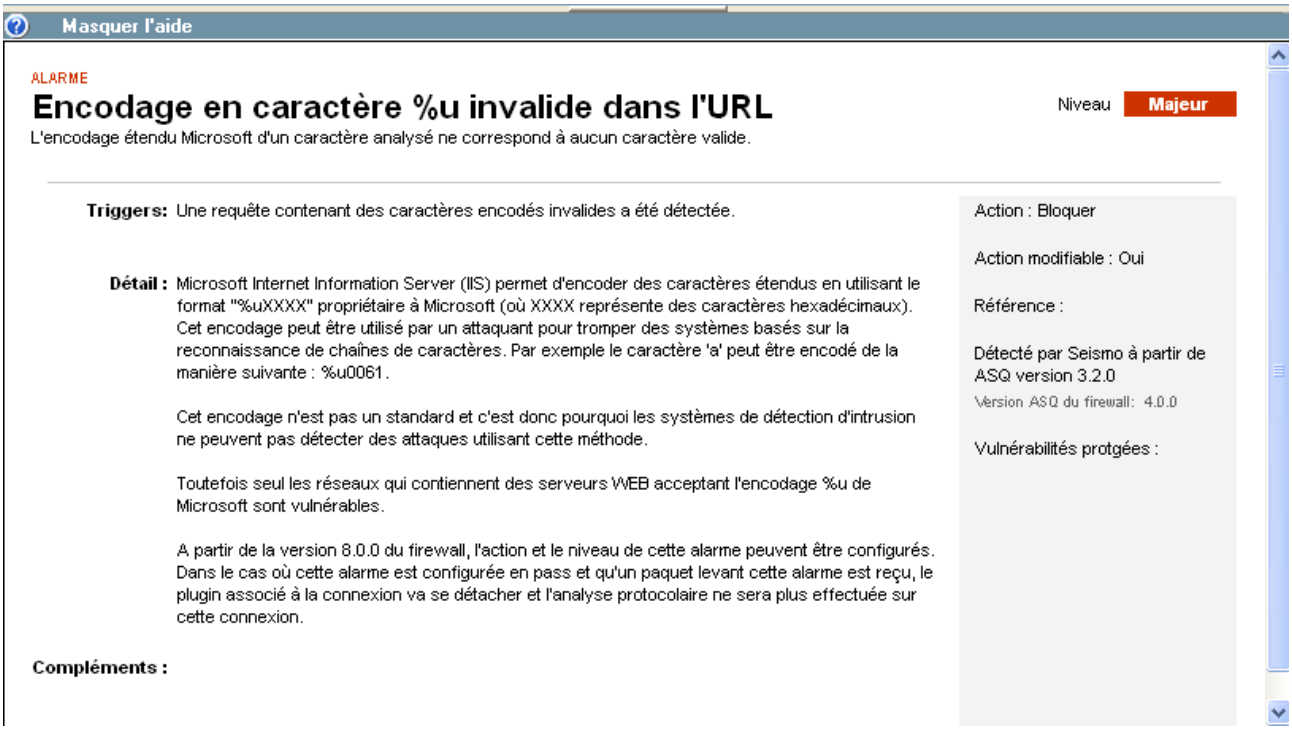
- Paquet RIP invalide
- Protocole eDonkey invalide
- Adresse dans la liste noire
- Adresse dans la liste blanche
- Paquet avec destination sur la même interface
- Problème dans le suivi de données
- Rejet pour qualité de service
- Détection de protocole non autorisé
- Protocole Skype détecté

Alarmes DoS

- Attaque de type Land
- Possible saturation ICMP
- Possible saturation UDP
- Possible saturation TCP SYN
- Bug Windows sur les données OOB
- Attaque possible des ressources

Alarmes HTTP

- Encodage en caractère %u invalide dans l'url. L'aide est la suivante :



- Evasion utilisant l'encodage %u dans l'url. L'aide est la suivante :
- Caractère d'échappement invalide dans l'URL
- Caractère NULL codé dans l'URL
- Caractère Pourcent codé dans l'URL
- Evasion utilisant l'encodage UTF-8
- Protocole http invalide
- Débordement dans une URL
- Débordement dans le protocole http

- Tunneling possible avec la méthode CONNECT
- Suite de slash dans l'URL
- Chemin avec auto-référence
- Chemin avec référence supérieure
- Encodage UTF-8 invalide dans URL
- Code malicieux possible dans l'entête http
- Chemin avec référence supérieure en dehors du répertoire racine
- Site avec rebond par redirect.
- Réponse 304 avec donnée.
- Données additionnelles en fin de réponse

Alarmes IGMP

- Type IGMP inconnu
- Demande IGMP pour une adresse non multicast
- Paquet IGMP invalide
- Somme de contrôle IGMB invalide

Alarmes IP

- Usurpation d'adresse de boucle
- Usurpation d'adresse IP
- Paquet broadcast
- Paquet multcast
- Adresse de classe expérimentale
- Mauvaise option IP
- Option IP inconnue
- Protocole IP non analysé
- Machine de réseau interne inconnue
- Débordement de fragment
- Recouvrement de fragment
- Routage par la source
- Fragment IP de taille nulle
- Port 0 utilisé comme service
- Petit fragment
- Sonde de port
- Utilisation de l'adresse privée d'une interface
- Usurpation d'adresse IP sur un bridge
- Usurpation de la plage d'adresse « link local » (RFC 3330)
- Utilisation de l'adresse broadcast en source
- Protocole IP invalide
- Somme de contrôle IP invalide
- Analyse de fragment IP
- Protocole GRE local
- Protocole IPSec ESP local
- Protocole IPSec AH local
- Usurpation d'adresse IP sur l'interface IPSec
- Protocole OSPF local

Alarmes MGCP

- Erreur du protocole MGCP
- Réponse MGCP sans requête
- Débordement dans le protocole MGCP
- Code malicieux possible dans le paramètre MGCP
- Paramètre MGCP interdit
- Champ SDP nécessaire manquant dans le protocole MGCP
- Limite des opérations MGCP dépassée

Alarmes SMTP

- Protocole SMTP invalide
- Caractère invalide dans l'entête SMTP

Alarmes SSL

- Données non chiffrées détectées
- Niveau de chiffrement non autorisé
- Différence dans la version SSL
- Paquet SSL invalide
- SSL Record Layer invalide

Alarmes FTP

- Attaque FTP bounce possible
- Tentative d'insertion de commande FTP PASV
- Commande FTP inconnue
- Débordement en FTP lors du login
- Débordement en FTP
- Attaque en force brute sur mot de passe FTP
- Exécution de commande via SITE EXEC
- FTP PASV DoS
- Protocole FTP invalide
- Commande port invalide
- Demande ICMP « information »
- Autorité par l'analyse ICMP
- Modification des données ECHO ICMP
- Protocole non analysé dans un message ICMP

Alarmes ICMP

- Type ICMP inconnu
- Réponse ICMP sans requête
- ICMP redirect
- Message ICMP invalide
- Demande ICMP « timestamp »
- Demande ICMP « mask »
- Somme de contrôle ICMP invalide
- Attaque possible par MTU faible

Alarmes rtcp

- Protocole RTCP invalide
- Version RTCP invalide
- Type de paquet RTCP invalide

Alarmes rtp

- Protocole RTP invalide
- Version RTP invalide
- Type de donnée RTP invalide

Alarmes Plugin SIP (TCP & UDP)

- Protocole SIP invalide
- Débordement dans le protocole SIP
- Code malicieux possible dans l'entête SIP
- Entête SIP nécessaire manquant
- Requête SIP usurpée
- Champ SDP nécessaire manquant dans le protocole SIP
- Valeur du champ SIP expires invalide
- Encodage UTF-8 invalide dans le protocole SIP
- Limite des opérations SIP dépassées
- Paramètre purpose manquant dans le protocole SIP
- Champ Via invalide dans le protocole SIP
- Paquet binaire dans le protocole SIP

Alarmes tcp

- Option TCP invalide
- Option TCP inconnue
- Mauvais numéro de séquence TCP
- Somme de contrôle TCP invalide
- Adresse multicast avec TCP
- Attaque Xmas tree
- Attaque possible par MSS faible
- Option TCP au mauvais moment
- Evasion de données sur TCP
- Adresse broadcast avec TCP
- Débordement de la file de données TCP
- Détection d'une connexion interactive
- Paquet TCP invalide par rapport à l'état
- Protocole TCP invalide

Alarmes udp

- Bouclage de port UDP
- Somme de contrôle UDP invalide
- Protocole UDP invalide

Annexe Q : Liste des commandes génériques FTP et détail du filtrage

Vérifier la trad des commandes une fois les labels traduits

- **ABOR** : Commande qui interrompt le transfert en cours. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **ACCT** : Commande qui spécifie le compte à utiliser pour se connecter. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **ADAT** : Commande qui envoie des données de sécurité pour l'authentification. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **AUTH** : Commande qui sélectionne le mécanisme de sécurité pour l'authentification. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **CCC** : Commande qui autorise le message non protégé.
- **CDUP** : Commande qui modifie le répertoire de travail au parent. Cette commande n'accepte pas d'argument. . Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **CONF** : Commande qui spécifie le message « confidentiel » utilisé pour l'authentification.
- **CWD** : Cette commande modifie le répertoire de travail. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **ENC** : Cette commande spécifie le message « privé » utilisé pour l'authentification. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.

- **EPRT** : Cette commande active le mode de transfert actif étendu. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **EPSV** : Cette commande sélectionne le mode de transfert passif étendu. Cette commande doit être passée avec au plus un argument. Cette commande est bloquée par défaut.
- **FEAT** : Cette commande affiche les extensions supportées par le serveur. Elle n'accepte pas d'argument. Le résultat de cette commande est filtré par le proxy si on demande le filtrage de la commande FEAT.
- **HELP** : Cette commande retourne les détails pour une commande donnée. Cette commande doit être passée avec au plus un argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **LIST** : Cette commande liste le contenu d'une localisation donnée d'une manière amicale.
- **MDTM** : Cette commande affiche le dernier temps de modification pour un fichier donné. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **MIC** : Cette commande spécifie le message « sain » utilisé pour l'authentification. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **MLSD** : Cette commande affiche le contenu du dossier normalisé. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **MLST** : Cette commande affiche l'information du fichier normalisé. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **MODE** : Cette commande spécifie le mode de transfert. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. Elle n'est autorisée qu'avec les arguments S, B, C et Z. Si l'analyse antivirale est activée, seul l'argument S est autorisé.
- **NLST** : Cette commande liste le contenu d'une localisation donnée de l'ordinateur de manière amicale. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **NOOP** : Cette commande ne fait rien. Elle n'accepte pas d'arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **OPTS** : Cette commande spécifie les options d'état pour la commande donnée. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PASS** : Cette commande spécifie le mot de pass utilisé pour la connexion. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PASV** : Cette commande sélectionne le mode de transfert passif. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PBSZ** : Cette commande spécifie la taille des blocs encodés. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PORT** : Cette commande sélectionne le mode de transfert actif. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PROT** : Cette commande spécifie le niveau de protection. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. En effet, seuls les arguments C, S E et P sont acceptés.
- **PWD** : Cette commande affiche le dossier de travail en cours. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **QUIT** : Cette commande termine la session en cours et la connexion. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **REIN** : Cette commande termine la session en cours (initialisée avec l'utilisateur). Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **REST** : Cette commande spécifie l'offset par lequel le transfert doit être repris. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. En effet, elle est interdite en cas d'analyse antivirale. Dans le cas contraire, le proxy vérifie qu'un seul argument est présent.
- **RETR** : Cette commande récupère un fichier donné. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC
- **SITE** : Cette commande exécute une commande spécifique du serveur. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **SIZE** : Cette commande affiche la taille de transfert pour un fichier donné. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **SMNT** : Cette commande modifie la structure de données du système en cours. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **STAT** : Cette commande affiche l'état en cours. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **STRU** : Cette commande spécifie la structure des données transférées. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. Elle n'est autorisée qu'avec les arguments F, R et P. Si l'analyse antivirale est activée, alors seul l'argument F est autorisé.

- **SYST** : Cette commande affiche l'information à propos du système d'opération du serveur. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **TYPE** : Cette commande spécifie le type des données transférées. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. Elle n'est autorisée qu'avec les commandes ASCII, EBCDIC, IMAGE, I, A, E, L. Si l'analyse antivirale est activée, seuls les arguments ASCII, IMAGE, I et A sont autorisés. L'option L peut être suivie d'un argument numérique. L'option L peut être suivie d'un argument numérique. Les options E, A, EBCDIC et ASCII acceptent les arguments suivants : N, C et T.
- **USER** : Cette commande spécifie le nom de l'utilisateur utilisé pour se connecter.
- **XCUP** : Cette commande modifie le dossier de travail au parent. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **XCWD** : Cette commande modifie le dossier de travail. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **XPWD** : Cette commande affiche le dossier de travail en cours. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.

Annexe R : Liste des commandes de modification FTP et détail du filtrage

- **ALLO** : Cette commande alloue de l'espace de stockage sur ce serveur. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **APPE** : Cette commande ajoute (ou crée) à la localisation donnée. Cette commande fait l'objet d'un filtrage plus important. En effet, cette commande est interdite lorsque l'analyse antivirale est activée (risque de contournement). Dans le cas contraire, on vérifie qu'au moins un argument est présent.
- **DELE** : Cette commande supprime un fichier donné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **MKD** : Cette commande crée un nouveau répertoire. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **RMD** : Cette commande supprime le répertoire donné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **RNFR** : Cette commande sélectionne un fichier qui doit être renommé. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **RNTO** : Cette commande spécifie le nouveau nom du fichier sélectionné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **STOR** : Cette commande conserve un fichier donné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **STOU** : Cette commande conserve un fichier donné avec un nom unique. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **XMKD** : Cette commande créée un nouveau répertoire. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **XRMD** : Cette commande supprime le répertoire donné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.

Annexe S : Liste des alarmes sensibles

Il existe 27 alarmes sensibles.

- Dns (4) : SFA_DNS_LABEL
  SFA_DNS_BADPOINTER
  SFA_DNS_LARGESTRING
  SFA_DNS_BADPROTO
- Edonkey (1) : SFA_EDONKEY_BADPROTO
- Ftp (4) : SFA_FTP_PASVINSERT
  SFA_FTP_UPOVERFLOW
  SFA_FTP_CMDOVERFLOW
  SFA_FTP_BADPROTO
- Http (7) : SFA_HTTP_WIDEBAD
SFA_HTTP_WIDEEVASION
SFA_HTTP_ESCNULL
SFA_HTTP_UTF8OVERLONG
SFA_HTTP_BADPROTO
SFA_HTTP_URLOVERFLOW
SFA_HTTP_OVERFLOW
- Mgcp (2) : SFA_MGCP_BADPROTO
SFA_MGCP_OVERFLOW
- Sip (2): SFA_SIP_BADPROTO
SFA_SIP_OVERFLOW
- Skype (1): SFA_SKYPE_DETECTED
- Smtp (1): SFA_SMTP_BADPROTO
- Ssl (3) : SFA_SSL_BADVERSION
SFA_SSL_BADPACKET
- SFA_SSL_BADRECORDLAYER

Annexe T : Liste des alarmes relatives aux protocoles

HTTP

- **Encodage en caractère %u invalide dans l'URL (Invalid %u encoding char in URL)** : cette alarme vérifie la validité des encodages de caractères en %u.
- **Evasion utilisant l'encodage %u dans l'URL (Evasion using %u encoding char in URL)** : cette alarme se déclenche par l'encodage %u d'un caractère ASCII (<256)
- **Code malicieux possible dans l'en-tête http (Possible malicious code in http header)** : cette alarme est déclenchée lors de la détection de caractères ayant un code ASCII > 127 dans l'entête http.
- **Caractère d'échappement invalide dans l'URL (Invalid escaped char in URL)** : cette alarme est déclenchée par un caractère d'échappement unicode invalide, par exemple un caractère %uXX ou XX n'est pas une valeur hexadécimale.
- **Caractère NULL codé dans l'URL (Escaped NULL char in URL :** cette alarme est déclenchée par la présence du caractère %00 dans l'URL.
- **Caractère Pourcent codé dans l'URL (Escaped percent char in URL)** : cette alarme est déclenchée par la présence du caractère %25 (encodage du '%') dans l'URL.
- **Evasion utilisant l'encodage UTF-8 (Evasion using UTF-8 encoding :** cette alarme est déclenchée par un ou plusieurs caractères encodés en UTF-8 (voir [RFC2279]).
- **Encodage UTF-8 invalide dans URL (Bad UTF-8 encoding in URL)** L'encodage UTF-8 d'un caractère analysé ne correspond à aucun caractère valide.
- **Protocole HTTP invalide (Invalid HTTP protocol)** : cette alarme est déclenchée par une utilisation impropre du protocole HTTP. Un complément au message de l'alarme spécifie la cause du rejet.
- **Débordement dans une URL (Possible buffer overflow on URL)** : Cette alarme est déclenchée par une URL dont la longueur dépasse la limitefixée par la configuration de l'ASQ.
- **Débordement dans le protocole HTTP (Possible buffer overflow on http request)** : Cette alarme est déclenchée par une ligne du corps de la requête dont la longueur dépasse la limite fixée par la configuration de l'ASQ.

- **Tunneling possible avec la méthode CONNECT (Tunneling using CONNECT method**) : Cette alarme est déclenchée par l'utilisation de la méthode CONNECT.
- **Suite de slash dans l'URL (Multiple slashes in URL) :** cette alarme est déclenchée par plusieurs « / » consécutifs dans une URL.
- **Chemin avec auto-référence (Directory self-reference)** : Cette alarme est déclenchée par une URL contenant une référence au répertoire courant (« . »)
- **Chemin avec auto-référence supérieure (Directory traversal)** : cette alarme est déclenché par une URL contenant une référence au répertoire parent (« .. »)
- **Encodage UTF-8 invalide dans URL (Bad UTF-8 encoding in URL)** : Cette alarme est déclenchée lors de la détection de champ UTF-8 invalide.
- **Chemin avec référence supérieure en dehors du répertoire racine (Directory traversal backward root folder)** : L'URL demandée contient une combinaison de points (".") et de slashs ("/").
- **Site avec rebond par redirect (Site with open redirect)** : Une redirection ouverte permet un rebond vers un autre site Web sans vérification du paramètre (exemple : www.realsite.fr/client.html?url=http://www.badsite.com.
- **Réponse 304 avec donnée (304 response with message body)** : Une réponse http « 304 Not modified » a été reçue avec un corps de message non vide. Les réponses http 304 sont utilisées par un serveur pour notifier au client qu'une page n'a pas été modifiée depuis sa dernière visite en réponse à un GET conditionnel. Les réponses 304 ne doivent pas contenir de corps de message.
- **Données additionnelles en fin de réponse (Additional data at end of reply)** : La quantité de données contenue dans une réponse http (sans keep-alive et contenant un champ d'entête Content-Lengh) dépasse la taille annoncée dans le champ Content-Lengh de l'entête http.

FTP

- **Attaque FTP bounce possible (Possible FTP bounce attack)** : Cette alarme peut-être déclenchée en mode actif ou passif.

En mode actif, le client demande au serveur de se connecter à un socket (via la commande PORT). On parle de rebond quand le client demande au serveur de se connecter à un socket qui se trouve sur une autre machine.
L'alarme est déclenchée par une commande PORT, dont l'adresse IP donnée en paramètre ne correspond pas à l'adresse source du paquet.
En mode passif, il y a rebond lorsqu'un client FTP demande à un serveur l'adresse d'un socket pour une connexion de données et que le serveur répond en spécifiant un socket sur une autre machine : l'alarme est déclenchée par une réponse à la commande PASV dont l'adresse IP donnée en paramètre ne correspond pas à l'adresse IP source du paquet.

- **Tentative d'insertion de commande FTP PASV (FTP PASV insertion attack)** : Déclenchée par une réponse à la commande PASV alors que celle-ci n'a pas été émise.
- **Commande FTP inconnue (Unknown FTP command)** : Une commande FTP inconnue a été détectée.
- **Débordement en FTP lors du login (Buffer Overflow on FTP login)** : cette alarme est déclenchée par une commande USER ou une commande PASS suivie d'un argument de plus de 100 caractères.
- **Débordement en FTP (Buffer Overflow on FTP)** : cette alarme est déclenchée par une commande (autre que USER ou PASS° suivie d'un argument de plus de 256 caractères.
- **Attaque en force brute sur mot de passe FTP (Brute force attack on FTP password)** : déclenchée par 5 tentatives de login successives.
- **Exécution de commande via SITE EXEC (Command execution using SITE EXEC)** : Déclenchée lors de la tentative d'exécution de commandes « dangereuse » sur le serveur.
- **FTP PASV Dos (FTP PASV DoS)** : Cette alrme détecte les ouvertures de connexions multiples sur un même serveur FTP. Au cours d'une même connexion FTP, Si au moins deux commandes pASV et leur réponse sont détectées et que ces réponses correspondent à deux ouvertures de ports différents, l'arme est déclenchée.
- **Protocole FTP invalide (Invalid FTP protocol)** : cette alarme est déclenchée par une session FTP que l'ASQ ne parvient pas à analyser. Quatre événements peuvent déclencher cette alarme.
- **Commande PORT invalide (Invalid PORT command)** : Une commande FTP « PORT » syntaxiquement invalide a été détectée.

EDONKEY

- **Protocole eDonkey invalide (Invalid eDonkey protocol)** : une trame eDonkey a la structure suivante (H = chiffre en hexadecimal). L'alarme est déclenchée par une trame eDonkey dont le champ taille est nulle ou strictement supérieur à 500 000 octets.

RIP

- Packet RIP invalide (Invalid RIP packet) : Déclenchée par un paquet RIP don't les paramètres ne sont pas conformes à RFC 1058 et RFC2453.

DNS

- **Récursion de label DNS (DNS label recursion)** : afin de ne pas répéter plusieurs occurrences d'un nom de domaine dans un paquet DNS, on peut remplacer une occurrence par un pointeur vers le début d'une autre.
- **DNS id spoofing (DNS id spoofing)** : L'identifiant DNS d'une réponse DNS est différent de celui de la requête. L'association entre la requête et la réponse DNS est faite en fonction de l'adresse IP et du port source utilisés par l'émetteur de la requête, qui doivent correspondre à l'adresse IP et au port de destination dans la réponse.
- **DNS zone change (DNS zone change)** : Un paquet DNS contenant l'opération Notify request.
- **DNS zone update (DNS zone update)** : Un paquet DNS contenant l'opération Zone Update.
- **Empoisonnement du cache DNS (DNS cache poisoning)** : déclenchée par une requête DNS contenant une ou plusieurs réponses (RP) additionnelles.
- **Protocole DNS invalide (Bad DNS protocol)** : Déclenchée par une utilisation impropre du protocole DNS, un complément au message de l'alarme spécifie la cause du rejet.
- **Débordement possible avec une chaine DNS (Possible buffer overflow using DNS string)** : un nom de domaine dans le paquet fait plus de 256 octets.
- **Mauvais pointeur (Bad pointer in packet)** : Un pointeur de nom de domaine pointe vers l'extérieur du paquet.

SSL

- **Données non chiffrées détectées (Unencrypted data detected)** : Des données non chiffrées ont été détectées dans une communication SSL.
- **Niveau de chiffrement non autorisé (Unauthorized cipher level)** : La négociation SSL a abouti à un niveau de chiffrement non autorisé par la politique de sécurité.
- **Différence dans la version SSL (SSL version mismatch)** : Le client SSL utilise une version du protocole différente de celle utilisée par le serveur.
- **Paquet SSL invalide (Invalid SSL packet)** : Un paquet SSL invalide a été détecté.
- **SSL Record Layer invalide (Invalid SSL Record Layer)** : Un record Layer SSL inconnu a été transmis (type, taille, contenu…). Les Records Layers SSL reçoivent des données non interprétées, des protocoles de plus haut niveau, dans des blocs non vide de taille arbitraire.
- **Protocole Skype détecté (Skype protocol detected)** : Un client Skype a probablement tenté d'ouvrir une connexion SSL. En effet, ce client de messagerie instantanée peut utiliser des connexions SSL pour contourner les équipements de sécurité classiques.

SMTP

- **Protocole SMTP invalide (Invalid SMTP protocol)** : Une communication SMTP invalide a été détectée.
- **Caractère invalide dans l'entête SMTP (invalid char in SMTP header)** : Un caractère non ASCII a été identifié dans l'entête SMTP.

MGCP

- **Erreur de protocole MGCP (MGCP protocol error)** : Une erreur a été détectée lors de l'analyse d'une communication MGCP. Un complément d'alarme précise le problème.
- **Réponse MGCP sans requête (MGCP without request)** : Le firewall a détecté une réponse MGCP n'étant associée à aucune requête. Un complément d'alarme précise la cause du rejet.
- **Débordement dans le protocole MGCP (Possible buffer overflow in MGCP request/reply)** : cette alarme est déclenchée par une requête ou une réponse dont une des lignes est plus longue que le

maximum autorisé (valuer configurable). Un complément au message de l'alarme spécifie quelle est la ligne concernée.

- **Code malicieux possible dans le paramètre MGCP (Possible malicious code in MGCP parameter)** : Déclenchée lors de la détection de caractères ayant un code ASCII > 127 dans un paramètre.
- **Paramètre MGCP interdit (Forbidden parameter in MGCP)** : Déclenchée lors de la détection d'un paramètre MGCP non autorisé.
- **Champ SDP nécessaire manquant dans le protocole MGCP (Missing mandatory SDP field in MGCP)** : Déclenchée lors de la détection de champ manquant dans le protocole SIP, un complément précise quel est le champ concerné.
- **Limite des opérations MGCP dépassée (MGCP operations limit exceeded)** : Déclenchée lorsque les limites sur les opérations MGCP sont dépassées (16 opérations au maximum, les requêtes sans réponses ayant un timeout de 2 secondes). Un complément d'alarme précise la cause du rejet.

RTP

- **Protocole RTP invalide (Invalid RTP protocol)** : Le protocole RTP est invalide. Un complément d'alarme précise la cause.
- **Version RTP invalide (invalid RTP version)** : Le numéro de version RTP est incorrect. Les deux premiers bits ne sont pas « 10 ».
- **Type de données RTP invalide (invalid RTP payload type)** : Le type de donnée détecté n'est pas dans la liste des types autorisés par la configuration. Un complément d'alarme précise la cause du rejet.

RTCP

- **Protocole RTCP invalide (Invalid RTCP protocol)** : Le protocol RTP est invalide. Un complément d'alarme précise la cause.
- **Version RTCP invalide (Invalid RTCP version)** : Le numéro de version RCTP est incorrecte les deux premiers bits ne sont pas « 10 ».
- **Type de paquet RTCP invalide (Invalid RCTP packet type)** : Le type de paquet détecté n'est pas dans la liste des types autorisés par la configuration. Un complément d'alarme précise la cause du rejet.

SIP

- **Protocole SIP invalide (invalid SIP protocol)** : déclenchée par une utilization impropre du protocole SIP, un complément au message de l'arme spécifie la cause du rejet.
- **Débordement dans le protocole SIP (Possible buffer overflow in SIP request/reply)** : Cette alarme est déclenchée par une requête ou une réponse dont une des lignes est plus longue que le maximum autorisé (valeur configurable). Un complément au message de l'alarme spécifie quelle est la ligne concernée.
- **Code malicieux possible dans l'entête SIP (Possible malicious code in SIP header)** : Déclenchée lors de la détection de caractères ayant un code ASCII > 127 dans l'entête SIP.

Entête SIP nécessaire manquant (Missing mandatory header in SIP) : déclenchée lorsque l'entête SIP, qui est obligatoire, n'est pas trouvé.

- **Requête SIP usurpée (Possibly spoofed SIP request)** : Déclenchée lors de la détection d'une requête SIP qui a probablement été usurpé.
- **Champ SDP nécessaire manquant dans le protocole SIP (Missing mandatory SDP field in SIP)** : déclenchée lors de la détection de champ manquant dans le protocole SIP, un complément précise quel est le champ concerné.
- **Valeur du champ SIP expires invalide (Bad expires field value in SIP)** : déclenchée lorsque la valeur de la date d'expiration n'est pas valide.
- **Encodage UTF-8 invalide dans le protocole SIP (Bad UTF-8 encoding in SIP)** : déclenchée lors de la détection de champ UTF-8 invalide.
- **Limite des opérations SIP dépassée (SIP operations limit exceeded)** : Déclenchée lorsque les limites sur les opérations SIP sont dépassées (8 opérations au maximum, les requêtes sans réponses ayant un timeout de 60 secondes). Un complément d'alarme précise la cause du rejet.
- **Paramètre purpose manquant dans le protocole SIP (Missing purpose parameter in SIP)** : Déclenchée lorsque le paramètre « purpose » n'est pas présent dans le « Call-info » pour au moins une URL.

- **Champ Via invalide dans le protocole SIP (Bad Via header in SIP)** : déclenchée lorsque le champ « Via » n'est pas valide, un complément d'alarmes précise la cause du rejet.
- **Paquet binaire dans le protocole SIP (Binary packet in SIP)** : un caractère ASCII « 0 » a été détecté dans le paquet.

GLOSSAIRE

Les termes définis dans ce glossaire couvrent les sujets abordés dans ce manuel.

100BaseT

Connue également sous le nom " Fast Ethernet", celle-ci est la version 100 Mbps de l'Ethernet au lieu des 10 Mbps standard. Tout comme l'Ethernet standard, le Fast Ethernet est un réseau partagé sur lequel la bande passante de 100 Mbps est répartie sur tous les nœuds.

A

Active Update

Le module Active Update des firewalls permet la mise à jour de la base des antivirus, les signatures contextuelles ASQ, la liste des serveurs antispam et les URLs utilisées pour le filtrage URL dynamique.

Adresse IP

(IP pour Internet Protocol). Numéro composé de 4 nombres séparés par un point qui identifie chaque ordinateur sur Internet.

Adresse IP privée

Quelques plages d'adresses IP, peuvent être librement utilisées comme adresses privées sur un Intranet, c'est-à-dire sur un réseau local utilisant le protocole TCP/IP. Les plages d'adresses privées sont :

- 172.16.0.0 à172.31.255.255.
- 192.168.0.0 à 192.168.255.255.
- 10.0.0.0 à 10.255.255.255.

AES (*Advanced Encryption Standard*)

Algorithme de chiffrement utilisant des clés de 128 ou 256 bits. Cet algorithme est plus performant et sécurisé que le 3-DES, utilisé comme standard de fait jusqu'à présent.

Algorithme d'échange de clés Diffie Hellmann

Un algorithme qui permet aux parties d'échanger leurs clés publiques de façon sécurisée afin d'arriver à une clé secrète partagée aux deux extrémités, sans devoir transmettre la clé secrète. Ainsi, le risque d'interception de la clé secrète est évité. Cet algorithme ne réalise pas de chiffrement de données, et s'utilise même sur les canaux non-sécurisés.

Les groupes de négociation Diffie Hellmann sont par exemple :

- Le groupe 14 qui utilise une longueur de clé de xxxx bits.
- Le groupe 15 qui utilise une longueur de clé de xxxx bits.
- Le groupe 16 qui utilise une longueur de clé de xxxx bits.

Algorithme de chiffrement de données (*DES*)

Un algorithme cryptographique utilisé pour le chiffrement des données. Il permet notamment le chiffrement par blocs de données.

Alias IP (*IP Alias)*

Une adresse supplémentaire associée à une interface

Analyse protocolaire

Une méthode d'analyse et de prévention d'intrusion basée sur la comparaison entre le trafic et les normes définissant les protocoles.

Analyseur de paquets

Lorsqu'une alarme se déclenche sur un firewall NETASQ, il est possible de visualiser le paquet responsable du déclenchement de cette alarme. Pour cela il faut vous munir d'un outil de visualisation de paquets comme WIRESHARK ou PACKETYSER. Spécifiez l'outil choisi dans le champ "Analyseur de paquets", celui-ci sera utilisé par le Reporter pour afficher les paquets malicieux.

Antispam

Système permettant de diminuer le nombre de messages électroniques non sollicités et parfois malveillants qui saturent les systèmes de messagerie et tentent d'abuser les utilisateurs.

Antispyware

Système permettant de détecter et/ou de bloquer la prolifération des logiciels espions (qui collectent des informations personnelles pour les transmettre à l'extérieur) sur les postes clients.

Antivirus

Système de détection et/ou d'éradication des virus et vers informatiques.

Antivirus (*Kaspersky*)

Un programme antivirus intégré et développé par Kaspersky Labs, qui détecte et élimine les virus en temps réel. Au fur et à mesure de la découverte de nouveaux virus, la base de signatures doit être mise à jour afin que le programme antivirus soit efficace.

Appliance

Boîtier hardware embarquant un logiciel ainsi que son système d'exploitation.

Appliance backup

Précédemment, celui-ci portait le nom "secondaire". Il s'agit d'un appliance de secours utilisé dans une architecture de haute disponibilité où il prend le relais sur les opérations de l'appliance principal lorsque celui-ci tombe en panne. Ainsi il assure la continuité de l'opération du système avec le minimum d'inconvénients aux utilisateurs du réseau.

ASQ (*Active Security Qualification*)

La technologie qui apporte aux firewalls NETASQ non seulement un haut niveau de sécurité mais aussi une aide à la configuration très performante et des outils d'administration intuitifs. Ce moteur de détection et de prévention d'intrusions intègre un système de prévention d'intrusions qui supprime toute activité malveillante en temps réel.

Attaque force brute

Méthode utilisée pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles. Cette méthode de recherche exhaustive ne réussit que dans les cas où le mot de passe cherché est constitué de peu de caractères.
Pour contrer cette attaque, il suffit simplement de choisir des mots de passe d'une grande longueur ou des clés suffisamment grandes. Ainsi, l'attaquant devra mettre beaucoup de temps pour trouver le bon mot de passe.

Authentification

Le processus de vérification de l'identité d'un utilisateur ou l'origine d'un message transmis, assurant que l'entité (utilisateur, machine…) réclamant un accès est bien celle qu'elle prétend être. L'authentification peut aussi faire référence à la procédure de vérification de l'intégrité d'une transaction.

Asic (*Application-Specific Integrated Circuit*)

Circuit intégré conçu spécialement pour une ou plusieurs fonctionnalités bien déterminées. Ces fonctions sont alors gérées directement par le circuit et pas par le logiciel. Un ASIC n'est pas reprogrammable.

B

Bande passante

La capacité de transmission d'un médium électronique (par exemple, les voies de communication). Cette capacité se mesure en bits ou octets par seconde sur une voie numérique et en Hertz sur une voie analogique (cycles par seconde).

Blowfish

Une méthode de cryptographie à clé secrète utilisant des clés entre 32 et 448 bits. Cette méthode est un remplacement gratuit de DES ou IDEA.

Bufferings

Stockage temporaire d'information afin de la manipuler et la traiter en une seule fois, plutôt qu'au fur et à mesure.

C

Carnet d'adresses

Il s'agit d'un outil central des applications NETASQ. Ce carnet peut contenir l'ensemble des informations de connexion nécessaires pour une connexion à une liste de firewalls, ainsi, l'accès de l'administrateur est simplifié car il ne lui est plus indispensable de retenir les mots de passe que cela implique.

Certificat

(Voir Certificat numérique.)

Certificat de l'autorité de certification

Autorité : une société ou organisation tierce de confiance qui délivre des certificats numériques. Son rôle est de garantir que le détenteur du certificat est bien celui qu'il prétend être. Les autorités de certification sont critiques à la sécurité des données et à l'e-commerce car elles garantissent l'intégrité de l'identité des parties échangeant des données.

Certificat numérique

L'équivalent numérique d'une pièce d'identité pour une utilisation dans un système de chiffrement de clés publiques, il est utilisé principalement pour vérifier l'intégrité de l'identité de l'utilisateur et aussi pour donner au destinataire du message un moyen de chiffrer sa réponse. La plupart du temps, le format X.509, qui contient les informations concernant l'utilisateur et l'autorité de certification, est employé.

Châssis

Une structure physique qui sert à héberger les composants électroniques. Au moins un châssis est nécessaire dans tout système informatique afin de contenir les câbles et cartes de circuit imprimé.

Cheval de Troie

Code inséré dans un type de logiciel d'apparence légitime, mais qui va exécuter des actions frauduleuses telles que le vol d'informations.

Chiffrement

Le processus de translation des données brutes (en clair) vers une version apparemment embrouillée (le cryptogramme) afin de protéger la confidentialité, l'intégrité et l'authenticité des données d'origine. Une clé secrète est souvent nécessaire pour désembrouiller (déchiffrer) le cryptogramme.

Clé privée

Une ou deux clés nécessaires dans un système de clés publiques ou asymétriques. La clé privé est habituellement gardée secrète par son propriétaire.

Clé publique

Une ou deux clés nécessaires dans une cryptographie de clé publique ou asymétrique. La clé publique est généralement reconnue publiquement.

Concentrateur (*Hub*)

Un point de connexion central dans un réseau reliant tous les segments d'un LAN.

Contexte

Le statut, condition ou mode actuel d'un système.

CPU (*Unité Centrale de Calcul*)

Plus connue sous le nom de processeur. Il s'agit d'une ressource interne au firewall responsable des calculs à effectuer.

Critères communs

Une norme internationale, les critères communs évaluent (sur des niveaux d'assurance d'évaluation allant de 1 à 7) la capacité d'un produit à apporter des fonctions de sécurité pour lesquelles il a été conçu, ainsi que la qualité de son cycle de vie (développement, production, livraison, mise en service et mises à jour).

Cryptographie

Le chiffrement et déchiffrement des données.

Cryptographie asymétrique

Un type d'algorithme de cryptographie utilisant des clés différentes pour le chiffrement et pour le déchiffrement. La plupart du temps, la cryptographie asymétrique est plus lente que la cryptographie symétrique et est utilisée pour l'échange des clés et pour les signatures numériques. RSA et Diffie-Hellman sont des exemples d'algorithmes asymétriques.

D

Datagramme

Un bloc d'informations transmis sur une voie de communication au sein d'un réseau.

Débit

Unité mesurant la vitesse de transmission des données dans une voie de communication. Pour une liaison numérique, il s'agit du nombre de bits transférés en un temps donné. Pour une connexion Internet, le débit s'exprime en kbps (kilobits par seconde).

Débordement du tampon

Une attaque qui procède souvent par l'envoi d'une quantité de données supérieure à ce que peut contenir le tampon, afin de provoquer une panne du programme (le tampon étant une zone de mémoire temporaire utilisée par l'application). Le but de cette attaque est d'exploiter la panne et d'écraser une partie du code de l'application avec du code malicieux. Ce dernier sera exécuté une fois entré dans la mémoire.

Déni de service

Le déni de service est généralement provoqué par une attaque informatique (par exemple, une attaque par saturation au moyen de virus paralysant un service de courrier électronique) ; cependant il peut être causé par une surcharge de demandes d'accès en raison d'un événement exceptionnel.

Dépassement de Tampon (*Buffer Overflow*)

Un dépassement ou débordement de tampon est un bug pouvant être exploité pour violer la politique de sécurité d'un système. Technique souvent utilisé par les pirates informatiques.

Détection de systèmes d'exploitation

Une méthode pour déterminer le système d'exploitation et d'autres caractéristiques d'une machine distante par l'utilisation des outils tels queso ou nmap.

DHCP (*Dynamic Host Configuration Protocol*)

Protocole permettant à une machine qui se connecte sur un réseau d'obtenir dynamiquement sa configuration (principalement sa configuration réseau). Le DHCP trouve une adresse IP seul. Le but étant la simplification de l'administration d'un réseau.

Dialup

Interface sur laquelle est branché le modem.

DMZ (*Zone démilitarisée*)

La zone tampon d'un réseau d'entreprise, située entre le réseau local et l'internet, derrière le firewall. Elle correspond à un réseau intermédiaire qui relie les serveurs publics (HTTP, SMTP, FTP...) et dont le but est d'éviter toute connexion directe avec le réseau interne afin de pouvoir le prévenir d'une attaque externe du web.

DNS (*Système de Noms de Domaine*)

Système distribué de bases de données et de serveurs, qui assure la traduction des noms de domaine utilisés par les internautes en numéros Internet utilisables par les ordinateurs, ceci pour permettre la transmission des messages d'un site à l'autre du réseau.

E

Encapsulation

Une façon de transmettre plusieurs protocoles au sein du même réseau. Les trames d'un type de protocole sont portées dans les trames d'un autre.

Enrôlement des utilisateurs

Lorsqu'un service d'authentification est mis en place, il faut définir chaque utilisateur autorisé en créant un objet "utilisateur". Plus la société est important, plus cette tâche est fastidieuse. Le service d'enrôlement Web de NETASQ permet de faciliter cette tâche. Désormais, c'est l'utilisateur "inconnu" qui demande la création de son compte et de son certificat (si une PKI a été définie par l'administrateur).

Entête

Un ensemble d'informations temporaire ajouté au début d'un texte afin de le transférer sur le réseau. Typiquement, un entête contient les adresses source et destination ainsi que les données décrivant le contenu du message.

Entête d'authentification

Un ensemble de données permettant de vérifier que le contenu d'un paquet n'a pas été modifié et aussi de valider l'identité de l'expéditeur d'un paquet.

Ethernet

Protocole de réseau informatique à commutation de paquets. Il s'agit d'une technologie permettant à toutes les machines d'un réseau local de se connecter sur une même ligne de communication.

Ethernet Gigabit

Une technologie Ethernet qui augmente la vitesse de transmission à 1 Gbps (1000Mbps).

Evasion de données

Aussi connue sous l'appellation "évasion des systèmes de détection d'intrusions", celle-ci est une méthode qui permet de tromper un système de détection d'intrusions en lui présentant des paquets formés à partir d'en-têtes similaires, mais qui contiennent des données différentes de celles que la machine cliente recevra.

F

Filtrage
Opération qui consiste à utiliser un filtre. (*Voir Règle de filtrage.)*

Filtrage d'URL
Service permettant d'empêcher la consultation de certains sites web. Les filtres peuvent être réalisés au moyen de catégories contenant de nombreuses URL (adresses web) interdites (exemple : sites de pornographie, sites de jeux, sites web mail…) ou de mots-clés (exemple : sexe, porno…).

Firewall
Fonction de base de la sécurité informatique péri métrique. Equipement ou logiciel permettant de filtrer les accès de/vers l'entreprise.

Firmware
Logiciel qui permet le fonctionnement d'un composant informatique avant les drivers.

Fonction de Hachage
Un algorithme qui convertit du texte de longueur variable vers une sortie de taille fixe. Cette fonction est souvent utilisée dans la création des signatures numériques.

Full duplex
Communication bidirectionnelle pour laquelle l'envoi et la réception peuvent s'effectuer simultanément.

G

Gatekeeper
Il s'agit d'éléments optionnels dans une solution H323 qui permettent de réaliser la traduction d'adresses et la gestion des autorisations.

H

Half-duplex
Mode de communication unidirectionnelle. Les données sont envoyées dans une seule direction à la fois.

Haute disponibilité
Une solution basée sur un groupe de deux firewalls identiques, qui se surveillent. Lorsqu'une panne survient dans le logiciel ou matériel du firewall pendant son utilisation, le deuxième firewall prend le relais. Le basculement entre les firewalls est complètement transparent pour l'utilisateur.

Hot swap

Echange d'éléments matériels comme les disques durs, les ventilateurs ou les cartes réseau "à chaud", c'est à dire alors que le matériel est toujours en fonctionnement.

Hub and spoke

(Vient de l'anglais Hub and Spoke). Dispositif informatique placé comme point de connexion central qui peut atteindre chacune des terminaisons situées à la périphérie.

Hypertexte

Terme utilisé (sur le Web) pour du texte qui contient des liens permettant de passer d'une partie d'un document à une autre, ou d'un document à d'autres documents.

I

ICMP (*Internet Control Message Protocol*)

Protocole assurant le contrôle et la gestion du protocole IP.

IDS (*Intrusion Detection System*)

Système permettant de détecter les tentatives d'intrusion mais ne les bloque pas.

IKE *(Pour Internet Key Exchange)*

Une méthode qui établit une SA qui authentifie les algorithmes de chiffrement et d'authentification à appliquer sur les datagrammes qu'elle couvre, ainsi que les clés secrètes associées.

Interface

Une interface est une zone, réelle ou virtuelle qui sépare deux élements. L'interface désigne ainsi ce que chaque élément a besoin de connaître de l'autre pour pouvoir fonctionner correctement.

IPS (*Intrusion Prevention System*)

Système permettant de détecter et de bloquer les tentatives d'intrusion, du niveau "réseau" de la norme OSI jusqu'au niveau "applicatif".

IPSEC

Protocole standardisé permettant l'établissement de tunnels VPN sécurisés, c'est à dire de véritables réseaux privés virtuels sur un réseau public comme Internet. Les informations transitant dans ces tunnels virtuels sont chiffrées et authentifiées, et sont donc complètement sécurisées.

ISAKMP (*Internet Security Association and Key Management Protocol)*

Association de Sécurité Internet et Protocole de Management de Clé). Protocole à travers lequel les transactions entre des entités TCP/IP sont établies.

K

Kernel *(Noyau)*
Cœur du système d'exploitation.

L

LAN (*Local Area Network*)
Un réseau local est un réseau informatique à une échelle relativement restreinte, par exemple une salle informatique, une habitation particulière, un bâtiment ou un site d'entreprise.

LDAP (*Lightweight Directory Access Protocol*)
Protocole permettant l'interrogation et la modification des services d'annuaire.

Leased line
Une connexion téléphonique permanente entre deux points, contrairement au dialup. Généralement utilisé par les entreprises pour connecter des entreprises distantes.

Liste de révocation des certificats (*CRL*)
Une liste des certificats révoqués ou considérés comme n'étant plus dignes de confiance avant leur expiration. Elle est publiée et mise à jour de façon régulière par une autorité de certification afin d'assurer la validité des certificats existants.

Load balancing (Répartition de charge)
Technique utilisée pour distribuer un travail entre plusieurs processus, ordinateurs, disques ou autres resources. Cela permet ainsi l'augmentation de la qualité des services, l'amélioration des temps de réponse des services, la capacité de pallier la défaillance d'une ou de plusieurs machines, la possibilité d'ajouter des serveurs sans interruption de service.

Logs
(Voir Traces).

M

MAC address (*Medium Access Control Address*)
Une adresse MAC est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire et utilisé pour attribuer mondialement une adresse unique au niveau de la couche de liaison (couche 2 du modèle OSI).

Man-in-the-middle attack (*Attaque de l'homme du milieu*)
Attaque dans laquelle l'attaquant est capable de lire, insérer et modifier comme il le souhaite les messages chiffrés entre 2 parties, sans que ni l'un ni l'autre ne puisse se douter que la ligne entre eux a été compromise. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. L'attaque HDM est particulièrement applicable dans le protocole original d'échange de clés Diffie-Hellman, quand il est utilisé sans authentification.

MAP

(Voir Translation unidirectionnelle).

Méthode défi/réponse

Une méthode d'authentification pour vérifier la légitimité des utilisateurs qui se connectent sur un réseau, où un utilisateur sera demandé (le défi) de fournir des informations personnelles (la réponse). Lorsqu'un utilisateur se connecte, le serveur utilisera les informations du compte pour renvoyer un "défi" à l'utilisateur. L'utilisateur saisira alors ce numéro sur une carte de la taille d'une carte de crédit. Celle-ci générera une réponse qui sera renvoyée au serveur.

Mode avancé (Routeur)

Mode de configuration dans lequel le firewall fonctionne comme un routeur entre ses différentes interfaces. Cela implique certains changements d'adresses IP sur les routeurs ou serveurs lorsque vous les déplacez dans un réseau différent (derrière une interface du réseau différente).

Mode Bridge ou mode transparent

Le mode transparent, aussi appelé "bridge" en anglais, permet de conserver le même adressage entre les interfaces. Il simule un pont filtrant, c'est-à-dire qu'il est traversé par l'ensemble du trafic du réseau. Cependant, vous pouvez ensuite filtrer les flux qui le traversent suivant vos besoins et donc protégéer telle ou telle partie du réseau.

Mode hybride

Le mode hybride utilise le mode transparent et le mode avancé simultanément. Ce mode ne peut être emplyé que pour les produits NETASQ possédant plus de deux interfaces réseau. Vous povez définir plusieurs interfaces en mode transparent (par exemple : zone interne et DMZ ou zone externe et DMZ) et certaines interfaves dans un plan d'adressage différent.

Modularité

Terme qui décrit un système qui a été divisé en petites unités qui, rassemblées, composeront l'ensemble du système.

MSS (*Maximum Segment Size) (MSS : Longueur maximum de segment*)

Il s'agit de la quantité de données en octets qu'un ordinateur ou tout équipement de communication peut contenir dans une trame seule et non fragmentée. Pour obtenir le meilleur rendement possible, la taille du segment de données et de l'en-tête doivent être inférieure au MTU.

N

NAT (*Network address translation*)

(*Translation d'adresses réseau*.) Mécanisme implanté sur un routeur qui permet de faire correspondre les addresses IP internes non-unique et souvent non routables d'un domaine vers un ensemble d'adresses externs uniques et routables. Ce mécanisme permet de pallier la carence d'adresses IPv4 sur Internet, le protocole IPv6 dispose d'un espace d'adressage plus important.

NETASQ EVENT REPORTER

Module de la suite d'administration NETASQ qui permet la visuaisation des informations de logs, générées par les firewalls.

NETASQ REAL-TIME MONITOR

Module de la suite d'administration NETASQ qui permet la visualisation de l'activité du firewall en temps réel.

NETASQ Shield

Agent de protection de postes et serveurs sous Microsoft Windows® intégrant la technologie NETASQ ASQ.

NETASQ UNIFIED MANAGER

Module de la suite d'administration NETASQ qui permet la configuration du/des firewall(s).

Non-repudiation

Il s'agit du fait de s'assurer qu'un contrat (notamment signé via Internet) ne peut être remis en cause par l'une des parties.

NTP (*Network Time Protocol*)

(Protocole horaire en réseau) est un protocole permettant de synchroniser les horloges des systèmes informatiques à travers un réseau de paquets, dont la latence est variable.

O

Objet

Objets utilisés pour la configuration du filtrage et de la translation d'adresses. Il peut s'agir de machines, d'utilisateurs, de plage d'adresses, de réseaux, de services, de protocoles, de groupes, de groupes d'utilisateurs et de groupes réseaux.

OSI

Norme internationale définie par l'ISO décrivant un modèle générique en 7 couches pour l'interconnexion de systèmes réseau hétérogènes. On parle souvent de la couche "réseau" à laquelle est lié le protocole IP, de la couche "Transport" à laquelle sont liés les protocoles TCP et UDP et de la couche application correspondant aux protocoles applicatifs (SMTP, HTTP, HTTPS, IMAP, Telnet, NNTP…).

P

Paquet

Désigne une unité d'information véhiculée sur un réseau. Un paquet contient un entête (contenant des informations sur le paquet et sur les données) et des données utiles qui doivent être transmis à la destination.

Partition

Section d'un disque ou d'une mémoire reservéà une application particulière.

Passerelle

Une machine qui se comporte comme l'entrée ou le point de connexion entre deux réseaux (par exemple, un réseau interne et l'internet) utilisant les mêmes protocoles.

PAT (*Port Address Translation*)

(*Redirection de ports*). La redirection de port permet de rediriger les paquets en provenance d'une ou plusieurs sources à destination d'une ou plusieurs adresses IP.

Peer-to-peer

Liaison poste à poste permettant grâce à un logiciel spécifique d'échanger facilement des fichiers ou des informations. Ce système ne requiert pas de serveur central, ce qui rend son contrôle très difficile mais permet une répartition de charge.

Ping (*Packet Internet Groper*)

Une commande informatique utilisée pour determiner si une adresse IP est accessible. Une requête ICMP est envoyée d'une machine à une autre. Si la machine ne répond pas, il se peut qe l'on ne puisse pas communiquer avec elle.

PKI (*Public Key Infrastructure*)

Système permettant la génération, la publication et la gestion de clés publiques ou privées numériques qui seront utilisées pour l'authentification et le chiffrement des communications des utilisateurs du système.

Plugin

Un programme auxiliaire qui ajoute une caractéristique ou un service particuliers à un système plus large et travaille avec un logiciel principal qui lui apporte de nouvelles fonctionnalités.

Politique de filtrage

L'un des aspects les plus importants en matière de sécurité des ressources que le firewall protège. Etablissement de règles de filtrage qui permet d'éviter les failles réseau

Politique de sécurité

Les règles d'une organisation et les regulations qui gouvernent les propriétés et l'implémentation de l'architecture du réseau en matière de sécurité.

Pont (*Bridge*)

Un équipement reliant deux segments LAN qui peuvent être de type similaire ou hétérogène (par exemple, Ethernet et Token Ring Le bridge s'insère dans un réseau afin de le segmenter et de contenir les flux dans les segments, ceci pour améliorer les performances. Les bridges apprennent de leurs expériences et créent des tables d'adresses des nœuds sur le réseau. Ils apprennent quels bridges appartiennent au segment en se souvenant des machines qui ont accusé réception de l'adresse envoyée.

Port Ethernet

(Voir Ethernet)

Scan de port

Un scan de port est une technique qui permet de rechercher les ports ouverts chez une machine du réseau. Elle est utilisée par les administrateurs pour contrôler les machines de leurs réseaux et par les pirates informatiques pour tenter de la compromettre.

PPP (*Point-to-Point Protocol*)

Une méthode qui permet d'établir une connexion d'un ordinateur vers Internet. Il s'agit du protocole le plus couramment utilisé pour se connecter à Internet sur les lignes téléphoniques normales.

PPPoE (*Point-to-Point Protocol over Ethernet*)

Protocole bénéficiant des avantages de PPP (séurité par chiffrement, contrôle de connexion…). Couramment utilisé pour les connexions haut-débit à Internetn par ADSL et câble.

PPTP (*Point-to-Point Tunneling Protocol*)

Protocole utilisé pour créer un réseau privé virtuel (VPN) surInternet. Internet devient un réseau ouvert. PPTP est utilisé pour s'assurer que les messages transmis d'un nœud VPN vers un autre soient sécurisés.

Protocole DHCP

Un logiciel qui attribue automatiquement des adresses IP aux postes client se connectant sur un réseau TCP/IP. Avec lui, les administrateurs peuvent se passer de l'attribution manuelle d'adresses. Typiquement, les logiciels DHCP s'exécutent dans les serveurs et se trouvent également dans les équipements réseau tels les routeurs RNIS et routeurs modem qui permettent à plusieurs utilisateurs d'accéder à l'internet. Les nouveaux serveurs DHCP mettent à jour les serveurs DNS automatiquement après les attributions.

Protocole FTP (*File Transfer protocol*)

Un protocole internet couramment utilisé pour l'échange de fichiers entre systèmes. Contrairement aux autres protocoles TCP/IP, le protocole FTP utilise deux connexions – l'une pour l'échange de paramètres et l'autre pour les données réelles.

Protocole HTTP

Le protocole utilisé dans le transfert entre un serveur web et un client web de documents en hypertexte.

Protocoles

Ensemble de règles standardisé qui définit le format et le déroulement d'une communication entre deux systèmes. Les protocoles sont utilisés à chaque niveau du modèle OSI.

Proxy

Système qui a pour fonction de relayer des connexions qu'il intercepte ou qui lui sont adressées. Ainsi le proxy se substitue à l'initiateur de la connexion et recrée intégralement une nouvelle connexion vers la destination initiale. Les systèmes proxy peuvent notamment être utilisés pour réaliser des opérations de cache ou de filtrage des connexions.

Proxy HTTP

Un serveur proxy qui se spécialise dans les transactions HTML.

Protocole Internet

Protocole utilisé pour le routage des paquets sur les réseaux. Son rôle est de sélectionner le meilleur chemin à travers les réseaux pour l'acheminement des paquets.

Proxy SMTP

Un server proxy qui spécifie les transactions SMTP (mail).

PVM

Logiciel qui permet d'utiliser un ensemble de stations de travail UNIX reliées à un réseau comme une machine parallèle. (PVM est le nom de code interne pour NETASQ SEISMO).

Q

QoS (*Quality of Service*)

(*Qualité de Service)*. Cela permet de véhiculer dans de bonnes conditions, un type de trafic donné en termes de disponibilité, débit…
Ainsi les ressources du réseau sont optimisées et les performances aux applications critiques sont garanties.

Quarantaine dynamique

Mise en quarantaine décidée suite à un évènement spécifique, par exemple, le déclenchement d'une alarme particulière.

Quarantaine statique

Mise en quarantaine décidée par l'administrateur au moment de la configuration du firewall.

QID

Identifiant de file d'attente QoS.

R

RADIUS (*Remote Authentication Dial-In User Service*)

Un protocole de contrôle d'accès qui utilise une méthode client-serveur pour centraliser des données d'authentification. Les informations de l'utilisateur sont transmises à un serveur RADIUS, qui vérifie l'information et autorise ou refuse les accès.

RAID (*Redundant array of independant disks*)

Architecture matérielle permettant d'accélérer, de sécuriser et/ou de fiabiliser les accès aux données stockées sur disques durs. Cette méthode est basée sur la multiplication des disques durs.

Redirection de port (REDIRECT)

Utilisation d'une seule adresse IP pour contacter plusieurs serveurs.

Règle de filtrage

Une règle créée pour exécuter plusieurs actions sur les paquets entrants et sortants. Parmi les actions possibles : bloquer, passer ou ignorer un paquet. Les règles peuvent également être configurées pour générer des alarmes qui avertiront l'administrateur du passage d'un certain type de paquet.

Règle de filtrage implicite

Règle de filtrage implicitement générée par le firewall suite à la modification de sa configuration par l'administrateur. Par exemple, en activant le proxy http, un jeu de règles de filtrage implicite est généré pour permettre les connexions entre le client et le proxy ainsi qu'entre le proxy et le serveur.

Rejeu

La protection contre le rejeu permet de ne pas donner à un attaquant la possibilité de ré-émettre une donnée déjà transmise.

RFC (*Request for Comments*)

Une série de documents qui communiquent des informations sur l'Internet. N'importe qui peut soumettre un commentaire, mais seul l'Internent Egineering Task Force (IETF) décide si les standards deviennent des RFC. Un n° est assigné à chaque RFC, et il ne peut être modifié une fois publié.

Routage dynamique

Routage qui s'adapte automatiquement aux changements qui surviennent dans un réseau, pour permettre aux paquets de données d'emprunter la meilleure voie disponible.

Routeur

Matériel de communication de réseau qui permet de limiter les domaines de diffusion et de déterminer le prochain nœud du réseau auquel un paquet de données doit être envoyé, afin que ce dernier atteigne sa destination finale le plus rapidement possible.

Routeur de filtrage

Un routeur qui met en œuvre les filtres de paquet.

Routing protocol

Une formule utilisée par les routeurs pour determiner le chemin approprié par lequel chaque donnée peut être expédiée. Grâce au protocole de routage, un réseau peut répondre dynamiquement à des conditions changeantes, cependant, toutes les décisions de routage doivent être définies.

RPC (*Remote Procedure Call*)

Protocole qui autorise un programme à utiliser des services d'un autre programme à l'aide d'un serveur d'applications. Ce protocole est utilisé dans le modèle client-serveur et permet de gérer les différents messages entre les entités.

RPV (*Réseau Privé Virtuel*)

Voir "Tunnel VPN".

S

SA (*Security Association*)

Extrêmité d'un tunnel VPN.

SCSI (*Small computer system interface*)

Standard définissant une interface entre un ordinateur et son ou ses périphériques de stockage, reconnue pour sa fiabilité et ses performances.

SEISMO

Module qui permet à l'administrateur réseau de collecter en temps réel des informations et de les analyser afin de découvrir d'éventuelles vulnérabilités susceptibles de détériorer son réseau. Il permet, entre autres, de remonter les alertes venant de l'ASQ et de maintenir ainsi une politique de sécurité optimale.

Serveur Proxy
(Voir Proxy)

Service
(Egalement appelé Daemon), désigne une application ayant un fonctionnement permanent en arrière-plan dans le système d'exploitation.

Clé de session
Une clé cryptographique valable une seule fois et pour une période limitée. Une fois le délai expiré, la clé est détruite, à condition que la clé soit interceptée, les données ne seront pas compromises.

Signature
Un code qui peut être attaché à un message, identifiant uniquement l'expéditeur. Comme une signature écrite, le but de la signature digitale est que la personne qui envoie réellement le message est celui qu'il prétend être.

Signature contextuelle
Signature d'une attaque, c'est-à-dire la formae que prend une attaque. L'ASQ s'appuie sur une base de signatures contextuelles pour détercter rapidement les attaques connues.

Signature numérique - Signature digitale
Méthode qui permet de vérifier les identités sur un réseau basé sur le chiffrement de clé publique.

Utilisation unique du mot de passe
Une méthode d'authentification sécurisée qui dissuade les abus de mots de passe en intégrant un nouveau mot de passe à chaque ouverture de session.

Slot
Fichiers de configuration au sein de l'application NETASQ UNIFIED MANAGER numérotés de 01 à 10 et permettant de génerer des politiques de filtrage, de NAT…

SMTP (*Simple Mail Transfer Protocol*)
(Protocole simple de transfert de courrier). Protocole de communication TCP/IP utilisé pour le courrier électronique vers les serveurs de messagerie électronique.

SNMP (*Simple Network Management Protocol*)
Protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes réseau à distance.

SSH (*Secure Shell*)
Programme informatique et protocole de communication sécurisé pour les cliets-serveurs Windows et UNIX.

SSL (*Secure Socket Layer*)
Protocole de sécurisation des échanges sur Internet. Ce protocole fournit une couche de sécurité (authentification, intégrité, confidentialité) aux protocoles applicatifs qu'il supporte.

Stateful Inspection

Méthode de filtrage des connexions réseau, inventé par Check Point, basée sur une conservation de l'état de la connexion. Les paquets ne sont autorisés que s'ils correspondent au déroulement normal de la connexion. Si une règle de filtrage autorise certaines connexions sortantes, elle autorisera implicitement les paquets entrants qui correspondent aux réponses de ces connexions.

Cryptographie à clé symétrique

Un type d'algorithme cryptographique dans lequel la même clé est utilisée pour l chiffrement et le déchiffrement. La difficulté de cette léthode réside dans la transmission de la clé à un utilisateur légitime. DES, IDEA, RC2 et RC4 sont des exemples d'algorithmes à clé symétrique.

T

Tampon (B*uffer*)

Zone de stockage intermédiaire.

Topologie en étoile/Réseau

Un réseau local dans lequel les machines sont reliées à un ordinateur central, un hub ou un switch. L'inconvénient de cette architecture est que les données doivent passer à travers le point central, pouvant provoquer un risque de saturation.

TCP (*Transmission Control Protocol)*

Protocole de transport fiable, en mode connecté. La sessionTCP fonctionne en trois phases : l'établissement de la connexion, les transferts de données, et la fin de la connexion.

Trace route

Mécanisme de découverte du chemin emprunté par un paquet pour aller d'un bout à l'autre d'un réseau.

Traces

Journaux de traces utilisés pour l'analyse de l'activité réseau.

Translation (map-bidirectionnel)

Ce type de translation permet de convertir une adresse IP (ou N adresses IP) en une autre (ou en Nadresse IP) lors du passage par le firewall, quelle que soit la provenance de la connexion.

Translation d'adresses

Le changement d'une adresse vers une autre. Par exemple, un assembleur traduirait des adresses symboliques en adresses de machine. Un système à mémoire virtuelle traduirait une adresse virtuelle en adresse réelle (la résolution d'adresses).

Translation unidirectionnelle (MAP)

Ce type de translation vous permet de convertir des adresses IP réelles de vos réseaux (interne, externe ou DMZ) en une adresse IP virtuelle sur un autre réseau (interne, externe ou DMZ) lors du passage par le firewall.

TTL (*Time-To-Live*)

Temps de vie. Cela indique le temps pendant lequel une information doit être conservée, ou le temps pendant lequel une information doit être gardée en cache.

Tunnel VPN

Lien virtuel utilisant une infrastructure non sécurisée comme Internet pour permettre des communications sécurisées (authentification, confidentialité, intégrité) entre différents équipements.

U

UDP (*User Datagram Protocol*)

Protocole de datagramme utilisateur. Un des principaux protocoles de communication utilise par Internet. Il fait partie de la couche transport de la pile protocole TCP/IP.
Ce protocole permet la transmission de paquets de manière très simple entre deux entités chacune étant définie par une adresse IP et un n° de port (pour différencier des utilisateurs sur la même machine).

URL (*Uniform Resource Locator*)

Chaîne de caractères utilisée pour adresser les ressources dans le www : document. Elle est informellement appelée une adresse Web.

UTM (*Unified Threat Management*)

Concept consistant à apporter une solution la plus unifiée possible pour contrer les multiples menaces informatiques (virus, vers, Trojan, intrusions, spyware, dénis de service…).

V

VLAN (*Virtual Local Area Network*)

Un réseau d'ordinateurs qui se comportent comme s'ils étaient connectés au même réseau même s'il se peut qu'ils soient physiquement localisés à différents segments du LAN. La configuration VLAN est effectuée via un software et non un hardware, ce qui le rend très flexible.

VPN (*Virtual Private Network)*

(VPN : Réseau Privé Virtuel) Interconnexion de réseaux de manière transparente et sécurisée pour les applications et protocols participants ; généralement utilise pour relier des réseaux privés au travers d'Internet.

VPN keep alive

Création artificielle du trafic afin de supprimer la latence due à l'établissement du tunnel d'une part, et d'éviter certains problèmes au niveau du NAT, d'autre part.

W

WAN (*Wireless Area Network*)
Réseau local sans fil.

Wifi (*Wireless Fidelity*)
Technologie d'accès réseau sans fil.