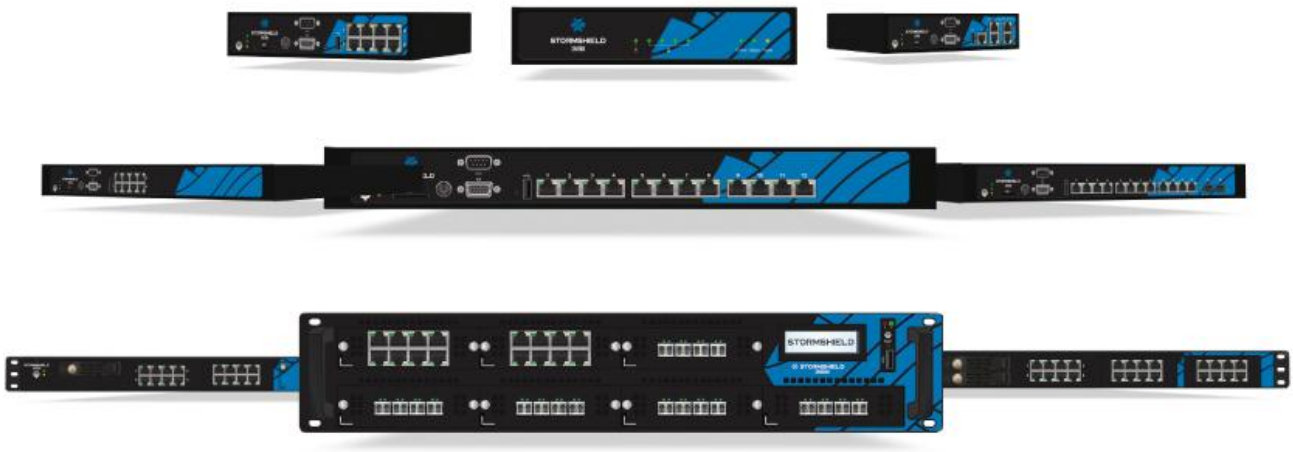
GUIDE

Firewalls Stormshield Network

PRÉSENTATION ET INSTALLATION PRODUITS

Gamme SN



Date	Version	Détails
Août 2014	V1.0	Création

Référence : snfrgde_installation-produit-GammeSN

SOMMAIRE

AVANT-PROPOS

Il est fortement recommandé de lire ce document dans son intégralité avant toute installation d'un Firewall Stormshield Network.

Ce guide d'installation vous présente les modèles de **la gamme Stormshield Network** commercialisée par la société NETASQ. Ce guide vous explique comment réaliser l'installation physique nécessaire à l'intégration dans votre architecture réseau. Il fournit également les indications nécessaires à l'ajout de transceivers et modules réseaux aux produits SN900, SN2000, SN3000 et SN6000.

Ce manuel a pour but de vous permettre l'intégration rapide d'un Firewall Stormshield Network dans votre réseau mais n'apporte pas d'information concernant la configuration du produit. Pour cette configuration, vous disposez d'un guide d'utilisation complet sous forme d'**aide en ligne**, consultable à l'adresse :

http://documentation.arkoon-netasq.com

Un document reprenant l'aide complète est téléchargeable depuis la ***Base Documentaire***, accessible depuis votre **Espace sécurisé** (consultez le chapitre Documentation).

Produits concernés

SN150, SN200, SN300, SN500, SN700, SN900, SN2000, SN3000 et SN6000.

Conditions générales d'utilisation et licence d'utilisation

Préambule

Les présentes Conditions (points 1 à 8) ont pour objet de définir les termes et conditions applicables à l'utilisation du (des) Produit(s) NETASQ par le Client.

Les présentes Conditions d'utilisation s'appliquent aux Produits de la gamme UTM distribués par NETASQ et à leurs éventuelles évolutions et mises à jour.

En ouvrant l'emballage du (des) Produit(s), en installant le logiciel d'administration et/ou en enregistrant le(s) Produit(s), le Client accepte sans réserve les présentes Conditions Générales d'utilisation et Licence d'utilisation du (des) Produit(s) ce qu'il reconnaît.

1. Documents contractuels

Les présentes Conditions complétées par les Conditions Générales de Vente NETASQ et la Charte Support Technique déterminent l'étendue des engagements existant entre NETASQ et le Client. Elles remplacent et annulent tout engagement oral ou écrit contraire antérieur relatif à l'objet des Conditions.

Les présentes Conditions ont été rédigées compte tenu de l'état de la technologie NETASQ existant au moment de leur rédaction.

Cependant, NETASQ applique une méthode de développement continu afin de faire évoluer ses Produits en permanence pour une meilleure protection des Clients. Dès lors, les présentes Conditions d'utilisation peuvent devenir obsolètes. Par conséquent, NETASQ dégage toute responsabilité quant aux inexactitudes qui pourraient apparaître dans ce document et aux dommages qui pourraient en résulter.

NETASQ se réserve le droit :

- d'apporter des changements et des améliorations à tout Produit décrit dans ce document, sans aucun préavis.
- de modifier ou remplacer les présentes Conditions à tout moment.

2. Garanties et Responsabilité

1) A compter de la date d'activation du(des) Produit(s), et nonobstant toute garantie légale dont le Client pourrait se prévaloir, Netasq garantit la partie matérielle du(des) Produit(s) leurs défauts (pièces et main d'œuvre) pendant une durée de douze (12) mois.

   A compter de la date d'activation du (des) Produit(s), et sauf souscription d'un contrat de maintenance, NETASQ ne garantit la partie logicielle du (des) Produit(s), ci-après désignés "les logiciels", que pour une période de quatre-vingt-dix (90) jours contre les défauts et les dysfonctionnements substantiels par rapport au manuel tel qu'il existe à la date de livraison et exclusivement sous les environnements conformes aux prérequis.

   En cas de défaut matériel et/ou logiciel, NETASQ procédera, à son choix :
   - soit à la réparation,
   - soit au remplacement du Produit.

   Au-delà de la période de garantie logicielle de quatre-vingt-dix (90) jours et sans souscription d'un contrat de maintenance, le(s) Produit(s) est (sont) fourni(s) "tel quel" sans garantie de n'importe quelle sorte, expresse ou induite.

   La souscription d'un contrat de maintenance est nécessaire au bon fonctionnement du (des) Produit(s) dans la mesure où la maintenance permet la mise à jour des logiciels de sécurité attachés au(x) Produit(s). Sans maintenance, le Client est averti que les fonctions de sécurité du (des) Produit(s) **ne seront plus assurées.**

   Il convient de se reporter aux conditions du contrat de maintenance lorsqu'un tel contrat est conclu.

2) En outre, et en cas de faute prouvée par le Client, NETASQ ne sera tenue que de la réparation des conséquences pécuniaires des dommages directs et prévisibles du fait de l'utilisation du (des) Produit(s).

   La responsabilité de NETASQ en cas de dommages directs se limite au montant reçu par NETASQ pour l'achat du Produit qui a effectivement causé les dommages.

   En aucun cas NETASQ ne pourra être tenue responsable des dommages indirectement liés à l'usage du (des) Produit(s), y compris d'éventuelles pertes d'exploitation dues à une interruption

de service ou toute autre cause, subis par le Client ou par tout autre tiers, même si NETASQ a été avisée de la possibilité de tels dommages.
NETASQ ne peut en aucun cas être tenue responsable de toute perte de données ou de revenu, ainsi que de tout dommage particulier, incident, consécutif ou indirect, lié à l'utilisation du (des) Produit(s) et de la documentation associée.

3) Le Client est seul responsable de l'adéquation du (des) Produit(s) à ses besoins.

4) NETASQ ne garantit pas que l'utilisation du (des) Produit(s) puisse(nt) être ininterrompue et exempte d'erreurs.

5) De même, NETASQ décline toute responsabilité en cas de mauvaise installation, paramétrage, configuration et/ou d'utilisation non conforme du (des) Produit(s). NETASQ ne saurait garantir un usage par le Client non conforme aux prérequis et conditions d'utilisation décrits dans les présentes Conditions. Il en est de même de toutes les conséquences d'un acte, de l'inaction, d'une erreur, d'un oubli ou d'un défaut relevant de la responsabilité du Client ou de tout prestataire mandaté par le Client. L'ensemble des tâches d'installation, de paramétrage, de configuration devront être réalisées par le Client conformément à l'état de l'art et à la réglementation en vigueur.

   Lorsque le Client ou tout prestataire mandaté par le Client a l'initiative du téléchargement, lancement, installation ou tout autre procédé des mises à jour du (des) Produit(s) proposées par NETASQ, NETASQ ne saurait être responsable du défaut d'activation des mises à jour par le Client ou tout prestataire mandaté par le Client.

   Le Client ou tout prestataire mandaté par le Client doit se conformer aux prescriptions de la documentation portant sur l'installation du (des) produit(s) NETASQ et notamment aux règles de sécurité, précautions d'installation, prérequis de connexion qui lui sont communiqués avec les présentes Conditions. L'inobservation de ces règles engage la seule responsabilité du Client.

6) Tout usage frauduleux ou illégal du (des) Produit(s) par le Client y compris ses préposés ou le prestataire mandaté par le Client engage sa seule responsabilité tant vis-à-vis de NETASQ que des tiers ayant subi un dommage de ce fait.

3. Licence d'utilisation

Par la présente licence, NETASQ concède au Client ayant enregistré le Produit le droit d'usage du Produit, personnel, non exclusif, non transférable et non cessible pour la durée de souscription.

Le Client ne peut utiliser le (les) Produit(s) que conformément à sa (leur) documentation. En particulier, la licence relative au(x) Produit(s) n'est concédée que dans le seul et unique but de permettre au Client son utilisation, à l'exclusion de toute autre finalité. Ainsi, le Client s'engage à l'utiliser conformément à sa destination.

La présente licence s'applique aux mises à jour.

En outre, le Client s'interdit de procéder à toute reproduction provisoire ou permanente du (des) Produit(s) ou de la documentation associée au Produit, par quelque moyen que ce soit, ainsi qu'à toute traduction, adaptation, arrangement, décompilation ou modification, notamment en vue de la création de solutions similaires.

NETASQ garantit qu'elle détient l'intégralité des droits de propriété intellectuelle, ou les autorisations, cessions ou licences de tout droit de tiers, sur le(s) Produit(s), lui permettant d'en concéder l'utilisation au Client.

4. Propriété Intellectuelle

Brevet
Le(s) Produit(s) incluent la technologie ASQ, pour laquelle NETASQ détient des brevets internationaux.

5. Données

1) Certains Produits de NETASQ permettent de récupérer et d'analyser les historiques de connexions et traces. Les informations ainsi analysées peuvent permettre un contrôle de l'activité des utilisateurs internes et peuvent fournir des informations nominatives. La législation en vigueur, dans le pays du Client peut imposer certaines mesures telles que notamment des déclarations administratives. Il relève de la responsabilité du Client de se conformer aux obligations légales en vigueur dans son pays ce que le Client reconnait.

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 du Client. Il relève de la responsabilité du Client de se conformer aux obligations légales applicables à ce type de dispositif ce que le Client reconnait.

3) NETASQ dégage toute responsabilité quant à l'utilisation du (des) Produit(s) non conforme à la législation locale du Client. NETASQ ne saurait être responsable du défaut de conformité légale du Client.

4) De façon générale, le Client garantit à NETASQ qu'il a satisfait à l'ensemble des obligations qui lui incombent aux termes de sa législation nationale et au regard des données à caractère personnel, et qu'il a, le cas échéant, informé les personnes physiques concernées de l'usage qui est fait desdites données personnelles. A ce titre, le Client garantit NETASQ contre tout recours, plainte ou réclamation émanant d'une personne physique dont les données personnelles seraient reproduites et transmises à NETASQ.

5) En aucun cas NETASQ ne peut être tenue responsable de la qualité, l'intégrité, la complétude et l'exactitude des données transmises par le Client, ni par conséquent des contenus et données qui seront disponibles sur le(s) Produit(s).

6. Force majeure

Aucune des parties ne pourra être tenue d'un manquement quelconque à ses obligations, si un tel manquement résulte : d'une décision gouvernementale, en ce compris tout retrait ou suspension d'autorisations quelles qu'elles soient, d'une grève totale ou partielle, interne ou externe à l'entreprise, d'un incendie, d'une catastrophe naturelle, d'un état de guerre, d'une interruption totale ou partielle ou d'un blocage des réseaux de télécommunications ou électriques, d'acte de piratage informatique ou plus généralement tout autre événement de force majeure présentant les caractéristiques définies par la jurisprudence.

La partie constatant l'événement devra sans délai informer l'autre partie de son impossibilité à exécuter sa prestation. La suspension des obligations ou le retard ne pourra en aucun cas être une cause de responsabilité pour non-exécution de l'obligation en cause, ni induire le versement de dommages et intérêts ou pénalités de retard.

7. Exportation

NETASQ informe que les Produits peuvent contenir des technologies et des logiciels soumis aux lois sur le contrôle des exportations des Etats-Unis et de l'Union Européenne ainsi qu'aux lois du pays où ils sont livrés ou utilisés. Conformément à ces lois, les Produits ne peuvent être vendus, loués ou transférés à des utilisateurs ou pays soumis à restriction. Le Revendeur, Client ou tout autre prestataire mandaté par le Client s'engage à respecter et à se conformer à ces lois.

Les Produits entrent dans la catégorie des Produits à double usage pouvant être utilisés dans un cadre civil ou militaire. En tant que Produits à double usage, ils sont soumis au Règlement (UE) n°428/2009 du Conseil du 5 mai 2009 modifié par les règlements UE n° 1232/2011 et n° 388/212 du Parlement et du Conseil européen respectivement du 16 novembre 2011 et du 19 avril 2012.

Afin de respecter les engagements internationaux de l'Union Européenne ainsi que ceux de ses membres, l'exportation de biens à double usage est soumise à contrôle et à autorisation.

NETASQ a pris toutes les mesures requises par les autorités françaises pour obtenir les licences d'exportation et les autorisations pour chaque pays vers lequel il exporte. Cela signifie que NETASQ est autorisée à exporter ses Produits, mais cela ne signifie pas qu'un tiers et/ou partenaire NETASQ peut exporter des Produits NETASQ vers les pays de destination indiqués dans des licences d'exportation accordées à NETASQ uniquement.

Tout Distributeur, Revendeur ou autre partenaire NETASQ quelle que soit la dénomination qu'on lui donne est averti que s'il exporte des Produits NETASQ à l'extérieur de l'Union Européenne, il doit déposer ses propres demandes auprès des autorités compétentes pour obtenir une licence d'exportation. Si un Produit a déjà été exporté à l'extérieur de l'Union Européenne sans autorisation, NETASQ recommande que le Distributeur,

Revendeur, Partenaire ou autre concerné prenne, sans délai, contact avec l'autorité compétente afin de régulariser la situation.

En raison de la nature des Produits, des processus de cryptologie sont mis en œuvre. NETASQ a obtenu les autorisations requises. Il appartient au Distributeur, Revendeur, Partenaire ou autre de procéder à une déclaration ou une demande d'autorisation auprès de l'ANSSI (en France) ou de l'organisme compétent (autres pays) pour le Produit concerné et le territoire visé. NETASQ accepte de fournir les informations et l'assistance susceptible d'être raisonnablement requise concernant les garanties nécessaires à l'obtention de ces autorisations.

8. Loi applicable-attribution de compétence

TOUT LITIGE RELATIF A LA DEFECTUOSITE ALLEGUEE DU LOGICIEL ET/OU DU (DES) PRODUIT(S) ET/OU A L'INTERPRETATION OU L'APPLICATION DES PRESENTES CONDITIONS GENERALES ET LICENCE D'UTILISATION SERA OBLIGATOIREMENT SOUMIS A LA COMPETENCE DES JURIDICTIONS DU LIEU DU SIEGE DE NETASQ, LE DROIT FRANÇAIS ETANT SEUL APPLICABLE.

Hypothèses issues des 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, etc.). 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.

Pour plus d'informations sur la conformité à la certification Critères Communs, consultez le lien : http://documentation.arkoon-netasq.com/common-criteria.html

Hypothèses sur les mesures de sécurité physiques

Les boîtiers appliances Firewall-VPN 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

Le mot de passe par défaut de l'utilisateur 'admin' (super administrateur) doit être modifié lors de la première utilisation du produit. Ce changement est proposé via l'Assistant de première installation, dans l'écran **Administration de l'équipement**. Dans l'interface d'administration web, ce mot de passe peut être modifié via le module **Administrateur** (menu **Système**), onglet *Compte Admin*.

Ce mot de passe doit être défini selon les bonnes pratiques décrites dans le Guide utilisateur, chapitre **Bienvenue**, partie **Sensibilisation des utilisateurs**, paragraphe **Gestion des mots de passe de l'utilisateur**, à l'adresse : http://documentation.arkoon-netasq.com/

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

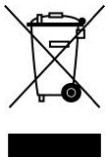
- Il est le seul à être habilité à se connecter via la console locale aux appliances Firewall-VPN, et ce uniquement lors de l'installation de l'appliance Firewall-VPN ou pour des opérations de maintenance, en dehors de l'exploitation.
- Il est chargé de la définition du profil des autres administrateurs.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

Hypothèses sur l'environnement de sécurité TI (Technologies de l'Information)

Les boîtiers appliances Firewall-VPN 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. Ils sont dimensionnés en fonction des capacités des équipements adjacents ou alors ces derniers réalisent des fonctions de limitation du nombre de paquets par seconde, positionnées légèrement en deçà des capacités maximales de traitement de chaque boîtier appliance Firewall-VPN installé dans l'architecture réseau.

Réglementations

Directive DEEE (Déchets d'Equipements Electriques et Electroniques)



Tous les produits Stormshield Network soumis à la directive DEEE 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.

Directive RoHS (Restriction of Hazardous Substances)

Pour plus d'informations sur la conformité RoHS ou sur le programme de recyclage des Firewalls Stormshield Network (DEEE), consultez le lien :

www.netasq.com/recycling

Certifications

INTRODUCTION

Merci d'avoir choisi un produit Stormshield Network. Destinés à sécuriser des structures de toutes tailles, les Firewalls **Stormshield Network- Gamme SN** sont des produits préconfigurés : pas d'installation matérielle, ni d'installation logicielle, pas de compétences Unix nécessaires mais une configuration conviviale au moyen d'une interface graphique.

La gamme **Stormshield Network (SN)** comprend neuf produits :

SN150, SN200, SN300, SN500, SN700, SN900, SN2000, SN3000 et SN6000.

L'architecture de la gamme SN de nouvelle génération a été conçue spécifiquement pour maximiser les performances du moteur de protection Stormshield Network. L'inspection des flux applicatifs complexes s'effectue ainsi à des débits de cœur de réseau et sans latence sensible (inférieure à 1 milliseconde).

L'accélération matérielle du chiffrement des données anticipe également la multiplication des accès VPN à haut débit.

Le Firewall SN 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 SN 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 Stormshield Network. 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, dépassement mémoire, etc.

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 SN 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, etc.). Le contrôle des utilisateurs peut aussi être réalisé au moyen d'une authentification via une base d'authentification interne ou externe.

Le Firewall SN gère également les mécanismes de translations d'adresses et de ports. Ces mécanismes apportent sécurité (en masquant votre plan d'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).

La solution de gestion des risques informatiques Stormshield Network Vulnerability Manager est basée sur la détection d'applications et des vulnérabilités associées. Elle permet de cibler rapidement les machines les plus vulnérables, identifier les applications impactées et connaître les correctifs à apporter.

Enfin, le Firewall SN intègre les fonctionnalités de passerelle VPN vous permettant d'établir des tunnels chiffrés avec d'autres équipements VPN. Ainsi, vos communications intersites ou avec vos utilisateurs nomades peuvent être sécurisées même en utilisant une infrastructure de communication non sûre comme Internet.

Outils d'administration

Grâce à l'interface d'Administration Web, vous pouvez administrer votre Firewall Stormshield Network depuis le système d'exploitation de votre choix. La nouvelle interface de configuration des Firewalls accessible via un navigateur web, bénéficie des toutes dernières avancées en matière d'ergonomie et de simplicité d'utilisation.

Le tableau de bord permet de bénéficier d'une vue d'ensemble des informations relatives à l'activité du Firewall, et à sa configuration.

Au travers de SN Activity Reports, disponible depuis un portail dédié, vous pouvez visualiser l'utilisation de l'accès Internet, les différentes attaques bloquées par votre Firewall et les machines vulnérables de votre réseau. De plus, de nombreuses interactions vous permettent d'agir directement sur la configuration de votre Firewall.

Stormshield Network Administration Suite

SN UNIFIED MANAGER en mode Global Administration vous permet de configurer et de mettre à jour plusieurs Firewalls, localement ou à distance et de manière sécurisée. Vous pouvez administrer, sans licence complémentaire jusqu'à cinq équipements simultanément.

SN REAL-TIME MONITOR est l'application d'analyse en temps réel des évènements sécurité et vous permet de visualiser simplement l'activité de votre Firewall. Le tableau de bord vous permet notamment de surveiller l'ensemble de vos Firewalls SN. Cette application constitue un excellent outil pour la sécurité de votre réseau grâce au large registre d'informations affichées.

Le Firewall SN est également doté de fonctions avancées de traçabilité. En cas de tentative d'intrusion, l'administrateur réseau peut accéder à l'ensemble des données envoyées avant l'attaque et comprendre comment elle a été préparée. SN EVENT REPORTER apporte une vision graphique et une analyse fine des traces générées sur le Firewall.

DES RECEPTION DE VOTRE FIREWALL

Plusieurs mécanismes de sécurité ont été mis en place pour garantir l'intégrité du produit reçu. Ils valident également le fait que votre produit n'a pas été manipulé frauduleusement. **Vérifiez-les soigneusement afin d'éviter tout litige ultérieur concernant l'application de la garantie.**

Toute non-conformité doit être signalée moins de 48 heures après la réception du produit, auprès votre revendeur.

Intégrité du produit

Scellés et étiquettes sur l'emballage

Chaque Firewall est livré dans un carton fermé par un ou deux scellés de garantie. Par ailleurs, sur cet emballage est apposée une étiquette affichant les informations d'identification du produit et sa version. Vérifiez que ces informations correspondent à votre commande.

Les scellés sur l'emballage

Chaque Firewall est livré dans un carton sur lequel sont apposés un scellé (SN150, SN200 et SN300) ou deux scellés « STORMSHIELD NETWORK QUALITY SEAL ».

Figure 1 : Scellé " Stormshield Network Quality seal"

IMPORTANT

Si ces scellés sont absents ou détériorés, contactez votre revendeur au plus vite pour connaître les raisons de l'ouverture du carton.

Etiquettes d'identification

Ces étiquettes, collées sur l'emballage du produit, affichent les informations relatives au Firewall (modèle, part number, version logicielle installée, etc.). Vous pouvez ainsi vérifier si la version installée est certifiée.

Figure 2 : Etiquettes d'identification

Etiquettes sur le produit

Etiquette de scellé

Une étiquette de scellé est apposée sur tous les Firewalls. **La rupture de cette étiquette entraîne l'annulation de la garantie.**

Figure 3 : Scellé du SN6000

Figure 4 : Scellé des autres modèles

Etiquette numéro de série

Cette étiquette, collée à l'arrière du Firewall (en-dessous pour les modèles SN150, SN2000, SN3000 et SN6000), affiche le numéro de série et le mot de passe d'enregistrement de votre produit.

Figure 5: Etiquette numéro de série

IMPORTANT

Notez votre mot de passe d'enregistrement ❶ et votre numéro de série ❷. Ces informations vous seront demandées au cours des phases d'installation et d'enregistrement de votre produit.

Etiquette produit

Cette étiquette, collée sous le produit, indique les informations relatives au Firewall telles que le modèle et la tension électrique supportée.

Figure 6: Etiquette produit

Contenu de l'emballage

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

A la livraison, vérifiez que l'emballage contient :

- Votre boîtier Firewall Stormshield Network,
- Un cordon secteur (deux pour SN3000 et SN6000),
- Un adaptateur secteur (SN150, SN200 et SN300)
- Un câble croisé RJ45, catégorie 5e,
- Un câble série DB9F, un câble série RJ45 vers DB9F (SN2000 et SN3000) ou un câble USB de type « A » vers « B » (modèle SN150).

Pour les modèles SN500, SN700 et SN900, l'emballage contient en plus :

- Le jeu d'équerres et visserie pour montage en baie de rackage,
- 4 pieds antidérapants.

Pour les modèles SN2000, SN3000 et SN6000, l'emballage contient en plus un jeu de glissières et visserie pour montage en baie de rackage.

NOTE

Les Firewalls SN500, SN700 et SN900 pouvant être installés sur un bureau ou en baie de rackage, leurs pieds antidérapants sont livrés séparément. Seuls les produits non rackables (SN150, SN200 et SN300) sont livrés avec les pieds préalablement collés.

Les documentations fournies sont les suivantes :

- Conditions Générales d'Utilisation et Licence d'Utilisation,
- Règles de Sécurité et Précautions d'Installation,
- Guide d'Installation Rapide

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

REGLES DE SECURITE

Avant toute installation, veuillez lire attentivement et respecter les consignes de sécurité suivantes.

IMPORTANT

Vous devez impérativement utiliser l'adaptateur secteur fourni avec votre produit.

Avant tout raccordement au secteur

1. Assurez-vous que votre Firewall, le cordon ou l'adaptateur secteur ne sont pas endommagés.
2. Assurez-vous que l'alimentation ou l'adaptateur secteur du produit est compatible avec la tension électrique de votre réseau d'alimentation secteur.
3. Lorsqu'il est équipé d'une prise de terre, le cordon ou l'adaptateur secteur du produit doit être raccordé à une embase secteur équipée d'une terre de protection. Assurez-vous que le raccordement est fiable, et que le circuit de mise à la terre de protection de votre installation est conforme aux normes en vigueur.
4. Afin de pouvoir déconnecter le produit, assurez-vous que la connexion au secteur est toujours aisément accessible.

Garantie et règles de sécurité

Le Firewall Stormshield Network ne doit d'aucune manière être ouvert. Seule la société NETASQ, commercialisant la gamme Stormshield Network, et ses agents de maintenance agréés sont habilités à le faire. Une étiquette de garantie protège tous les Firewalls Stormshield Network contre l'ouverture du boîtier.

Toute ouverture du Firewall entraîne l'annulation de la garantie.

IMPORTANT

N'ouvrez jamais votre boîtier Stormshield Network. L'ouverture de ce boîtier expose à des risques d'accidents matériels ou corporels.

IMPORTANT

N'insérez pas d'objet dans les découpes du boîtier : vous pourriez bloquer la rotation d'un ventilateur ou le détériorer, ce qui entraînerait un risque de surchauffe du boîtier. Vous pourriez aussi provoquer un court-circuit pouvant entraîner la défaillance de l'équipement.

IMPORTANT

Les câbles Ethernet cuivre raccordés à votre Firewall Stormshield Network ne doivent pas être connectés à d'autres équipements, situés dans des bâtiments différents.

Conformément aux obligations légales de sécurité, toute personne intervenant sur un produit Stormshield Network de la gamme SN est tenue de prendre connaissance et de respecter les consignes de sécurité ci-dessous :

A l'attention des services de maintenance :

ATTENTION

CET APPAREIL CONTIENT UNE PILE AU LITHIUM. IL Y A DANGER D'EXPLOSION EN CAS DE REMPLACEMENT INCORRECT DE CELLE-CI. REMPLACER UNIQUEMENT AVEC UNE PILE DE MEME TYPE OU D'UN TYPE EQUIVALENT RECOMMANDE PAR LE CONSTRUCTEUR. METTRE AU REBUT LES PILES USAGEES CONFORMEMENT AUX INSTRUCTIONS DE RECYCLAGE EN VIGUEUR.

Seul un personnel informé et habilité d'un centre de maintenance agréé peut être autorisé à intervenir sur ce composant.

En cas de problème matériel avec votre Firewall ou si l'un des accessoires n'est pas conforme à sa description, contactez votre partenaire certifié.

Installation hors baie de rackage

Dans ce type d'installation, votre produit doit être équipé de pieds antidérapants afin de limiter le risque de chute du produit.

Ces pieds antidérapants en matériau souple sont à fixer sous le châssis pour les modèles SN500, SN700 et SN900. Veuillez vous reporter au chapitre PRECAUTIONS D'INSTALLATION pour plus d'informations.

Montage en baie de rackage

Pour une installation en baie, veuillez placer les équipements lourds dans la partie basse de la baie et les éléments plus légers dans la partie haute.

Veuillez vous reporter au chapitre Installation en baie 19" pour le détail de l'installation en baie de rackage.

PRESENTATION DE LA GAMME SN

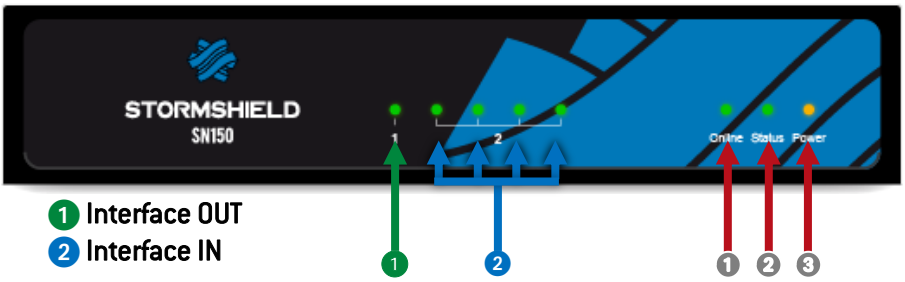
Les Firewalls Stormshield Network gamme SN s'appuient sur les technologies les plus avancées pour offrir hautes performances et protections optimales.

Modèle SN150

Le Firewall SN150 fonctionne sans ventilateur. Le produit est fourni avec un adaptateur secteur externe.

Face avant : voyants

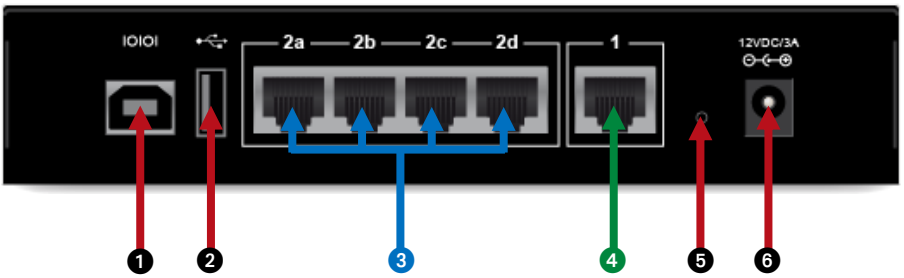
Ce modèle présente en façade les voyants décrits ci-dessous :



1. Voyant *Online* (vert)
2. Voyant *Status* (vert)
3. Voyant *Power* (jaune)

Face arrière : connectique

La connectique du modèle SN150 se situe en face arrière.



1. **Le port USB** permet d'accéder au produit en mode console*; il est possible de se connecter directement au Firewall depuis un ordinateur. Le Baudrate par défaut sur ce modèle est de 115200 bauds (8N1).
2. **Le port USB 2.0** peut être utilisé pour la configuration sécurisée ou les mises à jour. Vous pouvez également y brancher une clé USB ou un modem USB homologué.

Le modèle SN150 offre 5 interfaces Ethernet Gigabit :

3. La première zone est par défaut identifiée en mode **INTERNE 2 (IN).** Elle est constituée de 4 ports commutés (switch).
4. La deuxième zone est l'interface **EXTERNE 1 (OUT),** par défaut en mode externe. Elle constitue la zone destinée au raccordement à Internet.
5. Le bouton est celui de **mise en configuration usine** (*defaultconfig*).
6. Le branchement de l'adaptateur secteur démarre automatiquement ce produit.

** Cette connexion en mode console requiert l'installation d'un pilote. Selon votre système d'exploitation, téléchargez ce pilote depuis l'adresse :*
http://www.ftdichip.com/Drivers/VCP.htm

Autres modèles

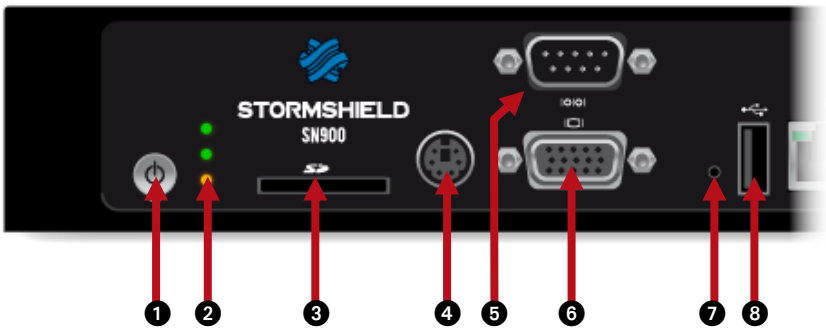
Généralités

Modèles SN200, SN300, SN500, SN700 et SN900

Pour plus d'informations sur les interfaces Ethernet, reportez-vous à la partie Raccordement au réseau du chapitre PRECAUTIONS D'INSTALLATION.

Face avant : connectique

L'essentiel de la connectique des Firewalls SN se situe en façade.



1. **Le Bouton d'Alimentation** permet la mise en marche ou l'arrêt du Firewall.
2. **Les voyants *Power*, *Status* et *Online*** (de bas en haut) sont décrits dans le chapitre suivant.
3. Cet emplacement est celui de la **Carte SD*** (Norme SDHC)
4. **Le port mini-din PS2** permet le branchement d'un clavier.
5. **Le port série** permet d'accéder au produit en mode console ; il est possible de se connecter directement au Firewall depuis un ordinateur. Le Baudrate par défaut sur ces modèles est de 9600 bauds (8N1).
6. **Le port VGA** permet le branchement d'un écran.
7. Le bouton est celui de **mise en configuration usine** (defaultconfig).
8. **Le port USB 2.0** peut être utilisé pour la configuration sécurisée ou les mises à jour. Vous pouvez également y brancher une clé USB, un clavier USB ou un modem USB.

Le type de carte SD conseillé doit être au minimum de Classe 6, standard SDHC.

Face avant : voyants

Les différents modèles présentent en façade les 3 voyants décrits ci-dessous :

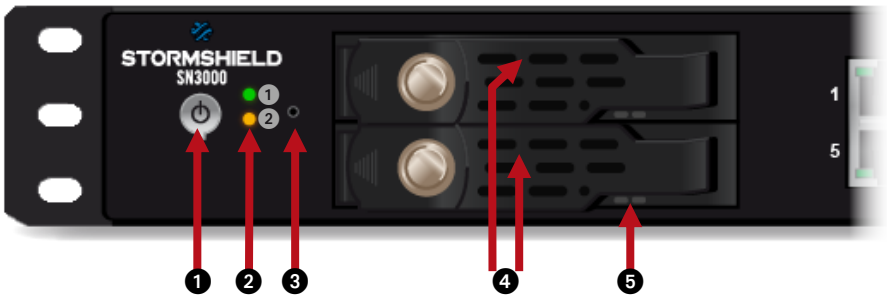
Face arrière : connectique

Le branchement du cordon de l'alimentation ou de l'adaptateur secteur s'effectue en face arrière du produit. La face arrière dispose de deux ports USB supplémentaires, permettant l'accès aux mêmes fonctionnalités que les ports USB situés en façade.

Modèles SN2000 et SN3000

Pour plus d'informations sur les interfaces Ethernet, reportez-vous à la partie Raccordement au réseau du chapitre PRECAUTIONS D'INSTALLATION.

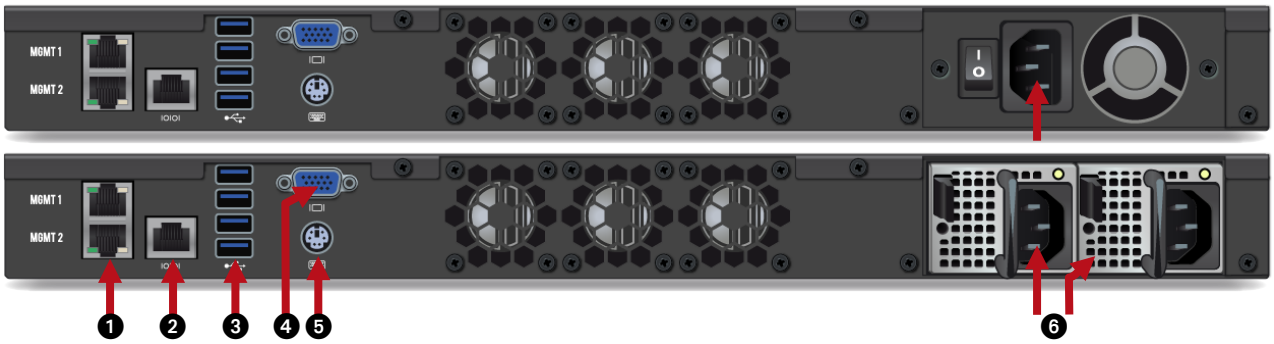
Face avant : connectique et voyants



1 Voyant *Online* (vert)
2 Voyant *Power* (jaune)

1. **Le Bouton d'Alimentation** permet la mise en marche ou l'arrêt du Firewall.
2. Les voyants *Power* et *Online* (de bas en haut).
3. Le bouton est celui de **mise en configuration usine** (defaultconfig).
4. **Rack des SSD** pour le stockage des traces (1 sur SN2000, 2 en RAID 1 sur SN3000).
5. **Les voyants des racks SSD** valident l'accès (voyant bleu de droite) et l'installation (voyant vert de gauche).

Face arrière : connectique

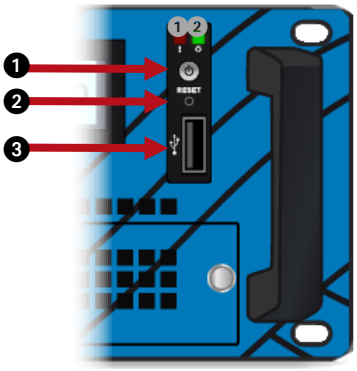


1. **Deux** ports dédiés au management du boîtier ou la configuration en HA (MGMT1 et MGMT2).
2. **Le port série** permet d'accéder au produit en mode console ; il est possible de se connecter directement au Firewall depuis un ordinateur. Le Baudrate par défaut sur ce modèle est de 9600 bauds (8N1).
3. **Quatre ports USB 3.0** qui peuvent être utilisés pour la configuration sécurisée ou les mises à jour. Vous pouvez également y brancher une clé USB, un clavier USB ou un modem USB.
4. **Le port VGA** permet le branchement d'un écran.
5. **Le port mini-din PS2** permet le branchement d'un clavier.
6. Une embase secteur (SN2000) ou deux embases secteur (SN3000) pour la redondance d'alimentation.

Modèle SN6000

Pour plus d'informations sur les interfaces Ethernet, reportez-vous à la partie Raccordement au réseau du chapitre PRECAUTIONS D'INSTALLATION.

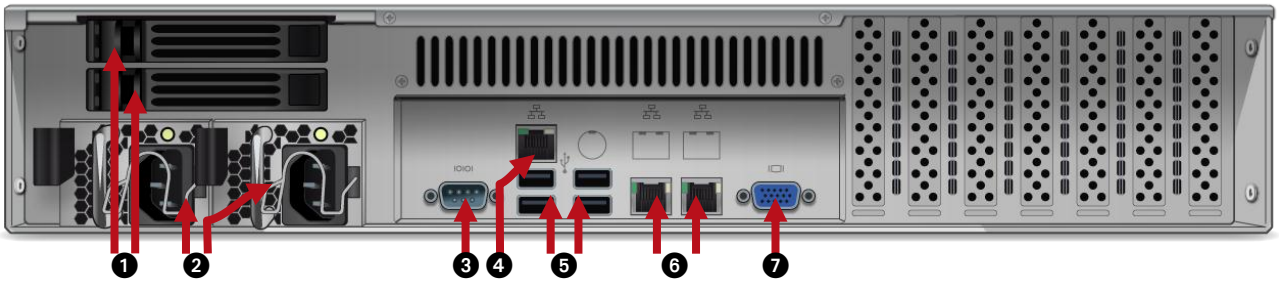
Face avant : connectique et voyants



1. **Voyant rouge :** indicateur de surchauffe ou de défaillance matérielle (ventilateurs)
2. **Voyant *Power* vert :** indiquant si le Firewall est sous tension.

1. **Le Bouton d'Alimentation** permet la mise en marche ou l'arrêt du Firewall.
2. **Le Bouton *Reset* :** reset électrique.
3. **Le port USB 2.0** peut être utilisé pour la configuration sécurisée ou les mises à jour. Vous pouvez également y brancher une clé USB, un clavier USB ou un modem USB.

Face arrière : connectique



1. **Racks des SSD pour stockage des traces** (2 en RAID 1 sur SN6000). Les voyants des racks SSD valident l'accès (voyant bleu du bas) et l'installation (voyant vert du haut).
2. **Deux embases secteur** pour la redondance d'alimentation
3. **Le port série** permet d'accéder au produit en mode console ; il est possible de se connecter directement au Firewall depuis un ordinateur. Le Baudrate par défaut sur ce modèle est de 9600 bauds (8N1).
4. Un port réseau dédié à l'administration du boîtier via IPMI.
5. **Quatre ports USB 2.0** qui peuvent être utilisés pour la configuration sécurisée ou les mises à jour. Vous pouvez également y brancher une clé USB, un clavier USB ou un modem USB.
6. Deux ports réseaux dédiés au management du boîtier ou la configuration en HA (gauche à droite : MGMT1 et MGMT2).
7. **Le port VGA** permet le branchement d'un écran.

Présentation

Modèle SN200

1 Interface **OUT**
2 Interface **IN**

Le Firewall multifonctions SN200 fonctionne sans ventilateur.
Le produit est fourni avec un adaptateur secteur externe.

Le modèle SN200 offre 5 interfaces Ethernet Gigabit regroupées en trois zones :

- La première zone est par défaut en mode externe (OUT) ; elle constitue la zone destinée au raccordement à Internet,
- La deuxième zone est par défaut identifiée en mode interne (IN). Elle est constituée de 2 ports commutés (switch),
- La troisième zone vous permet de définir un troisième secteur de protection (DMZ). Elle est constituée de 2 ports commutés (switch).

Modèle SN300

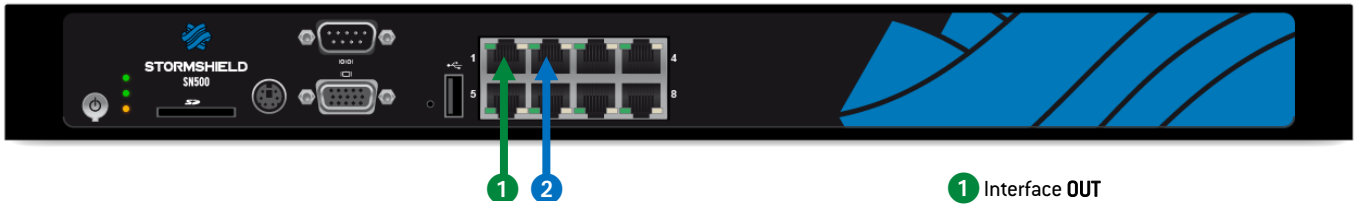
1 Interface **OUT**
2 Interface **IN**

Le Firewall multifonctions SN300 est équipé d'un ventilateur très silencieux. Le bruit émis par l'appareil, exprimé en puissance acoustique, ne dépasse pas 22dB(A).

Le produit est fourni avec un adaptateur secteur externe.

Le modèle SN300 offre 8 interfaces Ethernet Gigabit.

Modèle SN500

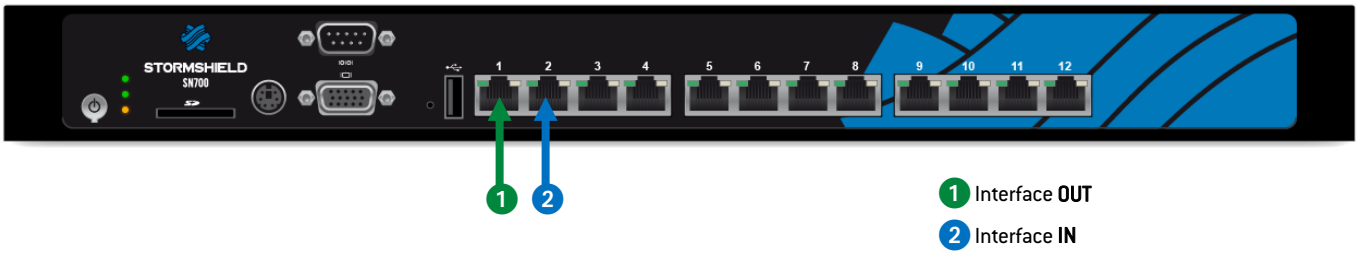


1 Interface **OUT**
2 Interface **IN**

Ce produit dispose d'une alimentation interne.

Le modèle SN500 offre 8 interfaces Ethernet Gigabit.

Modèle SN700



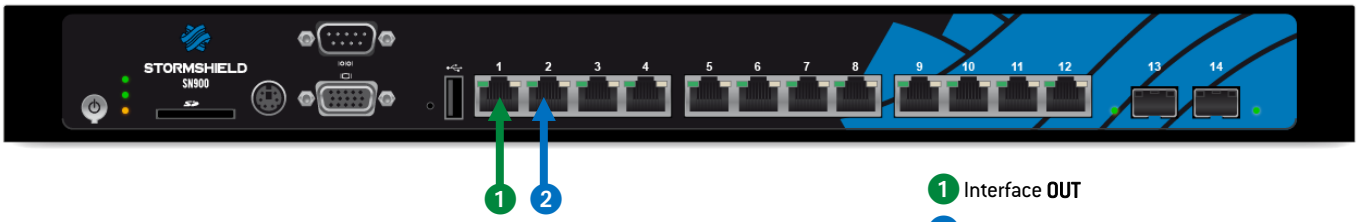
1 Interface **OUT**
2 Interface **IN**

Ce modèle est équipé d'un processeur multi-core, permettant de démultiplier la puissance de traitement.

Ce produit dispose d'une alimentation interne.

Le modèle SN700 offre 12 interfaces Ethernet Gigabit.

Modèle SN900



1 Interface **OUT**
2 Interface **IN**

Ce modèle est équipé d'un processeur multi-core, permettant de démultiplier la puissance de traitement.

Ce produit dispose d'une alimentation interne.

Le modèle SN900 offre 12 interfaces Ethernet Gigabit et permet l'ajout de 2 cages SFP pour transceiver Ethernet Gigabit. Les spécifications des transceivers homologués Stormshield Network sont détaillées dans l'ANNEXE E : TRANSCEIVERS FIBRE.

Modèle SN2000

1 Interface **OUT**
2 Interface **IN**

Ce modèle est équipé d'un processeur multi-core, permettant de démultiplier la puissance de traitement.

Ce produit dispose d'une alimentation interne et est équipé d'un SSD amovible.

Le modèle SN2000 offre 10 interfaces Ethernet Gigabit et permet d'accueillir 2 modules d'extension avec connectiques RJ45 (Gigabit) ou Fibre (Gigabit ou 10 Gigabit).

Les spécifications des modules d'extension et transceivers homologués Stormshield Network sont détaillées dans l'ANNEXE D : MODULES D'EXTENSION (SN2000, SN3000 OU SN6000) et l'ANNEXE E : TRANSCEIVERS FIBRE.

Modèle SN3000

1 Interface **OUT**
2 Interface **IN**

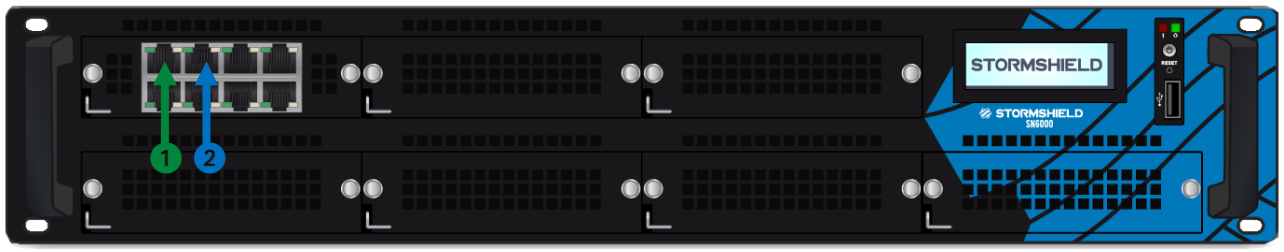
Ce modèle est équipé d'un processeur multi-core, permettant de démultiplier la puissance de traitement.

Ce produit dispose d'une alimentation interne redondante. De base, deux SSD amovibles sont installés en RAID.

Le modèle SN3000 offre 10 interfaces Ethernet Gigabit et permet d'accueillir 2 modules d'extension avec connectiques RJ45 (Gigabit) ou Fibre (Gigabit ou 10 Gigabit).

Les spécifications des modules d'extension et transceivers homologués Stormshield Network sont détaillées dans l'ANNEXE D : MODULES D'EXTENSION (SN2000, SN3000 OU SN6000) et l'ANNEXE E : TRANSCEIVERS FIBRE.

Modèle SN6000



1 Interface **OUT**
2 Interface **IN**

Ce modèle est équipé de deux processeurs multi-core, permettant de démultiplier la puissance de traitement.

Ce produit dispose d'une alimentation interne redondante. De base, deux SSD amovibles sont installés en RAID.

Le modèle SN6000 offre par défaut 10 interfaces Ethernet Gigabit et permet d'accueillir 7 modules d'extension avec connectiques RJ45 (Gigabit) ou Fibre (Gigabit ou 10 Gigabit).

Les spécifications des modules d'extension et transceivers homologués Stormshield Network sont détaillées dans l'ANNEXE D : MODULES D'EXTENSION (SN2000, SN3000 OU SN6000) et l'ANNEXE E : TRANSCEIVERS FIBRE.

Démarrage et extinction

ATTENTION

Il est **impératif** de ne *pas* débrancher le produit en **phase de démarrage, d'arrêt ou de mise à jour**. Sauf pour le SN6000, ces phases sont indiquées par l'état allumé des voyants suivants :

- Voyants *Power* 3 et *Status* 2 pour les modèles de SN150 à SN900,
- Voyants *Power* 3 pour les SN2000 et SN3000.

Démarrage

Pour tous les produits, la phase de démarrage s'effectue dans l'ordre suivant :

Power 3 **+ Status** 2 ⟹ **Online** 1

Les voyants *Power* et *Status* s'allument en premier, puis *Online*.

Au bout de quelques minutes, le voyant *Online* s'allume, suivi d'un bip sonore*, lorsque votre produit est opérationnel.

**Pour tous les modèles, sauf le SN150.*

Extinction du modèle SN150

Connectez-vous à l'interface de configuration. Rendez-vous dans le module **Maintenance** (menu **Système**), et cliquez sur le bouton « Arrêter le Firewall ».

Puis, attendez quelques minutes que les 2 voyants *Online* et *Status* soient éteints. Pour ce modèle, l'arrêt s'effectue dans l'ordre suivant :

Online 1 ⟹ **Status** 2

Le voyant *Power* reste allumé si le produit est sous tension.

Extinction des modèles SN200, SN300, SN500, SN700, et SN900

Appuyez une fois sur le bouton d'Alimentation pour éteindre votre Firewall.

Puis, attendez quelques minutes que les 3 voyants *Online*, *Status* et *Power* soient éteints.

Pour tous les produits, l'arrêt s'effectue dans l'ordre suivant :

Online 1 ⟹ **Status** 2 ⟹ **Power** 3

Un bip sonore vous avertit du lancement de la procédure d'arrêt.

Extinction des modèles SN2000, SN3000 et SN6000

Appuyez une fois sur le bouton d'Alimentation pour éteindre votre Firewall.

Pour les modèles SN2000 et SN3000, la procédure est identique à celle décrite dans le paragraphe précédent, sans le voyant *Status*.

Pour le modèle SN6000, seul le voyant *Power* éteint informe de l'arrêt du produit.

Remarques générales

- Le voyant *Status* 2 clignote en cas de défaut majeur du produit (modification hardware inattendue, interface réseau défaillante, etc.). Dans ce cas, contactez votre revendeur.
- En phase de démarrage, d'arrêt ou de mise à jour, seuls les voyants *Status* 2 et *Power* 3 sont allumés.
- En mode Haute Disponibilité, lorsque le Firewall est en mode passif, le voyant *Online* 1 émet un clignotement (de l'ordre de 2 secondes éteint pour 1 seconde allumé).
- Pendant la phase de mise en configuration usine (*defaultconfig*), les voyants *Online* et *Status* clignotent.
- Lorsqu'un modèle SN150 est arrêté (voyant Power seul allumé), vous pouvez le redémarrer en débranchant puis en rebranchant la prise secteur. Il est également possible de le redémarrer en mode console, en pressant n'importe quelle touche, comme suggéré à l'écran.

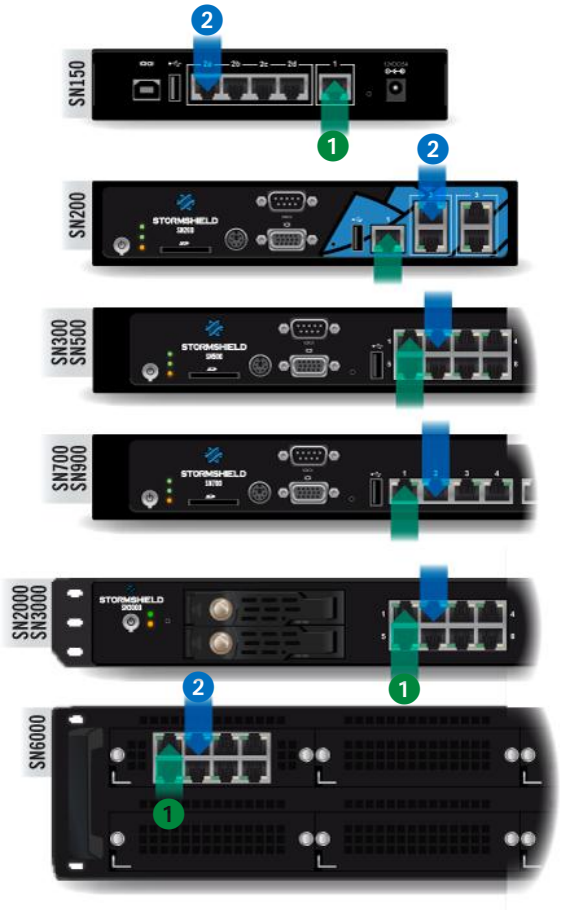
Connectiques Ethernet RJ45

Connectiques

Tous les modèles Stormshield Network de la gamme SN comportent des ports Ethernet (Gigabit) configurés en mode *auto-sense*, ils s'adaptent donc à la configuration du port Ethernet de l'équipement auquel ils sont raccordés. Les ports sont compatibles avec les câbles Ethernet RJ45 de type droit ou croisé.

ATTENTION

Tenez les câbles de données éloignés de toute source de perturbation électromagnétique telle que les câbles secteur, émetteurs radio, tubes fluorescents, etc.



Définition IN /OUT

Le port réseau **OUT** 1, dit "Externe" est réservé au modem ou au routeur Internet.
Par défaut, vous ne pouvez pas accéder à l'interface de configuration depuis ce port. L'accès à cette interface est par défaut bloqué.

Pour accéder à votre Firewall depuis un poste client, il faut vous connecter sur le port **IN** 2, dit "Interne" ou sur un autre port (excepté le port 1).

Pour plus d'informations concernant la procédure de démarrage de votre Firewall, reportez-vous au chapitre PREMIERE CONNEXION AU PRODUIT.

Voyants des interfaces

Les voyants associés aux interfaces Ethernet donnent des indications sur la connexion. Ces indications sont les suivantes :

Modèle SN150

Intitulé	Couleur	Etat	Indication
Led en façade ACT/LINK	Vert	Allumé	Lien établi entre le port Ethernet et l'équipement connecté.
		Eteint	Port Ethernet éteint ou lien non établi avec l'équipement connecté.
		Clignote	Le port Ethernet envoie ou reçoit des données. La vitesse de clignotement varie selon le volume du trafic.

Modèles SN200, SN300, SN500, SN700 et SN900

Intitulé	Couleur	Etat	Indication
Led de gauche ACT/LINK	Vert	Allumé	Lien établi entre le port Ethernet et l'équipement connecté.
		Eteint	Port Ethernet éteint ou lien non établi avec l'équipement connecté.
		Clignote	Le port Ethernet envoie ou reçoit des données. La vitesse de clignotement varie selon le volume de trafic.
Led de droite SPEED	Jaune	Allumé	Vitesse de média négociée à 1 Gbps.
	Vert	Allumé	Vitesse de média négociée à 100 Mbps.
		Eteint	Vitesse de média négociée à 10 Mbps.

Modèles SN2000 et SN3000

Face avant et arrière

Intitulé	Couleur	Etat	Indication
Led de gauche ACT/LINK	Vert	Allumé	Lien établi entre le port Ethernet et l'équipement connecté.
		Eteint	Port Ethernet éteint ou lien non établi avec l'équipement connecté.
		Clignote	Le port Ethernet envoie ou reçoit des données. La vitesse de clignotement varie selon le volume de trafic.
Led de droite SPEED	Jaune	Allumé	Vitesse de média négociée à 1 Gbps.
	Vert	Allumé	Vitesse de média négociée à 100 Mbps.
		Eteint	Vitesse de média négociée à 10 Mbps.

Modèle SN6000

Face avant

Intitulé	Couleur	Etat	Indication
Led de gauche ACT/LINK	Vert	Allumé	Lien établi entre le port Ethernet et l'équipement connecté.
		Eteint	Port Ethernet éteint ou lien non établi avec l'équipement connecté.
		Clignote	Le port Ethernet envoie ou reçoit des données. La vitesse de clignotement varie selon le volume de trafic.
Led de droite SPEED	Jaune	Allumé	Vitesse de média négociée à 1 Gbps.
	Vert	Allumé	Vitesse de média négociée à 100 Mbps.
		Eteint	Vitesse de média négociée à 10 Mbps.

Face arrière

IPMI

Intitulé	Couleur	Etat	Indication
Led de gauche LINK	Vert	Allumé	Lien établi entre le port Ethernet et l'équipement connecté (100Mbps).
		Eteint	Port Ethernet éteint ou lien non établi avec l'équipement connecté.
Led de droite ACTIVITY	Jaune	Clignote	Le port Ethernet envoie ou reçoit des données. La vitesse de clignotement varie selon le volume de trafic.
		Eteint	Port Ethernet éteint ou lien non établi avec l'équipement connecté.

MGMT1/2

Intitulé	Couleur	Etat	Indication
Led de droite ACT/LINK	Vert	Allumé	Lien établi entre le port Ethernet et l'équipement connecté.
		Eteint	Port Ethernet éteint ou lien non établi avec l'équipement connecté.
		Clignote	Le port Ethernet envoie ou reçoit des données. La vitesse de clignotement varie selon le volume de trafic.
Led de gauche SPEED	Jaune	Allumé	Vitesse de média négociée à 1 Gbps.
	Vert	Allumé	Vitesse de média négociée à 100 Mbps.
		Eteint	Vitesse de média négociée à 10 Mbps.

Connectiques Ethernet Fibre

Ces ports Ethernet sont disponibles sur le modèle SN900 et désignés par les numéros 13 et 14, ainsi que sur les modèles SN2000, SN3000 et SN6000, lors de l'ajout de modules d'extension.

Dans les deux cas, il est nécessaire d'ajouter un transceiver. Ces transceivers sont de type **SFP** pour les connexions **1Gbps** et **SFP+** pour les connexions **1Gbps/10Gbps**.

Pour plus d'informations, reportez-vous à la partie Raccordement au réseau du chapitre PRECAUTIONS D'INSTALLATION.

Voyants

Les voyants donnent les indications suivantes :

- Modèle SN900 équipé de transceivers de type SFP : une LED de couleur verte est allumée quand le lien est établi et clignote selon le volume de trafic.

- Modèle SN2000 et SN3000 équipés de modules d'extension 1Gbps et de transceivers de type SFP : une LED de couleur verte est allumée quand le lien est établi et clignote selon le volume de trafic.

- Modèle SN6000 équipé de modules d'extensions 1Gbps et de transceivers de type SFP :

Intitulé	Couleur / Etat	Indication
Led de droite SPEED	Jaune	Vitesse de média négociée à 1 Gbps.
Led de gauche ACT/LINK	Verte / Clignote	Lien établi entre le port Ethernet et l'équipement connecté. La vitesse de clignotement varie selon le volume de trafic.

- Modèles SN2000, SN3000 et SN6000 équipes de modules d'extensions 10Gbps et de transceivers de type SFP+ :

Intitulé	Couleur / Etat	Indication
Led du haut SPEED	Bleue	Vitesse de média négociée à 10 Gpps.
	Jaune	Vitesse de média négociée à 1 Gbps.
Led du bas ACT/LINK	Verte / Clignote	Lien établi entre le port Ethernet et l'équipement connecté. La vitesse de clignotement varie selon le volume de trafic.

PRECAUTIONS D'INSTALLATION

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

NOTE

Le branchement des produits est également expliqué dans le Poster **Guide d'installation rapide** se trouvant dans l'emballage.

Conditions d'utilisation

Les Firewalls Stormshield Network sont prévus pour fonctionner en permanence, dans un bureau ou un local technique informatique.

Si vous souhaitez installer votre équipement dans un bureau, choisissez une surface plane et dégagée. Ajoutez les pieds antidérapants aux modèles SN500, SN700 et SN900 : collez un pied antidérapant sous le boîtier, à proximité de chaque coin à environ 2 cm des bords. Ils assurent au Firewall une bonne stabilité et une protection contre les rayures.

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 non autorisés au Firewall doivent être évités.

NOTE

Assurez-vous que les câbles ne gênent pas les voies de passage, afin d'éviter tout risque d'arrachement ou de chute du produit.

Votre Firewall est destiné à un usage interne, à l'abri de tout risque de pluie, d'inondation ou d'humidité excessive. Il doit être installé à l'abri des chocs et vibrations, dans un environnement non poussiéreux, où la température ambiante est conforme aux spécifications du produit. La température ambiante idéale se situe aux alentours de 25°C.

Les tableaux ci-dessous indiquent pour l'ensemble de la gamme SN, la température de fonctionnement, la température de stockage et l'humidité.

Modèles SN150, SN200, SN300, SN500, SN700, SN900, SN2000 et SN3000 :

Température de fonctionnement	Humidité relative en fonctionnement (%)	Température de stockage	Humidité relative de stockage (%)
5° à 40°C (41° à 104°F)	20% à 90% à 40°C (104°F) sans condensation	-30° à 65°C (-22° à 149°F)	5% to 95% à 60°C (140°F) sans condensation

Modèle SN6000 :

Température de fonctionnement	Humidité relative en fonctionnement (%)	Température de stockage	Humidité relative de stockage (%)
10° à 35°C (50° à 95°F)	8% à 90% sans condensation	-30° à 65°C (-22° à 149°F)	5% to 95% à 60°C (140°F) sans condensation

IMPORTANT

Évitez notamment l'exposition directe au rayonnement solaire. Maintenez toujours un espace libre suffisant au niveau des ouïes de ventilation du produit, afin de garantir une circulation optimale de l'air, et éviter ainsi tout risque de surchauffe.

IMPORTANT

Ne posez aucun objet sur votre produit Stormshield Network.

IMPORTANT

Les produits Stormshield Network sont conformes aux exigences de la norme européenne EN55022, classe A ou classe B. Dans un environnement résidentiel, un produit classe A peut provoquer des perturbations radioélectriques, auquel cas l'utilisateur peut se voir obligé de prendre les mesures appropriées.

Installation

Tous les produits Stormshield Network peuvent être installés dans des baies 19 pouces. Les produits SN500, SN700 et SN900 sont livrés avec un kit d'installation contenant des équerres. Les produits SN2000, SN3000 et SN6000 sont livrés avec un jeux de glissières.

Un système de fixation pour mise en baie, sous forme de plateau rackable, peut être livré sur commande pour les modèles SN150, SN200 et SN300. Il est possible de disposer deux Firewalls de type SN150, SN200 ou SN300 sur un même plateau.

RAPPEL

Assurez-vous que la baie respecte les conditions de température et d'hygrométrie préconisées dans la partie Conditions d'utilisation.

NOTE

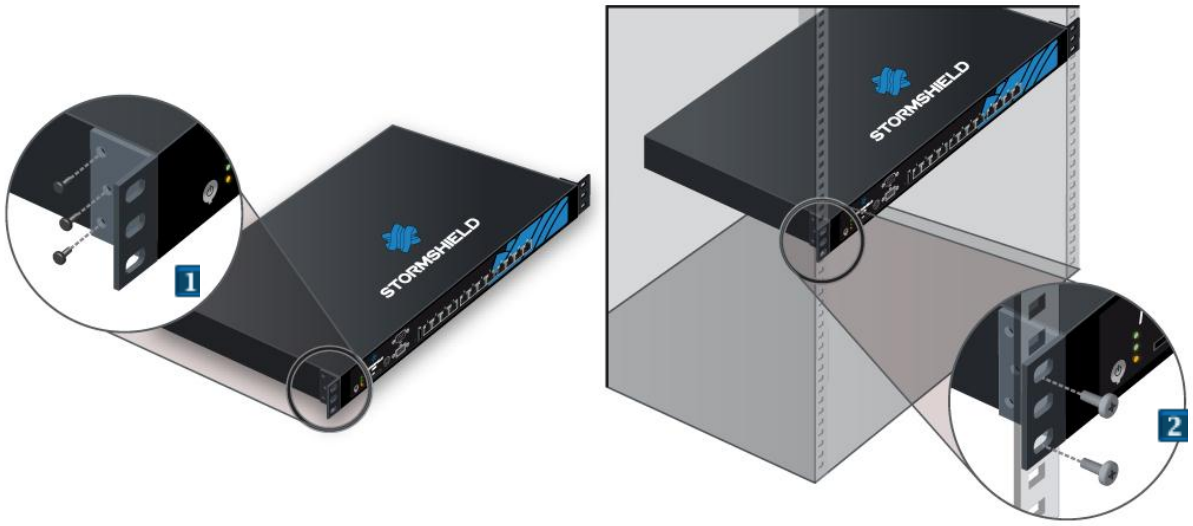
Le modèle SN150 peut également être fixé verticalement (fixations et vis non fournies).

Installation en baie 19" des modèles SN500, SN700 et SN900

L'espace minimum pour l'installation du Firewall SN doit être de 1U en hauteur.

Procédez comme suit :

1. Vissez les équerres sur les bords latéraux du Firewall au moyen des vis fournies.
2. Une fois les équerres installées, vous pouvez fixer l'ensemble aux montants situés à l'avant de votre baie de rackage au moyen d'écrous-cages.



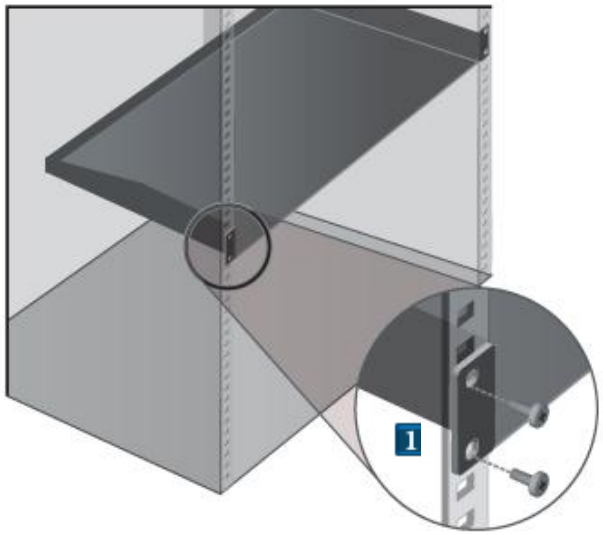
Installation en baie 19" des modèles SN2000, SN3000 et SN6000

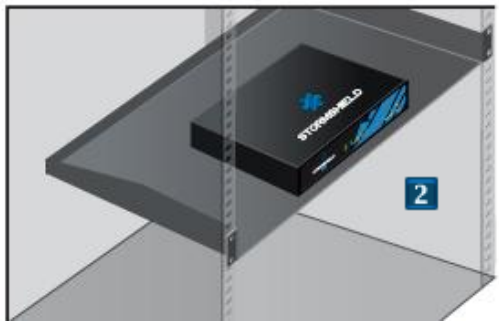
L'espace minimum pour l'installation du Firewall SN doit être de 1U en hauteur pour les modèles SN2000, SN3000 et de 2U en hauteur pour le modèle SN6000. Les procédures d'installation en baie par rails de montage sont décrites dans les documents **SN2000-SN3000_rack mounting** et **SN6000 _rack mounting**. Ces documents sont disponibles dans la rubrique ***Base Documentaire*** de votre Espace sécurisé (*Product > Stormshield Network Firewall > User Guide > Hardware*).

Installation en baie 19" du plateau pour les modèles SN150, SN200 et SN300

Dans ce type d'installation non standard, prévoyez une hauteur supérieure à 1U en raison de l'épaisseur du plateau et de la présence de pieds antidérapants sous l'équipement. Procédez comme suit :

1. Installation du plateau dans la baie. Vissez au moyen d'écrous-cages, le plateau de support sur les montants latéraux situés à l'avant de la baie.
2. Une fois le plateau installé, vous pouvez déposer (aucune fixation n'est nécessaire) un ou deux produits sur le plateau de support.





AVERTISSEMENT

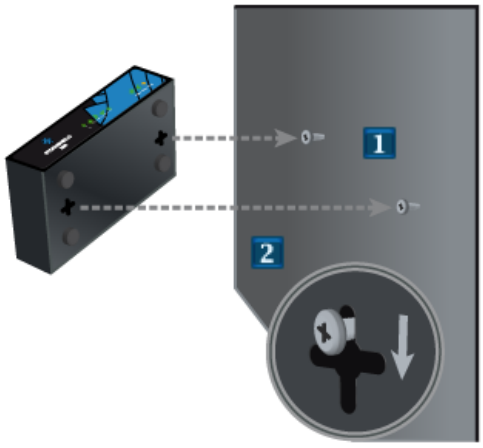
Si vous installez deux produits sur un même plateau, il est nécessaire de prévoir suffisamment d'espace entre les deux Firewalls pour ne pas entraver le flux d'air circulant par les côtés.

Fixation au mur du modèle SN150

Le modèle SN150 peut également être fixé verticalement à l'aide de fixations et vis (non fournies). La tête de ces vis doit être d'un diamètre inférieur à 8mm et leur diamètre de perçage doit être inférieur à 4mm.

Procédez comme suit :

1. Fixez au mur les 2 vis alignées horizontalement en respectant un écart de 12cm.
2. Une fois les vis fixées, vous pouvez insérer la tête des vis à l'intérieur des encoches prévues à cet effet, puis glissez légèrement le produit vers le bas afin d'y insérer les vis.



Raccordement au secteur

Les tensions supportées sont de 100V à 240V.

NOTE

Il est fortement recommandé de raccorder votre Firewall à un équipement de type « UPS » (onduleur). Pour les modèles SN3000 et SN6000 équipés d'alimentations redondantes, il est recommandé de les brancher sur 2 sources secteur différentes.

NOTE

En cas de coupure d'alimentation, le produit redémarre automatiquement à la remise sous tension.

Pour les modèles SN150, SN200 et SN300, branchez la fiche femelle de l'alimentation externe à l'arrière du Firewall. Puis insérez le cordon d'alimentation de l'alimentation dans une prise secteur adéquate.

Pour les modèles SN500, SN700, SN900 et SN2000, insérez la prise femelle du cordon secteur fourni dans l'embase du secteur mâle située sur la face arrière du Firewall. Puis, enfichez la partie mâle du cordon secteur fourni dans une prise secteur adéquate.

Pour les modèles SN3000 et SN6000, insérez la prise femelle des deux cordons secteurs fournis dans les deux embases du secteur mâle situées sur la face arrière du Firewall. Puis, enfichez la partie mâle des deux cordons secteurs fournis dans deux prises secteurs adéquates.

Raccordement pour l'administration du produit

L'administration du produit s'effectue par défaut par l'intermédiaire de son interface INTERNE. Cette interface, pour tous les modèles, est identifiée par le chiffre 2 (IN).

Pour obtenir la description des interfaces, reportez-vous au chapitre Présentation des modèles.

Raccordement au réseau

Tous les modèles sont équipés de ports Ethernet RJ45 Gigabit.

Le modèle SN900 propose en outre, deux ports optionnels permettant d'insérer des transceivers de type **SFP**.

Les modèles SN2000 et SN3000 proposent en outre, deux modules réseaux optionnels permettant soit l'ajout de ports Ethernet RJ45, soit d'insérer des transceivers de type SFP ou soit des transceivers de type SFP+, selon la référence de module commandée.

Le modèle SN6000 propose en outre, sept modules réseaux optionnels permettant soit l'ajout de ports Ethernet RJ45, soit d'insérer des transceivers de type SFP ou soit des transceivers de type SFP+, selon la référence de module commandée.

Utilisez obligatoirement les transceivers **SFP (1Gbps)** ou **SFP+ (1Gbps/10Gbps) homologués Stormshield Network** disponibles au catalogue.

Pour le choix du type de câble réseau en fonction du port réseau et des connectiques choisies, reportez-vous à l'ANNEXE D : MODULES D'EXTENSION (SN2000, SN3000 OU SN6000) et l'ANNEXE E : TRANSCEIVERS FIBRE.

Raccordement Ethernet RJ45

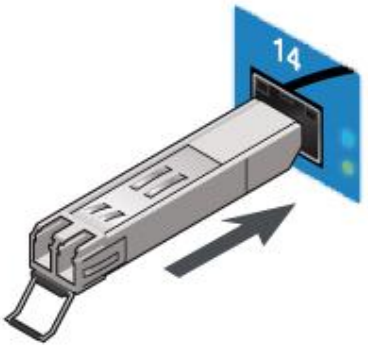
Ces interfaces doivent être reliées aux autres équipements réseaux avec un câble Ethernet RJ45.

NOTE

Un câble croisé est livré avec le Firewall Stormshield Network. Ce câble est de catégorie 5e, prévu pour un fonctionnement en 10Mbps, 100Mbps ou 1Gbps. Vérifiez la compatibilité de vos équipements.

Transceivers optionnels (SN900, SN2000, SN3000 et SN6000)

Ethernet Fibre Optique



Pour le transfert 1Gbps, deux types de transceivers sont disponibles selon la longueur du câblage et le type de fibre utilisée :

- SFP SX : distance courte
- SFP LX : distance longue.

Pour le transfert 10Gbps, deux types de transceivers sont disponibles selon la longueur du câblage et le type de fibre utilisée :

- SFP+ SR : distance courte
- SFP+ LR : distance longue.

NOTE

Seuls les connecteurs de fibres optiques de **type LC** sont supportés.

Des informations nécessaires au choix du matériel et à son raccordement sont détaillées à l'ANNEXE D : MODULES D'EXTENSION (SN2000, SN3000 OU SN6000) et l'ANNEXE E : TRANSCEIVERS FIBRE.

PREMIERE CONNEXION AU PRODUIT

Pré-requis

Configuration minimale pour administrer un Firewall Stormshield Network

Version minimale du système d'exploitation (firmware)

Pour les modèles SN150, SN200, SN300, SN500, SN700, SN900, SN2000 et SN3000, la version minimale du firmware est la V1.1.0 et **pour le modèle SN6000**, cette version est la V1.1.1.

Interface d'administration Web

L'interface de configuration des Firewalls multifonctions Stormshield Network est accessible via un navigateur web et bénéficie des toutes dernières avancées en matière d'ergonomie et de simplicité d'utilisation. Elle est compatible avec les navigateurs suivants :

- Internet Explorer 7 et +
- Firefox 3.6 et +

Suite d'Administration Stormshield Network

Stormshield Network supporte l'exécution des logiciels SN Administration Suite V1 à partir des environnements suivants :

- Microsoft Windows Server 2003 SP2,
- Microsoft Windows XP Service Pack 2 et plus,
- Microsoft Windows Vista Service Pack 2,
- Microsoft Windows 7 et 8,
- Microsoft Windows Server 2008 et 2012.

Préparation de l'accès Internet

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

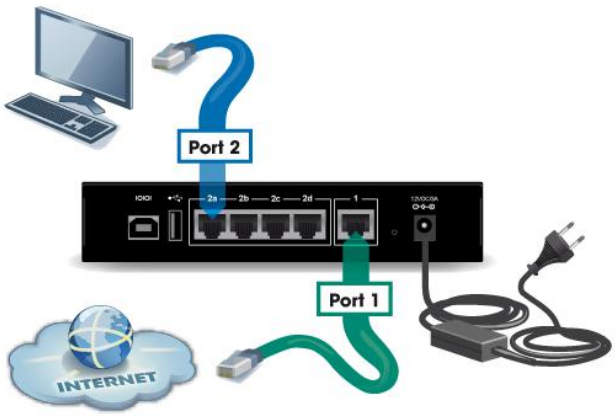
Branchement

Branchez votre Firewall SN sur le secteur, puis connectez les ports réseaux comme suit :

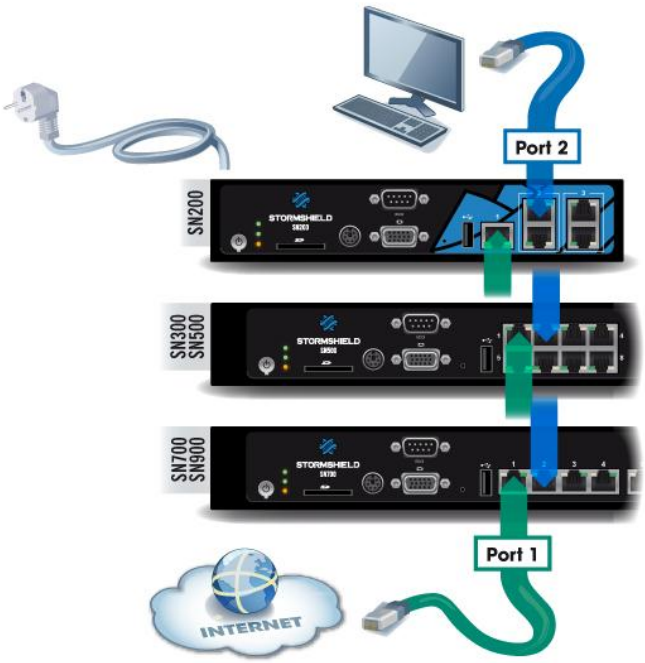
- Interface INTERNE 2 (IN) : Poste client
- Interface EXTERNE 1 (OUT) : Équipement d'accès Internet

Le poste client 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.

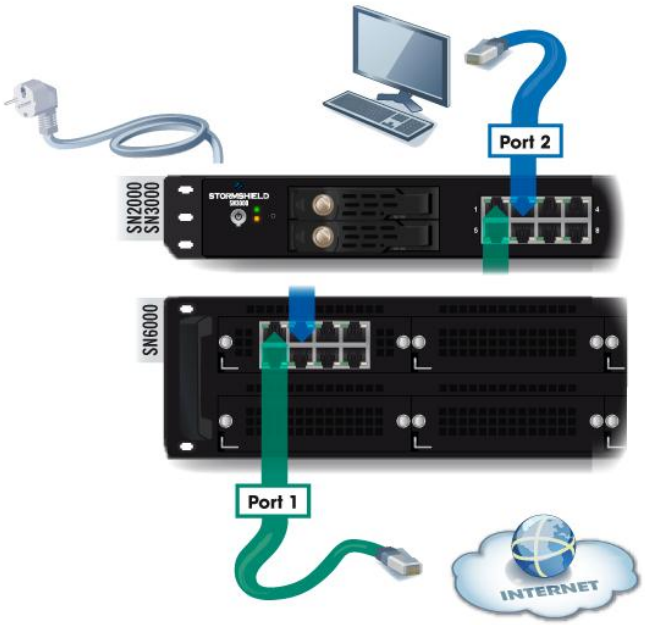
Pour une connexion directe du poste sur le Firewall, utilisez le câble Ethernet croisé, livré avec le produit.



Modèle SN150



Modèles SN200, SN300, SN500, SN700 et SN900



Modèles SN2000, SN3000 et SN6000

IMPORTANT

En configuration usine, le port réseau 1 est réservé au modem ou au routeur Internet. Dans ce cas, vous ne pourrez pas accéder à l'interface de configuration depuis ce port.

Configuration

A la réception de votre Firewall, celui-ci fonctionne en mode transparent (bridge) et possède l'adresse IP **10.0.0.254** et le masque de sous-réseau **255.0.0.0**. Si ces paramètres ne correspondent pas à votre réseau, ils sont cependant nécessaires à la phase de pré-configuration.

Pour vous connecter au Firewall, vous devez utiliser un poste ayant le DHCP activé, ou son adresse IP dans le même plan d'adressage que votre Firewall (10.0.0.0/8). Le DHCP est par défaut, activé sur les plateformes Windows. Si ça n'est pas le cas, reportez-vous au paragraphe suivant **Configuration réseau de votre poste client**. 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 Stormshield Network sera difficile.

NOTE

Dans le cas d'une configuration manuelle, nous vous proposons d'utiliser l'adresse IP 10.0.0.1 et le masque sous-réseau 255.0.0.0.

Configuration réseau de votre poste client

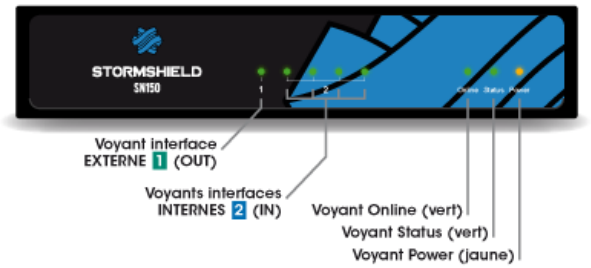
Si sur votre poste client, le DHCP n'est pas activé ou dans le cas d'une configuration manuelle, modifiez les paramètres de **Connexions réseau** de votre système d'exploitation.

Sur Windows, il faut généralement sélectionner « Protocole Internet (TCP/IP) » dans la liste, puis « Propriétés », cochez **Obtenir une adresse IP automatiquement**.

Pour configurer manuellement ce réseau, indiquez les informations d'adressage nécessaires. A la première connexion, l'adresse IP de ce poste devra appartenir au même plan d'adressage que celui du Firewall, soit par défaut 10.0.0.0/8.

Démarrage du SN150

Une fois branché sur le secteur, votre Firewall démarre automatiquement. Attendez quelques minutes que les 3 voyants *Online*, *Status* et *Power* soient allumés.



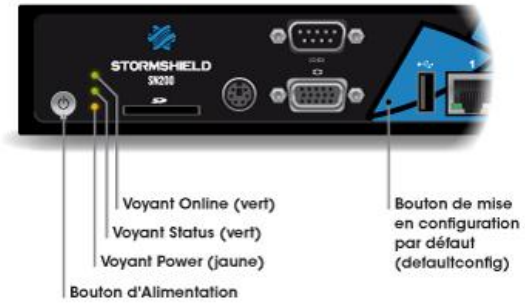
NOTE

Pendant le démarrage, vous pouvez, si nécessaire, insérer une clé USB contenant une configuration. Le mode console affiche le message suivant : « *Please insert your USB token to continue* ».

Le voyant *Online* allumé indique la fin de la phase de démarrage du produit.

Démarrage du SN200, SN300, SN500, SN700 et SN900

Appuyez une fois sur le **Bouton d'Alimentation** puis attendez quelques minutes que les 3 voyants *Online*, *Status* et *Power* soient allumés.



NOTE

Huit bips successifs vous permet, si nécessaire, d'insérer une clé USB contenant une configuration. Le mode console affiche le message suivant : «*Please insert your USB token to continue*».

Deux bips successifs et le voyant *Online* allumé indiquent la fin de la phase de démarrage du produit.

Démarrage du SN2000 et SN3000

Appuyez une fois sur le **Bouton d'Alimentation** puis attendez quelques minutes que les 2 voyants *Online* et *Power* soient allumés.

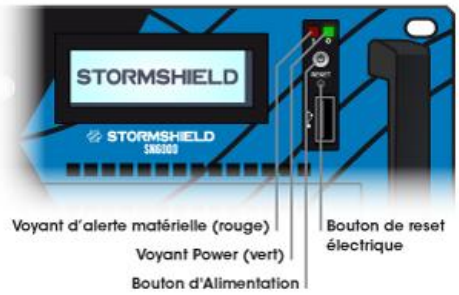
NOTE

Huit bips successifs vous permet, si nécessaire, d'insérer une clé USB contenant une configuration. Le mode console affiche le message suivant : «*Please insert your USB token to continue*».

Deux bips successifs et le voyant *Online* allumé indiquent la fin de la phase de démarrage du produit.

Démarrage du SN6000

Appuyez une fois sur le **Bouton d'Alimentation** et le voyant *Power* s'allume. Attendez quelques minutes que le produit démarre.



NOTE

Huit bips successifs vous permet, si nécessaire, d'insérer une clé USB contenant une configuration. Le mode console affiche le message suivant : «*Please insert your USB token to continue*».

Deux bips successifs et le voyant *Online* allumé indiquent la fin de la phase de démarrage du produit.

Première connexion au boîtier

La première connexion au boîtier nécessite une procédure de sécurisation si celle-ci s'effectue au travers d'un réseau qui ne soit pas de confiance. Cette opération n'est pas nécessaire si la station d'administration est branchée directement au produit.

L'accès au portail d'administration est sécurisé via le protocole SSL/TLS. Cette protection permet d'authentifier le portail via un certificat, assurant ainsi à l'administrateur qu'il est bien connecté au boîtier désiré. Ce certificat peut être le certificat par défaut du boîtier ou celui renseigné dans sa configuration (*Authentification > Portail captif*). Le certificat par défaut du boîtier a comme nom (CN) le numéro de série du boîtier et il est signé par l'autorité 'dont le nom est NETASQ - Secure Internet Connectivity ("O") / NETASQ Firewall Certification Authority ("OU").

Pour valider un accès sécurisé, le navigateur doit faire confiance à l'autorité de certification qui a signé le certificat utilisé, et appartenant à la liste des autorités de certification de confiance du navigateur. Ainsi pour valider l'intégrité du boîtier, il faut donc avant la première connexion, ajouter l'autorité NETASQ à la liste des autorités de confiance du navigateur. Cette autorité est disponible sur le lien :

http://www.netasq.com/pki/netasq-firewall-ca.crt.

Si le boîtier a configuré un certificat signé par une autre autorité, il faut y ajouter cette autorité à la place de celle de NETASQ.

En conséquence, la connexion initiale au boîtier ne déclenchera plus d'avertissement du navigateur relatif à l'autorité de confiance. En revanche, un message avertit toujours que le certificat n'est pas valide. En effet, le certificat définit le Firewall par son numéro de série, et non par son adresse IP. Pour éviter ce dernier avertissement, il faut spécifier au serveur DNS l'association entre le numéro de série et l'IP du Firewall.

Assistant de première Installation

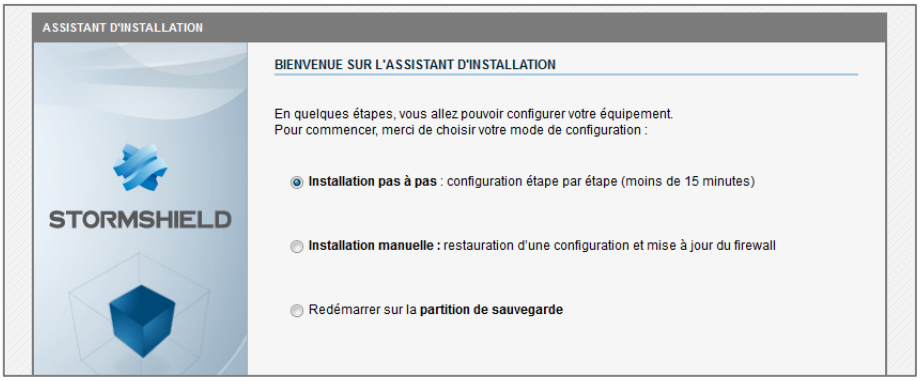
Depuis votre poste client, tapez l'adresse ci-dessous dans votre navigateur : https://10.0.0.254/install

Saisissez le mot de passe «**admin**».

IMPORTANT

Si vous avez connecté votre poste client sur le port 1, vous ne pourrez pas accéder à l'Assistant d'installation. Il faut connecter votre ordinateur sur le port 2 (ou sur un autre port), et redémarrer votre Firewall.

Un Assistant d'installation vous accueille afin de vous guider pour le paramétrage de votre Firewall.



NOTE

Le mot de passe par défaut de l'utilisateur 'admin' (super administrateur) doit être modifié lors de la première utilisation du produit. Ce changement est proposé via l'Assistant de première installation, dans l'écran *Administration de l'équipement*. Dans l'interface d'administration web, ce mot de passe peut être modifié via le module **Administrateur** (menu **Système**), onglet *Compte Admin*.

Ce mot de passe doit être défini selon les bonnes pratiques décrites dans le Guide, chapitre **Bienvenue**, partie *Sensibilisation des utilisateurs*, paragraphe *Gestion des mots de passe de l'utilisateur*, à l'adresse : http://documentation.arkoon-netasq.com/

Vous pourrez grâce à cet assistant :

- Configurer le réseau pour définir l'architecture réseau dans laquelle se trouve votre produit,
- Configurer votre politique de sécurité,
- Enregistrer votre produit pour obtenir les mises à jour,
- Effectuer les premières mises à jour,
- Télécharger et installer votre licence. Pour plus d'informations à ce sujet, veuillez vous référer à **l'Annexe A : MISE A JOUR DE LA LICENCE**.

L'étape d'enregistrement vous permet d'obtenir le mot de passe d'accès à votre **Espace sécurisé**. Une fois l'installation terminée, vous pouvez vous connecter à **l'interface graphique de configuration** à l'adresse suivante : https://10.0.0.254/admin

Suite d'Administration Stormshield Network

La Suite d'Administration Stormshield Network, regroupant les logiciels UNIFIED MANAGER, REALTIME MONITOR et EVENT REPORTER est téléchargeable depuis votre Espace sécurisé.

Connectez-vous à l'adresse suivante pour accéder ou obtenir les codes d'accès à votre **Espace sécurisé** : https://mystormshield.eu/

Vous pouvez également obtenir cette Suite à l'adresse : http://gui.arkoon-netasq.com/last-version

Documentation

• AIDE EN LIGNE

Le guide d'utilisation des Firewalls Multifonctions SN est disponible en ligne à l'adresse :
http://documentation.arkoon-netasq.com

• ESPACE SECURISE

Votre **Espace sécurisé** vous permet notamment de :

- Activer vos licences d'utilisation, une option logicielle ou télécharger les dernières mises à jour,
- Gérer vos licences,
- Vous inscrire aux mailing-lists techniques et commerciales,
- Accéder à la base documentaire et à la base de connaissance.

Connectez-vous à l'adresse suivante pour accéder ou obtenir les codes d'accès à votre **Espace sécurisé** :
https://mystormshield.eu/

• BASE DOCUMENTAIRE

Cette base, accessible depuis l'espace sécurisé, vous permet de consulter ou de télécharger diverses documentations techniques (Guides d'utilisation, Notes Techniques, etc.). Rendez-vous dans la rubrique ***Base Documentaire*** de votre **Espace sécurisé**.

• BASE DE CONNAISSANCE

La base de connaissance du support technique regroupe les diverses connaissances techniques liées à l'utilisation des produits Stormshield Network. Elle a vocation à permettre une meilleure compréhension de leur fonctionnement. Rendez-vous dans la rubrique ***Base de connaissance*** de votre **Espace sécurisé**.

Assistance

En cas de problème matériel avec votre Firewall ou si l'un des éléments n'est pas conforme à sa description, contactez votre partenaire certifié.

Pour les produits Stormshield Network, il existe différentes procédures de renvoi appelées RMA (return merchandise authorization). Les différents types de RMA sont les suivants :

1. RMA AVEC ECHANGE STANDARD :

   Si le produit dispose d'une maintenance **initiale** en cours de validité,
2. RMA AVEC ECHANGE EXPRESS :

   Si le produit dispose d'une maintenance **privilège** en cours de validité,
3. RMA AVEC ECHANGE DOA :

Si le produit a été enregistré moins de **30 jours** avant le déclenchement du RMA.

Les documents relatifs à ces procédures et à leur mise en œuvre sont disponibles dans la rubrique ***Base Documentaire*** (dossier *Operational*) depuis votre **Espace sécurisé**.

Afin de se conformer aux hypothèses de l'évaluation aux critères communs, les clients doivent souscrire à l'option **Echange sécurisé** et suivre la procédure dédiée à ce type d'échange. Cette option assure la confidentialité des éléments de configuration importés dans le produit Stormshield Network avant son envoi en réparation.

ANNEXE A : MISE A JOUR DE LA LICENCE

Votre produit est livré avec une licence temporaire. Il est donc nécessaire de mettre à jour cette licence.

NOTE

L'étape de la mise à jour de la licence est proposée dans l'assistant de première installation.

Si vous avez fait l'acquisition d'une option supplémentaire, vous devez mettre à jour le produit avec la licence qui autorise l'utilisation de cette option.

ATTENTION

Les options nécessitant un redémarrage du Firewall sont précisées dans l'**aide en ligne**, au chapitre Licence.

Référez-vous à la procédure suivante pour mettre à jour la licence du produit :

Récupération de la licence

1. Accédez à votre Espace Sécurisé à partir de l'adresse https://mystormshield.eu/
2. Indiquez votre identifiant et votre mot de passe puis validez, ou inscrivez-vous pour recevoir ceux-ci. La page d'accueil de l'accès client s'affiche.
3. Cliquez sur « Gestion des produits ». Vous visualisez alors la liste de tous les produits Stormshield Network enregistrés dans l'espace.
4. Sélectionnez le modèle du produit dont vous voulez récupérer la licence, puis cliquez sur le numéro de série de ce produit. Le détail de la licence s'affiche.

NOTE

Pour télécharger la licence, il est nécessaire de connaître la version de votre produit. Si vous ne la connaissez pas, celle-ci est indiquée sur une étiquette collée sur le carton d'emballage du produit. Si vous n'avez plus accès au carton ou si vous avez mis à jour votre produit depuis, connectez-vous au produit par l'interface d'Administration web. La version du produit est indiquée sur le Tableau de Bord de l'application web.

Installation de la licence

Si vous n'avez jamais installé de licence sur le produit, le détail de la licence sera celui de la licence temporaire. Pour installer la licence préalablement téléchargée depuis l'espace client, procédez comme indiqué ci-dessous :

Par l'interface d'Administration web, rendez vous dans l'onglet Général du module **Licence**.

- Pour installer une licence en manuel, injectez le fichier de licence téléchargé dans le champ adapté. Il est toutefois possible de paramétrer la recherche et l'installation de la licence en automatique.
- Pour les Firmwares en version 1.x, la procédure complète est détaillée dans l'aide en ligne, au chapitre Licence.

ANNEXE B : REINITIALISATION DU FIREWALL

Il est possible de restaurer la configuration usine d'un Firewall Stormshield Network. Cette opération ramène alors le produit dans la version initiale de sa configuration. Cette réinitialisation ne modifie pas la version du firmware et ne concerne que la partition active.

AVERTISSEMENT

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. Il est donc conseillé d'effectuer une sauvegarde au préalable.

ATTENTION

Il est **impératif** de ne *pas* débrancher le produit pendant la réinitialisation.

Après quelques minutes le Firewall aura retrouvé sa configuration usine et redémarrera. Cette réinitialisation peut durer **jusqu'à 10 minutes**, veuillez donc attendre la fin du redémarrage pour vous reconnecter au Firewall.

NOTE

Les voyants *Online* et *Status* clignotent pendant toute la durée de la réinitialisation. Deux bips successifs (sauf modèle SN150) et le voyant *Online* allumé indiquent la fin de la phase de redémarrage du produit.

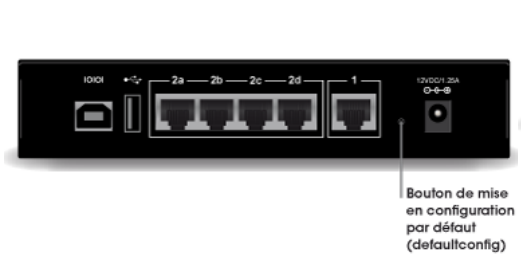
AVERTISSEMENT

Cette opération réinitialise aussi le mot de passe administrateur. L'identifiant et le mot de passe sont par défaut « admin ».

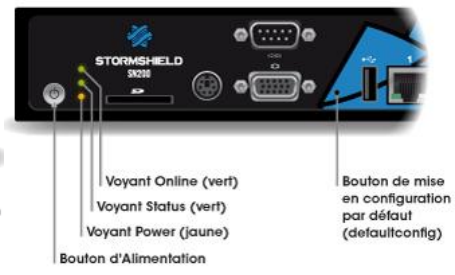
Tous les modèles sauf SN6000

Pour réinitialiser votre Firewall, munissez-vous d'une pointe très fine. Un petit poussoir est accessible par un trou, placé :

- pour les modèles SN150, sur la face arrière du produit, entre les interfaces Ethernet et la fiche de branchement de l'adaptateur secteur.
- pour les modèles SN200, SN300, SN500, SN700 et SN900, sur la face avant du produit, entre le port USB et le port VGA.
- pour les modèles SN2000 et SN3000, sur la face avant du produit, entre les voyants et les racks SSD.



SN150 model



SN200, SN300, SN500, SN700 and SN900 models

SN2000 and SN3000models

Maintenez le poussoir appuyé au moyen de la pointe pendant environ 5 secondes, jusqu'à ce que les voyants *Online* et *Status* clignotent et/ou entendre un signal sonore. La procédure de réinitialisation du Firewall se lance alors automatiquement.

Modèle SN6000

Il est possible de restaurer la configuration usine d'un SN6000, uniquement en se connectant en mode console. Tapez la commande suivante : `defaultconfig -f -r -p`

ANNEXE C : STOCKAGE EXTERNE DES TRACES SUR CARTE SD

La fonctionnalité de **Stockage externe des traces sur carte SD** est disponible sur l'ensemble des modèles de la gamme SN, à l'exception des modèles SN150, SN2000, SN3000 et SN6000. Cette fonctionnalité est proposée en souscrivant à l'option « External storage ».

NOTE

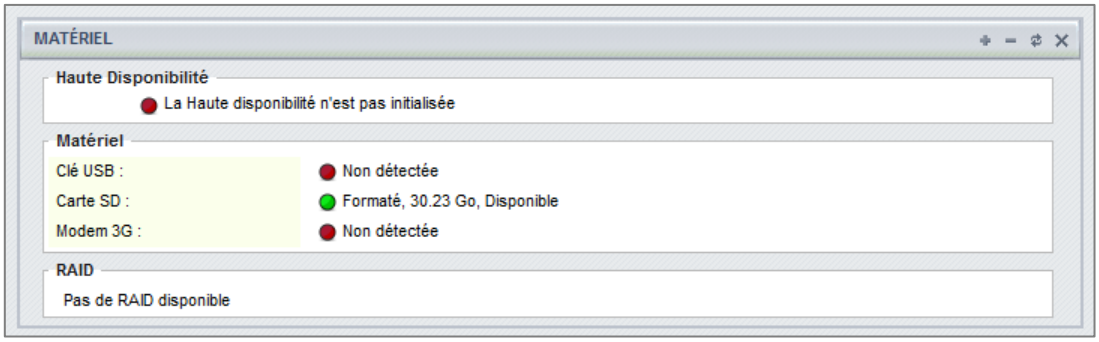
Ce stockage sur support externe s'effectue uniquement sur carte SD. Ce service n'est pas compatible avec d'autres supports de stockage comme une clé USB ou un disque dur externe.

Le type de carte SD doit être au minimum **de Classe 6** et **de standard SDHC**. La taille maximum de mémoire supportée est de 32Go.

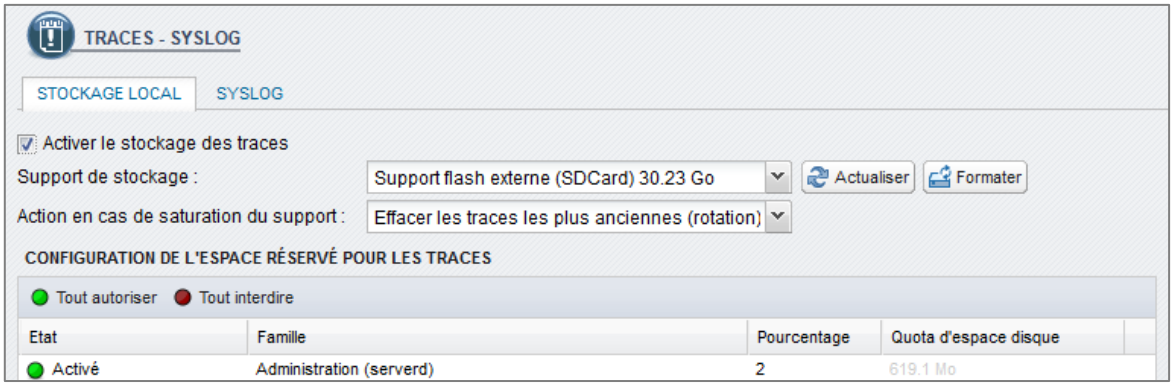
Première utilisation

Insérez la carte SD, comme décrit dans le schéma ci-contre, avec les connecteurs orientés vers le bas.

Lorsque vous insérez la carte SD pour la première fois, le composant *Matériel* (widget) du **Tableau de Bord** affiche les informations suivantes :



Pour activer le service, rendez-vous dans le menu **Notifications**, puis dans le module **Traces – Syslog**. L'onglet *Stockage local*, vous propose d'activer le stockage des traces.



Choisissez ensuite votre carte SD dans la liste de support de stockage. Un message vous propose de formater la carte. Après cette opération, votre carte SD est prête à recevoir l'ensemble des traces.

Ces traces pourront être consultées via l'interface web **SN Activity Reports** sous forme de rapports, et également par l'application SN Event Reporter.

Dans **SN Activity Reports,** 5 rapports sont activés par défaut. Le nombre de rapports activés peut être augmenté sur les modèles disposant d'un disque dur ou à l'aide d'une carte SD avec l'option « External storage » (sauf SN150).

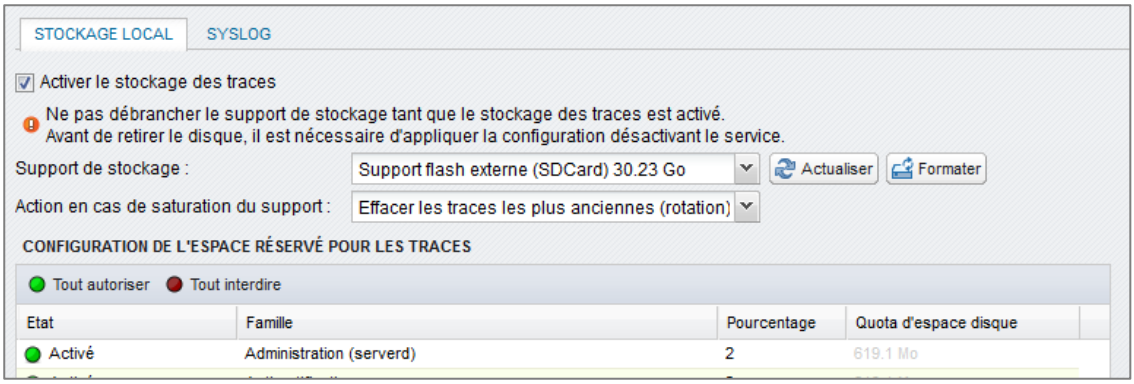
Consultez l'aide en ligne, chapitre *SN Activity Reports* pour plus d'informations.

Changement du support de stockage

IMPORTANT

Avant d'éjecter la carte SD du lecteur (pour changer de support, par exemple), il est impératif d'arrêter le service en décochant l'option d'activation du stockage des traces, dans le module **Traces - Syslog**.

Pour éjecter la carte SD, appuyez horizontalement et légèrement sur le support, puis relâchez.



ANNEXE D : MODULES D'EXTENSION (SN2000, SN3000 OU SN6000)

La procédure d'ajout d'un module d'extension au Firewall SN2000, SN3000 ou SN6000 se déroule en trois étapes principales :

Etape 1 Arrêt du Firewall.
Etape 2 Insertion du module.
Etape 3 Redémarrage du Firewall

NOTE

Les modules d'extension pour SN2000 / SN3000 et ceux pour SN6000 ne sont pas mécaniquement compatibles.
Les transceivers SFP/SFP+ pour modules d'extension Fibre doivent être commandés séparément.
Les transceivers SFP/SFP+ sont insérables / extractibles à chaud.

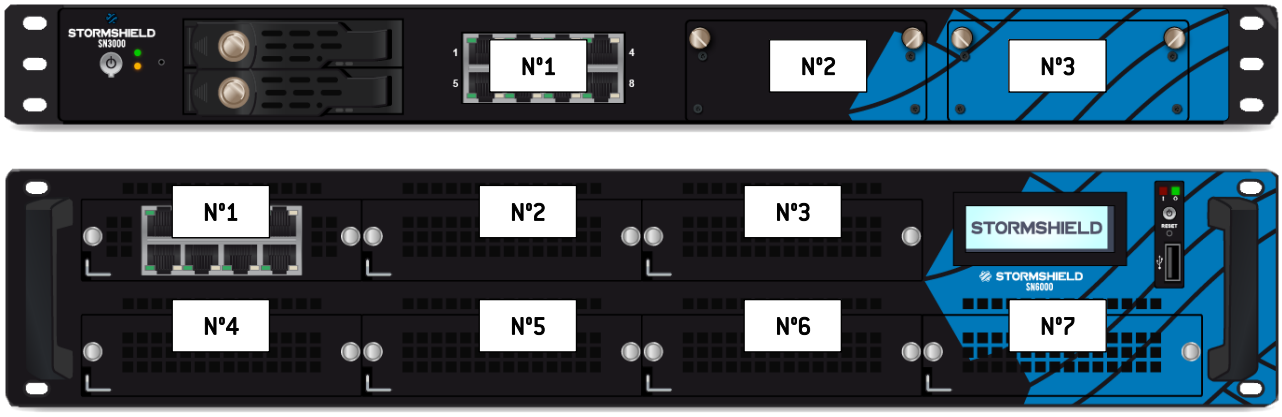
Description des modules d'extension pour SN2000, SN3000 et SN6000

Les produits SN2000, SN3000 et SN6000 acceptent les modules d'extension suivants :

- **Module 8 ports Cuivre 1GbE**
  - Connectique RJ45
  - 1000/100/10Base-T
- **Module 4 ports Fibre 1GbE**
  - 4 cages SFP, supportant au choix les transceivers suivants :
    - Transceiver Fibre SFP, 1000Base-SX (1Gbps Ethernet, courte distance).
    - Transceiver Fibre SFP, 1000Base-LX (1Gbps Ethernet, longue distance).
- **Module 4 ports Fibre 10GbE**
  - 4 cages SFP+, supportant au choix les transceivers suivants :
    - Transceiver Fibre SFP+, 10GBase-SR (10Gbps Ethernet, courte distance) / 1000BASE-SX (1Gbps Ethernet, courte distance).
    - Transceiver Fibre SFP+, 10GBase-LR (10Gbps Ethernet, longue distance) / 1000BASE-LX (1Gbps Ethernet, longue distance).

Ordonnancement des modules

Dans le cas d'ajout ou de suppression de modules d'extension, les ports seront **réordonnés** en configuration selon l'ordre présenté ci-dessous.



Procédures d'insertion/ enlèvement de modules réseaux

L'ajout de modules réseaux ne requiert pas de licence spécifique.

IMPORTANT

L'ajout ou l'enlèvement de modules réseaux doit impérativement s'effectuer sur le produit mis à l'arrêt.

Les contraintes concernant le placement des modules sont les suivantes :

- Les modules doivent être insérés de gauche à droite, en commençant par la rangée du haut.
- Il est impératif de ne pas laisser de slot vide entre deux modules dans une même rangée.

En outre, sur le modèle SN6000, pour obtenir les meilleures performances sur votre produit, il est conseillé de répartir les modules réseaux sur les 2 rangées, sans toutefois laisser de slot vide entre deux modules dans une même rangée. Cela permet d'équilibrer la charge de traitement par les processeurs. En effet, la première rangée de modules et les 2 ports réseaux situés à l'arrière sont gérés prioritairement par le 1er processeur et la seconde rangée, par le 2d processeur.

RAPPEL

Dans le cas d'ajout a posteriori de modules en fin de rangée 1, les ports des modules de la rangée 2 seront automatiquement décalés en configuration.

Insertion d'un module d'extension pour SN2000 ou SN3000

- A l'aide du bouton poussoir en face avant, lancer l'arrêt du Firewall,
- Après l'extinction, le déconnecter impérativement de toute alimentation électrique,
- Oter la face de bouchage, en dévissant les 2 vis moletées,
- Présenter le module d'extension, l'insérer à fond (appuyer plus fortement en fin de parcours),
- Visser complètement les 2 vis moletées,
- Reconnecter le Firewall à l'alimentation électrique,
- A l'aide du bouton poussoir en face avant, démarrer le Firewall.

Extraction d'un module d'extension pour SN2000 ou SN3000

- A l'aide du bouton poussoir en face avant, lancer l'arrêt du Firewall,
- Après l'extinction, le déconnecter impérativement de toute alimentation électrique,
- Dévisser complètement les 2 vis moletées,
- Extraire le module d'extension en tirant sur les 2 vis,
- Replacer la face de bouchage en vissant complètement les 2 vis moletées,
- Reconnecter le Firewall à l'alimentation électrique,
- A l'aide du bouton poussoir en face avant, démarrer le Firewall.

Extraction / Insertion d'un module d'extension pour SN6000

- A l'aide du bouton poussoir en face avant, lancer l'arrêt du Firewall,
- Après l'extinction, le déconnecter impérativement de toute alimentation électrique,
- Déverrouiller et extraire le module en place en levant le petit levier en bas à gauche, tout en tirant sur les 2 tiges,
- Présenter le module à insérer, l'engager à fond (jusqu'à entendre le "clic" de verrouillage),
- Reconnecter le Firewall à l'alimentation électrique,
- A l'aide du bouton poussoir en face avant, démarrer le Firewall.

ANNEXE E : TRANSCEIVERS FIBRE

RAPPEL

- Le modèle SN900 propose deux ports optionnels **SFP**.
- Utilisez obligatoirement les transceivers **SFP (1Gbps)** ou **SFP+ (1/10Gbps) homologués Stormshield Network** disponibles au catalogue.
- Pour les fibres optiques, seuls les connecteurs de **type LC** sont supportés.

Transceivers Ethernet homologués Stormshield Network

		SN900	SN2000, SN3000 et SN6000
CONNECTIQUE FIBRE			
GIGA - SFP	**Transceiver SFP, 1000Base-SX, fibre multimode :** Nécessite une fibre **multimode**. Distance maximum typique supportée (sous condition de qualité optimale) : 550m	supporté	supporté
GIGA - SFP	**Transceiver SFP, 1000Base-LX, fibre monomode :** Ethernet 1000Base-LX, nécessite une fibre **monomode**. Distance maximum typique supportée (sous condition de qualité optimale) : Monomode : 10km	supporté	supporté
10 GIGA - SFP+	**Transceiver SFP+, 10GBASE-SR/1000Base-SX, fibre multimode :** Ethernet 10GBASE-SR/1000Base-SX, nécessite une fibre **multimode**. Distance maximum typique supportée (sous condition de qualité optimale) : 300m à 10Gbps, 550m à 1Gbps.	non supporté	supporté
10 GIGA - SFP+	**Transceiver SFP+, 10GBASE -LR, fibre monomode :** Ethernet 10GBASE-LR /1000Base-LX, nécessite une fibre **monomode**. Distance maximum typique supportée (sous condition de qualité optimale) : 10 km	non supporté	supporté

NOTE

Seuls les transceivers 1 Gigabit ou 10 Gigabits distribués par Stormshield Network sont supportés. Toutefois des câbles Twinax peuvent être utilisés. Contactez votre partenaire en cas de besoin spécifique.

Installation

Pour installer votre transceiver, procédez comme suit :

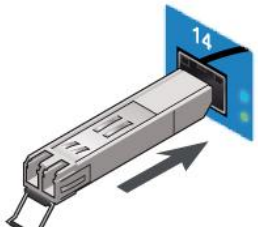
1. Retirez le cache du slot d'extension sur lequel vous voulez installer le transceiver
2. Insérez le transceiver, puis raccordez le câble optique correspondant à ce transceiver.

Pour les instructions de raccordement physique au réseau, référez-vous aux paragraphes **Transceivers optionnels**, partie Raccordement au réseau du chapitre PRECAUTIONS D'INSTALLATION.

Pour la configuration de ces interfaces, veuillez vous reporter aux indications du tableau des transceivers homologués Stormshield Network, décrits au chapitre précédent.

IMPORTANT

Le transceiver et la fibre sont équipés d'un embout de protection. Lorsque vous raccordez cette fibre optique au transceiver, ôtez les embouts de protection et conservez-les à l'abri de la poussière, pour une utilisation ultérieure.



IMPORTANT

Respectez le rayon de courbure indiqué dans la notice technique de votre fibre optique.

ANNEXE F : GESTION DES SSD

Le SSD (Solid-state drive) du modèle SN2000 est amovible. De base, les deux SSD sont installés en RAID sur les modèles SN3000 et SN6000 sont également remplaçables. La reconstruction d'un SSD en RAID ne requiert pas de licence spécifique.

NOTE

Sur le modèle SN2000, tout remplacement de SSD entraîne la perte des logs et des rapports statiques enregistrés sur la partition de traces, ainsi que les données mises en mémoire par l'option Cache HTTP si celle-ci est activée.

Détection de problèmes

Sur le modèle SN2000, en cas de problème avec la partition de logs, remontée par le widget **Propriétés** ou en mode console ou par connexion SSH, via la commande : `logdisk -c`.

Reconstruire la partition s'effectue par la commande suivante, mais efface les données enregistrées :

```
logdisk -f
```

Si celle-ci est toujours défaillante, vous pouvez décider de remplacer votre SSD.

En cas de SSD en RAID (modèles SN3000 et SN6000), lancez l'application SN REALTIME MONITOR et consultez le panneau **Matériel** ; l'encart *RAID* vous informe de l'état du ou des SSD. Vous pouvez également vous connecter au produit en mode console ou par connexion SSH, et obtenir ces informations par la commande suivante : `nraid -s`

Ajout et extraction des SSD

Selon le modèle, la procédure est la suivante :

- SN2000 :

Cette procédure s'effectue sur le produit mis à l'arrêt. Après avoir extrait le SSD défectueux, insérez le nouveau SSD, obtenu auprès de votre partenaire. Une fois le nouveau SSD réinséré, celui-ci sera détecté au prochain démarrage du produit.

- SN3000 et SN6000 (SSD en RAID) :

Cette procédure s'effectue sur le produit en fonctionnement. Après avoir extrait le SSD défectueux, insérez le nouveau SSD, obtenu auprès de votre partenaire. Une fois le nouveau SSD réinséré, tapez les commandes suivantes pour scanner le nouveau SSD inséré : `nraid -z`.

Tapez ensuite la commande pour reconstruire le raid : `nraid -r`

Option *Big Data*

En cas de souscription à l'option *Big Data*, les disques durs d'origine sont remplacés par des SSD d'une capacité supérieure. Après avoir arrêté le produit, vous pouvez extraire le ou les SSD. Insérez ensuite les nouveaux SSD. Ceux-ci seront automatiquement pris en compte au prochain démarrage du produit.

STORMSHIELD

documentation@stormshield.eu