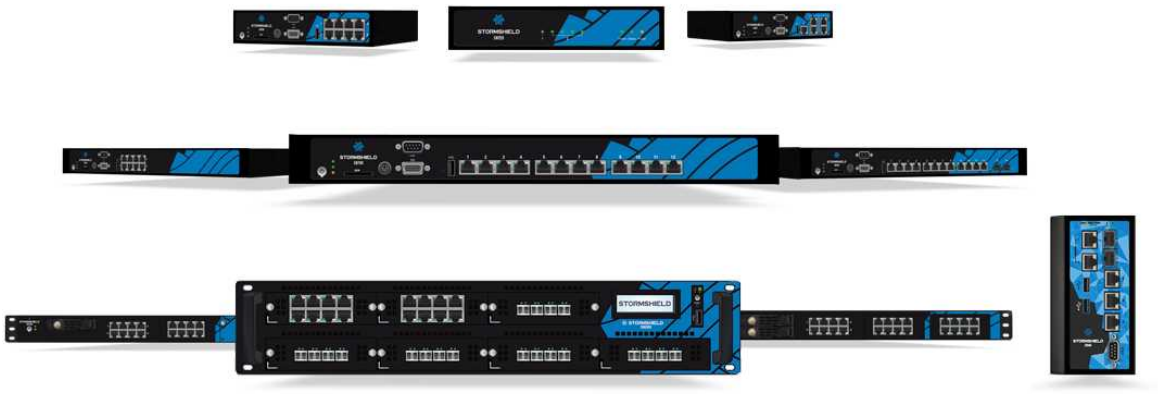
GUIDE

STORMSHIELD NETWORK SECURITY

PRÉSENTATION ET INSTALLATION PRODUITS 2016

Gamme SN



Date	Version	
Août 2014	V1.0	Création
Novembre 2014	V1.1	Mise à jour
Mai 2015	V1.2	Mise à jour (SN910)
Octobre 2015	V1.3	Mise à jour (SN510 et SN710)
Janvier 2016	V1.4	Mise à jour (Stormshield CGU)
Mai 2016	V1.5	Mise à jour (SNi40)
Décembre 2020	V1.6	Mise à jour (Conditions d'utilisation)

Reference: sns-fr-GammeSN_guide_installation-2016

Table des matières

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 Stormshield. 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 SN710, SN900, SN910, SN2000, SN3000, SN6000 et SNi40.

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.stormshield.eu

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

Produits concernés

SN150, SN200, SN300, SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN3000, SN6000 et SNi40.

Conditions générales d'utilisation et licence d'utilisation

Pour vous assurer d'avoir connaissance des Conditions générales d'utilisation et Licence d'utilisation actuelles ou pour accéder aux versions traduites, rendez-vous dans la rubrique BASE DOCUMENTAIRE de votre Espace sécurisé.

(version 1.0 - Janvier 2016)

STORMSHIELD NETWORK SECURITY
CONDITIONS GENERALES 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 de la (des) solution(s) matérielle(s) Stormshield Network Security (ci-après le(s) « Produit(s) ») par le Client.

Les présentes Conditions d'utilisation s'appliquent aux Produits distribués par Stormshield 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 reconnait.

1. Documents contractuels

Les présentes Conditions complétées par les Conditions Générales de Vente Stormshield et la Charte Support Technique déterminent l'étendue des engagements existant entre Stormshield 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 Stormshield existant au moment de leur rédaction.

Cependant, Stormshield 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, Stormshield dégage toute responsabilité quant aux inexactitudes qui pourraient apparaître dans ce document et aux dommages qui pourraient en résulter.

Stormshield 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, Stormshield 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, Stormshield 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, Stormshield 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, Stormshield 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 Stormshield en cas de dommages directs se limite au montant reçu par Stormshield pour l'achat du Produit qui a effectivement causé les dommages.
   En aucun cas Stormshield 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 Stormshield a été avisée de la possibilité de tels dommages.
   Stormshield 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. Stormshield ne garantit pas que l'utilisation du (des) Produit(s) puisse être ininterrompue et exempte d'erreurs.
5. De même, Stormshield décline toute responsabilité en cas de mauvaise installation, paramétrage, configuration et/ou d'utilisation non conforme du (des) Produit(s). Stormshield 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 taches 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), Stormshield 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) 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 Stormshield que des tiers ayant subi un dommage de ce fait.

3. Licence d'utilisation

Par la présente licence, Stormshield 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.

Stormshield 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

Copyright © Stormshield 2016. Tous droits réservés.

Toute reproduction, adaptation ou traduction de la présente documentation sans permission préalable est interdite.

Brevet

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

5. Données

1. Certains Produits 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 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. Stormshield dégage toute responsabilité quant à l'utilisation du (des) Produit(s) non conforme à la législation locale du Client. Stormshield ne saurait être responsable du défaut de conformité légale du Client.
4. De façon générale, le Client garantit à Stormshield 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 Stormshield contre tout recours, plainte ou réclamation émanant d'une personne physique dont les données personnelles seraient reproduites et transmises à Stormshield.
5. En aucun cas Stormshield 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

Stormshield 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° 388/2012 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.

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

Tout Distributeur, Revendeur ou autre Partenaire Stormshield quelle que soit la dénomination qu'on lui donne est averti que s'il exporte des Produits 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, Stormshield 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. Stormshield a obtenu les autorisations requises. Il appartient au Distributeur, Revendeur, Partenaire ou autre de procéder, sous sa seule responsabilité, aux formalités et démarches légales et/ou réglementaires qui pourraient être applicables aux Produits. Stormshield 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 D'UTILISATION ET LICENCE D'UTILISATION SERA OBLIGATOIREMENT SOUMIS A LA COMPETENCE DES JURIDICTIONS DU LIEU DU SIEGE SOCIAL DE STORMSHIELD, LE DROIT FRANÇAIS ETANT SEUL APPLICABLE.

Recommandations sur l'environnement d'utilisation

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).

Présentation

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

Sous l'impulsion des critères communs, Stormshield Network vous propose donc de prendre en compte les recommandations d'utilisation de la suite d'administration et du produit firewall énoncées ci-dessous. Ces recommandations 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.stormshield.eu/common-criteria.html

Veille sécurité

Consultez régulièrement les bulletins de sécurité des produits Stormshield publiés sur https://advisories.stormshield.eu.

Appliquez systématiquement une mise à jour de votre équipement si elle corrige une faille de sécurité. Ces mises à jour sont disponibles sur https://mystormshield.eu.

Mesures de sécurité physiques

Les boîtiers appliances firewall-VPN Stormshield Network doivent être 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.

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.stormshield.eu/

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

- Il est le seul à être habilité à se connecter via la console locale sur les boîtiers 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 des profils 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 l'Appliance ou sur d'autres équipements. Toutes les interventions sur les boîtiers appliances firewall-VPN se font sous sa responsabilité.

Environnement de sécurité TI (Technologies de l'Information)

Les boîtiers appliances firewall-VPN Stormshield Network doivent être 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 : https://www.stormshield.eu/about/recycling/

Certifications

CE

FC
Part 15 Subpart B

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 treize produits :

SN150, SN200, SN300, SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN3000, SN6000 et SNi40.

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 Security. 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 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

Chaque Firewall est livré dans un carton fermé sur lequel sont apposés un scellé (SN150, SN510, SN710, SN910, SN2000 et SN3000) ou deux scellés « STORMSHIELD 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.

Figure 1 : Scellé "Stormshield Quality seal"

Les étiquettes d'identification

Ces étiquettes affichent les informations relatives au Firewall (référence produit, part number, numéro de série, version logicielle installée, etc.). Vérifiez que ces informations correspondent à votre commande. Vous pouvez également vérifier si la version installée est certifiée.

Figure 2 : Étiquettes d'identification

Etiquettes sur le produit

Etiquette de garantie

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

Figure 3 : Étiquette de garantie du SN6000

Figure 4 : Étiquette de garantie 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, sur le côté pour le SNi40), 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, fournit des informations relatives au Firewall telles que le part number et les caractéristiques d'alimentation électrique du produit.

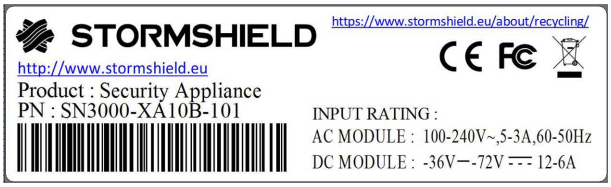


Figure 6: Etiquette produit

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 connecteur d'alimentation à vis six pôles (SNi40),
- Un câble croisé RJ45, catégorie 5e,
- Un câble série DB9F (SN200, SN300, SN500, SN700, SN900 et SNi40), ou un câble série RJ45 vers DB9F (SN510, SN710, SN910, SN2000 et SN3000) ou un câble USB de type « A » vers « B » (SN150).

Pour les modèles SN500, SN510, SN700, SN710, SN900 et SN910, l'emballage contient en plus :

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

Pour les modèles SN510, SN710, SN910, SN2000 et SN3000, les équerres sont montées.

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

Le modèle SNi40 est équipé d'une fixation pour rail DIN de 35mm de large (norme EN50022)

NOTE

Les Firewalls SN500, SN510, SN700, SN710, SN900 et SN910 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,
- Guide d'installation du jeu de glissières (SN2000, SN3000 et SN6000).

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.

Tous les modèles sauf SNi40

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

Avant tout raccordement

- Assurez-vous que votre produit Stormshield, le cordon ou l'adaptateur secteur ne sont pas endommagés.
- Assurez-vous que l'alimentation ou l'adaptateur secteur du produit est compatible avec la tension électrique de votre réseau d'alimentation secteur.
- Lorsqu'il est équipé d'une prise de terre, le cordon ou l'adaptateur secteur du produit doit être raccordé à 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.
- Afin de pouvoir déconnecter le produit, assurez-vous que la connexion au secteur est toujours aisément accessible.

Avant tout raccordement à une alimentation 48VDC (SN3000 et SN6000)

Considérations particulières pour la connexion d'un équipement à une source de tension continue :

- Veuillez respecter les instructions et avertissements contenus dans CEI, NEC, ANSI/NFPA 70 et CEC, Part I, C22.1, concernant le câblage et le raccordement de l'équipement à la source d'alimentation continue. L'équipement doit être installé par un électricien qualifié.
- Avant toute utilisation de l'équipement, assurez-vous que le chassis est relié de manière permanente et fiable à la terre de protection, à l'aide d'un câble jaune-vert de section utile minimum 1.5mm² (16 AWG).
- La connexion de l'équipement à la source d'alimentation doit comporter un dispositif de sectionnement homologué.
- L'équipement doit être connecté à la source d'alimentation à l'aide de câbles de section utile minimum 1.5mm² (16 AWG).

Garantie et règles de sécurité

Le Firewall Stormshield Network ne doit d'aucune manière être ouvert. Seule la société Stormshield, 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 destruction 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
RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT. METTRE LES BATTERIES AU REBUT CONFORMÉMENT AUX INSTRUCTIONS.

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, SN510, SN700, SN710, SN900 et SN910. 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.

Précautions

- **Kit d'installation :** Seul le kit d'installation fourni avec le produit doit être utilisé pour l'installation en baie.
- **Température ambiante de fonctionnement élevée :** en cas d'installation dans une baie fermée ou contenant plusieurs équipements, la température ambiante de fonctionnement à l'intérieur de la baie peut être supérieure à celle de la pièce. En conséquence, l'équipement doit être installé dans un environnement compatible avec la température ambiante maximale spécifiée par le fabricant.

- **Débit d'air réduit :** l'installation de l'équipement en baie doit permettre une ventilation suffisante pour garantir un fonctionnement en toute sécurité de l'équipement.
- **Charge mécanique :** le montage de l'équipement en baie doit être réalisé de manière à éviter tout danger résultant d'une charge mécanique mal répartie.
- **Surcharge des circuits :** il convient de prendre les précautions nécessaires pour la connexion de l'équipement au circuit d'alimentation et de réfléchir aux conséquences d'une éventuelle surcharge des circuits sur la protection contre les surintensités et sur le câblage d'alimentation. Notamment, les valeurs nominales de la plaque signalétique de l'équipement doivent être prises en compte.
- **Mise à la terre fiable :** une mise à la terre fiable des équipements montés en baie doit être assurée. Une attention toute particulière est requise pour les raccordements d'alimentation autres que ceux effectués directement sur le circuit principal (par exemple, en cas d'utilisation de blocs multiprises).
- **Courant de fuite :** une attention toute particulière est requise concernant la somme des courants de fuite en cas d'installation de l'équipement dans une baie fermée ou contenant plusieurs équipements.

Modèle SNi40

Avant tout raccordement

- Assurez-vous que votre produit Stormshield et ses accessoires ne sont pas endommagés.
- Assurez-vous que les caractéristiques électriques d'alimentation de votre produit, indiquées sur l'étiquette produit, sont compatibles avec celles de votre réseau d'alimentation.
- Le châssis de votre produit doit être raccordé à une terre de protection, à l'aide d'un conducteur de section utile minimum 1mm² (16 AWG). Assurez-vous que la connexion est permanente et fiable, et que le circuit de mise à la terre de protection de votre installation est conforme aux normes en vigueur.
- Avant toute opération de montage ou démontage de votre produit, assurez-vous que le produit est hors tension, connexion d'alimentation débranchée.
- Veuillez respecter les instructions et avertissements contenus dans les normes en vigueur (CEI, NEC, ANSI/NFPA 70 et CEC, Part I, C22.1), concernant le câblage et le raccordement de l'équipement à la source d'alimentation continue. L'équipement doit être installé par un électricien qualifié.
- La connexion de l'équipement à la source d'alimentation doit comporter un dispositif de sectionnement homologué et aisément accessible.
- L'équipement doit être connecté à la source d'alimentation à l'aide de câbles de section utile minimum 1mm² (16 AWG).

Garantie et règles de sécurité

Le Firewall Stormshield Network ne doit d'aucune manière être ouvert. Seule la société Stormshield, 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
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
RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT. METTRE LES BATTERIES AU REBUT CONFORMÉMENT AUX INSTRUCTIONS.

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.

Précautions pour le montage en armoire

- **Kit d'installation :** Seul le kit d'installation fourni avec le produit doit être utilisé pour l'installation.
- **Température ambiante de fonctionnement élevée :** en cas d'installation dans une armoire fermée ou contenant plusieurs équipements, la température ambiante de fonctionnement à l'intérieur de l'armoire peut être supérieure à celle de la pièce. En conséquence, l'équipement doit être installé dans un environnement compatible avec la température ambiante maximale spécifiée par le fabricant.
- **Débit d'air réduit :** l'installation de l'équipement en armoire doit permettre une ventilation suffisante pour garantir un fonctionnement en toute sécurité de l'équipement.
- **Charge mécanique :** le montage de l'équipement en armoire doit être réalisé de manière à éviter tout danger résultant d'une charge mécanique mal répartie.
- **Surcharge des circuits :** il convient de prendre les précautions nécessaires pour la connexion de l'équipement au circuit d'alimentation et de réfléchir aux conséquences d'une éventuelle surcharge des circuits sur la protection contre les surintensités et sur le câblage d'alimentation. Notamment, les valeurs nominales de la plaque signalétique de l'équipement doivent être prises en compte.
- **Mise à la terre fiable :** une mise à la terre fiable des équipements montés en armoire doit être assurée. Une attention toute particulière est requise pour les raccordements d'alimentation autres que ceux effectués directement sur le circuit principal (par exemple, en cas d'utilisation de blocs de dérivation).

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 (tous les modèles sauf SNi40)

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, SN510, SN700, SN710, SN900 et SN910 ; 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.

IMPORTANT
Lorsque le Firewall est stocké, il doit être mis sous tension pendant une période de 24 heures au moins une fois tous les 2 ans pour permettre de reformer les condensateurs électrolytiques internes. Tout manquement compromettra sa fiabilité.

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, SN510, SN700, SN710, SN900, SN910, 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% à 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% à 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 Firewalls Stormshield Network ont été testés et respectent les limites définies pour les appareils numériques de Classe A, en accord avec la section 15 de la réglementation de la FCC. Ces limites ont pour but de fournir une protection raisonnable contre les interférences nuisibles susceptibles de se produire lorsqu'un équipement est utilisé en environnement commercial. Les Firewalls Stormshield Network génèrent, utilisent et peuvent émettre des ondes radioélectriques qui peuvent, s'ils ne sont pas installés et utilisés conformément aux instructions du manuel, provoquer des interférences nuisibles aux communications radio. L'utilisation de votre équipement en zone résidentielle est susceptible de causer des interférences nuisibles. Dans ce cas, l'utilisateur devra résoudre ces problèmes à ses frais.

Les Firewalls Stormshield Network sont conformes aux exigences de la norme européenne EN55032, classe A. 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.

Conditions d'utilisation (modèle SNi40)

Le Firewall SNi40 est prévu pour fonctionner en permanence, dans un local technique.

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 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 Stormshield est destiné à un usage interne, en milieu industriel (voir spécifications du produit), 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 à l'abri des poussières, où la température est conforme aux spécifications du produit. La température ambiante idéale se situe aux alentours de 25°C. Le tableau ci-dessous indique la température de fonctionnement, la température de stockage et l'humidité.

Température de fonctionnement	Humidité relative en fonctionnement (%)	Température de stockage	Humidité relative de stockage (%)
-40° à 75°C (-40° à 167°F)	0% à 90% sans condensation	-40° à 85°C (-40° à 185°F)	5% à 95% sans condensation

IMPORTANT
Évitez notamment l'exposition directe au rayonnement solaire. Maintenez toujours un espace libre suffisant autour du produit, et une circulation optimale de l'air afin d'éviter tout risque de surchauffe.

IMPORTANT
Ne posez aucun objet sur votre produit Stormshield Network.

IMPORTANT

Les Firewalls Stormshield Network ont été testés et respectent les limites définies pour les appareils numériques de Classe A, en accord avec la section 15 de la réglementation de la FCC. Ces limites ont pour but de fournir une protection raisonnable contre les interférences nuisibles susceptibles de se produire lorsqu'un équipement est utilisé en environnement commercial. Les Firewalls Stormshield Network génèrent, utilisent et peuvent émettre des ondes radioélectriques qui peuvent, s'ils ne sont pas installés et utilisés conformément aux instructions du manuel, provoquer des interférences nuisibles aux communications radio. L'utilisation de votre équipement en zone résidentielle est susceptible de causer des interférences nuisibles. Dans ce cas, l'utilisateur devra résoudre ces problèmes à ses frais.

Les Firewalls Stormshield Network sont conformes aux exigences de la norme européenne EN55032, classe A. 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.

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). Les modèles SN3000 et SN6000 étant équipés d'alimentations redondantes, il est recommandé de les brancher sur 2 sources secteur différentes.

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

NOTE
Pour les modèles SN3000 et SN6000, des modules d'alimentation 48V DC peuvent être livrés séparément sur commande.

Pour les modèles SN150, SN200 et SN300, branchez la fiche de l'adaptateur secteur à l'arrière du Firewall. Puis reliez l'adaptateur à une prise secteur adéquate à l'aide du cordon secteur fourni.

Pour les modèles SN500, SN510, SN700, SN710, SN900, SN910 et SN2000, insérez la prise femelle du cordon secteur fourni dans l'embase 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 secteur fournis dans les deux embases secteur mâles situées sur la face arrière du Firewall. Puis, enfichez la partie mâle des deux cordons secteur fournis dans deux prises secteur adéquates.

Raccordement à une alimentation 24VDC (SNi40)

Les tensions supportées sont de 12VDC à 36VDC.

RAPPEL
L'équipement doit être installé par un électricien qualifié.

NOTE
Il est fortement recommandé de raccorder votre Firewall à un équipement de type « UPS » (onduleur). Le modèle SNi40 est équipé d'une alimentation redondante, il est recommandé de le raccorder à 2 sources indépendantes d'alimentation.

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

NOTE
Un adaptateur secteur peut être livré séparément sur commande.

Raccordement au réseau

Tous les modèles sont équipés par défaut de ports Ethernet RJ45 Gigabit.

Les modèles SN900, SN910 et SNi40 proposent en outre, par défaut, deux cages SFP permettant d'insérer des transceivers de type **SFP,** fournis en option.

Les modèles SN710, SN910, SN2000, SN3000 et SN6000 proposent en outre, un ou plusieurs emplacements pour différents types de modules d'extension, permettant l'ajout de ports Ethernet : cuivre RJ45, ou cage pour transceivers fibre de type SFP, ou cage pour transceivers fibre de type SFP+, selon la référence de module commandée. Un emplacement est disponible sur les modèles SN710 et SN910, deux sur les SN2000 et SN3000, et sept sur le SN6000.

IMPORTANT
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 aux chapitres Modules d'extension (SN710, SN910, SN2000, SN3000, SN6000) et Connectiques Ethernet Fibre.

INSTALLATION EN BAIE 19" ET ARMOIRE

Tous les produits Stormshield Network peuvent être installés dans des baies 19 pouces (sauf SNi40). 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.

Les produits SN500, SN700 et SN900 sont livrés avec un kit d'installation contenant des équerres. Les modèles SN510, SN710, SN910, SN2000 et SN3000, disposent d'équerres montées par défaut. Les produits SN2000, SN3000 et SN6000 sont livrés avec un jeu de glissières.

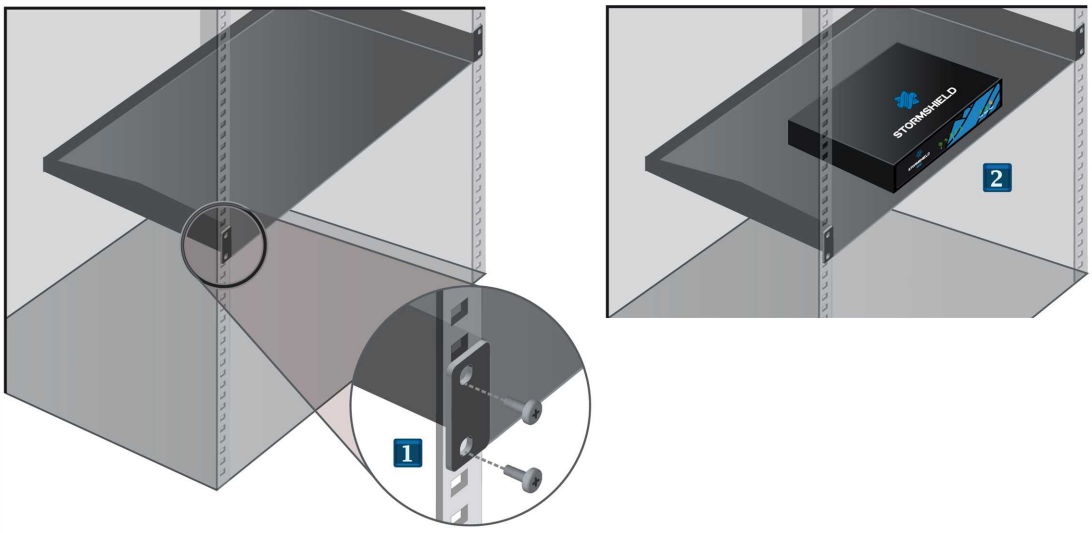
RAPPEL
Assurez-vous que la baie respecte les conditions de température et d'hygrométrie préconisées dans la partie Conditions d'utilisation.

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

Installation en baie 19" 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. Fixez au moyen de vis et d'écrous-cages (non fournis), le plateau sur les montants latéraux situés à l'avant de la baie.
2. Une fois le plateau installé, vous pouvez y déposer un ou deux produits (aucune fixation supplémentaire n'est nécessaire).



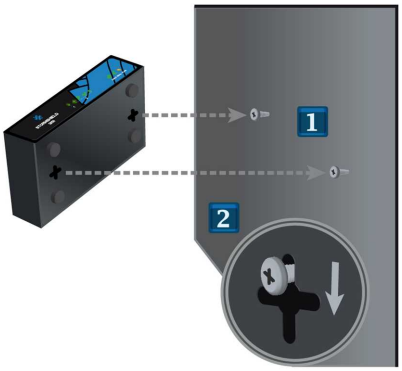
AVERTISSEMENT
Si vous installez deux produits sur un même plateau, il est nécessaire de prévoir suffisamment d'espace entre les deux Firewalls pour ne pas entraver le flux d'air circulant par les côtés.

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 le diamètre de la tige doit être inférieur à 4mm.

Procédez comme suit :

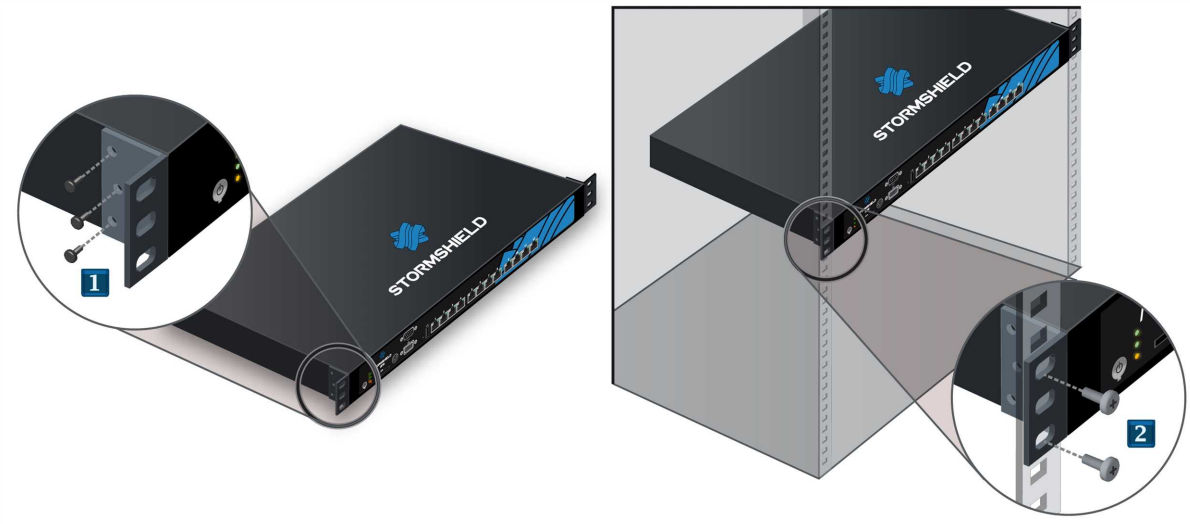
1. Fixez au mur les 2 vis alignées horizontalement en respectant un écart de 12cm (de centre à centre) et en les laissant dépasser légèrement pour tenir compte de l'épaisseur des pieds antidérapants.
2. Une fois les vis fixées, vous pouvez insérer la tête des vis à l'intérieur des encoches prévues à cet effet, puis glissez légèrement le produit vers le bas afin d'y insérer les vis.



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

L'espace minimum pour l'installation du Firewall SN doit être de 1U. Procédez comme suit :

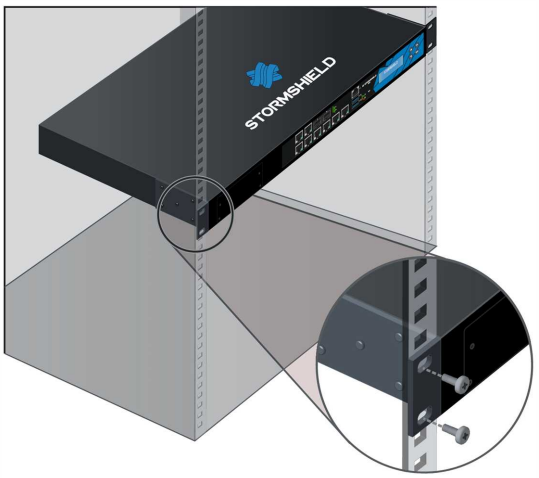
1. Vissez les équerres sur les bords latéraux du Firewall au moyen des vis fournies.
2. Une fois les équerres installées, vous pouvez fixer l'ensemble aux montants situés à l'avant de votre baie de rackage au moyen de vis et d'écrous-cages (non fournis).



Installation en baie 19" des modèles SN510, SN710 et SN910

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

Vous pouvez fixer l'ensemble aux montants situés à l'avant de votre baie de rackage au moyen de vis et d'écrous-cages (non fournis).



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

L'espace minimum pour l'installation du Firewall SN doit être de 1U pour les modèles SN2000, SN3000 et de 2U pour le modèle SN6000. Les procédures de montage des rails latéraux et d'installation en baie sont décrites dans les documents **SN2000-SN3000_rack mounting** et SN6000_rack mounting. Ces documents sont livrés avec les produits SN2000/3000 et SN6000 et disponibles dans la rubrique ***Base Documentaire*** de votre Espace sécurisé (*Product > Stormshield Network Firewall > User Guide > Hardware*).

Installation sur rail DIN du modèle SNi40

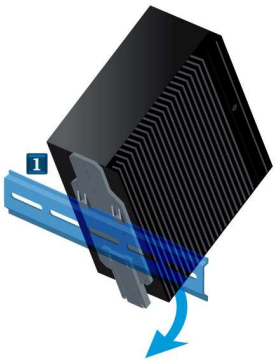
Pour l'installation en armoire, le modèle SNi40 dispose d'un kit de fixation sur rail DIN de 35mm de large (standard EN 50022).

RAPPEL

Assurez-vous que l'armoire respecte les conditions de température et d'hygrométrie préconisées dans la partie Conditions d'utilisation. L'équipement doit être installé par un électricien qualifié.

NOTE

Le modèle SNi40 doit être fixé verticalement.



Procédez comme suit :

1. Présentez le SNi40 face au rail DIN, puis insérez la partie supérieure du rail dans l'encoche du kit de fixation, prévue à cet effet. Puis, redressez le SNi40.
2. Poussez le produit contre le rail DIN jusqu'à entendre le clic de verrouillage. Vérifiez le verrouillage.

PRESENTATION DE LA GAMME SN

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

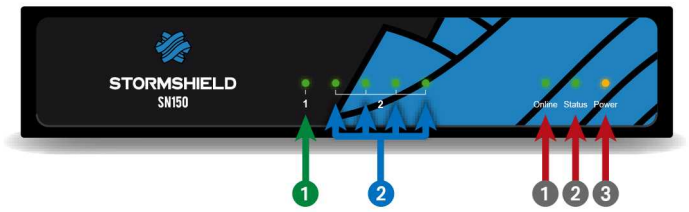
NOTE
Pour plus d'informations sur les interfaces Ethernet, reportez-vous à la partie Raccordement au réseau du chapitre PRECAUTIONS D'INSTALLATION.

Modèle SN150

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

Face avant : voyants

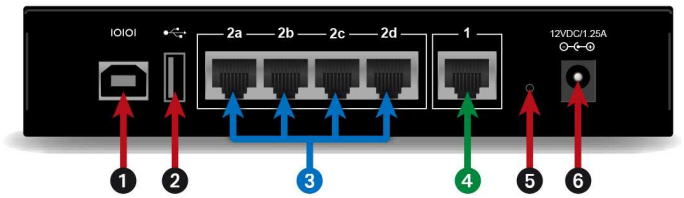
Ce modèle présente en façade les voyants décrits ci-dessous :



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

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

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 :

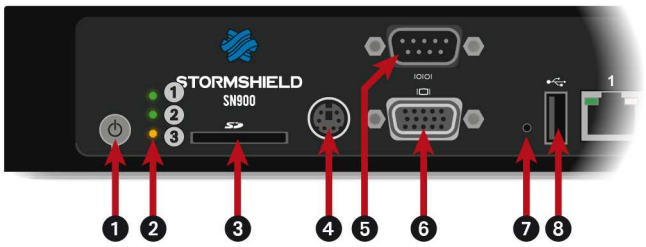
3. La première zone est par défaut identifiée en mode **INTERNE 2 (IN).** Elle est constituée de 4 ports commutés (switch).
4. La deuxième zone est l'interface **EXTERNE 1 (OUT),** par défaut en mode externe. Elle constitue la zone destinée au raccordement à Internet.
5. Le bouton est celui de **mise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

Modèles SN200, SN300, SN500, SN700 et SN900

Face avant : connectique et voyants

L'essentiel de la connectique de ces modèles se situe en façade.



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

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).
3. Cet emplacement est celui de la **carte SD*.**
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 homologué.

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

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 :

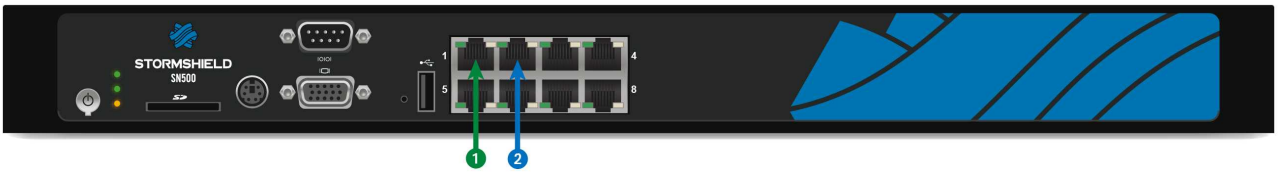
- La première zone est par défaut en mode externe (OUT). Elle constitue la zone destinée au raccordement à Internet,
- La deuxième zone est par défaut identifiée en mode interne (IN). Elle est constituée de 2 ports commutés (switch),
- La troisième zone vous permet de définir un troisième secteur de 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) à un mètre.
Le produit est fourni avec un adaptateur secteur externe.
Le modèle SN300 offre 8 interfaces Ethernet Gigabit.

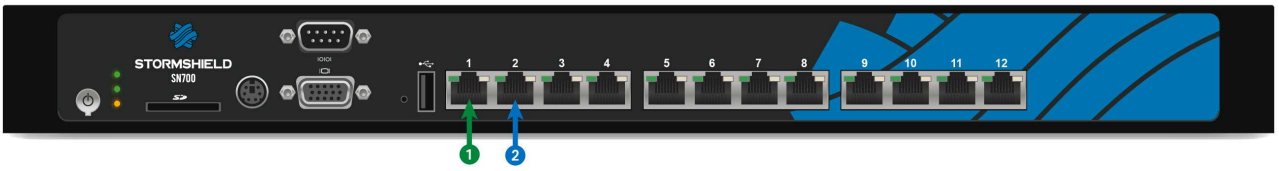
Modèle SN500



Ce produit dispose d'une alimentation interne.
Le modèle SN500 offre 8 interfaces Ethernet Gigabit.

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

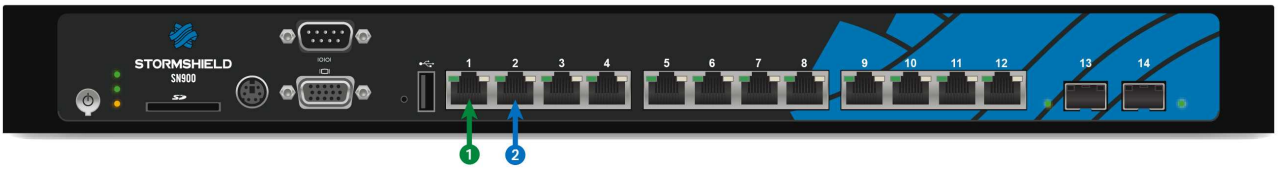
Modèle SN700



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.

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

Modèle SN900



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

Ce produit dispose d'une alimentation interne.

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

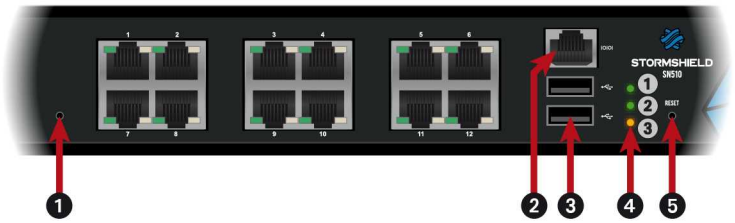
Le modèle SN900 offre 12 interfaces Ethernet Gigabit et 2 cages SFP pour l'ajout de transceivers Ethernet Gigabit. Les spécifications des transceivers homologués Stormshield Network sont détaillées dans le chapitre Connectiques Ethernet Fibre.

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 SN510 et SN710

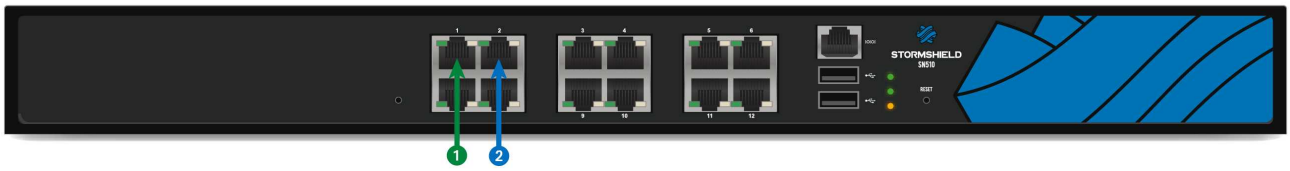
Face avant : connectique et voyants



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

1. Le bouton est celui de **mise en configuration usine** (*defaultconfig*).
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 ces modèles est de 115200 bauds (8N1).
3. **Deux 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 ou un modem USB homologué.
4. Les voyants *Power*, *Status* et *Online* (de bas en haut).
5. **Le Bouton *Reset* :** reset électrique.

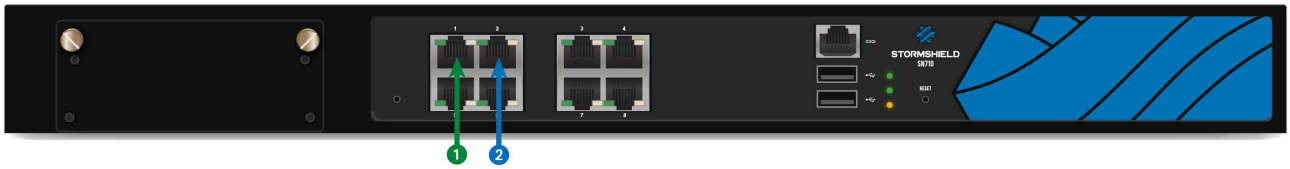
Modèle SN510



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 SN510 offre 12 interfaces Ethernet Gigabit.

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

Modèle SN710



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

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

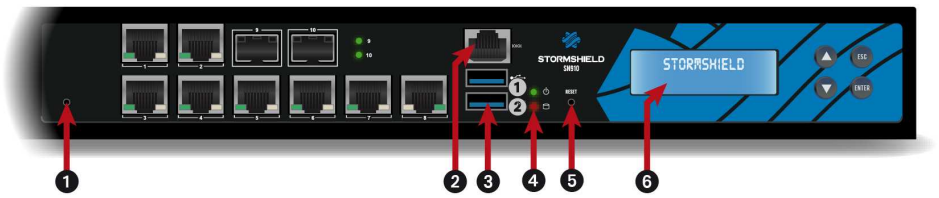
Ce produit dispose d'une alimentation interne.
Le modèle SN710 offre 8 interfaces Ethernet Gigabit. Il permet également d'accueillir un module d'extension avec connectiques RJ45 (Gigabit) ou Fibre (Gigabit ou 10 Gigabit).
Les spécifications des modules d'extension et transceivers homologués Stormshield Network sont détaillées dans les chapitres Modules d'extension (SN710, SN910, SN2000, SN3000, SN6000) et Connectiques Ethernet Fibre.

Face arrière : connectique

Le branchement du cordon de l'alimentation s'effectue en face arrière du produit. Un interrupteur permet la mise sous/hors tension du produit.

Modèle SN910

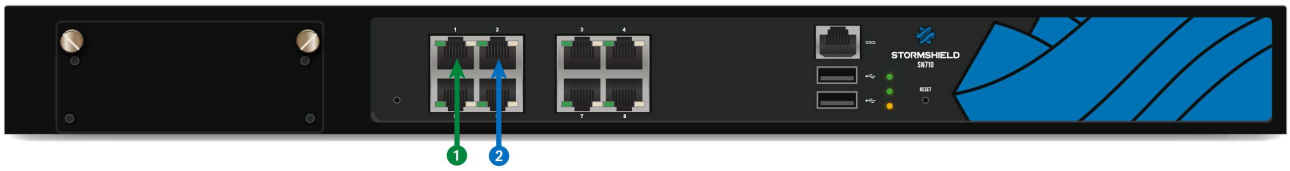
Face avant : connectique et voyants



1 Voyant *Online* (vert)
2 Voyant *Activité SSD* (rouge)

1. Le bouton est celui de **mise en configuration usine** (*defaultconfig*).
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 ces modèles est de 9600 bauds (8N1).
3. **Deux 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 homologué.
4. Les voyants *Power* et *Activité SSD* (de haut en bas).
5. **Le Bouton *Reset* :** reset électrique.
6. **L'écran LCD :** il indique la version du firmware installée, la partition active, le numéro de série du produit ainsi que l'état de la HA si celle-ci est activée.

Description



Ce modèle est équipé d'un processeur multi-core, permettant de démultiplier la puissance de traitement.
Ce produit dispose d'une alimentation interne.

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

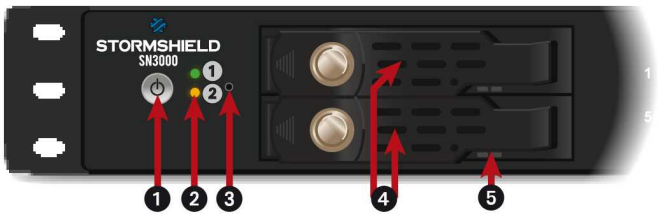
Le modèle SN910 offre 8 interfaces Ethernet Gigabit et 2 cages SFP pour l'ajout de transceivers Ethernet Gigabit. Il permet également d'accueillir un module d'extension avec connectiques RJ45 (Gigabit) ou Fibre (Gigabit ou 10 Gigabit).
Les spécifications des modules d'extension et transceivers homologués Stormshield Network sont détaillées dans les chapitres Modules d'extension (SN710, SN910, SN2000, SN3000, SN6000) et Connectiques Ethernet Fibre.

Face arrière : connectique

1. L'embase secteur
2. L'interrupteur de mise sous/hors tension du produit.
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 homologué.
4. **Le port VGA** permet le branchement d'un écran.

Modèles SN2000 et SN3000

Face avant : connectique et voyants



1. Voyant *Online* (vert)
3. 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).

Modèle SN2000

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.

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

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 les chapitres Modules d'extension (SN710, SN910, SN2000, SN3000, SN6000) et Connectiques Ethernet Fibre.

Modèle SN3000

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.

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

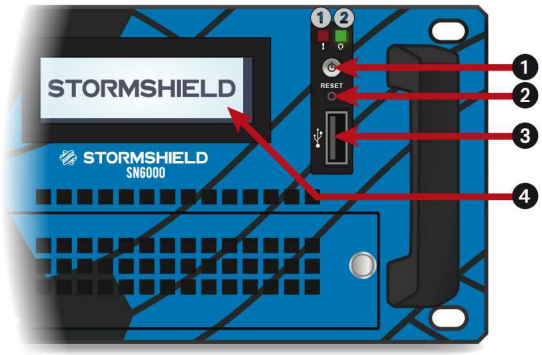
Le modèle SN3000 offre 10 interfaces Ethernet Gigabit et permet d'accueillir 2 modules d'extension avec connectiques RJ45 (Gigabit) ou Fibre (Gigabit ou 10 Gigabit).
Les spécifications des modules d'extension et transceivers homologués Stormshield Network sont détaillées dans les chapitres Modules d'extension (SN710, SN910, SN2000, SN3000, SN6000) et Connectiques Ethernet Fibre.

Face arrière : connectique

1. Deux ports dédiés au management du produit ou à 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 ces modèles 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 homologué.
4. **Le port VGA** permet le branchement d'un écran.
5. **Le port mini-din PS2** permet le branchement d'un clavier.
6. L'interrupteur de mise sous/hors tension du produit (SN2000 seulement).
7. Une embase secteur (SN2000) ou deux embases secteur (SN3000) pour la redondance d'alimentation.

Modèle SN6000

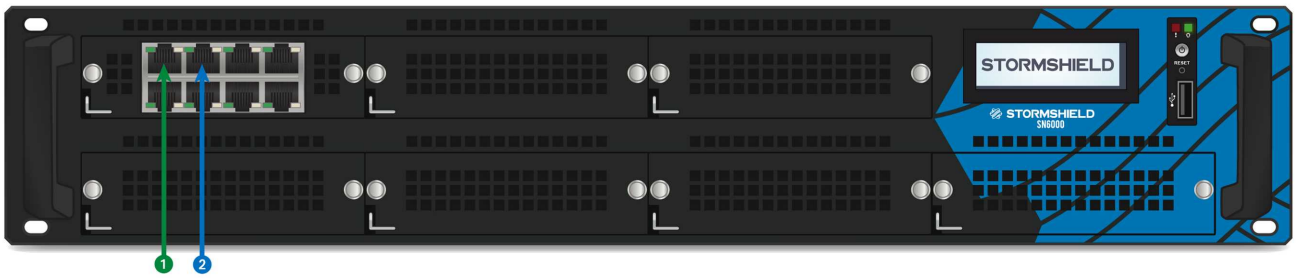
Face avant : connectique et voyants



1. **Voyant d'*alerte matérielle* (rouge) :** indicateur de surchauffe ou de défaillance matérielle (ex. : 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 homologué.
4. **L'écran LCD** indique la version du firmware installée, la partition active, le numéro de série du produit, l'adresse IP de l'interface IPMI, ainsi que l'état de la HA (si activée), du RAID et des modules d'alimentation.

Description



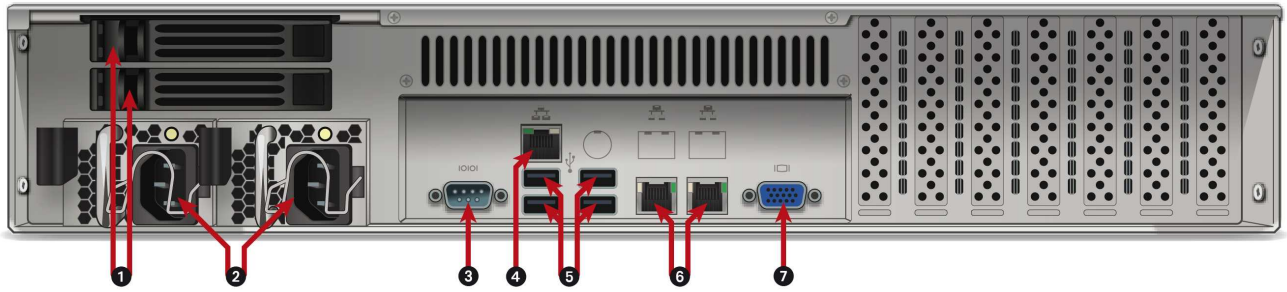
Ce modèle est équipé de deux processeurs multi-core, permettant de démultiplier la puissance de traitement. Ce produit dispose d'une alimentation interne redondante. De base, deux SSD amovibles sont installés en RAID.

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

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 les chapitres Modules d'extension (SN710, SN910, SN2000, SN3000, SN6000) et Connectiques Ethernet Fibre.

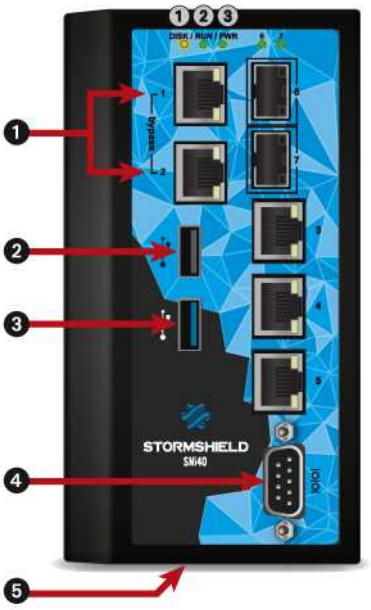
Face arrière : connectique



1. **Racks des SSD pour stockage des traces** (2 en RAID1). 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 produit via IPMI. Consultez l'annexe pour la CONFIGURATION ET ADMINISTRATION VIA IPMI (SN6000).
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 homologué.
6. Deux ports réseaux dédiés au management du produit ou à la configuration en HA (de gauche à droite : MGMT1 et MGMT2).
7. **Le port VGA** permet le branchement d'un écran.

Modèle SNi40

Connectique et voyants



1. Voyant *Activité SSD* (jaune)
2. Voyant *Run* (vert)
3. Voyant *Power* (vert)

1. **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.
2. **Le port USB 3.0** 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.
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 115200 bauds (8N1).
4. **Le Bouton *Reset*** (sous le boîtier): reset électrique.

Description

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

Le Firewall multifonctions SNi40 fonctionne sans ventilateur.

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

Ce produit est équipé d'une alimentation redondante 24VDC, le connecteur à vis six pôles fourni permet la connexion à 2 sources indépendantes d'alimentation.

Le modèle SNi40 offre 5 interfaces Ethernet Gigabit et 2 cages SFP pour l'ajout de transceivers Ethernet Gigabit.

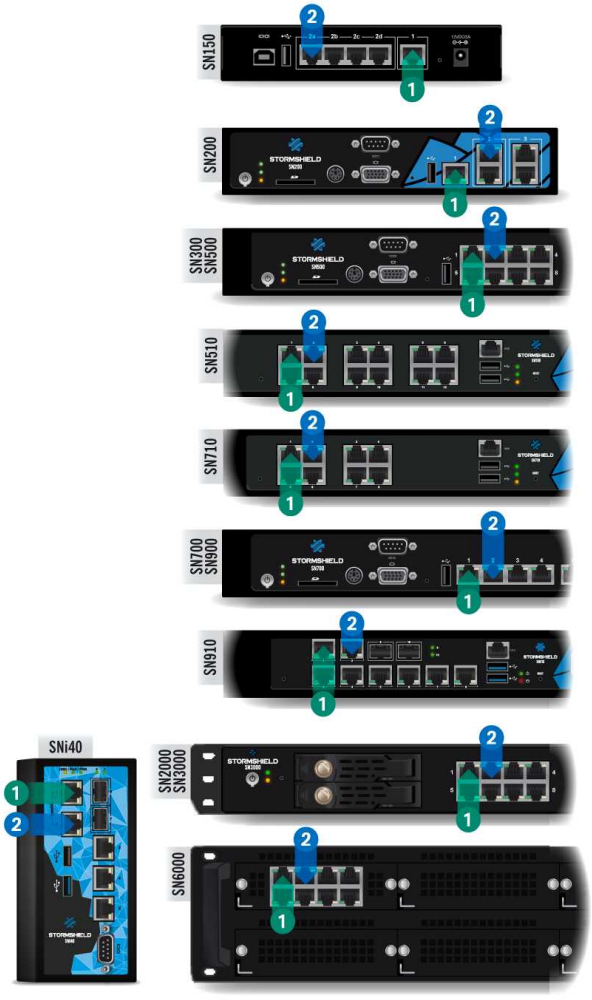
Les spécifications des transceivers homologués Stormshield Network sont détaillées dans les chapitres Transceivers optionnels Ethernet Fibre Optique et Connectiques Ethernet Fibre.

CONNECTIQUES RÉSEAU

Connectiques 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.



Connectiques

Les ports Ethernet (Gigabit) des modèles Stormshield Network de la gamme SN sont configurés en mode auto-sense, ils s'adaptent donc à la configuration du port Ethernet de l'équipement auquel ils sont raccordés. Ces ports sont compatibles avec les câbles Ethernet RJ45 de type droit ou croisé.
Les modèles SN710, SN910, SN2000, SN3000 et SN6000 permettent l'ajout de ports Ethernet RJ45 via l'insertion de modules d'extension.

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.
L'accès à cette interface est par défaut bloqué, vous ne pouvez donc pas accéder à l'interface de configuration depuis ce port.
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 l'état de 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, SN510, SN700, SN710, SN900, SN910, SN2000 et SN3000

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.

Modèle SNi40

Intitulé	Couleur	Etat	Indication
Led du haut ACT/LINK	Jaune	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 du bas 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 par défaut sur les modèles suivants :

- SN900 : ports n°13 et 14,
- SN910 : ports n°9 et 10,
- SNi40 : ports n°6 et 7.

Les modèles SN710, SN910, SN2000, SN3000 et SN6000 permettent l'ajout de connectiques Ethernet Fibre via l'insertion de modules d'extension.

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

Voyants

Les voyants donnent les indications suivantes :

- Modèles SN900, SN910 et SNi40 équipés de transceivers de type SFP (dans les ports Ethernet fibre disponibles par défaut) : une LED de couleur verte est allumée quand le lien est établi et clignote selon le volume de trafic.
- Modèles SN710, SN910, SN2000 et SN3000 équipés de modules d'extension 1Gbps avec 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'extension 1Gbps avec 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	Vert / Clignote	Lien établi entre le port Ethernet et l'équipement connecté. La vitesse de clignotement varie selon le volume de trafic.

- Modèles SN710, SN910, SN2000, SN3000 et SN6000 équipés de modules d'extensions 10Gbps avec transceivers de type SFP+ :

Intitulé	Couleur / Etat	Indication
Led de droite SPEED	Bleu	Vitesse de média négociée à 10 Gbps.
	Jaune	Vitesse de média négociée à 1 Gbps.
Led de gauche ACT/LINK	Vert / Clignote	Lien établi entre le port Ethernet et l'équipement connecté. La vitesse de clignotement varie selon le volume de trafic.

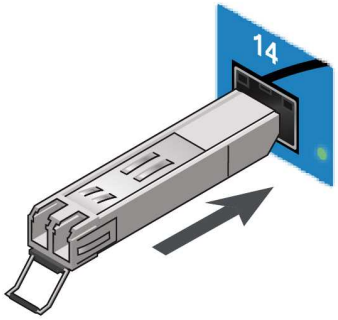
Transceivers optionnels Ethernet Fibre Optique (SN710, SN900, SN910, SN2000, SN3000, SN6000 et SNi40)

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

- Les modèles SN900, SN910 et SNi40 proposent par défaut, deux cages pour transceivers **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

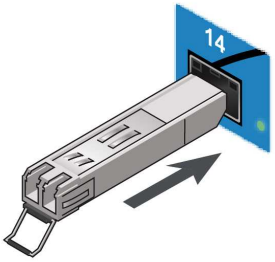
		SN900 et SNi40	SN710, SN910, SN2000, SN3000 et SN6000
CONNECTIQUE FIBRE			
GIGA - SFP	Transceiver SFP, 1000Base-SX : Nécessite une fibre multimode . Distance maximum typique supportée (sous condition de qualité optimale) : 550m	supporté	supporté
	Transceiver SFP, 1000Base-LX : Ethernet 1000Base-LX, nécessite 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 : 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
	Transceiver SFP+, 10GBASE-LR/1000Base-LX : Ethernet 10GBASE-LR /1000Base-LX, nécessite une fibre monomode. Distance maximum typique supportée (sous condition de qualité optimale) : 10 km	non supporté	supporté

Installation

Pour installer votre transceiver, procédez comme suit :

1. Retirez le cache éventuel de la cage dans laquelle vous voulez insérer le transceiver.
2. Insérez le transceiver, puis raccordez le câble optique correspondant à ce transceiver.

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.

Modules d'extension (SN710, SN910, SN2000, SN3000, SN6000)

La procédure d'extraction ou d'insertion d'un module d'extension pour Firewall SN710, SN910, SN2000, SN3000 ou SN6000 se déroule en trois étapes principales :

1. **Etape 1** Arrêt du Firewall.
2. **Etape 2** Extraction ou insertion du module.
3. **Etape 3** Redémarrage du Firewall

NOTE
Les modules d'extension pour SN710, SN910, 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 SN710, SN910, SN2000, SN3000 et SN6000

Les produits SN710, SN910, 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 8 ports Fibre 1GbE**
  8 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).

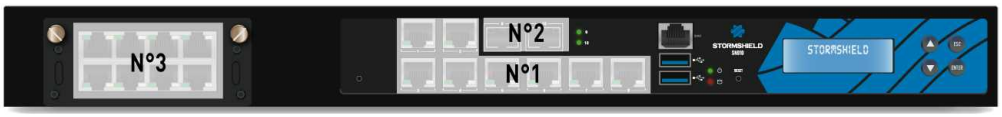
- **Module 2 ports Fibre 10GbE (non disponible pour SN6000)**
  2 cages SFP+, supportant au choix les transceivers suivants :
  - Transceiver Fibre SFP+, 10GBase-SR (10Gbps Ethernet, courte distance) / 1000BASE-SX (1Gbps Ethernet, courte distance).
  - Transceiver Fibre SFP+, 10GBase-LR (10Gbps Ethernet, longue distance) / 1000BASE-LX (1Gbps Ethernet, longue distance).
- **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 interfaces seront réordonnées selon l'ordre présenté ci-dessous.

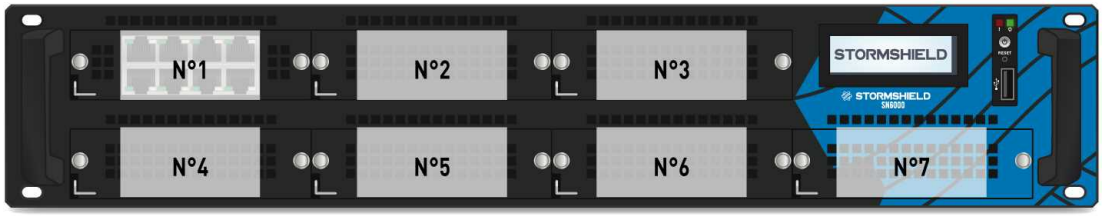
Modèle SN710 :

Modèle SN910 :



Modèles SN2000 et SN3000 :

Modèle SN6000 :



Procédures d'extraction ou d'insertion de modules d'extension

L'ajout de modules d'extension ne requiert pas de licence spécifique.

IMPORTANT
L'extraction et l'insertion d'un module d'extension doivent s'effectuer sur le produit mis à l'arrêt, et impérativement déconnecté de toute alimentation électrique.

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 d'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 d'une même rangée. Cela permet d'équilibrer la charge de traitement entre les deux 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 2nd processeur.

RAPPEL
Dans le cas d'ajout a posteriori de modules dans la rangée 1, les interfaces des modules de la rangée 2 seront automatiquement réordonnées.

Insertion d'un module d'extension pour SN710, SN910, SN2000 ou SN3000

- A l'aide du bouton d'Alimentation en face avant, ou depuis l'interface d'administration, lancer l'arrêt du Firewall,
- Après l'extinction, le déconnecter impérativement de toute alimentation électrique,
- Pour ôter la face de bouchage, dévisser les 2 vis moletées et l'extraire en tirant sur les 2 vis,
- Présenter le module à insérer, l'engager à fond (appuyer plus fortement en fin de parcours), puis visser les 2 vis moletées,
- Reconnecter le Firewall à l'alimentation électrique,
- A l'aide du bouton d'Alimentation en face avant, démarrer le Firewall.

Extraction d'un module d'extension pour SN710, SN910, SN2000 ou SN3000

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

Insertion d'un module d'extension pour SN6000

- A l'aide du bouton d'Alimentation en face avant, ou depuis l'interface d'administration, lancer l'arrêt du Firewall,
- Après l'extinction, le déconnecter impérativement de toute alimentation électrique,

- Déverrouiller et extraire le module vide en place en levant le petit levier en bas à gauche, tout en tirant sur les 2 poignées d'extraction,
- 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 d'Alimentation en face avant, démarrer le Firewall.

Extraction d'un module d'extension pour SN6000

- A l'aide du bouton d'Alimentation en face avant, ou depuis l'interface d'administration, 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 poignées d'extraction,
- Replacer le module vide 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 d'Alimentation en face avant, démarrer le Firewall.

PREMIERE CONNEXION AU 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 PRESENTATION DE LA GAMME SN.

Pré-requis

Configuration minimale pour administrer un Firewall Stormshield Network

Version minimale du système d'exploitation (firmware)

Pour les modèles suivants, les versions minimales du firmware sont les suivantes :

- **SN150, SN200, SN300, SN500, SN700, SN900, SN2000 et SN3000 :** V1.1.0
- **SN510 et SN710 :** V1.4.1 en version 1 et V2.2.0 en version 2
- **SN910 :** V1.2.3
- **SN6000 :** V1.1.1
- **SNi40 :** V2.3.4

Interface d'administration Web

L'interface de configuration des Firewalls 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 à partir des environnements suivants :

- Microsoft Windows 7 et 8,
- Microsoft Windows Server 2008 et 2012.

Préparation de l'accès Internet

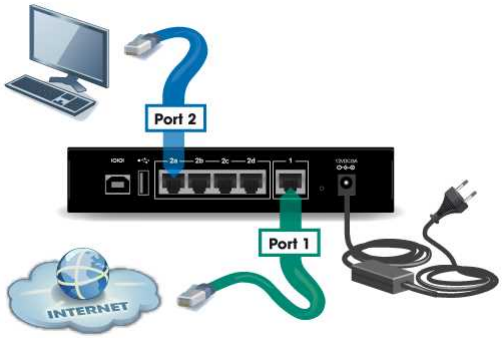
Avant l'installation du Firewall SN, assurez-vous que les équipements d'accès à Internet (si le Firewall doit être connecté à Internet) ont été convenablement installés et configurés.

Branchement

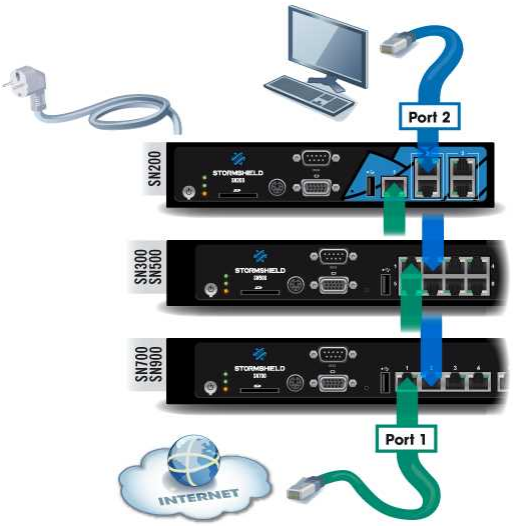
Branchez votre Firewall SN sur le secteur, puis connectez les ports réseaux comme suit :

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

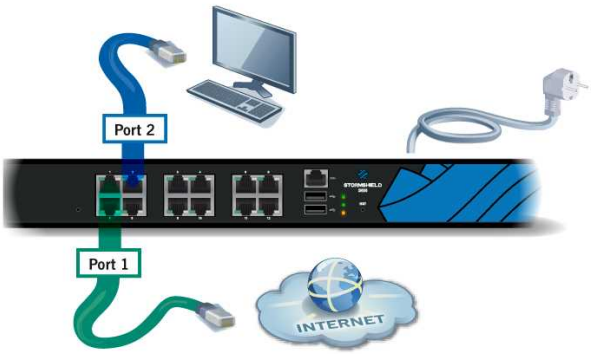
Le poste client peut être soit directement relié à l'interface interne du Firewall, soit connecté au réseau local, lui-même relié à l'interface interne du Firewall. Pour une connexion directe du poste sur le Firewall, utilisez le câble Ethernet croisé, livré avec le produit.



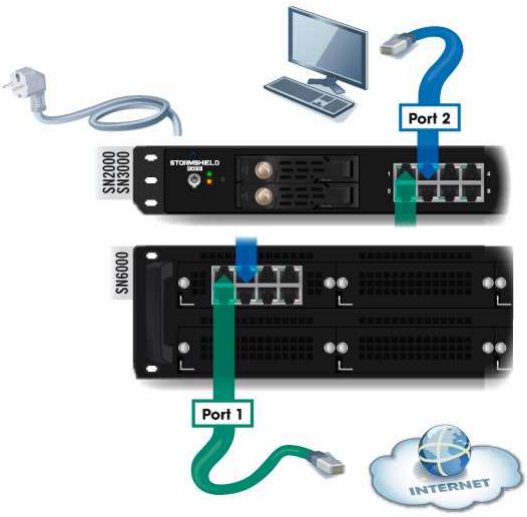
Modèle SN150



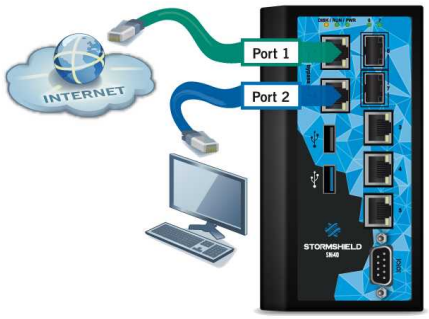
Modèles SN200, SN300, SN500, SN700 et SN900



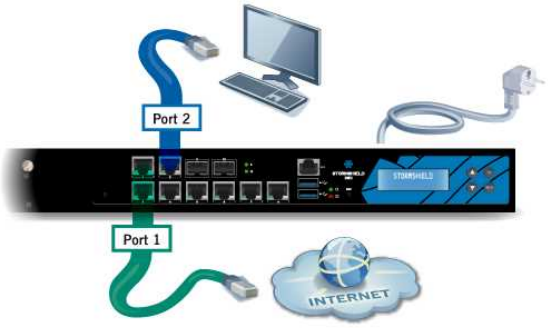
Modèles SN510 et SN710



Modèles SN2000, SN3000 et SN6000



Modèle SNi40



Modèle SN910

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

ATTENTION
Il est **impératif** de ne pas débrancher le produit en **phase de démarrage, d'arrêt ou de mise à jour.**

Sauf pour les SN910 et 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, et SN510 et SN710
- Voyants *Power* 3 pour les SN2000, SN3000 et SNi40

Pour les modèles SN150, SN200, SN300, SN500, SN510, SN700, SN710 et SN900, 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.

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.*

Pour le SN2000 et SN3000, la phase de démarrage s'effectue dans l'ordre suivant :

Power => Online (1)

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

Pour le SNi40, la phase de démarrage s'effectue dans l'ordre suivant :

Power => Run (1)

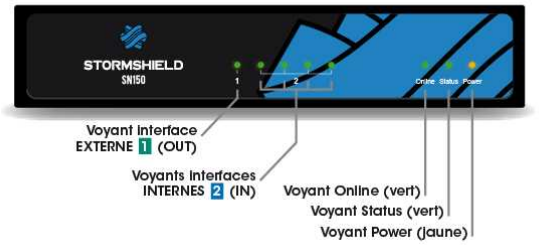
Le voyant *Power* s'allume en premier. Au bout de quelques minutes, le voyant *Run* s'allume, lorsque votre produit est opérationnel.

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.

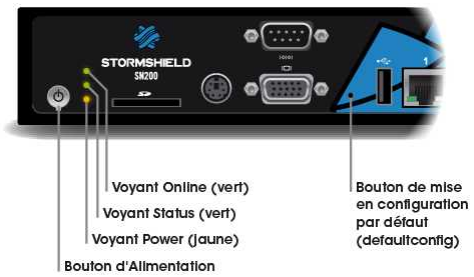


Démarrage des SN200, SN300, SN500, SN700 et SN900

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 permettent, 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 des SN510 et SN710

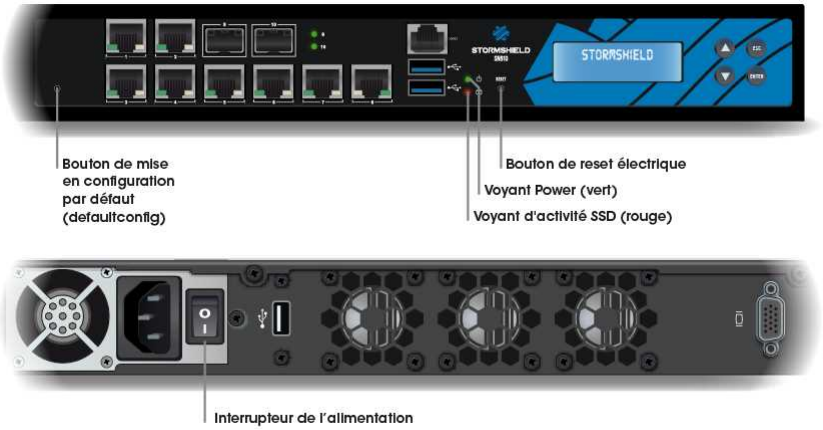
Branchez votre Firewall Stormshield Network sur le secteur en vous assurant que l'interrupteur de l'alimentation est positionné sur «ON». Votre Firewall démarre alors automatiquement. Attendez quelques minutes que les 3 voyants *Online*, *Status* et *Power* soient allumés.

NOTE

Huit bips successifs vous permettent, 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 SN910



Branchez votre Firewall Stormshield Network sur le secteur en vous assurant que l'interrupteur de l'alimentation est positionné sur «ON». Votre Firewall démarre alors automatiquement, le voyant Power s'allume. Attendez ensuite quelques minutes.

NOTE

Huit bips successifs vous permettent, 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 indiquent la fin de la phase de démarrage du produit.

Démarrage des SN2000 et SN3000

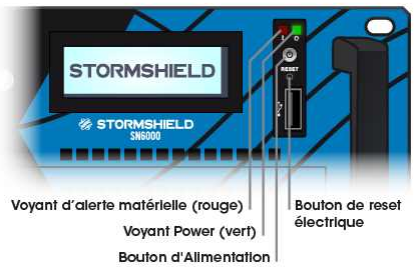
Appuyez une fois sur le Bouton d'Alimentation puis attendez quelques minutes que les 2 voyants Online et Power soient allumés.

NOTE
Huit bips successifs vous permettent, 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 permettent, 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 indiquent la fin de la phase de démarrage du produit.

Démarrage du SNi40

Une fois mis sous tension, votre Firewall démarre automatiquement. Attendez quelques minutes que les deux voyants *Power* et *Run* 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 *Run* allumé indique la fin de la phase de démarrage du produit.

Première connexion au boîtier

La première connexion au boîtier nécessite une procédure de sécurisation si cette connexion s'effectue au travers d'un réseau qui n'est 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.

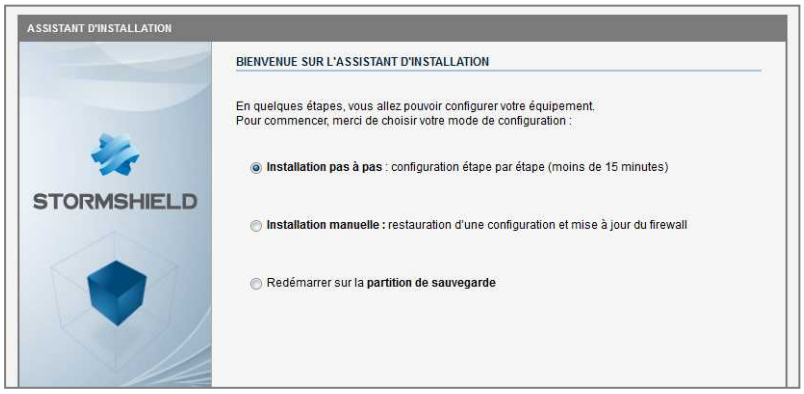
Assistant de première installation

Depuis votre poste client, tapez l'adresse suivante 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.stormshield.eu

Ce mot de passe ne doit être en aucun cas sauvegardé dans le navigateur Web.

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

LaSuite d'Administration Stormshield Network, regroupant les logiciels GLOBAL ADMINISTRATION, 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.stormshield.eu/last-version

Extinction

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.

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 ces modèles, l'arrêt s'effectue dans l'ordre suivant :

Online ❶ **+** ***Status*** ❷ **=>** ***Power*** ❸

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

SN510 et SN710

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 3 voyants *Online*, *Status* et *Power* soient éteints.

Pour ces modèles, l'arrêt s'effectue dans l'ordre suivant :

Online ❶ **+** ***Status*** ❷ **=>** ***Power*** ❸

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

SN910

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 le voyant *Power* soit éteint

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 relatif aux SN200, SN300, SN500, SN700, et SN900, sans le voyant *Status*.

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

SNi40

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 Run et Power soient éteints. Pour ce modèle, l'arrêt s'effectue dans l'ordre suivant :

Run ❶ **=>** ***Power*** ❷

Remarques générales

- Le voyant *Status* ❷ clignote en cas de défaut majeur du produit (anomalie matérielle, 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, ou *Run* pour le SNi40, 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 (*Run* pour le SNi40).
- 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.
- Lorsqu'un modèle SNi40 est arrêté (voyant *Power* et *Run* éteints), vous pouvez le redémarrer en le débranchant puis en le rebranchant sur sa source d'alimentation.
- Lorsqu'un modèle SN510, SN710 ou SN910 est arrêté (voyant *Power* éteint), vous pouvez le redémarrer en débranchant puis en rebranchant la prise secteur.
- Vous pouvez également arrêter votre Firewall en vous connectant en mode console et en tapant la commande suivante : `halt`.
- Lorsqu'un modèle SNi40 est arrêté (voyant *Power* et *Run* éteints), vous pouvez le redémarrer en le débranchant, attendez trente secondes, puis en le rebranchant sur sa source d'alimentation.
- Lorsqu'un modèle SN510, SN710 ou SN910 est arrêté (voyant *Power* éteint), vous pouvez le redémarrer en le débranchant, attendez trente secondes, puis en rebranchant la prise secteur.

DOCUMENTATION ET ASSISTANCE

AIDE EN LIGNE

Le guide d'utilisation des Firewalls Multifonctions SN est disponible en ligne à l'adresse : http://documentation.stormshield.eu

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.
- 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.

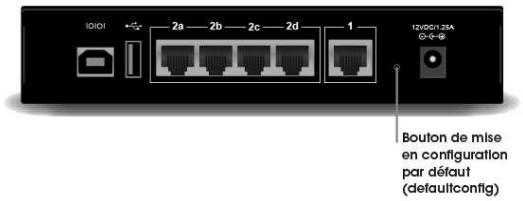
NOTE
Les voyants *Online* et *Status* (*Run* sur SNi40) clignotent pendant toute la durée de la réinitialisation. Deux bips successifs (sauf pour les modèles SN150 et SNi40) et le voyant *Online* (*Run* sur SNi40) allumé indiquent la fin de la phase de redémarrage du produit.

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

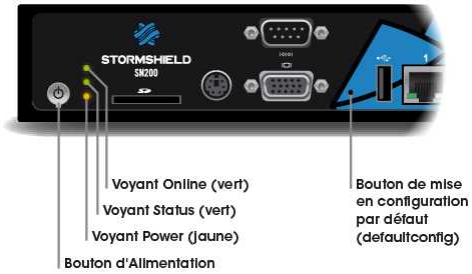
Tous les modèles sauf SN6000 et SNi40

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

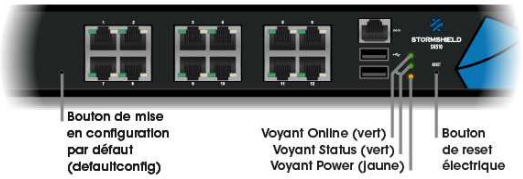
- pour les modèles SN150, sur la face arrière du produit, entre les interfaces Ethernet et la fiche de branchement de l'adaptateur secteur.
- pour les modèles SN200, SN300, SN500, SN700 et SN900, sur la face avant du produit, entre le port USB et le port VGA.
- Pour le modèle SN510, sur la face avant du produit, à gauche des interfaces Ethernet.
- Pour les modèles SN710 et SN910, sur la face avant du produit, entre l'emplacement pour module d'extension et les interfaces Ethernet.
- pour les modèles SN2000 et SN3000, sur la face avant du produit, entre les voyants et les racks SSD.



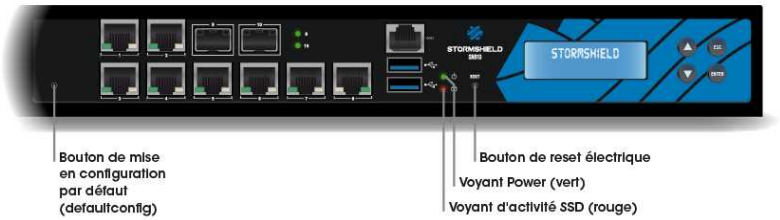
Modèle SN150



Modèles SN200, SN300, SN500, SN700 et SN900



Modèles SN510 et SN710



Modèle SN910

Modèles SN2000 et SN3000

Maintenez le poussoir appuyé au moyen de la pointe pendant environ 5 secondes, jusqu'à voir les voyants *Online* et *Status* clignoter et/ou entendre un signal sonore. La procédure de réinitialisation du Firewall se lance alors automatiquement. Après quelques minutes, le Firewall retrouve sa configuration usine, puis il redémarre.

Modèles SN6000 et SNi40

Il est possible de restaurer la configuration usine d'un SN6000 et d'un SNi40, uniquement en se connectant en mode console. Tapez la commande suivante : `defaultconfig -f -r -p`

La procédure de réinitialisation du Firewall se lance alors automatiquement. Après quelques minutes, le Firewall retrouve sa configuration usine, puis il redémarre.

ANNEXE C : STOCKAGE DES TRACES

Pour les modèles équipés d'un disque dur ou d'un SSD, le service de stockage des traces est actif par défaut, excepté pour le modèle SNi40. Pour l'activer, référez vous au chapitre *Activer le service de stockage des traces* ci-dessous.

Sur les modèles SN200, SN300, SN500, SN700 et SN900, vous pouvez souscrire à l'option **«External storage »**, permettant le stockage externe des traces sur carte SD.

Option « External storage » - stockage externe des traces sur carte SD

NOTE

Ce stockage sur support externe s'effectue uniquement sur carte SD. Ce service n'est pas compatible avec d'autres supports 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 mémoire maximum supportée est de 32Go.

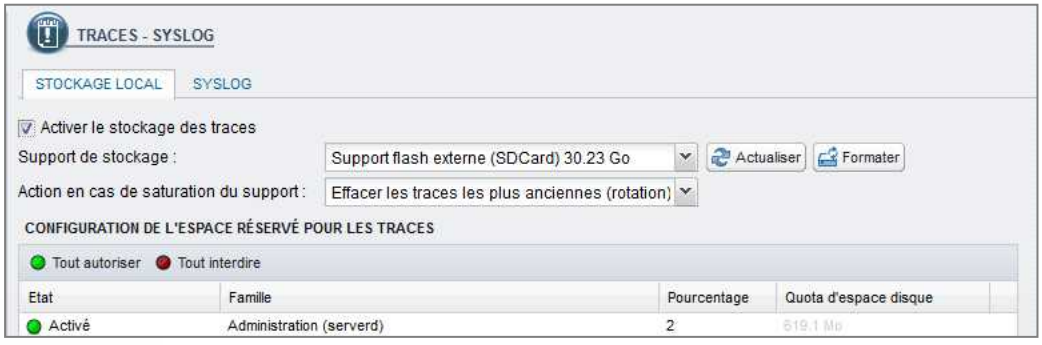
Insérez la carte SD, comme décrit dans le schéma ci-contre, avec le connecteur orienté vers le bas.

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

Vous devez ensuite activer et formater la carte SD, référez-vous au chapitre suivant.

Activer le service de stockage des traces

Pour activer le service, rendez-vous dans le menu **Notifications**, puis dans le module **Traces – Syslog**. Dans l'onglet *Stockage local*, cochez l'option *Activer le stockage des traces.*



Si vous souhaitez enregistrer les traces sur carte SD, disque dur ou sur SSD, cochez *Activer le stockage des traces*, puis sélectionnez votre support dans la liste de support de stockage. Un message vous propose de le formater.

Après cette opération, votre carte SD, disque dur ou SSD est prêt à recevoir l'ensemble des traces.

Changement du support de stockage

IMPORTANT
Avant d'éjecter la carte SD du lecteur ou de retirer le SSD d'un SN2000 (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.

Consultation des traces

Ces traces pourront être consultées via l'interface web **SN Activity Reports** sous forme de rapports, et également via 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 d'un SSD, ou à l'aide d'une carte SD avec l'option « External storage ».

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

ANNEXE D : GESTION DES SSD

Le SSD (Solid State Drive) du modèle SN2000 est amovible.

Par défaut sur les modèles SN3000 et SN6000, les deux SSD sont installés en RAID (RAID 1). Ces deux SSD sont également amovibles.

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

Il est possible de contrôler l'état SMART des SSD (Self-Monitoring, Analysis and Reporting Technology system). La technologie SMART surveille et informe de l'état de certains indicateurs de fiabilité comme la température, le nombre de secteurs réalloués, les erreurs de localisation des secteurs, etc. Elle permet ainsi d'anticiper les pannes.

Sur les modèles SN910, SN2000 et SNi40, l'état SMART du SSD est disponible dans l'encart *Matériel* du widget **Matériel**.

Sur les modèles SN3000 et SN6000, l'encart *RAID* du widget **Matériel** vous informe de l'état SMART des SSD, ainsi que de l'état du RAID.

Vous pouvez également vous connecter au produit en mode console ou par connexion SSH, et obtenir ces informations grâce aux commandes suivantes :

- pour l'état SMART des SSD : `smartinfo`
- si votre produit dispose du RAID : `nraid -s`

En cas de problème avec la partition de logs, remonté par le widget Propriétés ou en mode console ou par connexion SSH, via la commande `logdisk -c`, la reconstruction de la partition s'effectue à l'aide de la commande suivante : `logdisk -f`

IMPORTANT
Cette commande efface définitivement les données précédemment enregistrées sur la partition de logs.

Si l'état SMART d'un SSD remonte des erreurs, ou si la reconstruction de votre partition de logs échoue, vous pouvez contacter votre partenaire certifié afin de remplacer votre SSD.

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 1) :

Cette procédure s'effectue sur le produit en fonctionnement. Après avoir extrait le SSD défectueux, insérez le nouveau SSD, obtenu auprès de votre partenaire. puis tapez la commande suivante pour scanner ce nouveau SSD : `nraid -z`.

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

Option Big Data

En cas de souscription à l'option *Big Data* (disponible sur les modèles SN3000 et SN6000), les SSD d'origine sont remplacés par des SSD d'une capacité supérieure. Après avoir arrêté le produit, vous pouvez extraire les SSD. Insérez ensuite les nouveaux SSD. Ceux- ci seront automatiquement pris en compte au prochain démarrage du produit.

ANNEXE E : ECHANGE D'UN MODULE D'ALIMENTATION (SN3000 ET SN6000)

RAPPEL

Avant tout raccordement à une alimentation 48VDC, veuillez lire attentivement et respecter les REGLES DE SECURITE.

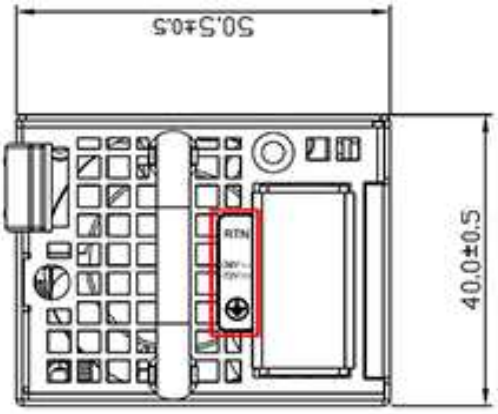
SN3000

AVERTISSEMENT

Certains équipements Stormshield Network SN3000 ne sont pas compatibles avec les modules d'alimentation 48VDC et ne doivent pas les utiliser.

Les produits concernés ont le « Part Number » suivant :SN3000-XA10A-101

Si votre SN3000 est concerné et que vous souhaitez utiliser un module d'alimentation 48VDC, veuillez contacter votre partenaire ou revendeur afin de procéder au remplacement de votre équipement.



1. Débrancher la connexion d'alimentation du module à extraire :
   - **Module secteur :** débrancher le cordon d'alimentation.
   - **Module 48VDC :** débrancher d'abord le cordon d'alimentation côté source d'alimentation. Ensuite, côté module, ôter le clip de protection ❶, puis à l'aide d'un tournevis, débrancher les 3 câbles d'alimentation.
2. Extraire le module : pousser le levier de déverrouillage latéralement, vers la poignée d'extraction et tirer le module à l'aide de cette poignée. Saisir le corps du module et l'extraire complètement.

3. Insérer le nouveau module, étiquette produit vers le haut. En fin d'insertion, pousser bien à fond, jusqu'à entendre un "clic" indiquant le verrouillage mécanique du module. Vérifier le verrouillage en tirant légèrement sur la poignée d'extraction : le module doit rester en place.
4. Raccorder le nouveau module à sa source d'alimentation :
   - **Module secteur :** brancher le cordon d'alimentation.
   - **Module 48VDC :** le cordon d'alimentation étant débranché côté source d'alimentation, à l'aide d'un tournevis, raccorder au module les 3 conducteurs du cordon d'alimentation ❶ puis replacer le clip de protection. Le câblage du module 48VDC doit être conforme au schéma ci-dessus. Brancher ensuite le cordon d'alimentation côté source d'alimentation.

Chaque module d'alimentation est équipé d'un voyant d'état (bicolore : vert/rouge pour le module secteur, bleu/rouge pour le module 48VDC) :

• Module opérationnel

- module raccordé à sa source d'alimentation et non inséré : vert (secteur)/bleu (48VDC).

- SN3000 à l'arrêt :

- module inséré et non raccordé à sa source d'alimentation, et autre module inséré et raccordé à sa source d'alimentation : vert (secteur)/bleu (48VDC), clignotant.
- module inséré et raccordé à sa source d'alimentation : vert (secteur)/bleu (48VDC), clignotant.

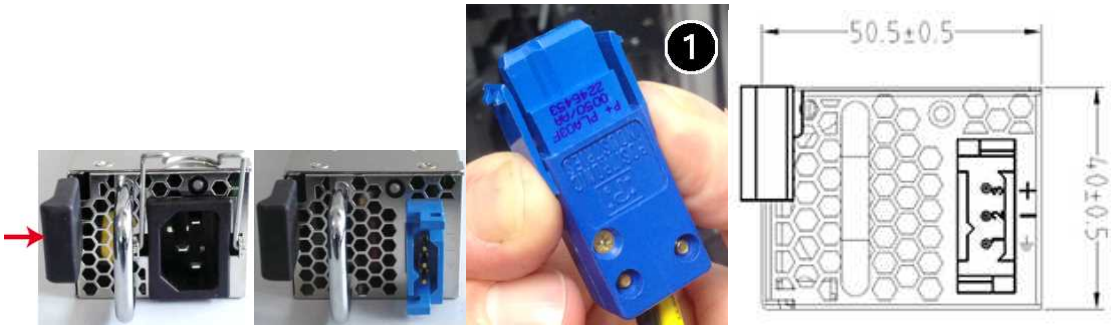
- SN3000 en fonctionnement :

- module inséré et alimenté : vert (secteur)/bleu (48VDC), fixe.
- module inséré et non alimenté : rouge, clignotant (+ bips buzzer).

• Module en panne

- module alimenté : rouge, fixe.

SN6000



1. Débrancher la connexion d'alimentation du module à extraire,
   - **Module secteur :** débrancher le cordon d'alimentation
   - **Module 48VDC :** débrancher le cordon d'alimentation côté module, en pinçant le connecteur verticalement ❶, et tirer.
2. Extraire le module : pousser le levier de déverrouillage latéralement, vers la poignée d'extraction et tirer. Saisir le corps du module et l'extraire complètement.

   ATTENTION
   L'enveloppe métallique du module sert de dissipateur et sa température peut atteindre +60°C à pleine puissance. Il est donc conseillé d'enfiler un gant de protection pour saisir le module.
3. Insérer le nouveau module, étiquette produit vers le haut. En fin d'insertion, pousser bien à fond, jusqu'à entendre un "clic" indiquant le verrouillage mécanique du module. Vérifier le verrouillage en tirant légèrement sur la poignée d'extraction : le module doit rester en place.
4. Raccorder le nouveau module à sa source d'alimentation :
   - **Module secteur :** brancher le cordon d'alimentation
   - **Module 48VDC** : brancher le connecteur du cordon d'alimentation ❶. Vérifier le verrouillage mécanique du connecteur en tirant légèrement.

Chaque module d'alimentation est équipé d'un voyant d'état (bicolore : vert/rouge) :

• Module opérationnel

- module raccordé à sa source d'alimentation et non inséré : vert, clignotant.

- SN6000 à l'arrêt :

- module inséré et non raccordé à sa source d'alimentation, et autre module inséré et raccordé à sa source d'alimentation : vert, clignotant.
- module inséré et raccordé à sa source d'alimentation : vert, clignotant.

- SN6000 en fonctionnement :

- module inséré et alimenté : vert, fixe.
- module inséré et non alimenté : rouge (secteur)/éteint(48VDC), fixe (+ bips buzzer).

• Module en panne

- module alimenté : rouge, fixe.

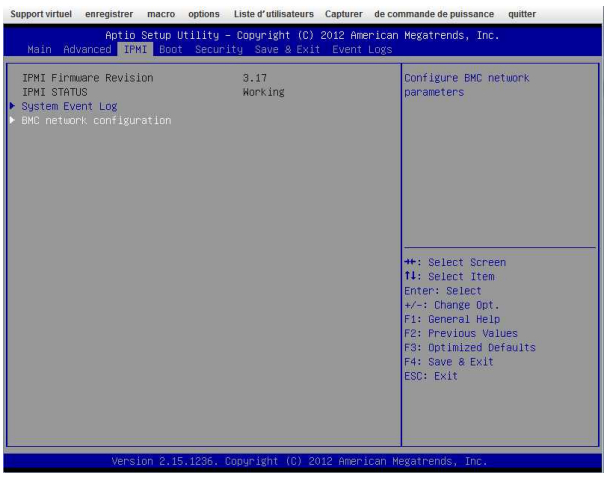
ANNEXE F : CONFIGURATION ET ADMINISTRATION VIA IPMI (SN6000)

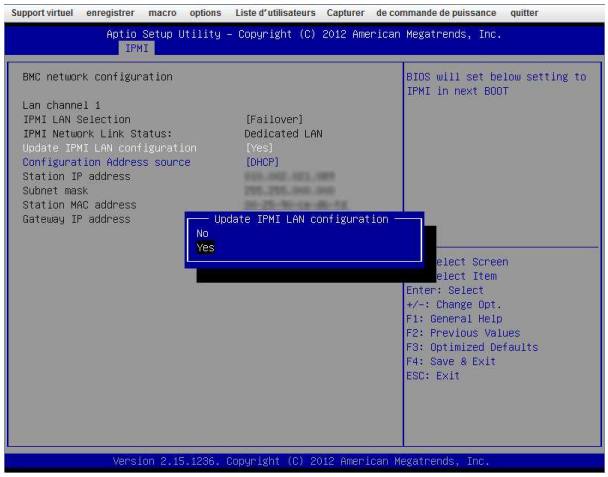
L'interface de gestion intelligente de matériel (IPMI - Intelligent Platform Management Interface) est un protocole réseau, permettant à distance d'obtenir des informations matérielles, de surveiller certains composants et de contrôler l'équipement (contrôle, redémarrage, interruption, etc.).

Paramétrage

Au démarrage du produit, à l'apparition du logo *Stormshield*, pressez la touche <del> pour accéder au BIOS.

Allez ensuite dans la section "IPMI/BMC network configuration" du menu IPMI, afin de configurer l'interface réseau dédiée à l'IPMI, puis sauvegardez et quittez.



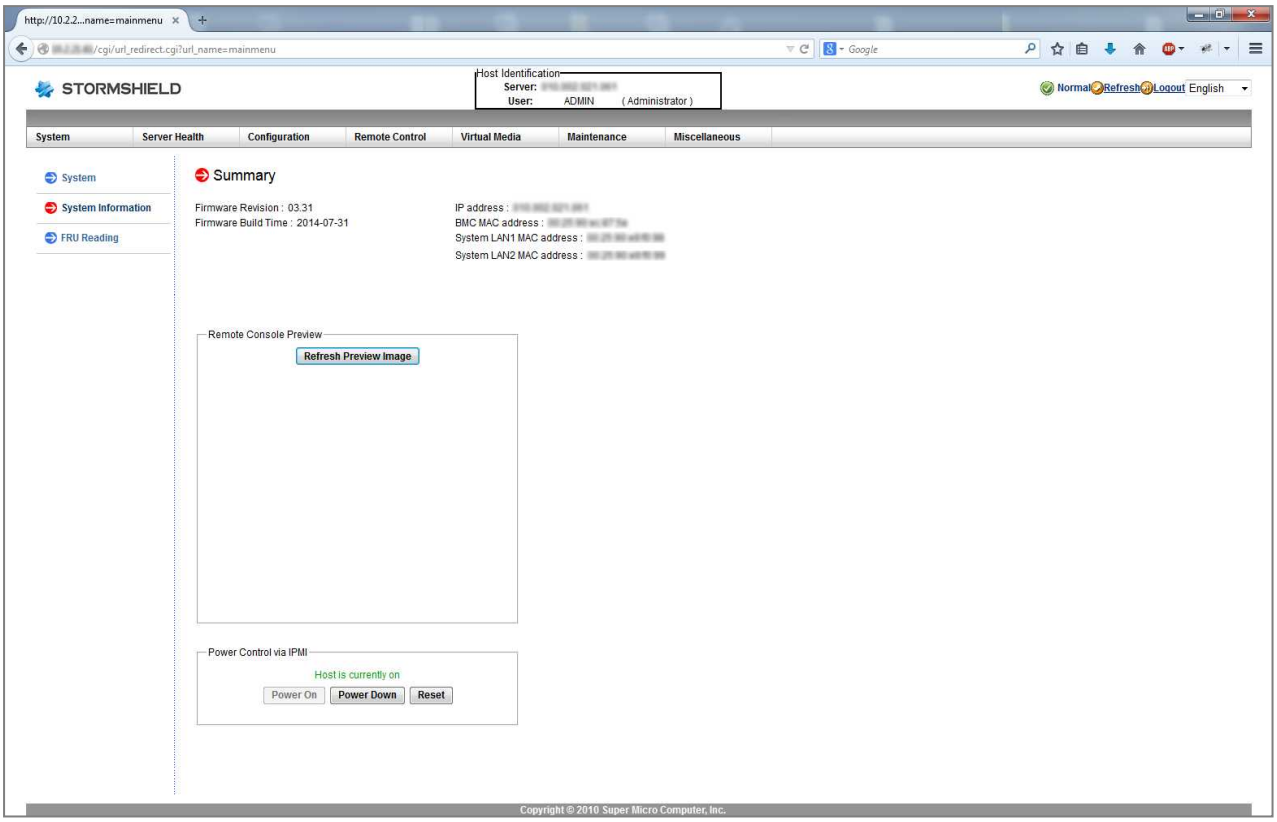


Connexion

Branchez le câble réseau à l'arrière du châssis, sur l'interface réseau dédiée.

Lancez votre navigateur et connectez-vous à l'interface dédiée en tapant l'adresse : **http://*<ip_if_ipmi>***
L'identifiant et le mot de passe sont par défaut « ADMIN ».

Le tableau de bord de l'interface web se présente ainsi :



IMPORTANT

Changer sans délai le mot de passe de l'administrateur "ADMIN" via le menu *Configuration/Users*. D'autre part, il est conseillé de placer l'interface IPMI sur un réseau d'administration dédié.

En cas de besoin, la documentation Supermicro suivante apporte une description détaillée de la carte mère (page 23, section 1-9) : http://www.supermicro.com/manuals/motherboard/C606_602/MNL-1306.pdf

Pour la description complète de l'interface IPMI, reportez-vous au document suivant :

http://www.supermicro.com/manuals/other/SMT_IPMI_Manual.pdf

STORMSHIELD

documentation@stormshield.eu