



STORMSHIELD



GUIDE

STORMSHIELD NETWORK SECURITY

GUIDE D'INSTALLATION ET DE PREMIÈRE CONFIGURATION D'UN FIREWALL SNS

Versions 3 et 4

Dernière mise à jour du document : 10 avril 2024

Référence : sns-fr-guide_installation_et_premiere_configuration



Table des matières

Historique des modifications	2
Avant de commencer	3
Architecture d'exemple	3
Rappel sur les mécanismes de sécurité	3
Enregistrer le firewall	5
Récupérer le mot de passe d'enregistrement et le numéro de série du firewall	5
Enregistrer le firewall depuis l'espace personnel MyStormshield	5
Vous ne possédez pas de compte MyStormshield	5
Vous possédez déjà un compte MyStormshield	6
Installer et raccorder le firewall	7
Installer le firewall	7
Raccorder le firewall à un poste client	7
Démarrer le firewall	7
Effectuer une première connexion sur le firewall	8
Accéder à l'interface d'administration du firewall	8
Comprendre l'interface graphique	9
Bandeau supérieur	9
Menu de gauche	10
Fenêtre active	10
Fenêtre inférieure	10
Modifier le mot de passe de l'utilisateur "admin"	10
Installer la licence du firewall	12
Récupérer le fichier de licence du firewall	12
Installer la licence sur le firewall	12
Mettre à jour le firewall	14
Identifier la version SNS actuellement installée	14
Télécharger le fichier de mise à jour	14
Installer la mise à jour	15
Configurer les paramètres réseau du firewall et finaliser son installation	16
Configurer les interfaces du firewall	16
Configurer l'interface in	16
Configurer les interfaces out et dmz1	17
Supprimer le bridge	17
Connecter le firewall à Internet	18
Raccorder le firewall à l'équipement d'accès à Internet	18
Configurer la passerelle par défaut	18
Mettre à jour les modules du firewall	19
Connecter le firewall au serveur web	20
Raccorder le firewall au serveur web	20
Créer un objet réseau représentant le serveur web	20
Configurer la politique de sécurité	21
Configurer la politique de filtrage URL	21
Configurer les URL	21



Configurer la politique de filtrage URL	22
Configurer la politique de filtrage/NAT	22
Choisir une politique de filtrage/NAT	22
Configurer la politique de filtrage	23
Configurer la politique de NAT	26
Tester la configuration et la sauvegarder	28
Pour aller plus loin	29



Historique des modifications

Date	Description
10 avril 2024	- Modification du lien du Guide de cycle de vie produits
13 février 2024	- Modification de la section "Effectuer une première connexion sur le firewall"
12 septembre 2022	- Modification des sections "Effectuer une première connexion sur le firewall", "Installer la licence du firewall", "Mettre à jour le firewall" et "Configurer la politique de filtrage URL" - Améliorations cosmétiques
23 juin 2022	- Améliorations cosmétiques
8 octobre 2021	- Nouveau document



Avant de commencer

Bienvenue dans le guide d'installation et de première configuration d'un firewall SNS.

L'objectif de cette documentation est de vous aider pas à pas de la réception de votre firewall jusqu'à la réalisation d'une première configuration depuis son interface d'administration.

Elle est complémentaire au [Guide de présentation et d'installation produits](#) ainsi qu'au [Guide d'installation rapide](#) fourni dans l'emballage de votre firewall. Reportez-vous à la page [Guides](#) pour les retrouver.

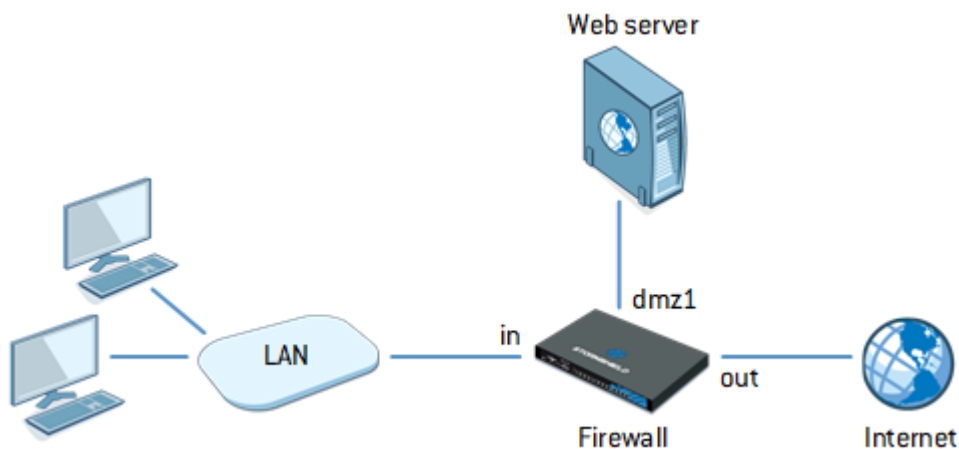
Dans cette documentation, Stormshield Network Security est désigné sous la forme abrégée SNS.

! IMPORTANT

Cette documentation concerne uniquement les firewalls physiques SNS. Pour les firewalls virtuels comme les modèles EVA ou PAYG, des [guides d'installation](#) spécifiques existent.

Architecture d'exemple

Les possibilités de configuration étant nombreuses, ce guide présente plusieurs manipulations que vous pouvez réaliser sur votre firewall. Certaines sont communes à toutes les situations, d'autres sont en lien avec une architecture servant d'exemple pour ce guide. Aidez-vous de ces éléments en les adaptant selon vos besoins.



Pour cette architecture, la configuration du firewall doit répondre aux besoins suivants :

- Les machines reliées au réseau "in" doivent pouvoir accéder :
 - À "Internet" par le biais des protocoles DNS, HTTP et HTTPS. Cet accès doit être soumis à un filtrage URL.
 - Au serveur web interne (protégé par le firewall) en HTTPS.
- "Internet" doit pouvoir joindre le serveur web interne (protégé par le firewall) en HTTPS.

Rappel sur les mécanismes de sécurité

Des mécanismes de sécurité sont mis en place pour garantir l'intégrité du firewall que vous avez reçu. Dès sa réception, nous vous recommandons de vérifier les éléments suivants.



- Vérifiez que le carton du firewall est fermé par un ou plusieurs scellés "STORMSHIELD QUALITY SEAL". Ces scellés ne doivent pas être détériorés.
- Vérifiez grâce aux étiquettes d'identification sur le carton de votre firewall que le modèle réceptionné correspond bien à celui que vous avez commandé.
- Vérifiez que l'étiquette "WARRANTY VOID IF REMOVED" sur votre firewall n'est pas détériorée.

i NOTE

Pour plus d'informations sur ces mécanismes, reportez-vous au [Guide de présentation et d'installation produits](#), chapitre **Dès réception de votre firewall**.



Enregistrer le firewall

Enregistrer votre firewall permet d'activer sa maintenance souscrite auprès de Stormshield. L'activation est automatique trois mois après la date de facturation si le firewall n'est pas enregistré entre temps.

Récupérer le mot de passe d'enregistrement et le numéro de série du firewall

Pour enregistrer votre firewall, vous devez posséder son mot de passe d'enregistrement (*Registration password*) ainsi que son numéro de série (*SN*). Ils se situent sur une étiquette collée sur votre firewall.



Enregistrer le firewall depuis l'espace personnel MyStormshield

Une fois les éléments récupérés, l'enregistrement se réalise depuis l'espace personnel MyStormshield. Il permet notamment d'associer votre firewall à votre compte MyStormshield. La procédure d'enregistrement est différente selon que vous possédez ou non déjà un compte.

Vous ne possédez pas de compte MyStormshield

L'enregistrement de votre firewall se réalise en même temps que la création de votre compte. Pour cela, accédez à la page de connexion de l'espace personnel [MyStormshield](#) et cliquez sur **Créer un compte/enregistrer un produit**.

Poursuivez ensuite selon si vous êtes :

- **Client et utilisateur des solutions Stormshield :**
 1. **Créez un nouveau compte de société.**
Complétez les étapes jusqu'à la création du compte et l'enregistrement du firewall.
- **Partenaire et revendeur des solutions Stormshield :**
 1. **Créez un nouveau compte partenaire.**
Complétez les étapes jusqu'à la création du compte partenaire. Durant ces étapes, vous n'avez pas la possibilité d'enregistrer votre firewall sur ce compte.
 2. **Créez ensuite un nouveau compte de société.**
Retournez sur la page de connexion de l'espace personnel [MyStormshield](#) puis débutez la création d'un nouveau compte de société.
Complétez les étapes jusqu'à la création du compte et l'enregistrement de votre firewall. Prenez soin de mettre en place une autorisation de cogérance pour permettre à votre compte partenaire de cogérer votre compte de société.

Pour plus d'informations, reportez-vous au guide [Créer un compte et enregistrer un produit](#).



Vous possédez déjà un compte MyStormshield

1. Connectez-vous à votre espace personnel [MyStormshield](#).
2. Rendez-vous dans la partie **Produit > Enregistrer un produit**.
3. Cliquez sur **Enregistrer une appliance SNS**.
4. Complétez les informations demandées jusqu'à l'enregistrement du firewall.

Si votre société n'apparaît pas dans le champ **Société cible** et que vous êtes partenaire et revendeur des solutions Stormshield, vous ne disposez peut-être pas encore :

- D'un compte de société vous permettant d'enregistrer vos produits,
- D'une autorisation de cogérance entre vos deux comptes (société et partenaire).

Pour plus d'informations, reportez-vous au guide [Enregistrer des produits](#).



Installer et raccorder le firewall

Commencez à installer votre firewall. Ceci vous permettra d'accéder à son interface d'administration dans le but de le configurer.

i NOTE

Des spécificités peuvent exister selon votre modèle de firewall. Complétez les informations de ce chapitre avec celles du [Guide de présentation et d'installation produits](#) et du [Guide d'installation rapide](#) fourni avec votre firewall.

Installer le firewall

- Installez votre firewall dans un endroit adapté (comme un local technique ou un bureau à accès protégé). Utilisez un système de montage particulier si nécessaire.
- Raccordez votre firewall à une source d'alimentation dont la tension est supportée. Si possible, privilégiez un raccordement à un équipement de type "ASI" (onduleur).
- Faites installer les modèles équipés d'une source de tension continue par un électricien qualifié.

Raccorder le firewall à un poste client

- Reliez un câble Ethernet sur un port interne de votre firewall ("IN" dans notre exemple) jusqu'à votre poste client ou votre réseau local sur lequel le poste client est connecté.
- L'équipement sur lequel le firewall est raccordé doit être configuré pour obtenir une adresse IP automatiquement (DHCP) ou posséder une adresse IP statique appartenant au réseau du firewall 10.0.0.0/8 (sauf l'adresse 10.0.0.254 qui est déjà attribuée au firewall).
- Ne raccordez pas de suite votre firewall jusqu'à votre équipement d'accès à Internet. Attendez d'avoir configuré les paramètres réseau du firewall.

Démarrer le firewall

- Une fois les branchements réalisés, démarrez votre firewall.
- Patientez le temps qu'il termine sa phase de démarrage. Ne le débranchez pas durant cette phase.



Effectuer une première connexion sur le firewall

Maintenant que votre firewall est installé et démarré, vous êtes en mesure de vous y connecter.

Accéder à l'interface d'administration du firewall

1. Dans un navigateur Web sur le poste client, accédez à l'adresse `https://10.0.0.254/admin`. Reportez-vous au [Guide de cycle de vie produits](#) pour connaître la liste des navigateurs web supportés.
2. Un avertissement apparaît indiquant que le domaine visité est invalide. Ce message est normal du fait que le certificat utilisé par le firewall est auto-signé. Continuez vers le site.
3. La page de connexion à l'interface d'administration du firewall apparaît. Saisissez "admin" comme identifiant et comme mot de passe, puis connectez-vous.
Par défaut, si vous faites quatre erreurs successives lors de l'authentification, vous devez attendre une minute avant de vous identifier à nouveau. Si vous tentez de vous identifier alors que le temps d'attente n'est pas écoulé, celui-ci est allongé d'une minute supplémentaire, dans la limite de dix minutes. Le nombre d'erreurs et le temps d'attente sont configurables. Pour plus d'informations, reportez-vous à la section Onglet Administration du firewall du *Manuel utilisateur SNS v4* ou *v3* de la version SNS utilisée.

L'interface d'administration s'affiche. Son apparence varie selon la version SNS pré-installée.

Interface d'administration d'un firewall SNS en version 4

Date	Mess...	Action	Priority	Source	Destination

Interface d'administration d'un firewall SNS en version 3

Date	Action	Priority	Sou Source	Des Destination	Message
02:15:59 PM		Minor			Interface up: em0
02:15:59 PM		Minor			Interface up: em1
02:15:59 PM		Minor			Firewall startup



Comprendre l'interface graphique

La fenêtre est composée de 4 zones :

1. Le bandeau supérieur permettant de choisir entre les vues **Monitoring** et **Configuration**, et donnant des informations sur l'état du firewall,
2. Le menu de gauche permettant d'accéder aux différents modules du firewall,
3. La fenêtre active du module sélectionné,
4. La fenêtre inférieure listant les erreurs, les avertissements, les commandes et les notifications.

En version 3, l'interface d'administration ne dispose pas des onglets **Monitoring** et **Configuration**, car tout est regroupé dans le menu de gauche.

The screenshot displays the Stormshield Network Security interface. The top header (Zone 1) includes the logo, version 4.7.1, and navigation tabs for MONITORING and CONFIGURATION. The left sidebar (Zone 2) lists various modules like DASHBOARD, AUDIT LOGS, and REPORTS. The main content area (Zone 3) shows the 'DASHBOARD' for 'EVA1' with a 'NETWORK' section and a 'PROTECTION' table. The bottom status bar (Zone 4) shows system logs and messages.


Bandeau supérieur

This close-up shows the top header of the interface. From left to right, it contains: the Stormshield logo and version 4.7.1; two tabs labeled 'MONITORING' and 'CONFIGURATION'; the device name 'EVA1'; and on the far right, the user name 'admin', a 'WRITING' status indicator, and a 'LOGS RESTRICTED ACCESS' notification.

Dans le bandeau supérieur, les éléments suivants sont affichés de gauche à droite (l'ordre peut être différent ou des éléments peuvent ne pas être disponibles en version 3) :




- Le numéro de version de votre firewall,
- Deux onglets permettant d'accéder aux deux vues du firewall : Monitoring et Configuration,
- Le modèle de votre firewall et son nom : survolez le nom pour afficher le numéro de série,
- Un pictogramme clignotant s'affichant si l'état de votre firewall requiert votre attention : survolez le pictogramme pour afficher les éléments surveillés et leur statut,
- Votre nom d'utilisateur : cliquez dessus pour accéder à vos préférences ou vous déconnecter,
- Vos droits de lecture et d'écriture : survolez les droits pour afficher plus d'informations,
- Vos droits d'accès aux logs : si vous êtes en accès restreint, cliquez dessus pour demander un accès complet,



- L'icône  permettant d'ouvrir la page du *Manuel Utilisateur SNS* en ligne se rapportant au module que vous consultez.

Menu de gauche

Le menu de gauche permet d'accéder aux différents modules correspondant aux différentes fonctionnalités. Les modules sont classés par catégorie. Vous pouvez :

- Réduire le menu en cliquant sur ,
- Déplier et de réduire les catégories en cliquant dessus,
- Mettre des modules en favori en cliquant sur l'icône  qui s'affiche en survolant le nom d'un module,
- Accéder rapidement aux modules favoris en cliquant sur l'icône  en haut du menu.

S'il y a des modules grisés dans le menu, cela peut indiquer :

- Qu'ils nécessitent une licence à laquelle vous n'avez pas souscrit, et donc, que vous n'y avez pas accès.
- Que l'utilisateur avec lequel vous êtes connecté n'a pas les privilèges nécessaires pour accéder à ces modules.

Les modules présents dans le menu changent suivant si vous êtes en vue **Monitoring** ou en vue **Configuration**.


Lorsque vous utilisez la barre de recherche, la recherche porte aussi bien sur le nom du module que sur son contenu.

Fenêtre active

Le contenu de cette fenêtre change suivant le module que vous affichez.

Fenêtre inférieure

La fenêtre inférieure liste les erreurs, les avertissements, les commandes et les notifications. Vous pouvez :

- Masquer ou afficher cette fenêtre en cliquant sur la flèche au milieu .
- Paramétrer les messages qui s'affichent en cliquant sur **Options**.

Modifier le mot de passe de l'utilisateur "admin"

Par mesure de sécurité, vous devez modifier le mot de passe par défaut de l'utilisateur "admin" lors de la première connexion au firewall.

1. Si le firewall est en version 4, rendez-vous dans l'onglet **Configuration** situé dans le bandeau supérieur. Tout changement de configuration s'effectue depuis cet onglet.
2. Via le menu de gauche, rendez-vous dans **Configuration > Système > Administrateurs**, onglet **Compte admin**.
3. Si le firewall est en version 4, renseignez *admin* dans le champ *Ancien mot de passe*.



4. Saisissez le nouveau mot de passe et confirmez-le. Aidez-vous des éléments suivants :

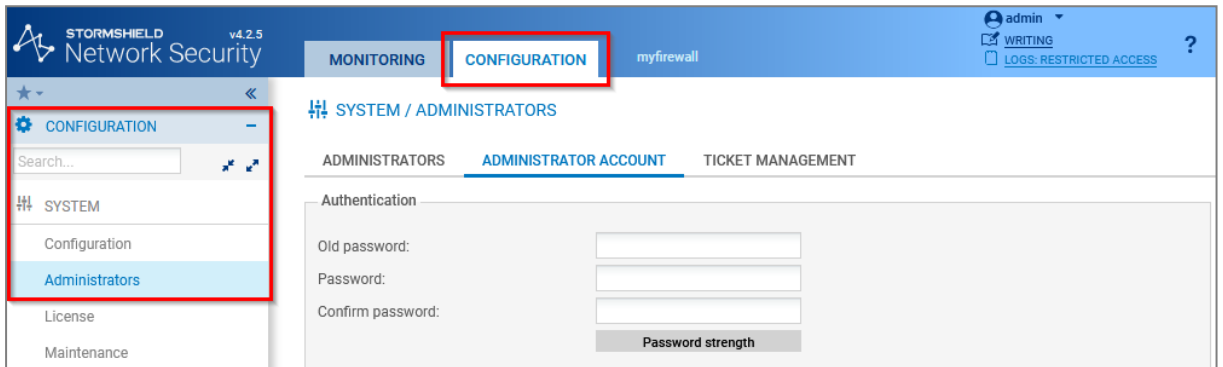
- Une jauge permet de connaître la robustesse du mot de passe tapé. Utilisez des majuscules et des caractères spéciaux pour renforcer son niveau de sécurité.
- Le mot de passe ne peut pas contenir les caractères :

" <tab> <space>

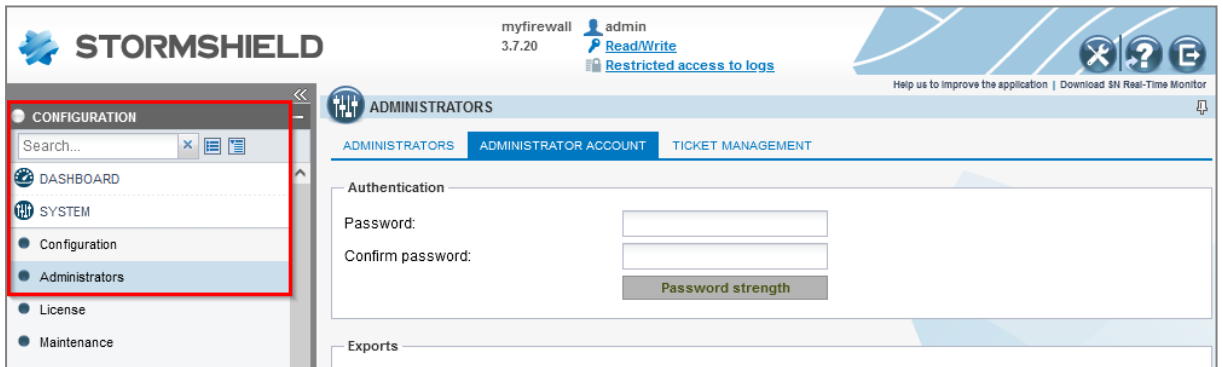
5. Cliquez sur **Appliquer**, puis **Sauvegarder**.

Lors de la prochaine connexion, le nouveau mot de passe devra être utilisé.

Interface d'administration d'un firewall SNS en version 4



Interface d'administration d'un firewall SNS en version 3





Installer la licence du firewall

Installer la licence définitive sur votre firewall remplace sa licence temporaire. Ceci active alors les fonctionnalités et options souscrites dans le pack de maintenance du firewall.

Récupérer le fichier de licence du firewall

1. Connectez-vous à votre espace personnel [MyStormshield](#).
2. Rendez-vous dans **Produit > Gestion des produits**.
3. Dans le cadre **Gestion des produits**, identifiez votre firewall en utilisant les boutons **Déplier** et **Replier** ou en renseignant son numéro de série dans la zone de recherche. Cliquez ensuite dessus.
4. Dans le cadre de droite, dans la zone **Téléchargement**, cliquez sur le lien à côté de **Fichier de licence**. Acceptez le téléchargement du fichier *.licence*.

The screenshot shows the 'Management of your products' interface. On the left, a search box contains 'SN210W'. Below it, a list of products is shown, with 'SN210W' highlighted in a red box. On the right, the 'Customized description' section is visible, and a 'License file' link is highlighted in a red box in the 'Downloads' section.

Installer la licence sur le firewall

1. Accédez à l'interface d'administration du firewall à l'adresse <https://10.0.0.254/admin>.
2. Rendez-vous dans **Configuration > Système > Licence**.
3. Dans la zone **Installation à partir d'un fichier**, sélectionnez le fichier de licence téléchargé précédemment.
4. Cliquez sur **Installer le fichier de licence**, puis patientez le temps que la licence s'installe.
5. Un redémarrage du firewall peut être requis afin d'activer certaines fonctionnalités de la nouvelle licence ou pour faire évoluer le modèle de firewall vers un autre. Si tel est le cas, un avertissement apparaît dans le bandeau supérieur. Pour redémarrer le firewall, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Configuration**, et cliquez sur **Redémarrer le firewall**.



Interface d'administration d'un firewall SNS en version 4

GENERAL	LICENSE DETAILS
Search for a new license Install the new license	
Local firewall date: Friday 19th August 2022	
● The [REDACTED] license is temporary. Please register your firewall in order to obtain the permanent license. Last check for license updates performed on: Friday 19th August 2022	
✔ Temporary license will expire in 864 days, on Tuesday 31st December 2024.	
✔ Maintenance will expire in 864 days, on Tuesday 31st December 2024.	
The Stormshield Vulnerability Manager option has not been subscribed.	
The advanced antivirus option has not been subscribed.	
The Extended Web Control option has not been subscribed.	
The sandboxing Breach Fighter option has not been subscribed.	
The industrial option has not been subscribed.	
Install license	
License file :	<input type="text"/> ...
<input type="button" value="Install"/>	

Interface d'administration d'un firewall SNS en version 3

GENERAL	LICENSE DETAILS
Search for a new license Install the new license	
Local firewall date: Friday 19th August 2022	
● The [REDACTED] license is temporary. Please register your firewall in order to obtain the permanent license. Last check for license updates performed on: Friday 19th August 2022	
✔ Temporary license will expire in 864 days, on Tuesday 31st December 2024.	
✔ Maintenance will expire in 864 days, on Tuesday 31st December 2024.	
The Stormshield Vulnerability Manager option has not been subscribed.	
The advanced antivirus option has not been subscribed.	
The Extended Web Control option has not been subscribed.	
The sandboxing Breach Fighter option has not been subscribed.	
Install from file	
License file :	<input type="text"/> ...
<input type="button" value="Install the license file."/>	



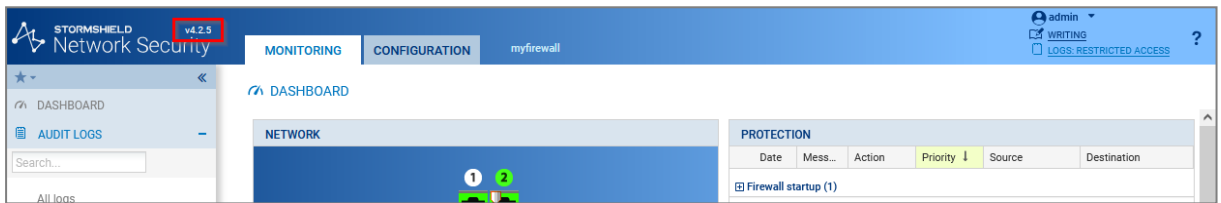
Mettre à jour le firewall

Mettre à jour votre firewall vers une version récente permet de bénéficier des dernières fonctionnalités disponibles ainsi que des derniers correctifs fonctionnels et de vulnérabilités.

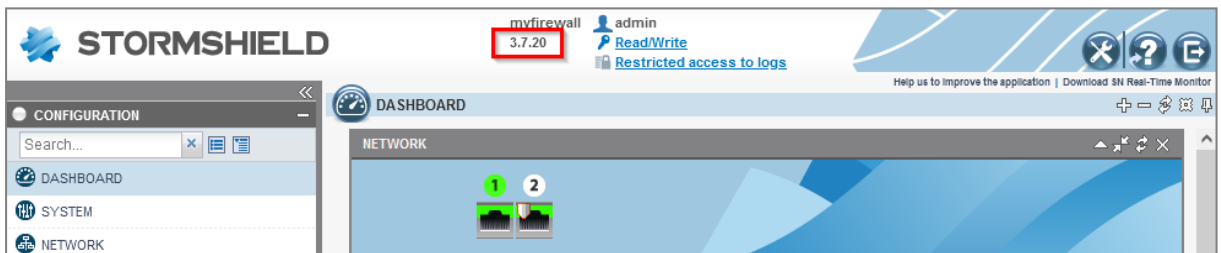
Identifier la version SNS actuellement installée

1. Accédez à l'interface d'administration du firewall à l'adresse <https://10.0.0.254/admin>.
2. Visualisez le numéro de version SNS dans le bandeau supérieur.

Interface d'administration d'un firewall SNS en version 4



Interface d'administration d'un firewall SNS en version 3



Télécharger le fichier de mise à jour

1. Connectez-vous à votre espace personnel [MyStormshield](#).
2. Rendez-vous dans **Téléchargements > Téléchargements**.
3. Dans les catégories, sélectionnez **Stormshield Network Security**, puis **Firmware**. Si besoin, sélectionnez en plus une branche de version (comme 4.X) pour affiner la liste.
4. Repérez la version que vous souhaitez installer sur votre firewall. Pour cela :
 - Consultez les notes de version pour connaître le contenu des versions SNS.
 - Assurez-vous que la nouvelle version est compatible avec votre modèle de firewall. Dans certains cas, une version intermédiaire peut être requise.
 - Si une version dispose de plusieurs versions correctives, privilégiez toujours la dernière afin de bénéficier des derniers correctifs fonctionnels et de vulnérabilités.
 - Utilisez une version dont la date de fin de vie n'a pas été atteinte. Pour plus d'informations, reportez-vous au document [Cycle de vie produits Network Security & Tools](#).
5. Pour la version souhaitée, cliquez sur le nom correspondant à votre modèle de firewall pour télécharger le fichier de mise à jour. Acceptez le téléchargement du fichier *.maj*.
6. Vous pouvez vérifier l'intégrité des binaires récupérés grâce à la commande `sha256sum <filename>` sous Linux ou `CertUtil -hashfile <filename> SHA256` sous Windows. Comparez ensuite le résultat avec l'empreinte (hash) indiquée dans MyStormshield en cliquant sur **Afficher** dans la colonne **SHA256** du fichier *.maj* concerné.



DASHBOARD [DOWNLOADS](#)

To view your download, click on a category below :

- STORMSHIELD NETWORK SECURITY
- STORMSHIELD DATA SECURITY
- STORMSHIELD ENDPOINT SECURITY
- STORMSHIELD VISIBILITY CENTER
- NETASQ

- ADMINISTRATION SUITE
- CENTRALIZED MANAGER
- EVENT ANALYZER
- FIRMWARE
- MANAGEMENT CENTER - SMC
- SSO AGENT
- TOOLS
- VPN CLIENT
- VPN SSL

- 4.X
- 3.X
- 3.7 - LTSB
- 2.X
- 1.X

STORMSHIELD NETWORK SECURITY - FIRMWARE - V 4.1.3 Published the 2020-12-12

Release Note : [EN / FR](#) User Guide : [EN / FR](#)

NAME	TYPE	FORMAT	SIZE	SHA256
EVA1, EVA2, EVA3, EVA4, EVAU, VPAYG	Firmware	maj	60M	Display
SN160-A, SN160W-A, SN210-A, SN210W-A, SN310-A	Firmware	maj	50M	Display
SN510-A, SN710-A, SNI40-A, SNI20-A	Firmware	maj	57M	Display
SN6100-A, SN3100-A, SN2100-A, SN910-A, SN6000-A, SN3000-A, SN2000-A	Firmware	maj	57M	Display
Virtual Image for EVA1, EVA2, EVA3, EVA4, EVAU, VPAYG	Firmware	kvm	84M	Display
Virtual Image for EVA1, EVA2, EVA3, EVA4, EVAU, VPAYG	Firmware	openstack	84M	Display
Virtual Image for EVA1, EVA2, EVA3, EVA4, EVAU, VPAYG	Firmware	ova	87M	Display
Virtual Image for EVA1, EVA2, EVA3, EVA4, EVAU, VPAYG	Firmware	vhd	84M	Display

Installer la mise à jour

1. Dans l'interface d'administration du firewall, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Mise à jour du système**.
2. Sélectionnez le fichier de mise à jour téléchargé précédemment.
3. Cliquez sur **Mettre à jour le firewall**, puis patientez le temps que la mise à jour s'installe.

Interface d'administration d'un firewall SNS en version 4

SYSTEM UPDATE [BACKUP](#) [RESTORE](#) [CONFIGURATION](#)

Available updates

No update available

System update

Select the update:

Interface d'administration d'un firewall SNS en version 3

SYSTEM UPDATE [BACKUP](#) [RESTORE](#) [CONFIGURATION](#)

Available updates :

No update available

Select the update :

Save the active partition on the backup partition before updating the firewall



Configurer les paramètres réseau du firewall et finaliser son installation

Configurez à présent les paramètres réseau de votre firewall et finalisez son installation.

À partir de ce chapitre :

- Toutes les manipulations effectuées sont en lien avec notre [architecture d'exemple](#).
- Les manipulations sont réalisées en version 4. Elles peuvent aussi être réalisées en version 3 avec des adaptations du fait que l'interface d'administration peut être différente.
- Même lorsque cela n'est pas précisé dans les procédures, toutes les manipulations sont à réaliser en étant connecté à l'interface d'administration du firewall.

ASTUCE

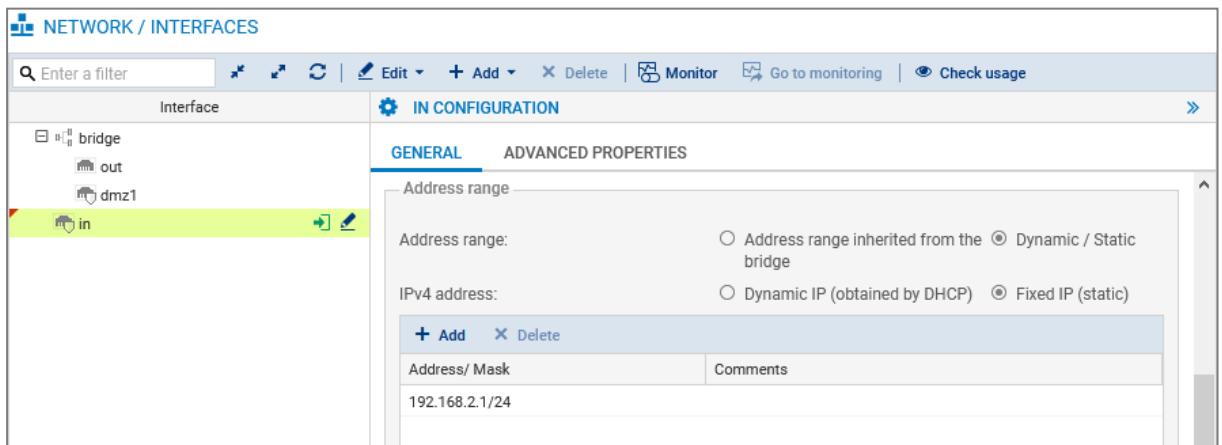
Pour obtenir des informations sur les modules de l'interface d'administration du firewall, appuyez-vous sur le manuel utilisateur [v4](#) ou [v3](#) de la version SNS utilisée.

Configurer les interfaces du firewall

Configurer l'interface *in*

1. Rendez-vous dans le module **Configuration > Réseau > Interfaces**.
2. Sélectionnez l'interface *in*, puis cliquez sur le bouton **Éditer**.
3. Dans l'onglet **Général**, complétez les informations de la zone **Plan d'adressage** :
 - Champ **Adressage** : sélectionnez **Dynamique / Statique**.
 - Champ **Adresse IPv4** : sélectionnez **IP fixe (statique)**.
 - Dans la grille : cliquez sur **Ajouter** et renseignez **192.168.2.1/24**.
4. Cliquez sur **Appliquer** pour valider.

La connexion au firewall est alors perdue. Pour poursuivre, utilisez la nouvelle adresse IP pour vous connecter au firewall. Si l'équipement relié au firewall utilise des paramètres IP renseignés manuellement, modifiez-les pour qu'ils appartiennent au nouveau sous-réseau de l'interface *in*.





Configurer les interfaces *out* et *dmz1*

1. Sélectionnez l'interface *out* et cliquez sur le bouton **Éditer**.
2. Dans l'onglet **Général**, complétez les informations de la zone **Plan d'adressage** :
 - Champ **Adressage** : sélectionnez **Dynamique / Statique**.
 - Champ **Adresse IPv4** : sélectionnez **IP fixe (statique)**.
 - Dans la grille : cliquez sur **Ajouter** et renseignez *203.0.113.1/24*.
3. Sélectionnez l'interface *dmz1*, puis cliquez sur le bouton **Éditer**.
4. Dans l'onglet **Général**, complétez les informations de la zone **Plan d'adressage** :
 - Champ **Adressage** : sélectionnez **Dynamique / Statique**.
 - Champ **Adresse IPv4** : sélectionnez **IP fixe (statique)**.
 - Dans la grille : cliquez sur **Ajouter** et renseignez *172.16.1.1/24*.
5. Cliquez sur **Appliquer** pour valider.

Interface	Port	Type	Status	IPv4 address	Comments
out	1	Ethernet, 1 Gb/s		203.0.113.1/24	
in	2	Ethernet, 1 Gb/s		192.168.2.1/24	
dmz1	3	Ethernet, 1 Gb/s		172.16.1.1/24	
bridge		Bridge		DHCP	

VERIFICATION OF THE CONFIGURATION

Warning bridge Bridge bridge consists of 0 interfaces

Supprimer le bridge

1. Sélectionnez le bridge restant, cliquez sur **Supprimer** et confirmez sa suppression.
2. Cliquez sur **Appliquer** pour valider.

Il reste ainsi les interfaces *in*, *out* et *dmz1* avec une adresse IPv4 statique.

Interface	Port	Type	Status	IPv4 address	Comments
out	1	Ethernet, 1 Gb/s		203.0.113.1/24	
in	2	Ethernet, 1 Gb/s		192.168.2.1/24	
dmz1	3	Ethernet, 1 Gb/s		172.16.1.1/24	



Connecter le firewall à Internet

Raccorder le firewall à l'équipement d'accès à Internet

Reliez un câble Ethernet du port "Externe" (OUT) de votre firewall jusqu'à votre équipement d'accès à Internet.

Configurer la passerelle par défaut

Configurer la passerelle par défaut permet au firewall de savoir où envoyer les paquets qui doivent sortir vers le réseau public (Internet).

Créer un objet réseau représentant la passerelle par défaut

i NOTE

Si l'interface *out* de votre firewall récupère une adresse IP depuis un serveur DHCP, le bail DHCP délivré entraîne la création automatique de l'objet réseau *Firewall_out_router*. Si la configuration de votre firewall correspond à ce cas (différent de notre exemple), poursuivez vers la section suivante **Définir la passerelle par défaut** sans créer un nouvel objet.

1. Rendez-vous dans le module **Configuration > Objets > Réseau**.
2. Cliquez sur **Ajouter** et assurez-vous d'être positionné sur l'onglet **Machine**.
3. Définissez un nom à l'objet (*my_gateway* dans notre exemple).
4. Renseignez l'adresse IPv4 de la passerelle par défaut et définissez sa résolution DNS (*Aucune (IP statique)* dans notre exemple). L'adresse MAC n'est pas requise.
5. Cliquez sur **Créer** pour valider.

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

Address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name: my_gateway

IPv4 address:

MAC address: 01:23:45:67:89:ab (optional)

Resolution

None (static IP) Automatic

Comments:



Définir la passerelle par défaut

1. Rendez-vous dans le module **Configuration > Réseau > Routage**.
2. Sur l'onglet **Routes statiques IPv4**, zone **Configuration générale**, sélectionnez l'objet représentant la passerelle par défaut (*my_gateway* dans notre exemple).
3. Cliquez sur **Appliquer**.

The screenshot shows the 'NETWORK / ROUTING' section with the 'IPV4 STATIC ROUTES' tab selected. Under the 'General' section, the 'Default gateway (router):' is set to 'my_gateway'. Below this is a table for 'STATIC ROUTES' with columns for Status, Destination network, Interface, Address range, Gateway, and Comments. The table is currently empty. At the bottom, there are 'CANCEL' and 'APPLY' buttons.

Mettre à jour les modules du firewall

Maintenant connecté à Internet, assurez-vous que les modules du firewall se mettent à jour.

- Le module **Active Update** permet de maintenir à jour automatiquement les modules du firewall lorsque ce dernier est connecté à Internet.
- Il est possible de déclencher manuellement ces mises à jour ou de les suivre depuis le module **Monitoring > Supervision > Système**, cadre **Active Update**.

The screenshot shows the 'MONITOR / SYSTEM' section with the 'REAL-TIME' tab selected. It displays a list of system services and their status. On the right, the 'Active Update' section shows the status of various update modules.

Name	Status	Last update
Antispam DNS blacklists (RBL)	Unavailable	
IPS: contextual protection signatures	Unavailable	
IPS: custom contextual protection sign...	Disabled	
Antivirus: ClamAV antivirus signatures	Unavailable	
Antispam: heuristic engine	Unavailable	
Vulnerability Manager	Unavailable	
Root Certification Authorities	Running	03:16:35 PM
Geolocation / Public IP reputation	Up to date	03:16:39 PM



Connecter le firewall au serveur web

Raccorder le firewall au serveur web

Reliez un câble Ethernet du port utilisé par l'interface *dmz1* de votre firewall jusqu'à votre serveur web.

Créer un objet réseau représentant le serveur web

Cet objet est indispensable afin de pouvoir configurer des règles impliquant le serveur web dans la politique de sécurité du firewall (configuration à venir dans notre exemple).

1. Rendez-vous dans le module **Configuration > Objets > Réseau**.
2. Cliquez sur **Ajouter** et assurez-vous d'être positionné sur l'onglet **Machine**.
3. Définissez un nom à l'objet (*srv_web_private* dans notre exemple).
4. Renseignez l'adresse IPv4 du serveur web et définissez sa résolution DNS (*172.16.1.5* et *Aucune (IP statique)* dans notre exemple). L'adresse MAC n'est pas requise.
5. Cliquez sur **Créer** pour valider.

CREATE AN OBJECT

- Host
- DNS name (FQDN)
- Network
- Address range
- Router
- Group
- IP Protocol
- Port
- Port group
- Region group
- Time object

Object name:

IPv4 address:

MAC address:

Resolution

None (static IP) Automatic

Comments:



Configurer la politique de sécurité

La politique de sécurité du firewall regroupe notamment les politiques de filtrage, de NAT, et de filtrage URL. Il existe 10 politiques de sécurité qui sont pré-configurées ou vides.

Configurer la politique de filtrage URL

La politique de filtrage URL permet de définir des règles autorisant ou bloquant l'accès à des URL. Pour être appliquée, la politique de filtrage URL doit être activée dans l'inspection applicative d'une règle de la politique de filtrage (configuration à venir dans notre exemple).

! ATTENTION

Le module **Filtrage URL** est différent du module **Filtrage SSL**. Pour filtrer et déchiffrer les connexions HTTPS, une configuration spécifique et avancée doit être mise en place. Pour plus d'informations, reportez-vous à la note technique [Filtrer les connexions HTTPS](#).

Configurer les URL

Dans notre exemple, nous souhaitons bloquer l'accès aux URL se terminant par **.exe**. Débutez par créer une catégorie personnalisée d'URL contenant le format d'URL à bloquer.

1. Rendez-vous dans **Configuration > Objets > URL (Objets Web en version 3)**, onglet **URL**.
2. Cliquez sur **Ajouter une catégorie personnalisée**.
3. Sur la nouvelle ligne, définissez un nom à la catégorie (**EXE** dans notre exemple).
4. Appuyez sur la touche Entrée de votre clavier ou cliquez dans la grille de gauche pour valider.
5. La nouvelle catégorie s'affiche alors en surbrillance. En cas contraire, sélectionnez-la.
6. Dans la grille de droite, cliquez sur **Ajouter une URL**.
7. Sur la nouvelle ligne, définissez l'URL que vous souhaitez bloquer. Dans notre exemple, nous renseignons ***.exe** permettant de bloquer toutes les URL se terminant par **.exe**.
8. Appuyez sur la touche Entrée de votre clavier ou cliquez dans la grille de droite pour valider.

The screenshot shows the 'OBJECTS / WEB OBJECTS' configuration page. The 'URL' tab is active. A table lists existing URL categories, with 'EXE' highlighted in green. To the right, the configuration for the 'EXE' category is shown, including 'Authorized characters' and a list of URLs. The 'URL' field contains '*.exe'. The interface includes navigation buttons and a page indicator 'Page 1 of 1'.

URL category	Comments
vpnssl_owa	
antivirus_byapa...	
authentication...	
EXE	

Authorized characters
Authorized characters: '*' '?' '!' ':' ';' ']' [a-z] [A-Z] [0-9]
Example: www.google.com/* or *.yahoo.com/*

URL CATEGORY: EXE

URL	Comments
*.exe	



Configurer la politique de filtrage URL

1. Rendez-vous dans le module **Configuration > Politique de sécurité > Filtrage URL**.
2. Dans le menu déroulant, observez la politique en cours d'édition. Conservez son nom. Si besoin, renommez-la en cliquant sur **Éditer > Renommer** ou choisissez-en une autre.
3. Cliquez sur **Ajouter**.
4. Modifiez les champs pour créer la règle bloquant l'accès aux URL se terminant par **.exe** :
 - Champ **Action** : sélectionnez une action permettant de bloquer l'accès. Il est possible de personnaliser la page notifiant un blocage à l'utilisateur dans le module **Configuration > Notifications > Messages de blocage**, onglet **Page de blocage HTTP**.
 - Champ **Catégorie d'URL** : sélectionnez la catégorie concernée (*EXE* dans notre exemple).
5. Vous pouvez compléter votre politique de filtrage URL en bloquant l'accès à des catégories dynamiques d'URL (comme "*shopping*" ou "*pornography*"). Chaque catégorie comporte plusieurs URL qui pourront être bloquées ou autorisées selon l'action souhaitée.
6. Positionnez les règles de blocage avant celle de *pass all* avec les boutons **Monter** et **Descendre**.
7. Cliquez sur **Appliquer**, puis sauvegardez la configuration.

	Status	Action	URL category	Comments
1	<input type="checkbox"/> off	Pass	authenticati...	authorize the URLs of authentication_bypass group
2	<input checked="" type="checkbox"/> on	BlockPage_00	EXE	
3	<input checked="" type="checkbox"/> on	BlockPage_00	pornography	
4	<input checked="" type="checkbox"/> on	Pass	any	default rule (pass all)

Configurer la politique de filtrage/NAT

La politique de filtrage/NAT regroupe un ensemble de règles de filtrage et de règles de NAT. Par défaut, le firewall utilise une politique **Block All** qui permet à un administrateur du firewall d'accéder à l'interface d'administration et de bloquer toutes les autres connexions.

Lors de la configuration de la politique de filtrage/NAT de votre firewall :

- Sauvegardez à tout moment les modifications en cours en cliquant sur **Appliquer**.
- Veillez à ne pas activer une politique de filtrage/NAT incomplète ou incorrecte qui pourrait rendre inaccessible l'interface d'administration de votre firewall.
- Gardez en mémoire que le firewall SNS est bloquant : tout flux non explicitement décrit dans la politique est rejeté sans journalisation, même si cette règle n'apparaît pas.

Choisir une politique de filtrage/NAT

1. Rendez-vous dans le module **Configuration > Politique de sécurité > Filtrage et NAT**.
2. Sélectionnez une politique vide parmi **Filter 05, 06, 07 ou 08** dans le menu déroulant.
3. Si souhaité, renommez la nouvelle politique en cliquant sur **Éditer > Renommer**.



SECURITY POLICY / FILTER - NAT

(8) Filter 08

(1) Block all

(2) High

(3) Medium

(4) Low

(5) Filter 05

(6) Filter 06

(7) Filter 07

(8) Filter 08

(9) Pass all High

(10) Pass all

New rule | Delete | Up | Down | Copy | Paste | Search in logs

Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
--------	--------	-------------	------------	----------	---------------------	----------

Page 0 of 0 | No data to display

Configurer la politique de filtrage

La configuration de la politique de filtrage s'effectue dans le module **Configuration > Politique de sécurité > Filtrage et NAT**, onglet **Filtrage**.

Pour répondre aux besoins de notre architecture d'exemple, créez les règles suivantes :

- Une règle permettant la résolution DNS des noms,
- Une règle permettant au réseau "in" d'accéder à "Internet" en HTTP,
- Une règle permettant au réseau "in" d'accéder à "Internet" en HTTPS,
- Une règle permettant au réseau "in" d'accéder au serveur web en HTTPS,
- Une règle permettant à "Internet" de joindre le serveur web en HTTPS.



ASTUCE

Ajoutez des séparateurs dans votre politique de filtrage afin d'optimiser son organisation.

Permettre la résolution DNS des noms

1. Cliquez sur **Nouvelle règle > Règle simple**.
2. Double-cliquez sur le numéro de la nouvelle règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État** : sélectionnez *On*.
4. Dans l'onglet **Action**, champ **Action** : sélectionnez *passer*.
5. Dans l'onglet **Source**, champ **Machines sources** : sélectionnez *Network_in*.
6. Dans l'onglet **Destination**, champ **Machines destinations** : sélectionnez *Internet*.
7. Dans l'onglet **Port / Protocole**, champ **Port** : sélectionnez *dns_udp*.
8. Cliquez sur **OK**.

FILTERING NAT

Searching...

+ New rule | Delete | Up | Down | Copy | Paste | Search in logs

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
on	pass	Network_in	Internet	dns_udp		IPS	Created on...

Page 1 of 1 | Displaying 1 - 2 of 2



Permettre au réseau "in" d'accéder à "Internet" en HTTP

1. Cliquez sur **Nouvelle règle > Règle simple**.
2. Double-cliquez sur le numéro de la nouvelle règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État** : sélectionnez *On*.
4. Dans l'onglet **Action**, champ **Action** : sélectionnez *passer*.
5. Dans l'onglet **Source**, champ **Machines sources** : sélectionnez *Network_in*.
6. Dans l'onglet **Destination**, champ **Machines destinations** : sélectionnez *Internet*.
7. Dans l'onglet **Port / Protocole**, champ **Port** : sélectionnez *http*.
8. Dans l'onglet **Inspection**, zone **Inspection applicative**, champ **Filtrage URL** : sélectionnez une politique de filtrage URL (*URLFilter_00* dans notre exemple).
9. Cliquez sur **OK**.

The screenshot shows the 'FILTERING' tab in the Stormshield interface. A table lists firewall rules. Rule 2 is highlighted in green, indicating it is selected. The rule is named 'Internet access from in to Internet (contains 2 rules, from 1 to 2)'. Rule 2 has the following configuration: Status: on, Action: pass, Source: Network_in, Destination: Internet, Dest. port: http, Protocol: http, Security inspection: IPS, and Comments: URL filter: URLFilter_00.

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
Internet access from in to Internet (contains 2 rules, from 1 to 2)								
1	on	pass	Network_in	Internet	dns_udp		IPS	Created on...
2	on	pass	Network_in	Internet	http		IPS	URL filter: URLFilter_00 Created on...

Permettre au réseau "in" d'accéder à "Internet" en HTTPS

1. Cliquez sur **Nouvelle règle > Règle simple**.
2. Double-cliquez sur le numéro de la nouvelle règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État** : sélectionnez *On*.
4. Dans l'onglet **Action**, champ **Action** : sélectionnez *passer*.
5. Dans l'onglet **Source**, champ **Machines sources** : sélectionnez *Network_in*.
6. Dans l'onglet **Destination**, champ **Machines destinations** : sélectionnez *Internet*.
7. Dans l'onglet **Port / Protocole**, champ **Port** : sélectionnez *https*.
8. Cliquez sur **OK**.

The screenshot shows the 'FILTERING' tab in the Stormshield interface. A table lists firewall rules. Rule 3 is highlighted in green, indicating it is selected. The rule is named 'Internet access from in to Internet (contains 3 rules, from 1 to 3)'. Rule 3 has the following configuration: Status: on, Action: pass, Source: Network_in, Destination: Internet, Dest. port: https, Protocol: https, Security inspection: IPS, and Comments: URL filter: URLFilter_00.

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
Internet access from in to Internet (contains 3 rules, from 1 to 3)								
1	on	pass	Network_in	Internet	dns_udp		IPS	Created on...
2	on	pass	Network_in	Internet	http		IPS	URL filter: URLFilter_00 Created on...
3	on	pass	Network_in	Internet	https		IPS	URL filter: URLFilter_00 Created on...

Permettre au réseau "in" d'accéder au serveur web en HTTPS

1. Cliquez sur **Nouvelle règle > Règle simple**.
2. Double-cliquez sur le numéro de la nouvelle règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État** : sélectionnez *On*.



4. Dans l'onglet **Action**, champ **Action** : sélectionnez *passer*.
5. Dans l'onglet **Source**, champ **Machines sources** : sélectionnez *Network_in*.
6. Dans l'onglet **Destination**, champ **Machines destinations** : sélectionnez l'objet définissant le serveur web (*srv_web_private* dans notre exemple).
7. Dans l'onglet **Port / Protocole**, champ **Port** : sélectionnez *https*.
8. Cliquez sur **OK**.

FILTERING NAT									
Searching...									
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments	
Internet access from in to Internet (contains 3 rules, from 1 to 3)									
1	on	pass	Network_in	Internet	dns_udp		IPS	Created on...	
2	on	pass	Network_in	Internet	http		IPS URL filter: URLFilter_00	Created on...	
3	on	pass	Network_in	Internet	https		IPS	Created on...	
Access from in to dmz (contains 1 rules, from 4 to 4)									
4	on	pass	Network_in	srv_web_private	https		IPS	Created on...	

Permettre à "Internet" de joindre le serveur web en HTTPS

1. Cliquez sur **Nouvelle règle > Règle simple**.
2. Double-cliquez sur le numéro de la nouvelle règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État** : sélectionnez *On*.
4. Dans l'onglet **Action**, champ **Action** : sélectionnez *passer*.
5. Dans l'onglet **Source** :
 - Champ **Machines sources** : sélectionnez *Internet*.
 - Champ **Interface d'entrée** : sélectionnez *out*.
6. Dans l'onglet **Destination**, champ **Machines destinations** : sélectionnez *Firewall_out*.
7. Dans l'onglet **Port / Protocole**, champ **Port** : sélectionnez *https*.
8. Cliquez sur **OK**.

Pour sauvegarder les modifications, cliquez sur **Appliquer**.

FILTERING NAT									
Searching...									
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments	
Internet access from in to Internet (contains 3 rules, from 1 to 3)									
1	on	pass	Network_in	Internet	dns_udp		IPS	Created on...	
2	on	pass	Network_in	Internet	http		IPS URL filter: URLFilter_00	Created on...	
3	on	pass	Network_in	Internet	https		IPS	Created on...	
Access from in to dmz (contains 1 rules, from 4 to 4)									
4	on	pass	Network_in	srv_web_private	https		IPS	Created on...	
Access from Internet to dmz (web server) (contains 1 rules, from 5 to 5)									
5	on	pass	Internet interface: out	Firewall_out	https		IPS	Created on...	



Configurer la politique de NAT

La configuration de la politique de NAT s'effectue dans le module **Configuration > Politique de sécurité > Filtrage et NAT**, onglet **NAT**.

Pour répondre aux besoins de notre architecture d'exemple, créez les règles suivantes :

- Une règle pour les flux sortants,
- Une règle pour les flux entrants.

Créer une règle pour les flux sortants

1. Cliquez sur **Nouvelle règle > Règle simple**.
2. Double-cliquez sur le numéro de la nouvelle règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État** : sélectionnez *On*.
4. Dans l'onglet **Source originale**, champ **Machines sources** : sélectionnez *Network_in*.
5. Dans l'onglet **Destination originale** :
 - Sous-onglet **Général**, champ **Machines destinations** : sélectionnez *Internet*.
 - Sous-onglet **Configuration avancée**, champ **Interface de sortie** : sélectionnez *out*.
6. Dans l'onglet **Source translatée** :
 - Champ **Machine source translatée** : sélectionnez *Firewall_out*.
 - Champ **Port source translaté** : sélectionnez *ephemeral_fw*.
 - Cochez la case **choisir aléatoirement le port source translaté**.
7. Cliquez sur **OK**.

FILTERING		NAT									
Searching...		+ New rule - X Delete		↑ ↓ ↺ ↻		Cut Copy Paste		Search in logs Search in monitoring		≡	
	Status	Original traffic (before translation)			Traffic after translation				Protocol	Comments	
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port			
1	on	Network_in	Internet interface: out	Any	Firewall_Out	ephemeral_fw	Any			Created on...	

Créer une règle pour les flux entrants

1. Cliquez sur **Nouvelle règle > Règle simple**.
2. Double-cliquez sur le numéro de la nouvelle règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État** : sélectionnez *On*.
4. Dans l'onglet **Source originale** :
 - Champ **Machines sources** : sélectionnez *Internet*.
 - Champ **Interface d'entrée** : sélectionnez *out*.
5. Dans l'onglet **Destination originale** :
 - Champ **Machines destinations** : sélectionnez *Firewall_out*.
 - Champ **Port destination** : sélectionnez *https*.
6. Dans l'onglet **Destination translatée**, champ **Machine destination translatée** : sélectionnez l'objet représentant le serveur web (*srv_web_private* dans notre exemple).
7. Cliquez sur **OK**.

Pour sauvegarder les modifications, cliquez sur **Appliquer**.



FILTERING NAT										
Searching...										
+ New rule - X Delete ↑ ↓ ↶ ↷ Cut Copy Paste Search in logs Search in monitoring										
	Status	Original traffic (before translation)			Traffic after translation				Protocol	Comments
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port		
1	on	Network_in	Internet interface: out	Any	Firewall_out	ephemeral_fw	Any			Created on...
2	on	Internet interface: out	Firewall_out	https	Any		srv_web_private			Created on...

<< < | Page 1 of 1 | > >> | Refresh

Displaying 1 - 2 of 2



Tester la configuration et la sauvegarder

Maintenant que votre firewall est configuré, assurez-vous que tout fonctionne correctement. Si tel est le cas, nous vous recommandons de sauvegarder la configuration du firewall afin de pouvoir la restaurer en cas de besoin.

Tester la configuration

Si des accès ne fonctionnent pas une fois la configuration finalisée, identifiez si le dysfonctionnement est lié à la configuration de votre firewall. Pour cela :

- Procédez à une vérification des règles de vos politiques de filtrage, de NAT et d'URL afin d'identifier une éventuelle erreur.
- Il est possible de positionner une règle de *pass all* en premier dans la politique de filtrage ou d'URL afin d'identifier si une règle est trop restrictive. Attention toutefois, ceci compromet la sécurité de votre environnement le temps de réaliser vos tests.

Sauvegarder la configuration

Réalisez une sauvegarde de la configuration de votre firewall dans le module **Configuration > Système > Maintenance**, onglet **Sauvegarder**. Vous pouvez également activer une sauvegarde automatique de sa configuration depuis ce même module.

Pour plus d'informations, reportez-vous sur le chapitre **Maintenance** du manuel utilisateur SNS.



Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions peuvent être disponibles sur les liens suivants :

- [Note technique concernant la Haute disponibilité](#) (SNS en version 4 uniquement).
- [Documentations techniques liées aux topologies VPN.](#)
- Site web de la documentation technique [SNS en version 4](#) ou [SNS en version 3](#) (notes de version, guides, notes techniques).
- [Outil de recherche d'un partenaire](#) si besoin d'accompagnement pour une configuration plus complexe.
- [Base de connaissances Stormshield](#) (authentification nécessaire).
- [Aide en ligne MyStormshield.](#)



STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2026. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.