



STORMSHIELD



GUIDE

**STORMSHIELD NETWORK SECURITY
ELASTIC VIRTUAL APPLIANCE**

GUIDE DE DÉPLOIEMENT D'UN FIREWALL VIRTUEL SNS EVA

Produits concernés : SNS 3.11 et versions supérieures

Dernière mise à jour du document : 10 avril 2024

Référence : sns-fr_EVA_Guide_Installation



Table des matières

Historique des modifications	3
Avant de commencer	4
Prérequis techniques et fonctionnement	5
Versions SNS compatibles	5
Caractéristiques techniques des modèles EVA	5
Hyperviseurs compatibles	5
Enregistrer le produit SNS EVA	6
Vous ne possédez pas d'espace MyStormshield	6
Vous possédez déjà un espace MyStormshield	6
Télécharger le fichier d'installation	7
Déployer le fichier d'installation sur un environnement virtuel	8
Déploiement sur une plate-forme VMWare	8
Déploiement sur une plate-forme XenServer	9
Configurer le firewall virtuel SNS EVA	10
Activer le firewall virtuel SNS EVA	11
Télécharger le kit d'activation	11
Importer le kit d'activation	11
Résoudre les problèmes	12
Pour aller plus loin	14
Annexe : procédure de migration d'un modèle V / VS-VU vers un modèle EVA	15
Obtenir et enregistrer un nouveau modèle EVA	15
Déployer le nouveau modèle EVA et activez-le	15
Sauvegarder la configuration du modèle V / VS-VU	15
Restaurer la configuration du modèle V / VS-VU sur le modèle EVA	16



Historique des modifications

Date	Description
10 avril 2024	Modification du lien du Guide de cycle de vie produits.
13 février 2024	Modification de la procédure de migration d'un modèle V / VS-VU vers un modèle EVA



Avant de commencer

Bienvenue dans le guide de déploiement d'un firewall virtuel SNS EVA.

Ce guide présente le déploiement d'un firewall SNS EVA sur un hyperviseur auto-hébergé. Pour déployer un firewall SNS EVA sur une plate-formes Cloud public, des notes techniques spécifiques existent ([3DS OUTSCALE](#), [Amazon Web Services](#) et [Microsoft Azure](#)).

Dans cette documentation, Stormshield Network Security Elastic Virtual Appliance est désigné sous la forme abrégée "SNS EVA" ou encore "EVA".

i NOTE

Les modèles EVA remplacent les modèles V / VS-VU. La procédure de migration d'un modèle V / VS-VU vers un modèle EVA est détaillée dans l'annexe [Procédure de migration d'un modèle V / VS-VU vers un modèle EVA](#).



Prérequis techniques et fonctionnement

Versions SNS compatibles

3.11 et versions supérieures

Caractéristiques techniques des modèles EVA

Modèle	RAM	HDD	vCPU
EVA1	max = 2 Go	10 Go (2 Go de swap)	max = 1
EVA2	max = 3 Go	10 Go (2 Go de swap)	max = 2
EVA3	max = 6 Go	10 Go (2 Go de swap)	max = 4
EVA4	max = 8 Go	10 Go (2 Go de swap)	max = 4
EVAU	max = 64 Go	10 Go (4 Go de swap)	max = 16

Les firewalls SNS EVA adaptent leurs capacités (nombre maximal de connexions, règles, objets, tunnels VPN, ...) en fonction des ressources allouées sur l'hyperviseur. À noter que :

- Une machine EVA doit disposer d'au moins 1 Go de mémoire. En cas d'utilisation intensive de l'antivirus et de l'analyse Sandboxing, 2 Go de mémoire minimum sont recommandés,
- Une machine EVA1 avec 2 Go de RAM et une machine EVA2 avec 2 Go de RAM présentent les mêmes capacités, seul le nombre de vCPU autorisés diffère.
- Il est possible de passer facilement d'un modèle EVA à un autre grâce au numéro de série générique "VMSNS" ne tenant pas compte du modèle. Cependant, **avant de diminuer la mémoire d'une machine virtuelle, assurez-vous que les nouvelles limites appliquées seront compatibles avec la configuration en place.**

Hyperviseurs compatibles

Vous devez être familiarisé avec l'un des environnements virtuels ci-dessous afin de déployer un firewall virtuel SNS EVA.

	Nombre d'interfaces connectées à la machine virtuelle	Version de l'hyperviseur
VMware ESXi	1 interface min. 10 interfaces max.	Pour plus d'informations, reportez-vous au Guide de cycle de vie produits .
Citrix XenServer	1 interface min. 7 interfaces max.	
Microsoft Hyper-V	1 interface min. 8 interfaces max.	
Linux KVM	1 interface min. Max : dépend de l'éditeur Linux choisi	



Enregistrer le produit SNS EVA

Pour enregistrer votre produit SNS EVA, vous devez posséder son numéro de série et son mot de passe d'enregistrement. Ils se situent dans l'e-mail que vous avez reçu après avoir passé votre commande.

Une fois ces éléments récupérés, l'enregistrement se réalise depuis l'espace [MyStormshield](#). Il permet notamment d'associer votre produit à votre espace MyStormshield. La procédure d'enregistrement est différente selon si vous possédez ou non déjà un espace.

Vous ne possédez pas d'espace MyStormshield

L'enregistrement de votre produit se réalise en même temps que la création de votre compte.

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

Vous possédez déjà un espace MyStormshield

L'enregistrement de votre produit se réalise depuis votre espace MyStormshield.

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



Télécharger le fichier d'installation

1. Dans votre espace [MyStormshield](#), rendez-vous dans **Téléchargements > Téléchargements**.
2. Dans les catégories, sélectionnez **Stormshield Network Security > Firmware**, puis sélectionnez la branche de version souhaitée parmi **4.X**, **4.3 - LTSB** (recommandée) ou **3.X**.
3. Repérez la version que vous souhaitez installer. Privilégiez toujours la dernière version disponible de la branche sélectionnée afin de bénéficier des derniers correctifs fonctionnels et de vulnérabilités.
4. Téléchargez l'image d'installation au format souhaité en cliquant sur son nom :
 - *kvm* pour les plate-formes basées sur KVM,
 - *openstack* pour les plate-formes basées sur Openstack,
 - *ova* pour les plate-formes VMWare,
 - *vhd* pour les plate-formes basées sur Microsoft Hyper-V.
5. Enregistrez le fichier sur votre poste de travail.

NOTE

Un seul fichier d'installation est disponible pour l'ensemble de la gamme EVA. C'est l'activation du firewall virtuel, grâce au kit d'activation contenant la licence, qui détermine le modèle EVA.



Déployer le fichier d'installation sur un environnement virtuel

Les procédures de ce chapitre concernent les plate-formes VMWare et XenServer. Vous devez les adapter si vous utilisez un autre environnement virtuel. Pour rappel, les prérequis techniques sont disponibles dans le chapitre [Prérequis techniques et fonctionnement](#).

Déploiement sur une plate-forme VMWare

1. Ouvrez vSphere Client depuis votre station d'administration.
2. Indiquez les paramètres de connexion à vCenter Server (Adresse IP / Nom d'hôte, Nom d'utilisateur et Mot de passe).
3. Cliquez sur **Connexion**.
4. Cliquez sur **Fichier > Déployer modèle OVF...**
5. Cliquez sur **Parcourir**, sélectionnez le fichier d'installation .ova téléchargé précédemment, puis cliquez sur **Suivant**.
6. Lisez et acceptez les conditions d'utilisation, puis cliquez sur **Suivant**.
7. Sélectionnez l'emplacement d'inventaire où installer la machine virtuelle et cliquez sur **Suivant**.
8. Sélectionnez l'hôte / cluster qui doit héberger la machine virtuelle et cliquez sur **Suivant**.
9. Sélectionnez l'emplacement de stockage et cliquez sur **Suivant**.
10. Validez le format de disque en cliquant sur **Suivant**.
11. Sélectionnez le réseau utilisé par chaque interface de la machine virtuelle et cliquez sur **Suivant**.
12. Remplissez le formulaire de configuration de base du firewall. Cette étape est optionnelle si vous déployez un firewall virtuel SNS PAYG.
 - Configuration globale :
 - **Customer ID** : identifiant client optionnel. Laissez ce champ vide à cette étape. Vous le remplirez plus tard dans le cadre du déploiement de firewalls virtuels SNS si vous souhaitez les associer à un client particulier,
 - **Hostname** : nom du firewall,
 - **Password** : indiquez puis confirmez le mot de passe du compte administrateur du firewall. Choisissez un mot de passe complexe respectant les recommandations d'organismes comme l'**ANSSI**.
 - Interface réseau 1 (out) :
 - **Gateway** : adresse IP de la passerelle par défaut du firewall. Laissez vide si DHCP,
 - **IP address 1** : adresse IP de la première interface réseau du firewall. Indiquez **DHCP** pour une attribution dynamique d'adresse,
 - **Netmask 1** : masque de réseau. Laissez vide si DHCP.
 - Interface réseau 2 (in) :
 - **IP address 2** : adresse IP de la deuxième interface réseau du firewall. Indiquez **DHCP** pour une attribution dynamique d'adresse,
 - **Netmask 2** : masque de réseau. Laissez vide si DHCP.
13. Cliquez sur **Suivant**.

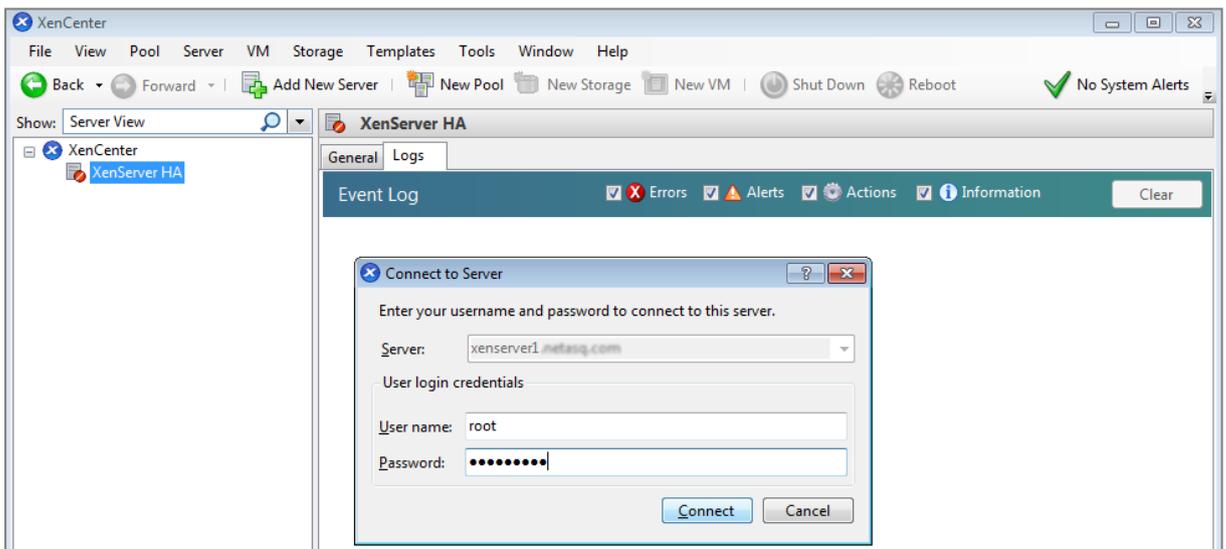


14. Vérifiez les informations du résumé et cliquez sur **Terminer**.
Le déploiement de votre firewall virtuel SNS se lance automatiquement.
Une fois terminé, poursuivez vers le chapitre [Activer le firewall virtuel SNS EVA](#).

Déploiement sur une plate-forme XenServer

1. Ouvrez XenCenter depuis votre station d'administration.
2. Indiquez les paramètres de connexion à XenServer :
 - Adresse IP/Nom,
 - Nom d'utilisateur,
 - Mot de passe.
3. Cliquez sur **Fichier > Import**.
4. Cliquez sur **Parcourir** et sélectionnez le fichier d'installation *.ova* téléchargé précédemment.
5. Lisez et acceptez les conditions d'utilisation.
6. Complétez les étapes liées à l'installation sur XenServer.

Une fois terminé, poursuivez vers le chapitre [Configurer le firewall virtuel SNS EVA](#).





Configurer le firewall virtuel SNS EVA

i NOTE

Les opérations décrites dans ce chapitre ne sont pas nécessaires pour une machine déployée sur VMWare si vous avez rempli le formulaire de configuration lors du déploiement. Dans ce cas, poursuivez vers le chapitre [Activer le firewall virtuel SNS EVA](#).

1. Sélectionnez et démarrez le firewall virtuel.
2. Accédez à la console d'administration du firewall virtuel.
3. Dans l'assistant de configuration, choisissez la langue de votre clavier.

```
#####  
## Configure keyboard mapping ##  
#####  
  
Current keyboard mapping: us.iso  
  
The available choices are:  
  1 - fr.iso  
  2 - german.iso  
  3 - it.iso  
  4 - pl_PL.IS08859-2  
  5 - spanish.iso  
  6 - swissfrench.iso  
  7 - us.iso  
Select your keyboard mapping number: █
```

4. Saisissez un mot de passe pour le compte administrateur et confirmez-le. Choisissez un mot de passe complexe respectant les recommandations d'organismes comme l'[ANSSI](#).

```
#####  
## Change SRP/SSH password for admin ##  
#####  
setting password for admin  
enter password:  
verify:  
Modify SRP/SSH password of user 'admin' successful
```

5. Les paramètres réseau des interfaces s'affichent (DHCP par défaut). Si vous les modifiez, indiquez l'adresse IP, le masque de sous-réseau puis la passerelle par défaut.

```
#####  
## Configure initial network connection ##  
#####  
  
Current network settings:  
  1st interface (out): DHCP  
  2nd interface (in): DHCP  
  
Change 1st network interface (out) settings ? [y|N]: █
```

6. L'assistant vous propose d'autoriser l'administration du firewall depuis son interface "out". Appuyez sur la touche **Entrée** du clavier pour l'accepter.

```
Will you configure your virtual appliance through its first interface 'out'?  
[Y|n]: █
```

Le firewall virtuel SNS EVA possède maintenant une configuration réseau de base.



Activer le firewall virtuel SNS EVA

Vous devez activer votre firewall afin de lui attribuer son modèle EVA, son numéro de série définitif, sa licence et les options souscrites.

Télécharger le kit d'activation

1. Dans votre espace [MyStormshield](#), rendez-vous dans **Produit > Gestion des produits**.
2. Naviguez dans la liste de vos produits jusqu'à identifier le produit concerné. Cliquez dessus.
3. À droite dans le cadre **Téléchargement**, sélectionnez la branche de version concernée. Elle doit correspondre à la version du fichier d'installation téléchargé précédemment.
4. Cliquez sur le lien **Télécharger le kit d'activation**, puis acceptez le téléchargement.

Importer le kit d'activation

1. Dans l'interface Web d'administration du firewall virtuel, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Mise à jour du système**.
2. Sélectionnez le kit d'activation (.maj) téléchargé précédemment.
3. Cliquez sur **Mettre à jour le firewall**. Le firewall redémarre automatiquement.

Votre firewall virtuel SNS EVA est maintenant déployé et activé.

Vous pouvez poursuivre vers l'un des chapitres suivants :

- [Résoudre les problèmes](#),
- [Pour aller plus loin](#),
- [Annexe : procédure de migration d'un modèle V / VS-VU vers un modèle EVA](#) si vous déployez un firewall virtuel SNS EVA dans le cadre de la procédure de migration d'un modèle V / VS-VU vers un modèle EVA.



Résoudre les problèmes

Ce chapitre liste certains problèmes fréquemment rencontrés.

Le numéro de série du firewall virtuel est toujours VMSNSX00Z0000A0

Le firewall n'est pas activé. Reportez-vous au chapitre [Activer le firewall virtuel SNS EVA](#).

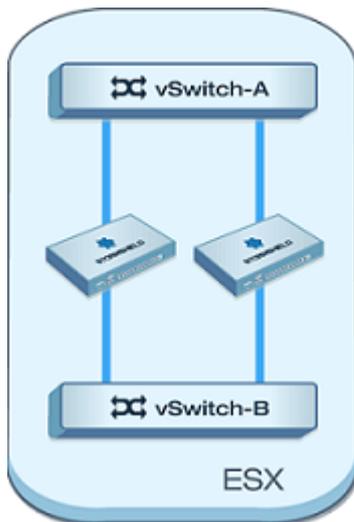
Certaines fonctionnalités du firewall virtuel ne sont pas disponibles

Vérifiez le numéro de série du firewall. S'il correspond à VMSNSX00Z0000A0, le firewall n'est pas activé. Reportez-vous alors au chapitre [Activer le firewall virtuel SNS EVA](#). Si le firewall est activé, vérifiez les détails de sa licence dans son interface Web d'administration dans **Configuration > Système > Licence**.

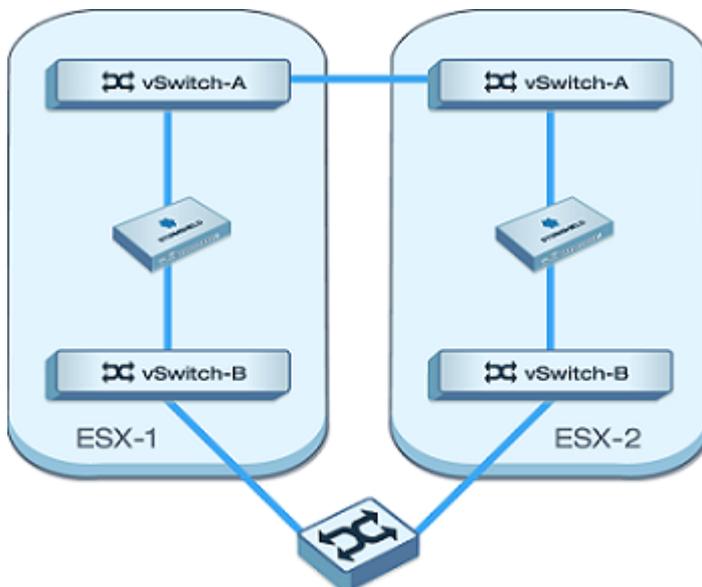
Des problèmes surviennent en haute disponibilité sur l'hyperviseur vSphere

Il est possible de rencontrer des problèmes avec les connexions à destination d'un cluster de firewalls en haute disponibilité dans les architectures suivantes :

Firewalls hébergés sur un même serveur ESX et connectés à des vSwitches :

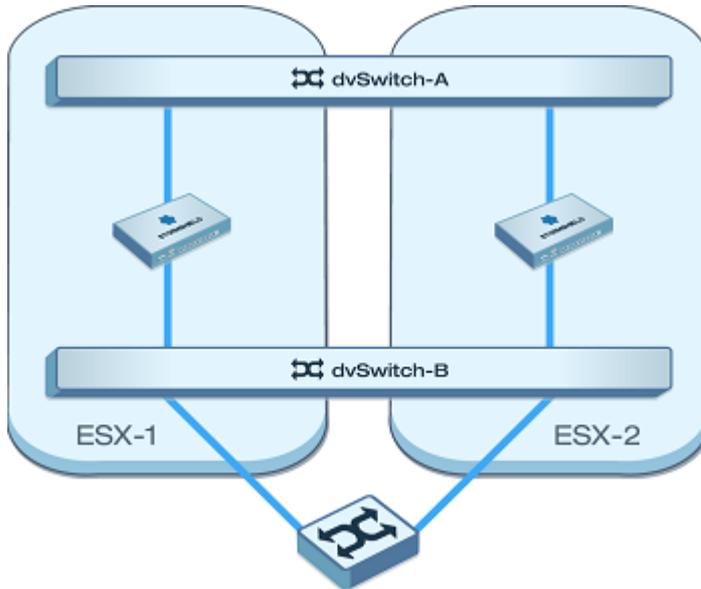


Firewalls hébergés sur deux serveurs ESX distincts et connectés à des vSwitches :





Firewalls hébergés sur deux serveurs ESX distincts et connectés à des dvSwitches :



Grâce aux outils VMWare tools, le switch virtuel (vSwitch/dvSwitch) apprend automatiquement les adresses MAC des équipements connectés sur ses ports.

Les deux membres d'un cluster SNS EVA ayant par défaut la même adresse MAC, le switch virtuel transmet toujours les paquets réseau destinés à l'adresse MAC d'un firewall vers ce firewall, quel que soit son état dans le cluster (actif ou passif). Ainsi, si le switch virtuel (vSwitch/dvSwitch) transmet des paquets vers le firewall passif, ceux-ci seront automatiquement ignorés.

La solution consiste à supprimer les adresses MAC forcées dans la configuration des deux firewalls. Réalisez cette manipulation :

Dans l'interface Web d'administration du firewall :

1. Rendez-vous dans **Configuration > Réseau > Interfaces**, onglet **Configuration avancée**.
2. Dans le champ **Adresse physique (MAC)**, supprimez toutes les adresses MAC personnalisées pour les interfaces réseau des firewalls virtuels.
3. Appliquez la modification.

Via la console système du firewall :

1. Dans le fichier de configuration `/usr/Firewall/ConfigFiles/network`, supprimez toutes les lignes contenant l'entrée `"MacAddress="`.
2. Tapez ensuite les commandes `ennetwork` puis `hasync` afin de prendre en compte les modifications et de synchroniser la configuration entre le firewall actif et le firewall passif.

En fonction des équipements réseau connectés aux firewalls, et principalement selon la valeur fixée aux timeout ARP, la restauration des connexions lors d'un changement de rôle des firewalls au sein du cluster (actif / passif) peut nécessiter un délai plus ou moins long.



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 sur SNS v4.](#)
- [Documentations techniques liées aux topologies VPN.](#)
- [Site web de la documentation technique SNS](#) (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.](#)



Annexe : procédure de migration d'un modèle V / VS-VU vers un modèle EVA

Pour migrer un modèle V / VS-VU vers un modèle EVA., le contrat de maintenance du modèle V / VS-VU concerné doit être en cours de validité. La migration est gratuite pour les modèles V / VS-VU achetés avant le 5 mars 2019.

Pour effectuer la migration d'un modèle, vous devez effectuer les actions suivantes. Pour migrer plusieurs modèles, répétez ces actions autant de fois que nécessaire.

Obtenir et enregistrer un nouveau modèle EVA

Prenez contact avec votre revendeur ou votre partenaire Stormshield et communiquez-lui le numéro de série du modèle V / VS-VU que vous souhaitez migrer. Suivez les indications jusqu'à obtenir le numéro de série EVA et son mot de passe d'enregistrement.

Si vous migrez plusieurs modèles V / VS-VU, vous devez obtenir autant de numéros de série EVA que nécessaire. Vous pouvez obtenir ces derniers en une seule demande.

Une fois le nouveau modèle EVA obtenu, enregistrez-le depuis votre espace [MyStormshield](#). Pour plus d'informations, reportez-vous au guide [Enregistrer des produits](#).

Déployer le nouveau modèle EVA et activez-le

Reportez-vous aux chapitres suivants pour effectuer les manipulations nécessaires :

1. [Télécharger le fichier d'installation](#).
2. [Déployer le fichier d'installation sur un environnement virtuel](#).
3. [Configurer le firewall virtuel SNS EVA](#).
4. [Activer le firewall virtuel SNS EVA](#).

Sauvegarder la configuration du modèle V / VS-VU

Prenez connaissance au préalable de tout changement important entre la version SNS installée sur le modèle V / VS-VU et celle sur le modèle EVA. Si nécessaire, adaptez la configuration du modèle V / VS-VU avant de la sauvegarder.

Vérifiez les changements de comportement de la nouvelle version :

- Pour SNS 3.11 LTSB : consultez la section [Préconisations](#) des notes de version 3.11 LTSB,
- Pour SNS 4.3 LTSB : consultez les sections [Points d'attention pour une mise à jour depuis une version 3.7 LTSB ou 3.11 LTSB](#) et [Changements de comportement](#) des notes de version 4.3 LTSB,
- Pour la version SNS 4.x la plus récente : consultez la section [Changements de comportement](#) des notes de version 4.

Vérifiez la compatibilité des logiciels clients Stormshield utilisés (SSO Agents, SSL VPN Client et VPN Clients) avec la nouvelle version. En cas d'incompatibilité, ces logiciels ne fonctionneront plus correctement. Pour plus d'informations, reportez-vous au [Guide de cycle de vie produits](#).

Pour sauvegarder la configuration du modèle V / VS-VU :



1. Dans l'interface Web d'administration du modèle V / VS-VU, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Sauvegarder**.
2. Cliquez sur **Télécharger la sauvegarde de configuration**.

Restaurer la configuration du modèle V / VS-VU sur le modèle EVA

1. Dans l'interface Web d'administration du firewall virtuel, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Restaurer**.
2. Sélectionnez le fichier de sauvegarde et cliquez sur **Restaurer la configuration à partir du fichier de sauvegarde**.

NOTE

Dans le cas d'un cluster de firewalls en haute disponibilité (HA) :

1. Déployez un second modèle EVA.
2. Sur le modèle EVA où la sauvegarde a été restaurée, configurez le cluster (création du cluster et intégration du second modèle EVA).



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2024. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.