



STORMSHIELD



GUIDE

**STORMSHIELD NETWORK SECURITY
ELASTIC VIRTUAL APPLIANCE**

SNS EVA VIRTUAL FIREWALL DEPLOYMENT GUIDE

Product concerned: SNS 3.11 and higher versions

Document last updated: April 10, 2024

Reference: sns-en_EVA_Installation-Guide



Table of contents

- Change log 3
- Getting started 4
- Technical requirements and operation 5
 - Compatible SNS versions 5
 - Technical characteristics of EVA models 5
 - Compatible hypervisors 5
- Registering your SNS EVA product 6
 - You do not have a MyStormshield user area 6
 - You already have a MyStormshield user area 6
- Downloading the installation file 7
- Deploying the installation file in a virtual environment 8
 - Deploying on a VMware platform 8
 - Deploying on a XenServer platform 9
- Configuring the SNS EVA virtual firewall 10
- Activating the SNS EVA virtual firewall 11
 - Downloading the activation kit 11
 - Importing the activation kit 11
- Troubleshooting 12
- Further reading 14
- Appendix: Migrating a V/VS-VU model virtual firewall to an EVA model 15
 - Obtaining and registering a new EVA model 15
 - Deploying the new EVA model and activating it 15
 - Backing up the configuration of V/VS-VU models 15
 - Restoring the configuration of the V/VS-VU model on the EVA model 16



Change log

Date	Description
April 10, 2024	Updates to the link of the Product lifecycle guide.
February 13, 2024	Changes to the process of migrating from a V/VS-VU model firewall to an EVA model.



Getting started

Welcome to the SNS EVA virtual firewall deployment guide.

This guide explains the process of deploying an SNS EVA firewall on a self-hosted hypervisor. Specific technical notes exist on the deployment of SNS EVA firewalls on a public cloud platform [[3DS OUTSCALE](#), [Amazon Web Services](#) and [Microsoft Azure](#)].

“Stormshield Network Security Elastic Virtual Appliance” is referred to in this document as “SNS “EVA” or “EVA” in the rest of this document.

i NOTE

EVA models replace V/VS-VU models. The process of migrating from a V/VS-VU model firewall to an EVA model is set out in the appendix [Migrating a V/VS-VU model virtual firewall to an EVA model](#).



Technical requirements and operation

Compatible SNS versions

3.11 and later versions

Technical characteristics of EVA models

Model	RAM	HDD	vCPU
EVA1	max = 2 GB	10 GB (2 GB for swap)	max = 1
EVA2	max = 3 GB	10 GB (2 GB for swap)	max = 2
EVA3	max = 6 GB	10 GB (2 GB for swap)	max = 4
EVA4	max = 8 GB	10 GB (2 GB for swap)	max = 4
EVAU	max = 64 GB	10 GB (4 GB for swap)	max = 16

SNS EVA firewalls scale their capacities (maximum number of connections, rules, objects, VPN tunnels, etc.) according to the resources allocated to the hypervisor. Note:

- An EVA must have at least 1 GB of memory. You are advised to set aside at least 2 GB of memory if you use the antivirus and sandboxing features frequently.
- An EVA1 machine with 2 GB of RAM and an EVA2 machine with 2 GB of RAM have the same capacities - only the number of vCPU allowed differs.
- The switch from one EVA model to another is facilitated by using a generic serial number "VMSNS" that is not dependent on the model. However, **before lowering the memory of a virtual machine, ensure beforehand that the new limits applied will be compatible with the existing configuration.**

Compatible hypervisors

You must be familiar with one of the virtual environments below before deploying an SNS EVA virtual firewall.

	Number of interfaces connected to the virtual machine	Version of the hypervisor
VMware ESXi	Min. 1 interface Max. 10 interfaces	For more information, refer to the Product lifecycle guide .
Citrix XenServer	Min. 1 interface Max. 7 interfaces	
Microsoft Hyper-V	Min. 1 interface Max. 8 interfaces	
Linux KVM	Min. 1 interface Max: depends on the Linux vendor chosen	



Registering your SNS EVA product

To register your SNS EVA product, you will need its serial number and registration password. You can find them in the e-mail you received after your order was placed.

Once you have all this information, you can register your firewall in the [MyStormshield](#) user area, where you can associate your firewall with your MyStormshield user area. The registration process varies depending on whether you already have a personal area.

You do not have a MyStormshield user area

Your product will be registered when your user area is created.

For further information, refer to the guide on [Creating accounts and registering products](#).

You already have a MyStormshield user area

Your product can be registered from your MyStormshield user area.

For further information, refer to the guide on [Registering products](#).



Downloading the installation file

1. In your [MyStormshield](#) user area, go to **Downloads > Downloads**.
2. From the list of categories, select **Stormshield Network Security > Firmware**, then select the desired version branch, either **4.X**, **4.3 - LTSB** (recommended) or **3.X**.
3. Locate the version that you wish to install. Always choose the most recent version available of the selected branch so that you benefit from the latest functional patches and bug fixes.
4. Download the installation image in the desired format by clicking on its name:
 - *kvm* for KVM platforms,
 - *openstack* for Openstack platforms,
 - *ova* for VMWare platforms,
 - *vhd* for Microsoft Hyper-V platforms.
5. Save the file on your workstation.

NOTE

Only one installation file is available for the entire EVA range. This file serves to activate the virtual firewall, by using the activation kit that contains the license, which will determine the EVA model.



Deploying the installation file in a virtual environment

The procedures in this chapter relate to the VMWare and XenServer platforms. You must adapt them if you are using another virtual environment. Please be reminded that technical requirements are listed in the chapter [Technical requirements and operation](#).

Deploying on a VMware platform

1. Open the vSphere client from your administration workstation.
2. Enter the login parameters for vCenter Server (IP address/Name, User name and Password).
3. Click on **Connect**.
4. Click on **File > Deploy OVF model...**
5. Click on **Browse**, select the *.ova* installation file downloaded earlier, then click on **Next**.
6. Read and accept the conditions of use, then click on **Next**.
7. Select the location of the inventory in which the virtual machine will be installed and click on **Next**.
8. Select the host/cluster that will host the virtual machine, and click on **Next**.
9. Select the storage location and click on **Next**.
10. Confirm the disk format by clicking on **Next**.
11. Select the network used by each interface of the virtual machine, and click on **Next**.
12. Fill in the form with the firewall's base configuration. This step is optional if you are deploying a SNS PAYG virtual firewall
 - Global configuration:
 - **Customer ID**: optional client identifier. Leave this field empty at this stage. You can fill it in later when you deploy SNS virtual firewalls if you wish to associate them with a particular client.
 - **Hostname**: firewall's name,
 - **Password**: enter, then confirm the password of the firewall's administrator account. Choose a complex password that follows the recommendations given by organizations such as the [ANSSI](#) (in French).
 - Network interface 1 (out):
 - **Gateway**: IP address of the firewall's default gateway. Leave this empty if DHCP is used,
 - **IP address 1**: IP address of the firewall's first network address. Select **DHCP** if addresses are dynamically assigned,
 - **Netmask 1**: network mask. Leave this empty if DHCP is used.
 - Network interface 2 (in):
 - **IP address 2**: IP address of the firewall's second network address. Select **DHCP** if addresses are dynamically assigned,
 - **Netmask 2**: network mask. Leave this empty if DHCP is used.
13. Click on **Next**.
14. Check the information in the summary and click on **Finish**.
Your SNS virtual firewall will automatically start deploying.

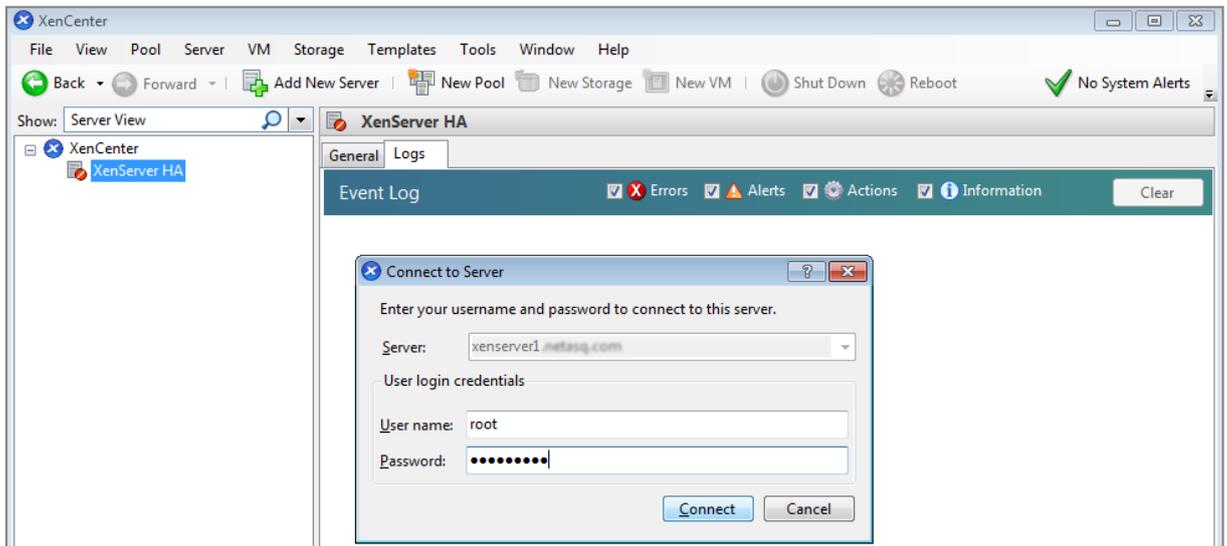


Once this is done, continue to the chapter [Activating the SNS EVA virtual firewall](#).

Deploying on a XenServer platform

1. Open XenCenter from your administration workstation.
2. Enter the login parameters for XenServer:
 - IP address/Name,
 - User name,
 - Password.
3. Click on **File > Import**.
4. Click on **Browse** and select the *.ova* installation file downloaded earlier.
5. Read and accept the conditions of use.
6. Complete the steps for the installation on Xenserver.

Once this is done, continue to the chapter [Configuring the SNS EVA virtual firewall](#).





Configuring the SNS EVA virtual firewall

i NOTE

The operations described below are not necessary for machines deployed over VMware if you have filled in the configuration form during deployment. If this is the case, continue to the chapter [Activating the SNS EVA virtual firewall](#).

1. Select and start up the virtual firewall.
2. Go to the administration console of the virtual firewall.
3. In the configuration wizard, choose your keyboard language.

```
#####
## 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. Enter a password for the administrator account and confirm it. Choose a complex password that follows the recommendations given by organizations such as the [ANSSI](#).

```
#####
## Change SRP/SSH password for admin ##
#####

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

5. The network settings of the interfaces appear (DHCP by default). If you change them, indicate the IP address, sub-network mask and default gateway.

```
#####
## Configure initial network connection ##
#####

Current network settings:
 1st interface (out): DHCP
 2nd interface (in): DHCP

Change 1st network interface (out) settings ? [y|N]: █
```

6. The wizard will ask if you wish to manage the firewall from its “out” interface. Press **Enter** to accept.

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

The SNS EVA virtual firewall now has a base network configuration.



Activating the SNS EVA virtual firewall

Your firewall must be activated so that you can assign an EVA model, permanent serial number, license and subscribed options to it.

Downloading the activation kit

1. In your [MyStormshield](#) user area, go to **Product > Product management**.
2. Browse the list of products until you identify the relevant product. Click on it.
3. On the right side of the **Downloads** section, select the desired version branch. It must match the version of the installation file downloaded earlier.
4. Click on the **Download the activation kit** link, then accept the download.

Importing the activation kit

1. In the virtual firewall's web administration interface, go to **Configuration > System > Maintenance, System update** tab.
2. Select the activation kit `[.maj]` downloaded earlier.
3. Click on **Update firmware**. The firewall will automatically restart.

Your SNS EVA virtual firewall is now deployed and activated.

You can continue to any of the following chapters:

- [Troubleshooting](#),
- [Further reading](#),
- [Appendix: Migrating a V/VS-VU model virtual firewall to an EVA model](#) if you are deploying an SNS EVA virtual firewall as part of migrating a V/VS-VU model firewall to an EVA model.



Troubleshooting

In this chapter, you will see some of the issues that occur most frequently.

The serial number of virtual firewall is still VMSNSX00Z0000A0.

The firewall has not been activated. Refer to the chapter [Activating the virtual SNS EVA firewall](#).

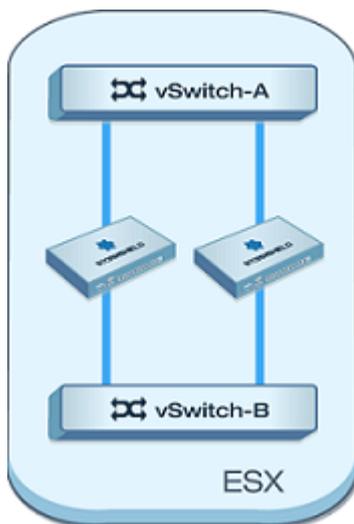
Some features on the virtual firewall are not available

Check the serial number of the firewall. If it is VMSNSX00Z0000A0, the firewall has not been activated. Refer to the chapter [Activating the virtual SNS EVA firewall](#). If the firewall has already been activated, check the details of its license in its web administration interface in **Configuration > System > License**.

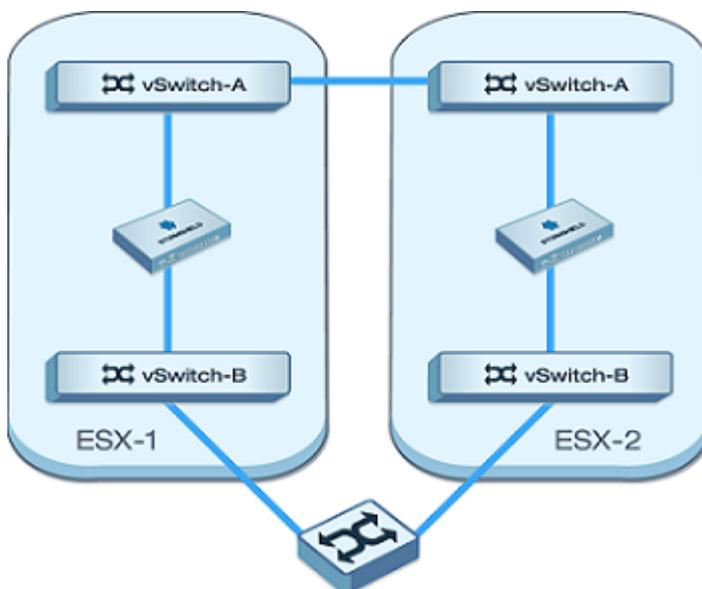
Issues arise on the vSphere hypervisor in high availability

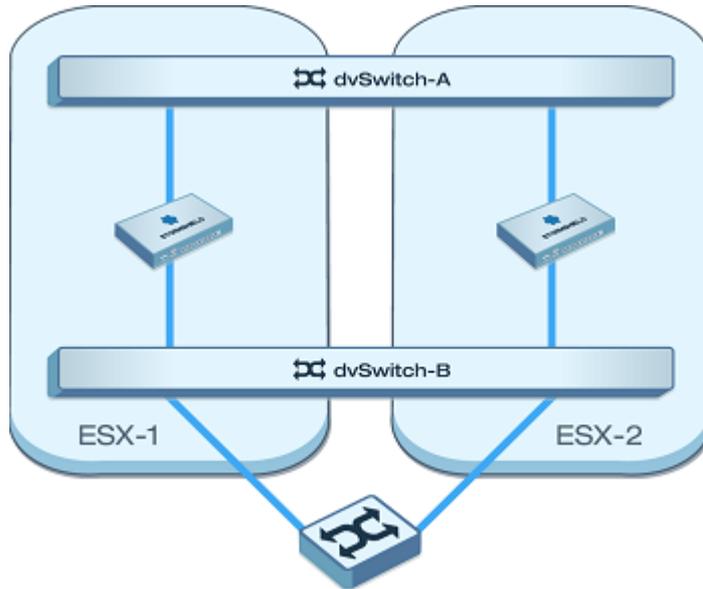
You may occasionally encounter issues when attempting to connect remotely to a high availability cluster in the following architectures:

Firewalls hosted on the same ESX server and connected to vSwitches:



Firewalls hosted on two separate ESX servers and connected to vSwitches:



**Firewalls hosted on two separate ESX servers and connected to dvSwitches:**

Thanks to VMWare tools, the virtual switch (vSwitch/dvSwitch) automatically learns the MAC addresses of appliances connected to these ports.

Since both members of a SNS EVA firewall cluster have the same MAC address by default, when there are network packets for a particular MAC address, the virtual switch always sends them only to the firewall bearing this address regardless of its status in the cluster (active or passive). Therefore, if the virtual switch (vSwitch/dvSwitch) sends packets to the passive firewall, these packets will be automatically ignored.

The solution is to delete the MAC addresses imposed in the configuration of both firewalls. Perform this operation:

From the firewall's web administration interface:

1. Go to **Configuration > Network > Interfaces, Advanced properties** tab.
2. In the **Physical (MAC) address** field, delete all the custom MAC addresses for the network interfaces of virtual firewalls.
3. Apply changes.

In the firewall's system console:

1. In the configuration file `/usr/Firewall/ConfigFiles/network`, delete all lines containing the entry `"MacAddress="`.
2. Next, type the commands `ennetwork` and then `hasync` in order to apply these changes and synchronize the active firewall's configuration with the passive firewall's configuration.

Depending on the network devices connected to the firewalls, and mainly according to their set ARP timeout values, more time may be required to restore connections when the roles of the firewalls are changed within the cluster (active/passive).



Further reading

You can find additional information and answers to your questions at the following links:

- [Technical note on high availability in SNS v4.](#)
- [Technical documentation on VPN topologies.](#)
- [SNS technical documentation website](#) (version release notes, user guides, technical notes, etc.).
- [Partner locator tool](#) if you need assistance on more complex configurations.
- [Stormshield knowledge base](#) (authentication required).
- [MyStormshield Online help.](#)



Appendix: Migrating a V/VS-VU model virtual firewall to an EVA model

A valid maintenance contract is required for the relevant V/VS-VU model before it can be migrated to an EVA model. Migration is free of charge on V/VS-VU models purchased before March 5, 2019.

Perform the following operations to migrate a model. Repeat these operations as many times as necessary to migrate several models.

Obtaining and registering a new EVA model

Get in touch with your Stormshield reseller or partner and provide them with the serial number of the V/VS-VU model that you would like to migrate. Follow the instructions given until you obtain the serial number of the EVA model and its registration password.

To migrate several V/VS-VU models, you must obtain as many EVA serial numbers as necessary. You can obtain the EVA serial numbers in a single request.

Once you have obtained the new EVA model, register it in your [MyStormshield](#) user area. For further information, refer to the guide on [Registering products](#).

Deploying the new EVA model and activating it

Go to the following chapters to perform the required operations:

1. [Downloading the installation file](#).
2. [Deploying the installation file in a virtual environment](#).
3. [Configuring the SNS EVA virtual firewall](#).
4. [Activating the SNS EVA virtual firewall](#).

Backing up the configuration of V/VS-VU models

Before you begin, take note of any major changes between the SNS version installed on the V/VS-VU model and on the EVA model. If required, adapt the configuration of the V/VS-VU model before backing it up.

Check the changes to behavior in the new version:

- For SNS 3.11 LTSB: refer to the section [Recommendations](#) in the version 3.11 LTSB release notes,
- For SNS 4.3 LTSB: refer to the sections [Points to note for updates from a 3.7 LTSB or 3.11 LTSB version](#) and [New firewall behavior](#) in the version 4.3 LTSB release notes,
- For the most recent SNS 4.x version: refer to the section [New firewall behavior](#) in the version 4 release notes.

Check the compatibility of the Stormshield client applications used (SSO agents, SSL VPN clients and VPN clients) with the new version. If any component is incompatible, these applications will stop functioning correctly. For more information, refer to the [Product life cycle guide](#).

To back up the configuration of the V/VS-VU model:



1. In the V/VS-VU model's web administration interface, go to **Configuration > System > Maintenance, Backup** tab.
2. Click on **Download the configuration backup**.

Restoring the configuration of the V/VS-VU model on the EVA model

1. In the virtual firewall's web administration interface, go to **Configuration > System > Maintenance, Restore** tab.
2. Select the backup file and click on **Restore the configuration from the backup file**.

NOTE

In a high availability (HA) firewall cluster:

1. Deploy a second EVA model firewall.
2. On the EVA model where the backup has been restored, configure the cluster (create the cluster and include the second EVA model).



STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2024. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.