GUIDE

STORMSHIELD NETWORK SECURITY
PAY AS YOU GO

SNS PAYG VIRTUAL FIREWALL DEPLOYMENT GUIDE

Product concerned: SNS 3.11.17 and later versions or SNS 4.3.9 and later versions

Document last updated: April 10, 2024

Reference: sns-en-pay_as_you_go_deployment_guide

Table of contents

Getting started

Welcome to the SNS PAYG virtual firewall deployment guide.

This document is intended for Stormshield partner resellers and integrators only.

SNS PAYG virtual firewalls have been designed for private cloud providers that offer hosted services and/or Internet access, either in the form of SaaS or IaaS. When you deploy them in your virtual infrastructure, you will be able to offer your clients a network security service that can be billed monthly based on the number and size of virtual firewalls used.

“Stormshield Network Security Pay As You Go” is referred to as “SNS PAYG” in the rest of this document.

IMPORTANT
This document relates only to SNS PAYG virtual firewalls. For physical SNS firewalls or virtual SNS EVA firewalls, refer to the specific **Installation guides**.

Requirements

The tables below set out all the technical requirements.

SNS versions

3.11.17 and later versions 4.3.9 and later versions

Hypervisors

You must be familiar with one of the virtual environments below before deploying an SNS PAYG 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	

Virtual machines must be able to access the Internet in HTTPS (port 443).

Use case

SNS PAYG virtual firewalls are mainly used in two cases: for the protection of access to hosted services, and the protection of users' Internet access. How they are used determines the required level of protection.

Protection of access to hosted services

As a service provider, you host your clients' servers and applications in your virtual infrastructure. When you deploy SNS PAYG, you secure your clients' connections to their resources in your datacenters:

- Connections by users in your clients' premises, and
- Connections by mobile users outside the premises.

In this case, only the VPN feature is necessary. Select **Standard** protection, which will protect user connections through a VPN.

Protection of users' Internet access

As an Internet service provider to your clients, you deploy SNS PAYG in your infrastructure to protect users who access the Internet through your datacenter.

In this case, full protection is necessary. Select **Premium** protection, which ensures protection of servers through features such as antivirus, Extended Web Control URL database, and vulnerability management.

Registering your SNS PAYG product

To register your SNS PAYG 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 gathered all this information, you can register your firewall in the MyStormshield personal area, where you can link your product to your MyStormshield user area. The registration process varies depending on whether you already have an user 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 Creating an account and registering a product.

You already have a MyStormshield user area

Register your product from your MyStormshield user area.

For further information, refer to the guide on Registering products.

Downloading the installation file

1. In your MyStormshield personal area, go to **Downloads** > **Downloads**.
2. In the various categories, select **Stormshield Network Security** > **Firmware** >, then **4.X** or **3.X** depending on the desired version branch.
3. In the **Stormshield Network Security - Firmware - V X.Y.Z** window, with X.Y.Z higher than or equal to 4.3.9 or 3.11.17, select the installation image in the desired format:
   - *kvm* for KVM platforms,
   - *openstack* for Openstack platforms,
   - *ova* for VMware platforms,
   - *vhd* for Microsoft Hyper-V platforms.
4. Save the file on your workstation.

Deploying the installation file on a platform

This procedure is an example based on a VMware platform. You must adapt it if you are using another virtual environment.

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.

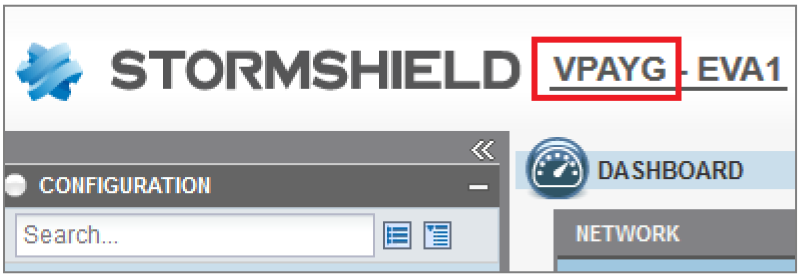
Activating the SNS PAYG virtual firewall

Downloading the activation kit

1. In your MyStormshield personal 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. Start the SNS PAYG virtual firewall. Its serial number by default is *VMSNSX00Z0000A0*.
2. In the virtual firewall's web administration interface, go to **Configuration** > **System** > **Maintenance**, **System update** tab.
3. Select the activation kit (*.maj*) downloaded earlier.
4. Click on **Update firmware**. The firewall will automatically restart.
5. Log in to its web administration interface and authenticate. When **VPAYG** appears in the upper banner, this confirms that you have an SNS PAYG firewall.



Creating the SNS PAYG virtual firewall template

Once the SNS PAYG firewall is initialized, you must create a template that you can duplicate later to create all your SNS PAYG virtual firewalls.

Configuring the firewall template

Edit the firewall’s configuration in order to create a template with the base configuration. For example:

- Edit the default filter policy to adapt it to your needs,
- Enable the NTP service to synchronize the time on the firewall,
- Enable the SSHD service if you wish to manage the firewall via SSH.

This list is not exhaustive. Enable all the services that your clients will need.

Deleting OVF env parameters (VMware only)

If you are using *OVF env* (vApp) properties, you are advised to reset their values so that firewalls created from the template will not inherit these values.

1. Open vSphere Client from your administration workstation.
2. Select your PAYG virtual machine and click on the **Configuration** tab in the panel on the right.
3. Select **Settings > vApp Options**. The *OVF env* parameters appear.
4. Click on **Edit** and clear all the values in the **Global configuration** and **Network interface** parameters.

Creating a backup of the virtual machine

We recommend that you create a backup of the virtual machine to anticipate changes that may be made to the template, e.g., version updates or changes to its base configuration.

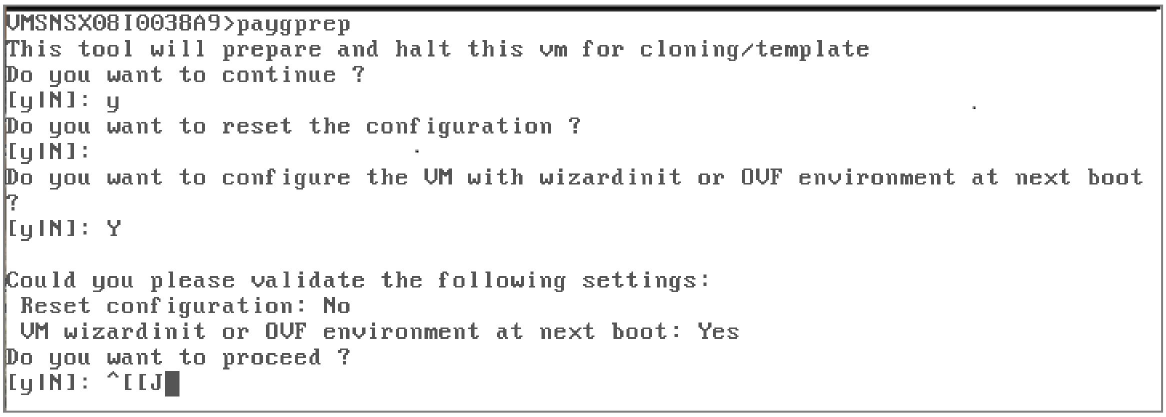
Converting the virtual machine to a PAYG template

Once you have finished configuring the virtual machine, you must convert it to a PAYG template

1. Access the firewall's console via the hypervisor or via an SSH client.
2. Run the command `paygprep`.
   You will be informed that the virtual machine will shut down at the end of the process.
3. When you see the question *Do you want to continue?*, answer *y* (Yes).
4. When you see the question *Do you want to reset the configuration?*, answer *n* (No), unless you wish to use a default configuration.
5. When you see the question *Do you want to configure the VM with wizardinit or OVF environment at next boot?*, answer *y* (Yes) if you wish to configure the network settings, host name, admin password and client ID of the new deployed machine when it boots.
   The summary of the settings that you have just defined will appear.
6. When you see the question *Do you want to proceed?*, answer *y* (Yes) if the information is correct.
   The virtual machine will start shutting down.

7. In your hypervisor, right-click on your PAYG virtual machine, and select the **Template** menu **> Convert to template** in vSphere or **Convert to template** in XenCenter and KVM. In Hyper-V, clone the virtual machine to create the template.

The virtual machine will be converted to the PAYG template. You can duplicate it whenever necessary.



```
VMSNSX08I0038A9>paygprep
This tool will prepare and halt this vm for cloning/template
Do you want to continue ?
[y|N]: y
Do you want to reset the configuration ?
[y|N]:
Do you want to configure the VM with wizardinit or OVF environment at next boot
?
[y|N]: Y

Could you please validate the following settings:
 Reset configuration: No
 VM wizardinit or OVF environment at next boot: Yes
Do you want to proceed ?
[y|N]: ^[[J
```

Deploying the SNS PAYG virtual firewall based on a template

Once you have created your SNS PAYG firewall template, you can deploy new machines based on it.

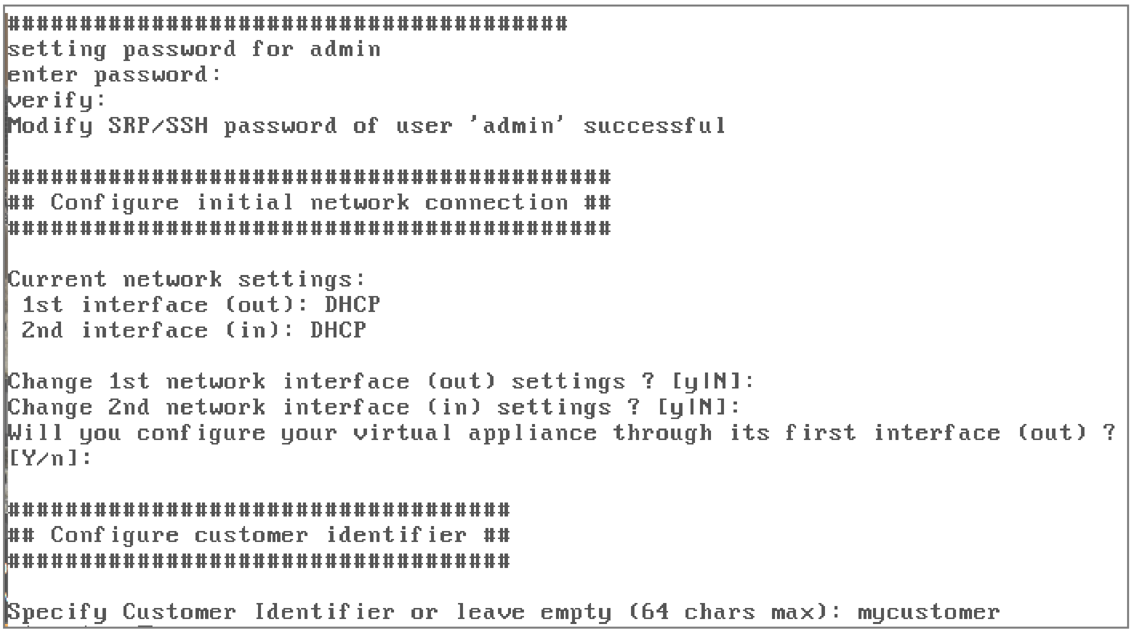
> **IMPORTANT**
> The virtual firewall must have Internet access so that it can enroll on the Stormshield Pay As You Go cloud service.

VMware environment

1. In vSphere Client, right-click on your template and select **New VM from this template**.
2. Name your SNS PAYG virtual firewall and select its location.
3. Select the calculation resources and storage. Do not select any cloning options.
4. Edit the parameters according to your needs: host name, customer ID, network parameters. Enter a Customer ID of your choice if you wish to associate this firewall with a particular client. This information will be provided together with the serial number in activity reports that will be sent along with the monthly invoice.
5. Click on **Finish** to confirm your settings.
6. Start up your virtual firewall.
   - **Once the network connection has been established**: the firewall will contact the cloud service to obtain an identity, a certificate and a license. This step will take several minutes. A message on the console will inform you when the firewall has been enrolled and that it will restart,
   - **If an enrollment error occurs**: check the Internet connection and restart the virtual firewall to start the enrollment process again.
7. As soon as the firewall is enrolled and restarted, it will have a new serial number, e.g., *VMSNSX08J0162B9-76DAA1B6*.

Other virtualization environments

1. Create a new SNS PAYG virtual firewall from a template (for XenServer and KVM) or a clone (for Hyper-V), and start it.
2. Open the console. A wizard will guide you through the configuration of your initial installation. You will be able to choose a password for the *admin* superuser, configure the network parameters for each interface detected, and specify a Customer ID.
   - **Once the network connection has been established**: the firewall will contact the cloud service to obtain an identity, a certificate and a license. This step will take several minutes. A message on the console will inform you when the firewall has been enrolled and that it will restart,
   - **If an enrollment error occurs**: check the Internet connection and restart the virtual firewall to start the enrollment process again.
3. As soon as the firewall is enrolled and restarted, it will have a new serial number, e.g., *VMSNSX08J0162B9-76DAA1B6*.



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

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

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

Change 1st network interface (out) settings ? [y|N]:
Change 2nd network interface (in) settings ? [y|N]:
Will you configure your virtual appliance through its first interface (out) ?
[Y/n]:

###################################
## Configure customer identifier ##
###################################

Specify Customer Identifier or leave empty (64 chars max): mycustomer
```

Managing the SNS PAYG virtual firewall

SNS PAYG virtual firewalls can be managed via the web administration interface. If you are managing a large number of firewalls, use the Stormshield Management Center server instead, or an orchestrator combined with the NSRPC API.

Use your hypervisor to change the virtual machine's system settings.

Looking up the virtual firewall's dashboard in the web administration interface

1. Log in to the virtual firewall's web administration interface (https://*firewall_IP_address*/admin). If it is configured in DHCP, note down its IP address in the console.
2. When **VPAYG-EVA** is shown in the upper banner, this means that monthly billing is based on the EVA model, which depends on the virtual machine’s resources.
3. The **Properties** widget in the **Dashboard** shows general information about the firewall.

This table presents the technical requirements of each EVA model:

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

An EVA must have at least 1 GB of memory. You are advised to set the aside at least 2 GB of memory if you use the antivirus and sandboxing features frequently.

Changing the amount of memory on the virtual firewall

You can increase the amount of memory on the SNS PAYG virtual firewall to switch to a different virtual firewall model so that you can operate more processors to manage more users.

Do note that pricing conditions will change when you increase memory. For further information, please contact your Stormshield sales representative.

> **IMPORTANT**
> You are advised against reducing the memory on the virtual firewall. However, if you choose to do so, ensure beforehand that the new limits applied will be compatible with the existing configuration.

1. In the web administration interface, go to **Configuration** > **System** > **Maintenance** > **Configuration tab** and click on **Shut down the firewall**.
2. Wait until the virtual firewall shuts down.
3. In your hypervisor, go to the virtual machine's properties and change the memory, e.g., from *1024 MB* to *3072 MB*. You may also add processors if you need them.
4. Restart the virtual machine.

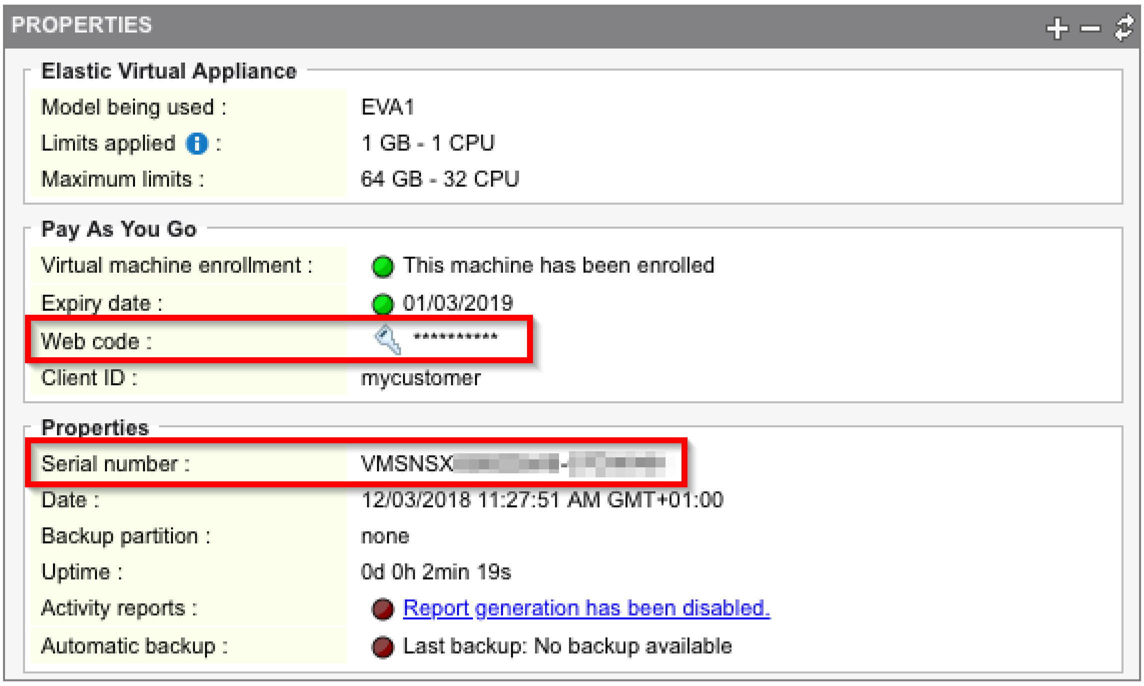
5. Log in again on to the web administration interface of the virtual firewall.
   On the **Dashboard**, the **Properties** widget shows the new virtual firewall model (e.g., VPAYG-EVA2 for 3 GB of memory) as well as its new limits. For further information on each model's limits, refer to the section Looking up the virtual firewall's dashboard in the web administration interface.

Registering the virtual firewall on MyStormshield

From your MyStormshield user area, you must register your SNS PAYG virtual firewall to access technical support and cloud backup services.

Fill in the required information until the firewall is registered. The serial number and password (Web code) will be indicated in the **Dashboard** of the firewall's web administration interface, under the **Properties** widget.

For further information, refer to the guide on Registering products.



Elastic Virtual Appliance

Model being used :	EVA1
Limits applied :	1 GB - 1 CPU
Maximum limits :	64 GB - 32 CPU

Pay As You Go

Virtual machine enrollment :	● This machine has been enrolled
Expiry date :	● 01/03/2019
Web code :	***********
Client ID :	mycustomer

Properties

Serial number :	VMSNSX[redacted]-[redacted]
Date :	12/03/2018 11:27:51 AM GMT+01:00
Backup partition :	none
Uptime :	0d 0h 2min 19s
Activity reports :	● Report generation has been disabled.
Automatic backup :	● Last backup: No backup available

Further reading

Additional information and answers to some of your questions may be found in the **Stormshield knowledge base** (authentication required).

documentation@stormshield.eu

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