

STORMSHIELD



INSTALLATION AND FIRST-TIME CONFIGURATION OF AN SNS FIREWALL GUIDE

Versions 3 and 4

Document last updated: February 13, 2024 Reference: sns-en-installation_and_first_time_configuration_guide



Table of contents

Change log	. 2
Getting started	. 3
Reference architecture Reminders regarding security mechanisms	3 3
Registering the firewall Finding the firewall's registration password and serial number Registering the firewall from the MyStormshield personal area You do not have a MyStormshield account You already have a MyStormshield account	5 5 5 5 5
Installing and physically connecting the firewall Installing the firewall Physically connecting the firewall to a client workstation Starting the firewall	. 7 . 7 . 7 . 7 . 7
Making the initial connection on the firewall	8
Accessing the firewall administration interface Understanding the graphical user interface Upper banner Left menu Active window Lower window Changing the "admin" account password	8 9 10 10 10 10
Installing the firewall license	12
Retrieving the firewall license file Installing the license on the firewall	12 12
Updating the firmware	14
Identifying the SNS version currently installed Downloading the update file Installing the update	14 14 15
Configuring the firewall's network settings and finalizing its installation	16
Configuring the firewall's interfaces Configuring the in interface Configuring the out and dmz1 interfaces Deleting the bridge Connecting the firewall to the Internet Physically connecting the firewall to the Internet access device Configuring the default gateway Updating the modules on the firewall	16 16 17 17 18 18 18 18 19
Connecting the firewall to the web server Physically connecting the firewall to the web server Creating a network object that represents the web server	20 20 20
Configuring the security policy	21
Configuring the URL filter policy	21 21







Configuring the URL filter policy	
Configuring the filter and NAT policy	22
Choosing a filter and NAT policy	
Configuring the filter policy	
Configuring the NAT policy	
Testing the configuration and backing it up	
Further reading	





Change log

Date	Description
February 13, 2024	- Section "Making the initial connection on the firewall" modified
September 12, 2022	- Sections "Making the initial connection on the firewall", "Installing the firewall license", "Updating the firmware" and "Configuring the URL filter policy" modified - Cosmetic improvements
June 23, 2022	- Cosmetic improvements
Ocrober 08, 2021	- New document







Getting started

Welcome! In this guide, we will walk you through the installation and first-time configuration of an SNS firewall, from the moment you receive your firewall up to the initial configuration from its administration interface.

This guide is a supplement to the *Product presentation and installation guide* and the *Quick Installation Guide* provided with your firewall. Refer to the **Guides** page to find the relevant version.

In this document, Stormshield Network Security is referred to in its short form: SNS.

IMPORTANT

This document relates only to physical SNS firewalls. Specific **installation guides** are available for virtual firewalls such as EVA or PAYG models.

Reference architecture

As there are many configuration possibilities, this guide presents several operations that you can perform on your firewall. Some of them work in all situations, while others work in an architecture that serves as an example in this guide. Use these examples by adapting them to your requirements.



For this architecture, the configuration of the firewall must meet the following requirements:

- Hosts connected to the "in" network must be able to access:
 - The "Internet" via DNS, HTTP and HTTPS. Their access must go through URL filtering.
 - The internal web server (protected by the firewall) via HTTPS.
- The "Internet" must be able to reach the internal web server (protected by the firewall) via HTTPS.

Reminders regarding security mechanisms

Security mechanisms are in place to guarantee the integrity of the firewall that you have received. We recommend that you check the following items as soon as you receive your firewall.



- Check that the cardboard box containing the firewall is sealed with one or several *STORMSHIELD QUALITY SEAL*(s). Ensure that these seals have not been tampered with.
- Using the identification labels on the firewall's cardboard box, ensure that the model you received is the model that you ordered.
- Ensure that the "WARRANTY VOID IF REMOVED" label on your firewall has not been tampered with.

NOTE

For more information about these mechanisms, refer to the *Product presentation and installation guide*, in the chapter **Upon receiving your firewall**.







Registering the firewall

After registering your firewall, you have to activate its Stormshield maintenance contract. If the firewall is not registered within three months from the billing date, it will be automatically activated.

Finding the firewall's registration password and serial number

To register your firewall, you will need its registration password and serial number (SN). You can find these on the label pasted on the firewall.



Registering the firewall from the MyStormshield personal area

Once you have gathered all this information, you can register your firewall in the MyStormshield personal area, where you can associate your firewall with your MyStormshield account. The registration process varies depending on whether you already have an account.

You do not have a MyStormshield account

Your firewall will be registered when your account is created. To do so, go to the connection page of the MyStormshield personal area and click on **Create an account/register a product**.

Next, continue according to the option that applies to you:

- Stormshield client and end user:
 - 1. **Create a new client account.** Complete the steps until the account is created and the firewall is registered.
- Stormshield partner and reseller:
 - 1. Create a new partner account.

Complete the steps until the partner account is created. During these steps, you will not be able to register your firewall on this account.

2. Next, create a new client account.

Go back to the connection page of the MyStormshield personal area and start creating a new client account.

Complete the steps until the account is created and your firewall is registered. Ensure that you set up authorization for co-management to allow your partner account to co-manage your client account.

For further information, refer to the guide on Creating an account and registering a product.





You already have a MyStormshield account

- 1. Log in to your MyStormshield personal area.
- 2. Go to Product > Register a product.
- 3. Click on Register SNS product.
- 4. Fill in the required information until the firewall is registered.

If your company does not appear in the **Associated company** field and you are a Stormshield partner and reseller, you probably do not yet have:

- A client account allowing you to register products,
- Authorization for co-management between your client and partner accounts.

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







Installing and physically connecting the firewall

Start with the installation of your firewall. This step will allow you to access its administration interface so that you can configure it.

🚺 NOTE

Specific features may vary depending on your firewall model. More information relating to this chapter can be found in the *Product presentation and installation guide* and *Quick Installation Guide* provided with your firewall.

Installing the firewall

- Install your firewall in a suitable location, such as a server room or restricted-access office. Use a special assembly system if necessary.
- Plug your firewall into a power supply unit with the right voltage. If possible, choose a connection to a UPS (uninterruptible power supply) device.
- Hire a qualified electrician to install models connected to a DC mains supply.

Physically connecting the firewall to a client workstation

- Use an Ethernet cable to link your firewall's internal port ("IN" in our example) to your client workstation or local network on which the client workstation is connected.
- The device on which the firewall is connected must be configured to automatically obtain an IP address (via DHCP), or have a static IP address that belongs to the firewall's network 10.0.0.0/8 (except for 10.0.0.254, which is already assigned to the firewall).
- Do not immediately connect your firewall to your Internet access device. Wait until you have configured the firewall's network settings.

Starting the firewall

- Once all the devices are connected, start your firewall.
- Wait while it finishes its startup sequence. Do not unplug it during this phase.





Making the initial connection on the firewall

Now that your firewall is installed and running, you can connect to it.

Accessing the firewall administration interface

- 1. Using a web browser on the client workstation, go to *https://10.0.0.254/admin*. Refer to the **Product Life Cycle** guide to see the list of supported web browsers.
- 2. A warning message appears, indicating that the visited domain is invalid. This is normal because the certificate that the firewall uses is self-signed. Continue to the site.
- 3. The page allowing the connection to the firewall's administration interface appears. Enter "admin" as the login and password, then log in. By default, If you enter the wrong login or password four consecutive times, you will need to wait for a minute before you can authenticate again. If you attempt to authenticate again before the minute is up, the waiting time will be extended by another minute, up to a maximum of 10 minutes. The number of tries and waiting time can be configured. For more information, refer to the Firewall administration tab section in the v4 or v3 user manual in the SNS version used.

The administration interface appears. Its layout varies according to the pre-installed version of SNS.

A STORMSHIELD V425									e admin	n 🔻	
Network Security	MONITORING	CONFIGURATION	myfirewall							RESTRICTED ACCESS	?
*- «											
Ch DASHBOARD	CA DASHBUARD										٨
🗎 AUDIT LOGS -	NETWORK				PROTECT	ION					Î
Search					Date	Mess	Action	Priority ↓	Source	Destination	
All less		<u> </u>	2			startup (1)					
All logs				Interface up: em0 (1)							
Network traffic					Interface ■	up: em1 (1))				
Alarms	PROPERTIES										
Web	Name:	myfirewall									
Vulnerabilities	Model:										
E-Mails	Serial number:										
VDN	Version:										
VEN	Uptime:										
System events	Date:										

Administration interface of an SNS firewall in version 4

Administration interface of an SNS firewall in version 3

🐳 STORMSHIELD	r 3	nyfirewall 3.7.20	Admin P Read/Write Restricted acces	<u>s to log</u>	<u>s</u>	/	×?(•
						Help us to Improve	the application Download SN Real-Time Moi	nitor
CONFIGURATION -	DASHBOARD						·····································	343
Search × 🔳 🛅	NETWORK						$rac{}{}_{\pi}$	^
C DASHBOARD	1	2						
🚯 SYSTEM	-							
B NETWORK								
OBJECTS								
USERS	ALARMS						≠ * + - \$ ×	
SECURITY POLICY	Date 👻	Action	Priority	Sou Sou	urce Des	Destination	Message	
	02:15:59 PN	1	🎑 Minor				Interface up: em0	
AFFEICATION PROTECTION	02:15:59 PN	1	🎑 Minor				Interface up: em1	
VPN	02:15:59 PN	1	🌋 Minor				Firewall startup	





Understanding the graphical user interface

The window consists of 4 zones:

- 1. The upper banner, which presents the **Monitoring** and **Configuration** views and provides information on the status of the firewall;
- 2. The menu on the left, which provides access to the various modules on the firewall;
- 3. The active window of the selected module;
- 4. The lower window, which shows errors, warnings, commands and notifications.

The administration interface does not have the **Monitoring** and **Configuration** tabs in version 3, as all modules are grouped in the menu on the left.

The stormshield v47.1 Network Security Monitoring con	IFIGURATION EVA1	e adm Ca wen Ca coss	n <u>ING</u> <u>RESTRICTED ACCESS</u>
C DASHBOARD			
AUDIT LOGS - NETWORK		PROTECTION	^
Search		Date Message Action Priority ↓ Source	Destination
All logo	1 2		
Airiogs		Interface up: em0 (1)	
Network traffic		Interface up: em1 (1)	
Alarms			
Web Name:	renkoronon		
Vulnerabilities Model:	EVA1		
E-Mails EVA model:	EVA1		
EVA memory capacity:	1 GB (Minimum 1 GB - Maximum 2 GB) ()		
VPN Number of CPUs on the EVA:	CPU 1 (Maximum CPU 1) ()		
System events Serial number:	WARRANG BUILD		
Filter Version:	4.7.1		
Uptime:	2m 47s		
Sandboxing Date:	12/20/2023 10:12:16 AM		
Users Maintenance expiry date:	11/12/2025		
al reports +		MESSAGES	
MONITORING +		Information IPv6 is enabled	
10:12:18 AM Dashboard: MONITOR LOG ALADM gme	v		×
4 ptio 10:12:18 AM Dashboard: MONITOR SYSTEM 6ms			
Clear log			
Copy 10:12:18 AM Dashboard: SYSTEM UPDATE CHECK 9ms			
10:12:18 AM Dashboard: MONITOR ANTIVIRUS 17ms			

Upper banner



In the upper banner, the following items are displayed from left to right (the order may vary or certain items may not be available in version 3):

- The version number of your firewall,
- Two tabs that show two firewall views: Monitoring and Configuration,
- The model number of your firewall and its name: scroll over the name to see the serial number,
- A flickering icon that shows whether the status of your firewall requires your attention: scroll over the icon to show monitored items and their status,
- · Your user name: click on it to go to your preferences or to log in,
- · Your read and write permissions: scroll over the permissions to see more information,
- Your permissions to access logs: if you are in restricted access mode, click on the item to request full access,
- The 🕻 icon, which opens the page in the online SNS user manual relating to the module you are viewing.





Left menu

The menu on the left provides access to various modules corresponding to available features. Modules are grouped by category. You can:

- Collapse the menu by clicking on K,
- Expand and collapse categories by clicking on them,
- Set modules as favorites by clicking on the kinetic icon that appears by scrolling over the name of a module,
- Quickly access favorite modules by clicking on the 📼 icon at the top of the menu.

If modules are grayed out in the menu, this may mean that:

- You have not subscribed to the required license and therefore cannot access them.
- The user account that you used for logging in does not have the necessary permissions to access these modules.

The modules in the menu vary depending on whether you are in **Monitoring** or **Configuration** view.

When you perform searches through the search bar, both the name of the module and its content will be part of the search.

Active window

The content of this window varies according to the module displayed.

Lower window

The lower window shows errors, warnings, commands and notifications. You can:

- Show or hide this window by clicking on the arrow in the middle
- Configure the messages that appear by clicking on **Options**.

Changing the "admin" account password

For security reasons, you must change the default password of the "*admin*" user during the initial connection to the firewall.

- 1. If the firewall is in version 4, go to the **Configuration** tab located in the upper banner. Changes to the configuration can be made in this tab.
- 2. From the menu on the left, go to **Configuration > System > Administrators,Administrator account** tab.
- 3. If the firewall is in version 4, enter admin in the Old password field.
- 4. Enter the new password and confirm it. Take note of the following points:
 - A progress bar will show the strength of the password that you typed. Use a combination of uppercase and lowercase characters to increase its level of security.
 - The password cannot contain:

" <tab> <space>

5. Click on Apply , then Save.

The new password must be used at the next connection.

Administration interface of an SNS firewall in version 4







SNS - INSTALLATION AND FIRST-TIME CONFIGURATION OF AN SNS FIREWALL GUIDE - V 3 AND 4 MAKING THE INITIAL CONNECTION ON THE FIREWALL

A stormshield v4.25 Network Security	MONITORING	CONFIGURATION	myfirewall	e admin writing Logs: restricted access	?
*- «					
CONFIGURATION -	₩ SYSTEM / ADM	AINISTRATORS			
Search 🗶 🖉	ADMINISTRATORS	ADMINISTRATOR AC	COUNT TICKET MANAGEM	IENT	
밖 SYSTEM	Authentication				
Configuration	Old password:				
Administrators	Password:				
License	Confirm password:				
Maintenance			Password strength		

Administration interface of an SNS firewall in version 3

崇 STORMSHIEL	_C	myfirewall 3.7.20	admin <u>ReadWrite</u> <u>Restricted acc</u>	ess to logs	×? ©
	<u>~</u>				Help us to improve the application Download SN Real-Time Monitor
Search × 🗉 🗎	^	ADMINISTRATORS ADMINISTRATOR		ET MANAGEMENT	
SYSTEM		Password:			
Configuration Administrators		Confirm password:			
License	1		Passv	word strength	
Maintenance		Exports			







Installing the firewall license

When the permanent license is installed on your firewall, it replaces the temporary license. This will activate the features and options subscribed in the firewall's maintenance pack.

Retrieving the firewall license file

- 1. Log in to your MyStormshield personal area.
- 2. Go to Products > Product management.
- 3. In the **Product management** area, identify your firewall with the help of the **Maximize** and **Minimize** buttons, or by entering its serial number in the search zone. Click on it.
- 4. In the **Downloads** section on the right, click on the link next to **License file**. Accept the download of the *.licence* file.

DASHBOARD C PRODUCT MANAGEMENT	8	
Management of your products	SN210W Registered on: 2020-07-08	
Find below all information regarding your	Download description of maintenance and options	Follow up on a case
Stormshield products.	Customized description	•
SearchBox: SN210W	Description:	Downloads
STORMSHIELD Minimize		
UTM SN210W Minimize		License file: SN210W
SN210W		You can find available firmware through the
• VM EVA Maximize		Firmware menu on the left
All V Download all licenses	ii.	Services
CSV license extract		General

Installing the license on the firewall

- 1. Go to the firewall's administration interface at *https://10.0.0.254/admin*.
- 2. Go to Configuration > System > License.
- 3. In the Install from file area, select the license file downloaded earlier.
- 4. Click on Install the license file, then wait while the license installs.
- 5. The firewall may need to be restarted to activate some of the features in the new license, or to upgrade the firewall model. A warning will appear in the upper banner if this is the case. To restart the firewall, go to Configuration > System > Maintenance, Configuration tab, and click on Restart the firewall.

Page 12/31





Administration interface of an SNS firewall in version 4

	GENERAL LICENSE DETAILS									
	Search for a new license Install the new license									
	Local firewall date: Friday 19th August 2022									
The The Icense is temporary. Please register your firewall in order to obtain the permanent license.										
	Last check for license updates performed	Last check for license updates performed on:Friday 19th August 2022								
	Z Temporary license will expire in 864 days, on Tuesday 31st December 2024.									
	Maintenance will expire in 864 days, on T	uesday 31st December 2024.								
	The Stormshield Vulnerability Manager o	ption has not been subscribed.								
	The advanced antivirus option has not be	en subscribed.								
	The Extended Web Control option has no	t been subscribed.								
	The sandboxing Breach Fighter option ha	is not been subscribed.								
	The industrial option has not been subsc	ribed.								
	Install license									
	License file :									
Search for a new license Install the new license Local firewall date: Friday 19th August 2022 The 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 :										

Administration interface of an SNS firewall in version 3

GENERAL LICENSE DETAILS									
Search for a new license 🧹 Inst	🔍 Search for a new license 💚 Install the new license								
Local firewall date: Friday 19th	Local firewall date: Friday 19th August 2022								
🔴 The 📲 👘 🖬 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 (lays, on Tuesday 31st December 2024.								
The Stormshield Vulnerability M	anager option has not been subscribed.								
The advanced antivirus option h	ias not been subscribed.								
The Extended Web Control opti	on has not been subscribed.								
The sandboxing Breach Fighter	option has not been subscribed.								
 Install from file 									
License file :									
	Install the license file.								





Updating the firmware

By updating your firewall to a more recent version, it will benefit from the latest features available and the latest functional patches and bug fixes.

Identifying the SNS version currently installed

- 1. Go to the firewall's administration interface at https://10.0.0.254/admin.
- 2. Locate the SNS version number in the upper banner.

Administration interface of an SNS firewall in version 4

A STORMSHIELD V425								() ac	lmin 🔻	
Network Security	MONITORING	CONFIGURATION	myfirewall						GS: RESTRICTED ACCESS	?
*- «										
C DASHBOARD	UN DASHBUARD									^
🗎 AUDIT LOGS 🛛 🗕	NETWORK			PROTECT	ION					
Search				Date	Mess	Action	Priority ↓	Source	Destination	
All loas		1	2	Firewall s	tartup (1)					_

Administration interface of an SNS firewall in version 3

STORMSHIELD)	myfirewall 3.7.20	Admin <u> <i>ReadWrite</i> Restricted access to logs </u>	× ? E
				Help us to improve the application Download \$N Real-Time Monitor
CONFIGURATION -	DA SHBOARD			수 — 參 🕮 4
Search × 🔳 🗎	NETWORK			
🝘 DASHBOARD		1 2		
🚯 SYSTEM				
& NETWORK				

Downloading the update file

- 1. Log in to your MyStormshield personal area.
- 2. Go to Downloads > Downloads.
- 3. Select **Stormshield Network Security** from the suggested categories, then **Firmware**. If necessary, select a version branch as well, such as 4.X, to narrow down the list.
- 4. Locate the version that you want to install on your firewall. To do so:
 - Refer to the version release notes to find out what the SNS versions contain.
 - Ensure that the new version is compatible with the model of your firewall. An intermediate version may be required in some cases.
 - If a version has several patch versions, always choose the most recent so that you benefit from the latest functional patches and bug fixes.
 - Use a version that has not already expired. For more information, refer to the Network Security & Tools Product lifeycle document.
- 5. To choose the desired version, click on the name that matches your firewall model to download its update file. Accept the download of the *.maj* file.
- 6. You can check the integrity of binary files by using the command sha256sum <filename> in Linux or CertUtil -hashfile <filename> SHA256 in Windows. Next, compare the result with the hash indicated in MyStormshield, by clicking on Show in the SHA256 column of the .maj file in question.





DASHBOARD DOWNLOADS 🛞						
STORMSHIELD NETWORK SECURITY STORMSHIELD DATA SECURITY STORMSHIELD ENDPOINT SECURITY STORMSHIELD VISIBILITY CENTER NETA SQ	ADMINISTRATIO CENTRALIZED M EVENT ANALYZE FIRMWARE MANAGEMENT O SSO AGENT TOOLS VPN CLIENT VPN SSL	NN SUITE IANAGER ER CENTER - SMC	8	4.X 3.X 3.7 - LTSB 2.X 1.X		95
STORMSHIELD NETWORK SECURITY - FIRMW	/ARE - V 4.1.3				Ρ	ublished 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	maj		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
					84M	Dieplov
Virtual Image for EVA1, EVA2, EVA3, EVA4, EVAU, VPAY	G	Firmware	openstac	N	0-411	Display
Virtual Image for EVA1, EVA2, EVA3, EVA4, EVAU, VPAY Virtual Image for EVA1, EVA2, EVA3, EVA4, EVAU, VPAY	G	Firmware Firmware	openstac ova		87M	Display

Installing the update

- 1. In the firewall administration interface, go to **Configuration > System > Maintenance**, **System update** tab.
- 2. Select the update file downloaded earlier.
- 3. Click on **Update firmware**, then wait while the update installs.

Administration interface of an SNS firewall in version 4

SYSTEM UPDATE	BACKUP	RESTORE	CONFIGURATION
Available updates			
-			
No update available			
Q Check for new	updates		
System update			
-,			
Select the update:			
			C Update firmware
—	erties		

Administration interface of an SNS firewall in version 3

SYSTEM UPDATE	BACKUP	RESTORE	CONFIGURATION
Available updates	:		Check for new updates
			No update available
Select the update :			Select an update file
			Save the active partition on the backup partition before updating the firewall
			🗘 Update firmware
$- \bigtriangledown$ Advanced pr	roperties –		





Configuring the firewall's network settings and finalizing its installation

You can now configure your firewall's network settings and finalize its installation.

From this chapter onwards:

- All operations are based on our reference architecture.
- Operations are performed in version 4. They can also be performed in version 3 with a few adaptations as the administration interface may be different.
- Even when it is not mentioned in the procedures, all operations must be performed when the user is logged in to the firewall administration interface.

💡 TIP

For more information about the modules of the firewall administration interface, refer to the v4 or v3 user guide in the SNS version used.

Configuring the firewall's interfaces

Configuring the in interface

- 1. Go to Configuration > Network > Interfaces.
- 2. Select the in interface, then click on Edit.
- 3. In the General tab, fill out the information in the Address range area:
 - Address range field: select Dynamic / Static.
 - IPv4 address field: select Fixed IP (static).
 - In the grid: click on Add, and enter 192.168.2.1/24.
- 4. Click on **Apply** to confirm.

The connection to the firewall will then be lost. To continue, use the new IP address to connect to the firewall. If the device connected to the firewall uses manually entered IP settings, change them so that they belong to the new sub-network of the *in* interface.

NETWORK / INTERFACES				
🔍 Enter a filter 🛛 🖈 🖉 📔 🛃	🖞 Edit 🝷 🕂 Add 👻 🗶 Delete 🔀 Monitor 🖾 Go to monitoring 👁 Check usage			
Interface	S IN CONFIGURATION	>		
□ "□" bridge	GENERAL ADVANCED PROPERTIES			
m dmz1	Address range			
in 🕂 🛃	Address range: O Address range inherited from the Dynamic / Static bridge			
	IPv4 address: O Dynamic IP (obtained by DHCP) Fixed IP (static)			
	+ Add × Delete			
	Address/ Mask Comments			
	192.168.2.1/24			





Configuring the out and dmz1 interfaces

- 1. Select the *out* interface and click on Edit.
- 2. In the General tab, fill out the information in the Address range area:
 - Address range field: select Dynamic / Static.
 - IPv4 address field: select Fixed IP (static).
 - In the grid: click on Add, and enter 203.0.113.1/24.
- 3. Select the dmz1 interface, then click on Edit.
- 4. In the General tab, fill out the information in the Address range area:
 - Address range field: select Dynamic / Static.
 - IPv4 address field: select Fixed IP (static).
 - In the grid: click on Add, and enter 172.16.1.1/24.
- 5. Click on Apply to confirm.

NETWORK / INTERFAC	DES					
Q Enter a filter	* * 0 4	Edit 🔹 🕂	Add - X Delete	🔠 Monitor 🛛 🖥	🛱 Go to monitoring 👁	Check usage
Interface		Port	Туре	Status	IPv4 address	Comments
m 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	
ា្ម bridge			Bridge		DHCP	
			~			
VERIFICATION OF THE CONF	IGURATION					
😑 Warning bridge	Bridge bridge consis	sts of 0 interf	aces			

Deleting the bridge

- 1. Select the remaining bridge, click on Delete and confirm.
- 2. Click on Apply to confirm.

As a result, the *in*, *out* and *dmz1* interfaces remain with a static IPv4 address.

NETWORK /	INTERFACES	1								
Q Enter a filter		2 C 4	🛃 Edit 👻 🚽	H Add 🔻	× Delete	Monitor	🖏 Go to i	monitoring	Check	k usage
	Interface		Port	Туре		Status		IPv4 address		Comments
m out			1	Ethernet, 1	Gb/s		1	203.0.113.1/2	24	
in 👘		•	2	Ethernet, 1	Gb/s			192.168.2.1/2	24	
🖶 dmz1			3	Ethernet, 1	Gb/s			172.16.1.1/24	Ļ	







Connecting the firewall to the Internet

Physically connecting the firewall to the Internet access device

Use an Ethernet cable to link your firewall's "External" (OUT) port to your Internet access device.

Configuring the default gateway

Once the default gateway is configured, the firewall will know where to send packets that must leave for the public network (Internet).

Creating a network object that represents the default gateway

🚺 NOTE

If the *out* interface on your firewall retrieves an IP address from a DHCP server, once it obtains a DHCP lease, the network object *Firewall out router* will be automatically created. If this is how your firewall was configured (different from our example), continue to the next section **Setting the default gateway** without creating a new object.

- 1. Go to Configuration > Objects > Network.
- 2. Click on Add and ensure that you are in the Host tab.
- 3. Give the object a name (my_gateway in our example).
- 4. Enter the IPv4 address of the default gateway and set its DNS resolution parameters (*None (static IP)* in our example). The MAC address is not required.
- 5. Click on **Create** to confirm.

CREATE AN OBJECT					
🖪 Host					
FON DNS name (FQDN)	Object name:	my_gateway		Q	
	IPv4 address:	10000			
	MAC address:	01:23:45:67:	89:ab (optional)		
Address range	Resolution				
🥸 Router	Name (statis ID)		_	Automotio	
Group	 None (static IF) 			Automatic	
IP Protocol	Comments:				
🖞 Port	Comments.				
11 Port group					
Region group					
(B) Time object					
			× CLOSE	+ CREATE AND DUPLICATE	+ CREATE





Setting the default gateway

- 1. Go to Configuration > Network > Routing.
- 2. In the **IPv6 static routes** tab, under **General configuration**, select the object that represents the default gateway (*my_gateway* in our example).
- 3. Click on Apply.

NETWORK / ROUTING									
IPV4 STATIC RC	IPV4 STATIC ROUTES IPV4 DYNAMIC ROUTING IPV4 RETURN ROUTES								
General									
Default gateway	(router):	my_gate	way	v 85+					
STATIC ROUTES									
Searching		+ Add X Delet	te						
Status ≞▼	Destination net	work (host, network	Interface	Address range	Gateway	Comments			
		×	CANCEL	✓ APPLY					

Updating the modules on the firewall

Now that you have an Internet connection, ensure that the modules on the firewall are up to date.

- With the **Active Update** module, the various modules on the firewall can be automatically updated whenever the firewall is connected to the Internet.
- You can manually launch these updates or track them in **Monitoring > Monitoring > System**, in the **Active Update** section.

AL-TIME HISTORY						
lapse all Expand all + A DHCP client	Add a column - Rer 4h 42m 9s	nove a column 0.0% used	••	▲ Active Update		<u>Go to monitoring con</u>
vatchdog service	4h 42m 6s 4h 42m 17s	0.0% used 0.0% used	· · · · ·	So to Active Update configuration	C Run all updates a	gain
System monitoring service	4h 42m 19s	0.0% used		Name	Status	Last update
/eb portal (administration, VPN S	SSL 4h 42m 8s	0.0% used	· •	Antispam DNS blacklists (RBL)	\rm Unavailable	
SQ monitoring	4h 42m 8s	0.0% used	••	IPS: contextual protection signatures	\rm Unavailable	
IRL filtering service	4h 42m 13s	0.0% used	••	IPS: custom contextual protection sign	O Disabled	
eolocation, IP reputation and ho	st r 4h 42m 17s	0.0% used	• • • •	Antivirus: ClamAV antivirus signatures	\rm Unavailable	
				Antispam: heuristic engine	\rm Unavailable	
				Vulnerability Manager	\rm Unavailable	
				Root Certification Authorities	C Running	03:16:35 PM
				Geolocation / Public IP reputation	💙 Up to date	03:16:39 PM





Connecting the firewall to the web server

Physically connecting the firewall to the web server

Use an Ethernet cable to link the port that your firewall's *dmz1* interface uses to your web server.

Creating a network object that represents the web server

This object is required so that rules involving the web server can be configured in the firewall's security policy - this will be seen in our example.

- 1. Go to Configuration > Objects > Network.
- 2. Click on Add and ensure that you are in the Host tab.
- 3. Give the object a name (*srv_web_private* in our example).
- 4. Enter the IPv4 address of the web server and set its DNS resolution parameters (*172.16.1.5* and *None (static IP)* in our example). The MAC address is not required.
- 5. Click on **Create** to confirm.

CREATE AN OBJECT				
🖪 Host				
FOON DNS name (FODN)	Object name:	srv_web_private	Q	
_ka	IPv4 address:	172.16.1.5		
Pa Network	MAC address:	01:23:45:67:89:ab (optional)	
PP Address range	Resolution			
🥸 Router				
Group	None (static IP)		O Automatic	
Protocol	Comments:			
🖞 Port				
🙀 Port group				
E Region group				
() Time object				
		× CLOSE	+ CREATE AND DUPLICATE	+ CREATE





Configuring the security policy

The firewall's security policy contains several policies, in particular filter, NAT and URL filter policies. There are 10 security policies, some of which are pre-configured; the others are blank.

Configuring the URL filter policy

The URL filter policy makes it possible to set the rules that allow or block access to specified URLs. The URL filter policy must be enabled in the application inspection of a filter policy rule before it can be applied - this will be seen in our example.

🕕 IMPORTANT

The **URL filtering** module is different from the **SSL filtering** module. To filter and decrypt HTTPS connections, a specific and advanced configuration must be set up. For more information, refer to the technical note Filtering HTTPS connections.

Configuring URLs

In our example, we want to block access to URLs ending in **.exe**. Start by creating a custom URL category containing the URL format to block.

- 1. Go to Configuration > Objects > URL (Web objects in version 3), URL tab.
- 2. Click on Add a customized category.
- 3. On the new line, give the category a name (EXE in our example).
- 4. Press Enter or click on the grid on the left to confirm.
- 5. The new category will appear highlighted. If it does not, select it.
- 6. In the grid on the right, click on Add a URL.
- On the new line, define the URL that you want to block. In our example, we entered *.exe, meaning that all URLs ending in .exe will be blocked.
- 8. Press Enter or click on the grid on the right to confirm.

OBJECTS / WEB OBJECTS	
URL CERTIFICATE NAME (CN) GROUPS OF CATEGORIES URL DA	TABASE
Add a customized category Remove Check usage Check URL classification	Classify
URL category Comments vpnssl_owa antivirus_bypa authentication	Authorized characters Authorized characters: '*' '?' '' '-'_' [a-z] [A-Z] [0-9] Example: www.google.com/* or *.yahoo.com/* URL CATEGORY: EXE Add a URL Remove
	URL A Comments *.exe
	I 4 4 Page 1 of 1 ▶ ▶ 2 Displaying 1 - 1 of 1





Configuring the URL filter policy

- 1. Go to Configuration > Security policy > URL filtering.
- 2. In the drop-down menu, observe the policy that is being edited. Keep its name. If necessary, rename it by clicking on **Edit > Rename** or choose another one.
- 3. Click on Add.
- 4. Modify the fields to create the rule that block access to URLs ending in .exe:
 - Action field: select an action that makes it possible to block access. To inform a user when a page is blocked, you can customize the page in Configuration > Notifications > Block messages, HTTP Block page tab.
 - URL category field: select the category in question (EXE in our example).
- 5. You can fill in your URL filter policy by blocking access to dynamic URL categories such as "shopping" or "pornography". Every category contains several URLs that can be blocked or allowed, depending on the desired reaction.
- 6. Place the block rules before the *pass all* rule by using the **Up** and **Down** buttons.
- 7. Click on Apply, then save the configuration.

➔	SECURITY POLICY / URL FILTERING													
(0)	(0) URLFilter_00 • Edit • ① URL database provider: Embedded URL database													
+	+ Add 🗙 Delete 🕇 Up 👃 Down 🗁 Cut 🔄 Copy 🏵 Paste + Add all predefined categories Check URL classification													
	Status 🚉	Action ≞▼	URL category	Comments										
1	⊕ off	Pass	authenticati	authorize the URLs of authentication_bypass group										
2	💽 on	😪 BlockPage_00	ම exe											
3	💽 on	😪 BlockPage_00	Difference pornography	pornography										
4	💽 on	Pass	≭ any	default rule (pass all)										

Configuring the filter and NAT policy

The filter and NAT policy groups a set of filter rules and NAT rules. The firewall uses a **Block all** policy by default, in which administrators of the firewall can access the administration interface and block all other connections.

When you configure your firewall's filter/NAT policy:

- Always save changes in progress by clicking on Apply.
- Be careful not to enable incomplete or incorrect filter/NAT policies that may prevent your firewall's administration interface from being reached.
- Remember that the SNS firewall blocks traffic: any traffic that is not explicitly described in the policy will be rejected without being logged, even when this rule does not appear.

Choosing a filter and NAT policy

- 1. Go to Configuration > Security policy > Filter NAT.
- 2. In the drop-down menu, select a blank policy out of Filter 05, 06, 07 or 08.
- 3. Rename the new policy by clicking on Edit > Rename if you wish to.





ł	SECURITY POLIC	Y / FILTER	- NAT												
	(8) Filter 08	-	Edit	• "3	Export	•									
	뤚 (1) Block all														
	(2) High														
	(3) Medium		⊢ New r	ule 🝷	× Delete	+ +	*	- 🛃 (Cut	🔄 Сору	9 F	Paste	🖏 Search i	n logs	≡
	(4) Low		tion	<u>-</u> *	Source	Destination	De	est. port		Protocol		Security	inspection	≞ ≢	Comments
1	(5) Filter 05														
	(6) Filter 06														
	(7) Filter 07														
	(8) Filter 08	0-													
	(9) Pass all High	J													
	(10) Pass all														
4	C C Page 0	of 0 $ $ >	» ;	С										No d	ata to display

Configuring the filter policy

The filter policy can be configured in **Configuration > Security Policy > Filter - NAT**, **Filtering** tab.

Create the following rules for the purposes of our reference architecture:

- A rule allowing DNS resolution,
- A rule allowing the "in" network to access the "Internet" using HTTP,
- A rule allowing the "in" network to access the "Internet" using HTTPS,
- A rule allowing the "in" network to access the web server using HTTPS,
- A rule allowing the "Internet" to reach the web server using HTTPS.

💡 TIP

Add separators to your filter policy for better organization.

Enabling DNS resolution

- 1. Click on **New rule > Single rule**.
- 2. Double-click on the number of the new rule to edit it; a new window will open.
- 3. In the General tab, Status field: select On.
- 4. In the Action tab, Action field: select pass.
- 5. In the Source tab, Source hosts field: select Network in.
- 6. In the Destination tab, Destination hosts field: select Internet.
- 7. In the **Port Protocol** tab, **Port** field: select *dns_udp*.
- 8. Click on OK.

F	ILTERING	NAT									
Searching			+ Nev	v rule 🝷	X Delete 1	* * 2 8	Cut 🔄 Copy	🕑 Paste 🕴	Search in logs		≡
		Status	Action	≞ v	Source	Destination	Dest. port	Protocol	Security inspection	≞₹	Comments
l	Internet	access from in t	o Internet (conta	ains 1 rule	s, from 1 to 1)						
	1	💽 on	📀 pass		며 Network_in	Internet	🖞 dns_udp		IPS		Created on
4	< F	Page 1 of	1 > _>	C						Displ	aying 1 - 2 of 2



Allowing the "in" network to access the "Internet" using HTTP

- 1. Click on **New rule > Single rule**.
- 2. Double-click on the number of the new rule to edit it; a new window will open.
- 3. In the General tab, Status field: select On.
- 4. In the Action tab, Action field: select pass.
- 5. In the Source tab, Source hosts field: select Network in.
- 6. In the Destination tab, Destination hosts field: select Internet.
- 7. In the Port Protocol tab, Port field: select http.
- 8. In the **Inspection** tab, under **Application inspection**, **URL filtering** field: select a URL filter policy (*URLFilter_00* in our example).
- 9. Click on **OK**.

FILTERING	NAT							
Searching		🕂 🕂 New rule 👻	X Delete 1	* * * 🖻	Cut 🔄 Copy	🕑 Paste 🗒	Search in logs	≡
	Status ≞▼	Status 🔄 Action 🖃 Source		Destination	Dest. port	Protocol	Comments	
⊡ Internet ac	ccess from in to Inte	ernet (contains 2 rule	s, from 1 to 2)					
1	💽 on	pass	📲 Network_in	Internet	🛱 dns_udp		IPS	Created on
2	2 💽 on		명 Network_in	Internet	🖞 http		IPS WRL filter: URLFilter_00	Created on
« < Pa	ge 1 of 1	> » C					Displa	ying 1 - 3 of 3

Allowing the *"in"* network to access the *"Internet"* using HTTPS

- 1. Click on New rule > Single rule.
- 2. Double-click on the number of the new rule to edit it; a new window will open.
- 3. In the General tab, Status field: select On.
- 4. In the **Action** tab, **Action** field: select *pass*.
- 5. In the Source tab, Source hosts field: select Network in.
- 6. In the Destination tab, Destination hosts field: select Internet.
- 7. In the **Port Protocol** tab, **Port** field: select *https*.
- 8. Click on OK.

FILTERING	NAT						
Searching		+ New rule +	X Delete 1	$ \psi_{i} = z^{k} - z^{k} $	🚰 Cut 🖸 Copy 👻) Paste 🖳 Search in logs	≡
	Status ≞▼	Action =	Source	Destination	Dest. port	Protocol Security inspection	<u>-</u> ▼ Comments
∃ Internet	access from in to Int	ernet (contains 3 ru	es, from 1 to 3)				
1	💽 on	🕤 pass	명 Network_in	Internet	╈ dns_udp	IPS	Created on
2	💽 on	pass	며 Network_in	Internet	İ http	IPS ©► URL filter: URLF	Created on
₿ 3	💽 on	🗿 pass	며 Network_in	Internet	🖞 https	IPS	Created on
« < F	Page 1 of 1	> » C					Displaying 1 - 4 of 4

Allowing the "in" network to access the web server using HTTPS

- 1. Click on New rule > Single rule.
- 2. Double-click on the number of the new rule to edit it; a new window will open.
- 3. In the General tab, Status field: select On.





- 4. In the Action tab, Action field: select pass.
- 5. In the Source tab, Source hosts field: select Network in.
- In the Destination tab, Destination hosts field: select the object that represents the web server (srv_web_private in our example).
- 7. In the **Port Protocol** tab, **Port** field: select *https*.
- 8. Click on OK.

FILTER	NG NAT						
Searchin	g	+ New	rule 👻 🗙 Delete 🛛	↑ ↓ x ² →	🛎 📴 Cut – 🖻 Copy	n 🕑 Paste 🗒 Se	arch in logs 🛛 🚍
	Status	≟• Action	<u>=</u> ▼ Source	Destination	Dest. port	Protocol Sec	urity inspection 🖃 Comments
⊟ Inter	rnet access from in	to Internet (conta	iins 3 rules, from 1 to 3)				
1	💽 on	🕤 pass	🖳 Network_	in 🕀 Internet	🖠 dns_udp	IPS	Created on
2	💽 on	🕤 pass	며 Network_	in 🕀 Internet	🖞 http	<mark>IPS</mark> ⊗♦	URL filter: URLFilter_00 Created on
3	💽 on	🕤 pass	📲 Network_	in 🕀 Internet	🕇 https	IPS	Created on
E Acc	ess from in to dmz	(contains 1 rules,	from 4 to 4)				
4	💽 on	📀 pass	📲 Network_	in 🖪 srv_web_	private 🍟 https	IPS	Created on
« <	Page 1 o	f1 > >	0				Displaying 1 - 6 of 6

Allowing the "Internet" to reach the web server using HTTPS

- 1. Click on New rule > Single rule.
- 2. Double-click on the number of the new rule to edit it; a new window will open.
- 3. In the General tab, Status field: select On.
- 4. In the Action tab, Action field: select pass.
- 5. In the **Source** tab:
 - Source hosts field: select Internet.
 - Incoming interface field: select out.
- 6. In the Destination tab, Destination hosts field: select Firewall out.
- 7. In the Port Protocol tab, Port field: select https.
- 8. Click on OK.

Click on Apply to save changes.

FILT	TERING	NAT							
Sear	ching		+ New rule +	🗙 Delete 🕇	4 💉 🖉 🖻 c	ut 🔄 Copy	🕑 Paste 🗒	Search in logs	≡
		Status ≞▼	Action =	Source	Destination	Dest. port	Protocol	Security inspection	Comments
Ξ	Internet acces	s from in to Inte	rnet (contains 3 rule	s, from 1 to 3)					
1		🜑 on	pass	📲 Network_in	Internet	🖠 dns_udp		IPS	Created on
2		💽 on	pass	₽ <mark>8</mark> Network_in	Internet	İ http		IPS WRL filter: URLFilter_00	Created on
3		🜑 on	pass	📲 Network_in	Internet	🖞 https		IPS	Created on
Ξ	Access from i	n to dmz (contai	ins 1 rules, from 4 to	4)					
4		💽 on	🕤 pass	B Network_in	srv_web_private	🖞 https		IPS	Created on
Ξ	Access from I	nternet to dmz (web server) (contain	s 1 rules, from 5 to 5)					
5	B	💽 on	pass	Internet interface: out	Firewall_out	覚 https		IPS	Created on
«	< Page	1 of 1	> » C					Displa	aying 1 - 8 of 8



Configuring the NAT policy

The NAT policy can be configured in **Configuration > Security Policy > Filter - NAT**, **NAT** tab.

Create the following rules for the purposes of our reference architecture:

- One rule for outgoing traffic,
- One rule for incoming traffic.

Creating a rule for outgoing traffic

- 1. Click on **New rule > Single rule**.
- 2. Double-click on the number of the new rule to edit it; a new window will open.
- 3. In the General tab, Status field: select On.
- 4. In the **Original source** tab, **Source hosts** field: select *Network_in*.
- 5. In the Original destination tab:
 - General sub-tab, Destination hosts field: select Internet.
 - Advanced properties tab, Outgoing interface tab: select out.
- 6. In the Translated source tab:
 - Translated source host field: select Firewall out.
 - Translated source port field: select ephemeral fw.
 - Select Choose random translated source port.
- 7. Click on OK.

FILTERING	NAT										
Searching		+ New rule	· ▼ X Delete	+ + +	۴	🖉 🔄 Cut	🔄 Copy 🛛 🐑 Paste	🔋 🛱 Search in logs	🖙 Search	in monitorin	g
		Origina	l traffic (before tran	slation)			Traffic after tran	Islation		Protocol	Comments
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port	Protocol	
1	💽 on	며 Network_in	Internet interface: out	¥ Any ■	÷	Firewall_out	↔ 🖞 ephemeral_fw	* Any			Created on
« < Pa	ge 1 of 1	> _ » C								Displa	aying 1 - 1 of 1

Creating a rule for incoming traffic

- 1. Click on **New rule > Single rule**.
- 2. Double-click on the number of the new rule to edit it; a new window will open.
- 3. In the General tab, Status field: select On.
- 4. In the **Original source** tab:
 - Source hosts field: select Internet.
 - Incoming interface field: select out.
- 5. In the Original destination tab:
 - **Destination hosts** field: select *Firewall_out*.
 - Destination port field: select https.
- 6. In the **Translated destination** tab, **Translated destination host** field: select the object that represents the web server (*srv web private* in our example).
- 7. Click on OK.

Click on Apply to save changes.





FIL	FERING	NAT										
Sear	ching		+ New rule	e ≠ X Delete	↑ ↓	×	🖉 🚰 Cut	🔄 Copy 🛛 🕑 Paste	🗒 Search in logs	🖙 Search	in monitorir	ng = •
		<u>=</u> *	Origina	al traffic (before tran	slation)			Traffic after translation				
		Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port	Protocol	comments
1		💽 on	면 Network_in	Internet interface: out	∗ Any	+	Firewall_out	⊀ 🖠 ephemeral_fw	* Any			Created on
2		💽 on	Internet interface: out	Firewall_out	🖞 https	+	* Any		f srv_web_private			Created on
«	< Pag	je 1 of 1	> » C								Displ	aying 1 - 2 of 2





Testing the configuration and backing it up

Now that your firewall is configured, ensure that everything is running correctly. If so, we recommend backing up the configuration of your firewall so that you can restore it whenever necessary.

Testing the configuration

If certain components are inaccessible when the configuration is finalized, check whether the malfunction relates to the configuration of your firewall. To do so:

- Verify the rules in your filter, NAT and URL policies in order to identify any potential errors.
- You can place a *pass all* rule at the beginning of a filter or URL policy to test whether a rule in particular is too restrictive. Be cautious, however, as this may compromise the security of your environment while you perform your tests.

Backing up the configuration

Back up your firewall's configuration in **Configuration > System > Maintenance**, **Backup** tab. You can also enable automatic backups of its configuration in this module.

For more information, refer to the **Maintenance** chapter in the SNS user manual.

Page 28/31





Further reading

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

- Technical note on high availability (SNS in version 4 only).
- Technical documentation on VPN topologies.
- Technical documentation website SNS version 4 or SNS version 3 (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.

Page 29/31





SNS - INSTALLATION AND FIRST-TIME CONFIGURATION OF AN SNS FIREWALL GUIDE - V 3 AND 4



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.



