GUIDE

STORMSHIELD NETWORK SECURITY

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

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.

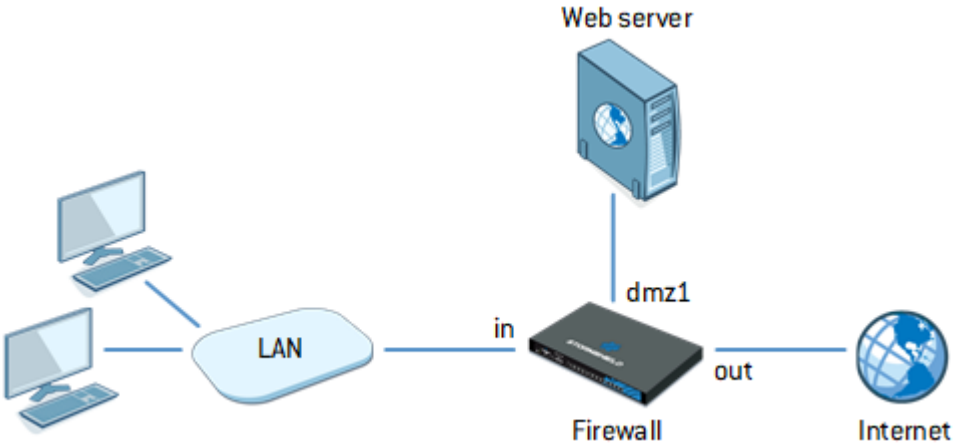
This guide is a supplement to the *Product presentation and installation guide* and the *Quick Installation Guide* provided with your firewall. Refer to the Guides page to find the relevant version.

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.

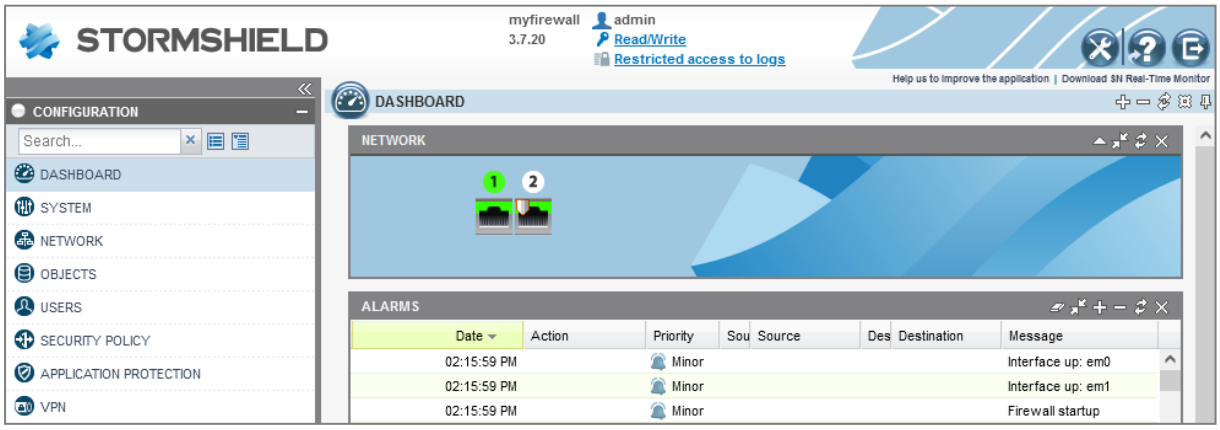
Accessing the firewall administration interface

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.

Administration interface of an SNS firewall in version 4

Administration interface of an SNS firewall in version 3

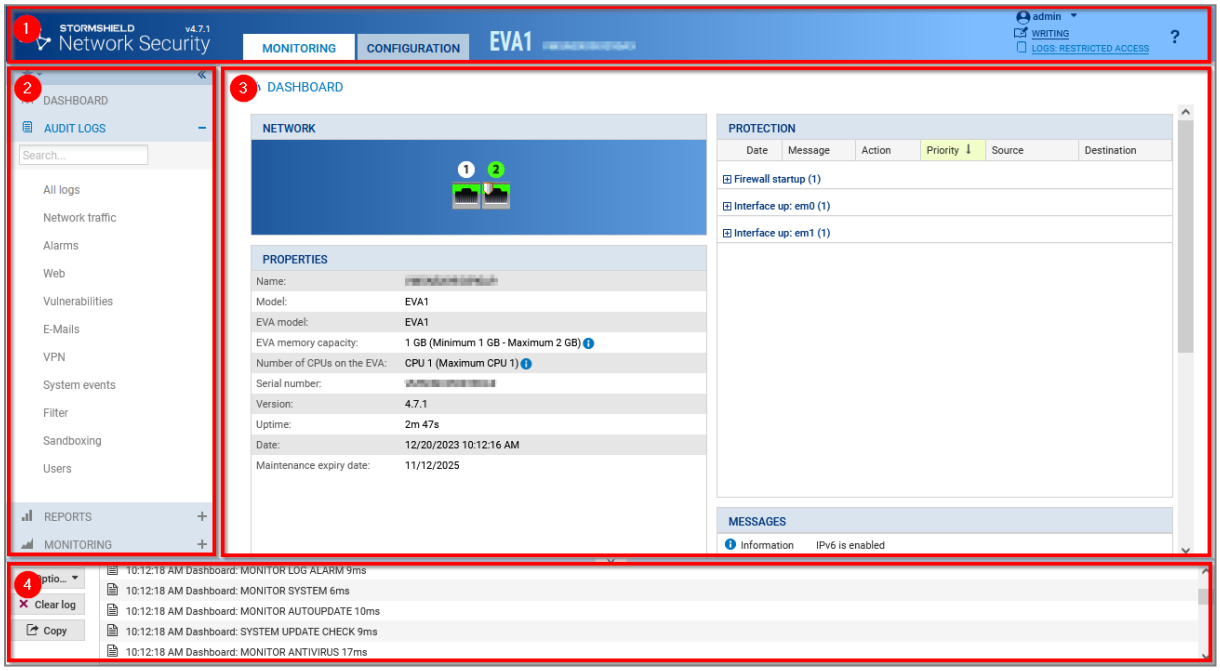


Understanding the graphical user interface

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.



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 ,
- Expand and collapse categories by clicking on them,
- Set modules as favorites by clicking on the 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

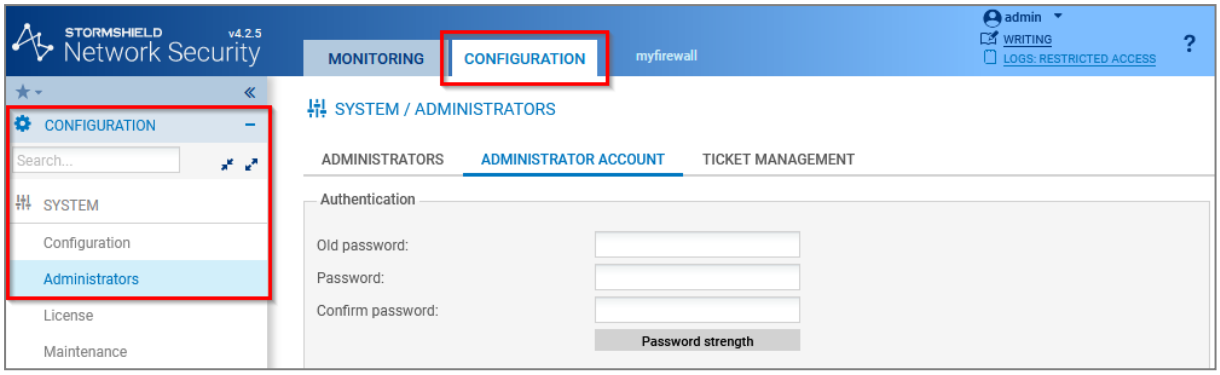
For security reasons, you must change the default password of the "*admin*" user during the initial connection to the firewall.

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:

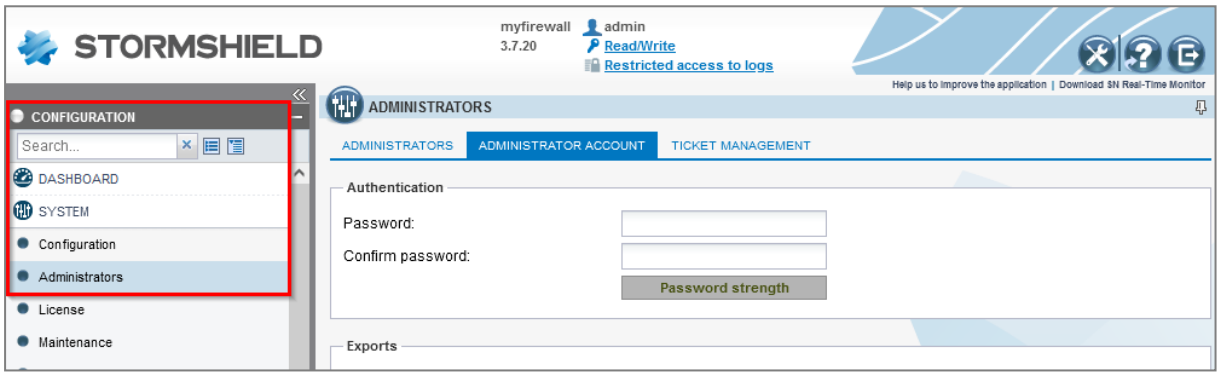
     ```
     " <tab> <space>
     ```
5. Click on **Apply** , then **Save**.

The new password must be used at the next connection.

Administration interface of an SNS firewall in version 4



Administration interface of an SNS firewall in version 3

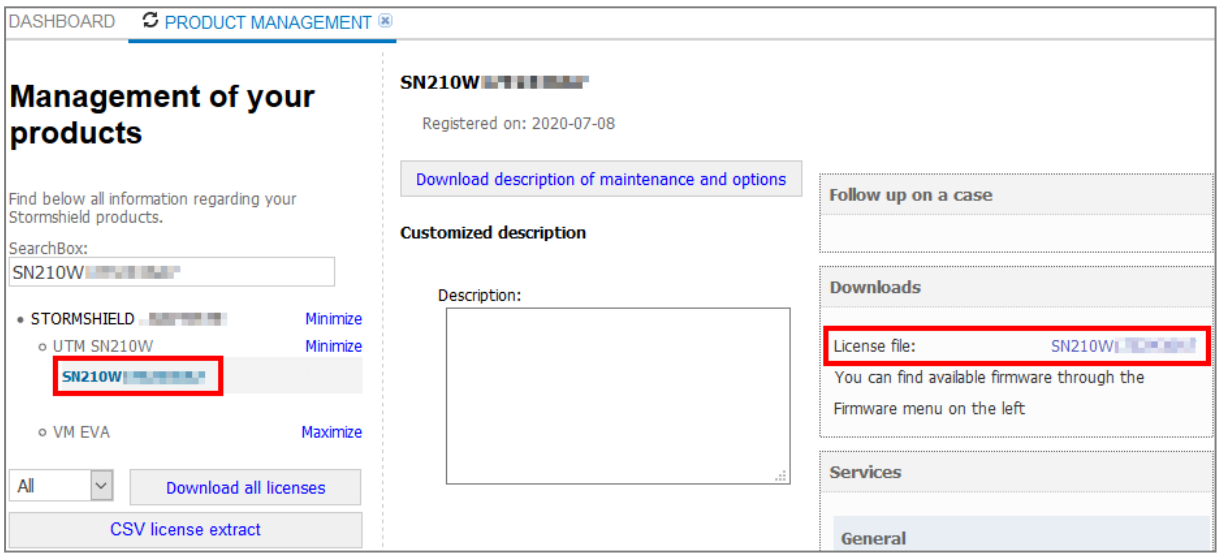


Installing the firewall license

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

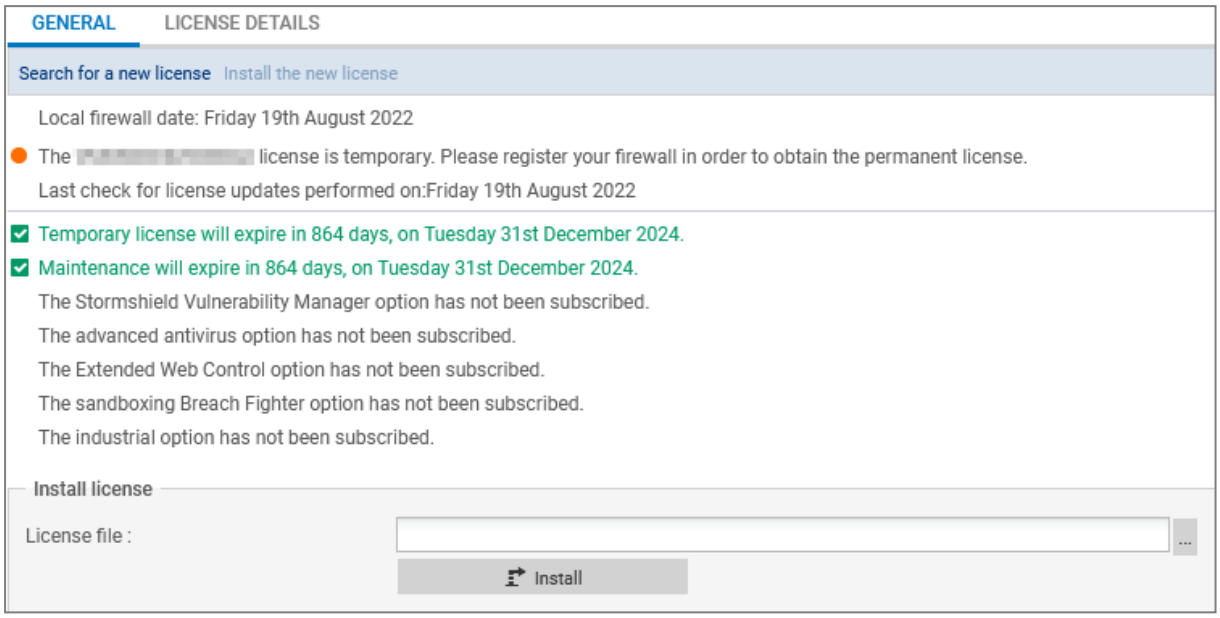
1. Log in to your MyStormshield personal area.
2. Go to **Products > Product management**.
3. In the **Product management** area, identify your firewall with the help of the **Maximize** and **Minimize** buttons, or by entering its serial number in the search zone. Click on it.
4. In the **Downloads**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



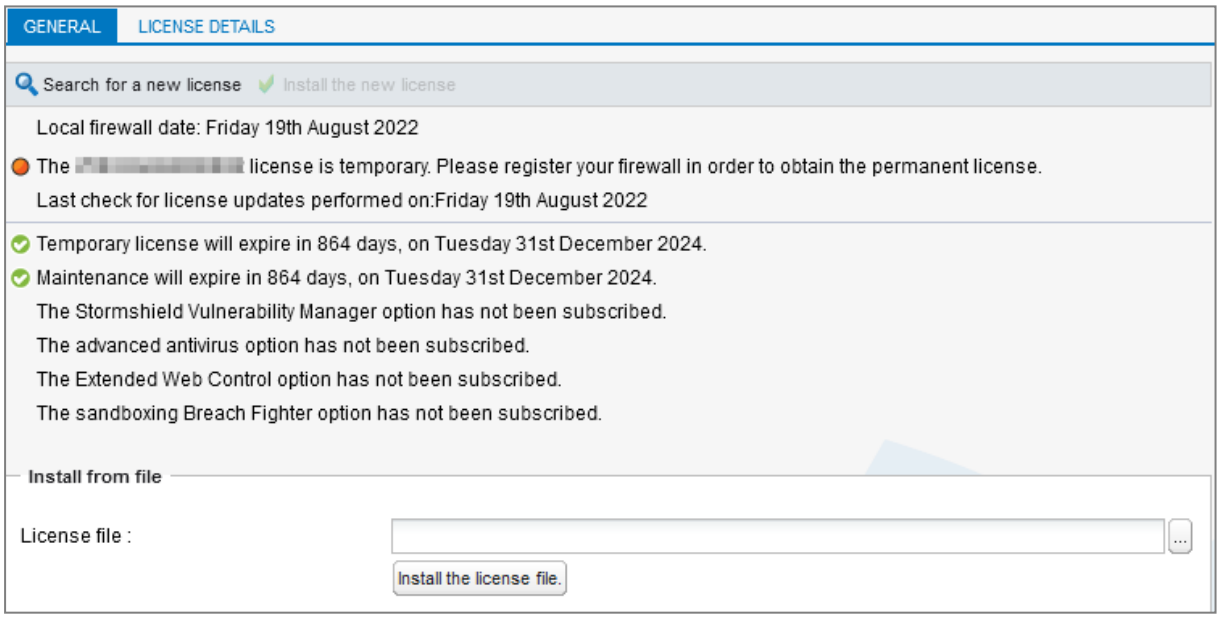
Installing the license on the firewall

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**.

Administration interface of an SNS firewall in version 4



Administration interface of an SNS firewall in version 3



Updating the firmware

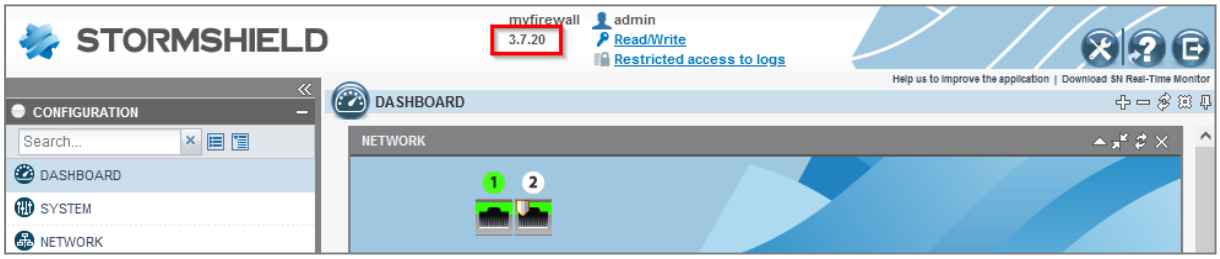
By updating your firewall to a more recent version, it will benefit from the latest features available and the latest functional patches and bug fixes.

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.

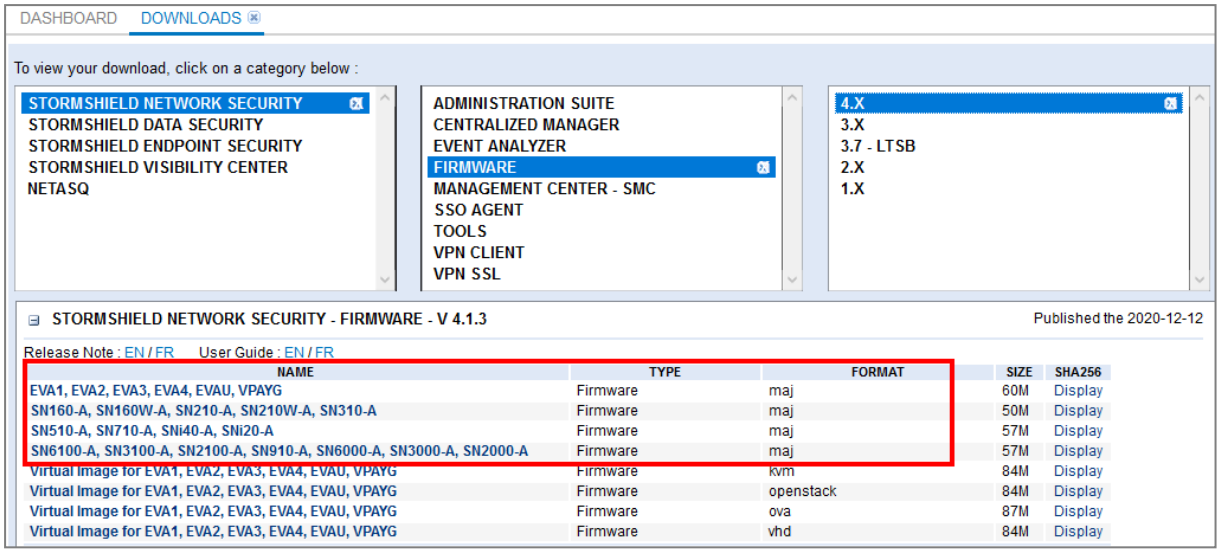
Administration interface of an SNS firewall in version 4

Administration interface of an SNS firewall in version 3



Downloading the update file

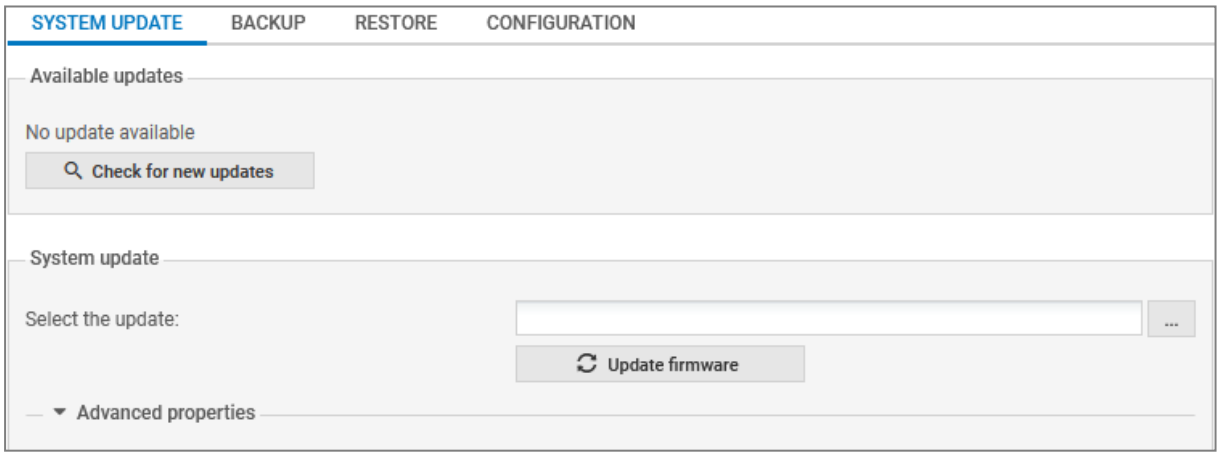
1. Log in to your MyStormshield personal area.
2. Go to **Downloads** > **Downloads**.
3. Select **Stormshield Network Security** from the suggested categories, then **Firmware**. If necessary, select a version branch as well, such as 4.X, to narrow down the list.
4. Locate the version that you want 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 lifecycle 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.



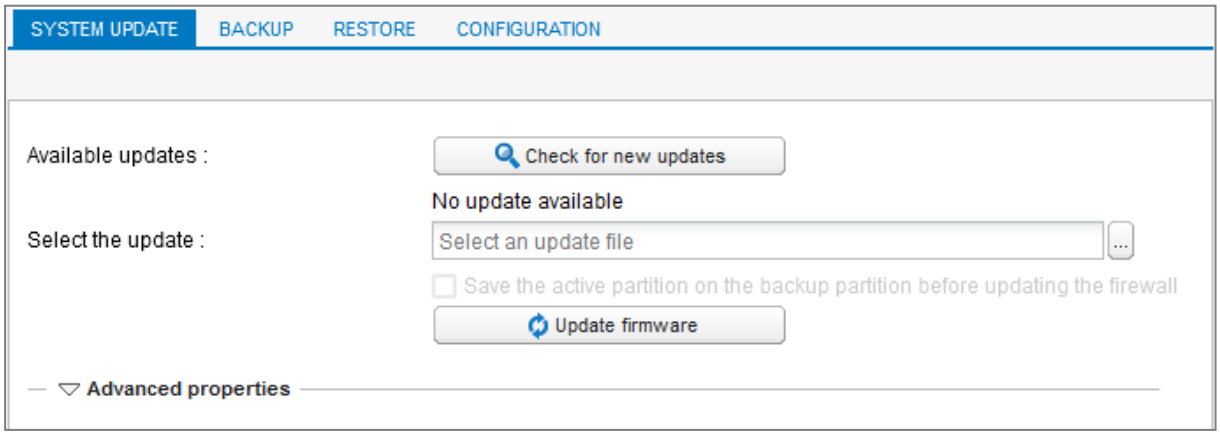
Installing the update

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



Administration interface of an SNS firewall in version 3



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.

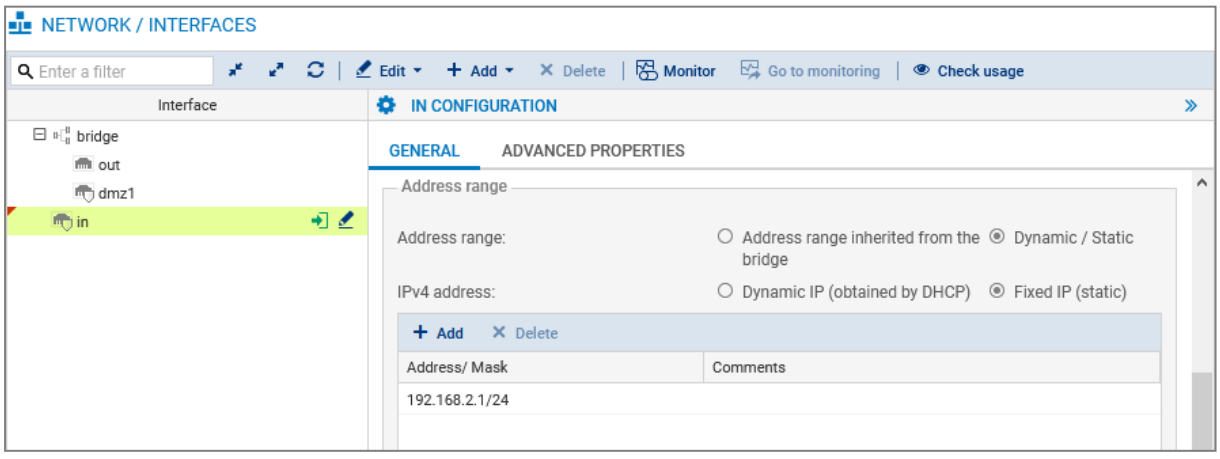
TIP
For more information about the modules of the firewall administration interface, refer to the v4 or v3 user guide in the SNS version used.

Configuring the firewall's interfaces

Configuring the *in* interface

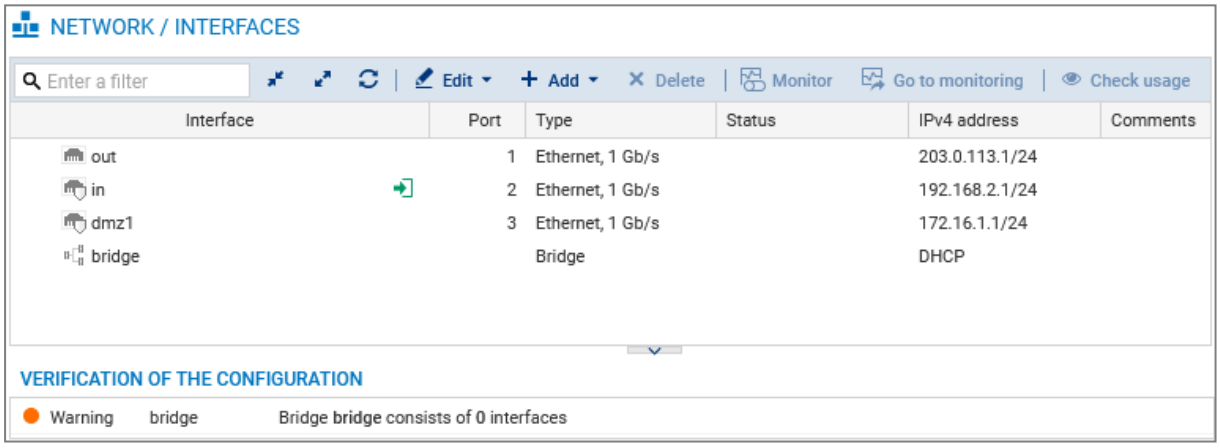
1. Go to **Configuration** > **Network** > **Interfaces**.
2. Select the *in* interface, then click on **Edit**.
3. In the **General** tab, fill out the information in the **Address range** area:
   - **Address range** field: select **Dynamic / Static**.
   - **IPv4 address** field: select **Fixed IP (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.



Configuring the *out* and *dmz1* interfaces

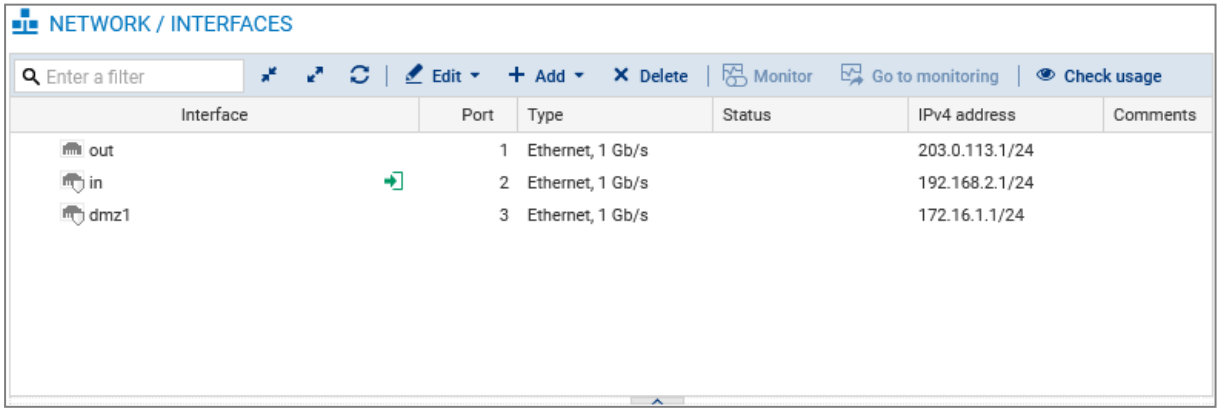
1. Select the *out* interface and click on **Edit**.
2. In the **General** tab, fill out the information in the **Address range** area:
   - **Address range** field: select **Dynamic / Static**.
   - **IPv4 address** field: select **Fixed IP (static)**.
   - In the grid: click on **Add**, and enter *203.0.113.1/24*.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



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.



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.

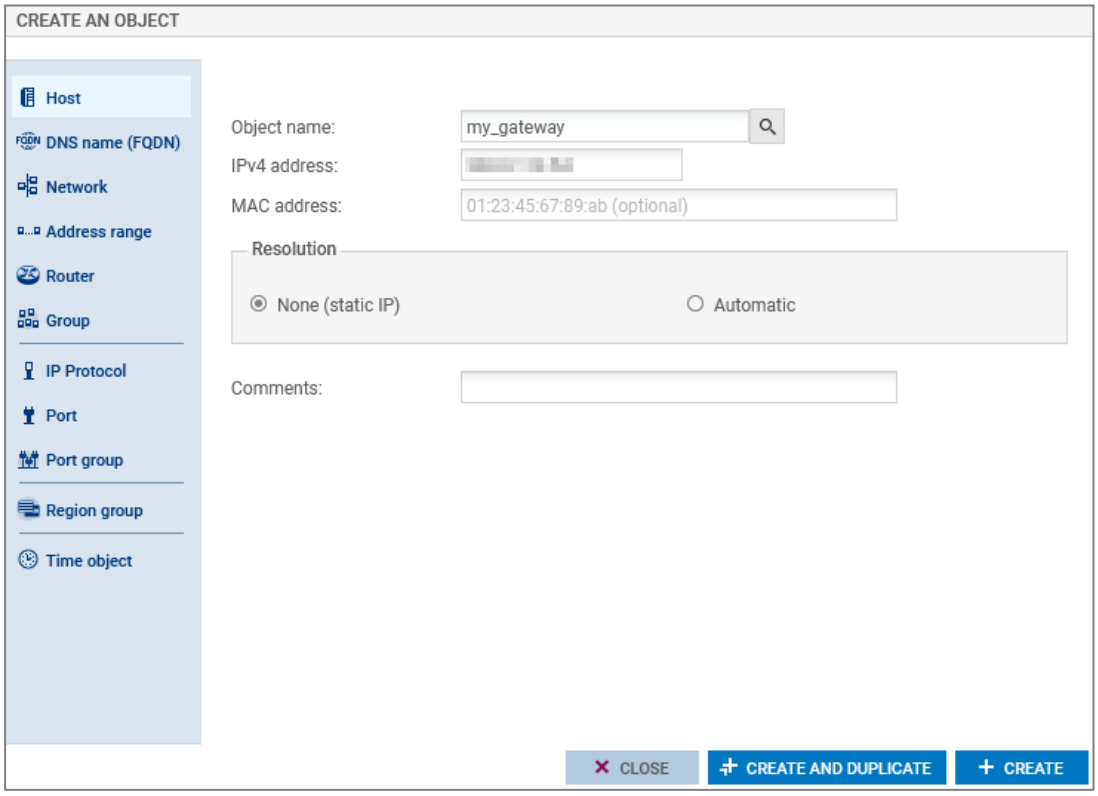
Configuring the default gateway

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

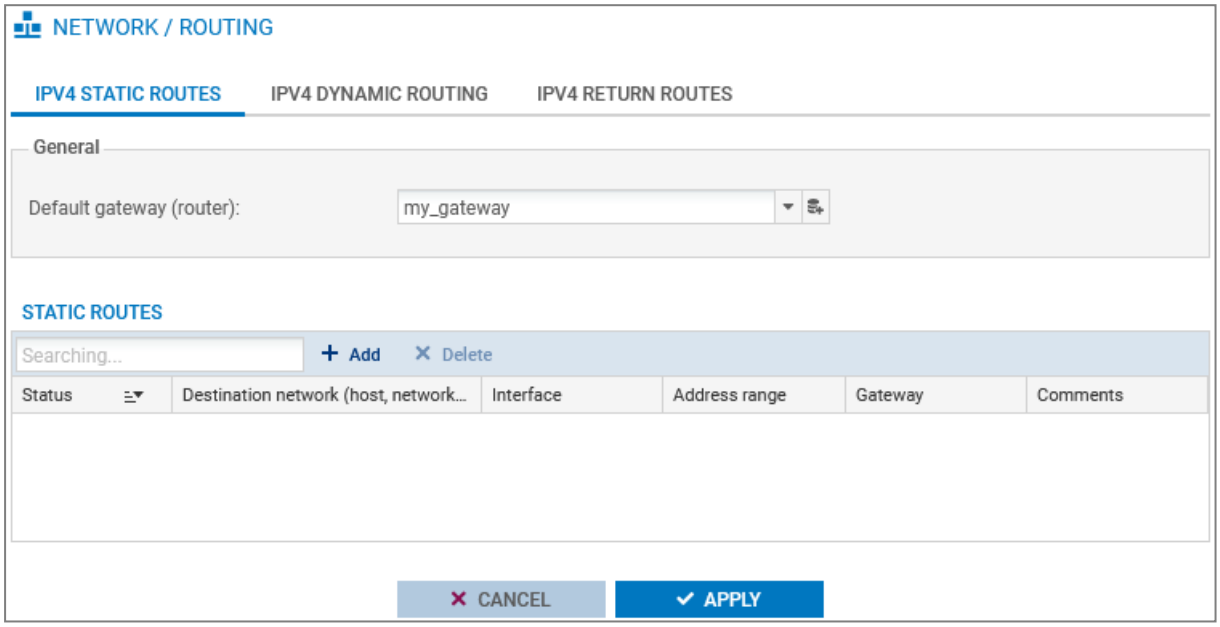
NOTE
If the *out* interface on your firewall retrieves an IP address from a DHCP server, once it obtains a DHCP lease, the network object *Firewall_out_router* will be automatically created. If this is how your firewall was configured (different from our example), continue to the next section **Setting 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.



Setting the default gateway

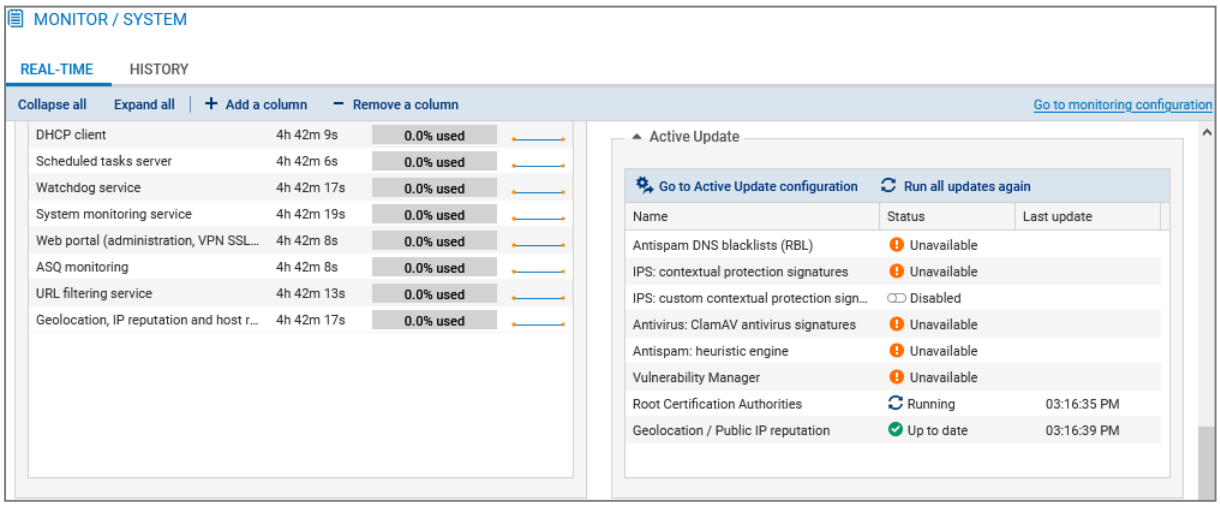
1. Go to **Configuration > Network > Routing**.
2. In the **IPv6 static routes** tab, under **General configuration**, select the object that represents the default gateway (*my_gateway* in our example).
3. Click on **Apply**.



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.



Connecting the firewall to the web server

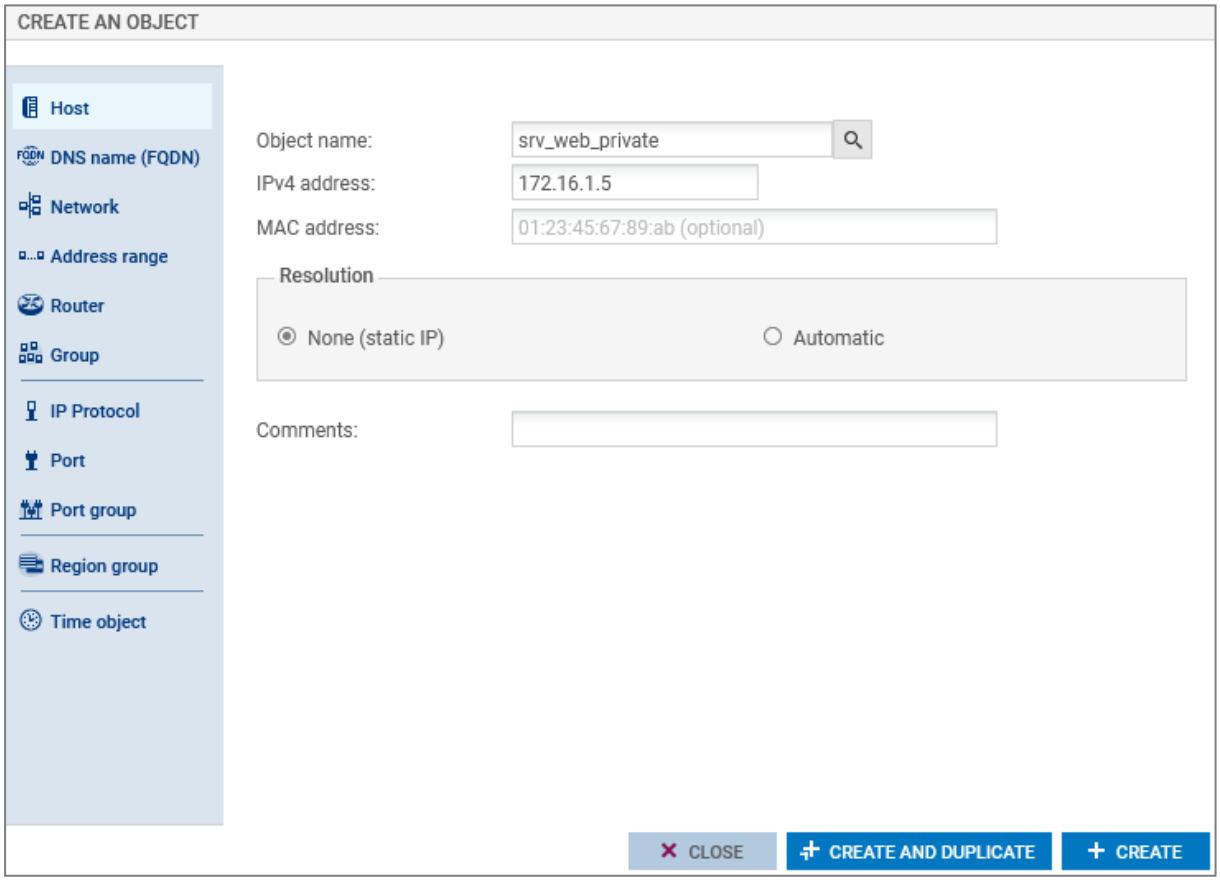
Physically connecting the firewall to the web server

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.



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

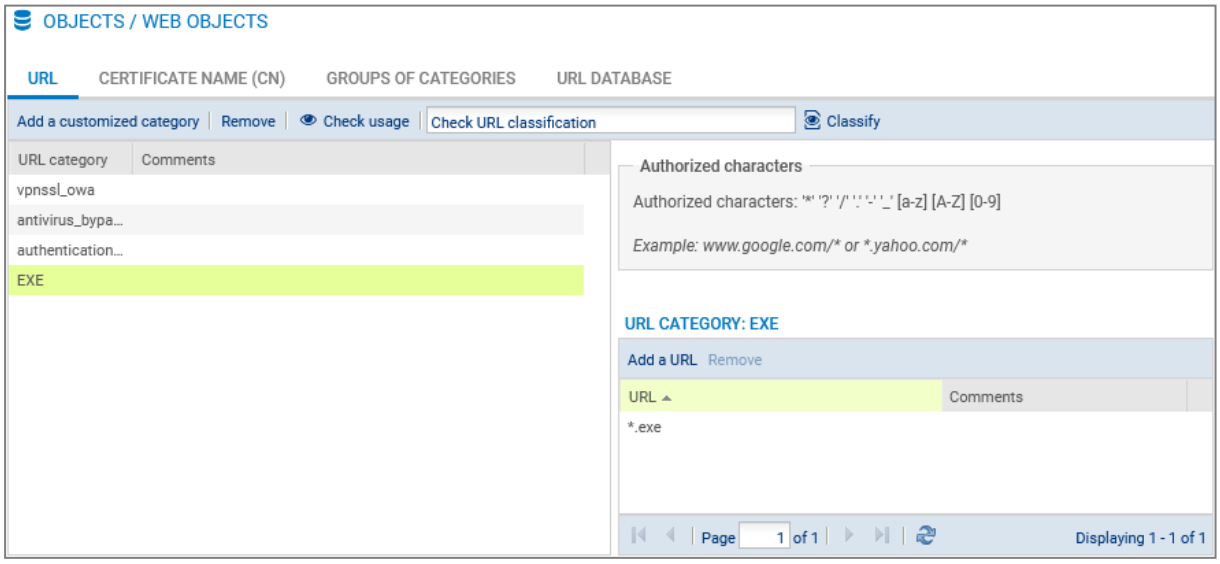
The URL filter policy makes it possible to set the rules that allow or block access to specified URLs. The URL filter policy must be enabled in the application inspection of a filter policy rule before it can be applied - this will be seen in our example.

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

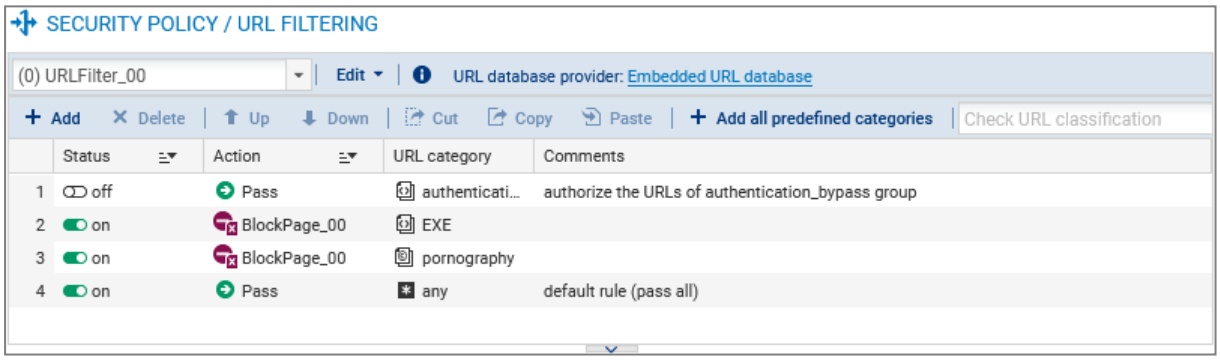
In our example, we want to block access to URLs ending in **.exe**. Start by creating a custom URL category containing the URL format to block.

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**.
7. 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.



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.



Configuring the filter and NAT policy

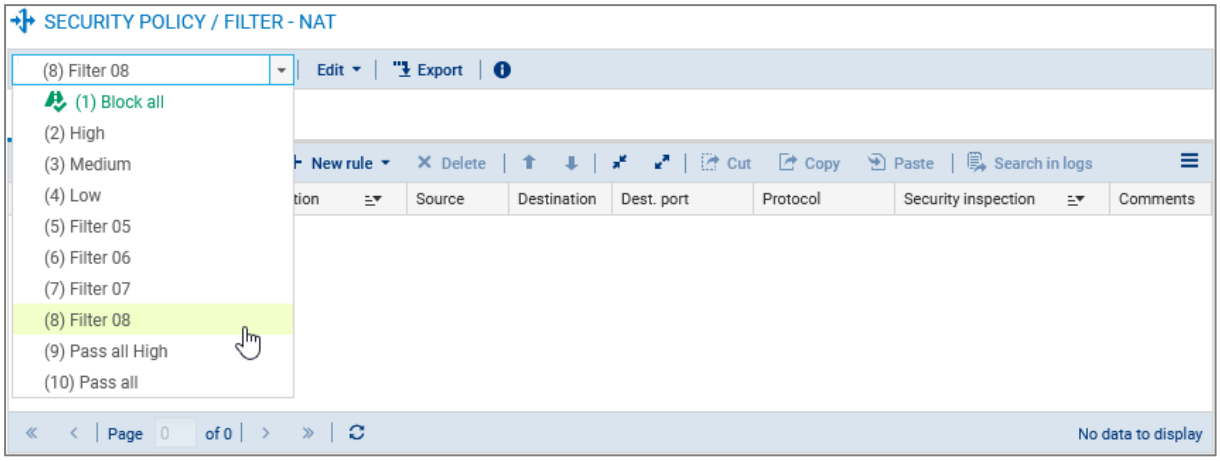
The filter and NAT policy groups a set of filter rules and NAT rules. The firewall uses a **Block all** policy by default, in which administrators of the firewall can access the administration interface and block all other connections.

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.



Configuring the filter policy

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

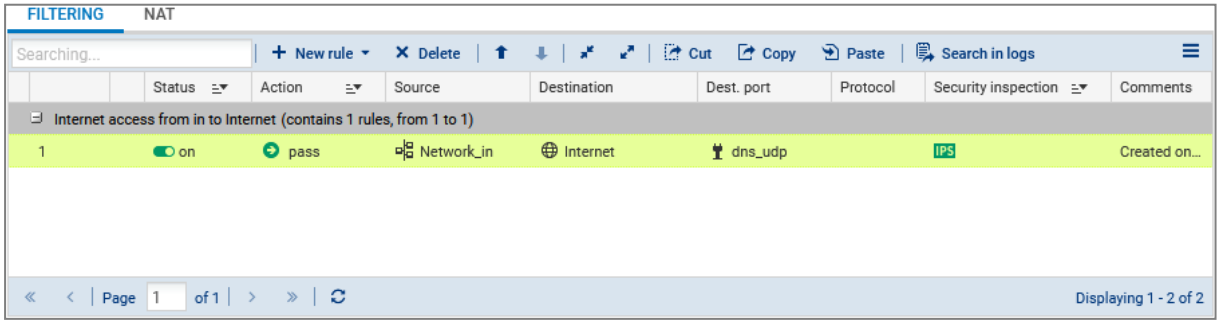
Create the following rules for the purposes of our reference architecture:

- 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.

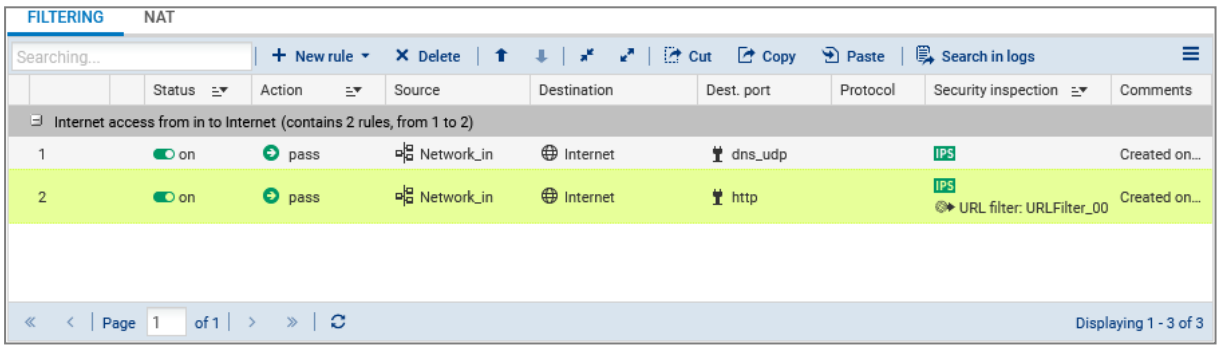
Enabling DNS resolution

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**.



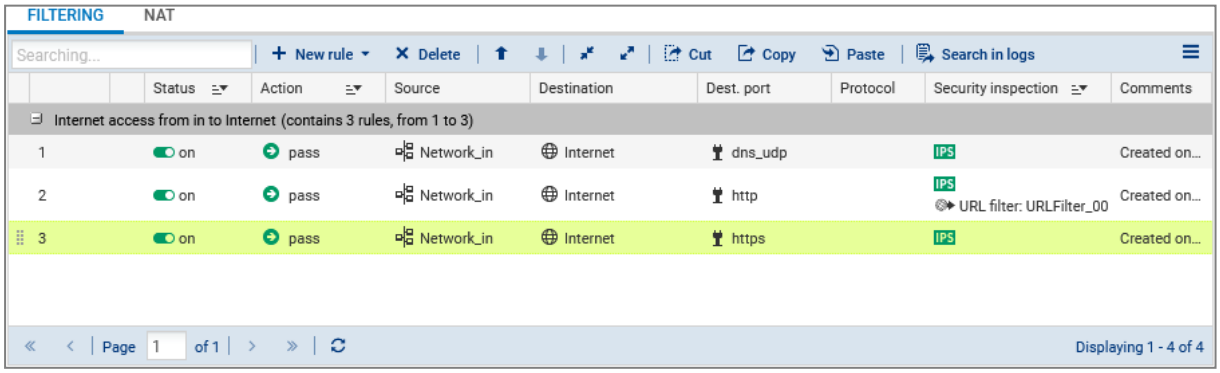
Allowing the "*in*" network to access the "*Internet*" using HTTP

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**.



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

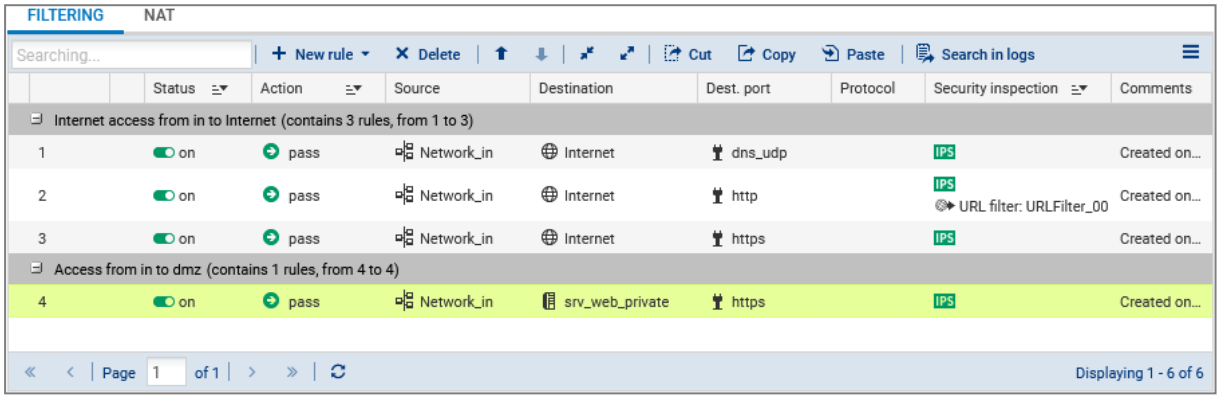
1. Click on **New rule** > **Single rule**.
2. Double-click on the number of the new rule to edit it; a new window will open.
3. In the **General** tab, **Status** field: select *On*.
4. In the **Action** tab, **Action** field: select *pass*.
5. In the **Source** tab, **Source hosts** field: select *Network_in*.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



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*.

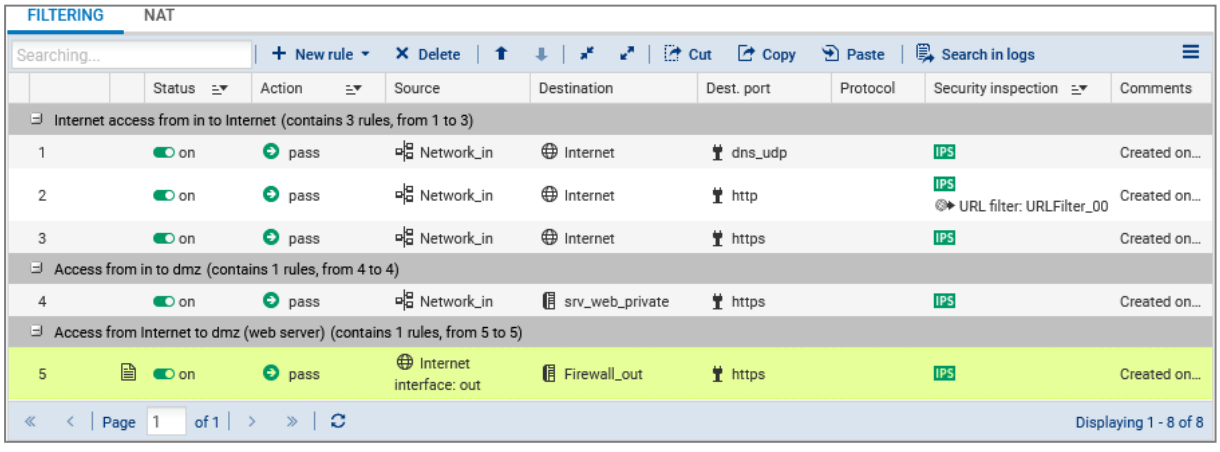
4. In the **Action** tab, **Action** field: select *pass*.
5. In the **Source** tab, **Source hosts** field: select *Network_in*.
6. In the **Destination** tab, **Destination hosts** field: select the object that represents the web server (*srv_web_private* in our example).
7. In the **Port - Protocol**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



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.



Configuring the NAT policy

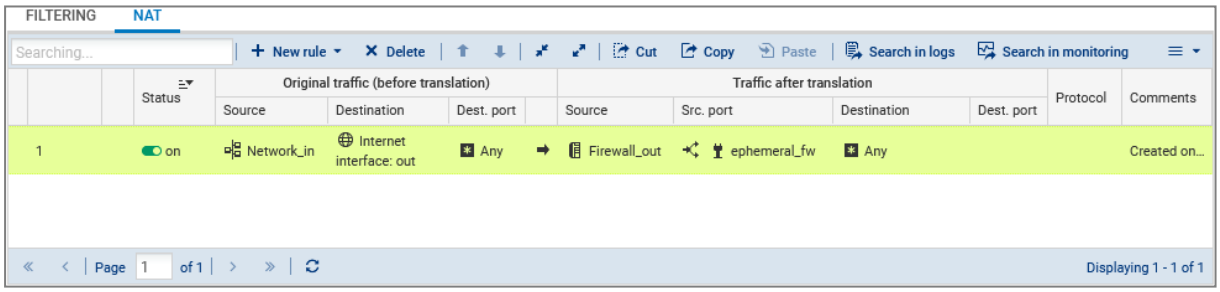
The NAT policy can be configured in **Configuration > Security Policy > Filter - NAT**, **NAT** tab.

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

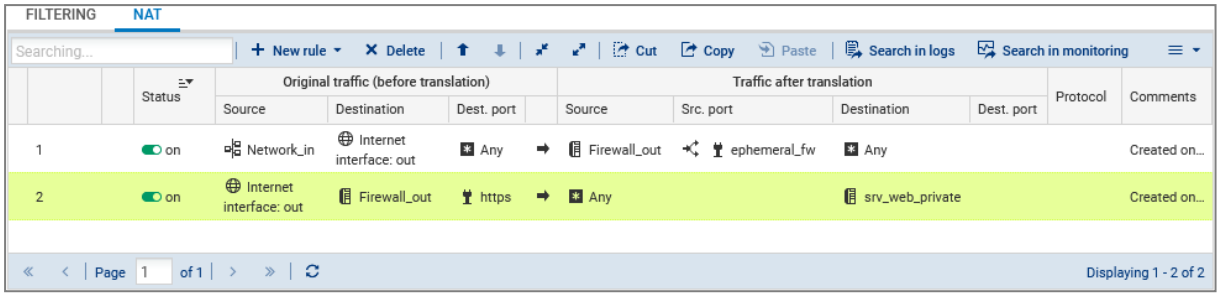
1. Click on **New rule > Single rule**.
2. Double-click on the number of the new rule to edit it; a new window will open.
3. In the **General** tab, **Status** field: select *On*.
4. In the **Original source** tab, **Source hosts** field: select *Network_in*.
5. In the **Original destination** tab:
   - **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**.



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.


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

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.

documentation@stormshield.eu