GUIDE

STORMSHIELD MANAGEMENT CENTER

ADMINISTRATION GUIDE

Version 3.0

Document last update: June 17, 2021

Reference: sns-en-SMC-administration_guide-v3.0

Table of contents

1. Getting started with the SMC server 7
1.1 Connecting to the SMC server's web interface 7
1.2 Connecting to the command line interface 7
1.3 Installing the SMC license 7
1.3.1 Troubleshooting 8
2. Warning before connecting SN firewalls to the SMC server 9
3. Connecting SN firewalls to the SMC server 10
3.1 Connecting a firewall with a factory configuration to the server 10
3.1.1 Declaring the firewall in the SMC server web interface 10
3.1.2 Building the firewall connecting package 10
3.1.3 Installing the connecting package on the firewall from a USB drive 12
3.2 Connecting a firewall already in production to the server 13
3.2.1 Declaring the firewall in the SMC server web interface 13
3.2.2 Building the firewall connecting package 13
3.2.3 Installing the connecting package on the firewall 15
3.3 Connecting a high availability cluster to the server 15
3.3.1 Declaring the cluster in the SMC server web interface 15
3.3.2 Building the cluster connecting package 15
3.3.3 Installing the connecting package on the active node of the cluster 17
3.4 Troubleshooting with the server's logs 18
3.4.1 Generating a firewall's connecting package 18
3.4.2 Installing the connecting package on the firewall 18
3.5 Importing SN firewalls from a CSV file 18
3.5.1 Creating the CSV file 18
3.5.2 Importing firewalls from the web interface 19
3.5.3 Importing firewalls in command line 19
4. Supervising SN firewalls 21
4.1 Monitoring and organizing firewalls 21
4.1.1 Getting information about firewalls 21
4.1.2 Exporting monitoring data 22
4.1.3 Organizing firewalls by folders 22
4.1.4 Checking usage of a firewall in the configuration 24
4.2 Accessing firewall logs and activity reports 24
5. Configuring SN firewalls 25
5.1 Editing firewall settings 25
5.2 Creating customized variables 25
5.2.1 Adding, changing or deleting customized variables 26
5.2.2 Defining the value of a customized variable for a firewall 26
5.3 Verifying configuration consistency 27
5.3.1 Disabling the consistency check 27
5.3.2 Disabling check areas 27
5.3.3 Restricting the number of inconsistencies reported 27
5.4 Deploying a configuration on firewalls 28
5.4.1 Deploying a configuration on a firewall from the web interface 28
5.4.2 Deploying a configuration on a high availability cluster 29
5.4.3 Deploying a configuration on a firewall in command line 29
5.4.4 Keeping the connection alive during deployment 30

5.4.5 Troubleshooting with the server's logs 30
5.4.6 Troubleshooting 30
5.5 Loading and deploying a former configuration 31
5.6 Generating a configuration comparison 31
5.7 Detecting changes to the local configuration on firewalls 32
5.7.1 Viewing local changes on a firewall 32
5.8 Managing network interfaces 32
5.8.1 Limitations to the configuration from the server 33
5.9 Accessing the web administration interface of firewalls 33
5.10 Using the Emergency mode 34
5.11 Converting a firewall connected to the SMC server into a high availability cluster 34
5.12 Importing or declaring a certificate for a firewall 34
5.12.1 Importing a certificate from the server's web interface 34
5.12.2 Importing a certificate from the command line interface 35
5.12.3 Importing a certificate on a high availability cluster 36
5.12.4 Troubleshooting 36
5.12.5 Declaring a certificate used by a firewall 37
5.12.6 Changing the certificate used by default in VPN topologies 37
5.13 Configuring the warning for an imminent certificate expiry 37
5.14 Disabling TPM (Trusted Platform Module) certificate protection during installation on the firewall 38
5.14.1 Finding out whether a certificate is TPM-protected 39
5.14.2 Disabling TPM certificate protection 39
5.14.3 Enabling TPM protection on existing certificates 39
5.15 Choosing the separator character in CSV files 40

6. Managing network objects 41
6.1 Deploying objects on firewalls 41
6.2 Creating variable objects 42
6.3 Checking usage of an object in the configuration 42
6.4 Importing objects 42
6.4.1 Creating the CSV file 43
6.4.2 Importing objects from the web interface 43
6.4.3 Importing objects in command line 44
6.5 Exporting objects 45

7. Creating and monitoring VPN tunnels 46
7.1 Creating policy-based VPN topologies 46
7.1.1 Configuring a policy-based mesh topology 47
7.1.2 Configuring a policy-based star topology 49
7.2 Creating route-based VPN topologies 51
7.2.1 Configuring a route-based mesh topology 52
7.2.2 Configuring a route-based star topology 55
7.2.3 Defining IPSec VTIs on SN firewalls 57
7.2.4 Defining the traffic routing policy 57
7.2.5 Editing the VTI network pool 58
7.3 Managing certificates and certification authorities 59
7.3.1 Adding a certification authority or chain of trust 60
7.3.2 Updating a certificate authority or chain of trust 61
7.3.3 Deleting a certification authority or chain of trust 61
7.3.4 Importing or declaring a certificate for a firewall 61
7.3.5 Updating a firewall's X509 certificate 61
7.3.6 Renewing firewall certificates obtained via SCEP or EST 61

7.3.7 Explanations regarding certificate statuses 62
7.4 Defining the contact IP address of firewalls for VPN topologies 63
7.4.1 Defining a firewall's default contact address 63
7.4.2 Defining a firewall's contact address in a specific VPN topology 64
7.5 Selecting the output interface of firewalls for VPN topologies 64
7.5.1 Creating the Host Object that corresponds to the interface 64
7.5.2 Selecting a firewall's output interface on SMC 64
7.5.3 Configuring a static route on the firewall optional 65
7.6 Editing, deleting and checking usage of a VPN topology 65
7.7 Managing packet fragmentation 66
7.8 Disabling a VPN topology 66
7.9 Monitoring the status of VPN tunnels 66
8. Creating filter and NAT rules 68
8.1 Understanding the order in which rules are read 68
8.2 Use case examples 69
8.2.1 Managing a pool without rule sharing 69
8.2.2 Managing a pool with shared and specific rules 69
8.2.3 Managing a multi-site environment with shared and specific rules and delegated filtering 69
8.2.4 Managing a multi-site pool with shared rule sets 71
8.3 Creating filter and NAT rules 71
8.4 Creating rule sets 72
8.4.1 Assigning rule sets to a firewall 72
8.4.2 Editing rule sets for a firewall 73
8.4.3 Importing or exporting rule sets 73
8.5 Identifying the rules 73
8.6 Changing the order in which rules are executed 73
8.7 Searching for a rule in the web interface or in SMC logs 74
8.8 Removing rules 74
8.9 Removing rule sets 75
8.10 Importing and exporting filter and NAT rules 75
8.10.1 Importing rules from a CSV file 75
8.10.2 Exporting rules to a CSV file 77
8.10.3 Importing rules from connected firewalls 78
8.11 Migrating local rules on a firewall to manage them in SMC 78
8.12 Managing URL filtering on SN firewalls from SMC 78
8.12.1 Creating the template URL filtering policy 79
8.12.2 Saving the URL filtering policy of the template firewall 80
8.12.3 Deploying the template URL filtering policy 81
8.13 Managing IPS Inspection profiles on SN firewalls from SMC 82
8.13.1 Editing the template IPS Inspection profiles 83
8.13.2 Saving the IPS Inspection profiles of the template firewall 84
8.13.3 Deploying the IPS Inspection profiles 85
8.14 Adding public IP address reputation groups 86
8.14.1 Finding out names of groups to be used 86
8.14.2 Adding address reputation groups to the SMC server 88
9. Running SNS CLI commands on a pool of firewalls 89
9.1 Creating the CLI command script 89
9.2 Using variables 90
9.2.1 Using variables specific to firewalls 90
9.2.2 Using global variables 90
9.2.3 Using a CSV file 90

9.3 Running the SNS CLI script from the web interface 91
9.4 Running the SNS CLI script in command line 92
9.4.1 Displaying the list of commands and options 92
9.4.2 Running a script 92
9.4.3 Adding scripts 93
9.4.4 Deleting scripts 93
9.4.5 Displaying the list of scripts 93
9.4.6 Examples of the use of scripts in command line with a CSV file 93
9.5 Running the SNS CLI script on a high availability cluster 94
9.6 Attaching files to a script and receiving files generated by script 95
9.6.1 Command arguments to be used in the script 95
9.6.2 Attaching files to a script 95
9.6.3 Receiving files generated by a script 96
9.7 Scheduling the execution of SNS CLI scripts 97
9.7.1 Scheduling the execution of scripts from the web interface 97
9.7.2 Scheduling the execution of scripts in command line 98
9.8 Updating firewalls by using SNS CLI scripts 98
9.9 Troubleshooting 100
9.9.1 The script file is too large 100
9.9.2 Certain characters are not supported in the script 100
9.9.3 The script fails to run on certain firewalls 100
9.9.4 The Execute script button remains grayed out 100

10. Maintaining SN firewalls 101
10.1 Backing up the configuration of firewalls 101
10.1.1 Backing up the configuration of the server and firewalls automatically 101
10.1.2 Backing up the configuration of firewalls manually 102
10.1.3 Excluding private keys from automatic firewall backups 102
10.2 Updating firewalls 102
10.3 Replacing an SN firewall through an RMA 102

11. Removing SN firewalls from the SMC server 103

12. Managing and maintaining the server SMC 104
12.1 Defining the server's network interfaces SMC 104
12.2 Verifying the SMC server version in command line 104
12.3 Changing the SMC server time zone and date 104
12.3.1 Changing the time zone 104
12.3.2 Changing the date manually 105
12.3.3 Changing the date via NTP 105
12.3.4 Displaying a comprehensive summary of the SMC server's date/time 105
12.4 Managing administrators 105
12.4.1 Managing administrators in the web interface 105
12.4.2 Allowing administrators to connect via an LDAP or Radius server 106
12.5 Viewing SMC server logs 112
12.6 Sending SMC logs to a remote server in Syslog format 112
12.6.1 Sending logs to a remote server without encryption 112
12.6.2 Sending logs to a remote server with encryption 113
12.6.3 Disabling the sending of logs to a remote server 113
12.6.4 Troubleshooting 113
12.7 Saving and restoring the SMC server configuration 114
12.7.1 Saving the server configuration from the web interface 114
12.7.2 Saving the server configuration from the command line interface 114

12.7.3 Restoring the server configuration from the web interface 115
12.7.4 Restoring server configuration from the command line interface 115
12.7.5 Restoring server configuration from the initialization wizard 115
12.8 Generating a server diagnostics report 116
12.8.1 Downloading the report from the web interface 116
12.8.2 Downloading the report in command line 116
12.9 Updating the SMC server 116
12.9.1 Updating the SMC server from the web interface 116
12.9.2 Updating the SMC server in command line 117
12.10 Resetting "root" and administrator passwords 117
12.10.1 Resetting the "root" administrator password 117
12.10.2 Resetting the administrator password 118
12.11 Disabling automatic synchronization of high availability clusters 118
12.12 Monitoring SMC with SNMP 118
12.12.1 Using the SNMP service 119
12.12.2 Using MIBs 119
12.13 Customizing the certificate of the SMC server web interface 119
12.13.1 Customizing the certificate 119
12.13.2 Reinitializing the certificate 120
12.14 Resetting the internal certification authority of the SMC server 120
12.15 Adding a disclaimer to the login page 120
Appendix A. Details of smc-xxx commands 122
Appendix B. Compatibility of SMC/SN firewalls 124
13. Further reading 125

In the documentation, Stormshield Management Center is referred to in its short form: SMC and Stormshield Network under the short form: SN.

This document is not exhaustive and minor changes may have been included in this version.

1. Getting started with the SMC server

To manage or maintain the SMC server, you can either connect to the web interface with a web browser or directly to the command line interface.

If you have forgotten your password, refer to the section Resetting "root" and administrator passwords.

1.1 Connecting to the SMC server's web interface

1. Connect to the IP address of the SMC server preceded by https://, from one of the following web browsers:
    - Microsoft Edge, latest stable version,
    - Google Chrome, latest stable version,
    - Mozilla Firefox, latest stable version.
2. Enter your login and password, or use the default administrator's login and password.

You can create several administrators for the SMC server's web interface and grant them read/write or read-only access rights. For more information, refer to the section Managing administrators.

The SMC server allows:

- An unlimited number of read/write connections on the SMC server,
- One direct connection via SMC in read/write mode for each firewall,
- An unlimited number of direct connections via SMC in read-only mode for each firewall.

1.2 Connecting to the command line interface

Connecting to the SMC server via the command line is required to perform maintenance or advanced operations on the server. You can connect:

- Via the console port your hypervisor,
- In SSH on port 22.

In both cases, connect with the "root" username and password specified when you initialized the server. For more information, refer to the *Stormshield Management Center Installation Guide*.

For details on commands that can be used to administer SMC, refer to the section Details of smc-xxx commands.

1.3 Installing the SMC license

Your license determines the maximum number of firewalls that can simultaneously log on to the SMC server.

To install the license:

1. Go to **SMC server** > **License**.
2. Select the license file. If a license has already been installed, its information will appear.
3. Click on **Apply**.

1.3.1 Troubleshooting

The SMC server rejects all new firewall connections

- *Situation*: The SMC server rejects all new firewall connections but keeps ongoing connections.
- *Cause*: You do not have a license, your license has expired, or you may have reached the maximum number of firewalls allowed to connect to the server according to your license.
- *Solution*: Look up the server logs and contact your Stormshield support center in order to obtain a valid license. A tool tip and the **Last activity** column will also provide an indication.

Your license is no longer valid after restoring the backup of a configuration

- *Situation*: You have restored the configuration of the SMC server, and your license is no longer valid.
- *Cause*: During the restoration of the configuration, the license that was installed at time of the backup is restored. If it expired in the interim, you no longer have a valid license.
- *Solution*: Once you have restored the configuration, reinstall your most recent license.

2. Warning before connecting SN firewalls to the SMC server

Take note of the following information if you wish to associate the SMC server with an environment of firewalls containing global configuration items already used in production.

When SMC deploys a configuration on a firewall, all existing global configuration items on this firewall will be deleted and replaced with configuration items defined in the SMC configuration, if any.

This includes:

- global objects defined on the firewall
- global filter rules defined on the firewall,
- global VPN tunnels defined on the firewall

These elements are invisible by default in the SNS web configuration interface. To display them, go to the firewall **Preferences**, section **Application settings** and enable the option **Display global policies (Filter, NAT, IPsec VPN and Objects).**

If you connect a firewall to SMC, you accept that any global items you may have created on this firewall will be overwritten as soon as the first configuration is deployed by SMC.

However, local objects, rules and VPN tunnels (used by default in the firewall web administration interface) will never be modified or deleted by SMC in a configuration deployment.

We recommend that you recreate these global items in the form of local items on the firewall or rewrite the rules in SMC before connecting the firewall to SMC, in order to avoid losing any configuration items and disrupting production.

In most frequent cases, the firewall does not have any global configuration elements and then no special precaution must be taken before connecting the firewall to SMC. Production will not be impacted.

In any case, we advise you to perform a backup of your firewall's configuration before connecting it to SMC.

3. Connecting SN firewalls to the SMC server

Connecting a firewall to the SMC server allows you to manage the firewall from the SMC server web interface. A connecting package generated by the SMC server must be installed on the firewall.

The SMC server 3.0 is compatible with Stormshield Network Security in at least version 2.5.0. Some features such as filter and NAT rules and VPN tunnels require SNS in at least version 3.0. For further detail, refer to Compatibility of SMC/SN firewalls.

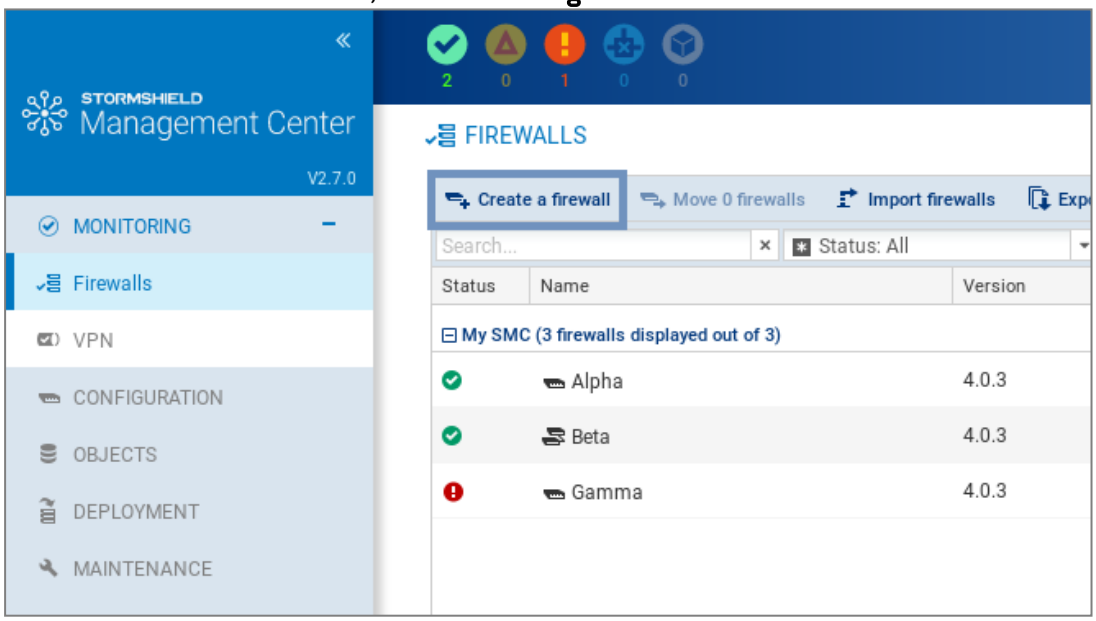
3.1 Connecting a firewall with a factory configuration to the server

The three following steps are required to connect a firewall with a factory configuration to the SMC server:

1. Declaring the firewall in the SMC server web interface
2. Building the firewall connecting package,
3. Installing the connecting package on the firewall.

3.1.1 Declaring the firewall in the SMC server web interface

1. In the SMC server web interface, select **Monitoring** > **Firewalls** and click **Create a firewall**.



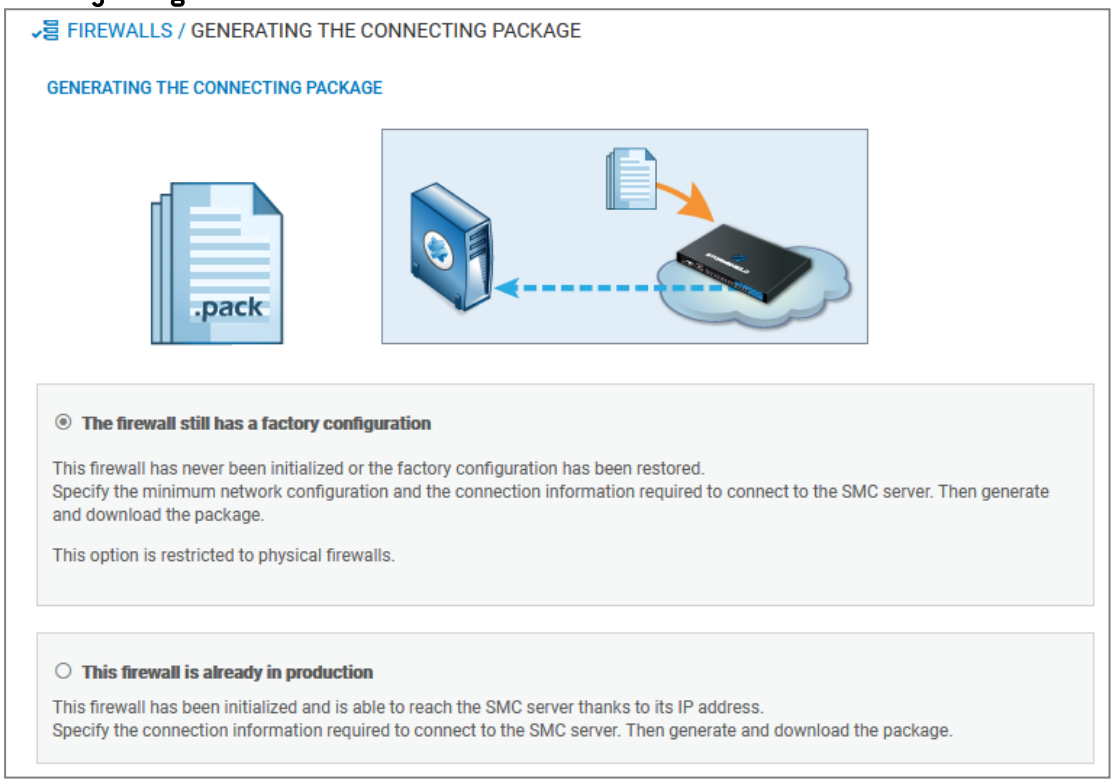
2. Complete the firewall properties. The **Firewall name**, **Description** and **Location** fields are filled in for information only and do not have any impact on the configuration.
3. For more information on the VPN contact address, refer to the section Defining the contact IP address of firewalls for VPN topologies.
4. For more information on the VPN output interface, refer to the section Selecting the output interface of firewalls for VPN topologies.
5. Select the folder in which you wish to organize the firewall. Folders are created in the **Configuration** > **Firewalls and folders** menu on the left. For more information, please refer to the section Organizing firewalls by folders.

3.1.2 Building the firewall connecting package

1. In the same window, select **Generate the connecting package** to generate the package while adding the new firewall. This connecting package will have to be installed on the firewall to connect to the SMC server.

> **TIP**
> You can build the package later, by editing the firewall in the **Firewalls** menu.

2. Click on **Create**.
3. In the **Generating the connecting package** panel, click on **Next** then select **The firewall still has a factory configuration**.



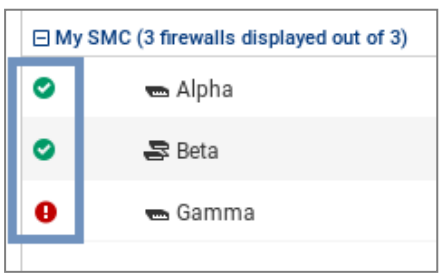
4. On next panel, select the version of the firewall and complete the minimum network configuration information for the firewall that would enable access to the SMC server.

5. Fill in the information to connect to the SMC server. The panel varies according to the version of the firewall. In 3.9.0 and higher versions:
   - **IP address or FQDN**: the firewall connects using these addresses to contact the SMC server. Depending on network topology, they can either be the SMC server's IP addresses or external IP addresses that the firewall can reach, and which are redirected to the SMC server through destination translation. You can set up to ten addresses or FQDNs to contact the SMC server, by order of priority. The firewall browses the addresses from 1 to 10 and connects to the SMC server through the first address reachable. If the address currently used has not the highest priority, the firewall regularly tries to reach an address with greatest priority.
   - **Port**: depending on network topology, they can either be the SMC server's ports (1754 by default) or external ports that the firewall can reach, and which are redirected to the SMC server's port through destination translation.
   - **OUT interface**: you can specify a different outgoing interface for each contact address.
   - For firewalls in version 3.3.X to 3.8.X, only one outgoing interface can be specified, and which will apply for all contact addresses.
   - On firewalls in versions lower than 3.3.X, only one address and a single contact port can be specified. The default outgoing interface cannot be changed.
6. Click on **Generate and download**.

3.1.3 Installing the connecting package on the firewall from a USB drive

IMPORTANT
The connecting package makes it possible to establish a connection from the firewall to the SMC server. Share this package only with trusted users.

1. Provide the connecting package to the administrator in charge of deploying the new firewall on the remote site.
2. Ensure the administrator:
   - copies the connecting package (*.pack*) and a SNS update file (*.maj*) to an empty USB drive. The required formats of the drive is FAT32, FAT16 or UFS. The version 2.3.0 of SNS is the minimum version required.
   - plugs the USB drive into the new firewall and connects the OUT interface to the network.
   - starts the firewall. The firewall first installs the SNS update file and reboots. After restarting, the firewall installs the connecting package: the IP addresses of the SMC server and of the OUT interface of the firewall are configured and the firewall connects to the SMC server.
3. In the SMC server web interface, verify that the state of the firewall changes in the **Firewalls** menu. It must be "On line".



4. To ensure the security of your appliance, log on directly to the firewall's administration interface by clicking on the icon and changing the firewall's administration password. For more information on direct access to the firewall's interface, refer to the section Accessing the web administration interface of firewalls.

TIP
The firewall administrator can see the connection settings to the SMC server on the firewall web administration interface: in the dashboard component and in the menu **Configuration** > **System** > **Management Center**. He/she can also install a new connecting package from the web administration interface.

3.2 Connecting a firewall already in production to the server

The three following steps are required to connect a firewall already in production to the SMC server:

1. Declaring the firewall in the SMC server web interface
2. Building the firewall connecting package,
3. Installing the connecting package on the firewall.

3.2.1 Declaring the firewall in the SMC server web interface

1. In the SMC server web interface, select **Monitoring** > **Firewalls** and click **Create a firewall**.
2. Complete the firewall properties. The **Firewall name**, **Description** and **Location** fields are filled in for information only and do not have any impact on the configuration.
3. For more information on the VPN contact address, refer to the section Defining the contact IP address of firewalls for VPN topologies.
4. For more information on the VPN output interface, refer to the section Selecting the output interface of firewalls for VPN topologies.
5. Select the folder in which you wish to organize the firewall. Folders are created in the **Configuration** > **Firewalls and folders** menu on the left. For more information, please refer to the section Organizing firewalls by folders.

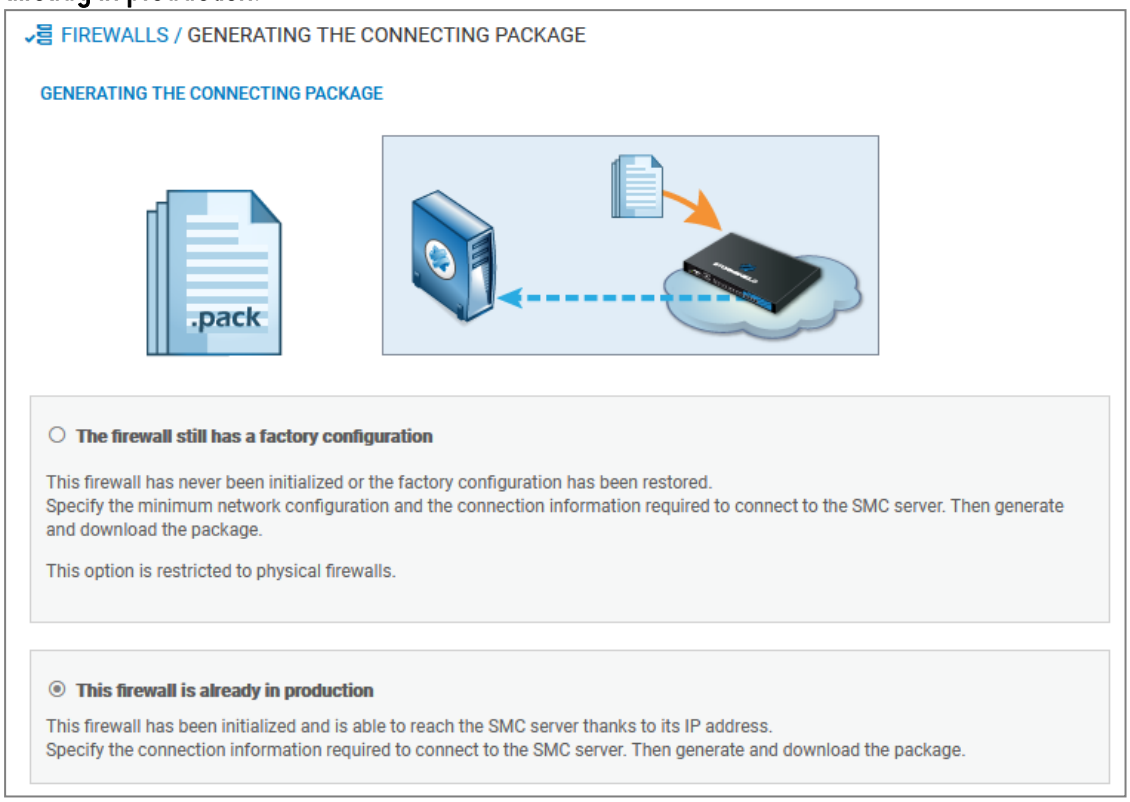
3.2.2 Building the firewall connecting package

1. In the same window, select **Generate the connecting package** to generate the package while adding the new firewall. This connecting package will have to be installed on the firewall to connect to the SMC server.

   TIP
   You can build the package later, by editing the firewall in the **Firewalls** menu.

2. Click on **Create**.

3. In the **Generating the connecting package** panel, click on **Next** then select **This firewall is already in production**.

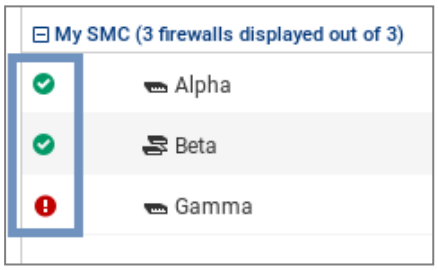


4. On next panel, select the version of the firewall and verify and edit the information to connect to the SMC server if necessary: The panel varies according to the version of the firewall. In 3.9.0 and higher versions:
   - **IP address or FQDN**: the firewall connects using these addresses to contact the SMC server. Depending on network topology, they can either be the SMC server's IP addresses or external IP addresses that the firewall can reach, and which are redirected to the SMC server through destination translation. You can set up to ten addresses or FQDNs to contact the SMC server, by order of priority. The firewall browses the addresses from 1 to 10 and connects to the SMC server through the first address reachable. If the address currently used has not the highest priority, the firewall regularly tries to reach an address with greatest priority.
   - **Port**: depending on network topology, they can either be the SMC server's ports (1754 by default) or external ports that the firewall can reach, and which are redirected to the SMC server's port through destination translation.
   - **OUT interface**: you can specify a different outgoing interface for each contact address.
   - For firewalls in version 3.3.X to 3.8.X and higher, only one outgoing interface can be specified, and which will apply for all contact addresses.
   - On firewalls in versions lower than 3.3.X, only one address and a single contact port can be specified. The default outgoing interface cannot be changed.
5. Click on **Generate and download**.

3.2.3 Installing the connecting package on the firewall

IMPORTANT
The connecting package makes it possible to establish a connection from the firewall to the SMC server. Share this package only with trusted users.

1. Provide the connecting package to the administrator in charge of managing the firewall on the remote site.
2. Ensure the administrator connects to the web administration interface of the firewall.
3. In the menu **Configuration** > **System** > **Management Center** of the firewall administration interface, ensure the administrator selects the connecting package. After the package has been installed, the administrator can see the SMC server connection settings in the same menu. They are also displayed in the SMC dashboard component.
4. In the SMC server web interface, verify that the state of the firewall changes in the **Firewalls** menu. It must be "On line".



3.3 Connecting a high availability cluster to the server

The three following steps are required to connect a high availability cluster to the SMC server:

1. Declaring the cluster in the SMC server web interface
2. Building the cluster connecting package,
3. Installing the connecting package on the active node of the cluster.

3.3.1 Declaring the cluster in the SMC server web interface

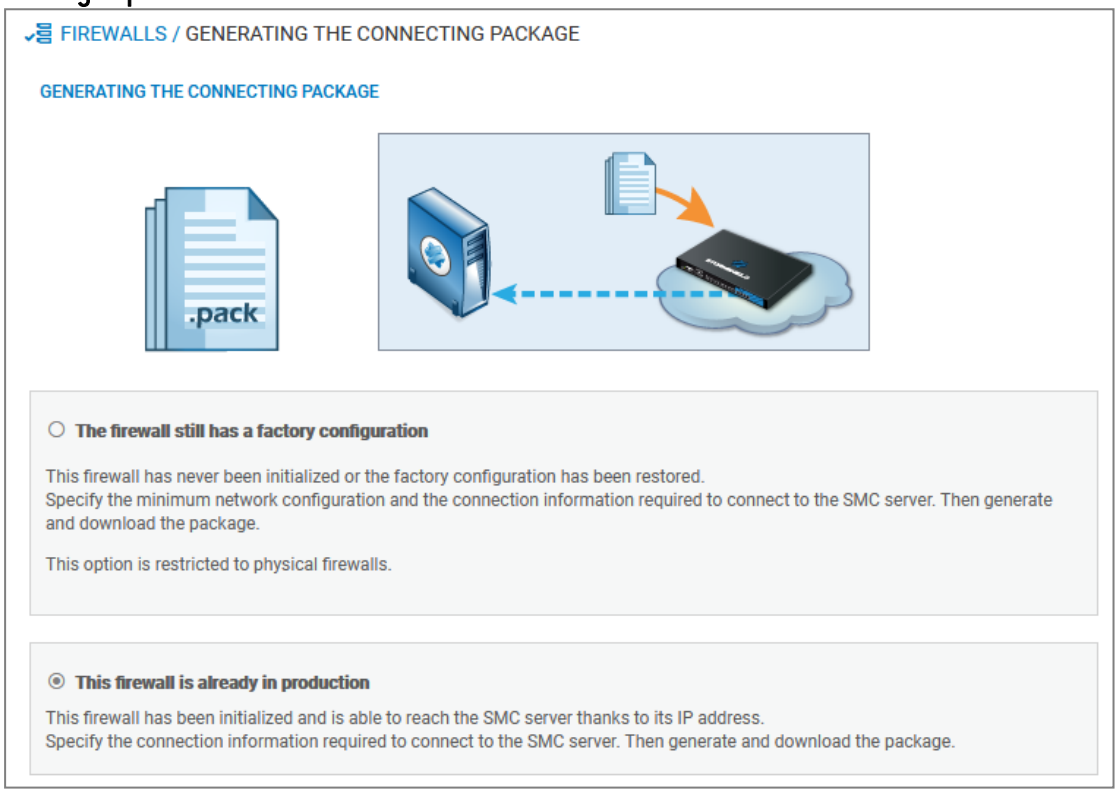
1. In the SMC server web interface, select **Monitoring** > **Firewalls** and click **Create a firewall**. The new firewall stands for the cluster; you do not need to declare both nodes of the cluster.
2. Complete the cluster properties. The **Firewall name**, **Description** and **Location** fields are filled in for information only and do not have any impact on the configuration.
3. For more information on the VPN contact address, refer to the section Defining the contact IP address of firewalls for VPN topologies.
4. For more information on the VPN output interface, refer to the section Selecting the output interface of firewalls for VPN topologies.
5. Select the folder in which you wish to organize the cluster. Folders are created in the **Configuration** > **Firewalls and folders** menu on the left. For more information, please refer to the section Organizing firewalls by folders.

3.3.2 Building the cluster connecting package

1. In the same window, select **Generate the connecting package** to generate the package while adding the new firewall. This connecting package will have to be installed on the firewall to connect to the SMC server.

> **TIP**
> You can build the package later, by editing the firewall in the **Firewalls** menu.

2. Click on **Create**.
3. In the **Generating the connecting package** panel, click on **Next** then select **This firewall is already in production**.



4. On next panel, select the version of the firewall and verify and edit the information to connect to the SMC server if necessary: The panel varies according to the version of the firewall. In 3.9.0 and higher versions:
   - **IP address or FQDN**: the firewall connects using these addresses to contact the SMC server. Depending on network topology, they can either be the SMC server's IP addresses or external IP addresses that the firewall can reach, and which are redirected to the SMC server through destination translation. You can set up to ten addresses or FQDNs to contact the SMC server, by order of priority. The firewall browses the addresses from 1 to 10 and connects to the SMC server through the first address reachable. If the address currently used has not the highest priority, the firewall regularly tries to reach an address with greatest priority.
   - **Port**: depending on network topology, they can either be the SMC server's ports (1754 by default) or external ports that the firewall can reach, and which are redirected to the SMC server's port through destination translation.
   - **OUT interface**: you can specify a different outgoing interface for each contact address.
   - For firewalls in version 3.3.X to 3.8.X and higher, only one outgoing interface can be specified, and which will apply for all contact addresses.
   - On firewalls in versions lower than 3.3.X, only one address and a single contact port can be specified. The default outgoing interface cannot be changed.
5. Click on **Generate and download**.

3.3.3 Installing the connecting package on the active node of the cluster

IMPORTANT
The connecting package makes it possible to establish a connection from the firewall to the SMC server. Share this package only with trusted users.

1. Provide the connecting package to the administrator in charge of managing the cluster on the remote site.
2. Ensure the administrator:
   - connects to the web administration interface of the active node of the cluster.
   - selects the connecting package In the menu **Configuration** > **System** > **Management Center** of the firewall administration interface. After the package has been installed, the administrator can see the SMC server connection settings in the same menu. They are also displayed in the SMC dashboard component.
   - performs a synchronization of both nodes from the administration interface of the active node. The passive node retrieves then the configuration contained in the firewall connecting package.
3. In the SMC server web interface, verify that the state of the cluster changes in the **Firewalls** menu. It must be "On line". The mode icon changes as well: .
   In case of failover, the passive node will become active and will automatically connect to the SMC server.
4. To view different types of information about both nodes of the cluster, edit the cluster in the **Firewalls** menu and open the **High availability** tab.

The SMC server regularly synchronizes both nodes in the high availability clusters of firewalls that it manages. To disable this automatic synchronization, refer to the section Disabling automatic synchronization of high availability clusters.

3.4 Troubleshooting with the server's logs

If you encounter issues while connecting a firewall to the SMC server, start by reading the following log files.

3.4.1 Generating a firewall's connecting package

Refer to the logs on the SMC server, in */var/log/fwadmin-server/server.log*

3.4.2 Installing the connecting package on the firewall

Refer to the logs on the firewall, in */log/l_system* (and */log/verbose.cad* if verbose mode has been enabled).

3.5 Importing SN firewalls from a CSV file

To quickly import a large number of firewalls in SMC and generate their connecting package, you can create a CSV file and import it on the server from the web interface or from the command line interface.

3.5.1 Creating the CSV file

An example of a CSV file "example-import-firewalls.csv" is available on the server, in the folder */opt/stormshield/examples/csv/*.

The file may contain the following parameters organized in columns and separated by commas. The order in which columns appear does not matter. Only the value of the first column #fwname is mandatory, the others may be left blank:

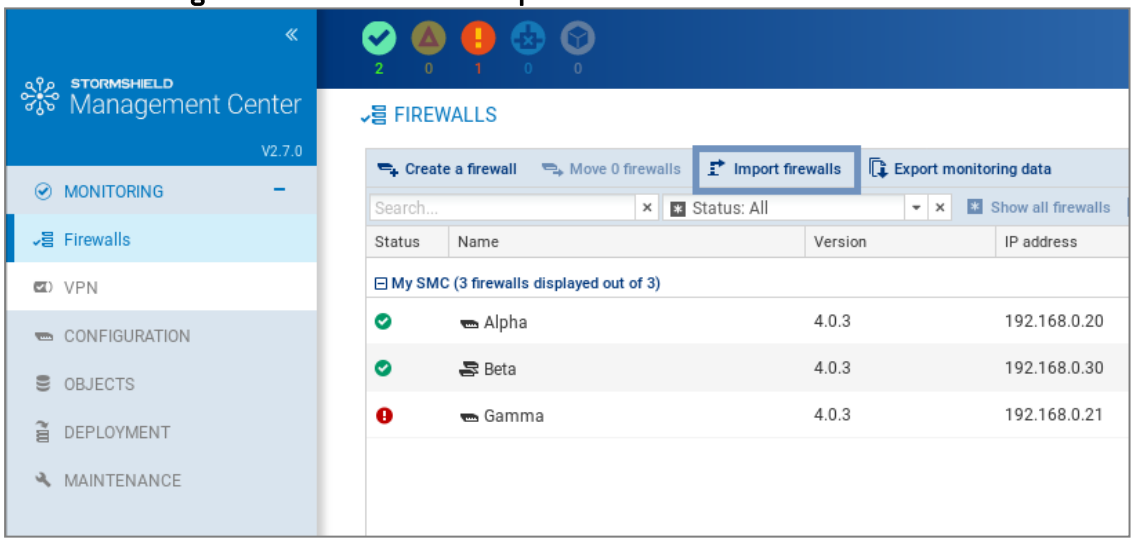
- #fwname: firewall's name,
- #fwversion: version of the firewall used for determining the version of the generated connecting package. If this field is empty, version 4.0.0 will be used.
- #fwdesc: firewall's description,
- #fwplace: location of the firewall,
- #folder: the destination folder of the firewall. A path in the form of <folder1>/<folder2>/... can be specified to indicate the destination folder in the hierarchy of folders. If the specified folders do not yet exist, the SMC server will create them. If this field is empty, the default folder will be the root folder.
- #vpn_fw_public_ip_address: firewall contact IP address manually specified in its settings and used in VPN topologies,
- #vpn_fw_local_address: firewall output interface used as source in VPN tunnels,
- #network_cfg_deploy: defines whether network interfaces can be managed via the SMC server,
- #pkg_fw_address: contact address of the firewall detected by SMC,
- #pkg_fw_netmask: subnet mask,
- #pkg_fw_gateway: the firewall's default gateway,

- #pkg_smc_addresses (IP1:PORT1:BINDADDR1,IP2:PORT2): the IP address, port and outgoing interface of the SMC server. This information is needed for the connecting package. The outgoing port and interface are optional. On SN firewalls in version 3.9 and upwards, you can specify an outgoing interface for each IP address. On firewalls from versions 3.3.X to 3.8.X, only the first outgoing interface will be taken into account.
- vpn_fw_subject_dn: for certificates obtained via SCEP or EST, the Distinguished Name of the subject of the firewall's default certificate,
- vpn_fw_issuer_dn: for certificates obtained via SCEP or EST, the Distinguished Name of the issuer of the firewall's default certificate.

IMPORTANT
Check that the CSV file editor has not modified the "," separator character, in which case the file may not be imported on the SMC server. For more information on the separator character, refer to the section Choosing the separator character in CSV files.

3.5.2 Importing firewalls from the web interface

1. Select **Monitoring** > **Firewalls** and click on **Import firewalls**.



2. Select the CSV file.
3. Select all the necessary options.
4. The following window will show a summary of the operations and enable connecting packages to be downloaded if you have selected this option.

If some of the firewalls in the file already exist on SMC, their properties will be updated with the new values found in the file. If any cell in the file is empty, the value will be considered empty and the older value will be overwritten.

If you wish to keep an existing value, delete the relevant column in the CSV file.

3.5.3 Importing firewalls in command line

IMPORTANT
When several administrators are connected at the same time, we recommend that you import

firewalls from the web interface instead of in command line, so that each administrator will be informed when changes are applied.

1. Start by copying the CSV file on the SMC server using the SSH protocol in the */tmp* folder for example. This example is used in the procedure below.
2. Connect to the SMC server via the console port or SSH connection with the "root" user.
3. Enter the command:
   `smc-import-firewalls /tmp/filename.csv`.

To change the value of the delimiter character, use the environment variable FWADMIN_CSV_DELIMITER.

Generated connecting packages are available in the folder */tmp/import-firewalls-[date of import]*.

The status of an import will be indicated for each firewall, as well as a summary when the import is complete.

You can also:

- Import firewalls without generating connecting packages, using the option `--firewall-only`:

```
smc-import-firewalls /tmp/filename.csv --firewall-only
```

- Generate only connecting packages, using the option `--package-only`:

```
smc-import-firewalls /tmp/filename.csv --package-only
```

If an imported firewall already existed in SMC, it will be automatically updated after the script is run.

4. Supervising SN firewalls

The different types of information about each firewall shown in **Monitoring** > **Firewalls** make it possible to view and monitor firewalls. The logs and activity reports of a firewall can also be accessed directly.

TIP
Click on the Stormshield logo in the upper banner to go back to the firewalls monitoring screen.

4.1 Monitoring and organizing firewalls

Look up the status of your environment in real time and organize your firewalls by a hierarchy of folders and sub-folders to which you can apply shared or specific filter and NAT rules.

4.1.1 Getting information about firewalls

From the **Monitoring** > **Firewalls** menu, you can see varied information about each firewall such as its health status, IP address, model, deployment number, maintenance end date, license options subscribed, etc.

Some columns are hidden by default in this monitoring view. To show a column:

1. Scroll over any column title with the mouse,
2. Click on the black arrow that appears,
3. Scroll over the **Columns** menu,
4. Select the columns that you prefer.

From this menu, you can also edit the configuration, access the web administration interface, logs and activity reports of a firewall, import a certificate on a firewall, check its usage and remove a firewall from the list.

Five different icons indicate the health status of the firewalls in the first column of the list:

- : the firewall is running,
- : the firewall has a non critical issue,
- : the firewall has a critical issue,
- : the firewall is disconnected,
- : the firewall has never been connected to the SMC server.

Scroll the mouse over the icons to display a tooltip detailing the health status for each firewall. For more information on health indicators, refer to the section on **Health indicators** in the *Stormshield Network User Configuration Manual*.

To filter the firewall list according to the health status:

- Click on the status icons in the upper banner of the interface.

- or -

- Use the status drop-down menu above the firewall list. The **Connected** filter displays firewalls that are **Running**, **Not critical** and **Critical**.

For each connected firewall, information about the CPU, the memory used and the disk space used are available. The values displayed about the CPU and memory apply to the latest hour. Move the mouse over the diagrams to see more details.

The "Local modification" and "Configuration validation" health indicators are provided by the SMC server and relate to deployment issues. For more information, refer to Detecting changes to the local configuration on firewalls and Validation of the deployment failed.

Troubleshooting

The firewall does not display a valid maintenance end date

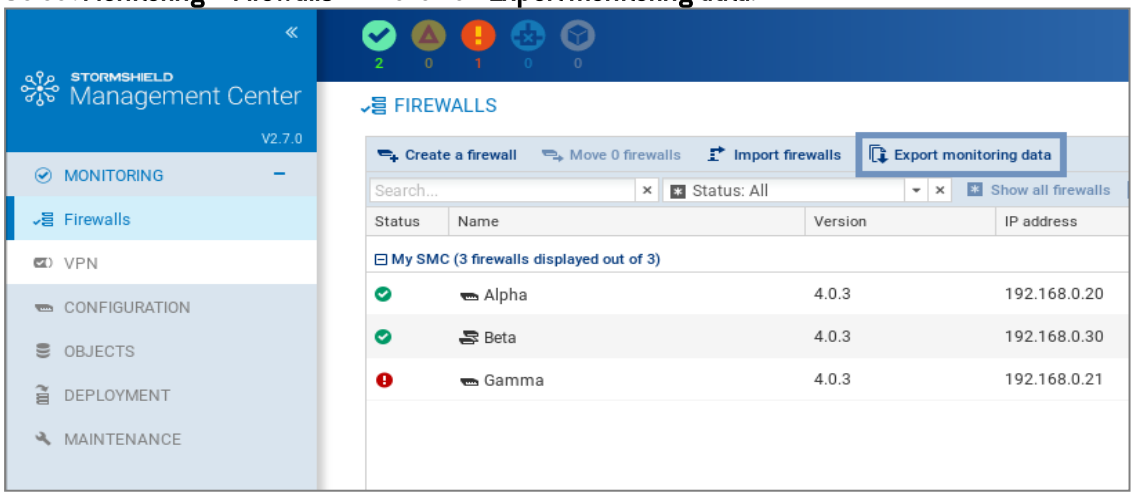
- *Situation*: In Monitoring view, the column indicating the date on which maintenance of the firewall ends is empty.
- *Cause*: Either the firewall's license is not valid or its version is lower than 2.5. The SMC server does not manage the maintenance end date for firewalls in versions 2.3 and 2.4.
- *Solution*: Contact your Stormshield support center in order to obtain a valid license or upgrade the firewall to version 2.5 or higher.

4.1.2 Exporting monitoring data

In the SN firewall monitoring panel, you can export and download monitoring data to a CSV file.

Data can be exported in read/write or read only mode.

1. Select **Monitoring** > **Firewalls** and click on **Export monitoring data**.



2. Save the CSV file.

By default, data in the file is separated by commas, but you can change the delimiter using the environment variable `FWADMIN_CSV_DELIMITER`.

Refer to the log file *export.log* if you encounter any issues. For more information, please refer to the section Viewing SMC server logs.

4.1.3 Organizing firewalls by folders

In order to manage firewalls and their configuration, the SMC server relies on hierarchically organized folders to which firewalls are attached.

Since folders are dynamically managed, you can create, move and delete folders at any time.

Folders contain firewalls as well as global filter and NAT rules. A firewall attached to a sub-folder inherits rules configured in its parent folders. For more information on filter and NAT rules, refer to the section Creating filter and NAT rules.

A firewall can belong to only one folder at a time.

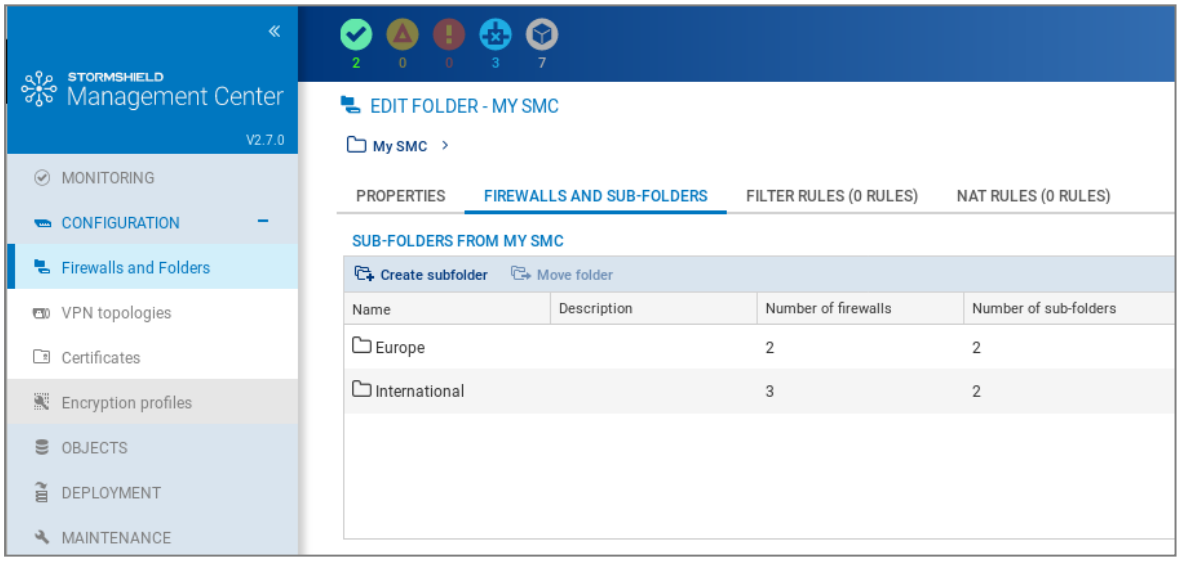
The default root folder **MySMC** cannot be deleted. You can rename it to fit your needs. If you do not create any folder trees, all firewalls will be attached to this root folder.

The tree is limited to four levels of sub-folders.

TIP
The **Search** field in the list of firewalls in **Monitoring > Firewalls** also applies to folder names.

Creating folders

1. Go to the *Firewalls and sub-folders* tab in **Configuration > Firewalls and sub-folders.**
2. Click on **Create a sub-folder** when you are in the desired parent folder.



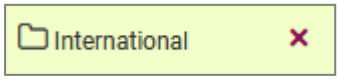
Organizing firewalls

There are several ways to do so:

- when you create a new firewall from **Monitoring > Firewalls** or **Configuration > Firewalls and folders**, in the **Firewalls and sub-folders** tab, you can choose its location.
- you can move an existing firewall from the same panels by clicking on **Move 1 firewall**. Multiple firewalls may be selected.

Removing folders

In the *Firewalls and sub-folders* tab in **Configuration > Firewalls and folders**, scroll over the folder name and select the red cross.



If you delete a folder, firewalls and rules in this folder will be moved by default to the parent folder.

4.1.4 Checking usage of a firewall in the configuration

In order to check whether a firewall is used:

1. Go to **Monitoring** > **Firewalls** or **Configuration** > **Firewalls and folders**,
2. Scroll over the name of the firewall and click on the icon . The results will be displayed in the column on the left. You can double-click on a result to view details.

4.2 Accessing firewall logs and activity reports

You can access the logs and activity reports of connected firewalls directly from the SMC server.

In **Monitoring** > **Firewalls**, move the mouse next to the name of a firewall and click the icon .

Authentication on the firewall is automatic:

- You do not need to set a login on this firewall,
- You do not need to configure any authorized administration host in the web administration interface of the firewall,
- Logging out from the SMC server web interface automatically disconnects the user from the firewall's interface.

For more information about the monitoring interface, refer to the *Stormshield Network User Configuration Manual*.

5. Configuring SN firewalls

Configure your firewalls, objects, rules, VPN topologies and network interfaces in the SMC server web interface and deploy the configuration on the firewalls. The firewall's web administration interface can also be accessed directly.

Certain configuration operations cannot be performed from the web interface of the SMC server. You can perform them using SNS CLI commands. For more information, please refer to the section Running SNS CLI commands on a pool of firewalls.

5.1 Editing firewall settings

To edit the settings of a firewall:

1. Go to **Monitoring** > **Firewalls** or **Configuration** > **Firewalls and folders**.
2. Scroll over to the name of the firewall and click the pen icon , or double-click the line on which the firewall is found.

The series of tabs that appears will allow you to:

- Modify the location of the firewall in the folder tree,
- Enable the configuration of network interfaces from the SMC server. This feature is disabled by default and the **Network interfaces** tab is in read-only mode.
- Generate a connecting package for the firewall. For more information about this package, refer to Connecting SN firewalls to the SMC server.
- Add customized variables used in SNS CLI scripts or in network objects,
- Create and manage filter and NAT rules,
- Manage network interfaces; refer to Managing network interfaces.
- Define the contact address and the output interface to be used by default in VPN topologies,
- Add a certificate on the firewall,
- Obtain information about high availability when clusters are used.

The **Firewall name**, **Description** and **Location** fields in the **Parameters** tab are filled in for information only and do not have any impact on the configuration.

TIP
The **Search** field in the firewalls list also applies to the **Description** and **Location** fields.

5.2 Creating customized variables

Global customized variables can be created for all SN firewalls connected to the SMC server, and can be used in:

- Host, Network and IP address range network objects in order to create objects with IP addresses that will be determined dynamically according to the firewall,
- SNS CLI scripts in order to execute grouped commands on your pool of firewalls.

Customized variables can be added, changed or deleted in any firewall's properties.

To set the values of each variable for specific firewalls, you need to go to the properties of the firewalls in question.

You can create as many customized variables as needed.

5.2.1 Adding, changing or deleting customized variables

1. Go to **Monitoring > Firewalls** or **Configuration > Firewalls and folders**.
2. Scroll over to the name of any firewall and click the pen icon , or double-click the line on which the firewall is found,
3. Go to the **Customized variables** tab. You can access the same **Customized variables** table shown in the table from any firewall; it allows you to customize the values of variables for the current firewall, as shown in the following section.
4. Click on **Manage global variables**.

Several actions can then be performed in the window:

- Whenever you click on **Add** and enter a name for the variable, the syntax %CUSTOM_X% will automatically be applied to the name. Spaces and dashes are not supported in variable names.
- Existing variables can be deleted, unless they are being used in objects.
- The **Copy to clipboard** button allows you to copy the variable in order to use it in network objects.
- The **Check usage** button displays all the firewalls and objects that use the variable. It can also be found in the **Custom variables** tab. In the results panel that opens in the lower part of the window, you can click on items to display and modify them.
- Variables can be exported and imported in CSV format. The columns in a CSV file are: #variable,#comment,#firewall,#value. Importing variables makes it possible to create or modify other variables, but not delete existing variables.
- Variables can be commented. Comments and variables can be seen in every firewall's properties, but can only be modified in the **Manage global variables** window.

- Whenever you click on **Add** and enter a name for the variable, the syntax %CUSTOM_X% will automatically be applied to the name. Spaces and dashes are not supported in variable names.
- Existing variables can be deleted, unless they are being used in objects.
- The **Copy to clipboard** button allows you to copy the variable in order to use it in network objects.
- The **Check usage** button displays in the left panel all the firewalls and objects that use the variable. It can also be found in the **Custom variables** tab.

- Variables can be exported and imported in CSV format. The columns in a CSV file are: #variable,#comment,#firewall,#value. Importing variables makes it possible to create or modify other variables, but not delete existing variables.
- Variables can be commented. Comments and variables can be seen in every firewall's properties, but can only be modified in the **Manage global variables** window.

5.2.2 Defining the value of a customized variable for a firewall

Values of variables do not have to be defined for all firewalls.

To define the value of a variable for a specific firewall:

1. Go to the **Customized variables** tab in the firewall's settings,
2. Double-click on the **Value on the firewall** column to assign a value to the variables defined in the previous step.

As variable names and comments are common fields for all firewalls, click on **Manage global variables** to change them.

5.3 Verifying configuration consistency

The consistency checker is a tool that analyzes the consistency of your configuration in real time. In the lower panel of the SMC server web interface, it shows warnings and errors if it has detected any.

To show the consistency check:

1. Select **Maintenance** > **Consistency check**.

- or -

1. Open the lower panel of the screen by clicking on the black arrow at the bottom of the interface .

The consistency checker shows all warnings and errors affecting all firewalls. However, error analyses take priority over warning analyses. If a firewall reports at least one error, the analysis of warnings on this firewall will be canceled.

You can filter these warnings and errors by firewall or by inconsistency, or by entering a character string in the search field.

By clicking on certain items (filter or translation rules, objects, etc.), you can go straight to the panels or items in question.

The consistency checker also runs when configurations are deployed. However, only errors are checked; warnings are ignored. When an error is detected, the deployment will fail.

5.3.1 Disabling the consistency check

The environment variable `FWADMIN_ENABLED_CFGCHECK` makes it possible to disable the consistency check whenever necessary.

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. Edit the file **/data/config/fwadmin-env.conf.local** by adding the following line at the end: `FWADMIN_ENABLED_CFGCHECK=false`.
3. Restart the server with the command `nrestart fwadmin-server`.

5.3.2 Disabling check areas

You can specifically disable checks in some areas or disable some of the configuration consistency checks.

1. To know which entries can be disabled, refer to the file **/opt/fwadmin-server/config/cfgcheck.ini** without modifying it.
2. In the file **/data/config/cfgcheck.ini**, add the keys or sections you want to disable.

5.3.3 Restricting the number of inconsistencies reported

The number of inconsistencies reported by the checker can be restricted by using the environment variable `FWADMIN_CFGCHECK_INCOHERENCIES_LIMIT`. By default, up to 100 inconsistencies are reported. Once this limit is reached, SMC will cancel all pending analyses.

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. In the file **/data/config/fwadmin-env.conf.local**, change the value of the environment variable: `FWADMIN_CFGCHECK_INCOHERENCIES_LIMIT`.
3. Restart the server with the command `nrestart fwadmin-server`.

5.4 Deploying a configuration on firewalls

Every time a configuration is created or modified on the SMC server, you will need to deploy the configuration on firewalls.

All deployments are saved in the deployment history. Refer to the section Loading and deploying a former configuration.

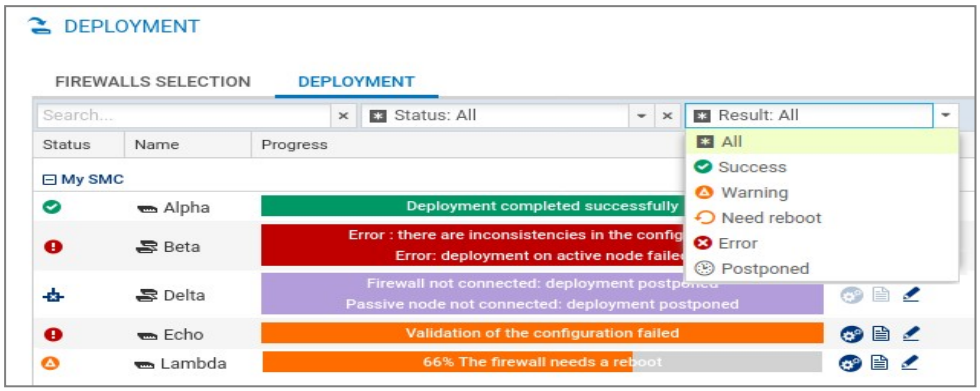
During a deployment, the following information will be sent to the firewalls:

- Objects used in filter and NAT rules relating to the firewall or its parent folders.
- Objects you have chosen to deploy on all firewalls or for which you have selected the firewalls they will be deployed on. For more information, please refer to the section Managing network objects.
- If the firewall is part of a VPN topology: Network, Host and/or Group objects and the certification authority associated with this topology, as well as information on the certificate selected for this firewall in the topology (the certificate has already been installed on the firewall).

5.4.1 Deploying a configuration on a firewall from the web interface

1. Go to **Deployment > Configuration deployment** or click on the button in the upper banner of the interface. This button turns orange when changes have been made to the configuration.
2. In the **Firewalls selection** tab, select firewalls.
3. Enter a comment at the bottom of the panel if needed. This comment will be displayed in the deployment history.
4. Click on **Deploy configuration** next to the comment field. The **Deployment** tab automatically opens. A status bar indicates the progress and the result of the deployment for each firewall. When a deployment or an SNS CLI script is running, you cannot launch another deployment but preparing another deployment in the **Firewalls selection** tab is possible.
5. During or after the deployment, you can click on the status bar of a firewall to display a summary of the deployment on this firewall. For more information regarding the deployment, use the command `clogs` in the command line interface.
6. See the deployment summary at the bottom of the panel, showing successful operations, warnings, errors and postponed deployments.

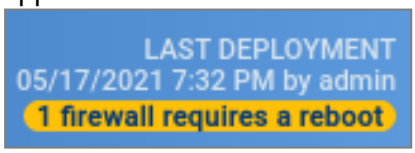
7. You can also filter the list of firewalls by selecting a deployment result in the drop down list at the top of the list.



If the deployment is successful, the deployment number will be incremented in the **Deployment** column.

> **TIP**
> If a configuration is deployed on disconnected firewalls, the deployment is postponed and firewalls retrieve the configuration the next time they are on line.

8. In case of error, see the SMC server logs. You can also connect to the logs and activity reports of a firewall by clicking the icon in the **Actions** column and refer to the firewall logs.
9. If the firewall requires a reboot to finalize the deployment, this is indicated by the health status "Reboot required". You can start the reboot directly from the deployment window by clicking on the **Reboot** button at the bottom of the window. You can also restart the firewall at a later point in time from the supervision, configuration and deployment windows or by clicking on the information displayed on the right-hand side in the top banner of the application:



10. After a configuration is deployed for the first time, the SMC server will regularly check whether the configuration deployed from the firewall continues to match the configuration on SMC. Refer to Detecting changes to the local configuration on firewalls.

5.4.2 Deploying a configuration on a high availability cluster

The steps are the same as in the section above.

The configuration is first deployed on the active node of the cluster. The SMC server then synchronizes both nodes of the cluster.

If the passive node is not connected to the active node at the time of deployment, the SMC server will perform a synchronization between both nodes when the passive node connects again to the active node.

5.4.3 Deploying a configuration on a firewall in command line

You can use the `smc-deploy` command to deploy a configuration in command line.

Apply the command to the list of targeted firewalls (on which the configuration is to be deployed) using one of these options:

- --all: deploys on all firewalls,
- --firewall-list <firewallNames>: deploys on certain firewalls (separated by commas).

To see the other options that this command offers, type `smc-deploy --help`.

At the beginning of the deployment, the deployment number will appear.

5.4.4 Keeping the connection alive during deployment

Before a new configuration deployed by SMC is installed on an SN firewall, its configuration will be backed up. So if a deployment alters the connection between the SMC server and an SN firewall, the most recent backup will be restored. This mechanism guarantees that the SMC server will always be able to reach the SN firewall. You can manage this feature for individual firewalls by using two environment variables:

Variable	Description
FWADMIN_SNS_DEPLOYMENT_TIMEOUT_BEFORE_ROLLBACK By default: 30 seconds	Sets the amount of time in seconds that SMC will attempt to reconnect. Once this duration is exceeded, the previous configuration will be restored. Setting the variable to 0 disables the feature.
FWADMIN_SNS_DEPLOYMENT_TIMEOUT_ROLLBACK By default: 180 seconds	Sets the amount of time in seconds between the restoration of the configuration and the reconnection to the SMC server. If the connection is not up again after this duration, the deployment will be considered a failure. We do not recommend setting a value lower than the default value.

5.4.5 Troubleshooting with the server's logs

If you encounter issues while deploying a configuration, start by reading the following log files.

SMC side

/var/log/fwadmin-server/cfg2ini.log, */var/log/fwadmin-server/server.log* and */var/log/fwadmin-server/connections.log*

Firewall side

/log/l_system

5.4.6 Troubleshooting

Validation of the deployment failed

- *Situation*: After the configuration was deployed on the firewall, the status of the firewall switched to **Critical** and indicated "Configuration validation". The command `CONFIG STATUS VALIDATE` therefore failed.
- *Cause*: The password used to validate the configuration on the SN firewall was probably changed and no longer matched the one saved on SMC. Check the server's logs to find out the exact cause.

- *Solution*: Connect to the firewall to fix the issue. If the reason is an invalid password; run the command `CONFIG STATUS REMOVE`.

5.5 Loading and deploying a former configuration

Each configuration deployed on firewalls is saved in the deployment history and can be loaded and deployed again.

To see the deployment history and deploy a configuration again:

1. Go to **Deployment** > **Deployment history**.
2. Select a deployment and click the icon to restore the configuration. Ongoing changes in the current configuration will be lost.
3. Repeat the steps described in the section Deploying a configuration on firewalls to deploy a configuration on firewalls.
4. If you load a configuration which is not the latest in the history, a warning message appears at the top of the window. The message remains until you deploy the configuration on firewalls or until you load the latest configuration deployed.

NOTE
The deployment history is cleared every time the SMC server is updated, therefore containing only the revisions of a current version. The history cannot be used to restore the configuration of an older version after the update.

5.6 Generating a configuration comparison

Before deploying a new configuration on your pool of firewalls, for each firewall, you have the possibility of comparing the last configuration deployed on the firewall in question with the configuration prepared on the SMC server and ready to be deployed on firewalls.

1. Go to **Deployment > Configuration deployment** or click on the button in the upper banner of the interface. This button turns orange when changes have been made to the configuration.
2. In the **Deployment** column, click on a firewall's icon to display its configuration comparison.
   - The comparison appears in raw format and only shows changes concerning the firewall in question. For clusters, only the active node will be taken into account.

From this window displaying the comparison, you can either download the comparison or download the configuration file in *.na* (format that can be used on SN firewalls) or *.tgz* (configuration files that can be read in a text editor) formats, or deploy the configuration on the firewall.

Once you have viewed the comparison, a status icon can be seen in the **Deployment** column indicating that:

- : the configuration has not been changed, so deployment is not necessary,
- : the configuration has been changed, and the changes have been listed in the display window. Click on the icon to see the changes that were made to the configuration.
- : the status is unknown, or the last comparison is no longer valid. Click on the icon to refresh the status.

To view changes to the local configuration on a firewall after it has been deployed, refer to Detecting changes to the local configuration on firewalls.

5.7 Detecting changes to the local configuration on firewalls

After a configuration is deployed for the first time, SMC will regularly check whether the configuration deployed from the server continues to match the one found on the firewall. The SMC server can therefore detect changes made directly on the SN firewall without going through SMC.

You can manage verifications by using an environment variable:

Variable	Description
FWADMIN_CONFIG_STATUS_CHECK_PERIOD By default: 120000 ms	The variable defines the frequency with which SMC will check the configuration on firewalls. The value is defined in milliseconds. Setting a variable to 0 disables the feature; the configuration on firewalls will no longer be verified.

If SMC detects changes to the configuration that were made locally, the status of the firewall switches to **Critical** and the "Local modification" health indicator will appear.

The version number will therefore be struck through in red because it no longer matches the configuration on the firewall.

Do note that SMC detects only changes to the files that it deploys. An SN firewall update will not be considered a local modification.

5.7.1 Viewing local changes on a firewall

In the **Deployment** menu, click on next to the version number to view changes made locally on the firewall. In the window that opens, you can:

- download the comparison of the configuration on the firewall with the latest configuration deployed from the SMC server.
- restore the configuration prior to the changes made locally.

5.8 Managing network interfaces

The network interfaces of your connected firewalls can be managed from the SMC server.

Go to the settings of the firewall in question and select the check box **Manage the configuration of network interfaces from SMC**. This option is disabled by default and the **Interfaces** tab of the firewall is in read-only mode.

As the SMC server automatically displays the interfaces of your SN firewall, you can configure them from a central point. For more information on interface configuration, refer to the *Interfaces* section in the *Stormshield Network User Configuration Manual*.

Version 3.0 of SMC makes it possible to configure the following network interfaces in IPv4:

- Ethernet interfaces
- Bridges
- VLANs
- Aggregates
  Two aggregation modes are possible - either LACP, which is the default mode, or Failover (only for SN firewalls in version 4.3 and higher).

When deploying the network configuration, the existing VLAN, aggregate and bridge interfaces on the firewall are not preserved. The network configuration deployed from the SMC server will overwrite the local configuration on the firewall.

5.8.1 Limitations to the configuration from the server

- Currently, configuration in IPv6 is not supported.
- High availability: The network interfaces used for high availability links are shown on the SMC server but cannot be configured.
- Monitoring: Currently interfaces cannot be monitored from the SMC server. To monitor the interfaces of a firewall, connect to the firewall in question.
- Configuring modems: Currently, the **Safety/Bypass** mode is not supported.
- The **Status** column does not make it possible to identify the state of the interface's connection, but only indicates whether it is enabled or disabled.
- For interfaces configured in DHCP, SMC does not display their values in detail.
- Bridge: A bridge can be modified and deleted even if it contains interfaces that are not managed by the SMC server.
- GRE/GRETAP interfaces are not supported. VLAN interfaces connected to a GRETAP are therefore not displayed on the SMC server.

5.9 Accessing the web administration interface of firewalls

The SMC server web interface does not allow configuring all parameters of a firewall. To complete the configuration, it is possible to connect directly to the web administration interface of a firewall, without the need to authenticate.

1. Go to **Monitoring** > **Firewalls**.
2. Scroll over the name of a firewall. The firewall must be on line.
3. Click on the icon.

Authentication on the firewall is automatic:

- You do not need to set a login on this firewall,
- You do not need to configure any authorized administration host in the web administration interface of the firewall,
- Logging out from the SMC server web interface automatically disconnects the user from the firewall's web administration interface.

TIP
The indication "Managed by SMC" appears at the top of the firewall administration interface.

For more information about the web administration interface, refer to the *Stormshield NetworkUser Configuration Manual*.

5.10 Using the Emergency mode

In case of temporary unavailability of the SMC server, if you need to edit the configuration of a firewall, connect directly to the IP address of the web administration interface of the firewall.

TIP
The indication "Managed by SMC - Emergency mode" appears at the top of the firewall web administration interface.

5.11 Converting a firewall connected to the SMC server into a high availability cluster

A standalone firewall connected to the SMC server can be converted into a high availability cluster:

1. From the SMC server web interface, connect to the web administration interface of the firewall by clicking the icon in the list of firewalls in the **Monitoring** menu.
2. Refer to the *Stormshield Network User Configuration Manual* under *High availability* to add a passive node. In a failover, the passive node will become active and will automatically connect to the SMC server

TIP
The icon in the **Mode** column is updated in the firewalls list of the SMC server web interface. To view details about both nodes of the cluster, edit the cluster in the **Firewalls** menu and open the **High availability** tab.

5.12 Importing or declaring a certificate for a firewall

A DER or PEM certificate is required for each firewall that is part of a VPN topology using .X509 authentication.

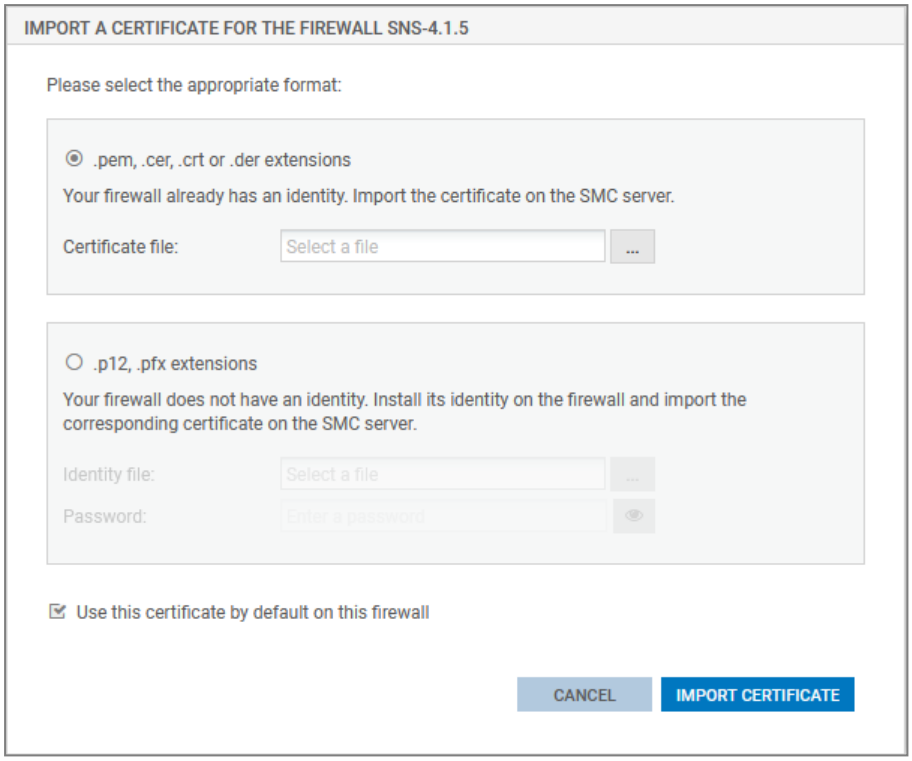
A PKCS#12 identity can be installed on the firewall from the SMC server, which retrieves the corresponding certificate.

The certificate can be imported on the SMC server from the server's web interface or from the command line interface. Several certificates may be imported for a single firewall.

Certificates used by an SN firewall can also be declared on SMC without having to import them on the server (SCEP or EST protocols).

5.12.1 Importing a certificate from the server's web interface

Certificates can be imported for a firewall from several panels in the web administration interface.



1. In the **Monitoring > Firewalls** menu, double click on a connected firewall.
2. In the **IPSec VPN** tab, select the **By file** option.
3. Click on **Import a new certificate**. The link will take you to the **Configuration** > **Certificates** menu.
4. Scroll over the name of the firewall in the **Firewall** column and click on the icon. For further information regarding the **Certificates** menu, refer to Managing certificates and certification authorities.

-or-

1. In the **Monitoring > Firewalls** menu, scroll over the name of a connected firewall and click on the icon.

-or-

1. In the **Configuration** > **Certificates**, click on **Import certificate** at the top of the grid. For further information regarding the **Certificates** menu, refer to Managing certificates and certification authorities.

-or-

1. During the configuration of a VPN topology, when choosing peers, click on the icon on the line of a firewall. For more information, please refer to the section Creating policy-based VPN topologies.

The option **Use this certificate by default on this firewall** allows you to select the certificate to be used for VPN negotiations. There can only be one default certificate for each firewall. To change the default certificate later, refer to the section Changing the certificate used by default in VPN topologies.

5.12.2 Importing a certificate from the command line interface

1. To import a certificate from the command line interface, connect to the SMC server via the console port or SSH connection with the "root" user.
2. Enter the command
`smc-install-certificate`

TIP
Display help using the option --help:

```
[root@smc] - {~} > smc-install-certificate --help
Usage: smc-install-certificate [options]

A tool that imports a certificate file (.p12 or .pfx) on a SNS Firewall.

The certificate's password will be prompted if not provided through the -p option.
It is required for the installation on the Firewall.

Options:
  -V, --version                output the version number
  -c, --certificate <filepath>  The certificate to import on the firewall
  -f, --firewall <name>         The target firewall name
  -F, --force                   Force disconnection of any read-write session currently logged in.
  -p, --password <password>     The password of the certificate
  -h, --help                    output usage information
```

Three of these options are mandatory:

- --certificate: path of the certificate(*.p12* or *.pem*) to be installed,
- --firewall: name of the firewall on which the certificate needs to be installed,
- --password: password that protects the certificate if a *.p12* file is used.

The operation will be saved in the log file*/var/log/misc/install-certificate.log*.

5.12.3 Importing a certificate on a high availability cluster

Import the certificate for the active node of the cluster.

The SMC server will then synchronize both nodes of the cluster.

5.12.4 Troubleshooting

The Import button remains grayed out

- *Situation*: You have selected the certificate and entered the password but the **Import** button remains grayed out.
- *Cause*: When running a script or deploying a configuration, you will not be able to import any certificates for any firewalls.
- *Solution*: Wait for the script to finish its run or for the configuration to be fully deployed.

Importing the certificate on a firewall causes an error

- *Situation*: When you import a certificate on a firewall, the SMC server returns the error "Insufficient privileges".
- *Cause*: You are unable to import a certificate on a firewall on which a session has been opened either directly or via SMC.
- *Solution*: Log off from the firewall and attempt to import the certificate again.

Other possible causes

- The file exceeds the maximum limit allowed, which is 1 MB.
- The file format is neither *.p12* nor *.pem*. The SMC server only supports *.p12* or *.pem* files.
- You have entered the wrong password.

5.12.5 Declaring a certificate used by a firewall

Certificates used by an SN firewall can also be declared in SMC by indicating their subject and issuer. You therefore do not need to import the certificate on the server.

This feature may be useful whenever the firewall generates its own keys and obtains a certificate automatically from the certification authority via SCEP or EST.

There can only be one certificate obtained via SCEP or EST for each firewall.

1. In the **Monitoring** > **Firewalls** menu, double click on a connected firewall.
2. In the **IPSec VPN**, select **By subject and issuer names** and enter the corresponding information.

To enable the renewal of expired certificates that were obtained via SCEP or EST, on the SMC server, indicate the address of an SCEP or EST server in the properties of a certification authority. For further information, refer to the section Managing certificates and certification authorities.

5.12.6 Changing the certificate used by default in VPN topologies

If you have imported several X509 certificates for a firewall, to find out which certificate is used by default in VPN topologies:

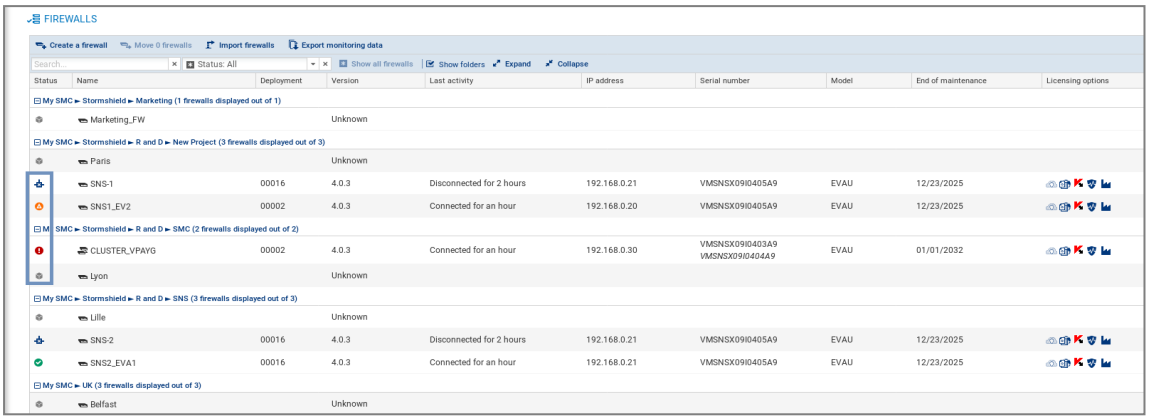
1. Go to **Monitoring** > **Firewalls**, and double click on the row of the firewall in question.
2. Open the **IPSec VPN** tab. The certificate used by default is the certificate selected in the **Certificate for authentication** section.

To change the certificate used by default, select another certificate from the drop-down list or import a new certificate.

You cannot delete the certificate used by default if it is in use in a VPN topology.

5.13 Configuring the warning for an imminent certificate expiry

Whenever the certificate of an SN firewall is close to expiry, the health status of the firewall switches to **Not critical** in the firewall monitoring window.



Once the certificate has expired, the firewall's health status will become **Critical** .

The firewall will start displaying a **Not critical** status by default 30 days before the expiry of the certificate.

The environment variable `FWADMIN_SNS_CERTS_PROBE_EXPIRATION_DELAY` allows this period to be configured. The lowest value allowed is one day.

To change the default 30-day period:

1. Log in to the SMC server via the console port or in SSH using the “root” account.
2. Change the value of the environment variable `FWADMIN_SNS_CERTS_PROBE_EXPIRATION_DELAY`. For example: `FWADMIN_SNS_CERTS_PROBE_EXPIRATION_DELAY = 20`
3. Restart the server with the command `nrestart fwadmin-server`
4. Deploy the configuration again on the firewalls.

The imminent expiry of certificates is also indicated in the **Configuration** > **Certificates** panel.

If you have changed the warning period, but have not yet redeployed the configuration on the firewalls, the status of certificates indicated in the **Certificates** panel (information provided by the SMC server) may not immediately match the firewall health status indicated in the monitoring panel (information provided by firewalls).

For further information regarding the **Certificates** panel, refer to the section Managing certificates and certification authorities.

5.14 Disabling TPM (Trusted Platform Module) certificate protection during installation on the firewall

More recent models of SN 3100 firewalls offer certificate protection with TPM chips from version 3.10 of SNS and upwards.

Whenever you install an identity (*.p12* format) on an SN firewall from the SMC server, certificate protection via TPM chip is enabled by default. The certificate is protected by a password stored on the TPM chip.

In SMC, TPM-protected certificates can only be used in IPSec VPN topologies with encryption profiles of the type IKEv2.

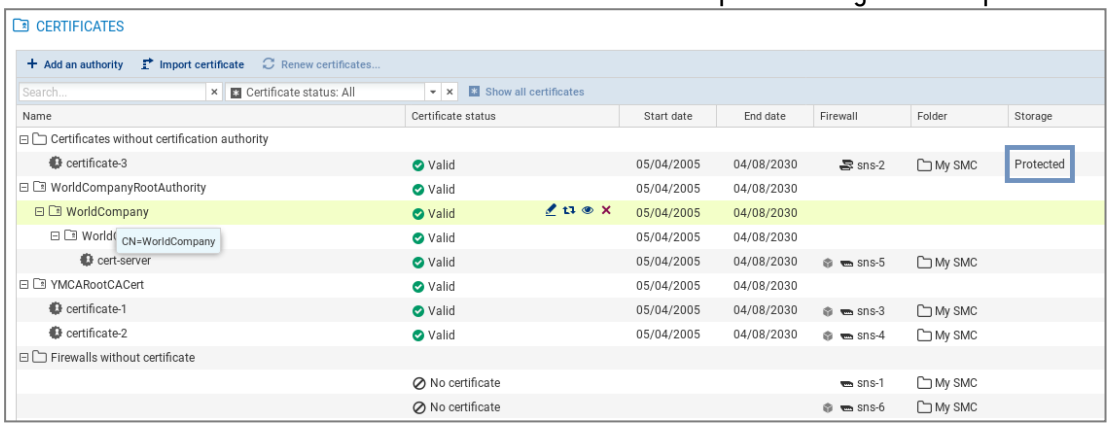
To create VPN topologies with IKEv1 encryption profiles, disable this protection using the environment variable `FWADMIN_FW_TPM_DISABLED`.

5.14.1 Finding out whether a certificate is TPM-protected

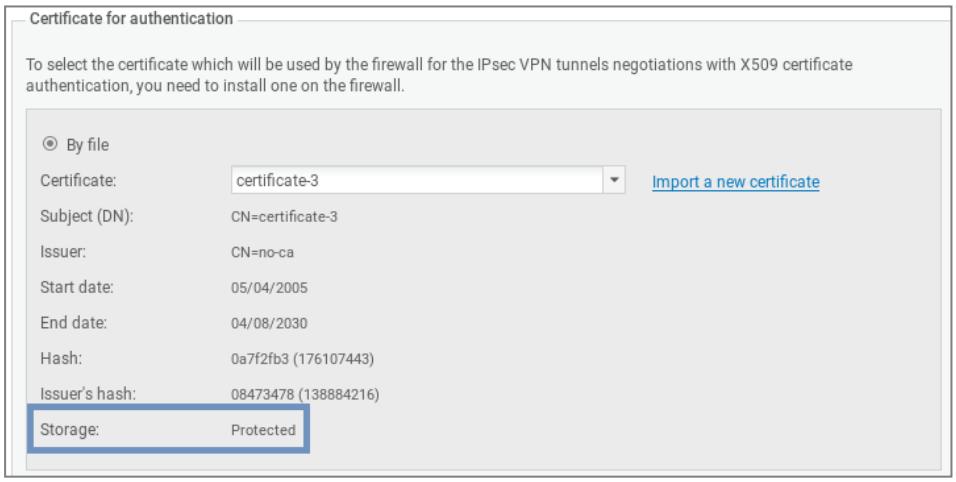
If a TPM chip has been installed and enabled on an SN model firewall, whenever you install a certificate on a firewall from the SMC server, the TPM chip will protect the certificate.

To find out whether a certificate is protected by a TPM chip, go to the following panels in the SMC server web administration interface:

- In the **Configuration** > **Certificats** menu, show the **Storage** column (hidden by default). The status **Protected** is indicated in the column if the certificate is protected by a TPM chip.



- In a firewall's **IPSEC VPN** properties, the status **Protected** is indicated in the X509 certificate's characteristics.



Whenever you install a new certificate on the firewall, the status will also be indicated in the window showing the results of the installation of a certificate.

5.14.2 Disabling TPM certificate protection

To disable TPM protection when you install a certificate on an SN firewall from the SMC server, the `FWADMIN_FW_TPM_DISABLED` environment variable needs to be modified:

1. Log in to the SMC server via the console port or in SSH using the “root” account.
2. In the file **/data/config/fwadmin-env.conf.local**, change the value of the environment variable:: `FWADMIN_FW_TPM_DISABLED=true`
3. Restart the server with the command `nrestart fwadmin-server`

5.14.3 Enabling TPM protection on existing certificates

- To enable TPM protection on a certificate that has already been installed on a firewall, run the following SNS CLI script from the **Scripts/SNS CLI scripts** menu:

```
PKI CERTIFICATE PROTECT caname=myca name=mycert tpm=ondisk
```

5.15 Choosing the separator character in CSV files

In SMC, *.csv* files can be used to import or export firewalls, filter rules or objects, for example.

The environment variable FWADMIN_CSV_DELIMITER makes it possible to set the separator character used to separate values in *.csv* files.

The default character is a comma.

To edit it:

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. In the file **/data/config/fwadmin-env.conf.local**, change the value of the environment variable:: `FWADMIN_CSV_DELIMITER=,`.
3. Restart the server with the command `nrestart fwadmin-server`.

6. Managing network objects

The menu **Network Objects** on the left of the web interface allows creating, editing or removing an object from the configuration deployed on firewalls.

All objects created from the SMC server belong to the firewall's global policy. They are available in the firewall web administration interface.

For more information about global objects, refer to the *Stormshield NetworkUser Configuration Manual*.

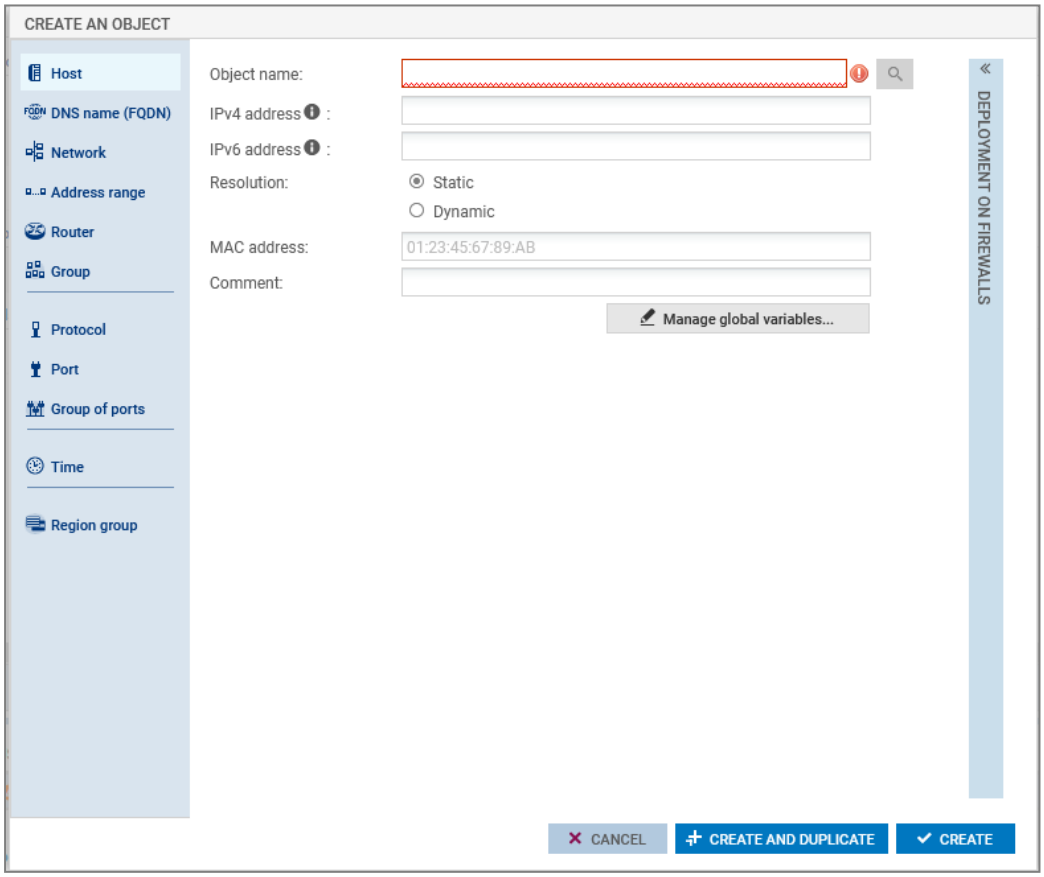
IMPORTANT
Before removing an object from the SMC server, ensure that doing so will not affect the operation of your firewalls.

6.1 Deploying objects on firewalls

After you have created or configured your network objects in the **Network objects** menu, you can choose how they will be deployed on firewalls.

By default, objects are deployed only on the firewalls that use them. However, you can force them to be deployed on certain firewalls or on all firewalls:

1. In the window for creating or editing objects, click on **Deployment on firewalls** to the right.



2. Force deployment on a selection of firewalls or on all firewalls.
3. Deploy the configuration.

In the list of objects in the **Network objects** menu, various icons allow identifying objects that have been forcibly deployed on a selection of firewalls ( ) or on all firewalls ( ).

6.2 Creating variable objects

Variable objects are Host, Network and IP address range objects whose IPv4 or IPv6 addresses vary according to the firewall on which they have been installed.

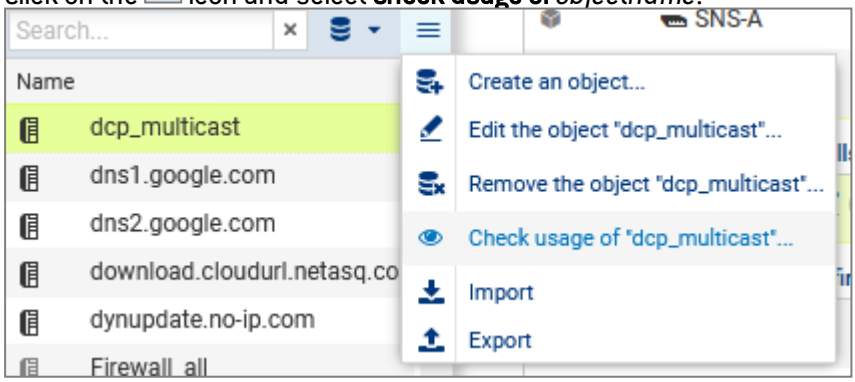
1. In the **Network objects** menu, create a Host, Network or IP address range object.
2. Fill in the **IPv4 address** or **IPv6 address** field with a %CUSTOM_X% variable. The value of this customized variable is defined in the **Customized variables** tab in the **Edit firewall** panel accessible by double clicking on the line of a firewall in monitoring view.
   - You can view the list of available variables by clicking on **Manage global variables**. Use the **Copy to clipboard** button to copy them to the desired field.

   > **EXAMPLE**
   > Enter the address 10.1.%CUSTOM_IP%.0/24. If for a given firewall, the customized variable equals "1" in its parameters, the address will be 10.1.1.0/24 for this firewall in the filter rule or in the VPN topology.
3. Complete the creation of the object.

For more information on the customized variables, refer to the section Creating customized variables.

6.3 Checking usage of an object in the configuration

1. In the **Network objects** menu, select an object.
2. Click on the icon and select **Check usage of** *objectname*.



3. In the results panel that opens in the lower part of the window, you can click on items to display and modify them.

6.4 Importing objects

To quickly import a large number of existing objects on SN firewalls or to easily create objects, you can use a CSV file and import it on the SMC server from the web interface or command line interface.

With the help of such files, you can specify the firewalls on which each object is to be deployed, among other functions.

An example of a CSV file "example-import-objects.csv" is available on the server, in the folder */opt/stormshield/examples/csv/*.

6.4.1 Creating the CSV file

You can either export existing objects from a firewall or create a new CSV file.

To export the CSV file from a firewall:

1. Connect to the firewall,
2. Go to **Objects** > **Network objects**.
3. Click on **Export**.

This file contains all the network objects and groups on your firewall, except router and time objects, which the firewall cannot export.

IMPORTANT
If you are modifying a CSV file that was exported from a firewall, check that the editing software has not modified the contents of the file, in which case the file may not be imported on the SMC server.

To create a new CSV file, and to find out details about header lines and the parameters to specify according to the object's category, you may:

- Choose to export objects from a firewall,
- Look up the example given on the SMC server as indicated above.

Specifying firewalls on which objects are to be deployed

By default, objects are deployed only on the firewalls that use them. However, in the CSV file, you may indicate the firewalls on which deployment will be forced using the *#deployment* column.

Example of a Host object being created:

1. Enter the following parameters in the columns of the file header:
```
#type,#name,#ip,#ipv6,#resolve,#mac,#deployment,#comment
```
2. Enter the values corresponding to the parameters in the lines after the header for each Host object to be imported (example):
```
host,dns1.google.com,8.8.8.8,2001:4860:4860::8888,,,ALL,"Google Public DNS Server"
```

The *#deployment* parameter may take on any of the following values:

- Empty or DEFAULT: this is its default behavior - the object is deployed only on the firewalls that use it.
- ALL: the object is deployed on all firewalls.
- "Firewall 1,Firewall 2": list of firewall names between quotation marks and separated by commas. The object is deployed on these firewalls as well as the firewalls that use it.

6.4.2 Importing objects from the web interface

You need read/write privileges to import objects.

1. In the **Network objects** menu, click on .
2. Select **Import**.

3. Select the CSV file to import.
4. If necessary, select the option that allows you to update existing objects by replacing them with objects found in the file.

In case of error, refer to the import summary.

No other actions can be performed on the server while objects are being imported.

6.4.3 Importing objects in command line

1. Start by copying the CSV file on the SMC server using the SSH protocol in the */tmp* folder for example.
2. Connect to the SMC server via the console port or SSH connection with the "root" user.
3. To import all object types, enter the command:
   `smc-import-objects --csv-file /tmp/file.csv`.
4. To view imported objects in the SMC web interface, refresh the page or log off and log on again.

Whether each object or group has been imported will be indicated, as well as a summary when the import is complete.

You can also choose the types of objects to import.

EXAMPLE
To import only Host and IP address range objects from a CSV file, enter the command:
`smc-import-objects --csv-file /tmp/file.csv --host --range`

The commands to be entered according to the type of object are:

Object type	Command
Host	--host
DNS name (FQDN)	--fqdn
Network	--network
IP address range	--range
Router	--router
Group [1]	--group
IP protocol	--protocol
Service (port)	--service
Port group	--servicegroup
Time	--time

Customized variables such as %CUSTOM_X% can be used instead of IPv4 or IPv6 address values in Host, Network and IP address range objects. These customized variables are defined in the **Customized variables** tab in the **Edit firewall** panel accessible by double clicking on the line of a firewall in monitoring view.

If an imported object already existed in SMC, an error will appear. You may use the `--update` option to overwrite the existing object with the one indicated in the CSV file.

[1] When importing a group, objects included in the group must already exist on the SMC server, otherwise the group will not be created. Import them beforehand through another CSV file or create them manually in the web interface.

6.5 Exporting objects

The SMC server makes it possible to export the entire contents of your object database in CSV format.

You only need read privileges to export objects.

1. In the **Network objects** menu, click on ☰.
2. Select **Export**.
3. Save the CSV file.

7. Creating and monitoring VPN tunnels

In SMC, you can create and manage site-to-site IPSec VPN topologies that connect private networks securely through a public network. VPN topologies can be configured based on policies or routes:

- A policy-based VPN tunnel links firewall-protected networks or sub-networks to one another, and encrypts and encapsulates traffic between these networks, which are described in a policy. Such topologies are used in the standard operating mode. This feature is available on SN firewalls in version 3.0 or later.
- A route-based VPN tunnel uses IPsec virtual tunnel interfaces (VTI) to link firewalls. These interfaces are considered as input and output points for the traffic passing through the tunnel. This traffic is described by routes. This feature is available on SN firewalls in version 3.3 or later.

In both cases, either star or mesh topologies can be used.

SMC 3.0 Version does not support VPN topologies in IPv6. If a topology includes network objects in IPv6, they will be ignored during deployment. If a topology relies on network objects with a dual IPv4/IPv6 configuration, only the configuration in IPv4 will be applied and the IPv6 configuration ignored.

Refer to the following sections to create policy-based or route-based VPN topologies.

7.1 Creating policy-based VPN topologies

In SMC, you can create and manage VPN tunnels that link firewall-protected networks or sub-networks, which are described in a policy.

Such topologies are used in the standard operating mode.

Firewalls or gateways act as entry and exit points for tunnels and may be:

- SN firewalls in at least version 3.0, managed by the SMC server,
- External peers, meaning SN firewalls or any other type of VPN gateway not managed by the SMC server.

SMC offers two VPN topologies: mesh or star.

- Mesh: all remote sites are interconnected,
- Star: a central site is connected to several satellite sites. Satellite sites do not communicate with one another. The central site must be an SN firewall managed by the SMC server.

Before configuring your topologies, you must:

- Create your traffic endpoints beforehand (Network, Host or Group) in the **Network objects** menu. For more information, please refer to the section Managing network objects.
- Create Host objects beforehand for your external peers if your topologies include them.
- if X509 certificate authentication has been selected, import a certificate beforehand for your firewalls managed by SMC included in your topologies and declare certification authorities beforehand as well. The corresponding procedures are described in the section Configuring a policy-based mesh topology.

In this section, we describe two use case scenarios, a policy-based mesh topology and a policy-based star topology. For further detail on each menu and option for configuring VPN tunnels, refer to the *Stormshield Network User Configuration Manual*.

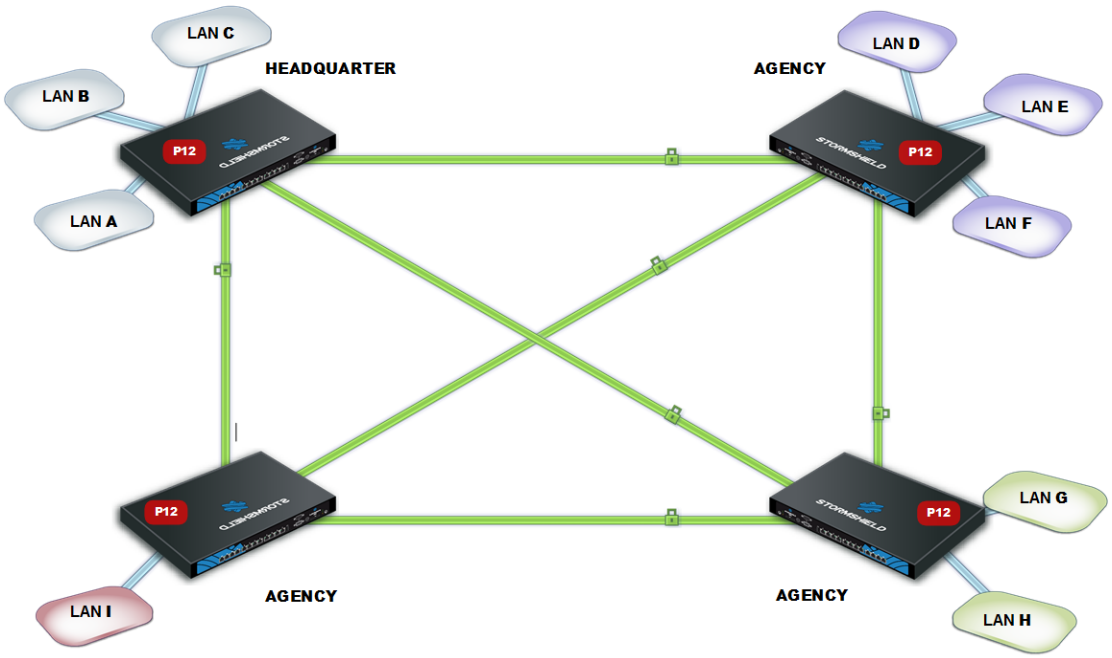
7.1.1 Configuring a policy-based mesh topology

Example of a scenario:

A company has its headquarters and two other sites in England and one site abroad. Every site has its own Research and Development department and the four R&D sub-networks need to share information. Every site is protected by a firewall managed by the SMC server.

The authentication method selected is X509 certificate authentication.

The certification authority that issues certificates can be found on one of the SN firewalls, such as the headquarters, for example, or may be an external authority.



To configure VPN tunnels between the four sites, follow the steps below.

Importing or declaring certificates for SN firewalls

To import or declare a certificate in PKCS#12 or PEM format from the SMC server web interface, refer to the section Importing a certificate from the server's web interface.

Certificates can also be imported from the command line interface. Refer to the section Importing a certificate from the command line interface

Declaring certificate authorities

On the SMC server, you need to declare the certification authorities to be trusted by the firewalls that SMC manages.

In order for the topology to be deployed, the SMC server must know the certification authorities' entire chain of trust. For further information and to find out how to add certification authorities, refer to the section Managing certificates and certification authorities.

Setting the CRL distribution points

You must give the SMC server the addresses of the distribution point(s) of the Certificate Revocation List (CRL) that firewalls would use for each declared authority. They can be external or you can also set SMC as a distribution point.

Setting external distribution points

1. In the properties of a certification authority, click on the **List of CRL distribution points** tab.
2. Add the addresses of the external distribution point(s) for the certificate revocation list.

Setting SMC as a distribution point

The SMC server can act as a CRL distribution point for SN firewalls from version 3.3.0 upwards:

1. In the properties of a certification authority, click on the **SMC as CRL distribution point** tab.
2. Select the CRL file (*.pem* or *.der* format) to import onto the server.
   The SMC server then makes the file available for the SN firewalls on the URI smc://[SMC address]:[SMC port]/api/certificates/authorities/[uuid CA].crl.
   As the CRL has an expiry date, it must be regularly imported onto the SMC server.
   As firewalls can contact the SMC server through several addresses (they are specified in the connecting package), you need to enter one URI for each address.
   You can also import a CRL on the SMC server in command line, with the command `smc-import-crl`.
3. In the **List of CRL distribution points** tab, add the URI address to the list. The CA UUID is shown in the SMC URL address as well as in the example provided in the tab.

Creating objects included in the topology

1. Go to the **Network objects** menu on the left.
2. Create as many objects as the number of traffic endpoints or hosts that will be included in your VPN topology, i.e., four objects in our example.

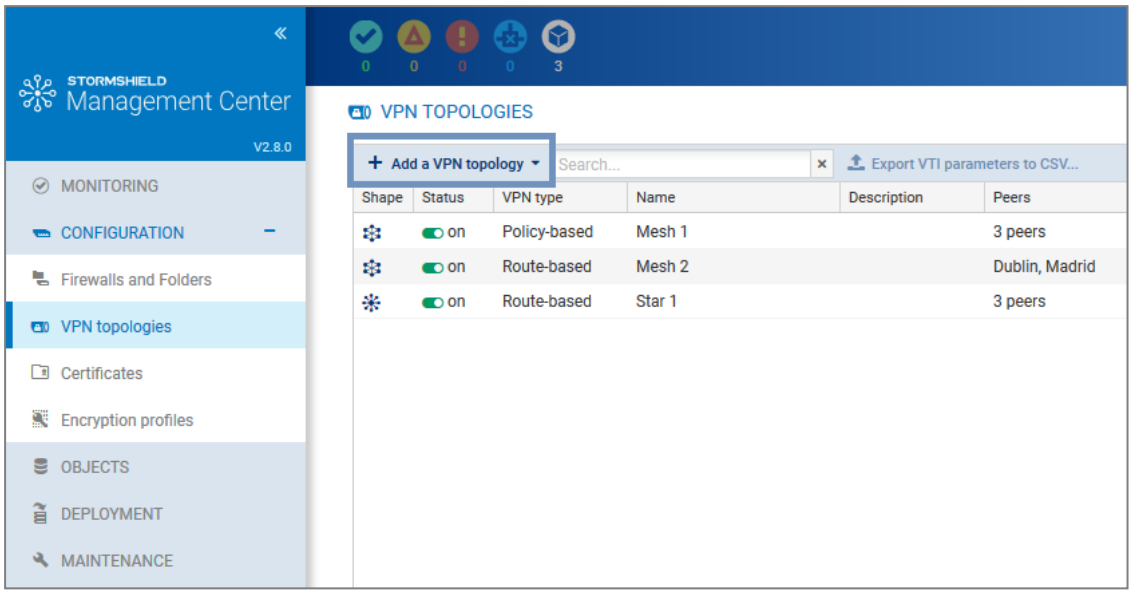
These may be Network, Host or Group objects.

IMPORTANT
It is not possible to use groups containing variable objects in VPN topologies. VPN tunnels configuration would be invalid.

Creating the VPN topology

You now have all the necessary elements for configuring your VPN topology.

1. In **Configuration > Topologies**, click on **Add a VPN topology** at the top of the screen and select **Mesh**.



2. In the window that opens, select **Policy-based VPN** and click on **Create the topology.**
3. Enter a name. A description is optional.
4. Select X.509 certificate authentication and select the certification authorities that issued the certificates for the firewalls involved in the VPN topology. If an authority's CRL has expired, a warning appears in the list of the **VPN topologies** menu.
5. Select the encryption profile. The SMC server offers three pre-configured profiles. Create your customized profiles in **Configuration > Encryption profiles**. Refer to the *Stormshield Network User Configuration Manual* for more information on encryption profile options.
6. Select your topology peers. You can only select connected or offline firewalls, and in at least version 3.
7. Select the traffic endpoints associated with each of your peers. For further information on the **Contact address** and **Output interface** parameters, refer to the sections Defining the contact IP address of firewalls for VPN topologies and Selecting the output interface of firewalls for VPN topologies.
8. Click on **Apply**.
9. Deploy the configuration on the firewalls involved in the topology. The VPN configuration belongs to the firewall's global policy.

7.1.2 Configuring a policy-based star topology

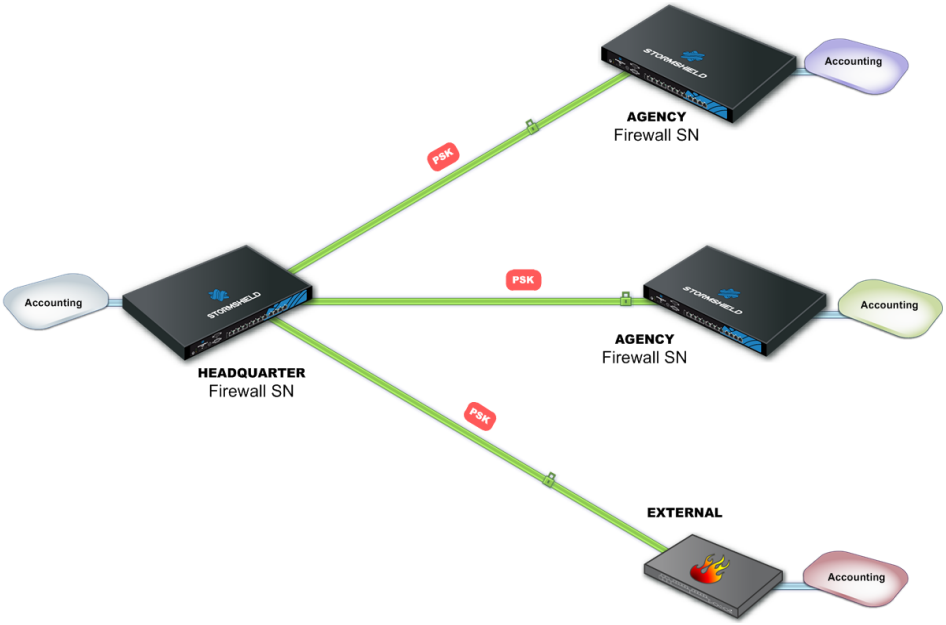
Example of a scenario:

A company with its head office in Paris has two branches in Bordeaux and Madrid. The Accounting sub-network at the head office needs to exchange information with the Accounting sub-networks in the branches. The company's three sites are protected by SN firewalls managed by the SMC server.

The company has just acquired a new organization that also has an Accounting department and whose network is protected by a firewall from another vendor.

The administrator needs to know the address range of this firewall, which will be declared as an external peer, and the address range of the sub-network.

The chosen authentication method is by pre-shared key (PSK).



To configure VPN tunnels between the four sites, follow the steps below.

Creating objects included in the topology

1. Go to the **Network objects** menu on the left.
2. Create as many objects as the number of traffic endpoints or hosts that will be included in your VPN topology, i.e., four Network objects in our example.
3. Your topology includes an external peer. Create a Host object for this firewall.

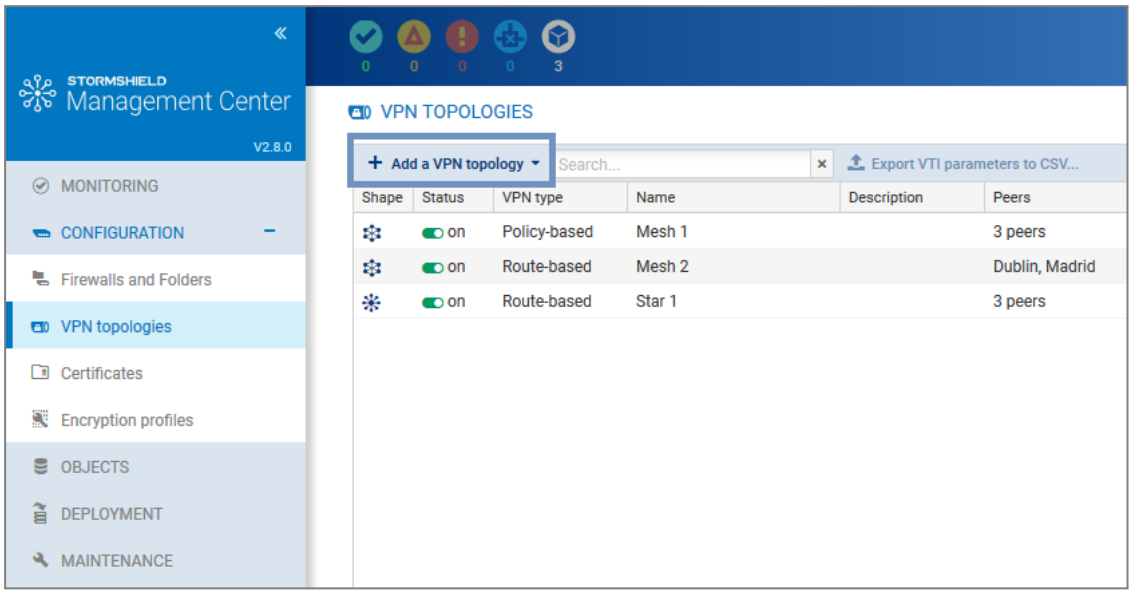
These may be Network, Host or Group objects.

IMPORTANT
It is not possible to use groups containing variable objects in VPN topologies. VPN tunnels configuration would be invalid.

Creating the VPN topology

You now have all the necessary elements for configuring your VPN topology.

1. In **Configuration > VPN Topologies**, click on **Add a VPN topology** at the top of the screen and select **Star**.



2. In the window that opens, select **Policy-based VPN** and click on **Create the topology.**
3. Enter a name. A description is optional.
4. Select pre-shared key authentication.
5. Generate a random key.
6. The strongest encryption profile is selected by default. The SMC server offers three pre-configured profiles. Create customized profiles in **Configuration > Encryption profiles**. Refer to the *Stormshield Network User Configuration Manual* for more information on encryption profile options.
7. Choose the center of your topology. It will then show a star icon in the list of firewalls below, and the firewall will appear in bold.
8. If needed, check the option **Do not initiate the tunnels (Responder-only)** if the IP address of the center of the topology is dynamic. Only the peers will then be able to mount the VPN tunnel. This option is available from the version 3.6.0 of the SN firewalls.
9. Select your topology peers. You can only select connected or offline firewalls, and in at least version 3.
10. Select the traffic endpoints associated with each of your peers. For further information on the **Contact address** and **Output interface** parameters, refer to the sections Defining the contact IP address of firewalls for VPN topologies and Selecting the output interface of firewalls for VPN topologies.
11. Click on **Apply**.
12. Deploy the configuration on the firewalls involved in the topology. The VPN configuration belongs to the firewall's global policy.

7.2 Creating route-based VPN topologies

In route-based VPN tunnels, traffic is routed via IPSec VTIs to link SN firewalls that the SMC server manages, as well as networks and hosts protected by these firewalls.

Firewalls must be in at least version 3.3.

These IPSec VTIs act as the traffic endpoints of tunnels, and all packets routed to these interfaces are then encrypted. This traffic is described by routes in a routing table or by policy-based routing (PBR) filter rules.

The following are some of the advantages of route-based VPN topologies:

- Routing by IPSec VTIs takes priority over a policy match in standard IPSec tunnels.
- They require fewer tunnels than in a standard Ipsec topology. Only one tunnel is needed between two firewalls, regardless of the number of networks that the firewall protects.

NOTE
Route-based topologies cannot include external peers, i.e., SN firewalls or any other type of VPN gateway not managed by the SMC server.

From the SMC server you can	On every firewall in the topology, you must then
Create route-based VPN topologies	Create IPSec virtual tunnel interfaces (VTI)
Monitor these topologies	Configure static routes if necessary
Define filter rules. SMC automatically generates VTI objects that represent peers in the topology, which can be used in these rules.	Configure return routes if necessary
For more information, see the next sections.	

SMC offers two VPN topologies: mesh or star.

- Mesh: all remote sites are interconnected,
- Star: a central site is connected to several satellite sites. Satellite sites do not communicate with one another.

If X509 certificate authentication is selected, prior to configuring your topologies, you must import a certificate for all the firewalls in your topologies that SMC manages, and also declare certification authorities. The corresponding procedures are described in the section Configuring a policy-based mesh topology.

In this section, we describe the configuration of a route-based mesh topology and the configuration of a route-based star topology. For further detail on each menu and option for configuring VPN tunnels, refer to the *Stormshield Network User Configuration Manual*.

For further information on setting up IPSec VTIs on firewalls, refer to the relevant Technical note.

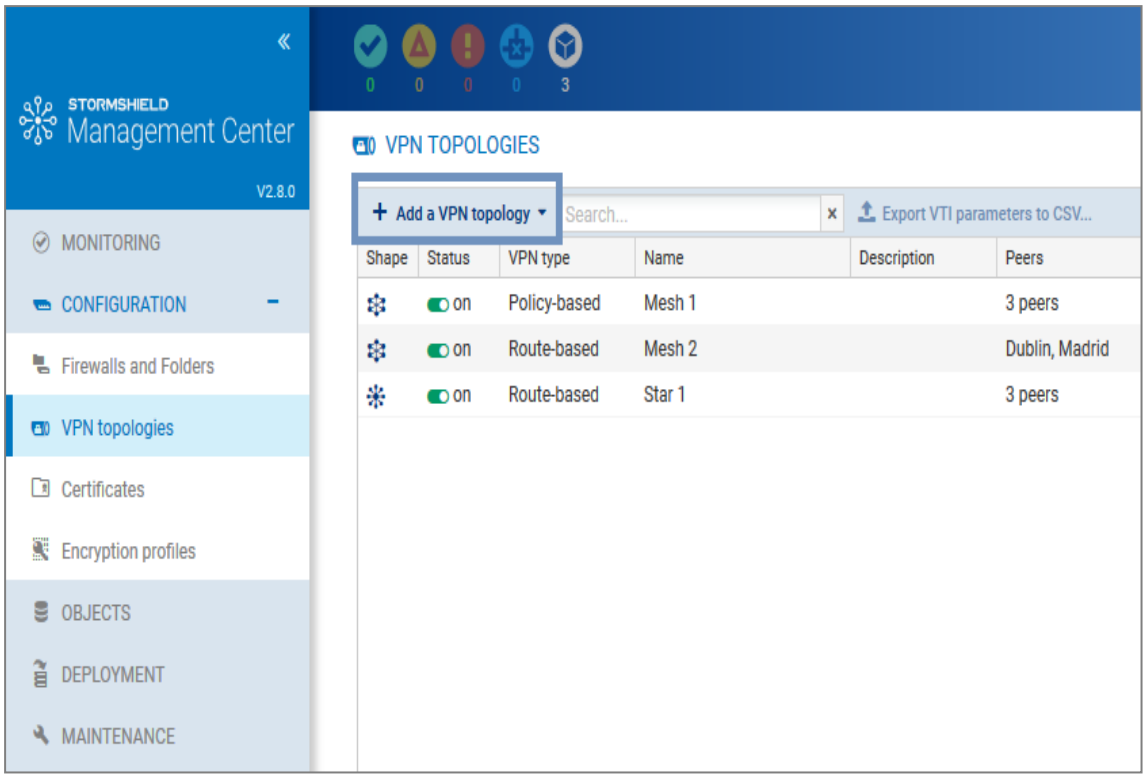
7.2.1 Configuring a route-based mesh topology

Depending on which authentication type you choose to secure your topology, there may be operations you must perform before creating the topology.

- For further information on X509 certificate authentication, refer to the section Configuring a policy-based mesh topology.
- For further information on pre-shared key authentication, refer to the section Configuring a policy-based star topology.

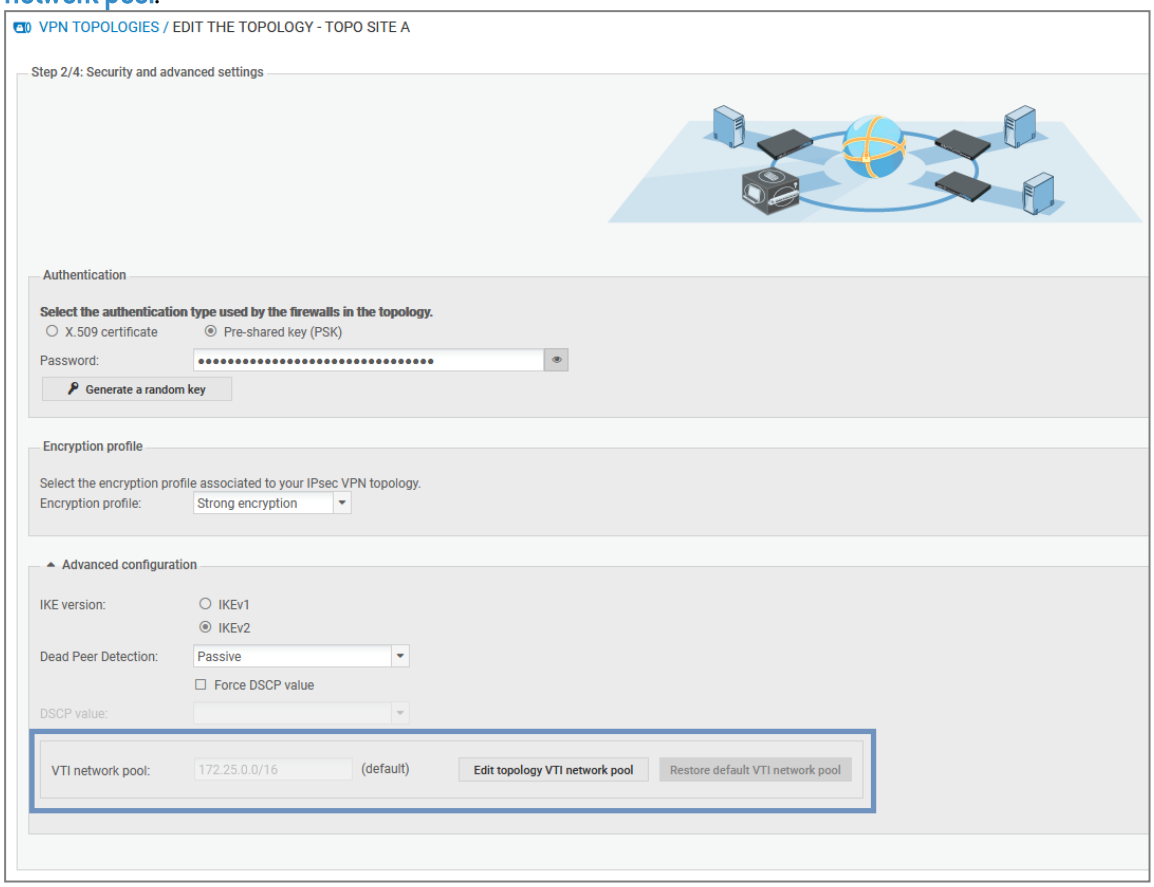
Follow the steps below to create a route-based VPN topology:

1. In **Configuration > Topologies**, click on **Add a VPN topology** at the top of the screen and select **Mesh**.



2. In the window that opens, select **Route-based VPN** and click on **Create the topology.**
3. Enter a name. A description is optional.
4. Choose the authentication type in the next step.
5. Select the encryption profile. The SMC server offers three pre-configured profiles. Create your customized profiles in **Configuration > Encryption profiles**. Refer to the *Stormshield Network User Configuration Manual* for more information on encryption profile options.

6. If you need to edit the default network pool for IPSec VTIs, expand the **Advanced properties** section. For more information on the **VTI network pool** field, refer to the section Editing the VTI network pool.



7. Select your topology peers in the next step. You can only select connected or offline firewalls, and in at least version 3.3. To ensure optimal performance, you can select up to 50 peers by default. The environment variable `FWADMIN_VPN_MESH_ROUTE_BASED_MAX_PEERS` makes it possible to configure this limit, which applies only to route-based mesh VPN topologies.
8. In the next step, double-click on the line of a firewall to open the **Peers and VTI** window:
   - For further information on the **Contact address** and **Output interface** parameters, refer to the sections Defining the contact IP address of firewalls for VPN topologies and Selecting the output interface of firewalls for VPN topologies.
   - IPSec VTIs will automatically be generated after the topology is created. Host VTI objects that represent remote peers will also be automatically generated, and can be used in filter rules to set up routing. You will see them in your object database as "VTI_on_FW1_with_FW2_in_topologyname". These objects are automatically deployed on firewalls. For further information, refer to the section Defining the traffic routing policy.
9. Click on **Apply** to close the window.
10. Click on **Apply** again at the end of step 4/4 to generate the topology.
11. SMC then suggests that you download the *.csv* file to configure IPSec interfaces. This file contains the information you need to create interfaces on every firewall in the topology. Refer to the section Defining IPSec VTIs on SN firewalls for further information.
12. Deploy the configuration on the firewalls in the topology. The VPN configuration belongs to the firewall's global policy.

Your topology is still not operational at this stage. Follow the instructions in Defining IPSec VTIs on SN firewalls and Defining the traffic routing policy to complete the process of setting up a route-based VPN topology.

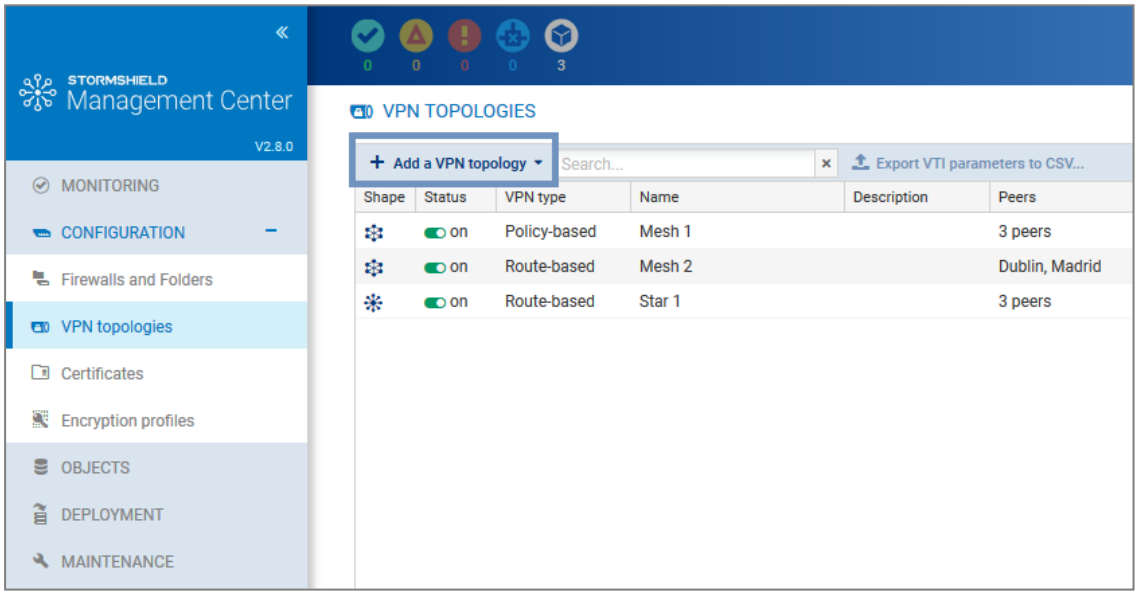
7.2.2 Configuring a route-based star topology

Depending on which authentication type you choose to secure your topology, there may be operations you must perform before creating the topology.

- For further information on X509 certificate authentication, refer to the section Configuring a policy-based mesh topology.
- For further information on pre-shared key authentication, refer to the section Configuring a policy-based star topology.

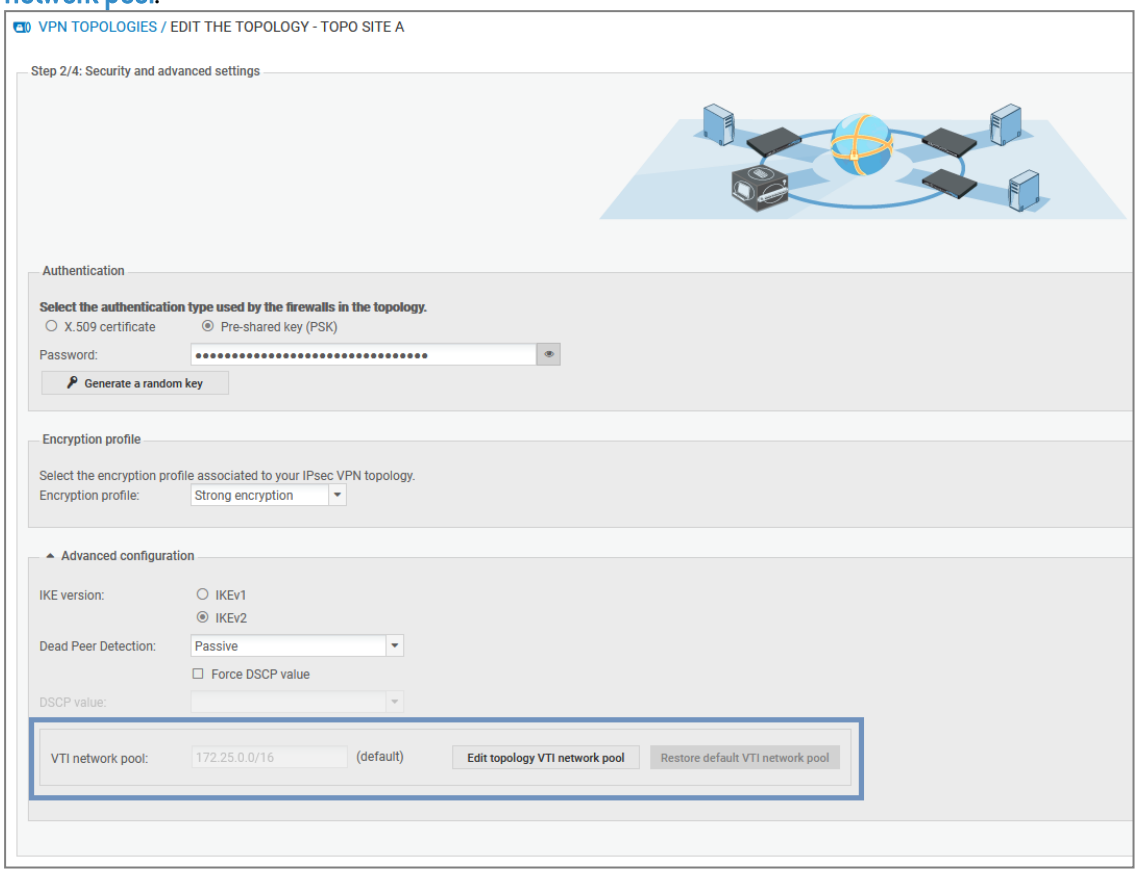
Follow the steps below to create a route-based VPN topology:

1. In **Configuration > VPN Topologies**, click on **Add a VPN topology** at the top of the screen and select **Star**.



2. In the window that opens, select **Route-based VPN** and click on **Create the topology.**
3. Enter a name. A description is optional.
4. Choose the authentication type in the next step.
5. Select the encryption profile. The SMC server offers three pre-configured profiles. Create customized profiles in **Configuration > Encryption profiles**. Refer to the *Stormshield Network User Configuration Manual* for more information on encryption profile options.

6. If you need to edit the default network pool for IPSec VTIs, expand the **Advanced properties** section. For more information on the **VTI network pool** field, refer to the section Editing the VTI network pool.



7. Choose the center of your topology. It will then show a star icon in the list of firewalls below, and the firewall will appear in bold.
8. If needed, check the option **Do not initiate the tunnels (Responder-only)** if the IP address of the center of the topology is dynamic. Only the peers will then be able to mount the VPN tunnel. This option is available from the version 3.6.0 of the SN firewalls.
9. Select your topology peers. You can only select connected or offline firewalls, and in at least version 3.3.
10. In the next step, double-click on the line of a firewall to open the **Peers and VTI** window:
    - For further information on the **Contact address** and **Output interface** parameters, refer to the sections Defining the contact IP address of firewalls for VPN topologies and Selecting the output interface of firewalls for VPN topologies.
    - IPSec VTIs will automatically be generated after the topology is created. Host VTI objects that represent remote peers will also be automatically generated. They can be used in filter rules to set up routing. You will see them in your object database as "VTI_on_FW1_with_FW2_in_topologyname". These objects are automatically deployed on firewalls. For further information, refer to the section Defining the traffic routing policy.
11. Click on **Apply** to close the window.
12. Click on **Apply** again at the end of step 4/4 to generate the topology.
13. SMC then suggests that you download the *.csv* file to configure IPSec interfaces. This file contains the information you need to create interfaces on every firewall in the topology. Refer to the section Defining IPSec VTIs on SN firewalls for further information.

14. Deploy the configuration on the firewalls in the topology. The VPN configuration belongs to the firewall's global policy.

Your topology is still not operational at this stage. Follow the instructions in Defining IPSec VTIs on SN firewalls and Defining the traffic routing policy to complete the process of setting up a route-based VPN topology.

7.2.3 Defining IPSec VTIs on SN firewalls

Connect to every firewall in your topology and manually create IPSec VTIs in **Network** > **Virtual interfaces** using the *.csv* configuration file downloaded from SMC.

Refer to the *Stormshield Network User Configuration Manual* as well for more information on how to create IPSec VTIs.

If you want IPSec interfaces to be automatically created, the *.csv* file contains all the information required to write serverd commands.

In this case, the column *#vti interface name* must be entered manually. The value of the interface name is in the format ipsecXX, where XX is an increment that depends on the number of interfaces already on the firewall.

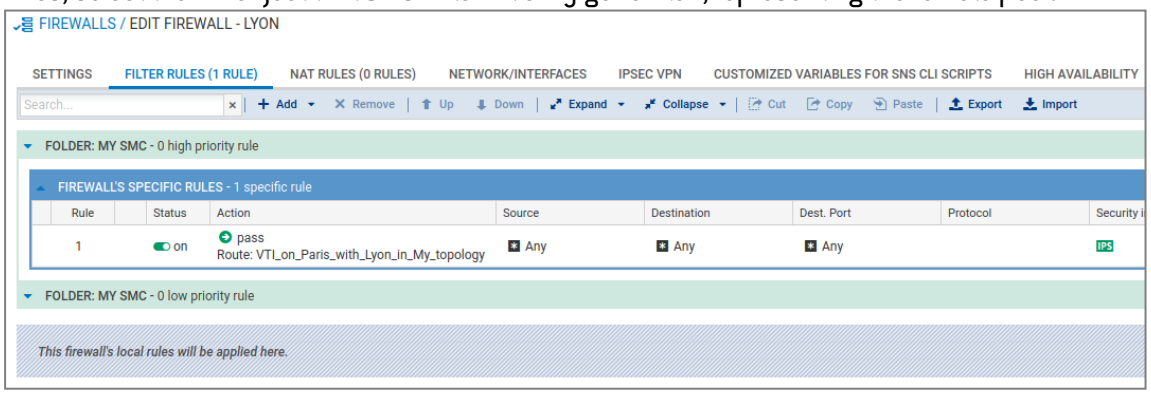
Now follow the last step.

7.2.4 Defining the traffic routing policy

You can configure static, dynamic or return routes on your firewalls to direct traffic to IPSec VTIs. You can also define filter rules directly from SMC to set up routing.

If you are setting up policy-based routing:

1. In SMC, create filter rules for each firewall to allow traffic to go through the tunnel. The remote peer must be defined as the **Gateway – router**. To do so, in the **Action** menu, **General** tab in rules, select the VTI object that SMC automatically generated, representing the remote peer.



2. Create return routes directly on each firewall.

If you are not using policy-based routing:

1. In SMC, create filter rules for each firewall to allow traffic to go through the tunnel.
2. On each firewall, create static routes dedicated to the remote peer's IPSec VTIs.

For help on how to configure routes on your firewalls, refer to the *Stormshield Network user configuration manual* and the Technical note dedicated to IPSec VTIs.

7.2.5 Editing the VTI network pool

When a route-based VPN topology is being created, the SMC server selects the IP addresses of IPSec VTIs from a private sub-network defined by default.

This sub-network is a reserve of available addresses and must be included in (or equal to) one of these three sub-networks:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

The sub-network suggested by default is 172.25.0.0/16.

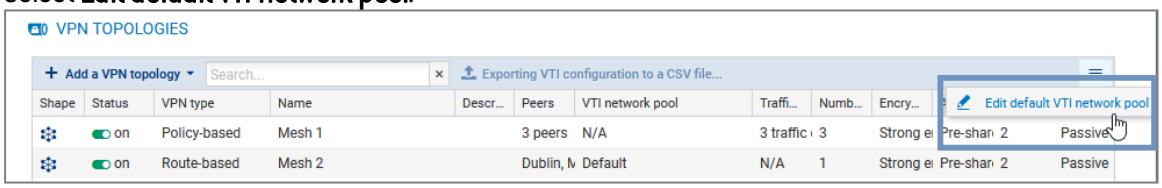
This default network pool is the same across all topologies. If necessary, you can edit the global pool, or a pool specific to a topology.

IMPORTANT
If you edit a topology's network pool of IPSec interfaces after the topology is created and deployed, you should verify the configuration of the interfaces already created on your firewalls.

Editing the default global network pool

The default network pool is the pool that is used when a new topology is created. To edit it:

1. In **Configuration** > **VPN topologies**, click on the ☰ icon on the top right side of the screen and select **Edit default VTI network pool**.



2. Indicate the new default network pool.

This change does not affect existing topologies, which will keep the final pool when they are created.

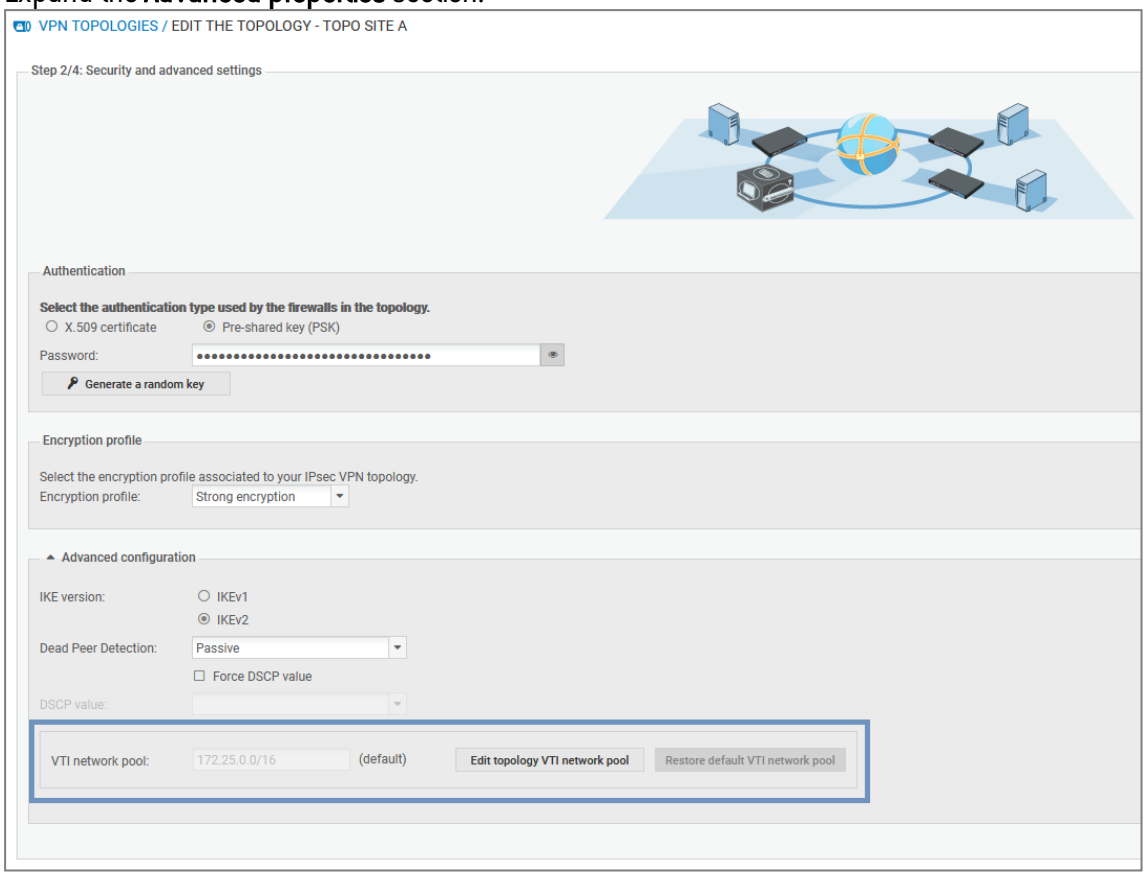
Editing a topology's specific network pool

The network pool can be edited during or after the creation of a new topology.

To edit it for an existing topology:

1. In Configuration > **VPN topologies**, click on the pencil icon that appears when you scroll over the **VTI network pool** column in the grid.

2. Expand the **Advanced properties** section.



3. Click on **Edit topology VTI network pool.**
4. Click on **Confirm changes** in the warning window. Verify the configuration of interfaces already created on your firewalls.
5. Indicate a new private sub-network from the three listed at the beginning of the section.
6. Deploy the configuration.

7.3 Managing certificates and certification authorities

The **Configuration** > **Certificates** menu makes it possible to view and manage certification authorities (CAs) and firewall certificates at the same time. From the same panel, you can add, update or delete certificates and certification authorities.

In the table, authorities, sub-authorities and certificates are presented in a tree structure displaying information on certificates, firewalls and topologies concerned.

- To select the columns to be displayed, scroll over the name of a column and click on the arrow that appears.
- To display the actions that can be performed on authorities and certificates, scroll over the **Certificate status** column. Action icons will appear.

Firewall certificates can be in X509 or issued via SCEP or EST, and allow different actions to be performed:

	Certification authorities	X509 certificates	SCEP/EST certificates

Icons when scrolling over the line			
Possible actions	• Changing the certification authority • Updating the certification authority • Seeing references • Removing from the SMC server	• Updating the certificate • Seeing references • Removing from the SMC server	• Renewing the certificate • Seeing references • Removing from the SMC server

Refer to the procedures below for more information on each of these actions.

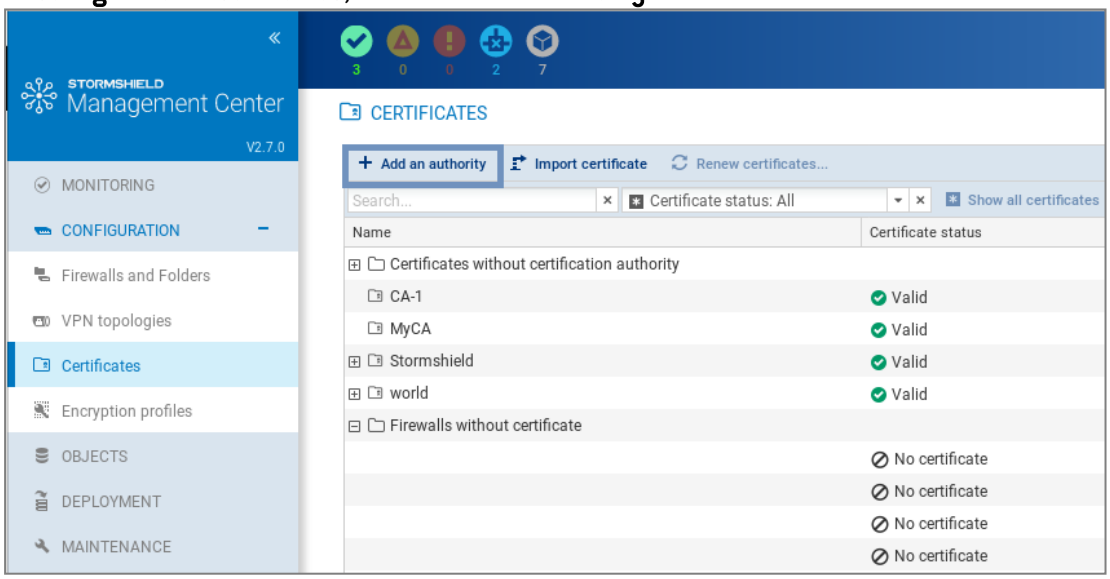
7.3.1 Adding a certification authority or chain of trust

The SMC server does not allow the use of certification authorities with unknown issuers. Therefore, when importing a certification authority, its entire chain of trust must be imported.

To import a chain of trust, import the certificates of the root certification authority and the various sub-authorities individually, starting with the certification authority of the highest level. You can also import all of them at one go by providing a "bundle" file.

Whenever you add a certification authority, the SMC server will verify its chain of trust.

1. In **Configuration** > **Certificates**, click on **Add an authority**.



2. Select a file in *.pem*, *.cer*, *.crt* or *.der* format and click on **Add**.
3. Add the addresses of the distribution point(s) for the certificate revocation list (CRL). For more information, refer to the section Setting the CRL distribution points.
4. If you renew firewall certificates via SCEP or EST, associate an SCEP or EST server with the certification authority in the **Certificate renewal** tab.
5. After the authority has been declared, you can change it or check its usage by scrolling over the name of the authority in the table to display the action icons in the **Certificate status** column.

You can also add a new authority during the configuration of a VPN topology, during the selection of the authentication method, by clicking on **Add an authority**.

7.3.2 Updating a certificate authority or chain of trust

Whenever you update a certification authority, the name, comments and list of certificate revocation list distribution points, if there is one, will be kept.

The public key must be the same as the one for the previous authority.

- To update a certification authority, scroll over the name of the certification authority and click on the icon in the **Certificate status** column.

7.3.3 Deleting a certification authority or chain of trust

Whenever you delete a certification authority, all authorities depending on it will also be deleted. If any of the intermediate authorities are used in a VPN topology, you will not be able to delete them.

- To delete a certification authority, scroll over the name of the certification authority and click on the icon in the **Certificate status** column.

7.3.4 Importing or declaring a certificate for a firewall

X509 certificates can be imported via the **Firewall** column in the table, as well as from other panels in the administration interface.

To import or declare a certificate, refer to the section Importing or declaring a certificate for a firewall.

After the certificate has been imported or declared, you can check its usage or delete it by scrolling over its line in the table to display the action icons in the **Certificate status** column.

You cannot delete it if it is in use in a VPN topology.

If you have imported several X509 certificates for a firewall, to find out which certificate is used by default in VPN topologies, refer to the section Changing the certificate used by default in VPN topologies.

7.3.5 Updating a firewall's X509 certificate

- To update an X509 certificate that has expired or is about to expire, scroll over the line of the certificate in the table and click on the icon in the **Certificate status** column.

The new certificate must have the same subject field as the previous certificate.

7.3.6 Renewing firewall certificates obtained via SCEP or EST

There are two ways to renew certificates obtained via SCEP or EST: individual renewal or the renewal of several certificates at the same time.

To ensure the successful renewal of SCEP or EST certificates, the address of the SCEP or EST server must be entered in the **Certificate renewal** tab of the certification authority that issued the certificates, as shown in the section Adding a certification authority or chain of trust.

The following conditions must be met in order to renew certificates:

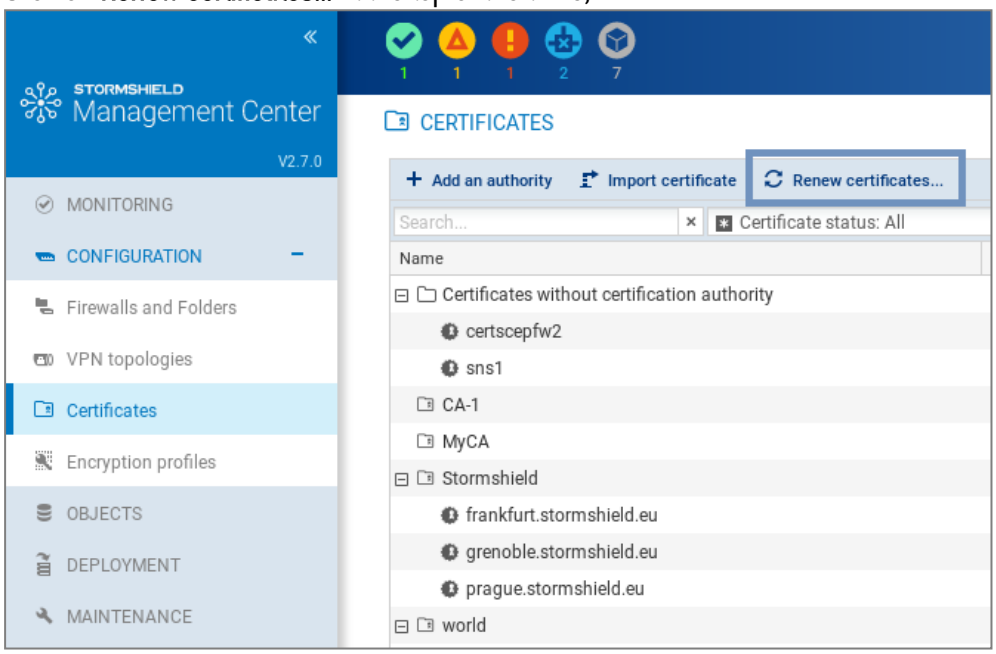
- SN firewalls must be at least in version 3.9.0 for SCEP and at least 3.10 or 4.1 for EST,
- the SN firewalls must be connected.

To renew a single certificate:

1. Scroll over the line of the certificate in the table and click on in the **Certificate status** column,
2. Confirm the renewal of the certificate.

To renew several certificates at the same time:

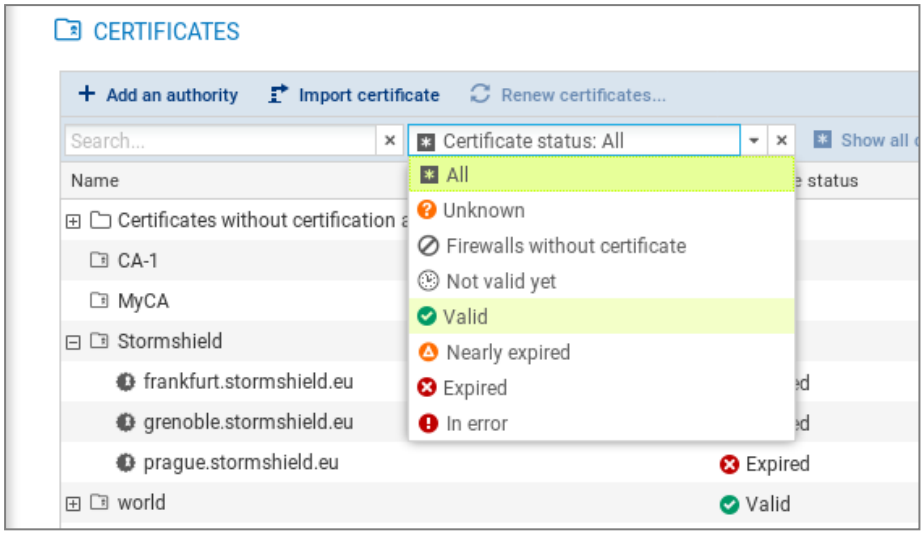
1. Click on **Renew certificates...** at the top of the table,



2. Select the certificates to be renewed,
3. Confirm the renewal of the certificates at the bottom of the table. If an error occurs, refer to the server logs for more information.

7.3.7 Explanations regarding certificate statuses

The filter above the table allows you to display certification authorities and certificates according to their status.



To view the entire certificate tree, click on **Show all certificates**.

The **Unknown** status applies only to certificates obtained via SCEP or EST. SCEP or EST certificates may be **Unknown** if the SMC server does not yet know the certificate. This happens when the SCEP or EST server cannot be reached or the firewall has not connected since the certificate was created.

The **Nearly expired** status appears by default 30 before the expiry of the certificate. To configure the warning when a certificate is close to expiry, refer to the section Configuring the warning for an imminent certificate expiry.

IMPORTANT
As the SMC server does not manage certificate revocation, revoked certificates will appear as "Valid".

7.4 Defining the contact IP address of firewalls for VPN topologies

Peers can contact a firewall in a VPN topology via a fixed IP address. There are two options in this case:

- the firewall is contacted by default on the IP address that was detected the last time the firewall logged on to the SMC server.
- however, you can define a customized contact address.

It is also possible to indicate that a firewall has a dynamic IP address and therefore cannot be contacted by its peers – it will always initiate the negotiation of the VPN tunnel. Such tunnels therefore cannot be set up between two peers with dynamic IP addresses.

For any given firewall, you can choose the address at which it will be contacted in most VPN topologies. You can define this default contact address in the firewall's parameters. If you need to define a different address in certain topologies, you can replace the default address directly in these topologies.

7.4.1 Defining a firewall's default contact address

1. Go to **Monitoring** > **Firewalls**, and double click on the firewall.
2. Go to the **IPSec VPN** tab, in **Default contact address**.

The parameter chosen here can be replaced with a different contact address in other topologies, as shown in the following section.

7.4.2 Defining a firewall's contact address in a specific VPN topology

1. In **Configuration** > **VPN topologies**, go to step 4 **Peers and endpoints configuration** when creating or modifying a topology.
2. Double-click in the **Contact address** column.
3. In the **IP address** field, select an object or **Any** to indicate that the IP address is dynamic.

7.5 Selecting the output interface of firewalls for VPN topologies

You can select the firewall output interface used as the source in a VPN tunnel. Two steps are required to do this:

1. In SMC, create the Host object that corresponds to the desired interface,
2. In SMC, select the output interface,
3. If necessary, configure a static route on the firewall.

7.5.1 Creating the Host Object that corresponds to the interface

- In the **Network Objects** menu, create a Firewall_xx Host object that corresponds to an interface configured in the **Configuration** > **Network** > **Interfaces** menu on the firewall. This object will not be deployed on the firewall. The firewall will use the indicated values in its own Firewall_xx object.

7.5.2 Selecting a firewall's output interface on SMC

On SN firewalls, the same parameter is found under **Configuration** > **VPN** > **IPSec VPN** > **Peers** > **Advanced properties** > **Local Address**.

For any firewall, you can choose the output interface that it will use in most VPN topologies. You can define this default output interface in the firewall's parameters. If you need to define a different interface in certain topologies, you can replace the default interface directly in these topologies.

Defining a firewall's default output interface

1. Go to **Monitoring** > **Firewalls**, and double click on the firewall.
2. In the **IPSec VPN** tab, select the desired value for the local address in **Default output interface**. The default value is **Any**.

The parameter chosen here can be replaced with a different interface in other topologies, as shown in the following section.

Defining a firewall's output interface in a specific VPN topology

1. In **Configuration** > **VPN topologies**, go to step 4 **Peers and endpoints configuration** when creating or modifying a topology.
2. Double-click in the **Output interface** column.
3. In the **VPN local address** field, select an interface.

7.5.3 Configuring a static route on the firewall optional

1. Connect directly to the firewall by clicking on the icon from the firewall monitoring view in SMC.
2. In the **Network** > **Routing** menu, create a new static route for each of the VPN tunnel's peers with the following parameters:
   - destination: peer's IP address
   - interface: interface dedicated to VPN communications (the same interface as that selected during the procedure above)
   - gateway: the interface's dedicated gateway for VPN communications

For more information on configuring static routes, refer to the *User Configuration Manual Stormshield Network*.

7.6 Editing, deleting and checking usage of a VPN topology

Edit or delete a topology from the list of your VPN topologies in **Configuration** > **VPN topologies**.

You can also check where generated VTI objects are used in a route-based topology.

To edit a topology:

- Double-click on the line of a topology
  -or-
- Scroll over a line to make the pen icon appear. The icon will appear in each column and allows directly opening the wizard corresponding to the column.

Redeploy the configuration after this operation.

Pour supprimer une topologie:

1. Scroll over the name of the topology in the list and click on the red cross.
2. Redeploy the configuration after this operation.

IMPORTANT
When a route-based VPN topology is modified or deleted in SMC, VTI objects will also be modified or deleted. If you are using such objects in the local configuration of your SN firewalls, first ensure that you delete them before modifying or deleting a topology in SMC.

To check whether VTI objects are in use:

By checking the usage of a route-based VPN topology, you can find out whether VTI objects, which SMC automatically generates when the topology is created, are used in a component of the configuration, such as a filter rule.

You cannot delete a route-based topology or remove peers from the topology as long as any of its objects is in use.

To check whether generated VTI objects are in use:

- Scroll over the name of the topology in the list and click on the icon. The results will be displayed in the lower panel. You can double-click on a result to view details.

7.7 Managing packet fragmentation

The Path MTU Discovery value and fragment size can be defined in the advanced settings via the **Configuration** > **VPN topologies** menu. This feature is supported on SN firewalls versions 3.11.7 to 4.0.0.

Parameter	Description
Path MTU Discovery	Select a value from the drop-down list. • **Disabled**: This option is disabled by default. • **Always add DF bit**: Stealth mode must be disabled on the relevant firewalls by using a CLI command so that this option can be selected. • **Keep DF bit**: If the encrypted packet initially had the DF bit, it will be kept.
Fragment size	Set the maximum size of IKE fragments in bytes. Default value: 1280 bytes Minimum value: 512 bytes

For further information on the corresponding Serverd commands that will be updated on the relevant SN firewalls, refer to the section IPSec config update in the *CLI / SSH Commands Reference Guide*.

7.8 Disabling a VPN topology

If you wish to work on a VPN topology without including it in a configuration deployment, the topology can be disabled.

This means that the tunnel configuration will therefore not be deployed on SN firewalls and the tunnels will not appear in the VPN topology monitoring window.

New topologies are enabled by default when you create them.

To disable a topology:

1. In **Configuration** > **VPN topologies**, go to the line of the topology in question, double-click in the **Status** column to switch the status from **on** to **off**.
2. Deploy the configuration again to apply the change.

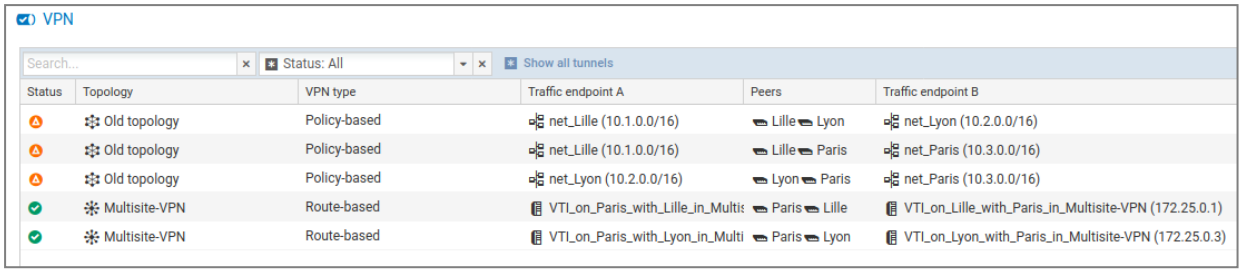
If a topology that has already been deployed is disabled in SMC, and if there has not been any new deployment in the meantime, its tunnels will always remain visible in the monitoring window.

7.9 Monitoring the status of VPN tunnels

The **Monitoring** > **VPN** menu makes it possible to look up the status of each tunnel configured in each topology.

NOTE
To be able to monitor the status of VPN topologies containing firewalls of version 4.2 or higher, you need to use an SMC server of version 2.8.1 or higher.

Scroll over the status icon of a tunnel to show a tool tip indicating its status as well as the status of peers.



In the **Topology identifier (rulename)** column, you can search for topologies by the rulename identifiers used in VPN audit logs on SN firewalls.

When the SMC server is updated, the configuration must be deployed again on firewalls so that the rulename identifier can be seen in logs.

8. Creating filter and NAT rules

This feature is available for SN firewalls in version 3.0 upwards.

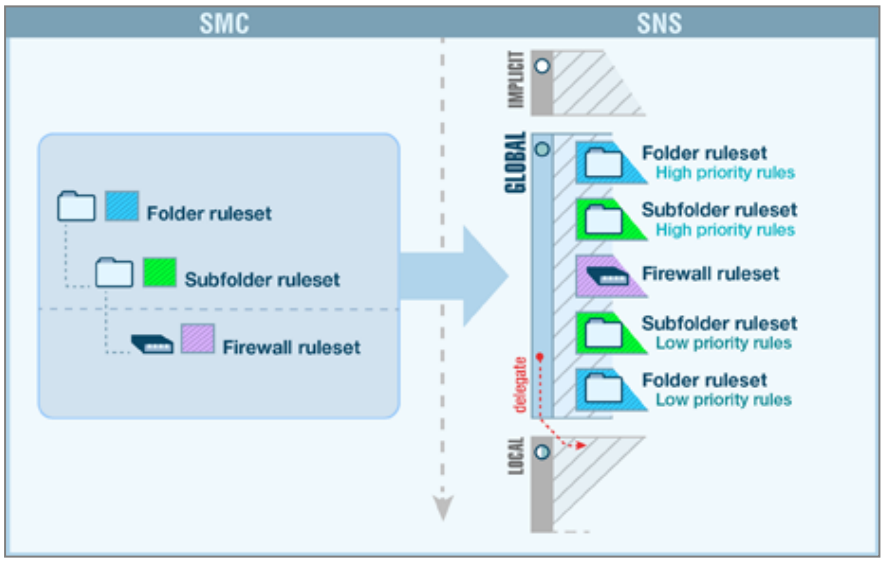
SMC makes it possible to deploy filter and NAT rules in your firewall pool. Rules apply to sets of firewalls (folders and sub-folders) or are specific to certain firewalls, therefore making it possible to configure a rule shared by several sites just once, while continuing to be able to deploy specific rules on a given site.

To organize your firewalls by folders, refer to the section Organizing firewalls by folders. Rules applied to the default root folder **MySMC** apply to the entire firewall pool.

For further detail on each menu and option for configuring rules, refer to the *Stormshield Network User Configuration Manual*.

Rules can be defined in the *Filter rules* and *NAT rules* tabs from the **Configuration > Firewalls and folders** menu or from a firewall's settings.

8.1 Understanding the order in which rules are read



Filter and NAT rules applied to a given firewall are the combination of two types of rules created in SMC:

- Rules shared by several firewalls, created in the folders (folder to which the firewall and its parent folders belong),
- Rules specific to the firewall, created in the firewall's settings. In the firewall monitoring view, the **Number of specific rules** column indicates the number of specific rules that each firewall has.

These rules are deployed in the firewall's global security policy. After these rules, the firewall's local security policy rules, if any, will be applied.

The firewall inherits rules from the folder it belongs to, as well as rules from its parent folders, which are applied in the following order:

- High-priority rules configured in the folders, from the most general to the most specific,
- Firewall's specific rules,
- Low-priority rules configured in the folders, from the most specific to the most general.

EXAMPLE
A high-priority rule in the **MySMC** folder cannot be overwritten by another rule. A low-priority rule in the **MySMC** folder will be overwritten by all the other rules defined in the folders or for a specific firewall.

8.2 Use case examples

8.2.1 Managing a pool without rule sharing

We will use the example of a service provider who manages SN firewalls for several clients:

- Each client only has one firewall,
- All firewalls are located in the **MySMC** root folder, and no sub-folders are used.
- The firewalls do not have any filter rules or NAT rules in common,
- The service provider does not wish to connect to each firewall in real time to define rules.

The service provider must therefore:

- Define specific rules on each firewall in SMC, going to the firewall's **Filter rules** or **NAT rules** tab.
- If necessary, define a "Block all" rule as the last rule on each firewall in order to ignore the rules found in the firewalls' local security policy.
- Deploy the configuration on the firewalls. These rules will be deployed in the firewalls' global security policy.

8.2.2 Managing a pool with shared and specific rules

We shall use the example of a service provider who also administers SN firewalls for several clients:

- Each client only has one firewall,
- The firewalls are organized in sub-folders named after clients,
- The firewalls have filter rules or NAT rules in common and specific rules.

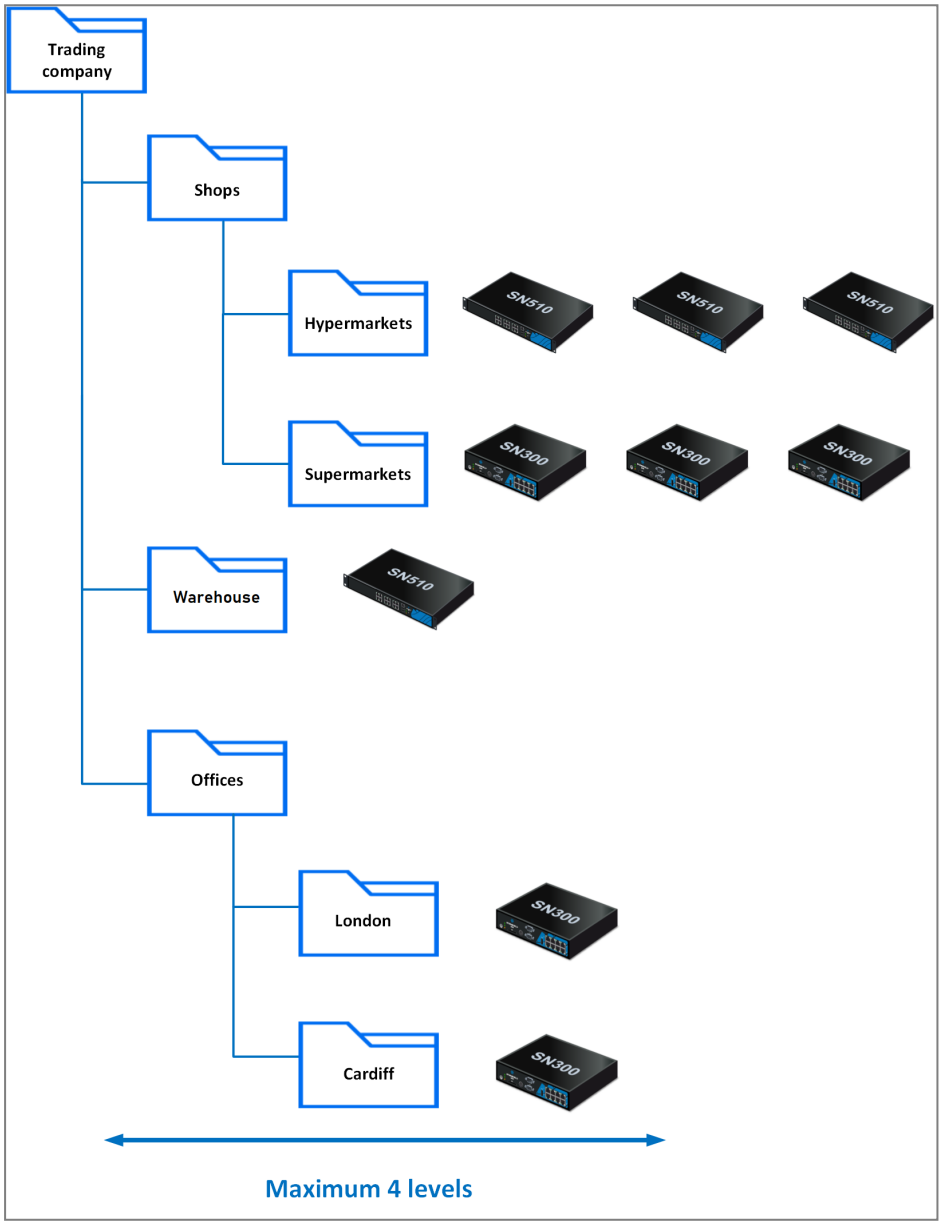
The service provider must therefore:

- define the rules shared by all firewalls in the **MySMC** folder, for example to provide all firewalls with access to its datacenter. For this purpose, a variable object will be used: a Host object representing a firewall interface. A single rule and a single object will therefore suffice for all firewalls. For more information, please refer to the section Managing network objects.
- Define specific rules on each firewall from SMC, going to the firewall's **Filter rules** or **NAT rules** tab.
- If necessary, define a "Block all" rule as the last low-priority rule in the **MySMC** folder in order to ignore the rules found in the firewalls' local security policy.
- Deploy the configuration on the firewalls. These rules will be deployed in the firewalls' global security policy.

8.2.3 Managing a multi-site environment with shared and specific rules and delegated filtering

We shall use the example of a trading company that has a warehouse, offices, hypermarkets and supermarkets spread out over several sites:

- The central administrator uses two levels of sub-folders under the root folder to organize its firewalls,
- Filter and NAT rules apply to all firewalls, and other rules apply only to certain folders,
- The administrator wishes to delegate the administration of certain traffic to local administrators in order to give them the possibility of implementing local rules on specific services, protocols, users or networks. A store may, for example, need to communicate with a CCTV service provider.



The central administrator must therefore:

- Define the rules shared by all firewalls in the **MySMC** folder using variable objects. For more information, please refer to the section Managing network objects.
- Define rules shared by warehouses/offices/stores in the corresponding folders and sub-folders.

- Define, if necessary, specific rules on certain firewalls from SMC, going to the firewall's **Filter rules** or **NAT rules** tab.
- Select the action **Delegate** for the rules concerned in the rule **Action** menu.
- Define a "Block all" rule as the last low priority rule on the root folder **MySMC**.
- Deploy the configuration on the firewalls. These rules will be deployed in the firewalls' global security policy.

8.2.4 Managing a multi-site pool with shared rule sets

We will use the example of a company that has several sites. Every site has the same number of departments with networks and firewalls that must be uniformly configured. The sites are not necessarily configured in the same folder on SMC.

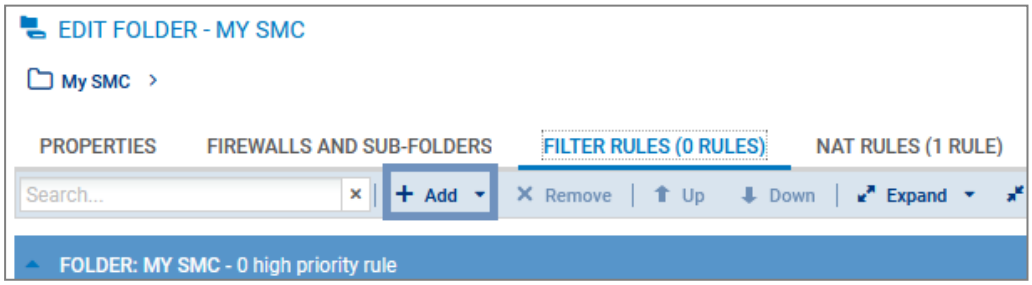
- The central administrator wants to define all filter and NAT rules for a specific department.
- The administrator does not wish to connect to the firewall of each department to define the rules.

The central administrator must therefore:

- Create a rule set containing all the filter and NAT rules dedicated to a department in the menu **Configuration > Rule set**.
- Select the firewalls on which the rule set is to be deployed.
- The next time the rule set is deployed, it will be applied to all the selected firewalls. For more information, refer to the section Creating rule sets.

8.3 Creating filter and NAT rules

1. In **Configuration > Firewalls and folders**, browse until you reach the level of the folder to which you wish to apply a rule or until you reach a specific firewall. In the case of specific rules, go directly to the firewall's settings as well from **Monitoring** view.
2. Open the **Filter rules** or **NAT rules** tab.
3. Click on **Add** and select either a low- or high-priority rule (priority can only be selected for folders), taking into account the desired order of application, as explained in the previous section.



4. Configure the rule:
   - When Host, Network or IP address range objects are used in the rule, you can use variable objects, whose IP addresses will be the value corresponding to the relevant firewall. For more information, please refer to the section Managing network objects.
   - Objects can be dragged and dropped between filter and translation rules or from the **Network objects** menu into rules.
   - You can create separators between rules in order to organize them by clicking on **Add**. These separators do not impact the security policy in any way. Click on the title of a separator to change its name or assign a color to it.
   - The following parameters cannot be completed with data returned by firewalls and must therefore be entered manually through text fields:
     - In **Source** > **General** > **Incoming interface**, click on **Customized interface**.
     - In **Destination** > **Advanced properties** > **Output interface**, click on **Customized interface**.
     - Menu **Action** > **Quality of Service** > **Queue**.
   - Refer to the *Stormshield Network User Configuration Manual* for more details on other menus and options.
5. Once the configuration of rules is complete, deploy the configuration on the firewalls concerned.

In addition to the rules of the current folder or of the firewall, the *Filter rules* and *NAT rules* tabs display the rules of parent folders in read-only. You can therefore view all the rules that apply to a firewall on a single screen, in the order in which they are applied.

8.4 Creating rule sets

Rule sets can be created to group filter or translation rules that you wish to deploy on one or several firewalls. This feature allows you to easily reuse rules on several firewalls regardless of where they are on the tree.

To create a rule set:

1. In **Configuration > Rule set**, click on **Create a set of filter rules** or **Create a set of NAT rules**. You cannot create rule sets containing both types of rules or containing another rule set.
2. Double-click on a rule set to edit its name and assign a color.
3. In the **Rules** tab, click on **Add a rule** to create rules that will be part of your filter or NAT rule set. For further information, refer to Creating filter and NAT rules.

You can also duplicate an existing rule set by clicking on .

8.4.1 Assigning rule sets to a firewall

There are two ways to assign rule sets to a firewall.

- In **Configuration > Rule set**:

  Select the rule sets from the list on the left. In the **Firewalls** tab, select the firewalls you wish to assign the rule sets to, and click on **Apply**. You can choose to add the rule sets to specific rules on the selected firewalls in the first or last position.

- In the security policy of a firewall in the **Filter rules** and **NAT rules** tabs:

  Click on **Add > Add a rule set**.

During the next deployment, the rule sets assigned to the firewall will be added to the selected firewalls. They will appear in the firewall's global policy as separators followed by their rules.

8.4.2 Editing rule sets for a firewall

From an SN firewall's editing window, you can:

- replace the rule set assigned to the firewall with another set,
- edit the rule sets assigned to the firewall. You will be redirected to the **Rule sets** screen.

8.4.3 Importing or exporting rule sets

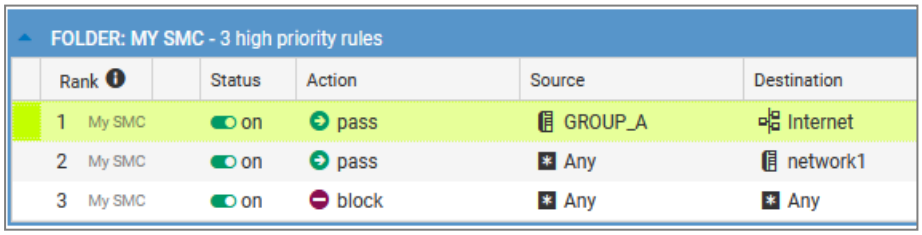
In **Configuration** > **Rule set**, you can:

- export all the filter or NAT rule sets to a CSV file. In this file, they will be represented as separators followed by their rules. For more information, please refer to Exporting rules to a CSV file.
- import all the filter or NAT rule sets from a a CSV file. Rule sets must be created on the SMC server before importing the CSV file, otherwise the import will fail. For more information, please refer to Importing rules from a CSV file.

8.5 Identifying the rules

In the **Filter rules** and **NAT rules** tabs of a firewall, the **Rule** column makes it possible to identify the rules applied to a firewall. This number can be seen in the firewall's administration interface and in logs.

In the folders view, the **Rule** column is replaced with the **Rank** column. It indicates the position of the rule in the folder containing the rule.



8.6 Changing the order in which rules are executed

You can change the order in which rules are executed by going to the **Filter Rules** or **NAT Rules** tabs of a folder or firewall and moving the rules within the same folder or on the same firewall or even into another folder or firewall.

You can select several rules at a time or a separator. Whenever a collapsed separator is selected, you are selecting all the rules contained in this separator.

Moving rules within the same firewall or folder

- Select the rule, separator or rule set, and use the toolbar's **Up** and **Down** buttons.

-or-

- Place the cursor on the left column of a rule, and drag and drop.

-or-

- Use the **Cut**/**Copy**/**Paste** buttons or the corresponding standard keyboard shortcuts. You can copy rules or separators from the active table or from parent folders.

Moving rules into another folder or onto another firewall

Use the toolbar's **Cut**/**Copy**/**Paste** buttons or the corresponding standard keyboard shortcuts to move the rule, rule set or separator into another folder or onto another firewall. You can copy rules from the active table or from parent folders.

You can also create rule sets to be reused on other firewalls, regardless of which folder they are in. For more information, refer to the section Creating rule sets.

8.7 Searching for a rule in the web interface or in SMC logs

The SMC server automatically assigns a unique ID to each filter and translation rule created. This ID or rule "name" will be shown in the SMC web interface, and in the web interface and logs of the relevant firewall whenever the rule is deployed. The default name can be changed in the rule's properties.

The rule name makes it easier to identify the rule when you are searching for it in SMC logs, or in the rule panel in the firewall's or SMC server's interface.

To find out the name of a rule in SMC:

1. Go to the filter and translation rule panel of a firewall or a folder,
2. Scroll over any column title with the mouse,
3. Click on the black arrow that appears,
4. Scroll over the **Columns** menu,
5. Select the **Name** column.

- or -

1. Double click on a rule to show its properties,
2. Display the **General** tab.
3. In **Advanced properties**, you can copy the name of the rule to perform a search in the SMC logs or in the firewall interface.

8.8 Removing rules

- Press **DELETE**.

-or-

- Click on **Remove** in the toolbar.

When a folder is removed, its rules are removed as well.

8.9 Removing rule sets

In **Configuration > Rule sets**, select the rule set that you wish to remove and click on .

If the rule set is in use, you will be warned and asked to confirm whether to remove it.

Removing a rule set from the firewall's editing window will not remove it on SMC, but the rule set will no longer be assigned to the firewall in question.

8.10 Importing and exporting filter and NAT rules

On the SMC server, rules can be imported and exported through the web interface or command line interface.

By importing and exporting logs, you can:

- easily deploy rules from one firewall or another SMC server on other firewalls.
- move the management of firewall rules to the SMC server when migrating a pool of firewalls in production to SMC. If this applies to your use case, refer to the section Migrating local rules on a firewall to manage them in SMC.

8.10.1 Importing rules from a CSV file

This feature makes it possible to import rules from a CSV file that was created manually or exported from a SN firewall. Files can contain both filter and NAT rules.

Creating the CSV file

An example of a CSV file "example-import-rules.csv" is available on the server, in the folder */opt/stormshield/examples/csv/*.

You can either export existing rules from a firewall or create a new CSV file.

To export the CSV file from a firewall:

1. Connect to the firewall.
2. Go to the menu **Security policy ⇒ Filtering and NAT**.
3. At the top of the panel, choose whether to display the global or local policy that you wish to export. Only rules from the active slot will be exported.
4. Click on **Export**.

IMPORTANT
Check that the CSV file editor has not modified the "," separator character, in which case the file may not be imported on the SMC server. For more information on the separator character, refer to the section Choosing the separator character in CSV files.

To create a new CSV file, and to find out details about header lines, you may:

- Choose to export rules from a firewall,
- Look up the example given on the SMC server as indicated above.

Do note that you must create a CSV file for each rule folder and a CSV file per firewall for the firewall's specific rules.

Importing rules from the web interface

You need read/write privileges to import rules.

If the rules reference objects from your SNS configuration that are not already in the SMC configuration, you must import them beforehand on the server. For more information on importing objects, refer to the section Importing objects.

1. In **Configuration** > **Firewalls and Folders**, browse until you reach the level of the folder or the firewall on which you want to import the rules.
2. Open the **Filter rules** or **NAT rules** tab. Both types of rules can be imported from either tab and from the same CSV file.
3. Click on **Import** in the toolbar.
4. Select the CSV file to import.
5. Choose whether to add the rules to existing rules or to replace them with the new imported rules. When you select the first option, new rules will be added after existing rules in a separator, and the date on which they were imported will be indicated.
   Rules are imported to the high-priority rules of a folder by default. To import rules to low-priority rules, indicate the value "low" in the column *#smc_folder_prio* in the CSV file (last column). If the file was exported from a firewall, there is no such column; add it manually.

NOTE
If you wish to import a security policy that contains rule sets, you must create them first on the SMC server. For more information, refer to the section Creating rule sets.

In case of error, refer to the import summary.

No other actions can be performed on the server while rules are being imported.

Importing rules in command line

The command for importing rules is: `smc-import-rules`

Various options can be added to this command.

During import, we recommend that you log on to the administration session exclusively with read/write access.

Rule sets cannot be imported in command line.

In both of the following cases, for each rule imported, the status of the import will be displayed. If there is a failure while importing a rule, the reason will be given and no rules or objects will be imported. However, the entire CSV file will be scanned so that the SMC server can detect potential errors. Correct any errors before attempting a new import.

Rules that were imported in command line are added after existing rules.

If the rules reference objects from your SNS configuration that are not already in the SMC configuration, you can also import them on the server together with the rules.

If you are importing rules and objects referenced in rules:

1. Export the list of objects in CSV format from an SN firewall by following the procedure in the section Creating the CSV file.
2. Copy both CSV files (rules and objects) on the SMC server using the SSH protocol in the */tmp* folder for example.
3. Connect to the SMC server via the console port or SSH connection with the “root” account,

4. Depending on the rule destination, type the command:
   - `smc-import-rules /tmp/rules-file.csv --objects /tmp/objects-file.csv --firewall destination-firewall`: the destination of these rules is a firewall,
   - `smc-import-rules /tmp/rules-file.csv --objects /tmp/objects-file.csv --folder destination-folder`: the destination of these rules is a folder, Rules are imported to the high-priority rules of a folder by default. To import rules to low-priority rules, add `--low-priority` at the end of the command or indicate the value "low" in the column *#smc_folder_prio* in the CSV file (last column). If the file was exported from a firewall, there is no such column; add it manually.

The CSV file containing the list of objects includes the full list of objects found in the configuration of the SN firewall, but at this stage, the SMC server will only import objects that were referenced in rules. If objects referenced in rules are already on the server, they will not be imported a second time.

However, if necessary, you can force the update of these objects using the option `--update`:

```
smc-import-rules /tmp/fichier-de-regles.csv --update --objects
/tmp/fichier-d-objets.csv --folder dossier-de-destination --low-priority
```

IMPORTANT
The SN firewall cannot export router and time objects. If your rules contain such objects, you will need to create them manually in SMC.

If you are importing rules only (without objects):

1. Start by copying the CSV file on the SMC server using the SSH protocol in the */tmp* folder for example.
2. Connect to the SMC server via the console port or SSH connection with the “root” account,
3. Depending on the rule destination, type the command:
   - `smc-import-rules /tmp/rules-file.csv --firewall destination-firewall`: the destination of these rules is a firewall,
   - `smc-import-rules /tmp/rules-file.csv --folder destination-folder`: the destination of these rules is a folder. Rules are imported to the high-priority rules of a folder by default. To import rules to low-priority rules, add `--low-priority` at the end of the command or indicate the value "low" in the column *#smc_folder_prio* in the CSV file (last column). If the file was exported from a firewall, there is no such column; add it manually.

8.10.2 Exporting rules to a CSV file

You only need read privileges to export rules.

1. In **Configuration** > **Firewalls and Folders**, browse until you reach the level of the folder or the firewall from which you want to export rules.
2. Open the **Filter rules** or **NAT rules** tab. Both types of rules can be exported from either tab and to the same CSV file. Rules are distinguished by type in the *#type_slot* column.
3. Click on **Export** in the toolbar.
4. Save the CSV file.

When rules are exported from a folder, only the rules found in the folder are exported, not the rules in parent folders. The *#smc_folder_prio* column in the file indicates the priority of the rule.

When rules are exported from a firewall, the entire policy is exported – the rules of the firewall and its parent folders. The *#folder* column in the file shows the name of the folder that contains each

rule. The *#ruleid* and *#rankid* columns indicate the number that identifies the rule in the policy and its position in a folder. For more information, refer to the section Identifying the rules.

If your security policy contains rule sets, they will be converted to separators followed by their rules in the CSV export file.

8.10.3 Importing rules from connected firewalls

To import rules from connected firewalls to the SMC server, the firewall must be in at least version 3.3.

This feature makes it possible to import rules from the firewall's global or local slot. In both cases, only the rules from the active slot will be imported.

If the rules reference objects from your SNS configuration that are not already in the SMC configuration, they will also be imported on the server.

1. Go to **Monitoring** > **Firewalls**, and double click on the firewall.
2. Open the **Filter rules** or **NAT rules** tab. In both cases, both types of rules will be imported.
3. Click on the arrow to the right of the **Add** button.
4. Click on **Import local filter and NAT rules** or **Import global filter and NAT rules**.
5. Follow the steps indicated.

At the end of the operation, the imported rules will be placed in a separator and are selected.

If the import via the web interface fails, you can import the rules in command line as indicated in the section Importing rules in command line. If errors occur, details will be provided.

8.11 Migrating local rules on a firewall to manage them in SMC

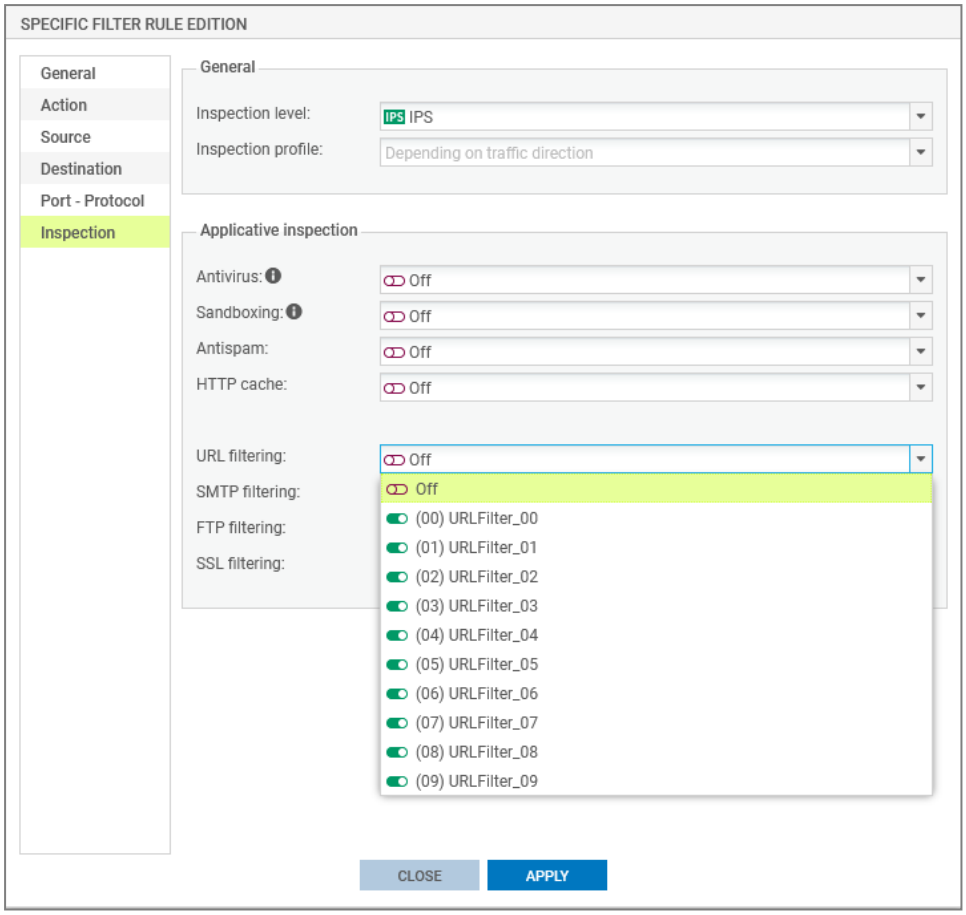
When a pool of firewalls in production is connected to SMC, proceed as follows to manage rules that already exist on a firewall in SMC:

1. Import rules from a firewall onto the SMC server by following the procedure set out in Importing rules from connected firewalls .
2. The Use case examples may give you ideas on choosing how to organize newly imported rules.
3. In SMC, deploy the rules on the firewall in question. They will appear in the firewall's global policy and will be applied as a priority.
4. Ensure that this new organization functions properly.
5. If necessary, define a "Block all" rule as the last low-priority rule in the **MySMC** folder in order to ignore the rules found in the firewalls' local security policy.
6. When the process is complete, delete the rules that have been migrated from the firewall's local policies to SMC.

If you do not create a "Block all" as the last rule in SMC, local filter and NAT rules, i.e., those created directly on a firewall, will be read after global rules (originating from SMC).

8.12 Managing URL filtering on SN firewalls from SMC

In SMC, you can create filter rules referencing URL filtering profiles configured locally on firewalls by selecting their identifier (00 to 09).



However you cannot set up these profiles directly in SMC and they may be different on each firewall even if they have the same identifier.

This section explains how to deploy a common URL filtering policy on all or part of your firewalls thanks to SMC, based on the URL filtering policy configured on a "template" firewall.

You will need two scripts to do so: a first one which allows collecting the URL filtering policy from the template firewall and another one which allows deploying this policy on the selected firewalls.

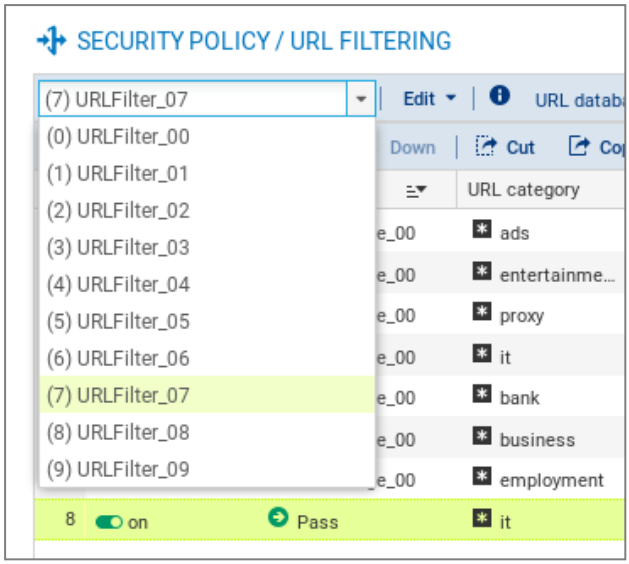
IMPORTANT
The template firewall and the target firewalls must be in the same version.

To apply this procedure, follow the three steps below in the order given.

8.12.1 Creating the template URL filtering policy

The first step consists in creating or editing one or more URL filtering profiles on a firewall (10 profiles available). This firewall stands for the template URL configuration to be deployed on other firewalls.

1. Connect to the web administration interface of the template firewall with its IP address or connect directly through SMC.
2. Open the menu **Security policy** > **URL filtering**.
3. Create or edit URL filtering profiles.



8.12.2 Saving the URL filtering policy of the template firewall

The following script allows collecting the URL filtering policy of the template firewall (URL filtering profiles and Web objects).

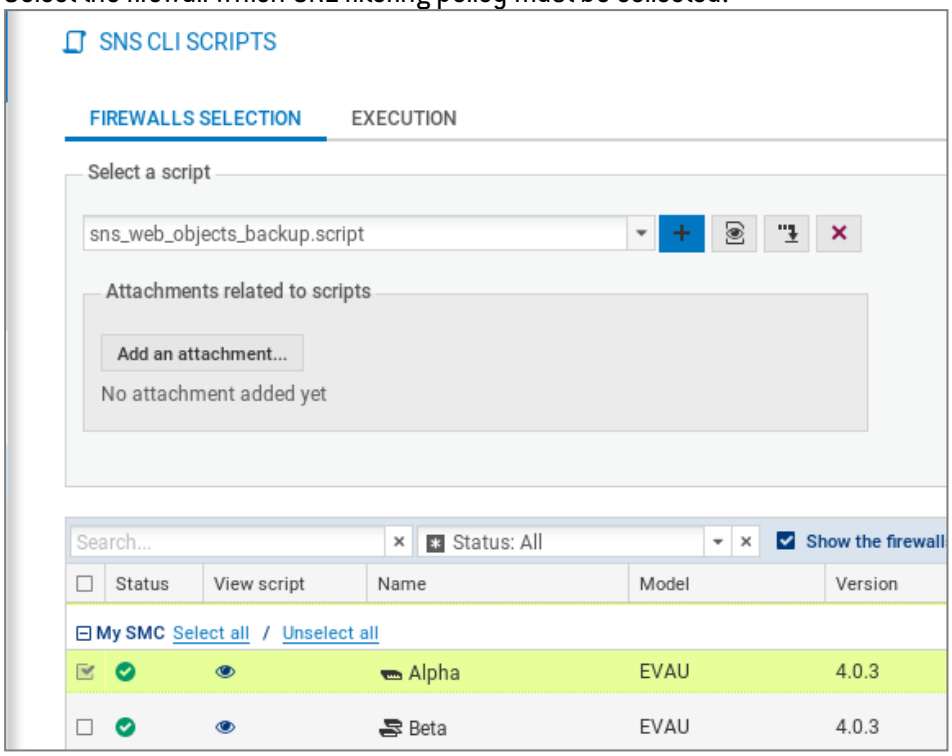
```
#####################################################################
# Save URLs, Certificate names, URL and CN groups and the           #
# URL base of a SNS #firewall                                       #
#                                                                   #
# The $SAVE_TO_DATA_FILE argument indicates the name of the file in #
# which the result of the execution will be saved                   #
#####################################################################

CONFIG BACKUP list=urlfiltering $SAVE_TO_DATA_FILE("backup-URL.na")
```

To use the script:

1. Copy it to a text editor and save it with the *.script* extension.
2. In SMC, open the menu **Deployment** > **SNS CLI Scripts**.
3. Select the script you saved previously.

4. Select the firewall which URL filtering policy must be collected.



5. Execute the script.
6. Download the archive generated by the script. The archive contains the backup file *backup-URL.na*.

For more information on SNS CLI scripts, please refer to the section Running SNS CLI commands on a pool of firewalls.

8.12.3 Deploying the template URL filtering policy

The following scripts allow deploying the URL filtering policy previously saved on the other firewalls.

- Script required if using filtering with an embedded Stormshield URL base:

```
#####################################################################
# Restore URLs, Certificate names, URL and CN groups and the URL#
# base of a SNS firewall                                            #
#####################################################################

# use the embedded categories
CONFIG OBJECT URLGROUP SETBASE base=NETASQ


# Restore the configuration
CONFIG RESTORE list=urlfiltering fwserial=local $FROM_DATA_FILE("backup-
URL.na")
```

- Script required if using filtering with an advanced Stormshield URL base (with the option Extended Web Control):

```
#####################################################################
# Restore URLs, Certificate names, URL and CN groups and the URL#
# base of a SNS firewall                                            #
```

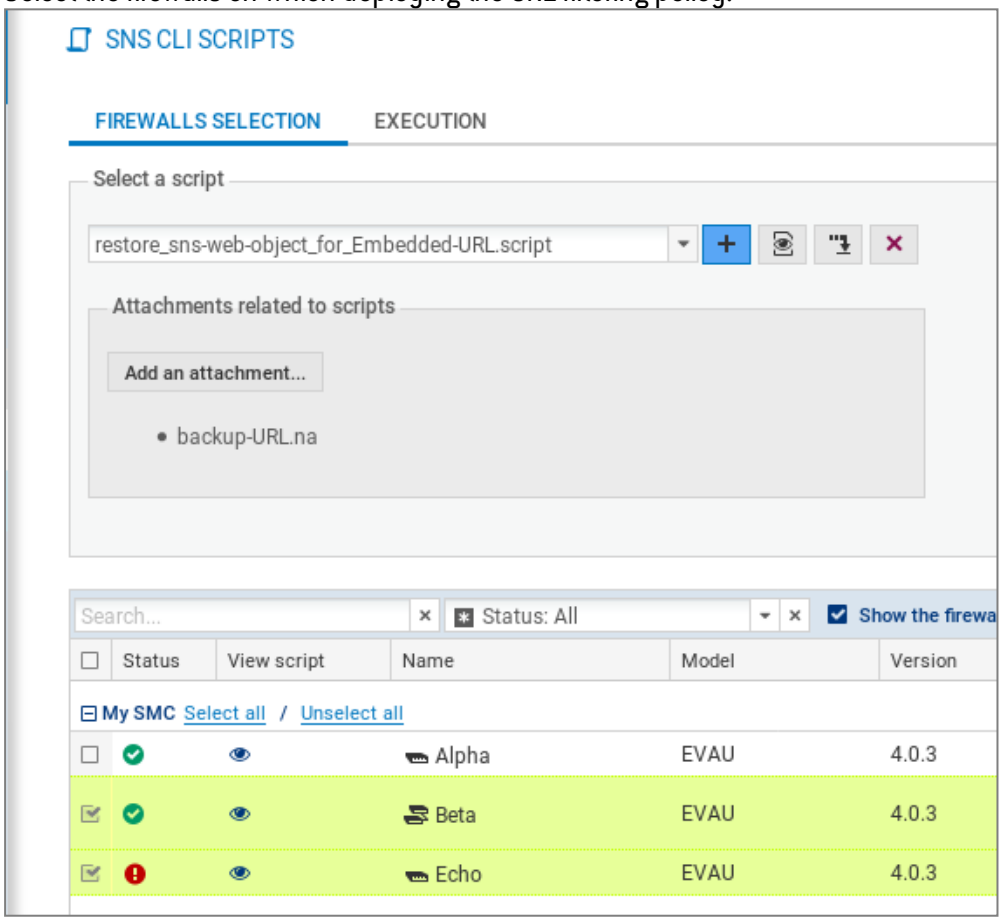
```
#################################################################

CONFIG OBJECT URLGROUP SETBASE base=CLOUDURL


# Restore the configuration
CONFIG RESTORE list=urlfiltering fwserial=local $FROM_DATA_FILE("backup-
URL.na")
```

To use the scripts:

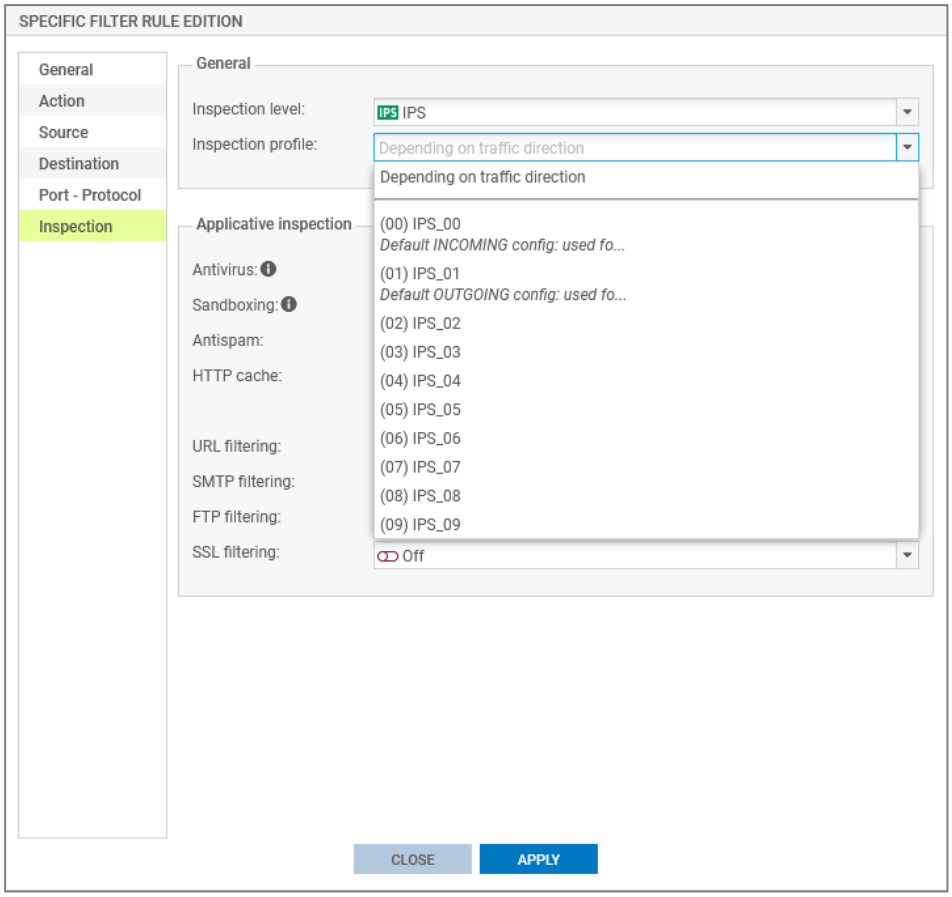
1. Copy the script adapted to the URL base you are using to a text editor and save it with the *.script* extension.
2. In SMC, open the menu **Deployment** > **SNS CLI Scripts**.
3. Select the script you saved previously.
4. Select the *.na* backup file previously created as attached file.
5. Select the firewalls on which deploying the URL filtering policy.



6. Execute the script.
7. You can connect to a firewall through SMC to see the URL filtering policy has been properly deployed.

8.13 Managing IPS Inspection profiles on SN firewalls from SMC

In SMC, you can create filter rules referencing IPS Inspection profiles configured locally on firewalls by selecting their identifier (00 to 09).



However you cannot set up these profiles directly in SMC and they may be different on each firewall even if they have the same identifier.

This section explains how to deploy common IPS Inspection profiles on all or part of your firewalls thanks to SMC, based on the profiles configured on a "template" firewall.

You will need two scripts to do so: a first one which allows collecting the profiles from the template firewall and another one which allows deploying these profiles on the selected firewalls.

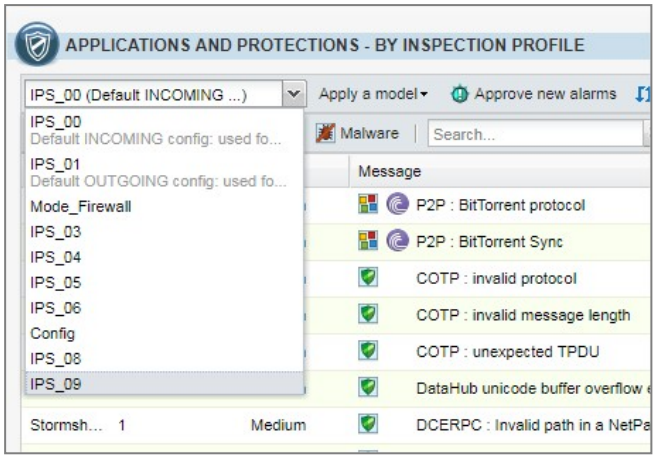
IMPORTANT
The template firewall and the target firewalls must be in the same version.

To apply this procedure, follow the three steps below in the order given.

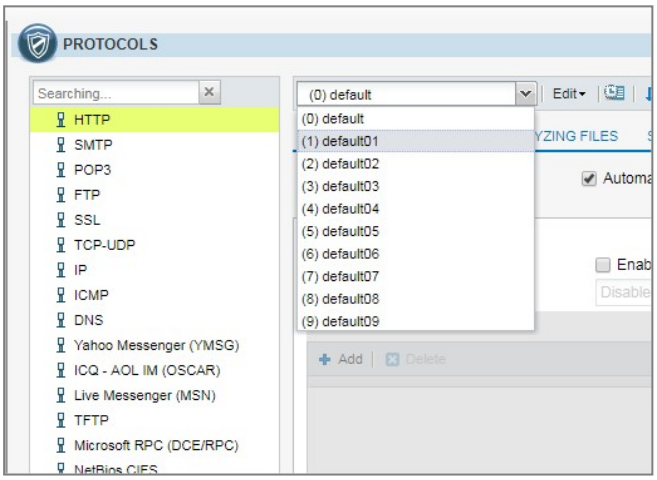
8.13.1 Editing the template IPS Inspection profiles

The first step consists in editing one or more IPS profiles among the 10 profiles available on a firewall. This firewall stands for the template IPS configuration to be deployed on other firewalls.

1. Connect to the web administration interface of the template firewall with its IP address or connect directly through SMC.
2. Open the menu **Application protection** > **Applications and protections**.
3. Edit settings for the wanted applications and protections.



4. Open the menu **Application protection** > **Protocols**.
5. Edit settings for the wanted protocols.



8.13.2 Saving the IPS Inspection profiles of the template firewall

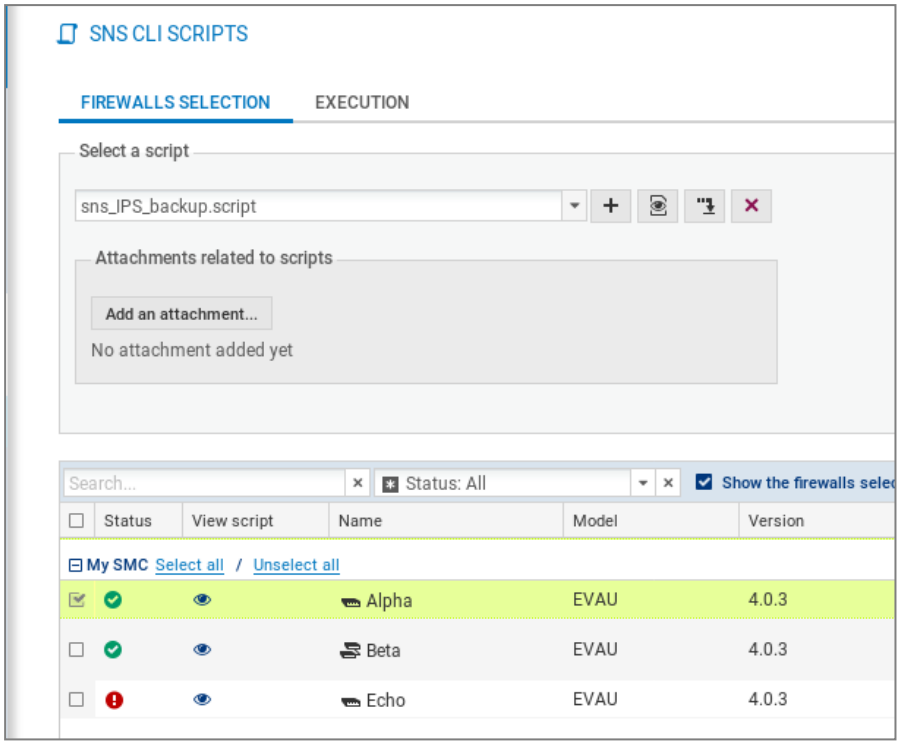
The script below makes it possible to retrieve the IPS Inspection profiles of the template firewall.

```
#######################################################################
# Save the IPS configuration for a given SNS firewall
#
# The $SAVE_TO_DATA_FILE argument indicates the name of the file in
# which the result of the execution will be saved
#######################################################################


CONFIG BACKUP list=securityinspection $SAVE_TO_DATA_FILE("backup-IPS-
Conf.na")
```

To save the profiles:

1. Copy the script to a text editor and save it with the *.script* extension.
2. In SMC, open the menu **Deployment** > **SNS CLI Scripts**.
3. Select the script you saved previously.
4. Select the firewall of which the IPS Inspection profiles must be saved.



5. Execute the script.
6. Download the archive generated by the script. The archive contains the backup file *backup-IPS-Conf.na*.

For more information on SNS CLI scripts, please refer to the section Running SNS CLI commands on a pool of firewalls.

8.13.3 Deploying the IPS Inspection profiles

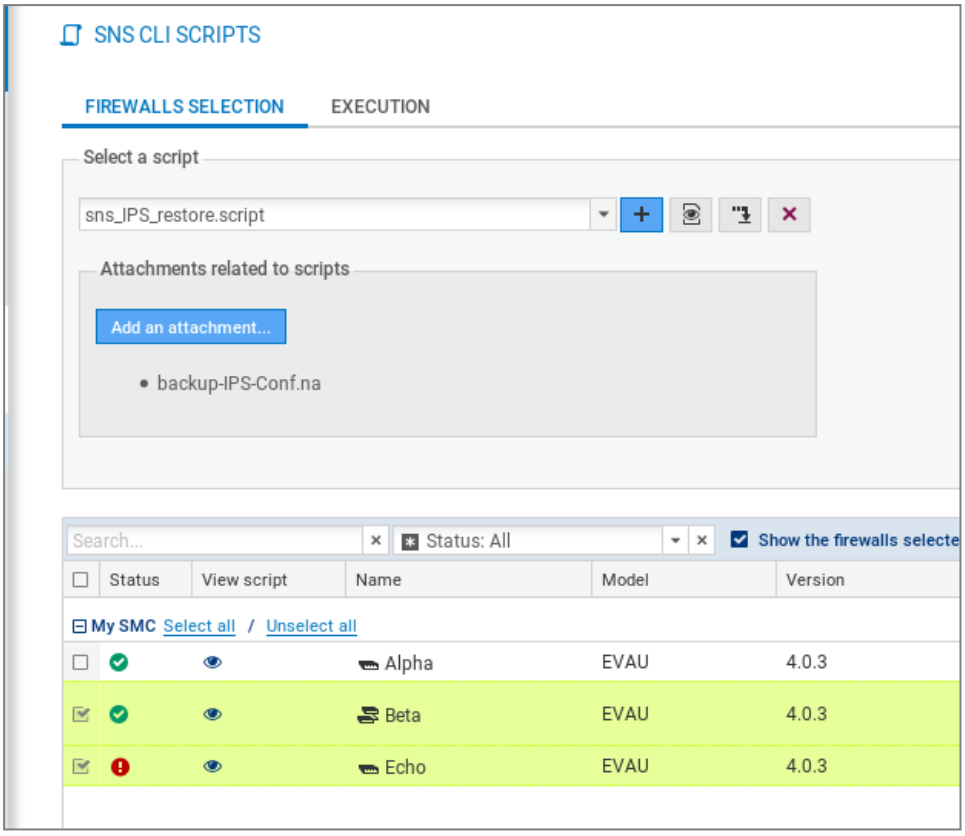
The script below makes it possible to deploy the IPS Inspection profiles previously saved on the other firewalls.

```
#############################################################
# Restore the IPS configuration for one or several SNS firewall(s)
#
# The $FROM_DATA_FILE argument indicates the name of the file that will
# be uploaded to the firewall(s)
#############################################################


# Restore the IPS configuration
CONFIG RESTORE list=securityinspection $FROM_DATA_FILE("backup-IPS-
Conf.na")
```

To deploy the profiles:

1. Copy the script to a text editor and save it with the *.script* extension.
2. In SMC, open the menu **Deployment** > **SNS CLI Scripts**.
3. Select the script you saved previously.
4. Select the *.na* backup file previously created as attached file.
5. Select the firewalls on which deploying the IPS Inspection profiles.



6. Execute the script.
7. You can connect to a firewall through SMC to see the profiles have been properly deployed.

8.14 Adding public IP address reputation groups

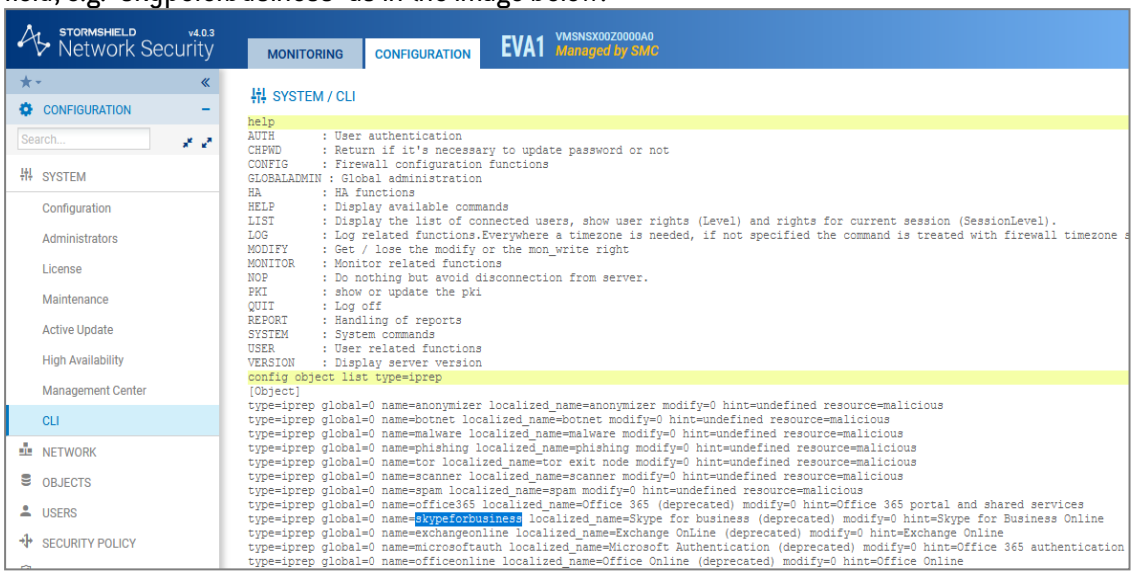
Filter rules may apply to hosts whose public IP addresses have been classified under one of the reputation groups defined on SN firewalls.

In order to benefit from updates of public IP address reputation groups without having to update your version of the SMC server, you can manually add new groups.

To add new address reputation groups, you need to know the names of the groups used on SN firewalls before adding them to the file *smc-ip-reputation.local*.

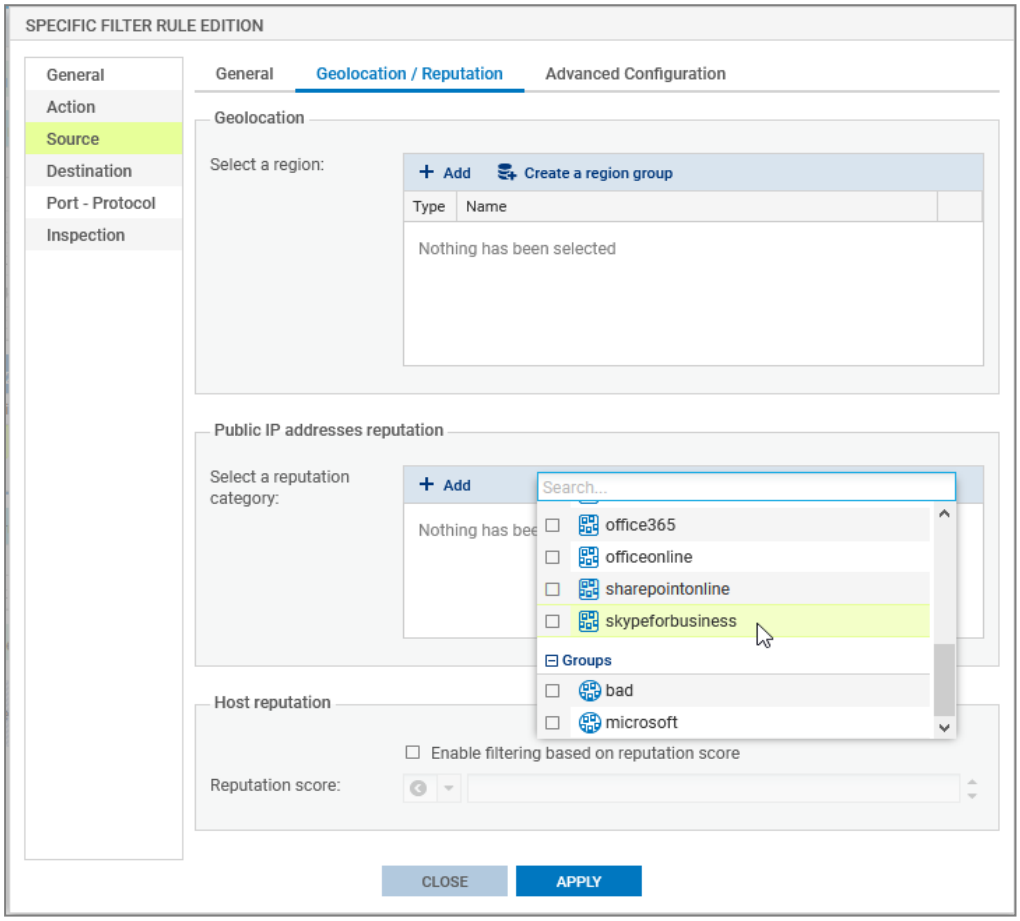
8.14.1 Finding out names of groups to be used

1. On an updated SN firewall, run the command `config object list type=iprep`.
2. The name to be used in order to add the group to the SMC server is the value of the "name" field, e.g. "skypeforbusiness" as in the image below.



8.14.2 Adding address reputation groups to the SMC server

1. Log on to the SMC server via the console port or in SSH using the "root" account.
2. Add the new group names to the file */data/config/smc-ip-reputation.local*.
3. In the server's web interface, refresh the display to view the new groups in the **Source** and **Destination** menus in filter rules:



9. Running SNS CLI commands on a pool of firewalls

SMC allows executing SNS CLI scripts on firewalls from version 2.4 upwards. This mode enables the configuration of all firewall features. Scripts therefore offer a solution for deploying the configuration of a pool of firewalls for features that are not available in the menus of the SMC server.

SNS CLI scripts can be executed from the web interface of the SMC server and from the command line interface.

To see an example of how scripts are used, refer to the section Updating firewalls by using SNS CLI scripts.

9.1 Creating the CLI command script

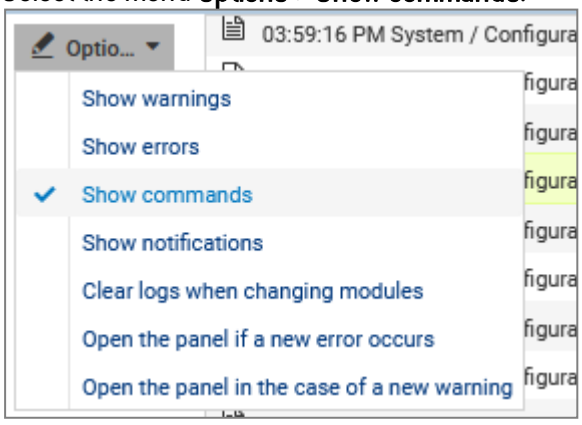
Create a UTF-8 encoded text file not exceeding 5 MB with the extension *.script* containing the commands to be run in your environment of firewalls.

The available executable commands on the CLI console are listed:

- In the firewall web administration interface, in the menu **Configuration** > **System** > **CLI Console**. Refer to the *Stormshield Network User Configuration Manual* to learn how to use the interface.
- In the *CLI Serverd Commands Reference Guide*.

To assist you, you may also display CLI commands in the web administration interface of a firewall in order to copy the commands used to perform an action that you wish to reproduce in your script:

1. Click on the black arrow at the bottom of a SN firewall's administration interface to expand the events panel.
2. Select the menu **Options** > **Show commands**.



3. Perform an action (create an object for example) that you wish to repeat in the script.
4. Copy the commands that were run to produce the action.
5. Paste them in your script.

To adapt commands to each firewall, use variables surrounded with the symbol %. To find out which variables to use, please refer to the section Using variables.

9.2 Using variables

The properties of firewalls indicated in the list of firewalls or in the settings of each firewall (**Monitoring** > **Firewalls** menu) are variables that can be used in scripts.

You can use even more variables with the help of a CSV file. Refer to the section Using variables.

Variables are case sensitive.

9.2.1 Using variables specific to firewalls

Insert variables surrounded with the symbol % in the CLI commands of your script.

These variables take on different values according to the firewall on which the script is run:

- FW_ADDRESS: IP address field of the firewall connected to the SMC server,
- FW_DESCRIPTION: Firewall's Description field,
- FW_LOCATION: firewall's Location field,
- FW_MODEL: firewall's model,
- FW_NAME: firewall's name,
- FW_SERIAL: firewall's serial number,
- FW_VERSION: firewall's version number,
- FW_ARCHITECTURE: architecture of the firewall's processor,
- FW_SIZE: firewall range,
- FW_VM: virtual firewall,
- FW_UPD_SUFFIX: variable used for the SN firewall update, taking on the value SNS-%FW_ARCHITECTURE%-%FW_SIZE%.maj (*SNS-amd64-M.maj* for example). For more information, refer to the section Updating firewalls by using SNS CLI scripts.
- HA_PEER_SERIAL: serial number of the passive firewall (without High availability, the value will be empty),
- HA_PEER_FIRMWARE: version number of the passive firewall (without High availability, the value will be empty),
- CUSTOM_X : customized fields

%CUSTOM_X% variables can be customized to fit your needs. Double-click on a firewall in the **Monitoring** > **Firewalls** menu and open the **Customized variables** tab. For more information, please refer to the section Creating customized variables.

9.2.2 Using global variables

These variables have the same value for all firewalls and refer to the server's date and time:

- NOW: full date in local format (example: "%NOW%" => "20151222-104727"),
- NOW_AS_DATE: date in local format (example: "%NOW_AS_DATE%" => "20151222"),
- NOW_AS_TIME: time in local format (example: "%NOW_AS_TIME%" => "104727").

9.2.3 Using a CSV file

In order to perform operations on a large number of firewalls, or to perform a complex operation on a firewall, we recommend that you use a CSV file.

CSV files can only be used in the command line interface. Variables associated with firewalls will then be read from this file and the script will be duplicated as many times as the number of lines in the CSV file for a given firewall.

An example of a CSV file "example-sns-cli-script.csv" is available on the server, in the folder */opt/stormshield/examples/csv/*.

To find out how to use CSV files in the command line interface, refer to the section Examples of the use of scripts in command line with a CSV file.

9.3 Running the SNS CLI script from the web interface

1. In the web interface of the SMC server, select **Deployment** > **SNS CLI scripts**.
2. In the **Firewalls selection** tab, select the script to run.
   - You can store a list of scripts on the SMC server,
   - The button makes it possible to show the raw contents of the script as it is found on your workstation.
3. In the **Attachments related to the script** menu, add the relevant files to attach to the script. These files will be deleted from the SMC server after the script has been successfully executed. For more information, please refer to the section Attaching files to a script and receiving files generated by script.
4. In the second part of the **Firewalls selection** tab, select the SN firewalls on which the script will be run. For each firewall:
   - The icon indicates, where applicable, that the firewall cannot be selected to run the script. The row will be grayed out in this case. Scroll over the icon with your mouse to find out why.
   - The icon makes it possible to view the contents of the script, including variables replaced with values associated with the firewall in question. The icon becomes if there is an error during the analysis of the script (missing attached file or unknown variable). View the contents of the script to find out which row is causing the issue.
5. Click on **Execute script** at the bottom of the tab. The **Execution** tab automatically opens.
6. Track the progress and results of the execution of scripts on each selected firewall. During the execution of a script or deployment of a configuration, you will not be able to run another script execution but you can prepare it in the **Firewalls selection** tab.

> **IMPORTANT**
> Executing script automatically adopts the reading/writing privileges on any administration sessions already open on the firewalls in question.

7. A summary of the execution process can be seen at the bottom of the panel, displaying successful operations, errors and the firewalls on which the script could not be deployed.
8. You can also filter the list of firewalls by selecting a status in the drop down list at the top of the list.
9. In case of error, see the SMC server logs. You can also connect to the logs and activity reports of a firewall by clicking on the icon in the **Actions** column.

9.4 Running the SNS CLI script in command line

From the command line interface, you can:

- add a script in the script folder on the SMC server and run it immediately.
- run a script that has already been stored on the SMC server,
- add a script in the script folder on the SMC server.
- delete a script from the script folder on the SMC server,
- show the list of scripts stored on the SMC server.

The main command `smc-sns-cli-script` must be followed by one of the five commands corresponding to these actions.

The scripts storage repository is named *nsrpc-scripts* and is available from */data/users/*.

9.4.1 Displaying the list of commands and options

- To display the list of commands, type --help:

```
fwadmin-sns-cli-script <command>

Commands:
  fwadmin-sns-cli-script add <file-path>    Add a SNS CLI script to the SMC
                                            scripts repository
  fwadmin-sns-cli-script delete             Delete a SNS CLI script from the SMC
  <script-name>                             scripts repository
  fwadmin-sns-cli-script exec <file-path>   Add a specific SNS CLI script and
                                            run it immediately
  fwadmin-sns-cli-script list               List all the installed SNS CLI
                                            scripts in the SMC scripts
                                            repository
  fwadmin-sns-cli-script run <script-name>  Run a specific SNS CLI script

Options:
  -h, --help  Show help
```

- Each of these commands has specific options. To display them, type `smc-sns-cli-script <name_of_action> -h`.

9.4.2 Running a script

- To add a script on the SMC server and run it immediately, use the command: `smc-sns-cli-script exec <file_path>`
- To run a script that has already been stored on the SMC server, use the command: `smc-sns-cli-script run <script_name>`

From the options that come with these commands, you must choose one of the following:

- --firewall-list: to be followed by a list of firewall names separated by commas,
- --all: indicates that the script will be run on all firewalls,
- --csv-file: to be followed by a path to a CSV file containing the list of firewalls and the associated variables. The command will then list the firewalls specified in this file. For more information, please refer to the section Using a CSV file.

The option --csv-file can be used together with the options --firewall-list and --all. In this case, both of these options specify the list of firewalls on which the script is to be run.

The following options are not mandatory:

- --dry-run: allows displaying the contents of the script including the variables associated with each firewall, for the purpose of reference only.
- --raw-output: allows showing how the script was run in raw text,
- --update: makes it possible to force the script to be added on the server if a script with the same name already exists. This option is only available for the command `exec`.

When the deployment of a configuration is in progress, or another script is being run, a new script cannot be run in command line. An error message will appear if the deployment has not fully ended on all connected firewalls or if the script has not finished running. Firewalls on which the configuration was deployed in batches will not prevent scripts from running.

To send or receive files attached to a script, please refer to the section Attaching files to a script and receiving files generated by script.

9.4.3 Adding scripts

To add a script in the script folder on the SMC server, use the command `smc-sns-cli-script add <file_path>`.

Option--update: makes it possible to force the script to be added on the server if a script with the same name already exists.

9.4.4 Deleting scripts

To delete a script from the SMC server, use the command `smc-sns-cli-script delete <script_name>`.

9.4.5 Displaying the list of scripts

To show the list of scripts found in the script folder of the SMC server, use the command `smc-sns-cli-script list`.

9.4.6 Examples of the use of scripts in command line with a CSV file

The following is an example of how a CSV file can be used with a script. For all firewalls in a pool (two in this example), we wish to create an object that represents the main Active Directory server and an object that represents the secondary AD server, taking into account the following conditions:

- The main AD server has to be an object with static IP address resolution,
- The secondary AD server has to be an object with dynamic IP address resolution,
- The name of each object has to indicate whether it is a main or secondary server,
- The comments of each object must indicate the name of the firewall on which it will be created.
- The IP address of each AD server is different for each firewall.

1. Create the script */var/tmp/ad.script*:

```
# Create a new host CONFIG OBJECT HOST NEW name=AD-%type%
comment="%type% AD server for FW %FW_NAME%" ip="%ip_addr%"
resolve=%mode%
CONFIG OBJECT ACTIVATE
```

2. Create the CSV file */var/tmp/ad.csv* for the pool of two firewalls:

```
firewall;type;ip_addr;mode
sns-paris;Main;1.1.1.1;static
sns-paris;Backup;1.1.2.2;dynamic
sns-lyon;Main;4.4.4.4;static
sns-lyon;Backup;4.4.5.5;dynamic
```

3. Enter the following command in the command line interface:

```
smc-sns-cli-script exec /var/tmp/ad.script --csv-file
/var/tmp/ad.csv
```

The following is the expected result for each of the firewalls sns-paris and sns-lyon:

```
# Create a new host
CONFIG OBJECT HOST NEW name=AD-Main comment="Main AD server for FW
sns-paris" ip="1.1.1.1" resolve=static
CONFIG OBJECT ACTIVATE
# Create a new host
CONFIG OBJECT HOST NEW name=AD-Backup comment="Backup AD server for
FW sns-paris" ip="1.1.2.2" resolve=dynamic
CONFIG OBJECT ACTIVATE
```

```
# Create a new host
CONFIG OBJECT HOST NEW name=AD-Main comment="Main AD server for FW
sns-lyon" ip="4.4.4.4" resolve=static
CONFIG OBJECT ACTIVATE
# Create a new host
CONFIG OBJECT HOST NEW name=AD-Backup comment="Backup AD server for
FW sns-lyon" ip="4.4.5.5" resolve=dynamic
CONFIG OBJECT ACTIVATE
```

TIP

In CSV files, fields are often separated by a comma or semi-colon. The `smc-sns-cli-script` command interprets semi-colons (;) as separators by default. The separator may be different depending on the CSV file. In order to change the separator, put the variable FWADMIN_SNS_CLI_CSV_DELIMITER before the command. For example:

```
FWADMIN_SNS_CLI_CSV_DELIMITER=, smc-sns-cli-script exec --csv-
file=/var/tmp/monfichier.csv /var/tmp/monscript.script
```

9.5 Running the SNS CLI script on a high availability cluster

The steps are the same as in both previous sections.

The script is first run on the active node of the cluster. The SMC server then synchronizes both nodes of the cluster.

If the passive node is not connected to the active node at the time of execution, the SMC server will perform a synchronization between both nodes when the passive node connects again to the active node.

9.6 Attaching files to a script and receiving files generated by script

Running certain script commands requires sending or receiving files to or from firewalls. For example:

- Updating firewalls,
- Installing licenses,
- Generating backups of firewall configurations.

Files can be sent or received from the web interface of the SMC server and from the command line interface.

9.6.1 Command arguments to be used in the script

For a command requiring an input file, use the following command arguments to specify the name of the file to be sent:

- `$FROM_DATA_FILE("myFileName.extension")` to attach a file without Unicode processing.
- `$FROM_TEXT_FILE("myFileName.extension")` to attach a file with Unicode processing.

For a command generating an output file, use the following command arguments to specify the name of the file to be received:

- `$SAVE_TO_DATA_FILE("myFileName.extension")` to back up a file without Unicode processing.
- `$SAVE_TO_TEXT_FILE("myFileName.extension")` to back up a file with Unicode processing.

To find out the locations of these files, please refer to the sections below Attaching files to a SNS CLI script and Receiving files generated by a SNS CLI script.

The script will not run if:

- No files have been specified in the argument of a command that requires an input file or generates an output file,
- An input or output file has been specified in the argument of a command that does not require one.

Example

The following command allows generating the backup file of a firewall named *backup-22-09-16.zip* on the SMC server:

```
CONFIG BACKUP list=all $SAVE_TO_DATA_FILE("backup-22-09-2016.zip")
```

TIP
You can use variables in the syntax for sending or receiving files. For example, to create configuration backups for several firewalls, write the following command:

```
CONFIG BACKUP list=all $SAVE_TO_DATA_FILE("backup-%FW_NAME%.na")
```

9.6.2 Attaching files to a script

In both of the following cases, the attached files will be deleted from the SMC server after the script has been successfully executed.

Via the web interface

1. In the web interface of the SMC server, select **Deployment** > **SNS CLI scripts**.
2. In the **Firewall selection** tab, after you have selected a script, select one or several attachments from the sub-menu **Attachments related to scripts**.

Via the command line interface

Copy the attachments at the root of the folder */var/tmp/sns-cli/input* on the SMC server using SSH.

The script execution engine retrieves the files needed at this location in order to forward them to the firewalls.

TIP
You can change the default folder in the environment variable `FWADMIN_SNS_CLI_ATTACHMENTS_DIR` located in the file **/data/config/fwadmin-env.conf.local**. You will then need to restart the server. `nrestart fwadmin-server`.

9.6.3 Receiving files generated by a script

Via the web interface

In the **Execution** tab in the **SNS CLI scripts** menu, retrieve all files and logs generated for each firewall the last time the script was run.

To retrieve files and logs generated in earlier script executions, refer to the following section Via the command line interface.

Receiving files and logs

Click on **Download all generated files** at the bottom of the **Execution** tab to download an archive that includes all generated files and execution logs for all firewalls at the same time. The archive will contain a folder per firewall.

To retrieve files and logs generated by running a script on a single firewall, click on the icon in the column **Generated files**.

Reading execution logs

To simply read execution logs for a given firewall, click on the icon in the column **Generated files**.

Via the command line interface

All files and logs generated for each firewall after running a script are saved by default in the folder */var/tmp/sns-cli/output* on the SMC server. The tree created as such will contain a folder for each script execution.

TIP
You can change the default folder in the environment variable `FWADMIN_SNS_CLI_OUTPUT_DIR`

located in the file */data/config/fwadmin-env.conf.local*. You will then need to restart the server.
`nrestart fwadmin-server`.

Example

When this command is run

```
CONFIG BACKUP list=all $SAVE_TO_DATA_FILE("backup-%FW_NAME%.na")
```

the following tree is obtained:

```
/var/tmp/sns-cli/output/latest -> 00001_20160219-171926
/var/tmp/sns-cli/output/00001_20160219-171926
/var/tmp/sns-cli/output/00001_20160219-171926/sns-2
/var/tmp/sns-cli/output/00001_20160219-171926/sns-1/backup-sns-2.na
/var/tmp/sns-cli/output/00001_20160219-171926/sns-2/output.log
/var/tmp/sns-cli/output/00001_20160219-171926/sns-1
/var/tmp/sns-cli/output/00001_20160219-171926/sns-1/backup-sns-1.na
/var/tmp/sns-cli/output/00001_20160219-171926/sns-1/output.log
```

The *latest* folder always directs to the last execution.

9.7 Scheduling the execution of SNS CLI scripts

Scripts can be scheduled to run at a given date and time using the web interface or command line. For example, you can schedule an update of your SN firewalls. Refer to the section Updating firewalls by using SNS CLI scripts.

9.7.1 Scheduling the execution of scripts from the web interface

1. In the web interface of the SMC server, select **Deployment** > **SNS CLI scripts**.
2. In the **Firewalls selection** tab, select the script to run.
3. In the **Optional: attachments related to the script** menu, select the relevant files to attach to the script. For more information, please refer to the section Attaching files to a script and receiving files generated by script.
4. In the second part of the **Firewalls selection** tab, select the SN firewalls on which the script will be run. For each firewall, in the **View script** column:
   - The icon indicates, where applicable, that the firewall cannot be selected to run the script. The row will be grayed out in this case. Scroll over the icon with your mouse to find out why.
   - The icon makes it possible to view the contents of the script, including variables replaced with values associated with the firewall in question. The icon becomes if there is an error during the analysis of the script (missing attached file or unknown variable). View the contents of the script to find out which row is causing the issue.
5. Click on **Schedule script** at the bottom of the tab.
6. Indicate the date and time to run the script. The time chosen here corresponds to the time on the SMC server.

7. Click on **Apply**.
   - An indicator at the top of the tab serves as a reminder of the script schedule. The only actions that can be performed are viewing the script, downloading the script or canceling the scheduled run.
8. View the results of the script run in the **Execution** tab when it is complete.

Only one script run can be scheduled at a time.

You cannot run another script while a script has been scheduled and is awaiting its run.

IMPORTANT
Executing script automatically adopts the reading/writing privileges on any administration sessions already open on the firewalls in question.

9.7.2 Scheduling the execution of scripts in command line

The `at` shell command makes it possible to schedule the execution of tasks. Among other functions, it allows the execution of the command `smc-sns-cli-script` to be scheduled.

As several tasks can be scheduled, they will be run in sequence.

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. Type the command `at` followed by the desired date and time in the format below:
   `at hh:mm MM/DD/YYYY`
3. Type the command `smc-sns-cli-script` followed by (in this order):
   - one of the subcommands described in the section Running the SNS CLI script in command line,
   - the name of the script,
   - the name of the firewalls concerned or the --all option to designate all firewalls,
   - ```
     [root@smc] - {~} > at 16:00 10/15/2019
     warning: commands will be executed using /bin/sh
     at> smc-sns-cli-script run monitor_qos.script --all
     at> smc-sns-cli-script run monitor_stat.script --all
     ```
4. Type Ctrl + D to confirm.
   ```
   at> < EOT >
   job 15 at Tue Oct 15 16:00:00 2019
   ```
5. After the scheduled date and time of the run, you can check the results in the folder */var/tmp/sns-cli/output/*. This folder contains a set of sub-folders named according to the date on which the scripts were run. To view the results of the execution of a script on a given firewall, look up the file *output.log* in one of these sub-folders.

If you need to attach files to the script, refer to the section Attaching files to a script and receiving files generated by script.

To see the list of scheduled tasks, use the `atq` command.

To delete a scheduled task, use the `atrm` command.

9.8 Updating firewalls by using SNS CLI scripts

SNS CLI scripts can be used to update your pool of SN firewalls.
   ```

You must first download the relevant update files in your secure MyStormshield area (*.maj*).

If you have standalone firewalls and high availability clusters, we recommend that you create a script for each use case (standalone firewalls, active nodes, passive nodes and both nodes at the same time).

We recommend that you back up the configuration of your firewalls before updating them.

Follow the steps below:

1. Create the update script using the commands described in the following examples, replacing 3.5.1 with the desired version (for further information on the variable %FW_UPD_SUFFIX%, refer to the section Using variables):
    - For standalone firewalls:
    ```
    SYSTEM UPDATE UPLOAD $FROM_DATA_FILE("fwupd-3.5.1-%FW_UPD_
    SUFFIX%")
    SYSTEM UPDATE ACTIVATE
    ```
    - For clusters:
        - Passive nodes:
        ```
        SYSTEM UPDATE UPLOAD fwserial=passive $FROM_DATA_FILE
        ("fwupd-3.5.1-%FW_UPD_SUFFIX%")
        SYSTEM UPDATE ACTIVATE fwserial=passive
        ```
        - Active nodes:
        ```
        SYSTEM UPDATE UPLOAD fwserial=active $FROM_DATA_FILE
        ("fwupd-3.5.1-%FW_UPD_SUFFIX%")
        SYSTEM UPDATE ACTIVATE fwserial=active
        ```
        - Both nodes at the same time:
        ```
        SYSTEM UPDATE UPLOAD fwserial=all $FROM_DATA_FILE("fwupd-
        3.5.1-%FW_UPD_SUFFIX%")
        SYSTEM UPDATE ACTIVATE fwserial=all
        ```

        IMPORTANT
        In this use case, both nodes may become unavailable at the same time during the update process.
2. In the web interface of the SMC server, select **Deployment** > **SNS CLI scripts**.
3. In the **Firewalls selection** tab, select the script to run.
4. In the **Optional: attachments related to the script** menu, select the update file(s) corresponding to the models and versions of your firewalls. For example, to update your SN510 and SN6000 firewalls to version 3.5.1, the attachments that need to be provided are *fwupd-3.5.1-SNS-amd64-M.maj* and *fwupd-3.5.1-SNS-amd64-XL.maj*.
5. Next, follow the usual steps for running a script, as shown in the section Running the SNS CLI script from the web interface from step 4 onwards.

    NOTE
    After an update script has been run on a cluster, the SMC server's automatic synchronization of both nodes will always fail as the update would have made one of the nodes unavailable. Details of this error, which does not prevent the update from proceeding properly, are provided in the **Execution** tab.
6. After a few minutes, check in the **Monitoring** > **Firewalls** panel that the version number has indeed changed in the **Version** column.

9.9 Troubleshooting

Refer to this section in order to resolve frequently encountered issues while using SNS CLI scripts.

9.9.1 The script file is too large

- *Situation*: When a script file is selected, an error message indicates that the script is too large.
- *Cause*: The size of the file must not exceed 5 MB by default.
- *Solution*: If necessary, increase the limit by adding the line below to the file `/data/config/fwadmin-env.conf.local`. Set the limit to 10 MB for example: `FWADMIN_SNS_CLI_SCRIPT_MAX_UPLOAD_SIZE=$((10*1024*1024))`

9.9.2 Certain characters are not supported in the script

- *Situation*: Certain accented or special characters do not display correctly in the script. The script could not be run.
- *Cause*: The *.script* file was not encoded in UTF-8.
- *Solution*: Change the encoding of the script to UTF-8.

9.9.3 The script fails to run on certain firewalls

- *Situation*: The **Execution** tab in the **SNS CLI scripts** menu indicates errors.
- *Cause*: The script calls up customized variables and/or attachments which are missing. The encoding of the script is wrong. Other problems may be the cause of the script's failure to run.
- *Solutions*:
  - Look for the cause of the error which appears in the status bar when the script is run for a given firewall.
  - Look up the log file in */var/log/fwadmin-server/server.log* for further detail.
  - Before running the script, you can view it for a given firewall in the **Firewalls selection** tab. Certain errors may be indicated.

9.9.4 The Execute script button remains grayed out

- *Situation*: Firewalls have been selected for the execution of a script but the execution button remains grayed out
- *Cause*: During the execution of a script or deployment of a configuration, you will not be able to run another script execution.
- *Solution*: Wait for the script to finish its run or for the configuration to be fully deployed.

10. Maintaining SN firewalls

The SMC server makes it possible to back up the configuration of SN firewalls and update your pool via SNS CLI scripts.

10.1 Backing up the configuration of firewalls

SMC makes it possible to set up automatic backups of the configuration of firewalls as well as the configuration of the SMC server. You can manually perform full backups of your firewall pool as well at any moment.

10.1.1 Backing up the configuration of the server and firewalls automatically

SMC can automatically and repeatedly back up the configuration of firewalls and the server itself in order to restore the entire pool when necessary.

By default, automatic backup is enabled. It is performed every hour.

Displaying backup list

- Go to the **Maintenance** > **Backup** menu on the left.

The list shows all saved backups. They are kept for seven days. After seven days, only one backup per day is saved. After one month, only one backup per week is saved. After 12 months, backups are deleted.

An icon in the **Status** column indicates whether the configurations of all firewalls have been backed up, and which firewalls present issues. Scroll over icons with the mouse to display a tool tip.

Retrieving a backup

- Click on in the **Actions** column.
  The archive contains a metadata file, the backup of the SMC server's configuration and the backups of each firewall's configuration in *.na* format.

Restoring a backup

To find out how to restore a backup of the SMC server's configuration, refer to the section Saving and restoring the SMC server configuration.

To find out how to restore a backup of a firewall's configuration, refer to the *Stormshield Network User Configuration Manual*.

Showing more details about a backup

- Double-click a line or click on in the **Actions** column.

Disabling automatic backup

- Uncheck **Enable automatic backup**.

10.1.2 Backing up the configuration of firewalls manually

You can also perform a one-off backup of the configuration of some or all of the firewalls in your pool.

1. Go to the **Maintenance** > **Backup** menu on the left.
2. In the **Manual** tab, enter a password if you wish to encrypt backups. The characters #, % and " are prohibited and the password must not exceed 255 characters.
3. Click on **Use the firewalls backup script.**
4. The SNS CLI scripts panel appears. The script to manually back up the firewall configuration is preloaded.
5. Select the firewalls for which you wish to back up the configuration, then run the script.

For more information on scripts, please refer to the section Running the SNS CLI script from the web interface.

This manual backup does not include the configuration of the SMC server. To back up the configuration of the server, refer to the section Saving and restoring the SMC server configuration or enable automatic backups.

10.1.3 Excluding private keys from automatic firewall backups

When the configuration of a firewall is backed up, it contains by default the full identity of the firewall, i.e., its certificates and private keys.

If you want to exclude private keys from automatic backups, to protect confidentiality for example, you can modify the environment variable `FWADMIN_AUTOBACKUP_EXCLUDE_PRIVATE_KEY`:

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. In the file **/data/config/fwadmin-env.conf.local**, change the value of the environment variable:: `FWADMIN_AUTOBACKUP_EXCLUDE_PRIVATE_KEY=true`
3. Restart the server with the command `nrestart fwadmin-server`

On firewalls equipped with initialized TPM chips (Trusted Platform Module), keys are excluded from automatic backups by default. The environment variable does not need to be modified.

For more information, on protecting certificates with TPMs, refer to the section Disabling TPM (Trusted Platform Module) certificate protection during installation on the firewall.

10.2 Updating firewalls

To update your pool of firewalls, the SMC server allows you to install update files on your firewalls in a single operation and run an update script on all firewalls.

To perform this operation, refer to the section Updating firewalls by using SNS CLI scripts.

10.3 Replacing an SN firewall through an RMA

If you need to replace a firewall that the SMC server manages, follow the usual procedure for replacing an appliance through an RMA (Return Material Authorization).

After you have restored the firewall's configuration on the new appliance using the *.na* backup file, the firewall will automatically log back on to the SMC server. There is nothing additional that you need to do; there is no need to generate a new connecting package.

11. Removing SN firewalls from the SMC server

1. To stop managing a firewall from the SMC server and remove it from the list of firewalls in the web interface, scroll over the name of the firewall in **Monitoring** > **Firewalls** and select the red cross.

The firewall will no longer be able to connect to the SMC server.

2. As a second step, connect to the firewall via SSH connection or console port and enter the following command lines:

```
nstop cad
setconf /Firewall/ConfigFiles/Cad/cad Server State 0
rm /Firewall/ConfigFiles/Cad/*.pem
```

The firewall will stop trying to connect to the SMC server.
In the case of a high availability cluster, enter these commands on the active node of the cluster and synchronize both nodes.

12. Managing and maintaining the server SMC

Management and maintenance operations are performed either from the web interface or from the command line interface, or both.

12.1 Defining the server's network interfaces SMC

In your hypervisor, you can define several interfaces on various networks for the SMC server. IPv6 addresses are not supported.

These interfaces can be seen in the **Maintenance** > **SMC Server** > **Parameters** panel in the server's web administration interface and can be modified.

All interfaces except eth0 are disabled by default. You need to enable them in the **Address range** column in this panel and configure them.

The interface eth0 cannot be disabled.

Only one gateway can be defined for all the interfaces. This will be the default gateway, and must be located in the same sub-network as the corresponding interface.

The */etc/network/interfaces* file accessible in command line contains information relating to the interfaces of the SMC server.

With regard to network topologies for which you need to configure static routes in addition to the default gateway, follow the procedure given in the Stormshield Knowledge base.

12.2 Verifying the SMC server version in command line

To see the SMC server version:

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. Enter the command `smc-version`.
3. The following information appears:
   - FWADMIN_VERSION: indicates the version under the form 1.2.3,
   - FWADMIN_BUILD_NUMBER: indicates the date of the build of the server and Stormshield hashes which can be provided to the Stormshield Network Security Support in case of issue.

12.3 Changing the SMC server time zone and date

By default the SMC server time zone is GMT+1 (Central European Time).

12.3.1 Changing the time zone

1. Log on to the SMC server via the console port or in SSH using the “root” account.
2. Enter the command `smc-date-time --timezone "timezone”` to change the time zone. Replace `timezone` with the correct time zone.
   - To see the available time zones, enter the command `ls -l /usr/share/zoneinfo/`.
   - To find the city in the zone of your choice (Asia for example), enter the command `ls /usr/share/zoneinfo/Asia`.

3. Restart the server with the command `reboot`. This step is required in order for the new time zone to be applied to all services.
4. Enter the command `smc-date-time` to check that the change has been properly applied.

12.3.2 Changing the date manually

1. Enter the command `smc-date-time --date-time "YYYY-MM-DD hh:mm:ss"` to change the date.
2. Enter the command `smc-date-time` to check that the change has been properly applied.

12.3.3 Changing the date via NTP

To enable NTP on the SMC server:

1. Enter the command `smc-date-time --ntp-servers ntp1.org,ntp2.com,IPaddress` separating each NTP server with a comma if there are several. NTP servers may also be identified by their IP addresses or DNS names.
2. Enter the command `date` to check the modification has been properly applied.

To disable NTP, you need to go back to manual date mode.

12.3.4 Displaying a comprehensive summary of the SMC server's date/time

- Enter the command `smc-date-time` to display all of the server's date/time parameters:

```
smc-date-time
TIMEZONE=Asia/Dubai
NTPSERVERS=none
LOCALDATE=2016-05-18 09:05:19
```

12.4 Managing administrators

There are three ways to manage the authentication of administrators on the SMC server:

- Create local accounts on the server in the web interface,
- Configure a connection to a LDAP server from the SMC server in the command line interface,
- Configure a connection to a RADIUS server from the SMC server in the command line interface.

12.4.1 Managing administrators in the web interface

Go to **Maintenance** > **SMC Server** > **Administrators** in the web administration interface to manage administrators. The panel displayed depends on whether you are connected to the server as the super administrator ("admin" user) or as another user.

There are three administrator profiles:

Profile	Rights over administrators	Rights over configuration
Super administrator	Add/Remove/Edit	Add/Remove/Edit/Deploy
Administrator with read/write access	Modify personal password	Add/Remove/Edit/Deploy
Administrator with read-only access	Modify personal password	Read only.

Several administrators can be connected to the web interface at the same time with read/write access. As such, changes made by any administrator will instantly appear on the screens of the other administrators, including items imported via CSV file. Refer to audit logs for full details on what changes were made.

When an administrator deploys a configuration on firewalls, the other administrators see that a deployment is in progress and who launched it.

Managing administrators as super administrator

The super administrator holds all the rights and decides which administrators are granted access:

- to the SMC web interface in read/write or read-only mode,
- to the firewall web interface in read/write or read-only mode.

Go to the **Administrators** panel:

- To add an administrator, click **Add an administrator**.
- To edit an administrator profile, double click the administrator line or move the mouse over the administrator name and select the pen icon .
- To remove an administrator, move the mouse over the administrator name and click on the red cross .

The admin user cannot be removed.

Only the super administrator is allowed to update the SMC server from the web administration interface.

Setting a password policy

Only the super administrator can set the password policy by choosing:

- The minimum number of characters required: the password can contain between one and 128 characters. A minimum of eight characters is required by default.
- The mandatory character types: alphanumeric, alphabetic and special or none. No character types are mandatory by default.

When a new SMC server is deployed, the password of the super administrator in the server initialization wizard must also contain at least eight characters.

To set a password policy:

1. Go to **Maintenance** > **SMC Server** > **Administrators**, and click on **Edit password policy**,
2. Select the minimum number of characters required,
3. Select the mandatory character types.

The password policy applies to all administrators.

Passwords that were set before this policy was applied will remain valid but we recommend that you change them to comply with the set policy.

The 128-character limit also applies to administrators' logins and names.

12.4.2 Allowing administrators to connect via an LDAP or Radius server

The SMC server can be connected to an LDAP and/or Radius server to authorize the company's users to manage a pool of firewalls.

This type of authentication is designed to operate with LDAP servers such as Active Directory on Microsoft Windows Server 2012 and 2016, and Radius servers on Microsoft Windows Server 2012 R2 and 2016.

Radius authentication only makes it possible to identify the users who have access to the SMC server, but does not allow groups and read/write access to be managed. It must be paired with LDAP authentication so that user privileges and groups can be managed.

When a super administrator tries to connect, the SMC server looks for the ID and password in its local user database first, and then on the Radius server if it does not find this information, then on the LDAP server.

When an ordinary administrator tries to connect, the SMC server looks for the ID and password on the Radius server first, and then on the LDAP server if it does not find this information, then in its local user database.

Authentication via LDAP or Radius server is configured in the SMC server's command line interface with two files:

- An *auth-server.ini* configuration file that enables the LDAP or Radius server connection settings to be defined,
- A *rights.csv* configuration file that enables the definition of groups and users authorized to connect to the SMC server as well as their access privileges on SMC and SNS.

To authorize administrators to connect to the SMC server via an LDAP or Radius server, follow the three steps below:

1. Configure the connection to the LDAP or Radius server,
2. Test the connection and display the list of users on the LDAP or Radius server, and groups on the LDAP server,
3. Authorize users and define their access privileges.

Configuring the connection to the LDAP or Radius server

To configure the connection to the LDAP or Radius server, modify the *auth-server.ini* file located in the SMC server's directory `/data/config/users`.

1. Log in to the SMC server via the console port or in SSH using the "root" account,
2. Go to the `/data/config/users/` directory,
3. As a precaution, save the *auth-server.ini* file before modifying it,

4. Modify the *auth-server.ini* file by filling in the following parameters provided by the LDAP or Radius server administrator:

Field	Description
section [radius-server]	
host	IP address or FQDN of the Radius server. If this field is empty, Radius server authentication is disabled. If the server's FQDN is being used, the DNS service must be configured beforehand.
port	Port number to access the Radius server: 1812 by default
pre-shared key	Secret key shared to enable authentication on the server
section [ldap-server]	
type	Active Directory server
host	IP address or FQDN of the LDAP server. If this field is empty, LDAP server authentication is disabled.
port	Port number to access the LDAP server: if SSL is enabled, 636 by default; otherwise, 389.
baseDN	baseDN allowing access to the LDAP server and using the following format: dc=sub,dc=domain,dc=com The baseDN can also refer to a more specific place in the Active Directory, for example an organizational unit: ou=unit,dc=domain,dc=com.
login	ID to connect to the LDAP server
password	Password to connect to the LDAP server
ssl	If the value is `true`, the connection to the LDAP server is secure via SSL/TLS protocols. When SSL is enabled, the default port changes. If SSL is enabled, the SMC server does not verify the certification authority that signed the LDAP server's certificate by default. For more information, refer to the section Verifying the certificate of the certification authority when the SSL protocol is enabled.

Sample *auth-server.ini* file:

```
[radius-server]
host=
port=1812
pre-shared-key=
[ldap-server]
; Possible values : activeDirectory/standard
type=activeDirectory
host=
baseDn="dc=mydomain,dc=com"
login=administrator
password="secret"
ssl=false
;The CA certificate of the Server CA certificate will not be checked until you uncomment the following line,
;and copy your CA certificate into /data/config/users/ldap-ca.pem
;sslCaCertificate=true
```

Listing users and groups found on the LDAP or Radius server

The `smc-auth-check` command sends a request to the LDAP or Radius server and:

- verifies that the syntax of the *auth-server.ini* file is correct,
- verifies that the network configuration of the SMC server allows it to contact the LDAP or Radius server,
- verifies that the ID and password defined in the *auth-server.ini* file are correct,
- and lists the users and groups on the server according to the configuration specified in the *auth-server.ini* file.

To see the list of users and groups:

1. Log in to the SMC server via the console port or in SSH using the "root" account,
2. Enter the command `smc-auth-check ldap` or `smc-auth-check radius`.

The `smc-auth-check` command lists all users and groups found on the LDAP or Radius server with the baseDn configuration provided in the *auth-server.ini* file. It is however possible to refine the search using one of the following options:

Option	Description
--list users	Restricts the search to user names only
--list groups	Restricts the search to group names only (LDAP)
--no-lookup	Will not display all users. This option makes it possible to test connectivity with the LDAP or Radius server according to the configuration provided in the *auth-server.ini* file.
--filter <text>	Filters results according to a specified text. This option makes it possible to list all users and groups that contain the specified text.

When configuring the *rights.csv* file in the next step, use the syntax of the "Distinguished Names" (dn) that are displayed in the lists of users and groups via this command.

Examples of requests:

```
**********************************
**                              **
** LDAP Server configuration    **
**                              **
**********************************


ldap://1.1.1.1:389

Host              1.1.1.1
Port              389
SSL               false
CA Certificate    ignored


Credentials

Login       administrator
Password    secret


Search parameters

Windows AD    true
BaseDN        dc=mydomain,dc=com
```

```
**********************************
**                              **
** RADIUS Server configuration  **
**                              **
**********************************


Connection parameters

Host              1.1.1.1
Port              1812
Pre-shared-key    secret
```

Authorizing users or groups

Create the *rights.csv* file. This file allows you to define the list of users and groups in the LDAP directory that are authorized to connect to the SMC server.

If you use a Radius server, you must also configure an LDAP server to obtain the same authorizations granted to users and groups in this *rights.csv* file. In this case, when a user logs in, the first authentication via Radius will identify the user and the second will determine whether the user belongs to a group, and identifies the privileges granted to this user.

You can grant access privileges in read/write or read-only mode to each user and group on the SMC server and on the SN firewalls.

To create this file:

1. Log in to the SMC server via the console port or in SSH using the "root" account,
2. Retrieve the sample file in `/opt/stormshield/examples/csv//example--rights.csv`,
3. Save it in `/data/config/users`,
4. Modify the file by filling in the following parameters:

Field	Authorized values	Description
type	`user` or `group` for LDAP `user` for Radius	Determine whether the Distinguished Name (DN) is a user or a group.
dn	example for LDAP: `CN=intern,OU=some-organization-unit,DC=mycompany,DC=com` For Radius, enter a user name.	For LDAP: Distinguished Name of the user or group as displayed using the `smc-auth-check` command (as explained in the previous section).
smcRights	`ro` or `rw`	Read-only (ro) or read/write (rw) access to the SMC server.
snsRights	`ro` or `rw`	Read-only (ro) or read/write (rw) access to SN firewalls when users access them from the SMC server. For more information on direct access, refer to the section Accessing the web administration interface of firewalls.

If a given user is part of an authorized LDAP group but you do not want to grant the same privileges to the user and the group, place the user line before the group line. The first `user` or `group` line that matches the authenticated user will be applied.

NOTE
User IDs (derived from the LDAP attribute sAMAccountName) must not contain spaces in order to be able to connect to the SMC server.

Sample *rights.csv* file:

```
type;dn;smcRights;snsRights
user;"CN=some-admin,OU=some-organization-unit,DC=mycompany,DC=com";rw;ro user;"CN=intern,OU=some-organization-unit,DC=mycompany,DC=com";ro;ro group;"CN=all-admins,OU=some-organization-unit,DC=mycompany,DC=com";rw;rw
```

Verifying the certificate of the certification authority when the SSL protocol is enabled

If you enable the SSL protocol in the *auth-server.ini* configuration file (`ssl=true`) in order to secure the connection between the SMC server and the LDAP server, SMC does not verify the certificate of the certification authority that signed the LDAP server's certificate by default. To have SMC verify the certificate:

1. Connect to the SMC server via the console port or SSH connection with the "root" account,
2. Copy the certificate of the certification authority provided by the LDAP server administrator named *ldap-ca.pem* in the `/data/config/users` directory,
3. Add the `sslCaCertificate = true` key in the *auth-server.ini* file,

4. Restart the SMC server using the `nrestart fwadmin-server` command to apply the configuration.

If a problem occurs with the certification authority, the `smc-auth-check` command will show the related error.

12.5 Viewing SMC server logs

The SMC server provides two types of logs:

- *server.log*: lists all actions saved on the SMC server. This file may be read from the server's web interface and from the command line interface using the `nlogs` command.
- *audit.log*: lists all actions performed by an administrator on the server. This file may be read from the server's web interface and from the command line interface using the `alogs` command.

To view server logs from the web interface:

1. Show the **Maintenance** > **Server logs** menu or show and hide the logs at any time by clicking on the black arrow at the bottom of the interface .
2. Move the cursor to select the minimum number of logs to display, from the least to the most critical: information, warning or error.
   A maximum of 1000 lines can be displayed. When the limit is reached, the oldest logs are replaced with the most recent ones in the interface.
3. To view the contents of the entire log file, log on to the SMC server via the console port or in SSH with the "root" user account and enter the command `nlogs`.

To view audit logs from the web interface:

1. Show the **Maintenance** > **Audit logs** menu or show and hide the logs at any time by clicking on the black arrow at the bottom of the interface .
2. You can show the **Details** column, which is hidden by default.

NOTE
The SMC server keeps logs of the past 12 weeks up to 100 MB per file. To provide legally required archiving for a year, send logs to a remote Syslog server.

To find out how to send logs to a remote Syslog server, refer to the section Sending SMC logs to a remote server in Syslog format.

12.6 Sending SMC logs to a remote server in Syslog format

SMC supports the Syslog protocol in order to collect all logs from the system and from SMC and send them to a remote Syslog server, with or without encryption.

To use the Syslog service on SMC:

1. Log in to the SMC server via the console port or in SSH using the “root” account.
2. Enter the command `smc-syslog-ng`. The service's current configuration will appear.

12.6.1 Sending logs to a remote server without encryption

1. Type the command `smc-syslog-ng --wizard` to select an operating mode.
2. Select the option **Store logs locally and send logs to a syslog-ng server through TCP**.

3. Enter the IP address or FQDN of the remote server as well as the port number.

12.6.2 Sending logs to a remote server with encryption

To encrypt communications when forwarding logs to the remote server, you will need three files issued by your PKI (Public Key Infrastructure):

- The client certificate in PEM format which allows the remote server to identify SMC,
- The client's private key in PEM format which would allow SMC to encrypt data so that only the remote server can decrypt it,
- The certificate of the certification authority in PEM format which would allow SMC to trust the remote server.

1. Before configuring the Syslog service, copy these three files on SMC, in `/tmp` for example.
2. Type the command `smc-syslog-ng --wizard` to select an operating mode.
3. Select the option **Store logs locally and send logs to a syslog-ng server through TCP with TLS**.
4. Enter the IP address or FQDN of the remote server as well as the port number.
5. Indicate the location of the certificates. The Syslog wizard will copy them into the folder `/data/certs/syslog-ng/`.

12.6.3 Disabling the sending of logs to a remote server

1. Type the command `smc-syslog-ng --wizard` to select an operating mode.
2. Select the option **Store logs locally in /var/log/messages (default)**.

12.6.4 Troubleshooting

The remote Syslog server is unreachable

- *Situation*: You have specified the name of the remote Syslog server using its FQDN but the server remains unreachable.
- *Cause*: The DNS service was probably not configured properly or is unable to resolve the FQDN.
- *Solution*: Check the resolution of the DNS server by typing the command `nslookup server-syslog.domain.com` in the SMC command line interface.

When logs are forwarded with encryption, the remote server does not receive SMC logs

- *Situation*: You have configured logs to be sent to a remote Syslog server with encryption. You have provided the certificates required, but the Syslog server did not accept the encrypted communication.
- *Cause*: The remote Syslog server probably did not accept the certificates as they may have expired or been revoked.
- *Solution*: Check the error message that the remote Syslog server returned by typing the following commands in the SMC command line interface:

```
MY_SERVER_ADDR=xxx.xxx.xxx.xxx
MY_SERVER_PORT=xxxx
openssl s_client -connect ${MY_SERVER_ADDR}:${MY_SERVER_PORT} -cert
/data/certs/syslog-ng/xxxx.pem -key /data/certs/syslog-ng/xxxx.pem -CAfile
/data/certs/syslog-ng/xxxx.pem
```

12.7 Saving and restoring the SMC server configuration

Saving and restoring the SMC server configuration is possible from the server web interface or from the command line interface.

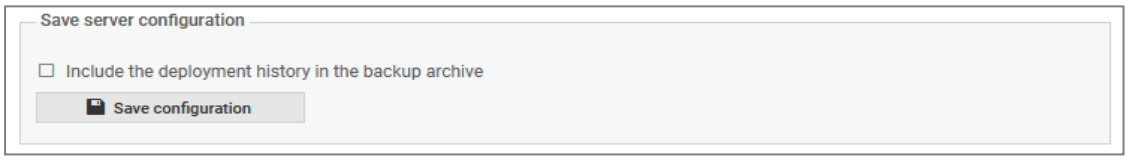
TIP
The following restriction applies to restore a server configuration: the SMC server version must be the same as the version of the server from which the backup file was generated.

Server logs are not contained in the backup file.

You can also define automatic backups of firewall configurations as well as the configuration of the SMC server. For more information, see the section Backing up the configuration of firewalls.

12.7.1 Saving the server configuration from the web interface

In the **Maintenance** > **SMC Server** > **Maintenance** menu, click on **Save configuration** in the **Save server configuration** pane.



The configuration backup file can be restored from:

- The SMC server web interface,
- The command line interface,
- The SMC server initialization wizard.

For more information, refer to sections Restoring the server configuration from the web interface, Restoring server configuration from the command line interface and Restoring server configuration from the initialization wizard.

12.7.2 Saving the server configuration from the command line interface

1. To save a server configuration from the command line interface, connect to the SMC server via the console port or SSH connection with the "root" user.
2. Enter the command
   `smc-config-backup`
   The name of the archive name is displayed.
3. To save the configuration without the deployment history, enter the command
   `smc-config-backup --no-history`

The configuration backup file can be restored from:

- The SMC server web interface,
- The command line interface,
- The SMC server initialization wizard.

For more information, refer to sections Restoring the server configuration from the web interface, Restoring server configuration from the command line interface and Restoring server configuration from the initialization wizard.

12.7.3 Restoring the server configuration from the web interface

In **Maintenance** > **SMC Server** > **Maintenance**, select a backup file to restore in the **Restore server configuration** pane.

To know how to create a server backup, refer to sections Saving the server configuration from the web interface and Saving the server configuration from the command line interface.

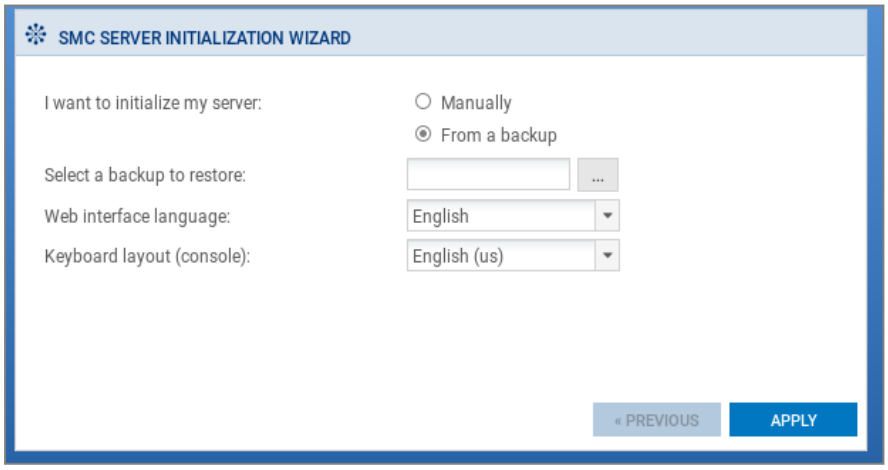
12.7.4 Restoring server configuration from the command line interface

1. To restore a server configuration from the command line interface, copy the backup file in */var/tmp* on the SMC server using SSH protocol.
2. Connect to the SMC server via the console port or SSH connection with the "root" user.
3. Enter the command `smc-config-restore --backup-file /path/to/backup`. Replace `backup-file /path/to/backup` by the name and path.
4. Reboot.

To know how to create a server backup, refer to sections Saving the server configuration from the web interface and Saving the server configuration from the command line interface.

12.7.5 Restoring server configuration from the initialization wizard

When initializing a new SMC server after the deployment of a new virtual machine, select a backup to restore from the first step of the server initialization wizard.



To know how to create a server backup, refer to sections Saving the server configuration from the web interface and Saving the server configuration from the command line interface.

The integrity of the backup file is verified before being restored and then logging in again is required.

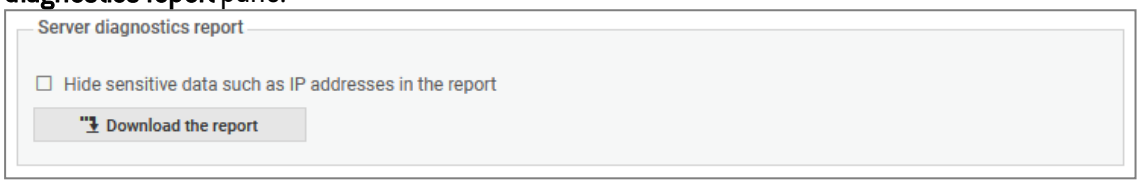
12.8 Generating a server diagnostics report

You can download a diagnostics report on the status of your SMC server's performance.

This report may provide useful information if issues arise on the server.

12.8.1 Downloading the report from the web interface

1. In **Maintenance** > **SMC Server** > **Maintenance**, click **Download the report** in the **Server diagnostics report** pane.



The report is presented as a *tar.gz* archive with its name containing the date and time of creation.

2. Double-click on the *index.html* file to open the report in HTML format.

12.8.2 Downloading the report in command line

1. Log on to the SMC server via the console port or in SSH using the "root" account.
2. Enter the command `smc-diag` or `smc-diag --help` in order to obtain details on the possible options.
   The report is presented as a *tar.gz* archive with its name containing the date and time of creation. The report is generated by default in the */tmp* folder.
3. Double-click on the *index.html* file to open the report in HTML format.

The --confidential option makes it possible to hide IP and MAC addresses.

12.9 Updating the SMC server

The SMC Version release notes contain highly important information. Please refer to them before updating the SMC server.

An update archive (*.upd*) is required to update the SMC server. Archiving involves the update of the web interface and of the operating system.

Before applying an update, we strongly recommend taking a snapshot of your virtual machine.

During the update process, firewalls continue to run. Firewalls do not need to be updated.

On every update the SMC configuration is migrated from the configuration file to the database. The unified configuration file is deleted. This file will be automatically updated on the older system before the migration process begins.

12.9.1 Updating the SMC server from the web interface

You need to be a super administrator in order to update the SMC server from the web interface.

1. Download the update archive on your workstation from your MyStormshield personal area.
2. In **Maintenance** > **SMC Server** > **Maintenance**, select the update file in the **Update SMC** pane.

3. Click on **Update SMC**.
4. When the update is completed, log back in to the SMC server.

During the update, the SMC server will not be available, so administrators will not be able to log in.

12.9.2 Updating the SMC server in command line

1. Download the update archive on your workstation from your MyStormshield personal area.
2. Copy the archive in */var/tmp* on the SMC server using SSH protocol.
3. Connect to the SMC server via the console port or SSH connection with the "root" user.
4. Enter the command `smc-update -u /var/tmp/archivename`. Replace `archivename` with the name of your archive.
   For versions of SMC lower than 2.6, the command to enter is `fwadmin-update -u /var/tmp/archivename`.
5. Wait for the update to end. During the process, the server remains available within the current version.
6. Enter the command `reboot`. The updated system restarts.

12.10 Resetting "root" and administrator passwords

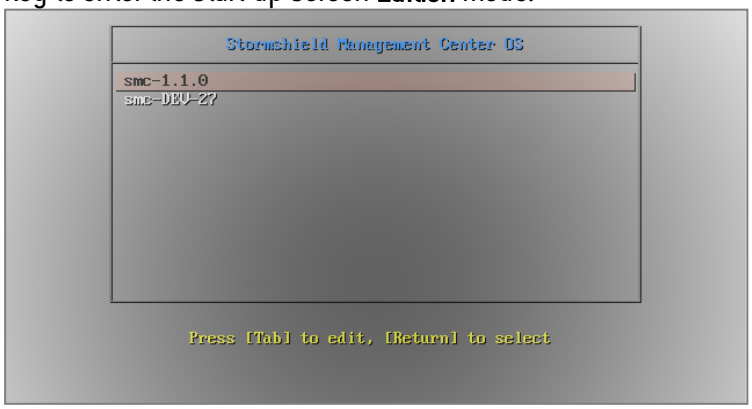
If you forgot the "root" administrator password used to connect to the SMC server via the console port or in SSH, or the administrator password for the server's web interface, follow this procedure.

12.10.1 Resetting the "root" administrator password

IMPORTANT
QWERTY keyboard layout is required to perform these actions.

Changing the server startup mode

1. From the virtual environment, restart the SMC server.
2. When the server restarts and the screen to select the server version displays, press the **TAB** key to enter the start-up screen **Edition** mode.



3. The command line to edit server startup displays. At the end of the line add: `rw init=/bin/bash`

4. Press **Enter** to confirm and start the server.

Changing the user password

1. The server starts. Enter the command `passwd` directly.
2. Enter and confirm the new password (QWERTY keyboard layout).
3. Enter the command `shutdown -nr now` to restart the server.

12.10.2 Resetting the administrator password

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. Enter the following commands:
   - `smc-ui-password` to change the main "admin" administrator password,
   - `smc-ui-password --username myOtherUser` to change the password of another administrator.

12.11 Disabling automatic synchronization of high availability clusters

The SMC server regularly synchronizes both nodes in the high availability clusters of firewalls that it manages.

If necessary, you can disable automatic synchronization:

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. Edit the file **/data/config/fwadmin-env.conf.local** by adding the following line at the end: `FWADMIN_HASYNC_ON_DESYNCHRO=false`
3. Restart the server with the command `nrestart fwadmin-server`

12.12 Monitoring SMC with SNMP

SNMP (Simple Network Management Protocol) is a communication protocol that allows network administrators to monitor devices and diagnose network and hardware issues remotely.

SMC offers the SNMP service via the command `smc-snmp`.

This service is not enabled by default on the SMC server. If you do enable it, you do not need to enable it again after restarting the server, as this setting will be remembered.

The SMC server uses SNMP version 2c by default. You may however choose another version (version 1 or v3 USM) in the configuration file located in */etc/snmp/snmpd.conf*.

12.12.1 Using the SNMP service

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. Enter one of the following commands:

Action	Command
Enable the service	`nstart snmpd ; update-rc.d -f snmpd remove ; update-rc.d snmpd defaults 98`
View the status of the service	`/etc/init.d/snmpd status`
Restart the service	`nrestart snmpd`
Disable the service	`nstop snmpd ; update-rc.d -f snmpd remove`

12.12.2 Using MIBs

SMC supports the following MIBs to monitor SMC:

Category	RFC	MIB
system	RFC 1213	.1.3.6.1.2.1.1
ifaces	RFC 1213 RFC 2863	.1.3.6.1.2.1.2 .1.3.6.1.2.1.31
ips	RFC 1213	.1.3.6.1.2.1.4
tcp	RFC 1213	.1.3.6.1.2.1.6
udp	RFC 1213	.1.3.6.1.2.1.7
snmp	RFC 1213	.1.3.6.1.2.1.11
mem	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.4
disk	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.9
load	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.10
cpu	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11
sysstats	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11
perf	RFC 1514	.1.3.6.1.2.1.25.4 .1.3.6.1.2.1.25.5

12.13 Customizing the certificate of the SMC server web interface

12.13.1 Customizing the certificate

The certificate that the SMC server web administration interface presents can be customized in two ways:

1. Connect to the SMC server via the console port or SSH connection with the “root” account.
2. Replace the files *server.crt* and *server.key* located in the folder `/etc/certs/uiserver` with your own certificates and private key
3. Restart the server with the command `nrestart fwadmin-server`

- or -

1. Connect to the SMC server via the console port or SSH connection with the “root” account.
2. Overwrite the environment variable `FWADMIN_UI_SERVER_CERT_PATH` in the file **/data/config/fwadmin-env.conf.local** with the path of the folder that contains your own certificate and private key.
3. Restart the server with the command `nrestart fwadmin-server`

12.13.2 Reinitializing the certificate

To revert to factory settings, use the command `smc-gen-ui-cert`. This command makes it possible to generate the SSL certificate presented to the web browser one more time. This certificate is self-signed.

12.14 Resetting the internal certification authority of the SMC server

The internal certification authority of the SMC server issues and manages certificates attached to connecting packages. These certificates make it possible to connect, authenticate and identify SN firewalls that connect to the server.

When a new connecting package is generated for a firewall that the SMC server already knows, the certification authority will revoke certificates that were attached to earlier connecting packages once the firewall with the new package connects. Likewise, when a firewall is deleted from the SMC server, all certificates attached to the various connecting packages generated for this firewall will be revoked.

This internal certification authority can be reset whenever necessary.

EXAMPLE
If you want to switch from a pre-production environment to a production environment, you may need to reset the certification authority due to the different security constraints in both environments.

To reset the internal certification authority:

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. Enter the command `smc-reset-ca`.
3. After the script is run, SN firewalls that were connected to the SMC server will be disconnected. Generate new connecting packages for each firewall and install them.

12.15 Adding a disclaimer to the login page

A warning message for administrators can be added to the login page of the SMC server's web administration interface. You can therefore warn them of particular restrictions or precautions they might need to know about when using the SMC server before they log on.

The message will then appear in the **Disclaimer** section.

To add a disclaimer file:

1. Create a text file named *login_disclaimer* containing the desired message. For a better layout, the text can be in HTML without using Javascript. UTF-8 encoding is supported.
2. Connect to the SMC server via the console port or SSH connection with the "root" user.
3. Add the *login_disclaimer* file (without any extension) to the folder *data/config*.

This file will be kept in the server's configuration backup.

Appendix A. Details of smc-xxx commands

This section sets out the list of commands specific to SMC that can be used in the command line interface to manage the server. To find out how to log on to the command line interface, refer to the section Connecting to the command line interface.

There are other smc-xxx commands that were not mentioned in this list as they are solely intended for the internal operations of the server.

The set of smc-xxx commands replaces the fwadmin-xxx commands used in 2.5 and lower versions. These commands will continue to be available and operational but will be removed in future versions.

Command	Action
`smc-config-backup`	Saves the configuration of the SMC server. See section Saving the server configuration from the command line interface.
`smc-config-restore`	Restores the configuration of the SMC server. See section Restoring server configuration from the command line interface.
`smc-date-time`	Displays and configures the system's date, time and time zone. See section Changing the SMC server time zone and date.
`smc-deploy`	Deploys the configuration on the SN firewalls. See section Deploying a configuration on firewalls.
`smc-diag`	Downloads a SMC server diagnostics report. See sectionGenerating a server diagnostics report
`smc-import-firewalls`	Creates firewalls in SMC and their connecting package. See section Importing SN firewalls from a CSV file.
`smc-gen-ui-cert`	Reset the certificate presented by the SMC server's web administration interface. See section Customizing the certificate of the SMC server web interface.
`smc-import-crl`	Imports a Certificate Revocation List (CRL). The CRL is automatically linked to the certification authority which signed it.
`smc-import-objects`	Imports network objects originating from a firewall export in CSV format. See section Importing objects.
`smc-import-rules`	Imports filter and NAT rules, and the objects linked to these rules, from the export of a SN firewall rules in the CSV format. See section Importing rules from connected firewalls .
`smc-install-certificate`	Installs a P12 certificate on a firewall. See section Importing or declaring a certificate for a firewall.
`smc-keyboard`	Changes the language of the keyboard in the command line interface.
`smc-auth-check`	Tests the connection to the LDAP server when it is used for the authentication on the SMC server, and displays the list of users and groups. See section Allowing administrators to connect via an LDAP or Radius server.
`smc-logs`	Displays logs of all actions saved on the SMC server. Equivalent to the `nlogs` command.

`smc-reset-ca`	Resets the internal certification authority of the SMC server. See section Resetting the internal certification authority of the SMC server.
`smc-sns-cli-script`	Runs SNS CLI commands on a pool of firewalls. See section Running SNS CLI commands on a pool of firewalls.
`smc-syslog-ng`	Configures the logging service in Syslog format. See section Sending SMC logs to a remote server in Syslog format.
`smc-ui-password`	Modifies the password of the user on the SMC server's web interface. See section Resetting the administrator password.
`smc-update`	Updating the SMC server See section Updating the SMC server.
`smc-version`	Displays the version of the SMC server. See section Verifying the SMC server version in command line.

Appendix B. Compatibility of SMC/SN firewalls

The SMC server manages SN firewalls from version 2.5.

This table lists the lowest versions of SN firewalls required in order to be compatible with the following SMC features:

Feature/Object	Version of SMC	Lowest version of SN firewall required
SNS CLI Scripts	1.1	2.5
Filter/translation rules	2.0	3.0
Policy-based VPN topologies	2.0	3.0
Router and time objects	2.1.0	3.1
Editing the firewalls output interface	2.2.0	3.3
Multiple addresses to contact SMC specified in the connecting package	2.2.1	3.3
SMC as CRL distribution point	2.2.1	3.3
Health indicators	2.5	3.6
"Responder-only" mode in star VPN topologies	2.5	3.6
AES GCM 16 encryption algorithm	2.5	3.6
Importing filter and NAT rule from the web interface	2.5	3.3
Closure of SAs (VPN Peer Inactivity)	2.6.1	3.7.2
CRLRequired parameter	2.6.1	3.8
Declaring an SCEP server associated with a certification authority / automatic renewal of SCEP certificates	2.6.1	3.9
Multiple outgoing interfaces in the connecting package	2.6.1	3.9
Securing certificates via TPM (Trusted Platform Module)	2.6.1	3.10
DSCP parameter in VPN topologies	2.6.1	3.10
Declaring an EST server associated with a certification authority/automatic renewal of EST certificates	2.7	3.10 and 4.1
Excluding private keys from automatic firewall backups	2.7	3.10 and 4.1
Route-based VPN topologies	2.8	3.3
Managing network interfaces (in read-only mode)	3.0	3.7

NOTE
To be able to monitor the status of VPN topologies containing firewalls of version 4.2 or higher, you need to use an SMC server of version 2.8.1 or higher.

13. Further reading

Additional information and answers to questions you may have are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu

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

Copyright © Stormshield 2021. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.