



STORMSHIELD



GUIDE

STORMSHIELD MANAGEMENT CENTER

ADMINISTRATION GUIDE

Version 2.5.1

Date: May 2, 2019

Reference: [sns-en-SMC-administration_guide-v2.5.1](#)



Table of contents

1. Getting started with the SMC server	6
1.1 Connecting to the SMC server's web interface	6
1.2 Connecting to the command line interface	6
1.3 Installing the SMC license	6
1.3.1 Troubleshooting	6
2. Warning before connecting SN firewalls to the SMC server	8
3. Connecting SN firewalls to the SMC server	9
3.1 Connecting a firewall with a factory configuration to the server	9
3.1.1 Declaring the firewall in the SMC server web interface	9
3.1.2 Building the firewall connecting package	9
3.1.3 Installing the connecting package on the firewall from a USB drive	10
3.2 Connecting a firewall already in production to the server	11
3.2.1 Declaring the firewall in the SMC server web interface	11
3.2.2 Building the firewall connecting package	12
3.2.3 Installing the connecting package on the firewall	13
3.3 Connecting a high availability cluster to the server	13
3.3.1 Declaring the cluster in the SMC server web interface	13
3.3.2 Building the cluster connecting package	13
3.3.3 Installing the connecting package on the active node of the cluster	14
3.4 Troubleshooting with the server's logs	15
3.4.1 Generating a firewall's connecting package	15
3.4.2 Installing the connecting package on the firewall	15
3.5 Importing SN firewalls from a CSV file	15
3.5.1 Creating the CSV file	15
3.5.2 Importing firewalls	16
3.6 Editing firewalls' outgoing interface to communicate with SMC	17
4. Supervising SN firewalls	18
4.1 Monitoring and organizing firewalls	18
4.1.1 Getting information about firewalls	18
4.1.2 Organizing firewalls by folders	19
4.1.3 Checking usage of a firewall in the configuration	20
4.2 Accessing the logs and activity reports of firewalls	20
5. Configuring SN firewalls	21
5.1 Editing firewalls	21
5.2 Managing objects	21
5.2.1 Deploying objects on firewalls	22
5.2.2 Creating variable objects	22
5.2.3 Checking usage of an object in the configuration	23
5.2.4 Importing objects from a CSV file	23
5.3 Deploying a configuration on firewalls	24
5.3.1 Deploying a configuration on a firewall from the web interface	25
5.3.2 Deploying a configuration on a high availability cluster	26
5.3.3 Deploying a configuration on a firewall in command line	26
5.3.4 Troubleshooting with the server's logs	26
5.3.5 SMC side	26
5.3.6 Firewall side	26
5.4 Loading and deploying a former configuration	26



5.5 Generating a configuration comparison	27
5.6 Accessing the web administration interface of firewalls	27
5.7 Using the Emergency mode	28
5.8 Converting a firewall connected to the SMC server into a high availability cluster	28
5.9 Importing or declaring a certificate for a firewall	28
5.9.1 Importing a certificate from the server's web interface	28
5.9.2 Importing a certificate from the command line interface	29
5.9.3 Importing a certificate on a high availability cluster	29
5.9.4 Declaring a certificate used by a firewall	30
5.9.5 Troubleshooting	30
6. Creating and monitoring VPN tunnels	31
6.1 Configuring a mesh topology	31
6.1.1 Importing or declaring certificates for SN firewalls	32
6.1.2 Declaring certificate authorities	32
6.1.3 Setting the CRL distribution points	32
6.1.4 Creating objects included in the topology	33
6.1.5 Creating the VPN topology	33
6.2 Configuring a star topology	34
6.2.1 Creating objects included in the topology	35
6.2.2 Creating the VPN topology	35
6.3 Managing certificate authorities	36
6.3.1 Adding a certificate authority or chain of trust	37
6.3.2 Updating a certificate authority or chain of trust	37
6.3.3 Deleting a certificate authority or chain of trust	37
6.4 Defining the contact IP address of firewalls for VPN topologies	38
6.4.1 Defining a firewall's default contact address	38
6.4.2 Defining a firewall's contact address in a specific VPN topology	38
6.5 Selecting the output interface of firewalls for VPN topologies	38
6.5.1 Creating the Host Object that corresponds to the interface	38
6.5.2 Selecting a firewall's output interface on SMC	38
6.5.3 Configuring a static route on the firewall	39
6.6 Editing and deleting a VPN topology	39
6.7 Monitoring the status of VPN tunnels	40
7. Creating filter and NAT rules	41
7.1 Understanding the order in which rules are read	41
7.2 Use case examples	42
7.2.1 Managing an environment without rule sharing	42
7.2.2 Managing an environment with shared and specific rules	42
7.2.3 Managing a multi-site environment with shared and specific rules and delegated filtering	42
7.3 Creating filter and NAT rules	44
7.4 Identifying the rules	44
7.5 Changing the order in which rules are executed	45
7.6 Removing rules	45
7.7 Importing rules	45
7.7.1 Importing rules from the web interface	46
7.7.2 Importing rules in command line	46
7.8 Migrating local rules on a firewall to manage them in SMC	47
7.9 Managing URL filtering on SN firewalls from SMC	48
7.9.1 Creating the template URL filtering policy	48
7.9.2 Saving the URL filtering policy of the template firewall	49
7.9.3 Deploying the template URL filtering policy	50



7.10 Managing IPS Inspection profiles on SN firewalls from SMC	51
7.10.1 Editing the template IPS Inspection profiles	52
7.10.2 Saving the IPS Inspection profiles of the template firewall	53
7.10.3 Deploying the IPS Inspection profiles	53
8. Running SNS CLI commands on an environment of firewalls	55
8.1 Creating the CLI command script	55
8.2 Using variables	56
8.2.1 Using variables specific to firewalls	56
8.2.2 Using global variables	56
8.2.3 Using a CSV file	56
8.3 Running the SNS CLI script from the web interface	57
8.4 Running the SNS CLI script in command line	57
8.4.1 Displaying the list of commands and options	58
8.4.2 Running a script	58
8.4.3 Adding scripts	59
8.4.4 Deleting scripts	59
8.4.5 Displaying the list of scripts	59
8.4.6 Examples of the use of scripts in command line with a CSV file	59
8.5 Running the SNS CLI script on a high availability cluster	60
8.6 Attaching files to a script and receiving files generated by script	60
8.6.1 Command arguments to be used in the script	61
8.6.2 Attaching files to a script	61
8.6.3 Receiving files generated by a script	62
8.7 Scheduling the execution of SNS CLI scripts	63
8.7.1 Scheduling the execution of scripts from the web interface	63
8.7.2 Scheduling the execution of scripts in command line	63
8.8 Updating firewalls by using SNS CLI scripts	64
8.9 Troubleshooting	65
8.9.1 The script file is too large	65
8.9.2 Certain characters are not supported in the script	65
8.9.3 The script fails to run on certain firewalls	66
8.9.4 The Execute script button remains grayed out	66
9. Maintaining SN firewalls	67
9.1 Backing up the configuration of firewalls	67
9.1.1 Backing up the configuration of the server and firewalls automatically	67
9.1.2 Backing up the configuration of firewalls manually	68
9.2 Updating firewalls	68
9.3 Replacing firewalls in the case of an RMA	68
10. Removing SN firewalls from the SMC server	69
11. Managing and maintaining the SMC server	70
11.1 Defining the SMC server's network interfaces	70
11.2 Verifying the SMC server version in command line	70
11.3 Changing the SMC server time zone and date	70
11.3.1 Changing the time zone	70
11.3.2 Changing the date manually	71
11.3.3 Changing the date via NTP	71
11.3.4 Displaying a comprehensive summary of the SMC server's date/time	71
11.4 Managing administrators	71
11.4.1 Managing administrators in the web interface	71

11.4.2 Authorizing administrators to connect via an LDAP server	72
11.5 Consulting the SMC server logs	75
11.6 Sending SMC logs to a remote server in Syslog format	76
11.6.1 Sending logs to a remote server without encryption	76
11.6.2 Sending logs to a remote server with encryption	76
11.6.3 Disabling the sending of logs to a remote server	76
11.6.4 Troubleshooting	76
11.7 Saving and restoring the SMC server configuration	77
11.7.1 Saving the server configuration from the web interface	77
11.7.2 Saving the server configuration from the command line interface	78
11.7.3 Restoring server configuration from the web interface	78
11.7.4 Restoring server configuration from the command line interface	78
11.7.5 Restoring server configuration from the initialization wizard	78
11.8 Generating a server diagnostics report	79
11.8.1 Downloading the report from the web interface	79
11.8.2 Downloading the report in command line	79
11.9 Updating the SMC server from the command line interface	80
11.10 Resetting "root" and administrator passwords	80
11.10.1 Resetting the "root" administrator password	80
11.10.2 Resetting the administrator password	81
11.11 Disabling automatic synchronization of high availability clusters	81
11.12 Monitoring SMC with SNMP	81
11.12.1 Using the SNMP service	82
11.12.2 Using MIBs	82
11.13 Customizing the certificate of the SMC server web interface	82
11.13.1 Customizing the certificate	82
11.13.2 Reinitializing the certificate	83
Appendix A. Details of fwadmin-xxx commands	84
Appendix B. Compatibility of SMC/SN firewalls	85

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

1. Getting started with the SMC server

To administer 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. Through your web browser, log on to the IP address of the SMC server preceded by https://.
2. Enter your username and password, or use the default admin username 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:

- One read/write connection on the SMC server at a time,
- An unlimited number of read-only 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 from VMware 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 fwadmin-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 **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 not displayed 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 administer 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 2.5.1 is compatible with Stormshield Network Security from the 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 the [Compatibility of SMC/SN firewalls](#) section.

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**.

Status	Name	Deployment	Ver...
Green	Alpha	00017	3.0...
Green	Beta	N/A	3.0...
Green	Charlie		3.0...

2. Complete the firewall properties. The **Firewall name**, **Description** and **Location** fields are just filled in for information 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](#).

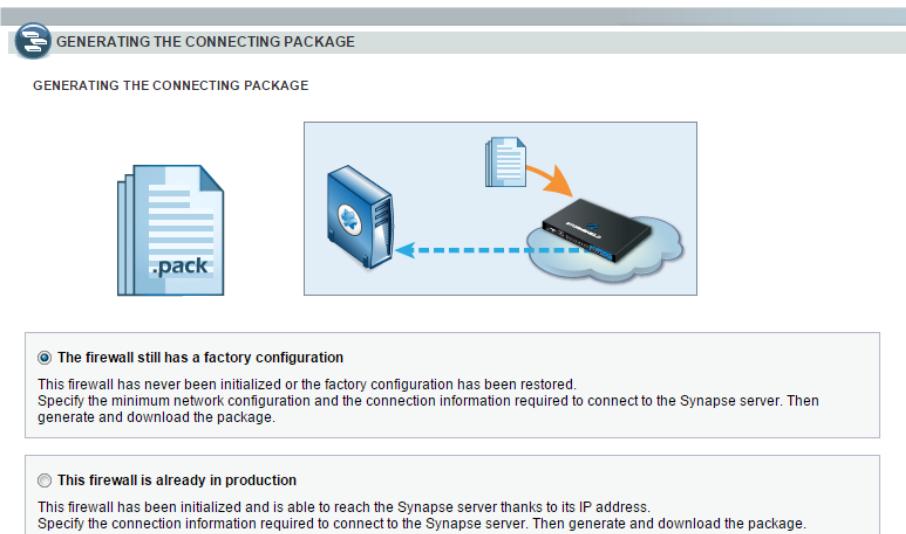
3.1.2 Building the firewall connecting package

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.



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. According to the firewall version, the panel is not the same.
 - **IP address or FQDN to reach:** the firewall connects to this address to reach the SMC server. Depending on network topology, it is either the SMC server IP address or an external IP address reachable by the firewall and redirected towards the SMC server through a destination translation.
 - **Public port number:** the firewall connects to this port to reach the SMC server. Depending on network topology, it is either the SMC server port (1754 by default) or an external port reachable by the firewall and redirected towards the SMC server port through a destination translation.
 - For firewalls in version 3.3.0 and upwards, you can set up to ten addresses or FQDN 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.
6. Click **Generate and download**.
7. To install the connecting package on the firewall, select one of the two procedures below.

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

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".

State	Name
●	Cluster_1
●	SNS_1
●	SNS_2

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](#).



The firewall administrator can see the connection settings to the SMC server on the firewall web administration interface: in the SMC 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 just filled in for information 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](#).

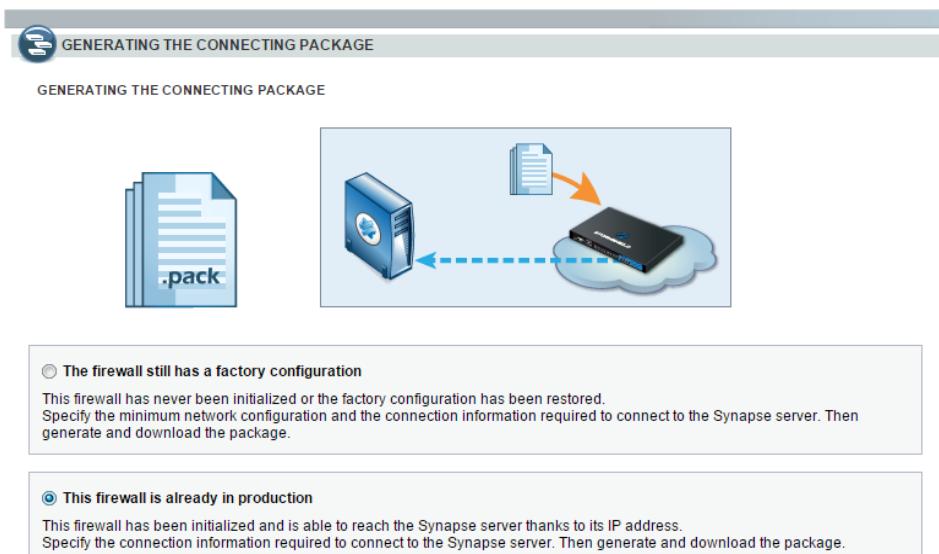
3.2.2 Building the firewall connecting package

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.



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**.

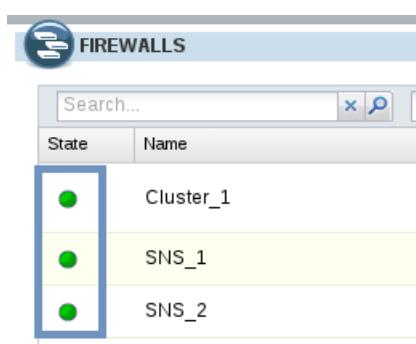


4. On next panel, select the version of the firewall and verify and edit the information to connect to the SMC server if necessary:
 - **IP address or FQDN to reach:** the firewall connects to this address to reach the SMC server. Depending on network topology, it is either the SMC server IP address or an external IP address reachable by the firewall and redirected towards the SMC server through a destination translation.
 - **Public port number:** the firewall connects to this port to reach the SMC server. Depending on network topology, it is either the SMC server port (1754 by default) or an external port reachable by the firewall and redirected towards the SMC server port through a destination translation.
 - For firewalls in version 3.3.0 and upwards, you can set up to ten addresses or FQDN 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.

5. Click **Generate and download**.

3.2.3 Installing the connecting package on the firewall

1. Provide the connecting package to the administrator in charge of administrating 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 installing the package, the administrator can see the connection settings to the SMC server 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 just filled in for information 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](#).

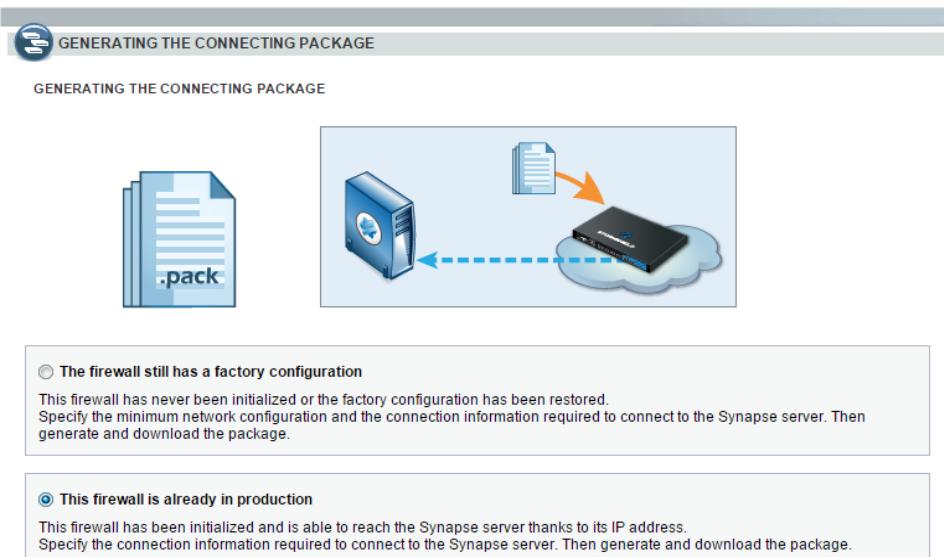
3.3.2 Building the cluster connecting package

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.



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:
 - **IP address or FQDN to reach:** the firewall connects to this address to reach the SMC server. Depending on network topology, it is either the SMC server IP address or an external IP address reachable by the firewall and redirected towards the SMC server through a destination translation.
 - **Public port number:** the firewall connects to this port to reach the SMC server. Depending on network topology, it is either the SMC server port (1754 by default) or an external port reachable by the firewall and redirected towards the SMC server port through a destination translation.
 - For firewalls in version 3.3.0 and upwards, you can set up to ten addresses or FQDN 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.
5. Click **Generate and download**.

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

1. Provide the connecting package to the administrator in charge of administrating 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 installing the package, the administrator can see the connection settings to the SMC server 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 looking up the following log files.

3.4.1 Generating a firewall's connecting package

Look up the logs on the SMC server, in `/var/log/fwadmin-server/server.log`

3.4.2 Installing the connecting package on the firewall

Look up the logs on the firewall, in `/log/_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 use a CSV file and import it on the server from the command line interface.

An example of a CSV file "example-firewalls-and-packages.csv" is available on the server, in the folder `/var/fwadmin/examples/csv`.

3.5.1 Creating the CSV file

The file may contain the following parameters organized in columns and separated by commas. Only the first column `#fwname` is mandatory:

- `#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 3.1 will be used.

- #fwdesc: firewall's description,
- #fwplace: location of the firewall,
- #fwfolder: 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.
- #vpn-fw-public-ip-address: firewall contact IP address manually specified in its settings and used in VPN topologies.
- #Vpn-fw-local-adress: firewall output interface used as source in VPN tunnels.
- #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,IP2:PORT2]: IP address and port of the SMC server - this information is needed for the connecting package,
- #custom1 to #custom10: customizable fields numbered from 1 to 10, which can be used in variable network objects and in SNS CLI scripts.

The order of parameters must always be the same.

3.5.2 Importing firewalls

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" account.
3. Enter the command:

```
fwdadmin-firewalls-and-packages /tmp/filename.csv.
```

Generated connecting packages are available in the folder /tmp/packages.

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

```
[root@smc] - {/var/tmp} > fwadmin-firewalls-and-packages firewall.csv --force
Remove all old files [.pack] in tree directory: /tmp/sns/data
[PARIS] firewall created successfully
[PARIS] connecting package created successfully
[BERLIN] firewall created successfully
[BERLIN] connecting package created successfully
[ROME] firewall created successfully
[ROME] connecting package created successfully
[MADRID] firewall created successfully
[MADRID] connecting package created successfully
[LONDON] firewall created successfully
[LONDON] connecting package created successfully
[NEWYORK] firewall created successfully
[NEWYORK] connecting package created successfully
[LISBON] firewall created successfully
[LISBON] connecting package created successfully
[ATHENS] firewall created successfully
[ATHENS] connecting package created successfully
[BERN] firewall created successfully
[BERN] connecting package created successfully
[VIENNA] firewall created successfully
[VIENNA] connecting package created successfully
[BRUSSELS] firewall created successfully
[BRUSSELS] connecting package created successfully
[AMSTERDAM] firewall created successfully
[AMSTERDAM] connecting package created successfully
Copy connection packages in directory: /tmp/packages
Remove all old files [.pack] in tree directory: /tmp/packages

R E S U M E
=====
Firewalls created successfully : 12
Firewalls updated successfully : 0
Firewalls ignored      : 0
Firewalls creation failure : 0

Firewalls package created successfully : 12
Firewalls package ignored   : 0
Firewalls package creation failure : 0

Copy connecting packages in directory : /tmp/packages
[root@smc] - {/var/tmp} > cd /tmp/packages/
[root@smc] - {/tmp/packages} > ls
fw-conn-AMSTERDAM-20180129-225121.pack fw-conn-BERLIN-20180129-225113.pack fw-conn-LONDON-20180129-225102.pack fw-conn-PARIS-20180129-225051.pack
fw-conn-ATHENS-20180129-225110.pack fw-conn-BRUSSELS-20180129-225119.pack fw-conn-MADRID-20180129-225059.pack fw-conn-ROME-20180129-225055.pack
fw-conn-BERLIN-20180129-225053.pack fw-conn-LISBON-20180129-225108.pack fw-conn-NEWYORK-20180129-225104.pack fw-conn-VIENNA-20180129-225117.pack
```

You can also:

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

```
fwadmin-firewalls-and-packages /tmp/filename.csv --firewall-only
```

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

```
fwadmin-firewalls-and-packages /tmp/filename.csv --package-only
```

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

3.6 Editing firewalls' outgoing interface to communicate with SMC

This feature is available for SN firewalls version 3.3 or later.

You can select an outgoing interface other than the default interface for the firewall to connect to the SMC server:

- Connect to the firewall via the command line interface.
- Enter the following commands, replacing **Firewall_interface** with the name of the desired interface configured on the firewall:

```
CONFIG FWADMIN UPDATE bindaddr=Firewall_interface
CONFIG FWADMIN ACTIVATE
```

4. Supervising SN firewalls

Different types of information about each firewall are displayed in **Monitoring > Firewalls** and allow seeing and supervising firewalls. Direct access to the logs and activity reports of a firewall is also possible.

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, etc.


TIP

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

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.

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 allows displaying firewalls which status is **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.

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 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, but can be renamed. 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.



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.

Name	Description	Number of firewalls	Number of sub-folders
France		6	2
International		9	5



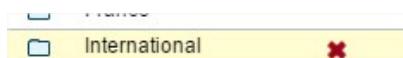
Organizing firewalls

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.

4.1.3 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 the logs and activity reports of firewalls

From the SMC server, you can directly access the logs and activity reports of connected firewalls.

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 **Logs and activity reports** interface of the firewall.

For more information about the logs and activity reports interface, refer to the *Stormshield Network User Configuration Manual*.

5. Configuring SN firewalls

Configure your firewalls, objects, rules and VPN topologies in the SMC server web interface and deploy the configuration on the firewalls. Direct access to the web administration interface of a firewall is also possible.

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 an environment of firewalls](#).

5.1 Editing firewalls

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,
- 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,
- 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,
- Create and manage filter and NAT rules,
- See the list of objects deployed on the firewall.

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



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

5.2 Managing 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](#).



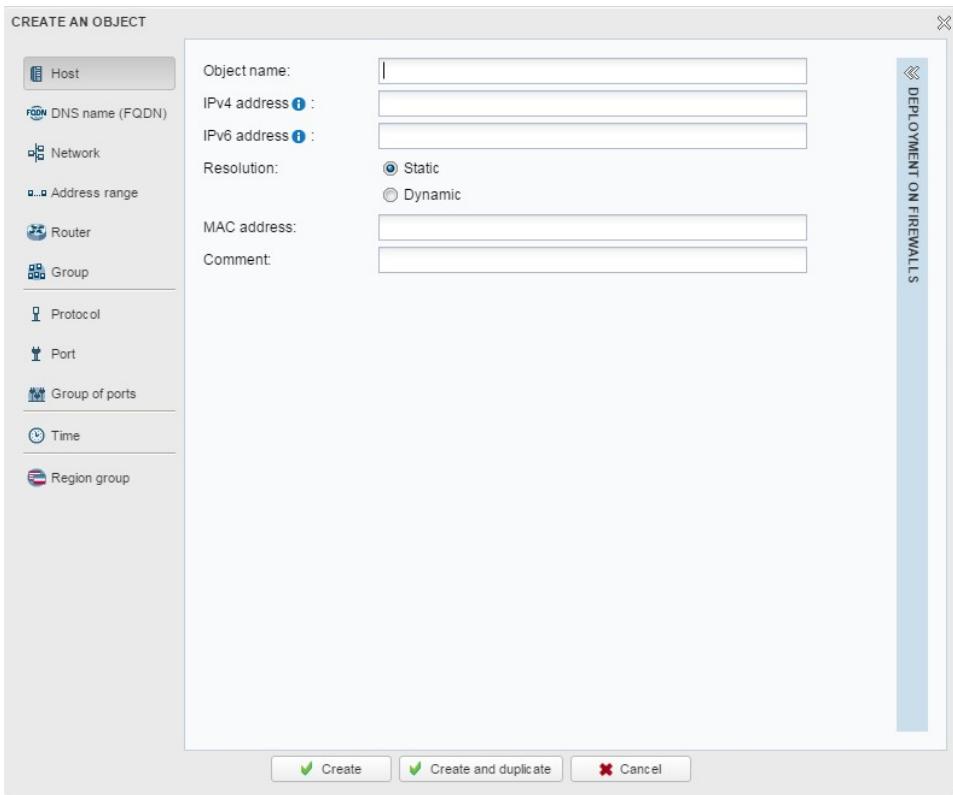
⚠ Warning

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

5.2.1 Deploying objects 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 (↖).

5.2.2 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.

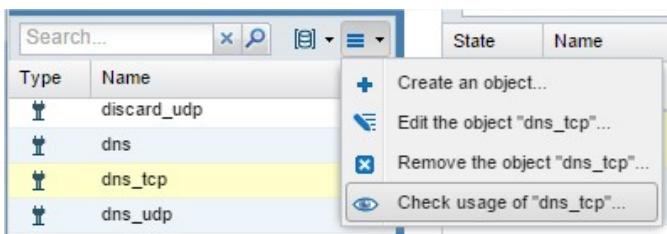
1. In the **Network objects** menu, create a Host or Network object.
2. Fill in the **IPv4 address** or **IPv6 address** field with the variable %FW_CUSTOMx%. This customized variable is defined in the **Customized variables** tab in the **Edit firewall** panel accessible by double clicking on the line of a firewall in monitoring view. "x" represents a number between 1 and 10.
 - For example: enter the address 10.1.%FW_CUSTOM1%.0/24. If for a given firewall, the customized field 1 in its parameters equals "1", 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.

5.2.3 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**.



5.2.4 Importing objects from a CSV file

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 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 `/var/fwadmin/examples/csv`.

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 the **Export** button.

This file contains all the network objects and groups on your firewall.

To create a new CSV file, and to find out details about headers 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 their 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.

Importing 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" user.
3. To import all object types, enter the command:
`fwadmin-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. For example, to import only Host and IP address range objects from a CSV file, enter the command:

```
fwadmin-import-objects --csv-file /tmp/fichier.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
Group 1	--group
IP protocol	--protocol
Service (port)	--service
Port group	--servicegroup

Customized variables such as %FW_CUSTOMx% 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.

¹When 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.

5.3 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](#).

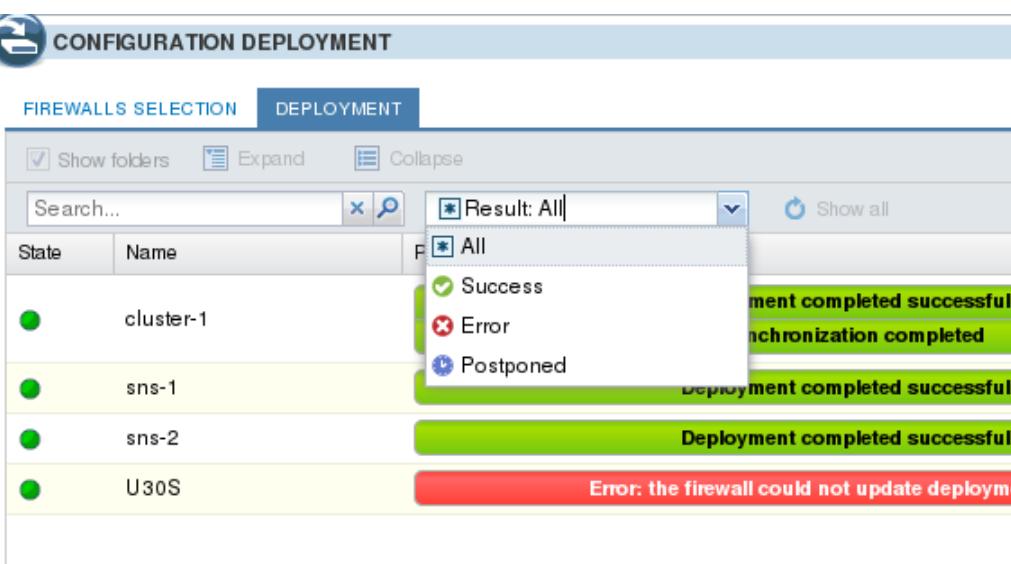
During a deployment, the following information will be sent to the firewalls:



- 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 objects](#).
- If the firewall is part of a VPN topology: Network, Host and/or Group objects and the certificate 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).

5.3.1 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 **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 logs about the deployment in progress on this firewall.
6. See the deployment summary at the bottom of the panel, showing successes, errors and the deployments postponed.
7. You can also filter the list of firewalls by selecting a status in the drop down list at the top of the list.



State	Name	Result
Success	cluster-1	Deployment completed successful
Success	sns-1	Synchronization completed
Success	sns-2	Deployment completed successful
Error	U30S	Error: the firewall could not update deployment

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



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.

5.3.2 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.

5.3.3 Deploying a configuration on a firewall in command line

You can use the `fwadmin-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 `fwadmin-deploy --help`.

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

5.3.4 Troubleshooting with the server's logs

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

5.3.5 SMC side

`/var/log/fwadmin-server/server.log`

5.3.6 Firewall side

`/log/_system`

5.4 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.

5.5 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.

5.6 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 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 Network User Configuration Manual](#).

5.7 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.



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

5.8 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 case of failover, the passive node will become active and will automatically connect to the SMC server.



The icon in the **Mode** column is updated in the list of firewalls on 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.

5.9 Importing or declaring a certificate for a firewall

A PKCS#12 or PEM certificate is required for each firewall that is part of a VPN topology using X509 authentication.

The certificate can be installed 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.

5.9.1 Importing a certificate from the server's web interface

There are three ways to import a certificate for a firewall from the web interface.

1. In the **Monitoring > Firewalls** menu, double click on a connected firewall.
2. In the **IPSec VPN** tab, select the relevant certificate or click on **Import a new certificate**.

-or-

1. In the **Monitoring > Firewalls** menu, scroll over the name of a connected firewall and click on the  icon.
2. In the window that opens, select the relevant certificate.
3. Choose whether to use this certificate as the default certificate used in VPN topologies.
-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 and monitoring VPN tunnels](#).

5.9.2 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
`fwadmin-install-certificate`



Display help using the option `--help`:

```
[root@synapse] ~ {~} > fwadmin-install-certificate -h
Usage: fwadmin-install-certificate [options] certificate firewall

Tool that imports a certificate file (.p12) 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:
  -h, --help           show this help message and exit
  -c PATH, --certificate=PATH
                      [Mandatory] The certificate to import on the Firewall
  -f FIREWALL_NAME, --firewall=FIREWALL_NAME
                      [Mandatory] The target firewall name
  -v, --verbose        Verbose mode. [default: False]
  --raw-output         Raw output mode (disables colors, spinners, ...).
                      [default: False]
  -p PASSWORD, --password=PASSWORD
                      The password of the certificate
[root@synapse] ~ {~} > _
```

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`.

5.9.3 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.

5.9.4 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 certificate authority via SCEP.

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.

5.9.5 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 run or configuration deployment to end.

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.

6. Creating and monitoring VPN tunnels

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

SMC allows creating and managing VPN tunnels that link networks or sub-networks protected by firewalls. These firewalls or gateways act as entry and exit points for tunnels and may be:

- SN firewalls in version 3 and up, 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 types of VPN topology: mesh or star.

- Mesh: all remote sites are able to communicate among themselves,
- Star: a central site communicates with 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 need to:

- Create your traffic endpoints beforehand (Network, Host or Group) in the **Network objects** menu. For more information, please refer to the section [Managing 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 certificate authorities beforehand as well. The corresponding procedures are described in the section [Configuring a mesh topology](#).

SMC 2.5.1 Version does not support VPN topologies in IPv6. If a topology includes network objects in IPv6, they will be ignored. If a topology relies on network objects with dual IPv4/IPv6 configuration, only the configuration in IPv4 will be applied and the IPv6 configuration ignored.

In this section, we describe two use case scenarios, a mesh topology and a star topology. For further detail on each menu and option for configuring VPN tunnels, refer to the [Stormshield Network User Configuration Manual](#).

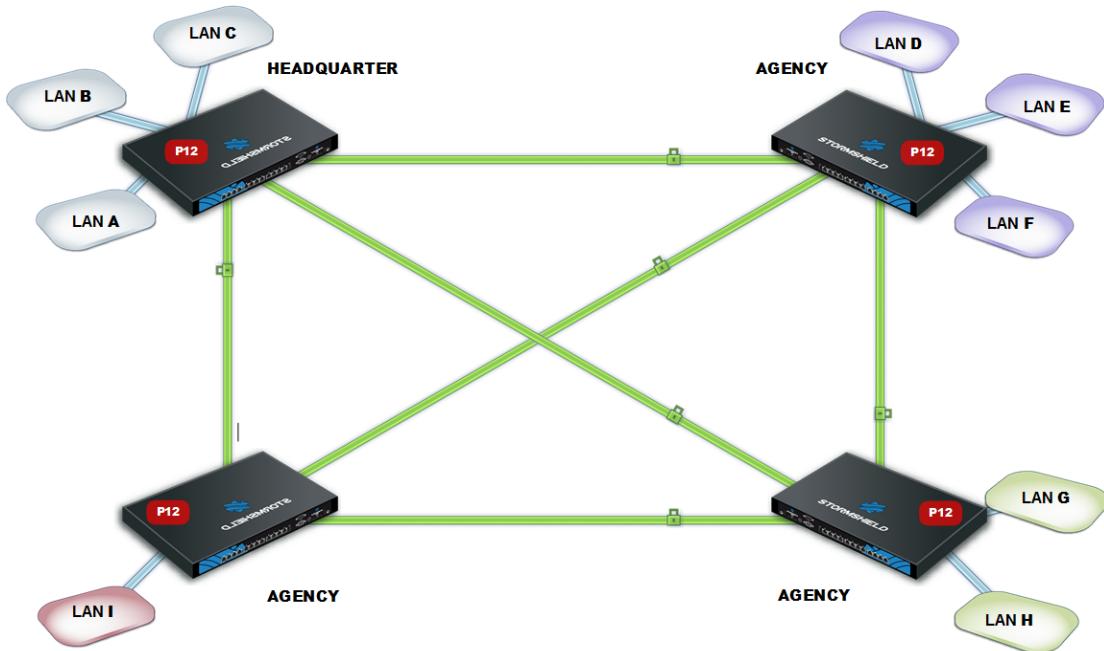
6.1 Configuring a mesh topology

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 certificate 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.

6.1.1 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](#)

6.1.2 Declaring certificate authorities

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

In order for the topology to be deployed, the SMC server must know the certificate authorities' entire chain of trust. For further information and to find out how to add certificate authorities, refer to the section [Managing certificate authorities](#).

6.1.3 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 certificate 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 certificate 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 expiration 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 fwadmin-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.

6.1.4 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.

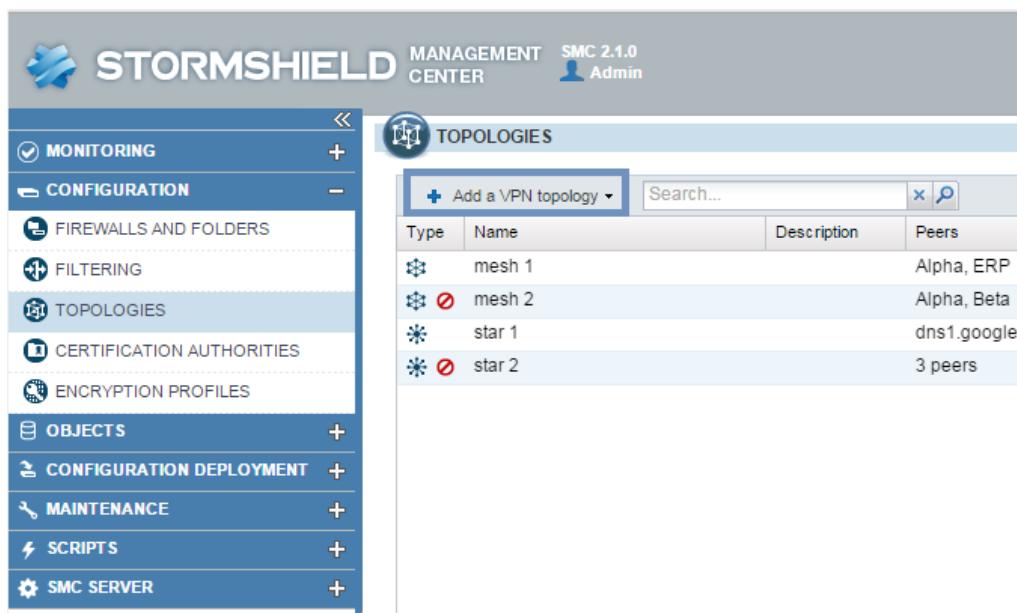
 **WARNING**

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

6.1.5 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**.



Type	Name	Description	Peers
mesh	mesh 1		Alpha, ERP
mesh	mesh 2		Alpha, Beta
star	star 1		dns1.google.
star	star 2		3 peers

2. Enter a name. A description is optional.
3. Select X.509 certificate authentication and select the certificate 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.
4. Select the encryption profile. The SMC server offers three pre-configured profiles. Create your customized profiles in **VPN > Encryption profiles**. Refer to the [Stormshield Network User Configuration Manual](#) for more information on encryption profile options.
5. Select your topology peers. You can only select connected or offline firewalls, and in at least version 3.
6. 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](#).
7. Click on **Apply**.
8. Deploy the configuration on the firewalls involved in the topology. The VPN configuration belongs to the firewall's global policy.

6.2 Configuring a star topology

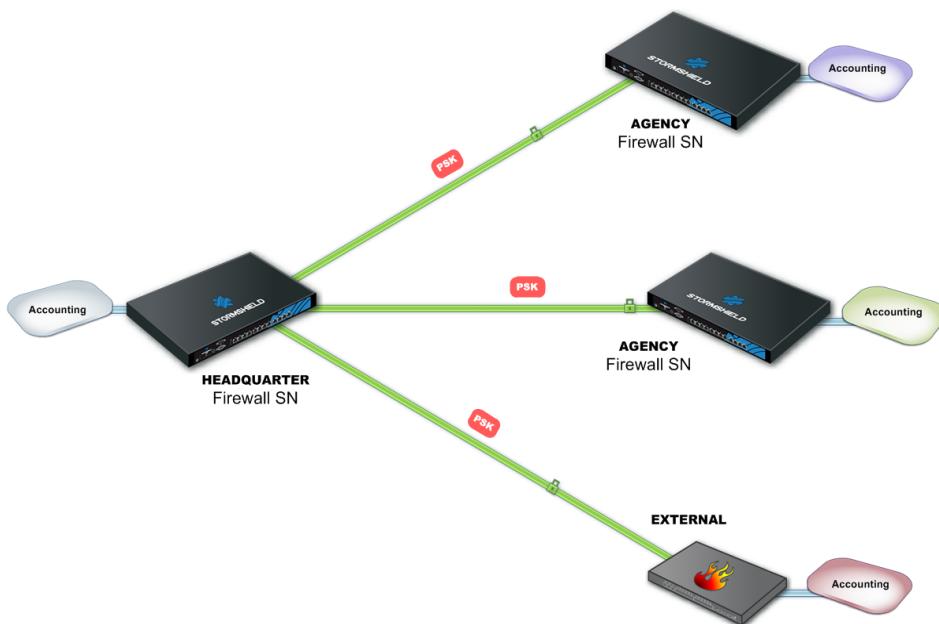
Example of a scenario:

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.

6.2.1 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.

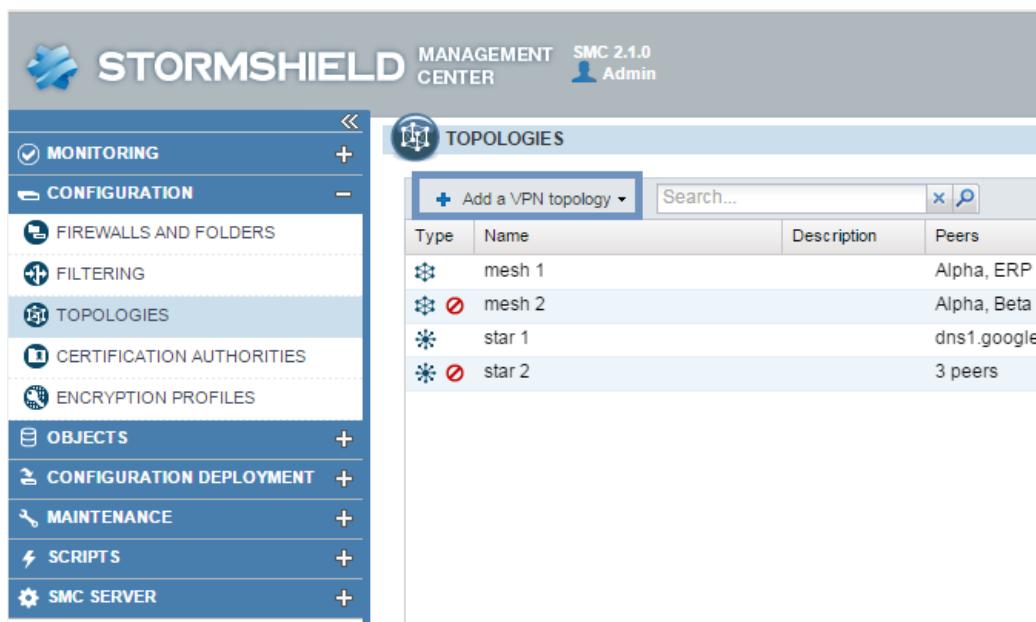
⚠️ WARNING

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

6.2.2 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 **Star**.



Type	Name	Description	Peers
mesh	mesh 1		Alpha, ERP
mesh	mesh 2		Alpha, Beta
star	star 1		dns1.google.
star	star 2		3 peers

2. Enter a name. A description is optional.
3. Select pre-shared key authentication.
4. Generate a random key.
5. 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.
6. 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.
7. 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.
8. Select your topology peers. You can only select connected or offline firewalls, and in at least version 3.
9. 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**.
10. Click on **Apply**.
11. Deploy the configuration on the firewalls involved in the topology. The VPN configuration belongs to the firewall's global policy.

6.3 Managing certificate authorities

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

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



6.3.1 Adding a certificate authority or chain of trust

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

1. In Configuration > Certificate Authorities, click on Add an authority.

Name	Subject
MyCA	CN=MyCA,OL
Stormshield_2	C=FR, ST=Rh
Stormshield	C=FR, ST=Rh

2. Select a file in .pem, .cer, .crt or .der.
3. Add the addresses of the distribution point(s) for the certificate revocation list (CRL). For more information, please refer to the section [Setting the CRL distribution points](#).
4. Once the authority has been declared, you can edit it or check its usage by scrolling over the name of the authority in the list of authorities in order to make the icons appear.

A new authority can also be added during the configuration of the VPN topology, during the selection of the authentication method, by clicking on **Add an authority**.

6.3.2 Updating a certificate authority or chain of trust

Whenever you update a certificate 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 certificate authority, scroll over the name of the certificate authority and click on the icon.

6.3.3 Deleting a certificate authority or chain of trust

Whenever you delete a certificate 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 certificate authority, scroll over the name of the certificate authority and click on the icon.

6.4 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.

6.4.1 Defining a firewall's default contact address

1. Go to **Monitoring > Firewalls**, and double click on the SN 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.

6.4.2 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.

6.5 Selecting the output interface of firewalls for VPN topologies

You can select the firewall output interface used as the source in a VPN tunnel. Three 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. Configure a static route on the firewall so that the tunnel works.

6.5.1 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.

6.5.2 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.

6.5.3 Configuring a static route on the firewall

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*](#).

6.6 Editing and deleting a VPN topology

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

To edit:

- 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.

To delete:

- Scroll over the name of the firewall in the list and click on the red cross.

In both cases, redeploy the configuration after these operations.



6.7 Monitoring the status of VPN tunnels

The **Monitoring > VPN** menu allows looking up the status of each tunnel configured in each topology.

Scroll over the status icon of a tunnel to display a tooltip indicating its status as well as the status of peers.

The screenshot shows the Stormshield Management Center interface. On the left, there is a navigation sidebar with the following items:

- MONITORING** (selected)
- FIREWALLS
- VPN
- CONFIGURATION**
- OBJECTS
- CONFIGURATION DEPLOYMENT
- MAINTENANCE
- SCRIPTS
- SMC SERVER

The main content area is titled "VPN". It includes a search bar and a dropdown menu set to "Status: All". Below this is a table with the following columns: Status, Topology, Traffic endpoint A, and Peers. The table contains four rows of data:

Status	Topology	Traffic endpoint A	Peers
?	* bar	some-network-2 (10.0.2.0/24)	sns-2 sns-1
?	* bar	some-network-2 (10.0.2.0/24)	sns-3 sns-1
?	* bar	some-network-1 (10.0.1.0/24)	sns-6 sns-1
!	foo	some-network-1 (10.0.1.0/24)	sns-6 sns-7

7. Creating filter and NAT rules

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

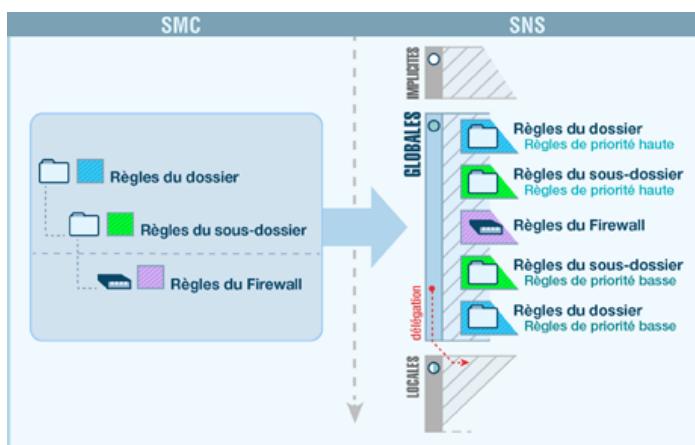
SMC allows deploying filter and NAT rules in your environment of firewalls. Rules apply to sets of firewalls (folders and sub-folders) or are specific to certain firewalls, therefore making it possible to configure a rule shared by several sites just once, while continuing to be able to deploy specific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

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.

7.1 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.

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

7.2 Use case examples

7.2.1 Managing an environment without rule sharing

We shall use the example of a service provider who administers 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.

7.2.2 Managing an environment 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:

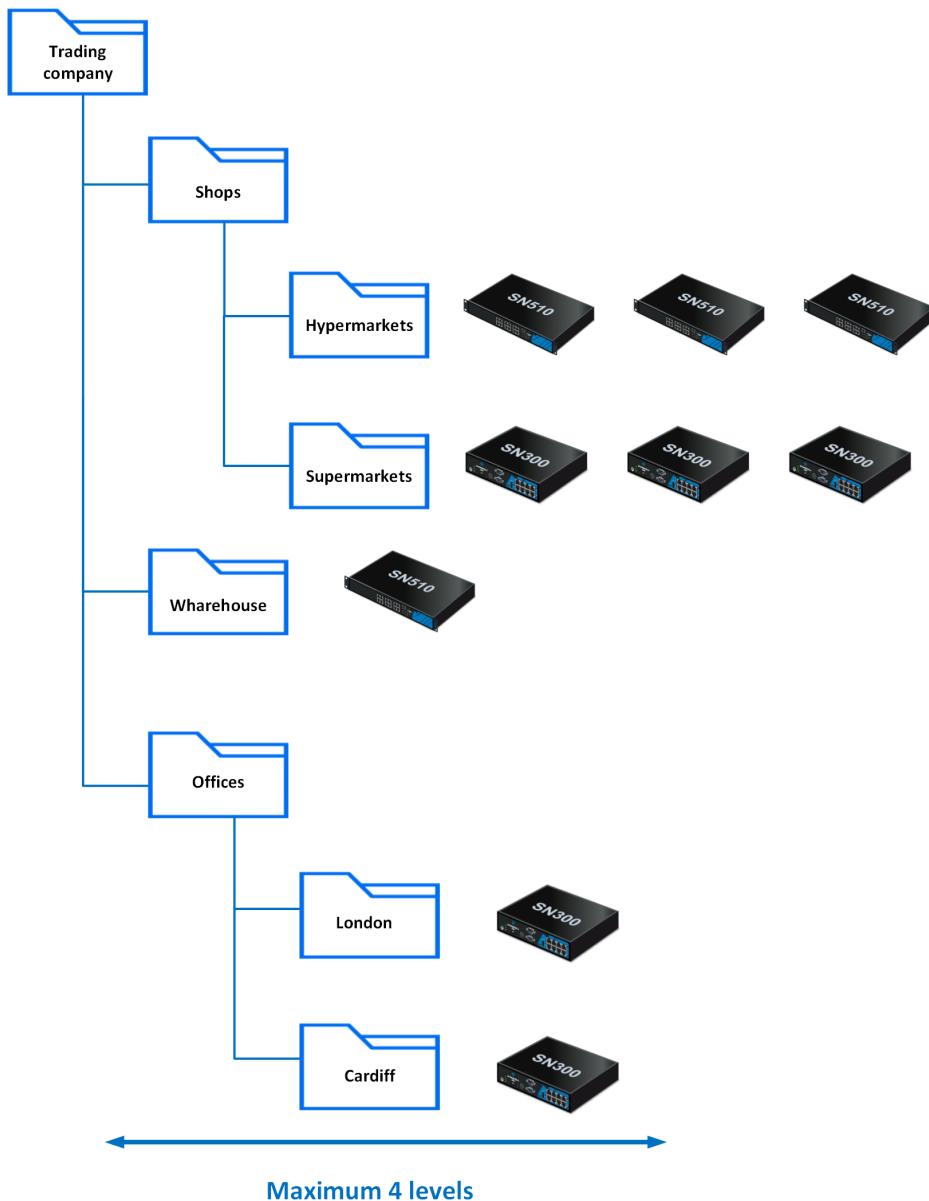
- Define the rules shared by all firewalls in the MySMC folder, for example to provide all firewalls with access to its datacenter. For this purpose, a variable object will be used: a Host object representing a firewall interface. A single rule and a single object will therefore suffice for all firewalls. For more information, please refer to the section [Managing 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.

7.2.3 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 variables objects. For more information, please refer to the section [Managing 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.



7.3 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 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.

7.4 Identifying the rules

In the **Filter rules** and **NAT rules** tabs of a firewall, the **Rule** column allows identifying the rules applied to a firewall. This number can be seen in the firewall's administration interface and in traces.

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.



FOLDER: MY SMC - 3 high priority rules					
Rank	Status	Action	Source	Destination	
1	My SMC on	pass	GROUPEA	Internet	
2	My SMC on	pass	Any	network2	network1
3	My SMC on	block	Any	Any	

7.5 Changing the order in which rules are executed

You can modify 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 or separator, 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 or separator into another folder or onto another firewall. You can copy rules from the active table or from parent folders.

7.6 Removing rules

- Press the **DELETE** key.
- or-
- Click on **Remove** in the toolbar.

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

7.7 Importing rules

You can import rules that already exist on SN firewalls:

- from the SMC server web interface,
- by importing a CSV file on the SMC server from the command line interface

This feature allows you to:

- move the management of SN 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.

- easily deploy rules from one firewall on other firewalls.

7.7.1 Importing rules from the web interface

In order to import a firewall's rules from the web interface, the firewall has to be in at least version 3.3 and must be connected to the SMC server.

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 SN 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 procedure below. If errors arise, details will be provided.

7.7.2 Importing rules in command line

This feature makes it possible to import a large amount of rules from a manually created CSV file.

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

An example of a CSV file "example-import-rules.csv" is available on the server, in the folder `/var/fwadmin/examples/csv`.

Creating the CSV file

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.
4. Click on the **Export** button.

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.

Importing rules on the SMC server.

The command for importing rules is: `fwadmin-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. Otherwise, use the `--force` option if another administrator is simultaneously logged on with write privileges.

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.

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 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:
`fwadmin-import-rules /tmp/rules-file.csv --objects /tmp/objects-file.csv --firewall destination-firewall`

or

```
fwadmin-import-rules /tmp/rules-file.csv --objects /tmp/objects-file.csv --folder destination-folder --low-priority
```

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`:

```
fwadmin-import-rules /tmp/rules-file.csv --update --objects /tmp/objects-file.csv --folder destination-folder --low-priority
```

WARNING

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:
 - `fwadmin-import-rules /tmp/your-rules-file.csv --firewall destination-firewall`: the destination of these rules is a firewall,
 - `fwadmin-import-rules /tmp/your-rules-file.csv --folder destination-folder --low-priority`: the destination of these rules is a folder,
You then need to choose the block of rules (`--low-priority` or `--high-priority`).

7.8 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](#).

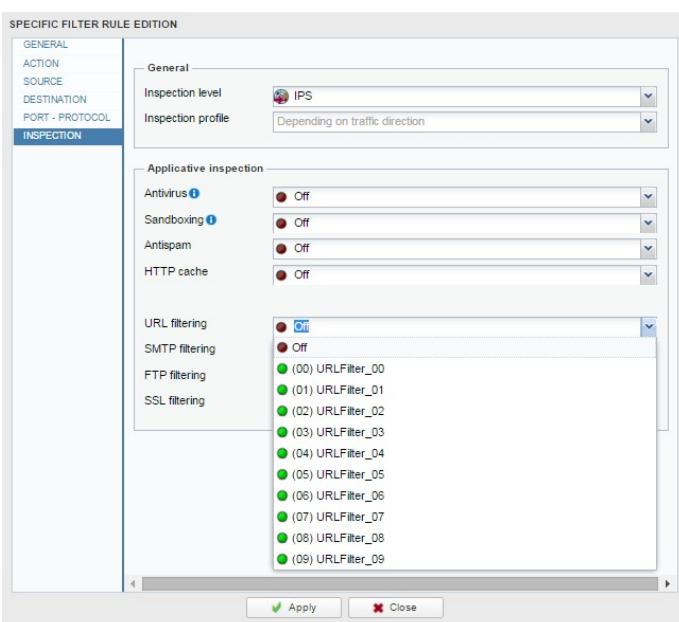


2. The [Use case examples](#) may give you ideas on choosing how to organize newly imported rules.
3. In SMC, deploy the rules on the firewall in question. They will appear in the firewall's global policy and will be applied as a priority.
4. Ensure that this new organization functions properly.
5. If 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).

7.9 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.

WARNING

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.

7.9.1 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.

		URL category
(0) SMC_URL_Filter	e_00	ads
(1) policy_SMC2	e_00	entertainment
(2) policy_SMC3	e_00	proxy
(3) URLFilter_03	e_00	it
(4) URLFilter_04	e_00	bank
(5) URLFilter_05	e_00	business
(6) URLFilter_06	e_00	employment
(7) URLFilter_07	e_00	it
(8) URLFilter_08		
(9) URLFilter_09		
6 Enabled BlockPage_00		
7 Enabled BlockPage_00		
8 Enabled Pass		

7.9.2 Saving the URL filtering policy of the template firewall

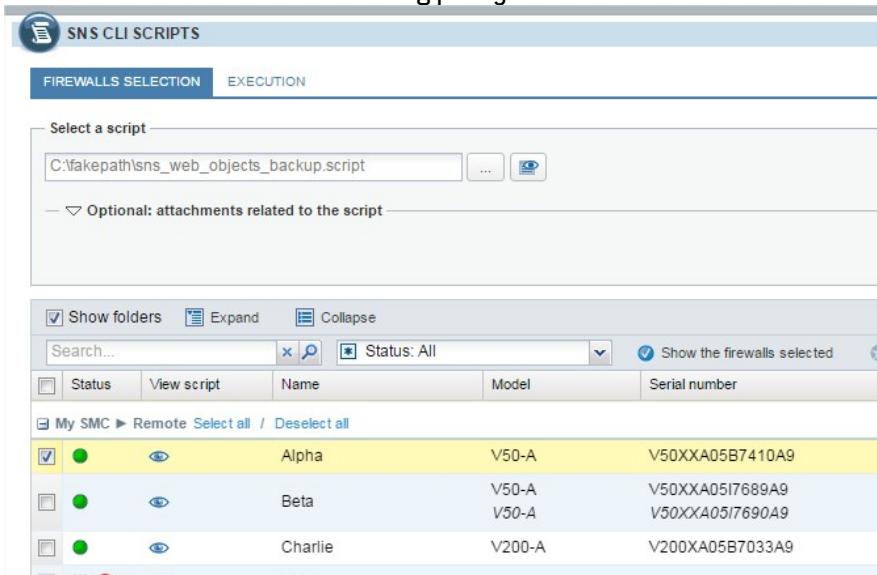
The following script allows collecting the URL filtering policy of the template firewall (URL filtering profiles and Web objects).

```
#####
# 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 **Scripts > SNS CLI Scripts**.
3. Select the script you saved previously.

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



The screenshot shows the 'SNS CLI SCRIPTS' interface with the 'FIREWALLS SELECTION' tab selected. A script path 'C:\fakepath\sns_web_objects_backup.script' is entered in the 'Select a script' field. Below it, a table lists three firewalls: Alpha (V50-A), Beta (V50-A), and Charlie (V200-A). The 'Show the firewalls selected' checkbox is checked, and Alpha is highlighted in yellow, indicating it is selected.

Status	View script	Name	Model	Serial number
<input type="checkbox"/>		Alpha	V50-A	V50XXA05B7410A9
<input type="checkbox"/>		Beta	V50-A V50-A	V50XXA05I7689A9 V50XXA05I7690A9
<input type="checkbox"/>		Charlie	V200-A	V200XA05B7033A9

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 an environment of firewalls](#).

7.9.3 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 **Scripts > 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.

The screenshot shows the 'SNS CLI SCRIPTS' interface. At the top, there are tabs for 'FIREWALLS SELECTION' and 'EXECUTION'. Under 'FIREWALLS SELECTION', a script path 'C:\fakepath\restore_sns-web-object_for_EMBEDDED-URL.na' is selected. Below it, an optional attachment 'backup-URL.na' is listed. A table lists three firewalls: Alpha (V50-A), Beta (V50-A), and Charlie (V200-A). The 'Beta' row is highlighted with a yellow background, indicating it is selected for deployment.

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

7.10 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).

The screenshot shows the 'SPECIFIC FILTER RULE EDITION' dialog. The left sidebar has tabs for GENERAL, ACTION, SOURCE, DESTINATION, PORT - PROTOCOL, and INSPECTION. The INSPECTION tab is selected. The right panel shows the 'General' section with 'Inspection level:' set to 'IPS' and 'Depending on traffic direction'. Below this, under 'Applicative inspection', there is a list of profiles: (00) IPS_00, (01) IPS_01, (02) IPS_02, (03) IPS_03, (04) IPS_04, (05) IPS_05, (06) IPS_06, (07) IPS_07, (08) IPS_08, and (09) IPS_09. The 'Apply' and 'Close' buttons are at the bottom.

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.

WARNING

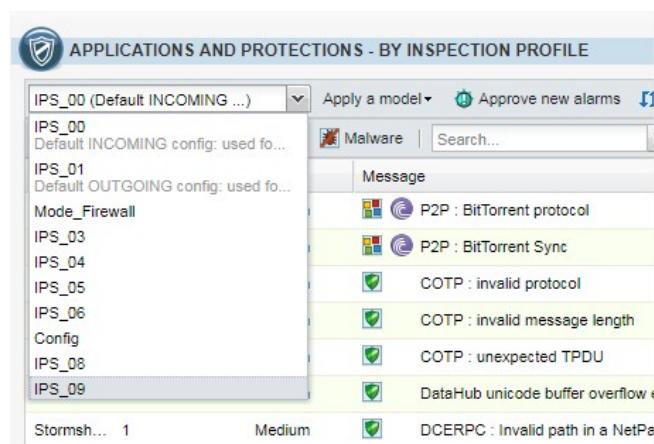
The template firewall and the target firewalls must be in the same version.

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

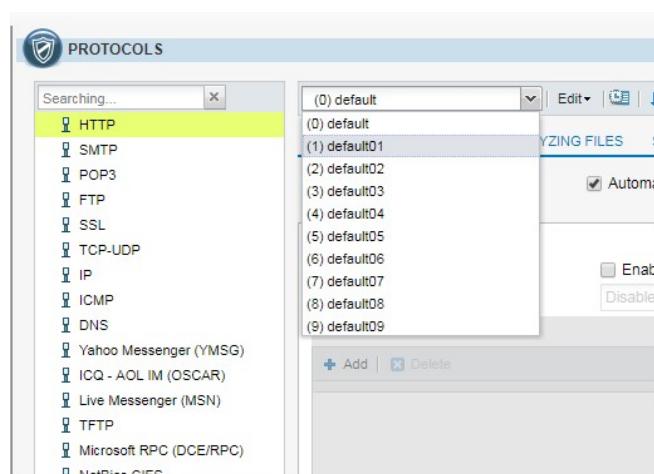
7.10.1 Editing the template IPS Inspection profiles

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.



7.10.2 Saving the IPS Inspection profiles of the template firewall

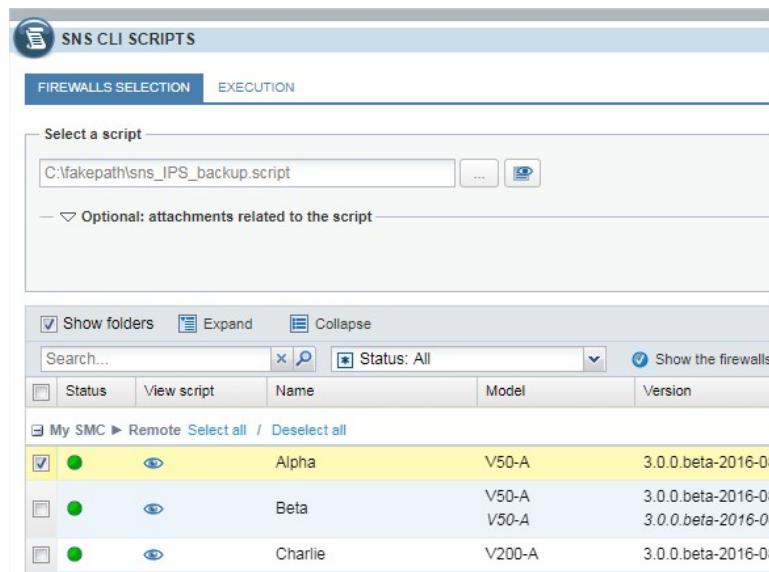
The script below makes it possible to retrieve the IPS Inspection profiles of the template firewall.

```
#####
# 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 **Scripts > 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 an environment of firewalls](#).

7.10.3 Deploying the IPS Inspection profiles

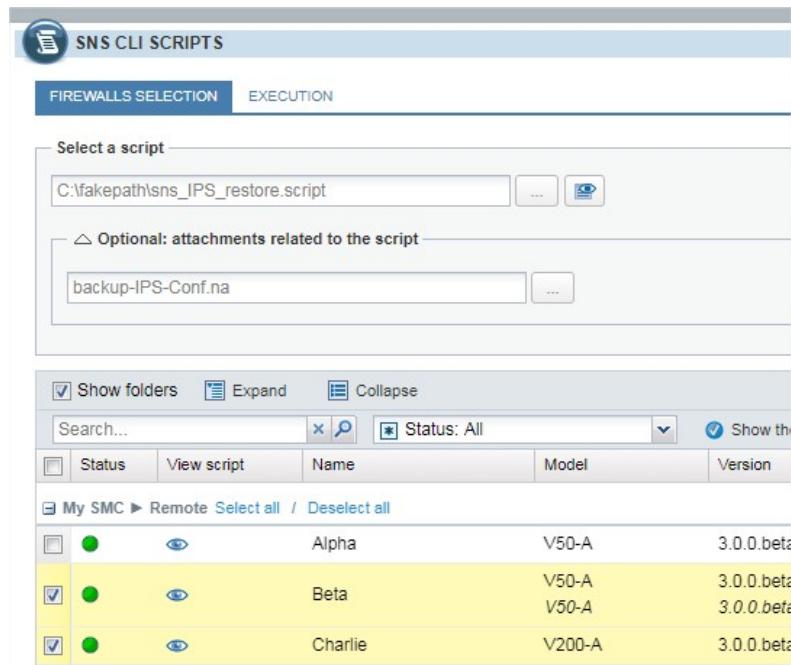
The script below makes it possible to deploy the IPS Inspection profiles previously saved on the other firewalls.

```
#####
# 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 **Scripts > 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.



The screenshot shows the SNS CLI Scripts interface. At the top, there are tabs for "FIREWALLS SELECTION" and "EXECUTION". The "EXECUTION" tab is selected. Below the tabs, there is a section titled "Select a script" with a text input field containing "C:\fakepath\sns_IPS_restore.script" and a browse button "...". Underneath this, there is a section titled "Optional: attachments related to the script" with a text input field containing "backup-IPS-Conf.na" and a browse button "...".

Below these sections, there is a search bar with "Search..." and a status filter "Status: All". A table below lists three firewalls: Alpha, Beta, and Charlie. Each row has a checkbox in the first column, and the checkboxes for Beta and Charlie are checked. The table columns are: Status, View script, Name, Model, and Version.

	Status	View script	Name	Model	Version
<input type="checkbox"/>	●	○	Alpha	V50-A	3.0.0.beta
<input checked="" type="checkbox"/>	●	○	Beta	V50-A	3.0.0.beta
<input checked="" type="checkbox"/>	●	○	Charlie	V200-A	3.0.0.beta

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

8. Running SNS CLI commands on an environment of firewalls

Stormshield Management Center 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 an environment 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 examples of how scripts are used, please refer to the section [Examples of the use of SNS CLI scripts](#).

8.1 Creating the CLI command script

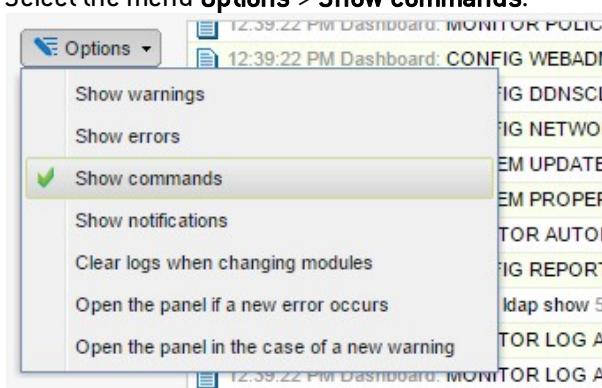
Create a UTF-8 encoded text file not exceeding 5 MB with the extension `.script` containing the commands to be run in your environment of firewalls.

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 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](#).

8.2 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 a CSV file](#).

Variables are case sensitive.

8.2.1 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),
- FW_CUSTOM1 to FW_CUSTOM10: customizable fields 1 to 10.

Ten variables can be customized to your needs (FW_CUSTOM1 to FW_CUSTOM10). Double-click on a firewall in the **Monitoring > Firewalls** menu and open the **Customized variables** tab. Fill in the fields with you customized values.

8.2.2 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").

8.2.3 Using a CSV file

If there are not enough customizable variables, and 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 `/var/fwadmin/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](#).

8.3 Running the SNS CLI script from the web interface

1. In the web interface of the SMC server, select **Scripts > 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 allows viewing the raw contents of the script as it is found on your workstation.
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 firewalls on which the script will be run. For each firewall:
 - The  icon indicates, where applicable, that the firewall cannot be selected for the execution of the script. As such, the row will be grayed out. Scroll over the icon with your mouse to find out why.
 - The  icon allows viewing 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.

 **WARNING**

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 the icon  in the **Actions** column.

8.4 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 `fwadmin-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/`.

8.4.1 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 <script-name>    Delete a SNS CLI script from the SMC
                                                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 `fwadmin-sns-cli-script <name_of_action> -h`.

8.4.2 Running a script

- To add a script on the SMC server and run it immediately, use the command:
`fwadmin-sns-cli-script exec <file_path>`

- To run a script that has already been stored on the SMC server, use the command:
`fwadmin-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:

- `--force`: allows forcing the previous session to shut down, for example in the case of a script run that did not end properly,



- `--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](#).

8.4.3 Adding scripts

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

Two options can be added to this command:

- `--force`: allows forcing the previous session to shut down, for example in the case of a script run that did not end properly,
- `--update`: makes it possible to force the script to be added on the server if a script with the same name already exists.

8.4.4 Deleting scripts

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

You can add the option `--force` to force an earlier session to log off.

8.4.5 Displaying the list of scripts

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

8.4.6 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 assertions:

- 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 environment 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:

```
fwadmin-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
```



In CSV files, fields are often separated by a comma or semi-colon. The `fwadmin-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=, fwadmin-sns-cli-script exec --csv-
file=/var/tmp/myfile.csv /var/tmp/myscript.script
```

8.5 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 performs a synchronization of 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.

8.6 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.

8.6.1 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")
```



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")
```

8.6.2 Attaching files to a script

Via the web interface

1. In the web interface of the SMC server, select **Scripts > SNS CLI scripts**.
2. In the *Firewalls selection* tab, after having selected a script, expand the **Optional: attachments related to the script** sub-menu and select one or several attachments.

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`.

8.6.3 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, please 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 including 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**.

View execution logs

To simply view 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 placed 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.

8.7 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](#).

8.7.1 Scheduling the execution of scripts from the web interface

1. In the web interface of the SMC server, select **Scripts > 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 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 for the execution of the script. As such, the row will be grayed out. Scroll over the icon with your mouse to find out why.
 - The  icon allows viewing 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.

 **WARNING**

The read/write privileges on any administration sessions already open on the firewalls in question are automatically adopted when a script is run.

8.7.2 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 scheduling the execution of the command `fwadmin-sns-cli-script`.

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” account.

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 fwadmin-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,
 - the --force parameter, to force the disconnection of users connected to the web interface when the script has been scheduled to run.

```
[root@smc] - {~} > at 16:00 10/15/2019
warning: commands will be executed using /bin/sh
at> fwadmin-sns-cli-script run monitor_qos.script --all --force
at> fwadmin-sns-cli-script run monitor_stat.script --all --force
```

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.

8.8 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, 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 with the commands described in the following examples, replacing 3.5.1 with the desired version (for more information on the %FW_UPD_SUFFIX% variable, 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
```

 **CAUTION**

In this case, both nodes can be then unavailable at the same time during the update process.

2. In the web interface of the SMC server, select **Scripts > 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 running an update script on a cluster, the automatic synchronization between both nodes performed by the SMC server always fails because the update makes one of the node unavailable. This error can be seen in the **Execution** tab and does not prevent the update from being run.

6. After a few minutes, check in the **Monitoring > Firewalls** panel that the version number has indeed changed in the **Version** column.

8.9 Troubleshooting

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

8.9.1 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))`

8.9.2 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.

8.9.3 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 details.
 - Before running the script, you can view it for a given firewall in the **Firewalls selection** tab. Certain errors may be indicated.

8.9.4 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 ongoing execution or deployment to end.



9. 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.

9.1 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 environment as well at any moment.

9.1.1 Backing up the configuration of the server and firewalls automatically

SMC can automatically and recurrently 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**.

9.1.2 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.

9.2 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](#).

9.3 Replacing firewalls in the case of an RMA

If you need to replace a firewall managed by the SMC server, apply the usual appliance replacement RMA procedure (Return Material Authorization).

After restoring the firewall configuration on the new appliance thanks to the *.na* backup file, the firewall automatically reconnects to the SMC server. No additional action is required, you do not need to generate a new connecting package.

10. Removing SN firewalls from the SMC server

1. To stop administrating 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.

11. Managing and maintaining the SMC server

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

11.1 Defining the SMC server's network interfaces

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 **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](#).

11.2 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 `fwadmin-version`.
3. The following information displays:
 - `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.

11.3 Changing the SMC server time zone and date

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

11.3.1 Changing the time zone

1. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. Enter the command `fwadmin-date-time --timezone "timezone"` to modify 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 `fwadmin-date-time` to check the modification has been properly applied.

11.3.2 Changing the date manually

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

11.3.3 Changing the date via NTP

To enable NTP on the SMC server:

1. Enter the command
`fwadmin-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.

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

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

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

11.4 Managing administrators

To manage the authentication of the administrators on the SMC server, there are two possibilities:

- 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.

11.4.1 Managing administrators in the web interface

Go to **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. Read-only administrators don't see configuration updates in real-time; they must refresh the browser page to do so.
-------------------------------------	--------------------------	--

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.

11.4.2 Authorizing administrators to connect via an LDAP server

The SMC server can be connected to an LDAP server to authorize the company's users to manage a pool of firewalls.

This type of authentication is intended to work with a LDAP server like Active Directory on Microsoft Windows Server 2012.

Authentication via LDAP server is configured in the SMC server's command line interface with two files:

- An *ldap-server.ini* configuration file that enables the LDAP server connection settings to be defined,
- An *ldap-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 server, follow the three steps below:

1. Configure the connection to the LDAP server,
2. Test the connection and display the list of users and groups on the LDAP server,
3. Authorize users and define their access privileges.

Configuring the connection to the LDAP server

To configure the connection to the LDAP server, modify the *ldap-server.ini* file located in the SMC server's directory `/data/config/users`.

1. Connect to the SMC server via the console port or SSH connection with the "root" account
2. Go to the `/data/config/users/` directory,
3. As a precaution, save the *ldap-server.ini* file before modifying it,

4. Modify the *ldap-server.ini* file by filling in the following parameters provided by the LDAP server administrator:

Field	Description
type	Active Directory type server
host	IP address or FQDN of the LDAP server. If this field is empty, LDAP 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 LDAP server: if SSL is enabled, port 636 by default; otherwise, port 389.
baseDN	baseDN allowing access to the LDAP server and using the following format: dc=sub,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 <code>true</code> , the connection to the LDAP server is secure via SSL/TLS protocols. When SSL is enabled, the default port is modified as a result. If SSL is enabled, the SMC server does not verify the certificate authority that signed the LDAP server's certificate by default. For more information, refer to the section Verifying the certificate of the certificate authority when the SSL protocol is enabled .

Example of the *ldap-server.ini* file:

```
[server]
type=activeDirectory
host=ldap.mycompany.com
port=636
baseDn="dc=mydomain, dc=com"
login="admin"
password="secret"
ssl=true
```

Listing users and groups found on the LDAP server

The `fwadmin-ldap-check` command sends a request to the LDAP server and:

- verifies that the syntax of the *ldap-server.ini* file is correct,
- verifies that the network configuration of the SMC server allows it to contact the LDAP server,
- verifies that the ID and password defined in the *ldap-server.ini* file are correct,
- and lists the users and groups on the server according to the configuration specified in the *ldap-server.ini* file.

To see the list of users and groups:

1. Connect to the SMC server via the console port or SSH connection with the “root” account,
2. Enter the `fwadmin-ldap-check` command.

The `fwadmin-ldap-check` command lists all users and groups found on the LDAP server with the `baseDn` configuration provided in the *ldap-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	Restricts the search to group names only
groups	
--no-lookup	Will not display all users. This option makes it possible to test connectivity with the LDAP server according to the configuration provided in the <i>ldap-server.ini</i> file.

--filter Filters results according to a specified text. This option makes it possible to list all users and <text> groups that contain the specified text.

When configuring the *ldap-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.

Authorizing users or groups

Create the *ldap-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.

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. Connect to the SMC server via the console port or SSH connection with the “root” account,
2. Recover the example file in `/var/fwadmin/examples/csv/example-ldap-rights.csv`,
3. Place it in the `/data/config/users` directory,
4. Modify the file by filling in the following parameters:

Field	Authorized values	Description
type	user or group	Determine whether the Distinguished Name (DN) is a user or a group.
dn	example: CN=intern,OU=some-organization-unit,DC=mycompany,DC=com	Distinguished Name of the user or group as displayed using the <code>fwadmin-ldap-check</code> 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 the 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 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 is 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.

Example of the *ldap-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
```

 **NOTE**

Recursive groups are not supported. If a user group contains a subgroup, the members of this subgroup cannot access the SMC server.

Verifying the certificate of the certificate authority when the SSL protocol is enabled

If you activate the SSL protocol in the *ldap-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 certificate 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 *ldap-server.ini* file,
4. Restart the SMC server using the `nrestart fwadmin-server` command to apply the configuration.

If there is a problem with the certificate authority, the `fwadmin-ldap-check` command displays the related error.

Forcing a connection to the SMC server via LDAP

When an administrator tries to connect, the SMC server looks for the ID and password in its local user database first and then on the LDAP server, if it does not find this information. In the event IDs and passwords are the same, the local user database has priority over the LDAP server.

However, you can ignore the local database and force a connection via LDAP:

- In the **Login** field on the SMC server's login page, use the syntax `identifier@domain` where the domain corresponds to the `baseDn` field defined in the *ldap-server.ini* configuration file.
Example: `john@mycompany.com`

11.5 Consulting the SMC server logs

The SMC server provides two types of log files:

- *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 command line interface using the `alogs` command.

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](#).

To view the *server.log* logs from the web interface:

1. Display and hide the logs from the *server.log* file at any time by clicking the logs button  at the right top of the interface or by clicking the black arrow at the bottom of the interface 
2. Move the cursor to select the minimum traces to display, from the less to the more critical: debug, information, warning or error.
A maximum of 1000 lines can be displayed. When the limit is reached, old logs are replaced by new ones in the interface.

3. To view the contents of the entire log file, connect to the SMC server via the console port or in SSH with the "root" user account and enter the command `nlogs`.

11.6 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. Connect to the SMC server via the console port or SSH connection with the "root" user.
2. Enter the command `fwadmin-syslog-ng`. The service's current configuration will appear.

11.6.1 Sending logs to a remote server without encryption

1. Type the command `fwadmin-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.

11.6.2 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 certificate 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 `fwadmin-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/`.

11.6.3 Disabling the sending of logs to a remote server

1. Type the command `fwadmin-syslog-ng --wizard` to select an operating mode.
2. Select the option **Store logs locally in `/var/log/messages` (default)**.

11.6.4 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=xxxx.xxxx.xxxx.xxxx
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
```

11.7 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.



The following restriction applies to the restoration of 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](#).

11.7.1 Saving the server configuration from the web interface

In **SMC Server > Maintenance**, click **Save configuration** in the **Save server configuration** pane.

Save server configuration

Include the configuration history in the backup archive

Save configuration

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 server configuration from the web interface](#), [Restoring server configuration from the command line interface](#) and [Restoring server configuration from the initialization wizard](#).

11.7.2 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
`fwdadmin-config-backup`
 The name of the archive name is displayed.
3. To save the configuration without the deployment history, enter the command
`fwdadmin-config-backup --no-history`

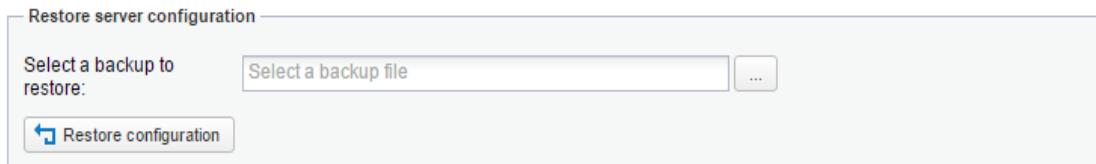
The configuration backup file can be restored from:

- The SMC server web interface,
- The command line interface,
- The SMC server initialization wizard.

For more information, refer to sections [Restoring server configuration from the web interface](#), [Restoring server configuration from the command line interface](#) and [Restoring server configuration from the initialization wizard](#).

11.7.3 Restoring server configuration from the web interface

In **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](#).

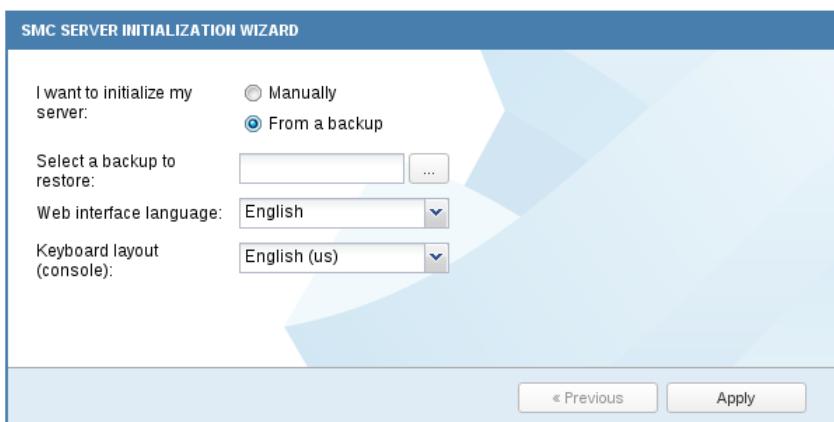
11.7.4 Restoring server configuration from the command line interface

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
`fwdadmin-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](#).

11.7.5 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.

11.8 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.

11.8.1 Downloading the report from the web interface

1. In **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.

11.8.2 Downloading the report in command line

1. Connect to the SMC server via the console port or SSH connection with the "root" account.
2. Enter the command `fwadmin-diag` or `fwadmin-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.

11.9 Updating the SMC server from the command line interface

An update archive is required to update the SMC server. Archiving involves the update of the web interface and of the operating system.

During the update process, firewalls continue to run. Firewalls do not need to be updated.

During each update, the unified configuration file will be migrated to the new version of the server. This file will be automatically updated on the older system before the migration process begins.

To update the server:

1. Download the upload 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 `fwadmin-update -u /var/tmp/archivename`. Replace `archivename` with the name of your archive.
5. Wait for the completion of the update. During the process, the server remains available within the current version.
6. Enter the command `reboot`. The updated system restarts.

For any specific information regarding updates between two versions, please refer to the [SMC release notes](#).

11.10 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.

11.10.1 Resetting the "root" administrator password

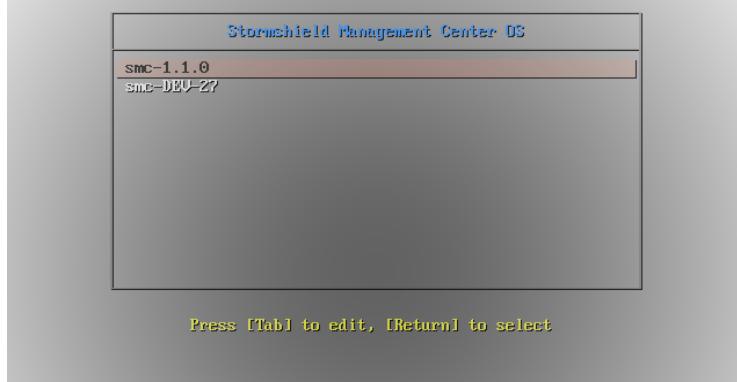


WARNING

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.

Modifying the 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.

11.10.2 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:
 - `fwadmin-ui-password --password myNewPassword` to modify the main "admin" administrator password,
 - `fwadmin-ui-password --username myOtherUser --password myNewPassword` to modify the main "admin" administrator password,

11.11 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 `fwadmin-server` service with the command `nrestart fwadmin-server`

11.12 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 `fwadmin-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`.

11.12.1 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	fwadmin-snmp enable
View the status of the service	fwadmin-snmp status
Restart the service	fwadmin-snmp reload
Disable the service	fwadmin-snmp disable

11.12.2 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	.1.3.6.1.2.1.2
	RFC 2863	.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

11.13 Customizing the certificate of the SMC server web interface

11.13.1 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`.

11.13.2 Reinitializing the certificate

To revert to factory settings, use the command `fwadmin-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.

Appendix A. Details of fwadmin-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 fwadmin-xxx commands that have not been mentioned in this list as they are solely intended for the internal operations of the server.

Command	Action
fwadmin-config-backup	Saves the configuration of the SMC server. See section Saving the server configuration from the command line interface .
fwadmin-config-restore	Restores the configuration of the SMC server. See section Restoring server configuration from the command line interface .
fwadmin-date-time	Displays and configures the system's date, time and time zone. See section Changing the SMC server time zone and date .
fwadmin-deploy	Deploys the configuration on the SN firewalls. See section Deploying a configuration on firewalls .
fwadmin-diag	Downloads a SMC server diagnostics report. See section Generating a server diagnostics report .
fwadmin-firewalls-and-packages	Creates firewalls in SMC and their connecting package. See section Importing SN firewalls from a CSV file .
fwadmin-gen-ui-cert	Reset the certificate presented by the SMC server's web interface. See section Customizing the certificate of the SMC server web interface .
fwadmin-import-crl	Imports a Certificate Revocation List (CRL). The CRL is automatically linked to the certification authority which signed it.
fwadmin-import-objects	Imports network objects originating from a firewall export in CSV format. See section Importing objects from a CSV file .
fwadmin-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 .
fwadmin-install-certificate	Installs a P12 certificate on a firewall. See section Importing or declaring a certificate for a firewall .
fwadmin-keyboard	Changes the language of the keyboard in the command line interface.
fwadmin-ldap-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 Authorizing administrators to connect via an LDAP server .
fwadmin-logs	Displays logs of all actions saved on the SMC server. Equivalent to the nlogs command.
fwadmin-monitor	Displays configurations pending deployment.
fwadmin-server	Shuts down/starts/restarts the service that manages the SMC web server by using the commands nstop, nstart and nrestart. Before shutting down the service, the monit service must also be shut down with nstop monit. To restart this service: nstart monit.
fwadmin-snmp	Configures the SNMP service. See section Monitoring SMC with SNMP .
fwadmin-sns-cli-script	Runs SNS CLI commands on a pool of firewalls. See section Running SNS CLI commands on an environment of firewalls .
fwadmin-syslog-ng	Configures the logging service in Syslog format. See section Sending SMC logs to a remote server in Syslog format .
fwadmin-ui-password	Modifies the password of the user on the SMC server's web interface. See section Resetting the administrator password .
fwadmin-update	Updates the SMC server. See section Updating the SMC server from the command line interface .
fwadmin-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 recaps 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
VPN	2.0	3.0
Router and time objects	2.1.0	3.1
Editing the firewalls output interface	2.2.0	3.3.0
Multiple addresses to contact SMC specified in the connecting package	2.2.1	3.3.0
SMC as CRL distribution point	2.2.1	3.3.0
Health indicators	2.5	3.6.0
"Responder-only" mode in star VPN topologies	2.5	3.6.0
AES GCM 16 encryption algorithm	2.5	3.6.0
Importing filter and NAT rule from the web interface	2.5	3.3

**STORMSHIELD**documentation@stormshield.eu

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

Copyright © Stormshield 2019. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.