GUIDE

STORMSHIELD MANAGEMENT CENTER

ADMINISTRATION GUIDE

Version 3.8

Document last updated: September 22, 2025

Reference: sns-en-SMC-administration_guide-v3.8

Table of contents

1. Getting started with the SMC server ... 8
1.1 Connecting to the SMC server's web interface ... 8
1.2 Connecting to the command line interface ... 8
1.3 Installing the SMC license ... 10
1.3.1 Troubleshooting ... 10
1.4 Recommendations on the operating environment ... 10
1.4.1 Recommendations ... 11
1.4.2 Configurations and usage mode subject to the evaluation of SNS firewalls ... 13
1.5 User awareness ... 16
1.5.1 Administrator management ... 16
1.5.2 User password management ... 17
1.5.3 Work environment ... 18
1.5.4 User access management ... 18
1.6 Warning before connecting SNS firewalls to the SMC server ... 18
2. Connecting SNS firewalls to the SMC server ... 20
2.1 Connecting a firewall with a factory configuration to the server ... 20
2.1.1 Declaring the firewall in the SMC server web interface ... 20
2.1.2 Building the firewall connecting package ... 21
2.1.3 Installing the connecting package on the firewall from a USB drive ... 22
2.2 Connecting a firewall already in production to the server ... 23
2.2.1 Declaring the firewall in the SMC server web interface ... 23
2.2.2 Building the firewall connecting package ... 23
2.2.3 Installing the connecting package on the firewall ... 25
2.3 Connecting a high availability cluster to the server ... 25
2.3.1 Declaring the cluster in the SMC server web interface ... 25
2.3.2 Building the cluster connecting package ... 26
2.3.3 Installing the connecting package on the active node of the cluster ... 27
2.4 Troubleshooting with the server's logs ... 28
2.4.1 Generating a firewall's connecting package ... 28
2.4.2 Installing the connecting package on the firewall ... 28
2.5 Importing SNS firewalls from a CSV file ... 28
2.5.1 Creating the CSV file ... 28
2.5.2 Importing firewalls from the web interface ... 29
2.5.3 Importing firewalls in command line ... 30
3. Monitoring SNS firewalls ... 31
3.1 Monitoring and organizing firewalls ... 31
3.1.1 Getting information about firewalls ... 31
3.1.2 Exporting monitoring data ... 32
3.1.3 Organizing firewalls by folders ... 33
3.1.4 Checking usage of a firewall in the configuration ... 34
3.2 Accessing the firewall monitoring interface ... 34
3.3 Accessing the Stormshield Log Supervisor (SLS) server ... 34
3.3.1 Adding a menu to access the SLS server ... 35
3.3.2 Filtering the SLS view by a firewall's logs ... 35
4. Configuring SNS firewalls ... 36
4.1 Editing firewall settings ... 36
4.1.1 Adding custom properties ... 37

4.1.2 Editing the value of a custom firewall property 38
4.1.3 Importing/exporting custom firewall properties 38
4.2 Creating custom variables 39
4.2.1 Adding, changing or deleting customized variables 40
4.2.2 Defining the value of a customized variable for a firewall 40
4.3 Verifying configuration consistency 41
4.3.1 Disabling the consistency check 41
4.3.2 Disabling check areas and changing the anomaly level 41
4.3.3 Restricting the number of inconsistencies reported 42
4.4 Deploying a configuration on firewalls 42
4.4.1 Deploying a configuration on a firewall from the web interface 43
4.4.2 Deploying a configuration on a high availability cluster 44
4.4.3 Deploying a configuration on a firewall in command line 44
4.4.4 Enabling warnings when configurations are modified 44
4.4.5 Keeping the connection alive during deployment 45
4.4.6 Troubleshooting with the server's logs 46
4.4.7 Troubleshooting 46
4.5 Completing the configuration of firewalls with a CSV file 46
4.5.1 Creating the CSV file 46
4.5.2 Importing the CSV file into SMC 47
4.6 Loading and deploying a former configuration 47
4.7 Generating a configuration comparison 48
4.8 Detecting changes to the local configuration on firewalls 48
4.8.1 Viewing local changes on a firewall 49
4.9 Accessing the web administration interface of firewalls 49
4.10 Using the Emergency mode 49
4.11 Converting a firewall connected to the SMC server into a high availability cluster 50
4.12 Importing or declaring a certificate for a firewall 50
4.12.1 Importing a certificate from the server's web interface 50
4.12.2 Importing a certificate from the command line interface 51
4.12.3 Importing a certificate on a high availability cluster 52
4.12.4 Troubleshooting 52
4.12.5 Declaring a certificate used by a firewall 53
4.12.6 Changing the certificate used by default in VPN topologies 53
4.13 Using SMC as an Active Update distribution point 53
4.13.1 Downloading Active Update databases 54
4.13.2 Using the SMC Active Update server 55
4.13.3 Customizing Active Update settings 57
4.14 Configuring the warning for an imminent certificate expiry 59
4.15 Configuring the warning for the imminent expiry of license options 60
4.16 Disabling TPM (Trusted Platform Module) certificate protection during installation on the firewall 60
4.16.1 Finding out whether a private key is TPM-protected 60
4.16.2 Disabling TPM private key protection 61
4.16.3 Enabling TPM protection on existing private keys 61
4.17 Choosing the separator character in CSV files 62

5. Managing objects 63

5.1 Deploying objects on firewalls 63
5.2 Creating variable objects 64
5.3 Checking usage of an object in the configuration 65
5.4 Importing objects 65
5.4.1 Creating the CSV file 66

5.4.2 Importing objects from the web interface ... 66
5.4.3 Importing objects in command line ... 67
5.5 Exporting objects ... 68
5.6 Using dynamic objects from SMC ... 68

6. Configuring the network and routing ... 69
6.1 Configure network interfaces ... 69
6.1.1 Enabling SMC to manage an SNS firewall's network ... 69
6.1.2 Forcing the retrieval of the firewall's interfaces ... 70
6.1.3 Configuring interfaces ... 70
6.1.4 Configuring IPsec interfaces (VTI) ... 71
6.2 Configuring routing ... 72
6.2.1 Configuring routes from SMC ... 72
6.2.2 Forcing the retrieval of the firewall's routes ... 73
6.2.3 Importing and exporting routes ... 74
6.2.4 Limitations to the route configuration from the SMC server ... 75
6.3 Monitoring router objects ... 75
6.4 Implementing SD-WAN ... 75
6.4.1 Creating an SLA object ... 76
6.4.2 Configuring link monitoring in a router object ... 77
6.5 Troubleshooting ... 78
6.5.1 If you notice configuration errors after having renamed an interface from SMC ... 78

7. Creating and monitoring VPN tunnels ... 79
7.1 Creating policy-based VPN topologies ... 79
7.1.1 Configuring a policy-based mesh topology ... 80
7.1.2 Configuring a policy-based star topology ... 82
7.2 Creating route-based VPN topologies ... 84
7.2.1 Configuring a route-based mesh topology ... 86
7.2.2 Configuring a route-based star topology ... 88
7.2.3 Defining IPsec VTIs on SNS firewalls ... 90
7.2.4 Defining the traffic routing policy ... 90
7.2.5 Editing the VTI network pool ... 91
7.2.6 Troubleshooting ... 93
7.3 Managing certificates and certification authorities ... 93
7.3.1 Adding a certification authority or chain of trust ... 94
7.3.2 Updating a certificate authority or chain of trust ... 94
7.3.3 Deleting a certificate authority or chain of trust ... 95
7.3.4 Importing or declaring a certificate for a firewall ... 95
7.3.5 Checking certificate validity ... 95
7.3.6 Updating a firewall's X509 certificate ... 96
7.3.7 Renewing firewall certificates obtained via SCEP or EST ... 96
7.3.8 Explanations regarding certificate statuses ... 97
7.4 Defining the contact IP address of firewalls for VPN topologies ... 98
7.4.1 Defining a firewall's default contact address ... 98
7.4.2 Defining a firewall's contact address in a specific VPN topology ... 98
7.5 Selecting the output interface of firewalls for VPN topologies ... 98
7.5.1 Creating the Host Object that corresponds to the interface ... 99
7.5.2 Selecting a firewall's output interface on SMC ... 99
7.5.3 Configuring a static route on the firewall (optional) ... 99
7.6 Editing, deleting and checking usage of a VPN topology ... 100
7.7 Managing packet fragmentation ... 100
7.8 Disabling a VPN topology ... 101

7.9 Monitoring the status of VPN tunnels 101
7.10 Setting the PRF in a custom encryption profile 102

8. Creating filter and NAT rules 103
8.1 Understanding the order in which rules are read 103
8.2 Use case examples 104
8.2.1 Managing an environment without rule sharing 104
8.2.2 Managing an environment with shared and specific rules 104
8.2.3 Managing a multi-site environment with shared and specific rules and delegated filtering 105
8.2.4 Managing a multi-site pool with shared rule sets 106
8.3 Creating filter and NAT rules 107
8.4 Creating rule sets 108
8.4.1 Creating a rule set 108
8.4.2 Assigning rule sets to a firewall 108
8.4.3 Editing rule sets for a firewall 109
8.4.4 Importing or exporting rule sets 109
8.4.5 Deleting rule sets 109
8.5 Identifying the rules 109
8.6 Changing the order in which rules are executed 110
8.7 Searching for a rule in the web interface or in SNS logs 110
8.8 Removing rules 111
8.9 Removing rule sets 111
8.10 Importing and exporting filter and NAT rules 111
8.10.1 Importing rules from a CSV file 111
8.10.2 Exporting rules to a CSV file 113
8.10.3 Importing rules from connected firewalls 114
8.11 Migrating local rules on a firewall to manage them in SMC 114
8.12 Managing URL filtering on SNS firewalls from SMC 115
8.12.1 Creating the template URL filtering policy 116
8.12.2 Saving the URL filtering policy of the template firewall 116
8.12.3 Deploying the template URL filtering policy 117
8.13 Managing IPS Inspection profiles on SNS firewalls from SMC 118
8.13.1 Editing the template IPS Inspection profiles 119
8.13.2 Saving the IPS Inspection profiles of the template firewall 120
8.13.3 Deploying the IPS Inspection profiles 121
8.14 Adding web services 122
8.14.1 Finding out the names of web services to be used 122
8.14.2 Adding web services on the SMC server 123

9. Configuring QoS 125
9.1 Configuring queues and traffic shapers 125
9.1.1 Adding queues and traffic shapers 125
9.1.2 Changing and deleting queues and traffic shapers 127
9.2 Configuring QoS on firewall interfaces 127
9.2.1 Requirements 127
9.2.2 Enabling SMC to manage an SNS firewall's network 127
9.2.3 Configuring QoS on an interface 128
9.2.4 Forcing the retrieval of the QoS configuration on a firewall 128
9.3 Configuring QoS in filter rules 128

10. Running SNS CLI commands on an environment of firewalls 129
10.1 Creating the CLI command script 129
10.2 Using variables 130

10.2.1 Using variables specific to firewalls ... 130
10.2.2 Using global variables ... 130
10.2.3 Using a CSV file ... 130
10.3 Running the SNS CLI script from the web interface ... 131
10.4 Running the SNS CLI script in command line ... 132
10.4.1 Displaying the list of commands and options ... 132
10.4.2 Running a script ... 132
10.4.3 Adding scripts ... 133
10.4.4 Deleting scripts ... 133
10.4.5 Displaying the list of scripts ... 133
10.4.6 Examples of the use of scripts in command line with a CSV file ... 133
10.5 Running the SNS CLI script on a high availability cluster ... 135
10.6 Attaching files to a script and receiving files generated by script ... 135
10.6.1 Command arguments to be used in the script ... 135
10.6.2 Attaching files to a script ... 136
10.6.3 Receiving files generated by a script ... 136
10.7 Scheduling the execution of SNS CLI scripts ... 137
10.7.1 Scheduling the execution of scripts from the web interface ... 137
10.7.2 Scheduling the execution of scripts in command line ... 138
10.8 Updating firewalls by using SNS CLI scripts ... 139
10.9 Troubleshooting ... 140
10.9.1 The script file is too large ... 140
10.9.2 Certain characters are not supported in the script ... 140
10.9.3 The script fails to run on certain firewalls ... 140
10.9.4 Scripts cannot be executed ... 140

11. Maintaining SNS firewalls ... 141
11.1 Backing up the configuration of firewalls ... 141
11.1.1 Backing up the configuration of the server and firewalls automatically ... 141
11.1.2 Backing up the configuration of firewalls manually ... 142
11.1.3 Excluding private keys from automatic firewall backups ... 142
11.2 Updating firewalls ... 142
11.3 Replacing an SNS firewall through an RMA ... 144

12. Removing SNS firewalls from the SMC server ... 145

13. Managing and maintaining the SMC server ... 146
13.1 Defining the SMC server's network interfaces ... 146
13.2 Verifying the SMC server version in command line ... 146
13.3 Changing the SMC server time zone and date ... 146
13.3.1 Changing the time zone ... 146
13.3.2 Changing the date manually ... 147
13.3.3 Changing the date via NTP ... 147
13.3.4 Displaying a comprehensive summary of the SMC server's date/time ... 147
13.4 Managing administrators from local and external directories ... 147
13.4.1 Managing administrator privileges as super administrator ... 149
13.4.2 Managing local administrators ... 149
13.4.3 Managing LDAP users ... 151
13.4.4 Managing Radius users ... 156
13.4.5 Restricting folder administrators' access privileges ... 159
13.4.6 Troubleshooting ... 162
13.5 Viewing SMC server logs ... 162
13.6 Sending SMC logs to a remote server in Syslog format ... 163

13.6.1 Sending logs to a remote server without encryption ... 163
13.6.2 Sending logs to a remote server with encryption ... 163
13.6.3 Disabling the sending of logs to a remote server ... 163
13.6.4 Troubleshooting ... 163
13.7 Saving and restoring the SMC server configuration ... 164
13.7.1 Saving the server configuration from the web interface ... 164
13.7.2 Saving the server configuration from the command line interface ... 165
13.7.3 Restoring server configuration from the web interface ... 165
13.7.4 Restoring server configuration from the command line interface ... 166
13.7.5 Restoring server configuration from the initialization wizard ... 166
13.8 Generating a server diagnostics report ... 166
13.8.1 Downloading the report from the web interface ... 166
13.8.2 Downloading the report in command line ... 167
13.9 Updating the SMC server ... 167
13.9.1 Updating the SMC server from the web interface ... 167
13.9.2 Updating the SMC server in command line ... 168
13.10 Disabling automatic synchronization of high availability clusters ... 168
13.11 Monitoring SMC with SNMP ... 168
13.11.1 Using the SNMP service ... 168
13.11.2 Using MIBs ... 169
13.12 Customizing the certificate of the SMC server web interface ... 169
13.12.1 Customizing the certificate ... 169
13.12.2 Reinitializing the certificate ... 170
13.13 Resetting the internal certification authority of the SMC server ... 170
13.14 Using Diffusion Restreinte mode on SNS firewalls ... 170
13.14.1 Enabling the consistency check for the “Diffusion Restreinte” mode ... 171
13.14.2 Enabling Diffusion Restreinte mode on SMC and firewalls ... 172
13.14.3 Disabling Diffusion Restreinte mode on SMC and firewalls ... 172
13.15 Adding a disclaimer to the login page ... 172
13.16 Connecting to the command line interface via SSH keys ... 173

14. Enabling and managing SMC's public API ... 174
14.1 Enabling the public API ... 174
14.2 Allowing administrators to create and revoke API keys ... 175
14.3 Editing the API key global policy ... 175
14.4 Creating API keys ... 176
14.5 Revoking API keys ... 177
14.6 Customizing the listening port of the public API ... 177

15. Further reading ... 177

Annexe A. Details of smc-xxx commands ... 178

Annexe B. Details of SMC_XXX environment variables ... 180

Appendix C. Compatibility of SMC/SNS firewalls ... 182

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

1. Getting started with the SMC server

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

SMC also has a public REST API. It is not enabled by default, and only the super administrator can enable it. For more information on SMC's public API, refer to the section Enabling and managing SMC's public API.

If you have forgotten your password, refer to the section Managing administrators from local and external directories and the *SMC Installation guide*.

1.1 Connecting to the SMC server's web interface

1. Connect to the IP address of the SMC server preceded by https://, from one of the following web browsers:
    - Microsoft Edge, latest stable version,
    - Google Chrome, latest stable version,
    - Mozilla Firefox, latest stable version.
2. Enter your login and password, or use the default administrator's login and password. IDs and passwords can originate from LDAP or Radius authentication servers.
   If you make four consecutive mistakes, you must wait for a minute before you can authenticate again. If you attempt to authenticate a fifth time before the minute is up, the waiting time will be extended by another minute, and may increase by up to 10 minutes.

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 from local and external directories.

The SMC server allows:

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

NOTE
We recommend that you customize the certificate of the SMC server web interface. For more information, refer to the section Customizing the certificate of the SMC server web interface.

1.2 Connecting to the command line interface

Some advanced or maintenance operations can only be performed in command line. Connect to the SMC server in to perform these operations. You can connect:

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

In both cases, connect:

- with the "root" username and password specified when you initialized the server. For more information, refer to the *Stormshield Management Center Installation Guide*.
- with your administrator credentials if you hold privileges for console and/or SSH access.

In SSH connections, if you enter the wrong ID five consecutive times, you must wait 15 minutes before you can log in again.

To connect transparently via SSH, you can also configure authentication using SSH keys. For more information, refer to the section Connecting to the command line interface via SSH keys.

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

The default “admin” user does not have access to SMC in console or SSH. Only access to SMC via the web interface is possible.

1.3 Installing the SMC license

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

An SNS high availability firewall cluster requires only one license.

To install the license:

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

1.3.1 Troubleshooting

The SMC server rejects all new firewall connections

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

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

- *Situation*: You have restored the configuration of the SMC server, and your license is no longer valid.
- *Cause*: When a configuration is being restored, the license that was installed at time of the backup will be 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.

1.4 Recommendations on the operating environment

The installation of an SNS firewall and an SMC server is part of implementing a global security policy. To ensure optimal protection of your assets, resources and information, installing an SNS firewall between your network and the Internet or installing an SMC server to help you to configure them correctly are only the first steps. This is mainly because most attacks come from the inside (accidents, disgruntled employees, dismissed employee having retained internal access, etc.).

The following is a list of security recommendations on how to use the SNS firewall and the SMC server.

IMPORTANT

- Check regularly for the Stormshield security advisories on https://advisories.stomshield.eu and for the latest security information regarding Stormshield products on https://security.stormshield.eu/.
- Always apply updates if they fix security flaws on your Stormshield products. Updates are available on https://mystormshield.eu.

1.4.1 Recommendations

Physical security measures

SNS firewalls and the SMC server are must be installed and stored according to the state of the art regarding sensitive security devices: secured access to the premises, shielded cables with twisted pairs, labeled cables, etc.

Organizational security measures

Super administrator

A particular administrator role, the super administrator, displays the following characteristics:

- The only administrator allowed to log on via the local console on SNS firewalls, and only during the installation of the SNS firewall or for maintenance operations outside of normal production use,
- In charge of defining the profiles of other administrators,
- All access to the premises where the SNS firewalls and the SMC server are stored must be under the super administrator's supervision, regardless the purpose of the access is to conduct operations on the SNS firewall or on other equipment. All operations performed will be this administrator's responsibility.

IMPORTANT
The default password of the super administrator must be changed the very first time the SNS firewall is used.

Password

User and administrator passwords must be chosen in such a way that it will take longer to successfully crack them, by implementing a policy that regulates how they are created and verified (e.g., mix of alphanumeric characters, minimum length, inclusion of special characters, no dictionary words, etc.).

Administrators can change their password in the web administration interface of:

- SNS in **Configuration > System > Administrators**, **Administrator account** tab,
- SMC in **Maintenance > SMC Server > Administrators**.

Administrators are aware of these best practices through their duties and are responsible for making users aware of these practices (see the next section User Awareness).

Good information flow control policies

The information flow control policies to be implemented, for equipments on the trusted networks to be protected, are defined as such:

- **Complete**: standard usage scenarios of how equipments are used have all been considered when defining the rules and their authorized limits have been defined,
- **Strict**: only the necessary uses of equipments are authorized,
- **Correct**: rules do not contradict each other,
- **Unambiguous**: the list of rules provides all the relevant elements for direct configuration of the SNS firewall by a qualified administrator.

Cryptographic keys

Cryptographic keys that were generated outside the SNS firewall and injected into it must have been generated according to the general security guidelines defined by the French National

Cybersecurity Agency (ANSSI) in the *Référentiel général de sécurité (RGS)* document (in French).

Human agents

Administrators are non-hostile, competent persons with the necessary means for accomplishing their tasks. They have been trained to perform operations for which they are responsible. Their skills and organization mean that:

- Different administrators with the same privileges do not perform contradictory administrative actions (e.g., inconsistent modifications to the information flow control policy),
- Logs are used and alarms are processed within the appropriate time frames.

IT security environment

SNS firewalls

SNS firewalls are installed in compliance with the current network interconnection policy and are the only passage points between the various networks on which the information flow control policy has to be applied. They are sized according to the capacities of adjacent devices or these devices limit the number of packets per second, set slightly below the maximum processing capacities of each SNS firewalls installed in the network architecture.

Besides the application of security functions, SNS firewalls do not provide any network service other than routing and address translation (e.g., no DHCP, DNS, PKI, application proxies, etc.). SNS firewalls are not configured to forward IPX, Netbios, AppleTalk, PPPoE or IPv6 information flows.

SNS firewalls do not depend on external “online” services (DNS, DHCP, RADIUS, etc.) to apply the information flow control policy.

The IT environment provides:

- NTP reliable timestamps,
- Up to date X.509 certificate revocation status, both for peers and administrators,
- A reliable enrolment infrastructure.

SMC server

A traffic control policy must be applied to the SMC server to allow only its administrators and managed SNS firewalls to log in to it.

The virtual machine must be appropriately scaled (RAM, CPU, disk space) to enable administration on SNS firewalls managed by the SMC server. The SMC operating system must never be modified, so that it can meet needs other than those it was designed to meet.

There must be sufficient and available bandwidth at all times between the SMC server and SNS firewalls so that all administration operations can be performed. The administrator must configure and even disable certain features to meet this requirement, otherwise restrict the number of packets per second to give priority to administration traffic.

The production and distribution of connecting packages, which allow the SMC server to manage SNS firewalls, must be managed and entrusted to individuals who are familiar with security requirements. Such packages must only be shared through secure channels (encrypted e-mails, secured USB keys, etc.) between the SMC server and SNS firewalls.

Interconnectivity

Remote administration workstations are secured and kept up to date on all known vulnerabilities affecting operating systems and hosted applications. They are installed in

premises with protected access and are dedicated exclusively to the administration of SNS firewalls, the SMC server and the storage of backups.

Network appliances with which the SNS firewall sets up VPN tunnels are subject to restrictions regarding physical access control, protection and control over their configuration, equivalent to the restrictions placed on SNS firewalls.

Workstations on which the VPN clients of authorized users are launched are subject to restrictions regarding physical access control, protection and control over their configuration, equivalent to the restrictions placed on workstations in trusted networks. They are secured and kept up to date on all known vulnerabilities affecting operating systems and hosted applications.

1.4.2 Configurations and usage mode subject to the evaluation of SNS firewalls

The usage mode subject to evaluation has the following characteristics.

- The evaluation covers the Stormshield UTM / NG-Firewall Software Suite installed on all versions of Stormshield firewalls, from the SN210 to SN6100 range, including industrial models SNi20 and SNi40. Certain models do not have large local log storage capacities and have to send events via syslog,
- SNS firewalls have to be stored in a location with secured access. Such measures, as well as organizational procedures for the operating environment, have to guarantee that the only physical access to the SNS firewalls take place under the surveillance of the super administrator,
- The local console is not used in production. Only the super administrator can log on to it, and hypothetically, such interventions are performed only when a decision has been made to make an exception to the operating context – to conduct a maintenance operation or a re-installation,
- Workstations on which the web administration interface will be used are secured, dedicated to such use, and up to date on all patches concerning the respective operating systems and the applications installed on them,
- The Stormshield Network IPsec VPN Client software is not part of the evaluation. Users can use an IPsec VPN client of their choice, however, these client workstations have to be secured as rigorously as remote administration workstations,
- When external services are used by the SNS firewall, they are not part of the evaluation. However, these servers have to be dedicated to such use, and up to date on all patches concerning the respective operating systems and the applications installed on them. External services are:
  - The NTP time servers,
  - The LDAP administrator and IPSec user directory server,
  - The syslog server,
  - The CRL or OCSP server,
  - The SMC server,
  - The EST certificate enrolment server.

- Those configuration parameters must remain in their factory (default) states:
  - CRLs: regularly downloaded from a CRL server,
  - Internal clock: regularly synchronized with NTP servers,
  - NSRPC administration services (port 1300/TCP): restricted to loopback,
  - IPv6 routing feature: even though it is supported, the IPv6 feature is disabled by default and must remain so for the duration of the evaluation,
  - ESP Anti-replay windows, IKE re-authentication and IKE PFS (Perfect Forward Secrecy): activated,
  - Maximum SA lifetimes: 24 hours for IKE SA and 4 hours for IPsec SA.
- Those application analysis functions are the only protocols covered by the certification:
  - FTP over TCP,
  - HTTP over TCP (including WebDAV extensions),
  - SIP over TCP or UDP,
  - SMTP over TCP,
  - DNS over TCP or UDP.

  And industrial protocols:
  - OPC UA over TCP,
  - MODBUS over TCP.

  Others must not be used in the running configuration.
- The following parameters must not be used in filter policy to associate a filter rule with:
  - An application inspection (HTTP, SMTP, POP3 and FTP proxies),
  - A schedule (Time object),
  - The "decrypt" action (SSL proxy),
  - A host reputation,
  - An FQDN object in source or destination (require external DNS services).
- The following features may be used, but are not considered security functions:
  - Address translation (network address translation or NAT),
  - Quality of Service,
  - High availability,
  - Embedded reports,
  - Filtering based on Geolocation and IP Reputation,
  - Filtering based on MAC address (Ethernet level),
  - Active Update.

- The usage mode subject to evaluation excludes the fact that the SNS firewall relies on services other than previously mentioned services. The optional modules provided by Stormshield to manage these services are disabled by default and have to stay that way. Specifically, these are:
  - Modules that allow handling external servers (e.g., Kerberos, RADIUS, etc.),
  - The dynamic routing module,
  - The static multicast routing module,
  - The internal public key infrastructure (PKI),
  - The SSL VPN module (Portal and Tunnel),
  - DNS cache,
  - Antivirus engines,
  - SSH, DHCP, MPD and SNMPD servers,
  - The DHCP client,
  - The DHCP relay,
  - Wifi connection for equipped devices,
  - Host reputation,
  - For SNi40 and SNi20 models: the hardware bypass capabilities,
  - Any custom IPS patterns,
  - FQDN objects (require external DNS services),
  - IPFIX messages,
  - Telemetry,
  - Breathfighter (Sandboxing),
  - Network Vulnerability Manager (SNVM).

  Administration and monitoring tools provide a way of checking at any moment during operation of these modules are disabled.

- The IKE & IPsec cryptographic algorithms implemented must be:

	Standard IPsec	IPsec DR
Identification	Pre-shared key or Certificate with RSA or ECDSA key (1)	Certificate with ECDSA or ECSDSA key (2) (3)
Authentication/Integrity	SHA-2 256 or 384 or 512 bit	SHA-2 256 bit
Key negotiation	Diffie-Hellman groups 14, 15, 16, 17, 18, 19, 20, 21, 28, 29 and 30 (4)	Diffie-Hellman group 28
Encryption	AES 128 or 192 or 256 bit in CBC or CTR or GCM mode	AES 256 bit in GCM or CTR mode

(1): The smallest size of an RSA key must be 2048 bits, or 3072 bits for use beyond 2030.
(2): The smallest size of a key must be 256 bits.
(3): Although the use of RSA keys is prohibited in a DR environment, an RSA root certificate can be used to sign an intermediate certificate dedicated to IPsec for example, when the certification authority used as the anchor on the firewall is the intermediate certificate.
(4): For use beyond 2030, the smallest group to use must be Diffie-Hellman group 15.

These cryptographic algorithms are needed for compliance with the general security guidelines defined by the French National Cybersecurity Agency (ANSSI) in the *Référentiel général de sécurité (RGS)* document (in French).

Do note that the recommendations on implementing the strengthened IPsec mode called *Diffusion Restreinte (DR) mode* that complies with ANSSI's reference document for IPsec DR are given in the SNS Technical note "IPsec - *Diffusion Restreinte* mode".

1.5 User awareness

1.5.1 Administrator management

The administrator of the VPN firewall or SMC server is in charge of instructing users on network security, the equipment which make up the network and the information which passes through it.

Most users in a network are computer novices and even more so in network security. It is thus incumbent upon the administrator or person in charge of network security to organize training sessions or at least programs to create user awareness of network security.

These sessions should be used to state the importance of managing user passwords and the work environment as well as the management of users' access to the company's resources, as indicated in the following section.

Initial connection to the appliance or SMC server

A security procedure must be followed if the initial connection to the appliance or SMC server takes place through an untrusted network. This operation is not necessary if the administration workstation is plugged in directly to the product.

Access to the administration portal is secured through the SSL/TLS protocol. This protection makes it possible to authenticate the portal via a certificate, thereby assuring administrators that they are indeed logged in to the desired appliance or SMC server. This certificate can either be the appliance's default certificate or the certificate entered during the configuration of the appliance (*Authentication* > *Captive portal*). For the SMC server, refer to Customizing the certificate of the SMC server web interface to replace the default certificate.

1.5.2 User password management

Throughout the evolution of information technologies, numerous authentication mechanisms have been invented and implemented to guarantee that companies' information systems possess better security. The result of this multiplication of mechanisms is a complexity which contributes to the deterioration of company network security today.

Users (novices and untrained users) tend to choose "simplistic" passwords, in general drawn from their own lives and which often correspond to words found in a dictionary. This behavior, quite understandably, leads to a considerable deterioration of the information system's security.

Dictionary attacks being an exceedingly powerful tool is a fact that has to be reckoned with. A study conducted in 1993 has already proven this point. The following is a reference to this study: (http://www.klein.com/dvk/publications/). The most disturbing revelation of this study is surely the table set out below (based on 8-character passwords):

Type of password	Number of characters	Number of passwords	Cracking time
English vocabulary 8 char. and +	Special	250000	< 1 second
Lowercase only	26	208827064576	9-hour graph
Lowercase + 1 uppercase	26/special	1670616516608	3 days
Upper- and lowercase	52	53459728531456	96 days
Letters + numbers	62	218340105584896	1 year
Printable characters	95	6634204312890620	30 years
Set of 7-bit ASCII characters	128	72057594037927900	350 years

Another tendency which has been curbed but which is still happening is worth mentioning: those now-famous post-its pasted under keyboards.

The administrator has to organize actions (training, creating user awareness, etc) in order to modify or correct these "habits".

EXAMPLE

- Encourage your users to choose passwords that exceed 7 characters,
- Remind them to use numbers and uppercase characters,
- Make them change their passwords on a regular basis,
- and last but not least, never to note down the password they have just chosen.

One classic method of choosing a good password is to choose a sentence that you know by heart (a verse of poetry, lyrics from a song) and to take the first letter of each word. This set of characters can then be used as a password.

EXAMPLE
"**S**tormshield **N**etwork, **L**eading **F**rench **m**anufacturer **o**f FIREWALL **a**nd VPN **a**ppliances…"
The password can then be the following: **SNLFmoFaVa**.

The ANSSI (French Network and Information Security Agency) offers a set of recommendations for this purpose to assist in defining sufficiently robust passwords.

1.5.3 Work environment

The office is often a place where many people pass through every day, be they from the company or visitors, therefore users have to be aware of the fact that certain persons (suppliers, customers, workers, etc) can access their workspace and by doing so, obtain information about the company.

It is important that the user realizes that he should never disclose his password either by telephone or by e-mail (social engineering) and that he should type his password away from prying eyes.

1.5.4 User access management

To round up this section on creating user awareness of network security, the administrator has to tackle the management of user access. In fact, the authentication mechanism on a Stormshield Network Firewall or SMC server, like many other systems, is based on a login/password system and does not necessarily mean that when the application enabling this authentication is closed, the user is logged off. This concept may not always be apparent to the uninitiated user. As such, although the application in question has been shut down, the user (who is under the impression that he is no longer connected) remains authenticated. If he leaves his workstation for just a moment, an ill-intentioned person can then usurp his identity and access information contained in the application.

Remind users to lock their sessions before they leave their workstations unattended. This seemingly tedious task can be made easier with the use of authentication mechanisms which automate session locking (for example, a USB token).

1.6 Warning before connecting SNS 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**, **Application settings** section 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.

2. Connecting SNS firewalls to the SMC server

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

IMPORTANT
As a package connects a single firewall to SMC, it must not be reused.

The SMC server 3.8 is compatible with Stormshield Network Security from version 4.3. For further detail, refer to Compatibility of SMC/SNS firewalls.

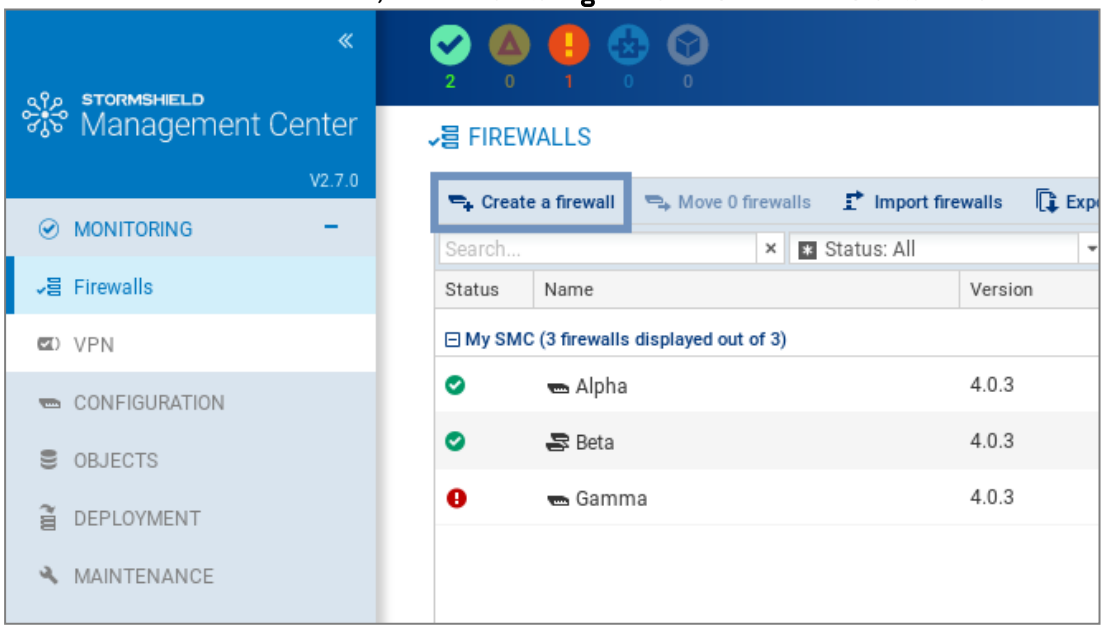
2.1 Connecting a firewall with a factory configuration to the server

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.

2.1.1 Declaring the firewall in the SMC server web interface

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



2. Complete the firewall properties. The **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.

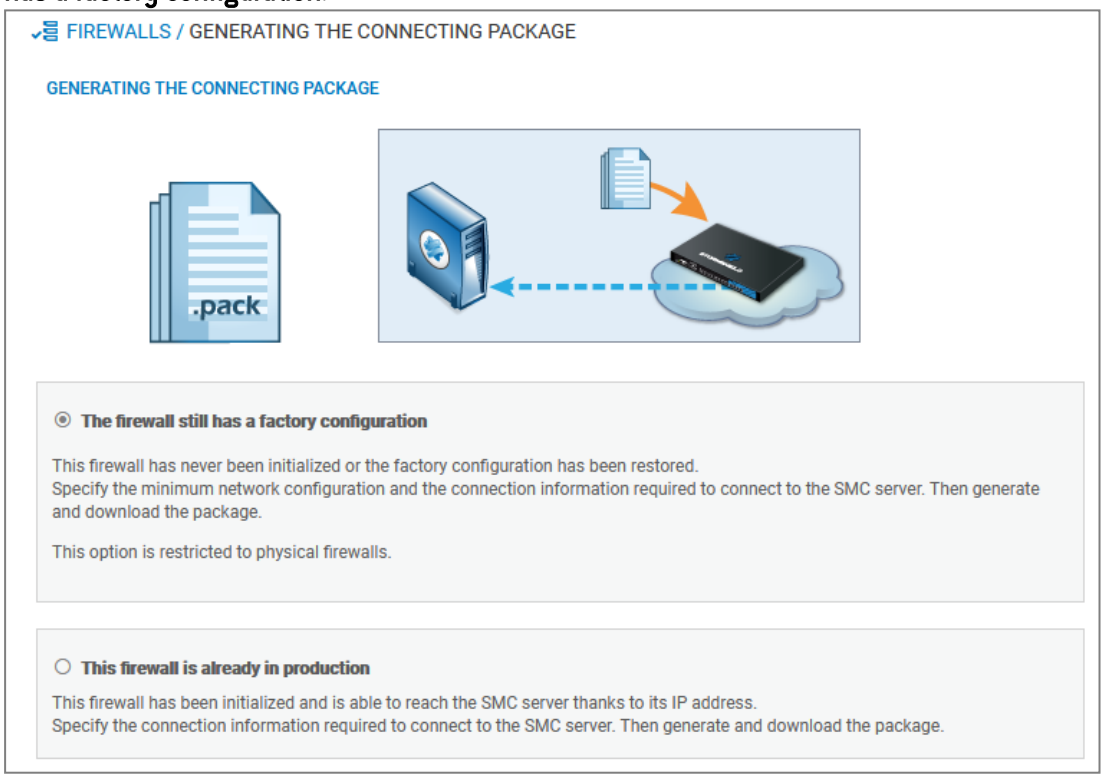
5. Select the folder in which you wish to organize the firewall. Folders are created in the **Configuration** > **Firewalls and folders** menu on the left. For more information, please refer to the section Organizing firewalls by folders. You need to hold write access privileges on the folder. For more information, refer to the section Restricting folder administrators' access privileges.

2.1.2 Building the firewall connecting package

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

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

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



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

5. Fill in the information to connect to the SMC server. According to the firewall version, the panel is not the same. In 3.9.0 and higher versions:
   - **IP address or FQDN**: the firewall connects using these addresses to contact the SMC server. Depending on network topology, they can either be the SMC server's IP addresses or external IP addresses that the firewall can reach, and which are redirected to the SMC server through destination translation. You can set up to ten addresses or FQDNs to contact the SMC server, by order of priority. The firewall browses the addresses from 1 to 10 and connects to the SMC server through the first address reachable. If the address currently used has not the highest priority, the firewall regularly tries to reach an address with greatest priority.
   - **Port**: depending on network topology, they can either be the SMC server's ports (1754 by default) or external ports that the firewall can reach, and which are redirected to the SMC server's port through destination translation.
   - **Local address**: you can specify a different outgoing interface for each contact address.
   - For firewalls in version 3.7.X to 3.8.X, only one outgoing interface can be specified, and which will apply for all contact addresses.
6. Click on **Generate and download**.

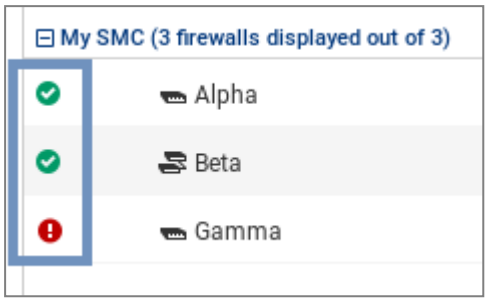
2.1.3 Installing the connecting package on the firewall from a USB drive

IMPORTANT
As a package connects a single firewall to SMC, it must not be reused.

IMPORTANT
The connecting package makes it possible to establish a connection from the firewall to the SMC server. Share this package only with users who have been made aware of security. Such packages must only be shared through secure channels (encrypted e-mails, secured USB keys, etc.) between SMC and SNS firewalls.

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

3. In the SMC server web interface, verify that the state of the firewall changes in the **Firewalls** menu. It must be "On line".



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

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

2.2 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.

2.2.1 Declaring the firewall in the SMC server web interface

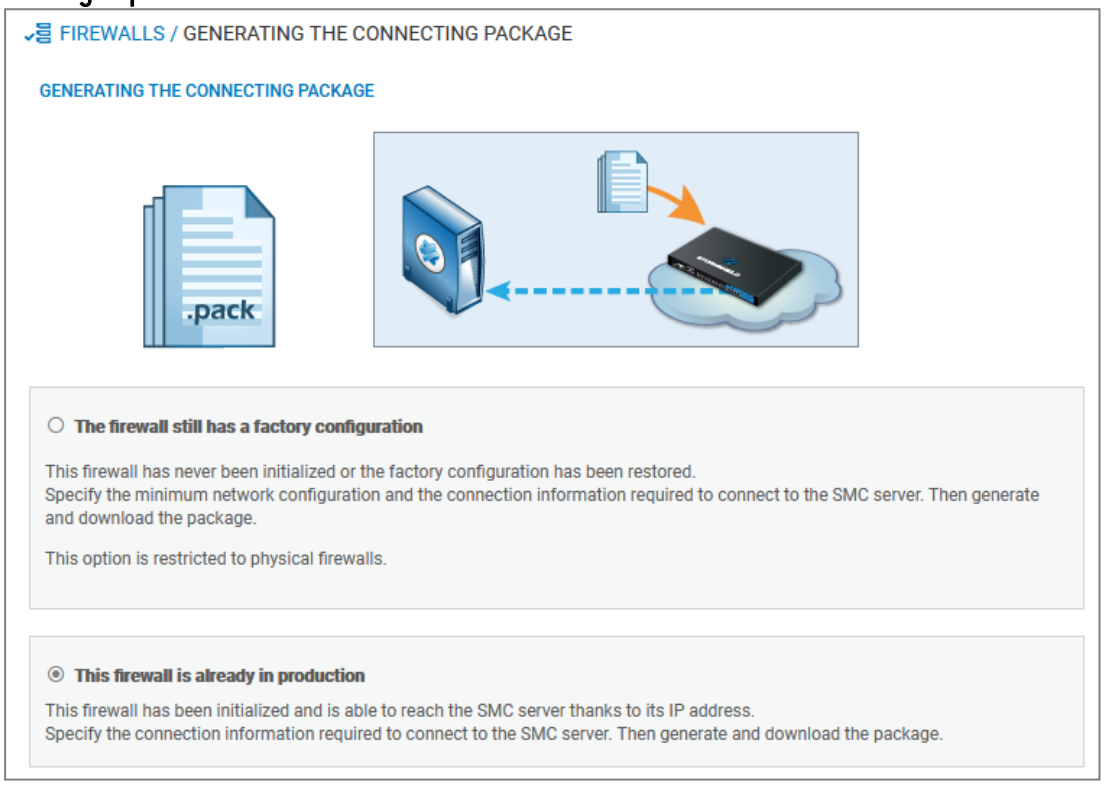
1. In the SMC server web interface, select **Monitoring** > **Firewalls** and click **Create a firewall**.
2. Complete the firewall properties. The **Description** and **Location** fields are just filled in for information and do not have any impact on the configuration.
3. For more information on the 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. You need to hold write access privileges on the folder. For more information, refer to the section Restricting folder administrators' access privileges.

2.2.2 Building the firewall connecting package

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

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

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



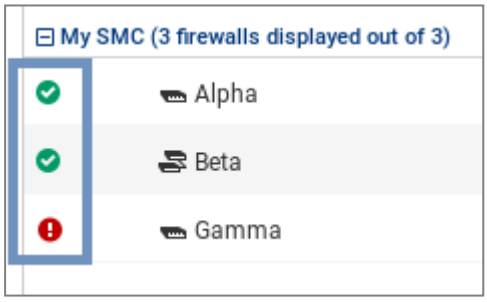
4. On next panel, select the version of the firewall. Verify and edit the information to connect to the SMC server if needed. The panel varies according to the version of the firewall. In 3.9.0 and higher versions:
   - **IP address or FQDN**: the firewall connects using these addresses to contact the SMC server. Depending on network topology, they can either be the SMC server's IP addresses or external IP addresses that the firewall can reach, and which are redirected to the SMC server through destination translation. You can set up to ten addresses or FQDNs to contact the SMC server, by order of priority. The firewall browses the addresses from 1 to 10 and connects to the SMC server through the first address reachable. If the address currently used has not the highest priority, the firewall regularly tries to reach an address with greatest priority.
   - **Port**: depending on network topology, they can either be the SMC server's ports (1754 by default) or external ports that the firewall can reach, and which are redirected to the SMC server's port through destination translation.
   - **Local address**: you can specify a different outgoing interface for each contact address.
   - For firewalls in version 3.7.X to 3.8.X, only one outgoing interface can be specified, and which will apply for all contact addresses.
5. Click on **Generate and download**.

2.2.3 Installing the connecting package on the firewall

IMPORTANT
As a package connects a single firewall to SMC, it must not be reused.

IMPORTANT
The connecting package makes it possible to establish a connection from the firewall to the SMC server. Share this package only with users who have been made aware of security. Such packages must only be shared through secure channels (encrypted e-mails, secured USB keys, etc.) between SMC and SNS firewalls.

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



2.3 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.

2.3.1 Declaring the cluster in the SMC server web interface

1. In the SMC server web interface, select **Monitoring** > **Firewalls** and click **Create a firewall**. The new firewall stands for the cluster; you do not need to declare both nodes of the cluster.
2. Complete the cluster properties. The **Firewall name**, **Description** and **Location** fields are filled in for information only and do not have any impact on the configuration.
3. For more information on the VPN contact address, refer to the section Defining the contact IP address of firewalls for VPN topologies.

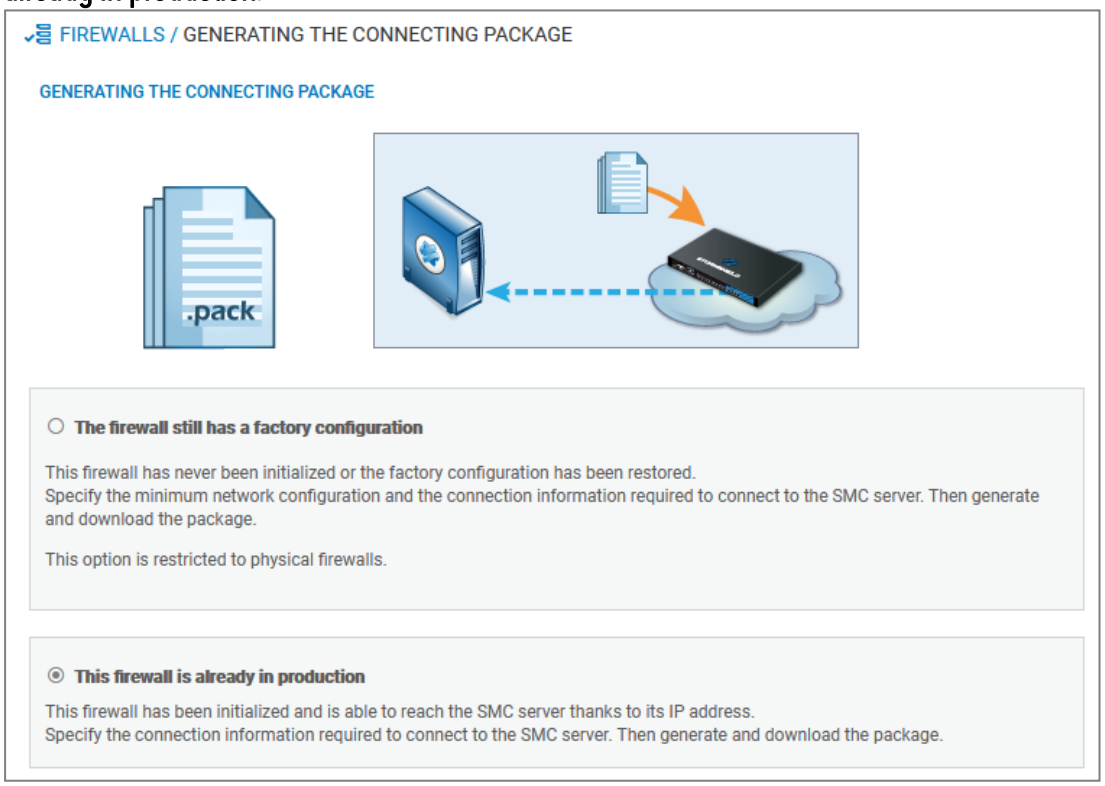
4. For more information on the VPN output interface, refer to the section Selecting the output interface of firewalls for VPN topologies.
5. Select the folder in which you wish to organize the cluster. Folders are created in the **Configuration** > **Firewalls and folders** menu on the left. For more information, please refer to the section Organizing firewalls by folders. You need to hold write access privileges on the folder. For more information, refer to the section Restricting folder administrators' access privileges.

2.3.2 Building the cluster connecting package

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

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

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



4. On next panel, select the version of the firewall. Verify and edit the information to connect to the SMC server if needed. The panel varies according to the version of the firewall. In 3.9.0 and higher versions:
   - **IP address or FQDN**: the firewall connects using these addresses to contact the SMC server. Depending on network topology, they can either be the SMC server's IP addresses or external IP addresses that the firewall can reach, and which are redirected to the SMC server through destination translation. You can set up to ten addresses or FQDNs to contact the SMC server, by order of priority. The firewall browses the addresses from 1 to 10 and connects to the SMC server through the first address reachable. If the address currently used has not the highest priority, the firewall regularly tries to reach an address with greatest priority.
   - **Port**: depending on network topology, they can either be the SMC server's ports (1754 by default) or external ports that the firewall can reach, and which are redirected to the SMC server's port through destination translation.
   - **Local address**: you can specify a different outgoing interface for each contact address.
   - For firewalls in version 3.7.X to 3.8.X, only one outgoing interface can be specified, and which will apply for all contact addresses.
5. Click on **Generate and download**.

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

IMPORTANT
As a package connects a single firewall to SMC, it must not be reused.

IMPORTANT
The connecting package makes it possible to establish a connection from the firewall to the SMC server. Share this package only with users who have been made aware of security. Such packages must only be shared through secure channels (encrypted e-mails, secured USB keys, etc.) between SMC and SNS firewalls.

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

4. To view different types of information about both nodes of the cluster, edit the cluster in the **Firewalls** menu and open the **High availability** tab.

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

2.4 Troubleshooting with the server's logs

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

2.4.1 Generating a firewall's connecting package

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

2.4.2 Installing the connecting package on the firewall

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

2.5 Importing SNS firewalls from a CSV file

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

You have to be a general administrator to perform this operation, i.e., you hold write privileges on all folders in the SMC web interface. For more information, refer to the section Restricting folder administrators' access privileges.

2.5.1 Creating the CSV file

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

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

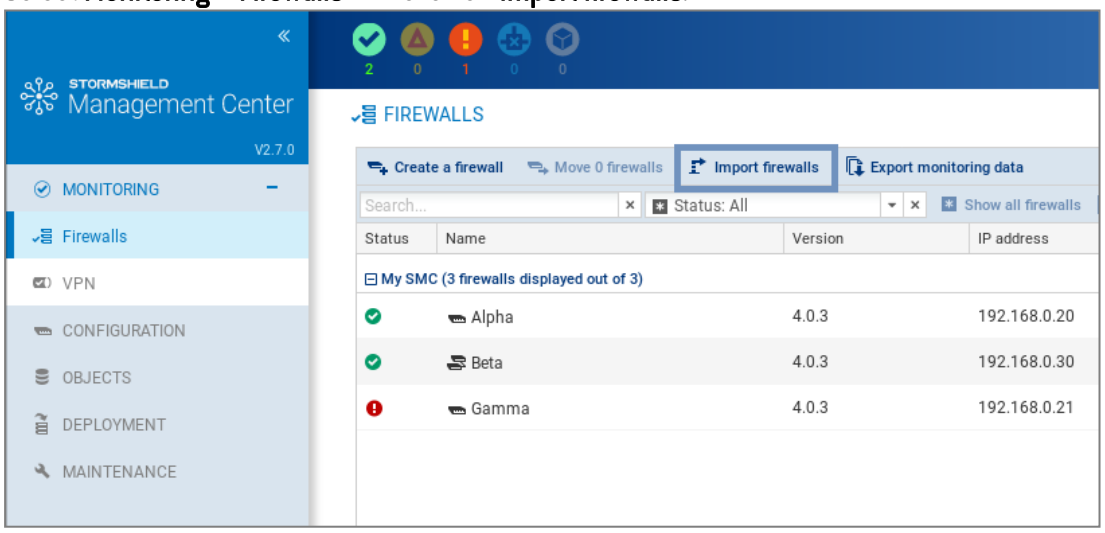
- #fwname: firewall's name,
- #fwversion: version of the firewall used for determining the version of the generated connecting package. If this field is empty, version 4.0.0 will be used.
- #fwdesc: firewall's description,
- #fwplace: location of the firewall,
- #folder: the destination folder of the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

- #network_cfg_deploy: determines whether network interfaces and routing can be managed via the SMC server. If nothing is entered in this field, the option will be disabled by default.
- #pkg_fw_address: contact address of the firewall detected by SMC,
- #pkg_fw_netmask: subnet mask,
- #pkg_fw_gateway: the firewall's default gateway,
- #pkg_smc_addresses (IP1:PORT1:BINDADDR1,IP2:PORT2): the IP address, port and outgoing interface of the SMC server. This information is needed for the connecting package. The outgoing port and interface are optional. On SNS firewalls in version 3.9 and upwards, you can specify an outgoing interface for each IP address. On firewalls from versions 3.7.X to 3.8.X, only the first outgoing interface will be taken into account.
- vpn_fw_subject_dn: for certificates obtained via SCEP or EST, the Distinguished Name of the subject of the firewall's default certificate,
- vpn_fw_issuer_dn: for certificates obtained via SCEP or EST, the Distinguished Name of the issuer of the firewall's default certificate.

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

2.5.2 Importing firewalls from the web interface

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



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

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

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

2.5.3 Importing firewalls in command line

IMPORTANT
When several administrators are connected at the same time, we recommend that you import firewalls from the web interface instead of in command line, so that each administrator will be informed when changes are applied.

1. Start by copying the CSV file on the SMC server using the SSH protocol in the */data/tmp* folder for example. This example is used in the procedure below.
2. Log in to the SMC server via the console of your hypervisor or in SSH.
3. Enter the command:
   `smc-import-firewalls /data/tmp/filename.csv`.

To change the value of the delimiter character, use the environment variable SMC_CSV_DELIMITER. For more information, refer to the section Choosing the separator character in CSV files.

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

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

```
[root@smc] - {~} > smc-import-firewalls /opt/stormshield/examples/csv/example-import-firewalls.csv

S U M M A R Y
Firewalls created successfully : 9
Firewalls updated successfully : 0
Firewalls ignored : 0

Firewalls package created successfully : 9
Firewalls package creation failure : 0

Packages have been generated in : /tmp/import-firewalls-2021-02-26_11-28-17
```

You can also:

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

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

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

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

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

3. Monitoring SNS firewalls

The various types of information about each firewall shown in **Monitoring** > **Firewalls** make it possible to view and monitor firewalls. You can also access a firewall's logs and activity reports directly, and your Stormshield Log Supervisor (SLS) server if you have one.

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

3.1 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.

3.1.1 Getting information about firewalls

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

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

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

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

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

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

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

To filter the firewall list according to the health status:

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

- or -

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

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

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

Troubleshooting

The firewall does not display a valid maintenance end date

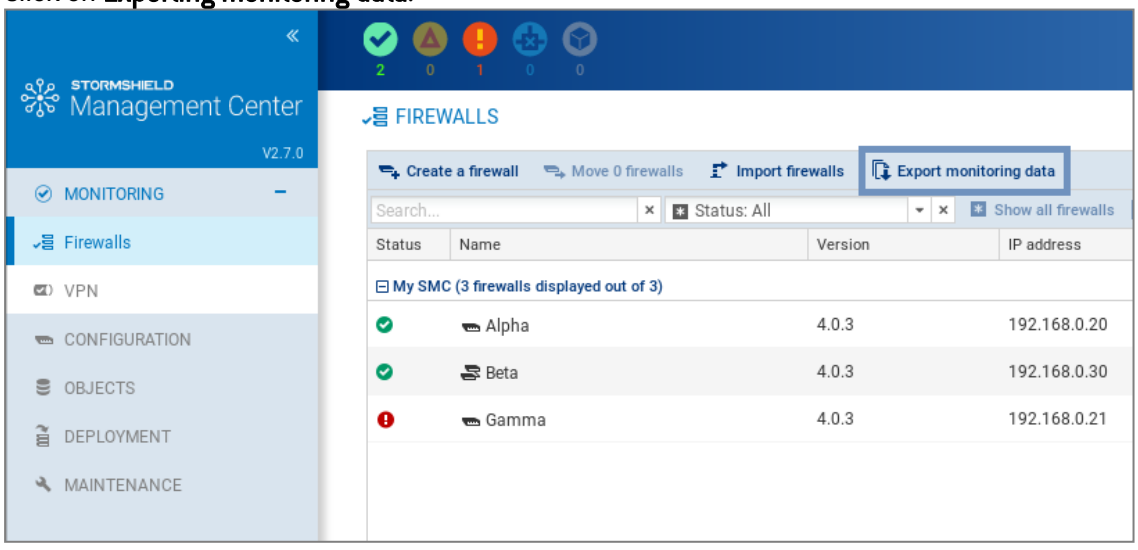
- *Situation*: In Monitoring view, the column indicating the date on which maintenance of the firewall ends is empty.
- *Cause*: Firewall license is not valid.
- *Solution*: Contact your Stormshield support center to obtain a valid license.

3.1.2 Exporting monitoring data

In the SNS firewall monitoring panel, you can export and download monitoring data to a CSV file. If you have filtered the data, only the lines that can be seen in the grid will be exported.

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

1. Select **Monitoring** > **Firewalls**.
2. If you want to export the data of some firewalls only, filter them by using the search field and **Status** field.
3. Click on **Exporting monitoring data**.



4. Save the CSV file.

By default, data in the file is separated by commas. You can change the delimiter using the environment variable `SMC_CSV_DELIMITER`.

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

3.1.3 Organizing firewalls by folders

To manage firewalls and their configuration, the SMC server relies on hierarchically organized folders to which firewalls are connected.

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 connected to a sub-folder inherits rules configured in its parent folders. For more information on filter and NAT rules, refer to the section Creating filter and NAT rules.

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

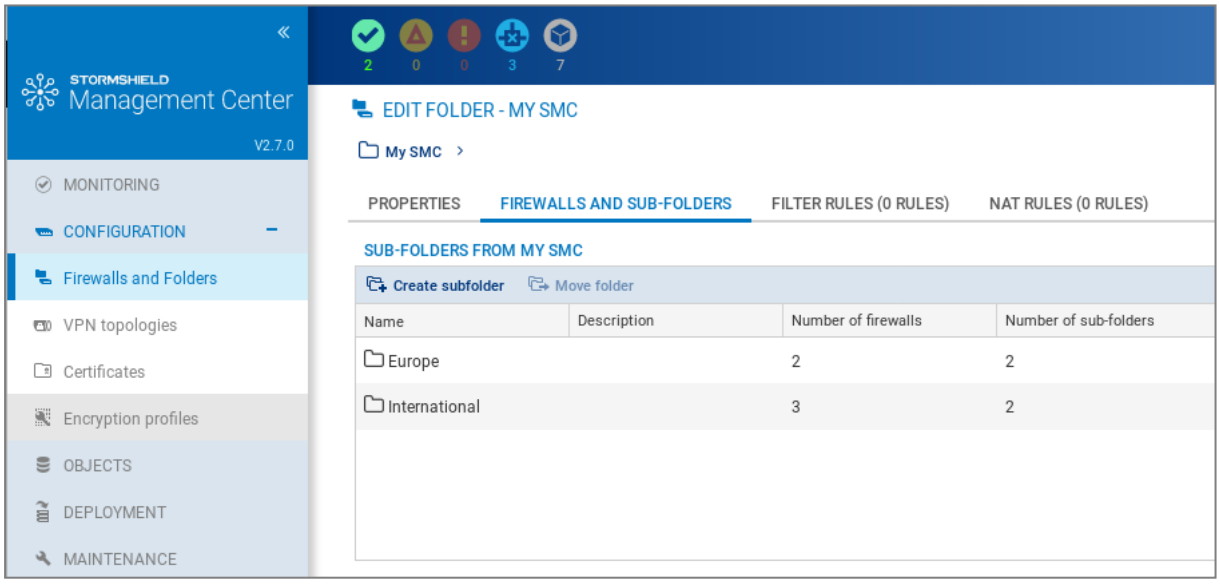
The default root folder **MySMC** cannot be deleted. You can rename it to fit your needs. If you do not create any folder trees, all firewalls will be connected to this root folder.

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

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

Creating folders

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



Organizing firewalls

There are several ways to do so:

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

Restricting administrators' write access privileges to certain folders

In SMC, administrators' write access privileges can be restricted to one or several folders. Likewise, the administration of a firewall group can be restricted to a single administrator,

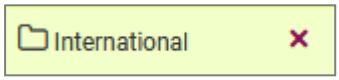
known as a "folder administrator", for security reasons. This administrator can look up the configuration of other firewalls that are connected to SMC, but in read-only access. The super administrator and general administrator can still access all folders in write mode.

Folder administrators can create and delete folders only in the folders on which they have write access privileges.

For more information on restricting folder administrators' access, refer to the section Restricting folder administrators' access privileges.

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.

3.1.4 Checking usage of a firewall in the configuration

In order to check whether a firewall is used:

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

3.2 Accessing the firewall monitoring interface

You can directly access the interface to monitor connected firewalls from the SMC server.

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

Authentication on the firewall is automatic:

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

For more information about the monitoring interface, refer to the *SNS User guide*.

3.3 Accessing the Stormshield Log Supervisor (SLS) server

WARNING
Folder administrators whose read access privileges are restricted to certain folders on SMC cannot perform this operation. For more information, refer to the section Restricting folder administrators' access privileges.

SLS is the log management solution that Stormshield offers.

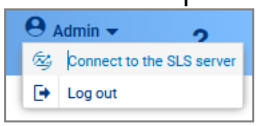
In SMC, you can access the interface of your SLS server by using a shortcut that can be configured in SMC.

You can also go straight to the SLS view, filtered by logs for a given firewall.

3.3.1 Adding a menu to access the SLS server

To add a menu that allows access to your SLS server from the upper banner of the SMC web interface:

1. Go to **Maintenance** > **SMC Server** > **Settings**.
2. Select the checkbox **Shortcut to the Stormshield Log Supervisor (SLS) server**.
3. Enter the IP address or FQDN of the SLS server.
4. Click on **Update**.
5. In the Administrator drop-down menu in the upper banner, check that the **Connect to the SLS server** menu exists and test the link. You should be able to access your SLS server's authentication portal.



An SLS icon is also available for each firewall in the firewall monitoring panel.

3.3.2 Filtering the SLS view by a firewall's logs

When you click on a firewall's icon in the monitoring view, the link leads to the SLS home page by default.

However, you can set a URL redirection parameter to go straight to the view filtered by a specific firewall's logs on your SLS server. Logs are filtered by the firewall's IP address.

To enable this feature:

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.
3. In the **Settings** tab, select the checkbox **Firewall IP address for SLS server**.
4. Choose to use SMC's default IP address or a custom address known to the SLS server.
5. Click on **Apply**.

In the firewall monitoring view, you can show the **IP address for SLS** column and use this address to search for a firewall.

4. Configuring SNS firewalls

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

To perform these operations, you need to hold write access privileges on the folders in question in the SMC web interface. For more information, refer to the section Restricting folder administrators' access privileges.

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.

4.1 Editing firewall settings

To edit the settings of a firewall:

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

The series of tabs that appears will allow you to:

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

The **Description** and **Location** fields in the **System** > **Configuration** tab are filled in for information only and do not have any impact on the configuration.

If the firewall belongs to a route-based VPN topology, modifying its name may have consequences on the firewall configuration. If you modify the name, SMC automatically renames the objects that correspond to the associated VTI interfaces. You should then verify the firewall local configuration. From version 3.4, if SMC manages the firewall routing and network configuration, you do not need to do anything. For more information, refer to the section Creating route-based VPN topologies.

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

4.1.1 Adding custom properties

WARNING
Folder administrators whose read access privileges are restricted to certain folders on SMC cannot perform this operation. For more information, refer to the section Restricting folder administrators' access privileges.

With custom properties, description criteria for firewalls can be added. In this way, firewalls can be identified and filtered more efficiently, using characteristics other than their names, versions or comments.

Such custom properties are therefore particularly useful for managing large firewall pools.

They can either be created directly in SMC or imported.

NOTE
Custom properties are meant only for administration via SMC, so are not deployed on the corresponding firewalls.

Firewalls can be filtered by their custom properties in the following modules:

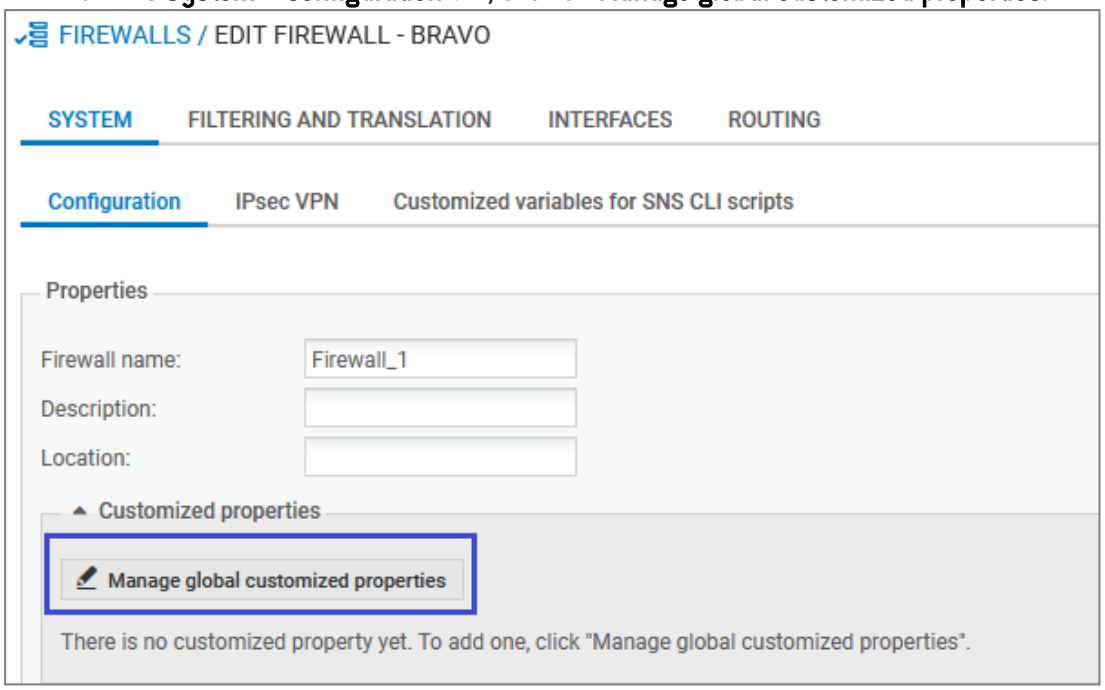
- Firewall and folder monitoring,
- Peer selection in a VPN topology,
- Firewall selection for the deployment of a configuration,
- Results of configuration deployments,
- Firewall selection for the deployment of CLI scripts,
- Results of CLI script deployments.

You can display the columns that represent these custom properties in the firewall monitoring and configuration windows.

Adding a custom property to a firewall

To add a custom property:

1. In a firewall's **System > Configuration** tab, click on **Manage global customized properties**.



   A window will open, displaying the available properties.
2. Click on **Add**.
3. Enter the **Name** of the property.
   Only alphanumeric and underscore characters are allowed.
4. Click on **Close**.
   In the window to edit the firewall's settings, a new field appears, bearing the name of the custom property that was added.
5. Enter the desired value (any character) for this custom property and click on **Apply**. Repeat the last operation for every firewall.

4.1.2 Editing the value of a custom firewall property

The value of a custom property can be changed at any time:

1. Edit the properties of the firewall in question.
2. In **System > Configuration > Customized properties**, enter the desired value (any character) of the custom property to change.
3. Click on **Apply**.

4.1.3 Importing/exporting custom firewall properties

Custom properties can be imported or exported in the **System > Configuration** tab of the window to edit the firewall's settings.

Exporting custom properties

1. Edit the properties of a firewall.
2. In the **System > Configuration** tab, click on **Manage global customized properties**.
   Another window will open, displaying the available properties.
3. Click on **Export**.

4. Open or save the export file containing custom properties.
5. Click on **Close**.

> **NOTE**
> The structure of an export file containing custom properties is as follows:
>
> #property,#firewall,#value
> Cp1, Fw2, value_cp1
> Cp2, Fw1, value_cp2
> Cp3, Fw1, value_cp3
> etc.

Importing custom properties

1. Create a CSV import file containing custom properties with the following structure:
   #property,#firewall,#value
   Cp1, Fw2, value_cp1
   Cp2, Fw1, value_cp2
   Cp3, Fw1, value_cp3
   etc.
2. Edit the configuration of a firewall.
3. In the **System > Configuration** tab, click on **Manage global customized properties**. Another window will open, displaying the available properties.
4. Click on **Import**.
5. Select the file created in step 1.
6. Click on **Open**.

SMC behavior during imports

- When a firewall specified in the import file is not connected to the SMC server, the whole import will be canceled.
- When a custom property already exists for a firewall connected to the SMC server, the value of this property will be changed for the firewall in question.
- When a custom property does not exist, it will be created and the corresponding value will be assigned to it for every firewall specified in the import file.
- When a custom property already exists on the SMC server and has been assigned a value for a particular firewall, its value will be replaced with the value assigned to this firewall in the import file.

4.2 Creating custom variables

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

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

Custom variables can be added in any firewall's properties.

To set the values of each variable for specific firewalls, you need to go to the properties of the firewalls in question, provided that you hold write access privileges on these firewalls.

Custom variables can be modified or deleted, as long as they are not used in the configuration of firewalls on which you do not have write access privileges. You can check where firewalls are being used as shown below. For more information, refer to the section Restricting folder administrators' access privileges.

You can create as many customized variables as needed.

4.2.1 Adding, changing or deleting customized variables

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

Several actions can then be performed in the window:

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

4.2.2 Defining the value of a customized variable for a firewall

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

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

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

Variable names and comments are common fields for all firewalls. Click on **Manage global variables** to edit them.

4.3 Verifying configuration consistency

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

To show the consistency check:

- Select **Maintenance** > **Consistency check**.

- or -

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

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

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

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

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

4.3.1 Disabling the consistency check

The consistency checker may affect the performance of the SMC server when it manages large pools (over 500 SNS firewalls).

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

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Edit the file **/data/config/fwadmin-env.conf.local** by adding the following line at the end: `SMC_CFGCHECK_ENABLED=false`.
3. Restart the server with the command `nrestart smc`.

In this case, you can still manually launch the consistency check when required, by clicking on the **Run verification** button in the consistency checker interface.

When the consistency check is disabled, automatic checks will still be launched for each deployment, to guarantee the consistency of the configuration across firewalls.

The `SMC_CFGCHECK_BEFORE_DEPLOY_ENABLED` environment variable can be used to disable these automatic checks if required.

4.3.2 Disabling check areas and changing the anomaly level

WARNING
Follow the recommendations given by the Stormshield Technical Assistance Center for these operations.

You can specifically disable checks in some areas or disable some of the configuration consistency checks. You can also change the "warning" or "error" levels in checks.

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. To know which entries can be disabled, refer to the file **/opt/fwadmin-server/config/cfgcheck.ini** without modifying it.
3. In the **/data/config/cfgcheck.ini** file:
   - Add the keys to disable in the `DOMAINS` section of the file, by indicating `false` as the value,
   - Add checks in the `CHECKS` section of the file, by indicating `error` or `warning` as the level, or use `false` as the value to disable the check.
4. Restart the server with the command `nrestart smc`.

EXAMPLE
/data/config/cfgcheck.ini file:

```
[DOMAINS]
RULE=false
IPSECDR=false

[CHECKS]
INVALID_INTERFACE_IN_STATIC_ROUTING=error
INVALID_INTERFACE_IN_RETURN_ROUTING=error
IP_COLLISION=warning
OVERLAPPING=warning
RETURN_ROUTE_GATEWAY_WITHOUT_MAC_ADDRESS=false
STATIC_ROUTE_WITHOUT_INTERFACE=false
```

4.3.3 Restricting the number of inconsistencies reported

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

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. In the file **/data/config/fwadmin-env.conf.local**, change the value of the environment variable: `SMC_CFGCHECK_INCOHERENCIES_INT`.
3. Restart the server with the command `nrestart smc`.

4.4 Deploying a configuration on firewalls

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

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

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

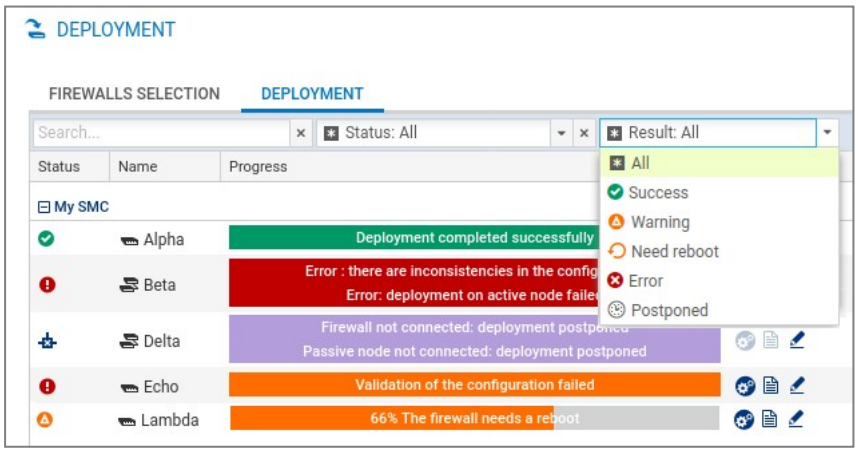
- Objects used in filter and NAT rules relating to the firewall or its parent folders.
- Objects you have chosen to deploy on all firewalls or for which you have selected the firewalls they will be deployed on. For more information, please refer to the section Managing objects.

- If the firewall is part of a VPN topology: Network, Host and/or Group objects and the certification authority associated with this topology, as well as information on the certificate selected for this firewall in the topology (the certificate has already been installed on the firewall).

You need to hold write access privileges on the firewalls to perform this operation. For more information, refer to the section Restricting folder administrators' access privileges.

4.4.1 Deploying a configuration on a firewall from the web interface

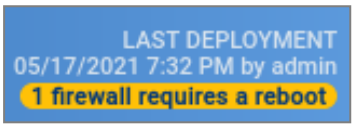
1. Go to **Deployment > Configuration deployment** or click on the button in the upper banner of the interface. This button turns orange when changes have been made to the configuration.
2. In the **Firewalls selection** tab, select firewalls.
3. Enter a comment at the bottom of the panel if needed.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



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

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

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



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

4.4.2 Deploying a configuration on a high availability cluster

The steps are the same as in the section above.

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

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

4.4.3 Deploying a configuration on a firewall in command line

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

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

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

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

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

4.4.4 Enabling warnings when configurations are modified

When you are about to deploy a configuration on a pool of firewalls, SMC may show a warning to inform you that other administrators have made changes to the configuration since it was last deployed.

You can then choose to either cancel the deployment or continue. If you choose to proceed with the deployment, changes made by other administrators will also be deployed on the selected firewalls.

This feature is disabled by default. To enable it:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. In the file **/data/config/fwadmin-env.conf.local**, add the environment variable `SMC_WARNING_MODIFICATION_ENABLED=true`.
3. Restart the server with the command `nrestart smc`.

WARNING
This feature includes the following limitations:

- SMC displays a warning only when it detects changes made to the configuration from the web administration interface. Changes made via the command line interface and the SMC public API are not taken into account.
- All changes to a firewall's configuration will trigger a warning, regardless of which firewalls are selected for the deployment, and even when the firewall in question is not part of the selection, or is not part of the administration perimeter of the administrator deploying the configuration.
- Any time a resource is created, i.e., an object or rule set, even if it is not in use or has been deleted immediately, a warning will be triggered.
- Any operation involving rule separators (collapsing/expanding) will trigger a warning.
- During a deployment, the list of pending changes will be purged, regardless of which firewalls are selected for the deployment. This means that if you make changes to firewall A, and another administrator deploys the configuration first on firewall B then on firewall A, the warning will appear only during the first deployment.
- If an administrator restores a backup on SMC, the list of pending changes will be purged. No warnings will be shown during the next deployment.
- When a configuration deployment fails on a firewall, the list of pending changes will be purged.

4.4.5 Keeping the connection alive during deployment

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

Variable	Description
SMC_DEPLOYMENT_TIMEOUT_BEFORE_ROLLBACK_INT By default: 30 seconds	Sets the amount of time in seconds that SMC will attempt to reconnect. Once this duration is exceeded, the previous configuration will be restored.
SMC_SNS_DEPLOYMENT_ROLLBACK_TIMEOUT_INT By default: 180 seconds	Sets the amount of time in seconds between the restoration of the configuration and the reconnection to the SMC server. If the connection is not up again after this duration, the deployment will be considered a failure. We do not recommend setting a value lower than the default value.
SMC_FW_DEPLOYMENT_ROLLBACK_ENABLED	Makes it possible to disable the feature. It is enabled by default.

4.4.6 Troubleshooting with the server's logs

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

SMC side

/data/log/fwadmin-server/server.log

Firewall side

/log/l_system

4.4.7 Troubleshooting

Validation of the deployment failed

- *Situation*: After the configuration was deployed on the firewall, the status of the firewall switched to **Critical** and indicated "Configuration validation". The command `CONFIG STATUS VALIDATE` therefore failed.
- *Cause*: The password used to validate the configuration on the SNS firewall was probably changed and no longer matched the one saved on SMC. Check the server's logs to find out the exact cause.
- *Solution*: Connect to the firewall to fix the issue. If the reason is an invalid password; run the command `CONFIG STATUS REMOVE`.

Configurations cannot be deployed on some firewalls

- *Situation*: Some firewalls cannot be selected for the deployment.
- *Cause*: An SNS CLI script is currently being executed or delayed on the firewall, so configurations cannot be deployed on this firewall for the moment.
- *Solution*: Wait until the script finishes executing, or until the firewall reconnects so that the execution can complete. You can also cancel the execution of the script from the **SNS CLI scripts** menu.

4.5 Completing the configuration of firewalls with a CSV file

In SMC, a CSV configuration file can be imported into the settings of each firewall, and can be applied whenever the configuration is deployed.

This file makes it possible to set SNS parameters that cannot be configured in SMC, or to load common parameters on a given firewall.

This feature applies only to parameters contained in configuration files that are generated by SMC. It does not allow operations on a firewall's local filter and NAT rules, for example.

4.5.1 Creating the CSV file

1. Create a CSV file with the following structure:

```
setconf, "file", "section", "field", "value"
setconf, "file", "section", "line"
delconf, "file", "section", "field", "value"
delconf, "file", "section", "line"
```

The authorized SNS operations setconf and delconf make it possible to edit or remove configuration settings.

For example:

```
setconf, network, loopback1, Address, 192.168.1.2
setconf, Global/VPN/01, Global, RemoteFetch, 1
```

For more information on configuration files in general, refer to SNS firewall documentation.

If you wish to change the default separator character in the file, refer to the section Choosing the separator character in CSV files.

2. Next, import the file into SMC as shown below.

4.5.2 Importing the CSV file into SMC

To import the configuration file into a firewall's settings:

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.
3. In the **System > Configuration** tab, expand **Additional firewall configuration** and click on **Import file**.

Once the CSV file has been imported into the firewall's settings, it will be applied to SMC configuration files every time the configuration is deployed on the firewall. The file can be replaced or deleted.

Export the file to view its content.

4.6 Loading and deploying a former configuration

WARNING
Folder administrators whose read access privileges are restricted to certain folders on SMC cannot perform this operation. For more information, refer to the section Restricting folder administrators' access privileges.

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.

If you load a configuration which is not the latest in the history, a warning message appears at the top of the window. The message remains until you deploy the configuration on firewalls or until you load the latest configuration deployed.

NOTE
The deployment history is cleared every time the SMC server is updated, therefore containing

only the revisions of a current version. The history cannot be used to restore the configuration of an older version after the update.

4.7 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 SNS firewalls) or *.tgz* (configuration files that can be read in a text editor) formats, or deploy the configuration on the firewall.

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

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

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

4.8 Detecting changes to the local configuration on firewalls

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

You can manage verifications by using an environment variable:

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

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

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

When a firewall is being updated, the detection of local changes is disabled until the next time the configuration is deployed. After a new deployment, SMC will resume monitoring local changes.

4.8.1 Viewing local changes on a firewall

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

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

4.9 Accessing the web administration interface of firewalls

The SMC server web interface does not allow all firewall settings to be configured. To complete the configuration, you can log in directly to a firewall's web administration interface without having to authenticate. In this case, you will need to hold read/write access privileges on the firewall web interface. For more information, refer to the section Managing administrator privileges as super administrator.

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

Authentication on the firewall is automatic:

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

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

For more information about the web administration interface, refer to the SNS *User guide*.

If the firewall is not in an administrator's administration perimeter, direct access to the firewall's administration interface is still possible, but in read-only mode. For more information, refer to the section Restricting folder administrators' access privileges.

4.10 Using the Emergency mode

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

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

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

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

1. From the SMC server web interface, connect to the web administration interface of the firewall by clicking the icon in the list of firewalls in the **Monitoring** menu.
2. Refer to the section High availability in the *SNS User Guide* to find out how to add a passive node. In a failover, the passive node will become active and will automatically connect to the SMC server

TIP
The icon in the **Mode** column is updated in the 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 **System > High availability** tab.

4.12 Importing or declaring a certificate for a firewall

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

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

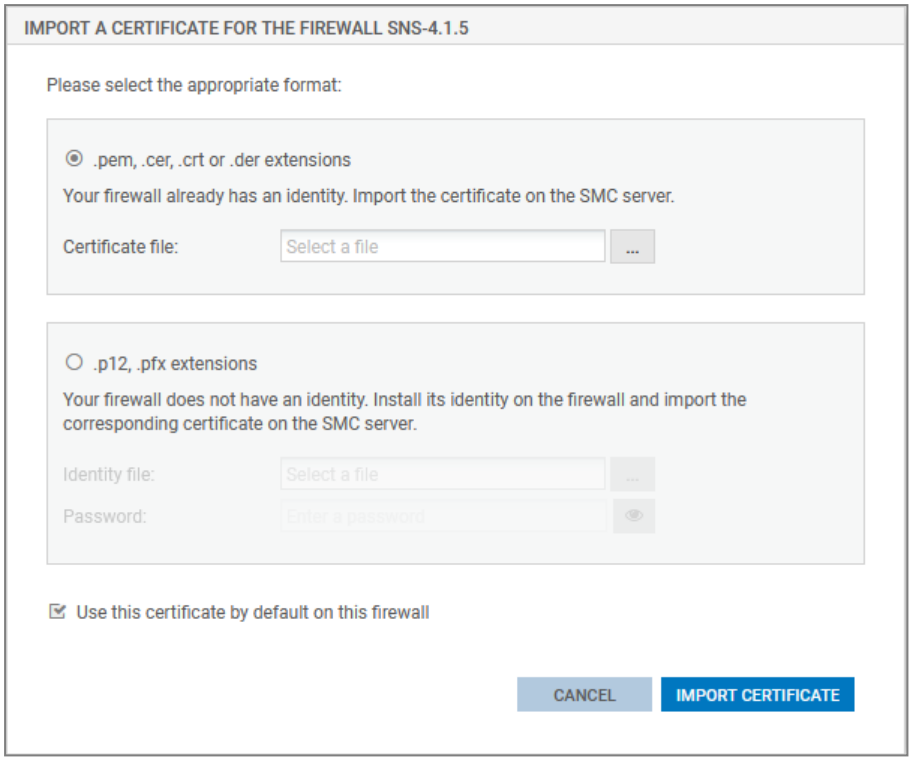
The certificate can be imported on the SMC server from the server's web interface or from the command line interface. Several certificates may be imported for a single firewall.

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

You need to hold write access privileges on the firewall to perform these operations. For more information, refer to the section Restricting folder administrators' access privileges.

4.12.1 Importing a certificate from the server's web interface

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



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

-or-

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

-or-

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

-or-

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

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

4.12.2 Importing a certificate from the command line interface

1. To import a certificate from the command line interface, connect to the SMC server via the console of your hypervisor or in SSH.
2. Enter the command
`smc-install-certificate`

TIP
Display help using the option --help:

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

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

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

Options:
  -V, --version                 output the version number
  -c, --certificate <filepath>  The certificate to import on the firewall
  -f, --firewall <name>         The target firewall name
  -p, --password <password>     The password of the certificate
  -u, --update                  Use this option to update an existing certificate
  -h, --help                    display help for command
```

Three of these options are mandatory:

- --certificate: path of the certificate (*.p12* or *. pfx*) 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*.

4.12.3 Importing a certificate on a high availability cluster

Import the certificate for the active node of the cluster.

The SMC server then synchronizes both nodes of the cluster.

4.12.4 Troubleshooting

The Import button remains grayed out

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

Importing the certificate on a firewall causes an error

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

Other possible causes

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

4.12.5 Declaring a certificate used by a firewall

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

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

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

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

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

4.12.6 Changing the certificate used by default in VPN topologies

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

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

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

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

4.13 Using SMC as an Active Update distribution point

WARNING
Folder administrators whose read access privileges are restricted to certain folders on SMC cannot perform this operation. For more information, refer to the section Restricting folder administrators' access privileges.

SNS firewalls include the Active Update feature, which queries Stormshield update servers to download the latest databases (context-based signatures, antivirus, Vulnerability Manager, etc.).

If your SNS firewalls are not connected to the Internet, they cannot access Stormshield update servers. If this is the case, you can use SMC as an Active Update distribution point and therefore upload updated databases to the internal network.

This feature is compatible with SNS firewalls from version 4.3 upwards.

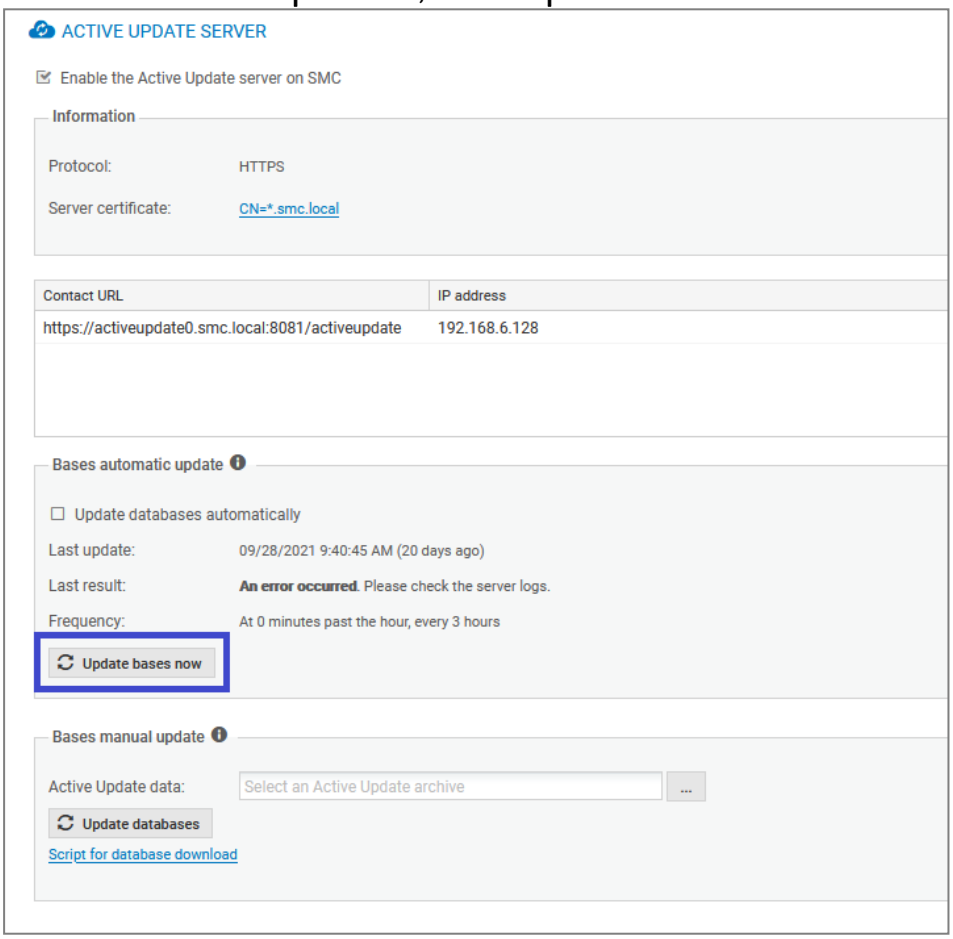
4.13.1 Downloading Active Update databases

You must download Active Update databases on the SMC server to be able to distribute them later on SNS firewalls. The steps vary depending on whether the SMC server is connected to the Internet.

Downloading databases with an Internet connection

DNS resolution must be enabled on the SMC server (**Maintenance** > **SMC Server** > **Settings** > **Domain name server** menu).

1. Open the **Configuration > Active Update server** menu.
2. Select **Enable the Active Update server on SMC**.
3. Click on **Apply** at the bottom of the window.
4. In the **Bases automatic update** area, click on **Update bases now**.



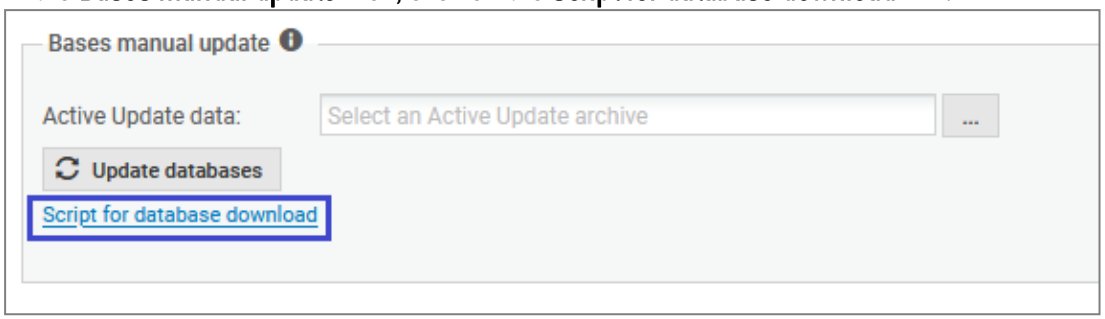
The SMC server connects to the Stormshield update server and downloads the databases.

5. If you want the databases to update automatically every three hours, select **Update databases automatically**.
   To change the frequency of updates or the number of databases to update, refer to Customizing Active Update settings.

Downloading databases without an Internet connection

1. Open the **Configuration > Active Update server** menu.
2. Select **Enable the Active Update server on SMC**.
3. Click on **Apply** at the bottom of the window.

4. In the **Bases manual update** area, click on the **Script for database download** link.



5. Copy and run the script `activeupdate-fetch.sh` on a Linux machine with an Internet connection. DNS resolution must be enabled on the machine.
   - By default, the script retrieves all databases from the URL *https://update1-sns.stormshieldcs.eu/package*. If you wish to specify which databases to retrieve, or a different URL, change the script settings before running the script.
   - The script uses */tmp* as the destination folder by default. If there is insufficient disk space in */tmp*, the script will fail. In this case, specify a different destination folder, using the script's "`-t`" option.
     For more information, refer to the help for the script `activeupdate-fetch.sh -h`.
6. In the **Active Update data** field, select the archive generated by the script.
7. Click on **Update the databases**.
8. Repeat these steps regularly so that the Active Update databases are always up to date on the SMC distribution point.

4.13.2 Using the SMC Active Update server

Once you have downloaded the databases on the SMC server, you must configure the SNS firewalls so that they use it as their Active Update server. This can be configured manually if you have few firewalls, or automatically using a script.

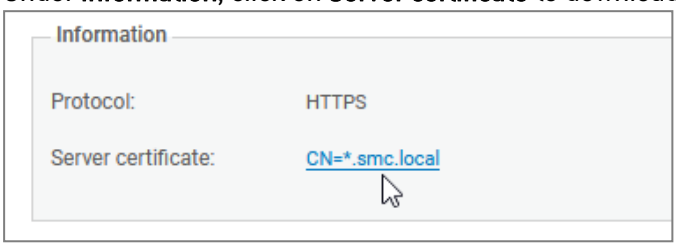
The *server.crt* and *server.key* files in the folder */etc/certs/activeupdate* are used for TLS negotiations. They are generated the first time SMC is run, and the certificate is self-signed. If you prefer to replace them with your own files, restart the SMC server after you select them.

Configuring SNS firewalls manually

1. In the web interface of the SMC server, select **Configuration > Active Update server**.
2. In the **Contact URL** column, click on the URL to copy it.
3. On each SNS firewall, declare the SMC server as the Active Update server by indicating the URL copied earlier. For more information about Active Update, refer to the SNS *User guide*.
4. Create the static object that was used in the URL copied in step 2, and assign to it the IP address used to contact the SMC server.

Configuring SNS firewalls automatically

1. First, import the SMC Active Update certificate on each SNS firewall:
   a. In the web interface of the SMC server, select **Configuration > Active Update server**.
   b. Under **Information**, click on **Server certificate** to download the certificate.



   c. Create the Active Update configuration script with the commands described in the following example by replacing `server.crt` if necessary with the file name of your certificate:

```
PKI IMPORT format=pem type=ca $FROM_DATA_FILE("server.crt")
```

   d. Follow the usual steps for running a script, as shown in the section Running the SNS CLI script from the web interface by selecting the file of the certificate in the **Attachments related to the script** menu.
2. Create objects on the SNS firewalls that would make it possible to verify the SMC certificate:
   a. Create the object creation script with the commands described in the following example.

```
CONFIG OBJECT HOST NEW name=activeupdate0.smc.local ip=<[private
or public SMC server IP address]> resolve=static update=1
CONFIG OBJECT HOST NEW name=activeupdate1.smc.local ip=<[private
or public SMC server IP address]> resolve=static update=1
CONFIG OBJECT ACTIVATE
```

   The value of the `name` setting consists of an object name of your choice followed by the domain name. The private IP address is the one that can be seen in the **IP address** column in the **Configuration > Active Update server** panel in SMC.
   b. Follow the usual steps for running a script, as shown in the section Running the SNS CLI script from the web interface.
3. Create the Active Update configuration script with the commands described in the following example.

```
CONFIG AUTOUPDATE SERVER
url=https://activeupdate0.smc.local:8081/activeupdate
CA="CN=*.smc.local" state=on
CONFIG AUTOUPDATE ACTIVATE
```

   You will find the value of the `url` and `CA` settings in the **Contact URL** and **Server certificate** fields in **Configuration > Active Update server**.
   You can add custom settings to the script. For further information, refer to the *CLI Serverd Commands Reference Guide*.

> **TIP**
> To specify several URLs and CAs, separate them with commas:
> `url=https://activeupdate0.smc.local:8081/activeupdate,https://activeupdate1.smc.local:8081/activeupdate/activeupdate`
> `CA="CN=*.smc.local,CN=*.smc.local" state=on`

4. Follow the usual steps for running a script, as shown in the section Running the SNS CLI script from the web interface.

4.13.3 Customizing Active Update settings

Some Active Update settings, such as the number of the port to which SNS firewalls must connect, or the frequency of automatic updates, cannot be configured in the SMC web interface. However, these settings can be modified in a configuration file.

In this file, you can also indicate an HTTPS proxy to contact, which will serve as a link between SMC and the Stormshield update server, if you wish.

1. Open the */data/config/activeupdate/config.ini* file.

```
[General]
State=false
Port=8081
Host=0.0.0.0

[Sync]
Source=https://update1-sns.stormshieldcs.eu/package
Categories=ALL
Tries=3
AutoUpdate=false
AutoUpdatePeriod=0 */3 * * *

[Proxy]
Host=
Port=
User=
Password=
CAPath=
```

2. Change the settings as desired:

State	Enables the Active Update server on SMC.
Port	Port of the SMC server on which SNS firewalls must connect.
Host	Names of network interfaces or IP addresses assigned to existing interfaces on the server, on which the SMC server listens. Replace the value 0.0.0.0 for example with `eth0` or `192.168.7.54` to indicate that only these interfaces are in use.
Source	URL of the Stormshield server from which Active Update databases are downloaded.
Categories	List of Active Update databases that you wish to download from the SMC server. The values of the database categories are as follows. Separate them with commas.

Database category	Value
All databases	ALL
Antispam: DNS blacklists	ANTISPAM
Antispam: heuristic engine	VADERETRO
Embedded URL database	URLFILTERING
Antivirus: ClamAV antivirus signatures	CLAMAV
Antivirus: antivirus signatures of the previous Advanced Antivirus service	KASPERSKY
Antivirus: antivirus signatures of the new Advanced Antivirus service	ADVANCEDAV1
IPS: contextual protection signatures	PATTERNS
Root Certification Authorities	ROOTCERTS
Geolocation/Public IP reputation	IPDATA
Vulnerability management	SEISMO
Application and web service icons	METADATA

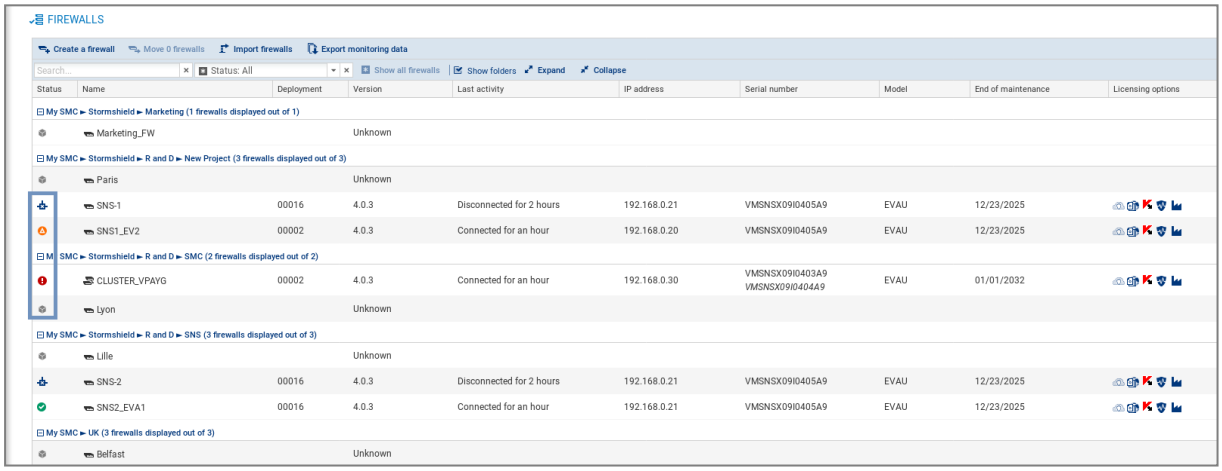
Tries	Number of tries when the database update fails.
AutoUpdatePeriod	Frequency of database updates. The possible values are in CRON format. By default, `0 */3 * * *` means that databases will be updated every 3 hours.
Host	Address or name of the HTTPS proxy server. May be an IP address or an FQDN.
Port	Number of the listening port on the proxy server.
User	User name to authenticate on the proxy server, if it requires authentication.

Password	Password to authenticate on the proxy server, if it requires authentication.
CAPath	Path to the certificate of the certification authority (CA) that signed the certificate presented by the proxy server.

3. Save the file. Changes will be immediately applied;
4. Only if the `State` setting has been modified, restart the SMC server with the command `nrestart smc`.

4.14 Configuring the warning for an imminent certificate expiry

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



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

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

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

To change the default 30-day period:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Change the value of the environment variable `SMC_SNS_CERTS_PROBE_EXPIRATION_INT`. For example: `SMC_SNS_CERTS_PROBE_EXPIRATION_INT= 20`
3. Restart the server with the command `nrestart smc`.
4. Deploy the configuration again on the firewalls.

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

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

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

4.15 Configuring the warning for the imminent expiry of license options

The status icons that appear in the upper banner of the interface as well as the **Licensing options** column in the firewall monitoring panel may show a **Critical** or **Not critical** status when subscribed license options (Breach Fighter, Extended Web Control, Advanced Antivirus, Stormshield Vulnerability Manager, Industrial Security Pack) have expired or are about to expire.

This warning is disabled by default.

The environment variables `SMC_FW_LICENSE_WARNING_INT` and `SMC_FW_LICENSE_CRITICAL_INT` make it possible to enable warnings and configure time frames.

To enable warnings:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Add the environment variables `SMC_FW_LICENSE_WARNING_INT = 90` and `SMC_FW_LICENSE_CRITICAL_INT = 30`.
3. Restart the server with the command `nrestart smc`.

In this example, a firewall will start displaying a **Not critical** status beginning 90 days before license options expire and **Critical** beginning 30 days before license options expire.

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

SNS firewalls offer the possibility of protecting certificates with TPMs.

Whenever you install an identity (*.p12* format) on an SNS firewall from the SMC server, the protection of the private key with a TPM is enabled by default. The private key is protected by a password stored on the TPM.

In SMC, TPM-protected keys can only be used in IPsec VPN topologies with IKEv2 encryption profiles.

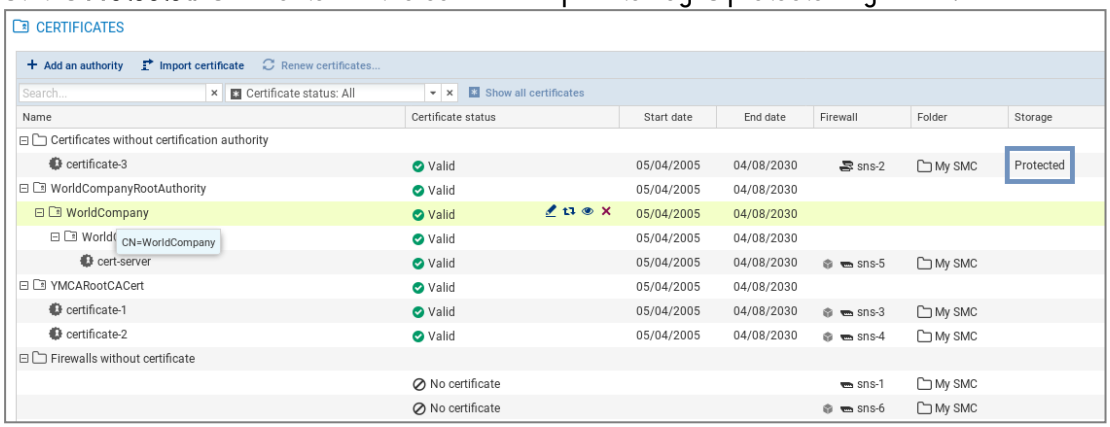
To create VPN topologies with IKEv1 encryption profiles, disable this protection using the environment variable `SMC_FW_TPM_ENABLED`.

4.16.1 Finding out whether a private key is TPM-protected

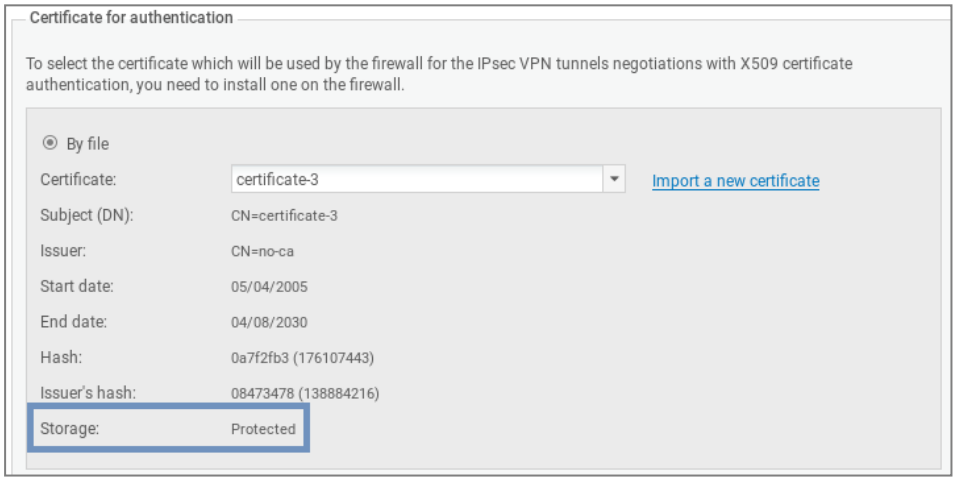
If a TPM has been installed and enabled on an SNS model firewall, whenever you install an identity on a firewall from the SMC server, the TPM will protect the corresponding private key.

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

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



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



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

4.16.2 Disabling TPM private key protection

To disable TPM protection when you install an identity on an SNS firewall from the SMC server, the `SMC_FW_TPM_ENABLED` environment variable must be modified:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. In the file **/data/config/fwadmin-env.conf.local**, change the value of the environment variable: `SMC_FW_TPM_ENABLED=false`
3. Restart the server with the command `nrestart smc`.

4.16.3 Enabling TPM protection on existing private keys

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

```
PKI CERTIFICATE PROTECT caname=<CA_name> name=<certificate_CN> tpm=ondisk
```

4.17 Choosing the separator character in CSV files

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

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

The default character is a comma.

To edit it:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. In the file **/data/config/fwadmin-env.conf.local**, change the value of the environment variable: `SMC_CSV_DELIMITER=","`.
3. Restart the server with the command `nrestart smc`.

5. Managing objects

The **Objects** menu on the left side of the web interface makes it possible to create, edit or remove 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 on global objects, refer to the *SNS user guide*.

Objects can be modified or deleted only when:

- They are not used in any firewall configuration,
- They are used in the configuration of firewalls on which you have write access privileges.

To check whether an object is in use, refer to the section Checking usage of an object in the configuration.

If you need to modify an existing object in order to use it in the configuration of your firewalls, and it is being used in the configuration by a firewall on which you do not have write access privileges, you will be prevented from modifying it. We recommend that you duplicate the object. To do so, go to the object editing panel.

For more information on the restriction of access privileges, refer to the section Restricting folder administrators' access privileges.

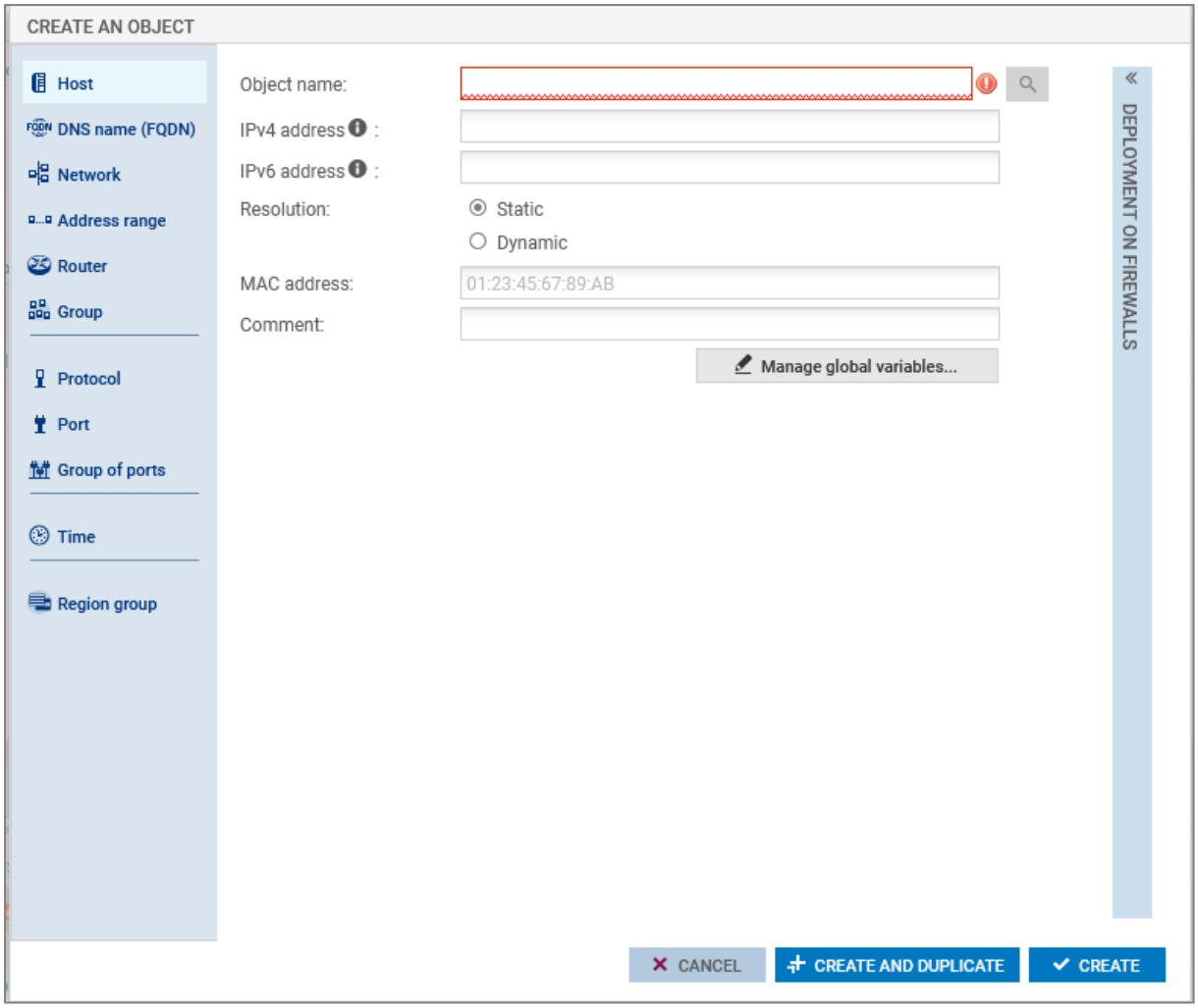
IMPORTANT
Before removing an object from the SMC server, ensure that doing so will not affect the operation of your firewalls.

5.1 Deploying objects on firewalls

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

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

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



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

In the list of objects in the **Objects** menu, various icons make it possible to identify objects that have been forcibly deployed on a selection of firewalls ( ) or on all firewalls ( ).

5.2 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.

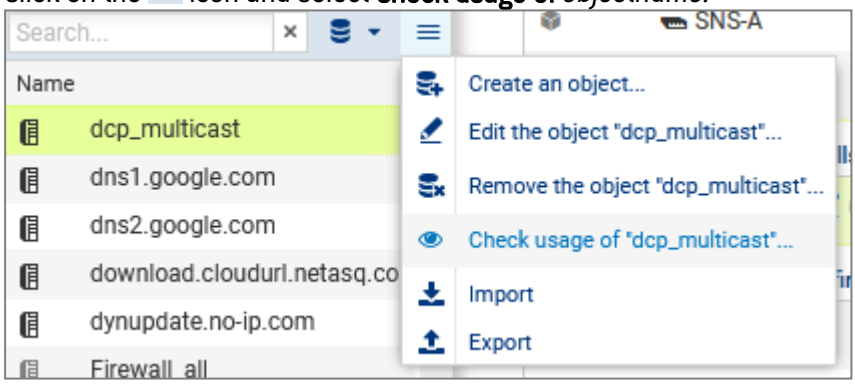
1. In the **Objects** menu, create a Host, Network or IP address range object.
2. Fill in the **IPv4 address** or **IPv6 address** field with a %CUSTOM_X% variable. The value of this customized variable is defined in the **Customized variables** tab in the **Edit firewall** panel accessible by double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

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

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

5.3 Checking usage of an object in the configuration

1. Select an object in the **Objects** menu.
2. Click on the ☰ icon and select **Check usage of** *objectname*.



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

5.4 Importing objects

WARNING
Folder administrators whose read access privileges are restricted to certain folders on SMC cannot perform this operation. For more information, refer to the section Restricting folder administrators' access privileges.

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

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

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

5.4.1 Creating the CSV file

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

To export the CSV file from a firewall:

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

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

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

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

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

Specifying firewalls on which objects are to be deployed

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

Example of a Host object being created:

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

The prescribed values of the *#resolve* parameter are "dynamic" and "static".

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.

5.4.2 Importing objects from the web interface

To import objects from the web interface:

1. In the **Objects** menu, click on the ☰ icon.
2. Select **Import**.
3. Select the CSV file to import.

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

In case of error, refer to the import summary.

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

5.4.3 Importing objects in command line

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

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

You can also choose the types of objects to import.

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

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

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

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

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

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

5.5 Exporting objects

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

You only need read privileges to export objects.

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

5.6 Using dynamic objects from SMC

By default, the SMC object database contains Firewall_xx and Network_xx objects, which correspond to network interfaces on the managed firewalls, e.g., Firewall_in and Firewall_out.

These dynamic objects do not have defined values, and are not deployed by SMC on firewalls.

Other dynamic objects can be created manually. They have to correspond to a known interface when they are used in a firewall's configuration. In the configuration, their values will be replaced with the value of the local object that bears the same name on each firewall. If the local object does not exist, the deployment of the configuration will fail.

If you wish to rename an interface on a firewall, the corresponding objects Firewall_xx and Network_xx will not be automatically renamed on SMC. You will need to rename them manually to prevent configuration errors. We recommend following the steps below when your firewall's network is managed by SMC:

1. On the firewall in question, directly change the name of the interface,
2. On SMC, force the retrieval of the interface and routing configuration from the menu **System** > **Configuration** in the firewall settings,
3. On SMC, create the Firewall_xx and/or Network_xx objects that bear the new interface name.
4. If the previous dynamic objects that bear the former names are used in the configuration of the firewall in question, replace them with the new objects.

6. Configuring the network and routing

In SMC, the interfaces and routes of your SNS firewalls can be managed centrally. Interfaces and routes already configured on firewalls are automatically retrieved in SMC. New interfaces and routes can be created and deployed on firewalls.

In SMC, the SD-WAN feature can also be implemented in your pool. This guarantees that the best links are selected according to the type of traffic, based on SLA (Service Level Agreement) criteria and monitoring options on gateways defined in router objects. Use such objects in filter rules to set up policy-based routing (PBR).

The **Monitoring** > **Routers** menu makes it possible to monitor in real time the quality of connections and the status of the gateways associated with router objects and deployed from SMC.

The configuration of interfaces and of routes in SMC is compatible with SNS firewalls in at least version 4.2.3 in read and write mode and in version 3.7 in read-only mode. The implementation of SD-WAN is compatible with SNS firewalls from version 4.3.3 upwards.

For more information on how to configure interfaces, routes and the SD-WAN feature, refer to the *SNS User guide:*

- Interfaces,
- Routing,
- SD-WAN and policy-based routing (PBR).

6.1 Configure network interfaces

From the SMC server, configure your firewalls' network interfaces.

To perform these operations, you need to hold write access privileges on the folders in question in the SMC web interface. For more information, refer to the section Restricting folder administrators' access privileges.

6.1.1 Enabling SMC to manage an SNS firewall's network

Go to the **System > Configuration** tab of the firewall in question and select **Configure the network for this firewall in SMC** to indicate that SMC manages the network for this firewall.

Next, go to the **Interfaces** > **Interfaces** and **Interfaces** > **IPsec interfaces (VTI)** tabs to configure the interfaces.

If this option is not selected, SMC will not manage the network for this firewall and the firewall's **Interfaces** tab will be in read-only mode.

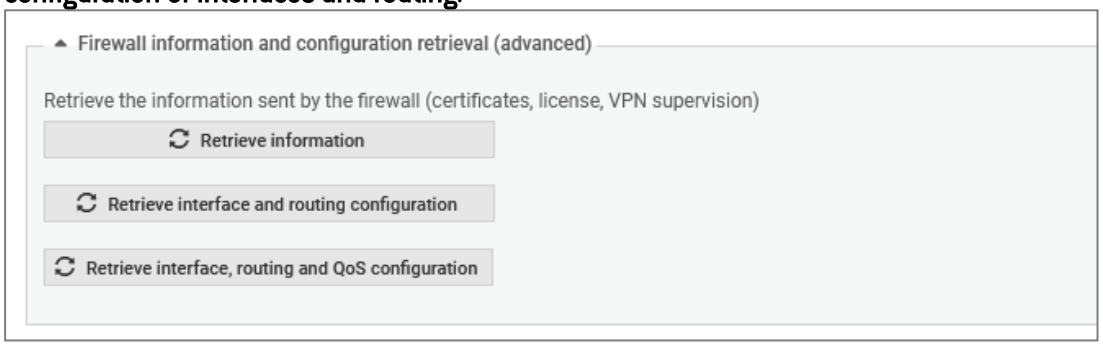
If you select this option when a firewall is already part of a route-based VPN topology, any associated IPsec interfaces (VTI) that are missing will automatically be created and shown in the **IPsec interfaces (VTI)** tab. For further information, refer to the section Configuring Ipsec interfaces (VTI).

6.1.2 Forcing the retrieval of the firewall's interfaces

When the **Interfaces** tab is in read-only mode, SMC retrieves the firewall's interfaces every time the page of the firewall's settings is opened. This is not the case when routing and network configuration is managed by SMC.

In the firewall's settings, you can then force the retrieval of the interface and routing configuration:

1. Go to the firewall's settings,
2. In the **System > Configuration** tab, select **Configure the network for this firewall in SMC** if it has not already been selected,
3. Expand **Firewall information and configuration retrieval (advanced)** and click on **Retrieve configuration of interfaces and routing**.



When you force a firewall's interfaces to be retrieved, and if the firewall has virtual IPsec interfaces (VTI), we recommend that you look up the server's logs to ensure that there is no conflict in the interface name, IP address or mask between the IPsec interfaces created on SMC and the IPsec interfaces created on the firewall. Identical names or addresses may delete interfaces used in routes or rules.

6.1.3 Configuring interfaces

The SMC server automatically displays the interfaces of your firewall in the **Interfaces > Interfaces** tab in the firewall's settings. You will then be able to configure them from a central point, or add them manually. For more information on interface configuration, refer to the *Interfaces* section in the SNS *User guide*.

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

- Ethernet interfaces
- Bridges
- VLANs
- Aggregates

There are three possible aggregate modes:

- LACP, which is the default mode.
- Failover, only on SNS firewalls in version 4.3 and higher.
- Broadcast, only on SNS firewalls in versions 4.3.25, 4.7.5, 4.8.1 and higher.

The interfaces that SMC does not support can also be retrieved in read-only mode (Wi-Fi, dialup, Loopback, GRETUN, GRETAP and USB/Ethernet). These interfaces are shown as **Other interface** in the grid.

They cannot be changed from SMC but can be used in the routing configuration.

When SMC retrieves the routes displayed in a firewall's Routing tab, the interfaces will also be retrieved automatically. If any interfaces were created on SMC but were not deployed, they will be overwritten when routes are retrieved.

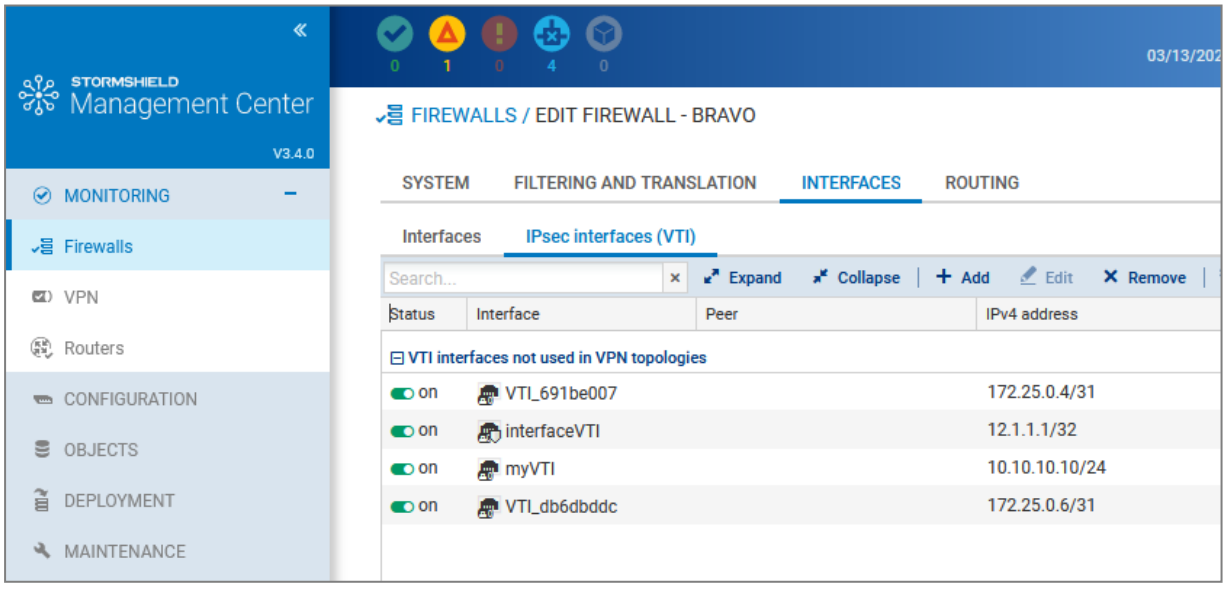
When deploying the network configuration, the existing VLAN, aggregate and bridge interfaces on the firewall are not preserved. The network configuration deployed from the SMC server will overwrite the local configuration on the firewall.

Limitations to the configuration of interfaces from the SMC server

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

6.1.4 Configuring IPsec interfaces (VTI)

The SMC server automatically displays the IPsec interfaces of your firewall in the **Interfaces > IPsec interfaces (VTI)** tab in the firewall's settings. You will then be able to configure them from a central point. The firewall must be in at least version 4.2.3.



The IPsec interfaces on firewalls can be used in route-based VPN topologies, and in the configuration of routes and policy-based routing filter rules.

For more information on IPsec interfaces, refer to *Creating or modifying an IPsec interface (VTI)* in the *SNS user guide* and in the technical note *IPsec virtual interfaces*.

IPsec interfaces shown in SMC originate from three different sources, and behavior may vary depending on whether the firewall's network configuration is managed by SMC or not:

The firewall belongs to a route-based VPN topology	SMC will automatically create the associated IPsec interfaces if SMC manages the firewall's network configuration. The interfaces are classified by VPN topology in the grid. They can neither be modified nor deleted. The **See VPN configuration** button makes it possible to go to the configuration panel of the VPN topology in question.
The IPsec interfaces were created on the firewall	SMC will retrieve them automatically during the migration from SMC version 3.3 to version 3.4, even if SMC does not manage the firewall's network configuration. If SMC manages the firewall's network configuration, you can force the interfaces to be retrieved at any time, as explained in Configure network interfaces. If they are used in a route-based VPN topology created from SMC, they will be associated with the topology in question in the grid of the **IPsec interfaces (VTI)** tab. If the network configuration is managed by SMC from version 3.4 onwards, we recommend that you no longer create IPsec interfaces directly on firewalls, as they will be overwritten the next time the configuration is deployed.
IPsec interfaces were created manually from SMC	This can be done only if SMC manages the firewall's network from version 3.4 onwards.

You can modify or delete IPsec interfaces only for firewalls for which SMC manages the network configuration, and if they do not belong to a route-based VPN topology.

As for IPsec interfaces used in route-based VPN topologies, some changes made in a topology may have an impact on the configuration of IPsec interfaces. In this case, the impact will immediately be replicated on the IPsec interfaces of firewalls for which SMC manages the network configuration.

As for firewalls with network configurations that SMC does not manage, changes made in a topology have the following consequences:

- If a topology is deleted, the associated IPsec interfaces will not be automatically deleted,
- If you change the name of a topology or a peer, the comment associated with the IPsec interface and shown in the **IPsec interfaces (VTI)** tab will not be automatically updated,
- If you change the VTI network pool of the topology, IP addresses of IPsec interfaces will be modified, and you must replicate the change manually on SNS firewalls.

6.2 Configuring routing

From the SMC server, you can manage and configure the static, dynamic, return and default routes of your firewalls in version 4.2.3 and upwards.

To perform these operations, you need to hold write access privileges on the folders in question in the SMC web interface. For more information, refer to the section Restricting folder administrators' access privileges.

WARNING
As of SNS version 4.8.1 EA, you will need at least version 3.6 to manage dynamic routing from SMC. You will not be able to deploy configurations with dynamic routing from SMC in a version lower than 3.6 on SNS firewalls in 4.8.1 EA versions and higher.

6.2.1 Configuring routes from SMC

Go to the **System > Configuration** tab of the firewall in question and select **Configure the network for this firewall in SMC**.

The first time you select this option, SMC retrieves automatically the firewall's routes in the **Routing** tab, if it is connected. SMC also retrieves the objects used in the routes.

In the **Routing** tab, you will be able to configure the following from a central point:

- static routes,
- return routes,
- default route,
- dynamic routing.

Static and return routes	To create new static and return routes, click on **Add** at the top of the grid.
Dynamic routing	Double-click on the line where dynamic routing appears in the grid. Select the BIRD version to use (v1 or v2). You can change the routing configuration to the format of the selected BIRD version, and select advanced options. For more information, refer to the Dynamic routing section in the SNS *User guide*. **NOTE** SMC does not support IPv6 for the BIRD configuration.
Default route	Double-click on the line in the grid and select a gateway.

When the configuration is deployed, the network configuration deployed from SMC takes priority over the firewall's local configuration and overwrites it.

For more information on route configuration, refer to the *Routing* section in SNS *User Manual*.

If the **Configure the network for this firewall in SMC** checkbox is not selected, the firewall's **Routing** tab will be in read-only mode. SMC then retrieves the firewall's routes every time the tab is opened. The objects contained in read-only routes will not be retrieved on SMC.

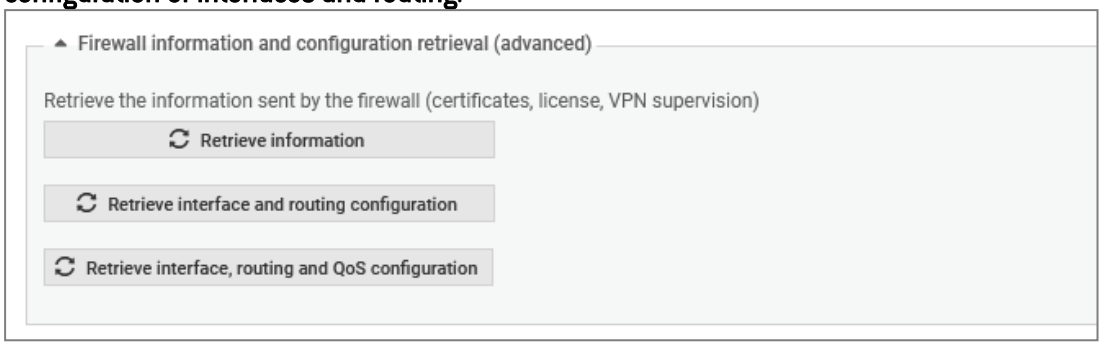
6.2.2 Forcing the retrieval of the firewall's routes

When the **Routing** tab is in read-only mode, SMC retrieves the firewall's routes every time the tab is opened. This is not the case when routing and network configuration is managed by SMC.

In the firewall's settings, you can then force the retrieval of the interface and routing configuration:

1. Go to the firewall's settings,
2. In the **System > Configuration** tab, select **Configure the network for this firewall in SMC** if it has not already been selected,

3. Expand **Firewall information and configuration retrieval (advanced)** and click on **Retrieve configuration of interfaces and routing**.



6.2.3 Importing and exporting routes

Routes can be manually imported and exported in command line.

Exporting routes

The `smc-export-routes` command makes it possible to generate a CSV file that includes the static routes, return routes and default routes of firewalls in at least version 4.2.4 and for which the network configuration is managed in SMC.

The command generates the CSV file in the */tmp* folder by default.

To export a firewall's routes:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Enter the command `smc-export- routes`. To change the default name of the output file (*smc_routes_date.time.csv*), add an argument to the command. For example: `smc-export-routes /data/tmp/my_routes.csv`.

Importing routes

The `smc-import-routes` command makes it possible to import from a CSV file to SMC the routes of firewalls in at least version 4.2.4 and for which the network configuration is managed in SMC. Running the command overwrites the routes that are already visible in SMC.

EXAMPLE
The structure of an import file containing routes is as follows:
#firewall,#type,#status,#destination,#gateway,#interface,#comment
SNS1,default,Enabled,any,gateway,auto,
SNS2,reverse,Enabled,,update1-sns.stormshieldcs.eu,out,
...

To import routes:

1. To create the CSV file, you can export routes as shown above and use the generated file as a base,
2. Copy the CSV file to the SMC server using the SSH protocol in the */tmp* folder for example,
3. Log in to the SMC server via the console of your hypervisor or in SSH.
4. Enter the command `smc-import-routes` followed by the path to the CSV file as the argument.

If the routes reference items from your SNS configuration that are not already in the SMC configuration (objects/interfaces), you must import them beforehand on the server.

6.2.4 Limitations to the route configuration from the SMC server

- Currently, configuration in IPv6 is not supported.
- SMC can retrieve the routes of an SNS firewall and the associated objects by enabling the network configuration management or by forcing the retrieval of the routes. If a retrieved object already exists on SMC (same type and name), the values of the object existing on SMC are then the values used in the configuration.
- If the default gateway set on an SNS firewall does not match any object in the firewall's object database, route retrieval will not be supported. An error log will be generated in the server's logs, explaining that the IP address must be represented by an object.
- Objects containing only IPv6 and/or MAC addresses cannot be used.
- Router objects can be used as gateways to a static route on SNS firewalls in at least version 4.3.0.
- Dynamic routing - The deployment of configurations with dynamic routing on SNS firewalls in 4.8.1 versions and higher from SMC in versions below 3.6 is not supported.
- Dynamic routing - SMC does not support the following parameters. If necessary, configure them directly from the SNS firewall. They will not be overwritten by the routing configuration originating from SMC:
  - the **"[BGPAuth]"** section,
  - the exclusion of IP address ranges in routes. For more information, refer to the Stormshield **Knowledge base**.

6.3 Monitoring router objects

The **Monitoring** > **Routers** menu makes it possible to monitor the quality of connections and the status of the gateways associated with an SNS firewall's router objects and deployed from SMC.

The grid is refreshed automatically every 60 seconds.

NOTE
If you modify a monitored router object or an SLA object, you must deploy the configuration again to refresh the monitored data.

In the monitoring panel, you can export and download monitoring data to a CSV file:

1. Click on **Exporting monitoring data** at the top of the panel,
2. Save the CSV file.

If you have filtered the data, only the lines that can be seen in the grid will be exported.

By default, data in the file is separated by commas. You can change the delimiter using the environment variable `SMC_CSV_DELIMITER`.

6.4 Implementing SD-WAN

SD-WAN (software-defined wide area network) is a set of software features with which interconnected secure networks and multiple WAN links can be more easily managed.

One of the functional approaches in SD-WAN is its ability to automatically and transparently choose the network links to take depending on the source of traffic and its associated performance constraints, such as accepted latency, availability rate, etc.

SMC allows this feature to be used on SNS firewalls from version 4.3.3 and upwards.

To implement SD-WAN on SMC, create SLA (*Software Level Agreement*) objects that establish these commitment criteria, then use them in router objects. Set link monitoring criteria as well in router objects.

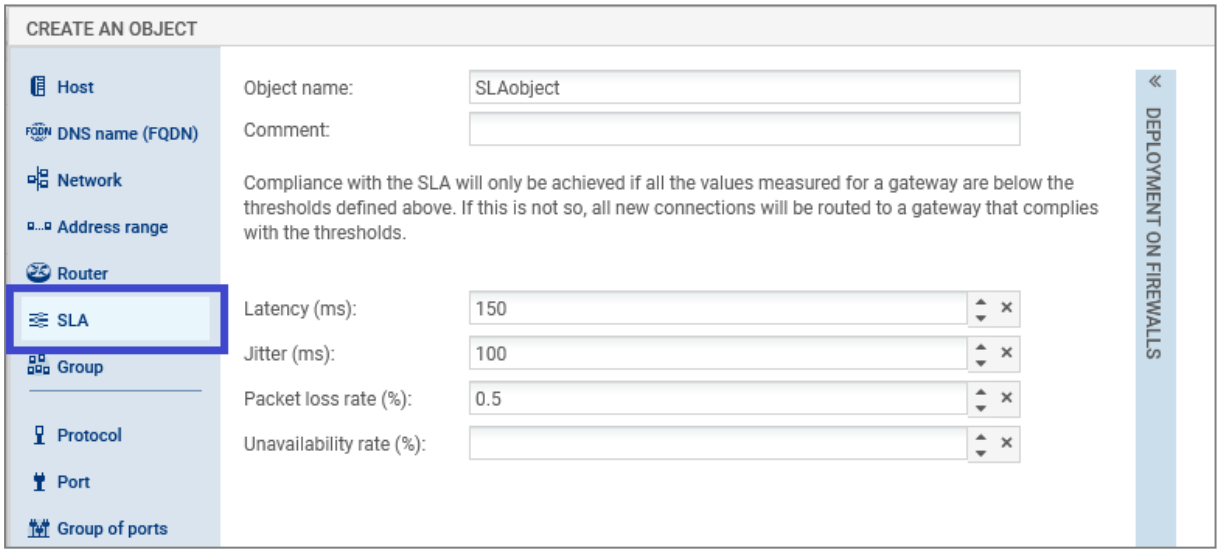
Next, create filter rules with these router objects to set up policy-based routing (PBR).

EXAMPLE
Create filter rules to optimize the selection of links for VoIP traffic.

For more information about the SD-WAN feature on SNS firewalls, refer to the technical note SD-WAN - Selecting the best network access.

6.4.1 Creating an SLA object

In SMC, specific criteria can be configured to determine whether a WAN link meets the quality level adapted to its type of traffic (VoIP, video, etc.).



To do so, for each traffic type, set an SLA commitment based on one or several thresholds out of the criteria below:

- Latency,
- Jitter,
- Packet loss rate,
- Unavailability rate.

As soon as any threshold is exceeded, the firewall will select another WAN link with a suitable SLA status for the traffic in question.

This SLA commitment is set through an SLA object that you can use in several router objects.

For the definition of these four commitment criteria, refer to the Router section in the *SNS User guide*.

To create a SLA object:

1. Create an SLA object in the **Objects** menu,
2. Configure the thresholds that must not be exceeded, for SMC to consider that a link meets the expected quality level and can be used by traffic. If any of its thresholds are exceeded, traffic will be directed to another gateway that meets the SLA commitment criteria.

Refer to the next section for information on how to use the SLA object in a router object.

SMC offers two SLA objects by default: Visio and SaaS/Productivity.

NOTE
SLA objects cannot be seen on SNS firewalls.

6.4.2 Configuring link monitoring in a router object

Monitoring options are available in router objects. These options make it possible to set the detection method and parameters to use to verify the availability of a router object's gateways:

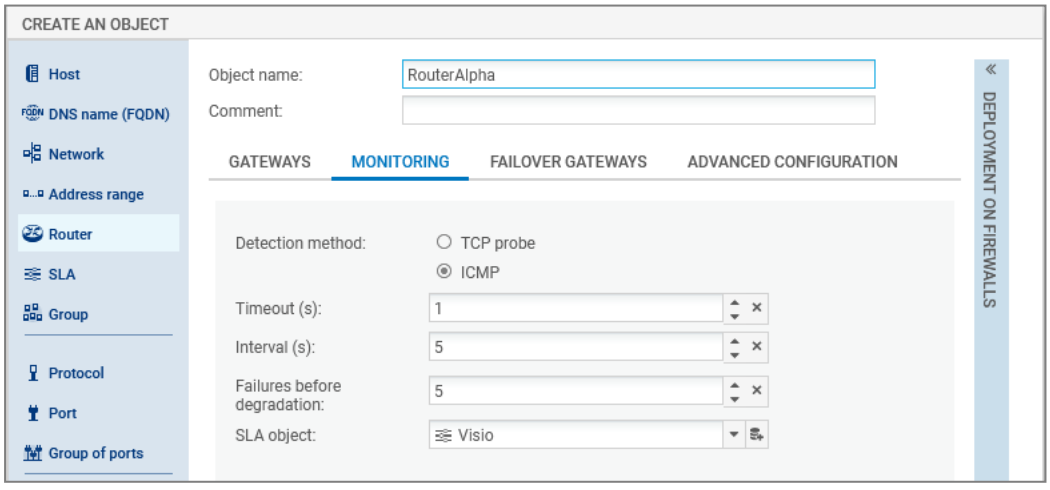
- Detection method,
- Expiry date,
- Interval,
- Failures before degradation.

To configure monitoring:

1. Display a router object's **Monitoring** tab,
2. Configure its settings. To understand the settings, refer to the Router section in the SNS *User guide*.

In the same **Monitoring** tab, you can associate an SLA object to set the thresholds that the gateways attached to the router object must meet.

These settings also apply to backup gateways defined in the object.



In the router monitoring panel, the status of connections and gateways associated with an SNS firewall can be monitored. For more information, refer to the section Monitoring router objects.

NOTE
If you modify a monitored router object or an SLA object, you must deploy the configuration again to refresh the monitored data.

6.5 Troubleshooting

Refer to this section for solutions to issues that may arise with interfaces and routing.

6.5.1 If you notice configuration errors after having renamed an interface from SMC

- *Situation*: You wish to rename an interface on a firewall that is managed by SMC, and the implicit objects Firewall_xx and Network_xx that are attached to this interface are not automatically renamed on SMC. This will cause configuration errors since the objects no longer reference an interface that exists on the firewall.
- *Cause*: Firewall_xx and Network_xx are dynamic objects that can be used in SMC in the configurations of several firewalls. They are not deployed on firewalls. As such, when you rename an interface, these dynamic objects will not be automatically renamed.
- *Solution*: To rename an interface, and work around the issue, we recommend that you follow the procedure indicated in Using dynamic objects from SMC.

7. Creating and monitoring VPN tunnels

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

- A policy-based VPN tunnel links firewall-protected networks or sub-networks to one another, and encrypts and encapsulates traffic between these networks. These networks are described in a policy. Such topologies are used in the standard operating mode.
- A route-based VPN tunnel uses IPsec virtual tunnel interfaces (VTIs) to link firewalls to one another. These interfaces are considered input and output points for the traffic passing through the tunnel and this traffic is defined by routes.

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

SMC 3.8 Version does not support VPN topologies in IPv6. If a topology includes network objects in IPv6, they will be ignored during deployment. If a topology relies on network objects with a dual IPv4/IPv6 configuration, only the configuration in IPv4 will be applied and the IPv6 configuration ignored.

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

WARNING
Write access privileges on all peers are required to create, modify or delete a VPN topology. For more information, refer to the section Restricting folder administrators' access privileges.

7.1 Creating policy-based VPN topologies

SMC allows creating and managing VPN tunnels that link networks or sub-networks protected by firewalls. These networks are described in a policy.

Such topologies are used in the standard operating mode.

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

- SNS firewalls in at least version 3.7, managed by the SMC server,
- External peers, meaning SNS firewalls or any other type of VPN gateway not managed by the SMC server.

SMC offers two VPN topologies: mesh or star.

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

Before configuring your topologies, you must:

- Create your traffic endpoints beforehand (Network, Host or Group objects) in the **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 the firewalls that SMC manages, and which are included in your topologies, and declare certification authorities beforehand as well. The corresponding procedures are described in the section Configuring a policy-based mesh topology.

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

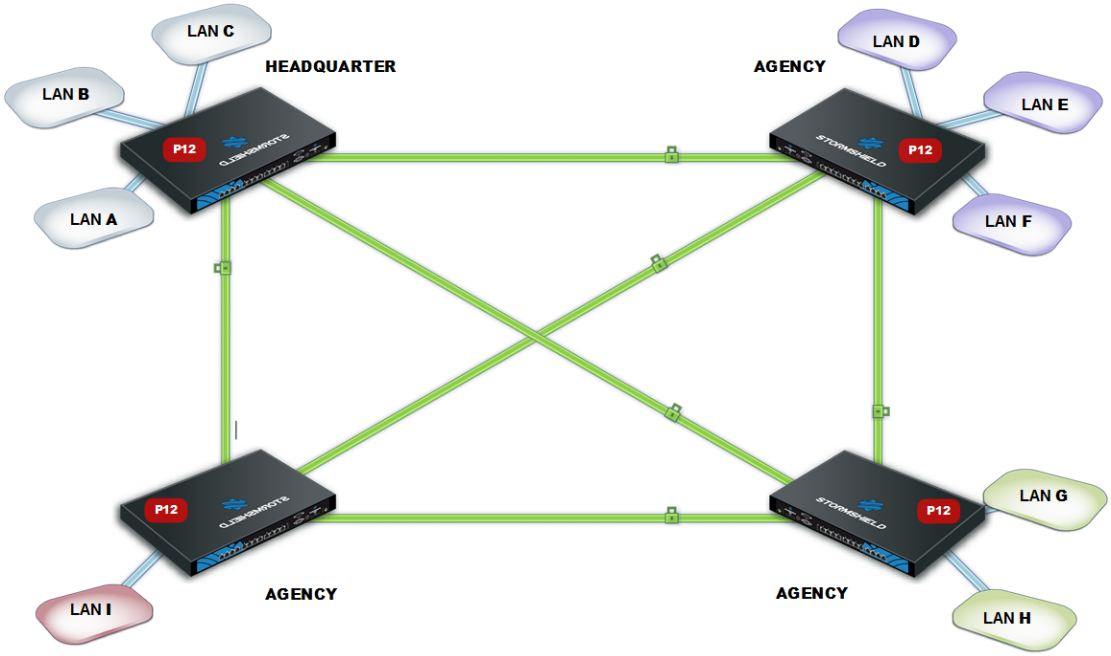
7.1.1 Configuring a policy-based mesh topology

Example of a scenario:

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

The authentication method selected is X509 certificate authentication.

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



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

Importing or declaring certificates for SNS firewalls

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

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

Declaring certificate authorities

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

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

Setting the CRL distribution points

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

Setting external distribution points

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

Setting SMC as a distribution point

The SMC server can act as a CRL distribution point for SNS firewalls:

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

Creating objects included in the topology

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

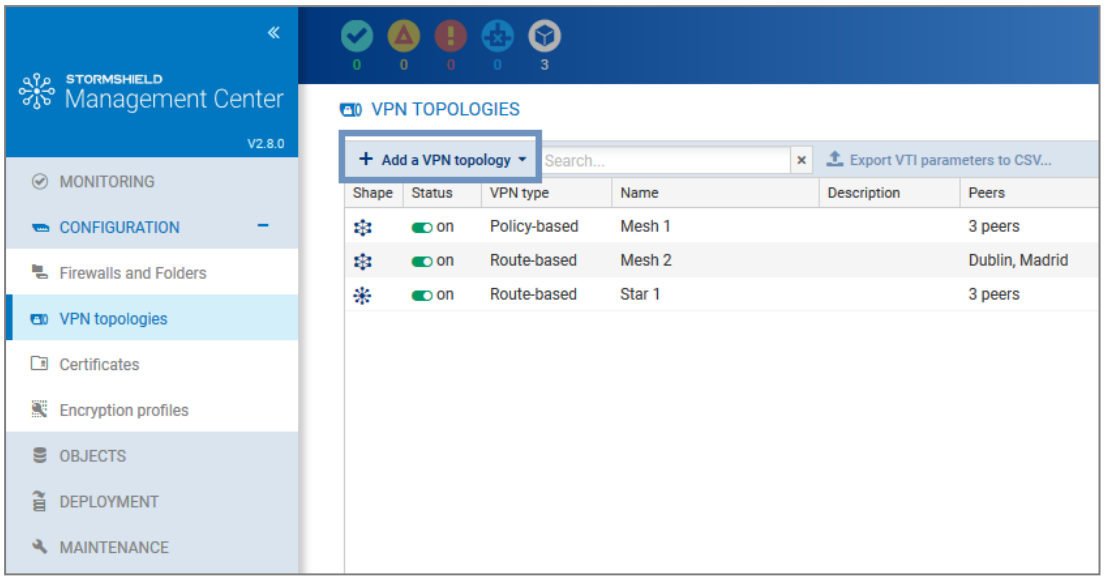
These may be Network, Host or Group objects.

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

Creating the VPN topology

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

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



2. In the window that opens, select **Policy-based VPN** and click on **Create the topology.**
3. Enter a name. A description is optional.
4. Select X.509 certificate authentication and select the certification authorities that issued the certificates for the firewalls involved in the VPN topology. If an authority's CRL has expired, a warning appears in the list of the **VPN topologies** menu.
5. If you wish to do so, indicate a post-quantum pre-shared key ID and its password. Such keys provide protection particularly from "store now, decrypt later" attacks. For more information, refer to the SNS User guide. This feature is available only when X.509 certificate authentication is used on firewalls in at least version 4.8.0, and only with IKEv2.
6. Select the encryption profile. The SMC server offers pre-configured profiles. Create your customized profiles in **Configuration > Encryption profiles**. Refer to the *SNS User guide* for more information on encryption profile options.
7. Select your topology peers. You can select connected or offline firewalls. You can also select firewalls that have never connected, on the condition that you have set a default custom or dynamic contact address in the **System** > **IPsec VPN** tab in the firewall settings. You need to hold write access privileges on the firewalls that you wish to select as peers. For more information, refer to the section Restricting folder administrators' access privileges.
8. Select the traffic endpoints associated with each of your peers. For further information on the **Contact address** and **Local address** settings, refer to the sections Defining the contact IP address of firewalls for VPN topologies and Selecting the output interface of firewalls for VPN topologies.
9. Click on **Apply**.
10. Deploy the configuration on the firewalls involved in the topology. The VPN configuration belongs to the firewall's global policy.

7.1.2 Configuring a policy-based star topology

Example of a scenario:

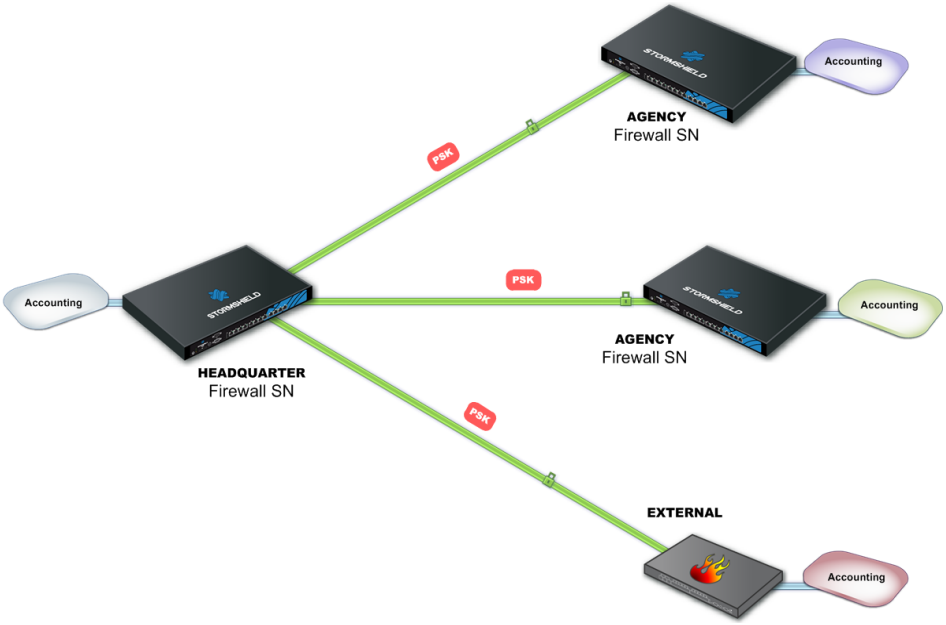
A company with its head office in Paris has two branches in Bordeaux and Madrid. The Accounting sub-network at the head office needs to exchange information with the Accounting

sub-networks in the branches. The company's three sites are protected by SNS firewalls managed by the SMC server.

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

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

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



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

Creating objects included in the topology

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

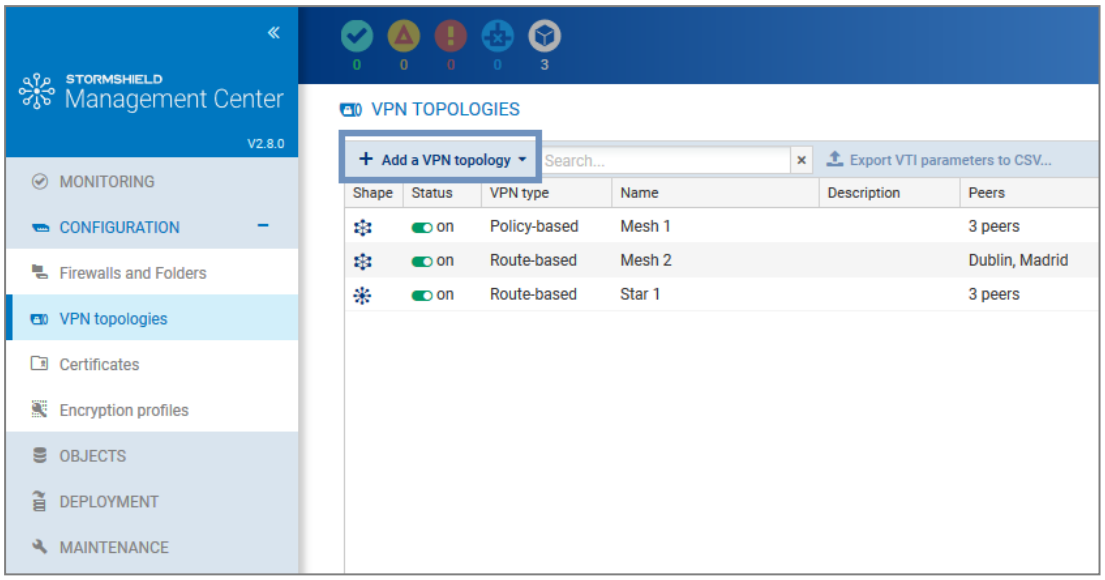
These may be Network, Host or Group objects.

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

Creating the VPN topology

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

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



2. In the window that opens, select **Policy-based VPN** and click on **Create the topology.**
3. Enter a name. A description is optional.
4. Select pre-shared key authentication.
5. Generate a random key.
6. The strongest encryption profile is selected by default. The SMC server offers pre-configured profiles. Create customized profiles in **Configuration > Encryption profiles**. Refer to the *SNS User guide* for more information on encryption profile options.
7. Choose the center of your topology. It will then show a star icon in the list of firewalls below, and the firewall will appear in bold.
8. If needed, check the option **Do not initiate the tunnels (Responder-only)** if the IP address of the center of the topology is dynamic. Only the peers will then be able to mount the VPN tunnel.
9. Select your topology peers. You can select connected or offline firewalls. You can also select firewalls that have never connected, on the condition that you have set a default custom or dynamic contact address in the **System** > **IPsec VPN** tab in the firewall settings. You need to hold write access privileges on the firewalls that you wish to select as peers. For more information, refer to the section Restricting folder administrators' access privileges.
10. Select the traffic endpoints associated with each of your peers. For further information on the **Contact address** and **Local address** settings, refer to the sections Defining the contact IP address of firewalls for VPN topologies and Selecting the output interface of firewalls for VPN topologies.
11. Click on **Apply**.
12. Deploy the configuration on the firewalls involved in the topology. The VPN configuration belongs to the firewall's global policy.

7.2 Creating route-based VPN topologies

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

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

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

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

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

From the SMC server, you can:

- Create route-based VPN topologies,
- Monitor these topologies,
- Define filter rules. SMC automatically generates VTI objects that represent peers in the topology, which can be used in these rules,
- Configure static routes and return routes if necessary and/or enable dynamic routing.

Virtual IPsec interfaces (VTI) are automatically created on firewalls with network configurations that SMC manages. These interfaces are listed in the **IPsec interfaces (VTI)** tab in a firewall's settings. For further information, refer to the section Configuring Ipsec interfaces (VTI).

If the topology contains firewalls with network configurations that SMC does not manage, you must manually create virtual IPsec interfaces on each firewall. The **Network managed by SMC** column during the selection of peers for a topology indicates whether the network configuration of the firewall is managed by SMC.

For more information, see the next sections.

NOTE
Modifying a route-based VPN topology may cause changes on associated virtual IPsec interfaces. For further information, refer to the section Configuring Ipsec interfaces (VTI).

SMC offers two VPN topologies: mesh or star.

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

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

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

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

NOTE
Comments associated with IPsec interfaces created by SMC are generated from the names of the

topology and of peers. If comments exceed 127 characters, they will be truncated. The same applies to comments for host VTI objects if they exceed 255 characters.

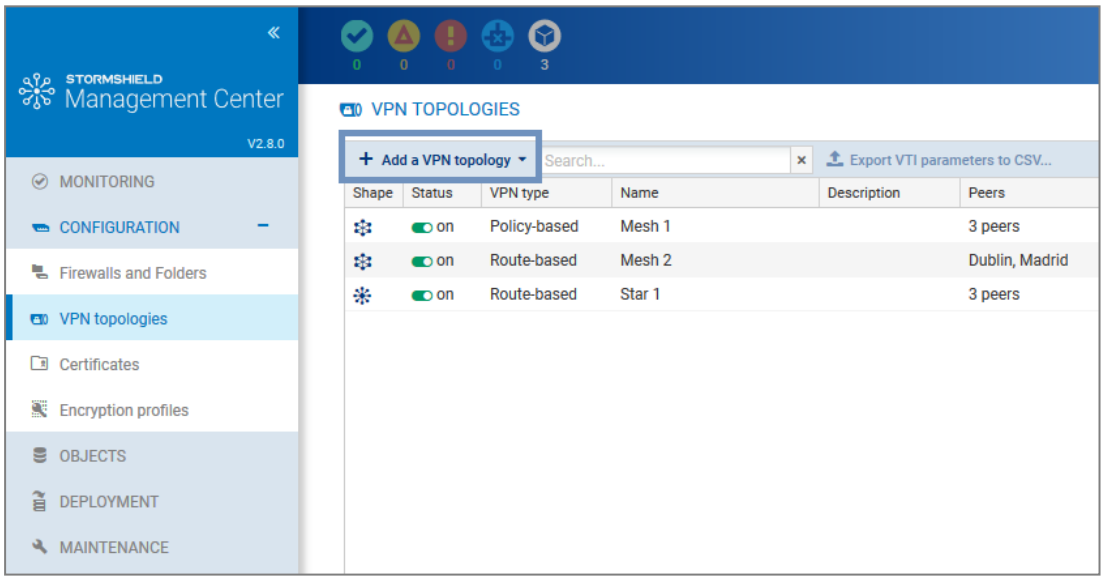
7.2.1 Configuring a route-based mesh topology

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

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

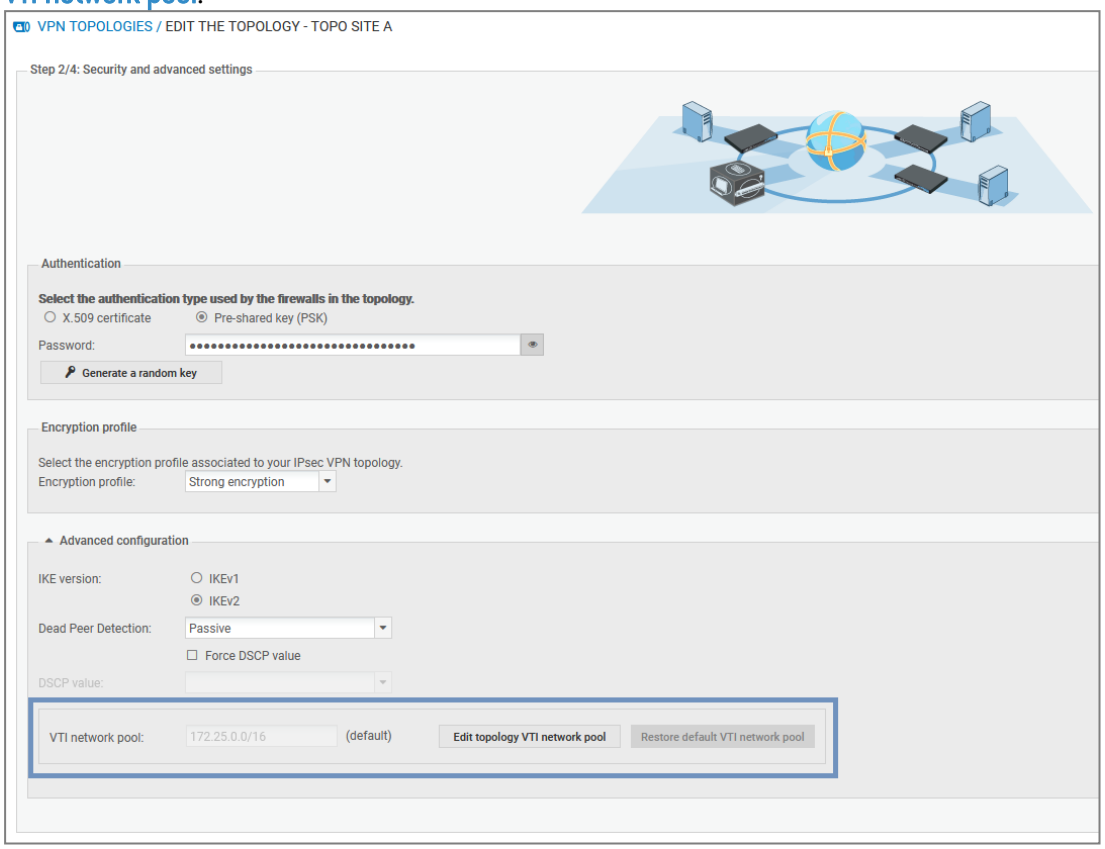
Follow the steps below to create a route-based VPN topology:

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



2. In the window that opens, select **Route-based VPN** and click on **Create the topology.**
3. Enter a name. A description is optional.
4. Choose the authentication type in the next step.
5. If you have chosen X.509 certificate authentication, you can indicate a post-quantum pre-shared key ID and its password. Such keys provide protection particularly from "store now, decrypt later" attacks. For more information, refer to the SNS User guide. This feature is available only on firewalls in at least version 4.8.0, and only with IKEv2.
6. Select the encryption profile. The SMC server offers pre-configured profiles. Create your customized profiles in **Configuration > Encryption profiles**. Refer to the *SNS User guide* for more information on encryption profile options.

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



8. Select your topology peers in the next step. You can select connected or offline firewalls. You can also select firewalls that have never connected, on the condition that you have set a default custom or dynamic contact address in the **System** > **IPsec VPN** tab in the firewall settings.
   To ensure optimal performance, you can select up to 50 peers by default. The environment variable `SMC_VPN_MESH_ROUTE_BASED_MAX_PEERS_INT` makes it possible to configure this limit. This limitation is valid only for mesh VPN topologies.
   You need to hold write access privileges on the firewalls that you wish to select as peers. For more information, refer to the section Restricting folder administrators' access privileges.
9. In the next step, double-click on the line of a firewall to open the **Peers and VTI** window:
   - For further information on the **Contact address** and **Local address** settings, refer to the sections Defining the contact IP address of firewalls for VPN topologies and Selecting the output interface of firewalls for VPN topologies.
   - IPsec VTIs will automatically be generated after the topology is created. Host VTI objects that represent remote peers will also be automatically generated. They can be used in routes or filter rules to set up routing. You will see them in your object database as "VTI_on_FW1_with_FW2_in_topologyname". These objects are automatically deployed on firewalls. For further information, refer to the section Defining the traffic routing policy.
10. Click on **Apply** to close the window.
11. Click on **Apply** again at the end of step 4/4 to generate the topology.

12. If the topology contains firewalls with network configurations that SMC does not manage, SMC will offer to download the IPsec interface *.csv* configuration file. IPsec interfaces must be created manually on these firewalls. Refer to the section Defining IPsec VTIs on SNS firewalls for further information. For firewalls with network configurations that SMC manages, SMC will automatically create the IPsec interfaces. Refer to Configuring IPsec interfaces (VTI). The *.csv* file indicates in the "created_by_smc" column whether interfaces were automatically created by SMC.
13. Deploy the configuration on the firewalls in the topology. The VPN configuration belongs to the firewall's global policy.

Your topology is still not operational at this stage. Follow the instructions in Defining IPsec VTIs on SNS firewalls if the topology includes firewalls with network configurations that SMC does not manage and Defining the traffic routing policy to complete the process of setting up a route-based VPN topology.

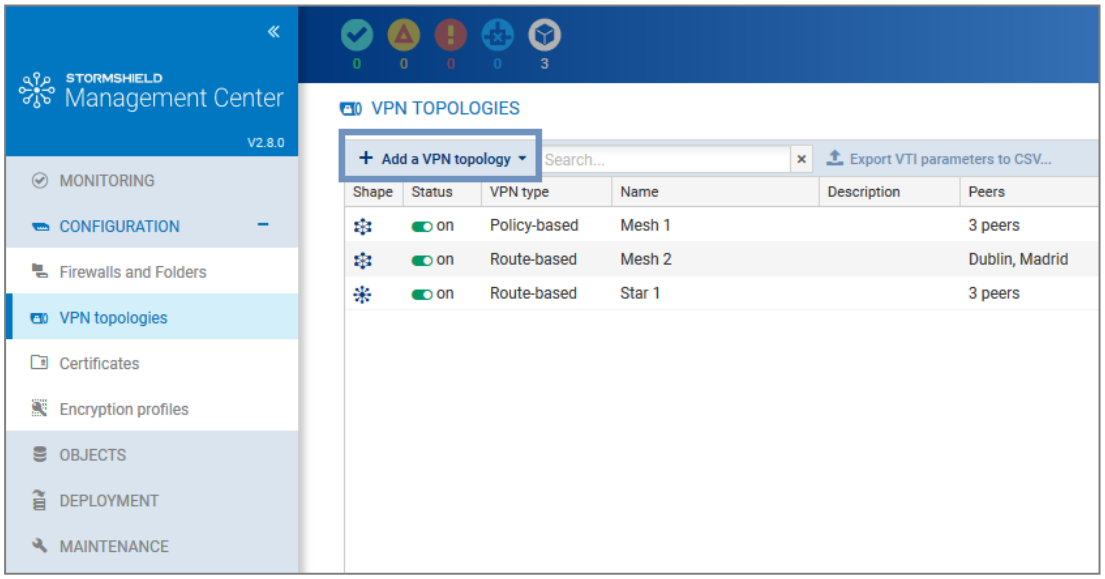
7.2.2 Configuring a route-based star topology

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

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

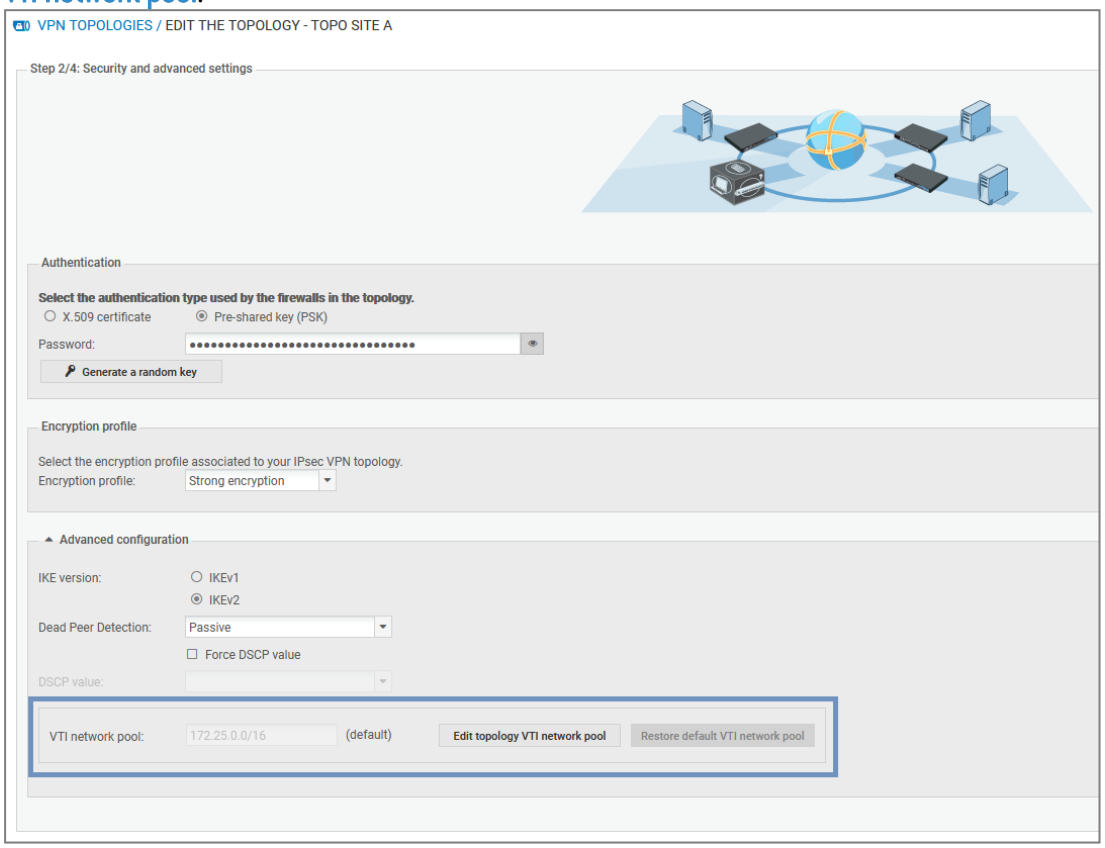
Follow the steps below to create a route-based VPN topology:

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



2. In the window that opens, select **Route-based VPN** and click on **Create the topology.**
3. Enter a name. A description is optional.
4. Choose the authentication type in the next step.
5. If you have chosen X.509 certificate authentication, you can indicate a post-quantum pre-shared key ID and its password. Such keys provide protection particularly from "store now, decrypt later" attacks. For more information, refer to the SNS User guide. This feature is available only on firewalls in at least version 4.8.0, and only with IKEv2.

6. Select the encryption profile. The SMC server offers pre-configured profiles. Create customized profiles in **Configuration** > **Encryption profiles**. Refer to the *SNS User guide* for more information on encryption profile options.
7. If you need to edit the default network pool for IPsec VTIs, expand the **Advanced properties** section. For more information on the **VTI network pool** field, refer to the section Editing the VTI network pool.



8. 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.
9. 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 SNS firewalls.
10. Select your topology peers. You can select connected or offline firewalls. You can also select firewalls that have never connected, on the condition that you have set a default custom or dynamic contact address in the **System** > **IPsec VPN** tab in the firewall settings. You need to hold write access privileges on the firewalls that you wish to select as peers. For more information, refer to the section Restricting folder administrators' access privileges.
11. In the next step, double-click on the line of a firewall to open the **Peers and VTI** window:
    - For further information on the **Contact address** and **Local address** settings, refer to the sections Defining the contact IP address of firewalls for VPN topologies and Selecting the output interface of firewalls for VPN topologies.
    - IPsec VTIs will automatically be generated after the topology is created. Host VTI objects that represent remote peers will also be automatically generated. They can be used in routes or filter rules to set up routing. You will see them in your object database as "VTI_on_FW1_with_FW2_in_topologyname". These objects are automatically deployed on firewalls. For further information, refer to the section Defining the traffic routing policy.

12. Click on **Apply** to close the window.
13. Click on **Apply** again at the end of step 4/4 to generate the topology.
14. If the topology contains firewalls with network configurations that SMC does not manage, SMC will offer to download the IPsec interface *.csv* configuration file. IPsec interfaces must be created manually on these firewalls. Refer to the section Defining IPsec VTIs on SNS firewalls for further information. For firewalls with network configurations that SMC manages, SMC will automatically create the IPsec interfaces. Refer to Configuring IPsec interfaces (VTI). The *.csv* file indicates in the "created_by_smc" column whether interfaces were automatically created by SMC.
15. Deploy the configuration on the firewalls in the topology. The VPN configuration belongs to the firewall's global policy.

Your topology is still not operational at this stage. Follow the instructions in Defining IPsec VTIs on SNS firewalls if the topology includes firewalls with network configurations that SMC does not manage and Defining the traffic routing policy to complete the process of setting up a route-based VPN topology.

7.2.3 Defining IPsec VTIs on SNS firewalls

This step is necessary for firewalls with network configurations that SMC does not manage. For more information, see the section Configure network interfaces.

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

Refer to the *SNS User guide* as well for more information on how to create IPsec VTIs.

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

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

Now follow the last step.

7.2.4 Defining the traffic routing policy

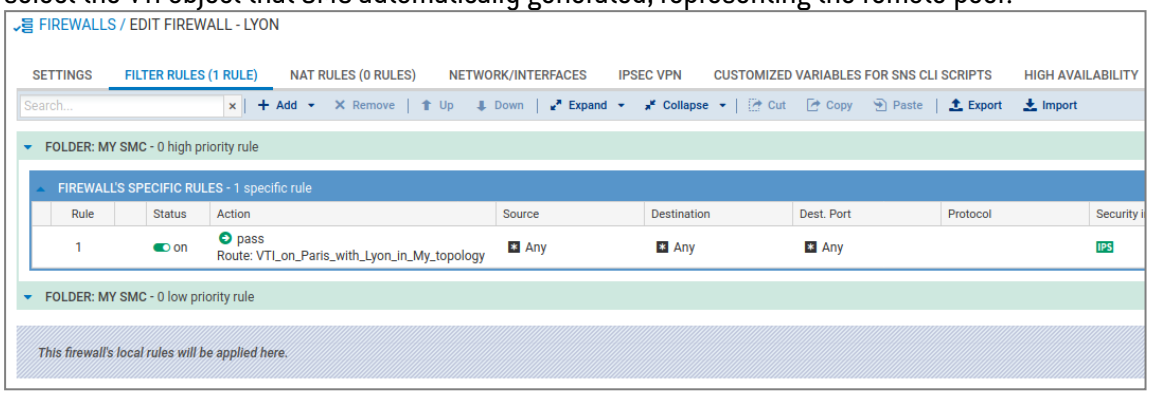
You can configure static, dynamic or return routes to direct traffic to IPsec VTIs. You can also define filter rules to set up routing.

You can perform these operations directly from SMC if the firewalls included in the topology are in at least version 4.2.4 and if network configuration has been enabled on SMC.

Otherwise, you must configure the routes directly on your firewalls.

If you are setting up policy-based routing:

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



2. Create return routes in each firewall's Routing tab.

If you are not using policy-based routing (PBR):

1. On each firewall, create static routes dedicated to the remote peer's IPsec VTIs.
2. Configure a filter policy for each firewall to allow traffic to go through the tunnel.

For help on how to configure routes on your firewalls, refer to the *SNS user guide* and the Technical note dedicated to IPsec VTIs.

Refer to the section Configuring the network and routing as well.

7.2.5 Editing the VTI network pool

WARNING
Folder administrators whose read access privileges are restricted to certain folders on SMC cannot perform this operation. For more information, refer to the section Restricting folder administrators' access privileges.

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

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

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

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

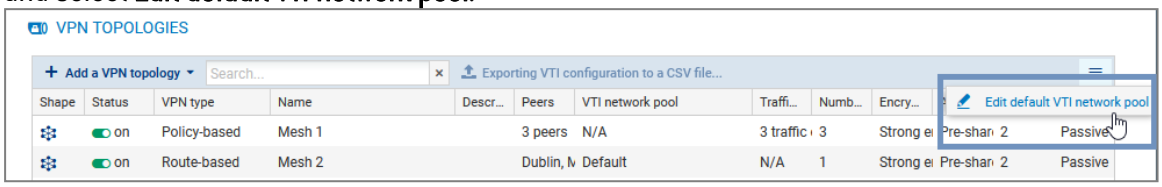
This default network pool is the same across all topologies. If necessary, you can edit the global pool, or a pool specific to a topology.

IMPORTANT
If you edit a topology's network pool of IPsec interfaces after the topology is created and deployed, you should verify the configuration of the interfaces already created on your firewalls, if SMC does not manage the network configuration.

Editing the default global network pool

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

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



2. Indicate the new default network pool.

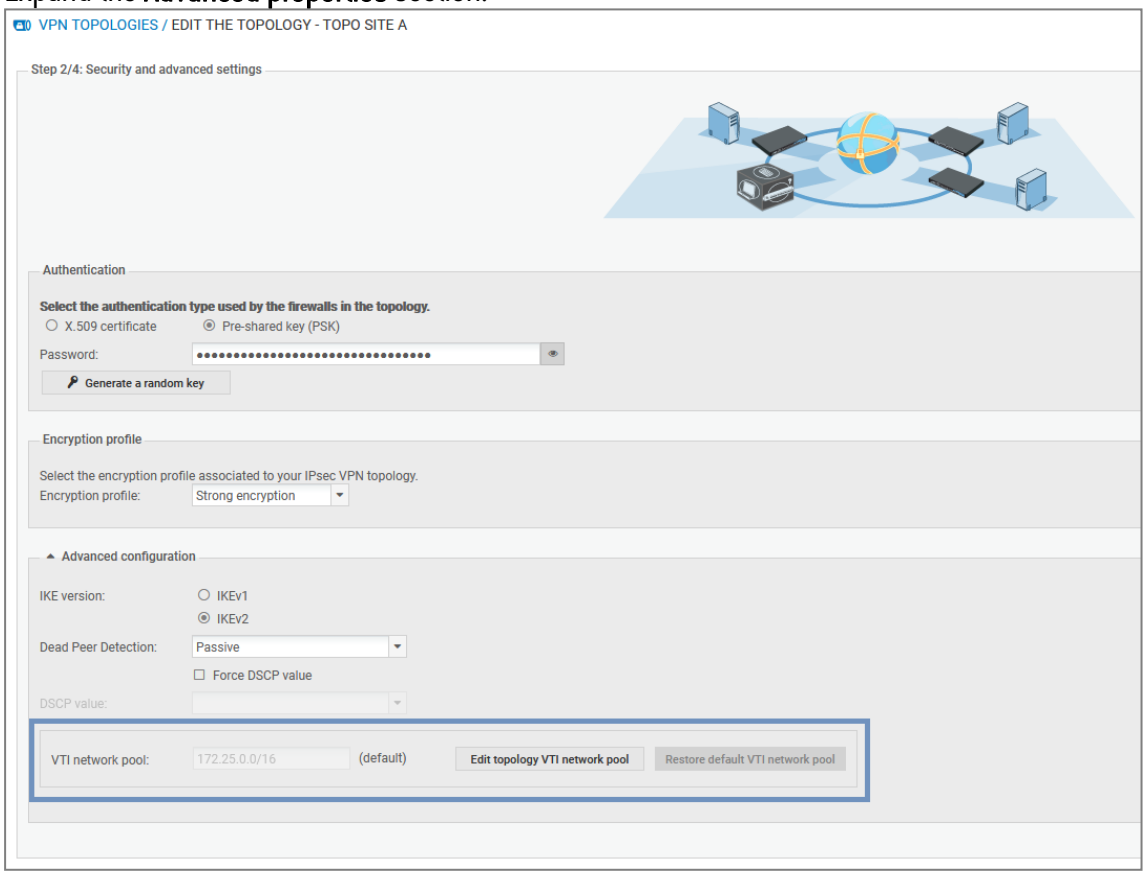
This change does not affect existing topologies, which will keep the final pool when they are created.

Editing a topology's specific network pool

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

To edit it for an existing topology:

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



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

7.2.6 Troubleshooting

Refer to this section to resolve frequently encountered issues while creating route-based VPN topologies.

Tunnels in route-based VPN topologies are not operational.

- *Situation*: In Monitoring view, a topology appears as non-operational.
- *Cause*: If the topology includes SNS firewalls with network configurations that SMC does not manage, it is possible that not all the virtual IPsec interfaces were created manually on the firewalls in question.
- *Solution*: Ensure that all the virtual IPsec interfaces were created on the firewalls. To see the list of firewalls in the topology with network configurations that SMC does not manage, refer to the **Network managed by** SMC column during the selection of peers for a topology. To access this step, in **Configuration** > **VPN topologies**, double-click in the **Peers** column of the topology in question.

For more information, refer to Configuring a route-based mesh topology and Defining IPsec VTIs on SNS firewalls.

7.3 Managing certificates and certification authorities

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

To perform these operations, you need to hold write access privileges on the folders containing the firewalls to which these changes apply. For more information, refer to the section Restricting folder administrators' access privileges.

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

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

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

	Certification authorities	X509 certificates	SCEP/EST certificates
Icons when scrolling over the line			
Possible actions	• Changing the certification authority • Updating the certification authority • Seeing references • Removing from the SMC server	• Updating the certificate • Seeing references • Removing from the SMC server	• Renewing the certificate • Seeing references • Removing from the SMC server

WARNING
The following characters are not supported in certificate names:

,	< and >
+	#
=	;
"	double space

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

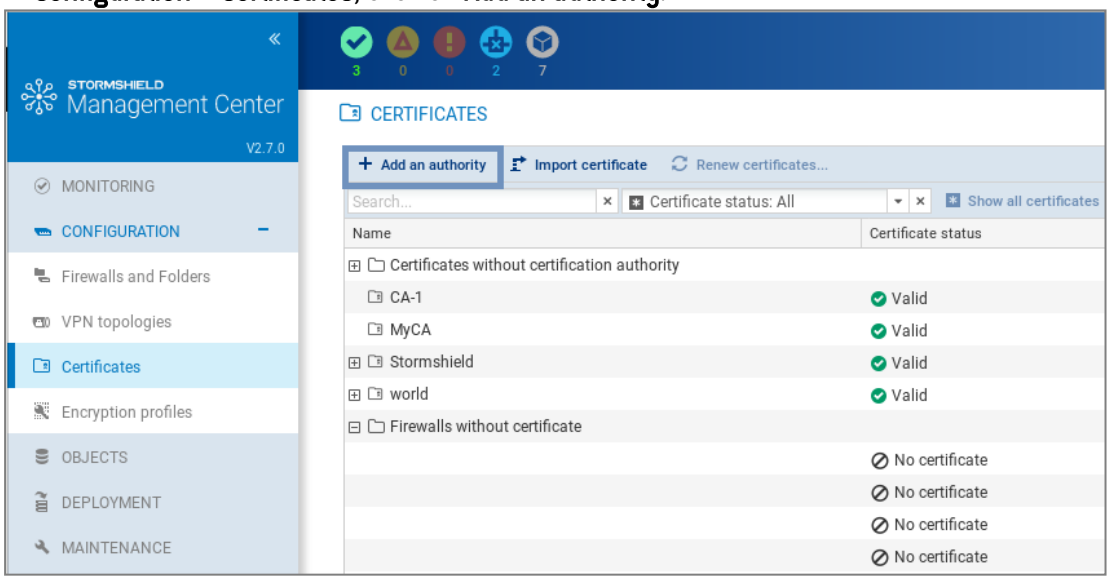
7.3.1 Adding a certification authority or chain of trust

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

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

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

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



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

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

7.3.2 Updating a certificate authority or chain of trust

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

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

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

7.3.3 Deleting a certificate authority or chain of trust

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

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

7.3.4 Importing or declaring a certificate for a firewall

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

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

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

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

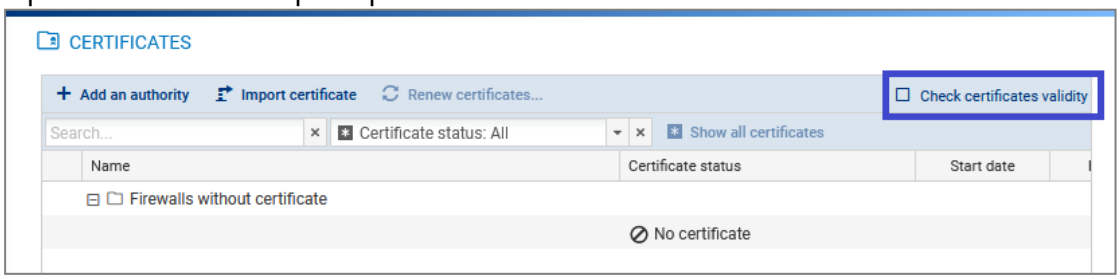
If you have imported several X509 certificates for a firewall, to find out which certificate is used by default in VPN topologies, refer to the section Changing the certificate used by default in VPN topologies.

7.3.5 Checking certificate validity

You can configure SNS firewalls to look up the CRL (certificate revocation list) when they need to verify the validity of the certificates that VPN tunnel peers use.

This verification is mandatory in DR (*Diffusion Restreinte*) mode.

1. Select **Check certificate validity** at the top right side to make the presence of a valid CRL mandatory, and therefore detect revoked certificates. In the absence of a valid CRL, or if the peer presents a revoked certificate, the VPN tunnel cannot be set up. This option is equivalent to the CRLRequired parameter on SNS firewalls.



2. For each certificate, configure if necessary the local IP address to use for the verification and frequency of verifications. To do so:
   a. Show the **Local IP address for CRL verification** and/or **CRL verification frequency** columns by scrolling over the name of a column and clicking on the arrow, then on **Columns**.
   b. Select a certificate.
   c. In the **Local IP address for CRL verification** column, select the desired address. *Any* can be used by default.
   d. In the **CRL verification frequency** column, enter the number of seconds between each verification. The default frequency is 21600 seconds, or 6 hours.

7.3.6 Updating a firewall's X509 certificate

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

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

7.3.7 Renewing firewall certificates obtained via SCEP or EST

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

If necessary, you can choose the SNS firewall address that must be used for the renewal of the certificate.

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

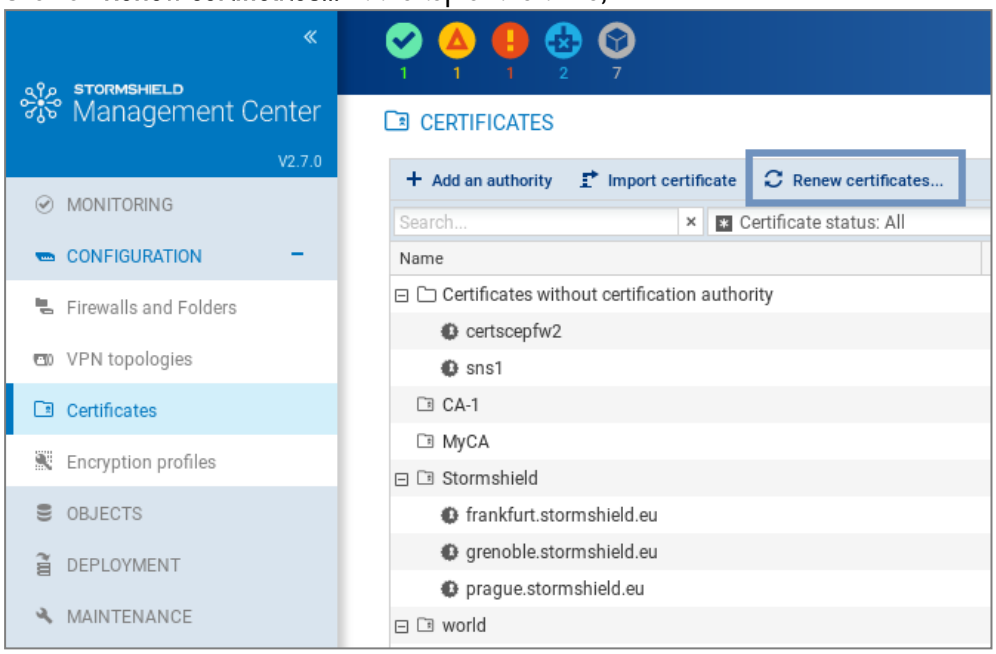
- SNS firewalls must be at least in version 3.9.0 for SCEP and at least 3.10 or 4.1 for EST,
- the SNS firewalls must be connected.

To choose a specific address for a certificate renewal:

1. Show the **Local IP address for renewal** column by scrolling over the name of a column and clicking on the arrow, then on **Columns**.
2. Click in the column of a certificate and select the desired address of the SNS firewall from the drop-down list.

To renew certificates:

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



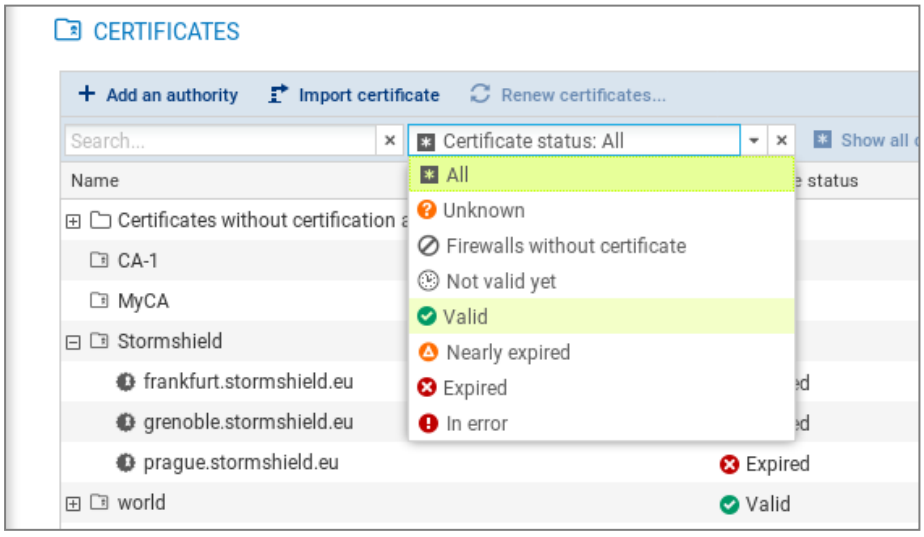
2. Select the certificates to be renewed,
3. Confirm the renewal of the certificates at the bottom of the table. If an error occurs, refer to the server logs for more information.

TIP

To renew a single certificate, scroll over its line in the table and click on in the **Certificate status** column.

7.3.8 Explanations regarding certificate statuses

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



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

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

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

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

7.4 Defining the contact IP address of firewalls for VPN topologies

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

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

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

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

7.4.1 Defining a firewall's default contact address

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

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

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

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

7.5 Selecting the output interface of firewalls for VPN topologies

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

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

7.5.1 Creating the Host Object that corresponds to the interface

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

7.5.2 Selecting a firewall's output interface on SMC

On SNS 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 **System > IPsec VPN** tab, select the desired value for the local address in **Default local address**. 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 **Local address** column.
3. In the **VPN local address** field, select an interface.

7.5.3 Configuring a static route on the firewall (optional)

Depending on your firewall's routing configuration, create a static route, if necessary, for each peer of the VPN tunnel 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 how to create routes on SMC, refer to the section Configuring the network and routing.

7.6 Editing, deleting and checking usage of a VPN topology

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

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

If the peers from the same topology are firewalls that have been organized in several folders managed by different folder administrators, only a general administrator or an administrator with write access privileges on all the folders in question can modify or delete it. For more information, refer to the section Restricting folder administrators' access privileges.

To edit a topology:

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

Redeploy the configuration after this operation.

To delete a topology:

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

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

To check whether VTI objects are in use:

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

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

To check whether generated VTI objects are in use:

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

7.7 Managing packet fragmentation

The Path MTU Discovery value and fragment size can be defined in the advanced settings via the **Configuration** > **VPN topologies** menu.

Parameter	Description

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

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

7.8 Disabling a VPN topology

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

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

New topologies are enabled by default when you create them.

To perform this operation, you need to hold write access privileges on all firewalls included in the topology. Otherwise, a general administrator will be able to disable it. For more information, refer to the section Restricting folder administrators' access privileges.

To disable a topology:

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

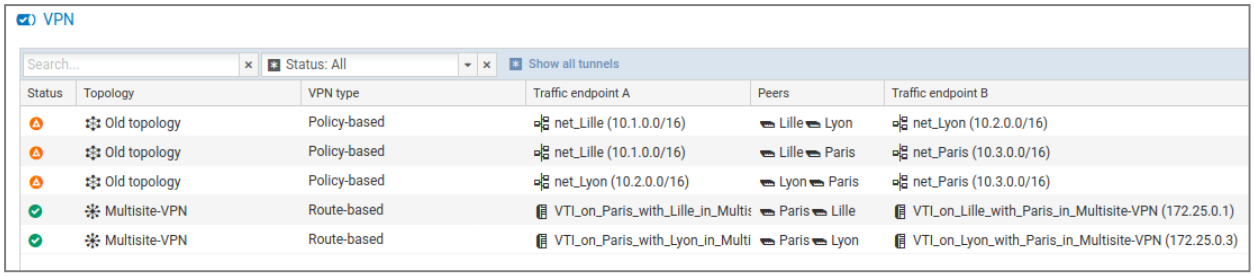
If a topology that has already been deployed is disabled in SMC, and if there has not been any new deployment in the meantime, its tunnels will always remain visible in the monitoring window.

7.9 Monitoring the status of VPN tunnels

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

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

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



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

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

7.10 Setting the PRF in a custom encryption profile

In VPN IKEv2 topologies, the PRF (Pseudo-random Function) is an algorithm that is negotiated during phase 1 (IKE phase) of the IPsec tunnel.

It is supported on SNS firewalls from version 4.2.3 and upwards. For lower versions, the value of the PRF is not deployed.

SMC offers default encryption profiles that cannot be edited. You can create your own encryption profiles if you wish to customize the fields.

NOTE
To ensure compatibility with "*Diffusion Restreinte* (DR)" mode, the PRF of an IKEv2 encryption profile must be set to SHA256. For more information on DR mode, refer to Using Diffusion Restreinte mode on SNS firewalls.

To create an encryption profile and configure the PRF:

1. In **Configuration** > **Encryption profiles**, click on **Create an encryption profile**.
2. Enter a name and description if necessary.
3. In the **IKE** tab, indicate the algorithm that must be negotiated as a PRF (**Pseudo-random function** field).
4. Fill in the other fields. For information on the fields, refer to the SNS *User guide*.
5. Click on **Create**.

8. Creating filter and NAT rules

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

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

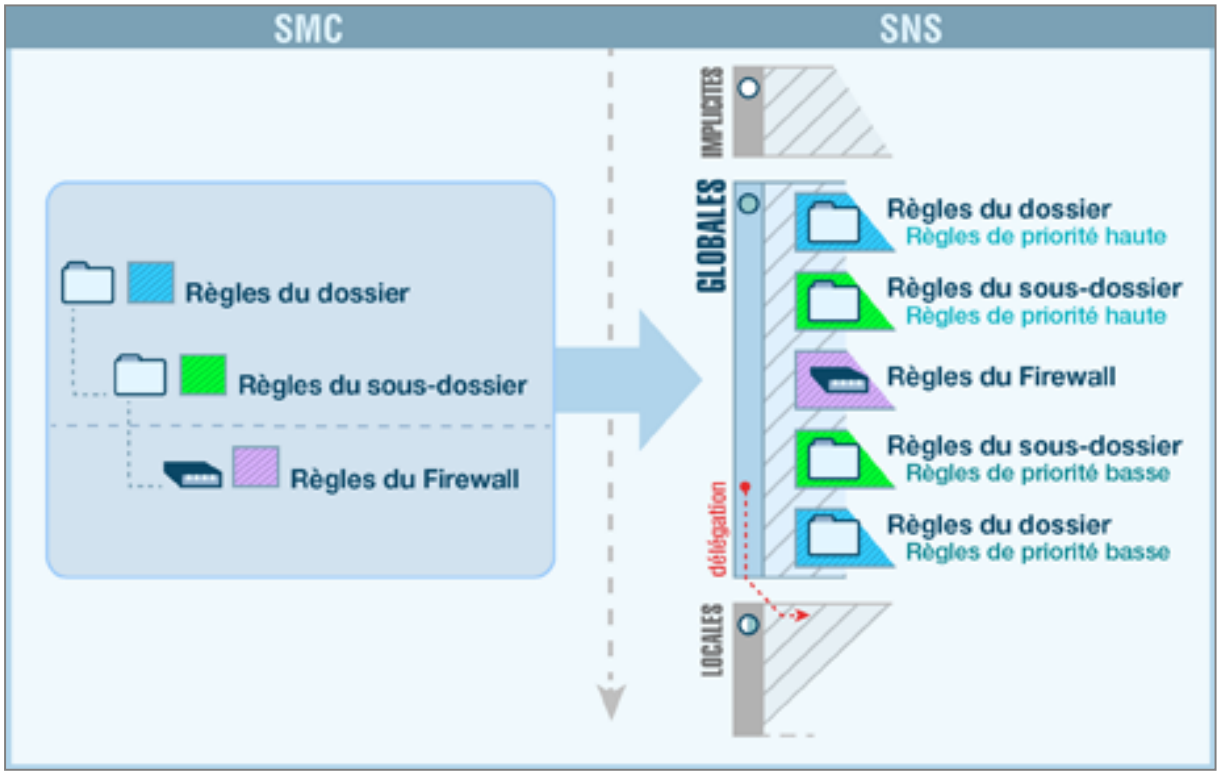
To perform these operations, you need to hold write access privileges on the folders in question in the SMC web interface. For more information, refer to the section Restricting folder administrators' access privileges.

For further details on each menu and option for rule configuration, refer to the SNS *User guide*.

Rules can be defined in the **Filtering and translation** tab from the **Configuration** > **Firewalls and folders** menu or from a firewall's settings.

8.1 Understanding the order in which rules are read

To view a firewall's filter or NAT rules, in the **Monitoring** > **Firewalls** menu, double click on a firewall and select the **Filtering and translation** tab. Rules are arranged by order of priority.



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

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

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

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

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

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

8.2 Use case examples

8.2.1 Managing an environment without rule sharing

We will use the example of a service provider who manages SNS 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:

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

8.2.2 Managing an environment with shared and specific rules

We shall use the example of a service provider who also administers SNS 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:

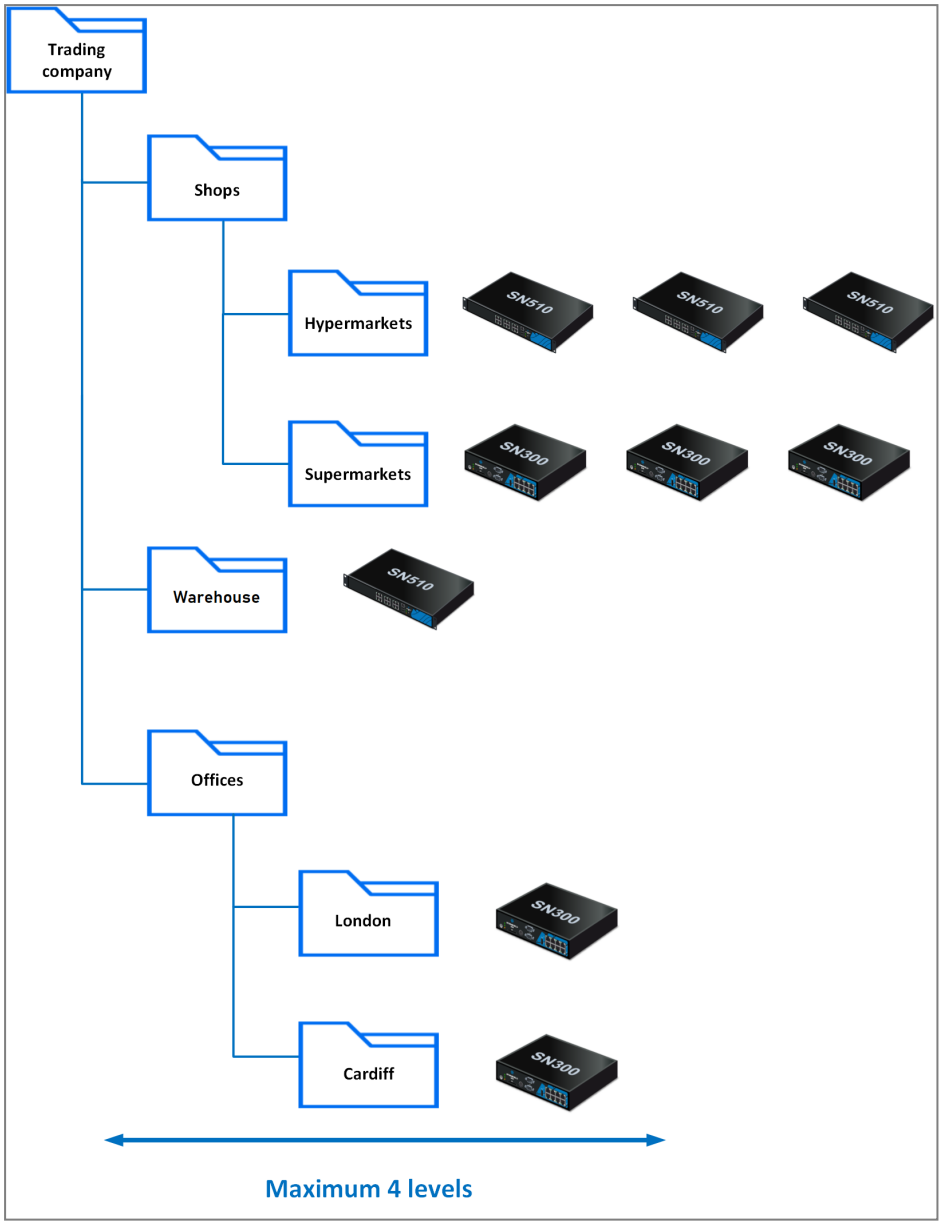
- Define the rules shared by all firewalls in the **MySMC** folder, for example to provide all firewalls with access to its datacenter. For this purpose, a variable object will be used: a Host object representing a firewall interface. A single rule and a single object will therefore suffice for all firewalls. For more information, please refer to the section Managing objects.
- Set specific rules on each firewall from SMC, going to the firewall's **Filtering and translation** tab.

- If necessary, define a "Block all" rule as the last low-priority rule in the **MySMC** folder in order to ignore the rules found in the firewalls' local security policy.
- Deploy the configuration on the firewalls. These rules will be deployed in the firewalls' global security policy.

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

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

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



The central administrator must therefore:

- Define the rules shared by all firewalls in the **MySMC** folder using variable objects. For more information, please refer to the section Managing objects.
- Define rules shared by warehouses/offices/stores in the corresponding folders and sub-folders.
- Set specific rules on some firewalls from SMC, by going to the firewall's **Filtering and translation** tab.
- Select the action **Delegate** for the rules concerned in the rule **Action** menu.
- Define a "Block all" rule as the last low priority rule on the root folder **MySMC**.
- Deploy the configuration on the firewalls. These rules will be deployed in the firewalls' global security policy.

8.2.4 Managing a multi-site pool with shared rule sets

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

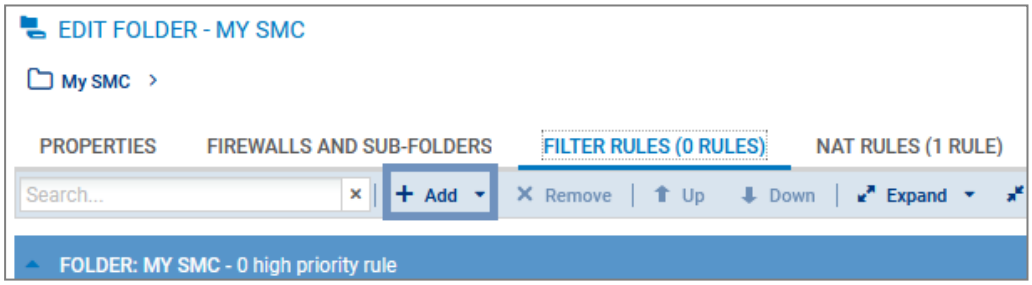
- The central administrator wants to define all filter and NAT rules for a specific department.
- The administrator does not wish to connect to the firewall of each department to define the rules.

The central administrator must therefore:

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

8.3 Creating filter and NAT rules

1. In **Configuration > Firewalls and folders**, browse until you reach the level of the folder to which you wish to apply a rule or until you reach a specific firewall. In the case of specific rules, go directly to the firewall's settings as well from **Monitoring** view.
2. Open the **Filtering and translation** tab and select **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 **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** (if the rule applies to a folder or rule set).
     - In **Destination > Advanced configuration > Outgoing interface**, click on **Customized interface** (if the rule applies to a folder or rule set).
     - Menu **Action** > **Quality of Service** > **Queue**.
     - Menu **Action** > **Quality of Service** > **ACK queue**.
   - Refer to the *SNS User guide* 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 and local rules in read-only. You can therefore view all the rules that apply to a firewall on a single screen, in the order in which they are applied.

8.4 Creating rule sets

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

8.4.1 Creating a rule set

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

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

8.4.2 Assigning rule sets to a firewall

You need to hold write access privileges on the firewall in question to assign rule sets to it. For more information, refer to the section Restricting folder administrators' access privileges.

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

- In **Configuration > Rule set**:

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

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

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

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

8.4.3 Editing rule sets for a firewall

You need to hold write access privileges on the firewall in question to perform the following operations. For more information, refer to the section Restricting folder administrators' access privileges.

From a firewall's security policy, you can:

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

8.4.4 Importing or exporting rule sets

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

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

8.4.5 Deleting rule sets

You can delete a rule set only when:

- It is not used by any firewall.
- It is used by firewalls on which you have write access privileges.

For more information, refer to the section Restricting folder administrators' access privileges.

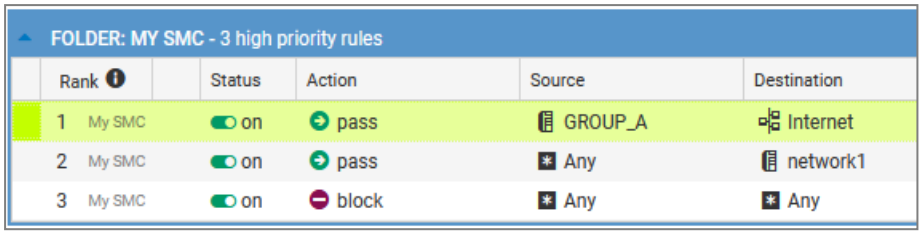
To delete a rule set:

- In **Configuration** > **Rule sets**, click on the red cross on the row of a rule set.

8.5 Identifying the rules

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

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



8.6 Changing the order in which rules are executed

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

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

Moving rules within the same firewall or folder

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

and **Down**

buttons.

-or-

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

-or-

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

Moving rules into another folder or onto another firewall

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

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

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

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

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

To find out the name of a rule in SMC:

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

4. Scroll over the **Columns** menu,
5. Select the **Name** column.

- or -

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

8.8 Removing rules

- Press **DELETE**.

-or-

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

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

8.9 Removing rule sets

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

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

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

8.10 Importing and exporting filter and NAT rules

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

By importing and exporting logs, you can:

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

8.10.1 Importing rules from a CSV file

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

Creating the CSV file

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

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

To export the CSV file from a firewall:

1. Connect to the firewall.
2. Go to the menu **Security policy ⇒ Filtering and NAT**.

3. At the top of the panel, choose whether to display the global or local policy that you wish to export. Only rules from the active slot will be exported.
4. Click on **Export**.

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

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

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

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

Importing rules from the web interface

You need read/write privileges to import rules.

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

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

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

In case of error, refer to the import summary.

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

Importing rules in command line

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

Various options can be added to this command.

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

Rule sets cannot be imported in command line.

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

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

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

If you are importing rules and objects referenced in rules:

1. Export the list of objects in CSV format from an SNS firewall by following the procedure in the section Creating the CSV file.
2. Copy both CSV files (rules and objects) on the SMC server using the SSH protocol in the */tmp* folder for example.
3. Log in to the SMC server via the console of your hypervisor or in SSH.
4. Depending on the rule destination, type the command:
   - `smc-import-rules /tmp/rules-file.csv --objects /tmp/objects-file.csv --firewall destination-firewall`: the destination of these rules is a firewall,
   - `smc-import-rules /tmp/rules-file.csv --objects /tmp/objects-file.csv --folder destination-folder`: the destination of these rules is a folder, Rules are imported to the high-priority rules of a folder by default. To import rules to low-priority rules, add `--low-priority` at the end of the command or indicate the value "low" in the column *#smc_folder_prio* in the CSV file (last column). If the file was exported from a firewall, there is no such column; add it manually.

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

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

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

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

8.10.2 Exporting rules to a CSV file

You only need read privileges to export rules.

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

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

When rules are exported from a firewall (in SMC), the entire policy is exported – the rules of the firewall and its parent folders. The *#folder* column in the file shows the name of the folder that contains each rule. The *#ruleid* and *#rankid* columns indicate the number that identifies the rule in the policy and its position in a folder. For more information, refer to the section Identifying the rules.

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

8.10.3 Importing rules from connected firewalls

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

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

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

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

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

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

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

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

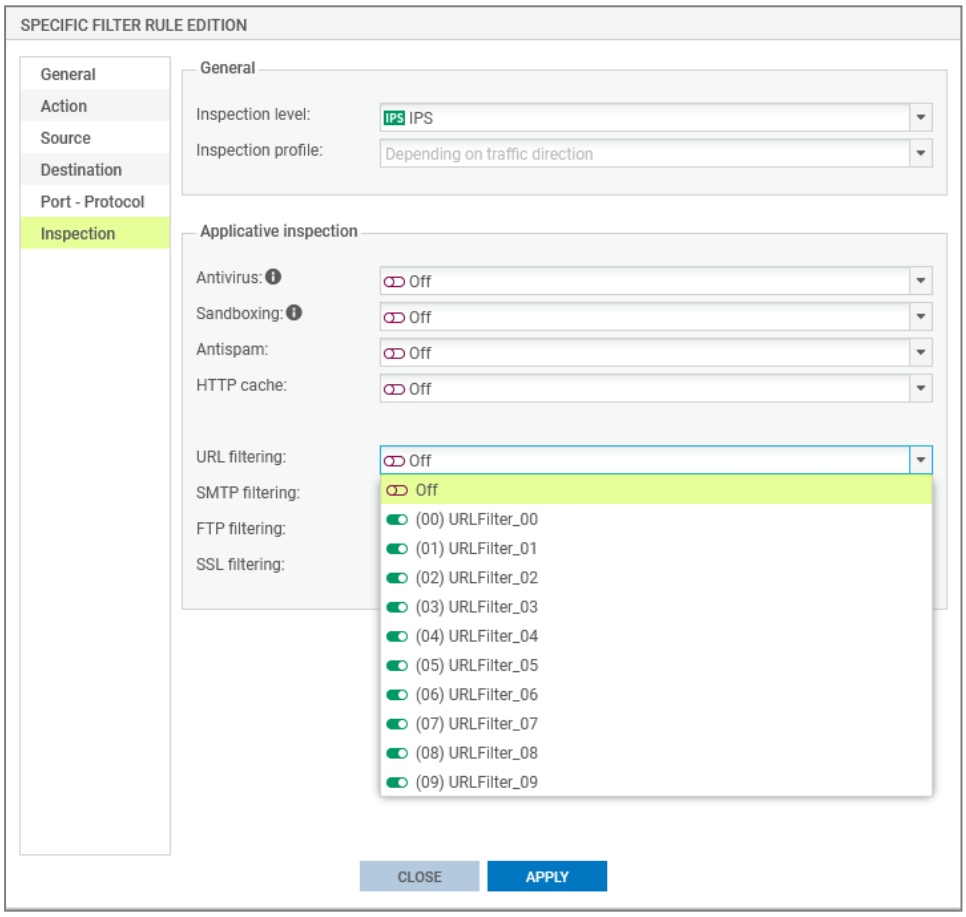
1. Import rules from a firewall onto the SMC server by following the procedure set out in Importing rules from connected firewalls.
2. The Use case examples may give you ideas on choosing how to organize newly imported rules.
3. In SMC, deploy the rules on the firewall in question. They will appear in the firewall's global policy and will be applied as a priority.
4. Ensure that this new organization functions properly.

5. If necessary, define a "Block all" rule as the last low-priority rule in the **MySMC** folder in order to ignore the rules found in the firewalls' local security policy.
6. When the process is complete, delete the rules that have been migrated from the firewall's local policies to SMC.

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

8.12 Managing URL filtering on SNS firewalls from SMC

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



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

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

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

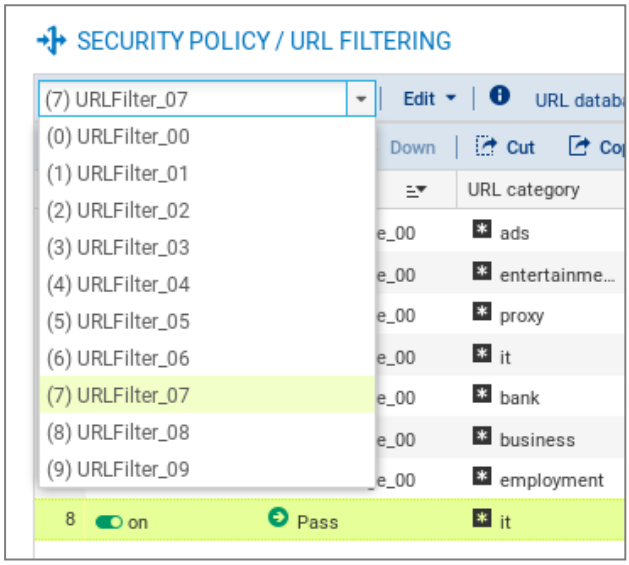
IMPORTANT
The template firewall and the target firewalls must be in the same version.

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

8.12.1 Creating the template URL filtering policy

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

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



8.12.2 Saving the URL filtering policy of the template firewall

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

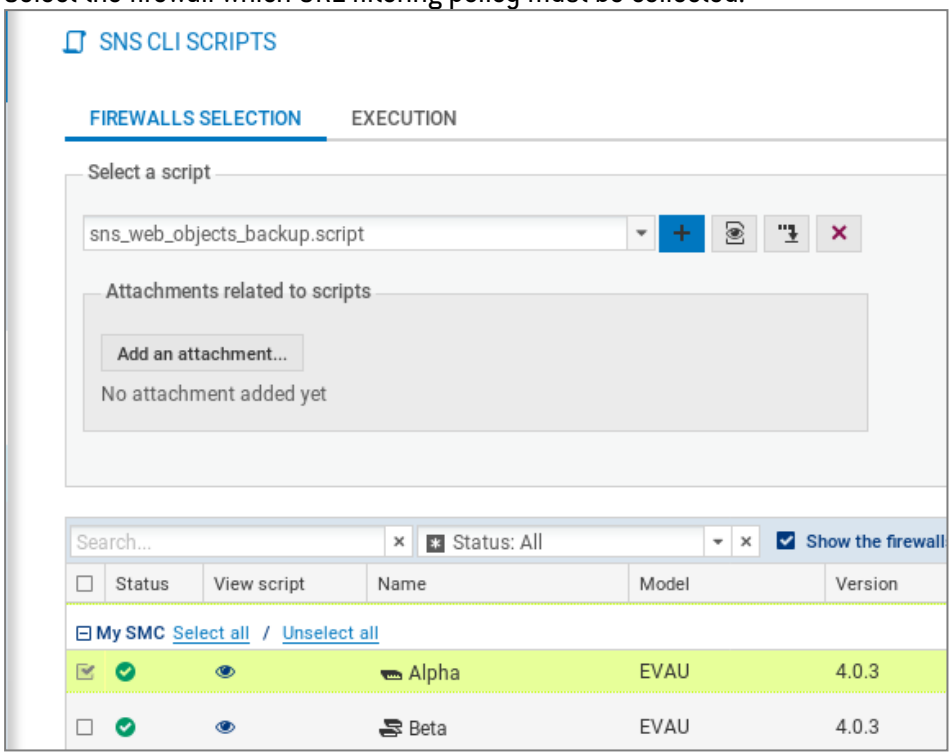
```
#######################################################################
# Save URLs, Certificate names, URL and CN groups and the             #
# URL base of a SNS #firewall                                         #
#                                                                     #
# The $SAVE_TO_DATA_FILE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

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

To use the script:

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

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



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

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

8.12.3 Deploying the template URL filtering policy

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

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

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

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


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

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

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

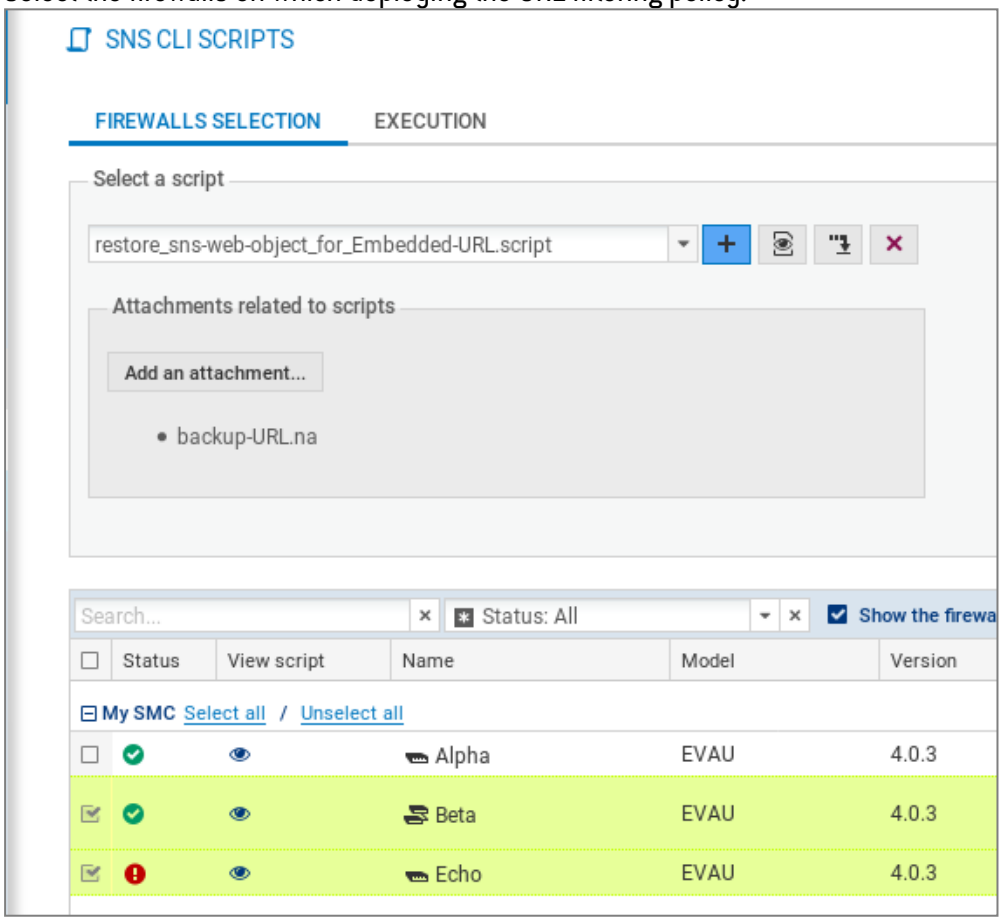
```
#################################################################

CONFIG OBJECT URLGROUP SETBASE base=CLOUDURL


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

To use the scripts:

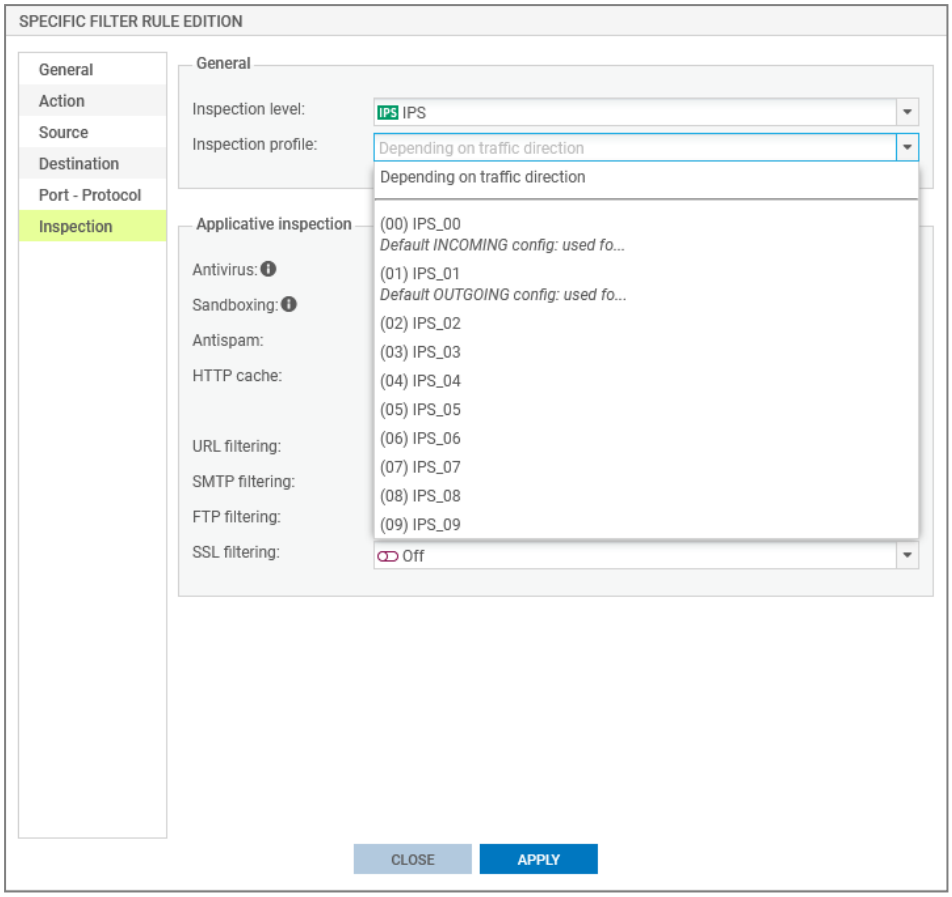
1. Copy the script adapted to the URL base you are using to a text editor and save it with the *.script* extension.
2. In SMC, open the menu **Deployment** > **SNS CLI Scripts**.
3. Select the script you saved previously.
4. Select the *.na* backup file previously created as attached file.
5. Select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



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

8.13 Managing IPS Inspection profiles on SNS firewalls from SMC

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



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

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

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

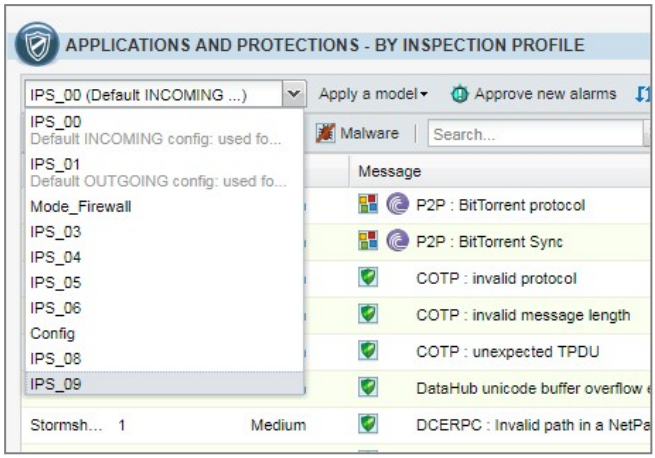
IMPORTANT
The template firewall and the target firewalls must be in the same version.

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

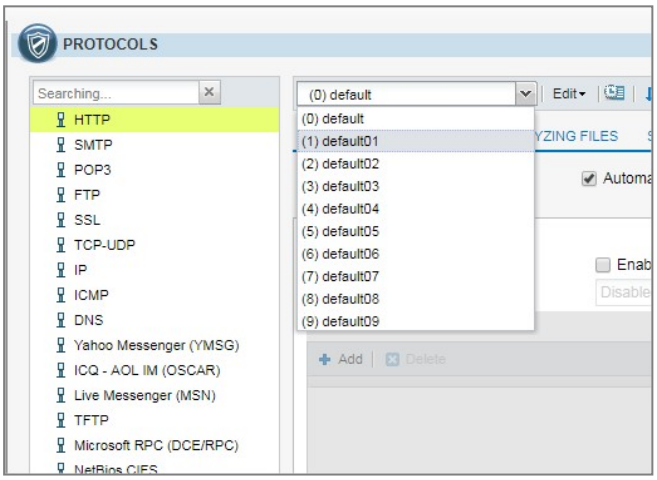
8.13.1 Editing the template IPS Inspection profiles

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

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



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



8.13.2 Saving the IPS Inspection profiles of the template firewall

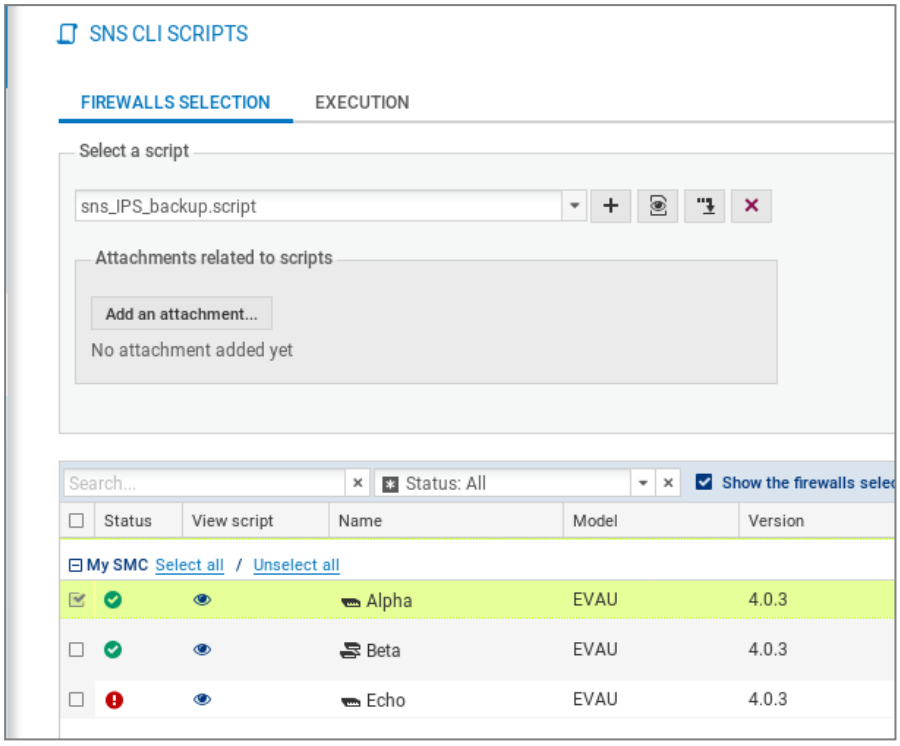
The script below makes it possible to retrieve the IPS Inspection profiles of the template firewall.

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


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

To save the profiles:

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



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

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

8.13.3 Deploying the IPS Inspection profiles

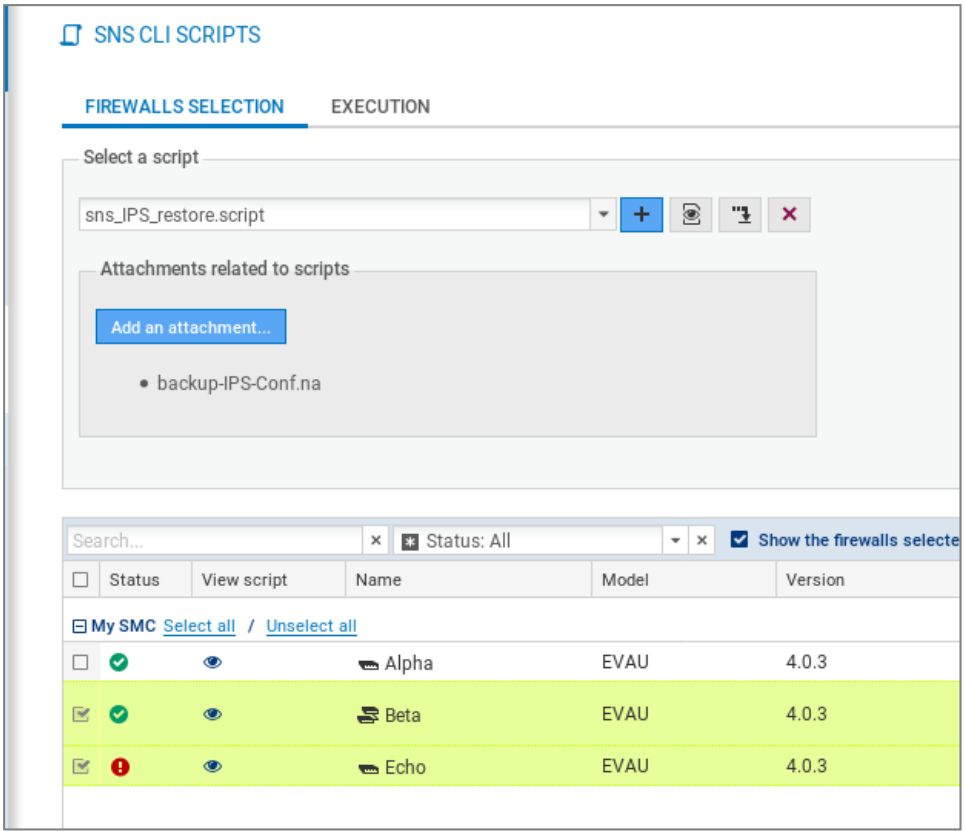
The script below makes it possible to deploy the IPS Inspection profiles previously saved on the other firewalls.

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


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

To deploy the profiles:

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



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

8.14 Adding web services

Filter rules may apply to hosts with public IP addresses that have been classified under one of the web services (previously known as "reputation groups") defined on SNS firewalls.

To benefit from updates of web services on SNS firewalls without having to update your version of the SMC server, you can manually add new web services.

To add new web services, you must know the names of the services used on SNS firewalls, and add them to the file */data/config/smc-webservices.local*, as shown below.

8.14.1 Finding out the names of web services to be used

To find out the names of the web services, you can retrieve the list either from the Stormshield Security portal, or from an SNS firewall.

From the Stormshield Security portal:

1. Go to the list of web services that are available on the Stormshield Security portal.
2. Retrieve the list in *.txt* format by clicking on the button at the bottom of the page.
3. Copy the list and add it to the SMC server as shown in the procedure below.

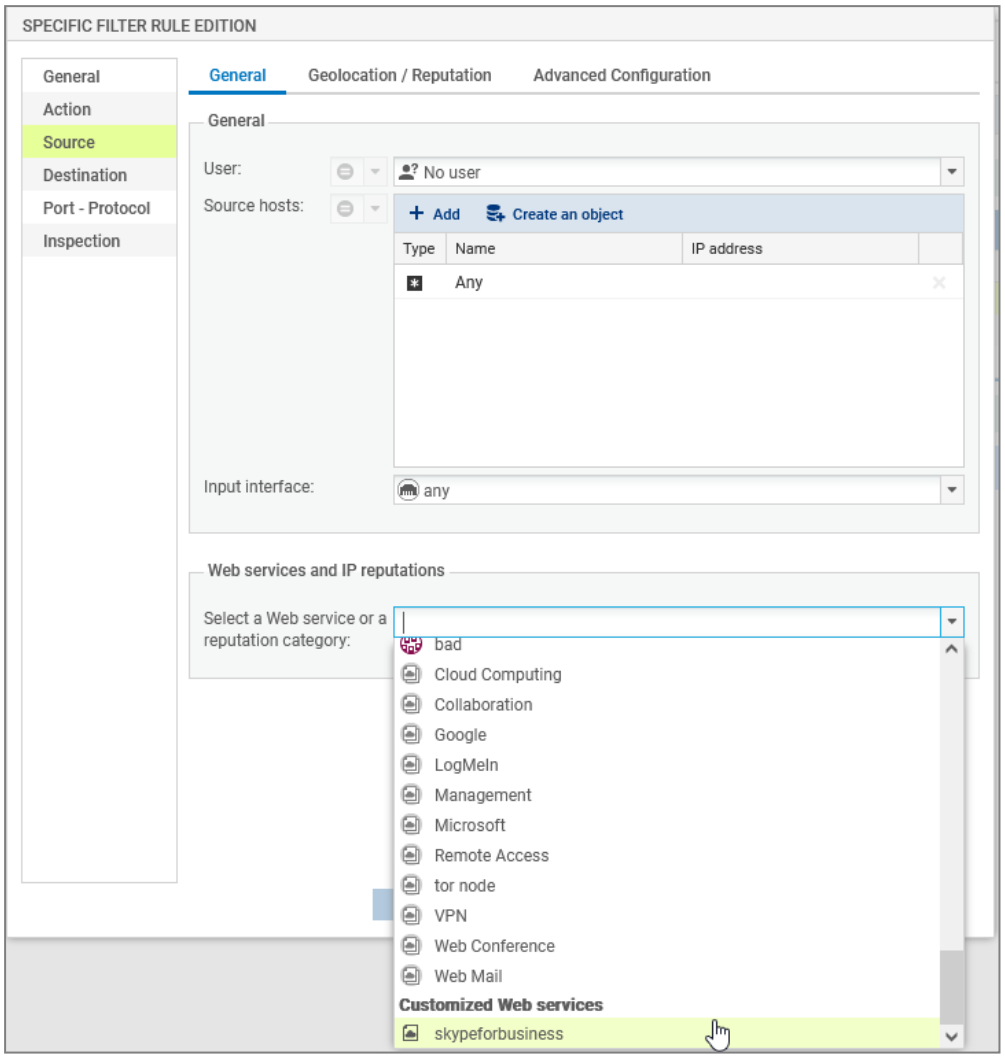
From an SNS firewall:

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

8.14.2 Adding web services on the SMC server

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Add new web service names in the file */data/config/smc-webservices.local* by following the syntax below:
   webservice1
   webservice2
   webservice3

3. In the server's web interface, refresh the display to view the new web services in the **Source** and **Destination** menus in filter rules:



9. Configuring QoS

QoS, or quality of service, refers to any technology that is capable of managing data transmission while reducing packet loss, latency and jitter on high-priority network traffic. The aim of this concept is to monitor and manage network resources by prioritizing certain types of data and network traffic.

In SMC, you can configure QoS on SNS firewalls as of version 4.3.15 LTSB and 4.5.3.

To configure QoS in SMC:

1. Add queues and traffic shapers in the **Configuration** menu.
2. Associate these queues and traffic shapers with interfaces in the firewall settings. These queues will be the default queues.
3. Configure QoS in filter rules in the firewall settings, to assign specific queues to different sets of network traffic.

NOTE
QoS cannot be monitored from SMC. To monitor QoS on a firewall, log in directly to the firewall's web administration interface.

For more information on QoS and details on how to configure it on firewalls, refer to the technical note Configuring QoS on SNS firewalls.

9.1 Configuring queues and traffic shapers

Before applying QoS to firewall network interfaces and in filter rules, you must first add and configure queues and traffic shapers.

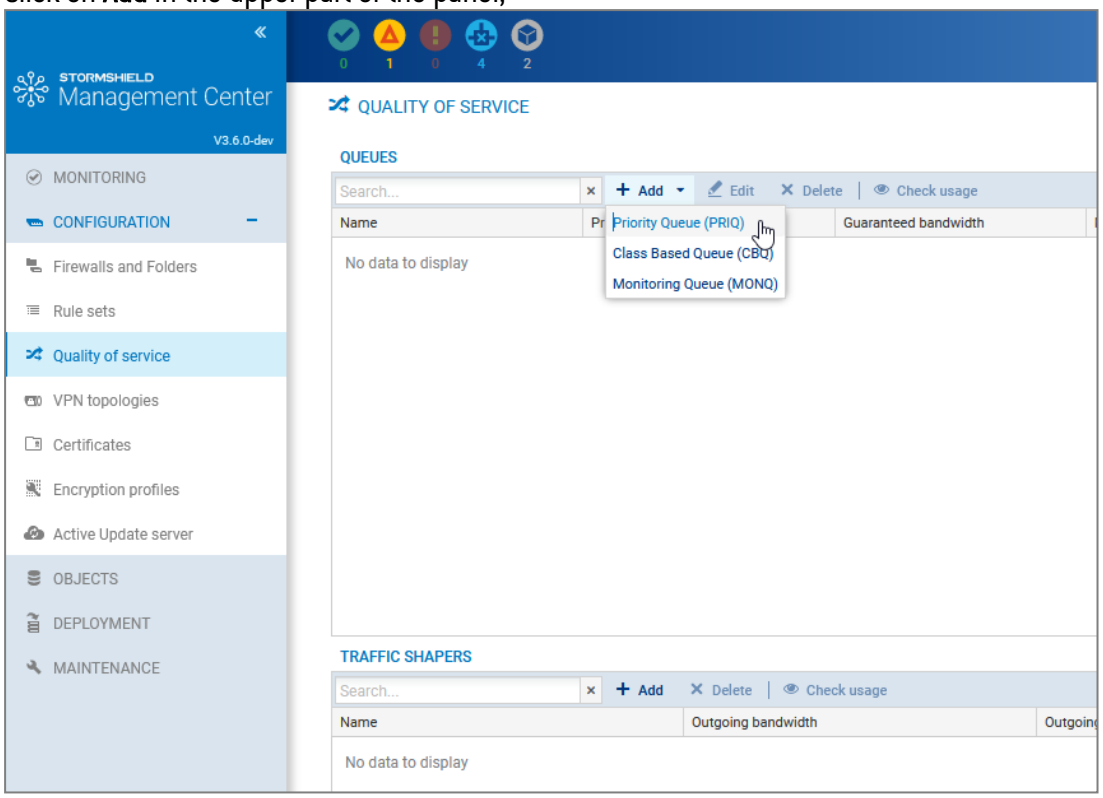
- Queues can be used to reserve bandwidth for a particular type of traffic, or to restrict such traffic by setting a guaranteed or maximum amount of bandwidth. You can also define priority queues to prioritize packets based on their source. You need to define default queues and acknowledgment queues to be associated with network interfaces, and then other queues to use in filter rules.
- Traffic shapers are traffic regulators that allow you to set the maximum bandwidth that can be used on each network interface on which QoS has been enabled.

9.1.1 Adding queues and traffic shapers

To add queues and traffic shapers, go to **Configuration** > **Quality of service**.

For queues:

1. Click on **Add** in the upper part of the panel,



2. Select the queue type:

Priority Queue (PRIQ)	Prioritizes packets with a ranking from priority 0 (traffic with the highest priority) to priority 7 (traffic with the lowest priority). Packets associated with a filter rule that uses a PRIQ are processed before packets that are not assigned to a PRIQ, or which are attached to a PRIQ with lower priority.
Class Based Queue (CBQ)	Used for reserving or limiting bandwidth, by indicating the guaranteed or maximum amount of bandwidth to apply to outgoing traffic, and for return traffic on connections. At least one of the values has to be a value other than 0.
Monitoring Queue (MONQ)	Does not have any influence on network traffic, but makes it possible to save the bandwidth information used by monitored traffic.

3. In the window that opens, name the queue and fill in the mandatory fields according to the chosen queue type. Custom variables can be used for CBQ to indicate bandwidth values. In this case, copy and paste the name of the desired variable (e.g., %CUSTOM_VAR1%). The unit used is kbit/s.
4. Add the queue.

For a traffic shaper:

1. Click on **Add** in the lower part of the panel,
2. Name the traffic shaper,
3. In the **Outgoing bandwidth** column, enter the value corresponding to 90% of the bandwidth on the link attached to the interface.
4. In the **Unit** column, indicate the bandwidth unit.
5. In the **Incoming bandwidth** column, enter the value corresponding to 90% of the bandwidth on the link attached to the interface,

6. In the **Unit** column, indicate the bandwidth unit.
7. Confirm by clicking on **Apply**.

Custom variables can be used to indicate bandwidth values. In this case, copy and paste the name of the desired variable (e.g., %CUSTOM_VAR2%). The unit used is kbit/s.

For detailed advice on the configuration of queues and traffic shapers, refer to the technical note Configuring QoS on SNS firewalls.

9.1.2 Changing and deleting queues and traffic shapers

Queues and traffic shapers can be modified or deleted, as long as they are not used by firewalls on which you do not have write access privileges. You can check where firewalls are being used by clicking on the **Check usage** button in each grid.

For more information, refer to the section Restricting folder administrators' access privileges.

9.2 Configuring QoS on firewall interfaces

To implement QoS on your network, you need to associate queues and traffic shapers with interfaces on your firewalls.

For each QoS-enabled interface, you will need to associate:

- A traffic shaper.
- A default queue: any traffic that does not have a defined QoS queue in the filter rule that applies to such traffic will join this queue.
- A default acknowledgment queue.

To perform these operations, you need to hold write access privileges on the folders in question in the SMC web interface. For more information, refer to the section Restricting folder administrators' access privileges.

9.2.1 Requirements

- The implementation of QoS in SMC is compatible with SNS firewalls from version 4.3.15 LTSB and 4.5.3 upwards.
- You need to configure queues and traffic shapers on SMC in advance. To configure them, refer to the section Configuring queues and traffic shapers.
- Network management from SMC has to be enabled on each relevant firewall.

9.2.2 Enabling SMC to manage an SNS firewall's network

Go to the **System > Configuration** tab of the firewall in question and select **Configure the network for this firewall in SMC** to indicate that SMC manages the network for this firewall.

If this option is not selected, SMC will not manage the network for this firewall and the firewall's **QoS** tab will be in read-only mode.

9.2.3 Configuring QoS on an interface

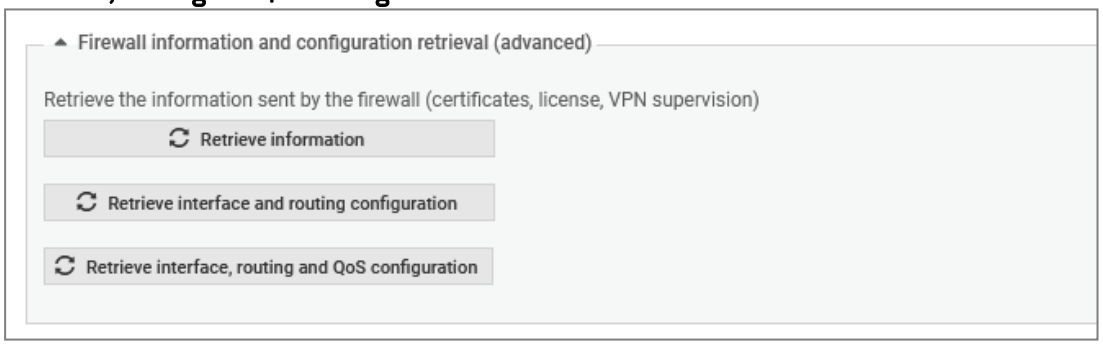
1. Go to the firewall's **QoS** tab,
2. Click on **Add**,
3. Select the interface,
4. Select a traffic shaper,
5. Select a default queue,
6. Select a default acknowledgment queue.

QoS cannot be configured on GRETAP interfaces in SMC. Connect directly to the firewall to do so.

9.2.4 Forcing the retrieval of the QoS configuration on a firewall

If QoS has already been configured locally on the firewall, you can retrieve its configuration in SMC. Network management from SMC has to be enabled on the firewall.

1. Go to the firewall's settings,
2. In the **System > Configuration** tab, select **Configure the network for this firewall in SMC** if it has not already been selected,
3. Expand **Firewall information and configuration retrieval (advanced)** and click on **Retrieve interface, routing and QoS configuration**.



9.3 Configuring QoS in filter rules

By default, network traffic uses queues that are associated with the interfaces through which they enter and leave the network. To set specific queues by traffic type, you need to create filter rules. By doing so, you can prioritize traffic types based on their source.

1. You can create a filter rule from a rule set, folder settings or firewall settings.
2. Configure the rule as indicated in the section Creating filter and NAT rules.
3. In **Action**, **General** tab, ensure that the action has been set to **Pass**. Otherwise, you will not be able to configure QoS in the rule.
4. In the **Quality of service** tab, select the queue, and if necessary, the acknowledgment queue (**ACK queue**).
5. For more information on the **Fairness** field, refer to the SNS User Guide.

10. Running SNS CLI commands on an environment of firewalls

SMC makes it possible to run SNS CLI scripts on firewalls. This mode enables the configuration of all firewall features. Scripts therefore offer a solution for deploying the configuration of a pool of firewalls for features that are not available in the menus of the SMC server.

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

You need to hold write access privileges on the firewalls to be able to run SNS CLI scripts. For more information, refer to the section Restricting folder administrators' access privileges.

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

10.1 Creating the CLI command script

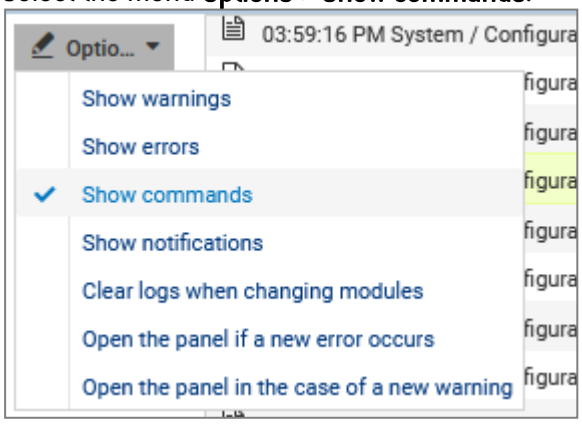
Create a UTF-8 encoded text file not exceeding 5 MB with the extension *.script* containing the commands to be run in your environment of firewalls.

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 SNS *User guide* on 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.

10.2 Using variables

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

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

Variables are case sensitive.

10.2.1 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 SNS firewall update, taking on the value SNS-%FW_ARCHITECTURE%-%FW_SIZE%.maj (*SNS-amd64-M.maj* for example). For more information, refer to the section Updating firewalls by using SNS CLI scripts.
- HA_PEER_SERIAL: serial number of the passive firewall (without High availability, the value will be empty),
- HA_PEER_FIRMWARE: version number of the passive firewall (without High availability, the value will be empty),
- CUSTOM_X : customized fields

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

10.2.2 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").

10.2.3 Using a CSV file

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

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

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

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

10.3 Running the SNS CLI script from the web interface

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

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

7. A summary of the execution process can be seen at the bottom of the panel, displaying successful operations, errors and the firewalls on which the script could not be deployed.
8. You can also filter the list of firewalls by selecting a status in the drop down list at the top of the list.

> **TIP**
> If the script has been executed on offline firewalls, the actual execution will be postponed until the next time the firewalls are connected.

9. In case of error, see the SMC server logs. You can also connect to the logs and activity reports of a firewall by clicking on the icon in the **Actions** column.

10.4 Running the SNS CLI script in command line

From the command line interface, you can:

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

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

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

10.4.1 Displaying the list of commands and options

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

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

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

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

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

10.4.2 Running a script

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

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

- --firewall-list: to be followed by a list of firewall names separated by commas,
- --all: indicates that the script will be run on all firewalls,

- --csv-file: to be followed by a path to a CSV file containing the list of firewalls and the associated variables. The command will then list the firewalls specified in this file. For more information, please refer to the section Using a CSV file.

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

The following options are not mandatory:

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

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

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

10.4.3 Adding scripts

WARNING
Folder administrators whose read access privileges are restricted to certain folders on SMC cannot perform this operation. For more information, refer to the section Restricting folder administrators' access privileges.

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

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

10.4.4 Deleting scripts

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

10.4.5 Displaying the list of scripts

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

10.4.6 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 backup AD server, taking into account the following conditions:

- The main AD server has to be an object with static IP address resolution,
- The backup 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 backup 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 */data/tmp/ad.script*:

```
# Create a new host

CONFIG OBJECT HOST NEW name=name=%type%AD.%FW_NAME%".com
comment="%type% AD server for FW %FW_NAME%" ip="%ip_addr%"
resolve=%mode%
CONFIG OBJECT ACTIVATE
```

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

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

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

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

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

```
CONFIG OBJECT HOST NEW name=MainAD.paris.com comment="Main AD server for
FW paris" ip="1.1.1.1" resolve=static
100 code=00e01700 msg="Object successfully added"
CONFIG OBJECT ACTIVATE
100 code=00a00100 msg="Ok"
CONFIG OBJECT HOST NEW name=BackupAD.paris.com comment="Backup AD server
for FW paris" ip="1.1.2.2" resolve=dynamic
100 code=00e01700 msg="Object successfully added"
CONFIG OBJECT ACTIVATE
100 code=00a00100 msg="Ok"
```

```
CONFIG OBJECT HOST NEW name=MainAD.lyon.com comment="Main AD server for FW
lyon" ip="4.4.4.4" resolve=static
100 code=00e01700 msg="Object successfully added"
CONFIG OBJECT ACTIVATE
100 code=00a00100 msg="Ok"
CONFIG OBJECT HOST NEW name=BackupAD.lyon.com comment="Backup AD server
for FW lyon" ip="4.4.5.5" resolve=dynamic
100 code=00e01700 msg="Object successfully added"
CONFIG OBJECT ACTIVATE
100 code=00a00100 msg="Ok"
```

In CSV files, fields are often separated by a comma or semi-colon. The `smc-sns-cli-script` command interprets semi-colons (;) as separators by default. The separator may be different depending on the CSV file. To change the separator expected by the command, the value of the variable `SMC_SNS_CLI_CSV_DELIMITER` must be changed:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. In the file **/data/config/fwadmin-env.conf.local**, change the value of the environment variable: `SMC_SNS_CLI_CSV_DELIMITER=,`.
3. Restart the server with the command `nrestart smc`.

10.5 Running the SNS CLI script on a high availability cluster

The steps are the same as in both previous sections.

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

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

10.6 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.

10.6.1 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 makes it possible to generate the backup file of a firewall named *backup-22-09-16.na* on the SMC server:

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

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

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

10.6.2 Attaching files to a script

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

Via the web interface

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

Via the command line interface

Copy the attachments at the root of the folder */data/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 `SMC_SNS_CLI_ATTACHMENTS_DIR` located in the file **/data/config/fwadmin-env.conf.local**. You will then need to restart the server: `nrestart smc`.

10.6.3 Receiving files generated by a script

Via the web interface

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

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

Receiving files and logs

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

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

Reading execution logs

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

Via the command line interface

All files and logs generated for each firewall after running a script are saved by default in the folder */data/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 `SMC_SNS_CLI_OUTPUT_DIR` located in the file */data/config/fwadmin-env.conf.local*. You will then need to restart the server: `nrestart smc`.

Example

When this command is run

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

the following tree is obtained:

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

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

10.7 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 SNS firewalls. Refer to the section Updating firewalls by using SNS CLI scripts.

10.7.1 Scheduling the execution of scripts from the web interface

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

5. Click on **Schedule script** at the bottom of the tab.
6. Indicate the date and time to run the script. The time chosen here corresponds to the time on the SMC server.
7. Click on **Apply**.
   - An indicator at the top of the tab serves as a reminder of the script schedule. The only actions that can be performed are viewing the script, downloading the script or canceling the scheduled run.
8. View the results of the script run in the **Execution** tab when it is complete.

Only one script run can be scheduled at a time.

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

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

10.7.2 Scheduling the execution of scripts in command line

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

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

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Type the command `at` followed by the desired date and time in the format below:
   `at hh:mm MM/DD/YYYY`
3. Type the command `smc-sns-cli-script` followed by (in this order):
   - one of the subcommands described in the section Running the SNS CLI script in command line,
   - the name of the script,
   - the name of the firewalls concerned or the --all option to designate all firewalls,
   - ```
     [root@smc] - {~} > at 16:00 10/15/2019
     warning: commands will be executed using /bin/sh
     at> smc-sns-cli-script run monitor_qos.script --all
     at> smc-sns-cli-script run monitor_stat.script --all
     ```
4. Type Ctrl + D to confirm.
   ```
   at> < EOT >
   job 15 at Tue Oct 15 16:00:00 2019
   ```
5. After the scheduled date and time of the run, you can check the results in the folder */data/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.
   ```

10.8 Updating firewalls by using SNS CLI scripts

WARNING
If you do not wish to use SNS CLI scripts to update your firewall pool, refer to the section Updating firewalls to use the feature created for this purpose.

To update firewalls by using SNS CLI scripts, download the relevant update files in advance from your MyStormshield personal area (.maj).

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

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

Follow the steps below:

1. Create the update script using the commands described in the following examples, replacing 3.7.1 with the desired version (for further information on the variable %FW_UPD_SUFFIX%, refer to the section Using variables):
   - For standalone firewalls:
     ```
     SYSTEM UPDATE UPLOAD $FROM_DATA_FILE("fwupd-3.7.1-%FW_UPD_
     SUFFIX%")
     SYSTEM UPDATE ACTIVATE
     ```
   - For clusters:
     - Passive nodes:
       ```
       SYSTEM UPDATE UPLOAD fwserial=passive $FROM_DATA_FILE
       ("fwupd-3.7.1-%FW_UPD_SUFFIX%")
       SYSTEM UPDATE ACTIVATE fwserial=passive
       ```
     - Active nodes:
       ```
       SYSTEM UPDATE ACTIVATE fwserial=active
       ```
2. In the web interface of the SMC server, select **Deployment** > **SNS CLI scripts**.
3. In the **Firewalls selection** tab, select the script to run.
4. In the **Optional: attachments related to the script** menu, select the update file(s) corresponding to the models and versions of your firewalls. For example, to update your SN510 and SN6000 firewalls to version 3.7.1, the attachments that need to be provided are *fwupd-3.7.1-SNS-amd64-M.maj* and *fwupd-3.7.1-SNS-amd64-XL.maj*.
5. Next, follow the usual steps for running a script, as shown in the section Running the SNS CLI script from the web interface from step 4 onwards.

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

10.9 Troubleshooting

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

10.9.1 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: `SMC_SNS_CLI_SCRIPT_MAX_UPLOAD_SIZE_INT=$((10*1024*1024))`

10.9.2 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.

10.9.3 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 server's log file in */data/log/fwadmin-server/server.log* for further detail.
  - Before running the script, you can view it for a given firewall in the **Firewalls selection** tab. Certain errors may be indicated.

10.9.4 Scripts cannot be executed

- *Situation*: Firewalls have been selected for the execution of a script but the execution button remains grayed out, or some firewalls cannot be selected.
- *Cause*: A script is currently being executed or a configuration is being deployed or delayed on a firewall. Scripts therefore cannot be executed on this firewall for the moment.
- *Solution*: Wait until the script execution or deployment ends, or until the firewall reconnects so that the deployment can complete.

11. Maintaining SNS firewalls

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

11.1 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 back up your firewall pool as well at any moment.

11.1.1 Backing up the configuration of the server and firewalls automatically

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

Automatic backups are disabled by default..

Only the super administrator ("admin" user) is allowed to enable or disable automatic backups, and download backups of the SMC server's configuration. All administrators can download configuration backups of SNS firewalls.

WARNING
On firewalls equipped with initialized TPM modules (Trusted Platform Module), private keys are excluded from automatic backups by default.

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 SNS *user guide*.

Showing more details about a backup

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

Enable automatic backup

- Select **Enable automatic backup**.

11.1.2 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. The password must also comply with the password policy on the firewalls in question.
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.

WARNING
On firewalls equipped with initialized TPM modules (Trusted Platform Module), private keys are excluded from automatic backups by default.

11.1.3 Excluding private keys from automatic firewall backups

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

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

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. In the file **/data/config/fwadmin-env.conf.local**, change the value of the environment variable: `SMC_AUTOBACKUP_EXCLUDE_PRIVATE_KEY_ENABLED=true`
3. Restart the server with the command `nrestart smc`.

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

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

11.2 Updating firewalls

SMC makes it possible update your firewall pool.

WARNING
We strongly recommend that you update no more than 10 firewalls simultaneously.

You need to hold write access privileges on the firewalls in order to update them. For more information, refer to the section Restricting folder administrators' access privileges.

Firewalls on which the TPM has been enabled cannot be updated from SMC.

1. Download the relevant update files in advance from your secure MyStormshield area (*.maj*).
2. In the web interface of the SMC server, select **Deployment** > **Updating firewalls**.
3. In the first part of the **Firewall selection** tab, import one or several update files in *.maj* format by clicking on :
   - Imported files are stored on the SMC server. They are kept for 14 days by default. With the environment variable SMC_SNS_UPDATE_MAX_KEEP_DAYS_INT, the duration for the storage of update files can be changed.

     WARNING
     Ensure that you have enough disk space to store the files, as disk saturation may cause malfunctions.
   - The button makes it possible to indicate the URL of an HTTPS server from which SMC can import update files.
   - The button allows you to view the header of the update file, to confirm that the file is compatible with the version of the firewalls to be updated.
   - The **Save the active partition on the backup partition before updating the firewall** checkbox offers the option of saving the system's active partition on the backup partition, to keep a record of it. Depending on the size of the partition, configuration and firewall model, the operation may last a while. The environment variable SMC_SNS_UPDATE_SYSTEM_CLONE_TIMEOUT_INT makes it possible to configure the maximum amount of time allowed for the backup.
     For EVA firewalls that do not have backup partitions, selecting this checkbox does not prevent the firewall from being updated, but the update will run without backing up the active partition. We recommend that you back up a snapshot of the host before updating it.
4. Select the update file to be applied.
5. In the second part of the **Firewall selection** tab, select the firewalls to be updated.
   - The icon indicates, where applicable, that the firewall cannot be selected to run the update. In this case, the row will be grayed out. Scroll over the icon with your mouse to find out why.
   - Offline firewalls can be selected. Updates for these firewalls are postponed and launched the next time the firewalls connect. When a firewall reconnects, if SNS CLI script executions or configuration deployments are already pending, the update will be run first, followed by the script execution or configuration deployment.
   - In a high availability cluster, the passive firewall is updated first. When it restarts, it becomes the active firewall while the other firewall is updated. This ensures service continuity.
6. Click on **Update firewalls** at the bottom of the tab. The **Execution** tab automatically opens.

7. Track the progress and results of the update on each selected firewall. When an update is pending on a firewall, you cannot run SNS CLI scripts or deploy configurations on this firewall, and vice versa. You can launch updates on other firewalls.

> **IMPORTANT**
> The read/write privileges on any administration sessions already open on the firewalls in question are automatically adopted when an update is run.

8. Filter the list of firewalls by selecting a status in the drop down list at the top of the list, if necessary.
9. In case of error, see the SMC server logs. You can also connect to the logs and activity reports of a firewall by clicking on the icon in the **Actions** column.
10. After a few minutes, check in the **Monitoring** > **Firewalls** panel that the version number has indeed changed in the **Version** column.

Firewalls can also be updated from SMC, by using SNS CLI scripts. To perform this operation, refer to the section Updating firewalls by using SNS CLI scripts.

11.3 Replacing an SNS firewall through an RMA

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

Once the new appliance is ready:

1. In SMC, in the **System > Configuration** tab of the firewall properties, select **Allow another firewall to connect with the same package as part of a defective hardware replacement (RMA)** to allow the new appliance, which is presenting a different serial number, to connect to SMC instead of the former appliance.
2. Restore the firewall's configuration on the new appliance by using a *.na* backup file
   The firewall will automatically log back in to SMC.

There is nothing additional that you need to do; there is no need to generate a new connecting package.

12. Removing SNS firewalls from the SMC server

To perform this operation, you need to hold write access privileges on the folders containing the firewalls to be removed. For more information, refer to the section Restricting folder administrators' access privileges.

To stop managing a firewall from the SMC server, and to remove it from the list of firewalls in the web interface:

1. Scroll over the name of the firewall in **Monitoring** > **Firewalls** and click on 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 in SSH or via the console of your hypervisor and enter the following command lines:

   ```
   nstop cad
   setconf /usr/Firewall/ConfigFiles/Cad/cad Server State 0
   rm /usr/Firewall/ConfigFiles/Cad/*.pem
   rm /usr/Firewall/ConfigFiles/Cad/*.tpm
   rm /usr/Firewall/ConfigFiles/nsconf_int
   encad
   ```

   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.

13. 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.

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

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

The interface eth0 cannot be disabled.

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

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

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

13.2 Verifying the SMC server version in command line

To see the SMC server version:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Enter the command `smc-version`.
3. The following information appears:
   - SMC_DISTRIB_VERSION: indicates the version in the form 1.2.3,
   - SMC_DISTRIB_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.

13.3 Changing the SMC server time zone and date

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

13.3.1 Changing the time zone

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

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

13.3.2 Changing the date manually

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

13.3.3 Changing the date via NTP

To enable NTP on the SMC server:

1. Enter the command `smc-date-time --ntp-servers ntp1.org,ntp2.com,IPaddress` separating each NTP server with a comma if there are several. NTP servers may also be idenified 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.

The polling frequency of an NTP server is the default frequency of the NTP daemon.

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

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

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

13.4 Managing administrators from local and external directories

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

- Create local accounts on the SMC server,
- Configure a connection to a LDAP server from the SMC server,
- Configure a connection to a RADIUS server from the SMC server.

In the **Maintenance > SMC Server > Administrators** menu in the web administration interface, administrators who have local accounts on the SMC server or accounts from other Radius or LDAP authentication servers can be managed.

There are four administrator profiles: super administrator ("admin" user), general administrator, folder administrator, and read-only administrator.

The panel displayed depends on whether you are connected to the server as the super administrator (“admin” user) or as another administrator.

The three administrator profiles in write mode have the following privileges:

	Super administrator	General administrator	Folder administrator
Administrators	Add/Remove/Edit	Modify personal password	Modify personal password
SNS firewall configuration	• Add/Remove/Edit • Deployment • Automatic and manual backup	• Add/Remove/Edit • Deployment • Manual backup	Only in folders on which the administrator has write access: • Add/Remove/Edit • Deployment • Manual backup
SMC maintenance	• Install and update license • Update server • Save and restore server configuration • Define server's network interfaces • Generate a diagnostics report • Enable DR mode • Manage access to SLS server	• Generate a diagnostics report • Enable consistency check for DR mode • Manage access to SLS server	Generate a diagnostics report
Manage API keys	• Enable public API • Revoke API keys	Create/revoke API keys if privileges are enabled	Create/revoke API keys in read-only if privileges are enabled

For more information on folder administrators, refer to the section Restricting folder administrators' access privileges.

Read-only administrators can access all panels in the web administration interface, but cannot change anything other than their own passwords.

When the super administrator tries to connect, the SMC server looks for the ID and password from its local user database.

When a general administrator or folder administrator attempts to connect, the SMC server will first search for the ID and password on the Radius server if it has been configured, then on the LDAP server if it has been configured, then in its local database if it has been configured.

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

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

NOTE
The “root” user does not appear in the list of administrators, but holds access privileges to the server in SSH or via the console on a hypervisor. However, the super administrator cannot access the server in SSH or via a console.

To manage administrators as the super administrator, go to the **Administrators** menu:

- To add an administrator, click on **Add an administrator**.
- To edit an administrator profile, double click on the administrator line or move the mouse over the administrator name and select the pencil icon. An administrator's **Read/WriteSMC** privilege cannot be withdrawn if this administrator holds active API keys that also have the **Read/Write** privilege. For more information, please refer to the section Enabling and managing SMC's public API.
- To remove an administrator, move the mouse over the administrator name and select the red cross icon. Administrators that hold active API keys cannot be deleted. For more information, please refer to the section Enabling and managing SMC's public API.

The admin user cannot be removed.

NOTE
Only the super administrator is allowed to update the SMC server, back up and restore the SMC configuration and enable or disable automatic backups from the web administration interface.

13.4.1 Managing administrator privileges as super administrator

The super administrator holds all privileges and decides whether to grant other administrators access to:

- to the SMC web interface in read/write or read-only mode,
- the firewall web interface in read/write or read-only mode,
- the command line interface in SSH,
- the command line interface via the console on a hypervisor.

The super administrator can also restrict administrators' write access privileges to only certain folders, and therefore to only certain firewalls. For more information, refer to the section Restricting folder administrators' access privileges. This restriction does not apply to access via SSH and console.

Administrators who are allowed to access the command line interface in SSH or via the console on a hypervisor must request privilege escalation by using the “sudo” command to run certain commands relating to the system (network, user accounts, system files, etc.):

```
[admin-a@smc] - {~} > tcpdump
tcpdump: eth0: You don't have permission to capture on that device
(socket: Operation not permitted)
[admin-a@smc] - {~} > sudo tcpdump
Password:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

It is also the super administrator who assigns permissions to other administrators to create or revoke API keys that allow SMC's public API routes to be used.

In order for this action to be available, the public API must be enabled from SMC's web interface. For more information on SMC's public API, refer to the section Enabling and managing SMC's public API.

13.4.2 Managing local administrators

The accounts of local administrators are created locally on the SMC server.

Adding local administrators

To add a local administrator:

1. Go to **Maintenance** > **SMC Server** > **Administrators**, and click on **Add an administrator**.
2. Fill in the following mandatory fields:

Field	Description
ID	Identifier of the local administrator.
Name	Name of the local administrator shown in SMC.

3. Select the access privileges. For more information, refer to the section Managing administrator privileges as super administrator and the section Restricting folder administrators' access privileges.
4. Set a password for the administrator in line with the password policy described in the following section.

The following terms are reserved on SMC, so cannot be used as IDs: root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, sshd, dhcpcd, messagebus, fwadmin-server, nobody.

Defining a password policy for local accounts

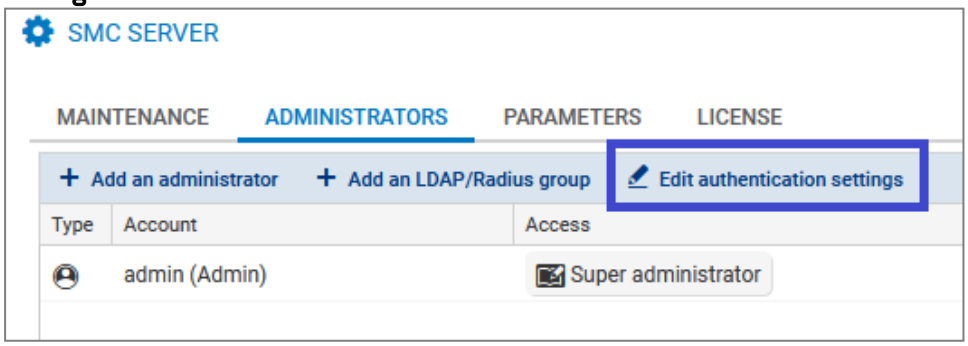
Only the super administrator can set the password policy for administrators with a local account, by choosing:

- The minimum number of characters required: the password can contain between one and 128 characters. A minimum of 12 characters is required by default.
- The mandatory character types: alphanumeric, alphabetic and special or none. No character types are mandatory by default.

When a new SMC server is deployed, the password of the super administrator in the server initialization wizard must also contain at least 12 characters.

To set a password policy:

1. Go to **Maintenance** > **SMC Server** > **Administrators**, and click on **Edit local authentication settings**.



2. In the **Local** tab, enable local authentication if necessary.
3. Select the minimum number of characters required.
4. Select the mandatory character types.

The password policy applies to all administrators who have a local account.

It also applies to passwords used for encrypting backups. For more information, please refer to the section Saving and restoring the SMC server configuration.

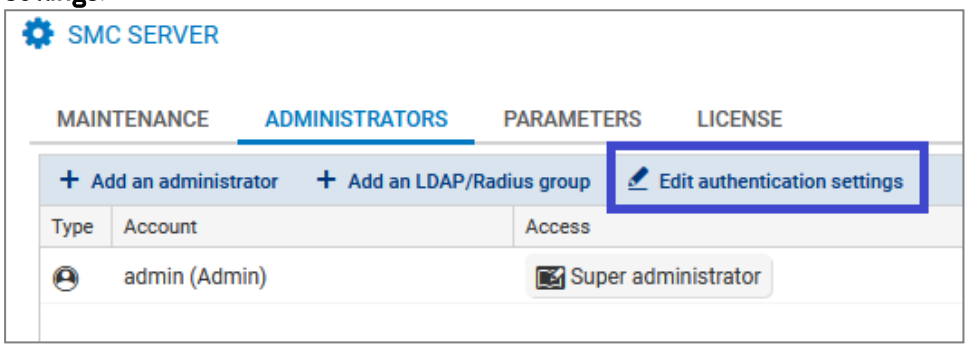
Passwords that were set before this policy was applied will remain valid but we recommend that you change them to comply with the set policy.

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

Disabling local authentication

The super administrator can disable local authentication and therefore allow administrators to authenticate only through a Radius or LDAP authentication server.

1. Go to **Maintenance** > **SMC Server** > **Administrators**, and click on **Edit local authentication settings**.



2. In the **Local** tab, unselect **Local authentication enabled**.
3. Click on **Apply**.

The super administrator continues to hold the privilege of authenticating with their local password. This is the only authentication mode available to them.

13.4.3 Managing LDAP users

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 an LDAP server such as Active Directory on Microsoft Windows Server 2016, 2019 and 2022 or OpenLDAP in at least version 2.5.

Authentication via Radius server is configured in the SMC web administration interface.

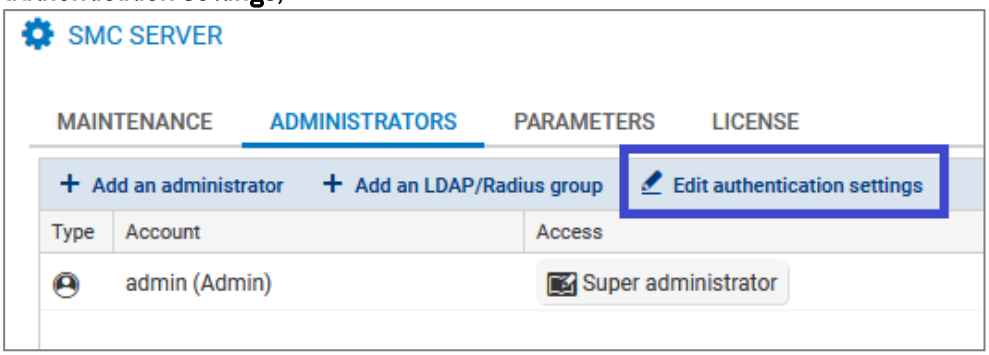
To authorize administrators to connect to the SMC server via an LDAP server, follow the three steps below:

1. Configure the connection to the LDAP server,
2. Test the connection to the server,
3. Authorize users and define their access privileges.

Configuring the connection to the LDAP server

To configure and enable the connection to an LDAP server:

1. Go to **Maintenance** > **SMC Server** > **Administrators**, and click on **Edit local authentication settings**,



2. In the **LDAP** tab, select **LDAP authentication enabled**.

3. Fill in the following fields:

Field	Description
Server type	Active Directory or OpenLDAP server
Host	IP address or FQDN of the main LDAP server. If the server's FQDN is used, the DNS service must be configured beforehand. If you use the SSL protocol with identity verification for the certification authority to secure the connection to the LDAP server, the host name must be the same as the common name (CN) of the LDAP server's certificate.
Backup host	Optional - IP address or FQDN of the backup LDAP server. If the server's FQDN is used, the DNS service must be configured beforehand. Only this parameter is required for the backup LDAP server, as the other parameters belong to the main server.
Port	Port number to access the LDAP server: if SSL is enabled, 636 by default; otherwise, 389.
Base DN	Base DN that enables access to the LDAP server and uses the following format: dc=sub,dc=domain,dc=com. With an OpenLDAP server, the Base DN can also refer to a more specific location, e.g., an organizational unit: ou=unit,dc=domain,dc=com
ID	This field appears if an Active Directory server is used. Refers to the ID of the administrator with which a request can be submitted to the Active Directory LDAP server. For example: Administrator.
Administrator DN	This field appears if an OpenLDAP server is used. Refers to the DN of the administrator with which a request can be submitted to the OpenLDAP LDAP server. For example: cn=admin.
Password	Password to connect to the LDAP server
Encrypt with SSL	If the option is enabled, the connection to the LDAP server is secured via SSL/TLS protocols. When SSL is enabled, the default port changes. If SSL is enabled, the SMC server does not verify the certification authority that signed the LDAP server's certificate by default.
Check identity of the LDAP server CA	This option makes it possible to verify the certification authority that signed the LDAP server's certificate, when SSL is enabled. Provide the CA's certificate in the field below.
Certificate	In this field, the certificate of the certification authority that signed the certificate that the LDAP server used for the secure SSL connection can be forwarded to the SMC server.

NOTE
All fields are case sensitive. We recommend that you carefully check the configuration of your LDAP directory.

Testing the connection to the LDAP server

To test the connection to an LDAP server, use the *ldapsearch* tool available in command line on the SMC server.

Use the following parameters with the `ldapsearch` command to test the connection to an LDAP server and perform a search in the directory:

Parameter	Description
-H	IP address or FQDN of the LDAP server, preceded by ldap:// and followed by the port number (port 389 is used by default).
-D	Unique name used to authenticate on the server. This name must match a specific entry in the directory and must be allowed to perform searches in the directory. It can either be an administrator or a user. The format expected by default is: CN=Administrator,DC=mydomain,DC=com To query an Active Directory, the format can also be: Administrator@mydomain.com.
-W	If a term is entered, an authentication password will be requested before launching the search
-b	Branch of the LDAP tree in which you want to launch the search. To search in the entire directory, indicate the base DN. For example: DC=mydomain,DC=com.

EXAMPLES

For Active Directory:

```
ldapsearch -H ldap://1.2.3.4:536 -D "Administrator@mydomain.com" -W -b
"DC=mydomain,DC=com"
```

For OpenLDAP:

```
ldapsearch -H ldap://1.2.3.4:536 -D
"cn=Administrator,dc=mydomain,dc=com" -W -b "dc=mydomain,dc=com"
```

The search can be filtered by adding attributes after the command. Add for example the attribute "member" to show group members.

EXAMPLE

```
ldapsearch -H ldap://1.2.3.4:536 -D "Administrator@mydomain.com" -W -b
"CN=Users,DC=mydomain,DC=com" member
```

Allowing LDAP users

To allow LDAP users to authenticate on the SMC server, the super administrator must add them to the list of administrators in the web administration interface.

1. Go to **Maintenance** > **SMC Server** > **Administrators**, and click on **Add an administrator**.
2. Fill in the following mandatory fields:

Field	Description
ID	LDAP user's identifier. This field corresponds to the `sAMAccountName` attribute if the LDAP server is an Active Directory and to the attribute `uid` if the LDAP server is an OpenLDAP. It is optional if the **LDAP DN** field is entered.
LDAP DN	LDAP user's DN. This field corresponds to the `DistinguishedName` and `dn` attributes, regardless of the LDAP server configured. It is optional if the **ID** field is entered.
Name	Name of the LDAP user shown in SMC.

3. Select the access privileges. For more information, refer to the section Managing administrator privileges as super administrator and the section Restricting folder administrators' access privileges.
4. Unselect **This administrator can use local authentication** if you do not wish to define local authentication for the LDAP user.

The following terms are reserved on SMC, so cannot be used as IDs: root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, sshd, dhcpcd, messagebus, fwadmin-server, nobody.

NOTE
The IDs of users authenticated via the LDAP directory must not contain spaces in order to be able to connect to the SMC server.

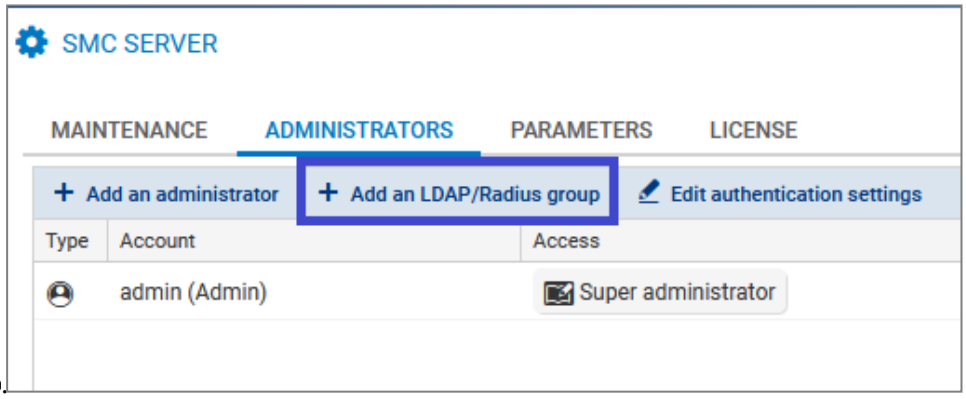
Adding LDAP groups

Users can belong to LDAP groups.

By default SMC searches for users belonging to a group with the `memberOf` attribute. This attribute is used in directories similar to Active Directory. In some OpenLDAP directories, this attribute must be configured.
Other attributes can be used to search for users in a group. For more information, refer to the section Changing the default LDAP attributes used by SMC.

To add an LDAP user group:

1. In the **Maintenance > SMC server > Administrators** menu, click on **Add an LDAP/Radius group**.



2. Fill in the following mandatory fields:

Field	Description
LDAP DN	DN of the LDAP group to which LDAP users belong. This field corresponds to the `DistinguishedName` and `dn` attributes, regardless of the LDAP server configured.
Name	Name of the LDAP group shown in SMC.

3. Select the access privileges. For more information, refer to the section Managing administrator privileges as super administrator.

If an administrator has a personal account in his/her name, and is also a member of one or several groups, the privileges that apply will be those assigned to the personal account.

NOTE
The IDs of users authenticated via the LDAP directory must not contain spaces in order to be able to connect to the SMC server.

Changing the default LDAP attributes used by SMC

In the **SMC Server** window > **Administrators** > **Add an administrator**, the **ID** and **LDAP DN** fields correspond to the following LDAP attributes by default:

ID	• `sAMAccountName` if an Active Directory server is used • `uid` if an OpenLDAP server is used
LDAP DN	• `DistinguishedName` and `dn` regardless of the LDAP server configured

SMC also relies on the `memberOf` attribute to search for groups in which users belong. It may have to be configured manually on some LDAP servers.

The following environment variables make it possible to change these three attributes:

- `SMC_LDAP_FIELD_NAME_LOGIN`
- `SMC_LDAP_FIELD_NAME_DN`
- `SMC_LDAP_FIELD_NAME_MEMBEROF`

To change their values:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. In the file **/data/config/fwadmin-env.conf.local**, change the values of these environment variables:
3. Restart the server with the command `nrestart smc`.

13.4.4 Managing Radius users

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

This type of authentication is intended to work with a Radius or FreeRADIUS server on Microsoft Windows Server 2016, 2019 and 2022.

Authentication via Radius server is configured in the SMC web administration interface.

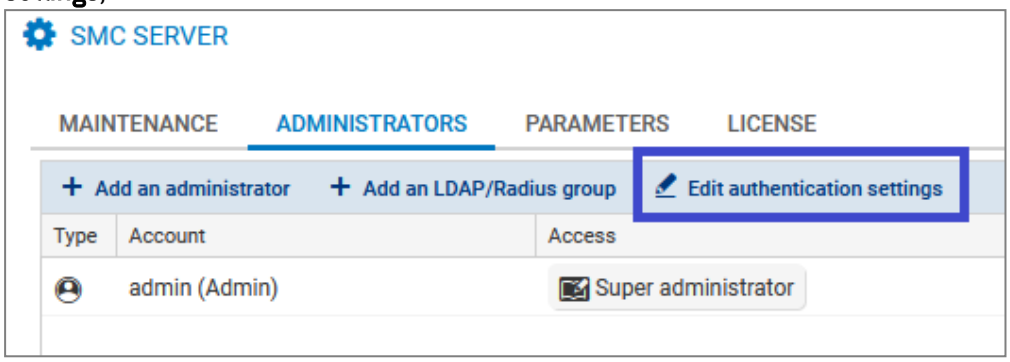
To authorize administrators to connect to the SMC server via a Radius server, follow the three steps below:

1. Configure the connection to the Radius server,
2. Test the connection to the server,
3. Authorize users and define their access privileges.

Configuring the connection to the Radius server

To configure and enable the connection to a Radius server:

1. Go to **Maintenance** > **SMC Server** > **Administrators**, and click on **Edit local authentication settings**,



2. In the **Radius** tab, select **Radius authentication enabled**.
3. Fill in the following fields:

Field	Description
Main server	
Host	IP address or FQDN of the main Radius server. If the server's FQDN is used, the DNS service must be configured beforehand.
Port	Port number to access the Radius server: 1812 by default
Pre-shared key	Secret key shared to enable authentication on the server
Backup server - Optional	
Host	IP address or FQDN of the backup Radius server. If the server's FQDN is used, the DNS service must be configured in advance.
Port	Port number to access the Radius server: 1812 by default
Pre-shared key	Secret key shared to enable authentication on the server

Testing the connection to the Radius server

To test the connection to a Radius server, use the *radtest* tool available in command line on the SMC server:

EXAMPLE

```
radtest <user-id> <user-password> <radius-server-ip>:<radius-server-
port> <NAS-server-port> <pre-shared-key>
```

```
[root@smc] - {~} > radtest user-radius password 1.2.3.5:1812 1812 P@s5w0rD
Sent Access-Request Id 4 from 0.0.0.0:46901 to 1.2.3.5:1812 length 87
        User-Name = "user-radius"
        User-Password = "password"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1812
        Message-Authenticator = 0x00
        Framed-Protocol = PPP
        Cleartext-Password = "password"
Received Access-Accept Id 4 from 1.2.3.5:1812 to [redacted]:46901 length 20
```

Allowing Radius users

To allow Radius users to authenticate on the SMC server, the super administrator must add them to the list of administrators in the web administration interface.

1. Go to **Maintenance** > **SMC Server** > **Administrators**, and click on **Add an administrator**.
2. Fill in the following mandatory fields:

Field	Description
ID	Identifier of the Radius user.
Name	Name of the Radius user shown in SMC.

3. Select the access privileges. For more information, refer to the section Managing administrator privileges as super administrator and the section Restricting folder administrators' access privileges.
4. Unselect **This administrator can use local authentication** if you do not wish to define local authentication for the Radius user.

The following terms are reserved on SMC, so cannot be used as IDs: root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, sshd, dhcpcd, messagebus, fwadmin-server, nobody.

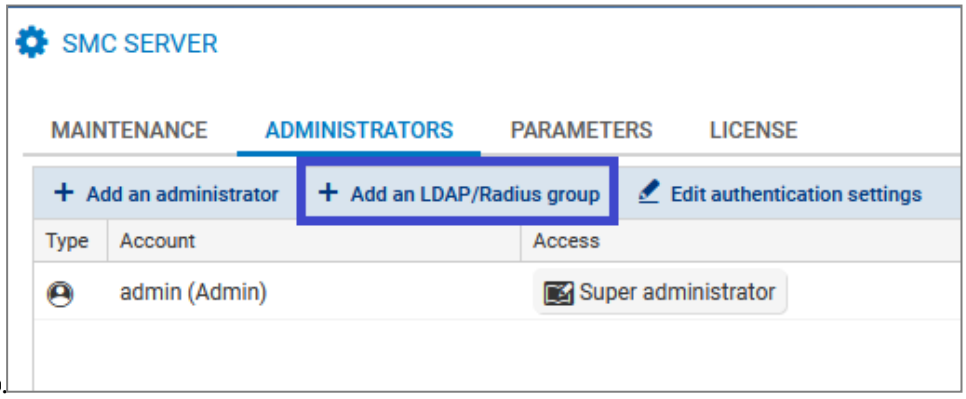
NOTE
The IDs of users authenticated via the Radius directory must not contain spaces in order to be able to connect to the SMC server.

Adding Radius groups

Users can belong to Radius groups.

To add a Radius user group:

1. In the **Maintenance > SMC server > Administrators** menu, click on **Add an LDAP/Radius group**.



2. Fill in the following mandatory fields:

Field	Description
Radius identifier	Identifier of the Radius group.
Name	Name of the Radius group.

3. Select the access privileges. For more information, refer to the section Managing administrator privileges as super administrator.

If an administrator has a personal account in his/her name, and is also a member of one or several groups, the privileges that apply will be those assigned to the personal account.

NOTE
The IDs of users authenticated via the Radius directory must not contain spaces in order to be able to connect to the SMC server.

13.4.5 Restricting folder administrators' access privileges

SMC can segment the administration of your firewall pool by assigning different administrators to separate firewall groups. To do so, you can restrict an administrator's write access to a firewall group, based on the folder tree available in SMC. By segmenting administration, a perimeter can be defined for each administrator, thereby increasing security on your firewall pool.

For more information on folder management, refer to the section Organizing firewalls by folders.

EXAMPLE
If your firewall pool extends across several countries or continents, you can choose to assign a different administrator for each country or continent. Individual administrators can then manage only firewalls in the folder corresponding to their zone. They can also look up the configuration of other firewalls and of the SMC server in read-only mode.

Only the super administrator can restrict other administrators' write access privileges to certain folders.

The super administrator can then define two administrator profiles that hold write access privileges:

General administrator	• Holds write access privileges to the root SMC folder, meaning all sub-folders, and therefore all SNS firewalls. • Can change the configuration of all SNS firewalls connected to SMC. • Can create and change all configuration items found in SMC (objects, rules, VPN topologies, QoS, certificates, encryption profiles, etc.). • Can perform certain maintenance operations on the SMC server.
Folder administrator	• Write access privileges are restricted to one or several folders, and to the firewalls contained in them. • Can change only the configuration on firewalls that they manage. • Can create configuration items and use them for firewalls that they manage. • Can create VPN topologies only with the firewalls that they manage. • Can directly access the interface of firewalls that they manage via SMC in read/write. • Can access in read-only mode the configuration of firewalls outside their administration perimeter, all configuration items found in SMC, and the configuration of the SMC server. • Can directly access the interface of firewalls outside their administration perimeter via SMC, but in read-only mode.

For more details on administrator profiles, as well as the implications and limitations of restricting access privileges to folders, refer to the section Managing administrators from local and external directories and the sections below.

Restricting folder administrators' write privileges

The super administrator selects the folder(s) on which folder administrators hold write privileges. This means that the super administrator gives the administrator full write access to

these folders, any sub-folders and the firewalls that they contain, as well as future sub-folders or firewalls.

The folder administrator can always view in read-only mode the configuration of firewalls outside their administration perimeter.

To restrict an administrator's privileges:

1. Go to **Maintenance** > **SMC Server** > **Administrators**.
2. Double-click on the row of the administrator.
3. In the **Folders** drop-down list, select the folder(s) that the administrator will be able to manage.
4. Apply changes.

In the firewall monitoring view, folder administrators see only the firewalls in their administration perimeter by default, meaning the firewalls that belong in the folders to which they have write access.

To display all firewalls, click on **See read-only folders**.

Understanding the implications of restricting write access

Folder administrators can create configuration items (objects, rules, QoS queues, etc.) and use them to configure the firewalls that they manage. They can also use all the configuration items available in SMC, and which have been added by other administrators.

However, they cannot modify or delete these items if they are used in the configuration of firewalls that are not in their administration perimeter.

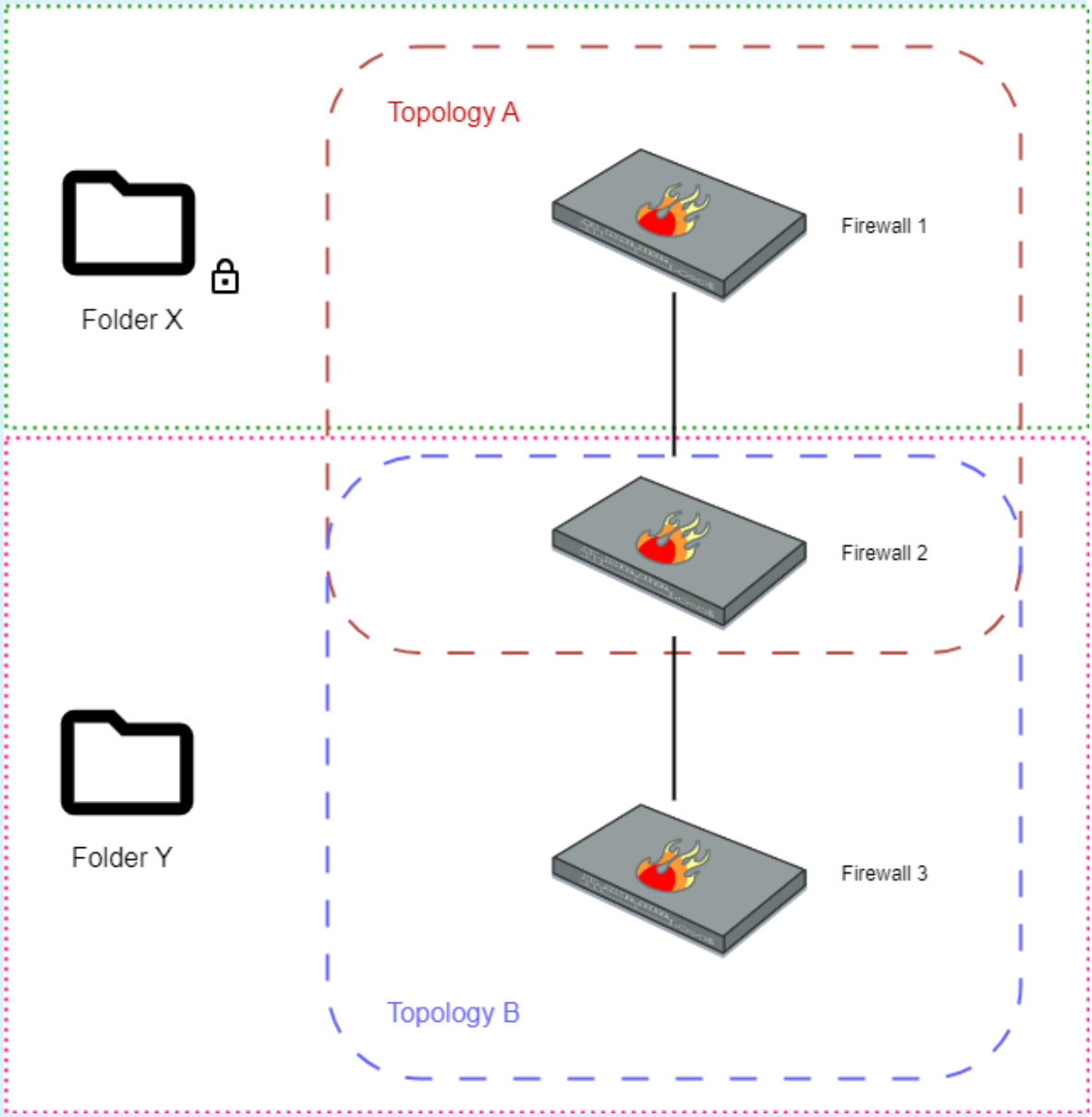
Managing VPN topologies with restricted access to folders

To create, modify or delete a VPN topology, folder administrators must hold write access privileges to all firewalls included in the topology.

Otherwise, i.e., if the peers from the same topology are firewalls that have been organized in several folders managed by different folder administrators, only a general administrator can create, modify or delete the topology.

Write access privileges to the folder prevail over write access privileges to a topology. As such, folder administrators retain permissions to configure firewalls to which they have write access, even if these firewalls are part of a topology to which the administrators do not have full access.

EXAMPLE



In this example, firewall 1 is organized in folder X, and firewalls 2 and 3 are organized in folder Y. The administrator of folder Y cannot modify topology A as it includes firewall 1, on which the administrator does not have write access privileges. However, the administrator retains write access privileges on firewall 2, although it is part of topology A.

Limitations of actions on the general SMC configuration

Folder administrators cannot perform the following operations on the general SMC configuration:

- Adding or changing global custom properties on firewalls,
- Importing objects via a CSV file,
- Changing the default VTI network pool in VPN topologies,
- Loading and deploying older configurations,
- Enabling or modifying the consistency check for "*Diffusion Restreinte* (DR)" mode,
- Entering or changing a shortcut to the Stormshield Log Supervisor (SLS) server,
- Adding an SNS CLI script or an attachment to a script,
- Changing the settings of the Active Update server,
- Creating API keys with write privileges to access the public SMC API.

13.4.6 Troubleshooting

Refer to this section for solutions to issues that may arise when managing administrators.

Administrators whose IDs contain accented characters are unable to log in to SMC.

- *Situation*: When an administrator from an LDAP authentication server uses an ID that contains an accented character, the connection to SMC is denied.
- *Cause*: When you add an administrator from an LDAP server in SMC with a name that contains an accented character (**LDAP DN** field), the accent in the SMC ID is not supported.
- *Solution*: To log in, administrators have to enter their logins without accents.

13.5 Viewing SMC server logs

The SMC server provides two types of logs:

- *server.log*: lists all actions saved on the SMC server. This file may be read from the server's web interface and from the command line interface using the `nlogs` command.
- *audit.log*: lists all actions performed by an administrator on the server. This file may be read from the server's web interface and from the command line interface using the `alogs` command.

To view server logs from the web interface:

1. Show the **Maintenance** > **Server logs** menu or show and hide the logs at any time by clicking on the black arrow at the bottom of the interface .
2. Move the cursor to select the minimum number of logs to display, from the least to the most critical: information, warning or error.
   A maximum of 1000 lines can be displayed. When the limit is reached, the oldest logs are replaced with the most recent ones in the interface.
3. To view the entire contents of the file, connect to the SMC server via the console of your hypervisor or in SSH and enter the command `nlogs`.

To view audit logs from the web interface:

1. Show the **Maintenance** > **Audit logs** menu or show and hide the logs at any time by clicking on the black arrow at the bottom of the interface .
2. You can show the **Details** column, which is hidden by default.

NOTE
The SMC server keeps logs of the past 12 weeks up to 100 MB per file. To provide legally required archiving for a year, send logs to a remote Syslog server.

To find out how to send logs to a remote Syslog server, refer to the section Sending SMC logs to a remote server in Syslog format.

13.6 Sending SMC logs to a remote server in Syslog format

SMC supports the Syslog protocol in order to collect all logs from the system and from SMC and send them to a remote Syslog server, with or without encryption.

To use the Syslog service on SMC:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Enter the command `smc-syslog-ng`. The service's current configuration will appear.

13.6.1 Sending logs to a remote server without encryption

1. Type the command `smc-syslog-ng --wizard` to select an operating mode.
2. Select the option **Store logs locally and send logs to a syslog-ng server through TCP**.
3. Enter the IP address or FQDN of the remote server as well as the port number.

13.6.2 Sending logs to a remote server with encryption

To encrypt communications when forwarding logs to the remote server, you will need three files issued by your PKI (Public Key Infrastructure):

- The client certificate in PEM format which allows the remote server to identify SMC,
- The client's private key in PEM format which would allow SMC to encrypt data so that only the remote server can decrypt it,
- The certificate of the certification authority in PEM format which would allow SMC to trust the remote server.

1. Before configuring the Syslog service, copy these three files on SMC, in `/tmp` for example.
2. Type the command `smc-syslog-ng --wizard` to select an operating mode.
3. Select the option **Store logs locally and send logs to a syslog-ng server through TCP with TLS**.
4. Enter the IP address or FQDN of the remote server as well as the port number.
5. Indicate the location of the certificates. The Syslog wizard will copy them into the folder `/data/certs/syslog-ng/`.

13.6.3 Disabling the sending of logs to a remote server

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

13.6.4 Troubleshooting

The remote Syslog server is unreachable

- *Situation*: You have specified the name of the remote Syslog server using its FQDN but the server remains unreachable.
- *Cause*: The DNS service was probably not configured properly or is unable to resolve the FQDN.
- *Solution*: Check the resolution of the DNS server by typing the command `nslookup server-syslog.domain.com` in the SMC command line interface.

When logs are forwarded with encryption, the remote server does not receive SMC logs

- *Situation*: You have configured logs to be sent to a remote Syslog server with encryption. You have provided the certificates required, but the Syslog server did not accept the encrypted communication.
- *Cause*: The remote Syslog server probably did not accept the certificates as they may have expired or been revoked.
- *Solution*: Check the error message that the remote Syslog server returned by typing the following commands in the SMC command line interface:

```
MY_SERVER_ADDR=xxx.xxx.xxx.xxx
MY_SERVER_PORT=xxxx
openssl s_client -connect ${MY_SERVER_ADDR}:${MY_SERVER_PORT} -cert
/data/certs/syslog-ng/xxxx.pem -key /data/certs/syslog-ng/xxxx.pem -CAfile
/data/certs/syslog-ng/xxxx.pem
```

13.7 Saving and restoring the SMC server configuration

Only the super administrator is allowed to back up or restore the configuration of the SMC server.

The configuration can be backed up and restored from the web interface of the server ("admin" user) or the command line interface ("root" user).

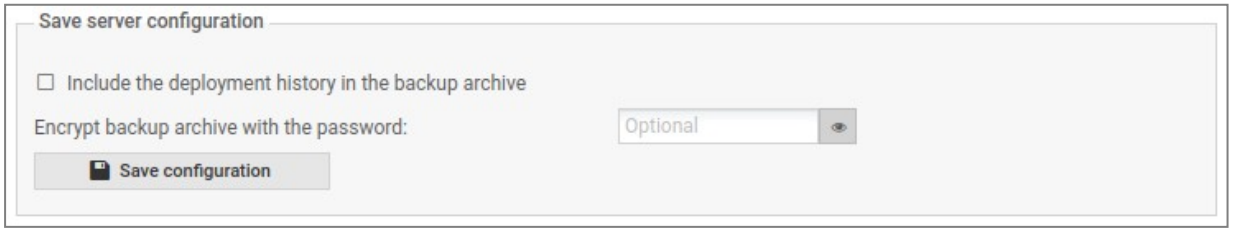
TIP
The following restriction applies to the restoration of a server configuration: the SMC server version must be the same as the version of the server from which the backup file was generated.

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.

13.7.1 Saving the server configuration from the web interface

As the "admin" user, In the **Maintenance** > **SMC Server** > **Maintenance** menu, click on **Save configuration** in the **Save server configuration** pane.



SMC makes it possible to encrypt the backup by setting a password. The password must comply with the password policy set for administrators who have local accounts.

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.

13.7.2 Saving the server configuration from the command line interface

1. To back up the server configuration from the command line interface as the "root" user, connect to the SMC server via the console of your hypervisor or in SSH.
2. Enter the command
   `smc-config-backup`
   The name of the archive name is displayed.
3. To save the configuration without the deployment history, enter the command `smc-config-backup --no-history`.
4. If you wish to encrypt the backup, type the command `smc-config-backup --password <my_password>`. Replace `my_password` with the encryption password of the backup. The password must comply with the password policy set for administrators who have local accounts.

The configuration backup file can be restored from:

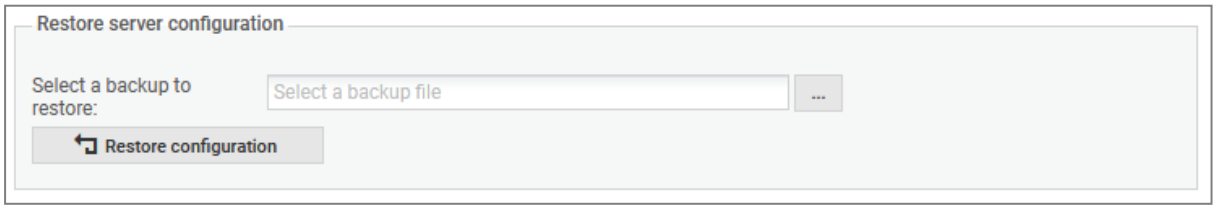
- The SMC server web interface,
- The command line interface,
- The SMC server initialization wizard.

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.

13.7.3 Restoring server configuration from the web interface

As the "admin" user, in **Maintenance** > **SMC Server** > **Maintenance**, select a backup file to restore in the **Restore server configuration** pane.

If the backup file has been encrypted with a password, a window will ask you to enter it.



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.

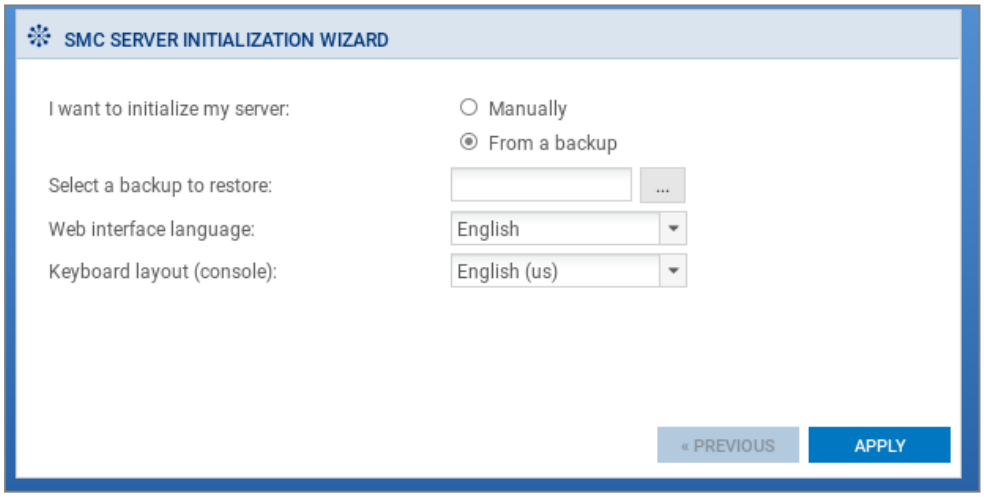
13.7.4 Restoring server configuration from the command line interface

1. To restore a server configuration from the command line interface as a "root" user, copy the backup file in */data/tmp* on the SMC server using SSH.
2. Log in to the SMC server via the console of your hypervisor or in SSH.
3. Enter the command `smc-config-restore --backup-file /path/to/backup`. Replace `/path/to/backup` with the path and name of the file.
4. If the backup file has been encrypted with a password, enter the command `smc-config-restore --backup-file /path/to/backup --password <my_password>`. Replace `/path/to/backup` with the path of the file and `my_password` with the encryption password of the backup.
5. 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.

13.7.5 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. if necessary, enter the encryption password of the backup.



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.

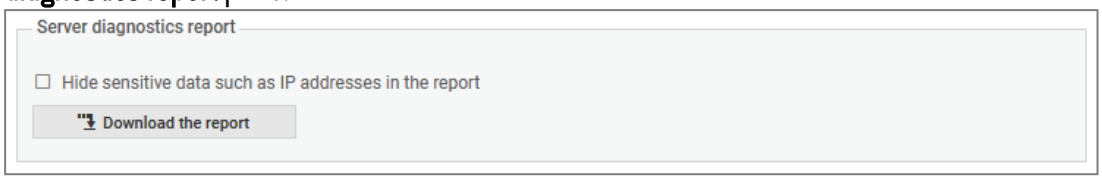
13.8 Generating a server diagnostics report

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.

13.8.1 Downloading the report from the web interface

1. In **Maintenance** > **SMC Server** > **Maintenance**, click **Download the report** in the **Server diagnostics report** pane.



The report is presented as a *tar.gz* archive with its name containing the date and time of creation.

2. Double-click on the *index.html* file to open the report in HTML format.

13.8.2 Downloading the report in command line

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Enter the command `smc-diag` or `smc-diag --help` in order to obtain details on the possible options.
   The report is presented as a *tar.gz* archive with its name containing the date and time of creation. The report is generated by default in the */tmp* folder.
3. Double-click on the *index.html* file to open the report in HTML format.

The --confidential option makes it possible to hide IP and MAC addresses.

13.9 Updating the SMC server

The SMC Version release notes contain highly important information. Please refer to them before updating the SMC server.

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

Before applying an update, we strongly recommend taking a snapshot of your virtual machine.

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

On every update the SMC configuration is migrated from the configuration file to the database. The unified configuration file is deleted. This file will be automatically updated on the older system before the migration process begins.

TIP
Depending on the configuration of your hypervisor, the update can take some time. To monitor the progress of the update, see the file /var/log/update.log.

13.9.1 Updating the SMC server from the web interface

You need to be a super administrator in order to update the SMC server from the web interface.

1. Download the update archive on your workstation from your MyStormshield personal area.
2. In **Maintenance** > **SMC Server** > **Maintenance**, select the update file in the **Update SMC** pane.
3. Click on **Update SMC**.
4. When the update is completed, log back in to the SMC server.

During the update, the SMC server will not be available, so administrators will not be able to log in.

13.9.2 Updating the SMC server in command line

1. Download the update archive on your workstation from your MyStormshield personal area.
2. Copy the archive in */data/tmp* on the SMC server using SSH.
3. Log in to the SMC server via the console of your hypervisor or in SSH.
4. Enter the command `smc-update -u /data/tmp/archivename`. Replace `archivename` with the name of your archive.
   For versions of SMC lower than 2.6, the command to enter is `fwadmin-update -u /data/tmp/archivename`.
5. Wait for the update to end. During the process, the server remains available within the current version.
6. Enter the command `reboot`. The updated system restarts.

13.10 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. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Edit the file **/data/config/fwadmin-env.conf.local** by adding the following line at the end: `SMC_HASYNC_ON_DESYNCHRO_ENABLED=false`
3. Restart the server with the command `nrestart smc`.

13.11 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.

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*.

> **NOTE**
> If you want to use the version 3 of SNMP, the related authentication and encryption protocols supported by SMC are SHA256 and AES-128.

13.11.1 Using the SNMP service

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Enter one of the following commands:

Action	Command
Enable service	`/etc/init.d/snmpd restart ; update-rc.d -f snmpd remove ; update-rc.d snmpd defaults 98`

View the status of the service	`/etc/init.d/snmpd status`
Restart the service:	`/etc/init.d/snmpd restart`
Disable the service	`nstop snmpd ; update-rc.d -f snmpd remove`

13.11.2 Using MIBs

SMC supports the following MIBs to monitor SMC:

Category	RFC	MIB
system	RFC 1213	.1.3.6.1.2.1.1
ifaces	RFC 1213 RFC 2863	.1.3.6.1.2.1.2 .1.3.6.1.2.1.31
ips	RFC 1213	.1.3.6.1.2.1.4
tcp	RFC 1213	.1.3.6.1.2.1.6
udp	RFC 1213	.1.3.6.1.2.1.7
snmp	RFC 1213	.1.3.6.1.2.1.11
mem	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.4
disk	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.9
load	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.10
cpu	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11
sysstats	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11
perf	RFC 1514	.1.3.6.1.2.1.25.4 .1.3.6.1.2.1.25.5

13.12 Customizing the certificate of the SMC server web interface

13.12.1 Customizing the certificate

The certificate that the SMC server web administration interface presents can be customized in two ways:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Replace the files *server.crt* and *server.key* located in the folder `/etc/certs/uiserver` with your own certificates and private key. File permissions must remain the same.
3. Restart the server with the command `nrestart smc`.

- or -

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Overwrite the environment variable `SMC_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 smc`.

13.12.2 Reinitializing the certificate

To go back to factory settings:

1. Use the command `smc-gen-autosigned-cert` by indicating the destination folder and subject of the certificate. This command makes it possible to generate the SSL certificate presented to the web browser one more time. This certificate is self-signed.
   ```
   smc-gen-autosigned-cert /etc/certs/uiserver/ <certificate subject>
   ```
2. Restart the server with the command `nrestart smc`.

13.13 Resetting the internal certification authority of the SMC server

The internal certification authority of the SMC server issues and manages certificates attached to connecting packages. These certificates make it possible to connect, authenticate and identify SNS firewalls that connect to the server.

When a new connecting package is generated for a firewall that the SMC server already knows, the certification authority will revoke certificates that were attached to earlier connecting packages once the firewall with the new package connects. Likewise, when a firewall is deleted from the SMC server, all certificates attached to the various connecting packages generated for this firewall will be revoked.

This internal certification authority can be reset whenever necessary.

EXAMPLE
If you want to switch from a pre-production environment to a production environment, you may need to reset the certification authority due to the different security constraints in both environments.

To reset the internal certification authority:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Enter the command `smc-reset-ca`.
3. After the script is run, SNS firewalls that were connected to the SMC server will be disconnected. Generate new connecting packages for each firewall and install them.

13.14 Using *Diffusion Restreinte* mode on SNS firewalls

In SMC, a set of security settings that comply with "*Diffusion Restreinte* (DR)" mode can be enabled on SNS firewalls. This feature guarantees a very high level of confidentiality for communications that pass through the IPsec VPN.

To enable DR mode in SMC, you must first verify whether the configurations on connected firewalls are compatible with DR mode requirements, and where necessary, fix the anomalies in incompatible configurations.

For more information regarding DR mode on SNS firewalls, refer to the *SNS User guide* and the technical note IPSec - *Diffusion Restreinte* mode.

This feature is available on SNS firewalls in at least version 4.3.

Firewalls in DR mode can be connected to an SMC server on which DR mode is not enabled.

13.14.1 Enabling the consistency check for the "*Diffusion Restreinte*" mode

WARNING
Folder administrators whose read access privileges are restricted to certain folders on SMC cannot perform this operation. For more information, refer to the section Restricting folder administrators' access privileges.

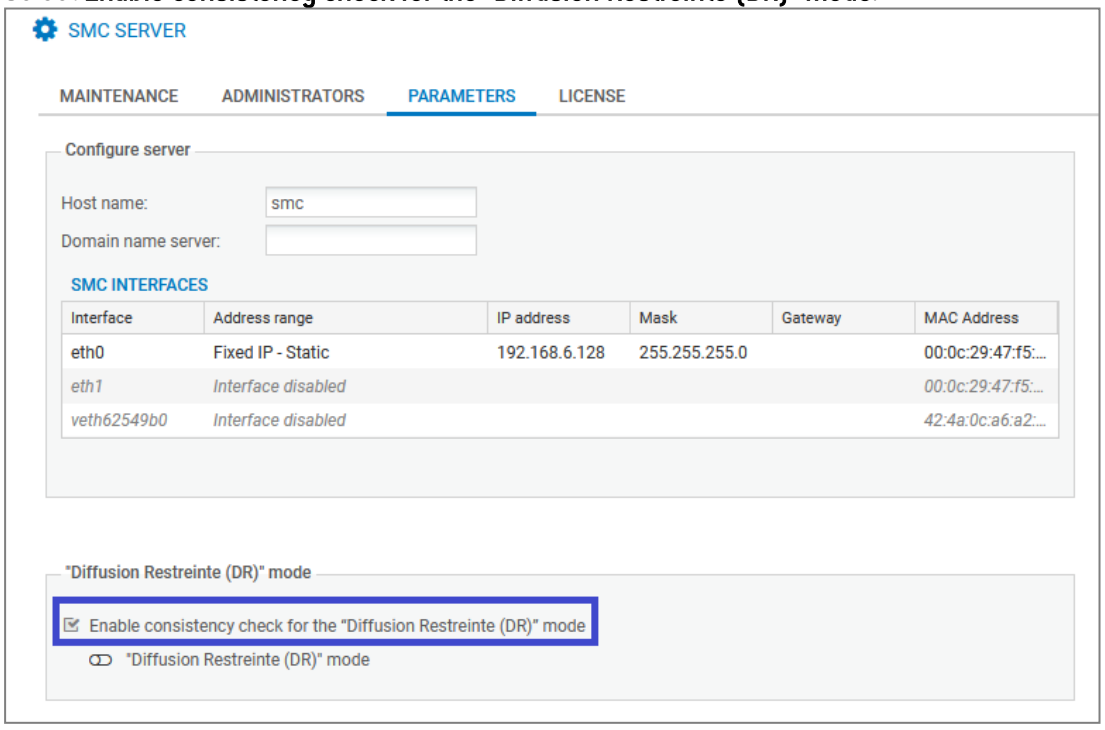
A consistency checker in SMC makes it possible to verify whether the configurations on connected firewalls are compatible with DR mode requirements:

- Signature algorithms and key sizes of firewall and authority certificates,
- Encryption profiles, authentication method and IKE version in VPN topologies. We recommend that you use the DR encryption profile that SMC provides by default. To look up this profile, go to **Configuration > Encryption profiles**. For more information on selecting encryption profiles in topologies, refer to Creating and monitoring VPN tunnels.
- Versions of firewalls connected to SMC.

This consistency check is mandatory prior to enabling DR mode.

To enable the DR mode consistency check:

1. Go to **Maintenance > SMC Server > Settings** tab > **"ANSSI Diffusion Restreinte (DR)" mode**.
2. Select **Enable consistency check for the "Diffusion Restreinte (DR)" mode**.



3. Click on **Apply**.

If there are any messages indicating that there are incompatibilities in the configuration, they will be shown in the consistency check at the bottom of the screen. You can select **Display only DR mode inconsistencies** to see only messages from the DR mode consistency check.

13.14.2 Enabling *Diffusion Restreinte* mode on SMC and firewalls

The super administrator (*admin* account) can enable DR mode on the SMC server and connected SNS firewalls.

In high availability clusters, DR mode only needs to be enabled on the active node; it will be automatically enabled on the passive node.

All firewalls must be connected to the SMC server to enable DR mode.

To enable DR mode:

1. Enable the consistency checker as described in the previous section.
2. Enable **ANSSI "Diffusion Restreinte (DR)" mode**.
3. Accept the conditions and click on **Enable DR mode**.
   When DR mode is enabled on the SMC server, an automatic deployment enables DR mode on the firewalls connected to the server.
4. Immediately restart the firewalls manually.

Enabling DR mode on the SMC server has the following consequences:

- Anomalies relating to the consistency check in DR mode are reported in the form of errors instead of warnings,
- SMC connecting packages can only be created on firewalls in SNS version 4.3 or higher,
- Firewalls on which DR mode has never been enabled can no longer be connected to SMC.

13.14.3 Disabling *Diffusion Restreinte* mode on SMC and firewalls

The super administrator (*admin* account) can disable DR mode on the SMC server. Disabling DR mode from SMC does not disable it on firewalls.

To disable DR mode:

1. Go to **Maintenance > SMC Server > Settings** tab > **"ANSSI Diffusion Restreinte (DR)" mode**.
2. Disable "**ANSSI Diffusion Restreinte (DR)**" mode.
   DR mode is disabled on the SMC server. This operation does not make any changes to firewalls, which can continue to connect to the SMC server.

13.15 Adding a disclaimer to the login page

A warning message for administrators can be added to the login page of the SMC server's web administration interface. You can therefore warn them of particular restrictions or precautions they might need to know about when using the SMC server before they log on.

The message will then appear in the **Disclaimer** section.

To add a disclaimer file:

1. Create a text file named *login_disclaimer* containing the desired message. For a better layout, the text can be in HTML without using Javascript. UTF-8 encoding is supported.
2. Log in to the SMC server via the console of your hypervisor or in SSH.
3. Add the *login_disclaimer* file (without any extension) to the folder *data/config*.

This file will be kept in the server's configuration backup.

13.16 Connecting to the command line interface via SSH keys

For a transparent connection to the SMC command line interface via SSH, you can configure the use of SSH keys.

Prior to configuring this feature, you must generate a pair of SSH keys on your workstation.

Administrator SSH keys are saved in the folder `/data/ssh` in SMC.

To add an SSH key allowing you to connect to SMC:

1. Ensure that you are able to access SMC via SSH in your profile. For more information, refer to the section Managing administrator privileges as super administrator.
2. On your workstation, copy your public SSH key.
3. Connect to SMC in SSH using your password.
4. Create the file `/data/ssh/authorized_key.<user-name-smc>`. Replace <user-name-smc> with your ID as defined in your SMC profile.
5. Paste your public key in the file that you have just created.

You are now ready to connect to SMC via SSH.

If the SMC server is hosted in the Amazon Web Services (AWS) cloud, follow the procedure in the *Installation guide* to generate the key pair.

14. Enabling and managing SMC's public API

SMC has a standard REST API with which your SMC servers can be used and queried through your own orchestration tools.

All SMC features are not yet available in the public API. It will be enriched as new versions are released.

The public API is not enabled by default. Only the SMC super administrator can enable it.

Authentication over the public API is secured by API keys that administrators generate. These keys have read/write or read-only privileges as well as a validity period that can be configured.

All operations performed via the public API are recorded in audit logs.

To make it easier to use the API, OpenAPI documentation is available on the SMC server through the address *https://<@SMCIP>/docs/papi* or via the link shown in the SMC web interface.

Documentation can also be found on Stormshield's Technical Documentation website.

NOTE
In case of intensive use of the API, i.e., several write requests within a few seconds, while other users are using the administration web interface at the same time, the performance of SMC may be impacted. Some requests may fail.
Likewise, if you plan a regular intensive use, we recommend that you disable configuration consistency checking to avoid impacting SMC performance. For more information, see the section Verifying configuration consistency.

14.1 Enabling the public API

SMC's public API is disabled by default.

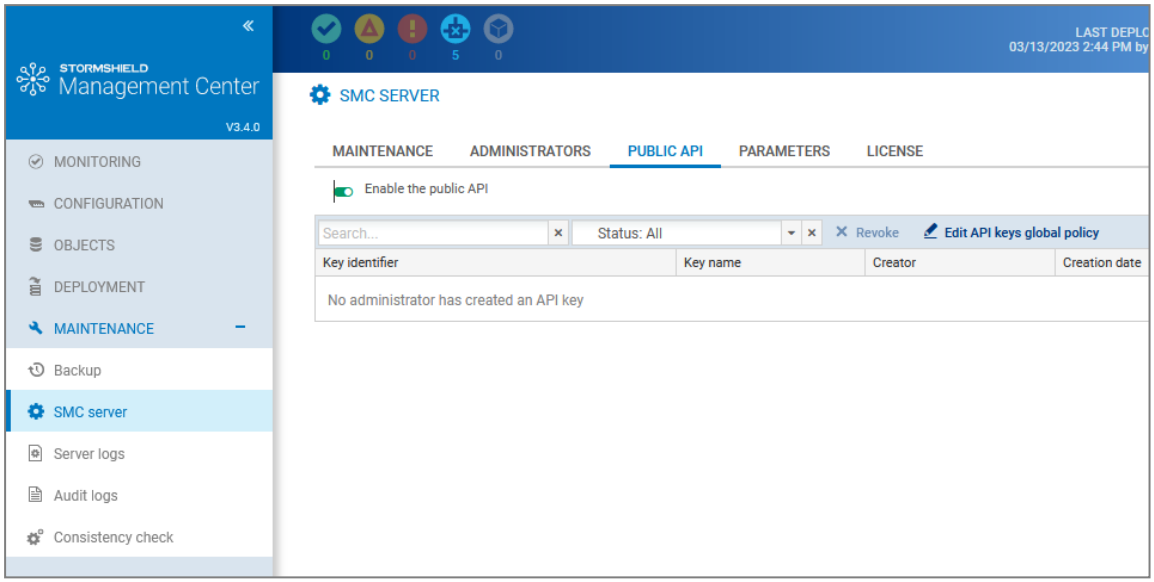
Only the super administrator can enable or disable it from the SMC web administration interface.

When the public API is enabled:

- Access to routes on the API is allowed,
- Access to documentation about the API is allowed,
- The super administrator can grant permissions to create and revoke API keys to other administrators,
- Administrators with the relevant privileges can create and revoke API keys.

To enable the public API:

1. In **Maintenance** > **SMC server**, show the **Public API** tab,
2. Select **Enable Public API**.



The **Public API** tab displays the API keys created by other administrators. The super administrator cannot create API keys, but can revoke them. For more information on revoking keys, refer to Revoking API keys.

14.2 Allowing administrators to create and revoke API keys

An API key is required for authentication on a public API. Administrators can create API keys in the SMC web administration interface, by setting read/write or read-only permissions for the keys, as well as an expiry date. For more information on creating keys, refer to Creating API keys.

The API keys created must be added to the *Authorization* header in each API request.

EXAMPLE OF AN API REQUEST
In command line: `curl -H "Authorization: Bearer <API_KEY>" https://<IP_SMC>/api/v1/firewalls`

Permissions to create and revoke API keys are granted by the super administrator, in administrators' profiles.

NOTE
The super administrator cannot create API keys.

To grant an administrator permissions to create and revoke API keys:

1. In **Maintenance** > **SMC server**, show the **Administrators** tab,
2. Double-click on the profile of an administrator,
3. Select **API keys creation/revocation** in **Access privileges**.

This option is grayed out if the public API is disabled.

14.3 Editing the API key global policy

The super administrator can set a default validity period for API keys. When another administrator creates a key, the validity period set by the super administrator will then be suggested by default in the **Expiry date** field, which the administrator can edit.

To edit the API key global policy:

1. In **Maintenance** > **SMC server**, show the **Public API** tab,
2. Click on **Edit the API key global policy**.
3. Set the validity period suggested by default to administrators when they create a key, and apply. This period cannot exceed 25 years.

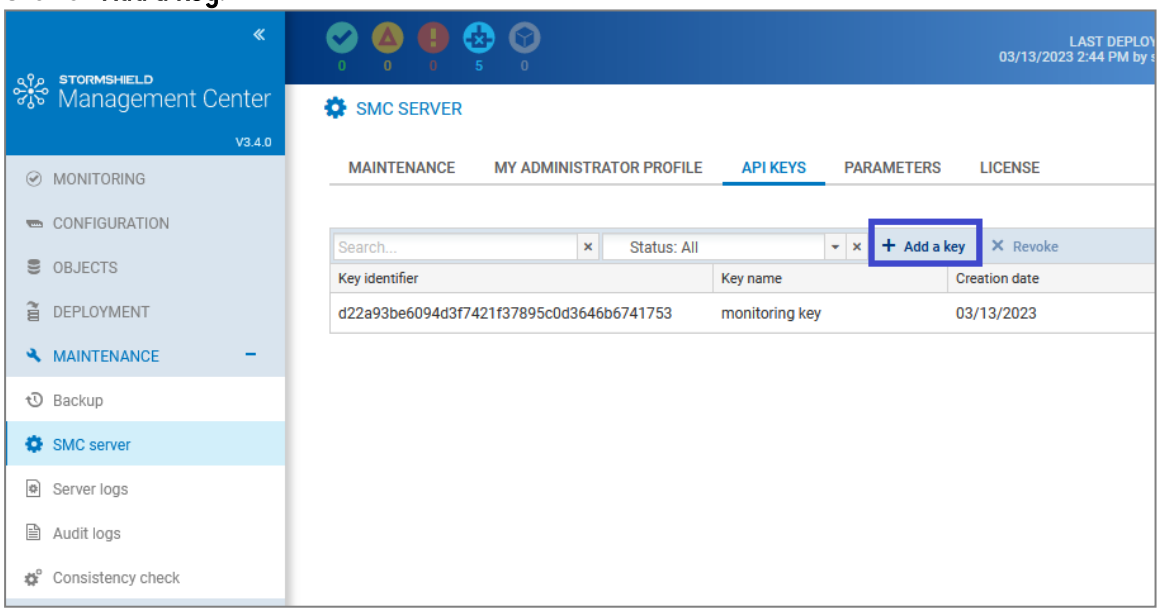
14.4 Creating API keys

Administrators who hold the **API keys creation/revocation** privilege can create the API keys to use for authentication on the public API. For more information on this privilege, refer to Allowing administrators to create and revoke API keys.

These keys contain an ID, name, expiry date and read/write or read-only permission. They are required for every public API request.

To create a key:

1. In **Maintenance** > **SMC server**, show the **API keys** tab. Keys that have already been created will be listed along with their information.
2. Click on **Add a key**.



3. Enter a name and expiry date. The default validity period is set by the super administrator. For more information, refer to the section Editing the API key global policy.
4. In the **Usage** field, select the desired option. You cannot select **Write** if you do not hold this permission yourself in SMC as an administrator.
5. When you click on **Apply**, the key will not be saved in the database. It must be copied and stored in a safe place as it will no longer be available later.

API keys can be used in API documentation to test requests:

1. Click on the **See API documentation** link in the **API keys** tab in Administrator view, or in the **Public API** tab in Super administrator view.

2. Click on

.
3. Enter the API key in the **Value** field.
4. Click on **Authorize** then on **Close**.

When the profile of an SMC administrator is deleted, API keys associated with this administrator will be automatically deleted if they had been revoked earlier. For more information on revocation, see the next section.

14.5 Revoking API keys

The super administrator can revoke all API keys and administrators can revoke the API keys that they created themselves. When API keys are revoked, you can no longer use them to submit requests on the API.

As super administrator:

1. In **Maintenance** > **SMC server**, show the **Public API** tab,
2. Select the key to revoke in the grid,
3. Click on **Revoke**.

As super administrator, if you wish to delete the profile of an administrator, you must first revoke the API keys associated with them. Profiles cannot be deleted if the administrator still holds active keys.

Similarly, an administrator's **Read/Write** privilege in **SMC** cannot be withdrawn if this administrator holds active API keys that also have the **Read/Write** privilege. The keys in question must be revoked first.

As administrator:

1. In **Maintenance** > **SMC server**, show the **API keys** tab.
2. Select the key to revoke in the grid,
3. Click on **Revoke**.

14.6 Customizing the listening port of the public API

The public API and its documentation use port 443 by default.

The default port can be changed by modifying the environment variable SMC_PUBLIC_API_PORT_INT:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. In the file **/data/config/fwadmin-env.conf.local**, add the environment variable `SMC_PUBLIC_API_PORT_INT="portNumber"`.
3. Restart the server with the command `nrestart smc`.

15. Further reading

Additional information and answers to questions you may have are available in the Stormshield knowledge base (authentication required).

Annexe A. Details of smc-xxx commands

This section sets out the list of commands specific to SMC that can be used in the command line interface to manage the server. To find out how to log on to the command line interface, refer to the section Connecting to the command line interface.

There are other smc-xxx commands that were not mentioned in this list as they are solely intended for the internal operations of the server.

The set of smc-xxx commands replaces the fwadmin-xxx commands used in 2.5 and lower versions. These commands will continue to be available and operational but will be removed in future versions.

Command	Action
`smc-config-backup`	Saves the configuration of the SMC server. See section Saving the server configuration from the command line interface.
`smc-config-restore`	Restores the configuration of the SMC server. See section Restoring server configuration from the command line interface.
`smc-date-time`	Displays and configures the system's date, time and time zone. See section Changing the SMC server time zone and date.
`smc-deploy`	Deploys the configuration on the SNS firewalls. See section Deploying a configuration on firewalls.
`smc-diag`	Downloads a SMC server diagnostics report. See section Generating a server diagnostics report
`smc-export-routes`	Exports to a CSV file the static routes, return routes and default routes of firewalls in at least version 4.2.4 and for which the network configuration is managed in SMC. See section Configuring routing.
`smc-import-firewalls`	Creates firewalls in SMC and their connecting package. See section Importing SNS firewalls from a CSV file.
`smc-import-routes`	Imports the routes of firewalls in at least version 4.2.4 and for which the network configuration is managed in SMC. See section Configuring routing.
`smc-gen-autosigned-cert`	Resets the certificate presented by the SMC server's web administration interface. See section Customizing the certificate of the SMC server web interface.
`smc-import-crl`	Imports a Certificate Revocation List (CRL). The CRL is automatically linked to the certification authority which signed it.
`smc-import-objects`	Imports objects originating from a firewall export in CSV format. See section Importing objects.
`smc-import-rules`	Imports filter and NAT rules, and the objects linked to these rules, from the export of a SNS firewall rules in the CSV format. See section Importing rules from connected firewalls.
`smc-install-certificate`	Installs a P12 certificate on a firewall. See section Importing or declaring a certificate for a firewall.
`smc-keyboard`	Changes the language of the keyboard in the command line interface.

`smc-logs`	Displays logs of all actions saved on the SMC server. Equivalent to the `nlogs` command.
`smc-redundancy --secondary <BACKUP_NODE_IP>`	Enables redundancy between two SMC servers. See section Setting up SMC server redundancy in the *Administration guide*.
`smc-reset-ca`	Resets the internal certification authority of the SMC server. See section Resetting the internal certification authority of the SMC server.
`smc-sns-cli-script`	Runs SNS CLI commands on a pool of firewalls. See section Running SNS CLI commands on an environment of firewalls.
`smc-syslog-ng`	Configures the logging service in Syslog format. See section Sending SMC logs to a remote server in Syslog format.
`smc-update`	Updating the SMC server See section Updating the SMC server.
`smc-version`	Displays the version of the SMC server. See section Verifying the SMC server version in command line.

Annexe B. Details of SMC_XXX environment variables

This section maps the names of environment variables prior to 3.4.0 and the names from version 3.4.0 onwards.

There are other variables that were not mentioned in this list as they are solely intended for the internal operations of the server.

Older FWADMIN_XXX variables will continue to be available and operational but will be removed in future versions.

Environment variables are configured in the **/data/config/fwadmin-env.conf.local** file. To know the purpose of the variables, refer to the sections of the *SMC Administration guide* or to the Stormshield Knowledge base.

- Variables with names that end with "_ENABLED" must contain the boolean values “true” or “false”.
- Variables with names that end with "_INT" must contain numbers. Check that the value matches the corresponding unit if there is one.
- In all other cases, the variable values are considered character strings.
- If the variable is not defined, the default value is the value chosen by SMC.

Variable name	Unit	Default value
SMC_AUTOBACKUP_EXCLUDE_PRIVATE_KEY_ENABLED		false
SMC_BASE_STATION_ENABLED		false
SMC_CERT_SUBJECT_AS_PEER_LOCALID_ENABLED		false
SMC_CFGCHECK_BEFORE_DEPLOY_ENABLED		true
SMC_CFGCHECK_ENABLED		true
SMC_CFGCHECK_INCOHERENCIES_INT		100
SMC_CONFIG_STATUS_CHECK_PERIOD_INT	msec	120000
SMC_CSV_DELIMITER		,
SMC_DECBACKUP_DIR		/opt/stormshield/security
SMC_DEPLOYMENT_TIMEOUT_BEFORE_ROLLBACK_INT	sec	30
SMC_EXPORT_TIMEOUT_INT	msec	30000
SMC_FW_CONFIG_GENERATION_TIMEOUT_INT	msec	900000
SMC_FW_CONNECTION_TIMEOUT_INT	sec	60
SMC_FW_DEPLOYMENT_ROLLBACK_ENABLED		true
SMC_FW_DEPLOYMENT_TIMEOUT_INT	sec	300
SMC_FW_DEPLOYMENT_VPN_PEER_INACTIVITY_INT		0
SMC_FW_LICENSE_CRITICAL_INT	days	0

SMC_FW_LICENSE_WARNING_INT	days	0
SMC_FW_TPM_ENABLED		true
SMC_GETSA_POLLING_PERIOD_INT	msec	30000
SMC_GETSPD_POLLING_PERIOD_INT	msec	30000
SMC_HAINFO_POLLING_PERIOD_INT	msec	30000
SMC_HASYNC_ON_DESYNCHRO_ENABLED		true
SMC_LDAP_FIELD_NAME_DN		
SMC_LDAP_FIELD_NAME_LOGIN		
SMC_LDAP_FIELD_NAME_MEMBEROF		
SMC_MESSAGING_RESPONSE_CHUNK_TIMEOUT_INT	sec	30
SMC_MESSAGING_RESPONSE_DEFAULT_TIMEOUT_INT	sec	120
SMC_MONITOR_ROUTE_POLLING_PERIOD_INT	msec	60000
SMC_MONITOR_STAT_POLLING_PERIOD_INT	msec	60000
SMC_PROXY_RESPONSE_TIMEOUT_INT	sec	300
SMC_SNS_CERTS_PROBE_EXPIRATION_INT	days	30
SMC_SNS_CLI_ATTACHMENTS_DIR		/data/tmp/sns-cli/input
SMC_SNS_CLI_CSV_DELIMITER		;
SMC_SNS_CLI_OUTPUT_DIR		/data/tmp/sns-cli/output
SMC_SNS_CLI_SCRIPT_MAX_UPLOAD_SIZE_INT	bytes	2097152
SMC_SNS_CLI_STEP_TIMEOUT_INT	sec	120
SMC_SNS_DEPLOYMENT_ROLLBACK_TIMEOUT_INT	sec	180
SMC_SNS_UPDATE_HA_LINK_TIMEOUT_INT	sec	1800
SMC_SNS_UPDATE_MAX_KEEP_DAYS_INT	days	14
SMC_SNS_UPDATE_SYSTEM_CLONE_TIMEOUT_INT	sec	1800
SMC_SYSTEM_PROP_POLLING_PERIOD_INT	msec	3600000
SMC_UI_PORT_INT		443
SMC_UI_SERVER_CERT_PATH		/etc/certs/uiserver
SMC_VPN_MESH_ROUTE_BASED_MAX_PEERS_INT		50

Appendix C. Compatibility of SMC/SNS firewalls

The SMC server manages SNS firewalls from version 4.3 upwards.

This table recaps the lowest versions of SNS firewalls required in order to be compatible with the following SMC features:

Feature/Object	Version of SMC	Lowest version of SNS firewall required
Managing network interfaces (in read-only mode)	3.0	3.7.0 [1]
Managing network interfaces (in write mode)	3.0.1	4.2.3
Managing "*Diffusion Restreinte* (DR)" mode	3.1	4.3.21 LTSB or 4.7
Active Update distribution point	3.1	4.3.3
Various versions of IKE supported on the same firewall	3.1.3	3.7.0
Managing routing (in read-only mode)	3.2	3.7.0
Routing (in write mode)	3.2	4.2.3
SD-WAN support	3.2	4.3.3
Managing IPSec virtual tunnel interfaces (VTI)	3.4	4.2.3
Web services filtering	3.4	4.4
QoS configuration	3.6	4.3.15 LTSB or 4.5.3
Managing BIRD v2 dynamic routing	3.6	4.8.1

NOTE
To be able to monitor the status of VPN topologies containing SN firewalls in version 4.2 or higher, you need to use an SMC server in version 3.0 or higher.

[1] As of SMC version 3.6, compatibility with 3.x versions of SNS will no longer be tested.

documentation@stormshield.eu

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

Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.