STORMSHIELD

STORMSHIELD MANAGEMENT CENTER

RELEASE NOTES

Version 3

Document last updated: June 29, 2026

Reference: sns-en-SMC-release_notes-v3.9.2

Table of contents

New behavior 3
Resolved vulnerabilities for SMC 3.9.2 5
SMC 3.9.2 fixes 6
Compatibility 8
Recommendations 9
Known issues 13
Explanations on usage 14
Documentation resources 16
Installing this version 17
Previous versions of SMC v3 19
Contact 107

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

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

New behavior

Changes introduced in version 3.7

To connect an SNS firewall to SMC, you must generate and install a different connecting package on each firewall. To ensure that each firewall has been connected with its own package, SMC now checks the serial numbers of firewalls that connect to it.

As a result, if an SMC connecting package is used by mistake for several firewalls, SMC 3.7 will now only allow the first firewall to connect, and reject the others. This will prevent the firewalls in question from taking turns to connect to SMC, and from being considered a single firewall.

If this describes your use case before version 3.7, please refer to the section Information prior to an update of the server to restore the normal function of all your firewalls.

Changes introduced in version 3.6

Lowest version of SNS firewalls managed by SMC 3.6

As of SMC version 3.6, SMC no longer supports SNS firewalls in versions lower than 4.3.

Managing dynamic routing during an SNS firewall update

When an SNS firewall is being updated to version 4.8.1 EA or higher, SMC now automatically downloads the firewall's local dynamic routing configuration when it reconnects after the update.

Backing up the SMC server

The SMC server's configuration backup no longer contains system files relating to users and groups. When a backup is being restored, SMC now retrieves the information relating to users and groups that was stored on the host (logins, passwords, etc.).

Changes introduced in version 3.4

RSYNC command

Some system packages have been removed because SMC does not use them and as part of this cleaning, the RSYNC system command has been removed. To copy files, you can still use the `cp` command.

Interfaces with network or broadcast addresses

SMC no longer allows interfaces to be created with network or broadcast addresses, to ensure that interfaces correspond to SNS firewalls.

When a network has a /31 subnet mask, both of its available addresses will still be accepted, as they are not considered network and broadcast addresses.

For more information before updating to SMC version 3.4, refer to Recommendations.

Configuration deployment and automatic backups

SMC now generates a warning when an automatic backup is scheduled to start while a configuration deployment is in progress. The automatic backup will then be canceled.

Change introduced in version 3.2.1

In SMC, SNS firewalls in versions lower than 3.7 can no longer be connected and managed.

If you have SNS firewalls in versions below 3.7 that are connected to SMC, they will no longer be able to connect to SMC 3.9.2. We recommend that you update your SNS firewalls to a version that SMC supports.

Resolved vulnerabilities for SMC 3.9.2

The indicated severity is the level at the time of the initial publication of the security advisory on https://advisories.stormshield.eu/.

PostgreSQL vulnerabilities

Moderate severity vulnerabilities were fixed after the PostgreSQL component was upgraded.

Details on these vulnerabilities can be found on our website https://advisories.stormshield.eu/2026-012.

SMC 3.9.2 fixes

Active Update server

Active Update server certificate format

The certificate that SMC generated for Active Update was not compatible with SNS in versions 5.1.x and higher.

SMC version 3.9.2 provides a certificate that is compatible by default with all versions of SNS.

The certificate is automatically updated when version 3.9.2 is installed, except when a custom certificate is used.

WARNING
If you are using the SMC Active Update server with the default certificate, refer to the Recommendations section before updating SMC to version 3.9.2.

Authorities and certificates

Support reference 86360

Retrieving information about SNS firewall certificates

If you have opted to declare the certificates used by firewalls in SMC by entering their subjects and senders in the **System > IPsec VPN** tab in firewall properties, SMC now runs commands to retrieve certificate information gradually every day at midnight.

Previously, SMC would run commands simultaneously on all relevant firewalls, which could cause overloading and downgrade server performance.

Filter and NAT rules

Support reference 86366

Importing rules

Filter and NAT rules can now be imported on SMC from a CSV file containing up to 16,000 rules.

If an issue occurs while deploying a large quantity of rules on SNS firewalls, refer to the Stormshield knowledge base.

VPN topologies

Support reference 86361

Deploying VPN topologies on SNS firewalls with DR mode enabled

VPN topologies can now be deployed across firewalls on which *Diffusion Restreinte* mode has been enabled, and which are in version 5.x.

SMC public API

Support reference 86238

The "vpnLocalAddress" and "publicIpAddress" fields are now correctly fetched by route API calls:

- GET /papi/v1/vpn/topologies/{uuid}
- GET /papi/v1/vpn/topologies

Compatibility

For more information, refer to the Product life cycle guide.

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 and versions below 5.1.0
	3.9	5.1.0
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
In order to deploy route-based VPN topologies or virtual IPsec interfaces (VTIs) on SNS firewalls in version 5.1.0 or higher, you need to use an SMC server in version 3.9 or higher. Refer to the Recommendations section in the Release notes prior to any update.

[1] As of SMC version 3.6, compatibility with 3.x versions of SNS will no longer be tested.

Recommendations

Information prior to an update of the SMC server

Updating to version 3.9.2 - Active Update server

If you are using the Active Update server feature in previous versions of SMC with the certificate that is provided by default to set up communication between SMC and SNS firewalls, refer to the information below.

Version 3.9.2 applies changes to the certificate that is provided for the Active Update feature. SNS firewalls with an earlier version of the certificate will no longer be able to communicate with SMC 3.9.2 or update their databases.

To continue using the feature after an update to version 3.9.2, import the Active Update certificate again on each affected firewall, then recreate the Active Update configuration script. For help on these operations, refer to the section *Using the SMC Active Update server* in the SMC *Administration guide*, and refer to steps 1 and 3 in *Configuring SNS firewalls automatically*.

Updating to version 3.9 - Firewalls in version 5.1.0

WARNING
Information if you have route-based VPN topologies or VTIs in your configuration.

As a result of the new settings for virtual IPsec interfaces (VTI) on firewalls in version 5.1.0, which were announced in SMC 3.9.1 new features and enhancements, we recommend that you begin by updating the SMC server to version 3.9, and subsequently updating your firewalls to version 5.1.0, in order to ensure that SMC continues to be compatible with the firewalls.

Updates to version 3.7 - Connecting SNS firewalls to SMC

If in an earlier version of SMC, you had used the same connecting package to connect several firewalls, they may have taken turns to connect to SMC under the same name. Furthermore, version 3.7 could prevent them from connecting. To restore the configuration before the update to version 3.7:

1. Generate a new connecting package for each firewall.
2. Install it on the corresponding firewall.

The command `smc-import-firewalls /data/tmp/filename.csv --package-only` can be used to generate several packages at one go.

If after an update to version 3.7, a firewall is still unable to connect to SMC:

1. Select **Allow another firewall to connect with the same package as part of a defective hardware replacement (RMA)** in the **System** > **Configuration** tab of the firewall properties in the SMC interface.

If the issue affects several firewalls:

1. Log in to the SMC server via the console of your hypervisor or in SSH.
2. Disable the firewall serial number verification feature, by using the environment variable SMC_LOCK_SERIAL_NUMBER_ENABLED=false in the file **/data/config/fwadmin-env.conf.local**.
3. Restart the server with the command `nrestart smc`.
4. When all firewalls have been able to reconnect, enable the firewall serial number verification feature again by using the environment variable.

Managing dynamic routing from SMC

As of SMC version 3.6, when an SNS firewall is being updated to version 4.8.1 EA or higher, SMC automatically downloads the firewall's local dynamic routing configuration when it reconnects after the update.

As a result, Stormshield advises against making changes to a firewall's dynamic routing configuration between the end of its update and its reconnection to SMC.

Managing the configuration of SNS firewall network interfaces during an update from a version previous to 3.4 to a version higher than 3.4

After an update to a version higher than 3.4, the SMC server needs to retrieve again the configuration of interfaces and routing of SNS firewalls.

As such, please take note of the following points:

1. Before updating SMC, make sure you deploy the current changes to the firewall network configuration. Otherwise, changes will be lost.
2. Interface and route configuration remains read-only on SMC as long as the SNS firewall does not reconnect to SMC after the update.

After updating to a version higher than 3.4, if you manage a pool of over 200 firewalls, synchronizing the network configuration of SNS firewalls can cause the system to slow down. If this occurs, we recommend that you temporarily disable the consistency checker before updating SMC, and enabling it again later. To do so:

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: `FWADMIN_ENABLED_CFGCHECK=false` (replaced by the variable `SMC_CFGCHECK_ENABLED` from version 3.4 onwards).
3. Restart the server with the command `nrestart fwadmin-server`.
4. After the update, once all the firewalls are connected back, delete the line in the file and restart the server.

Interfaces with network or broadcast addresses

SMC no longer allows interfaces to be created with network or broadcast addresses, to ensure that interfaces correspond to SNS firewalls.

Before updating SMC, ensure that you do not have such interfaces in your configuration. Otherwise, the SMC administration interface will become unusable, and you will need to restore a snapshot or shadow copy of your virtual machine.

Size of the System disk

After successive updates of the SMC server, it may happen that free space on the System disk is not enough to allow new updates to be installed:

1. Use the following command to check the state of the system disk:

```
df -h /
```

For example:

```
[root@smc] - {~} > df -h /
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       1.9G  1.5G  215M  88% /
```

2. If the disk is almost full, you need to deploy a new virtual machine using the following procedure:
   a. Back up the 3.x SMC server configuration.
   b. Shut down the SMC server.
   c. Deploy a new SMC server in the same 3.x version.
   d. Restore the the configuration from your backup on the new virtual machine.
3. Update your new SMC server to the new 3.y version.

EXAMPLE

To update from a 3.1.4 version to a 3.1.6 version:

a. Back up the 3.1.4 SMC server configuration.
b. Shut down the server.
c. Deploy a new 3.1.4 server.
d. Restore the backed up configuration on the new 3.1.4 server.
e. Update the new server to version 3.1.6.

To get help or more information on these procedures, refer to the *SMC Administration guide* or contact the Technical Assistance Center.

Access to the SMC server during updates

When you update your SMC server, we recommend that you prevent other administrators from accessing SMC for the duration of the update. If you do not do so, they will not be informed of updates in progress and any configurations they are working on will not be saved.

Minimum hardware recommendations

Refer to the section *Adapting the size of the virtual environment according to the number of SNS firewalls* in the *SMC installation guide* to correctly scale your virtual environment.

Warning before connecting SNS firewalls to the SMC server

Take note of the following information if you wish to connect the SMC server with a pool of SNS firewalls that are already used in production, and which contain global configuration items.

Whenever SMC deploys a configuration on a firewall, all global configuration items found 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 items 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)**.

By connecting an SNS firewall to SMC, you accept that these global items, which could have been set up on this firewall, will be overwritten as soon as SMC deploys the configuration.

However, local objects, rules and VPN tunnels (which you handle by default in the firewalls' web administration interface) will never be modified or deleted when SMC deploys a configuration.

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

In most cases, in which the firewall to be connected does not have any global configuration items, no particular precautions need to be taken in connecting the firewall to SMC, and doing so will leave no impact on production.

In any case, we advise you to back up your firewall's configuration before connecting it to SMC.

Known issues

The up-to-date list of the known issues related to this version of SMC is available on the Stormshield Knowledge base. To connect to the Knowledge base, use your MyStormshield customer area identifiers.

Explanations on usage

Replacing an SNS firewall's connecting package

In SMC, you can generate a new connecting package at any time for a firewall that is already connected to SMC, but the firewall's web administration interface does not allow the replacement of a package that has already been installed. A CLI command can be used to replace a package. For more information, refer to the section Installing a new connecting package on an SNS firewall in the *Administration guide*.

Various versions of the IKE protocol supported on the same firewall

In VPN topologies, different versions of the IKE protocol can be supported on the same firewall only if there is a single firewall in common across several topologies. If several topologies configured with various versions of IKE have several firewalls in common, the version of the topology that was created first in the topology configuration screen will be the one deployed.

Using the All object in VPN topologies

Within a policy-based VPN topology, when two different peers use the *All* object to define traffic endpoints, then the connection between SMC and the SNS firewall may fail, unless you have configured policy-based routing rules to support this use case. In star topologies, the same problem occurs if the *All* object is used to define the center of the star and one of the satellites.

Using VTI objects generated by route-based VPN topologies

When a route-based VPN topology is modified or deleted in SMC, Host VTI objects that this topology automatically generates to represent remote peers 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.

Deploying VPN topologies

VPN topologies cannot be deployed from the SMC server if the name of an SNS firewall is too long. The names of VPN topologies on firewalls cannot exceed 127 characters.

Configuring routing on SMC

Several of the interfaces used for contacting the SMC server can be configured, but only one default gateway can be declared on a single interface. Routing must be configured manually for the other interfaces. An article in the Stormshield Knowledge base sets out the procedure to follow.

Using global network objects in a local configuration

On SNS firewalls, global objects may be used in local configurations. However, when SMC deploys a configuration on a firewall, existing global objects on the firewall will be deleted and replaced with objects defined in the SMC configuration. To keep the local configuration running, you need to impose the deployment of necessary global objects on affected firewalls.

For more information, refer to the section Warning before connecting SNS firewalls to the SMC server.

Migrating a V model virtual firewall to an EVA model

V-50, V-100 and V-200 virtual firewalls can no longer be upgraded to EVA models using the variable %FW_UPD_SUFFIX% in an SNS CLI script run from the SMC server.

To work around this issue, replace the variable %FW_SIZE% with the value "XL-VM" in the upgrade script.

Documentation resources

The following technical documentation resources are available on the Stormshield Technical Documentation website or on Stormshield Institute website. We suggest that you rely on these resources for a better application of all features in this version.

Guides

- Stormshield Management Center Installation guide
- Stormshield Management Center Administration guide
- SMC public API documentation
- Stormshield Network Configuration and Administration Manual

Videos

- CLI Commands and Scripts, available on Institute.

Installing this version

To update your SMC server to version 3.9.2, we recommend that you carefully follow the procedure below.

Before installing the version, ensure that you have read the Product life cycle guide and the sections New firewall behavior and Recommendations.

Do note that the server's update mechanism will automatically restart at the end of the procedure.

Update paths

To update your SMC server, intermediate updates may be required depending on its original version:

Original version	Intermediate updates required
2.x	Version 3.1.6
3.0 and higher	None

For more information, you can refer to the Stormshield Knowledge base (authentication required).

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 3.9.2 version of Stormshield Management Center:

1. Log in to MyStormshield with your login and password.
2. In the panel on the left, select the **Downloads** section.
3. In the panel on the right, select the relevant product and version.
4. Download the files *build.sha256sum*, *build.sha256sum.sign* and *smc-sign.crt* as well if you wish to check the integrity of binary files.

Checking the integrity of binary files

Enter one of the following commands to check the integrity of Stormshield Management Center binary files:

- Linux operating system: `sha256sum -c build.sha256sum`
- In PowerShell on a Windows operating system:
  - Enter `cat build.sha256sum`. The command will return the hashes and associated files.
  - To compare a file's hash, copy it and enter `(Get-FileHash my-file.ext -A SHA256).Hash -eq "hash"`.

Verifying the signature of the *build.sha256sum* file

The *build.sha256sum.sign* file is the signature of the *build.sha256sum* file. Verifying it will guarantee that *build.sha256sum* has not been modified.

OpenSSL is required to verify the file's signature.

1. If you need to install OpenSSL in Microsoft Windows, use the widget tool and the PowerShell command below:
```
> winget install ShiningLight.OpenSSL
```
2. Next, run the "Win64 OpenSSL Command Prompt" program.

To verify the signature in Linux and Windows operating systems:

1. Use the certificate *smc-sign.crt*:
```
openssl x509 -in smc-sign.crt -pubkey -noout -out smc-sign.pem
openssl dgst -sha256 -verify smc-sign.pem -signature
build.sha256sum.sign build.sha256sum
```

If you want to verify whether the certificate was indeed issued by the SMC certification authority, use the command:

```
openssl verify -CAfile Stormshield.Management.Center.2.pem smc-sign.crt
```

Updating the SMC server

For the procedures on updating the server from the web interface or command line interface, refer to the section Updating the SMC server in the *Administration guide*.

Updating the SMC server when redundancy has been set up

The update procedure is specific and has to follow the steps described in the section Setting up SMC server redundancy in the *Administration guide*.

Previous versions of SMC v3

In this section, you will find the features and fixes from previous versions of SMC v3.

3.9.1	New features	Resolved vulnerabilities	Bug fixes
3.8.1			Bug fixes
3.8	New features		Bug fixes
3.7.1	New features	Resolved vulnerabilities	Bug fixes
3.6	New features	Resolved vulnerabilities	Bug fixes
3.5.4			Bug fixes
3.5.3	New features		Bug fixes
3.4.3		Resolved vulnerabilities	
3.4.2			Bug fixes
3.4.1			Bug fixes
3.4	New features		Bug fixes
3.3.3	New features	Resolved vulnerabilities	Bug fixes
3.3.2	New features	Resolved vulnerabilities	Bug fixes
3.3.1	New features	Resolved vulnerabilities	Bug fixes
3.2.2			Bug fixes
3.2.1	New features		Bug fixes
3.1.6		Resolved vulnerabilities	Bug fixes
3.1.5			Bug fixes
3.1.4			Bug fixes
3.1.3	New features		Bug fixes
3.1.2			Bug fixes
3.1.0	New features	Resolved vulnerabilities	Bug fixes
3.0.1	New features	Resolved vulnerabilities	Bug fixes
3.0	New features		Bug fixes

SMC 3.9.1 new features and enhancements

Object database

Using objects in groups

Groups can now contain the same object twice, if the object belongs to two separate sub-groups.

Such groups can be used in filter rules and translation rules.

Pagination of objects in groups

In the window where object groups, port groups and region groups can be added and edited, available objects and objects belonging to the group are now shown by page. With this enhancement, objects can be instantly displayed.

Managing SNS firewalls

Deleting firewalls in SMC

When a firewall or cluster is deleted in SMC, the operation will now automatically delete the configuration that connects these firewalls to SMC, on firewalls in version 4.8.14 and higher, and version 5.0.2 and higher. As a result, these firewalls will no longer attempt to connect to SMC after they have been deleted from the server. For this condition to apply, the firewalls have to be connected to SMC when they are deleted.

Deleting firewalls from SMC does not affect the firewall's global configuration.

Find out more

Updating SNS firewalls

As of SNS version 4.8.9, firewalls and clusters on which the TPM is initialized can be updated from SMC.

Find out more

Environment variables

SMC_IMPORT_RULES_FROM_SNS_TIMEOUT_INT variable

The new environment variable SMC_IMPORT_RULES_FROM_SNS_TIMEOUT_INT makes it possible to set the maximum time allowed for retrieving local and global rules from a firewall that is connected to SMC.

The default timeout is 600 seconds, and the minimum accepted value is 30 seconds.

SMC_BULK_RULES_OPERATIONS_TIMEOUT_INT variable

The new environment variable SMC_BULK_RULES_OPERATIONS_TIMEOUT_INT makes it possible to set the timeout after which copied/pasted or cut/pasted filter and translation rules expire.

The default timeout is 600 seconds, and the minimum accepted value is 30 seconds.

Description of environment variables in the *Administration guide*

A description, as well as the highest and lowest values where applicable, have been added for each environment variable in the section Details of SMC_XXX environment variables in the SMC *Administration guide*.

Routing configuration

BIRD dynamic routing

These three new tokens can be used in BIRD v1 and BIRD v2 configurations:

- rcvbuflen
- sndbuflen
- connect

Configuring virtual IPsec interfaces (VTIs)

SMC 3.9 supports the new **Destination IPv4 address** field on virtual IPsec interfaces. This field is available as of SNS version 5.1.0. The address must belong to the interface's address range.

The API route PUT /papi/v1/firewalls/{uuidOrName}/interfaces also supports this new field. When the field is used with SNS in a version lower than 5.1.0, an error will appear.

A new column, "ipv4_dst_address", can now be found in the *.csv* file used in the configuration of IPsec interfaces. SMC suggests downloading this file when you create a route-based topology that includes firewalls with network configurations that SMC does not manage. This feature shows an IP address for firewalls in version 5.1.0 and higher. For more information on the use of the file, refer to the section Configuring a route-based mesh topology in the *Administration guide*.

Refer to the Recommendations section prior to any update.

Configuring routes on firewalls that have never connected

SMC now makes it possible to configure routes in advance on an SNS firewall that has never connected to the server, by using the API route PUT /papi/v1/firewalls/{uuidOrName}/routes.

Routes that are created in this way can be seen in the SMC web administration interface, and are deployed during the firewall's initial connection.

VPN topologies

Optimized VPN tunnel monitoring

Efficiency and resource usage are now optimized during the retrieval and display of IPsec VPN tunnels.

Administrator authentication

Hardened password policy

A minimum entropy value can now be imposed to increase the strength of administration passwords that are set in SMC. The default value is 64 bits.

In addition, after an update to version 3.9, passwords have to meet the following default requirements:

- Minimum length of 16 characters,
- At least one alphanumeric character,
- At least one special character,
- Entropy of 64 bits.

These values can be configured in the password policy in **SMC server** > **Administrators**.

These hardening measures do not apply to passwords that are already in use, which will continue to function.

Find out more

Automatic switching between Radius and LDAP servers

When both LDAP and Radius are enabled for user authentication, SMC will verify accounts in the following order:

1. Radius server
2. LDAP server
3. Local accounts

Prior to SMC version 3.9, whenever the Radius server was unavailable, the account verification would automatically switch to the LDAP server, potentially creating a security vulnerability.

The automatic switch is now disabled by default. A new checkbox in the Radius settings allows the user to enable it.

WARNING
By enabling this option, during a switch, the security level of your authentication will be same level that you have set in your LDAP configuration.

However, during the update to version 3.9, the checkbox will be selected by default if both authentication methods had already been enabled.

Reading logs

Display of the SMC server name in *auth.log*

The name that is given to the SMC server now appears in the log *auth.log*. This file logs every operation that was performed to access the SMC server in SSH or console mode. The displayed name makes it easier to use filters in external log aggregators.

Find out more

System

Optimized usage checks

The feature that checks how various items (objects, certificates, interfaces, etc.) are used has been optimized. The optimization allows SMC to reduce its resource consumption and respond more quickly.

Public SMC API - New routes

New API routes were added to SMC version 3.9. They are listed below. For more information on the public SMC API routes, refer to the online documentation. This documentation is also available from the SMC web administration interface.

Automatic backups of the SMC configuration and SNS firewall configuration

A new API route is available in the public SMC API to download a backup of SMC and firewall configurations.

Route	Makes it possible to
POST /papi/v1/backup/download	Download the latest automatic backup of the SMC server configuration and firewall configuration. The downloaded file *latest-backup.tar.gz.enc* is protected by a password that must meet the requirements in the SMC user password policy. Use the following OpenSSL command to decrypt the file: `openssl enc -d -aes-256-cbc -pbkdf2 -iter 200000 -md sha256 -in latest-backup.tar.gz.enc -out latest-backup.tar.gz && tar -xzf latest-backup.tar.gz`

Managing object groups

Two new routes are available in the public SMC API to granularly manage members of object groups:

Route	Makes it possible to
POST /papi/v1/objects/groups/{uuidOrName}/members	Add one or several objects individually to a group.
DELETE /papi/v1/objects/groups/{uuidOrName}/members	Delete one or several objects individually from a group.

SMC 3.9.1 resolved vulnerabilities

The indicated severity is the level at the time of the initial publication of the security advisory on https://advisories.stormshield.eu/.

Node.js vulnerabilities

Two low severity vulnerabilities were fixed after the Node.js component was upgraded.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2026-008
- https://advisories.stormshield.eu/2026-009

OpenSSL vulnerabilities

High severity vulnerabilities were fixed after the OpenSSL component was upgraded.

Details on these vulnerabilities can be found on our website https://advisories.stormshield.eu/2026-004.

PostgreSQL vulnerabilities

Moderate severity vulnerabilities were fixed after the PostgreSQL component was upgraded.

Details on these vulnerabilities can be found on our website https://advisories.stormshield.eu/2026-005.

SMC 3.9.1 fixes

Filter and NAT rules

Support reference 85834

Moving rule separators

When a separator containing filter or translation rules is moved, the operation no longer causes an error or duplicates rules.

Support reference 86235

Adding and moving rules

In some cases, when new filter or translation rules were added, or when existing rules were copied and pasted or dragged and dropped, the rules in question were not inserted in the desired position in the rule sequence. This issue has been fixed.

Support reference 86188

Using port groups in rules

When a "Port group" object is used in a filter or translation rule, the rule behavior is now as follows:

- The consistency checker returns an error if none of the ports in the group uses the protocol that was selected in the rule's **Port - Protocol** menu, or if none of the ports is an "Any" port.
- The consistency checker returns an error if, for example, UDP was selected for all the ports in the group, but TCP was selected in the rule's **Port - Protocol** menu. The opposite case also applies.
- A rule can be deployed if a protocol is selected in the rule's **Port - Protocol** menu, and if at least one port in the group uses the protocol.

Support reference 86187

Copying a large set of rules

Very large sets of copied filter or translation rules are now better managed. The copying process is faster, and no longer causes errors.

When necessary, the new environment variable SMC_BULK_RULES_OPERATIONS_TIMEOUT_INT can be used to set a timeout after which copied rules expire. For more information, refer to the section Details of SMC_XXX environment variables.

Support reference 86320

Translation rules with an IP protocol

Translation rules in which a type of IP protocol has been selected can now be created and copied.

Active Update server

Support reference 86139

Active Update server certificate format

The format of the certificate that SMC generated for Active Update was not compatible with SNS 4.3.31 LTSB and higher versions of 4.3 QS, 4.8.7 and higher versions of 4.8 LTSB, and 5.0.0 and higher versions.

In order to use Active Update on SMC for all SNS versions, the certificate now contains the following extensions:

- subjectKeyIdentifier = hash
- basicConstraints = critical, CA:true
- keyUsage = critical, digitalSignature, keyCertSign, cRLSign

The Active Update certificate is automatically updated when SMC is updated to version 3.9, unless a customized certificate is used.

Object database

Support reference 85573

Importing objects

When objects fail to be imported through a CSV file, the error message now specifies the names of the firewalls that are causing the issue, instead of their UUIDs.

Support reference 86196

SMC updates canceled when duplicate objects exist

The presence of duplicate objects in the object database may cause errors when SMC is updated. When this occurs, updates will now be canceled, and server logs will report an error listing the objects in question. If the list contains more than 10 objects, the file *duplicate_objects.txt*, which lists all the objects, will be created in the folder var/log.

If you encounter this issue, begin by deleting duplicates and modifying the configuration, then start the server update process once again.

Administrator authentication

Support reference 86185

Authentication failure

When an administrator's authentication fails, an issue prevented the administrator from reconnecting immediately. This issue has been fixed.

Support reference 86169

LDAP users authenticated over a Radius server

SMC once again supports the authentication of users from an LDAP group over a Radius authentication server.

Support reference 86214

Accented characters and commas in the LDAP DN

LDAP user authentication now supports accented characters and commas in the LDAP DN.

System

Support reference 86177

SMC server redundancy

When the main node encounters an issue and the backup node takes over, configurations can once again be deployed from the backup node.

Support reference 86164

Saturation of the /tmp directory

Temporary files that are created in the /tmp directory after a configuration deployment will now be automatically deleted after the database is restored.

High availability

Support reference 84720

Display of firewall end of maintenance dates

When both nodes in a cluster have different end of maintenance dates, the dates now appear correctly after a switch.

Version 3.9.0 not published

Version 3.9.0 is not available to the public.

SMC 3.8.1 fixes

The certificate used to sign new updates of SMC server has been replaced in version 3.8.1. Its validity date has been extended. This certificate is used to check the integrity of the SMC update file.

Update files prior to version 3.8.1, containing the old expired certificate, no longer allow SMC to be updated.

There is no functional change between version 3.8.1 and version 3.8.0.

SMC 3.8 new features and enhancements

Managing SNS firewalls

Versions of managed firewalls

Firewalls in version 5 can now be managed from SMC version 3.8.

To know the highest versions that can be managed from a given version of SMC, refer to the Product life cycle guide.

Updating firewalls from SMC

Firewalls can now be updated directly from the SMC administration interface, and from the public API. Previously, updates could only be applied via SNS CLI script. Go to the new firewall update panel through the **Deployment** menu.

If a firewall is not connected when the update is launched, it will be postponed and launched the next time the firewall connects again.

Firewalls that use TPMs cannot be updated from this panel.

Find out more

SNS firewall configuration

Firewall configuration consistency check

If you permanently disable the consistency check using the `SMC_CFGCHECK_ENABLED` environment variable, a new **Run verification** button manually launches a configuration verification from the consistency checker only when requested.

Furthermore, when the consistency checker is disabled, automatic checks are still conducted every time a configuration is deployed. The new `SMC_CFGCHECK_BEFORE_DEPLOY_ENABLED` environment variable can be used to disable these automatic checks.

Find out more

New consistency checks

New consistency checks make it possible to ensure the proper use of KEM (Key Encapsulation Mechanism) encryption algorithms in SMC.

Disabling *Diffusion Restreinte* (DR) mode

From version 3.8 upwards:

- When DR mode is disabled on SMC, configurations are no longer deployed, and DR mode will be disabled on firewalls that are connected to SMC.
- Firewalls in DR mode can be connected to an SMC server on which DR mode is not enabled.

Find out more

VPN topologies

New encryption profiles

Two new encryption profiles are now available in the configuration of VPN topologies:

- PQCEncryption
- PQCTransition

They contain new key exchange algorithms that provide protection from "store now, decrypt later" attacks (Quantum-safe Key Encapsulation Mechanism (KEM)).

Post-quantum pre-shared keys

Post-quantum pre-shared keys (PPK) can now be configured in the settings of VPN topologies that use X.509 certificate authentication.

Find out more

Discontinuation of support for 3DES in encryption profiles

VPN topologies associated with an encryption profile that uses 3DES can no longer be deployed when a peer in the topology is in SNS version 5 and higher.

In addition, 3DES can no longer be selected in new encryption profiles.

Object database

Creating host and group objects from router objects

In the window to create and edit router objects, the following items can now be directly created:

- **Host** objects from the **Host** column in the **Gateways** and **Backup gateways** tab.
- **Host** or **Group** objects from the **Device(s) for testing availability** column in the **Gateways** and **Backup gateways** tab.

Using the @ character

The @ character can now be used in object comments.

Network configuration

Support for 50 and 100 Gbps full duplex media

In the advanced configuration of interfaces that support it, 50 and 100 Gbps full duplex media can now be selected for compatible firewall models.

System

Server diagnostics report

In the diagnostics report, a new section shows the serial numbers of firewalls that attempt to connect instead of another firewall that is connected with the same connecting package, for example.

Environment variables

SMC_MONITOR_ROUTE_POLLING_PERIOD_INT variable

With the new SMC_MONITOR_ROUTE_POLLING_PERIOD_INT environment variable, you can adjust the frequency with which a firewall is queried to monitor configured routes. The default value of

the variable is 60000 milliseconds, which is the lowest value. To disable the variable and stop querying, indicate 0 as a value.

SMC public API

New API routes were added to SMC version 3.8. They are listed below. For more information about the SMC public API routes, refer to the online documentation. This documentation is also available from the SMC web administration interface.

Updating SNS firewalls

Five new API routes are available in the SMC public API to update SNS firewalls.

Route	Makes it possible to
POST /papi/v1/sns-update/attachments	Attach one or several firewall update files.
POST /papi/v1/sns-update	Indicate the URL of an HTTPS server on which SMC can download the update files.
POST /papi/v1/sns-update/execute	Run an update on one or several firewalls that are connected to SMC. Firewalls that use TPMs cannot be updated via SMC.
GET /papi/v1/sns-update/progress	Track the progress of an ongoing update on one or several firewalls.
POST /papi/sns-update/cancel	Cancel a pending update.

Topologies and VPN tunnels

Two new API routes are available in the SMC public API to manage VPN topologies and tunnels:

Route	Makes it possible to
POST /papi/v1/vpn/topologies	Add a VPN topology.
DELETE /papi/v1/vpn/topologies/{uuidOrName}	Delete a VPN topology.

Firewalls

Two new API routes are available in the SMC public API to manage firewalls:

Route	Makes it possible to
PUT /papi/v1/firewalls/{uuidOrName}	Change a firewall's information.
DELETE /papi/v1/firewalls/{uuidOrName}	Remove a firewall from the SMC server

SMC 3.8 fixes

Authentication

Support reference 85506

LDAP ID format

The use of the `userPrincipalName` attribute in a name@domain format instead of the default `sAMAccountName` (Active Directory) or `uid` (OpenLDAP) attributes is now correctly supported in user authentication. The SMC_LDAP_FIELD_NAME_LOGIN environment variable in the file **/data/config/fwadmin-env.conf.local** makes it possible to select this attribute.

Support reference 85928

Accented characters in the LDAP DN

Users' LDAP DNs can now contain accented characters.

Filter and NAT rules

Support reference 85838

Displaying rules

The **Expand** button in filter and NAT rules now correctly expand the sections that are defined by rule separators.

Support reference 85858

Deploying filter rules

Filter rules that have a combination of the following characteristics are now correctly deployed:

- Configured with the **IDS** and **Firewall** inspection levels,
- The option **Synchronize this connection between firewalls (HA)** in the **Advanced properties** tab in the **Action** menu is disabled.

Support reference 86026

Editing a rule in a rule set

When a destination port is selected in a rule that belongs to a rule set, it no longer causes a validation error.

Support reference 86068

Changing the order in which rules are executed

Rules can now be correctly dragged and dropped to change their order in a filter policy that contains rules and rule sets, as this no longer disrupts the order of the rules.

Object database

Support reference 85877

Naming host and network objects

If a host object has a prefix Network_ before its name, or if a network object has a prefix Firewall_ before its name, the consistency checker will now show errors, preventing the configuration from being deployed.

Firewall configuration

Support reference 85830

Changes to the file *ConfigFiles/sshd-banner*

The configuration comparison no longer shows changes made to a firewall's *ConfigFiles/sshd-banner* file.

Support reference 86019

Fixes to the configuration comparison

The configuration comparison wrongly showed differences in the configuration of filter rules, even though they were identical on firewalls and on SMC, in the following cases:

- After deployment of a new filter rule,
- After redeployment of a rule that showed differences on a firewall.

This issue has been fixed.

System

Support reference 85909

SMC server redundancy

The syntax of the command allowing server redundancy to be enabled has been corrected. `--secundaryIP` has been replaced with `--secondary`. The command to use is now `smc-redundancy --secondary <BACKUP_NODE_IP>`.

Support reference 85881

Restoring the SMC server configuration

Now, when a backup of the server's configuration is restored from the web administration interface, the backup correctly overwrites and replaces all the data that was in the database.

Public API

Support reference 85905

Order in which rules returned by the API are executed

The order in which rules that are returned by the GET route /papi/v1/firewalls/{uuidOrName}/filter-policy and POST route /papi/v1/firewalls/{uuidOrName}/filter-policy/rules now correspond to the order of the same rules that are shown in the SMC administration interface.

SMC 3.7.1 new features and enhancements

Active Update server

Proxy server

You can now specify a proxy server to be contacted, which will act as a link between SMC and the Stormshield update server that hosts the Active Update databases.

Find out more

Firewall configuration

Additional SNS firewall configuration

The firewall configuration can now be completed or additionally loaded, by importing a CSV file containing configuration parameters for each firewall. This file is applied to configuration files that are generated by SMC when the configuration is deployed on firewalls. Changes that are made in this manner will be included in the configuration comparison.

Find out more

SMC public API

New API routes were added to SMC version 3.7. They are listed below. For more information about the SMC public API routes, refer to the online documentation. This documentation is also available from the SMC web administration interface.

Managing certificates

One new API route is available in the public SMC API to manage certificates:

Route	Makes it possible to
POST /papi/v1/firewalls/{uuidOrName}/certificates	Add a certificate on a firewall, even when the firewall is offline or has never connected. This certificate and its password are securely stored. They are automatically sent to the firewall the next time it connects, and are subsequently deleted from the SMC server.

Topologies and VPN tunnels

One new API route is available in the public SMC API to manage VPN topologies and tunnels:

Route	Makes it possible to
PUT /papi/v1/vpn/topologies/{uuidOrName}	Edit a VPN topology.

Static

One new API route is available in the public SMC API to manage routing:

Route	Makes it possible to
PUT /papi/v1/firewalls/{uuidOrName}/routes	Edit the static routing configuration on a firewall.

Interfaces

One new API route is available in the public SMC API to manage the interfaces of a firewall:

Route	Makes it possible to
PUT /papi/v1/firewalls/{uuidOrName}/interfaces	Add, change or delete firewall interfaces that are supported by SMC. With the API route, these operations can also be run on the interfaces on an offline firewall, which are supported by SMC.

Firewalls

One new API route is available in the public SMC API to manage firewalls:

Route	Makes it possible to
POST /papi/v1/firewalls	Create a firewall.

SMC 3.7.1 resolved vulnerabilities

The severity level mentioned is the level in effect when the advisory is first published on the https://advisories.stormshield.eu/ website.

Node.js vulnerability

A low severity vulnerability was fixed after the Body-parser and Express components were updated.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2024-32.

SMC 3.7.1 fixes

System

Support reference 85567

Memory saturation

When "Possible EventEmitter memory leak detected" and "Out of memory: Killed process 49106 (node)" logs appear in server logs, indicating that the memory is full, SMC will need to be restarted. SMC now restarts autonomously when this occurs.

Support reference 85985

Running crontab jobs

An issue that occurred in version 3.7.0 prevented the "root" user from running crontab jobs. This issue has been fixed. Other SMC users who hold SSH access privileges are now no longer able to run crontab jobs.

Managing administrators

Support reference 85998

Connecting to the SMC web administration interface

An error in the propagation of configuration data to the database in version 3.6 would prevent connections to the web administration interface. The SQL error log in the *postgres.log* file indicated the following message: "ERROR: insert or update on table "account_folder" violates foreign key constraint "fk_account_uuid"". This issue has been fixed.

VPN topologies

Support reference 85950

Changing peers in VPN topologies

Adding or deleting peers in a route-based topology no longer changes the order of the IPsec interfaces on SNS firewalls that are part of the topology.

Support reference 85482

Unknown tunnel statuses

VPN tunnel monitoring and the indication of their status now function properly.

Network configuration

Support reference 85743

Interface port numbers

The physical port number of interfaces that SMC displays is now consistent with the number shown by SNS firewalls.

Firewall monitoring

Support reference 85778

Direct access to the SNS firewall monitoring interface

The button **Connect to the reporting application of this firewall** makes it possible to directly access the firewall's monitoring interface once again.

Object database

Support references 85996 and 85997

Automatic deletion of duplicate host objects

In version 3.6 and lower, if an object database contained strictly identical host objects, it could not be updated to SMC version 3.7.0, which imposed the condition of unique object names. The update to version 3.7.1 fixes the issue by automatically deleting duplicate host objects from the object database when they exist. The update process may take longer, depending on the number of duplicate objects found in the database.

Support reference 85817

Using IP protocol objects

IP protocol objects that were created in SMC can now be used in the **Port/Protocol** menu in filter rules.

If you had configured the forced deployment of the following IP protocol objects, after the update to version 3.7, the forced deployment will be lifted:

- gre
- icmp
- icmpv6
- igmp
- stcp
- tcp
- udp
- vpn-ah
- vpn-esp

Authorities and certificates

Support reference 85855

Importing ED25519 certificates

Certificates with a KeySize field that does not contain any value can now be imported again into SMC.

Support reference 86016

Displaying revoked certificates

When SMC is used as a CRL distribution point, the list of revoked certificates will now be correctly retrieved when a CRL is imported. It will be updated in the **SMC** tab **as the CRL distribution point** of a certification authority. This regression appeared in SMC version 3.6.

Deploying configurations

Support reference 84587

Detecting local changes during deployment

The tracking of local changes to a firewall's configuration is now disabled during the deployment of the configuration, thereby preventing critical errors from being randomly reported.

Filter and NAT rules

Support reference 85760

Editing a rule in a rule set

When a rule in a rule set is being edited, adding a single destination port into the rule no longer prevents changes from being applied.

Environment variables

Support reference 85814

Keeping the connection between SMC and SNS firewalls

When the default value of the environment variable SMC_FW_CONNECTION_TIMEOUT_INT is loaded in addition, it is now correctly applied.

SMC 3.6 new features and enhancements

Managing administrators

Restricting administrators' access privileges

The SMC super administrator can now restrict administrators' write access privileges to only certain folders, and therefore to only certain firewalls. With this feature, you can strengthen security on your firewall pool by segmenting its administration. In this way, individual administrators manage their own SNS firewalls, while retaining read-only access to other firewalls connected to SMC.

This restriction can be configured in administrators' profiles.

Find out more

Firewall configuration

Implementing QoS

You can now configure QoS (Quality of Service) on your SNS firewall pool from SMC.

In the new **Configuration** > **Quality of Service** menu, you can add queues and traffic shapers. A new **QoS** tab in the firewall settings then allows you to associate them with network interfaces on firewalls. You can also select queues that were created on SMC in filter rules.

SMC also allows you to retrieve the QoS configuration, if it already exists on your firewalls.

The implementation of QoS in SMC is compatible with SNS firewalls from version 4.3.15 LTSB and 4.5.3 upwards.

Find out more

Dynamic routing with BIRD version 2

SMC 3.6 allows you to configure and deploy dynamic routing that uses version 2 of BIRD on SNS firewalls in version 4.8.1 EA and upwards. Version 1 of BIRD can still be used in SMC.

Do note that dynamic routing can no longer be managed on SNS firewalls in 4.8.1 EA versions and higher from a version of SMC below 3.6. The firewall will reject the deployment of the configuration, and report an error.

We advise you to read the following recommendation on updating SMC to version 3.6, and updating SNS firewalls to version 4.8.1 EA.

Find out more

Firewall network interfaces

Broadcast mode is now available in SMC for aggregate interfaces. This mode is compatible with SNS firewalls in versions 4.3.25, 4.7.5, 4.8.1 and higher.

Please refer to the SNS release notes for more information.

Find out more

Environment variables

SMC_PROXY_RESPONSE_TIMEOUT variable

The default value of the SMC_PROXY_RESPONSE_TIMEOUT variable has been increased from 120 seconds to 300 seconds. As some commands that SMC sends to SNS firewalls require more than 120 seconds to run, the higher value prevents them from failing.

Find out more

VPN topologies

Using Diffie-Hellman groups in encryption profiles

On firewalls in version 4.8 and upwards, several Diffie-Hellman (DH) key exchange methods can now be configured in encryption profiles for IKE and IPsec proposals.

The SMC public API has been updated as a result, through routes on topologies. The "proposals" field now contains an additional detail named "dh". The "pfs" field is now a table, so that several values can be returned.

Obsolescence of Diffie-Hellman groups

The following DH groups are now obsolete in SMC, and on SNS firewalls. They now appear in encryption profiles with the caption 'obsolete'.

- DH25 (ECDH with 192-bit NIST ECG)
- DH26 (ECDH with 224-bit NIST ECG)
- DH27 (ECDH with 224-bit Brainpool ECG)

SMC documentation

Access to documentation

In the SMC web administration interface, the link to documentation now leads to the Technical documentation website. This will provide you with all documentation on the latest version of the product.

To use SMC in offline mode, you can download PDF and HTML versions of documents on the website.

SMC public API

New API routes were added to SMC version 3.6. They are listed below. For more information about the SMC public API routes, refer to the online documentation. This documentation is also available from the SMC web administration interface.

Customizing the port of the public API

Th default listening port on the SMC public API can now be changed by using the environment variable SMC_PUBLIC_API_PORT_INT.

Find out more

Variables

Six new API routes are available in the public SMC API to manage the global variables and values that have been assigned to them for each firewall:

Route	Makes it possible to
GET /papi/v1/variables	Lists all global variables and values assigned for each firewall.
POST /papi/v1/variables	Adds a global variable.
GET /papi/v1/variables/{uuidOrName}/uses	Lists the uses of a global variable in objects.
DELETE /papi/v1/variables/{uuidOrName}	Deletes a global variable.
PUT /papi/v1/variables/{uuidOrName}	Edits a global variable.
PUT /papi/v1/variables/{variableUuidOrName}/{firewallUuidOrName}	Assigns or modifies the value of a global variable on a firewall.

Managing certificates

Four new API routes are available in the public SMC API to manage certificates:

Route	Makes it possible to
GET /certificates	Lists certificates that have been imported on all firewalls and their respective properties.
GET /certificates/{uuid}	Lists the properties of a certificate that was imported on a firewall.
GET /certificates/authorities	Lists all certification authorities and their respective properties.
GET /certificates/authorities/{uuid}	Lists the properties of a certification authority.

Interfaces

One new API route is available in the public SMC API to list the interfaces of a firewall:

Route	Makes it possible to
GET /firewalls/{uuidOrName}/interfaces	Lists all interfaces on a firewall and their respective properties.

Static

One new API route is available in the public SMC API to list routes:

Route	Makes it possible to
GET /firewalls/{uuidOrName}/routes	Lists all routes on a firewall and their respective properties.

QoS

15 new API routes are available in the public SMC API to manage the QoS configuration:

Route	Makes it possible to
GET /qos/queues/	Lists all queues added on SMC and their respective properties.

GET /qos/queues/{uuidOrName}	Lists the properties of a queue.
POST /qos/queues	Adds a queue.
PUT /qos/queues/{uuidOrName}	Edits a queue.
DELETE /qos/queues/{uuidOrName}	Deletes a queue.
GET /qos/traffic-shapers	Lists all traffic shapers added on SMC and their respective properties.
GET /qos/traffic-shapers/{uuidOrName}	Lists the properties of a traffic shaper.
POST /qos/traffic-shapers	Adds a traffic shaper.
PUT /qos/traffic-shapers/{uuidOrName}	Edits a traffic shaper.
DELETE /qos/traffic-shapers/{uuidOrName}	Deletes a traffic shaper.
GET/firewalls/{uuidOrName}/interfaces-with-qos	Lists all the interfaces on a firewall with which QoS data has been associated.
GET/firewalls/{uuidOrName}/interfaces-with-qos/{ifaceUuidOrName}	Lists QoS data associated with a specific interface on a firewall.
POST /firewalls/{uuidOrName}/interfaces-with-qos/{ifaceUuidOrName}	Associates a traffic shaper and queues with a network interface.
PUT /firewalls/{uuidOrName}/interfaces-with-qos/{ifaceUuidOrName}	Edits the QoS configuration on a network interface.
DELETE /firewalls/{uuidOrName}/interfaces-with-qos/{ifaceUuidOrName}	Deletes the QoS configuration on a network interface.

Filter and NAT rules

Seven new API routes are available in the public SMC API to manage filter and NAT rules individually for firewalls and folders:

Route	Makes it possible to
DELETE /rules/{uuid}	Deletes a filter rule, translation rule or separator.
POST /firewalls/{uuidOrName}/filter-policy/rules	Adds a filter rule on a firewall by selecting its position.
POST /firewalls/{uuidOrName}/nat-policy/rules	Adds a translation rule on a firewall by selecting its position.
POST /folders/{uuidOrName}/filter-policy/rules	Adds a filter rule in a folder by selecting its position.
POST /folders/{uuidOrName}/nat-policy/rules	Adds a translation rule in a folder by selecting its position.
PUT /filter-policy/rules/{uuid}	Edits a filter rule.
PUT /nat-policy/rules/{uuid}	Edits a translation rule.

Resolved vulnerabilities for SMC 3.6

OpenSSL vulnerabilities

Medium severity vulnerabilities were fixed after the OpenSSL component was upgraded.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2023-036
- https://advisories.stormshield.eu/2024-022
- https://advisories.stormshield.eu/2024-023

OpenSSH vulnerability

Terrapin attack vulnerability

A medium severity Terrapin attack vulnerability was fixed after the OpenSSH component was upgraded. The various encryption algorithms that were affected and used by SMC were removed.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2024-01.

SMC 3.6 fixes

System

Robustness

The system has been enhanced in order to limit the risk of the server unexpectedly shutting down or suddenly disconnecting. Now SMC is both more robust and more reliable.

VPN topologies

Support reference 84974

Using "Any" remote site

"Any" remote site can now be used in several VPN topologies, through the contact address during the selection of peer traffic endpoints, without causing the configuration deployment to fail.

Support reference 85685

In a route-based VPN topology, using the “Any” contact address for several peers no longer causes the configuration deployment to fail.

Support reference 85502

Displaying the Local address column

In step 4 when configuring a VPN topology, the **Outgoing interface** column has been renamed **Local address**.

Support reference 85696

VTI network pool

In step 2 when configuring a VPN topology, changes to the default VTI network pool are now correctly applied if the new sub-network entered belongs to the private IP address ranges:

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

Reading logs

Support reference 85429

Deleting logs

Every time SMC starts or restarts, the following log would appear:

```
psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed
```

This log was a false negative that had no impact on the operation of SMC, and has since been removed.

Direct access to SNS firewalls from SMC

Support reference 85375

Accessing the SD-WAN monitoring view

The SD-WAN monitoring view on firewalls in version 4.3.23 or 4.3.24 can now be accessed by connecting directly to the firewall from SMC.

Support reference 85158

Installing a connecting package

Administrators can now install connecting packages on a firewall by connecting directly to the firewall from SMC, without being logged out from SMC.

Authorities and certificates

Support reference 85304

Importing certificates in command line

Certificates can now be updated using the command `smc-install-certificate` with the `-u` option.

Firewall configuration

Support reference 85554

Using customized variables

All custom variables that use the former %FW_CUSTOMX% format are now correctly converted to the new %CUSTOM_varX% format, even when the variables are written in lowercase, e.g., %FW_customX%. The former format therefore can no longer be used.

Support reference 85550

Using the consistency check

The consistency check no longer reports false anomalies, notably with regard to the overlap of IP addresses.

Support reference 85331

Using environment variables to configure timeout periods

The following environment variables are no longer available:

- SMC_HASYNC_TIMEOUT_INT
- SMC_LICENSEDUMP_TIMEOUT_INT
- SMC_POLLING_TIMEOUT_INT

They have been replaced with the variable SMC_PROXY_RESPONSE_TIMEOUT_INT. It allows configuring the maximum time to wait for a response from an SNS firewall for four requests initiated by SMC:

- Synchronizing both nodes of a cluster,
- Retrieving firewall license information: options and validity dates,
- Retrieving firewall monitoring information,
- Connecting to the firewall administration interface.

The default value of the variable is 300 seconds.

Object database

Support reference 85560

Managing time objects

Dates associated with a time object now match the dates that you have entered when creating or editing the object. Previously, there was a lag, which caused issues when the object was used in rules that filter traffic over a given period, for example.

Support reference 85344

Deleting a group that is used in a router object

Groups can no longer be deleted from the object database if they belong to a router object.

Port range in a Port object

Support reference 85478

When creating a Port object, the automatic verification of the “From” field now correctly works.

Filter and NAT rules

Support reference 85255

Displaying local rules in SMC

When local filter rules on SNS firewalls contain global objects in their configurations, they now appear correctly in SMC, even when the deployment of these global objects is forced on the firewalls.

Support reference 85654

Importing local rules

During failed attempts to import a firewall's local filter rules into SMC, an error message now indicates the reasons for the failure.

Support reference 85484

Choosing options in filter rules

Filter rules that contain the following configuration no longer cause the configuration deployment to fail:

- The options **Force source packets in IPsec** and **Force return packets in IPsec** have been selected in the advanced properties of the **Action** menu,
- The options **Syslog server** and **IPFIX collector** have been unselected in the advanced properties of the **Action** menu,
- The option **Via IPsec VPN tunnel** has been selected in the advanced properties of the **Source** menu.

Active Update server

Support reference 85565

Active Update server certificate

If you are using the SMC Active Update server, you can now replace the default server certificate with a certificate of your choice without causing errors.

Monitoring SMC with SNMP

Support reference 85561

Restarting the SNMP service

The SNMP service now correctly restarts with the `nrestart snmpd` command.

Managing SNS firewalls

Support reference 85389

Using custom variables with firewalls in versions below 3.7

The former custom variable format used on SNS firewalls in versions below 3.7 would cause SMC to shut down. As of SMC version 3.6, SNS firewalls in versions lower than 3.7 can no longer connect to SMC.

Support reference 85549

Monitoring memory use

On the SNS firewall monitoring screen, the graph in the **Memory (%)** column functions once again, and accurately indicates the amount of memory used on firewalls.

Configuring SMC

Support reference 85400

Adding interfaces

Interfaces can now be added to the SMC server without the need to configure a DNS server.

SMC 3.5.4 fixes

Network configuration

Support reference 85571

Creating interfaces in SMC

When users attempted to create a new interface for an SNS firewall in SMC with the same name as an existing interface, the existing interface would be deleted when the list of interfaces was expanded in the **Interfaces** tab in the firewall's settings. Interfaces with the same name can no longer be created, and the existing interface is no longer deleted.

Support reference 85454

Retrieving blackhole interfaces

When a blackhole interface of any type exists in the local configuration of an SNS firewall that is attached to SMC, SMC can now correctly retrieve it and display it in the firewall's settings. Previously, retrieving such interfaces would cause configuration deployments to fail.

Routing configuration

Support reference 85406

Retrieving interfaces and routes of an SNS cluster in SMC

Interfaces and routes of an SNS firewall cluster configured in high availability, in which the HA link is provided by a VLAN interface, are now correctly retrieved.

Configuration deployment

Support references 85188, 85419 and 85463

Deploying reserved objects and managing interfaces

When a configuration is deployed from SMC to SNS firewalls that have interfaces that SMC does not support (displayed as **Other interface**), the deployment no longer fails when Firewall_<interface-name> or Network_<interface-name> objects are used in filter and translation rules, or in static or return routes.

If the interface mentioned in the object is not known to SMC, the consistency checker will display a warning.

SMC 3.5.3 new features and enhancements

System

SMC server redundancy

You can now set up a redundancy system between two SMC servers, which makes it possible to guarantee service continuity. When the main node fails, SNS firewalls automatically connect to the backup node. The configuration on both nodes is synchronized every hour.

Find out more

Changes to system folders

Files saved in the folder */var/tmp* have been moved to */data/tmp*.

The folder */var/fwadmin* has been deleted and its files have been moved to */data/fwadmin*.

The symbolic link between the folders */var/tmp* and */data/tmp* has been deleted. Files saved in */var/tmp* will no longer be kept from one update to another.

SMC server diagnostics report

The server's diagnostics report contains a new section that provides statistics on the size of your configurations in SMC: number of firewalls managed, number of rules, routes, interfaces, etc. With these statistics, performance issues can be more easily diagnosed.

MAC-then-Encrypt mechanisms

For security reasons, MAC-then-Encrypt mechanisms have been removed from the SMC server.

Configuring SNS firewalls

Warning when firewall configuration is modified

This new feature is disabled by default. When it is enabled, a warning now appears when the configuration is deployed on SNS firewalls, if other administrators have made changes to the configuration since the last deployment. The administrator can then choose whether to continue with the deployment or cancel it.

Find out more

Network configuration

Blackhole keyword

From SNS firewalls in these versions onwards:

- 4.3.21 LTSB and higher 4.3 LTSB versions,
- 4.7 and upwards,

You can now select the blackhole keyword as the gateway of the default route or of a static route that aims to destroy a specific traffic stream.

Among other uses, this mechanism can be used in a configuration that contains IPsec tunnels - when a tunnel is down, packets that were meant for it will therefore be destroyed instead of being redirected to the firewall's default gateway.

Microsoft Windows compatibility

Windows Server 2022 support

SMC is now compatible with Microsoft Hyper-V for Windows Server 2022 hypervisors with regard to installation. It is also compatible with LDAP and Radius servers on Windows Server 2022 with regard to user authentication.

Authentication

Protection from brute force attacks

When administrators connect to the SMC command line interface via their SSH accounts or the SSH root account, the connection will now be suspended for 15 minutes after five consecutive authentication errors.

Configuring a Radius server

Support reference 85187

The values of the attributes NAS-IP-Address and NAS-IP-Identifier, used in Radius requests, can now be configured with the environment variables:

- SMC_RADIUS_NAS_IP_ADDRESS
- SMC_RADIUS_NAS_IDENTIFIER

SMC public API

Topologies and VPN tunnels

Three new API routes are available in the public SMC API to manage VPN topologies and tunnels:

Route	Makes it possible to
GET /papi/v1/vpn/topologies	List all the VPN topologies configured in SMC, regardless of whether they are deployed. The route indicates all configuration components, such as the name of the topology, authentication method, the name and content of the encryption profile, peers, etc. With the route, topologies can also be filtered by name or IKE version used. The "name" field enables partial case-insensitive searches.
GET /papi/v1/vpn/topologies/{uuid}	List all the configuration components of a specific VPN topology configured in SMC, regardless of whether it is deployed.
GET /papi/v1/vpn/tunnels	List all the VPN tunnels deployed in SMC. The route indicates all the monitoring properties of a VPN tunnel, such as the name of the topology, the status of the tunnel, traffic endpoints, etc. With the route, tunnels can also be filtered by topology name, type, form or status. The "topologyName" field enables partial case-insensitive searches.

Configuration deployment

Two new API routes are available in the public SMC API to manage configurations deployed:

Route	Makes it possible to

POST /papi/v1/deployment	Deploy the configuration on the firewalls.
GET /papi/v1/deployment	Find out the status of the current deployment or last deployment.

Filter and NAT rules

Eight new API routes are available in the public SMC API to manage the filter and NAT rules that are specific to a firewall or shared by several firewalls:

Route	Makes it possible to
GET /papi/v1/folders/{uuidOrName}/filter-policy	List all the filter rules found in a folder. Only rules contained in the folder are indicated, not rules in the parent folder or in sub-folders. Rules are sorted by priority (high or low).
GET /papi/v1/folders/{uuidOrName}/nat-policy	List all the NAT rules found in a folder. Only rules contained in the folder are indicated, not rules in the parent folder or in sub-folders. Rules are sorted by priority (high or low).
PUT /papi/v1/folders/{uuidOrName}/filter-policy	Edit the filter rules found in a folder.
PUT /papi/v1/folders/{uuidOrName}/nat-policy	Edit NAT rules found in a folder.
PUT /papi/v1/firewalls/{uuidOrName}/filter-policy	Define filter rules for a specific firewall.
PUT /papi/v1/firewalls/{uuidOrName}/nat-policy	Define NAT rules for a specific firewall.
GET /papi/v1/firewalls/{uuidOrName}/filter-policy	List filter rules for a specific firewall. Only the rules that are specific to the firewall are listed, not rules found in the folder to which the firewall belongs.
GET /papi/v1/firewalls/{uuidOrName}/nat-policy	List NAT rules for a specific firewall. Only the rules that are specific to the firewall are listed, not rules found in the folder to which the firewall belongs.

Folders

One new API route is available in the public SMC API to manage folders:

Route	Makes it possible to
GET /papi/v1/folders	List all folders found in SMC, and for each folder, its name, UUID and the firewalls that it contains.

Object database

27 new API routes are available in the public SMC API to manage the object database:

Route	Makes it possible to
GET /papi/v1/objects	List all objects found in the SMC object database.

POST /papi/v1/objects/[*object type*]	Add host, group, network, port, DNS name, time, router, SLA, IP protocol, address range, port group and geolocation objects. For example: POST /papi/v1/objects/hosts
PUT /papi/v1/objects/[*object type*]/{uuidOrName}	Edit host, group, network, port, DNS name, time, router, SLA, IP protocol, address range, port group and geolocation objects. For example: PUT /papi/v1/objects/hosts/{uuidOrName}
DELETE /papi/v1/objects/{type}/{name} DELETE /papi/v1/objects/{uuid}	Delete objects from the SMC object database based on their names UUIDs.

SMC 3.5.3 fixes

SMC update

Support reference 85420

Configuration of translation rules

When translation rules are imported from a CSV file, the "random" value can no longer be used in the "nat_from_port_load_balancing" field if the "nat_from_port" field is empty.

If you have imported translation rules with this configuration, updating your firewall to version 3.5.3 will fix this inconsistency. If nothing was entered in the "nat_from_port" field, the value of the "nat_from_port_load_balancing" will automatically be cleared.

Special characters "<", ">" and "@"

The presence of the characters "<" and ">" in the descriptions or comments of filter and NAT rules, separators and objects no longer causes SMC updates to version 3.5.x to fail. However, during the update to version 3.5.3, these characters will be deleted and the rest of the description or comment will be kept.

Likewise, the "@" character is now supported once again in the descriptions of rules and rule separators.

Active Update server

Support reference 85414

When the Active Update server feature was enabled on SMC, the two following issues could occur, and have been fixed:

- SMC would become unreachable when it could not connect to Stormshield update servers to download databases. When there are connection issues now, SMC remains accessible and an error will be reported in the server's logs.
- When the Active Update server feature was disabled, the automatic update of databases would continue. The automatic update is now disabled.

Network configuration

Changes to the dynamic routing configuration on the SNS firewall

Support reference 85427

You can now directly access the interface of an SNS firewall from SMC and change its dynamic routing configuration without making SMC unavailable in some cases.

Object database

Object database export

Support reference 85367

The object database can be exported once again to CSV files.

Filter and NAT rules

Importing the global rules of an SNS firewall

Support reference 85144

When a firewall's global rules are imported in SMC, if one of the rules uses an object containing a custom variable, the value of the firewall's variable no longer overwrites the value in SMC.

Rules applying to web services

Support reference 85251

When filter rules that apply to web services are imported via a CSV file, if some web services are not known to SMC, an error will now be generated for each web service that SMC does not recognize.

Synchronizing the connection in an HA cluster

Support reference 84975

In the **Action** menu of a filter rule, under the **Advanced properties** tab, the option **Synchronize this connection between firewalls (HA)** can now be unselected.

Importing the rules from a firewall into SMC

Support reference 84919

When the local rules of an SMC firewall are imported into SNS, the import would fail when a host object on the firewall and a DNS name (FQDN) object in SMC have the same name. Such rules can now be imported without overwriting the DNS name object.

Renaming of application protocols dcerpc and steam

Support reference 85307

The protocols dcerpc and steam, available in filter and NAT rules, have been renamed dcerpc_tcp and steam_udp to make them compatible with the naming system of such protocols on SNS firewalls.

Size of QoS Queue and QoS ACK Queue fields

Support reference 84935

The maximum size of the QoS Queue and QoS ACK Queue fields has been raised from 9 to 31 characters.

Do note that this change takes effect on firewalls from SNSversion 4.3.0 onwards. The deployment of a configuration on a firewall in a version lower than 4.3.0 will fail if the value of the QoS Queue and QoS ACK Queue fields exceeds 9 characters.

Custom variables in filter rules

Support reference 84616

The "%" character can no longer be used in the **Group name** and **Domain name** fields in a filter rule's **Source** menu. Custom variables are therefore no longer supported in these fields.

Configuring SNS firewalls

Importing SNS firewalls via a CSV file

Support reference 85093

When firewalls are imported via a CSV file from the SMC web administration interface, and when the **Generate connecting packages** checkbox is selected, the files required to generate packages may randomly become corrupted during the import. Connecting packages are now correctly generated when firewalls are imported via a CSV file.

Deploying VPN topologies

Support reference 85016

When a VPN topology that is based on X.509 certificate authentication is deployed, and if the **Local IP address for CRL verification** field is entered, this IP address is now correctly deployed on SNS firewalls that belong to the topology.

Direct access to a firewall interface

Support reference 83550

When you directly access a firewall's interface via SMC, the last page visited will be shown. If you access the interface for the first time, the main page of the firewall's administration interface will now appear. Previously, the last page visited on another firewall would be shown.

Version 3.5.2 not published

Version 3.5.2 is not available to the public.

Version 3.5.1 not published

Version 3.5.1 is not available to the public.

Version 3.5.0 not published

Version 3.5.0 is not available to the public.

Resolved vulnerabilities for SMC 3.4.3

Authentication

Connecting to SMC

A high severity vulnerability regarding the authentication to the SMC server was fixed.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-030.

We strongly recommend you update your SMC version.

SMC 3.4.2 fixes

Network configuration

Update of the SNS firewalls virtual IPsec interfaces

Support reference 85227

After updating SMC, if there are route-based VPN topologies in your configuration and if the network configuration is managed by SMC, SMC is now able to retrieve correctly the details about the virtual IPsec interfaces of the SNS firewalls. An issue retrieving interfaces details had been detected in version 3.4.1.

SMC 3.4.1 fixes

Network configuration

Order of the SNS firewalls interfaces

Support references 85148 and 84475

When the firewalls network configuration is managed by SMC, deploying the configuration from SMC can no longer modify the order of the interfaces as it was defined previously on the firewalls, whatever the type of the interface.

OpenSSL

TLS settings

The compliance of TLS settings has been updated according to the French ANSSI recommendations.

SMC 3.4 new features and enhancements

SMC public API

New public REST API

Your orchestration solutions can now communicate with SMC via a standard REST API. Via this API, you can now:

- obtain monitoring information about SNS firewalls connected to SMC,
- run scripts on SNS firewalls connected to SMC to perform all types of operations.

The use of 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.

The SMC super administrator can disable the public API at any time. Acces to this API is disabled by default.

For easier use of the API, OpenAPI documentation is provided on the Stormshield technical documentation website as well as in SMC itself.

Find out more

Network configuration

Creating and managing IPsec virtual tunnel interfaces (VTI)

You can now create and manage virtual IPsec interfaces in SMC, from the **IPsec interfaces (VTI)** tab in an SNS firewall's settings. The firewall must be in at least version 4.2.3. These interfaces can then be used in the routing configuration.

Find out more

Automatic VTI creation

When you create a route-based VPN topology, the required virtual IPsec interfaces will now be automatically created in SMC for every firewall in the topology that has its network configuration managed by SMC. These interfaces can be seen in the **IPsec interfaces (VTI)** tab, and are classified by the VPN topology to which they belong.

On firewalls for which SMC does not manage the network configuration, you must continue to create the interfaces manually on the firewall itself.

Using SNS firewall interfaces

In filter and translation rules, the known interfaces of an SNS firewall that has already connected to SMC can now be selected.

However, this operation cannot be performed in folders and rule sets.

Checking the consistency of routes

A warning used to be raised by the consistency checker when an object was set as the gateway of a static route or return route, but did not belong to the interface address range used in this route. This warning has been removed as it could mislead the user when SMC does not know the address range of the interface used.

Filter and NAT rules

Filtering by web service

SMC now makes it possible to create web service filter rules. The list of web services can be found in the **General** tab of a filter rule's **Source** and **Destination** menus. This list has been grouped with the IP reputations list.

The file */data/config/smc-ip-reputation.local* has been renamed */data/config/smc-webservices.local*. During the update to SMC version 3.4, data found in this file will be kept.

However, the following IP reputations have been migrated to web services:

IP reputations	Web services
office365	o365common
skypeforbusiness	o365skype
exchangeonline	o365exchange
sharepointonline	o365sharepoint

The IP reputations microsoftauth and officeonline have been removed.

Find out more

VPN topologies

Improvements to the *.csv* configuration file for IPsec interfaces.

The *.csv* configuration file for IPsec interfaces, suggested for download after the creation of a route-based VPN topology, contains new information. It now indicates the name of the Host object representing the virtual IPsec interface found on the remote firewall and its IP address. With this information, return routes can be created automatically with an SNS CLI script.

System

Keeping the connection between SMC and SNS firewalls

The keepalive mechanism that maintains the connection between SMC and SNS firewalls is now the same for all firewalls. It can be configured on the SMC side using the environment variable `SMC_FW_CONNECTION_TIMEOUT_INT`. The default value is 60 seconds. On the SNS side, SMC no longer recognizes the `PingValidity` token.

Environment variables

Environment variables renamed in SMC_XXX format

The FWADMIN_XXX environment variables used in version 3.3.3 and earlier versions for the configuration of the SMC server have been replaced with SMC_XXX variables. Older variables will continue to be available and operational but will be removed in future versions.

To find out the new versions of variables, refer to the Administration guide.

The environment variables `FWADMIN_SERVICES_NUM_INSTANCES_CFGCHECK` and `FWADMIN_SERVICES_NUM_INSTANCES_CFG2INI` are no longer recognized.

SMC 3.4 fixes

Managing administrators

Disabling local authentication

Support reference 84575

The super administrator can once again disable local authentication mode for an administrator, by unselecting the option **This administrator can use local authentication** in the administrator's settings.

Translation rules

Importing and exporting translation rules

Support reference 84525

In the CSV file to import/export files, SMC now correctly applies the column *nat_from_port_load_balancing*, corresponding to the option **Choose random translated source port** in the **Translated source** tab. Previously, when rules were imported, SMC would ignore the column, and when rules were exported, the column did not appear in the CSV file.

When importing rules, the *random* value must be indicated in the *nat_from_port_load_balancing* column in order for SMC to apply it.

VPN topologies

Local changes on the firewall

Support reference 84401

In the SNS firewall monitoring view, the warning icon  indicates, among other things, that changes were made locally on the firewall. When a VPN topology deployed from SMC was disabled locally on the firewall, the icon would indicate the local change. However, it would persist when the VPN topology was enabled again later from the firewall. The warning icon now no longer appears when local changes are canceled.

SMC update

Checking the license

Support reference 84464

When SMC is updated, the validity of the server's license is now checked at the beginning of the update process. This makes it possible to immediately show an error message if the license is missing or expired, and shut down the process immediately.

SNS CLI scripts

Adding attachments

Support reference 84372

In the SNS CLI script window, firewalls on which a script was to be run could not be selected when too many attachments were added. You can now add as many attachments as necessary, then select the firewalls.

Routing configuration

Using a router object as the gateway of a static route

Support reference 84883

Routes are now correctly displayed in the **Routing** tab in read-only mode when a ping to the gateway of a router object directs to a different machine on the gateway (**Device(s) for testing availability** column in the **Gateway** tab in the router object).

Showing routes that use server objects

Support reference 84905

Routes configured on an SNS firewall that use server objects are now correctly displayed in SMC in the **Routing** tab.

System

Deleting an error in console mode

Support reference 84290

On an SMC server in console mode, the error message "Unknown ioctl 1976" would appear every minute in the server's logs. Although this error had no impact on the operation of SMC, it has been removed.

Removal of log from *connections.log*

Support reference 84697

The log "Possible EventEmitter memory leak detected", which appeared regularly in the log *connections.log,* has been deleted. It had no impact on the operation of SMC.

Server diagnostics report

Support reference 85060

Since version 3.3.3, it was no longer possible to generate the diagnostics report of the SMC server from the web interface and from the command line interface. This issue has been fixed.

SMC 3.3.3 new features and enhancements

Authentication

Protection from brute force attacks

When an administrator connects to SMC via the web interface, the connection is now temporarily blocked after several unsuccessful authentication attempts.

Find out more

Authorities and certificates

Certificate security

For security reasons, users who have access to SMC via the console of their hypervisor or in SSH, can no longer read the certificate used to sign connecting packages and deployment files.

Only the "root" user can do so now.

Signing connecting packages and deployment files

The certificate used to sign connecting packages and configuration deployment files has been updated to use a more recent and more secure algorithm.

Configuration backup

Backups

Now, only the super administrator ("admin" user) can back up the configuration of the SMC server.

Securing configuration backups

Backups of the SMC server's configuration can now be encrypted with a password. The password must comply with the password policy set for administrators.

Find out more

System

HSTS header

The SMC server now supports the HSTS security header.

Resolved vulnerabilities for SMC 3.3.3

OpenSSH vulnerability

SSH connection
A high severity vulnerability was fixed after the configuration of the OpenSSH component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-06.

OpenSSL vulnerabilities

Two medium severity vulnerabilities were fixed after the OpenSSL component was upgraded in version 3.0.8 and the Node.js component was upgraded in version 16.19.1.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2023-015
- https://advisories.stormshield.eu/2023-016

SMC 3.3.3 fixes

System

Time required to start SMC

Support reference 84950

Since version 3.3.0 of SMC, the server required additional time to start, a duration that could last for up to 130 seconds. This issue has been fixed.

SMC 3.3.2 new features and enhancements

Managing administrators

New password policy

The password policy applied by default when SMC is deployed for the first time has been modified and requires now a minimum of 12 characters instead of 8.

If you have updated your SMC server from a version previous to 3.3.2, we recommend you to change the default password policy and set a minimum of 12 characters.

Find out more

Network configuration

Blackhole interface

Blackhole virtual interfaces can now be selected during the creation of a static route that aims to destroy a specific stream of traffic. Among other uses, this mechanism can be used in a configuration that contains IPsec tunnels - when a tunnel is down, packets that were meant for it will therefore be destroyed instead of being redirected to the firewall's default gateway.

Active Update server

New Active Update database

SMC now supports the "AdvancedAV1" Active Update database, which contains antivirus signatures of the new Advanced Antivirus service.

Find out more

Resolved vulnerabilities for SMC 3.3.2

Node.js vulnerability

Clandestine HTTP requests

A medium severity vulnerability was fixed after the Node.js component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-024.

OpenSSL vulnerability

Protection against buffer overflow attacks

A medium severity vulnerability was fixed after the OpenSSL component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-026.

SMC 3.3.2 fixes

System

Node.js error

Support reference 84703

Unexpected errors will not happen again on the Node.js environment of the SMC application. It could happen in some cases, for example when deploying the configuration on firewalls or when accessing a SNS firewall administration interface through SMC administration interface.

Configuration deployment

Improvement of server logs dealing with deployment

Support reference 84827

When a configuration deployment fails, the content of server logs has been improved in order to better describe the error.

SMC 3.3.1 new features and enhancements

3DS Outscale hosting

The SMC server can now be hosted by 3DS Outscale in Bring Your Own License (BYOL) mode.

You can choose from various types of instances so that the resources of the SMC server can be optimally adapted based on the number of firewalls to manage.

Find out more

SNS CLI scripts

Delayed script execution

The execution of SNS CLI scripts can be launched or scheduled on firewalls that are offline at the time of execution. Scripts will be automatically executed the next time such firewalls connect to SMC.

Find out more

SNS firewall monitoring

Shortcut to SLS (Stormshield Log Supervisor)

If you have an SLS server to centrally manage logs collected from your SNS firewalls, you can now configure shortcuts to the SLS server in SMC. This will allow you to read logs from the entire pool, or logs filtered by a firewall of your choice.

Find out more

VPN topologies

New Diffie-Hellman groups

In encryption profiles, you can now select Diffie-Hellman groups 31 (EC25519) and 32 (EC448).

Filter and NAT rules

ACK queue

In order to support QoS on firewalls in at least version 4.3.0, the new **ACK queue** field in the **Action > QoS** menu of a filter rule makes it possible to set a specific queue for TCP ACK traffic.

Find out more

S7+ protocol added

The S7+ application protocol can now be selected in filter and translation rules.

Resolved vulnerabilities for SMC 3.3.1

Node.js vulnerability

Clandestine HTTP requests

A high severity vulnerability was fixed after the Node.js component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-018/.

Javascript library

A low severity vulnerability was fixed after the Javascript Moment.js library was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-022/.

SMC 3.3.1 fixes

Object database

Network objects

Support reference 84405

Network objects with a subnet mask in /32 can no longer be used or imported in the firewall configuration. The consistency checker will raise an alarm if such objects are found on SMC.

Router objects

Support reference 84643

Router objects can now be created even when the HTTPS port object does not exist in the SMC object database.

Monitoring SMC with SNMP

Status of the SNMP service after updating SMC

Support reference 84438

When SNMP is enabled on the SMC server, it will now automatically restart after SMC is updated. The service remains enabled after SMC is restarted.

System

`service` command

Support reference 84381

SMC no longer supports the `service` command. Since version 3.0, the use of the `service --status-all` command, which listed the services on the system, would make SMC stop functioning.

Some errors caused SMC to stop

Some errors, which could occur during a configuration deployment for example, caused SMC server to stop. SMC now continues to run correctly even if these errors occur.

Configuration deployment

Use of the same peer in VPN topologies

Support references 84584 and 84647

Whenever the same peer was used twice in a VPN topology, SMC would no longer restart during a deployment. This would make the deployment fail and SMC would display an error message.

Filter rules

Use of the @ character in the comments of a rule

Support reference 84423

The local filter rules on SNS firewalls now display correctly in SMC when the @ character is used in comments.

Display of local filter rules

Support references 84396, 84440 and 84442

The local filter rules on SNS firewalls now display correctly in SMC when:

- they use a group of regions, a category of public IP address reputations or web services that SMC does not know.
- they use router objects,
- they use objects that SNS did not export in SMC,

Configuration of SNS firewalls

Managing network interfaces

Support reference 84529

SMC now no longer deploys the network configuration if it has not retrieved all network interfaces beforehand.

Importing SNS firewalls

Support reference 84644

The #vpn_fw_public_ip_address parameter functions again when importing SNS firewalls from a CSV file.

Consistency check on network interfaces

Support reference 84576

The consistency check no longer fails when it analyzes network interfaces with IP addresses in /32.

Authorities and certificates

Verification of the revocation list

Support reference 84603

SMC now forces SNS firewalls to retrieve the certificate revocation list (CRL) after every time the configuration is deployed. So when a VPN topology is deployed with the CRL verification option enabled, tunnels will be operational immediately. There is no longer any need to wait for the firewalls to retrieve the CRL.

Changes to the CRL

Support reference 84646

SMC now ignores the CRL file *CA.crl.pem* in the folder *ConfigFiles/Global/Certificates/<topo_name>/* of SNS firewalls, so it no longer raises any alerts when this file is modified locally.

Version 3.3.0 not published

Version 3.3.0 is not available to the public.

SMC 3.2.2 fixes

SMC Certification authority

Update of the certification authority

The certification authority (CA) which manages the certificate of the license used by SMC has been renewed until June 09, 2026.

SMC 3.2.1 new features and enhancements

Network configuration

SD-WAN - Selecting the best link

In SMC, specific criteria can be centrally managed 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, you can set an SLA (Service Level Agreement) commitment based on one or several thresholds out of the criteria below:

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

As soon as any threshold is not being met, the firewall will select another WAN link with a suitable SLA status for the traffic in question.

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

Router objects now also include monitoring options that are the same for all gateways specified in the object.

Regardless of the type of traffic, you can also set up a more general configuration to ensure that all communications will automatically be redirected to a backup link when an Internet connection is down.

In the new **Routers** monitoring panel, the status of all gateways and the quality of connections can be looked up in real time, therefore saving time in the event of a failure. If a router issue is detected on a firewall, a probe will warn the user.

This monitoring data can be exported in *.csv* format.

SD-WAN can be managed from SMC on SNS firewalls in at least version 4.3.3.

Find out more

Configuring routing from SMC

Routing can now be configured in SMC. It can be accessed in read/write mode on SNS firewalls in at least version 4.2.4, and in read-only mode on firewalls in version 3.7 and upwards. Only IPv4 is supported.

In SMC, in the new **Routing** tab of each firewall's settings, configure and deploy:

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

Routing configurations already found on SNS firewalls can now also be looked up in the **Routing** tab.

This new feature therefore makes it possible to look up routing configuration and prepare changes even when firewalls are offline.

For example, in the static route configuration in SMC, dedicated routes to Virtual IPsec interfaces (VTIs) can be created in route-based VPN topologies. Below is the feature allowing you to view all types of interfaces in SMC.

There are new consistency checks that allow you to check the compatibility of the routing configuration and guarantee the validity of the deployment.

Find out more

Viewing all types of network interfaces

In SMC, some interface types could already be viewed, added and modified in the **Interfaces** tab of each firewall's settings. It is now possible to retrieve all existing types of interfaces on SNS firewalls in SMC. Wi-Fi, dialup, IPsec, Loopback, GRETUN, GRETAP and USB/Ethernet interfaces are shown in read-only mode as "Other interface" in the **Interfaces** tab.

All of these interface types can be used in the SMC routing configuration.

Find out more

Managing administrators

"root" account password

You can now set the "root" account password, which will allow you to access the SMC server in command line, when you manually initialize the server from the virtual environment. Previously, this password was set in the SMC initialization wizard, which can be accessed from your web browser.

Find out more

Customizing the querying of LDAP authentication servers

You can now change the LDAP attributes used by default in SMC to query authentication servers, by using three new environment variables.

Find out more

Filter and NAT rules

Naming copied rules

When a rule with a customized name is copied then pasted in the same context (firewall, folder or rule set), the "_copy" suffic is now added to the end of the name. This makes it possible to keep track of the relationship with the original rule and makes it easier to create rules with similar properties and names.

If the rule is pasted in a different context and a rule with the same name does not yet exist, the name will remain the same.

When a rule with a name generated by default by the system is copied and pasted, a new default name will be assigned to it.

Integrity of SMC server binary files

Checking the integrity of binaries

SMC binary files are now signed to guarantee better protection from corruption.

Refer to Installing this version to find out the new procedure for checking binary files.

SMC 3.2.1 fixes

SMC update

Update process

Support reference 84277

During the SMC update process, errors that were not serious and did not affect the update process would appear in command line mode. The server now only shows relevant errors.

Managing administrators

Authentication via OpenLDAP

Support reference 84152

In the LDAP authentication settings of the **Administrators** menu, the **ID** field of the connection account was renamed **Administrator DN** for OpenLDAP servers. The expected ID format for this field is a DN (without the base DN), such as "cn=administrator".

Configuration of SNS firewalls

Naming firewalls

Support reference 84452

The error message and audit log generated during an attempt to create a firewall with the same name as an object found in the database have been improved to indicate that a firewall or an object with the same name already exists.

Configuration deployment

Synchronizing nodes of a cluster

Support reference 84333

When the automatic synchronization of an HA cluster was disabled through the environment variable `FWADMIN_HASYNC_ON_DESYNCHRO`, deploying the configuration on a cluster would automatically desynchronize nodes. This issue has been fixed.

VPN topologies

Deploying an IKEv2 topology

Support reference 84230

When an IKEv2 VPN topology is deployed from SMC, changing a peer's settings directly on an SNS firewall no longer causes any serverd errors.

Failed tunnel negotiation

Support reference 84490

The negotiation of a tunnel fails whenever a peer's certificate contains the firewall's contact IP address in the certificate's *Subject Alternative Name* field. This is because the firewall will use this address as the peer's **Local ID**.

To prevent this from happening, the use of the certificate's *Subject* field as the peer's **Local ID** can be forced by setting the FWADMIN_CERT_SUBJECT_AS_PEER_LOCALID variable to "True". This variable is set to "False" by default.

Reading logs

Audit logs

Support reference 84279

Logs regarding anonymous users were generated in audit logs. As such information is not relevant, these logs are no longer generated.

Resolved vulnerabilities for SMC 3.1.6

Server protection

Protection against denial of service attacks

A low severity vulnerability was fixed after the OpenSSL and NodeJS components were upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-011/.

SMC 3.1.6 fixes

Authorities and certificates

Access to the Certificate Revocation List

Support reference 84433

SNS firewalls no longer return an error when a certificate is deployed with the value “any” as the **Local IP address for CRL verification**.

SMC 3.1.5 fixes

SMC update

Updating from 2.8.x to 3.1.4 version

Support reference 84331

Because of an issue during migration of the authentication configuration on the SMC server, it is not possible to update from a 2.8.x version to the 3.1.4 version. Version 3.1.5 fixes this issue. You can now update from SMC 2.8.x to SMC 3.1.5.

SNS firewall monitoring

Status of licensing options

Support reference 84121

When at least one of the license options Breach Fighter, Extended Web Control, Kaspersky, Stormshield Vulnerability Manager and Industrial Security Pack had expired for a firewall, SMC displayed the **Critical** status, even if the option was no longer used.

The warning for the imminent expiry of license options is now disabled by default.

The Administration guide will help you enabling the feature.

Configuration of SNS firewalls

Managing network interfaces

Support reference 84270

SMC could not display the network interfaces of an SNS firewall which used an interface of the type aggregate. This issue has been fixed and SMC now automatically displays all the types of managed interfaces.

SMC 3.1.4 fixes

SMC update

Updating from 2.8.x to 3.1.3 version

Support references 189860CW and 189875CW

Because of an issue during migration of the authentication configuration on the SMC server, it is not possible to update from a 2.8.x version to the 3.1.3 version. Version 3.1.4 fixes this issue. You can now update from SMC 2.8.x to SMC 3.1.4.

SMC 3.1.3 new features

Managing administrators

Managing connections to external authentication servers

Connections to LDAP, OpenLDAP and Radius authentication servers can now be configured directly in the web interface of the SMC server.

As a result, administrator accounts are more easily and securely managed.

The *auth-server.ini* file, which previously made it possible to configure these connections in command line, no longer exists. If you have configured connections to external severs via this file in the past, the parameters will automatically be migrated in the SMC database and you will find them in the web interface.

Find out more

VPN topologies

Various versions of the IKE protocol supported on the same firewall

From version 3.7 of SNS firewalls onwards, the same firewall can be used in several topologies configured with various versions of IKE.

If a firewall in a version lower than 3.7 is used in several topologies with various versions of IKE, the consistency checker will report an error that will then prevent the deployment.

Different versions of IKE can be supported on the same firewall only if there is a single firewall in common across several topologies. If several topologies configured with various versions of IKE have several firewalls in common, the version of the topology that was created first in the topology configuration screen will be the one deployed.

Update of the SMC certification authority

In SMC previous versions, the certification authority of the component checking the signature of the license file expired on July 4, 2022. In version 3.1.2, the certification authority has been updated in order to extend the validity period. You must update SMC to be able to continue using your current license after July 4, 2022.

SMC 3.1.3 fixes

Configuration deployment

Deployment on firewalls with TPMs

Support reference 167766PW

Configurations can now be deployed from SMC to an SNS firewall in version 4.2.4 and above, using a TPM. Previously, the progress of the deployment remained stuck at 57% because the use of a TPM was not compatible with the feature that backs up the configuration on the SNS firewall when connection issues occur with SMC. This feature was introduced in version 4.2.4 of SNS.

As this backup feature is enabled by default, you can disable it if you use a TPM, using the environment variable FWADMIN_FW_DEPLOYMENT_DISABLE_ROLLBACK. To find out more about this feature, refer to Deploying a configuration on firewalls.

Configuration of SNS firewalls

Detection of changes in the local configuration on firewalls with TPMs

Support reference 168275PW

The feature enabling the SMC server to detect changes performed in the local configuration on an SNS firewall using a TPM is now working correctly.

SMC 3.1.2 fixes

Updating the SMC server

Access to the web administration interface after an update to version 3.1.0

After an update to version 3.1.0, users would no longer be able to access the web interface whenever the **Outgoing interface** field was specified in certification authorities to manage certificate renewals.

This field is now managed individually in version 3.9.2 by firewall, instead of by certification authority.

Users can now access the interface again.

Managing administrators

Logins containing the "." character

Support references 188742CW and 168382PW

Users can now log in again to the SMC server if their logins contain the "." character, regardless of the origin of the administrator account (local, LDAP or Radius).

Connection with an LDAPS account

Support references 168375PW, 168393PW, 188642CW and 188403CW

After an update to version 3.1.2, users can now connect to the SMC server again with an LDAPS account.

Active Updates

Manually updating Active Update databases

Support reference 168411PW

All Active Update databases can now be manually updated again from the file generated by the database download script.

SMC 3.1 new features

Managing administrators

Access to the SMC server in SSH or console mode

All administrators can now be assigned access privileges to the SMC server via the console on the hypervisor or in SSH. Previously, only the "root" user was allowed.

This change makes it possible to facilitate access to advanced management features on the SMC server and identify administrator connections and operations, as well as any elevation of privilege, in server logs.

Administrators who authenticate via LDAP or Radius authentication servers can also access SMC through the console on the hypervisor or in SSH. The super-administrator can grant them privileges through the administration interface.

Managing administrators from external authentication servers

Administrators and groups that have accounts on an LDAP authentication server can now be managed directly in the SMC server's web interface.

The *rights.csv* file is no longer used, and the commands `smc-auth-check` and `smc-ui-password` are no longer available.

Likewise, Radius user groups can be added to the interface, the same way they are added on SNS firewalls, by using a VSA

The OpenLDAP 2.5.x authentication server is now supported.

Defining a backup authentication server

To guarantee that administrators have uninterrupted access to the SMC server, you can define a backup LDAP or Radius authentication server that will take over when the main server fails.

Find out more

Offline environment

Active Update server

The SMC server can now stand in for the Active Update server that communicates with Stormshield update servers, to distribute Active Update databases to SNS firewalls, even when they are not connected to the Internet. The service will automatically download databases on a regular basis. In this way, firewalls will always be equipped with the latest databases (context-based signatures, antivirus, Vulnerability Manager, etc.).

If the SMC server and SNS firewalls run in a closed network without Internet access, you can manually download Active Update databases and distribute them to SNS firewalls via the SMC server's Active Update server.

Find out more

Increased security

Compliance with ANSSI '*Diffusion Restreinte*' mode

The SMC server now makes it possible to implement *Diffusion Restreinte* mode on SNS firewalls. This mode complies with ANSSI recommendations with regard to sharing communications that pass through the IPsec VPN. A consistency check on the configuration of the server and firewalls will assist you in deploying this mode by automatically detecting the parameters that need to be changed.

When DR mode is enabled on the SMC server, the configuration will be deployed on SNS firewalls. The firewalls must then be manually restarted.

Find out more

Configuration of SNS firewalls

Using custom firewall properties

Custom properties can now be created in addition to the default Name, Description and Location properties on firewalls, and specific values can be assigned to each firewall.

You can therefore filter the list of firewalls or perform searches based on these properties, which can be imported or exported in CSV format, and can also be found in exports of monitoring data.

Find out more

SNS firewall monitoring

Exporting SNS firewall monitoring data

Exported monitoring data now consists only of firewall data displayed in the panel when the list is filtered.

Find out more

Status of licensing options

The status icons in the upper banner of the administration interface and the **Licensing options** column in the firewall monitoring panel now alert the user when a license option or its maintenance package has expired or is about to expire.

Environment variables make it possible to configure alert thresholds.

Find out more

Filter and NAT rules

Looking up local rules

Firewalls' local rules are now displayed in read-only mode in the filter and NAT rule panel.

SMC server configuration

Dynamic address assignment via DHCP

You can now choose whether to assign a dynamic IP address to the SMC server via DHCP. This option is available in the SMC server initialization wizard, or in the server's settings in the administration interface.

Authorities and certificates

Verification of the Certificate Revocation List (CRL)

The environment variable FWADMIN_VPN_CRL_REQUIRED is no longer supported to verify the validity of the certificates. The **Check certificate validity** checkbox is now available in the **Configuration** > **Certificates** panel.

In the certificate management panel, the administrator can now specify for each firewall:

- The local IP address to renew SCEP/EST certificates on SNS firewalls,
- The local IP address that allows the revocation list to be verified,
- The frequency with which the revocation list is verified.

The value of the previous variable FWADMIN_VPN_CRL_REQUIRED will not be kept when the SMC server is updated, and the **Outgoing interface** field in the certificate renewal panel has been removed.

Local IP address for the renewal of certificates obtained via SCEP or EST

For SNS firewalls that have certificates obtained via SCEP or EST, you can now specify the local IP address that will be used to renew certificates for each firewall. Previously, the renewal address was indicated in the certification authority settings, and was therefore the same for all certificates issued by the same authority.

Find out more

VPN topologies

Configuring PRF in encryption profiles

You can now choose an algorithm that must be negotiated as a PRF (Pseudo-Random Function) in the **IKE** tab in the encryption profiles used in VPN topologies. This option is supported from version 4.2.3 of SNS firewalls onwards and is only compatible with IKEv2 topologies.

Find out more

New encryption profiles

The three encryption profiles offered by default on the SMC server – "Strong encryption", "Mobile encryption" and "Good encryption" – have been renamed "Strong encryption legacy", "Mobile encryption legacy" and "Good encryption legacy". If you have modified them, they will revert to their default configuration.

The "Good encryption legacy" profile now uses AES instead of Blowfish and Diffie-Hellman group 2 replaces Diffie-Hellman group 14 in phase 2.

Three new profiles – "Strong encryption", "Mobile" and "Good encryption" – replace the previous profiles.

All six profiles are in read-only mode.

Object database

Importing router objects

SNS firewalls in version 4.3.0 make it possible to export router objects and the associated gateways. The SMC server now supports importing/exporting router objects in the same format as SNS firewalls.

The use of the CSV format (before SMC 3.1) is no longer supported for router objects. The gateway configuration associated with a router object is not compatible with SMC in versions lower than 3.1.

Hosting Amazon Web Services

The SMC server can now be hosted by Amazon Web Services (AWS) in BYOL (Bring Your Own License) mode.

You can choose between several types of instances to adapt the SMC server's resources as closely as possible to the number of firewalls to manage.

Find out more

Resolved vulnerabilities for SMC 3.1

Server protection

Protection of the server memory

A low severity vulnerability was fixed after the PostgreSQL component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

Protection against buffer overflow attacks

A medium severity vulnerability was fixed after the OpenSSL component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

SMC 3.1 fixes

Authorities and certificates

Subject length in certificates

Support reference 184536CW

Previously, the SMC server would truncate text entered in the Subject (DN) field in certificates when it exceeded 140 characters, causing the deployment of VPN topologies to fail. The SMC server now accepts certificates with subjects that exceed 140 characters.

Updating certificates in command line

Support reference 167610PW

Certificates installed on a firewall can now be updated using the command `smc-install-certificate`.

Filter and NAT rules

Filtering by user name

Support reference 167465PW

Traffic that filters user names containing apostrophes can now be declared in filter rules.

Warning regarding the analysis of encrypted traffic

Support reference 167465PW

The consistency check no longer raises a warning when a traffic decryption rule is placed before a rule that analyzes the same decrypted traffic.

Updating an SMC server in a version lower than 2.7.0

Support reference 185398CW

SMC servers in versions lower than 2.7.0 could not be updated to a 3.0.0 version if a block filter rule that performed destination NAT with a "network-any" value was defined in the policy. SMC servers containing such a rule can now be updated to a 3.1.0 version.

Object database

Searching for object groups

Support reference 167465PW

In the window to create or edit object groups, the **Search** field now extends to the IP addresses of objects.

Forced deployment of objects

Support reference 167698PW

When updating the SMC server to version 3.x, objects with forced deployment set on SNS firewalls now keep this parameter when they are migrated.

VPN topologies

IKE fragmentation

Support reference 167619PW

Previously, IKE fragmentation could not be enabled from the SMC server on SNS firewalls in version 3.7.x. It can now be enabled on firewalls in version 3.7.22, and fragment size can be configured.

SNS firewall monitoring

Display error in the firewall monitoring window

Support references 186959CW and 186343CW

In some error cases on SNS firewalls, the monitoring window in the administration console would no longer display. This issue has been fixed.

SMC 3.0.1 new feature

VPN topologies

Traffic endpoints

In VPN topologies, it is now possible to set the traffic endpoints to the *All* value in order to allow all traffic through the tunnels.

Resolved vulnerability in SMC 3.0.1

Server protection

Protection against denial of service (DoS) attacks

A low severity vulnerability was fixed after the NodeJS component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

SMC 3.0.1 fixes

Filter and NAT rules

Filtering by domain name

Support reference 82060

Domain names used as criteria in filter rules can now be entered in any format, not only as URLs.

Exporting to CSV files

Support reference 82236

The value of the **Inspection** field in a filter rule is now correctly exported when it is either *firewall*, *IDS* or *IPS*.

Configuration deployment

Deployment status

If the SN firewall automatically restores a configuration after it is deployed from SNS, this deployment will no longer be considered successful and its number will no longer be incremented.

Configuration on a cluster

Deploying a configuration that includes a network configuration on a cluster no longer causes the cluster to restart.

SMC 3.0 new features

Authentication

Nested groups

Administrators that belong to an LDAP group nested in another can now connect to the SMC server.

Configuration of SN firewalls

Managing network interfaces

The network interfaces of SN firewalls can now be managed from a central point on the SMC server. On SN firewalls in at least version 3.7, SMC displays network interfaces in read-only mode. On SN firewalls from version 4.2.3 upwards, the configuration of network interfaces can be enabled in write mode in their SMC settings.

The Ethernet interfaces, bridges, VLANs and IPv4 aggregates of compatible firewalls will therefore appear on the SMC server. Their configuration can be managed without the need to connect to each firewall individually. SMC verifies the configuration of supported interfaces and reports errors through the consistency checker.

Find out more

Keeping the connection alive during deployment

When the wrong configuration is accidentally deployed, the connection between the server and firewall may be lost. On SN firewalls from version 4.2.3 upwards, the previous configuration will be restored if the connection was lost. This guarantees that the firewall will always remain reachable from the SMC server.

Find out more

Restarting after a deployment

SN firewalls may sometimes need to be restarted after a network configuration is deployed in order for changes to be applied. In such cases, SMC reports the information using the new “Reboot required” health status, and the firewalls in question can then be rebooted directly from the SMC server. This feature is supported only on firewalls in version 4.2.3.

Find out more

Detecting local modifications

After its initial deployment on a connected SN firewall, SMC now detects local modifications to the configuration of items that SMC manages. You can then decide whether to deploy the configuration currently found on the SMC server, which will overwrite local modifications. You can also restore the latest configuration deployed on the firewall in question.

Find out more

Importing firewalls from a CSV file

The command that makes it possible to import SN firewalls from a CSV file in command line has been renamed `smc-import-firewalls`. The previous command `smc-firewalls-and-packages` is no longer supported.

Find out more

Filter and NAT rules

Creating rule sets

Rule sets can now be created to group filter or translation rules that you wish to deploy on one or several firewalls. As such, a set of rules corresponding to a specific application in the configuration of various firewalls can be reused, regardless of their location in the folder tree.

Find out more

SMC 3.0 fixes

Configuration of SN firewalls

Inaccessible audit logs

Support references 79393 and 80772

On some versions of SN firewalls, access to audit logs would occasionally fail during connections to the firewall via the SMC server. This issue has been fixed.

Network configuration via USB key impossible

Support reference 79258

Due to a missing section in the connecting package, USB keys could not be used to load the network configuration on firewalls in factory configuration. The section has been added and USB keys can now be used.

Initialization of the SMC server

Ambiguous parameter

Support reference 82014

The `DNS configuration (leave blank if no DNS)` parameter requested whenever the SMC server is initialized manually, has been changed to `DNS server IPs (comma separator or leave blank if no DNS)` to remove any ambiguity.

Updates

Time zone not saved

Support reference: 80779

The set time zone is now saved after SMC is updated.

Loss of scripts

Support reference: 71885

Scripts that automatically run when a network interface on the SMC host system is enabled are now saved after updates.

Ambiguous error message

Support reference: 0081991

When there are issues restoring the server from a backup, the ambiguous error message that appears has been changed to more clearly indicate the cause of the error.

Filter and NAT rules

Importing rules

Support reference: 79314

When filter rules were imported from a CSV file, the "!" operator (NOT) would be ignored. This issue has been fixed, and fields are now imported with this operator taken into account.

Support references: 78561 and 79308

Rules containing the value "any" in a `#nat_to_target` field in the CSV file could not be imported because this value is prohibited. The value of this field is now automatically set to "none" and the import no longer fails.

Support reference: 80828

Filter and NAT rules containing domain names can now be imported.

Support reference: 80590

Rules can now be imported through a CSV file containing some IPRep categories that were previously missing.

Adaptation of protocol name

Support reference 82222

In filter rules, the "ldap" protocol has been renamed "ldap_tcp" to maintain consistency between SNS and SMC.

Error during copy and paste

Support reference: 78373

In the filter and NAT rule window, copying and pasting text contained in the search field now pastes only the text without duplicating the highlighted rule.

System

Frequently encountered errors

Support reference: 81714

Errors regarding the connection to the serial port were displayed every five minutes. This issue has been fixed.

Contact

To contact our Stormshield Technical Assistance Center (TAC):

- https://mystormshield.eu/
  All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under **Technical support** > **Manage cases**.
- +33 (0) 9 69 329 129
  In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu.



STORMSHIELD

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

Copyright © Stormshield 2026. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.