STORMSHIELD

STORMSHIELD NETWORK SECURITY

RELEASE NOTES

Version 4.8 LTSB

Document last updated: November 13, 2025

Reference: sns-en-release_notes-v4.8.13-LTSB

Table of contents

Change log 3
Points to note for updates from a 4.3 LTSB version 4
New firewall behavior 7
New features and enhancements in SNS version 4.8.13 LTSB 14
SNS version 4.8.13 LTSB bug fixes 15
Compatibility 17
Known Issues 18
Limitations and explanations on usage 19
Documentation resources 30
Installing this version 31
Previous versions of SNS v4 33
Contact 321

In the documentation, Stormshield Network Security is referred to in its short form: SNS and Stormshield Network in its short form: SN.

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

To guarantee security on your firewall and to maintain it in optimal operating condition, ensure that you apply the most recent firmware update, as well as the configuration recommendations that Stormshield has given.

LTSB (Long-Term Support Branch) label

Major or minor versions with this label are considered versions that will be stable over a long term, and will be supported for at least 12 months. These versions are recommended for clients whose priority is stability instead of new features and optimizations.

For more information, refer to the **Network Security & Tools Product lifecycle document**.

Change log

Date	Description
November 13, 2025	New document

Points to note for updates from a 4.3 LTSB version

IMPORTANT
If you intend to update a firewall from a 4.3 LTSB version to version 4.8 LTSB, we encourage you to read this section carefully.

NOTE
The exhaustive list of new automatic behavior relating to the update of your SNS firewall to version 4.8 LTSB from the latest 4.3 LTSB version available can be found in New firewall behavior in these release notes.

Update path from version 4.3 LTSB

We strongly recommend that you update your firewall from the latest SNS 4.3 LTSB version to SNS 4.3.24 LTSB if necessary.

An exhaustive list of behavioral changes in SNS 4.8 LTSB can be found in the New firewall behavior section of these Release Notes.

Original version	Intermediate updates required
4.3.23 LTSB or lower	Version 4.3.24 LTSB is recommended, as the firewall's backup partition would become unusable following a direct update to the new version.
4.3.24 LTSB or higher	None

BIRD dynamic routing

Version 1 of the BIRD dynamic routing engine is now considered obsolete and will be removed in a future SNS release. Version 2 of the BIRD dynamic routing engine is available in SNS 4.8. LTSB, we strongly advise you to migrate BIRD v1 configurations to BIRD v2.

When updating a configuration using BIRD v1 to SNS 4.8 LTSB, the initial configuration is retained, and it is necessary to manually migrate the configuration from BIRD v1 to BIRD v2.

If your SNS firewalls are managed by an SMC server, it is not possible to manage the dynamic routing of your SNS 4.8 LTSB firewalls from an SMC version lower than 3.6.

Firewalls equipped with a TPM

After upgrading to SNS 4.8 LTSB, the secrets stored in the TPM need to be sealed with the new system specifications using the CLI / Serverd command:

```
SYSTEM TPM PCRSEAL tpmpassword=<TPMpassword>
```

Note that in the case of a cluster, this action must be performed for both cluster members from the active firewall, adding the "serial=passive" parameter to seal passive firewall secrets from the active firewall.

For more information on the TPM module, please refer to the Trusted Platform Module section of the SNS user manual, as well as the Technical Note on Configuring the TPM and protecting private keys in SNS firewall certificates.

For firewalls supporting Secure Boot in UEFI (models SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN3100, SN-L-Series-2200, SN-L-Series-3200, SN-XL-Series-5200, SN-XL-Series-6200, SNi10, SNi20, SNxr1200), we strongly recommend that you activate Secure Boot before resealing your secrets.

For more information on the impact of enabling Secure Boot, please refer to the Technical Note Managing Secure Boot in SNS firewalls' UEFI.

Suppression of OSCAR, MSN, YMSG and eDonkey protocol analysis

As the OSCAR, MSN, YMSG and eDonkey protocols are obsolete, the intrusion prevention engine no longer supports their analysis. After updating to SNS 4.8 LTSB a configuration with a filtering rule relating to one of these protocols, this rule is ignored and a warning message is displayed within the filtering policy concerned.

SSL VPN

As SNS 4.8 LTSB adds the data-cipher option to the SSL VPN client configuration file, SSL VPN v2 clients are no longer compatible with SNS 4.8 LTSB.

Compression is now disabled by default. It is possible to view and change the compression status (enabled or disabled) from the CLI console. We strongly advise against re-enabling compression, as this feature will no longer be supported in a later version of SNS.

Reputation categories

The reputation categories Exchange Online, Microsoft Authentication, Office 365, Office Online, SharePoint Online and Skype for business, present in previous versions, are no longer available since version SNS 4.4.1. Once a configuration using one of these categories has been updated to SNS 4.8 LTSB, the filtering rules using these categories become inoperative until they are replaced by the Web services introduced in SNS 4.4.1.

Features and algorithms obsolete in SNS 4.8 LTSB version

The features and algorithms listed below have become obsolete in version SNS 4.8 LTSB and will be removed in a future SNS firmware version.

Network Vulnerability Manager (SNVM)

The SNVM module is obsolete. It will be supported for the lifetime of SNS 4.8 LTSB. For more information on the end-of-life date of the SNVM module, please refer to the Services section of the *Product Lifecycle*.

URL / SSL filtering

The embedded URL database is obsolete. To continue using URL / SSL filtering, you can subscribe to the Extended Web Control option.

PPTP server VPN

PPTP server functionality is obsolete.

SCEP protocol (certificate registration)

The hash algorithms md2, mdc-2, md4, md5, rmd160, and the encryption algorithm des-ede3-cbc are obsolete.

SNMP v3 agent

The MD5 authentication algorithm and the DES and SHA1 encryption algorithms used by the SNMPv3 Agent are obsolete.

Internal LDAP directory

The MD5, SMD5, SHA, SSHA, SHA256, SHA384 and SHA512 password hashing algorithms used by the internal LDAP directory are obsolete.

SSL VPN Portal

SSL VPN Portal functionality is obsolete.

New firewall behavior

This section lists the changes made to the automatic behavior of the firewall when your SNS firewall in version 4.8.13 LTSB is updated from the latest 4.3 LTSB version available.

If necessary, we also encourage you to read about the New firewall behavior in SNS version 4.3 introduced since the last available 3.7.x LTSB version.

Changes introduced in version 4.8.13 LTSB

- SPNEGO authentication - SPNEGO authentication is obsolete, and will be phased out in SNS version 5.1. Warning messages will inform you that the module is obsolete:
  - When you attempt to enable SPNEGO authentication in **Configuration > Users > Authentication**,
  - In response to the CLI/Serverd command `MONITOR MISC` if SPNEGO authentication has been enabled,
  - In the **Messages** section of the dashboard, if the SPNEGO authentication has been enabled.

Changes introduced in version 4.8.10 LTSB

- SNMPV1 - SNMP version 1 is obsolete, and will be phased out in SNS version 5.1. A warning message informing you that it is obsolete will appear in the **SNMPV1 - SNMPV2C** tab in **Configuration > Notification > SNMP agent**.

Changes introduced in version 4.8.9

- SMC-managed firewalls - On SMC-managed firewalls, updates to SNS in version 4.8.9 or higher are blocked when these two conditions are combined:
  - The private key of the certificate that is used for communications with the SMC server is protected by the TPM,
  - The firewall is in version SNS 4.8.2 or lower.

  To perform the update, protection on the SMC certificate must also be lifted, either from the Web administration interface, or through the CLI/Serverd command `CONFIG FWADMIN PROTECT tpm=none tpmpassword=<password>`. For more information, refer to the section Protecting private keys in SNS firewall certificates, in the technical note *Configuring the TPM and protecting private keys in SNS firewall certificates*.
- ClamAV antivirus - The ClamAV antivirus engine is obsolete and will be phased out in SNS version 5. Updates to the engine will end in September 2025. Warning messages will inform you that the module is obsolete:
  - In the **Application protection** > **Antivirus** module,
  - In the **Messages** section of the dashboard, if the ClamAV antivirus is used.

  In addition, the antivirus icon in the **Services** section of the dashboard will be orange.
  Firewalls cannot be updated to SNS version 5 if ClamAV is used.
  If you wish to continue using an antivirus module, subscribe to the advanced antivirus option. For further information, please contact your reseller.

Changes introduced in version 4.8.7

- Firewalls equipped with a TPM - On SNS 4.8.7 and higher versions, TPM protection is incomplete as long as the Secure Boot feature is not enabled. We recommend enabling it before updating the SNS firewall to version 4.8.7 if the TPM has been initialized. For more information, refer to the technical note Configuring the TPM and protecting private keys in SNS firewall certificates.
- Firewalls with TPM-protected VPN certificates - After an update to SNS version 4.8.7, and if the certificates that are used for IPsec VPN or SSL VPN services are TPM-protected, the TPM has to be resealed.
- Network Vulnerability Manager (SNVM) - The **SNVM** module is obsolete, and will be discontinued in SNS version 5. It will be supported throughout the lifetime of SNS 4.8 versions. For more information on the end of life date for the SNVM module, refer to the section Services in the *Product life cycle guide*. Warning messages will inform you that the module is obsolete:
  - If DR mode is enabled, in the **Message** section of the dashboard,
  - If DR mode is not enabled, in the **Message** section of the dashboard, and in the **SNVM** module.

    Policy-based routing - As policy-based routing has priority over static routing, it is now correctly applied when traffic that has no explicit routing instructions is abandoned (decision to send such traffic to a blackhole gateway).

Changes introduced in version 4.8.5

- Internal LDAP directory - The CRYPT password hash algorithm used by the internal LDAP directory is now obsolete. As such, internal LDAP directories can no longer be created using this algorithm. Existing directories that use this algorithm are not affected.

Changes introduced in version 4.8.3 EA

Find out more

- Firewalls equipped with a TPM - After an update to SNS version 4.8.3, secrets stored in the TPM must be sealed with the new technical characteristics of the system, by using the CLI/Serverd command:
  `SYSTEM TPM PCRSEAL tpmpassword=<TPMpassword>`
  Do note that in clusters, this action must be applied to both members from the active firewall, by adding the parameter "*serial=passive*" from the active firewall to seal the secrets of the passive firewall.
  For more information on the TPM, refer to the section Trusted Platform Module in the SNS user guide.
- Web services in filters - When a custom web service with a name that is exactly 20 characters long is used in a filter rule, the rule would not function. A warning message will then appear in the **Messages** widget on the **Dashboard**. The message indicates the filter policy and rule number that caused the error.
  To work around the issue:
  - Change the name of the web service (to fewer than 20 characters) in the CSV import file that was initially used,
  - Import this file once again in **Objects** > **Web services** > **Import custom services** tab,
  - Modify the filter rule to use the new name of the web service.

- In the factory settings on firewalls in SNS version 4.8.3 EA or higher, downgrades to a lower firmware version are now allowed once again by default.
- URL/SSL filtering - The built-in URL database is obsolete. As such, it will no longer be updated, and is set to be deleted in a future SNS firmware version.
  To continue applying URL/SSL filtering, you can:
  - Subscribe to the Extended Web Control option,
  - Continue using the built-in URL filtering engine, by combining it with a URL filter database provided by a third-party vendor, for example:
    - French URL database provided by the *Rectorat de Toulouse* (Academy of Toulouse), by following the method described in the Stormshield Knowledge Base (authentication required),
    - Polish URL database provided by Dagma, by following the instructions here: https://stormshield.pl/pomoc/baza-wiedzy/item/zmiana-klasyfikacji-url-na-rozszerzona-klasyfikacje-dedykowana-dla-polskiego-rynku.
- PPTP server VPN - The PPTP server feature is obsolete and is set to be deleted in a future SNS firmware version.
- SCEP (certificate enrollment) - Hash algorithms md2, mdc-2, md4, md5 and rmd160, and the encryption algorithm des-ede3-cbc, are obsolete. They are set to be deleted in a future SNS firmware version.

Changes introduced in version 4.8.1 EA

Find out more

- Firewalls in SNS version 4.8.1 EA reject downgrades to versions lower than SNS 4.7.3 or SNS 4.3.24 LTSB.
- Firewalls equipped with a TPM - After an update to SNS version 4.8, secrets stored in the TPM must be sealed with the new technical characteristics of the system, by using the CLI/Serverd command:
  `SYSTEM TPM PCRSEAL tpmpassword=<TPMpassword>`
  Do note that in clusters, this action must be applied to both members from the active firewall, by adding the parameter "*serial=passive*" from the active firewall to seal the secrets of the passive firewall.
  For more information on the TPM, refer to the section Trusted Platform Module in the SNS user guide.
- SNMPv3 agent - Authentication algorithm MD5 and encryption algorithms DES and SHA1, which the SNMPv3 agent uses, are obsolete and will be removed in a future SNS firmware release.
- Internal LDAP directory - Password hash algorithms MD5, SMD5, SHA, SSHA, SHA256, SHA384 and SHA512, which the Internal LDAP directory uses, are obsolete and will be removed in a future SNS firmware release.
- SSL VPN portal - The SSL VPN portal feature is obsolete and is set to be deleted in a future SNS firmware version.
- BIRD dynamic routing
  - Version 1 of the BIRD dynamic routing engine is now considered obsolete. Version 2 of the BIRD dynamic routing engine is now available,
  - If your SNS firewall pool is managed by an SMC server, it will not be possible to manage dynamic routing on your firewalls in 4.8.1 EA versions and higher from SMC in version 3.6 and below.

- SNMP agent - The value assigned to the *sysname* field presented by the SNMP agent now follows a new order.

Changes introduced in version 4.7.7

- Sandboxing - Only files that have been classified as archive, Office document, executable, PDF and Java files will now be sandboxed to reduce the load on the service. Files that have been classified as other or unknown files will no longer be analyzed.

Changes introduced in version 4.7.5

- SNMP agent - The value returned by the OID *1.3.6.1.2.1.1.7* is now 76, corresponding to a device that provides services on OSI layers 3, 4 and 7. Previously, the value returned was 72.

Changes introduced in version 4.7.3

- SN1100 - The maximum number of IPsec tunnels that SN1100 firewalls accepted was too high. The number has been reduced to match announced data.

Changes introduced in version 4.7.2 EA

Find out more

- Routing - Loopback objects that are used as default gateways are automatically replaced with the blackhole object when the firewall is updated to SNS version 4.7.2 EA or higher.
- Oscar and Gnutella - Protocols Oscar and Gnutella are now considered obsolete. These protocol scans are automatically disabled when the firewall is updated to SNS version 4.7.2 EA.

Changes introduced in version 4.7.1 EA

Find out more

- IPsec DR - During the generation of certificate request payloads, ANSSI's IPsec DR guidelines recommend replacing the algorithm with SHA2 (previously SHA1). SNS in versions 4.7 and up comply with with this recommendation.
  If IPsec DR mode is enabled on an SNS firewall in version 4.7, VPN tunnels can only be negotiated with peers that comply with this recommendation.
- VPN Exclusive client (with DR mode) - the VPN Exclusive client in version 7.4 or higher must be used to set up IPsec tunnels in DR mode with firewalls in SNS versions 4.7 and higher.
- Firewalls equipped with a TPM - After an update to SNS version 4.7, secrets stored in the TPM must be sealed with the new technical characteristics of the system, by using the CLI/Serverd command:

  ```
  SYSTEM TPM PCRSEAL tpmpassword=<TPMpassword>
  ```

  Do note that in clusters, this action must be applied to both members from the active firewall (by adding the parameter "serial=passive" from the active firewall to seal the secrets of the passive firewall).
  For more information on the TPM, refer to the section Trusted Platform Module in the SNS user guide.

- Extended Web Control (EWC) URL classification - The Bitdefender URL database is now the database used.

  To set up a URL/SSL filter policy, you are advised to operate in blacklist mode, i.e., explicitly place the URL categories to be prohibited in URL/SSL filter rules with a *block* action. These rules must then be placed above the rule that allows all the other categories.

  While updating a firewall, which uses a whitelisted URL/SSL filter policy, to SNS version 4.7.1 or higher (filter rules explicitly allow some categories and are placed above the rule that blocks all other categories), we strongly recommend adding a rule that allows the URL categories *misc* (miscellaneous), *unknown*, *computersandsoftware* (software download websites) and *hosting* (websites hosting) to avoid affecting user experience. This rule must be placed above the rule that blocks all the other categories.

  For more information on the migration of URL/SSL filter policies when the firewall is updated to SNS version 4.7 or higher, please refer to the **Technical Note** Migrating a security policy to the new EWC URL database.

  IMPORTANT
  URL/SSL filter policies that have been updated after the firewall was updated to SNS version 4.7.1 must be thoroughly checked.

- Resetting to factory configuration - Resetting a firewall to its factory configuration (*defaultconfig*) now deletes by default all custom configuration files added by the administrator. If you do not wish to delete them, use the command `defaultconfig -T`.
- Synchronizing MAC addresses (HA) - On elastic virtual appliances (EVA) deployed in versions 4.7 and higher and in a high availability (HA) configuration, the synchronization of MAC addresses during a cluster switch is now disabled by default.
- Hardening of the system - As the system has been hardened in SNS version 4.7, this makes the backup partition unusable in SNS version 4.3.23 LTSB and lower versions when they are directly updated to SNS version 4.7. You are advised to update your firewall to SNS version 4.3.24 LTSB or a higher version before updating to SNS version 4.7.

Changes introduced in version 4.6.9

Find out more

- SSH connections to the firewall - On firewalls in factory configuration and in SNS version 4.6.9 and upwards, the encryption algorithms ssh-rsa, hmac-sha2-256 and hmac-sha2-512 are no longer allowed for SSH connections to the firewall.

Changes introduced in version 4.6.8

Find out more

- BIRD dynamic routing - In configurations that use BGP with authentication, the "source address <ip>;" directive must be used so that BGP sessions continue to be set up after the SNS firewall has been updated.

Changes introduced in version 4.6.3

Find out more

- SSL/TLS-based protocols - For security reasons, encryption suites that base their key exchanges on Diffie-Hellman methods (DHE-based suites) have been removed. Only ECDHE-based suites are now available on SNS firewalls.
  This change may have an impact on connections initiated to or from the firewall for various SSL-secured protocols (HTTPS, SSH, LDAPS, SMTPS, etc.) as well as SSL connections established through the firewall's proxy. Due to this change, SNS firewalls may become incompatible with older client applications and external services/machines that use such protocols.

  The ECDHE-based encryption suites available on SNS firewalls are:
  - TLS_AES_128_GCM_SHA256,
  - TLS_CHACHA20_POLY1305_SHA256,
  - TLS_AES_256_GCM_SHA384,
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  - TLS_EMPTY_RENEGOTIATION_INFO_SCSV.

Changes introduced in version 4.5.3

Find out more

- Hardening of the operating system - Text editors Vim and JOE have been removed from the system and replaced with vi.
- Quality of Service (QoS) - The **Treatment when full** field, in which the packet congestion processing algorithm in queues (**TailDrop** or **BLUE**) could be selected, has been removed from QoS settings. The algorithm used by default is now **TailDrop** and can only be changed via the CLI/Serverd command `CONFIG OBJECT QOS DROP`.
- IPsec DR mode - When DR mode is enabled for the first time, Diffie-Hellman group DH28 is now suggested as the default group for IKE DR and IPsec DR profiles.

Changes introduced in version 4.5.2

Find out more

- Quality of Service (QoS) - Queues are no longer defined by percentage of bandwidth. After certain SNS firewalls, on which the QoS configuration used queues defined by percentage of bandwidth, are updated to versions 4.5.2 and higher, this percentage will automatically be converted to equivalent absolute bandwidth values.

Changes introduced in version 4.5.1

Find out more

- SSL VPN - SNS version 4.5 is only compatible with the SSL VPN client in version 3.1 or the OpenVPN client in versions 2.5 and higher. The SSL VPN (or OpenVPN) client can be updated on client workstations before the firewall is updated to SNS version 4.5. The configuration on OpenVPN clients (available on the captive portal) must also be updated after the firewall is updated to version 4.5.
- QoS - The definition of queues by percentage of bandwidth is obsolete. After being updated to SNS version 4.5, firewalls on which the QoS configuration used queues defined by percentage of bandwidth, a warning message will appear in the grid of queues, asking the administrator to change the configuration of such queues.
- Kerberos - Kerberos authentication is now TCP-based by default (*kerberos_tcp* object - port 88/TCP).

Changes introduced in version 4.4.1

Find out more

- Reputation categories - Exchange Online, Microsoft Authentication, Office 365, Office Online, SharePoint Online and Skype for business reputation categories, which could be found in versions prior to SNS 4.4.1, are no longer available. Filter rules that use them will therefore not function until these categories are replaced with the web services introduced in SNS version 4.4.1.
- Stealth mode - SNS firewalls in factory configuration are now in stealth mode by default. Do note that disabling stealth mode will affect packet processing performance. As the firewall must keep a log of each packet so that it can respond to ICMP error messages, stealth mode allows the firewall to save resources that would have been used on logging these packets.

New features and enhancements in SNS version 4.8.13 LTSB

IPsec VPN - Certificates

Support reference 85930

In order to comply with the prescription "Other methods of generating unique numbers are also acceptable" in RFC 5280, SNS firewalls are now able to verify locally retrieved CRLs for certificates that are generated with *SubjectKeyIdentifier* and *AuthorityKeyIdentifier*.

Virtual IPsec interfaces (VTI)

In IPsec policies that are based on virtual IPsec interfaces, with any of the configurations listed below, a warning message now appears prompting the administrator to edit the configuration:

- Traffic selectors are networks instead of IP addresses,
- Remote and local traffic selectors are not in the same IP sub-network,
- Identical virtual interfaces are used in several rules in the filter policy.

Sandboxing

Support reference 86046

To prevent the saturation of processing queues, the firewall no longer sends the sandboxing infrastructure any e-mails without attachments, or any attachments in a format that is not supported by the sandboxing service.

CLI/Serverd command - SYSTEM PROPERTY

The CLI/Serverd command `SYSTEM PROPERTY` now provides the BIOS version with the `BIOSRevision` configuration token.

Privileges for access to private data

Now, when you connect to the firewall with an administrator account:

- Other than the 'admin' account,
- That has permissions to access private data,

And you access a module that contains private data, a pop-up will open, asking whether you wish to acquire privileges to access private data.

SNS version 4.8.13 LTSB bug fixes

System

SSL VPN

Support reference 85904

When the listening port of the SSL VPN service is changed, a message now appears, indicating the need to restart the firewall to correctly apply the change.

Bypass mechanism - SNi20/SNi40 industrial firewalls

The bypass would no longer activate when the firewall's hardware manager was unexpectedly disrupted. This issue is now fixed. This regression appeared in SNS version 4.8.7 ?).

SMC server redundancy

Support reference 86112

When the main SMC server fails, the SNS firewall will connect to the backup server. Previously, when the main server recovered, no operations (deployment, firewall access, etc.) could be performed from it. This issue has been fixed.

List of group objects

Support reference 86221

In the object database, if the number of groups to be displayed exceeds 4096 entries, the comments that are associated with each group would not be displayed. This issue has been fixed in the web interface, and when the list of groups is exported in CSV format.

Virtual Pay As You Go (PAYG) machines

Support reference 86111

The enrollment of virtual PAYG machines now functions properly once again, and no longer wrongly displays a message indicating anyway that the enrollment was successful.

Certificate revocation list (CRL) retrieval mechanism

Support reference 86153

The CRL retrieval mechanism can once again set up its connections with a source IP address that is identified as <Firewall_interface_name>.

High availability

Support references 84970 - 85311 - 85657 - 85802

The synchronization of some files in the cluster has been improved. This prevents the inappropriate generation of error messages in the system log file when some of these files are justifiably absent.

Restoring configurations

Support reference 84995 - 85981 - 86070

The reloading of the configuration immediately after a deployment in SMC, or after a configuration has been restored, is now optimized.

Objects

Support reference 86070

In a configuration that contains a large number of objects, the list of objects would take a long time to appear in the web administration interface. The mechanism has been optimized to reduce the display time.

Disk monitoring - SNi20

Support reference 86265

The hardware monitoring module now recognizes M2 model disks that may be installed on SNi20 model firewalls, and no longer wrongly generates an alert indicating that a disk is missing.

Intrusion prevention engine

SCTP - High availability (HA)

Support reference 85372

During every HA swap, the date on which SCTP associations were established would be incremented by one second. This issue has been fixed.

Web administration interface

SSL VPN portal

Support reference 86186

Servers with a name that contains an uppercase letter are no longer wrongly shown as disabled. This regression appeared in SNS version 4.8.0.

Compatibility

For more information, see the Product life cycle guide.

Known Issues

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

Limitations and explanations on usage

QoS

IMPORTANT
This is an early-access feature.
Ensure that you have read the section on Known issues before enabling this feature or updating an existing QoS configuration to an SNS 4.8 version or higher.

The following limitations have been placed on the QoS implemented:

- Maximum bandwidth supported: 1 Gbps,
- Interfaces supported:
  - Ethernet,
  - IPsec,
  - GRETAP,
  - Virtual IPsec (VTI),
  - VLAN.
- PRIQ and CBQ queues are not compatible with one another and must not be used on the same traffic shaper,
- All thresholds set on queues must be expressed either in absolute values only or percentages only.
- The amount of reserved bandwidth must not exceed the bandwidth assigned to the traffic shaper,
- When QoS is enabled, non-QoS traffic will be affected by an overall decrease in throughput on the SNS firewall. This is due to the fact that traffic using bypass queues cannot use all the available bandwidth, as multi-CPU architectures are not optimally managed by the QoS engine.

Authentication - TOTP

Support reference 84686

When advanced TOTP authentication settings are modified (**Lifetime**, **Code size,** and **Hash algorithm**), this authentication method would fail if it is used together with Google Authenticator or Microsoft Authenticator, which are code-generating applications.
A warning message has been added, asking the user to check whether the advanced settings are compatible with the code generator used.

Dynamic multicast routing

Dynamic multicast routing implemented in version 4.8 has the following limitations:

- IGMPv1 is not supported,
- IGMP Snooping is not supported,
- PIM Dense Mode is not supported,
- PIM Sparse-Dense Mode is not supported,

- PIM BiDir is not supported,
- Multicast BGP Extension is not supported,
- MSDP (Multicast Source Discovery protocol) is not supported,
- AnycastRP is not supported,
- IPv6 and the MLD (Multicast Listener Discovery) protocol are not supported,
- Static multicast routing and dynamic multicast routing cannot be enabled at the same time,
- Dynamic multicast routing tables are not synchronized in HA,
- Bridges and bridged interfaces cannot be selected as interfaces participating in dynamic multicast routing,
- The Cisco AutoRP protocol is not supported,
- SNS firewalls may be included in a Cisco AutoRP infrastructure when Cisco devices are configured to support BSR standards,
- In HA configurations, interfaces that participate in dynamic multicast routing must have a static IP address,
- The intrusion prevention engine does not analyze the PIM protocol,
- The number of interfaces on the firewall that participates in dynamic multicast routing is restricted to 31.

Web services

If web services are used in the firewall's configuration, the DNS protocol analysis must be enabled.

Jumbo frames supported on SN160, SN210 and SN310 firewall models

Even though the size of jumbo frame MTUs can be set to a maximum of 9216 bytes on SN160, SN210 and SN310 firewalls, do note that due to the hardware limitations on these models, the software will verify the checksums of packets with MTUs higher than 1600 bytes. As a result, this may affect the overall performance of these firewall models.

TPM-equipped firewalls

Support reference 83580

After an update to SNS version 4.8, secrets that are stored in the TPM have to be sealed. This operation is performed using a dedicated wizard in the graphical interface. In the case of an HA cluster, the passive firewall is resealed from the graphical interface of the active firewall.

For more information on the TPM, refer to the section Trusted Platform Module in the SNS user guide.

PROFINET RT protocol

Support reference 70045

The network controller used on SNi40, SN2000, SN3000, SN6000, SN510, SN710, SN910, SN2100, SN3100 and SN6100 firewalls has been upgraded and allows VLANs with an ID value of 0. This measure is necessary for the industrial protocol PROFINET-RT.

However, IX network modules (fiber 2x10Gbps and 4x10Gbps equipped with INTEL 82599) and IXL modules (see the list of affected modules) were not upgraded and therefore cannot manage PROFINET-RT.

IPsec VPN

Optimized distribution of encryption/decryption operations

In a configuration containing a single IPsec tunnel through which several data streams pass through, enabling the mechanism that optimizes encryption/decryption operations may disrupt the sequence of packets and cause the recipient to reject encrypted packets based on the size of the anti-replay window configured.

Interruption of phase 2 negotiations

The Charon IPsec management engine, used in IKEv1 policies, may interrupt all tunnels with the same peer if a single phase 2 negotiation fails.

This occurs when the peer does not send notifications following a failed negotiation due to a difference in traffic endpoints.

As mentioned earlier, the behavior of the Racoon IPsec management engine was modified in version 4.1.0 so that this issue no longer occurs in Racoon <=> Charon tunnels.

However, you may still encounter this issue when the Charon IPsec management engine negotiates with an appliance that does not send failure notifications.

IPsec-related constraints

Several constraints are imposed when IKEv1 and IKEv2 peers are used in the same IPsec policy:

- "Aggressive" negotiation mode is not allowed for IKEv1 peers using pre-shared key authentication. An error message appears when there is an attempt to enable the IPsec policy.
- The hybrid authentication method does not function for IKEv1 mobile peers.
- Backup peers are ignored. A warning message appears when the IPsec policy is enabled.
- The "*non_auth*" authentication algorithm is not supported for IKEv1 peers. In such cases, the IPsec policy cannot be enabled.
- In configurations that implement NAT-T (NAT-Traversal - transporting the IPsec protocol through a network that performs dynamic address translation), the translated IP address **must** be defined as the ID of a peer that uses pre-shared key authentication and for which a local ID in the form of an IP address had been forced.

PKI

A Certificate Revocation List (CRL) is not required. Even if no CRLs are found for the certification authority (CA), negotiation will be allowed.

A CRL can be made mandatory with the use of the "CRLRequired=1" parameter in the CLI command "CONFIG IPSEC UPDATE". When this parameter is enabled, you must have all the CRLs in the certification chain.

Support reference 37332

DPD (Dead Peer Detection)

The VPN feature DPD (Dead Peer Detection) makes it possible to check whether a peer is still up by sending ISAKMP messages.

If a firewall is the responder in an IPsec negotiation in main mode, and DPD has been set to "inactive", this parameter will be forced to "passive" in order to respond to the peer's DPD queries. During this IPsec negotiation, DPD will be announced even before the peer is identified, so before even knowing whether DPD queries can be ignored for this peer.

This parameter has not been modified in aggressive mode, as in this case DPD would be negotiated when the peer has already been identified, or when the firewall is the initiator of the negotiation.

IPsec VPN IKEv2

In configurations that implement NAT-T (NAT-Traversal - transporting the IPsec protocol through a network that performs dynamic address translation), the translated IP address **must** be defined as the ID of a peer that uses pre-shared key authentication and for which a local ID in the form of an IP address had been forced.

Backup peers

A backup configuration can no longer be defined for IPsec peers. In order to implement a redundant IPsec configuration, you are advised to use virtual IPsec interfaces and router objects in filter rules (PBR).

Network

4G modems

In order to ensure a firewall's connectivity with a 4G USB modem, HUAWEI equipment in the following list must be used:

- E3372h-153,
- E8372h-153,
- E3372h-320.

Other key models may work, but they have not been tested.

Routing - Network directly connected to an interface on the firewall

Support reference 79503

Whenever a network is directly connected to an interface on the firewall, the firewall creates an implicit route to access this network. This route is applied prior to PBR rules (Policy Based Routing): PBR is therefore ignored for such networks.

Spanning Tree protocols (RSTP / MSTP)

Stormshield Network firewalls do not support multi-region MSTP configurations. A firewall implementing an MSTP configuration and interconnecting several MSTP regions may therefore malfunction when managing its own region.

If MSTP has been enabled on a firewall and it is unable to communicate with equipment that does not support this protocol, it would not automatically switch to RSTP.

Due to the way they operate, RSTP and MSTP cannot be enabled on VLAN interfaces and PPTP/PPPoE modems.

Interfaces

On SN160(W) and SN210(W) firewall models, the presence of unmanaged switches would cause the status of the firewall's network interfaces to stay permanently "up", even when they are not physically connected to the network.

The firewall's interfaces (VLAN, PPTP interfaces, aggregated interfaces [LACP], etc.) are grouped together in a common pool for all configuration modules. When an interface previously used in a module is released, it becomes reusable for other modules only after the firewall is rebooted.

Deleting a VLAN interface will change the order of such interfaces the next time the firewall starts. If such interfaces are listed in the dynamic routing configuration or monitored via SNMP MIB-II, this behavior would change the order of interfaces, and may potentially cause the service to shut down. You are therefore strongly advised to disable any unused VLAN interfaces instead of deleting them.

On SN160(W) models, configurations that contain several VLANs included in a bridge will not be supported.

Configurations containing a bridge that includes several unprotected interfaces, and a static route leaving one of such interfaces (other than the first), are not supported.

Bird dynamic routing

In configurations that use BGP with authentication, the "source address <ip>;" directive must be used. For further information on Bird configuration, refer to the **Bird Dynamic Routing** Technical Note.

When a Bird configuration file is edited from the web administration interface, the **Apply** action will send this configuration to the firewall. If there are syntax errors, the configuration will not be applied. A warning message indicating the row numbers that contain errors will prompt the user to correct the configuration. However, if a configuration containing errors is sent to the firewall, it will be applied the next time Bird or the firewall is restarted, preventing Bird from loading correctly.

Policy-based routing

If the firewall has been reset to its factory settings (*defaultconfig*) after a migration from version 2 to version 3 then to version 4, the order in which routing will be evaluated changes and policy-based routing [PBR] will take over priority (policy-based routing > static routing > dynamic routing > … > default route). However, if the firewall has not been reset, the order of evaluation stays the same as in version 1 (static routing > dynamic routing > policy-based routing [PBR] > routing by interface > routing by load balancing > default route).

System

Support reference 78677

Cookies generated for multi-user authentication

After a new security policy is implemented on mainstream web browsers, SNS multi-user authentication no longer functions when users visit unsecured websites via HTTP.

When this occurs, an error message or a warning appears, depending on the web browser used, and is due to the fact that the authentication cookies on the proxy cannot use the "Secure" attribute together with the “SameSite” attribute in an unsecured HTTP connection.

The web browser must be manually configured to enable browsing on these websites again.

Find out more

Support reference 51251

DHCP server

Whenever the firewall receives INFORM DHCP requests from a Microsoft client, it will send its own primary DNS server to the client together with the secondary DNS server configured in the DHCP service. You are advised to disable the Web Proxy Auto-Discovery Protocol (WPAD) on Microsoft clients in order to avoid such requests.

Support reference 3120

Configuration

The NTP client on firewalls only supports synchronization with servers using version 4 of the protocol.

Restoring backups

If a configuration backup is in a version higher than the current version of the firewall, it cannot be restored. For example, a configuration backed up in 4.0.1 cannot be restored if the firewall's current version is 3.9.2.

Dynamic objects

Network objects with automatic DNS resolution (dynamic objects), for which the DNS server offers round-robin load balancing, cause the configuration of modules to be reloaded only when the current address is no longer found in responses.

DNS (FQDN) name objects

DNS name objects cannot be members of object groups.

Filter rules can only be applied to a single DNS name object. A second FQDN object or any other type of network object cannot be added as such.

DNS name objects (FQDN) cannot be used in a NAT rule Do note that no warnings will be displayed when such configurations are created.

When a DNS server is not available, the DNS name object will only contain the IPv4 and/or IPv6 address entered when it was created.

If a large number of DNS servers is entered on the firewall, or if new IP addresses relating to DNS name objects are added to the DNS server(s), several requests from the firewall may be required in order to learn all of the IP addresses associated with the object (requests at 5-minute intervals).

If the DNS servers entered on client workstations and on the firewall differ, the IP addresses received for a DNS name object may not be the same. This may cause, for example, anomalies in filtering if the DNS object is used in the filter policy.

Filter logs

When a filter rule uses load balancing (use of a router object), the destination interface listed in the filter logs may not necessarily be correct. Since filter logs are written as soon as a network packet matches the criteria of a rule, the outgoing interface will not yet be known. As such, the main gateway is systematically reported in filter logs instead.

High availability

Migration

When the passive member of a cluster is migrated from SNS v3 to SNS v4, established IPsec tunnels will be renegotiated; this is normal.

HA interaction in bridge mode and switches

In a firewall cluster configured in bridge mode, the average duration of a traffic switch was observed to be around 10 seconds. This duration is linked to the failover time of 1 second, in addition to the time that switches connected directly to the firewalls take to learn MAC addresses.

Policy-based routing

A session routed by the filter policy may be lost when a cluster is switched over.

Models

High availability based on a cluster of firewalls of differing models is not supported.

VLAN in an aggregate and HA link

Support reference 59620

VLANs belonging to an aggregate (LACP) cannot be selected as high availability links. This configuration would prevent the high availability mechanism from running on this link — the MAC address assigned to this VLAN on each firewall will therefore be 00:00:00:00:00:00.

Ethernet interface

In high availability configurations, if the nodes of the cluster communicate through an Ethernet interface, the interface has to be reserved solely for this purpose. It will not be supported as the parent interface of a virtual VLAN interface.

VLAN interfaces

In high availability configurations, the interface that is used for communications between the nodes of a cluster can be isolated in a VLAN. In this case, some of the advanced features relating to the communication of cluster members will not be available.

IPv6 support

In SNS version 4, the following are the main features that are unavailable for IPv6 traffic:

- IPv6 traffic through IPsec tunnels based on virtual IPsec interfaces (VTI),
- IPv6 address translation (NATv6),
- Application inspections (Antivirus, Antispam, URL filtering, SMTP filtering, FTP filtering and SSL filtering),
- Use of the explicit proxy,
- DNS cache,
- SSL VPN portal tunnels,
- SSL VPN tunnels,
- Kerberos authentication,
- Vulnerability management,
- Modem interfaces (especially PPPoE modems).

High availability

In cases where the firewall is in high availability and IPv6 has been enabled on it, the MAC addresses of interfaces using IPv6 (other than those in the HA link) must be defined in the

advanced properties. Since IPv6 local link addresses are derived from the MAC address, these addresses will be different, causing routing problems in the event of a switch.

Notifications

IPFIX

Events sent via the IPFIX protocol do not include either the proxy's connections or traffic sent by the firewall itself (e.g., ESP traffic for the operation of IPsec tunnels).

Activity reports

Reports are generated based on logs recorded by the firewall, which are written when connections end. As a result, connections that are always active (e.g., IPsec tunnel with translation) will not be displayed in the statistics shown in activity reports.

Whether logs are generated by the firewall depends on the type of traffic, which may not necessarily name objects the same way (*srcname* and *dstname*). In order to prevent multiple representations of the same object in reports, you are advised to give objects created in the firewall's database the same name as the one given through DNS resolution.

Intrusion prevention

GRE protocol and IPsec tunnels

Decrypting GRE traffic encapsulated in an IPsec tunnel would wrongly generate the alarm "*IP address spoofing on the IPsec interface*". This alarm must therefore be set to *Pass* for such configurations to function.

HTML analysis

Rewritten HTML code is not compatible with all web services (apt-get, Active Update) because the "Content-Length" HTTP header has been deleted.

Support reference 35960

Keep initial routing

The option that makes it possible to keep the initial routing on an interface is not compatible with features for which the intrusion prevention engine must create packets:

- reinitialization of connections when a block alarm is detected (RESET packet sent),
- SYN Proxy protection,
- protocol detection by plugins (filter rules without any protocol specified),
- rewriting of data by certain plugins such as web 2.0, FTP with NAT, SIP with NAT and SMTP protections.

NAT

H323 support

Support for address translation operations on the H323 protocol is basic, namely because it does not support NAT bypasses by gatekeepers (announcement of an address other than the connection's source or destination).

Instant messaging
NAT is not supported on instant messaging protocols

Proxies

Support reference 35328

FTP proxy
If the "Keep original source IP address" option has been enabled on the FTP proxy, reloading the filter policy would disrupt ongoing FTP transfers (uploads or downloads).

Support reference 31715

URL filtering
Separate filters cannot be used to filter users within the same URL filter policy. However, special filter rules may be applied (application inspection), with a different URL filter profile assigned to each rule.

Filtering

Outgoing interface
Filter rules that specify an out interface included in a bridge without being the first interface of such a bridge will not be applied.

Multi-user filtering
Network objects may be allowed to use multi-user authentication (several users authenticated on the same IP address) by entering the object in the list of multi-user objects (Authentication > Authentication policy).

Filter rules with a 'user@object' source (except 'any' or 'unknown@object'), with a protocol other than HTTP, do not apply to this object category. This behavior is inherent in the packet processing mechanism that the intrusion prevention engine runs. The message warning the administrator of this restriction is as follows: "This rule cannot identify a user logged on to a multi-user object."

Geolocation and public IP address reputation
Whenever a filter rule specifies geolocation conditions and public address reputation, both of these conditions must be met in order for the rule to apply.

Host reputation
If IP addresses of hosts are distributed via a DHCP server, the reputation of a host whose address may have been used by another host will be assigned to both hosts. In this case, the host's reputation may be reinitialized using the CLI command `monitor flush hostrep ip = host_ip_address`.

Authentication

Captive portal - Logout page
The captive portal's logout page works only for password-based authentication methods.

SSO Agent

The SSO agent authentication method is based on authentication events collected by Windows domain controllers. Since these events do not indicate the source of the traffic, interfaces cannot be specified in the authentication policy.

Support reference 47378

The SSO agent does not support user names containing the following special characters: " <tab> & ~ | = * < > ! ( ) \ $ % ? ' ` @ <space>. As such, the firewall will not receive connection and disconnection notifications relating to such users.

Multiple Microsoft Active Directory domains

In the context of multiple Microsoft Active Directory domains linked by an approval relationship, an Active Directory and SSO agent need to be defined in the firewall's configuration for each of these domains.

SPNEGO and Kerberos cannot be used on several Active Directory domains.

The IKEv1 protocol requires extended authentication *(XAUTH)*.

Multiple directories

Users can only authenticate on the default directory via SSL certificate and Radius.

CONNECT method

Multi-user authentication on the same machine in cookie mode does not support the CONNECT method (HTTP). This method is generally used with an explicit proxy for HTTPS connections. For this type of authentication, you are advised to use "transparent" mode. For further information, please refer to our online help at documentation.stormshield.eu, under the section "Authentication".

Users

The management of multiple LDAP directories requires authentication that specifies the authentication domain: user@domain.

The <space> character is not supported in user logins.

Logging out

Users may only log out from an authentication session using the same method used during authentication. For example, a user authenticated with the SSO agent method will not be able to log off via the authentication portal as the user would need to provide a cookie to log off, which does not exist in this case.

Temporary accounts

Whenever a temporary account is created, the firewall will automatically generate an 8-character long password. If there are global password policies that impose passwords longer than 8 characters, the creation of a temporary account would then generate an error and the account cannot be used for authentication.

In order to use temporary accounts, you will therefore need a password policy restricted to a maximum of 8 characters.

Radius

RADIUS authentication without passwords (push mode) cannot be used with an SN SSL VPN Client in version 4.0 and an SNS firewall in version 4.8.4.

Vulnerability manager

Support reference 28665

The application inventory carried out by the Vulnerability manager is based on the IP address of the machine initiating the traffic in order to index applications.

For hosts with an IP address shared among several users, for example an HTTP proxy, a TSE server or a router that dynamically translates the source, may greatly increase the load on the module. You are therefore advised to place the addresses of these machines in an exclusion list (unsupervised elements).

1000Base-LX media

When the command `ifconfig` is run, an anomaly with the Intel driver would wrongly display 1000Base-LX media as 1000Base-T media. However, the system accurately recognizes them, and their operation is not affected.

Documentation resources

Technical documentation resources are available on the Stormshield technical documentation website. We recommend that you rely on these resources to get the best results from all features in this version.

Please refer to the Stormshield Knowledge base for specific technical information that the TAC (Technical Assistance Center) has created.

Installing this version

To update your firewall to SNS version 4.8.13 LTSB, 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 section New firewall behavior.

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

Checking the compatibility of Stormshield Network client applications

If Stormshield client applications (SSO agents, SSL VPN clients and VPN clients) are used in your architecture, check their compatibility with the version of the SNS firewall that you wish to install. If any component is incompatible, these applications will stop functioning correctly.

For more information, refer to the Product life cycle guide and the Version release notes of the client applications in question.

Creating a configuration backup

Before upgrading your firewall, we recommend that you back up its current configuration.

If you have enabled Automatic configuration backup on your firewall, ensure that it is available on the configured backup server. If you do not use this feature, we recommend that you enable it.

You can create configuration backup files from the firewall's web administration interface, in **Configuration > System > Maintenance > Backup.** For more information, refer to the Backup tab section in the SNS user manual.

Updating a high availability firewall cluster

The procedure is specific and must follow the steps described in the section Updating a cluster in the technical note *High availability on SNS*.

Updating the firewall

Update paths

To update your firewall, you may need to apply one or more intermediate updates, depending on its original version:

Original version	Intermediate updates required
4.3.23 LTSB or lower	Version 4.3.24 LTSB is recommended, as the firewall's backup partition would become unusable following a direct update to the new version.
4.3.24 LTSB or higher	None

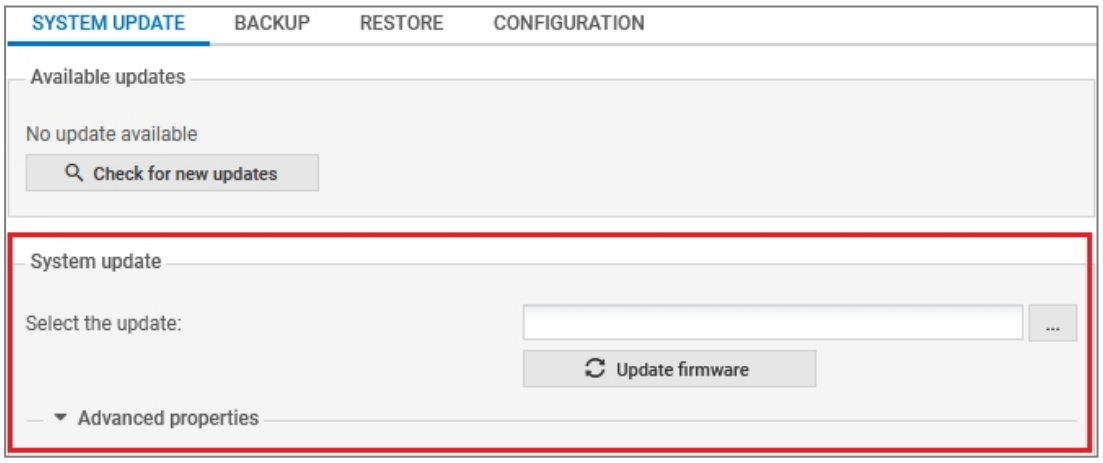
Downloading the update

1. In the firewall's web administration interface, go to **Configuration > System > Maintenance**, **System update** tab.
2. If an LTSB version update is available, it will appear under **Available updates**. Click on the link to download the update (*.maj* file).
   If the update server cannot be accessed, or if you wish to install another version, download it from your personal MyStormshield area by referring to the procedure Downloading the latest available version of a product.
   For more information on the LTSB label, refer to the Product life cycle guide.
3. Enter one of the following commands to check the integrity of the retrieved binary files:
   - Linux operating systems:
     ```
     sha256sum <filename>
     sha1sum <filename>
     ```
   - Windows operating systems:
     ```
     CertUtil -hashfile <filename> SHA256
     CertUtil -hashfile <filename> SHA1
     ```

   Next, compare the result obtained with the SHA1 hash indicated in the firewall's web administration interface or with the SHA256 hash indicated in MyStormshield.

Installing the update

1. In the firewall's web administration interface, in **Configuration** > **System** > **Maintenance**, **System update** tab, select the update file (*.maj* file) downloaded earlier.
2. Click on **Update firmware**.



3. The update will start: **do not unplug the firewall during the operation**. The firewall will restart when the update is complete.
   You will be logged out and asked to re-authenticate once the firewall has restarted.
   If an issue prevents the update from proceeding, you will be informed before the operation begins.
4. After the firewall has restarted, and to ensure that the update has been applied, log in to the web administration interface and go to the **Monitoring** > **Dashboard** tab.
   The installed SNS version is indicated in the **Version** field.

Previous versions of SNS v4

In this section, you will find new features, resolved vulnerabilities and fixes from previous versions of SNS v4.8 LTSB.

4.8.12		Resolved vulnerabilities	Bug fixes
4.8.11			Bug fixes
4.8.10	New features		Bug fixes
4.8.9	New features	Resolved vulnerabilities	Bug fixes
4.8.8			Bug fixes
4.8.7	New features	Resolved vulnerabilities	Bug fixes
4.8.6	New features		Bug fixes
4.8.5	New features		Bug fixes
4.8.4	New features	Resolved vulnerabilities	Bug fixes
4.8.3 EA	New features	Resolved vulnerabilities	Bug fixes
4.8.2 EA			Bug fixes
4.8.1 EA	New features		Bug fixes
4.7.10	New features		Bug fixes
4.7.9		Resolved vulnerabilities	Bug fixes
4.7.8			Bug fixes
4.7.7	New features	Resolved vulnerabilities	Bug fixes
4.7.6	New features	Resolved vulnerabilities	Bug fixes
4.7.5	New features	Resolved vulnerabilities	Bug fixes
4.7.4			Bug fixes
4.7.3	New features	Resolved vulnerabilities	Bug fixes
4.7.2 EA	New features	Resolved vulnerabilities	Bug fixes
4.7.1 EA	New features		Bug fixes
4.6.11	New features	Resolved vulnerabilities	Bug fixes
4.6.10	New features	Resolved vulnerabilities	Bug fixes
4.6.9	New features	Resolved vulnerabilities	Bug fixes
4.6.8	New features		Bug fixes
4.6.7	New features	Resolved vulnerabilities	Bug fixes
4.6.6		Resolved vulnerabilities	Bug fixes

4.6.5	New features		Bug fixes
4.6.4	New features	Resolved vulnerabilities	Bug fixes
4.6.3		Resolved vulnerabilities	Bug fixes
4.6.2			Bug fixes
4.6.1			Bug fixes
4.6.0	New features	Resolved vulnerabilities	Bug fixes
4.5.4	New features		Bug fixes
4.5.3	New features	Resolved vulnerabilities	Bug fixes
4.5.2	New features	Resolved vulnerabilities	Bug fixes
4.5.1	New features		Bug fixes
4.4.1	New features	Resolved vulnerabilities	Bug fixes
4.3.x LTSB		4.3 LTSB version	
4.2.14		Resolved vulnerabilities	Bug fixes
4.2.13			Bug fixes
4.2.12			Bug fixes
4.2.11	New features	Resolved vulnerabilities	Bug fixes
4.2.10		Resolved vulnerabilities	Bug fixes
4.2.9		Resolved vulnerabilities	Bug fixes
4.2.8		Resolved vulnerabilities	Bug fixes
4.2.7		Resolved vulnerabilities	Bug fixes
4.2.6			Bug fixes
4.2.5	New features	Resolved vulnerabilities	Bug fixes
4.2.4	New features	Resolved vulnerabilities	Bug fixes
4.2.2		Resolved vulnerabilities	Bug fixes
4.2.1	New features	Resolved vulnerabilities	Bug fixes
4.1.6	New features	Resolved vulnerabilities	Bug fixes
4.1.5			Bug fixes
4.1.4			Bug fixes
4.1.3	New features	Resolved vulnerabilities	Bug fixes
4.1.2			Bug fixes
4.1.1	New features	Resolved vulnerabilities	Bug fixes
4.0.3	New features	Resolved vulnerabilities	Bug fixes

4.0.2	New features	Resolved vulnerabilities	Bug fixes
4.0.1	New features	Resolved vulnerabilities	Bug fixes

Resolved vulnerabilities in SNS version 4.8.12 LTSB

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

CLI/Serverd

A low severity vulnerability was fixed in the CLI/serverd command mechanism.

Details on this vulnerability can be found on our website: https://advisories.stormshield.eu/2025-003/.

SNS version 4.8.12 LTSB bug fixes

System

Routing

Support reference 85724

A warning message now appears when the filter policy is being reloaded, to indicate that a policy-based routing rule cannot be applied, because a static or default route was not configured on the firewall.

High availability (HA)

Support reference 86211

During a switch in the cluster, TCP connections that were set up with a high Window Scale Factor (8 and above) will not resume properly with the new active firewall, which is unable to correctly manage the amount of data that it receives in these TCP connections. As a result, the firewall will block some data packets. To work around this issue, change the value of the token *RecoveryToLite*, which was added for this purpose in the section *[IPSConnection]* in the file *ConfigFiles/Protocols/tcpudp/0x*, to 1.

Do note that once this value is changed, sequence numbers will be ignored, relieving packet analysis.

Proxy - Antivirus

Support references 85841 - 86055

An issue, which could cause the firewall to freeze unexpectedly when updating the antivirus database, has been fixed.

Monitoring of power supply modules - SN-S-Series-220/320 firewalls

The absence of an additional power supply module on an SN-S-Series-220/320 model firewall no longer wrongly generates an alert indicating that a power supply module is defective.

Optimization

Support reference 85277

Physical memory is now optimally managed when the Maximum Transmission Unit (MTU) exceeds 4000 bytes.

Intrusion prevention engine

Managing connections spread out over multiple CPUs

Support reference 85947

An anomaly, which occurred when comparing sets of connections or UDP sessions spread out over several CPUs over very short intervals, has been fixed. This anomaly occasionally disconnected these sessions.

Protocol analysis

Support references 85910 - 86013

Issues have been identified and fixed in the code of the intrusion prevention engine. These issues occasionally caused packet loss.

TCP protocol

Support reference 85929

The use of the option **Enable automatic adjustment of memory allocated to data tracking** together with advanced options, such as TCP Selective ACKnowledgment (SACK), no longer wrongly causes a data queue overflow, which is described by the block alarm "TCP data queue overflow" (tcpudp:84).

PAYG VM

Support reference 85559

The host objects *enroll-sns.stormshieldcs.eu* and *accounting-sns.stormshieldcs.eu* that are used in PAYG VMs have been added to the SNS configuration.

Hardware

Profinet protocol

Support reference 86082

Profinet packets that use VLAN 0 are now correctly processed by firewalls that use the igc driver, or which are equipped with an IX port. These packets are no longer wrongly blocked.

Web administration interface

High availability - Redundant links

Support reference 86154

When creating a cluster with two HA links, the IP addresses of the secondary link are now correctly taken into account.

SNS version 4.8.11 LTSB bug fixes

System

URL/SSL filtering

Support reference 86204

Following an update to SNS version 4.8.10, if you were using a depreciated built-in URL database, or a third-party database (e.g., the Université de Toulouse database), URL and SSL filter rules could not be created or edited. This issue has been fixed. This issue did not affect the function of rules that were configured before the update to SNS version 4.8.10.

New features and enhancements in SNS version 4.8.10 LTSB

New DNS servers

Servers from the European provider dns0 are added to firewalls' host objects, under the names *dns1.dns0.eu* and *dns2.dns0.eu*. If factory settings are restored on the firewall after an update to SNS version 4.8.10, dns0 servers will be used by default. Objects corresponding to Google's DNS service will not be removed.

CLI/Serverd command - LIST

The CLI/Serverd command `LIST` now provides the full user ID (UID) in the form username@domain.

More information on the **`LIST`** command.

Changes to the hosting of the Bitdefender URL classification service

URL classification requests are now sent to a Bitdefender service that is hosted by Stormshield, instead of directly on Bitdefender infrastructure. Currently in a transitional stage until December 31, 2025, requests will switch to the service hosted by Bitdefender after five unsuccessful requests on Stormshield infrastructure.

Script for EVA firewalls in VMWare

In a VMware environment, a "user-data" script can now be set when an EVA firewall's OVF template is deployed in vSphere Client.

SNS version 4.8.10 LTSB bug fixes

System

IPsec VPN

Support reference 85864

In configurations with mobile IPsec clients, the client with the last IP address in the network will now receive DNS attributes.

Support reference 85770

In IPsec VPN configurations that use VTIs, when the configuration was reloaded with the CLI/SSH command `ennetwork -f`, traffic would sometimes be blocked in VPN tunnels. This issue has been fixed.

Support reference 85940

Previously, IKE security associations would sometimes be duplicated if peers attempted to renegotiate them at the same time, causing performance issues as a result. The calculation of when SAs are renegotiated has been modified to prevent them from being duplicated.

Multicast routing

Support reference 85809

Previously, when a default route was configured, sending multicast traffic over a bridge would cause abnormally high CPU consumption. This issue has been fixed.

EWC (Extended Web Control)

Support reference 86059

Previously, when the IP address that was configured for the object *ewc-sns.stormshieldcs.eu* did not match the address obtained through DNS resolution, the EWC URL filtering service would not automatically apply the IP address obtained by DNS resolution. This issue has been fixed.

Support reference 85849

The IP address of the object *ewc-sns.stormshieldcs.eu* has been updated in the firewall configuration.

EWC licenses are now accurately recognized, and all URL categories appear when you scroll down the list of the **URL category** column.

LDAPS server

Support reference 85766

The use of global host objects to configure an LDAPS server, as announced in SNS version 4.8.7, is now fully operational.

Web administration interface

Changing tabs in the Maintenance module

In **System > Maintenance**, a pop-up window now appears if you change tabs after having made changes, prompting you to save the new configuration.

Network objects

Support reference 86044

Previously, when you checked the usage of an object in **Configuration > Configuration > Objects > Network**, and then clicked on a **Filter - NAT** rule ID in the side panel, in some cases, a window would appear with an error message indicating that the rule did not exist, and the side panel would not function. This issue has been fixed.

Antivirus

Support reference 86144

An error message regarding the antivirus license no longer appears when you configure a rule with the antivirus. The message would wrongly indicate that you needed to subscribe to an antivirus license, although you already had one, and the antivirus was operational.

Write privileges

Support reference 86058

Previously, when a firewall was managed by SMC, and if an administrator other than the super-administrator connected to the web administration interface without going through the SMC proxy mode and requested write privileges, an error message would appear, and the user would not be able to obtain these privileges. This issue has been fixed.

New features and enhancements in SNS 4.8.9

Updates to the objects *updateX-sns.stormshieldcs.eu* and *licenceX-sns.stormshieldcs.eu*

The default IP addresses of the dynamic objects *updateX-sns.stormshieldcs.eu* and *licenceX-sns.stormshieldcs.eu* have been updated.

BACnet/IP

Services can now be blacklisted and whitelisted in **Configuration > Application protection > Protocols** for the BVLL and NPDU layers of the **BACnet/IP** protocol.

For more information, refer to the BACnet/IP section in the *SNS user manual*.

SNMP

Firewalls can now be queried with the OID (Object Identifier) 1.3.6.1.2.1.1.2 to find out their models.

A new SNMP table *snsMemUsageTable* is available with the OID 1.3.6.1.4.1.11256.1.10.10. It provides information on memory consumption in percentages.

Download MIBs from your MyStormshield personal area (authentication required): in **Downloads > Downloads > Stormshield Network Security > SNMP MIB > MIB corresponding to your SNS version.**

Resolved vulnerabilities in SNS version 4.8.9

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

Intrusion prevention engine

A moderate severity vulnerability was fixed in the intrusion prevention engine.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2024-029/.

SNS version 4.8.9 bug fixes

System

Proxy

Previously, sandboxing (Breach Fighter) files with names that were too long would cause the proxy to shut down unexpectedly. This issue has been fixed. This regression appeared in SNS version 4.8.3.

Support reference 84388

The management of proxy connections has been improved. The proxy now uses the protocol-specific connection pool before using the shared connection pool, thereby preventing errors indicating that there are too many connections, even when the maximum number of connections has not been reached.

IPsec VPN

Support reference 85641

When an IKE security association is renegotiated, authentication information is now transferred to the new security association, and the intrusion prevention engine no longer shuts down the connection.

Support reference 84803

VPN tunnels are renegotiated whenever the peer certificate is modified. This regression appeared in SNS version 4.8.0.

SSL VPN

Support references 84495/84933/85038/85081/85213

Changes have been made to the way the SSL VPN configuration is loaded, in order to reduce the number of times disks are accessed.

Certificates and PKI

Support reference 85968

Previously, when a sub-certification authority and its parent authority both had CRLDPs, only the parent authority's CRL was downloaded. This issue has been fixed, and the firewall now downloads both CRLs.

Support reference 85948

The CLI/Serverd command `PKI SCEP QUERY` now correctly factors in the *bindaddr* and *bindport* arguments, which respectively make it possible to specify a local IP address, and a specific local port for SCEP requests.

More information on the **`PKI SCEP QUERY`** command.

High availability

Support reference 85747

Now, when a cluster is connected to SMC in 3.2.3 and higher versions, or when the retrieval of information on a firewall from the cluster is forced, error logs will no longer be generated.

MIB STORMSHIELD-HA-MIB

You can now receive responses when you query the following MIB STORMSHIELD-HA-MIB tables:

- snsNodePowerSupplyTable,
- snsNodeDiskTable,
- snsNodeCpuTable,
- snsNodeFanTable.

TPM

On SMC-managed firewalls, updates to SNS in version 4.8.9 or higher are blocked when the following conditions are combined:

- The private key of the certificate that is used for communications with the SMC server is protected by the TPM,
- The firewall is in SNS version 4.8.2 or lower.

This will prevent the connection between SMC and the firewall from being lost.

TPM - IPsec VPN/SSL VPN

Support reference 86126

It is no longer necessary to resealed the TPM module when the certificates used for IPsec VPN or SSL VPN services are protected by the TPM. This behavior appeared in SNS version 4.8.7,

This situation wrongly caused the error message "Symmetric key access error" to be displayed in the dashboard.

LDAP server

Support reference 86089

The use of global host objects to configure an LDAP server, as announced in SNS version 4.8.7, is now fully operational.

Multicast routing

Support reference 85614

Previously in multicast routing configurations, if the network cable between a firewall in Last Hop Router (LHR) position and a router used as a Rendezvous Point (RP) was disconnected, or the router restarted, traffic was cut off. This issue has been fixed.

Extended Web Control (EWC)

A new implicit rule has been added to guarantee access to the Extended Web Control (EWC) server when the source address is forced with the *bindaddr* argument in a CLI/Serverd command. The addition of this implicit rule now prevents traffic from passing through the intrusion prevention engine. This new rule can be seen in **Configuration > Security policy > Implicit rules.**

Virtual machines

High availability configuration (HA) and Pay As You Go (PAYG)

Support reference 85730

The license manager in a cluster has been improved to allow the passive firewall to retrieve its license by synchronizing with the active firewall during the cluster's Pay As You Go enrollment.

Intrusion prevention engine

TCP connections

Support reference 85712

In some TCP connections that use the proxy, the intrusion prevention system would send ACK packets in loop, regardless of the reply that was received. Now, only 10 new attempts are allowed, to prevent packets from being sent in loop.

OPC UA protocol

The NodeID inspection by the OPC UA protocol analysis engine has been modified to comply with protocol specifications, and no longer causes valid OPC UA packets to be wrongly blocked.

NAT

Previously, when child connections failed, the intrusion prevention system would not correctly release ports used by the NAT. This issue has been fixed. This regression appeared in SNS version 4.8.0.

Managing users

Support reference 85999

Previously, when connections were purged, a search would be launched to link the source IP addresses of connections to users, if any. The user search is now performed when the connection is created, to prevent latency. This regression appeared in SNS version 3.4.0.

BIRD

Support reference 86033

CIDRs can once again be used instead of interface names in the BIRD configuration. This regression appeared in version 4.8.1

Support references 84495/84933/85038/85081/85213

The mechanism that updates protected addresses has been optimized to reduce the number of times disks are accessed.

Support reference 86007

On the memory buffer, a character limit on interface names would make it impossible to edit the BIRD configuration if there were too many interfaces. This issue has been fixed.

Web administration interface

TPM

Support reference 86093

In **Configuration** > **Objects** > **Certificates and PKI**, the option to initialize the TPM now no longer appears when you right-click on a certificate if your firewall is not equipped with a TPM.

SNS version 4.8.8 bug fixes

NOTE
As announced in the version 4.8.7 release notes, the fix regarding the maximum number of hosts on the SNS firewall has been removed. It will be reviewed and included in a future version.

Elastic Virtual Appliances (EVA)

Deployment

Support reference 86050

EVAs are now correctly deployed on Microsoft Hyper-V and KVM hypervisors. This regression appeared in SNS version 4.8.4.

New features and enhancements in SNS 4.8.7

IPsec VPN

Support reference 85633

Firewalls can now be forced to remain in *responder* mode throughout the IPsec VPN tunnel's lifetime, by using the token `reauth=2` in the CLI/Serverd commands `CONFIG IPSEC PEER NEW` and `CONFIG IPSEC PEER UPDATE`.

More information on the commands **`CONFIG IPSEC PEER NEW`** and **`CONFIG IPSEC PEER UPDATE`**.

Detection of obsolete hash algorithms

When certificates are signed with an obsolete hash algorithm (SHA1 and MD5), or by a CA that has been signed with an obsolete hash algorithm, they will now be flagged:

- By a warning message in the dashboard,
- By an alert in the certificate in **Configuration > Objects > Certificates and PKI**.

IPsec encryption load balancing - Firewalls equipped with 2.5 GbE network cards

The IPsec encryption load balancing mechanism is now compatible with firewalls that are equipped with 2.5 GbE network cards.

Updating non-volatile memory (NVM) on 2.5 GbE i226 network cards

Support reference 85329

The non-volatile memory (NVM) on 2.5 GbE i226 network cards has been updated.

The energy efficient Ethernet option can now be enabled. To do so, go to **Configuration > Network > Interfaces**, then to the **Advanced properties** tab of the interface that you wish to configure, and select **Enable IEEE 802.3az (EEE)**.

This update will also enable the management of interconnections between 2.5Gb/s and 100Mb/s ports.

Trusted Platform Module (TPM)

The operation of the TPM has been enhanced: the TPM module sealing policy does no longer take into account the PCR hash linked to the firewall startup sequence. The procedure to initialize the TPM has been revised and is now done with the help of a dedicated wizard in the graphic interface. In a HA cluster, the resealing of the passive firewall is made from the graphic interface of the active firewall. It is recommended to seal the TPM to take advantage of the new sealing policy.

For more information, refer to the technical note Configuring the TPM and protecting private keys in SNS firewall certificates.

BACnet/IP

Services can now be blacklisted and whitelisted in **Configuration > Application protection > Protocols** for the BVLL and NPDU layers of the **BACnet/IP** protocol.

Resolved vulnerabilities in SNS version 4.8.7

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

OpenSSL

A low severity vulnerability was fixed in OpenSSL.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2024-035/.

Multicast routing

A moderate severity vulnerability was fixed in the multicast routing mechanism.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2025-002/.

SNS version 4.8.7 bug fixes

System

Proxy

Support reference 85644

Previously, an issue would prevent proxy connections from being purged, causing them to saturate. When a proxy connection ends, it will now be automatically purged after 10 seconds.

TLS proxy

Support reference 85895/85961

When sessions are cached in the TLS proxy, they would sometimes cause an unexpected shutdown of the proxy, or excessive memory consumption. This issue has been fixed.

SSL VPN portal

Support reference 85899

The SSL VPN portal can now be accessed again when a single server is configured. This regression appeared in SNS version 4.8.0.

OpenVPN

Support reference 85690

Previously, when OpenVPN searched for a certification authority (CA) group, it used a temporary path, which could cause an error while restarting. OpenVPN now uses a permanent path.

Support reference 85842

Previously, temporary files found in the folder */var/tmp/Openvpn/* were not deleted, which could eventually prevent VPN tunnels from being set up, as the maximum number of files in a folder was reached. Such files are now deleted.

IPsec VPN

Support reference 85831

The maximum number of tasks handled by the IPsec VPN tunnel manager is valid only when Denial of Service (DoS) protection is enabled. In addition, the engine no longer needs to be restarted when the limit is reached.

Support reference 85717

When IPsec VPN tunnels that use virtual interfaces (VTIs) were deployed through SMC, they were negotiated before the end of the deployment, and were not operational. This issue has been fixed.

Certificates and PKI

The firewall now correctly verifies the content of the *basicConstraints* extension in a certification authority's (CA) certificate.

You can configure whether to import a CA for which this extension does not have a value, by using the `StrictCACheck` configuration token found in the **ConfigFiles > system** file. When the value of this token is set to 0, this means that such CAs can be imported.

Support reference 85968

Length of the additional alarm message of the *l_alarm* log

Support reference 85621

The maximum number of characters for the additional alarm message of *l_alarm* logs is now 512 characters. Ellipses are now added to the end of messages if they are truncated.

LDAPS server

Support reference 85766

Global host objects can now be used to configure an LDAPS server.

Access port to the firewall's web administration server

Support reference 85510

Now, when the access port to the firewall's web administration server is changed:

- For ports below 1024 that used to be above 1024,
- For ports above 1024 that used to be below 1024,

New configured ports will only be taken into account after firewall is restarted. A message in the upper banner in the form of a notification will indicate that the firewall must be restarted in order to apply the new configuration.

Bypass

Support reference 85358

The suspension of the connection when a firewall is powered up again with bypass mode enabled now lasts six seconds or less.

Filter - NAT

Support reference 85713

Previously, some operational filter policies in SNS 3.11 versions would stop loading in SNS version 4.8, thereby blocking traffic that passed through the firewall. The filter policy will now load, but a warning message will appear in the confirmation of the configuration in **Configuration > Security policy > Filter - NAT**.

Support reference 85677

When IPv6 is enabled, an error in the filter rule optimization mechanism would occasionally make some filter rules non-operational. This issue has been fixed.

PKI

Support reference 85798

The DN of certificates created with the command `PKI EST QUERY` and the DN of certificates created with the commands `PKI CERTIFICATE CREATE`, `PKI REQUEST CREATE` and `PKI`

`CA CREATE` are now encoded with the same encoding, which improves compatibility with special characters and third-party PKI programs.

Backup server

Support reference 86010

The name of the object that is used as the backup server can now contain up to 255 characters.

High availability (HA)

Support reference 85781/85949

Using the firewall's administration interface in a high availability cluster now no longer causes the configuration synchronization icon to blink unexpectedly. This regression appeared in SNS version 4.8.1.

High availability - Switch optimisation

Support reference 85773

Now, when **Reboot all interfaces during switchover (except HA interfaces)** is selected, only bridged interfaces will restart.

TPM

Support reference 85600

TPM-equipped firewalls that are managed by SMC now no longer lose their communications with SMC when a connecting package is re-imported.

TPM health indicator

Support reference 86012

The TPM health indicator is operational once again. This regression appeared in SNS version 4.8.5.

Memory leaks

Support reference 86009

On firewalls that are managed by SMC, a memory leak issue has been fixed. This regression appeared in SNS version 4.8.4.

Multicast routing

Support reference 85614

Previously, firewalls that received multicast traffic from a PIM router used as a RP, and which lost the connection with this router, would no longer forward traffic after reconnecting to the router. This issue has been fixed.

Virtual Pay As You Go (PAYG) machines

Support reference 85987

Since SNS version 4.8.0, virtual PAYG machines with expired licenses could no longer set up more than 1,000 connections, even after renewing their licenses. This issue has been fixed.

Intrusion prevention engine

Black list

Support reference 85782

The maximum number of blacklisted IP addresses is now applied, and can no longer be exceeded.

IPS connections

Support reference 85716/85718

When one or several sub-networks are used, the intrusion prevention system no longer blocks IPS connections when the protocol alarm "Packet for destination on the same interface" (*ip:95*) is set to **Allow**.

DCERPC protocol

Support reference 85661

Previously, when connections that were launched with the DCERPC protocol failed, the intrusion prevention system would not correctly release ports. This issue has been fixed.

Hosts

Previously, the maximum number of reserved hosts and the number of hosts in general were the same, which could affect the firewall's performance. This issue has been fixed.

Broadcast mode

Support reference 85763

The management of fragmented packets that are sent over a bridge in broadcast mode has been improved to prevent any further blocking.

Web administration interface

Inspection profile

Inspection profiles can now be renamed, copied and edited in the **General configuration** tab in **Configuration > Application protection > Inspection profiles**.

In addition, a **Profiles** tab gives an overview of the profiles and protocols that are associated with them.

Protocols - Filtering in the Sandboxing tab

The filtering feature in the **Sandboxing** tab for HTTP/SMTP/POP3 and IMAP protocols, and in the SSL protocol's certification authority grid, is now operational once again. This regression

appeared in SNS version 4.8.0.

Network traffic

Support reference 85937

IP addresses can be blacklisted once again, by right-clicking on them in **Monitoring > Network traffic**.

Printing information on temporary accounts

Support reference 85946/85962

The contents of the temporary account information print page can now be read again. This regression appeared in SNS version 4.8.0.

SSL VPN portal

Support reference 85920

Now, when **Access only to application servers** in **Configuration > VPN > SSL VPN portal** is selected, the SSL VPN remains enabled. This regression appeared in SNS version 4.8.0.

Static DHCP interface

Support reference 85534

DHCP interfaces can no longer be made static when a DNS name object or associated Firewall_ifname_router object is used in a filter or NAT rule, as this would result in preventing the firewall from loading a filter or NAT policy.

New features and enhancements in SNS 4.8.6

Power

Support reference 85754

On the following firewall models:

- SN-L-Series-2200 and SN-L-Series-3200,
- SN1100,
- SN2100,
- SN3000,
- SN3100,
- SN6100,

Information can now be obtained regarding the firewall's power supply, even when it is faulty. Such information can be accessed through the CLI / Serverd command:

```
MONITOR POWER
```

More information on the command **MONITOR POWER**.

SNS version 4.8.6 bug fixes

System

Restriction on the number of IP reputation objects

Support reference 85733

The restriction on the number of IP reputation objects, which include web services, custom web services, and IP reputation groups, has been raised and adapted to each firewall model.

GRETAP and bridges

Support reference 85957

The network configuration manager no longer shuts down unexpectedly when there is a GRETAP interface in a bridge. This regression appeared in SNS version 4.8.4.

SN-L-Series-2200 and SN-L-Series-3200 fans

Support reference 85744

The two unused fans on SN-L-Series-2200 and SN-L-Series-3200 models are no longer detected by monitoring, and no longer wrongly raise alerts.

Sequence of modules on SN-XL-Series-5200 and SN-XL-Series-6200 models

Modules on SN-XL-Series-5200 and SN-XL-Series-6200 models are once again in the right order (1 to 8 from left to right, and from top to bottom). This regression appeared in SNS version 4.8.3.

SSO Agent authentication method

Support reference 85959/85960

An issue with getting users and groups, which occurs when the SSO Agent authentication method is used, has been fixed. This regression appeared in SNS version 4.8.0.

Web administration interface

Certificates and PKI

Support reference 85731

In **Configuration > Objects > Certificates and PKI**, the certificate type is now taken into account if the user has manually indicated it. This regression appeared in SNS version 4.7.0.

Administrators - *admin* account

The private and public keys of the super administrator account (*admin* account) are now exported in a text format file (.txt), and no longer in CSV format.

New groups or users

Support reference 85813

Now in **Configuration > Users > Users**, newly created users and groups appear when existing users and groups are being configured.

New features and enhancements in SNS 4.8.5

Zero trust network access (ZTNA) - Verifying the compliance of client workstations

In **Configuration > VPN > SSL VPN > Client workstation verification (ZTNA)**, the option **Allow tunnels to be set up for Linux or Mac Stormshield SSL VPN client**s was added. If this option is selected, specific Windows criteria will not be applied to client workstations with a Linux or Mac Stormshield SSL VPN client (soon available).

Expired Certificate Revocation Lists (CRL)

Support reference 85690

A warning message now appears in the Message widget in the dashboard to warn the user when the configuration allows SSL VPN tunnels to be set up with an expired CRL.

Default NTP key type

When NTP keys are added, the default key type is now SHA256.

IPsec VPN

Support reference 85633

The *IkeDeleteDelay* configuration token can now be directly configured using the CLI/serverd command:

```
CONFIG IPSEC UPDATE
```

This token makes it possible to set an interval (in seconds) between a request to shut down an IKE security association and its actual shutdown during a reauthentication. The token accepts values between 0 and 20.

SSL VPN

Now, if compression is enabled on the firewall, a window appears when you access the **SSL VPN** module informing you that you are strongly advised to disable compression for security reasons.

You can view and change the compression status (enabled or disabled) using the CLI / serverd commands:

```
CONFIG OPENVPN SHOW
CONFIG OPENVPN UPDATE compress=<0|1>
```

More information on **CONFIG OPENVPN SHOW** and **CONFIG OPENVPN UPDATE** commands

SNS version 4.8.5 bug fixes

System

SSL VPN

Users can once again set up their VPN tunnels by authenticating with external services (push mode) when the *HostChecking* function is enabled. This regression appeared in SNS version 4.8.3.

High availability (HA)

Support reference 85551

The passive firewall no longer attempts to launch CRL retrieval tasks. This is because the active firewall regularly performs this task, and CRLs that are retrieved in this way are immediately synchronized with the passive firewall.

Monitoring Certificate Revocation List (CRL) validity dates

Support reference 85624

The mechanism that monitors CRL validity dates no longer raises minor alerts for CRLs with an initial lifetime that is shorter than 24 hours. Such alarms used to be raised every 3 hours.

Web services

Support reference 85853

When a web service group already contains a web service, using the search bar to add a new web service now no longer deletes the existing web service. This regression appeared in SNS version 4.8.0.

Command-based configuration server (serverd)

Support reference 84546/84672

When **Logs - Audit logs** modules are opened, the command-based configuration server (serverd) would sometimes unexpectedly close. This issue has been fixed.

Alarms

Support reference 85900

Alarms indicating the recovery of certain health indicators were systematically generated whenever the firewall started, even in the absence of any anomalies. This regression, which first appeared in SNS version 4.8.4, has been fixed.

Backup

On firewalls that are equipped with a TPM, the wording of the error message that appears when the wrong TPM password is entered during a backup has been changed for better clarity.

Intrusion prevention engine

BIRD dynamic routing

Support reference 84579

Only the routes that BIRD sends to the kernel are now retrieved in the table of protected network addresses.

Web administration interface

IPsec VPN

In **Monitoring** > **Monitoring** > **IPSec VPN tunnels**, the values of the **Status** and **Role** fields in the **Security association** section are now correctly translated.

TCP-UDP protocol

In **Configuration** > **Application protection** > **Protocols** > **TCP-UDP**, the **Support** section is now correctly translated.

Return routes

Support reference 858111

In **Configuration** > **Network** > **Routing** > **IPv4/IPv6 return routes**, USB/Ethernet (4G modem) interfaces can no longer be selected in the **Interface** field of the return route.

Administrator

Support reference 85474

The **Domain name** field can now be left empty, or *none* can be entered as a value when creating or changing an administrator.

Time object

Support reference 85805

When a custom time object is created, edited or used, it no longer raises an error. This regression appeared in SNS version 4.8.0.

New features and enhancements in SNS 4.8.4

Certificates and PKI

In **Objects > Certificates and PKI**, the **Hashes** section has been renamed **Details**, and three new fields have been added: **Key type**, **Key size** and **Extended Key Usage**.

Firewalls now check whether the certificate associated with a CRL is indeed authorized to sign CRLs (presence of the "crlSign" *keyUsage* value).

Filter - NAT

When a filter rule in the Filter - NAT module is edited, an information icon appears in the Action tab of the editing window, warning the user that a log level other than the standard level may cause log saturation.

Sandboxing

Support reference 85532

Enhancements have been applied to reduce the number of files sent for sandboxing, and to limit the risk of overcrowding the waiting lsit.

Encryption

Enhancements have been applied to the cryptographic function verification binary file (*cryptotest*). When this utility is run in verbose mode, it now includes a verification of the TPM, if the firewall has one. In the resulting *verbose* file, the utility shows the name of the user who launched the verification.

Several error messages have also been reworded for clarity.

Monitoring

SNMP alerts (traps) are now generated whenever the following health indicators return to normal operating conditions:

- Fan status,
- Temperatures of processors and their percentage of use,
- Memory consumption,
- Disk status,
- R.A.I.D status,
- Certificate status,
- CRL status,
- TPM status,
- Password status.

Resolved vulnerabilities in SNS version 4.8.4

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

Firewall administrator management

Support reference 85555

A low severity vulnerability was fixed in the firewall administrator management mechanism.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2024-028.

ClamAV antivirus

A moderate severity vulnerability was fixed in ClamAV.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2024-034.

SNS version 4.8.4 bug fixes

System

Proxies

Support references 85568 - 85625 - 85701

Issues in the SSL proxy, which could cause traffic using the proxy to unexpectedly be blocked, have been fixed.

POP3 proxy - Antispam and/or antivirus

Support reference 81432

During the antivirus and/or antispam analysis, the POP3 proxy would wrongly detect batch e-mail processing (pipelining) and inappropriately fragment messages. This issue has been fixed.

IPsec VPN

Support reference 85786

When the IPsec configuration on a firewall in a version lower than SNS 4.8 uses a phase 2 profile with the PFS field set to *None*, upgrading such a firewall to SNS version 4.8 will no longer wrongly delete the corresponding token in the IPsec configuration file. This anomaly prevented the setup of IPsec tunnels that use this phase 2 profile.

Phase 1 of an IPsec tunnel is now automatically deleted when the only associated phase 2 has been deleted following an idle timeout.

Support reference 85721

After deploying via SMC an IPsec configuration that:

- Uses virtual interfaces (VTIs),
- Has a peer defined in **Do not initiate the tunnel (ResponderOnly)** mode.

Attempts to set up the tunnel will no longer cause the firewall to unexpectedly freeze.

Support reference 85676

High availability configurations that handle a heavy volume of traffic now have better stability. This prevents the IPsec tunnel manager from shutting down unexpectedly.

SSL VPN

Users can once again set up their VPN tunnels by authenticating with external services (push mode). This regression appeared in SNS version 4.8.3.

Imported certification authority

Support reference 85740

CRLs from imported certification authorities can now be deleted.

Importing certificates

Support reference 85731

Certificates in .cert and .crt format are now identified as PEM certificates during import. They were previously considered P12 certificates, which subsequently caused errors.

SN160(W)/SN210(W)/SN310 model firewalls

Support reference 84495 - 84933 - 85038 - 85081 - 85213

Changes have been made to reduce the frequency of disk access to the configuration file *ConfigFiles/Openvpn/openvpn*, as this would cause SN160(W)/SN210(W)/SN310 model firewalls to unexpectedly restart.

High availability (HA) - CRL

Support reference 85558

CRLs that originate from global CAs are now synchronized every 60 minutes between the active and passive firewalls.

Support reference 85553

CRLs that are retrieved by the active firewall are now immediately synchronized with the passive firewall. Previously, these synchronizations occurred only every 60 minutes. As such, if a switch occurred in the cluster during this time frame, the new active firewall would not necessarily know all the CRLs, and could then prevent IPsec tunnels from being set up, for example.

Audit logs

Support reference 85563

When the firewall is restarted within five minutes after a filter is created in **Logs - Audit logs > All logs**, the filter will no longer be deleted.

Bird dynamic routing

Support reference 85756

The BIRD dynamic routing engine now no longer restarts in loop when it is in verbose mode. This regression appeared in SNS version 4.8.0.

Support reference 85271

When the OSPF protocol is used in dynamic routing, the size of the *socket* buffer has been increased to stop packet loss.

Support reference 85755

BIRD v1 and BIRD v2 can no longer be started at the same time.

Virtual interfaces

Support reference 85669

In GRE tunnels, whenever the size of a packet exceeded the MTU, the ICMP response packet would not indicate the right MTU value. This issue has been fixed.

Backup partition

Support reference 85527

On firewalls:

- In SNS version 4.8,
- With a backup partition in SNS version 4.3.23 LTSB or lower,

Malfunctions may occur when the backup partition is used. Firewalls cannot be updated to SNS version 4.8 if the backup partition is not in SNS version 4.3.24 LTSB or higher.

Filter - NAT

Support references 68445 - 70036 - 85660

The right value now appears in the *#set_tos* column when filter rules are exported to a CSV file, and new columns have been added for QoS and synproxy.

Wi-Fi interfaces

Support reference 84615

The network configuration manager no longer shuts down unexpectedly during startup when the Wi-Fi interface has the country code for Jamaica.

CLI/serverd commands

Support reference 85797

When the CLI/serverd `SYSTEM UPDATE UPLOAD` command was used without arguments, serverd would shut down unexpectedly, and log the user out of the console. This issue has been fixed.

Intrusion prevention engine

Memory

In some cases, the firewall would unexpectedly freeze while processing errors due to memory shortage. This issue has been fixed.

Web administration interface

Applications and protections

Support reference 85779

The index of a protocol profile that was edited in the *Applications and protections* module once again matches the index configured in the security profiles. This regression appeared in SNS version 4.8.0.

QoS

Support reference 85458

The list of prohibited characters in QoS queue names is now the same as the list in the section **Allowed or prohibited names** in the *SNS user guide.*

New features and enhancements in SNS 4.8.3 EA

IPsec VPN - SN-XL-Series-5200 and SN-XL-Series-6200 models

Some settings in the IPsec tunnel manager have been changed to significantly increase the number of IPsec tunnels that can be set up simultaneously on SN-XL-Series-5200 and SN-XL-Series-6200 model firewalls.

Packet management has also been enhanced to increase IPsec throughput.

High availability - System report (sysinfo)

The *sysinfo* command that is run on the active firewall in a cluster can now generate and retrieve the system report on the passive firewall.

This operation can be performed by using the CLI/Serverd command `SYSTEM INFORMATION [fwserial=(<serial>|passive|active|local)]` by selecting the parameter *passive*.

More information on the **SYSTEM INFORMATION** command.

SSL proxy

The SSL proxy now supports these two encryption suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

Changing the *admin* account password through SSH

In console mode on the firewall using an SSH connection, the old password of the *admin* account now has to be entered in order to change it.

Resolved vulnerabilities in SNS version 4.8.3 EA

RADIUS authentication - Captive portal and web administration interface

A moderate severity vulnerability was fixed in the RADIUS protocol.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2024-030.

SSH access - Multi-user mode

A low severity vulnerability was fixed in multi-user SSH access mode.

Details on this vulnerability can be found on our website
https://advisories.stormshield.eu/2024-016.

CLI/serverd commands

Several low severity vulnerabilities were fixed in the CLI/serverd command mechanism.

Details on these vulnerabilities can be found on our website:
https://advisories.stormshield.eu/2024-024.

SNS version 4.8.3 EA bug fixes

System

GRE/GRETAP encapsulation in an IPsec tunnel

Support reference 85626

GRE/GRETAP packets can once again be encapsulated in an IPsec tunnel. This regression appeared in SNS version 4.7.3.

High availability and dynamic objects

Support reference 81176

During a switch in a cluster, the dynamic object database now appears immediately on the newly active firewall. Previously, this step would require several minutes and block network traffic that uses these objects during this time frame.

SD-WAN

Priority calculations have been revised to prevent issues with gateways being too frequently switched. As such, there is no longer any status scale between downgraded gateways. The gateway selection mechanism now follows these rules:

- Active gateways take priority over downgraded gateways,
- Main gateways take priority over backup gateways.

Filtering and NAT - Web services

Support reference 85539

When a custom web service with a name that is exactly 20 characters long is used in a filter rule, the rule would not function.

A warning message will then appear in the **Messages** widget on the **Dashboard**. The message indicates the filter policy and rule number that caused the error.

To work around the issue:

1. Change the name of the web service (to fewer than 20 characters) in the CSV import file that was initially used,
2. Import this file once again in **Objects** > **Web services** > **Import custom services** tab,
3. Modify the filter rule to use the new name of the web service.

Configuration

Support reference 85434

The number of IP addresses defined on an interface can no longer exceed the limit allowed on the firewall. Do note that previously, excess IP addresses were not enabled, but no error message was displayed when the configuration was validated. This anomaly has been fixed.

The command `system ping host` no longer wrongly raises the error "Format error" when it is used with a fully qualified domain name (FQDN) as an argument. This regression appeared in SNS version 4.8.

When a firewall with a defective disk is updated, the configuration file folder will no longer be deleted, as this would make the firewall unreachable.

Support reference 85725

In the factory settings on firewalls in SNS version 4.8.3 EA or higher, downgrades to a lower firmware version are now allowed once again by default.

This behavior can be edited exclusively through the CLI/Serverd command: `SYSTEM UPDATE DOWNGRADE state=off` to prohibit downgrading to a lower version, based on the following rules:

- Virtual firewalls: downgrading to any version lower than the current version is prohibited.
- Physical firewalls: downgrading to any version lower than the versions of the main partition and the backup partition is prohibited.

WARNING
The CLI/serverd command `SYSTEM UPDATE DOWNGRADE state=on` can no longer be used to allow downgrades to lower firmware versions once again.

System report (*sysinfo*)

Support reference 85593

Information regarding verbose mode being enabled is now correctly reported in the system report.

Intel interfaces using the *igc* kernel module

Support reference 85486

When a VLAN is configured on an interface that uses the *igc* kernel module, and the interface is included in a bridge with the option **Keep initial routing/Keep VLAN IDs** enabled, packets from other crossing VLANs will no longer be wrongly rejected.

This applies to the following firewall models and firewalls equipped with these network modules:

- Firewalls: SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-720 and SN-M-Series-920.
- Modules: NA-EX-CARD-8x2_5G-C (8 x 2.5 Gb copper Ethernet) and NC-1-8x2_5G-C (8 x 2.5 Gb copper Ethernet).

Virtual EVA firewalls deployed on the Linux KVM hypervisor

Support reference 85635

On virtual EVA firewalls deployed on the Linux KVM hypervisor, the firewall now correctly applies the status of a disconnected interface in the hypervisor's configuration. This issue distorted the calculation of the high availability (HA) quality factor.

Support reference 85722

When a virtual machine is suddenly shut down while being configured on a KVM hypervisor, it no longer corrupts some of its configuration files.

IP reputation - Storage devices

Support references 84495 - 84933 - 85038 - 85081 - 85213

The mechanism that opens IP reputation metadata files has been modified to restrict the number of times the storage device can be accessed. In some cases, when the disk is accessed too often, the firewall would unexpectedly restart.

Host reputation

Support reference 85635

An issue with access privileges, which prevented the host reputation manager from functioning correctly, has been fixed. This regression appeared in SNS version 4.7.

Telemetry

A memory leak issue has been fixed in the telemetry manager.

Monitoring - Telemetry

The telemetry service is no longer wrongly displayed as shut down in the dashboard.

Authentication – TS Agent

Support reference 85401

Authentication through the TS Agent method would logically fail for users whose logins contained a space (prohibited character), but no error message would appear to indicate the issue. An alarm is now raised when this occurs. The list of prohibited characters is also provided in addition to information about the alarm.

SN160(W)/SN210(W)/SN310 model firewalls

Support references 84495 - 84933 - 85038 - 85081 - 85213

Changes have been made to the mechanism that calculates Security and System indicators, in order to reduce the number of times disks are accessed. The mechanism would previously cause SN160(W)/SN210(W)/SN310 model firewalls to unexpectedly restart.

Syslog - TLS 1.3

Support reference 85579

When logs are sent via syslog by using TLS 1.3, the operation would no longer fail when the certificate that was used for authentication was signed by a subordinate CA.

IPsec VPN - Certificate-based authentication

Support reference 85607

After the IPsec tunnel manager was updated, the firewall would wrongly interpret the SerialNumber as the Surname, thereby preventing IPsec tunnels from being set up. This issue has been fixed.

IPsec VPN in DR mode - UDP encapsulation and dynamic NAT

Support reference 85629

Tunnels configured in DR mode, on which UDP encapsulation has been enabled, and the source port of one peer's traffic is translated (dynamic NAT), can now be correctly set up: the remote firewall detects the need to encapsulate the traffic in UDP.

Automatic backups - Custom server

On firewalls that use automatic configuration backups to a custom server that was authenticated with a certificate, clicking on **Check usage** in **Objects** > **Certificates and PKI** after having selected this certificate now correctly indicates that this certificate is being used in the firewall configuration. Likewise, this certificate cannot be deleted without raising an error.

Quality of Service (QoS)

Support reference 85590

An issue that could cause the firewall to freeze when a QoS queue was deleted has been fixed.

Partition size allocated to reports

Changes to the size of the partition dedicated to storing reports were no longer applied. This regression, which first appeared in SNS version 4.8.0, has been fixed.

Web administration interface

SSL VPN

Support reference 85663

The certificate presented by the server or by the SSL VPN client can now be changed again. This regression appeared in SNS version 4.8.1.

Captive portal

Support reference 84750

The interface *sslvpn_udp* can now be selected in the captive portal's profiles. Users who present from this interface can therefore access the captive portal now.

Microsoft Active Directory external LDAP directory

Support reference 85764

After a new external LDAP directory such as Microsoft Active Directory is created, users found in this directory are now correctly shown again in the user module. This regression appeared in SNS version 4.8.0.

SNS version 4.8.2 EA bug fixes

System

High availability - System backup mechanism on the backup partition

In a high availability (HA) configuration, an issue in the system backup mechanism on the backup partition (dumproot) resulted in a failure to update the passive firewall. This regression appeared in SNS version 4.8.1 EA.

Telemetry

An issue with competing access, which could cause the telemetry manager to shut down unexpectedly, has been fixed.

New features and enhancements in SNS 4.8.1 EA

Zero trust network access (ZTNA) - Verifying the compliance of client workstations

In order to implement zero trust network access (ZTNA), you can now configure policies to check the compliance of client workstations that set up SSL VPN tunnels with the SNS firewall. When it is enabled, client workstations or users that do not comply with the criteria in the policy will not be able to set up SSL VPN tunnels with the SNS firewall.

Only the Stormshield SSL VPN client in version 4.0 and higher is compatible with the client workstation compliance check feature. Every workstation in the corporate network has to therefore use the Stormshield SSL VPN client in version 4.0 and higher when the feature is enabled.

However, there is an option to allow incompatible SSL VPN clients to set up SSL VPN tunnels. This option should be used only on a temporary basis, for example to gradually upgrade a pool of SSL VPN clients to a compatible version.

For more information on implementing zero trust network access (ZTNA) and the client workstation compliance check feature, refer to the technical note **Configuring and using the SSL VPN on SNS firewalls**.

Multifactor authentication in IKEv2 via EAP

As of SNS version 4.8, multifactor authentication is supported for IKEv2-based mobile tunnels via EAP (Extensible Authentication Protocol).

Multifactor authentication can also be provided in the following ways:

- EAP-Generic Token Card: the mobile peer must present a login/password pair,
- Certificate and EAP-Generic Token Card: the mobile peer must present a certificate and login/password pair,
- For increased security, you can use time-based one-time passwords (TOTP) with the EAP methods above, by using the Stormshield TOTP solution.

Note:

- EAP methods are not compatible with the *Diffusion Restreinte* (DR) mode, and IKEv1-based tunnels that need to use Xauth for multifactor authentication,
- The Stormshield VPN Exclusive client in version 7.4 and higher needs to be used in order to set up IKEv2-based mobile tunnels via EAP.

For more information, refer to the technical note **Mobile IKEv2 IPsec VPN - EAP and Certificate Authentication**.

Protection against post-quantum attacks

SNS version 4.8 begins with the option of setting post-quantum pre-shared keys (PPK) for peers using the IKEv2 protocol with certificate-based authentication.

The computing power of quantum computers will very likely allow it to decrypt keys that were negotiated using the Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH) methods, therefore endangering the security of the IKEv2 protocol.

Malicious users would now be able to carry out "store now, decrypt later" attacks, by intercepting IPsec communications and storing them in order to decrypt them later using a quantum computer.

Clients who wish to protect themselves against such attacks can use SNS version 4.8, which follows the recommendations in RFC 8784, and therefore makes it possible to use PPKs meant to protect data encryption key exchanges. Do note that to be effective, these PPKs must have a sufficiently high entropy (minimum 256 bits according to RFC).

To find out more on the use of PPKs for the IKEv2 protocol, refer to RFC 8784.

For more information on how to configure PPKs, refer to the IPsec VPN sections Peers and Identification in the *SNS user guide*.

Dynamic multicast routing

The multicast routing configuration panel has been simplified and a monitoring panel has been added.

Dynamic multicast routing is no longer an early-access feature.

More information on dynamic multicast routing.

BIRD dynamic routing

Version 2 added, version 1 obsolete

Version 2 of the BIRD dynamic routing engine is now available. In the **Dynamic routing** configuration panel, you can:

- Enable a version of **BIRD** in a new **General** tab,
- Prepare a migration to the new version of the engine in the **BIRD v2** tab before activating it. When editing the BIRD v2 configuration, you can display the BIRD v1 configuration in a panel on the right.

Version 1 of the BIRD dynamic routing engine is now considered obsolete, and a message in the **Messages** widget on the dashboard informs you of this.

For more information, refer to the technical note BIRD v2 dynamic routing.

SNS firewall pools managed by an SMC server

If your SNS firewall pool is managed by an SMC server, it is not possible to manage dynamic routing on your firewalls in 4.8.1 EA versions and higher from SMC in version 3.6 and below. The SNS firewall will then reject the deployment of the configuration by the SMC server, and report an error.

For more information on SMC versions, refer to the section New features and enhancements in SMC 3.6 in the *SMC version release notes*.

New 4 *bypass* (NA-EX-CARD-BP-8xG-C) hardware module

As of SNS version 4.8, the hardware module **NA-EX-CARD-BP- 8xG-C** is supported, making it possible to have 1 to 4 *bypass* modules on the following firewall models:

- SN-M-Series-520,
- SN-M-Series-720,
- SN-M-Series-920,
- SN1100 (only in the left extension slot).

More information on how to operate and enable the bypass feature.

Support for new firewall models

As of SNS version 4.8, the following firewall models are supported:

- SN-L-Series-2200 and SN-L-Series-3200,
- SN-XL-Series-5200 and SN-XL-Series-6200.

Protection against denial of service attacks (DoS and DDoS)

Protection against DoS and DDoS attacks has been strengthened. These improvements apply to UDP and TCP, and you can set new detection thresholds in inspection profiles.

More information on configuring protections against TCP-UDP denial of service attacks.

Increased security

Hardening of the system

Hardening the system in SNS version 4.8 increases the security of the product.

NTP keys - Selection of algorithms added

You can now select SHA1, SHA256, SHA384, SHA512 and AES-CBC-128 as algorithms in the configuration of NTP keys.

More information on date and time settings.

Analyzing extension mechanisms for DNS (EDNS)

The intrusion prevention system now includes the analysis of extension mechanisms for DNS (EDNS), which are described in RFC 6891.

New restrictions for certificates used in TLS connections

The following certificates can no longer be used during TLS connections on the SNS firewall:

- Certificates containing the restriction "*CA:TRUE*" (it has to be "*CA:FALSE*"),
- Certificates containing the XKU "*OCSP Server*".

SNMPv3 agent - Obsolete algorithms

Authentication algorithm MD5 and encryption algorithms DES and SHA1, which the SNMPv3 agent uses, are obsolete and will be removed in a future SNS firmware release. An indication that these algorithms are obsolete now appears in the SNMPv3 agent configuration panel.

Now you can change the algorithms that the SNMPv3 agent uses with the following CLI/Serverd commands:

```
CONFIG SNMP ACCESS USERV3 username=<username> authtype=SHA256
authpass=<passphrase> privtype=AES privpass=<passphrase>
CONFIG SNMP ACTIVATE
```

After an update to SNS version 4.8, *DES* will be selected by default as the encryption algorithm if no algorithm has been selected earlier. Do note that password encryption remains disabled as long as no password has been entered in the field associated with the encryption algorithm.

Internal LDAP directory - Obsolete algorithms

Password hash algorithms MD5, SMD5, SHA, SSHA, SHA256, SHA384 and SHA512, which the Internal LDAP directory uses, are obsolete and will be removed in a future SNS firmware release. An indication that these algorithms are obsolete now appears in the advanced configuration panel of the internal LDAP directory.

SSL VPN portal - Obsolete features

The SSL VPN portal feature is obsolete and will be deleted in a future SNS firmware version. An indication that this feature is obsolete now appears in the SSL VPN portal configuration panel.

Removal of the OSCAR protocol scan

Considered obsolete since SNS version 4.6.9, the OSCAR protocol scan has been removed from the SNS firewall. Do note that this protocol scan was automatically disabled when the firewall was updated to SNS version 4.7.2 EA.

RSA key size

The size of RSA keys generated on the SNS firewall is now 4096 bits by default.

Integration into various environments

Link aggregation - Support for *broadcast* mode

As of SNS version 4.8, aggregates can be configured in broadcast mode directly in the firewall administration interface, under an aggregate's **Advanced configuration** tab. This mode, which was introduced in SNS version 4.7.5, could only be configured by modifying a configuration file on the firewall.

More information on configuring an aggregate.

Multiple Diffie-Hellman (DH) groups

Several DH groups can now be specified in the same IKE and IPsec encryption profile to facilitate the migration of peers to a single group.

More information on encryption profiles.

HTTP and SSL proxies - WebSocket support

As of SNS version 4.8, HTTP and SSL proxies support WebSocket. Do note that in the IPS profiles of incoming connections (such as *IPS_00*), the alarm *http:301* blocks WebSocket support by default (*Block* action).

IPsec DR - OCSP

In an IPsec DR context, and in line with RFC 4806, peers can now validate the certificate of the remote gateway that is presented when the IKEv2 tunnel is being set up, but without exposing the OCSP server.

This configuration is possible only by using the CLI/Serverd command set:

```
CONFIG IPSEC OCSP
```

More information on the CONFIG IPSEC OCSP commands.

Asynchronous authentication

The SNS firewall's authentication mechanism can now manage user authentication asynchronously, thereby enabling better integration of third-party multifactor authentication solutions.

SD-WAN

SD-WAN route management has been improved.

OpenVPN - Source address of TCP requests

The source IP address of TCP requests sent by OpenVPN can now be specified. This parameter can only be modified through the following CLI/Serverd commands:

```
CONFIG OPENVPN UPDATE BindAddr=(<firewall_ip_object>|"")
CONFIG OPENVPN ACTIVATE
```

When OpenVPN is the only engine on the SNS firewall that listens on the TCP port, performance has been shown to improve.

More information on the CONFIG OPENVPN commands.

Sending data to sekoia.io servers

If you have a subscription allowing you to send data to sekoia.io servers, you can now configure the authentication key provided by Sekoia (*Intake Key*) in the Syslog profile configuration.

More information on configuring Syslog profiles.

TLS 1.3 traffic - Analysis of server certificates

You can now specify the source IP address of requests sent by the intrusion prevention engine when it attempts to retrieve the server certificate for every TLS 1.3 traffic stream that passes through the firewall so that any potential security flaws relating to this certificate can be analyzed.

You can apply this configuration with the following CLI/serverd command:

```
CONFIG PROTOCOL SSL PROFILE IPS CONFIG index=<slot>
TLSServerCertBindAddr=<host>
```

More information on the CONFIG PROTOCOL SSL PROFILE IPS CONFIG command.

Changes to performance

TLS 1.3 - Cache added when certificate retrieval fails

When a request fails to get a certificate, the requests that follow now receive an instant response with the help of a cache. This cache is enabled by default and keeps data for 6 hours.

You can customize the cache duration (in seconds) using the CLI/Serverd command:

```
CONFIG PROTOCOL SSL COMMON IPS CONFIG TLSCertCacheErrorTTL=<60..259200>
```

More information on the CONFIG PROTOCOL SSL COMMON IPS CONFIG command.

You can disable this cache by setting the value of the *TLSServerCertCacheError* configuration token to *0* in the *ConfigFiles/Protocols/ssl/* file of the policy that is used.

Improved user experience

Initial configuration via USB key - New operations

Certificates and their CRLs can now be imported during the initial configuration of an SNS firewall via USB key, by using the *certimport* and *crlimport* operations.

For more information on these operations, refer to the sections certimport operation and crlimport operation in the technical note *Initial configuration via USB key*.

Stealth mode

When stealth mode is disabled, a link that directs to the IP protocol settings now appears in the warning in the **Messages** widget on the dashboard.

More information on IP protocol furtive mode.

URL objects module

The URL object configuration panel has been improved. **Category groups** are now configured in the **Certificate names (CN)** tab.

More information on configuring URL objects.

Disabling the button to reset the firewall to its factory settings (*defaultconfig*).

Support reference 84328

The button to reset the firewall to its factory settings can now be disabled, to prevent the firewall's configuration from being accidentally reset.

The button can only be disabled by using the following CLI/SSH command:

```
setconf /usr/Firewall/ConfigFiles/system DefaultConfig EnableButton 0 &&
nhup hardwared
```

Application inspection profiles

Only global inspection profiles, named IPS_00, IPS_01... by default, are now displayed in the **Application Protection** > **Inspection Profiles** module.

Better visibility of certain information

Alarm messages relating to high availability or hardware failures

Alarm messages relating to high availability or hardware failures now show:

- The SNS firewall's serial number,
- The system node name, if it has been defined.

MIB STORMSHIELD-PROPERTY-MIB - OID snsSystemNodeName added

The OID *snsSystemNodeName* has been added to the MIB **STORMSHIELD-PROPERTY-MIB**, which returns a value corresponding to the system node name.

Configuration restoration alarms

A system alarm appears on the dashboard when a configuration is restored using a CLI/Serverd command or via a USB key, indicating:

- Whether the restoration is full or partial,
- The results of the file content hash (SHA2 method),
- The user that ran the CLI/Serverd command.

sfctl command - Using the name of an object in filters

For easier troubleshooting, you can now use the name of an object in filters when the *sfctl* command is used with the parameters *-H type=modifier*.

More information on the **sfctl command**.

Addition of filters for the commands MONITOR GETSA, GETSPD and GETIKESA

Filters can now be used in the following IPsec VPN monitoring CLI/Serverd commands:

```
MONITOR GETSA Global=<0|1> List=<full|light>
MONITOR GETIKESA Global=<0|1> List=<full|light>
MONITOR GETSPD Global=<0|1> List=<full|light>
```

For more information on these commands, refer to the sections **MONITOR GETSA**, **MONITOR GETIKESA** and **MONITOR GETSPD** of the *CLI/Serverd commands reference guide*.

Firewall hardware activity monitoring mechanism (watchdog)

The management of the firewall hardware activity monitoring mechanism (watchdog) has been enhanced. Real-time monitors are now shown in a tooltip, and the configuration of the monitoring mechanism can now be managed in the administration interface of virtual firewalls.

SNMP agent

The value assigned to the *sysname* field presented by the SNMP agent now follows this order:

1. The value specified in the **Name** field in the **Configuration of MIB-II information** (**Notifications** > **SNMP agent** module),
2. Otherwise, the value specified in the **Firewall name** field (**System** > **Configuration** > **General configuration** tab),
3. Otherwise, the serial number of the firewall.

Telemetry

Status of the telemetry service

The status of the telemetry service is now shown in the dashboard.

New data reported by the telemetry service

The telemetry service in SNS version 4.8 now reports new data:

- Data regarding the use of the IPsec VPN module:
  - Number of site-to-site or mobile tunnels configured and enabled in the active IPsec policy,
  - Number of tunnels configured in IKEv1 or IKEv2 in the active IPsec policy,
  - Number of times each authentication method was used in tunnels configured in the active IPsec policy,
  - Maximum number of site-to-site or mobile tunnels connected,
- Data regarding the TLS 1.3 cache:
  - Total number of entries in the TLS 1.3 cache,
  - Total number of times the cache was purged when it was saturated,
  - Number of failed certificate requests.

By sending such data, which is completely anonymous, you will be helping Stormshield to refine the dimensions and restrictions on future hardware platforms and SNS versions.

 More information on telemetry services.

SNS 4.8.1 EA bug fixes

System

IPsec VPN

A mechanism that verifies and restricts the number of requests to set up IPsec tunnels has been added to avoid saturating the queue.

SSL VPN

Support reference 84391

The option to prevent users from setting up more than one SSL tunnel (option that can be enabled using the CLI/Serverd command `CONFIG OPENVPN UPDATE ForceOneTunnelPerUser=1`) did not function when the presented user name included its domain name (e.g., john.doe@acme.com). This anomaly has been fixed.

More information on the command **CONFIG OPENVPN UPDATE**.

Authentication policy

Support references 79493 - 84414 - 84713

The **Block** action has been removed from the choice of values allowed for the default authentication method:

- Choosing this value would wrongly block users during authentication on the SSL VPN when **Internet** was selected as the source object in the SSL VPN authentication rule.
- Choosing this value together with an authentication rule that specified the use of the default authentication method would not block corresponding authentication traffic,
- Choosing this value without setting any specific authentication rule in the authentication policy would wrongly allow authentication on the firewall via SSH.

Dashboard - Health indicators

Support reference 85392

The health indicator of certificates found in the **Dashboard** module no longer wrongly raises alarms when a CA has a lifetime longer than 68 years. This behavior persists on SN160(W), SN210(W) and SN310 firewall models.

High availability

Support reference 84512

In high availability configurations, when users view web administration interface modules without making any changes, the icon indicating the need to synchronize the configuration between members of the cluster no longer appears by mistake.

SN-S-Series-220/320 and SN-M-Series-520 firewalls - Starting on 4G modems and USB keys

When a user's network configuration does not make any reference to a 4G modem/USB key, starting SN-S-Series-220/320 or SN-M-Series-520 model firewalls with a 4G modem/USB key

connected to one of the the firewall's USB ports will no longer fail while the startup partition is being selected.

SD-WAN monitoring

Support reference 84874

Router objects used in static routes are now effectively monitored.

Web services

Support references 84662 - 84444

When custom web services are imported from a CSV file, quotation marks framing a comment in the source file are no longer supported.

Dynamic DNS

Support references 84480 - 85395

Performing the following actions in this sequence now correctly enables the dynamic DNS service on the firewall:

1. Configure a dynamic DNS profile.
2. Apply changes.
3. Enable the profile.
4. Apply changes.

Running a firewall shutdown/restart command and system backup simultaneously on the backup partition

When a shutdown (HALT)/restart(REBOOT) command was run at the same time as a system backup on the backup partition (*dumproot*), the system backup could fail, and even corrupt the backup partition.

Improvements have been made to prevent this situation. Now:

- When a *dumproot* is in progress, the firewall's shutdown/reboot mechanism is put on active standby and will start only when the *dumproot* ends,
- When a shutdown/restart command is launched on the firewall, *dumproot* will not launch and generates a system event.

Virtual firewalls - Prohibiting a downgrade to an earlier firmware version

On virtual firewalls, the configuration token that makes it possible to prohibit downgrades to an earlier firmware version is now correctly applied.

This function can be managed exclusively through the CLI/Serverd command:

```
SYSTEM UPDATE DOWNGRADE state=<on|off>
```

 More information on the command **SYSTEM UPDATE DOWNGRADE**.

CLI/serverd commands - CONFIG LDAP UPDATE HELP

Support reference 85301

The CLI/serverd command `CONFIG LDAP UPDATE HELP` no longer wrongly references the *realbindaddr* parameter instead of *bindaddr*.

More information on the command `CONFIG LDAP UPDATE`.

Logs

Support reference 84831

When the log manager is unavailable, it no longer wrongly causes the intrusion prevention engine to freeze temporarily.

CRL verification

Support reference 85402

The mechanism that verifies CRLs now correctly performs DNS requests again when three or more DNS servers are specified on the firewall. Do note, however, that this anomaly did not apply to CRL downloads.

SNMPv3 traps - securityName

Support reference 85435

When an SNMPv3 trap for the **securityName** event is configured with values containing spaces, the *Error in format* serverd error is no longer returned.

IPFIX collector - Network connection logs

Support reference 85054

Network connection logs were not sent to the IPFIX collector whenever they originated from a filter policy rule with **Firewall** as its inspection level. This issue has been fixed.

Network

GRE/GRETAP

Support references 84395 - 76800

GRE/GRETAP tunnels based on an outgoing interface that has been configured in DHCP are now set up correctly after the firewall has been restarted, or when this source interface changes its IP address.

BIRD version 1 dynamic routing

Support reference 85322

Issues that occurred while adding a default route on a protected interface, or when an interface with a default route added by BIRD is changed from public to protected, have been fixed. These issues would wrongly add the network *0.0.0.0/0* or *0.0.0.0/32* to the table of protected addresses. This would then wrongly raise an alarm regarding an IP spoofing attempt, which could cause legitimate traffic to be dropped.

Elastic Virtual Appliances (EVA)

Hypervisor based on Qemu 8.1 and higher versions

Support reference 76697

EVAs in SNS version 4.7 and higher are now correctly deployed on hypervisors that are based on Qemu 8.1 and higher versions.

Web administration interface

Changing the super-administrator password (*admin* account)

Support reference 85581

When the *admin* account password is being changed through the web administration interface, quotation marks are once again not accepted. A regression that allowed these characters appeared in SNS version 4.7.1 EA.

External LDAP - Showing the list of users

Support reference 85287

When an external directory held more than 1000 users, the list of users would not appear in the **Users** module on the SNS firewall. This issue has been fixed, and the directory's first 500 users now appear by default in the list of users.

Filter - NAT

Support reference 76697

Changes to an interface's IP address are now correctly applied in the tooltip showing this object's properties in the **Filtering and NAT** module.

IPsec VPN monitoring

Support reference 85292

After these operations have been performed:

1. Create and apply a filter on the columns of the **IPsec VPN monitoring** module.
2. Quit the module and go back to it.

The filter is shown as being active, and is now correctly applied.

Audit logs

Support reference 85292

In **Logs - Audit logs > All logs**, log type can now be added as a filter criterion.

In the details of a log, scrolling over the flag of a source or destination country now correctly displays the "Country name (Country code)" information.

DHCP IPv6 address

Support reference 85336

When an interface in IPv6 is configured via DHCP, all tooltips that are supposed to specify this address no longer wrongly show the interface's IPv4 address.

IPv6 address - Monitoring users connected via the TS agent method

When IPv6 is disabled on the SNS firewall, the module that monitors users connected via the TS agent method no longer wrongly presents in the *IP address* column the IPv6 address of the host associated with the user known to the Windows server.

Gateways in a router object

Support reference 85211

Changes to the name of a gateway belonging to router object are now correctly applied in the list of gateways that make up the router object.

Authentication - Radius

Support reference 85128

In the configuration of the Radius authentication method, the icon located at the end of the **Pre-shared key** field on the server and backup server (if any) was partially hidden. This anomaly has been fixed.

Version 4.8.0 not published

Version 4.8.0 is not available to the public.

New features and enhancements in SNS 4.7.10

Sandboxing

Support reference 85532

Enhancements have been applied to reduce the number of files sent for sandboxing, and to limit the risk of overcrowding the waiting lsit.

SNS version 4.7.10 bug fixes

System

Proxies

Support references 85568 - 85625 - 85701

Issues in the SSL proxy that could cause the firewall to freeze unexpectedly have been fixed.

POP3 proxy - Antispam and/or antivirus

Support reference 81432

During the antivirus and/or antispam analysis, the POP3 proxy would wrongly detect batch e-mail processing (pipelining) and inappropriately fragment messages. This issue has been fixed.

IPsec VPN

Support reference 85676

High availability configurations that handle a heavy volume of traffic now have better stability. This prevents the IPsec tunnel manager from shutting down unexpectedly.

Support reference 85721

After deploying via SMC an IPsec configuration that:

- Uses virtual interfaces (VTIs),
- Has a peer defined in **Do not initiate the tunnel (ResponderOnly)** mode.

Attempts to set up the tunnel will no longer cause the firewall to unexpectedly freeze.

SN160(W)/SN210(W)/SN310 model firewalls

Support reference 84495 - 84933 - 85038 - 85081 - 85213

Changes have been made to reduce the frequency of disk access to the configuration file *ConfigFiles/Openvpn/openvpn*, as this would cause SN160(W)/SN210(W)/SN310 model firewalls to unexpectedly restart.

High availability (HA) - CRL

Support reference 85558

CRLs that originate from global CAs are now synchronized every 60 minutes between the active and passive firewalls.

Support reference 85553

CRLs that are retrieved by the active firewall are now immediately synchronized with the passive firewall. Previously, these synchronizations occurred only every 60 minutes. As such, if a switch occurred in the cluster during this time frame, the new active firewall would not necessarily know all the CRLs, and could then prevent IPsec tunnels from being set up, for example.

Audit logs

Support reference 85563

When the firewall is restarted within five minutes after a filter is created in **Logs - Audit logs > All logs**, the filter will no longer be deleted.

Importing certificates

Support reference 85731

Certificates in .cert and .crt format are now identified as PEM certificates during import. They were previously considered P12 certificates, which subsequently caused errors.

Intrusion prevention engine

Memory

In some cases, the firewall would unexpectedly freeze while processing errors due to memory shortage. This issue has been fixed.

Web administration interface

QoS

Support reference 85458

The list of prohibited characters in QoS queue names is now the same as the list in the section *Allowed or prohibited names* in the SNS user guide.

Resolved vulnerabilities in SNS 4.7.9

RADIUS authentication - Captive portal and web administration interface

A moderate severity vulnerability was fixed in the RADIUS protocol.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2024-030.

CLI/serverd commands

Several low severity vulnerabilities were fixed in the CLI/serverd command mechanism.

Details on these vulnerabilities can be found on our website:
https://advisories.stormshield.eu/2024-024.

SNS 4.7.9 bug fixes

System

GRE/GRETAP encapsulation in an IPsec tunnel

Support reference 85626

GRE/GRETAP packets can once again be encapsulated in an IPsec tunnel. This regression appeared in SNS version 4.7.3.

Configuration

Support reference 85434

The number of IP addresses defined on an interface can no longer exceed the limit allowed on the firewall. Do note that previously, excess IP addresses were not enabled, but no error message was displayed when the configuration was validated. This anomaly has been fixed.

When a firewall with a defective disk is updated, the configuration file folder will no longer be deleted, as this would make the firewall unreachable.

SD-WAN

Priority calculations have been revised to prevent issues with gateways being too frequently switched. As such, there is no longer any status scale between downgraded gateways. The gateway selection mechanism now follows these rules:

- Active gateways take priority over downgraded gateways,
- Main gateways take priority over backup gateways.

System report (*sysinfo*)

Support reference 85593

Information regarding verbose mode being enabled is now correctly reported in the system report.

IP reputation - Storage devices

Support references 84495 - 84933 - 85038 - 85081 - 85213

The mechanism that opens IP reputation metadata files has been modified to restrict the number of times the storage device can be accessed. In some cases, when the disk is accessed too often, the firewall would unexpectedly restart.

Host reputation

Support reference 85635

An issue with access privileges, which prevented the host reputation manager from functioning correctly, has been fixed. This regression appeared in SNS version 4.7.

Intel interfaces using the igc kernel module

Support reference 85486

When a VLAN is configured on an interface that uses the igc kernel module, and the interface is included in a bridge with the option **Keep initial routing/Keep VLAN IDs** enabled, packets from other crossing VLANs will no longer be wrongly rejected.

This applies to the following firewall models and firewalls equipped with these network modules:

- Firewalls: SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-720 and SN-M-Series-920.
- Modules: NA-EX-CARD-8x2_5G-C (8 x 2.5 Gb copper Ethernet) and NC-1-8x2_5G-C (8 x 2.5 Gb copper Ethernet).

Telemetry

A memory leak issue has been fixed in the telemetry manager.

An issue with competing access, which could cause the telemetry manager to shut down unexpectedly, has been fixed.

Authentication – TS Agent

Support reference 85401

Authentication through the TS Agent method would logically fail for users whose logins contained a space (prohibited character), but no error message would appear to indicate the issue. An alarm is now raised when this occurs. The list of prohibited characters is also provided in addition to information about the alarm.

SN160(W)/SN210(W)/SN310 model firewalls

Support references 84495 - 84933 - 85038 - 85081 - 85213

Changes have been made to the mechanism that calculates Security and System indicators, in order to reduce the number of times disks are accessed. The mechanism would previously cause SN160(W)/SN210(W)/SN310 model firewalls to unexpectedly restart.

Syslog - TLS 1.3

Support reference 85579

When logs are sent via syslog by using TLS 1.3, the operation would no longer fail when the certificate that was used for authentication was signed by a subordinate CA.

IPsec VPN - Certificate-based authentication

Support reference 85607

After the IPsec tunnel manager was updated, the firewall would wrongly interpret the SerialNumber as the Surname, thereby preventing IPsec tunnels from being set up. This issue has been fixed.

IPsec VPN in DR mode - UDP encapsulation and dynamic NAT

Support reference 85629

Tunnels configured in DR mode, on which UDP encapsulation has been enabled, and the source port of one peer's traffic is translated (dynamic NAT), can now be correctly set up: the remote firewall detects the need to encapsulate the traffic in UDP.

Automatic backups - Custom server

On firewalls that use automatic configuration backups to a custom server that was authenticated with a certificate, clicking on **Check usage** in **Objects** > **Certificates and PKI** after having selected this certificate now correctly indicates that this certificate is being used in the firewall configuration. Likewise, this certificate cannot be deleted without raising an error.

Quality of Service (QoS)

Support reference 85590

An issue that could cause the firewall to freeze when a QoS queue was deleted has been fixed.

Virtual EVA firewalls deployed on the Linux KVM hypervisor

Support reference 85635

On virtual EVA firewalls deployed on the Linux KVM hypervisor, the firewall now correctly applies the status of a disconnected interface in the hypervisor's configuration. This issue distorted the calculation of the high availability (HA) quality factor.

Support reference 85722

When a virtual machine is suddenly shut down while being configured on a KVM hypervisor, it no longer corrupts some of its configuration files.

Filtering and NAT - Web services

Support reference 85539

When a custom web service with a name that is exactly 20 characters long is used in a filter rule, the rule would not function.

A warning message will then appear in the **Messages** widget on the **Dashboard**. The message indicates the filter policy and rule number that caused the error.

To work around the issue:

1. Change the name of the web service (to fewer than 20 characters) in the CSV import file that was initially used,
2. Import this file once again in **Objects** > **Web services** > **Import custom services** tab,
3. Modify the filter rule to use the new name of the web service.

Network

BIRD dynamic routing

Support reference 85322

Issues that occurred while adding a default route on a protected interface, or when an interface switches from public to protected with a default route added by BIRD, have been fixed.

These issues would wrongly add the network *0.0.0.0/0* or *0.0.0.0/32* to the table of protected addresses. This would then wrongly raise an alarm regarding an IP spoofing attempt, which could cause legitimate traffic to be dropped.

Web administration interface

Captive portal

Support reference 84750

The interface *sslvpn_udp* can now be selected in the captive portal's profiles. Its absence prevented users who presented from this interface from accessing the captive portal.

SNS 4.7.8 bug fixes

System

High availability - System backup mechanism on the backup partition
In high availability configurations, an issue in the system backup mechanism on the backup partition (*dumproot*) caused the passive firewall update to fail. This regression appeared in SNS version 4.7.7.

New features and enhancements in SNS 4.7.7

Sandboxing

Support reference 85532

Only files that have been classified as archive, Office document, executable, PDF and Java files will now be sandboxed to reduce the load on the service. Files that have been classified as other or unknown files will no longer be analyzed.

Resolved vulnerabilities in SNS 4.7.7

CLI/serverd commands

Several vulnerabilities were fixed in the CLI/serverd command mechanism.

Details on these vulnerabilities can be found on our website: https://advisories.stormshield.eu/2024-024.

SNS 4.7.7 bug fixes

System

IPsec VPN

Support references 84983 - 85253 - 85452

In addition to the fix implemented in version 4.7.1 EA for IPsec VPN, the mechanism that reloads rules in the IPsec VPN policy has been patched, and the firewall's routing engine no longer shuts down unexpectedly when some configurations remain unchanged.

Dynamic objects

Support reference 85397

Enhancements have been made to prevent the proxy from reloading systematically when dynamic objects (FQDNs or hosts) are used in a filter or address translation mechanism on the SNS firewall, as this would slow down connections.

System backup mechanism on the backup partition

Support reference 85390

The system backup mechanism on the backup partition (*dumproot*) has been enhanced. When a backup is abruptly stopped, the main partition is no longer corrupted, and the firewall no longer restarts for an indefinite number of times. Only the backup partition remains damaged, and a new backup has to be launched to restore the status of both partitions.

Intrusion prevention engine

Connection management

Support reference 85370

An issue in the way connections are managed by the intrusion prevention engine, which could cause the firewall to restart unexpectedly, has been fixed.

Maximum size of COTP packets

Support reference 85353

The maximum value of COTP packets is now 65535 bytes. The previous maximum value was 4096 bytes, and could wrongly raise the block alarm *Possible attack on capacity* (ip:91).

Web administration interface

Application protection - HTTP protocol

Support reference 85588

The **Apply the NAT rule on scanned traffic** option is now available again in the HTTP protocol analysis global configuration. This regression appeared in SNS version 4.7.1.

New features and enhancements in SNS 4.7.6

Hardware alarm messages

Alarm messages relating to hardware failures now show the serial number of the firewall.

Resolved vulnerabilities in SNS 4.7.6

WI-Fi network

A high severity vulnerability was fixed in the Wi-Fi network management mechanism.

Details on this vulnerability can be found on our website: https://advisories.stormshield.eu/2024-018.

SN-S-Series-220/320 model firewalls

A low severity vulnerability has been fixed in the serial port management mechanism on SN-S-Series-220/320 model firewalls.

Details on this vulnerability can be found on our website: https://advisories.stormshield.eu/2024-017.

SNS 4.7.6 bug fixes

NOTE
As announced in the version 4.6.7 release notes, the fix regarding the label length of a web service that is compatible with a traffic block rule (support reference 84722) has been removed. It will be reviewed and included in a future version.

System

High availability - Automatic backups

Support reference 84782

In high availability configurations where automatic configuration backups in Stormshield's cloud have been enabled, when the roles of firewalls in the cluster were regularly switched more often than the configured frequency of automatic backups (7 days by default), these backups would never be activated. This issue has been fixed.

High availability - Updating the passive firewall when the backup partition is being copied

Support reference 85390

The mechanism that updates the passive firewall in a cluster has been enhanced to better manage partition backups on it. With these improvements, backups will no longer be abruptly stopped, as this may corrupt the partitions on the passive firewall.

High availability - Updating the active firewall in command line

Support reference 84997

In high availability configurations, attempts to update the active firewall using the command `SYSTEM UPDATE UPLOAD fwserial=active` no longer fail, and no longer present the error "Source and destination firewalls are the same".

More information on the command **SYSTEM UPDATE UPLOAD**.

High availability - TOTP authentication

Support reference 85575

In high availability configurations, the database of users who have completed their TOTP enrollment can now be effectively synchronized once again. This regression appeared in SNS version 4.7.1 EA.

VLAN in a link aggregate

The network configuration checker no longer takes into account the case used in names of VLANs that are part of an aggregate. Case sensitivity used to prevent the network configuration from being reloaded.

Running an automatic update and system backup simultaneously on the backup partition

Support reference 84744

When an automatic update (*autoupdate*) was run at the same time as a system backup on the backup partition (*dumproot*), the system backup could fail, especially when the firewall was managed via SMC.

Improvements have been made to prevent this situation. Now:

- When a *dumproot* is in progress, the *autoupdate* mechanism is put on active standby and will start only when the *dumproot* ends,
- When an *autoupdate* is in progress, the *dumproot* will not launch and generates a system event.

IPsec VPN

Support reference 85603

When a traffic endpoint has an IP address found in the network of a tunnel's destination hosts, attempting to set up such an IPsec tunnel no longer causes the firewall to freeze unexpectedly. This regression appeared in SNS version 4.7.3.

IPsec VPN - *Diffusion Restreinte* (DR) mode

Support reference 85507

For configurations in DR mode, if a peer in a site-to-site tunnel has enabled the **Do not initiate the tunnel (Responder only)** option, the tunnel will no longer be prevented from setting up correctly.

Static multicast routing in VLANs

Support reference 85562

An issue regarding random static disruptions to routed multicast traffic in VLANs has been fixed.

Deployments via SMC - Competing access

Support reference 84003

Issues regarding competing access have been fixed so that attempts to deploy configurations via SMC will no longer be unexpectedly blocked.

GRETAP

Support reference 85384

In configurations that use CPU load balancing for encryption on SN-M-Series-520 and SN-M-Series-720 model firewalls, an issue regarding packets being rejected in a GRETAP tunnel's key renegotiation phase has been fixed.

Intrusion prevention engine

SD-WAN

Support reference 85436

When a static route uses a router object with gateways that are all attached to protected interfaces, gateways in such router objects are now correctly switched in the table of protected addresses in the intrusion prevention engine.

Web administration interface

SMC - Removal of TPM protection

Support reference 85594

TPM protection can now be removed from the key used in communications with the SMC server via the firewall's web administration interface.

New features and enhancements in SNS 4.7.5

Link aggregation - Support for *broadcast* mode

As of SNS version 4.7.5, packets can be sent and received over all links included in an aggregate (*broadcast* mode).

Do note that the device that is connected to the firewall's aggregated interfaces in *broadcast* mode must support such communications:

- Either by having one active interface and a second passive interface (main/backup),
- Or by ignoring frames that originate from one of the links.

This configuration can only be created by directly editing the firewall's **ConfigFiles/network** network configuration file, and setting the *Laggmode* token to *broadcast*, then confirming changes with the *ennetwork* command.

DCERPC protocol

UUIDs have been added to the list of known UUIDs in the DCERPC protocol analysis engine:

- '0b6edbfa-4a24-4fc6-8a23-942b1eca65d1': 'IRPCAsyncNotify',
- '1c1c45ee-4395-11d2-b60b-00104b703efd': 'IwbemFetchSmartEnum',
- '3dde7c30-165d-11d1-ab8f-00805f14db40': 'BackupKey',
- '423ec01e-2e35-11d2-b604-00104b703efd': 'IwbemWCOSmartEnum',
- 'ae33069b-a2a8-46ee-a235-ddfd339be281': 'IRPCRemoteObject',
- 'd4781cd6-e5d3-44df-ad94-930efe48a887': 'IwbemLoginClientID',
- 'f6beaff7-1e19-4fbb-9f8f-b89e2018337c': 'Eventlog'.

TLS protocol

Support reference 85368

TLS protocol analyses can now be disabled after setting up the connection, to improve performance when high volumes of traffic must be processed.

High availability - System node name

When a system node name has been set for members of a cluster, the name will be specified in brackets in the following selection fields:

- **Configuration** > **System update** tab > **System update**: **Select the firewall to update** field,
- **Configuration** > **Configuration** tab > **Maintenance** > **Reboot/Shut down the firewall** field,
- **Configuration** > **Configuration** tab > **High availability** > **Make a firewall stay active**.

Resolved vulnerabilities in SNS 4.7.5

Email Notifications

A low severity vulnerability was fixed in the e-mail notification module.

Details on this vulnerability can be found on our website: https://advisories.stormshield.eu/2024-007.

OpenSSL

A moderate severity vulnerability was fixed in OpenSSL.

Details on this vulnerability can be found on our website: https://advisories.stormshield.eu/2024-011.

SNS 4.7.5 bug fixes

System

SSL VPN

Support reference 85485

In SSL VPN connections with certificate authentication, HTML tags or quote characters (") in the user name are now correctly processed.

Support reference 85485

SSL VPN tunnel monitoring no longer displays lines of 'UNDEF" users, which correspond to connection attempts. Now, only established connections will be displayed in the monitoring module.

EVA on Microsoft Azure

Support reference 85325

The file integrity verification mechanism has been adapted to no longer wrongly raise alarms for EVAs deployed on the Microsoft Azure platform. These alarms, which affected in particular the host's boot loader or libraries specific to this platform, disrupted how Microsoft Azure managed and backed up virtual machines.

Disk access

Support references 84495 - 84933 - 85038 - 85081 - 85213 - 84626 - 85197

Improvements have been made to restrict the number of times the disk is accessed. In some cases, when the disk is accessed too often, SN160(W), SN210(W) and SN310 model firewalls would unexpectedly restart.

High availability - SCTP associations

Support reference 82047

When SCTP associations were not synchronized when the filter policy was reloaded on the active firewall, it could create an inconsistency within the cluster: SCTP connections that were deleted on the active firewall when the filter policy was reloaded were still considered active on the passive firewall. This issue has been fixed.

Certificate Check

Support reference 85206

The mechanism that retrieves and verifies TLS server certificates now takes into account the trusted CAs added by the administrator account. These CAs are stored in a different directory from the one used for storing downloaded CAs.

URL/SSL filtering - Extended Web Control (EWC) - Miscellaneous category

URLs that have been recognized by the URL category provider in the EWC solution, and which do not belong to any predefined category, are now classified under the **Miscellaneous** category, and no longer under **Unknown**.

URL/SSL filtering - Extended Web Control (EWC) - Warning messages

Improvements have been made in cases when an unknown URL category was used in the configuration of the SNS firewall after the migration of a security policy to the new EWC URL database:

- Warning messages no longer appear in the menu on the left, in front of the names of the **Filter - NAT**, **URL filtering** and **SSL filtering** modules, when the unknown categories are in a disabled rule or in an inactive policy,
- In warning messages, the output from the CLI/Serverd command *MONITOR MISC* now indicates the unknown categories and the policy in question.

SNMP agent

Support reference 83679

An error was fixed in the value returned by the OID *1.3.6.1.2.1.1.7*. This value is now 76, corresponding to a device that provides services on OSI layers 3, 4 and 7. Previously, the value returned was 72.

GRETAP

Support reference 85417

An anomaly in the formatting of outgoing GRETAP packets (several extra bytes at the beginning of the packet) was fixed. This anomaly, which appeared in versions 4.3.16 LTSB and 4.6.1, made GRETAP network captures more difficult to analyze but did not in any way affect the proper operation of GRETAP communications.

Certificates and PKI - TPM

Support reference 85431

When a certificate that was initially protected by the TPM was renewed via EST or SCEP, the TPM protection would not be maintained. It will now be automatically applied after the renewal operation.

Authentication - TS agent

Support reference 85403

Users who were already authenticated via the TS Agent method were unable to connect to the firewall's web administration interface. This issue has been fixed.

Intrusion prevention engine

TCP connections - Proxy

Support references 84867 - 85385

At the end of a TCP packet exchange, if the server or client ignores the connection shutdown packet that the peer sends, the firewall's intrusion prevention engine will stop wrongly sends ACK or FIN/ACK packets in loop.

SMTP protocol

Support reference 84220

SMTP connections that are initiated by a client that sent a *STARTTLS* command before the *EHLO* command will no longer be wrongly blocked when they generate the "Invalid SMTP protocol" alarm.

SMTP - UTF-8 support

Support reference 83791

The SMTP protocol analysis engine no longer wrongly blocks UTF-8 characters in SMTP traffic when the server specifically allows them through the option SMTPUTF8.

Vulnerability management

Support reference 85526

The size of the cache that contains vulnerabilities detected on the firewall's client hosts has been increased to prevent the intrusion prevention engine from consuming too much CPU when the cache is full. The size of this cache has therefore been increased from 128 to 2048 possible entries.

Web services

Support reference 85539

Whenever a web service with a name longer than 19 characters was used in a filter rule, the filter policy would not be applied and a warning in the dashboard would ask the administrator to correct the name of the service in question.

Web administration interface

Filtering - Authentication rule - Web objects

Support reference 85447

When an authentication rule has been defined in the filter policy, web objects can no longer be created or edited directly from this rule. This operation would make the web administration interface unstable.

Certificates and PKI

Support reference 85388

The use of certification authorities (CAs) with names that contain an apostrophe can now be verified.

IPsec VPN

Support reference 85442

After importing a CA and several identities that it has signed, only the certificate of the first imported identity could be used to create an IPsec peer. Attempts to select another imported certificate would fail. This issue has been fixed.

Host object with automatic DNS resolution

Support reference 85515

The "/" character is no longer allowed at the end of the name of host objects that have been configured in automatic DNS resolution.

Authentication - TOTP

Support reference 85473

Changing the **Number of valid codes before and after current code** no longer wrongly displays the window indicating that the TOTP database must be reinitialized and that the TOTP enrollment procedure has to be repeated for all users.

SNS 4.7.4 bug fixes

System

SSL VPN and LZ4 compression

Support reference 85547

When LZ4 compression for SSL VPN is activated, the update to version 4.7.4 no longer prevents the SSL VPN tunnel manager from starting. This regression appeared in SNS version 4.7.3 after the update of the OpenVPN component.

New features and enhancements in SNS 4.7.3

Monitoring

An information message now appears in the **Monitoring** module and via the CLI/Serverd command `MONITOR MISC` when custom settings have been implemented on the firewall (presence of customized configuration files in some firewall folders).

More information on the CLI/Serverd command **MONITOR MISC**.

Synchronization of the object database with DNS servers

It is now possible to indicate the source IP address of DNS requests sent for the automatic synchronization of the object database. The traffic from these queries can then be routed through a VPN tunnel. This new parameter can only be modified through the CLI/Serverd commands:

```
CONFIG OBJECT SYNC UPDATE bindaddr=<host>
CONFIG OBJECT SYNC ACTIVATE
```

To reset the configuration to the default settings, use the commands:

```
CONFIG OBJECT SYNC UPDATE bindaddr=
CONFIG OBJECT SYNC ACTIVATE
```

More information on the CLI/Serverd command **CONFIG OBJECT SYNC UPDATE**.

Certificates and PKI

Support reference 83969

When a certificate raises an alarm (revoked certificate, expired certificates, etc.), a message indicating the reason for the alarm will now appear when scrolling over the certificate in question in the **Certificates and PKI** module.

Monitoring - Dashboard - Certificates

Support reference 85412

When a certificate raises an alarm, especially when the TPM (Trusted Platform Module) has been initialized and all certificates found on the firewall are not protected by the TPM, scrolling over the **Certificates** health indicator in the **Dashboard** module will now display a message indicating the reason for the alarm.

Resolved vulnerabilities in SNS 4.7.3

OpenSSH

A high severity vulnerability was fixed in OpenSSH.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2023-035.

SN-S-Series-220/320 and SN-M-Series-520 firewalls

A high severity vulnerability was fixed in the microcode of SN-S-Series-220/320 and SN-M-Series-520 firewall processors.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2024-004.

OpenVPN

A moderate severity vulnerability was fixed in OpenVPN.

Details on this vulnerability can be found on our website:
https://advisories.stormshield.eu/2024-005.

SNS 4.7.3 bug fixes

System

Proxies

Support references 85428 - 85495 - 85491

Issues regarding proxies that were unexpectedly blocked when configurations were reloaded have been corrected.

Network captures with *tcpdump* on a *usbus* interface

Support references 85083 - 85313

Launching a network capture with *tcpdump* on a *usbus* interface no longer causes the firewall to unexpectedly restart.

Elastic Virtual Appliances (EVA)

Support reference 85273

On an EVA virtual firewall, limiting the number of CPUs when hyperthreading is enabled no longer causes the firewall to restart unexpectedly.

QoS

Support reference 85019

Due to an issue that occurs when a CBQ queue used as an acknowledgment queue (ACK) in a filter rule is deleted, the firewall may sometimes unexpectedly restart. This issue has been fixed.

Switching to a lower SNS version

Support reference 85247

When a firewall switches to a lower SNS version without being reset to its factory configuration (*defaultconfig*), attempts to display the list of available alarms no longer cause the intrusion prevention engine and the command-based configuration server (serverd) to unexpectedly restart.

NAT

Support reference 84819

An issue has been fixed in the NAT manager. This issue would wrongly fill the table of translated ports used for traffic that requires child connections (e.g. FTP, RTSP and others). As a result, this would prevent child connections from being created, and disrupt the traffic in question.

Filter - NAT

Support references 85357 - 85376

In filter rules that use a set of network objects, one of which is linked to a disabled DHCP-configured interface, restarting the firewall will no longer wrongly enable the "(1) *Block all*" filter rule. This regression appeared in SNS version 4.7.0.

Support reference 85239

In a situation such as the following:

- The firewall has a bridge that groups several interfaces. On this bridge:
  - Traffic from one of the bridge interfaces to an interface outside the bridge is allowed by a filter rule in *Firewall* mode,
  - Traffic from another bridge interface to the same interface outside the bridge is blocked by another filter rule.
- A connection has been established between a client host and the server through the first rule,
- An infected host or an intrusion probe located on the same interface as the server sent a *reset* packet with the same references as the established connection (source/destination addresses and source/destination ports).

Although the packet from the infected host or intrusion probe was rightly blocked, the source interface of the client host was wrongly modified and its established connection with the server was shut down. This issue has been fixed.

Connection to the web administration interface with the *admin* account

Support references 85266 - 85309 - 85349 - 85437 - 85494

Under certain circumstances, attempts to connect to the web administration interface with the *admin* account would fail and cause the command-based configuration server (serverd) to unexpectedly restart. This issue has been fixed.

High availability (HA)

Support references 77890 - 83274

On a high availability firewall that has switched roles several times in the cluster, some packets would take the wrong return route while presenting the IP address of the right return route. This issue, which caused the shutdown of the traffic in question, has been fixed.

High availability - Synchronization of certificate revocation lists (CRL)

CRLs that were retrieved on the active firewall are now synchronized with the passive firewall once again. This regression appeared in SNS version 4.7.2 and raised an alarm whenever a CRL on the passive firewall expired.

E-mail alerts

Support references 84511 - 82823

When e-mails are sent by the firewall via an encrypted connection with an SMTP server over TLS, reloading the configuration of the e-mail sending service would wrongly cause a switch to unencrypted mode, which could result in a connection failure between the firewall and the SMTP server. This issue has been fixed.

Memory leaks

Support reference 85363

Memory leak issues have been fixed in the firewall's configuration engine and its SNMP agent management engine.

IPsec VPN

Packets that were encrypted in the first IPsec tunnel were no longer allowed to then pass through a second tunnel that was set up via virtual IPSec interfaces. This regression, which first appeared in SNS v4, has been fixed.

IPsec monitoring

Support reference 85399

Monitoring of SAs (security associations) no longer fails when the peer contains an IP address range.

Internal LDAP directory

Support reference 84495

Optimizations have been made to prevent the systematic reloading of the LDAP directory manager when some modifications are applied.

DHCP interface

Support reference 85305

When the media speed of a DHCP-configured interface is manually modified, it no longer loses its IP address.

BIRD dynamic routing - BGP and MD5 authentication

Support reference 85373

In a BIRD dynamic routing configuration that uses BGP with MD5 authentication, the absence of a source address for the BGP configuration now results in a warning message prompting the administrator to enter a source address in the BIRD configuration. This prevents a malfunction of the BGP session in question. This regression appeared in SNS versions 4.6.9 and 4.3.21 LTSB.

Listening port on the web administration interface

Support reference 85450

Attempts to change the listening port on the web administration interface (TCP/443 by default) no longer result in a system error in the firewall's configuration engine, and are now correctly applied.

IPsec VPN - IKEv1 - Certificate authentication and XAuth

Support reference 85283

During the setup of an IKEv1 IPsec tunnel with certificate authentication and XAuth, user groups are now correctly saved in the intrusion prevention engine's tables. Such groups can once again

be used in filter rules. This regression appeared in SNS version 4.2.

Encryption/PKI

Support reference 85476

The CLI/Serverd command `CONFIG FWADMIN PROTECT` would wrongly allow the decryption of any TPM-protected private key without requiring the TPM password. This issue has been fixed.

Log management service - TCP Syslog

Support reference 85297 - 85396

The firewall's log management service no longer stops when its configuration is modified and the connection between the TCP Syslog server and the firewall is unreliable or unstable.

Intrusion prevention engine

IPS analysis - Alarms

Support reference 85210

Packets that raise one of the alarms occurring before the filter inspection would still pass through the firewall despite the presence of a filter rule configured to block the corresponding network traffic. This issue has been fixed.

Refer to the list of alarms occurring before the filter inspection in the Stormshield knowledge base (authentication required).

LDAP protocol

Support reference 84561

The LDAP protocol analysis engine now correctly manages GSSAPI authentication packets, which no longer wrongly generate "Bad LDAP protocol" (ldap_tcp:427 error) alarms.

Web administration interface

DHCP server and log partition operations

Support reference 84501

Enabling the DHCP server on the firewall no longer prevents maintenance operations on the log partition via the web administration interface (unmounting/mounting, formating, etc.).

IPsec VPN

Support reference 85423

In line with what was announced in SNS 4.7.1 release notes, the wizard that creates mobile IPsec VPN rules in *config* mode now makes it possible to select a network group as local resources.

Cluster creation wizard

Support reference 85405

If an interface included in a bridge or an interface without an IP address is present on the firewall, it no longer prevents the cluster creation wizard from launching.

New features and enhancements in SNS 4.7.2 EA

Server certificate retrieval mechanism

Support reference 84671

The maximum waiting time for a response to a server certificate retrieval request has been reduced, and can now be configured on each SSL protocol inspection profile. The value of the waiting time can be anywhere between 1 and 10 seconds, and is set to 2 seconds by default.

Do note that this configuration can only be changed and enabled with the following CLI/serverd commands:

```
CONFIG PROTOCOL SSL PROFILE IPS CONFIG TLSServerCertTimeout=[1-10] index=
[0-9]
CONFIG PROTOCOL SSL ACTIVATE
```

More information on the **CONFIG PROTOCOL SSL IPS CONFIG** command.

IPsec VPN - *Diffusion Restreinte* (DR) mode

On firewalls configured in DR mode, ESP traffic encapsulation can now be enabled/disabled in UDP for individual peers. To keep the firewall operating in DR mode during its update to SNS version 4.7.2 and higher, encapsulation is enabled by default.

Sandboxing

The classification of files without extensions and specific MIME types has changed. Such files are no longer systematically analyzed to optimize sandboxing on all other file types.

SD-WAN

Support reference 85253

For SD-WAN configurations that use SLA thresholds and in which the main gateways of a router object present very close SLA scores, the time to wait before changing gateways has been reduced (from a maximum of 25 to 9 seconds).

Support reference 83962

In the routing statistics log file, the value of the last latency measurement made until the present moment has been replaced with:

- Average latency,
- Minimum latency,
- Maximum latency.

This data is calculated over the moving window period in which measurements are saved (15 minutes by default).

More information on:

- Firewall log files,
- SD-WAN SLA thresholds.

Resolved vulnerabilities in SNS 4.7.2 EA

DHCP

A moderate severity vulnerability was fixed in the firewall's DHCP server service.

Details on this vulnerability can be found on our website : https://advisories.stormshield.eu/2023-023.

IPsec VPN

A moderate severity vulnerability was fixed in the IPsec tunnel manager.

Details on this vulnerability can be found on our website : https://advisories.stormshield.eu/2023-024.

NSRPC service

A moderate severity vulnerability was fixed in the NSRPC service.

Details on this vulnerability can be found on our website : https://advisories.stormshield.eu/2023-027.

SNS 4.7.2 EA bug fixes

System

IPsec VPN

Support references 84572 - 84708 - 85270 - 85272

When the subject of a certificate from a trusted CA contains a non-ASCII encoded character, this no longer prevents the setup of IPsec tunnels based on this CA.

IPsec VPN - Verification of peer certificate revocation (CRL)

Support reference 82506

Deploying a VPN topology, on which the CRLRequired parameter is enabled, from an SMC server no longer overwrites the CA's certificate revocation list (CRL) on the SNS firewall.

Multi-user SSH authentication - SCP command

Support reference 84848

Accounts that have been declared as firewall administrators with the "Console (SSH)" permission can once again run the SCP command in SSH. This issue did not affect the "admin" account.

Extended Web Control (EWC) URL classification and SSL filtering

Support reference 85374

Following several attempts to access the same prohibited URL, the block page that appears, and the log relating to the SSL protocol would wrongly indicate the *default* category instead of the category to which the URL belongs. This anomaly has been fixed.

SNi40 industrial firewalls

Support reference 85078

On SNi40 firewalls with bypass configured in Safety mode, the bypass active mode could wrongly appear as Safety mode. This issue has been fixed.

SN-S-Series-320 and SN-M-Series-520 model firewalls

The maximum number of HTTP/FTP/SMTP/POP3 connections allowed on SN-S-Series-320 and SN-M-Series-520 model firewalls was wrong and will be fixed when the firewall is updated to version 4.7.2 or higher.

IPsec load balancing on CPUs - SN510, SN2000, SN2100 and SN3100 model firewalls

An issue with competing access in the IPsec encryption load balancing mechanism on CPUs has been fixed on SN510, SN2000, SN2100 and SN3100 model firewalls. Reminder: IPsec encryption load balancing can be configured using the CLI/Serverd command `CONFIG IPSEC CRYPTOLB UPDATE`.

Proxies

Support references 85041 - 85048 - 85260 - 85286 - 85314

Proxies no longer freeze when an SSL decryption rule encounters certificates with the following characteristics:

- Certificates with a blank Subject field,
- Certificates signed by a certification authority that the proxy has not recognized as trusted (e.g., self-signed certificates).

And the action associated with the SSL protocol analysis of **Unknown certificates** is set to **Delegate to user.**

Support reference 85254

Issues with memory leaks on proxies have been fixed.

IPsec tunnel monitoring

Support reference 85318

In IPsec tunnel monitoring, an anomaly that caused tunnels set up with peers in *Responder-only* mode to appear as bypass policies has been fixed.

SSL VPN

Support reference 84612

Checks have been added to prohibit *ping* argument values greater than half of the *pingrestart* argument value in the CLI/Serverd command `CONFIG OPENVPN UPDATE`. Such a configuration would prevent the SSL VPN client from setting up a tunnel again after a disconnection, and would require the SSL VPN service to be restarted on the client workstation.

More information on the command **`CONFIG OPENVPN UPDATE`**

CLI/SSH commands

Support reference 85110

The help returned from the command `sfctl --help -F` now specifies the existence of the token *assoc*.

NTP client service

The NTP client service no longer stops functioning on firewalls that have over 1024 interfaces.

SD-WAN

Inconsistencies in the measurement unit used for calculations and the display of gateway unavailability rate have been fixed.

Routing

Support reference 85320

By updating to version 4.7.2 EA a firewall on which the default route was defined with a *loopback* object (e.g., the *localhost* object with the IP address 127.0.0.1), this object would automatically be replaced with the *blackhole* object. This ensures the compatibility of the routing configured earlier.

Intrusion prevention engine

ICMP request

Support references 84197 - 85387

On firewalls with:

- A server behind a protected interface,
- Two separate Internet access links.

Following a request from an unprotected network to the server, if the server did not listen on the requested port, type 3 ICMP packets that it sent would always take the default route. Packets now take the configured return route.

NTP protocol

Support reference 85077

Verifications of the NTP field *reference_timestamp* would wrongly raise a 451 alarm in the NTP plugin. As this verification was unnecessary, it has been removed.

High availability

Support reference 84766

During a switch in the cluster, an anomaly in the processing of some established TCP/UDP connections could cause the cluster to become unstable. This anomaly has been fixed.

Web administration interface

IPsec VPN

Support reference 85312

The presence of a space in the name of a mobile IPsec VPN configuration prevents the IPsec policy from reloading and makes it inoperational. The firewall's web administration interface and the CLI/Serverd command `CONFIG IPSEC POLICY MOBILE UPDATE` now prohibit spaces from being entered in the names of mobile IPSsec policies.

Support reference 85334

The names of IPsec VPN rules can no longer be deleted, as rules with a blank name field prevent the IPsec policy from fully reloading.

SMTP filtering

Support reference 85347

The web administration interface no longer wrongly prohibits the definition of several rules that reference the same sender for different recipients. This regression appeared in version 4.0.

High availability - monitoring

Support reference 85398

The versions of the firmware installed on the main and backup partitions of the passive cluster member are now correctly displayed.

New features and enhancements in SNS 4.7.1 EA

Extended Web Control (EWC) URL classification

The Extended Web Control URL classification now uses the Bitdefender URL database.

To set up a URL/SSL filter policy, you are advised to operate in blacklist mode, i.e., explicitly place the URL categories to be prohibited in URL/SSL filter rule groups with a *block* action. These rules must then be placed above the rule that allows all the other categories.

While updating a firewall, which uses a whitelisted URL/SSL filter policy, to SNS version 4.7.1 or higher (filter rules explicitly allow some categories and are placed above the rule that blocks all other categories), we strongly recommend adding a rule that allows the URL categories *misc* (miscellaneous), *unknown*, *computersandsoftware* (software download websites) and *hosting* (websites hosting) to avoid affecting user experience. This rule must be placed above the rule that blocks all the other categories.

For more information on the migration of URL/SSL filter policies when the firewall is updated to SNS version 4.7 or higher, please refer to the **Technical Note** Migrating a security policy to the new EWC URL database.

IPsec DR mode - Generation of certificate request payloads

During the generation of certificate request payloads, ANSSI's IPsec DR guidelines recommend replacing the algorithm with SHA2 (previously SHA1).

SNS in versions 4.7 and higher and SNS 4.3 LTSB versions (from version 4.3.21 LTSB onwards) comply with this recommendation.

If IPsec DR mode is enabled on an SNS firewall in version 4.7, VPN tunnels can **only** be negotiated with peers that comply with this recommendation.

As such, in order for the negotiation of VPN tunnels in IPsec DR mode to continue functioning after the SNS firewall is updated to version 4.7, ensure that all IPsec DR-compatible peers in your architecture comply with this recommendation:

- SNS firewalls must all be updated to a version that complies with this recommendation,
- For firewalls from other vendors, contact them before any updates for more information,
- For Stormshield VPN Exclusive clients, ensure that every VPN client is in version 7.4.018 or higher and configure any additional parameters on them. For more information, refer to the **Technical note** IPsec VPN - *Diffusion Restreinte* mode,
- For all other VPN clients, get in touch with the relevant software vendor for more information before applying any updates.

TS agent authentication method (Citrix/RDS authentication)

SNS version 4.7 introduces a multi-user transparent authentication method for virtual desktop infrastructures (VDI) – the TS agent method.
This method relies on exchanges between the SNS firewall and one or several SN TS agents deployed directly on VDI servers (Citrix Virtual Apps and Desktops or Microsoft Remote Desktop Services).

Each SNS firewall can manage up to 100 TS agents.

For more information, refer to the **Technical note** SN TS Agent - Installation and deployment.

SSL VPN - Enhanced performance

In SNS version 4.7, a higher number of SSL VPN tunnels can be set up simultaneously on some firewall models. The throughput passing through each SSL VPN tunnel has also been increased.

	Number of simultaneous SSL VPN connections in UDP	
Model	**Earlier than SNS v4.7**	**SNS v4.7**
SN510	100	100
SN710	150	150
SN-M-Series-720	300	300
SN910	150	500
SN-M-Series-920	500	500
SN1100	500	800
SN2100	400	1000
SN3100	500	1000
SN6100	500	1000

IPsec VPN - Obsolete Diffie-Hellman methods

As some Diffie-Hellman methods are now obsolete (and indicated as such in the **Encryption profiles** tab in the **IPsec VPN** module), administrators are advised to change their IPsec VPN configurations if they use these methods.

These methods are:

- DH1 MODP Group (768-bits),
- DH2 MODP Group (1024-bits),
- DH5 MODP Group (1536-bits),
- DH25 NIST Elliptic Curve Group (192-bits),
- DH26 NIST Elliptic Curve Group (224-bits),
- DH27 Brainpool Elliptic Curve Group (224-bits).

Offline Active Update

SNS version 4.7 introduces the possibility of updating various security databases from the web administration interface by using a single update pack downloaded from the MyStormshield client area.

The date on which security databases were last updated offline or online via Active Update will now be shown in the Active Update widget in the System monitoring module. A warning message will also indicate when the last update of a database was too long ago.

For more information on Offline Active Update.

"Compromised URLs" web category

A "Compromised URLs" category has been added to the **URL filtering** and **SSL filtering** modules so that malicious URLs can be blocked when URL/SSL filtering is used in filter rules.
This category, which Stormshield's security teams continuously update to provide you with increased security, can be retrieved via Active Update (offline/online).

Logs - Additional information on blocked IP addresses or domains

When communications with a malicious IP address or domain are blocked, logs will now provide a direct link to additional information hosted on the Stormshield Security portal.

TPM - Protection of all private keys enabled

As of SNS version 4.7, all private keys of certificates on TPM-equipped firewalls can be secured with the TPM. Previously, this feature was limited to certificates used for authentication in an IPsec VPN.

This protection method can now also apply to certificates used particularly in the following cases:

- SSL/TLS decryption,
- Communications between SNS firewalls and SMC servers,
- Sending of logs to a syslog server,
- SSL VPN,
- Internal LDAP.

For more information on protecting private keys with the TPM.

NOTE
Following the update of a firewall to version SNS 4.7.1, even when the TPM was already initialized and certificates were already protected, a message in the dashboard could wrongly indicate that the TPM was not initialized or that automatic updates were not password-protected.
To work around this issue, ensure that you protect any certificates used in the firewall configuration that have not yet been TPM-protected. To do so, use the CLI/Serverd command "`MONITOR CERT`" to display the certificates in question, then protect them in **Configuration > Objects > Certificates and PKI**.

Static routing

The *blackhole* keyword can now be selected as a:

- Gateway when defining a static route,
- Default gateway of the firewall.

More information on the use of the *blackhole* keyword

Increased security

SSL VPN

Support reference 84357

LZ4 compression is no longer enabled in the default SSL VPN configuration, and does not affect existing configurations.

Integration

Quality of Service (QoS)

As of SNS version 4.7, QoS is supported on PPPoE and PPTP interfaces.

Automatic backups

The network interface used for connecting to automatic backup servers can now be selected (custom servers and Stormshield Cloud backup servers).

Amazon Web Services cloud

As of SNS version 4.7, Stormshield Elastic Virtual Appliance (EVA) instances deployed in the Amazon Web Services cloud can use Elastic Network Adapter (ENA) interfaces.

User experience

Mobile IPsec VPN policy in *config* mode

Network groups can now be selected as the local network when creating or editing a mobile IPsec policy in *config* mode.
Do note that if the Stormshield IPsec VPN client or TheGreenBow VPN client is used, the group cannot contain more than 8 networks/routes.

Application protection

It is now possible to search for IPS protections by their IDs.

Health indicators - NTP servers

An NTP server health indicator has been added to the **Dashboard** and in the **System monitoring** module.

This indicator makes it possible to:

- Highlight a flaw or response anomaly for an NTP server configured on the firewall,
- Report the absence of an NTP configuration when a service enabled on the firewall requires particular attention with regard to time synchronization in order to run properly (e.g., TOTP authentication).

Scheduled reloading of filter rules

Support reference 81691

The scheduled reloading of filter rules (*enfilter -u* command activated every day at midnight) can now be disabled by assigning a value of 0 to the *DailyRefresh* configuration token found in the *[Global]* section of the configuration file *ConfigFiles/Filter/filter*.

SD-WAN

The mechanism that manages gateway priorities has been optimized to prevent the default route from being reloaded unnecessarily when gateways have close priority scores.

When a gateway exceeds an SLA threshold, an entry will be systematically generated in the system log file.

SD-WAN monitoring

For a selected gateway, a "Real time chart" tab makes it possible to display the following charts:

- The gateway's latency measured over the last 10 minutes,
- The status of the gateway over the same period.

High availability

Unicast synchronization

A unicast synchronization can now be set between members of a cluster during the creation of the cluster. This option is required in order to deploy high availability in cloud infrastructures that do not support the multicast protocol.

MAC address synchronization

It is now possible to choose whether MAC address synchronization must be forced when a cluster switches (**High availability > Advanced configuration > Force MAC address synchronization** option).

For elastic virtual appliances (EVA) deployed in versions 4.7 and higher and in a high availability configuration, this synchronization is now disabled by default. For physical firewalls in factory configuration, this synchronization remains enabled by default.

This option may need to be disabled in configurations that use link aggregation (LACP), for example.

More information on high availability.

SNS 4.7.1 EA bug fixes

System

IPsec VPN

Support references 84983 - 85133 - 85253

The mechanism that reloads rules in the IPsec VPN policy has been enhanced to limit the risk of the firewall's routing engine unexpectedly shutting down when some configurations remain unchanged.

sysinfo command

Support reference 84415

The system diagnostic command *sysinfo* no longer wrongly calls up some deleted binary files. This measure is implemented as part of hardening the operating system.

Multi-user SSH authentication

Support references 84532 - 84847

When the SSH key of the admin account was saved on the firewall, no other administrators could connect to the firewall via SSH. This regression, which first appeared in SNS version 4.3.3, has been fixed.

Authentication - brute force attacks

Support reference 81350

When the brute force attack protection mechanism is activated, the alarm generated no longer contains a destination address that is systematically 0.0.0.0. This regression appeared in SNS version 4.1.1.

RADIUS authentication

Support reference 84162

When administrators connected via a Radius method, no other entries would be generated in the authentication log file. This anomaly has been fixed.

Support references 84484 - 84497

The default maximum response time for Radius requests can now be raised to 600 seconds. This value can be modified by using the CLI/Serverd command `CONFIG.AUTH.RADIUS`.

More information about the CLI/Serverd command `CONFIG.AUTH.RADIUS`.

TOTP authentication and SSH access to the firewall

Support reference 84947

TOTP authentication was not applied to console connections via SSH to the firewall when the TOTP authentication rule specified an authentication source other than the object *any*.

Custom web services

The icon indicating the use of a custom web service in the firewall's configuration no longer wrongly appears in green when the service belongs to a group, but is not used.

Static routing

Support references 85213 - 85027 - 85218

An anomaly in the mechanism that reloads IPsec policies has been fixed to prevent potential failures while loading static routes.

Dynamic multicast routing

The dynamic Rendez-vous Point (RP) election mechanism has been optimized for architectures in which several firewalls are candidates for RP election with multicast address ranges that overlap.

High availability (HA) - SNMPv3

Support reference 81702

SNMPv3 parameters *EngineBoots* and *EngineTime* are now automatically synchronized as soon as a cluster is created and every time roles are switched in this cluster. The purpose of this synchronization is to stop causing errors on some SNMP monitoring tools.

Object database - Imports

Support reference 83327

After databases were imported via a CSV file, imported objects would not immediately appear in the firewall's local database even after the screen was refreshed. Users needed to disconnect and re-connect to the web administration interface to make these objects appear. This anomaly has been fixed.

Filter - NAT

The use of the comparison mathematical operator "different from" (icon  or "!=") in a filter rule would result in the wrong address range being generated for the rule in question.

Default route - DHCP - IPv6

Support reference 85124

In a configuration such as the following:

- The firewall's default gateway is learned via DHCP,
- IPv6 is enabled on the firewall.

Any changes (name, protection status, etc.) made to an interface with a DHCP address range no longer cause the firewall's default route to be deleted.

SD-WAN

Support references 84839 - 85165

If no changes have been made, the firewall no longer wrongly generates a "*Remote host unreachable*" log entry for every static route when its network configuration is being reloaded.

Captive authentication portal and SSL VPN

Support reference 84801

The configuration of the captive portal on the listening port that is reserved and used by the SSL VPN (*sslvpn* port) now raises an error indicating that this port is reserved.

Intrusion prevention engine

OPC UA protocol

A verification of the authentication token of the OPC UA command *CreateSessionRequest* has been removed. This verification would wrongly block legitimate OPC UA traffic.

DCERPC protocol

UUIDs belonging to the "[MS-WMI]: Windows Management Instrumentation Remote Protocol" class have been added to the list of known UUIDs in the DCERPC protocol analysis engine to stop wrongly raising the block alarm "DCERPC unknown UUID" (alarm nb-cifs:310).

These UUIDs are:

- '027947E1-D731-11CE-A357-000000000001':'IEnumWbemClassObject',
- '9556DC99-828C-11CF-A37E-00AA003240C7':'IWbemServices',
- 'F309AD18-D86A-11D0-A075-00C04FB68820':'IWbemLevel1Login'.

Analysis of TCP options

Support reference 83234

The activation of the alarm "Misplaced TCP option" (tcpudp:58), when its action is set to *pass*, no longer wrongly stops the analysis of the options that follow the TCP packet and no longer raises the alarm "Wrong TCP sequence number" (tcpudp:16).

LDAP protocol

Support reference 83800

The alarm "Possible attack on capacity" (alarm ip:91) is no longer wrongly raised when a CRL larger than 128 KB is downloaded via an LDAP request.

TLS v1.3 protocol

Support references 84244 - 84761 - 84780- 84783 - 84784 - 84785 - 84786 - 84787 - 84788 - 84789 - 84791 - 84796 - 84799 - 84805 - 84806 - 84845

An issue in the TLS v1.3 protocol analysis engine has been fixed. This regression, which appeared in SNS version 4.5.3, could cause the firewall to freeze.

Filtering - Web services

Support reference 84721

Using in two separate filter rules two web services with names in which only the last character differed would wrongly cause the consistency checker to detect an overlap of these filter rules. This anomaly has been fixed.

High availability - SCTP associations and TCP/UDP connections

Support reference 84792

In high availability configurations, following a double switch (active - passive - active), dates on which SCTP associations and TCP/UDP connections are made are no longer incorrect.

High availability - SCTP protocol

If the properties of source and destination hosts that are part of an SCTP association are not available when the association is synchronized among members of the cluster, the SCTP association in question will no longer be deleted but a new attempt to synchronize this association will be scheduled.

Network

8-port RJ45 module

Support references 82270 - 85269

When an unexpected freeze on the 8-port RJ45 network module is detected, the firewall will be automatically restarted to allow this module to reconnect to the network.

Web administration interface

Administrators with restricted access privileges

Verifications have been added to prevent administrators authenticated with restricted privileges from displaying modules that are ordinarily not allowed, by directly entering a URL that contains the name of the module in question.

Telemetry

Administrators other than the super administrator (admin account) can no longer enable or disable telemetry.

Configuration of the firewall via SSH

In **System** > **Configuration** > **Firewall administration** tab, the fields relating to **Remote SSH access (requires 'admin' account)** are now all grayed out for any connected administrator that is not the super administrator (*admin* account).

Authentication policy

Multiple rules could no longer be dragged and dropped simultaneously in the authentication policy grid. This regression, which first appeared in SNS version 4.1, has been fixed.

Double-clicking on either the **Source** or **Methods (assess by order)** column of an authentication rule for which the method was set to "Prohibit" no longer wrongly replaces the "Prohibit" value with "Default method".

DHCP relay - Google Chrome

Support reference 84593

In the configuration module of a DHCP relay (**DHCP** > **DHCP relay** module), if an administrator connected to the firewall's web administration interface via Google Chrome makes changes to

the **IP address used to relay DHCP queries**, the changes are now applied. When the module is changed, the value of the address is no longer reset to "automatic".

Preferences - Log display

Support reference 84956

The values selected for the fields **Number of lines displayed per page** and **Minimum number of characters to start searching** in the **Preferences** module are now correctly interpreted and no longer prevent logs from being displayed. This regression appeared in SNS version 4.4.

Objects

Support references 84588 - 84719

Objects used in the firewall's configuration can no longer be forcibly deleted, to avoid generating inconsistencies in the configuration.

Antivirus

Support reference 85330

If a license containing only ClamAV as the antivirus engine is installed on the firewall, the **Antivirus** module now appears correctly and the message "No access" no longer appears.

Version 4.7.0 not published

Version 4.7.0 is not available to the public.

New features and enhancements in SNS 4.6.11

SD-WAN - Calculation of jitter

To obtain higher jitter values (variation in latency), the formula to calculate this in has been changed to follow the model based on the difference between two consecutive transmission periods (RFC 4689 and 5481).

Resolved vulnerabilities in SNS 4.6.11

OpenSSH

A high severity vulnerability was fixed in OpenSSH.

Details on this vulnerability can be found on our website : https://advisories.stormshield.eu/2023-035.

DHCP

A moderate severity vulnerability was fixed in the firewall's DHCP server service.

Details on this vulnerability can be found on our website : https://advisories.stormshield.eu/2023-023.

SNS 4.6.11 bug fixes

System

Proxies

Support references 85428 - 85495 - 85491

Issues regarding proxies that were unexpectedly blocked when configurations were reloaded have been corrected.

Network captures with *tcpdump* on a *usbus* interface

Support references 85083 - 85313

Launching a network capture with *tcpdump* on a *usbus* interface no longer causes the firewall to unexpectedly restart.

Elastic Virtual Appliances (EVA)

Support reference 85273

On an EVA virtual firewall, limiting the number of CPUs when hyperthreading is enabled no longer causes the firewall to restart unexpectedly.

QoS

Support reference 85019

Due to an issue that occurs when a CBQ queue used as an acknowledgment queue (ACK) in a filter rule is deleted, the firewall may sometimes unexpectedly restart. This issue has been fixed.

SD-WAN

Inconsistencies in the measurement unit used for calculations and the display of gateway unavailability rate have been fixed.

Support reference 85253

For SD-WAN configurations that use SLA thresholds and in which the main gateways of a router object present very close SLA scores, enhancements now make it possible to prevent excessively frequent changes to the priorities of these gateways.

Switching to a lower SNS version

Support reference 85247

When a firewall switches to a lower SNS version without being reset to its factory configuration (*defaultconfig*), attempts to display the list of available alarms no longer cause the intrusion prevention engine and the command-based configuration server (serverd) to unexpectedly restart.

NAT

Support reference 84819

An issue has been fixed in the NAT manager. This issue would wrongly fill the table of translated ports used for traffic that requires child connections (e.g. FTP, RTSP and others). As a result, this would prevent child connections from being created, and disrupt the traffic in question.

Filter - NAT

Support references 85357 - 85376

In filter rules that use a set of network objects, one of which is linked to a disabled DHCP-configured interface, restarting the firewall will no longer wrongly enable the "(1) *Block all*" filter rule. This regression appeared in SNS version 4.6.8.

Support reference 85239

In a situation such as the following:

- The firewall has a bridge that groups several interfaces. On this bridge:
  - Traffic from one of the bridge interfaces to an interface outside the bridge is allowed by a filter rule in *Firewall* mode,
  - Traffic from another bridge interface to the same interface outside the bridge is blocked by another filter rule.
- A connection has been established between a client host and the server through the first rule,
- An infected host or an intrusion probe located on the same interface as the server sent a *reset* packet with the same references as the established connection (source/destination addresses and source/destination ports).

Although the packet from the infected host or intrusion probe was rightly blocked, the source interface of the client host was wrongly modified and its established connection with the server was shut down. This issue has been fixed.

Connection to the web administration interface with the *admin* account

Support references 85266 - 85309 - 85349 - 85437 - 85494

Under certain circumstances, attempts to connect to the web administration interface with the *admin* account would fail and cause the command-based configuration server (serverd) to unexpectedly restart. This issue has been fixed.

High availability (HA)

Support references 77890 - 83274

On a high availability firewall that has switched roles several times in the cluster, some packets would take the wrong return route while presenting the IP address of the right return route. This issue, which caused the shutdown of the traffic in question, has been fixed.

Intrusion prevention engine

IPS analysis - Alarms

Support reference 85210

Packets that raise one of the alarms occurring before the filter inspection would still pass through the firewall despite the presence of a filter rule configured to block the corresponding network traffic. This issue has been fixed.

Refer to the list of alarms occurring before the filter inspection in the Stormshield knowledge base (authentication required).

LDAP protocol

Support reference 84561

The LDAP protocol analysis engine now correctly manages GSSAPI authentication packets, which no longer wrongly generate "Bad LDAP protocol" (ldap_tcp:427 error) alarms.

New features and enhancements in SNS 4.6.10

IPsec VPN - *Diffusion Restreinte* (DR) mode

On firewalls configured in DR mode, ESP traffic encapsulation can now be enabled/disabled in UDP for individual peers. To keep the firewall operating in DR mode during its update to SNS version 4.6.10 and higher, encapsulation is enabled by default.

IPsec VPN *Diffusion Restreinte* (DR) mode - Generating Certificate Request Payloads

During the generation of certificate request payloads, ANSSI's IPsec DR guidelines recommend replacing the algorithm with SHA2 (previously SHA1).

SNS versions 4.6 (from 4.6.10 onwards), 4.3 LTSB (from version 4.3.21 LTSB onwards) and SNS versions 4.7 and higher comply with with this recommendation.

If IPsec DR mode is enabled on an SNS firewall in version 4.6.10, VPN tunnels can **only** be negotiated with peers that comply with this recommendation.

As such, in order for the negotiation of VPN tunnels in IPsec DR mode to continue functioning after the SNS firewall is updated to version 4.6.10, ensure that all IPsec DR-compatible peers in your architecture comply with this recommendation:

- SNS firewalls must all be updated to a version that complies with this recommendation,
- For firewalls from other vendors, contact them before any updates for more information,
- For Stormshield VPN Exclusive clients, ensure that every VPN client is in version 7.4.018 or higher and configure any additional parameters on them. For more information, refer to the technical note IPsec VPN - *Diffusion Restreinte* mode,
- For all other VPN clients, get in touch with the relevant software vendor for more information before applying any updates.

Sandboxing

The classification of files without extensions and specific MIME types has changed. Such files are no longer systematically analyzed to optimize sandboxing on all other file types.

Server certificate retrieval mechanism

Support reference 84671

The maximum waiting time for a response to a server certificate retrieval request has been reduced, and can now be configured on each SSL protocol inspection profile. The value of the waiting time can be anywhere between 1 and 10 seconds, and is set to 2 seconds by default.

Do note that this configuration can only be changed and enabled with the following CLI/serverd commands:

```
CONFIG PROTOCOL SSL PROFILE IPS CONFIG TLSServerCertTimeout=[1-10] index=
[0-9]
CONFIG PROTOCOL SSL ACTIVATE
```

More information on the `CONFIG PROTOCOL SSL IPS CONFIG` command.

Resolved vulnerabilities in SNS 4.6.10

IPsec VPN

A moderate severity vulnerability was fixed in the IPsec tunnel manager.

Details on this vulnerability can be found on our website : https://advisories.stormshield.eu/2023-024.

NSRPC service

A moderate severity vulnerability was fixed in the NSRPC service.

Details on this vulnerability can be found on our website : https://advisories.stormshield.eu/2023-027.

SNS 4.6.10 bug fixes

System

IPsec VPN

Support references 84572 - 84708 - 85270 - 85272

When the subject of a certificate from a trusted CA contains a non-ASCII encoded character, this no longer prevents the setup of IPsec tunnels based on this CA.

VPN - Verification of peer certificate revocation (CRL)

Support reference 82506

Deploying a VPN topology, on which the CRLRequired parameter is enabled, from an SMC server no longer overwrites the CA's certificate revocation list (CRL) on the SNS firewall.

IPsec VPN - IKEv1 - Certificate authentication and XAuth

Support reference 85283

During the setup of an IKEv1 IPsec tunnel with certificate authentication and XAuth, user groups are now correctly saved in the intrusion prevention engine's tables. Such groups can once again be used in filter rules. This regression appeared in SNS version 4.2.

Multi-user SSH authentication - SCP command

Support reference 84848

Accounts that have been declared as firewall administrators with the "Console (SSH)" permission can once again run the SCP command in SSH. This issue did not affect the "admin" account.

SNi40 industrial firewalls

Support reference 85078

On SNi40 firewalls with bypass configured in Safety mode, the bypass active mode could wrongly appear as Safety mode. This issue has been fixed.

SN-S-Series-320 and SN-M-Series-520 model firewalls

The maximum number of HTTP/FTP/SMTP/POP3 connections allowed on SN-S-Series-320 and SN-M-Series-520 model firewalls was wrong and will be fixed when the firewall is updated to version 4.6.10 or higher.

IPsec load balancing on CPUs - SN510, SN2000, SN2100 and SN3100 model firewalls

An issue with competing access in the IPsec encryption load balancing mechanism on CPUs has been fixed on SN510, SN2000, SN2100 and SN3100 model firewalls. Reminder: IPsec encryption load balancing can be configured using the CLI/Serverd command `CONFIG IPSEC CRYPTOLB UPDATE`.

8-port RJ45 module

Support references 82270 - 85269

When an unexpected freeze on the 8-port RJ45 network module is detected, the firewall will be automatically restarted to allow this module to reconnect to the network.

Proxies

Support references 85041 - 85048 - 85260 - 85286 - 85314

Proxies no longer freeze when an SSL decryption rule encounters certificates with the following characteristics:

- Certificates with a blank Subject field,
- Certificates signed by a certification authority that the proxy has not recognized as trusted (e.g., self-signed certificates).

And the action associated with the SSL protocol analysis of **Unknown certificates** is set to **Delegate to user.**

Support reference 85254

Issues with memory leaks on proxies have been fixed.

IPsec tunnel monitoring

Support reference 85318

In IPsec tunnel monitoring, an anomaly that caused tunnels set up with peers in *Responder-only* mode to appear as bypass policies has been fixed.

SSL VPN

The following can no longer be selected for the SSL VPN server:

- A TCP listening port below 1024,
- A UDP listening port below 1024, except UDP/443.

Intrusion prevention engine

ICMP request

Support references 84197 - 85387

On firewalls with:

- A server behind a protected interface,
- Two separate Internet access links.

Following a request from an unprotected network to the server, if the server did not listen on the requested port, type 3 ICMP packets that it sent would always take the default route. Packets now take the configured return route.

NTP protocol

Support reference 85077

Verifications of the NTP field *reference_timestamp* would wrongly raise a 451 alarm in the NTP plugin. As this verification was unnecessary, it has been removed.

High availability

Support reference 84766

During a switch in the cluster, an anomaly in the processing of some established TCP/UDP connections could cause the cluster to become unstable. This anomaly has been fixed.

Web administration interface

IPsec VPN

Support reference 85312

The presence of a space in the name of a mobile IPsec VPN configuration prevents the IPsec policy from reloading and makes it inoperational. The firewall's web administration interface and the CLI/Serverd command `CONFIG IPSEC POLICY MOBILE UPDATE` now prohibit spaces from being entered in the names of mobile IPSsec policies.

Support reference 85334

The names of IPsec VPN rules can no longer be deleted, as rules with a blank name field prevent the IPsec policy from fully reloading.

SMTP filtering

Support reference 85347

The web administration interface no longer wrongly prohibits the definition of several rules that reference the same sender for different recipients. This regression appeared in version 4.0.

High availability - monitoring

Support reference 85398

The versions of the firmware installed on the main and backup partitions of the passive cluster member are now correctly displayed.

New features and enhancements in SNS 4.6.9

Embedded reports

Support references 84495 - 84626 - 84933 - 85038 - 85081 - 85197

The mechanism that backs up the database of embedded reports to a disk is now launched once daily at 12:30 a.m. and when the product is shut down/restarted, to reduce disk writing operations that may cause instability on SN160(W), SN210(W) and SN310 products.

Emerson DeltaV industrial protocol

Version 4.6.9 introduces the automatic detection of the Emerson DeltaV industrial protocol.

Storage devices

Support references 84901 - 85018 - 85145

The **Messages** module in the **Dashboard** can inform the administrator when a firmware update for the system storage device is available and must be installed with the assistance of Stormshield's technical support.
Reminder: this update makes it possible to fix any issues regarding malfunctions on the firewall.

New card for 8-port 2.5 Gb/s copper modules

The 2.5 Gb/s copper 8-port card (reference NA-EX-CARD-8x2.5G-C) has been supported since SNS version 4.6.2.
The use of this card is intended for SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN2100 and SN3100 firewall models.

PKI

The alarm 'Get CRL failed' now specifies the URL of the Certificate Revocation List (CRL) that could not be reached.

SSH connections to the firewall

On firewalls in factory configuration and in SNS version 4.6.x and upwards, the encryption algorithms ssh-rsa, hmac-sha2-256 and hmac-sha2-512 are no longer allowed for SSH connections to the firewall.

OSCAR analysis

A warning has been added to the configuration panel of the OSCAR protocol analysis to indicate that this protocol has considered obsolete since SNS version 4.6.9.

Resolved vulnerabilities in SNS 4.6.9

ClamAV antivirus

A moderate severity vulnerability was fixed in ClamAV.

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

ICMP

Support reference 84949

A moderate severity vulnerability was fixed in the ICMP protocol analysis engine.

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

SNS 4.6.9 bug fixes

System

IPsec VPN

Support references 85095 - 85252

Firewalls on which the option **Do not initiate the tunnel (Responder only)** is enabled no longer wrongly generate phase 1 re-authentication requests.

Support reference 84821

In a configuration resembling the following on site A:

- An initial IPsec tunnel to site B is defined in the IPsec policy,
- A second tunnel to site C is based on a virtual IPsec interface (VTI),
- A static route specifies the network to site C,
- The network defined for site C's traffic endpoint overlaps with the network defined for site B's traffic endpoint.

Network traffic towards site C (VTI-based tunnel) will no longer be wrongly channeled through the tunnel to site B (tunnel defined in the IPsec policy).

Support reference 85284

Changes have been made to the mechanism that loads the IPSec management engine to prevent competing access to its configuration file. Such access would prevent the IPsec configuration from loading when the firewall started up.

Support reference 84856

In the IPsec configuration file, the presence of a string (e.g., certificate CN, certificate name, etc.) that may reference an obsolete encryption algorithm (e.g. des, blowfish, etc.) no longer blocks the firewall's firmware updates.

Support references 85179 - 84968

IPsec VPN tunnels with phase 2 (IPsec) encryption profiles that use Diffie-Hellman DH18 MODP (modp8192) groups such as Perfect Forward Secrecy (PFS), can now renegotiate their Security Association (SA) keys again. This regression, which shut down the IPsec tunnel, appeared in SNS version 4.2.

Configuration - IPsec

Support reference 84881

The presence of a rule separator in the IPSec VPN policy, combined with the presence of FQDN objects in the object database, no longer wrongly raises an error during requests to resolve FQDN objects.

Router objects

Support reference 84963

Updating to SNS version 4.6.9 (and upwards) firewalls that use router objects:

- Created in versions earlier than SNS 4.3,
- With names that contain the characters "+" (*plus*) or "^" (circumflex accent),

No longer prevents these router objects from functioning in the firewall's configuration.

Configuration – Network objects

Support reference 85274

Objects belonging to auto-generated groups (e.g., *Network_internals*) can now be correctly renamed. This operation no longer generates the system error "The object is included in one or several groups", and the new object name is correctly applied in all groups and configuration modules that use it. This regression appeared in SNS version 4.6.2.

GRETAP tunnels

When the IP address of an active GRETAP tunnel's endpoint is edited, the changes are now correctly applied.

Authentication - RADIUS

Support references 84484 - 84497

The default maximum response time for Radius requests can now be raised to 600 seconds. This value can be modified by using the CLI/Serverd command `CONFIG.AUTH.RADIUS`.

More information about the CLI/Serverd command `CONFIG.AUTH.RADIUS`.

Authentication – SSO Agent

Support reference 85052

In configurations that have simultaneously used several SSO agents, but in which the first agent in the list has since been deleted, the SSO Agent authentication engine now starts correctly when the authentication policy is reloaded.

SNMP Agent

Support references 84861 - 85133 - 85213 - 85232

Issues regarding the management of SNMP tables, which could cause the SNMP agent to shut down unexpectedly, have been fixed.

Monitoring - SN-S-Series and SN-M-Series firewalls

Support reference 85261

SN-S-Series and SN-M-Series firewalls in factory configuration that are equipped with a single power supply module out of two possible modules no longer wrongly generate a major alarm indicating that the second module is missing, unplugged or defective.

SSL VPN – TOTP

Support references 84966 - 84992

The use of customized certificates for the SSL VPN service and TOTP authentication with Stormshield SSL VPN clients no longer requires the client to enter a second TOTP at every connection.

Virtual machines

IPsec load balancing on CPUs

Support reference 85225

An issue regarding IPsec encryption load balancing on CPUs has been fixed on virtual EVA firewalls deployed on hypervisors that use the SR-IOV specification (Single Root I/O Virtualization).

Reminder: IPsec encryption load balancing can be configured using the CLI/Serverd command `CONFIG IPSEC CRYPTOLB UPDATE`.

More information about the CLI/Serverd command `CONFIG IPSEC CRYPTOLB UPDATE`.

Intrusion prevention engine

TCP protocol

Support references 84807 - 84515

In some cases, when an RST packet is received when a connection is closing, the connection could be left half-closed. This would prevent attempts to connect to the same IP address and over the same port, and would raise the alarm 'Invalid TCP packet for current connection state' (alarm tcpudp:97) until the timeout of the half-closed connection is reached. This issue has been fixed.

OPC-UA protocol

Support reference 85275

The OPC-UA protocol's analysis engine is now based on the protocol's 1.0.5 specification. This specification makes it possible to stop wrongly blocking *ReverseHello* messages, as this would disrupt OPC-UA connections in progress.

Web administration interface

Monitoring - Logs

Support reference 85279

Refreshing log display with the **Last hour** filter enabled no longer causes a growing lag between the time on displayed logs and the actual time on the firewall.

OPC-DA protocol

Support reference 85129

The entry *OPC-DA 3.0 Type Lib* no longer appears wrongly and repeatedly in the list of OPC-DA operations to analyze.

Dashboard - Advanced antivirus

Support reference 85281

In a configuration such as the following:

- The antivirus is enabled,
- No rules in the active filter policy involve the antivirus.

The firewall's **Dashboard** no longer wrongly indicates a critical status for the antivirus.

New features and enhancements in SNS 4.6.8

IPsec DR mode compliance

The behavior of the IKE key negotiation engine has been modified to enable its compliance with the requirements of the ANSSI's IPsec DR guidelines. Changes made will not be noticeable in nominal use cases of SNS products.

High availability and TPM

Support reference 85055

In a high availability configuration such as the following:

- Members of the cluster are equipped with TPMs that have been initialized,
- The health status of TPMs is included in the calculation of the quality factor.

When the TPM on the passive firewall (firewall that was initially passive or which became passive after a switch due to a downgraded quality index) encounters a failure, this firewall will be restarted to recover its TPM in a working condition.

SNS 4.6.8 bug fixes

System

Authentication - SSO agent

Support reference 85133

In configurations that use SSO agent authentication based on a main external LDAP directory and a backup external LDAP directory, switching from the main directory to the backup directory would cause the authentication engine to unexpectedly shut down. This issue has been fixed.

Storage devices

Support references 84901 - 85018 - 85145

Issues that could result in SN2100 and SN3100 firewalls unexpectedly shutting down have been fixed by updating the firmware of the system storage device.

Interfaces - Object database

Support references 85267 - 85294

When an interface does not have an IP address (such as a dialup that is not yet connected after a firewall is restarted), *Firewall_* and *Network_* objects linked to this interface will be automatically generated again. This regression, which first appeared in SNS version 4.6.6, would prevent the filter policy from being loaded.

Intrusion prevention engine

SSLProtocol

Even though the alarm "Invalid SSL packet" (ssl alarm:118) is set to *pass* (alarm that does not block packets), packets that raise this alarm would wrongly stop the SSL protocol analysis. This anomaly has been fixed.

UDP

Support references 84913 - 85142 - 85157

An issue during the analysis of some UDP packets has been resolved to no longer cause the unexpected shutdown of the firewall.

Web administration interface

Certificates and PKI - TPM

Support references 84223 - 84462

On firewalls with TPMs that have not been initialized, the health status of the TPM would indicate a minor alarm, and any attempt to access the **Certificates and PKI** module would show

a message asking the administrator to initialize the TPM. Administrators can now click on the button found in this message to stop reminders and switch off the minor alarm.

New features and enhancements in SNS 4.6.7

HART-IP protocol

SNS version 4.6.7 introduces support for the dynamic analysis of the hart-ip protocol. Port objects *hart-ip_tcp* (TCP/5094), *hart-ip_udp* (UDP/5094) and *hart-ip* (ANY/5094) have also been added to the firewall's object database.

Resolved vulnerabilities in SNS 4.6.7

Connection portal

A low severity vulnerability was fixed on the firewall connection portal.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-020.

SNS 4.6.7 bug fixes

System

Network interfaces

Support reference 85117

The two alternative renegotiation mechanisms of the IKE security associations (reauthentication and rekeying mechanisms) are no longer wrongly launched one after the other. This regression, which would sometimes cause packet loss in configurations in *Diffusion Restreinte* (DR) mode, appeared in SNS version 4.2.0.

SSL VPN

Support reference 84841

Editing the SSL VPN configuration on a firewall with an SSL VPN tunnel that has already been set up would sometimes prevent the tunnel manager from restarting. This issue, which occasionally prevented SSL VPN tunnels from setting up after the configuration was edited, has been fixed.

Certificates and PKI

Support references 76892 - 85114

When a certificate signing request (CSR) is created using the CLI/Serverd command `PKI REQUEST CREATE`, and if Subject Alternative Names (SAN) or User Principal Names (UPN) are specified (IP addresses, FQDNs, etc.), they are now correctly applied and appear in the CSR and signed certificate.

Certificates and PKI - IPsec - *Diffusion Restreinte* (DR) mode

Support reference 84942

In a configuration with a trust chain such as: Certification authority (certificate signed in RSA) -> Sub certification authority (certificate signed in ECDSA or ECSDSA on an ECP 256 or BP 256 curve) used as a trust anchor -> Certificate (signed in ECDSA or ECSDSA on an ECP 256 or BP 256 curve), IPsec tunnels in DR mode would wrongly refuse to set up. This issue has been fixed to comply with reference RFCs for *Diffusion Restreinte* (DR) mode.

System – SNi20

Support references 84870 - 85037

Watchdog, which monitors the firewall's hardware activity, would wrongly be activated before the system's software monitoring mechanism when watchdog was set to its default value of 120 seconds. This issue has been fixed.

IPsec tunnel monitoring

Support reference 84776

Refreshing the IPsec tunnel monitoring screen no longer causes the system error *Command processing failed*.

Monitoring memory on SN310 firewalls

Support references 85022 - 85155

An anomaly in the management of memory monitoring data could wrongly raise an alert on memory usage and a change in the status of the corresponding health indicator in the **Dashboard** on SN310 firewalls. This anomaly has been fixed.

Filter - NAT

Support reference 84495

The mechanism that reloads filter and NAT rules has been optimized to prevent unnecessary access to the configuration, which can corrupt the list of filter and NAT policies.

Support reference 84734

If the filter policy contains two block rules to and from a MAC address, which are placed before the rule that allows the SSL VPN tunnel, traffic passing through the SSL VPN tunnel will no longer be wrongly blocked.

Logs - Syslog - IPFIX

Support references 84493 - 84876

In configurations that send logs via UDP/syslog or IPFIX without specifying the firewall IP address that must be used for such operations, and when a high volume of logs is sent, an issue with competing access would occasionally cause the firewall's network to be lost. This would then require the firewall to be restarted. This issue has been fixed.

Updating the firewall via the web administration interface

Support reference 84962

An issue occurring when the firewall is updated via the web administration interface could cause the interface to suddenly freeze and prevent the firewall from being updated. This issue has been fixed.

BIRD dynamic routing

Support reference 85221

In configurations that use the BGP protocol with TCP-MD5 authentication, the "setkey no" directive, which no longer functions, is automatically replaced with its equivalent "setkey yes" in the bird/bird6 configuration file when the firewall is updated to SNS version 4.6.7 or higher.

Intrusion prevention engine

High availability - SCTP protocol

Support reference 85118

SCTP associations are now correctly synchronized when the corresponding SCTP traffic follows a filter rule that has an IP address as its destination.

Purging intrusion prevention engine tables

The engine has been optimized to reduce the time required to purge certain intrusion prevention engine tables and prevent the risk of packets being rejected during this operation. This issue appeared in SNS version 4.5.0.

Filter - NAT

Support references 84667 - 84955 - 84957 - 85004 - 85061 - 85072 - 85131 - 85132 - 85133 - 85142 - 85157 - 85173

When the filter policy is reloaded after a rule that contains address translation is edited, the firewall will no longer unexpectedly freeze.

Filtering and NAT - Web services

Support reference 84722

The *block* action now functions in a filter rule that uses a web service with a name that is exactly 20 characters long.

Web administration interface

URL filtering / SSL filtering / SMTP filtering

Support reference 85164

In URL filtering, SSL filtering or SMTP filtering modules, deleting the first filter rule no longer desynchronizes the IDs of the other rules in the policy.

VLAN interfaces

Support reference 85226

When a user attempts to delete a VLAN when Bird dynamic routing is enabled, this will once again display the window indicating that this operation is not allowed, and that dynamic routing must be disabled beforehand. This regression appeared in SNS version 4.0.1.

Resolved vulnerabilities in SNS 4.6.6

DHCP

A high severity vulnerability was fixed in the firewall's DHCP client service.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-019.

SNS 4.6.6 bug fixes

System

IPsec VPN

Support reference 84823 - 84437

The *half_open_timeout* parameter can now be customized using the CLI/Serverd command CONFIG IPSEC UPDATE HalfOpenTimeout=<value> (30 seconds by default).

This parameter makes it possible to define the period after which an incomplete IKE association will be deleted (pending authentication of the IPsec client, for example.

Support reference 84701

In an IPsec configuration such as the following:

- One of the remote networks overlapped with a local network directly connected or reachable via a static route,
- The remote network in question was not placed in the first position in the IPsec policy,
- The *BypassLocalTraffic* option was enabled (using the CLI/Serverd command `CONFIG IPSEC UPDATE slot=<1-10> BypassLocalTraffic=1`).

The corresponding IPsec phase 2 negotiations would not be saved in the Security Policy Database and the tunnel would not set up. This issue has been fixed.

IPsec VPN - IKEv1 - Certificate authentication and XAuth

Support reference 84775

During the setup of an IKEv1 IPsec tunnel with certificate authentication and XAuth, user groups are now correctly saved in the intrusion prevention engine's tables. Such groups can once again be used in filter rules. This regression appeared in SNS version 4.2.

IPsec VPN - DR mode

Support reference 85051

For tunnels in DR mode, CREATE_CHILD_SA requests now end, and the renegotiation of the Child SA keys in phase 1 no longer fails.

Kerberos authentication and TOTP

Support reference 84859

In configurations that use Kerberos authentication and TOTP, the OTP code field is now correctly displayed in the captive portal. When a user logs in, the error "TOTP code missing" no longer appears.

Certificate-based authentication

Support reference 84981

In configurations that use certificate authentication, and which have a backup LDAP directory configured, the lack of a response from the main LDAP server will now trigger the switch to the

backup LDAP server.

Elastic Virtual Appliances (EVA)

Support reference 84714

The hyper-threading mechanism is enabled by default again on EVAs that have the expected number of virtual CPUs. This regression appeared in SNS version 4.2.

Multicast packets

Support reference 85180

When the intrusion prevention engine rewrote multicast packets, it could result in a double de-referencing that would cause the firewall to unexpectedly restart. This issue has been fixed.

Web administration interface

VLAN interfaces

Support reference 84822

VLANs would fail to be created if they were attached to an interface with a name that exceeded 10 characters. This a to the fact that after the web administration interface imposed a shorter name generated for the VLAN, it would appear in the list of interfaces, but would not actually be created. It would not be possible, for example, to assign a fixed IP address to it at the end of these operations. This issue has been fixed.

New features and enhancements in SNS 4.6.5

Availability of SN-S-Series-220 and SN-S-Series-320 firewalls

SN-S-Series-220 and SN-S-Series-320 firewalls are now available. Refer to the Product Life Cycle guide for more information on these models' compatibility with SNS versions.

A presentation of these firewalls can be found on the Stormshield website under Our Stormshield Network Security firewalls.

SNS 4.6.5 bug fixes

NOTE
The fix added in version 4.6.4 regarding memory leaks in the monitoring management engine has been removed. It will be reviewed and included in a future version.

System

SNMPv3 - Traps

Support reference 85085
After the update of an existing SNMPv3 configuration to version SNS 4.4 or higher, the authentication type assigned to SNMPv3 traps would be wrong. This anomaly has been fixed.

SN2100 and SN3100 firewall models - Updating firmware on SSD disks

To prevent SSD disks from potentially malfunctioning on SN2100 and SN3100 model firewalls, a firmware update of such disks is automatically applied when the firewall is updated to SNS version 4.6.5 or higher. Reminder: this update had already been applied since SNS version 4.6.2 to the firewall models listed in the section Version 4.6.2 bug fixes.

SSH connection over the firewall

Support reference 85106
Adding an SSH banner would cause an error in the configuration of the firewall's SSH server. This anomaly has been fixed.

Intrusion prevention engine

High availability - SCTP protocol

Support reference 85130
An issue was fixed in the bulk update mechanism in established SCTP associations. This issue occurred after the passive firewall was restarted.

New features and enhancements in SNS 4.6.4

Availability of SN-M-Series-520 firewalls

SN-M-Series-520 firewalls are now available. Refer to the Product Life Cycle guide for more information on these models' compatibility with SNS versions.

A presentation of these firewalls can be found on the Stormshield website under Our Stormshield Network Security firewalls.

Resolved vulnerabilities in SNS 4.6.4

ClamAV antivirus

A moderate severity vulnerability was fixed in ClamAV.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-013.

Logs

A low severity vulnerability was fixed in the log management module.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-006.

SNS 4.6.4 bug fixes

System

SNMP Agent

Support references 84911 - 84990

A memory leak issue has been fixed in the SNMP agent. This regression appeared in SNS versions 4.5.4 and 4.3.12.

Monitoring

Support references 84989 - 85015 - 85043

Memory leaks have been fixed in the disk monitoring mechanism.

High availability (HA)

Support reference 71538

An anomaly in the mechanism that retrieves HA information may prevent such information from being displayed in the firewall's web administration interface (**Monitoring** > **System/High availability** module). The mechanism has been optimized to reduce the frequency of this anomaly.

High availability (HA) - VLAN

Support reference 84710

A configuration in which the only active HA link passes through a VLAN interface would sometimes make the cluster unavailable. This regression, which first appeared in SNS versions 4.3.3 and 4.4.0, has been fixed.

IPsec VPN

Support reference 84677

When an IPsec tunnel is created, selecting the *All* object for remote networks no longer wrongly includes IPv6 addresses when the IPv6 option has not been enabled on the firewall.

IPsec VPN through a dialup default gateway

Support reference 82369

When the default gateway is based on a PPPoE modem (dialup connection), IPsec tunnels set up through this default gateway now recover correctly after the dialup connection goes down temporarily and recovers.

IPsec VPN IKEv2

Support reference 84920

User certificates with neither the Extended Key Usage Client Auth nor Extended Key Usage ServerAuth extension were not evaluated by user access privilege rules

(**Configuration** > **Users** > **Access privileges** module): the IPsec tunnel defined for this peer would be set up but the filter policy would block the peer and consider it invalid.
This issue was fixed by adding a UACForceCert configuration token: by assigning a value of 1 to it, the token forces the user access rules to evaluate such certificates.
This token can be configured with the CLI/Serverd command `CONFIG.IPSEC.UPDATE UACForceCert=<0|1>`

More information on the `CONFIG.IPSEC.UPDATE` command.

Monitoring

Memory leak issues have been fixed in the monitoring management engine.

SSL VPN

Support reference 84564

Whenever a listening port lower than 1024 was selected for the SSL VPN server, in particular port UDP/443, the SSL VPN server would no longer restart and no specific message in the web administration interface would indicate that this port could not be used.
Port UDP/443 can now be selected again for the SSL VPN server.

This regression appeared in SNS version 4.3.0.

DNS resolution of dynamic objects

Support reference 84889

In a configuration with several DNS servers defined, an issue in the DNS resolution mechanism for host objects with automatic/dynamic resolution and for FQDN objects was fixed when one of the DNS servers remained operational while the others were unreachable.

Hardware

SN1100, SN2100, SN3100, SNi20, SNi40 and SNxr1200 - CPU microcode

The microcode on Intel processors that equip SN1100, SN2100, SN3100, SNi20, SNi40 and SNxr1200 model firewalls has been updated.

Intrusion prevention engine

ICMPv6 protocol

An anomaly that wrongly raised the 'Invalid ICMP message" alarm (icmp:67), when this alarm was associated with the Pass action, has been fixed in the ICMPv6 protocol analysis engine.

Web administration interface

Conversion to lowercase

Support reference 84964

An anomaly in the function that converts some configuration fields to lowercase would occasionally cause the web administration interface to freeze in the module in question. This anomaly has been fixed.

Logs

Support reference 84895

Administrators with IDs that contain an "@" character can now create an object or add one to a group from the Logs view.

SNMP Agent

Support reference 84952

The values of the **Location (sysLocation)** and **Contact (sysContact)** fields in the **Configuration of MIB-II information** were not in quotes whenever they contained a space. This anomaly has been fixed.

Resolved vulnerabilities in SNS 4.6.3

Internal authentication service on the firewall (HTTPS)

A high severity vulnerability was fixed in the firewall's internal authentication service (HTTPS).

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-004.

Compression of HTTPS pages

A high severity vulnerability was fixed in the HTTPS page compression mechanism.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-003.

Internal authentication service on the firewall (SSH)

A high severity vulnerability was fixed in the firewall's internal authentication service (SSH).

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-005.

ClamAV antivirus

A moderate severity vulnerability was fixed in ClamAV.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-027.

OpenSSL

Several vulnerabilities were fixed in OpenSSL.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2023-008 (low severity),
- https://advisories.stormshield.eu/2023-009 (moderate severity),
- https://advisories.stormshield.eu/2023-010 (low severity).

SIP protocol

A high severity vulnerability was fixed in the SIP protocol analysis engine.

Details on this vulnerability can be found on our website: https://advisories.stormshield.eu/2023-007.

SNS 4.6.3 bug fixes

System

High availability (HA) with a backup link

Support reference 84458

In a HA configuration with a main and backup link, whenever the main link was down and became operational again, the cluster would continue to use the backup link by mistake. This anomaly has been fixed.

System monitoring – CPU load

Support reference 66123

The CPU consumption monitor would occasionally report unrealistic values. This anomaly has been fixed.

Firewall updates through a dialup default gateway

Support references 80557 - 84626 - 84768

During attempts to update firewalls connected to a PPPoE modem (*dialup*), an issue with the order in which services were shut down during the firewall's restart phase would occasionally prevent the firewall from being updated. This issue has been fixed.

Proxies

Support references 84517 - 84824 - 84826 - 84868 - 84877 - 84879

The analysis of a self-signed certificate without a *Subject* field in traffic that matches an SSL decryption rule will no longer cause the proxy to hang.

Support reference 84909

The presence of the **HTTP cache** option in a filter rule set up in a version earlier than SNS 4.3.0 no longer prevents the proxy from starting after a firewall update.

Support reference 84991

In a configuration combining sandboxing and advanced antivirus, the management of temporary files generated for analyzes could cause the affected partition to fill abnormally and significantly degrade proxy performance (slower web access). This anomaly has been fixed.

SSL VPN portal

As the signature of the Java applet used for the SSL VPN portal is close to expiry, users will see a warning message after the signature expires. This applet's signature has been renewed and the applet will be automatically updated when the firewall is updated to SNS version 4.6.3.

Intrusion prevention engine

QoS - SN160(W) model firewalls

Support reference 84937

An anomaly in the management of QoS on SN160(W) firewall models, which occasionally caused the firewall to freeze, has been fixed.

Web administration interface

Interfaces - High availability (HA)

Support reference 84863

HA-dedicated interfaces can no longer be edited from the firewall's web administration interface. This operation, which was allowed by mistake, prevented HA from operating.

High availability (HA) - TPM initialization

Support reference 84530

In HA configurations, initializing the TPM on the active firewall from the web administration interface now correctly launches the initialization of the TPM on the passive firewall.

SNS 4.6.2 bug fixes

System

DMA remapping (DMAR) on SN-M-Series-720 and SN-M-Series-920 firewalls

Support reference 84882

The DMAR mechanism was optimized to improve performance and allow core dump files to be obtained for the purpose of analysis when issues arise on the firewall.

Monitoring power supply modules on SN-M-Series-720 and SN-M-Series-920 firewalls

Support reference 84880

If tasks ran in the wrong sequence while the firewall started up, an alert would sometimes be raised by mistake regarding the operation of power supply modules on SN-M-Series-720 and SN-M-Series-920 firewalls. This issue has been fixed.

Updating firmware on SSD disks

To prevent SSD disks from potentially malfunctioning, a firmware update of such disks is automatically applied when the following firewall models are updated to SNS version 4.6.2:

- SN510, SN710 and SN910 equipped with a 256 GB Innodisk SSD 3TE7,
- SN1100 equipped with a 512 GB Innodisk SSD 3TE7,
- SN3000 with the BIG DATA option (equipped with a 1 TB Innodisk SSD 3TE7).

QoS

The maximum length allowed for the name of a QoS queue that the intrusion prevention engine uses for detections is now the same as for standard QoS queues (31 characters maximum).

Deleting QoS queues

Checks have been added to prevent QoS queues from being deleted when they are used in the firewall configuration.

Network interfaces - SN-M-Series-720 and SN-M-Series-920 models

The speed of network interfaces on SN-M-Series-720 and SN-M-Series-920 firewalls can now be forced to 2.5 Gbit/s.

High availability - SNMPv3

Support reference 84500

SNMP parameters (including *AuthoritativeEngineID* in SNMPv3) are now automatically synchronized as soon as a cluster is created and every time roles are switched in this cluster. The purpose of this synchronization is to stop causing errors on some SNMP monitoring tools.

Updates - Static routing

Support reference 84716

When an SNS 4.6 version is updated from a configuration that contains a static route based on a nonexistent route, routes will no longer stop being reloaded after this faulty route is processed: the routes that follow will be correctly inserted again in the routing tables.
This regression appeared in SNS version 4.3.

Renaming nested object groups

Support reference 81223

Attempts to rename a group included in a group, which is itself included in another group, would fail and cause the system error "The object is included in one or several group(s)". Since the new name of the group was not applied in the object database, any filter rule using the renamed group would then become invalid. This issue has been fixed.

System report (*sysinfo*)

Support references 84211 - 84210

Checks to confirm whether verbose mode has been enabled/disabled for BIRD, BIRD6 and the global VPN policy have been added to the system report generator (accessible from **Configuration** > **Maintenance** > **Configuration** tab).

Checks to confirm whether verbose mode has been enabled/disabled for the proxy were wrongly removed, and are now available again in the system report generator. This regression appeared in version 4.5.1.

Intrusion prevention engine

Maximum number of protected hosts

Support reference 84794

An issue with applying the change made in SNS version 4.5.2 regarding the maximum number of protected hosts has been fixed. So when the firewall is updated to SNS version 4.6.2, it will automatically be restarted a second time if the configuration requires it.

Processing of fragmented packets

Support reference 83882

In configurations that handle a high volume of traffic, an issue with buffer management during the processing of fragmented packets has been fixed. This issue caused the firewall to freeze unexpectedly.

SNS 4.6.1 bug fixes

System

TLS connection to a syslog server

Support reference 84831

In the SSL negotiation phase, there is now an idle timeout for when the firewall attempts to connect to a syslog server in TLS. With this addition, the firewall's log management mechanism will no longer freeze unexpectedly when the syslog server fails to respond during the SSL negotiation phase.

ARP requests to GRE interfaces

Support reference 84625

The firewall no longer sends ARP requests unnecessarily to interfaces that support GRE tunnels. This regression appeared in SNS version 4.4.

GRE tunnels

Support reference 75479

During advanced troubleshooting, packets captured via *tcpdump* over GRE interfaces were malformed. This issue has been fixed.

GRE interfaces

Support reference 84625

In configurations that use GRE interfaces when non-IP packets are present, memory leak issues would sometimes cause network traffic to freeze unexpectedly, which would then require the firewall to be restarted. This issue has been fixed.

IPsec VPN

Support reference 84611

A configuration token *RemoteFetch* has been added to the CLI/Serverd command `CONFIG IPSEC UPDATE`. When this token is set to "0", you can simultaneously:

- Disable the retrieval of remote CRLs on the IPsec tunnel manager when a tunnel is being set up, and
- Disable the OCSP mechanism in the IPsec tunnel manager.

This will prevent an unnecessary wait of several seconds for IPsec tunnels to set up when there are no CRL distribution points (CRLDPs) or none have been configured.

More information about the CLI/Serverd command `CONFIG IPSEC UPDATE`.

Authentication - TOTP

Support reference 84779

To change their passwords via the captive portal, enrolled users must now enter a TOTP.

Support reference 84808

User names are no longer case-sensitive in TOTP authentication.

SN SSL VPN Client and TOTP

Support reference 84689

During the initial connection using SN SSL VPN Client with TOTP authentication enabled, the TOTP field had to be left blank so that the configuration file could be automatically retrieved. The TOTP had to be entered only for the connections that followed. This issue has been fixed.

Advanced antivirus

The new Advanced antivirus license can now be effectively enabled on firewalls that have always used ClamAV; the system message "Not available with this license" no longer appears by mistake.

DHCP - Default route

Support reference 84545

When the firewall obtains an IP address for one of its interfaces via a DHCP server that uses the option *routers x.x.x.x*, the firewall no longer loses its default route if the relevant DHCP lease expires and is not renewed (due to an unreachable DHCP server, for example).

New features and enhancements in SNS 4.6.0

Advanced antivirus - New antivirus engine

The advanced antivirus solution, which is accessible as an option on SNS firewalls, is now based on the *Bitdefender* antivirus engine.

The new antivirus database may take several minutes to download in the following cases:

- When updating a firewall that uses the advanced antivirus from an SNS 3.x or 4.x version to SNS 4.6, except SNS 4.3 versions from version 4.3.13 onwards as the advanced antivirus is already based on *Bitdefender*,
- When switching from ClamAV to the advanced antivirus on a firewall in SNS version 4.6,
- When a passive firewall switches to active mode after the update of a firewall cluster using the advanced antivirus from an SNS 3.x or 4.x version to SNS 4.6, except SNS 4.3 versions from version 4.3.13 onwards as the advanced antivirus is already based on *Bitdefender*,

During this interval, the antivirus analysis will fail, and depending on the configuration of the SNS firewall, traffic may be blocked.

If the firewall is updated to a previous version, it will no longer have an antivirus engine. While the operation required to recover the former antivirus engine exists, it is not supported. You can perform it by following the procedure described in the article **After a downgrade from a version using Bitdefender, I cannot enable Kaspersky** (authentication required).

Telemetry - Antivirus

A new telemetry probe makes it possible to report the number of viruses that the advanced antivirus detected when it is enabled on the firewall.

By sending such data, which remains anonymous, you will be helping Stormshield to improve its future hardware platforms and SNS versions.

More information about telemetry.

Authentication - RADIUS

Support reference 84645

The argument *BindMethodExternal* was added to the CLI/Serverd command **CONFIG AUTH ADVANCED**, making it possible to specify which interface on the firewall must be used for sending RADIUS requests.
This configuration can be built by using the CLI/Serverd command sequence:

```
CONFIG AUTH ADVANCED BindMethodExternal=<interface>
CONFIG AUTH ACTIVATE
```

Resolved vulnerabilities in SNS 4.6.0

IPsec VPN

A moderate severity vulnerability was fixed in the IPsec tunnel manager.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-025.

SNS 4.6.0 bug fixes

System

Network interfaces - routing

Support reference 84706

When the network configuration is reloaded, the routes attached to the interfaces configured in DHCP no longer disappear for several seconds. This regression appeared in SNS version 4.3.

IPsec VPN

In configurations where IPsec tunnels go through a PPPoE (dialup) modem, the IPsec tunnel manager would no longer restart after the dialup was reloaded or after the firewall restarted This regression, which first appeared in SNS version 4.3, has been fixed.

SN160(W) - SN210(W) - SN310 firewalls

Support reference 84725

Some client MAC addresses with the prefix 6c:a1:00 no longer produce corrupted ARP replies from SN160(W), SN210(W) and SN310 model firewalls. This regression appeared in SNS version 4.5.

Authentication

Support reference 84358

When users enter the wrong password for connections via the SSL VPN client or on the captive portal, the firewall no longer wrongly generates the error "LDAP unreachable Bind error" in the alarm log file.

Authentication - TOTP

Support reference 84660

When the default listening port of the web administration interface (TCP/443) is changed, it is now correctly reflected in the link that appears in the window to connect to the firewall, and which leads to the TOTP enrollment page.

RADIUS authentication - Configuration with a backup RADIUS server

Support reference 84555

Under certain circumstances, a double RADIUS authentication request would be sent simultaneously to the main RADIUS server and backup RADIUS server. This anomaly, which would cause the immediate rejection of the authentication attempt, has been fixed.

High availability - Configurations containing several hundred VLANs

Support reference 84522

In some high availability configurations containing several hundred VLANs, requests to show the high availability status will no longer cause abnormally excessive CPU consumption.

DMA remapping (DMAR) on SN1100 firewalls

The DMAR mechanism was optimized to improve performance and allow core dump files to be obtained for the purpose of analysis when issues arise on the firewall.

IPFIX collector - Firewall interface numbers

Support reference 78226

The firewall interface numbers that the IPFIX collector retrieves now match the numbers retrieved in SNMP tables.

Intrusion prevention engine

TLS 1.3 protocol

Support reference 84674

To avoid mistakenly blocking certain streams of TLS 1.3 traffic, the mechanism that analyzes TLS 1.3 certificates on SSL servers is now automatically disabled when a firewall is migrated from a version lower than SNS 4.3 to a version higher than or equal to SNS 4.6.0. It is also disabled by default in the incoming SSL analysis profile *SSL_00* for firewalls in factory configuration in version 4.6.0 or higher.

The mechanism that analyzes TLS 1.3 certificates on SSL servers can be enabled again once its effects are assessed in **Configuration > Application protection > Protocols > SSL**.

New features and enhancements in SNS 4.5.4

TOTP authentication

The configuration interface for the TOTP authentication method has been upgraded to improve user experience.

SNS 4.5.4 bug fixes

NOTE
The fix added in version 4.5.3 regarding the verification of TLS server certificates (Support reference 84244) has been removed. It will be reviewed and included in a future version.

System

SNMP agent - MIB and traps

Support reference 78102

To keep up to date with the recommendations in RFC2578, and to resolve a compatibility issue with some monitoring applications, all SNMP tables in which the first index was set to 0 have been duplicated to new tables in which the first index is set to 1.

Older SNMP tables (index beginning with 0) will still be used by default, but are tagged as obsolete and will be phased out in a future SNS version.

To activate the new SNMP tables (index beginning with 1) on the firewall, you must:

1. Connect to the firewall in SSH/Console mode as a super-administrator (*admin* account),
2. Edit the section [Config] in the ConfigFiles/snmp configuration file and set the configuration token IndexStartAt1 to "1",
3. Run the SNMP agent using the command *ensnmp*.

IPsec tunnel monitoring

The module that monitors the encapsulation of IPsec tunnels in UDP has been fixed and no longer wrongly indicates encapsulation as disabled all the time.

Routing

When tasks are not run in the right sequence during the firewall startup phase, issues may occur when loading certain services such as IPsec or sandboxing. This issue has been fixed.

Intrusion prevention engine

SIP and network address translation (NAT)

Support reference 68822

In a configuration that uses NAT for SIP connections within a rule in firewall mode, when the firewall receives a second INVITE request for a connection that has already been set up, NAT will no longer malfunction and the established SIP connection will no longer shut down unexpectedly.

New features and enhancements in SNS 4.5.3

Quality of Service (QoS) - Filtering

QoS bypass queues can now be selected for filter rules in security policies.

Quality of Service (QoS) - Traffic shapers

Configuration parameters for traffic shapers have been improved for the application of QoS. Incoming and outgoing throughput can now be configured separately for each interface. Class-based queuing can therefore be set up in LAN/WAN/DMZ and multiple WAN architectures.

SN-M-Series-720 and SN-M-Series-920 firewall support

SNS version 4.5.3 and higher supports SN-M-Series-720 and SN-M-Series-920 firewalls.

More information about SN-M-Series firewalls

Resolved vulnerabilities in SNS 4.5.3

vim file editor

A medium severity vulnerability was fixed by removing the Vim file editor.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-006.

SNS 4.5.3 bug fixes

System

High availability - IPsec VPN

Support references 84273 - 84460

An issue regarding the synchronization of Security Associations (SA) during a switch in a cluster, which could cause IPsec VPN tunnels to malfunction, has been fixed.

High availability (HA) - Synchronization

Support reference 84340

The HA synchronization mechanism no longer causes errors when it does not detect the file relating to the backtracking mechanism for configurations deployed via SMC.

Authentication - TOTP

Unselecting the checkbox for authentication via TOTP on the captive portal (**Users** > **Authentication** menu) would wrongly disable the TOTP enrollment page on the captive portal, even though this page is necessary for other modules that potentially use TOTP (e.g., SSL VPN, web administration interface, SSH/Console or IPsec/Xauth). This anomaly has been fixed.

IPsec VPN

Support reference 84568

A parameter was missing from the keepalive option when the command to reload an IPsec policy was called. This anomaly caused system event 52 "The event returned an unhandled error code: IPSEC_KEEPALIVE_30->4" but would not prevent IPsec VPN tunnels from being set up anyway.
This regression, which first appeared in SNS version 4.3.8, has been fixed.

Support reference 84569

When a keepalive packet is successfully sent, it no longer wrongly raises system event 52 "The event returned an unhandled error code: IPSEC_KEEPALIVE_30->4". This regression appeared in SNS version 4.3.8.

Support references 82578 - 84680

Issues with competing access, which caused instability in IPsec tunnels, have been fixed. These issues prevented effective tunnel monitoring, and generated entries such as "job load of XXX exceeds limit of YY" in IPsec VPN logs.

IPsec VPN through a dialup default gateway

Support reference 84631

When the default gateway is based on a PPPoE modem (dialup connection), IPsec tunnels set up through this default gateway now recover correctly after the dialup connection goes down temporarily and recovers.

Dynamic NAT and DHCP for outgoing interfaces

Support reference 83297

When filter rules were reloaded in the intrusion prevention engine, if there was among them a dynamic NAT rule associated with the use of DHCP to define the addresses of outgoing interfaces, it would cause the firewall to freeze. This issue has been fixed.

Custom web services

Support reference 84496

Under certain conditions, custom web services that contained a wildcard (*) in their FQDN could fail to be correctly applied in block filter rules. This anomaly has been fixed.

In large databases of custom web services, imports of custom web services would be disrupted and a warning message would appear when the partition designated to receive the custom service database reaches 95% of its capacity.

Log management mechanism

Support references 84605 - 84577

Issues regarding memory leaks in the log management mechanism, which could cause it to shut down unexpectedly, have been fixed.

Static routing - IPsec VPN

Support reference 84507

When filter rules are reloaded after a static route used by an IPsec tunnel is changed, the firewall's static route engine no longer runs the risk of shutting down unexpectedly.

Bird dynamic routing

Support reference 84337

Networks declared in Bird dynamic routing are once again classified correctly as protected networks in the intrusion prevention engine, and no longer wrongly raise an alarm regarding an IP spoofing attempt. This regression appeared in SNS version 4.3.

SSL VPN

Support reference 84610

The *inactive=<seconds>* function on the SSL VPN can now be correctly applied by using the CLI/Serverd command `CONFIG OPENVPN UPDATE`.

Intrusion prevention engine

Reloading the network configuration

Support references 84522 - 84198

The mechanism that reloads the network configuration (especially when no changes are made to the configuration) has been optimized to shorten reloading time, and reduce associated CPU consumption and the duration of the firewall's downtime during such operations.

IEC61850 MMS protocol - IDS mode

The IDS inspection mode applied to a filter rule that affects IEC61850 MMS traffic no longer wrongly behaves like the IPS inspection level, and no longer blocks triggering packets instead of raising only the relevant alarms.

HTTP protocol

Support reference 82824

Following a PUT or POST request sent by the client, and when the HTTP server sends back a response other than the message "100 Continue", the HTTP protocol analysis engine no longer raises the block alarm "Additional data at end of reply" (http:150) by mistake.

TLS protocol - Verification of server certificates

Support reference 84244

The mechanism that verifies server certificates has been optimized - when several requests regarding the verification of the same server certificate are received at almost the same time, only one internal request will be sent to avoid saturating the mechanism's queue, and avoid potentially causing the mechanism to freeze for several tens of seconds.

Web administration interface

HTML tags in log messages

Support reference 84494

When the web administration interface detects HTML tags in error messages associated with certain log entries, it no longer wrongly displays the error message "XSS protection: HTML tag found in following commands".

Filtering with QoS - HTML tags in warning messages

The warning message that appears after enabling or disabling a filter rule that refers to a deleted QoS queue contained HTML tags by mistake. This anomaly has been fixed.

Certificates and PKI

Support reference 84470

Attempts to generate the CRL of a sub-certification authority no longer wrongly require the root certification authority's private key and no longer causes a system error.

Certificates and PKI - CRL distribution points (CRLDP)

Support reference 84618

When CRDLPs were added (**Objects** > **Certificates and PKI** > **Certificate profiles** tab of the selected CA) the option to **Enable regular retrieval of certificate revocation lists (CRL)** was no longer offered. This anomaly, which could prevent certificate-based IPsec tunnels from being set up, has been fixed.

New features and enhancements in SNS 4.5.2

IPsec VPN

Support reference 84280

Data returned by the `showSPD` command is now more comprehensive and includes information regarding VPN tunnel endpoints.

Resolved vulnerabilities in SNS 4.5.2

ClamAV antivirus

A moderate severity vulnerability was fixed in ClamAV.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-017.

SNS 4.5.2 bug fixes

System

IPsec VPN - Router objects

Support reference 82369

In configurations where IPsec VPN tunnels were set up through a router object, switching from one gateway to another within this router object could prevent some IPsec VPN tunnels from being automatically set up again. This regression, which first appeared in SNS version 4.2, has been fixed.

Quality of Service (QoS)

Issues relating to packet loss in traffic shapers configured with low bandwidth have been fixed.

Whenever traffic went through a default QoS queue, return packets would not take the same queue. This issue, which caused packet loss, has been fixed.

The maximum length allowed for queue names in the CLI/Serverd command `CONFIG OBJECT QOS QID REMOVE` has been raised from 20 to 32 characters. Using this command therefore no longer causes issues when handling strings with names that exceed 20 characters.

The parallel processing of priority-based queues (PRIQ) no longer blocks other such queues when one of them saturates an interface.

Disabling then enabling QoS again with the command `sfctl` (`sfctl -q 0 && sfctl -q 1`) no longer prevents QoS queues from being processed.

Qualité de service (QoS) - Monitoring

Support reference 84509

In configurations that have more than 32 interfaces (physical, VLAN, etc.), the command used while monitoring QoS could cause the SNS firewall to freeze. This regression, which first appeared in SNS version 4.3, has been fixed.

Configuration backups

The TOTP database is now included in the backed up items.

TOTP authentication

Whenever an LDAP domain name exceeds 30 characters, the enrollment QR code and TOTP information now appear correctly in the authentication portal.

Static routing and IPsec VPN tunnels

Support reference 84367

In configurations with a static route that passes through the IPsec interface, reloading the filter policy would disconnect traffic passing through the IPsec VPN tunnel. This regression, which first appeared in SNS version 4.3, has been fixed.

SSL traffic towards the SNS firewall

Support reference 84264

As TLS 1.2 is the lowest protocol version that can be used for SSL traffic towards the SNS firewall, the configuration tokens corresponding to SSL v3, TLS v1.0 and TLS v1.1 have been removed from the configuration file of the SSL protocol so that they cannot be used.

SSL proxy

Support reference 84524

In configurations that contain an SSL decryption rule and an SSL filter rule set to “Do not decrypt”, the proxy of the SNS firewall could wrongly exclude one of the TLS extensions negotiated between the client and the proxy. This issue, which made it impossible to set up connections corresponding to this TLS extension, has been fixed.

Removal of a network interface alias

Support reference 79663

Checks have been added to prevent interface aliases from being deleted when they are used in the configuration of the SNS firewall.

High availability (HA) - Synchronization

Support reference 83721

Anomalies that may cause excessive memory consumption have been fixed in the mechanism that synchronizes the HA configuration.

USB devices/4G modems - Huawei E3372h-320

Support reference 84253

Fixes have been included to support version 10 of the firmware on Huawei E3372h-320 USB devices/4G modems.

SNMP agent - link aggregation

Support reference 82991

When a physical link was lost in an aggregate, "*aggregate link down*" SNMP traps could sometimes get lost, and were not re-sent over the other physical links in the aggregate. This issue has been fixed.

Intrusion prevention engine

HTTP protocol

Support reference 84292

An issue regarding the HTTP protocol analysis, which would cause the SNS firewall to freeze, has been fixed.

Number of protected hosts

Support reference 84537

An issue regarding the maximum number of protected hosts, which would arise when an SNS firewall was updated to version 4.3.7 or higher, has been fixed.

New features and enhancements in SNS 4.5.1

IMPORTANT
SNS version 4.5 is only compatible with the SSL VPN client in version 3.1 or OpenVPN client 2.5 (or higher).
The SSL VPN client (or OpenVPN client) must be updated on client workstations before the firewall is updated to SNS version 4.5.

Two-factor authentication (2FA)

In SNS version 4.5, the authentication processes managed by the firewall can be made more secure through a new 2FA method in which time-based one-time passwords (TOTP) can be used.
This additional step to protect access is built into the firewall and does not require any third-party TOTP solution. Users who authenticate with an SNS TOTP only need to use an application on their smartphones or in their browsers to generate TOTPs.

The advantage of this method is that it can be enabled for all types of authentication: captive portal, SSL VPN tunnel, web administration interface, console or SSH connections and IPsec/Xauth VPN tunnels.

Do note that since this 2FA method is built into each firewall, users must use as many TOTPs as the number of firewalls to which they must connect.

More information about TOTP authentication.

Dynamic multicast routing

IMPORTANT
This is an early-access feature and not intended for use on firewalls in a production environment. Please refer to the section on Limitations and explanations on usage before enabling this feature.

SNS 4.5 versions support dynamic multicast routing over IGMPv2 and v3, and PIMv2.
Dynamic multicast routing can be configured in **Configuration** > **Network** > **Multicast routing** or by using CLI/Serverd `CONFIG MULTICASTROUTING` commands.

NOTE
Dynamic multicast routing and static multicast routing cannot be enabled at the same time.

More information about dynamic multicast routing.

S7 Plus protocol

In SNS version 4.5, the S7 Plus industrial protocol (intellectual property of Siemens) can now be analyzed.

More information about S7 Plus protocol analysis.

OPC-DA protocol

The protocol analysis engine now makes it possible to differentiate read and write operations for the OPC-DA protocol. This guarantees that OPC-DA traffic passing through the firewall will be more thoroughly monitored.

More information about OPC-DA protocol analysis.

IEC 60870-5-104 protocol

Support reference 82460

A new alarm "IEC 60870-5-104: Invalid TESTFR act message with connection context" (iec104:756) was created to allow IEC 60870-5-104 *TESTFR act* packets to pass through (stateful inspection of packets) while leaving the IEC 60870-5-104 protocol analysis enabled.

Description of network interfaces

Support reference 81461

Descriptions (optional) added to network interfaces from the web administration interface are now stored in `key=value` format in the network interface configuration file. These descriptions can then be retrieved when the program is restored via USB key.

Automatic disconnection of expired SSL VPN sessions

A maximum idle timeout can now be set on the SSL VPN service, after which inactive SSL VPN sessions will be automatically disconnected.

This option can only be configured through the CLI/Serverd command:

```
CONFIG OPENVPN UPDATE Inactive=x (seconds)
```

HTTPS block pages

The pages that make it possible to block HTTPS traffic not allowed by SSL filtering have been modified. The template for these pages can be completely customized.

Telemetry

The telemetry service in SNS version 4.5 now reports new data:

- Number of objects by type,
- Number of filter and NAT rules,
- Number of IPS alerts,
- Number of IPS signatures used.

By sending such data, which is completely anonymous, you will be helping Stormshield to refine the dimensions and restrictions on future hardware platforms and SNS versions.

More information about telemetry.

IPsec encryption profiles

Diffie-Hellman groups DH31 and DH32 are now available in IPsec encryption profiles. Do note that these profiles cannot be selected if the firewall is in ANSSI *Diffusion Restreinte* mode.

More information about IPsec encryption profiles.

IPsec VPN logs

Support reference 82931

In the log line "Installing IPSEC SA failed", *SPI in* and *SPI out* values are now included to facilitate the analysis of the issue encountered.

Alert when NVM utilities are updated for Intel network cards

Event 152 "Network card software" makes it possible to inform the administrator of automatic updates or failures while updating NVM utilities that manage firmware versions of Intel network cards.

SNS 4.5.1 bug fixes

System

Admin account passwords containing UTF-8 characters

Support references 81324 - 80974 - 82761 - 84322 - 84503

Whenever the password of the *admin* account contained UTF-8 characters (e.g., the € character), it could no longer be changed in the web administration interface. This regression, which first appeared in SNS version 4.1, has been fixed.

Time taken to list certificates protected by the TPM

Support reference 83999

It now takes much less time to list all the certificates protected by a TPM due to restricted access to the TPM while this operation is in progress.

Showing comments assigned to members of a group

Support reference 82069

Comments assigned to members of a group are now shown when the contents of the group are listed (by scrolling over the group or by using the command `CONFIG OBJECT GROUP SHOW`).

SSL certificate authentication

Support reference 80325

When SSL certificate authentication is deleted, the user's connection to the firewall's web administration interface or the authentication captive portal is no longer wrongly blocked.

SSL proxy

Support reference 84316

An anomaly that occurred when the SSL proxy verified the trust chain has been fixed - access to Cisco Webex servers is no longer wrongly blocked.

Monitoring

Support reference 84203

When the monitoring data file is corrupted, monitoring services no longer freeze and a new monitoring data file is generated.

Disabling the parent interface of a VLAN

Support reference 81749

Whenever the parent interface of a VLAN was disabled, the firewall would wrongly send a GARP (Gratuitous ARP) packet with the IP address of the disabled interface as well as the legitimate GARP packet with the VLAN's IP address. This anomaly has been fixed.

Handling excessively long pre-shared keys (PSK) with CLI/Serverd commands

Support reference 83626

Simplified error messages are now shown when handling (creating or modifying with CLI/Serverd commands) PSKs that are too long. Now only a single message appears: "PSK too long".

Storing logs on SD cards - SN160(W), SN210(W) and SN310 firewalls

Log storage devices can no longer be formatted while logs are still active.

Network

Multicast routing

Support reference 84250

Fragmented multicast packets arriving on the firewall are now correctly forwarded to all network interfaces involved in multicast routing.

Version 4.5.0 not published

Version 4.5.0 is not available to the public.

New features and enhancements in SNS 4.4.1

Granularity of QoS and routing by application for web services according to the SLA (SD-WAN)

In SNS version 4.4, you can identify the services associated with certain widely recognized web traffic and therefore differentiate Salesforce traffic from YouTube, Microsoft 365 or Zoom traffic, for example. Custom web services can also be created as necessary.
Granular SLA, QoS and routing by application policies can then be defined for each web service used in the organization, making it possible to guarantee optimal connectivity for high-priority web traffic.

More information about web services.

Security policy adapted to real-time SaaS applications

The ability to identify web services also makes it possible to adapt the security policy to the various traffic streams identified, by disabling some unnecessary security analyses for such traffic. For example, there is no need to force the identified application traffic to pass through the proxy, allowing such traffic to move more quickly, while relieving the proxy for the benefit of other web traffic.

These web service objects and custom web services also make it possible to lift some restrictions relating to FQDN objects.

IEC61850 MMS protocol

The intrusion prevention engine analyzes the IEC61850 MMS protocol in addition to the MMS protocol.

Jumbo frames supported on SN160(W), SN210(W) and SN310 firewall models

Jumbo frames are now supported on SN160(W), SN210(W) and SN310 firewall models starting from version SNS 4.4. This makes it possible, in particular, to correctly configure such firewalls when an ISP uses a Maximum Transmision Unit (MTU) slightly higher than 1500 bytes.

Even though this MTU can be set to a maximum of 9198 bytes on SN160(W) and SN210(W) firewalls, and 8996 bytes on SN310 firewalls, do note that due to the hardware limitations on these models, the software will verify the checksums of packets with MTUs higher than 1600 bytes. As a result, this may affect the overall performance of these firewall models.

SSL VPN - Backup link

On a firewall that has two separate Internet links, a backup IP address can now be set for the SSL VPN server (different network from the one that includes the primary address). Doing so would alleviate network issues on the interface initially defined and allow clients to continue using the SSL VPN service. The information for the backup connection is automatically added to the configuration file of the SSL VPN client.
This backup IP address can only be configured through the CLI/Serverd commands:

```
CONFIG OPENVPN UPDATE serverPublicAddrSecondary=w.x.y.z
CONFIG OPENVPN ACTIVATE
```

The SSL VPN service can also be configured so that all SSL VPN sessions that have reached the maximum idle timeout configured will be automatically disconnected.

IPsec performance

Support reference 81691

The mechanism that optimizes the distribution of the IPsec service's encryption and decryption operations has been modified. The changes improve its performance when encryption is applied with an incoming interface containing plaintext traffic and an outgoing interface containing encrypted traffic.

CPUs can now be distributed in a static manner to process packets from the IPsec service on the firewall. This configuration can only be modified with the following CLI/serverd command:

```
CONFIG IPSEC CRYPTOLB UPDATE ifincoming=<interface> ifoutgoing=<interface>
state=<0|1>
```

SNMPv3 - Secure communications

In SNS version 4.4, SHA2 has been added to the list of algorithms (SHA1 and MD5) that can be used to secure SNMPv3-based communications.

SNMP agent - Listening IP address on the service

It is now possible to specify the firewall interface through which SNMP requests will move. This can be done by using the *bindaddr* argument in the CLI/Serverd command:

```
CONFIG SNMP SYSTEM BindAddr=<host>
```

Find out more

Prohibiting a downgrade to an earlier firmware version

On firewalls in version 4.4, downgrades to an earlier firewall version can be prohibited. This makes it possible to prevent a fixed vulnerability from being reintroduced, for example.

This function can be enabled exclusively through the CLI/Serverd command:

```
SYSTEM UPDATE DOWNGRADE off
```

Do note that downgrades to an earlier firmware version are allowed by default.

Find out more

Telemetry

Telemetry on firewalls in SNS version 4.4 has added to existing indicators (percentage of CPU used, percentage of memory used and volume of logs generated) data regarding the use of the proxy: number of connections by protocol and number of simultaneous connections through the proxy.

By sending such data, which is completely anonymous, you will be helping Stormshield to refine the parameters of the proxy's performance for future SNS versions.

Resolved vulnerabilities in SNS 4.4.1

IXL network cards

A moderate severity vulnerability was fixed in the IXL network card firmware.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-049.

Network cards with an I210 controller

Moderate severity vulnerabilities have been fixed in the firmware on network cards with an I210 Intel controller (SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SNi20 and Sni40 firewall models).

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2020-038,
- https://advisories.stormshield.eu/2020-039,
- https://advisories.stormshield.eu/2020-043.

A low severity vulnerability has been fixed in the firmware on network cards with an I210 Intel controller (SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SNi20 and SNi40 firewall models).

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2020-046.

SNS 4.4.1 bug fixes

System

SSH connection to a cluster

Administrators connected to the active member of the cluster in SSH with their own account (other than the *admin* account) were forced to enter the password of the *admin* account if they also wanted to connect to the passive member of the cluster in SSH. This anomaly has been fixed.

HTTP requests

Support reference 83085

After a component was changed in SNS version 4.1.1, the *User-Agent* and *Connection: close* headers were no longer found in HTTP requests, which could prevent CRLs from being automatically retrieved. This issue has been fixed.

SSL proxy

Support reference 73331

The SSL proxy now accepts the "_" character in FQDN names for the SNI (Server Name Indication) extension.

CLI/serverd commands

The help returned from the command `CONFIG IPSEC PEER NEW HELP` now indicates a range of correct values for the token *ikedscp* (<0-63> instead of the previous wrong value of <0-56>).

The help returned from the command `CONFIG COMMUNICATION SYSLOG PROFILE UPDATE HELP` now specifies the existence of the token *LogRouterStat*.

Hardware management - SN160(W), SN210(W) and SN310 model firewalls

Support references 82933 - 84307

When a SN160(W), SN210(W) or SN310 model firewall is powered down, an anomaly in the order in which the hardware management mechanisms were shut down prevented the *Online* LED from switching off. This anomaly, which could give the false impression that the firewall has not been correctly shut down, has been fixed.

Filter - NAT

Support reference 82534

An anomaly while exporting NAT rules in a CSV file has been fixed: the export now factors in the contents of the **Protocol** column.

Support reference 79079

An SSL VPN interface (TCP/UDP) can now be selected directly as the source interface in a filter rule.

IPsec VPN and GRE

Support reference 82051

ESP -> GRE -> ESP double encapsulation (encapsulation of an IPsec tunnel in a GRE tunnel, which is in turn encapsulated in an IPsec tunnel) is operational once again. This regression appeared in SNS version 4.1.

Limiting the duration of remote administrator sessions

The function allowing the super-administrator to limit the maximum idle timeout allowed for administrator accounts on the firewall is operational once again (regression appeared in SNS version 4.2).

HTTP proxy

Support reference 80100

Changing the ICAP configuration (in particular disabling this configuration) of an HTTP protocol analysis profile while a connection involving ICAP is in progress no longer makes the proxy suddenly freeze.

Inactive Ethernet interface with a forced MAC address and attached VLAN

Support reference 80970

When forcing the MAC address of an Ethernet interface that is parent to a VLAN, the VLAN would not inherit the forced MAC address. This anomaly has been fixed.

Console mode and serial port enabled

Support reference 82054

On firewalls with an enabled console mode and serial port display configuration, connecting a keyboard and monitor was exceptionally mandatory in order to restart in *single user* mode (e.g., to change the password of the *admin* account). This issue has been fixed.

Logs

Support reference 82287

The size of the log processing queue and the memory allocated to this process have been increased to minimize the risk of losing logs when the firewall handles a high volume of traffic.

Intrusion prevention

MMS protocol - IDS mode

The IDS mode applied to a filter rule that affects MMS traffic wrongly behaved like the IPS mode and blocked triggering packets instead of raising only the relevant alarms.

NTP protocol

The "NTP: KoD denied" (alarm ntp:456) alarm is no longer raised by mistake for legitimate NTP traffic when an NTP KoD (Kiss'o'Death) packet is not found in the whitelist and is set to the IP address of the NTP server.

SIP protocol

In a filter rule of incoming SIP traffic, with the option **Redirect incoming SIP calls (UDP)** enabled (internal SIP server), OPTIONS requests that serve to request the capacity of the SIP server are no longer blocked by mistake. This regression appeared in SNS version 4.0.3.

Ethernet protocols

The analysis profile "(0)" was always applied for the analysis of Ethernet protocols (Profinet IO, Profinet RT, IEC 61850, etc.) and other profiles were ignored. This issue has been fixed.

TCP-UDP protocol

An anomaly in the management of the connection counter on the TCP-UDP protocol analysis engine has been fixed.

ARP requests while reloading the configuration of the intrusion prevention engine

Support reference 84272

An issue with competing access relating to ARP requests sent while reloading the configuration of the intrusion prevention engine would occasionally end up freezing the firewall unexpectedly. This issue has been fixed.

Web administration interface

Directory configuration

Support reference 82849

Choosing *None* in the backup LDAP server selection field no longer causes the system error "Invalid backup host".

IPsec VPN

Support reference 83017

The *Inactive* value can no longer be assigned to DPD (Dead Peer Detection) mode when an IPsec peer is being created or modified. This value was in fact no longer supported and caused a system error "Argument error Command: CONFIG IPSEC PEER UPDATE dpd_mode=off".

URL/SSL/SMTP filtering

Support reference 83587

Modifying a URL/SSL/SMTP filter rule by dragging and dropping no longer activated the **Apply** button, even though the changes were applied. This anomaly has been fixed.

VLAN interfaces

Support reference 83873

Creating a VLAN, renaming it without having saved changes to the configuration beforehand, then creating another VLAN on the same physical interface and renaming the second VLAN, would cause an error indicating that both VLANs had the same name. This anomaly has been fixed.

Authentication - Microsoft Active Directory

Support reference 52539

Whenever the request to display users in an external Microsoft Active Directory exceeded the *MaxSizeLimit* parameter set on the Microsoft Active Directory server, the system error message *No user found* is no longer shown by mistake: the firewall now shows the maximum number of users that can be retrieved and shows a message indicating that the maximum number of retrievable users has been reached.

Searches in logs

Support reference 77587

Optimizations have been implemented to reduce the search time in logs.

SSL VPN domain name

Support reference 74996

The DNS **Domain name** field meant for clients of the SSL VPN service would wrongly reject the "_" character. This anomaly has been fixed.

Filtering

Support reference 80794

Whenever a rule that uses the ICMP protocol as a filtering criterion was cloned, and its copy was modified by replacing ICMP with another protocol, and the copy was in turn cloned in a third rule, the third rule would wrongly contain references to the ICMP protocol of the original rule. This inappropriate behavior, which prevented the filter policy from being enabled and caused an error “This rule contains a filter on ICMP messages, but ICMP is not the defined protocol”, has been fixed.

Network objects - MAC address range

Support reference 77968

During the creation of a MAC address network object, the use of condensed notation (without separators such as ":" or "-", e.g., 01af3b54c89c) is accepted and no longer raises the error message "Invalid MAC address".

System monitoring

Support reference 81041

The system monitoring mechanism would wrongly and systematically send the command to verify the synchronization of the cluster, even when HA was not enabled on the firewall. This anomaly, which displayed the error message "200 HA not initialized" every minute in the panel that displays message at the bottom of each configuration module, has been fixed.

Version 4.4.0 not published

Version 4.4.0 is not available to the public.

Version 4.3 LTSB

Long-Term Support Branch

Version 4.3 LTSB (for Long-Term Support Branch) of SNS has its own set of dedicated Release Notes.

Major or minor versions labeled “LTSB” are considered versions that will be stable over a long term, and will be supported for at least 12 months. These versions are recommended for clients whose priority is stability instead of new features and optimizations.

For more information, refer to the Network Security & Tools Product lifecycle document.

Resolved vulnerabilities in SNS 4.2.14

ClamAV antivirus

A moderate severity vulnerability was fixed in ClamAV.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-017.

SNS 4.2.14 bug fixes

System

High availability (HA) - Synchronization

Support reference 83721

Anomalies that may cause excessive memory consumption have been fixed in the mechanism that synchronizes the high availability configuration.

SSL traffic towards the SNS firewall

Support reference 84264

As TLS 1.2 is the lowest protocol version that can be used for SSL traffic towards the SNS firewall, the configuration tokens corresponding to SSL v3, TLS v1.0 and TLS v1.1 have been removed from the configuration file of the SSL protocol so that they cannot be used.

IPsec VPN - Router objects

Support reference 82369

In configurations where IPsec VPN tunnels were set up through a router object, switching from one gateway to another within this router object could prevent some IPsec VPN tunnels from being automatically set up again. This regression, which first appeared in SNS version 4.2, has been fixed.

Intrusion prevention engine

Number of protected hosts

Support reference 84537

An issue regarding the maximum number of protected hosts, which would arise when an SNS firewall was updated to version 4.2.11 or higher, has been fixed.

SNS 4.2.13 bug fixes

Intrusion prevention engine

Sending ARP requests while reloading the configuration of interfaces in the intrusion prevention engine

Support reference 84272

An issue with competing access, which would occur when the intrusion prevention engine reloaded the configuration of interfaces while ARP requests were being sent, has been fixed. This issue made the firewall freeze.

SNS 4.2.12 bug fixes

System

Creating interfaces

Support reference 75064

Configurations that contain several hundred interfaces (virtual, VLAN, etc.) no longer cause excessive CPU consumption after network interface configuration files are repeatedly reloaded.

High availability

Support reference 84100

In a high availability configuration, when a link is lost on the active node of the cluster, the switch from the active to passive node now takes place faster. This allows the passive node to switch more quickly to an active state, therefore minimizing interruption to network traffic.

Outgoing traffic statistics - SSL VPN

Support reference 79814

The counters that counted packets leaving the network interface linked to the SSL VPN were no longer refreshed This anomaly, which first appeared in SNS version 4.1, has been fixed.

Regular CRL retrieval

Support reference 84431

When the command `PKI CONFIG UPDATE` is used, an incorrect value (such as *Any*) can no longer be entered in the *checkcrlbindaddr* argument.

New features and enhancements in SNS 4.2.11

Intrusion prevention

Multicast IP addresses presented as source addresses

Support reference 84041

A new alarm "Multicast IP src packet" (alarm ip:755), which makes it possible to block by default packets that present a multicast address as a source address, has been added to the intrusion prevention engine.

Resolved vulnerabilities in SNS 4.2.11

OpenSSL

A high severity vulnerability was fixed in OpenSSL.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-008/.

vim file editor

Moderate severity vulnerabilities affecting the *vim* file editor have been fixed.

Details on these vulnerabilities can be found on our website https://advisories.stormshield.eu/2022-004.

ClamAV antivirus

A moderate severity vulnerability was fixed in ClamAV.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-005.

Intrusion prevention engine

A high severity vulnerability was fixed in the intrusion prevention engine.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-009.

SNS 4.2.11 bug fixes

System

Filter - NAT

Support reference 82567

In some cases, the **TCP (c/s)** connection threshold set in the Quality of Service (QoS) settings in a filter rule were not applied. This issue has been fixed.

Resolved vulnerabilities in SNS 4.2.10

SSL VPN

A high severity vulnerability was fixed in SSL VPN.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-003.

CPU micro-codes - SN1100, SN2100, SN3100 and SN6100 firewall models

Moderate severity vulnerabilities have been fixed in the CPU micro-codes on SN1100, SN2100, SN3100 and SN6100 firewall models.

Details on these vulnerabilities can be found on our website https://advisories.stormshield.eu/2021-067.

SNS 4.2.10 bug fixes

System

IPsec VPN with NAT-T and *Path MTU Discovery* (PMTUD) enabled

Support reference 83292

When the PMTUD option (CLI/Serverd command `CONFIG IPSEC UPDATE slot=<1-10> PMTUD=<0|1>`) was enabled for an IPsec tunnel going through NAT-T and using the combination of AES-CBC 256 and SHA2_256 algorithms, packets with an MTU that was too high would occasionally be generated. Such packets would then be blocked by the network devices that they are supposed to pass through.

Proxies

Support reference 79295

The SSL proxy now correctly processes certificates that present both an empty *Subject* field and a filled in *SubjectaltName* field.

HTTP proxy

Support reference 83607

Issues with competing access to connection counters, which could cause the proxy to shut down unexpectedly, have been fixed.

URL classification - Extended Web Control (EWC)

Support reference 83619

An anomaly affecting communication with EWC servers would occasionally occur after several unsuccessful attempts to classify a URL. This anomaly has been fixed.

Using an explicit proxy and Extended Web Control (EWC) URL classification database

Support reference 82913

Using an explicit proxy and the EWC URL database at the same time would sometimes make the URL classification engine shut down unexpectedly. This issue has been fixed.

NAT - VLANs

Support reference 79759

In a configuration that supports several VLANs on the same physical interface and which implements address translation with ARP publication on the same VLANs, GARP (*Gratuitous ARP*) packets would be wrongly sent to only one of these VLANs. This issue has been fixed.

Intrusion prevention

Android WhatsApp and *Facebook* applications

Support reference 82865

Legitimate packets from *Android WhatsApp* or *Facebook* applications would sometimes wrongly trigger the block alarm "Different SSL version" (ssl:117 alarm). This regression, which first appeared in SNS version 4.2.1, has been fixed.

Web administration interface

Dashboard - Virtual *Pay As You Go* (PAYG) machines

Support reference 83326

The PAYG widget found on virtual machines in *Pay As You Go* mode no longer show HTML markers by mistake.

Resolved vulnerabilities in SNS 4.2.9

CPU microcode - SNi20 model firewalls

Moderate and high severity vulnerabilities have been fixed in the CPU microcode on SNi20 model firewalls.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2021-040,
- https://advisories.stormshield.eu/2021-043.

CPU microcode - SN2100 and SN3100 model firewalls

Moderate and low severity vulnerabilities have been fixed in the CPU microcode on SN2100 and SN3100 model firewalls.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2021-041,
- https://advisories.stormshield.eu/2021-042.

SNS 4.2.9 bug fixes

System

Authentication - SSL VPN

Support references 78073 - 81741

In a configuration using a main external LDAP directory and a backup external LDAP directory, switching from the main directory to the backup directory would occasionally cause the authentication engine to shut down unexpectedly, preventing uses from accessing the SSL VPN. This issue has been fixed.

Authentication to an LDAPS server

Support reference 84199

The firewall was occasionally unable to authenticate on an LDAPS server when a certificate signed by a CA with a CRL was presented. This issue has been fixed.

Hardware monitoring - Disks

Support reference 84083

The mechanism that analyzes the results of SMART tests has been adapted to stop raising inappropriate alerts on some SSD references.

SNMP Agent

Support reference 81710

Several anomalies that could cause memory leaks in the SNMP agent have been fixed.

Web administration interface

High availability

Support reference 83724

When an error occurs while attempting to connect a firewall to a cluster, the web administration interface no longer freezes when the “High Availability configuration in progress” message appears.

Resolved vulnerabilities in SNS 4.2.8

Connections via console or SSH

A high severity vulnerability was fixed on connections via console or SSH.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-069/.

Intrusion prevention

A medium severity vulnerability was fixed in intrusion prevention engine.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-050/.

SNS 4.2.8 bug fixes

System

IPsec VPN

Support references 83903 - 84062

IPsec VPN tunnels that were set up with certificate authentication would occasionally fail when the private key was protected by the TPM. A "No private key found for <CN>" error would then be logged. This issue has been fixed.

High availability (HA) - Firewall updates

Whenever the passive firewall in an HA cluster was updated to SNS version 4.2.3 or higher, then switched to active mode, the new passive firewall in SNS version 4.2.3 or higher could not be successfully updated. This issue has been fixed.

Authentication

Support reference 83411

Whenever an **Authentication rule** filter rule redirected traffic to the captive portal (authentication portal), **Sponsorship** could no longer be selected as the authentication method on this captive portal's page. This anomaly appeared in SNS version 4 and has since been fixed.

Network

Support references 82366 - 83624 - 84201

Bird dynamic routing engine

Despite the static routes declared in the Bird configuration and the dynamic routes that Bird learned, the corresponding networks were not automatically added to the table of protected addresses. This issue has been fixed.

Intrusion prevention

Antivirus analysis

Support reference 80792

Since Zoom application traffic is incompatible with the antivirus analysis, these CNs have been added to the CN group *proxyssl_bypass*.

SMB/CIFS protocol

Support reference 83660

An issue that caused SMB packets to be blocked was fixed after the SMB/CIFS protocol analysis engine factored in the padding bytes at the end of SMB packets.

NTP

The "NTP: KoD denied" (ntp:456) alarm is no longer raised by mistake and in loop when the KoD (Kiss-of-Death) is attributed to the IP address of the NTP server.

HTTP

Support reference 83553

The HTTP protocol analysis has been optimized to avoid consuming too much memory and inappropriately overloading the firewall.

Resolved vulnerabilities in SNS 4.2.7

Vim file editor

Moderate severity vulnerabilities affecting the Vim file editor have been fixed.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2021-061/,
- https://advisories.stormshield.eu/2021-062/,
- https://advisories.stormshield.eu/2021-063/,
- https://advisories.stormshield.eu/2021-064/.

IPsec VPN

A moderate severity vulnerability was fixed in the IPsec VPN tunnel manager.

Details on these vulnerabilities can be found on our website https://advisories.stormshield.eu/2021-065/.

SNS 4.2.7 bug fixes

System

IPsec VPN

Support reference 82645

In IPsec configurations that use groups containing address ranges, mounted tunnels could be interrupted when such groups were modified, generating *TS_UNACCEPTABLE* errors as a result. This issue has been fixed.

Support reference 83354

Whenever an IPsec policy contained one or several *bypass* rules (in which the peer is *None* and the rule was created to exclude the following rules from the encryption policy), these *bypass* rules were not applied to networks defined by static routes.
This issue was fixed with the addition of an IPsec *bypass* option in the step during which the static route is defined.

4G USB key

Support reference 82757

Huawei E3372h-320 4G USB keys are now supported, so they no longer cause the host firewall to unexpectedly restart.

Authentication by SSL certificate with TLS v1.3

Support reference 82759

SSL certificate-based authentication would no longer work whenever the firewall used TLS v1.3. This issue has been fixed on the firewall after support for post-handshake authentication was enabled. Do note that the web browser used must also allow post-handshake authentication for the method to work.

Captive portal - External LDAP directory

Support reference 82686

Whenever a user referenced in an external LDAP directory connects to the captive portal, the system event “LDAP unreachable” (event 19) is no longer raised. This regression appeared in SNS version 4.1.4.

Firewalls with TPMs (SNi20, SN3100) connected to an SMC server

Support references 83380 - 83579

Configurations deployed from SMC to an SNi20 or SN3100 model firewall on which the TPM was initialized would sometimes not succeed, and remain stuck in the step of creating the configuration backup. This issue has been fixed.

SNS 4.2.6 bug fixes

System

IPsec VPN - Routing

Support reference 80662

When a change of status is applied to a network route associated with an IPsec Security Policy, the service no longer shuts down unexpectedly and causes the firewall to freeze.

Web administration authentication interface - Captive portal

Support reference 83011

Issues that could prevent sponsorship e-mails from being sent, or which could unexpectedly log out users from the web administration interface with an “Invalid session” message, have been fixed.

SNMP Agent

Support reference 82661

The correct value is now returned in the OID *UCD-SNMP-MIB::memCached.0*.

Intrusion prevention

SIP

Support references 79839 - 79344

Anomalies in the SIP protocol analysis engine, which could cause the firewall to freeze, have been fixed.

FastPath mode

Support reference 83291

An issue with competing access in the intrusion prevention engine, which could cause the firewall to freeze, has been fixed.

COTP protocol

Support references 82784 - 83342

An issue with the COTP protocol analysis, which could cause the firewall to freeze, has been fixed.

New features in SNS 4.2.5

SPNEGO authentication

The spnego.bat script, available in the MyStormshield personal area, now supports AES256-SHA1, which replaces RC4-HMAC-NT, the previous cryptographic algorithm used.

When this new version of the script is used during the deployment of SPNEGO authentication, support for **AES 256-bit encryption via Kerberos** must be enabled in the properties of the firewall account on Active Directory, in the **Account** tab, under **Account options**.

Resolved vulnerabilities in SNS 4.2.5

Curl library

A moderate severity vulnerability was fixed in the *Curl* library.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-048/.

OpenSSL

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

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2021-054/,
- https://advisories.stormshield.eu/2021-055/.

c-ares library

A moderate severity vulnerability was fixed in the *c-ares* library.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-057/.

SNS 4.2.5 bug fixes

System

IPsec VPN

Support reference 82714

Issues regarding the interruption of IPsec tunnel negotiation or the sudden shutdown of the IPsec tunnel manager have been resolved after updating the tunnel manager and an idle timeout was defined for it. These issues also generated "*ignoring IKE SA setup: job load of XXX exceeds limit of YY*" entries in IPsec VPN logs.

CRL verification

Support reference 82370

Whenever a CRL contained an object identified by a fully qualified domain name (FQDN), the DNS resolution of this FQDN would function correctly again when the firewall verified the CRL. This regression appeared in SNS version 4.2.1.

SNMP Agent

Support reference 81710

The mechanism that manages the SNMP alarm table has been enhanced to stop OIDs from being duplicated, as this prevented some alarms from being raised.

Support reference 81710

A memory leak issue on SNMP agent has been fixed.

Network link aggregation

Support reference 82211

In configurations that use network link aggregation, if a link was lost in an aggregate, a switch could not be made before a 3-second wait, thereby disrupting traffic for 3 seconds. This issue has been fixed.

Monitoring power supply - SN1100 model firewalls

Power supply could not be monitored on SN1100 model firewalls. This issue has been fixed.

Network

Renewing a DHCP lease

Support references 82238 - 82359

When a UNICAST packet originating from port 67 and going to port 68 attempted to pass through the firewall (especially during a DHCP lease renewal), the firewall would occasionally freeze and fail to transmit the packet if the packet's source and outgoing interface are not part of a bridge.

This issue can now be fixed by changing the value of the **UseAutoFastRoute** parameter to **Off** with the following CLI/Serverd command:

```
CONFIG PROTOCOL TCPUDP COMMON IPS CONNECTION UseAutoFastRoute=<On|Off>
```

Find out more

New features in SNS 4.2.4

System

Hardening the operating system

Verification of the integrity of executable files now extends to the userland section of the system.

Only shell scripts are still allowed, but they must be explicitly called by the interpreter, e.g., sh script.sh instead of ./script.sh. If these scripts are run from the event scheduler (*eventd*), the interpreter must be added for each task described in the configuration file of the event scheduler.

These scripts must also be located only in the root partition (/) so that they can be run. As firmware updates will erase the contents of the "/" folder, these scripts must be moved back to the "/" folder after each firmware update.

Do note that the system performance measurement tools that this file integrity verification mechanism allows may display slightly higher memory consumption values than those shown in earlier versions of SNS. The use of *nmemstat* is no longer allowed.

Stealth mode

An SNS firewall in factory configuration is no longer in stealth mode by default, to make it easier to integrate the firewall into existing infrastructures.

However, this mode can still be enabled manually by using the *Stealth* argument in the CLI/Serverd command `CONFIG PROTOCOL IP COMMON IPS CONFIG`:

```
CONFIG PROTOCOL IP COMMON IPS CONFIG Stealth=<On|Off>
CONFIG PROTOCOL IP ACTIVATE
```

Find out more

Path MTU Discovery (PMTUD)

In configurations that involve an IPsec VPN, ICMP 3/4 responses are now fully managed through such tunnels after support for Path MTU Discovery was enabled.

It is disabled by default, but can be managed through the CLI/Serverd command:

```
CONFIG IPSEC UPDATE slot=<1-10> PMTUD=<0|1|2>
CONFIG IPSEC ACTIVATE
CONFIG IPSEC RELOAD
```

These commands are explained in detail in the CLI SERVERD Commands Reference Guide.

NOTE

Stealth mode must be disabled so that the PMTUD can function through IPsec.

Find out more

IPsec VPN - DR mode

Warnings are displayed in the **Messages** widget on the dashboard when the IPsec DR mode is enabled and one of the following conditions is met:

- The proxy is used in a filter rule,
- The NSRPC service is open to the outside,

- The SSL VPN service Is active,
- The DNS cache service Is active,
- The DHCP service Is active.

IPsec VPN - IKEv2

PseudoRandom Functions (PRFs) with the following values can now be selected:

- PRF_HMAC_SHA2_256 [RFC4868],
- PRF_HMAC_SHA2_384 [RFC4868],
- PRF_HMAC_SHA2_512 [RFC4868].

This configuration can only be created in command line using the argument *prf* added to the CLI/Serverd command: `CONFIG IPSEC PROFILE PHASE1 PROPOSALS UPDATE` (any changes must then be confirmed using the command `CONFIG IPSEC ACTIVATE`).

These commands are explained in detail in the CLI SERVERD Commands Reference Guide.

NOTE
The use of PRF_HMAC_SHA2_256 is imposed in IPsec DR mode.

Active Update

Packets in the Active Update module are now signed by a new Stormshield certification authority, which replaces the previous Netasq certification authority.

For clients that use internal mirror sites, the packets hosted on your own servers must be updated so that packets signed by the new certification authority are used. This operation is necessary so that the Active Update module can continue to update its databases.

For Linux environments, a new version of the Active Update mirroring script (*updater.sh)* is available on Mystormshield (**Downloads** > **Stormshield Network Security** > **Tools**). This version makes it possible to retrieve all packets signed by the new certification authority.

Find out more

It is now possible to specify the firewall interface from which requests are sent to automatic update servers. The interface can be specified through the *bindaddr* argument added to the CLI/Serverd command `CONFIG AUTOUPDATE SERVER`. Changes to this parameter must then be applied using the command `CONFIG AUTOUPDATE ACTIVATE`.

Find out more

Automatic checks for firmware updates

Automatic checks for the availability of firmware updates can be enabled or disabled using the CLI/serverd command `SYSTEM CHECKVERSION state=0|1`.
This mechanism is enabled by default.

Network management

The management of a SNS firewall's network is now optimized so that the firewall no longer restarts every time SMC sends a network configuration. The firewall now informs SMC to restart only when it is necessary.

Stormshield Management Center (SMC) agent

On SNS firewalls managed via SMC in version 3.0, if the link with the SMC server cannot be set up within 30 seconds after a deployment (this period can be configured in the administration

console of the SMC server), the previous configuration will be restored.

On firewalls in high availability, it is now possible to choose whether to restart the passive firewall when applying changes to the network configuration that were applied to the active firewall.

This option can only be configured with the CLI/serverd command `HA SYNC`:

`HA SYNC Ennetwork=0|1`: If 0 is selected, the passive firewall will not restart (default behavior), 1 will restart it.

Find out more

Synchronization of the object database with DNS servers

The automatic synchronization of the object database with DNS servers configured on the firewall can now be enabled/disabled and its frequency can be changed.

These operations can only be configured with the CLI/serverd command `CONFIG OBJECT SYNC`:

- `CONFIG OBJECT SYNC STATE=<0|1>` to disable/enable synchronization,
- `CONFIG OBJECT SYNC UPDATE period=<period>` to set a synchronization frequency between 1 min and 1 day inclusive (e.g., *period=6h5m4s*).

These changes must be confirmed using the command `CONFIG OBJECT SYNC ACTIVATE`.

Find out more

Modifying logs enabled by default

Unlike what was announced in the 4.2.1 release notes, the storage of all log types on disk has been enabled again by default.

Hardware

Support for SN1100 firewall models begins with this version 4.2.4.

Web administration interface

Creating IPsec peers

When a new IPsec peer is created, the wizard now offers version 2 of the IKE protocol by default for this peer.

Resolved vulnerabilities in SNS 4.2.4

RTSP, SIP, H323 and MGCP protocol analyzes

A high severity vulnerability was fixed in the RTSP, SIP, H323 and MGCP protocol analyzer.

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

Proxies

A medium severity vulnerability was fixed in the explicit HTTP proxy and SMTP proxy.

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

DHCP service

A medium severity vulnerability was fixed in the DHCP service.

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

Curl library

A medium severity vulnerability was fixed in the *Curl* library.

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

SNS 4.2.4 bug fixes

System

SSL VPN

Support reference 78163

The browser language is now taken into account in the Stormshield SSL VPN client's download link presented by the captive portal of the firewall that hosts this service.

Support reference 79149

Additional controls have been implemented to display an error when the **Available networks** field is defined by a group that contains an IP address range. Such configurations prevented the SSL VPN service from running.

Support reference 73463

The SSL VPN management engine now runs correctly with the AES-GCM encryption suites (128-, 192- or 256-bit keys) recommended by the ANSSI (French network and information security agency).

Proxies

Support reference 81624

In configurations that use multi-user authentication, the application of "*img-src https://**" CSP (content-security-policy) directives would sometimes cause the proxy service to unexpectedly restart. This issue has been fixed.

Support references 79257 - 79144

In configurations that use the explicit HTTP proxy or SMTP proxy without protocol analysis, and when a client connection sent the FIN flag immediately after sending the CONNECT flag, the proxy would keep the log of this closed connection in memory by mistake. An accumulation of such connection logs would then consume an excessive amount of firewall memory. This issue has been fixed.

SSL proxy

Support reference 77207

The SSL proxy would sometimes restart when all of the following conditions occurred:

- An SSL filter policy applied a "Pass without decrypting" action when a CN could not be categorized,
- A connection matched this rule ("Pass without decrypting") because the classification of the CN failed.
- A simultaneous connection to the same website was classified with the action "Block without decrypting".

This issue has been fixed.

System events

Support reference 80426

System event no. 19 "LDAP unreachable" is activated when there are issues accessing an LDAP directory defined in the firewall configuration.

Automatic CRL verification

Support reference 82035

An anomaly during the automatic verification of CRL distribution points (CRLDP) listed in a sub-authority has been fixed. This anomaly would wrongly generate the alarm 'The CRL published on the distribution point is invalid".

Automatic verification of CRLs and external proxy

Support reference 81259

The verification of CRLs through an external proxy would occasionally not function because the port to reach the proxy was not correctly applied. This issue has been fixed.

Retrieving firmware updates and external proxy

Support references 79538 - 81331

The automatic retrieval of firmware through an external proxy would occasionally not function because the proxy was not applied. This issue has been fixed.

IPsec VPN

Support reference 77960

When IPsec VPN was used together with Path MTU Discovery (PMTUD), the Don't Fragment (DF) bit was not included in ESP packets and therefore prevented PMTUD from being used. This configuration is now supported.

Find out more

Support references 81013 - 81002

When the phase 1 lifetime of a tunnel lapses, the user is no longer deleted by mistake from the firewall's authentication tables if the other tunnels used by this user are still active.

Support reference 77477

IPsec configurations which included a NAT rule that applies to packets going to the tunnel and a QoS rule for traffic passing through this tunnel would flood the firewall's memory and make the cluster unstable in a high availability configuration. This issue has been fixed.

IPsec VPN - *Diffusion Restreinte* (DR) mode

On firewalls configured in *Diffusion Restreinte* (DR) mode, DR encryption profiles now allow only the use of 256-bit keys for AES-GCM and AES-CTR.

An error in the implementation of ECDSA based on Brainpool 256 elliptic curves prevented IPsec tunnels in DR mode from being set up with the TheGreenBow IPsec VPN client implementing DR mode. This error has been fixed.

WARNING
Fixing this error in fact makes it impossible to set up IPsec tunnels in DR mode based on ECDSA and Brainpool 256 elliptic curves between a firewall in version SNS 4.2.1 or SNS 4.2.2 and a firewall in version SNS 4.2.4 or higher.

External LDAP directory

Support reference 81531

After an external LDAP directory was created and made accessible via a secure connection, enabling the option **Check the certificate against a Certification Authority** and selecting a trusted CA no longer cause an internal error on the firewall.

LDAP directory - Backup server

Support reference 80428

In an LDAP(S) configuration defined with a backup server, when:

- The firewall switched to the backup LDAP(S) server because the main server stopped responding, and
- The backup server also does not respond,

The firewall will then immediately attempt to connect to the main server again without waiting for the 10-minute timeout defined in factory settings.

IP address reputation and geolocation service

Support reference 81048

In some cases, the IP address reputation and geolocation service would unexpectedly shut down after competing access that occurs when a configuration is reloaded. Even when it was automatically restarted, service could still be disrupted. This issue has been fixed.

Support references 77326 - 77980 - 79673 - 74614 - 80572 - 80624 - 79664 - 79589

An anomaly relating to the IP address reputation and geolocation service would sometimes result in memory corruption, which would cause the firewall to unexpectedly restart. This issue has been fixed.

Initial configuration via USB key

Support reference 80866

In an initial configuration via USB key, when an additional .CSV configuration file was imported into the installation sequence, the command entered in the last line of the file was not executed. This issue has been fixed.

Captive portal

Support reference 79386

Closing the logout page of the captive portal would log the user out again, regardless of the browser used.

Authentication service

Support reference 81423

An issue during communication with an external LDAP server configured on the firewall (network issue, partial response from the server, etc.) would cause the firewall's authentication service to freeze, logging out users and preventing them from logging back in. This issue has been fixed.

SNMP agent

Support reference 81710

A memory leak issue in the management of the SNMP agent queue has been fixed.

Support references 81573 - 81588 - 81529

When the firewall receives an SNMP request, the response address that the SNMP agent uses is correct again and corresponds to the IP address of the firewall queried during this SNMP request.

Support references 82734 - 82735

Syntax errors have been corrected in STORMSHIELD-VPNSP-MIB, STORMSHIELD-VPNSA-MIB, STORMSHIELD-VPNIKESA-MIB and STORMSHIELD-ALARM-MIB MIB files.

Certificates

Support reference 82110

An anomaly in how empty OCSP fields are managed would wrongly generate the error message "XSS Protection" when the properties of the certificate in question were displayed. This anomaly has been fixed.

Hardware bypass - SNi20 model firewalls

Support reference 82241

The hardware bypass mechanism could be non-functional on some SNi20 firewalls. This problem has been fixed.

Network

Static routing and IPsec VPN

Support reference 80862

In policy-based IPsec VPN configurations (non-VTI), whenever a static route was created for the remote network via the IPsec interface, traffic was not encrypted and sent to this network as it was supposed to be. This issue has been fixed.

Multicast routing - Address translation

Support reference 80359

Multicast network traffic packets are no longer duplicated if multicast routing is applied after a destination NAT rule is applied to this traffic.

Bridge - MAC addresses

Support reference 80652

On interfaces attached to a bridge, when a network device is moved and the network traffic that it generates is no longer linked to the same physical interface, the firewall automatically maps the MAC address of the device to the new interface once a Gratuitous ARP request is received from the new device.

This switch was not correctly applied whenever the MAC address was different after the network device was moved This anomaly has been fixed.

Intrusion prevention

FastPath mechanism

Support reference 82078

The combination of NAT and the insertion of inappropriate routes into the tables of the intrusion prevention engine could cause inadequate use of the FastPath mechanism, causing the firewall to freeze. This issue has been fixed.

Hardware

The Intel update utility in the microcode of Intel network cards would occasionally fail to recognize additional cards installed on SN6100 firewalls. This anomaly has been fixed.

Monitoring

IPsec tunnels

Support reference 82043

Mobile IPsec tunnels set up and defined in Config mode now appear in the IPsec tunnel monitoring module.

Web administration interface

High availability

Support reference 80888

Changes to the minimum duration of connections that must be synchronized are now correctly applied (High availability > Advanced properties).

Version 4.2.3 not published

Version 4.2.3 is not available to the public.

Resolved vulnerabilities in SNS 4.2.2

Authentication portal

A moderate severity vulnerability was fixed in the authentication portal's management API.

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

OpenLDAP

A moderate severity vulnerability was fixed after the OpenLDAP component was upgraded.

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

OpenSSL

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

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

CLI/serverd commands

A high severity vulnerability was fixed in the CLI/serverd command mechanism.

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

ClamAV

Moderate severity vulnerabilities was fixed in ClamAV.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu,
- https://advisories.stormshield.eu,
- https://advisories.stormshield.eu.

FreeBSD

A moderate severity vulnerability was fixed after the application of a FreeBSD fix.

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

Hardware

A low severity vulnerability was fixed after a new microcode for Intel processors was applied.

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

SNS 4.2.2 bug fixes

System

Certificates and PKI

Support reference 81909

Whenever the **Certificates and PKI** module was opened, the automatic search process that ordinarily displays the list of CAs, identities and certificates would fail when the DN of a certificate exceeded 127 characters. This would then prevent the contents of the **Certificates and PKI** module from being displayed. This issue has been fixed.

IPsec VPN

Support reference 82179

Whenever an IPsec policy met both of the following conditions:

- The policy started with one or several bypass rules with *None* set as the peer, and which were created as an exclusion to the subsequent rules in the encryption policy. The routing policy manages traffic that matches these rules.
- These rules were followed by several rules regarding mobile IPsec tunnels.

The generated IPsec configuration file would then be wrong and only the first mobile tunnel configured could be set up. This issue has been fixed.

IPsec VPN - IKEv1 site-to-site tunnels

Support references 82199 - 82197

After the IPsec IKEv1 tunnel manager was changed, firewalls in version 4.2.1 could no longer negotiate IPsec IKEv1 tunnels with SNS firewalls in version 4.1.x or lower when both of the following conditions were met:

- The firewalls in version 4.1.x used an IPsec policy based exclusively on IKEv1 peers,
- The firewalls in version 4.2.1 initiated the negotiation.

This issue occurred due to the introduction of the ESN function which 4.1.x versions (and lower) do not support, and an issue relating to the new IPsec tunnel manager.
To resolve these issues, firewalls in version 4.2.2 (or higher) now disable ESN when the peer is in IKEv1.

Virtual machines

IPsec VPN

Support reference 81914

During the installation of SNS 4.2.1 EVAs (elastic virtual appliances) in OVA format, the IPsec VPN tunnel manager would fail to start, preventing IPsec tunnels from being set up. This issue has been fixed.

Web administration interface

IPsec VPN - Authentication by certificate

Support reference 82185

During the selection of an IPsec peer's certificate, the drop-down list would sometimes display only certificates created by default, such as those issued by the CAs of the SSL proxy and SSL VPN.
This list now correctly displays all the other certificates found in the PKI.

New features in SNS 4.2.1

System

ANSSI *Diffusion Restreinte* (DR) mode

SNS firewalls offer the implementation of a strengthened IPsec mode called***Diffusion Restreinte* (DR) mode** that complies with the recommendations of the French Network and Information Security Agency (ANSSI).

In SNS version 4.2, many strengthening measures were added to DR mode, in particular:

- IPsec tunnels are now exclusively negotiated over UDP port 4500, making NAT-T (NAT traversal) detection unnecessary,
- IPsec VPN tunnels can now be only IKEv2-based,
- ESN support for ESP anti-replay is implemented,
- Creating an IPsec VPN policy enables the *CRLRequired* configuration token,
- Restrictions regarding the authentication and encryption algorithms allowed,
- Two specific "DR mode" encryption profiles (one for IKE, one for IPsec) were added to existing profiles (StrongEncryption, GoodEncryption and Mobile).

IMPORTANT
DR mode in SNS version 4.2 is not compatible with DR mode in earlier SNS versions, and the firewall does not allow updates of firewalls with DR mode enabled to SNS version 4.2.0 or higher. DR mode must be disabled before updating the firewall.

Find out more

Modifying logs enabled by default

The possibility of storing some logs, including connections, on disk is now disabled by default on firewalls in SNS version 4.2 in factory configuration. The only logs enabled and stored by default are the following in their respective log files:

- Administration (*l_server*),
- Authentication (*l_auth*),
- System events (*l_system*),
- Alarms (*l_alarm*),
- Filter policies (*l_filter*),
- IKE/IPsec negotiation (*l_vpn*),
- IPsec VPN (*l_vpn*),
- SSL VPN (*l_xvpn*),
- Filter statistics and IPsec statistics (*l_monitor*),
- Sandboxing (*l_sandboxing*).

The storage of other logs on disk can be manually enabled in **Logs - Syslog - IPFIX**.

Find out more

IPsec VPN IKEv1

The daemon that manages IKEv1 IPsec VPN tunnels is now the same as the one that manages IKEv2 IPsec VPN tunnels (strongSwan charon).

The configurations listed below are no longer allowed in version 4.2:

- IKEv1 rules based on pre-shared key authentication in aggressive mode (mobile and site-to-site tunnels),
- IKEv1 rules based on hybrid mode authentication (mobile tunnels),
- IKEv1 backup peers.

You must therefore ensure the compliance of the active IPsec policy, and that it meets the restrictions for a combined IKEv1/IKEv2 policy, before updating the firewall to version 4.2.

Find out more

IPsec VPN

encryption/decryption operations in the IPsec module are distributed more efficiently, leading to improved IPsec throughput in configurations that contain a single IPsec tunnel.

This optimization mechanism can be enabled or disabled manually using the CLI/serverd command:

```
CONFIG IPSEC UPDATE slot=<x> CryptoLoadBalance=<0|1>
```

where <x> is the number of the active IPsec policy.

These commands are explained in detail in the CLI SERVERD Commands Reference Guide.

Find out more

A new CLI/Serverd command `PKI CA CHECKOCSP` was added so that the URL of an OCSP server can be loaded into certificates used in the negotiation of IPsec tunnels.

Find out more

Logs - IPsec VPN rule type

A field specifying the type of VPN rule (mobile tunnel or site-to-site tunnel) was added to IPsec VPN logs.

Find out more

Logs - IPsec VPN rule name

In the IPsec VPN configuration module, it is now possible to look for the name of a rule directly in IPsec VPN logs to display matching logs.

SNMP agent

In IKEv2 or IKEv1 + IKEv2 IPsec policies, an SNMP trap is now raised whenever an IPsec VPN peer cannot be reached.

A new MIB (STORMSHIELD-OVPNTABLE-MIB) makes it possible to monitor via SNMP users who connected through SSL VPN.

STORMSHIELD-VPNSA-MIB offers additional IPsec statistics. Two new IPsec MIBs were added to it:

- STORMSHIELD-VPNIKESA-MIB: provides information on negotiated IKE SAs,
- STORMSHIELD-VPNSP-MIB: provides information on SPs (Security Policies).

Find out more

Calculation of entropy - TPM (Trusted Platform Module)

Firewalls equipped with a TPM now use it as a source of entropy in cryptographic functions, therefore improving their entropy.

Calculation of entropy - Password policy

Entropy, which is calculated based on the unpredictability of a password and the number of characters it contains, has been included in the definition of the password policy to guarantee that these passwords are robust.

A minimum entropy value can now be imposed on passwords defined on the firewall (service accounts, administration accounts, automatic backup passwords, etc.).

Find out more

High availability

In a high availability configuration, when an interface on a node in the cluster fails, the time it takes for a passive node to switch to active mode has been significantly shortened on SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100 models, therefore minimizing interruption to network traffic.

Find out more

SPNEGO authentication

Support reference 73844

The firmware in version 4.2 introduces Windows Server 2019 support for the SPNEGO authentication method. Version 1.7 of the *spnego.bat* script, available in Mystormshield, must be used in this version of Windows Server.
This version of the script is also compatible with Windows Server 2016, 2012 and 2012 R2.

Authentication - Internal LDAP directory

For better security, passwords contained in the internal LDAP directory can now be hashed using SHA2 or PBKDF2.

Find out more

Authentication - Captive portal

On firewalls configured in strict HTTPS mode (using the CLI/Serverd command `CONFIG AUTH HTTPS sslparanoiac=1`), the configuration of the captive portal no longer allows the selection of certificates other than server certificates containing the *ExtendedKeyUsage ServerAuth*.

Before updating firewalls to version 4.2, a captive portal certificate that complies with this requirement must therefore be selected.

Authentication – SSO Agent

SSO agents now connect to the firewall's authentication service over TLS v1.2 instead of SSLv3. The SSO agent v3.0 or higher must therefore be used with SNS firewalls in version 4.2.

Logs - Location of *verbose.** files

Log files created when verbose mode is enabled on firewall services are now placed in a dedicated folder /log/verbose and no longer directly in the /log folder. Existing files will automatically be moved to this new folder when the firewall is updated to version 4.2.

CLI/serverd commands

CLI/Serverd commands are now given versions to allow changes to be tracked. A section setting out the CLI/Serverd commands that were changed, added or deleted between the last SNS version and the previous SNS LTSB version has been added to the first part of the CLI/Serverd commands reference guide.

The CLI/serverd commands relating to IPsec VPN (`CONFIG IPSEC PROFILE PHASE1` and `CONFIG IPSEC PROFILE PHASE2`) were modified to enable the verification of the configuration before it is applied to the firewall.
Service disruptions can therefore be prevented if there are anomalies in the configuration.

Find out more

Restoring configurations

A mechanism that monitors the integrity of the network configuration now makes it possible to prevent configuration errors on firewalls when they are deployed via SMC or when backups are restored.

A consistency analysis is conducted before a configuration is partially restored.
When the analysis mechanism detects an anomaly, it will display a warning message. The administrator can however proceed with the restoration, but changes must be made to the configuration to ensure that the modules that will be restored are operational.

SSL VPN

As part of the process of hardening the SNS operating system, the configuration file meant for the Stormshield SSL VPN client includes the parameter *auth-nocache* to force the client not to cache the user's password (except for SSL VPN clients configured in **Manual mode**).

Firewall's SSH key

As part of the process of hardening the SNS operating system, the firewall's SSH keys (firewall key for SSH connections to the firewall, keys created for high availability and *admin* account key) are now encrypted by default with ECDSA instead of RSA, which was used in versions prior to SNS 4.2.

The firewall's SSH key is now generated when the firewall's SSHD service is enabled (not when the firewall starts) to enhace its entropy (key robustness). The key can also be generated again using the CLI/Serverd command `CONFIG SSH REGENHOSTKEY`.

The SSH key of the *admin* account is always generated every time the password to this account is changed. This password should therefore be changed after the firewall is updated to version 4.2.

Find out more

TLS v1.3 protocol

SNS version 4.2 introduces TLS v1.3 support for services on the firewall (captive portal, LDAPS, Syslog TLS, Autoupdate, etc.).

Clients going in the direction of the firewall can now use only 1.2 and 1.3 of the TLS protocol.
The usable version of the TLS protocol can be configured with the CLI Serverd command:

```
CONFIG CRYPTO UPDATE ClientTLSv12=<0|1> ClientTLSv13=<0|1>
```

For more details on this command, refer to the CLI SERVERD Commands Reference Guide.

Do note that the server hosting an external LDAP directory must support and use a compatible encryption suite in the implementation of the LDAPS protocol based on TLS1.2 or TLS 1.3.
The list of such encryption suites is provided in the SNS v4 User Configuration Manual.

NSRPC

SHA256 is now the algorithm used in the NSRPC library to calculate password hashes.

Updates - Logs

Support reference 79529

Logs regarding operations performed before the firewall was restarted have been added to the *update.log* files to identify the causes of firmware update failures.

Intrusion prevention

TLS v1.3 protocol

The intrusion prevention engine now detects and analyzes decrypted frames from TLS v1.3, which secures communications. In particular, this makes it possible to:

- Allow 0-RTT mode,
- Decide which values/extensions to adopt (GREASE extensions [Generate Random Extensions And Sustain Extensibility], extensions defined in RFC on TLS v1.3 or unknown extensions can be configured).
- Define a blacklist of TLS extensions.

Do note that related traffic can now be analyzed by protocol alarms.

Find out more

RDP over UDP protocol

The intrusion prevention engine now detects and analyzes UDP-based RDP traffic in addition to TCP-based RDP traffic.

Do note that related traffic can now be analyzed by protocol alarms.

IPv6 protocol

In version 4.2, IPv6 packets containing non-compliant RDNSS (*Recursive DNS Server*) options are detected and blocked (cf. RFC 8106).

Web administration interface

IPsec VPN monitoring

The IPsec VPN monitoring module now includes two tables that present the characteristics of the selected IPsec VPN tunnel's Security Associations (SAs):

- Table of IKE SAs:
  - Name of the IPsec rule,
  - IKE version of the tunnel,
  - Local gateway,
  - IP address of the local gateway,
  - Remote gateway,
  - IP address of the remote gateway,
  - SA state,
  - Role (responder/initiator),
  - Initiator cookie,
  - Responder cookie,
  - Local ID,
  - Peer ID,
  - Whether NAT-T is enabled,
  - Authentication algorithm used,
  - Encryption algorithm used,
  - PseudoRandom Function (PRF) algorithm used,
  - Perfect Forward Secrecy (PFS) used,
  - Lifetime lapsed.
- Table of IPsec SAs:
  - SA state,
  - Local gateway,
  - Remote gateway,
  - Bytes in,
  - Bytes out,
  - Lifetime lapsed,
  - Authentication algorithm used,
  - Encryption algorithm used,
  - Whether there is an ESN,
  - Whether UDP encapsulation of ESP packets is enabled.

Dashboard

The dashboard includes a new **Messages** widget that displays system notifications and warnings. Messages appear if:

- IPv6 is enabled on the firewall,
- DR mode is enabled on the firewall,
- The authentication engine uses the firewall's default certificates.

Interface monitoring

The interface monitoring module can now show real-time and historical curves of throughput and the number of packets exchanged for VLANs defined on the firewall.

Curves showing the history of throughput and packets exchanged are now also available for interface aggregates.

Protocols - NTP

Clicking on the link to **Protection against Time Poisoning attacks** (**Configuration** > **Application protection** > **Protocols** > **NTP** > **IPS** tab) now allows direct access to the configuration of the firewall clock.

Find out more

Certificates and PKI

The web administration interface now makes it possible to create certificates in which the FQDN contains the special character "*" (e.g., *.stormshield.eu).

Resolved vulnerabilities in SNS 4.2.1

Intel processors

Intel processor microcodes used on SN510, SN710, SN910, SN2000, SN3000, SN2100, SN3100 and SN6100 firewall models have been updated to fix vulnerabilities CVE-2020-0543, CVE-2020-0548 and CVE-2020-0549.

Web administration interface/Block pages

To address a possible XSS vulnerability, the HTML preview display of HTTP block pages is no longer available. Only the raw text of the HTML code on block pages is displayed.

Web administration interface/Authentication portal

An additional protection feature against code injection has been added to responses sent by the firewall's web administration interface and authentication portal.

OpenSSL

A vulnerability with an overall CVSS score of 3.0 was fixed after the OpenSSL component was upgraded.

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

NDP requests

When NDP requests (IPv6) without replies were accumulated up to a certain threshold, the protection mechanism would be activated in the firewall's NDP table. In an exchange with an unknown host, this would cause the first few packets to be dropped until NDP requests were resolved.

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

Authentication – SSO Agent

SNS firewalls will now reject negotiations with SSO agents that use AES_CBC encryption suites. The SSO agent v3 must therefore be used with SNS firewalls in version 4.2.

ClamAV

A vulnerability with an overall CVSS score of 5.8 was fixed in ClamAV.

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

SNMP

Support reference 80471

A vulnerability with an overall CVSS score of 5.5 in the SNMP protocol analysis protection mechanism has been fixed.

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

SNS 4.2.1 bug fixes

System

Configuration backups - Trusted Platform Module (TPM)

Support reference 79671

During the backup of a configuration with the *privatekeys* parameter set to *none* (this parameter can only be modified via CLI/Serverd command: `CONFIG BACKUP`), private keys stored in *ondisk* mode on the TPM are no longer wrongly decrypted.

Support reference 79671

Multiple configuration backups can no longer be launched simultaneously or too close apart, so private keys stored in *ondisk* mode on the TPM will no longer be wrongly decrypted.

High availability

The option **Reboot all interfaces during switchover (except HA interfaces)** has been optimized in high availability configurations. It informs third-party network connection devices (switches, etc.) any time members of the cluster switch roles. This option is no longer enabled on link aggregates when the option **Enable link aggregation when the firewall is passive** is selected.

Find out more

The errors that occur when the passive member of the cluster is updated are now correctly shown in the firewall's web administration interface.

High availability - SSH keys

When a high availability configuration generated in version 4.2 switches to an earlier SNS version (after resetting the firewall to its factory configuration), the cluster's SSH keys are now deleted correctly.

High availability - LDAP directory

Support reference 78461

An anomaly during the synchronization of LDAP data, due to errors in managing the special character "\" when it is used in the password to access the directory, made this LDAP directory inoperable. This anomaly has been fixed.

High availability - Synchronizing objects

Support reference 77441

The mechanism that synchronizes objects between members of the cluster would stop operating whenever the DNS server that resolved FQDN objects did not accept TCP-based DNS requests. This anomaly has been fixed.

Proxies

Support reference 79204

Issues with memory leaks on proxies have been fixed.

Support references 79957 - 80108 - 79952

Configurations that use multi-user authentication would sometimes fail to fully load web pages that embed CSP (*content-security-policy*) directives. This anomaly has been fixed.

Support reference 79858

An issue with competing access when saving new connections via the proxy has been fixed. This issue would cause the firewall to unexpectedly shut down and switch the roles of the members in a high availability configuration.

SMTP proxy

Support reference 78196

The proxy would sometimes restart unexpectedly after queuing e-mails and receiving an SMTP 421 error from the server. This anomaly has been fixed.

Support reference 77586

When the SMTP proxy is enabled together with SSL decryption of outgoing traffic and antivirus analysis on SMTP traffic (with the action *Pass without analyzing* for the options **When the antivirus analysis fails** and **When data collection fails** in the SMTP protocol analysis settings), the same events will no longer be wrongly logged multiple times in the *l_smtp* file.

HTTP proxy

Support reference 79584

In configurations that meet all the following conditions:

- HTTP proxy is used,
- Kaspersky antivirus is enabled,
- URL filtering is enabled.

Sending several HTTP requests through an internet browser within the same TCP connection (pipelining) no longer causes the proxy to suddenly restart.

SNMP agent

Support references 77226 - 78235

The OID "SNMPv2-MIB::sysObjectID.0", which made it possible to identify the type of device queried, presented the default *net-snmp* value instead of the Stormshield value. This anomaly has been fixed.

Support references 77787 - 78693 - 77779 - 78164 - 78967

Excessive memory consumption issues that caused the SNMP agent service to unexpectedly shut down have been fixed.

Support reference 78761

SNMP informRequest messages are now considered valid SNMP requests and no longer raise the blocking alarm “Invalid HTTP protocol” (snmp:388).

Directory configuration

Support references 70940 - 71329 - 75280 - 77783

The maximum length of the character string the represents the subject of the certificate that was imported to allow the SSL connection to the internal LDAP directory has been raised from

128 to 256 characters.

IPsec VPN

Support references 78593 - 73609

In IPsec topologies deployed via SMC, peer certificates were not displayed in the firewall's IPsec configuration.

As such, the administrator would sometimes select a certificate again for the peer, making the IPsec configuration ineffective. This issue has been fixed.

IPsec VPN - Implicit filter rules

Support reference 77096

The implicit "Allow ISAKMP (UDP port 500) and the ESP protocol for IPsec VPN peers" filter rule now allows IPsec traffic initialized by internal loopback interfaces.

IPsec VPN - Peer names

Peer names longer than 44 characters no longer prevent the setup of the IPsec tunnels concerned.

Host reputation

Support reference 77080

Invalid objects in the list of hosts whose reputations are monitored no longer cause a system error during attempts to reload the proxy.

Find out more

Filtering and NAT

Support reference 78647

Exporting NAT/filter rules in CSV format would wrongly generate the "Any" value for the "#nat_to_target" field in the export file, in cases where filter rules were not associated with any NAT rules. This anomaly would then prevent such CSV files from being imported into SMC if the filter rules concerned had a "Block" rule.

Support reference 76700

When there were configuration errors in the filter policy, the firewall would not load any filter rules (including implicit rules) when it restarted and blocked all traffic as a result. This issue, which required access to the firewall in serial console/VGA in order to enable a working policy, has been fixed.

Support reference 79526

Whenever a group contained 128 or more objects with at least one that had a forced MAC address, rules that used this group would no longer be applied when traffic matched them. This anomaly has been fixed.

Support references 79533 - 79636 - 80412 - 80376

When a time object was enabled or disabled, the re-evaluation of connections that match the filter rule containing this time object no longer cause the firewall to unexpectedly restart.

Support reference 79311

NAT rules that specified a destination IP address and/or destination port for the traffic after translation no longer functioned through an IPsec tunnel. This anomaly has been fixed.

SSL VPN

During attempts to set up an SSL VPN tunnel with a firewall on which stealth mode was disabled, the firewall no longer wrongly ignores the first packet sent by the SSL VPN client, and the tunnel can be set up correctly.

SSL VPN tunnel monitoring

Support reference 77801

Names of users connected via SSL VPN were displayed in plaintext in these tunnels' monitoring module, even when the connected administrator did not have privileges to access personal data. This anomaly has been fixed.

Authentication - Temporary accounts

Support reference 79296

When the security policy on the firewall required passwords longer than 8 characters, adding, changing or deleting the authentication method for temporary accounts no longer generates a system error.

Certificates and PKI

The Certificate Revocation Lists (CRLs) entered in certificates are now downloaded together with those specified in the CAs.

Initial configuration via USB key

Support reference 75370

When several devices, such as USB keys and SD cards, are connected, only the USB key will now be taken into account.

Intrusion prevention

SSL protocol

Support reference 77817

An error in the declaration of the *ExtensionLength* SSL protocol analysis field would wrongly raise "Invalid SSL packet" blocking alarms (ssl alarm:118) for legitimate *Client Hello* SSL packets. This anomaly has been fixed.

SMB v2 protocol

Support reference 78216

An anomaly in the SMB protocol analysis engine would wrongly raise the "Invalid NBSS/SMB2 protocol" alarm (nb-cifs alarm:157), blocking legitimate SMBv2 traffic as a result. This anomaly has been fixed.

SMB - CIFS protocol

Support references 77484 - 77166

Anomalies in the SMB - CIFS protocol analysis would wrongly raise the "Invalid NBSS/SMB protocol" blocking alarm (nb-cifs alarm:158) during legitimate access to shared Microsoft Windows disk resources. These anomalies have been fixed.

DNS protocol

Support reference 77256

An anomaly in the DNS protocol analysis would wrongly raise the “Possible DNS rebinding attack” blocking alarm (dns alarm:154) when a DNS server responded with an external IP address consisting of its IPv6 address concatenated with its IPv4 address (*IPv4 - IPv6 mapping*). This anomaly has been fixed.

SMTP protocol

Support reference 77661

In a configuration such as the following:

- The intrusion prevention engine analyzes SMTP protocol,
- Antivirus analysis is enabled for SMTP traffic,
- Kaspersky antivirus is used on the firewall,
- A Maximum size for antivirus and sandboxing analysis (KB) has been configured.

When e-mails containing attachments that exceed the defined size are analyzed, the blocking alarm “Invalid SMTP protocol” (smtp alarm:121) is no longer wrongly raised.

FastPath mode

Support references 76810 - 77932

An issue with competing access when connection statistics were injected into the intrusion prevention engine has been fixed. This issue could cause significant CPU consumption and network packets to unexpectedly be rejected over IX interfaces (2x10Gbps and 4x10Gbps fiber modules).

Hardware

Configuration via USB key

Support references 79645 - 79283

Whenever a firewall is configured via USB key, an information message now appears in the console and a waiting period of two minutes is initiated when the USB key needs to be removed to continue ongoing operations (firmware updates, connecting a firewall to a cluster, etc.). Removing the USB key suspends the counter.

This mechanism makes it possible to prevent key decryption errors on firewalls equipped with a TPM (SN3100 and SNi20).

Find out more

Virtual machines

Serial numbers of VPAYG firewalls

Support reference 76157

The high availability monitoring mechanism did not recognize serial numbers of VPAYG firewalls (serial number of the firewall, to which an extension such as "-XXXXXXXX" is added). This anomaly has been fixed.

EVA firewalls deployed over VMWare with 10Gb/s interfaces

Support reference 76546

For firewalls deployed in a VMWare infrastructure, the maximum throughput displayed for 10Gb/s interfaces that use the *vmxnet3* driver is no longer wrongly limited to 10Mb/s.

Web administration interface

Interfaces

Support reference 77682

Whenever a parent GRETAP interface of a VLAN was deleted, the VLAN would be hidden from the list of interfaces even though it was still defined in the firewall configuration. This operation now leaves the VLAN visible at the root of the list of available interfaces.

Support reference 77014

The system now correctly detects the connection status of USB/Ethernet (4G) interfaces and displays it in the **Configuration** > **Network** > **Interfaces** module.

Interfaces - Modem configuration profiles

Administrator accounts in read-only mode could not display the configuration profiles of modems. This anomaly has been fixed.

Interfaces - GRETAP

Support reference 78800

The correct MTU is now assigned to GRETAP interfaces when they are created (1462 bytes, instead of 1500 as in the four previous versions).

Protocols

Support reference 78157

After the profile name of a protocol analysis is edited, and the configuration module is changed, the **Edit** menu is no longer empty when the user goes back to the edited protocol analysis module.

Protocols - BACnet/IP

The service with a *confirmedTextMessage* confirmation would wrongly appear twice in the *Remote Device Management* group (IDs 19 and 20). ID 20 is now correctly assigned to the *reinitializeDevice* service.

Automatic backups - Custom server

Support reference 78018

The port defined during the creation of the custom backup server appears correctly again in the URL shown in the configuration module.

Do note that the anomaly affected only the display.

Find out more

Authentication - Radius method

Support reference 76824

During access to the configuration of the Radius server, if the pre-shared key field was accidentally erased, a blank pre-shared key would be entered instead of the previous value. This issue has been fixed and the firewall now refuses empty values for this field.

URL filtering - SSL filtering

Support reference 77458

The results of a URL categorization (**URL filtering** and **SSL filtering** modules) are no longer continuously displayed at the bottom of the screen when a module is changed.

Support reference 79017

Modifying several SSL filter rules or URL filter rules at the same time would generate an abnormally high number of system commands. This anomaly has been fixed.

Web objects

Support reference 76327

Immediately after a new URL or certificate category is created, clicking on the column to sort contents:

- No longer creates system errors if no other categories were selected during the creation operation,
- Does not wrongly show the contents of another category if it was selected during the creation operation.

Web objects - Object groups

Support reference 76325

The search field for groups of categories is no longer case-sensitive.

IPsec VPN

Support reference 74210

When an IPsec rule separator is added to a policy that contains more than one page of rules, the user is no longer sent back to the first page of the IPsec policy every time.

Support references 74966 - 75821

Double-clicking on an IPsec rule separator correctly opens it in edit mode, and the modification of the separator is fully functional again.

Support reference 75810

When a peer is created or modified, switching from certificate authentication to pre-shared key authentication, followed by a switch back to certificate authentication without reloading the configuration page, no longer causes system errors due to the detection of the certificate initially selected.

Support references 77246 - 77264 - 77274

When a peer with a configuration that contained errors (indicated by a message in the **Checking the policy** field) was created or modified, it could still be validated anyway. This anomaly, which caused an error while reloading the IPsec VPN configuration, has been fixed.

Support reference 77443

Creating, modifying or deleting a pre-shared key from the table of pre-shared keys for mobile tunnels (**Configuration > IPsec VPN** module > **Identification** tab) no longer creates a key conflict or prevents the setup of IPsec tunnels that use such keys.

IPsec VPN - Peers

Additional controls have been added to better manage the duplication, renaming or deletion of peers in the process of modification (changes not saved).

Certificates and PKI

Support reference 78965

After an external CA was imported into the PKI (this operation can only be performed in command line), it could no longer be declared as the default CA (for the SSL proxy for example), or selected when an identity was created (user, server, etc.). This anomaly has been fixed.

Aliases can now be entered (*Subject Alternative Name* field) when a server identity is created. The latest versions of web browsers sometimes require this field.

Captive portal

Support reference 78805

During the redirection to the authentication page, the **Password** field was selected by default instead of the **User name** field if it was empty. This anomaly has been fixed.

Filtering and NAT - Geolocation and public IP address reputation

Support reference 80980

When a geographic group or a public IP address reputation group is used in a filter/NAT rule, the tool tip that appears when the user scrolls over the group no longer wrongly displays “Object not found”.

Version 4.2.0 not published

Version 4.2.0 is not available to the public.

New features in SNS 4.1.6

System

SNMP agent

In IKEv2 or IKEv1 + IKEv2 IPsec policies, an SNMP trap is now raised whenever an IPsec VPN peer cannot be reached.

Resolved vulnerabilities in SNS 4.1.6

OpenSSL

A vulnerability with an overall CVSS score of 3.0 was fixed after the OpenSSL component was upgraded.

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

ClamAV

A vulnerability with an overall CVSS score of 5.8 was fixed in ClamAV.

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

Vulnerabilities with an overall CVSS score of 5.3 was fixed in ClamAV.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu,
- https://advisories.stormshield.eu.

Authentication portal

A vulnerability with an overall CVSS score of 4.3 was fixed in the authentication portal's management API.

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

OpenLDAP

A vulnerability with an overall CVSS score of 4.5 was fixed after the OpenLDAP component was upgraded.

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

SNMP

Support reference 80471

A vulnerability with an overall CVSS score of 5.5 in the SNMP protocol analysis protection mechanism has been fixed.

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

SNS 4.1.6 bug fixes

System

Configuration backups - Trusted Platform Module (TPM)

Support reference 79671

During the backup of a configuration with the *privatekeys* parameter set to *none* (this parameter can only be modified via CLI/Serverd command: `CONFIG BACKUP`), private keys stored in *ondisk* mode on the TPM are no longer wrongly decrypted.

Support reference 79671

Multiple configuration backups can no longer be launched simultaneously or too close apart, so private keys stored in *ondisk* mode on the TPM will no longer be wrongly decrypted.

Filtering and NAT

Support reference 79526

Whenever a group contained 128 or more objects with at least one that had a forced MAC address, rules that used this group would no longer be applied when traffic matched them. This issue has been fixed.

Support references 80043 - 79636 - 80412 - 80376 - 79771

When a time object was enabled or disabled, the re-evaluation of connections that match the filter rule containing this time object no longer cause the firewall to unexpectedly restart.

Proxies

Support references 79957 - 80108

Configurations that use multi-user authentication would sometimes fail to fully load web pages that embed CSP (*content-security-policy*) directives. This issue has been fixed.

Support reference 81624

In configurations that use multi-user authentication, the application of "*img-src https://**" CSP (content-security-policy) directives would sometimes cause the proxy service to unexpectedly restart. This issue has been fixed.

Support reference 79858

An issue with competing access when saving new connections via the proxy has been fixed. This issue would cause the firewall to unexpectedly shut down and switch the roles of the members in a high availability configuration.

SMTP proxy

Support reference 78196 - 79813 - 81759

The proxy would sometimes restart unexpectedly after queuing e-mails and receiving an SMTP 421 error from the server. This issue has been fixed.

HTTP proxy

Support reference 79584

In configurations that meet all the following conditions:

- HTTP proxy is used,
- Kaspersky antivirus is enabled,
- URL filtering is enabled.

Sending several HTTP requests through an internet browser within the same TCP connection (pipelining) no longer causes the proxy to suddenly restart.

SSL proxy

Support reference 77207

The SSL proxy would sometimes restart when all of the following conditions occurred:

- An SSL filter policy applied a “Pass without decrypting” action when a CN could not be categorized,
- A connection matched this rule (“Pass without decrypting”) because the classification of the CN failed.
- A simultaneous connection to the same website was classified with the action “Block without decrypting”.

This issue has been fixed.

High availability

The errors that occur when the passive member of the cluster is updated are now correctly shown in the firewall’s web administration interface.

System events

Support reference 80426

System event no. 19 "LDAP unreachable" is activated again when there are issues accessing an LDAP directory defined in the firewall configuration.

SNMP agent

Support references 77226 - 78235

The OID "SNMPv2-MIB::sysObjectID.0", which made it possible to identify the type of device queried, presented the default *net-snmp* value instead of the Stormshield value. This anomaly has been fixed.

Support references 80036 - 77779

Excessive memory consumption issues that caused the SNMP agent service to unexpectedly shut down have been fixed.

Regular CRL retrieval

Support reference 81259

When an explicit proxy is defined on the firewall with a specific network port, the mechanism that regularly retrieves CRLs now correctly uses the port of the explicit proxy to access the Internet.

LDAP directory - Backup server

Support reference 80428

In an LDAP(S) configuration defined with a backup server, when:

- The firewall switched to the backup LDAP(S) server because the main server stopped responding, and
- The backup server also does not respond,

The firewall will then immediately attempt to connect to the main server again without waiting for the 10-minute timeout defined in factory settings.

External LDAP directory

Support reference 81531

After an external LDAP directory was created and made accessible via a secure connection, enabling the option **Check the certificate against a Certification Authority** and selecting a trusted CA no longer cause an internal error on the firewall.

IP address reputation and geolocation service

Support reference 81048

In some cases, the IP address reputation and geolocation service would unexpectedly shut down after competing access that occurs when a configuration is reloaded. Even when it was automatically restarted, service could still be disrupted. This issue has been fixed.

Support reference 77980

An anomaly relating to the IP address reputation and geolocation service would sometimes result in memory corruption, which would cause the firewall to unexpectedly restart. This issue has been fixed.

Network

Static routing and IPsec VPN

Support reference 80862

In policy-based IPsec VPN configurations (non-VTI), whenever a static route was created for the remote network via the IPsec interface, traffic was not encrypted and sent to this network as it was supposed to be. This issue has been fixed.

Bridge - MAC addresses

Support reference 80652

On interfaces attached to a bridge, when a network device is moved and the network traffic that it generates is no longer linked to the same physical interface, the firewall automatically maps the MAC address of the device to the new interface once a Gratuitous ARP request is received from the new device.

This switch was not correctly applied whenever the MAC address was different after the network device was moved This issue has been fixed.

Intrusion prevention

SMB - CIFS protocol

Support references 77484 - 77166

Anomalies in the SMB - CIFS protocol analysis would wrongly raise the "Invalid NBSS/SMB protocol" blocking alarm (nb-cifs alarm:158) during legitimate access to shared Microsoft Windows disk resources. These anomalies have been fixed.

Virtual machines

Serial numbers of VPAYG firewalls

Support reference 76157

The high availability monitoring mechanism did not recognize serial numbers of VPAYG firewalls (serial number of the firewall, to which an extension such as "-XXXXXXXX" is added). This issue has been fixed.

Hardware

Configuration via USB key

Support references 79645 - 79283

Whenever a firewall is configured via USB key, an information message now appears in the console and a waiting period of two minutes is initiated when the USB key needs to be removed to continue ongoing operations (firmware updates, connecting a firewall to a cluster, etc.). Removing the USB key suspends the counter.

This mechanism makes it possible to prevent key decryption errors on firewalls equipped with a TPM (SN3100 and SNi20).

Web administration interface

Filtering and NAT - Geolocation and public IP address reputation

Support reference 80980

When a geographic group or a public IP address reputation group is used in a filter/NAT rule, the tool tip that appears when the user scrolls over the group no longer wrongly displays “Object not found”.

SNS 4.1.5 bug fix

It is highly recommended to apply the 4.1.5 update to firewalls in major versions 4.x.x.

As a preventive measure, the certificate used to sign new version updates has been replaced in version 4.1.5. This new certificate, issued by the « Stormshield Product and Services Root CA » trusted certification authority will be used to check the integrity and the signature of all future SNS versions.

Once the new version has been installed, all updates signed with the old certificate will be refused.

IMPORTANT
To install an older version signed with the old certificate on a firewall in version SNS 4.1.5, you must use the USB Recovery procedure. The standard downgrade procedure will not be supported.

SNS 4.1.4 bug fixes

System

VPN SSL in portal mode

Support reference 80332

After a regression in compatibility with Java 8 that was introduced in the previous fix version of SNS, the component that the SSL VPN used in portal mode was compiled with version 8 of the Java development kit to ensure compatibility with:

- Java 8 JRE,
  - or -
- OpenWebStart.

This makes it possible to work around the suspension of public versions of Java JRE 8, scheduled in the near future.

New features in SNS 4.1.3

System

Log out when idle

The super administrator can now restrict how long administrator accounts stay idle on the firewall. The administrators of these accounts can still define a timeout for their own accounts, but the duration cannot exceed the one defined by the super administrator.

Find out more

IPsec VPN (IKEv1 + IKEv2)

The warning that appeared when a combined IKEv1/IKEv2 IPsec policy was used has been deleted.
Having proved to be stable for a long time, this feature is no longer considered experimental and can be used in a production environment without particular precautions.
Refer to the Explanations on usage regarding combined IKEv1 and IKEv2 IPsec policies.

Resolved vulnerabilities in SNS 4.1.3

OpenSSL

Vulnerability CVE-2020-1968 (*Raccoon attack*) was fixed after the OpenSSL component was upgraded to version 1.0.2x.

Vulnerability CVE-2020-1971, which can cause a denial of service attack if a CRL in the firewall's PKI was previously compromised, was fixed after the OpenSSL component was upgraded to version 1.0.2x.

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

FreeBSD - ICMPv6

Vulnerability CVE-2020-7469, regarding the management of error messages in the ICMPv6 network stack, which could lead to *use-after-free* attacks, was fixed after the FreeBSD security patch was applied.

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

Authentication by certificate

Additional controls have been set up to detect occurrences of the special character "*" in the e-mail address field of certificates. These controls make it possible to stop interpreting this character in requests to the LDAP directory, as it could allow unjustified connections to the firewall.

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

SNS 4.1.3 bug fixes

System

Proxies

Support reference 75970

When the proxy must send a block page, the absence of a *Content-Length* header in the reply (HTTP HEAD reply) does not wrongly raise the alarm "Additional data at end of a reply" (alarm http:150) anymore.

Support reference 78432 - 79297

Issues with memory leaks in proxies, which would sometimes restart the service unexpectedly, have been fixed.

Support references 78802 - 79204 - 78210 - 77809 - 79584

An issue with enabling brute force protection, which could freeze the proxy, has been fixed.

Support reference 67947

In configurations with a filter policy that implements:

- A **global** decryption rule,
- A **local** filter rule that uses an **explicit** proxy and has a rule ID that is equal to or lower than the ID of the global decryption rule.

Operations that reload the proxy's configuration (changing the filter policy, changing the SSL/URL filter policy, changing the SSL/URL filter engine, changing the antivirus engine, etc.) no longer ends connections processed by the proxy.

Support reference 79584

An issue with the management of the SSL context, which could freeze the proxy, has been fixed.

Hardware monitoring

Support reference 77170

On SN2100, SN3100 and SN6100 firewalls, the mechanism that monitors fan rotation speed has been optimized so that it no longer wrongly reports alarms that create doubts about the operational status of fans.

High availability (HA)

Support references 78758 - 75581

Memory leak issues, especially in the mechanism that manages HA status and role swapping in a cluster, have been fixed.

High availability (HA) and IPsec VPN (IKEv2 or IKEv1 + IKEv2)

Support reference 79874

An issue with competing access between the log mechanism on IPsec VPN and the HA cache after the synchronization of the IPsec configuration would sometimes shut down the IPsec VPN service. This issue has been fixed.

DHCP relay

Support reference 79298

The option **Relay DHCP queries for all interfaces** (**Configuration** > **Network** > **DHCP** > **DHCP relay**) now excludes interfaces that were created when the PPTP server was enabled (**Configuration** > **VPN** > **PPTP server**), and which prevented the DHCP relay service from starting.

SSL VPN

Support references 73353 - 77976

The SSL VPN client now applies the interval before key renegotiation set by default on the SSL VPN server to 14400 seconds (4 hours). Users who do not have the Stormshield Network SSL VPN client must retrieve a new configuration file from the firewall's authentication portal so that the client applies the interval.

Find out more

VPN SSL in portal mode

Support reference 68759

SSL VPN in portal mode now uses a component that is component with:

- Java 8 JRE,
  - or -
- OpenWebStart.

This makes it possible to work around the suspension of public versions of Java JRE 8, scheduled in the near future.

IPsec VPN

Support reference 79553

When IPsec VPN x509 topologies deployed via SMC (Stormshield Management Center) were updated to version 4.1 (certificate-based authentication), the IPsec VPN tunnels involved would not be able to set up. This issue has been fixed.

IPsec VPN IKEv1 - Certificate-based authentication

Support reference 79156

In configurations that use only IKEv1 IPsec VPN tunnels, an anomaly in the mechanism that compares the *Distinguished Name*s (DN) defined in the certificates that local and remote peers present, prevented such tunnels from setting up. This issue has been fixed.

Sandboxing

Support reference 76120

"Sandboxing license not available" alerts are no longer wrongly raised on firewalls that do not have a sandboxing (Breach Fighter) license and for which sandboxing was not enabled in the configuration.

TPM

On firewalls equipped with a TPM (Trusted Platform Module), *ondisk* certificates can again be encrypted, and the system can access the module when the TPM's symmetric key is changed.

Certificates and PKI

Support reference 78734

Whenever a request to display CRL distribution points (CRLDP) was applied to a sub-certification authority (sub-CA), the CRLDPs of the sub-CA's parent authority would be returned instead.
This anomaly has been fixed and the command applied to a sub-CA now correctly displays its CRLDPs.

Network

Default gateway

Support reference 78996

Default gateways located in a public IP network outside the firewall's public address range can again be defined on the firewall.

Bridge - MAC addresses

Support reference 74879

On interfaces attached to a bridge, when a network device is moved and the network traffic that it generates is no longer linked to the same physical interface, the firewall now automatically maps the MAC address of this device to the new interface once a *Gratuitous ARP* request is received from this device. This makes it possible to ensure uninterrupted filtering on the moved device.
The device will be switched only if the MAC address is the same after it is moved

Interface monitoring - History curves

Support references 78815 - 73024

As the mechanism that retrieves interface names to generate history curves was case sensitive, some history curves were not displayed. This anomaly has been fixed.

Intrusion prevention

DCERPC protocol

Support reference 77417

The DCERPC protocol analyzer would sometimes wrongly create several hundred connection skeletons, causing excessive CPU consumption on the firewall.
This issue, which could prevent the firewall from responding to HA status tracking requests and make the cluster unstable, has been fixed.

sfctl command

Support reference 78769

Using the *sfctl* command with a filter on a MAC address no longer restarts the firewall unexpectedly.

Web administration interface

Dashboard - Interfaces

Support reference 77313

After a link aggregate is created, the order in which interfaces appear in the **Network** widget of the dashboard is no longer wrongly changed.

Captive portal

Support reference 78651

Customized logos displayed on the captive portal (**Configuration** > **Users** > **Authentication** > **Captive portal** > **Advanced properties**) are now correctly applied.

SNS 4.1.2 bug fixes

IMPORTANT
Firewalls that are part of an IPsec x509 topology (certificate-based authentication) deployed via SMC (Stormshield Management Center) **must not be** updated to version 4.1.1 or 4.1.2.
For more information on this topic, refer to this article in the Stormshield knowledge base.

IMPORTANT

In certain conditions, the proxy can be impacted by a memory leak, leading to unwanted restarts of the service. If you believe you have been affected by this problem, please contact Stormshield support.

System

Multi-user authentication

Support reference 78887

After CSP (content-security-policy) directives were implemented in phases on some websites and these directives were verified by mainstream browsers, users who have SNS multi-user authentication would see a degraded display of such websites.

This issue was fixed by adding the firewall's FQDN to the list of websites allowed to use external resources for the sites in question.

Support reference 78677

After the recent implementation of a new security policy on mainstream web browsers, SNS multi-user authentication would longer function. Depending on the web browser used, the error message "Too Many Redirects" or a warning would appear in the browser's web console.

To fix this issue, the authentication cookies that the proxy generates now contain the attributes "SameSite" and "Secure" when HTTPS is used.

When a user visits an unsecured website, i.e., one that uses HTTP, the "Secure" attribute of the cookie cannot be used. The web browser must be manually configured to enable browsing on these websites again.

Find out more

Proxies

Support reference 78190

The mechanism that generates system event and alert notifications has been optimized to no longer excessively increase the CPU load when the number of connections passing through the firewall surges.

Intrusion prevention

RDP/COTP protocols

Support reference 78923

The mechanism that evaluates filter rules in connections that involve RDP/COTP now correctly applies related translation rules again, and no longer wrongly blocks such traffic.

New features in SNS 4.1.1

Option to disable stealth mode

Stealth mode has been enhanced with the possibility of disabling it and allowing responses to ICMP requests (option **Enable stealth mode** in the **Application protection** > **Protocols** > **IP protocols** > **IP** module > **Global configuration** tab).

This option allows the firewall to be integrated more easily into existing infrastructures by moderating stealth mode on the firewall, and also prevents packets from being silently ignored. For example, the firewall can adopt the role of a device visible on the network when:

- A packet exceeds the MTU and has a DF bit set to 1 (dfbit=1): the firewall blocks the packet and sends a response ICMP packet.
- A packet passes through the firewall correctly: the firewall decrements the TTL ("Time To Live").

The value of this option, defined in the configuration of the IPS engine's IP protocol processes, replaces the former configuration methods based on the sysctl commands `net.inet.ip.icmpreply=1` and `net.inet.ip.stealth=0`.

Intrusion prevention

Filtering and analysis of IEC61850 protocols

SNS version 4.1 supports the IEC61850 protocol analysis (MMS, Goose and SV) and verifies the compliance of IEC61850 packets that pass through the firewall.

These protocols are used mainly in infrastructures that transport electricity to control, oversee and monitor electrical controllers

RDP protocol

The protocol analysis for RDP traffic has been improved.

HTTP

Protocols derived from HTTP report a specific alarm (alarm *732* "HTTP: invalid upgrade protocol stack") that allows the user to configure alarms an filters more granularly for these protocols.

DHCP client

New DHCP options (60 [vendor-class-identifier], *77* [user-class] and 90 [authsend]) allow SNS firewalls to authenticate on networks of telecoms operators that offer VLAN services. SNS firewalls can therefore be integrated into the operator's network without the need for the PPPOE connection mode.

These options can only be modified through the *CLI / Serverd* command:

```
config network interface update ifname=xxx DHCPVendorClassId="aaa"
DHCPUserClass="bbb" DHCPAuthsend="ccc"
config network interface activate
```

These commands are explained in detail in the CLI SERVERD Commands Reference Guide.

Update

The hash algorithm of firmware update files has been changed to comply with the highest standards.

New SNi20 firewall models

Compatibility

Version 4.1.0 of the firmware ensures compatibility with new SNi20 industrial firewalls.

In order to ensure service continuity in an industrial setting, the SNi20 firewall is equipped with a hardware bypass function, which when enabled, allows network traffic to pass through in the event of a power outage or appliance breakdown.

Hardware-based security for VPN secrets

SNi20 firewalls are equipped with a trusted platform module (TPM) that secures VPN secrets. With the TPM, a level of security can be added to SNi20 appliances that act as VPN concentrators, which may not necessarily be physically secure. Support for this module begins with this version 4.1.0.

SNi20 and SNi40 model firewalls

Link aggregation

Link aggregation (LACP) is now supported on SNi20 and SNi40 firewall models starting from version 4.1.0.

Network loop management protocols

RSTP and MSTP network loop management protocols are now supported on SNi20 and SNi40 firewall models starting from version 4.1.0.

Serverd

To reduce the attack surface on SNS, the Serverd service can be configured to listen only on the firewall's loopback address. This behavior is enabled by default on firewalls in factory configuration,

and can only be modified with the command:

```
CONFIG CONSOLE SERVERDLOOPBACK state=0/1
```

These commands are explained in detail in the CLI SERVERD Commands Reference Guide.

IPsec VPN mobile peers

Multiple mobile policies can now be supported simultaneously when peers are distinguished by their logins (ID). These policies can be added in **Configuration > VPN > IPsec VPN**, *Peers* tab.

Using the peer's login (ID) also makes it possible to change the VPN configuration of a particular mobile peer distinguished by its login, without affecting the tunnels of other mobile peers.

Admin account

To change the password of the *admin* user (super administrator), the old password now needs to be entered as well.

IPsec VPN and LDAP groups

During IPsec VPN connections via SSO authentication, the firewall now retrieves the groups associated with users added from the LDAP, so that these groups can be used in filter rules.

SSL VPN and certificates

To authenticate peers (client or server) in TLS, Stormshield firewalls now only accept certificates that have the *Key Usage* field with the "ServerAuth" attribute, i.e., certificates that comply with X509 v3.

Certification authorities (CAs) and global certificates

Global certificates and certification authorities are now shown and identified as such when the option **Display global policies (Network objects, Certificates, Filtering, NAT and IPsec VPN)** is enabled in the **Preferences** module.

Certificates and PKI

When a certificate is imported in p12 format, the type of certificate (server or user certificate) is now automatically detected.

Certificate enrollment

Stormshield firewalls now support the EST (Enrollment over Secure Transport) certificate enrollment protocol, which is particular due to its use of HTTPS requests secured by the TLS protocol.

The following operations can be performed when EST is set up on Stormshield firewalls:

- Distribution of the public key of the certification authority (CA) that signs certificates,
- Certificate creation or renewal requests by the PKI administrator,
- Certificate creation or renewal requests by the certificate holder (enrollment),

The existing certificate can directly authenticate renewal requests, which no longer require a password, if the EST server allows it.

These operations can only be performed using *CLI / serverd* commands that begin with:

```
PKI EST
```

For more information on the syntax of these commands, refer to the CLI SERVERD Commands Reference Guide.

Certificates generation

Certificates can now be generated with new and more efficient algorithms that use elliptic curve cryptography. The following *CLI / Serverd* commands now offer the options of SECP, Brainpool and RSA:

```
PKI CA CREATE
```

```
PKI CERTIFICATE CREATE
```

```
PKI REQUEST CREATE
```

```
PKI CA CONFIG UPDATE
```

The `size` parameter in these commands also needs to be set. Its value must correspond to the selected algorithm:

Algorithm	Sizes allowed
RSA	768, 1024, 1536, 2048 or 4096
SECP	256, 384, or 521
Brainpool	256, 384, or 512

For more information on the syntax of these commands, refer to the CLI SERVERD Commands Reference Guide.

High availability

LACP link aggregation

On firewalls containing LACP aggregates, a weight can now be assigned to each interface in the aggregate to calculate the quality of high availability.
Assign the value *1* to the new *LACPMembersHaveWeight* parameter in the following *CLI / Serverd* commands:

```
CONFIG HA CREATE
```

```
CONFIG HA UPDATE
```

This will display the interfaces of the aggregate in the **Impact of the unavailability of an interface on a firewall's quality indicator** table in the **High availability** module of the web administration interface.

Without these commands, the default behavior remains the same: the aggregate will be considered a single interface, and the cluster will switch only when all the interfaces in the aggregate are lost.

For more information on the syntax of these commands, refer to the CLI SERVERD Commands Reference Guide.

High availability monitoring via SMC

Monitoring of firewalls configured in high availability is now optimized, and gets the value of the **System node name** field.

Loss of network modules

The health status calculation that determines the switch from one node to another in a cluster has been enhanced so that the system will recognize the loss of network modules more easily, even after the firewall is restarted.

NAT rules with ARP publication

In high availability configurations, firewalls may send a Gratuitous ARP (GARP) for all their interfaces in order to maintain traffic routing, so that the network can be informed whenever the

location of a MAC address changes.

This operating mode has been improved so that all virtual IP addresses from an **ARP broadcast** of a NAT rule will send a series of Gratuitous ARPs (GARP) during a switch.

Authentication

New SN SSO Agent pour Linux

A new Linux-based SN SSO Agent supports directories that run on non-Windows systems, such as Samba 4. It can be configured in the **Authentication** module in the web administration interface, and detected through logs exported via Syslog. Exported logs are filtered by regular expressions configured earlier in the interface.

For more information on the configuration and operation of the SN SSO Agent for Linux, refer to the technical note SSO Agent for Linux.

SSO Agent - Syslog

Backup syslog servers can now be configured for the SSO agent authentication method.

Temporary accounts

The password that the firewall automatically generates when a temporary account is created (**User > Temporary accounts**) now meets the minimum password length required in the firewall's password policy (module **System > Configuration** > **General configuration** tab).

LDAP

Backup LDAP servers can now be configured on ports other than the main LDAP server port.

SN6100 firewall - Performance

The configuration of memory occupation has been optimized on the IPS engine of SN6100 appliances.
Details on the performance of SN6100 firewall models are provided in the SN6100 Network Security datasheet.

SNS - SMC synchronization

The synchronization of SNS with SMC has been enhanced to allow smoother data exchange between both products, especially during direct access to the firewall administration interface from SMC.

NTP client

The interface that NTP requests go through can now be configured. The time synchronization daemon on an SNS firewall previously made such requests go through the default interface.

This new parameter can only be modified through the *CLI / Serverd* command:

```
CONFIG NTP SERVER ADD name=<hostname|groupname> bindaddr=<Firewall_obj>
```

For more information on the syntax of this command, refer to the CLI Serverd Commands Reference Guide.

Network objects

Address range objects now make it possible to configure MAC address ranges.

SSL proxy

The keys generated by the SSL proxy now use the same encryption algorithms as what the certification authority of the SSL proxy uses instead of the algorithms defined by default.

Configuration backups

The algorithm used to derive the passwords that protect configuration backups has been updated to comply with the highest standards.

System

The random kernel generator has been upgraded so that it is now based on a faster, more robust algorithm.

Initial configuration via USB

Bird dynamic routing

Dynamic routing can now be configured by importing *bird.conf* configuration files for IPv4 and *bird6.conf* configuration files for IPv6. The CSV format of the command file has also been enriched for this purpose.

For further information regarding the preparation of *.bird* and *.bird6* files, refer to the technical note Initial configuration via USB key.

setconf operation

In an initial configuration via USB key, the *setconf* command offers a new feature that allows writing lines in sections in addition to writing values in keys (tokens). The CSV format of the command file has been enriched for this purpose.

For further information regarding the *setconf* command, refer to the technical note Initial configuration via USB key.

New *sethostname* operation

A new *sethostname* operation has been added to the initial configuration via USB key, and makes it possible to set the firewall's host name. The CSV format of the command file has been enriched for this purpose.

For further information regarding the *sethostname* operation, refer to the technical note Initial configuration via USB key.

Dashboard

SSO agents and syslog servers are now monitored, and their statuses shown in the dashboard.

LDAP directories

Secure connections to internal LDAP directories are now based on standard protocol TLS 1.2.

Exclusion of the proxy for automatic backups

Automatic backups can now be configured to avoid going through the proxy set on the firewall.

This new parameter can only be modified through the *CLI / Serverd* command:

```
CONFIG AUTOBACKUP SET
```

For more information on the syntax of this command, refer to the CLI Serverd Commands Reference Guide.

Web administration interface

System node name

A system node name can now be defined for the firewall (**Configuration** > **General configuration** > **Advanced properties** tab).

This name is particularly useful in high availability configurations, as it easily identifies the member of the cluster on which you are connected when you open a session in console mode, for example.

When this system node name is configured, it appears in parentheses in the upper banner of the web administration interface, after the name of the firewall.

Filter - NAT - HTTP cache feature

The *HTTP cache* function can no longer be used in filter rules.

If a firewall used this function in an earlier firmware version, it will automatically be disabled when it is upgraded to version 4.1.0 or higher.

Regular CRL retrieval

The IP address presented by the firewall can now be specified for **Regular retrieval of certificate revocation lists (CRL)**.

This address can only be configured through the CLI / Serverd command:

```
PKI CONFIG UPDATE CHECKBINDADDR=ip_address
```

For more information on the syntax of this command, refer to the CLI Serverd Commands Reference Guide.

Resolved vulnerabilities in SNS 4.1.1

FreeBSD

Vulnerabilities CVE-2019-15879 and CVE-2019-15880 relating to *cryptodev* were fixed after a FreeBSD security patch was applied.

JQuery

Support reference 78384

Vulnerabilities (CVE-2020-11022 and CVE-2020-11023) were fixed after the JQuery library was upgraded.

Intel processors

Several vulnerabilities – CVE-2019-11157, CVE-2019-14607 and CVE-2018-12207 – that could affect Intel processors were fixed after a FreeBSD security patch was applied and Intel microcode was updated.

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

Command line

The SNS command line service (serverd) was vulnerable to brute force attacks only through protected interfaces, and only when access to the administration server over port 1300 was allowed in the configuration of implicit rules. This flaw has been fixed.

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

NetBIOS

A vulnerability made it possible to send specially crafted NetBIOS packets through the firewall during NetBIOS sessions to launch denial of service attacks.

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

Certificates and PKI

Additional controls have been set up for operations such as user identities being downloaded or the publication of a certificate in the LDAP directory. These controls block JavaScript code from being run, as malicious users would have been able to inject it into the certificate.

Web administration interface / Captive portal / Sponsorship

Additional controls have been implemented for connections via the web administration interface, the captive portal or sponsorship, to prevent JavaScript code or additional HTML tags from being executed through the optional disclaimer page.

ClamAV antivirus

Vulnerabilities CVE-2020-3327 and CVE-2020-3341 were fixed after the ClamAV antivirus engine was upgraded to version 0.102.3.

SNS 4.1.1 bug fixes

System

SSL VPN

Support reference 76762

The **Available networks or hosts** field was wrongly used to calculate the possible number of SSL VPN clients, and therefore skewed the calculation. This issue has been fixed.

SSL VPN Portal

Support reference 77062

Even though a maximum of servers were accessible via the SSL VPN Portal, additional machines could still be declared. This would cause the firewall's authentication engine to restart repeatedly. Now, servers can no longer be created once the limit is reached, which varies according to the firewall model.

Find out more

Support references 77168 - 77132 - 77388

The SLD would occasionally restart and log off all users whenever two users logged in via the SSL VPN portal and accessed the same resource.

Hardware bypass - SNi40 model firewalls

Support reference 78382

On SNi40 industrial firewalls with the hardware bypass function enabled (**Configuration** > **General configuration** tab), an issue that hardware monitoring processes encounter with competing access to the bypass mechanism would sometimes wrongly enable bypass, and provide the wrong status in the firewall's web administration interface. This issue has been fixed.

Directory configuration

Support reference 76576

The default port used to access the backup LDAP server is now the same as the port that the main LDAP server uses.

Monitoring gateways

Support references 71502 - 74524

During the startup sequence of the gateway monitoring mechanism, if any of the gateways used in filter rules switched from an internal "maybe down" status (pinging failed) to an internal "reachable" status, the filter would still consider such gateways disabled. This anomaly has been fixed.

When the status of a gateway changes, it will now be logged as an event.

Support reference 75745

On firewalls that process many connections, and which use configurations with many gateways, replies to pings may take longer to reach the gateway monitoring mechanism. When this occurs, the mechanism would continuously re-send pings, and restart without sending notifications such as logs or system events. This issue has been fixed.

Support reference 77579

The gateway monitoring mechanism, which would sometimes restart unexpectedly, has been fixed.

Support reference 76802

In some configurations, the process that relied on the gateway monitoring engine would consume an excessive amount of the firewall's CPU resources. This issue has been fixed.

URL filtering - Extended Web Control

Support reference 78169

When a firewall is upgraded to a 4.1.x firmware version, it no longer prevents the generation of URL category groups used by Extended Web Control.

Proxies

Support references 77514 - 76343 - 78378 - 78438 - 78469 - 77896

Issues regarding proxies, which were blocked when the antispam was used together with the Kaspersky antivirus, have been fixed.

Support references 76535 - 75662

Potential competing access between SSL and HTTP proxy queues would sometimes shut down the proxy manager unexpectedly. This issue has been fixed.

Support reference 71870

The proxy daemon no longer shuts down unexpectedly whenever the maximum number of simultaneous connections through the SSL proxy is reached.

Support references 70598 - 70926

The behavior of the HTTP proxy has been changed so that the SLD daemon on the firewall will no longer be overwhelmed when too many requests are redirected to the authentication portal. This new mechanism implements protection against brute force attacks.

SSL proxy

Support references 76022 - 76017

Changes to some parameters (e.g., memory buffers or TCP window sizes) of the SSL proxy, meant to optimize the amount of data exchanged through this proxy, are now correctly applied.

Support reference 77207

An anomaly in the SSL decision-making cache mechanism (decrypt, do not decrypt, etc) that occurs when there are simultaneous connections with the same destination IP addresses with different ports, would occasionally corrupt this cache and freeze the SSL proxy. This anomaly has been fixed.

Support reference 78044

When attempts to connect to an unreachable SSL server resulted in the SSL proxy immediately returning an error message, the firewall would not properly shut down such connections. An increasing amount of such connections wrongly considered active would then slow down legitimate SSL traffic. This anomaly has been fixed.

SMTP proxy

Support reference 77207

In configurations that use the SMTP proxy in an SMTP filter rule:

- In “Firewall” security inspection mode

  or

- In "IDS" or "IPS" security inspection mode but without SMTP protocol analysis (**Application protection** > **Protocols** > **SMTP** module > **IPS** tab: **Automatically detect and inspect the protocol** checkbox unselected),

when the SMTP server shut down a connection after sending an SMTP/421 server message, the STMP proxy would occasionally freeze. This issue has been fixed.

Local storage

Support reference 75301

Firewalls with damaged SD cards (and therefore damaged log storage partitions) would restart in loop. This issue has been fixed.

IPsec VPN IKEv1

Support reference 77679

In IPsec configurations that use mobile peers with certificate authentication, and for which no peer IDs were specified, the message indicating a switch to experimental mode no longer appears by mistake.

Support reference 77358

When IPsec VPN tunnels were set up with remote users (also known as mobile or nomad users), phase 1 of the IKE negotiation would fail because fragmented packets were not correctly reconstructed after they were received. This anomaly has been fixed.

Support reference 65964

The IPsec management engine (*Racoon*) used for IKEv1 policies no longer interrupts the phase 2 negotiation with a peer when another phase 2 negotiation fails with the same peer.

IPsec VPN IKEv2 or IKEv1 + IKEv2

Support reference 74391

When an extremely large CRL – containing several thousand revoked certificates – is automatically reloaded, the IPsec IKEv2 tunnel manager no longer restarts in loop.

Support reference 75303

When the Bird dynamic routing engine (*bird* for IPv4 or *bird6* for IPv6) was restarted too often, it would cause the IKE daemon to malfunction, preventing IPsec VPN tunnels from being negotiated. This anomaly has been fixed.

Support reference 75137

Creating several mobile peers that use the same certificate no longer causes the certificate to be loaded repeatedly. This behavior consumed much more memory unnecessarily when many peers were involved.

Support reference 77722

The presence of the same trusted certification authority with a CRL in both the local IPsec policy and global IPsec policy no longer causes a failure when the IPsec configuration is enabled on the firewall.

Support reference 77097

The management of the authentication process was enhanced for the setup of IPsec VPN tunnels in configurations where several LDAP directories are declared and one or several of these LDAP directories take longer than usual to respond.

These enhancements now make it possible to stop blocking attempts to set up other tunnels during the waiting phase.

IPsec VPN - Virtual interfaces

Support reference 77032

During the decryption of IPv6 traffic that was transported in IPv4 IPsec tunnels through virtual interfaces, the firewall would no longer look for return routes among the IPv6 virtual interfaces. Such IPv6 packets are now correctly exchanged at each tunnel endpoint.

IPsec VPN - Logs

Support reference 77366 - 69858 - 71797

Text strings exceeding the maximum length allowed when they are sent to the firewall's log management service are now correctly truncated and no longer contain non-UTF-8 characters. This anomaly would cause a malfunction when logs were read through the web administration interface.

In addition:

- The maximum supported length of a log line is now 2048 characters,
- The maximum supported length of a text field contained in a log line is now 256 characters.

Initial configuration via USB key

Support reference 77603

An anomaly in how special characters (spaces, ampersands, etc.) are managed when CSV files are imported, could prevent some data from being applied (e.g., certificates with names that contain spaces). This anomaly has been fixed.

Antivirus

Support references 77399 - 77369 - 78378 - 78156 - 78579

The antivirus engine no longer freezes at startup, or when its configuration is reloaded in the absence of a Breach Fighter sandboxing license, or when sandboxing is not properly configured.

Network objects

Support reference 77385

When a global network object linked to a protected interface is created, this object will now be correctly included in the *Networks_internals* group.

Restoration of network objects

Support reference 76167

When local or global network objects are restored using a backup file (file with a ".na" extension), the firewall's network routes are reloaded to apply changes that may affect network objects involved in routing.

TPM

Support reference 76664

When a certificate is revoked, the associated .pkey.tpm file is now properly deleted.

Support reference 76665

When a PEM certificate is imported on the firewall without its private key, the debug command `tpmctl -a -v` no longer wrongly returns a TPM file reading error message (*tpm file read error*).

SNMP agent

Support references 65418 - 71393

SNMP responses such as SNMP_NOSUCHOBJECT, SNMP_NOSUCHINSTANCE and SNMP_ENDOFMIBVIEW are now correctly interpreted and no longer cause SNMP protocol analyses to stop unexpectedly.

Support reference 71584

The use of the value *snmpEngineBoots* has changed in order to comply with RFC 3414.

Support references 74522 - 74521

The anomalies observed in table indexing, which reflected the hardware status of cluster members in the HA MIB, have been fixed.

Connection from Stormshield Management Center (SMC)

During the initial connection from SMC to the web administration interface of a firewall in version 4.0.1 or higher, attempts to retrieve the archive containing all the interface data would fail, thereby preventing connections to the firewall from SMC. This anomaly has been fixed.

Reports

In some cases, running the system command *checkdb -C*, which allows the integrity of the report database to be verified, would actually cause it to be deleted. The system that enabled interaction with this database has therefore been enhanced to introduce more thorough verifications, especially in error management.

For more information on the syntax of this command, refer to the CLI /SSH Commands Reference Guide.

Behavior when the log management service is saturated

Support references 73078 - 76030

When the log management service on the firewall is saturated, it is now possible to define how the firewall manages packets that generate alarms and those intercepted by filter rules that have been configured to log events:

- Block such packets since the firewall is no longer able to log such events,
- Do not block such packets and apply the configuration of the security policy even though the firewall is unable to log such events.

The behavior of the intrusion prevention system can be configured in the firewall's administration interface via **Configuration** > **Application protection** > **Inspection profiles**.

A percentage threshold, above which the firewall will consider that its log management service is saturated, can also be set. Once this percentage is reached, the firewall will apply the configured action to packets that need to be logged.

The threshold can be changed only with the following *CLI / Serverd* commands:

```
CONFIG SECURITYINSPECTION COMMON LOGALARM BlockOverflow=<0|1>
BlockDrop=<0-100>
```

```
CONFIG SECURITYINSPECTION COMMON LOGFILTER BlockOverflow=<0|1>
BlockDrop=<0-100>
```

For more information on the syntax of these commands, refer to the CLI SERVERD Commands Reference Guide.

High availability

Support reference 70003

The validity of the license for the **Vulnerability manager** option is now verified before the configuration is synchronized to avoid unnecessarily generating error messages in logs such as "Target: all From: SNXXXXXXXXXXXXX Command: SYNC FILES failed: Command failed : Command has failed : code 1".

Support reference 56682

The test process in which nodes in the same cluster confirm the availability of other nodes has been enhanced so that the passive node will not be wrongly switched to active mode, thereby creating a configuration with two active nodes.

High availability - IPsec VPN (IKEv2 policy or IKEv1 + IKEv2 policy)

In high availability configurations that apply IKEv2 or IKEv1+IKEv2 IPsec policies, an anomaly sometimes wrongly detected the replay of ESP sequence numbers and packet loss after two failovers in the cluster. This anomaly has been fixed.

High availability - link aggregation

Support reference 76748

In a high availability configuration, an active node switching to passive mode would no longer wrongly disable VLAN interfaces that belonged to a link aggregate (LACP).

Maintenance - High availability

Support reference 75986

In a high availability configuration, the option that allowed an active partition to be copied to the backup partition from the other member of the cluster is available again (module **System** > **Maintenance** > **Configuration** tab).

Filter - NAT - MAC addresses

Support reference 76399

A rule that has a host object as its destination with a forced MAC address (host in a DHCP reservation, for example) now correctly filters traffic that matches it.

High availability - Filtering and NAT - Time objects

Support reference 76822 - 73023 - 76199

To prevent network instability in high availability clusters, the re-evaluation of filter rules is now optimized when there is a change in the status of time objects used in one or several of these rules.

Support reference 76822

The re-evaluation of filter rules has been optimized when time objects used in several rules in the filter policy change their status.

Routers

Support references 75745 - 74524

After a firewall is restarted, the router monitoring service now correctly applies the last known status of these routers.

Certificates and PKI

Attempts to import a certificate already found in the firewall's PKI when the “Overwrite existing content” option is unselected, no longer duplicate this certificate on the firewall.

During a connection to a firewall from an SMC server, the firewall now checks that the certificate of the SMC server contains an *ExtendedKeyUsage* field with the attribute *ServerAuth*.

Monitoring certificates and CRLs

Support reference 76169

In a HA cluster, the mechanism that monitors the validity of certificates and CRLs on the passive firewall no longer wrongly generates system events every 10 seconds. Typical events are Passive certificate validity (event 133) or Passive CRL validity (event 135).

In addition, the mechanism that monitors the validity of CRLs now only generates alerts when a CRL exceeds half of its lifetime and is due to expire in less than 5 days.

Firmware updates

The certificate used to sign firmware updates now contains a specific OID monitored by the mechanism that verifies the firewall's update files.

Radius authentication

Support reference 74824

In a configuration that uses Radius server authentication via pre-shared key, selecting another host object in the Server field, then saving this only change no longer causes the initial pre-shared key to be deleted.

Automatic backups

Support reference 75051

The mechanism that checks the certificates of automatic backup servers was modified after the expiry of the previous certificate.

Support reference 77432

The absence of the "/log" folder no longer prevents automatic backups from functioning properly.

Network interfaces

Support reference 76645

When a bridge is deleted, all occurrences of this bridge will now be correctly removed from configuration files, and no longer prevents new interfaces from being displayed when new network modules are added.

DHCP relay

Support reference 75491

When GRE interfaces are defined on the firewall, selecting “Relay DHCP queries for all interfaces” no longer causes the DHCP relay service to restart in loop.

Network

Bird dynamic routing

Support reference 77707

The *check link* directive used in the *protocol direct* section in the Bird dynamic routing configuration file is now correctly applied for IXL network interfaces (fiber 4x10Gbps and 2x40Gbps network extension modules for SN2100, SN3100 and SN6100 models; 4x10G BASE-T modules for SN710, SN910, SN2000, SN2100, SN3000, SN3100 and SN6100 models; fiber 10Gbps onboard ports on SN6100 models) and IGB network interfaces (SNi20, SNi40, SN2000, SN3000, SN6000, SN510, SN710, SN910, SN2100, SN3100 and SN6100).

Interfaces

Support references 73236 - 73504

On SN2100, SN3100, SN6100 and SNi40 firewall models, packets would occasionally be lost when a cable was connected to:

- One of the management ports (MGMT) on SN2100, SN3100 or SN6100 models, or

- One of the interfaces of an SNi40 firewall.

This issue has been fixed by updating the driver on these interfaces.

Wi-Fi

Support reference 75238

Changes to the access password of a Wi-Fi network hosted by the firewall are now correctly applied.

Hardware monitoring

System events (ID 88 and 111) are now generated when a defective power supply module reverts to its optimal status (when the module is replaced or plugged back in).

Intrusion prevention

TNS protocol - Oracle

Support references 77721 - 71272

Analyses of TNS - Oracle client-server communications that undergo packet fragmentation and address translation (NAT) would desynchronize traffic due to packets being rewritten. This issue has been fixed.

TCP protocol

Support reference 76621

When a threshold was defined for the **Maximum number of simultaneous connections for a source host** in the TCP configuration, and when a TCP-based filter rule blocked an attempted Syn Flood denial of service attack, the packets that raised the alarm were correctly blocked but no alarm would be raised in the corresponding log file (*l_alarm*). This anomaly has been fixed.

RTSP protocol

Support reference 73084

When an RTSP request that uses an RTP/AVP/UDP transport mode passes through the firewall, the RTSP analysis engine no longer deletes the *Transport* field and broadcast channels are set up correctly.

Policy Based Routing (PBR)

Support reference 77489

When a firewall-initiated connection was created, the system would query the intrusion prevention engine to determine the need for policy-based routing, which would lead to issues with competing access and cause the firewall to freeze. This issue has been fixed.

HTTP

The HTTP protocol analysis no longer raises an alarm or blocks traffic when there is an empty field in the HTTP header, especially when SOAP messages are encapsulated in an HTTP request.

Support references 74300 - 76147

When a value is entered in the **Max. length for a HTML tag (Bytes)** field (**Application protection** > **Protocols** > **HTTP** module > **IPS** tab > **HTML/Javascript analyses**), and a packet presents an attribute that exceeds this value, the firewall no longer wrongly returns the error “Possible attribute on capacity (parser data handler (not chunked))" but the error “Capacity exceeded in an HTML attribute".

NTP

Support reference 74654

To improve compatibility with certain vendors, the maximum size of NTP v3 packets considered valid is now set to 120 bytes by default.

Connection counter

Support reference 74110

The mechanism that counts simultaneous connections has been optimized to no longer raise the alarm “Maximal number of connexions per host reached” (alarm tcpudp:364).

DNS protocol

Support reference 71552

Requests to update DNS records are now better managed in compliance with RFC 2136 and no longer trigger the block alarm "Bad DNS protocol" (alarm dns:88).

Quarantine when alarm raised on number of connections

Support reference 75097

When “Place the host under quarantine” is the action set for the alarm “Maximal number of connexions per host reached” (alarm tcpudp:364), the host that triggered this alarm is now correctly added to the blacklist for the quarantine period configured.

Filtering - SIP protocol

Support reference 76009

An error message now appears when there is an attempt to enable a filter rule such as:

- The option **Redirect incoming SIP calls (UDP)** is enabled (**Action** > **Advanced properties**> **Redirection**),
- Two or more destination ports are defined, one relying on ANY as a protocol, and at least another based on UDP or TCP.

Policy-based routing

Support reference 76999

In PBR, when routers were changed directly in filter rules, IPState connection tables (for GRE, SCTP and other protocols) now apply the new router IDs.

Hardware

SN6000 model firewalls

Support references 75577 - 75579

In a few rare cases, a message warning of missing power supply modules would be wrongly sent on SN6000 firewalls equipped with an IPMI module in version 3.54. A mechanism that restarts the IPMI module has been set up to deal with this issue.

This mechanism is disabled by default and does not affect traffic going through the firewall, but temporarily prevents the refreshment of component data. The mechanism needs about five minutes to run its course, the time it takes to restart the IPMI module and to refresh data on components.

This new parameter can only be modified through the *CLI / SSH* command:

```
setconf /usr/Firewall/ConfigFiles/system Monitord EnableRestartIPMI <0|1>
```

For more information on the syntax of this command, refer to the CLI /SSH Commands Reference Guide.

Virtual machines

EVA on Microsoft Azure

Support reference 76339

The Microsoft Azure Linux Guest Agent log file (file waagent.log) was moved to the "/log" folder on the firewall to avoid saturating the "/var" file system on the firewall.

Web administration interface

Users and groups

Support reference 78413

In directories that have several thousand entries (especially in nested groups), requests to display users and groups for a selection (e.g., the **Filter - NAT** module) could take an unusually long time and cause the display of the module to freeze. This issue has been fixed.

Reports

Support reference 73376

The “Top sessions of Administrators” report now shows all the sessions of the firewall's administrators, i.e., sessions of the *admin* (super administrator) account and of all users and user groups added as administrators. The report previously contained only sessions of the *admin* (super administrator) account

40 Gb/s network modules

The maximum throughput indicated in each interface’s configuration panel is now 40 Gb/s for the network modules concerned.

Protocols

Support reference 75435

The search filter applied to the protocol tree (Application protection > Protocols) now stops being applied after a module is reloaded.

Interface monitoring

Support reference 76162

The theoretical throughput of Wi-Fi interfaces now factors in the standard used (A/B/G/N) and no longer indicates 10 Mb/s systematically.

Hardware monitoring / High availability

The serial number of both members of the cluster now appears in the list of indicators.

LDAP directories

Support reference 69589

Users can now correctly access an external LDAP directory hosted on another Stormshield firewall via a secure connection (SSL) when the option "Check the certificate against a Certification authority" is selected.

Filter - NAT

Support reference 76698

Network objects defined with only a MAC address are now correctly listed as available network objects when a filter rule is being created.

Static routing - Return routes

Support references 77012 - 77013

USB/Ethernet (4G modem) interfaces can now be selected as the routing interface when a static route or return route is added.

Filtering - Implicit rules

Support reference 77095

When the administrator requests to disable all implicit rules, the system command to disable them is now correctly applied.

SSL VPN

Support reference 76588

When the SSL VPN configuration module is opened, the window indicating that the captive portal is not enabled on external interfaces no longer appears by mistake when it is enabled.

Global router objects

Support reference 76552

Double-clicking on a router object now correctly opens the window to edit routers instead of the window for hosts.

Protocols - DNS

Support reference 72583

After the action applied to a DNS registration type is changed, displaying other DNS profiles successively no longer causes an error when the table of DNS registration types and applied actions is refreshed.

User names

Support reference 74102

User names are no longer case-sensitive when they are saved in the tables of the intrusion prevention engine. This guarantees that names are mapped to filter rules based on the names of authenticated users.

Authentication methods

Support reference 76608

During a user's initial access to the Users > Authentication module, the message asking the user to save changes before quitting, even though none were made, will no longer appear.

Version 4.1.0 not published

Version 4.1.0 is not available to the public.

New features in SNS 4.0.3

IMPORTANT

Firewalls must not be upgraded from SNS in version 3.10.x or higher to a 4.0.x version. This operation is not supported.

For further information, refer to Recommendations.

System

WebGUI file signature

A signature has been added for SNS WebGUI files to strengthen SMC communication mechanisms.

Obsolete features and algorithms

Filter - NAT - HTTP cache feature

As the use of the *HTTP cache* function in filter rules will be phased out in a future version of SNS, a warning message now appears to encourage administrators to modify their configurations.

This message appears under the filter grid in the **Checking the policy** field.

IPsec VPN - Obsolete authentication and encryption algorithms

As some algorithms are obsolete and will be phased out in a future version of SNS, a warning message now appears to encourage administrators to modify their configurations. The algorithms in question are:

- Authentication algorithms: *md5*, *hmac_md5* and *non_auth*,
- Encryption algorithms: *blowfish*, *des*, *cast128* and *null_enc*.

This message appears when these algorithms are used in the profiles of IPsec peers.

IPsec VPN - Backup peers

As the use of backup peers (designated as the “Backup configuration”) is obsolete and will be phased out in a future version of SNS, a warning message now appears to warn administrators and encourage them to modify their configurations. This message appears under the IPsec policy grid in the **Checking the policy** field.

For this configuration, use virtual IPsec interfaces instead, with router objects or dynamic routing.

Resolved vulnerabilities in SNS 4.0.3

S7 protocol

The firewall would restart unexpectedly whenever:

- S7 traffic included an exchange containing an invalid request packet followed by an invalid response packet,
  and
- The alarm "S7: invalid protocol" (alarm s7:380) was set to "Pass",
  and
- The option "Log each S7 request" was enabled in the S7 protocol parameters.

This flaw has been fixed.

SIP over TCP protocol

An anomaly, which could result in a SIP session double lock and the sudden shutdown of the SIP over TCP protocol analysis, has been fixed.

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

SNMP

Support reference 76629

Running an SNMP operation when a wrong OID (that does not begin with ".") is added to the blacklist in the SNMP protocol parameters, no longer causes the firewall to reboot in loop.

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

FreeBSD

If a field in the IPv6 header was not properly initialized, it would cause a memory leak that cannot be exploited.

This vulnerability (CVE-2020-7451) was fixed after a security patch was applied to the FreeBSD TCP network stack.

NetBIOS

A vulnerability made it possible to send specially crafted NetBIOS packets through the firewall during NetBIOS sessions to launch denial of service attacks.

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

SNS 4.0.3 bug fixes

System

IPsec VPN (IKEv1)

Support reference 75824

Whenever a remote peer switched to its backup peer (designated as the “Backup configuration”), the IKE daemon would sometimes restart unexpectedly and shut down open IPsec tunnels. This anomaly has been fixed.

GRETAP and IPsec

Support reference 76066

The system command *ennetwork -f* no longer makes the firewall reboot in loop in configurations containing GRETAP interfaces that communicate through IPsec tunnels.

SSL VPN

A new certificate, with which Java JAR compiled files can be signed, has been installed and replaces the former certificate due to expire soon (05/24/2020).

SN910 model firewalls

Support reference 76528

After a upgrade of the firewall from an SNS 3.9.x version to an SNS 4.0.x version, the ports of IX interfaces were no longer in the right order on SN910 firewalls equipped with an IX card.

An automatic mechanism has been set up to restore the order of ports.

Daemon shutdown time

Support reference 74990

In some rare cases, a daemon would shut down after a certain duration and prevent the firewall from completing its update. This duration has been shortened to allow the firewall update to run properly.

Network

Wi-Fi network

Support references 73816 - 75634 - 75958

Devices that use *Intel Wireless-N 7260* or *Qualcomm Atheros AR6004 802.11a/b/g/n* Wi-Fi cards would occasionally encounter connectivity issues on the firewall’s Wi-Fi. This anomaly has been fixed.

Intrusion prevention

TDS protocol

The analysis of the *Status* field in TDS (Tabular Data Stream) packets no longer wrongly raises the alarm "TDS: invalid protocol" (alarm tds:423).

NB-CIFS protocol

The analysis of NB-CIFS traffic from Microsoft Windows hosts no longer wrongly raises the alarm "Invalid NBSS/SMB2 protocol" (alarm nb-cifs:157).

LDAP protocol

Authentication via SASL (Simple Authentication and Security Layer) now supports the NTLMSSP protocol, and therefore no longer generates errors when analyzing LDAP traffic that uses this protocol.

NTP

NTP packets that present a zero *origin timestamp* no longer wrongly raise the alarm "NTP: invalid value" (alarm ntp:451).

DNS protocol

Support references 72754 - 74272

The DNS protocol analysis has been modified to reduce the number of false positives from the "DNS id spoofing" alarm (alarm dns:38).

Web administration interface

Access to private data (logs)

To get back full access to logs (private data), click directly on the message “Logs: Restricted access” in the upper banner.

Directory configuration

Support reference 76069

When an external LDAP directory is set as the default directory, the name of this directory is no longer wrongly replaced with *NaN* when its parameters are modified.

Interfaces

Support reference 76497

The IP addresses of interfaces 11 and up were replicated on the second interface of the firewall, displaying wrong information as a result. This anomaly has been fixed.

Authentication

During the configuration of the RADIUS authentication method, the “Pre-shared key” fields were not applied. This anomaly has been fixed.

New features in SNS 4.0.2

IMPORTANT

The update of a firewall from an SNS version 3.10.x and upwards to an SNS version 4.0.x must not be performed and is not supported.

Details are available in Recommendations section.

Stability and performance

The synchronization of SNS with SMC has been enhanced to allow smoother data exchange between both products, especially during direct access to the firewall administration interface from SMC.

Increased security during firmware updates

Security is now tighter during firmware updates. In addition to update packages being protected by signatures to ensure their integrity, Stormshield now also secures communications with the update servers used. These communications now take place in HTTPS and over port 443.

Hardware

SSH commands

A new *CLI / SSH* command makes it possible to operate the TPM, and begins with:

```
tpmctl
```

It includes a command that allows new *PCRs* (*Platform Configuration Registers*) to be approved after the BIOS or hardware modules are updated.

For more information on the syntax of this command, refer to the CLI SSH Commands Reference Guide.

Resolved vulnerabilities in SNS 4.0.2

Authentication portal (captive portal)

New checks are now conducted during the verification of parameters used in the URL of the firewall's captive portal.

Details on this vulnerability (**CVE-2020-8430**) can be found on our website https://advisories.stormshield.eu.

CLI / Serverd commands

The CLI Serverd command `CONFIG AUTOUPDATE SERVER` has been enhanced so that the use of the "url" parameter is now better monitored.

Libfetch library

The vulnerability **CVE-2020-7450** was fixed after a security patch was applied to the FreeBSD *libfetch* library.

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

Web administration interface

Additional checks are now implemented during the verification of parameters used in the URL of the firewall's web administration interface.

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

SNS 4.0.2 bug fixes

System

SSL proxy

Support reference 74927

To prevent compatibility issues with embedded programs or certain browsers, especially in iOS 13 and MacOS 10.15, the size of certificate keys that the SSL proxy generates for SSL connections has been raised to 2048 bits.

Support reference 74427

When the certification authority of the SSL proxy expired, the firewall would sometimes stop attempting to generate new keys unnecessarily for some events, e.g., when reloading the filter policy or network configuration, or when changing the date on the firewall. This would cause excessive CPU usage.

Proxies

Support references 66508 - 71870

In heavy traffic, the proxy would sometimes shut down during a failed HTTP header analysis. This issue has been fixed.

Support reference 71870

The proxy no longer shuts down unexpectedly whenever the SSL proxy is used and the maximum number of simultaneous connections is reached.

Support references 70721 - 74552 - 75874

Memory consumption is now optimized when the proxy is used.

Proxy - URL filtering

Support reference 73516

The connection between the HTTP/HTTPS proxy and the URL filtering engine of the Extended Web Control solution would occasionally be lost; this would display the *URL filtering is pending* page to clients whose connections used the proxy. This issue has been fixed.

Filter - NAT

Support references 76343 - 76231

If several consecutive rules use the same object, they will no longer prevent the filter policy from reloading.

IPsec VPN

Support references 74551 - 74456

An anomaly in the IPsec function **key_dup_keymsg()**, which would generate the error*Cannot access memory at address* and cause the firewall to shut down suddenly, has been fixed.

Support reference 74425

A parameter would occasionally prevent *ResponderOnly* mode from running properly whenever *Dead Peer Detection* (DPD) was enabled. This anomaly has been fixed.

IPsec VPN (IKEv2 / IKEv1 + IKEv2)

Support reference 68796

In configurations that use IKEv2 IPsec policies or which combine IKEv1 and IKEv2, the firewall would sometimes fail to send a network mask to the Stormshield IPsec VPN client when it set up the mobile tunnel in config mode. The network mask that the IPsec client arbitrarily chose would then occasionally conflict with the local network configuration on the client workstation.

The firewall now always sends the network mask /32 (255.255.255.255) to the IPsec VPN client for mobile tunnels in config mode.

Global host objects included in router objects

Support reference 71974

When global host objects included in router objects are renamed, the change is correctly applied in the router object concerned.

Certificates and PKI

Support reference 76048

When certification authorities are imported, spaces in the import path are now correctly interpreted and no longer cause the import to fail.

ANSSI "Diffusion Restreinte" mode

When the ANSSI "Diffusion Restreinte" mode is enabled (**System** > **Configuration** > **General configuration** tab), a mechanism now checks the compatibility of Diffie-Hellmann (DH) groups used in the configuration of IPsec peers with this mode. The list of allowed DH groups has been updated; now only DH 19 and 28 groups must be used.

Excessive memory consumption of the serverd daemon

Support references 76158 - 75155

The memory consumption of the serverd daemon would increase to an excessive extent with the number of remote connections set up via SMC. This issue, which could prevent connections from being set up with the firewall's web administration interface, has been fixed.

Sandboxing

Support reference 76121

When no Sandboxing license has been installed (Stormshield Breach Fighter option) or when the license has expired, the AVD daemon would no longer shut down unexpectedly when users attempt to reload their configuration.

Network

Static routing

Support reference 72938

On the incoming interface of a bridge, policy-based (PBR) routing instructions now take priority over the option to keep initial routing. This new order of priority does not apply to DHCP responses when the IPS automatically adds the option to keep initial routing.

Support reference 72508

Router objects with load balancing that have been configured as the default gateway on the firewall would sometimes override static routes. As a result of this, connections would be initiated from the firewall with the wrong source IP address. This anomaly has been fixed.

Trusted Platform Module (TPM)

Support reference 76181

When the IKE2 / IKEv1+IKEv2 IPsec tunnel manager retrieves the encryption key stored on the TPM, it no longer causes memory leaks.

Intrusion prevention

SIP

Support reference 75997

When a sent SIP packet and its reply contained a field with an anonymous IP address, and the 465 alarm "SIP: anonymous address in the SDP connection" was configured to **Pass**, the firewall would restart unexpectedly. This anomaly has been fixed.

SNMPv3 protocol

Support reference 72984

The SNMP protocol analysis no longer wrongly raises the **Prohibited SNMP user name** alarm (snmp:393) for IDs specified in the whitelist of the SNMPv3 protocol.

Trusted Platform Module (TPM)

Support reference 76181

An anomaly in a function would sometimes cause a shortage of handles, or object identifiers, used for authentication on the TPM, making communication with the TPM impossible. This anomaly has been fixed.

Elastic Virtual Appliances (EVA)

CLIB /B serverd commands

The CLIB / Serverd MONITORB HEALTH command run on an EVA now returns the value *N/A* for absent physical modules (e.g., fan, disk, etc.) instead of *Unknown*, which caused an anomaly on SMC administration consoles.

Web administration interface

Authentication portal (captive portal)

Support reference 76398

The focus of the connection window in the captive portal is no longer set by default on the *Cancel* value. Pressing [Enter] on the keyboard after typing the login and password no longer logs off the user by mistake.

New features in SNS 4.0.1

Filtering

MAC address filtering

SNS now makes it possible to define and use network objects that are based on MAC addresses only. Such objects can be used in filter policies for level 2 filtering similar to stateful mode.

Industrial protocols

PROFINET support

PROFINET is a set of protocols used in the production, agriculture and transport sectors. PROFINET consists of four main protocols (among others): PROFINET-IO, PROFINET-RT, PROFINET-DCP and PROFINET-PTCP.

You can now filter by these protocols in SNS in order to secure such environments.

Industrial licenses

Industrial licenses are now verified and the configuration of industrial protocols is suspended if the license is missing (or when firewall maintenance has expired).

User comfort

New graphical user interface

The SNS version 4.0.1 graphical interface has been fully reworked to improve user comfort. It is now easier to switch between configuration and monitoring modules.

New simplified dashboard

The dashboard has been simplified to provide a clearer view of the status of the firewall. A drill down mechanism enables access to detailed information if it is needed for analyses.

New network configuration panel

The network configuration panel has been simplified to streamline the configuration of interfaces.

New certificate management panel

The certificate management panel has been simplified to facilitate PKI configuration.

New log display panel

The log display panel has been simplified and offers logs in the form of views by specific themes.

New responsive captive portal

The captive portal now has a new responsive design. Its display can be adapted to the size of the screen, so that the captive portal can be used on smartphones or tablets.

Initial installation wizard removed

The initial installation wizard has been removed.

Management

New health indicators

Two new health indicators are available: the first relating to CPU temperature, and the second relating to the administration password if it is too old or is still the default password.

Wi-Fi interface monitoring

Monitoring on Wi-Fi interfaces can now be viewed.

ARPING support

The ARPING command is now available to assist in analyses.

Exporting an identity (containing the private key) or a certificate

You can now export identities (user, server or smart card certificates and the associated private key) or certificates only (user, server or smart card).

Update procedure in cluster mode optimized

The update procedure for clusters has been optimized to prevent update files from being downloaded twice.

Refreshing SSHD configuration

The configuration of the SSHD service has been reworked to ensure compliance with the latest security standards.

Telemetry

A telemetry service is now available on SNS to maintain anonymous statistics regarding the life cycle of SNS firewalls. These statistics serve to improve the quality and performance of future products. The indicators reported in this version are:

- Percentage of CPU use,
- Percentage of memory use,
- Volume of logs generated.

Disabled by default, this service can be enabled/disabled in the module **Configuration** > **General configuration** > **Advanced properties** tab.

Stability and performance

HA mechanisms reworked

High availability synchronization has been simplified to ensure higher stability and better performance.

Proxy mechanisms reworked

The sandboxing features in Breach Fighter have been extracted from the proxy service and now run in a separate service for higher stability.

Improved IPS performance

The IPS connection manager has been enhanced to improve performance.

Simplified DCERPC plugin

The DCERPC plugin has been modified to enable easier configuration.

Overall improved performance

The operating system on SNS firewalls has been upgraded to provide better performance.

ClamAV antivirus

A new parameter in ClamAV makes it possible to restrict the duration of the antivirus analysis. This acts as a new layer of protection against zip bombs. As such, if the length of the analysis implies that the analyzed file contains an overwhelming amount of data, the analysis will be stopped.

Set by default to 120 seconds, this parameter can only be modified through the command:

```
CONFIG ANTIVIRUS LIMITS MaxProcTime=<time>
```

For more information on the syntax of these commands, please refer to the CLI SERVERD Commands Reference Guide.

Hardware

Hardware-based security for VPN secrets on compatible SN3100 models

Ever since revision A2 of SN3100 model firewalls, they now implement a trusted platform module (TPM) dedicated to securing VPN secrets. With the TPM, an extra level of security can be added to SN3100 appliances that act as VPN concentrators, which may not necessarily be physically secure. This module is supported from version 4.0.1 onwards and can be configured in the interface and in command line.

SN6100 - Seventh and eighth 8x1G modules supported

From SNS version 4.0.1 onwards, eight 8x1G modules can be supported on SN6100 appliances.

Resolved vulnerabilities in SNS 4.0.1

Certificates and PKI

Additional checks have been implemented when certificates are processed, in order to prevent the execution of JavaScript that can be embedded in specially crafted certificates for malicious purposes. Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

ClamAV

The vulnerability **CVE-2019-15961**, which would enable denial of service attacks through specially crafted e-mails, was fixed with the upgrade of the ClamAV antivirus engine.

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

OpenSSL

Vulnerabilities (CVE-2019-1563, CVE-2019-1547 and CVE-2019-1552) were fixed with the upgrade of the OpenSSL cryptographic library.

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

RTSP protocol

Support reference 70716

A flaw in the IPS analysis of the RTSP protocol with the interleaving function, mainly used by IP cameras, would occasionally cause the appliance to restart. This flaw has been fixed.

Do note that interleaving support is not enabled in factory configuration.

SNS 4.0.1 bug fixes

System

IPsec VPN (IKEV1 + IKEv2)

Support reference 73584

In configurations that use both IKEv1 and IKEv2 peers, as UID (LDAP) and CertNID fields used for authentication are applied, user privilege verifications for IPsec tunnel setup are no longer ignored.

Support reference 72290

On firewalls that host IKEv1 and IKEv2 peers, groups belonging to users who set up mobile IKEv1 tunnels with certificate authentication and XAUTH are now taken into account.

Automatic backups - Cloud Backup

Support reference 73218

Configurations backed up in Cloud Backup can now be restored again.

System - Time zone

Support reference 69833

The Europe/Moscow time zone on the system has been updated to fix a time difference of one hour.

Firewalls with IXL cards

For firewalls equipped with IXL cards:

- Fiber 4x10Gbps and 2x40Gbps network extension modules for SN2100, SN3100 and SN6100 models,
- 4x10G BASE-T modules for SN710, SN910, SN2000, SN2100, SN3000, SN3100 and SN6100 models.
- Fiber 10Gbps onboard ports on SN6100 models.

Support reference 73005

An issue with latency, which could affect firewalls connected using an IXL card on third-party equipment, has been fixed.

Support reference 72957

To prevent some negotiation issues relating to the automatic detection of media speed, the available values for IXL network cards can now be selected in the **Network** > **Interfaces** module.

Filter - NAT

The fields **Force source packets in IPsec**, **Force return packets in IPsec** and **Synchronize this connection between firewalls (HA)** were added to the CSV export file in filter and NAT rules.

High availability

When an alias is added to an existing network interface, firewalls in a HA cluster are no more switched.

High availability - IPsec VPN

Support reference 74860

As the SAD's (Security Association Database) anti-replay counters are sent to the passive firewall, sequence numbers are incremented in line with the high availability (HA) mechanism's operating mode.

Whenever the passive firewall detected IPsec traffic in HA configurations (e.g. monitoring frames from virtual IPsec interfaces), it would also send incremented sequence numbers to the active firewall.

As a result of these successive increments, sequence numbers would quickly reach the maximum values allowed. This would then wrongly activate IPsec anti-replay protection and block traffic going through tunnels. This issue has been fixed.

High availability and monitoring

Support reference 73615

A vulnerability to memory leaks has been fixed in high availability configurations with monitoring enabled.

Initial configuration via USB key

Support reference 73923

Firmware can now be updated again via USB key.

Authentication by certificate

A content check has been applied to some parameters used in the creation of cookies.

Reports

Support reference 74730

When the firewall is restarted, an anomaly occurs when the report database is enabled, causing several error messages to appear in the console:

```
checkdb[181]: Missing database file: /var/db/reports/reports.db
enreport: checkdb: Unable to restore the reports database
enreport: Unable to mount the reports database.
```

This anomaly has been fixed.

Serial port - File editors

Support reference 72653

A display bug that occurred during the use of Joe / Jmacs editors via serial link has been fixed.

Intrusion prevention

Support reference 73591

Enabling verbose mode on the intrusion prevention engine that analyzes some protocols (DCE RPC, Oracle, etc.) no longer causes the firewall to suddenly reboot.

Web administration interface

Static routing

Support references 73316 - 73201

In the **Network** > **Routing** module, the IPsec interface can now be selected again during the definition of a static route.

Network objects

Support reference 73404

Accented characters in the comments of network objects no longer prevent the pages of the web administration interface from loading correctly.

DHCP - Server

Support reference 73071

A warning message now appears to indicate that IP address reservations can no longer be added while a display filter is enabled.

DHCP - Relay

Support reference 72951

If network interfaces were specified to relay DHCP requests, they were replaced with the default value (*automatic*) after quitting and displaying the DHCP module again. This anomaly has been fixed.

Special characters

Support references 68883 - 72034 - 72125 - 73404

A bug during the conversion of special characters to UTF-8 (e.g. Asian or accented characters) generated XML errors and prevented affected modules, such as filtering and NAT, from being displayed. This anomaly has been fixed.

Certificates and PKI

Support reference 74111

CRLs containing several thousand revoked certificates would fail to display correctly on some firewall models. This issue has been fixed; now only the first 1000 items are displayed.

SNMP agent

Support reference 74337

During the configuration of the SNMPv3 server, both encryption algorithm buttons would always stay active even after they have been selected. This anomaly has been fixed.

Modbus protocol

Support reference 71166

The firewall would not take into account the information entered in the Allowed UNIT IDs table (**Application protection** > **Protocols** > **Industrial protocols** > **Modbus** > **General settings**). The same information would also not appear in the table after quitting the module.

Contact

To contact our Technical Assistance Center (TAC) Stormshield:

- 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.

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