STORMSHIELD

STORMSHIELD NETWORK SECURITY

RELEASE NOTES

Version 4.3 LTSB

Document last updated: February 13, 2024

Reference: sns-en-release_notes-v4.3.24-LTSB

Table of contents

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

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

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**.

Points to note for updates from a 3.7 LTSB or 3.11 LTSB version

IMPORTANT
If you intend to update a firewall from a 3.7 LTSB/3.11 LTSB version to version 4.3 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 4.3 LTSB from the latest 3.7 LTSB version available can be found in New firewall behavior in these release notes.

Extended Web Control (EWC) URL classification

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

Due to the new URL database, the firewall's initial security policy (filter policy, URL filter policy and SSL filter policy) must be reviewed after the firewall is updated.

Refer to the technical note Migrating a security policy to the new EWC URL database to find out how to migrate a URL/SSL filter policy during an update of the firewall to SNS version 4.3.24 LTSB or higher.

HTTP cache feature

The HTTP cache function is no longer available in filter rules. Before updating your firewall, ensure that you:

- Delete the "HTTP cache" options in the filter rules in question,
- Disable the proxy cache.

Otherwise, the proxy will no longer function.

High availability (HA)

The ports used for communication over HA links have changed. The filter policy must therefore be adapted accordingly on the members of the cluster and on any intermediate equipment through which HA traffic may pass before updating the firewall. The purpose of this step is to prevent connection loss between the members of the cluster.

The ports used by HA are listed in the HA network traffic section in the High availability on SNS technical note.

IPsec VPN

IPsec VPN and HA

IPsec tunnels that were set up will not be synchronized between both members of the cluster during an update, but will be suspended and renegotiated to let encrypted traffic pass through.

DR mode

DR mode set in 4.3 LTSB is not compatible with DR mode in earlier SNS versions, and the firewall does not allow updates of firewalls with DR mode enabled.

Refer to the IPsec VPN - *Diffusion Restreinte* mode technical note on how to configure DR mode in versions 4.3 LTSB.

IKEv1

The configurations listed below are no longer allowed in version 4.3 LTSB:

- 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.

Algorithms not supported

Versions 4.3 LTSB of the firmware no longer support the following algorithms:

- Blowfish,
- DES,
- CAST128,
- MD5,
- HMAC_MD5,
- NON_AUTH,
- NULL_ENC.

If the IPsec policy of the firewall to be updated to version 4.3 LTSB uses any of these algorithms, they must be replaced in the firewall's IPsec configuration before performing the update.

NAT-T

NAT-T - 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 set efined 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.

Quality of Service (QoS)

QoS configurations set in versions earlier than SNS 4.3 LTSB are no longer valid, and QoS must be configured again following a firewall update.

Refer to the technical note Configuring QoS on SNS firewalls on how to configure QoS in version 4.3 LTSB.

Filtering

SNS now makes it possible to define and use MAC address-based network objects in filter policies. When a MAC address is specified in an object used in a filter rule, any traffic originating from this object that matches this filter rule will not be evaluated if the MAC address presented during the exchange is different from the object's address.

TPM-equipped firewalls

After an update to SNS version 4.3, secrets stored in the TPM must be sealed with the new technical characteristics of the system, by using the command: `tpmctl -svp <TPMpassword>`.

For more information on this topic, refer to the Stormshield knowledge base.

SSL VPN

The latest 3.x version of the SSL VPN client must be used.

Netmask assigned to clients

The minimum mask size for the network object assigned to TCP and UDP clients in the SSL VPN configuration is now /28.

If the mask of this network object was /29, it must be changed before migrating the firewall to version 4.3 LTSB.

Authentication

Captive portal

The captive portal no longer accepts the selection of certificates other than server certificates that contain the ExtendedKeyUsage ServerAuth.

SSO Agent

The latest 3.x version of the SSO agent must be used.

Dynamic routing

Internal names of interfaces on SN160 and SN210(W) firewall models

The internal name for interfaces has changed on SN160 and SN210(W) firewall models.

To prevent inconsistencies in the configuration, we strongly recommend using the user names of interfaces (e.g, *out*) instead of internal names (e.g, *eth0*) regardless of firewall model.

BGP protocol

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.

Industrial protocols

Industrial licenses are verified and the configuration of industrial protocols will be suspended if the license is missing (or when firewall maintenance has expired).

System

Hardening of the operating system

The hardening of the operating system imposes the following constraints for custom scripts:

- Only *shell* scripts are allowed and they must be explicitly called up by the interpreter (e.g., sh script.sh instead of ./script.sh).
- For scripts launched through the event scheduler (*eventd*), the interpreter must be added for each task described in the event scheduler configuration file.
- Scripts must be located only in the root partition (/) so that they can be run.

TLS protocol - Cryptographic suites

The cryptographic suites that the firewall uses to initiate its own TLS connections (LDAPS, SYSLOG TLS, SMTPS, etc.) have been updated. The following are the suites that can now be used:

- 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.

This update may affect the firewall's compatibility with servers that use less robust suites. You are therefore advised to check the compatibility of TLS services that interact with the firewall. In the specific case of the LDAPS service in Microsoft Azure, the firewall must be forced to initiate connections that use less robust cryptographic suites (ECDHE-RSA-AES128-SHA256, DHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384 or DHE-RSA-AES256-SHA256) by executing the CLI/Serverd command `CONFIG CRYPTO SSLParanoiac=0`.

The firewall must be restarted for changes to be applied.

TLS protocol and firewall services

Firewall services (LDAP, authentication, proxy, etc.) that use the TLS protocol now impose the use of TLS 1.2 or 1.3. Connection attempts in older versions of this protocol will no longer succeed.

Active Update

Use of internal mirror sites

If you use an internal Active Update mirror site, packets hosted on your server must be updated with packets signed by the new certification authority.

The Active Update mirror site can also be hosted on a Stormshield Management Center (SMC) server.

Find out more on using SMC as an Active Update distribution point.

Increased security for 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.

SN Real-Time Monitor (SNRTM)

SN Real-Time Monitor is not compatible with firewalls in versions 4.3 LTSB.
Firewall monitoring must now be done via the **Monitoring** tab in the web administration interface.

Virtual firewalls

To update a firewall initially in version SNS 3.7 or higher to version 4.3 LTSB, follow the procedure for migrating a V/VS-VU virtual firewall to an EVA model.

Notable changes introduced between the last 3.7 LTSB version and the last 3.11 LTSB version

IPsec VPN and CRL

When the *CRLRequired* parameter is enabled in the configuration of a VPN policy, you now must have all the CRLs in the certification chain.

SSL VPN

Strengthened security

The level of security implemented during the negotiation and use of SSL VPN tunnels (OpenVPN) has been raised.

If you use the Stormshield VPN SSL client with **automatic mode disabled**, or another OpenVPN client, the configuration of SSL VPN clients must be changed accordingly. To do so, download the SSL VPN configuration from the captive portal of the SNS firewall that hosts the SSL VPN service and import it on the clients. With the Stormshield VPN SSL client in automatic mode, the client will automatically retrieve its configuration.

The new requirements to follow are:

- Stronger authentication and encryption algorithms:
  - SHA256,
  - ECDHE-RSA-AES128-SHA256,
  - AES-256-CBC (except on SN160(W), SN210(W) and SN310 firewalls, which continue to use AES-128-CBC).
- LZ4-based data compression (can be enabled or disabled),
- Strict verification of certificates presented by the server (certificate name and "server" certificates).

If you are not using the Stormshield VPN SSL client, you must work with a recent version of OpenVPN (2.4.x) or OpenVPN Connect (smartphones and tablets) clients.

SSL VPN and certificates

In SSL VPN configurations that use certificates without the *KeyUsage* field, some external services may no longer be able to communicate with the firewall.

To authenticate peers (client or server) in TLS, Stormshield firewalls now only accept certificates that have the *Key Usage* field, i.e., certificates that comply with X509 v3.

New firewall behavior

This section lists the changes made to the automatic behavior of the firewall when your SNS firewall in version 4.3.24 LTSB is updated from the latest 3.7 LTSB version available.

Changes introduced in version 4.3.24 LTSB

- SN1100 - The maximum number of IPsec tunnels that SN1100 firewalls accepted was too high. The number has been reduced to match announced data.
- 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 4.3.24 LTSB 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 4.3.24 LTSB 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 4.3.24 LTSB must be thoroughly checked.

Changes introduced in version 4.3.23 LTSB

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 4.3.23 LTSB 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 4.3.23 LTSB.

Changes introduced in version 4.3.22 LTSB

Find out more

- SSH connections to the firewall - On firewalls in factory configuration and in SNS version 4.3 LTSB (from version 4.3.22 LTSB onwards), 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 4.3.21 LTSB

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 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 4.3.21 LTSB, VPN tunnels can only be negotiated with peers that comply with this recommendation.
- VPN Exclusive client (with DR mode) - the VPN Exclusive client 7.4 (or higher) must be used to set up IPsec tunnels in DR mode with firewalls in SNS version 4.3.21 LTSB and higher 4.3 LTSB versions.

Changes introduced in version 4.3.18 LTSB

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 4.3.17 LTSB

Find out more

- IPsec VPN on SN 160(W), SN210(W) and SN310 model firewalls - The ESN (*Extended Sequence Number*) option is no longer automatically enabled when the selected encryption algorithm is compatible with hardware acceleration. Automatically enabling it would negatively affect performance.

Changes introduced in version 4.3.16 LTSB

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 4.3.15

Find out more

- 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`.
- TLS 1.3 protocol - 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.x to a version higher than or equal to SNS 4.3.15. It is also disabled by default in the incoming SSL analysis profile *SSL_00* for firewalls in factory configuration in version 4.3.15 or higher.

Changes introduced in version 4.3.11

Find out more

- Hardening of the operating system - Text editors Vim and JOE have been removed from the system and replaced with vi.
- IPsec/IPv6 - The keepalive function can no longer be enabled on IPsec tunnels in IPv6.
- 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 4.3.10

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 version 4.3.10 or higher, this percentage will automatically be converted to equivalent absolute bandwidth values.

Changes introduced in version 4.3.9

Find out more

- IPsec IKEv2 VPN - Whenever an IPsec IKEv2 tunnel set up with a mobile peer in config mode is abruptly shut down by the remote client, the IP address that is assigned to it remains locked and unavailable. The *unique* parameter (for *UniqueIDs*) has been added to the CLI/Serverd commands `CONFIG IPSEC PEER NEW` and `CONFIG IPSEC PEER UPDATE` so that this behavior can be modified.
  For example, to allow users to recover their previous IP addresses, use the parameter *unique=no*, then reload the configuration of the VPN policy by using the CLI/Serverd commands `CONFIG IPSEC ACTIVATE` and `CONFIG IPSEC RELOAD` (this will shut down tunnels in progress).

Changes introduced in version 4.3.7

Find out more

- Stealth mode - SNS firewalls in factory configuration are now in stealth mode by default.

Changes introduced in version 4.3.3

Find out more

- QoS - QoS configurations set in versions earlier than SNS 4.3 are no longer valid, and QoS must be configured again following a firewall update.
- High availability and link aggregation - On configurations equipped with link aggregation, when high availability is initialized, the **Enable link aggregation when the firewall is passive** option is enabled by default.
- TPM-equipped firewalls (SNi20, SN1100 and SN3100) - After an update to SNS version 4.3, secrets stored in the TPM must be sealed with the new technical characteristics of the system, by using the command: `tpmctl -svp <TPMpassword>`.
  For more information on this topic, refer to the Stormshield knowledge base. .
- TLS 1.3 protocol - Some TLS 1.3 traffic that previously could not be blocked, can now be blocked due to a new server certificate analysis.
- TLS 1.3 protocol - When the firewall analyzes TLS 1.3 certificates from SSL servers, permissions may need to be explicitly granted in peripheral security devices for the firewall's IP address(es) to access the SSL servers contacted.
- TLS 1.3 protocol - The SSL proxy now supports the TLS 1.3 protocol.
- IPsec profiles/Diffie-Hellman groups - When an IKE/IPsec profile is created, the Diffie-Hellman group suggested by default is now DH14 (more secure) instead of DH1.
- Protection from brute force attacks - Remote SSH access to the firewall is now protected from brute force attacks.
- RADIUS authentication - The maximum number of tries and the idle timeout allowed to set up a connection to a RADIUS server (main server and backup server) can now be configured.
- RADIUS authentication - RADIUS servers can now be reached in IPv6.
- SSL VPN - The minimum mask size for the network object assigned to TCP and UDP clients in the SSL VPN configuration is now /28. If the mask of this network object was /29, it must be changed before migrating the firewall to version 4.3.3 or higher.
- Certificate enrollment - When they submit a certificate enrollment request, users must now personally define the encryption key used to encrypt their private key.
- Hardening of the operating system - A specific local port for connection to agents/servers (main and backup) can no longer be specified for the RADIUS and SSO Agent authentication methods. These options could only be configured by using the *AgentBindPort* and *BackupBindPort* tokens found in the configuration files for these authentication methods.
- Hardening of the operating system - SNS firewalls now generate a system event whenever the mechanism that verifies the integrity of executable files refuses to run a binary.

Changes introduced in version 4.2.7

Find out more

- SSL certificate authentication with TLS v1.3 - To support post-handshake authentication on the firewall, the web browser used must allow post-handshake authentication so that the SSL certificate authentication method can function with TLS v1.3.

Changes introduced in version 4.2.5

Find out more

- SPNEGO authentication - The spnego.bat script, available in the MyStormshield personal area, now supports AES256-SHA1, replacing the previous cryptographic algorithm used, RC4-HMAC-NT.

Changes introduced in version 4.2.4

Find out more

- Hardening of the operating system - Only *shell* scripts are allowed, but they must be explicitly called up by the interpreter (e.g., sh script.sh instead of ./script.sh).
- Hardening of the operating system - For scripts launched through the event scheduler (*eventd*), the interpreter must be added for each task described in the event scheduler configuration file.
- Hardening of the operating system - Scripts must be located only in the root partition (/) so that they can be run.
- Stealth mode - SNS firewalls in factory configuration are no longer in stealth mode by default.
- IPsec DR mode - New warnings now appear in the **Messages** widget of the dashboard when IPsec DR mode is enabled.
- IPsec DR mode - After fixing an anomaly in the implementation of the ECDSA algorithm based on Brainpool 256 elliptic curves, IPsec tunnels could no longer be set up in DR mode, based on ECDSA and Brainpool 256 elliptic curves, between firewalls in SNS version 4.2.1 or SNS 4.2.2 and firewalls in SNS version 4.2.4 (or higher).
- Active Update - For clients who use internal mirror sites, you need to update the Active Update packets hosted on their own servers so that packets signed by the new certification authority are used.
- Stormshield Management Center 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 configuration is restored, the previous configuration will be restored.
- Logs - The possibility of storing all types of logs on a disk (including connection logs) has been enabled again by default on firewalls in factory configuration

Changes introduced in version 4.2.2

Find out more

- IPsec VPN - The firewall disables the ESN when the peer is in IKEv1.

Changes introduced in version 4.2.1

Find out more

- IPsec VPN - ESN support for ESP anti-replay is automatically enabled.
- IPsec VPN - 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. Refer to the **IPsec VPN technical note - *Diffusion Restreinte* mode** on how to configure DR mode in SNS 4.2 versions and higher.
- 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.
- IPsec VPN - version 4.2 no longer supports the following algorithms:
  - Blowfish,
  - DES,
  - CAST128,
  - MD5,
  - HMAC_MD5,
  - NON_AUTH,
  - NULL_ENC.

  If the IPsec policy of a firewall that must be updated to version 4.2 uses any of these algorithms, they must be replaced in the firewall's IPsec configuration before performing the update.
- NAT-T - 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 set efined 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.
- Logs - A field specifying the type of VPN rule (mobile tunnel or site-to-site tunnel) was added to IPsec VPN logs.
- SNMP - An SNMP trap is now raised whenever an IPsec VPN peer cannot be reached.
- SNMP - A new MIB (STORMSHIELD-OVPNTABLE-MIB) is available.
- SNMP - STORMSHIELD-VPNSA-MIB offers additional IPsec statistics.
- Authentication - Captive portal - The configuration of the captive portal no longer accepts the selection of certificates other than server certificates that contain the *ExtendedKeyUsage ServerAuth*.
- Authentication - SSO Agent - The SSO agent v3.0 or higher must be used with SNS firewalls in version 4.2..
- SSL VPN - The SSL VPN client must be in v2.9.1 or higher, and we recommend using the latest version of the SSL VPN client with SNS firewalls in version 4.2.
- Logs - 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.
- SSL VPN - 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).
- TLS v1.3 protocol - TLS v1.3 is used for services on the firewall (captive portal, LDAPS, Syslog TLS, Autoupdate, etc.).

- The cryptographic suites that the firewall uses to initiate its own TLS connections (LDAPS, SYSLOG TLS, SMTPS, etc.) have been updated. The following are the suites that can now be used:
  - ECDHE-ECDSA-AES128-GCM-SHA256,
  - ECDHE-RSA-AES128-GCM-SHA256,
  - DHE-RSA-AES128-GCM-SHA256,
  - ECDHE-ECDSA-CHACHA20-POLY1305,
  - ECDHE-RSA-CHACHA20-POLY1305,
  - ECDHE-ECDSA-AES256-GCM-SHA384,
  - ECDHE-RSA-AES256-GCM-SHA384,
  - DHE-RSA-AES256-GCM-SHA384,
  - TLS_AES_128_GCM_SHA256,
  - TLS_CHACHA20_POLY1305_SHA256,
  - TLS_AES_256_GCM_SHA384.

  This update may affect the firewall's compatibility with servers that use less robust suites. You are therefore advised to check the compatibility of TLS services that interact with the firewall. In the specific case of the LDAPS service in Microsoft Azure, the firewall must be forced to initiate connections that use less robust cryptographic suites (ECDHE-RSA-AES128-SHA256, DHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384 or DHE-RSA-AES256-SHA256) by executing the CLI/Serverd command `CONFIG CRYPTO SSLParanoiac=0`. The firewall must be restarted for changes to be applied.

Changes introduced in version 4.1.6

Find out more

- After signature certificates are updated, the USB Recovery procedure must be used to install a version lower than 4.1.6 on a firewall in version 4.1.6 or higher.

Changes introduced in version 4.1.4

Find out more

- SSL VPN - A new version of the component that SSL VPN uses in portal mode is offered to users of this service.

Changes introduced in version 4.1.3

Find out more

- IPsec VPN (IKEv1 + IKEv2) - The warning that appeared when a combined IKEv1/ IKEv2 IPsec policy was used has been deleted.
- SSL VPN - The SSL VPN client now applies the interval before key renegotiation set by default on the SSL VPN server to 14400 seconds (4 hours).
- Default gateway - Default gateways located in a public IP network outside the firewall's public address range can again be defined on the firewall. This behavior already existed in version 3.11.

Changes introduced in version 4.1.1

Find out more

- LDAP directories - Secure connections to internal LDAP directories are now based on standard protocol TLS 1.2.
- HTTP cache function - The HTTP cache function can no longer be used in filter rules. The proxy cache must be disabled before you update your configuration. Otherwise, the proxy will no longer function.
- Directory configuration - The default port used to access the backup LDAP server is now the same as the port that the main LDAP server uses.
- SNMP agent - The use of the value *snmpEngineBoots* has changed in order to comply with RFC 3414.
- Configuring protected mode - A new setting (stealth mode) makes it possible to allow the firewall's response to ICMP requests. This new setting takes priority over `sysctl net.inet.ip.icmpreply` calls.

Changes introduced in version 4.0.3

Find out more

- IPsec VPN - 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. This message appears when these algorithms are used in the profiles of IPsec peers.

Changes introduced in version 4.0.2

Find out more

- Tighter 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.

Changes introduced in version 4.0.1

Find out more

- The network controller used on SNi40, SN2000, SN3000, SN6000, SN510, SN710, SN910, SN2100, SN3100 and SN6100 firewalls has been upgraded and now allows VLANs with an ID value of 0. This measure is necessary for the industrial protocol PROFINET-RT.
- The internal name for interfaces has changed on firewall models SN160 and SN210(W). For configurations based on these firewall models and which use Bird dynamic routing, the dynamic routing configuration must be manually changed to indicate the new network interface names.
- Preferences in the web administration interface - When the firewall is updated to SNS version 4.0.1 or higher, preferences in the web administration interface will be reset (e.g., custom filters).

- 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).
- Industrial license - Industrial licenses are now verified and the configuration of industrial protocols is suspended if the license is missing (or when firewall maintenance has expired).
- New graphical 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.
- Different MAC addresses on SN310 firewalls - When an SN310 model firewall switches to SNS v4, this will change MAC addresses on the firewall's network interfaces. This difference in addresses may have an impact if the firewall's former MAC addresses were entered on third-party network devices (e.g., DHCP servers or routers).
- IPsec and HA - IPsec tunnels that were set up will not be synchronized between both members of the cluster during an update, but will be renegotiated to let encrypted traffic pass through.
- Filtering and MAC addresses - SNS now makes it possible to define and use MAC address-based network objects in filter policies. When a MAC address is specified in an object used in a filter rule, any traffic originating from this object that matches this filter rule will not be evaluated if the MAC address presented during the exchange is different from the object's address.

Notable changes introduced between the last 3.7 LTSB version and the last 3.11 LTSB version

IPsec VPN and CRL

When the *CRLRequired* parameter is enabled in the configuration of a VPN policy, you now must have all the CRLs in the certification chain.

SSL VPN

Strengthened security

The level of security implemented during the negotiation and use of SSL VPN tunnels (OpenVPN) has been raised.

If you use the Stormshield VPN SSL client with **automatic mode disabled**, or another OpenVPN client, the configuration of SSL VPN clients must be changed accordingly. To do so, download the SSL VPN configuration from the captive portal of the SNS firewall that hosts the SSL VPN service and import it on the clients. With the Stormshield VPN SSL client in automatic mode, the client will automatically retrieve its configuration.

The new requirements to follow are:

- Stronger authentication and encryption algorithms:
  - SHA256,
  - ECDHE-RSA-AES128-SHA256,
  - AES-256-CBC (except on SN160(W), SN210(W) and SN310 firewalls, which continue to use AES-128-CBC).
- LZ4-based data compression (can be enabled or disabled),
- Strict verification of certificates presented by the server (certificate name and "server" certificates).

If you are not using the Stormshield VPN SSL client, you must work with a recent version of OpenVPN (2.4.x) or OpenVPN Connect (smartphones and tablets) clients.

SSL VPN and certificates

In SSL VPN configurations that use certificates without the *KeyUsage* field, some external services may no longer be able to communicate with the firewall.

To authenticate peers (client or server) in TLS, Stormshield firewalls now only accept certificates that have the *Key Usage* field, i.e., certificates that comply with X509 v3.

New features and enhancements in SNS 4.3.24 LTSB

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 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 4.3.24 LTSB 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 4.3.24 LTSB or higher, please refer to the **Technical Note** Migrating a security policy to the new EWC URL database.

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.`

Resolved vulnerabilities in SNS 4.3.24 LTSB

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.

SNS 4.3.24 LTSB 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 4.3.21.

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).

The packet from the infected host or intrusion probe was rightly blocked, but 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.

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

Support reference 85439

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

The command that makes it possible to monitor changes to the configuration, used in particular by the SMC server, no longer causes the internal LDAP directory manager to restart.

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 version 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.

SSO agent management

Support references 85430 - 85443

A memory leak issue has been fixed in the SSO agent manager.

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.).

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 4.3 version or higher.

The following limitations have been placed on QoS implemented in SNS version 4.3:

- 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 traffic shaper's bandwidth.

SD-WAN

IMPORTANT
This is an early-access feature.
Refer to the section on Known issues before enabling this feature.

TPM-equipped firewalls

Support reference 83580

After an update to SNS version 4.3 LTSB, 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 module, refer to the section Trusted Platform Module in the SNS v4.3 LTSB user manual.

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

The EAP (Extensible Authentication Protocol) protocol cannot be used for the authentication of IPsec peers using the IKEv2 protocol.

In a configuration that implements an IPsec tunnel based on IKEv2 and address translation, the identifier that the source machine presents to the remote peer in order to set up the tunnel corresponds to its real IP address instead of its translated IP address. You are therefore advised to force the settings of the local identifier to be presented (**Local ID** field in the definition of an IKEv2 IPsec peer) using the translated address (if it is static) or an FQDN from the source firewall.

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 cause a lag and may potentially cause the service to shut down. You are therefore strongly advised to disable any unused VLAN interfaces instead of deleting them.

The possibility of adding WiFi interfaces in a bridge is currently in experimental mode and cannot be done via the web administration interface.

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 using 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.

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.

Vulnerability management

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).

Documentation resources

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

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

Installing this version

To update your firewall to SNS version 4.3.24 LTSB, we recommend that you carefully follow the procedure below.

Before starting the update, ensure that you have read:

- The Product Life Cycle guide,
- The section Points to note for updates from a 3.7 LTSB or 3.11 LTSB version.

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 Configuration automatic 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** tab. For more information, refer to the Backup tab section in the SNS user manual.

Updating a high availability firewall cluster

If the update applies to a firewall cluster in high availability mode (HA), 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 a firewall to version 4.3.24 LTSB, intermediate updates may be required based on its original version:

Starting point	Action
2.X version	Update to version 3.7.16 LTSB, then to the latest 3.7.X LTSB version available
3.X version	Update to the latest 3.7.X LTSB or 3.11.X LTSB version available
4.0.X version to 4.1.5 version	Update to version 4.1.6
4.1.6 version or higher	No intermediate updates required

V/VS-VU firewall	See Migrating a V/VS-VU model virtual firewall to an EVA model

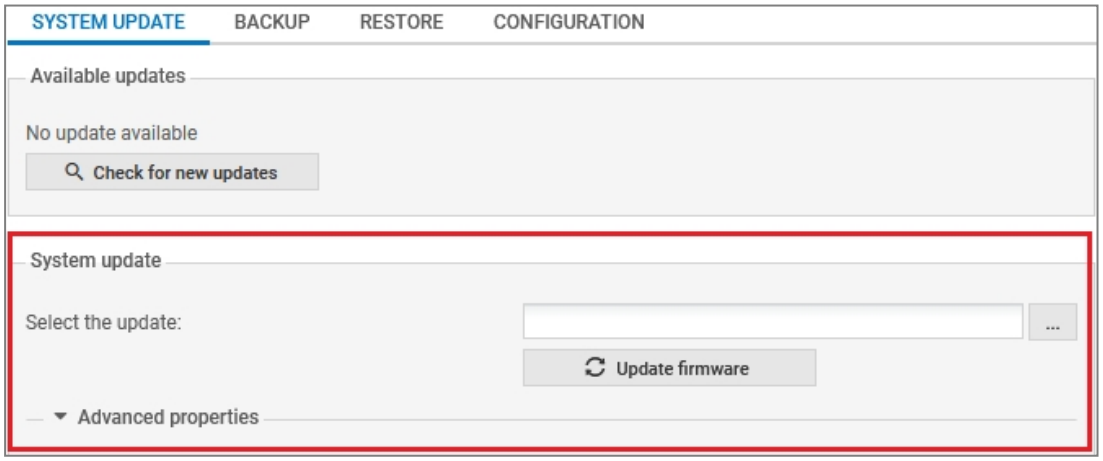
Downloading the update

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 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**. When the update is complete, you will be logged out and asked to re-authenticate.
   If an issue prevents the update from proceeding, you will be informed before the operation begins.

Previous versions of SNS v4.3 LTSB

In this section, you will find new features, resolved vulnerabilities and fixes from previous versions of SNS v4.3 LTSB.

4.3.23 LTSB	New features	Resolved vulnerabilities	Bug fixes
4.3.22 LTSB	New features	Resolved vulnerabilities	Bug fixes
4.3.21 LTSB	New features		Bug fixes
4.3.20 LTSB	New features	Resolved vulnerabilities	Bug fixes
4.3.19 LTSB	New features	Resolved vulnerabilities	Bug fixes
4.3.18 LTSB	New features		Bug fixes
4.3.17 LTSB	New features	Resolved vulnerabilities	Bug fixes
4.3.16 LTSB	New features	Resolved vulnerabilities	Bug fixes
4.3.15	New features	Resolved vulnerabilities	Bug fixes
4.3.12.2		4.3.12.2 version Release Notes	
4.3.12	New features		Bug fixes
4.3.11	New features	Resolved vulnerabilities	Bug fixes
4.3.10	New features	Resolved vulnerabilities	Bug fixes
4.3.9	New features		Bug fixes
4.3.8	New features	Resolved vulnerabilities	Bug fixes
4.3.7	New features	Resolved vulnerabilities	Bug fixes
4.3.6	New features	Resolved vulnerabilities	Bug fixes
4.3.5			Bug fixes
4.3.4	New features	Resolved vulnerabilities	Bug fixes
4.3.3	New features	Resolved vulnerabilities	Bug fixes
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

New features and enhancements in SNS 4.3.23 LTSB

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
```

For more information on the syntax of these commands, please refer to the CLI SERVERD Commands Reference Guide.

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 4.3.23 LTSB 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

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).

Resolved vulnerabilities in SNS 4.3.23 LTSB

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

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 4.3.23 LTSB 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.

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.

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.

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 4.3.23 or higher.

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.

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.

Routing

Support reference 85320

By updating to version 4.3.23 LTSB 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.

For more information on the syntax of this command, please refer to the CLI SERVERD Commands Reference Guide.

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 4.3.22 LTSB

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 4.3.22 LTSB 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 4.3.15 LTSB.
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.

SD-WAN

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.

SSH connections to the firewall

On firewalls in factory configuration and in SNS version 4.3.22 LTSB (and later 4.3 LTSB versions), 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 4.3.22 LTSB.

Resolved vulnerabilities in SNS 4.3.22 LTSB

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 4.3.22 LTSB bug fixes

System

Router objects

Support reference 84963

Updating to SNS version 4.3.22 LTSB (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 4.3.15 LTSB.

GRETAP tunnels

When the IP address of an active GRETAP tunnel's endpoint is edited, the changes are now correctly applied.

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.

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.

IPsec VPN

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.

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.

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`.

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.

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 4.3.21 LTSB

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.

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 4.3 LTSB versions (from version 4.3.21 LTSB onwards) and comply with this recommendation.

If IPsec DR mode is enabled on an SNS firewall in version 4.3.21 LTSB, VPN tunnels can only be negotiated **only** 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 4.3.21 LTSB, ensure that all IPsec DR-compatible peers in your architecture comply with this recommendation:

- On SNS firewalls, you must update all of them to an SNS 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.

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

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.

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.

IPsec VPN

It is now possible to set the amount of time to wait before a newly created SA (Security Association) is used. This can prevent potential issues with competing access when an SA is already in use for the same IPsec traffic endpoints. This *NewSADelay* option can only be configured by using the CLI/Serverd command `CONFIG.IPSEC.UPDATE NewSADelay=<value>`.

More information on the `CONFIG.IPSEC.UPDATE` command.

The mechanism that optimizes the distribution of the IPsec service's encryption and decryption operations on the SNS firewall has been improved.

SNS 4.3.21 LTSB bug fixes

System

IPv6 Bird dynamic routing

Support reference 84849

Whenever OSPFv6 or BGPv6 peers could not be reached, enabling IPv6 Bird dynamic routing would cause excessive consumption of memory buffers. This issue has been fixed.

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.

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.

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.

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 4.3.19 LTSB, would prevent the filter policy from being loaded.

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.

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.

Network

You can now configure how frequently ARP requests will be sent to a gateway so that ARP entries on the SNS firewall never expire. This makes it possible to prevent packet loss in some specific cases.

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.

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.

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.

Web administration interface

Monitoring

Support reference 84535

Expanding a category in the **Reports** section of the **Monitoring** tab no longer wrongly takes the user back to the previous screen.

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 4.3.20 LTSB

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.

Resolved vulnerabilities in SNS 4.3.20 LTSB

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 4.3.20 LTSB bug fixes

System

IPsec VPN

Support references 82578 - 84680

The management of resources used for IPsec VPN has been improved to reduce entries such as "job load of XXX exceeds limit of YY" in VPN IPsec logs.

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.

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.

SSL VPN

Support reference 85229

Users who belong to many groups from the LDAP directory can set up SSL VPN tunnels again. This regression appeared in SNS version 4.3.18.

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.

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.

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.

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.

IPsec tunnel monitoring

Support reference 84776

Refreshing the IPsec tunnel monitoring screen no longer causes the system error *Command processing failed*.

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.

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 85249

In a configuration that uses the BGP protocol with TCP-MD5 authentication, reloading the BGP configuration no longer prevents BGP sessions from being renegotiated. This regression appeared in SNS version 4.3.18.

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 4.3.20 or higher. The presence of the previous directive prevented authenticated BGP sessions from being opened after the firewall is updated. This regression appeared in SNS version 4.3.18.

Intrusion prevention engine

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.

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.

New features and enhancements in SNS 4.3.19 LTSB

HART-IP protocol

SNS version 4.3.19 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 4.3.19 LTSB

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 4.3.19 LTSB bug fixes

System

IPsec VPN

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 - 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.

Proxy

Support reference 84971

An issue regarding competing access in the management of connection source ports, which caused the proxy to suddenly freeze, has been fixed.

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.

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.

Filter - NAT

Support references 85004 - 85061 -85072 - 85131 - 85132 - 85133 - 85142 - 85157 - 85173 - 84957 - 84667-84955

When the filter policy is reloaded after a rule that contains address translation is edited, the firewall will no longer unexpectedly freeze.

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.

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 is due 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 4.3.18 LTSB

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.

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).

SNS 4.3.18 LTSB bug fixes

NOTE
The fix added in version 4.3.17 LTSB regarding memory leaks in the monitoring management engine has been removed. It will be reviewed and included in a future version.

System

IPsec VPN

Support reference 84823

The *half_open_timeout* can now be customized with the CLI / Serverd command CONFIG IPSEC UPDATE HalfOpenTimeout=<value> (30 seconds by default).

This parameter sets the timeout after which incomplete IKE associations are deleted (for example, a pending IPsec client authentication).

IPsec VPN - IKEv1 - Authentication by certificate and XAuth

Support reference 84775

When an IPsec IKEv1 tunnel with certificate and XAuth authentication is set up, the groups of the users are now correctly recorded in the tables of the intrusion prevention engine. The use of groups in filtering rules works properly again. This regression appeared in version SNS 4.2.

Certificates and PKI

Support reference 80053

The custom attributes set when a sub-certification authority (organization, organizational unit and state) or server identity (organization, organizational unit and location) is created are no longer wrongly replaced by the parent authority's attributes when they are different.

SN2100 and SN3100 firewall models - Updating firmware on SSD disks

To prevent SSD disks from potentially malfunctioning on SN2100 and SN3100 model firewalls, firmware update of such disks is automatically applied when the firewall is updated to SNS version 4.3.18 LTSB or higher. Reminder: this update had already been applied since SNS version 3.4.15 to the firewall models listed in the section Version 4.3.15 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.

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.

sfctl command

Support reference 84362

Changing the size of the window that displays the results of the *sfctl -T* command while data is being refreshed no longer causes segmentation errors that cause the *sfctl -T* command to stop functioning.

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 4.3.17 LTSB

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 4.3.17 LTSB

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.

PPTP and L2TP

A moderate severity vulnerability was fixed in a library used in PPP and L2TP.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2023-017.

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 4.3.17 LTSB 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 version 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) - TPM

Support references 85030 - 85031

When the password of the TPM is changed on the active member of the cluster, it is now immediately applied to the passive member to avoid a situation in which unsynchronized TPM passwords would prevent the passive member from accessing the keys of certificates protected by its TPM.

High availability (HA) - Logs

Support reference 84458

When an HA link lost many packets, the message "HA link is down" would be wrongly indicated in logs even though the link was still operational. When this occurs, the message now indicated in logs is "HA link is faulty".

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 version 4.3.3, 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 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.

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.

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.

Network

Bird dynamic routing

Support reference 83650

Bird dynamic routing has been optimized to improve the speed with which routes are forwarded from the Bird dynamic routing engine to the intrusion prevention engine to prevent latency issues during the transmission of network packets.

Bridge with two LACP link aggregates

Support reference 84552

When a bridge contains two LACP link aggregates, both aggregates now have the same MAC address as the bridge. In the case of clusters, this configuration will make it possible to prevent the passive member of the cluster from sending gratuitous ARP packets with the wrong MAC address.

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

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 4.3.7.

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.

Removal of an authentication method

Support reference 84411

Removing an authentication method from the list of available methods now fully erases the configuration settings of this method.

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.

VLAN interfaces

Support reference 83873

This sequence of actions:

1. Create and rename the first VLAN.
2. Do not apply configuration changes.
3. Create and rename the second VLAN connected to the same physical interface.

No longer wrongly raises an error indicating that both VLANs have the same name.

Antivirus - Dashboard

After migrating a configuration to version 4.3.15 (or higher) without any filter rules that use the antivirus, the antivirus monitoring icon (**Monitoring** > **Dashboard** module) no longer remains orange by mistake with the message "Download in progress".

Filter - NAT

Support reference 84980

After a search in the logs of a filter rule (right-click on a rule and select the action **Search in logs** in the pop-up menu), the same operation on another filter rule no longer wrongly keeps the ID of the first rule as a search criterion.

New features and enhancements in SNS 4.3.16 LTSB

Long-Term Support Branch (LTSB)

SNS version 4.3 is labeled “LTSB” so that it can be considered a version that will be stable over a long term, and will be supported for at least 12 months.

Refer to Compatibility to find out which products are compatible. For more information on the LTSB label, refer to the Network Security & Tools Product lifecycle document.

Resolved vulnerabilities in SNS 4.3.16 LTSB

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 4.3.16 LTSB bug fixes

System

High availability (HA)

Support reference 84843

A connection synchronization in HA (*bulk update*) would occasionally repeat itself indefinitely when it exceeded 5 seconds. This anomaly has been fixed.

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, in some cases, the cluster would continue to use the backup link. This anomaly has been fixed.

System monitoring – CPU load

Support reference 66123

Anomalies in the CPU consumption mechanism have been fixed to prevent unrealistic values from being reported.

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.

GRE interfaces

Support reference 84625

In configurations that use GRE interfaces when non-IP packets are present, memory leak issues would sometimes cause some services to shut down unexpectedly, which would then require the firewall to be restarted. 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 4.3.16.

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.

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.

GRE tunnels

Support reference 75479

During advanced troubleshooting, packets captured via *tcpdump* over GRE interfaces were malformed. This issue 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.

New features and enhancements in SNS 4.3.15

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 to version SNS 4.3.15,
- When switching from ClamAV to the advanced antivirus on a firewall in SNS version 4.3.15,
- When a passive firewall switches to active mode after a software update of a firewall cluster using the advanced antivirus in SNS version 4.3.15.

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).

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 4.3.15 is the first SNS 4.3 version that builds in support for SN-M-Series-720 and SN-M-Series-920 firewalls.

Find out more about SN-M-Series firewalls

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 4.3.15

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 4.3.15 bug fixes

System

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.

Updating firmware on SSD disks

Support reference 84295

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 4.3.15:

- 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).

Updates - Static routing

Support reference 84716

When an SNS 4.3 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.

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.

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.

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.

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.

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.

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.

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.

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).

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.

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.

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`.

Support reference 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.

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.

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).

Authentication

Support reference 84358

Whenever a user enters the wrong password during attempts to connect to the captive portal or via SSL VPN Client, the system event "LDAP unreachable Bind error" will no longer be generated.

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.

SSL certificate authentication

Support reference 80325

Adding the SSL certificate authentication method with the option **Enable searching in several LDAP directories**, and applying this change, then deleting the same authentication method, no longer blocks the connection to the firewall's web administration interface or the captive portal.

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

Maximum number of protected hosts

Support reference 84794

An issue with applying the change made in SNS version 4.3.10 regarding the maximum number of protected hosts has been fixed. So when the firewall is updated to SNS version 4.3.15, it will automatically be restarted a second time if the configuration requires it.

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.

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 4.3.15. It is also disabled by default in the incoming SSL analysis profile *SSL_00* for firewalls in factory configuration in version 4.3.15 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**.

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.

Web administration interface

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.

Version 4.3.14 not published

Version 4.3.14 is not available to the public.

Version 4.3.13 not published

Version 4.3.13 is not available to the public.

Version 4.3.12.2

ANSSI-certified version

Version 4.3.12.2 of SNS has its own set of **dedicated Release Notes**.

Version 4.3.12.2 has been **certified by the by the ANSSI** (French Network and Information Security Agency) which attest to the level of trust given to a security product in terms of its design and robustness.

New features and enhancements in SNS 4.3.12

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).

SNS 4.3.12 bug fixes

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 (*admin* or administrator account with Console [SSH] permissions),
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.

New features and enhancements in SNS 4.3.11

Blackhole interface

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

Resolved vulnerabilities in SNS 4.3.11

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 4.3.11 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.

IPsec VPN

The keepalive function on IPsec VPN tunnels in IPv6 has been removed to improve the stability of IPsec tunnels.

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.

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.

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.

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.

Restoration of the SNS firewall configuration or configuration deployment via SMC

Support reference 84630

An issue preventing configurations from being restored on the SNS firewall or new configurations from being deployed on the SNS firewall via the SMC server has been fixed. This issue generated the error "*Unable to move restored files to their final location*".

Network

8-port RJ45 module

Support reference 82270

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

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".

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 4.3.10

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.

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 4.3.10

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 4.3.10 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.

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.

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.

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.

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 SNS firewall handles a high volume of traffic.

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.

Maximum 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.

Competing access

Support reference 84486

An issue with competing access between two mechanisms on the intrusion prevention engine, which could cause the SNS firewall to freeze and disconnect its network access, has been fixed.

New features and enhancements in SNS 4.3.9

tpmctl command

Support reference 83999

The `tpmctl` command has been optimized.
In particular, these optimizations significantly shorten the time needed to list the status of certificates protected by the TPM when there are many certificates to list.

IPSec VPN IKEv2 - Mobile peers in config mode

Support reference 84482

Whenever an IPsec IKEv2 tunnel set up with a mobile peer in config mode is abruptly shut down by the remote client, the IP address that is assigned to it remains locked and unavailable. The *unique* parameter (for *UniqueIDs*) has been added to the CLI/Serverd commands **`CONFIG IPSEC PEER NEW`** and **`CONFIG IPSEC PEER UPDATE`** so that this behavior can be modified.

For example, to allow users to recover their previous IP addresses, use the parameter *unique=no*, then reload the configuration of the VPN policy by using the CLI/Serverd commands `CONFIG IPSEC ACTIVATE` and `CONFIG IPSEC RELOAD` (this will shut down tunnels in progress).

SNS 4.3.9 bug fixes

System

High availability, link aggregation and recovery of ARP requests

Optimizations have been applied to significantly speed up the recovery of ARP requests after a forced switch in a cluster that uses link aggregation.

User enrollment

Support reference 84344

An issue relating to user enrollment via the captive portal, particularly on firewalls that do not have a default certification authority (CA), has been fixed. This regression appeared in SNS version 4.3.0.

PKI CA CHECK CLI/Serverd command

Support reference 84347

The CLI/Serverd command `PKI CA CHECK` now also checks Autoupdate configuration files.

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.

New features and enhancements in SNS 4.3.8

Site-to-site IPsec tunnels with IPv6 traffic endpoints

The *keepalive* option can now be enabled on IPsec tunnels that have IPv6 traffic endpoints.

Static routes using router objects as gateways

Support reference 84239

In configurations that use a router object as the gateway for a static route without specifying the network interface used, this interface is determined dynamically so that it can be added to protected network interfaces.

Resolved vulnerabilities in SNS 4.3.8

SOFBUS and LACBUS protocol analyzes

A medium severity vulnerability was fixed in the SOFBUS and LACBUS protocol analyzer.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-015/.

SNS 4.3.8 bug fixes

System

SSL VPN

Support reference 83972

SSL VPN tunnels no longer fail to set up during the TLS negotiation phase when the authentication of the Stormshield SSL VPN client required too much time (e.g., in two-factor authentication).

Router and link monitoring - Logs

Support reference 84125

An anomaly in tracking the changing statuses of routers and links would cause a "Remote host unreachable" log to be written in the system log file every minute. This anomaly has been fixed.

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.

Refreshing IP addresses of FQDN objects

The IP addresses of FQDN objects are now correctly refreshed in the filter policy. This regression appeared in SNS version 4.3.6.

Viewing URL and SSL filtering groups

The help in the CLI/SSH command `tproxyd` command no longer wrongly indicates the possibility of viewing information about URL and SSL filtering groups. Ever since SNS version 4.1, such information is returned with the command `urlctl -g`.

The CLI/SSH command `sysinfo` displays information about URL and SSL filtering groups once again, as it now refers to the `urlctl -g` command to retrieve it. This regression appeared in SNS version 4.1.

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.

Intrusion prevention

Command displaying QoS rules in the console

Several anomalies have been fixed in the system command that displays rules relating to QoS (`sfctl -s qos` command):

- Filter rules regarding ICMP and which use a QoS queue with a **Connection threshold** (**Action** > **Quality of service** tab) no longer wrongly display the UDP threshold,
- Filter rules that use a QoS queue without a **Connection threshold** are now displayed.

New features and enhancements in SNS 4.3.7

Support for extra-hardened SNxr1200 firewall

SNS version 4.3.7 introduces support for extra-hardened SNxr1200 firewall.

More information about the SNxr1200 firewall.

Restriction on memory consumption by services on the firewall

A mechanism that restricts the amount of memory used by services on the firewall has been set up to prevent any service from using an excessive amount of memory.

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 4.3.7

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 4.3.7 bug fixes

System

High availability

Support reference 70868

When in a cluster:

- Each member has a unique link aggregate connected to the same network switch,
- This aggregate is used as the first interface in a bridge,
- The option **Enable link aggregation when the firewall is passive** is enabled,

So when a switch occurs, the MAC address of the bridge is no longer imposed, to the detriment of the aggregate's MAC address on the new active member.

Link aggregation without IP address

Support reference 83524

When a configuration in SNS version 3.x, which contains a link aggregate without an IP address (inactive aggregate) was migrated to an SNS 4.x version, it wrongly attempted to activate this aggregate, therefore triggering the system error "AggX error: The interface is active but does not have an IP address". This issue has been fixed and the aggregate remains disabled after the migration.

Importing objects via a CSV file

Support reference 84224

Additional controls have been implemented to avoid importing objects via a CSV file that may contain characters that do not conform to the UTF-8 standard (includes comments in objects).

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.

Intrusion prevention

ICMP

As SNS firewalls in factory configuration are in stealth mode by default, disabling stealth mode no longer wrongly raises the alarm "Invalid ICMP message" (alarm icmp:67) when the destination cannot be reached.

Web administration interface

Removing an IPsec encryption profile

During an attempt to remove a local IPsec encryption profile, a window appears to confirm the operation: pressing Esc no longer confirms the removal by mistake but cancels it as requested.

New features in SNS 4.3.6

SSL VPN

The SSL VPN engine (TCP and UDP) has been optimized for better performance.

Resolved vulnerabilities in SNS 4.3.6

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

Medium 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 4.3.6 bug fixes

System

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.

HTTP proxy

Support reference 83607

Issues with competing access to connection counters, which could cause the proxy to shut down unexpectedly, have been fixed.

IPsec VPN - Protocol selection

Support references 83711 - 83777

Selecting the only protocol allowed to set up an IPsec tunnel (TCP, UDP, ICMP or GRE in the **Protocol** column of the tunnel grid) would sometimes prevent IPsec tunnels from being monitored in the web administration interface. This regression, which first appeared in SNS version 4.2, has been fixed.

Host reputation

Support reference 77080

Hosts referenced in the host reputation monitoring list could previously be deleted from the object database. This inappropriate operation, which would cause a system error that prevented the proxy from starting, has been fixed.

Traffic statistics - Virtual IPsec interfaces

Support reference 82960

The counters that counted packets passing through virtual IPsec interfaces were no longer refreshed (SNMP requests or *netstat* system command). This anomaly, which first appeared in SNS version 4.1, has been fixed.

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.

Local connection of an administrator with the "Console (SSH)" permission

Support reference 84289

When administrators with the **Console (SSH)** permission attempted to connect locally (in console mode or with a monitor/keyboard), their attempts would fail and could cause the console to freeze after two attempts. This issue has been fixed.

IPsec VPN with certificate-based authentication - Topology deployed via SMC

Support reference 84231

Whenever an IPsec VPN topology with certificate-based authentication was deployed from an SMC server, any attempt to modify the firewall (via the web administration interface) of the peer defined in this topology would wrongly display a system error message “A mandatory token for this message has not been specified”. This issue has been fixed.

QoS - Modifying a default queue initially configured in percentage

Any attempt to reconfigure a default queue (or a default ACK queue) that was initially configured in bandwidth percentage would cause an error and display the error message “Reference needed for percentage”. This issue has been fixed.

Hosts with dynamic IP address resolution used in sub-groups

Support references 84202 - 81951

Whenever a host was:

- Configured with dynamic IP address resolution,
- Placed in a sub-group that is in turn used in a configuration module on the firewall (filter rules, permissions to access the web administration interface, etc.).

Changes to this host’s IP address would be ignored in the configuration module in question. This issue has been fixed.

Intrusion prevention

SOFBUS - LACBUS protocol

An anomaly in the engine that analyzes the SOFBUS protocol would wrongly raise the "SOFBUS: invalid protocol” alarm (modbus:741). This anomaly has been fixed.

Android WhatsApp and *Facebook* applications

Support reference 82865

Legitimate packets from *Android WhatsApp* or *Facebook* applications would sometimes wrongly trigger the block alarm "SSL version mismatch" (ssl:117 alarm). This regression, which first appeared in SNS version 4.2.1, has been fixed.

SSL protocol

Enabling the option **Allow 0-RTT** could wrongly raise the alarm "SSL: invalid answer with connection state” (ssl:735 alarm). This issue has been fixed.

SNS 4.3.5 bug fixes

System

Updating the firewall

Support reference 84361

The firewall would occasionally restart in loop after an update to SNS version 4.3. This issue has been fixed.

New features in SNS 4.3.4

SD-WAN

Using the CLI/Serverd command `MONITOR ROUTER name=router_name` makes it possible to display the values of SD-WAN metrics of the various gateways that make up the router specified as an argument.

For more information, refer to the CLI Serverd Commands Reference Guide.

Resolved vulnerabilities in SNS 4.3.4

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 4.3.4 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.

Firewall managed from Stormshield Management Center (SMC)

Support reference 81863

When an administrator connects to a firewall from their SMC connecting server, this administrator's connection identifier will now correctly appear in the right upper banner of the firewall's web administration interface.

Values of SD-WAN monitoring parameters

To fit most SD-WAN requirements, the default values and values acceptable as availability testing parameters have been changed:

- Idle timeout: 1s by default (as opposed to 2s prior to SNS 4.3.4),
- Frequency: 5 seconds by default, with a minimum of 2 seconds (as opposed to 15s prior to SNS 4.3.4),
- Number of tries: 5 (as opposed to 3 prior to SNS 4.3.4).

Logs - SD-WAN statistics

Support reference 83961

Statistics regarding SD-WAN metrics (latency, jitter, packet loss rate, etc.) are now collected every 10 minutes (instead of 15) to be better synchronized with routing statistics.

VPN logs

Support reference 83792

Anonymized VPN logs (without any specific access privileges granted) would occasionally reveal information about the remote user certificate by mistake (*remoteid* field). This anomaly has been fixed.

Network configuration

Support reference 84225

When there are two sections with the exact same name in the network configuration file, the mechanism that reloads network parameters would freeze. This issue has been fixed.

Static routing
An anomaly which sometimes prevented some routes from being correctly applied (unroutable gateways) has been fixed.

SD-WAN - Logs
In configurations that use SD-WAN, the system log now indicates what caused the links to switch.

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.

QoS
After a traffic shaper was assigned to an interface, its default queue or default ACK queue could no longer be changed. This anomaly has been fixed.

Defining a CBQ QoS queue by using both an absolute value and a percentage for its min. and max. bandwidth characteristics (or reverse min. and max.) could generate inconsistencies in the QoS configuration and block matching traffic. This type of configuration is now explicitly rejected.

QoS configured in a protocol alarm

Support reference 84237

Renaming a QoS queue that is used in a protocol alarm would make this queue disappear from the alarm configuration and cause a system error. This issue has 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.

IPsec VPN - Encryption profiles

Support reference 84245

When AES-GCM_16 is selected as the phase 1 (IKE) algorithm, the field that makes it possible to specify an authentication algorithm is now grayed out.
As the only authentication method that AES-GCM-16 supports is prfsha256, it will be automatically selected.

Enabling the ANSSI *Diffusion Restreinte* (DR) mode

Support reference 82914

When DR mode is enabled on an IPsec configuration that does not meet all of this mode's requirements, the warning message indicating that the IPsec configuration has been disabled now comes with a blinking symbol indicating that the firewall must be manually restarted in order to apply changes (upper right section of the screen).

New features in SNS 4.3.3

SD-WAN and QoS

IMPORTANT

These are early access features.

You must refer to the Known issues and Limitations and explanations on usage before enabling these features or updating an existing QoS configuration to an SNS 4.3 version.

Selecting the best link

Specific criteria can now be configured to determine whether a WAN link meets the quality level appropriate for its type of traffic (VoIP, video, etc.).

To do so, for each type of traffic, you can define a Service Level Agreement (SLA) based on one or several thresholds from the following criteria:

- Latency,
- Jitter,
- Packet loss.

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

This configuration can be applied to standard traffic or encrypted communications.

Regardless of the type of traffic, you can also set up a more general configuration to ensure that all communications will automatically be switched to a backup link when the quality of the main link is degraded.

You can view the quality of your various links at any time from the firewall's web administration interface.

For further information, refer to the sections Network objects - Router, Monitoring - SD-WAN and Reports in the SNS User guide.

Improved Quality of Service (QoS) feature

The Quality of Service (QoS) feature has been enhanced to meet the requirements of recent infrastructures. With these changes, the definition of traffic priority as well as bandwidth restriction and reservation can be significantly improved.

For more information, refer to the section Quality of Service (QoS) in the User guide.

IMPORTANT

QoS configurations defined in versions earlier than SNS 4.3 are not automatically valid. Traffic shapers must be set so that these QoS configurations can be enabled after an update to SNS version 4.3.

Static routing - Router objects

Router objects can now be selected as gateways when a static route is created or modified. For each static route, this makes it possible to set a link selection policy.

You can always apply a different link selection policy to specific traffic streams by configuring them directly in the rules of your filter policy (policy-based routing). These configurations have higher priority than static routing configurations.

For further information, refer to the sections IPv4/IPv6 static routes, Network objects - Router and Filtering in the SNS User guide.

NOTE
Router objects defined with load balancing are not compatible with this feature.

TLS protocol 1.3

Analysis of server certificates

The intrusion prevention engine now attempts to retrieve the server certificate for every TLS v1.3 traffic stream that passes through the firewall so that any security flaws relating to this certificate can be analyzed and attack signatures and applications that rely on the analysis of this certificate can be enabled.

This analysis is enabled by default on the firewall. Some TLS 1.3 traffic can now be blocked, but previously could not due to this new protocol analysis.

Find out more

SSL proxy

The SSL proxy now supports the TLS 1.3 protocol.

SOFBUS and LACBUS industrial protocols

SNS firewalls can now detect and analyze SOFBUS and LACBUS protocols. This analysis is disabled by default and makes it possible to detect abnormal behavior and filter specific SOFBUS and LACBUS commands to minimize the attack surface and risk of compromise. These protocols are used mainly in water management infrastructures, and are the intellectual property of LACROIX Sofrel.

Find out more

Network captures

A new network capture tool is now available in the web administration interface of SNS firewalls and can be used to resolve issues. The most common filter criteria (IP, port, interface, etc.) can be entered in a filter creation wizard, which will allow users who are unfamiliar with *tcpdump* or the format of its filters to create network captures. The *tcpdump* filter can also be manually entered for advanced users.

With this new tool, up to five simultaneous captures can be run. To access it, the firewall must be equipped with a storage medium on which captures can be saved (e.g., internal storage or SD card).

Find out more

Remote access to the firewall via SSH

Opening access to the firewall's administrator accounts

Administrators declared on the firewall can now be assigned access privileges to the firewall in SSH. Such access is restricted by default to the *nsrpc shell* interpreter (CLI/Serverd commands are used) and can be extended to the operating system's *shell* interpreter if the *super-administrator* (*admin* account) allows it.

Find out more

Protection from brute force attacks

Remote access to the firewall via SSH is now protected from brute force attacks. If this protection mode is already enabled on the firewall, its perimeter will be automatically extended.

Find out more

RADIUS authentication

Dashboard

RADIUS servers are now monitored and their statuses shown in the **Services** widget of the **Dashboard**.

Idle timeout and maximum number of connection attempts

The maximum number of attempts and idle timeout allowed to set up a connection with a RADIUS server (main and backup servers) can now be configured. This simply requires changing the CLI/Serverd command `CONFIG AUTH RADIUS` by adding the arguments *timeout*, *retry*, *btimeout and bretry*.

Find out more

Support for RADIUS VSAs

Users authenticated via RADIUS can now be associated with groups in the firewall after support for RADIUS VSAs was enabled. This makes it possible in particular to add administrators whose users or groups come from other domains. For this feature to work, the RADIUS server must also be configured to use VSAs.

Support for VSAs on the firewall is enabled by default but can be disabled using the CLI/Serverd command `CONFIG AUTH RADIUS` with the argument *[VSAusergroup=<0|1>]*.

Find out more

IPv6 support

RADIUS servers can now be reached in IPv6, which means that RADIUS servers with objects that use IPv6 addresses can be configured in the firewall.

Support for the *domain* attribute

A user's domain name can now be copied to the field in the RADIUS request allowing the inclusion of RADIUS authentication in a federation that consists of several domains.

Source IP address of RADIUS requests

The source IP address of RADIUS requests can now be configured.

Find out more

Processing RADIUS requests

RADIUS requests are now asynchronously processed to facilitate their integration with OTP platforms.

LDAP server

The firewall's internal LDAP server now uses a TLS configuration in line with the recommendations given by the French Network Information Security Agency (ANSSI).

Find out more

VPN

IPsec VPN IKEv2 - Support for MOBIKE

MOBIKE can now be used with mobile peers. With MOBIKE, mobile users no longer need to renegotiate their tunnels when they change IP addresses.

MOBIKE can only be enabled by using the CLI/Serverd commands `CONFIG IPSEC PEER NEW` and `CONFIG IPSEC PEER UPDATE` with the argument *[mobike=<0|1>]* depending on whether you are adding or updating a peer.

An additional parameter makes it possible to define in an IPsec policy the interfaces on which the IPsec engine builds its list of IP addresses that it shares via MOBIKE. In this way, the IP addresses shared when MOBIKE is used can be kept to a strict minimum. The list of interfaces affected can only be modified using the CLI/Serverd command `CONFIG IPSEC UPDATE` with the argument *[UsedInterface=<itf1,itf2,...>]*.

NOTE

MOBIKE is not compatible with the ***Diffusion Restreinte*** **(DR) mode** that complies with the recommendations of the French Network Information Security Agency (ANSSI).

SSL VPN

The speed with which connections are set up, and SSL VPN support for the TLS 1.3 protocol have been enhanced. You must use a TLS 1.3-compatible SSL VPN client to benefit from these enhancements. Do note that Stormshield Network SSL VPN Client in version 2.9 is not compatible with this protocol.

These enhancements now require a minimum mask size of /28 for the network object assigned to UDP and TCP clients in the SSL VPN configuration.

High availability and link aggregation

In configurations that contain network link aggregates, when high availability is initialized, the **Enable link aggregation when the firewall is passive** option is enabled by default. This option optimizes swap time.

High availability - Direct links between members of the cluster

In high availability configurations with direct HA links between both members of the cluster (without any intermediate network switch), when HA links are down after the main firewall fails, the switch to the other member of the cluster takes place immediately.

Link aggregation - Redundancy

Redundancy link aggregates can now be created. With the redundancy feature, a backup link can be set up in case the main link (identified as *Master* in the aggregate) stops responding. A **Redundancy** aggregate must contain two links.

This new feature is available only on SN510, SN710, SN910, SN1100, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100, SNi20 and SNi40 models. SNS firewalls support this feature only with Cisco switches.

Find out more

Telemetry service

When SNS firewall administrators connect to the web administration interface, a window prompts them to enable the telemetry service if it has been disabled.

Find out more

Certificates and PKI

Web enrollment - Certificate enrollment

The web enrollment service has been enhanced to allow users to submit certificate requests from the latest versions of mainstream web browsers. When users submit a request, they must now define the encryption key themselves, to encrypt their private key.

Find out more

Refreshing the CRL of a CA

A new CLI/Serverd command `SYSTEM CHECKCRL` is available, and makes it possible to force the refreshment of a certification authority's (CA) certificate revocation list (CRL).

Find out more

Hardening of the operating system

Executable file integrity verification mechanism

SNS firewalls now generate a system event when the executable file integrity verification mechanism refuses to run a binary file.

Secure Boot

The **Secure Boot** feature can now be enabled in the UEFI of Sni20, SN1100 and SN3100 firewalls. When this feature is enabled, the security of the system can be increased, in particular by verifying the signature of the system that was loaded when the firewall started up.

Resolved vulnerabilities in SNS 4.3.3

IXL network cards

Moderate severity vulnerabilities have been fixed in the drivers of IXL network cards and NVM utilities.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2020-029/,
- https://advisories.stormshield.eu/2020-031/,
- https://advisories.stormshield.eu/2020-032/,
- https://advisories.stormshield.eu/2020-033/,
- https://advisories.stormshield.eu/2020-036/,
- https://advisories.stormshield.eu/2020-040/,
- https://advisories.stormshield.eu/2021-066/.

SNS 4.3.3 bug fixes

System

IPsec VPN

Support reference 78214

Site-to-site IPsec tunnels with *all* as the source traffic object no longer wrongly activate the sending of keepalive packets with the broadcast address (255.255.255.255) as the source address. Such packets were blocked because the alarm “Broadcast address used in source address” (ip:89) was raised.
Do note that this anomaly did not disrupt legitimate traffic in IPsec tunnels.

Support reference 82729

Whenever a certificate was identified by a name (DN - Distinguished Name) longer than 128 characters, the firewall would retain only the first 128 characters. The deployment of an IPsec configuration via SMC with such a certificate would therefore fail because the DNs of the certificates do not match.
The maximum size has been raised to 240 characters, the technical limit.

Support reference 81471

In configurations using IPsec VPN tunnels that handle a high network load, when an ARP entry expires, network packets will no longer be lost.

Support reference 81691

Due to an anomaly in the sequencing of processes/threads when priority is dynamically changed, packets would sometimes get lost on firewalls handling heavy traffic. This anomaly has been fixed.

Support reference 83059

IPsec tunnels in which a peer has a name that contains an accented character can now be correctly set up again. This regression appeared in SNS version 4.2.

IPsec VPN IKEv2

Support reference 79713

The reauthentication of an IPsec IKEv2 tunnel in phase 1 would sometimes end too quickly, causing legitimate packets to be wrongly rejected. To prevent this situation, a new setting can be used to delete the older IKE SA later.

IPsec VPN - Certificates

Support references 78593 - 78611 - 73609

For IPsec peers that were deployed via SMC (global IPsec policy) and used certificates defined locally on the firewall, the certificates used were not shown in details of peers. This issue has been fixed.

SSL VPN

Support reference 81349

The OpenVPN daemon would sometimes shut down unexpectedly, logging out all users connected via the SSL VPN as a result. This issue has been fixed.

Proxies

Support reference 79295

Proxies and proxy-based modules (URL classification, etc.) now correctly manage certificates that contain both an empty*Subject* field and a filled in *Subjectaltname* field.

Creating interfaces

Support reference 75064

Configurations containing several hundred interfaces (e.g., virtual interfaces, VLAN interfaces, etc.) would cause excessive CPU consumption after the network interface configuration file was repeatedly reloaded.

Host reputation

Support reference 78563

Data relating to the host reputation function no longer consumes an excessive amount of disk space. This issue prevent reports from being displayed.

> **NOTE**
> The host reputation database must be reinitialized to apply this fix (Application protection module > Host reputation > **Reset scores for all hosts in the database** button).

UDP Kerberos authentication

Support reference 78725

The UDP-based Kerberos authentication method no longer worked from SNS version 4.0.3 onwards after support for FAST pre-authentication was introduced in this method (RFC6113). This issue has been fixed.

Authentication to an LDAPS server

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.

Initial configuration via USB key

Support reference 81713

When a firewall is configured via USB key, changes to the reference time zone specified in the additional configuration file in CSV format is now correctly applied.

Network objects - Importing with CSV files

Support reference 78683

Network objects imported via CSV files are now immediately factored into the firewall's configuration.

Automatic updates

Support reference 72728

An issue with scheduled automatic updates that were not applied, occurring whenever the update frequency of a subsystem (antivirus definitions, etc.) was changed, has been fixed.

Whenever a specific port is indicated in an Active Update customized URL, it will now be correctly applied.

Event scheduler

Support reference 77428

The %STATE% macro, which can be used in the event scheduler, is now operational and returns the expected values.

Disk monitoring

Support references 75125 - 75126

An issue with alarms being wrongly raised over the disk status of firewalls has been fixed.

Interface monitoring - VLANs and aggregates

Support reference 80066

For VLANs attached to interfaces that are included in aggregates, the right throughput is now shown in the interface monitoring module, and no longer remains frozen at 10 Mb/s.

ICMP - IPv6

Support reference 82547

In configurations that use IPv6, an issue with competing access could make the firewall freeze whenever it received “destination unreachable” ICMP packets. This issue has been fixed.

PPTP Server

The PPTP server that enables the setup of tunnels between a PPTP client and the firewall now functions again. This regression appeared in SNS version 4.2.

Access to the console via a serial port

Support references 82054 - 81429

On firewall models other than SN210(W) and SN310, access to the console via a serial port no longer made it possible to interrupt the startup sequence to change the password of the admin account in single user mode. This issue has been fixed.

SNMP Agent

Issues with competing access, which can cause the service to shut down, have been fixed in the mechanism that verifies the number of SNMP notifications received.

Support reference 78695

A bandwidth anomaly on link aggregates and on VLANs in the link aggregates, which was reported in the ifSpeed and ifHighSpeed OIDs of the IF-MIB MIB, has been fixed.

Connecting to the web administration interface with certificate-based authentication

Support reference 79815

On firewalls with a configuration that included several LDAP directories, if an administrator with an account from one of the secondary directories authenticated via certificate, the authentication would fail. This issue has been fixed.

SSH connection - Password containing the *$* character

Support reference 82949

Passwords containing the *$* character (e.g., pas$$word) can now be saved correctly. Users connecting via SSH therefore no longer need to add an escape character \ before each *$* character when they enter their passwords.

High availability

Support reference 82211

The ARP cache clearing mechanism, a high availability option, has been enhanced to remove entries at the right moment. Before this fix, such entries were occasionally deleted too early, potentially causing delays in the recovery of some network traffic streams.

High availability - Diffusion Restreinte mode

Enabling *Diffusion Restreinte* mode in Stormshield Management Center on a high availability configuration (either by direct activation or by restoring a configuration) now makes the passive member of the cluster restart correctly.

High availability (HA) and link aggregation

Support references 82211 - 82855

In high availability configurations:

- That use link aggregates linked to a network switch,
- On which theoption **Enable link aggregation when the firewall is passive** is enabled,
- And for which each member of the aggregates affects the calculation of the quality index (*LACPMembersHaveWeight* parameter set to 1 via the CLI/SERVERD commands `CONFIG HA CREATE` or `CONFIG HA UPDATE`),

when the switch is lost and subsequently recovered, random swaps may occur within the cluster. This issue has been fixed.

Filtering and NAT

Support references 81369 - 83651

When a NAT policy containing many rules is reloaded, network packets may get lost. An optimization mechanism that prevents such packet loss can be enabled using the CLI/Serverd command `CONFIG PROTOCOL IP COMMON IPS CONFIG`, by adding the *natdiff* parameter to the existing parameters in the *OptimizeRuleMatch* option.

Use the following parameters in a default configuration:
OptimizeRuleMatch=equal,diff,cache,natdiff.
Any changes must then be confirmed with the command `CONFIG PROTOCOL IP ACTIVATE`.

Do note that this mechanism is disabled by default.

NAT - VLANs

Support reference 79759

In configurations that support several VLANs on the same physical interface, and which implement NAT with ARP publication on the same VLANs, GARP (*Gratuitous ARP*) packets would occasionally be sent by mistake on only one of these VLANs. This issue has been fixed.

Firewalls equipped with a TPM

Support reference 83580

Known PCRs (Platform Configuration Registers) on the TPM may occasionally be modified after a firmware update, invalidating the policy that grants access to secrets stored in the TPM.
The CLI/Serverd command `SYSTEM TPM PCRSEAL tpmpassword=<password> [serial=(<serial>|passive|active|local)]` was created so that this access policy can be updated by saving the new acceptable PCR values in the TPM from the web administration interface via the **CLI console** module.
In high availability configurations, this command can also make it possible to select the member of the cluster on which this operation must be performed.

Intrusion prevention

Intrusion prevention engine performance

Support references 76810 - 77932

Changes have been made to the mechanism that allocates memory to connections for the intrusion prevention engine in order to improve its performance.

Intrusion prevention engine statistics

Support references 79713 - 82437 - 81466

The mechanism that manages the statistics of the intrusion prevention engine has been optimized. These changes help to prevent potential packet loss when these statistics are recurrently processed on a firewall that handles heavy network traffic.

IP protocol

Support reference 79787

Whenever the firewall received fragmented IP packets, an anomaly occurring when the packets are rewritten during the protocol analysis would cause the destination host to not receive the first fragment when the re-sent packet was smaller than the original packet. This issue has been fixed.

DNS protocol

Support reference 82274

"Possible DNS rebinding attack" (dns:154) alarms were wrongly raised during the protocol analysis of DNS traffic originating from Microsoft hosts. This issue has been fixed.

Support references 79494 - 80912

The DNS traffic protocol analysis engine was sensitive to the case used in DNS server responses and would raise the “DNS query mismatch” alarm (dns:151) whenever the case was different from the one used in the request. This reaction has been changed in order to be compatible with 1035, 8490 and 4343.

RDP protocol in COTP

Support reference 81814

When RDP packets are analyzed in COTP, going to Microsoft Windows servers and passing through a connection broker, the block alarms "COTP: invalid message length" (cotp:385) and "Invalid COTP protocol" (cotp:379) are no longer raised.

SIP

Support reference 82964

An anomaly in the SIP protocol analysis engine, which could cause the firewall to freeze, has been fixed.

Firewall administration

Support reference 78531

An anomaly during the initialization of the monitoring library would sometimes unexpectedly restart the firewall's administration service. As such, the response time for administration sessions via the web interface or the SSH console would become longer. This anomaly has been fixed and additional information has been provided in advanced logs (verbose mode).

Intrusion prevention engine

Support reference 81690

Whenever the intrusion prevention engine received certain interruption signals, it would stop writing additional logs (core files) making it possible to identify why the engine restarted. This issue has been fixed.

Reputation/location information queues

Whenever a host reputation request is submitted and the reputation/location information queue is full, the right alarm is now raised (“Possible attack on capacity”). Statistics indicating that the

queue is full are also correctly updated.

SMB/CIFS protocol

Support reference 83660

An anomaly was fixed after the SMB/CIFS protocol analysis engine factored in the padding bytes at the end of SMB packets.

Web administration interface

Quality of Service (QoS)

During the verification to determine the usage of a QoS queue, and when no valid object was found, the resulting information messages would have issues displaying special characters (e.g., apostrophes, accents, etc.) This issue has been fixed.

SSL filtering - URL filtering

Support references 80809 - 80813

Due to an anomaly in the system command used when the mouse is scrolled over URL category groups or certificate categories groups, the message “This object does not exist” would wrongly appear. This anomaly has been fixed.

Configuration

Support reference 82560

Administrators who held all privileges (other than the super-administrator admin account) could no longer access the **Configuration** panel in the web administration interface. This regression appeared in SNS version 4.2.1 and has since been fixed.

Configuration - NTP servers

Support reference 81719

The authentication keys associated with NTP servers can now be edited again. This regression appeared in SNS version 4.2.1.

IPsec - Local and global policies

Support reference 82376

It was no longer possible to rename an object in the local IPsec policy, then switch to the global IPsec policy and rename an object in it (and vice versa). This regression appeared in SNS version 4.2.1 and has since been fixed.

IPsec - Diffie-Hellman groups

When an IKE/IPsec profile is created, the Diffie-Hellman group suggested by default is now DH14 (the most secure) and no longer DH1.

IPsec - Check peer usage

In the **Configuration** module > **VPN > IPsec VPN**, **Peers** tab, the function that makes it possible to check the usage of a peer in the firewall configuration (by right-clicking on the peer in question)

now takes more factors into account in its verification.

IPsec VPN - Certificate-based authentication

Support reference 83287

When displaying the properties of an IPsec peer that uses certificate-based authentication, the CA that issued the selected certificate would not be displayed. This anomaly has been fixed and the Certificate field is shown as <CA>:<Certificate>.

Network objects

Support reference 79812

When a port range object is being created, simply changing the type of object to create to a port object would still result in a port range object being created. This issue has been fixed.

Support reference 80539

A window indicating that a network object had been modified would occasionally appear by mistake when the **Network objects** module was used. This issue has been fixed.

Firewall administration

Support reference 78529

In the **Administration** tab of the **Configuration** module, when a host allowed to access the firewall's administration pages was created directly, the host was correctly added to the object database, but would not automatically appear in the list of hosts allowed. This issue has been fixed.

Monitoring - IPsec VPN tunnels

In **Monitoring - IPsec VPN tunnels**, the link to the configuration of the policy associated with an IPsec tunnel (available by right-clicking on the tunnel), now takes into account the fact that the linked policy is global or local and redirects to the corresponding policy.

Network interfaces

Support reference 83039

Manual changes to the MAC address of a network interface are now saved in the display of the Interfaces module.

Certificates and PKI

Support reference 83828

In the details of a certificate, the "subject" field had been wrongly renamed "issuer" since version 4.0.1. This anomaly has been fixed.

Support reference 83709

Attempts to download an imported certificate or CRL issued by a sub-CA imported on the firewall would result in a failure and "Certification authority not found" system error message. This issue has been fixed.

Support reference 83570

Any attempt to verify the use of a certificate imported on the firewall would result in a failure and “No valid certificate found” system error message. This issue has been fixed.

Support reference 82474

When several identities issued by the same external CA were imported on the firewall, the CA’s tree would contain errors and the modules that made it possible to handle certificates (certificates and PKI, IPsec VPN, etc.) would display this CA as many times as the number of imported identities. This regression appeared in SNS version 4.1 and has since been fixed.

Firewalls with a TPM (SNi20, SN3100) - Enabling IPv6

Support reference 83578

When the TPM has been initialized on SNi20 or SN3100 firewalls, the TPM password is now required to enable IPv6 support, so that the configuration can be correctly backed up without triggering the “TPM operation error: unauthorized” system error message.

Proxies

Support reference 84079

A new certificate signing CA could not be chosen for the proxy when the new CA had the same password as the old CA. This regression appeared in SNS version 4.2 and has since been fixed.

Version 4.3.2 not published

Version 4.3.2 is not available to the public.

Version 4.3.1 not published

Version 4.3.1 is not available to the public.

Version 4.3.0 not published

Version 4.3.0 is not available to the public.

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 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** > **Report an incident / Follow up on an incident**.

- +33 (0) 9 69 329 129

In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu.

STORMSHIELD