STORMSHIELD

STORMSHIELD NETWORK SECURITY

RELEASE NOTES

Version 5

Document last updated: June 12, 2025

Reference: sns-en-release_notes-v5.0.1-Beta

Table of contents

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

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

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

Change log

Date	Description
June 11, 2025	New document

New firewall behavior

This section lists the changes made to the automatic behavior of the firewall when your SNS firewall in version 5.0.1 Beta is updated from the latest 4.8 version available.

If necessary, we also encourage you to read about the New firewall behavior in SNS version 4.8 introduced since the last available 4.3 LTSB version.

Changes introduced in version BETA 5.0.1

- SSL VPN - Attempts to update to version 5 SSL VPN configurations that use algorithms other than AES-128-GCM, AES-192-GCM, AES-256-GCM and ChaCha20-Poly1305, or with compression enabled, are denied.
- Attempts to update a firewall to version 5 are denied if the certificate used by the firewall has been signed with the obsolete SHA1 algorithm.
- A certificate is automatically generated the first time a firewall in SNS version 5 is started. It is used by default by the firewall's TLS-based authentication services (web administration interface and captive portal).
- Automatic backups - When the automatic backup module is configured to use a certificate that is signed with the obsolete SHA1 algorithm, the certificate will be rejected and the automatic backup will be suspended without sending data for security reasons. An error message prompts the administrator to generate a new customized certificate that is signed using a secure algorithm.
- Password policy - The password policy set on firewalls in factory configuration has been hardened. It now imposes a minimum length of 16 characters (previously 8), a mandatory combination of alphanumeric, uppercase, lowercase and special characters, and a minimum entropy of 64 (previously 20).
- Password encoding - UTF-8 is now the character set used by the firewall to encode passwords for firewalls in factory configuration. This prevents connection issues over SSH when the password contains non-ASCII characters (e.g., "€", accented characters, etc.).
- Several obsolete features have been removed from SNS version 5:
  - SNVM (Stormshield Network Vulnerability Manager),
  - PPTP (Point-to-Point Tunneling Protocol) VPN,
  - SSL VPN application portal (web application mode and Java applet).
- URL/SSL filtering - The embedded URL base has been removed.
  To continue applying URL/SSL filtering, you can:
  - Subscribe to the Extended Web Control option,
  - Continue using the built-in URL filtering engine, by combining it with a URL filter database provided by a third-party vendor, for example:
    - French URL database provided by the *Rectorat de Toulouse* (Academy of Toulouse), by following the method described in the Stormshield Knowledge Base (authentication required),
    - Polish URL database provided by Dagma, by following the instructions here: https://stormshield.pl/pomoc/baza-wiedzy/item/zmiana-klasyfikacji-url-na-rozszerzona-klasyfikacje-dedykowana-dla-polskiego-rynku.

- SNMP agent - Obsolete password encryption algorithms can no longer be selected in the SNMP v3 agent control panel. Only the AES-SHA2 (SHA256) algorithm is available by default. When a configuration using an algorithm other than SHA256 is migrated to SNS version 5, a message appears, stating that the algorithm used is obsolete. The algorithm can now be changed through the CLI/Serverd command `CONFIG SNMP USERV3`.

  More information on the command **`CONFIG SNMP USERV3`**.
- SNMP agent - SNMP tables with an index starting at 1 are now used by default, and older tables (index starting at 0) are tagged as obsolete. These older tables will be phased out in a future SNS version.
  When upgrading to SNS version 5 or higher from a firewall using the older tables, a warning appears, prompting the administrator to enable new SNMP tables by following the **procedure described in the SNS v5 user guide**.
- SNMP agent - A message indicates that SNMP version 1 is obsolete. This version will be phased out in a future SNS version.
- EVA - EVA virtual firewalls in factory configuration are now equipped with a 4 GB /data partition, compared to 2 GB in previous SNS versions. This change does not apply to EVAs that were installed in an earlier version and updated to SNS version 5.
- Explicit HTTP proxy - The explicit HTTP proxy is obsolete and will be phased out in a future SNS version.
- SSL VPN - Attempts to update to version 5 SSL VPN configurations that use algorithms other than AES-128-GCM, AES-192-GCM, AES-256-GCM and ChaCha20-Poly1305, or with compression enabled, are denied.
- SSL/TLS-based protocols - The MD4, MD5, RIPEMD-160 (rmd160), MD2 and MDC-2 hash functions, and the DES-EDE3-CBC encryption algorithm have been removed as they are obsolete.
- IPsec - The 3DES encryption algorithm is no longer available in SNS version 5. Since IPsec configurations using this algorithm will not be successfully updated to version 5, edit your IPsec configuration and replace 3DES with another algorithm before updating your firewall to SNS version 5.
- Internal LDAP directory - CRYPT, MD5, SMD5, SHA and SSHA hash functions have been removed as they are obsolete.
- Network captures - For security reasons, the permissions required to make network captures have been set to a more restrictive value.
- IPv6 - The "Land style attack" alarm (ip:21 alarm) is no longer triggered in IPv6, and no longer generates a log entry. This protection is now provided in the firewall operating system kernel.
- SSL VPN - Enabling the Data Channel Offload (DCO) option that uses the AES-256-GCM encryption suite for SSL VPN makes TheGreenBow VPN clients incompatible with the Stormshield SSL VPN feature.
- SSL VPN - After a firewall in factory configuration is updated to version 5, the Data Channel Offload (DCO) option is enabled by default when the SSL VPN service is used. If you plan to set up TCP-based SSL tunnels, we strongly recommend that you disable the DCO option, which is intended for UDP-based SSL tunnels, and severely downgrades performance for TCP-based SSL tunnels.
- Object groups - The maximum number of items that a group can contain is now limited to 3000 objects. While configurations containing groups of more than 3,000 items can be updated to version 5, objects can no longer be added to such groups after an update.

- Routing by interface - Routing by interface is no longer available in SNS version 5. The system will prevent v4 configurations that use this feature from being migrated to SNS version 5.
- Modems - ISDN modems (telephone modems connected by serial cable) are no longer supported on firewalls in SNS version 5.

New features and enhancements in SNS 5.0.1 Beta

Captive portal, SSL VPN and permission management with Microsoft Entra ID authentication

SNS version 5.0 introduces support for the OpenID Connect (OIDC) authorization protocol, to enable compatibility with Microsoft Entra ID SSO authentication.

This allows users to authenticate with their Microsoft Entra ID accounts, and depending on the permissions defined, allows them to be granted access to the firewall's captive portal, set up tunnels over Stormshield SSL VPN, or to be recognized in filter rules that require authentication.

IPsec VPN - Hybrid cryptography for post-quantum encryption

As of SNS version 5.0, hybrid cryptography can be used to protect against quantum attacks, by using hybrid algorithms that are standardized by NIST in the Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM).

You can use algorithms that are resistant to post-quantum attacks, in addition to the usual algorithm, to protect the key exchange from quantum attacks. Do note that symmetric cryptography is not vulnerable to such attacks.

The following algorithms are supported in SNS version 5.0:

- ML-KEM-512,
- ML-KEM-768,
- ML-KEM-1024.

Two encryption profiles that use these hybrid algorithms are now offered in the **Encryption profiles** tab of the IPsec VPN module:

- PQCEncryption: for configurations with peers that exclusively use post-quantum encryption standards,
- PQCTransition: for configurations that are transitioning to post-quantum encryption standards.

SSL VPN - Performance

The SSL VPN service now includes the Data Channel Offload (DCO) module: when DCO is enabled, encryption/decryption operations on data packets passing through SSL VPN tunnels are processed in the operating system kernel, instead of the firewall's SSL VPN service. This improves performance, and enables the SSL VPN service to process the setup of many more SSL VPN tunnels.

Do note that DCO:

- Is compatible only with UDP-based SSL VPN tunnels,
- Is not enabled by default when an existing configuration is migrated,
- Requires the selection of the AES-GCM encryption suite.

IPsec VPN - DR transition mode

In *Diffusion Restreinte* (DR) mode, which was introduced in SNS version 4.2, policies that comply with IPsec DR specifications set by the ANSSI are not allowed to coexist with policies that comply with the IPsec standard (RFC 7292 IKEv2bis).

In SNS version 5.0, IPsec VPN tunnels that behave like tunnels in DR mode can be configured, while retaining the possibility of setting up IPsec VPN tunnels that comply with the standard. This feature, known as "DR transition mode", applies to complex architectures in which the process of making them DR-compliant has to go through a transitional phase, during which IPsec DR and standard (non-DR) policies are made to coexist.

For more information on DR transition mode, refer to the technical note **Transition DR Mode: gradually make IPsec architecture compatible with DR mode**.

Increased security

Hardening of the system

As part of the process of hardening the SNS operating system, privilege management has been strengthened for maintenance operations, firewall updates, and the use of certain services (SNMP agent, e-mail sending, etc.).

Certificates signed with SHA1

As of SNS version 5.0, certificates that have been signed with SHA1 are no longer supported, and can no longer be used in the various modules that allow the use of certificates (SSL VPN, telemetry, automatic backups, etc.).

Verifying the activation of Secure Boot

The web administration interface displays a warning message when Secure Boot is not enabled on the firewall. Do note that Secure Boot imposes constraints once it is enabled: to assess these constraints and follow the procedure to enable Secure Boot, refer to the technical note Managing Secure Boot in firewalls' UEFI.

Password policy

The password policy now allows a combination of upper/lower case alphanumeric characters, and special characters to be used. This option is selected by default on firewalls in factory configuration,

Integration into various environments

SD-WAN

Monitoring of available SD-WAN gateways has been improved to be better equipped to factor in specific cases of network failures in environments with multiple WAN access authorizations.

For further information on configuring SD-WAN, refer to the Technical note SD-WAN - Selecting the best the network link.

Changes to performance

Overall performance

SNS version 5 improves the overall performance of Stormshield firewalls.

For more information on firewall performance, refer to the product datasheets that can be found on the Stormshield corporate website.

Proxy

Proxy performance has been enhanced, allowing up to 25% additional throughput.

Asynchronous reloading of filter rules

Filter policies can now be reloaded asynchronously to minimize the impact on network traffic: filter rules are not immediately reassessed, but when they are used.

This mechanism is particularly useful in configurations that contain a significant number of rules and concurrent connections.

This feature is not enabled by default, and must be enabled through the following CLI/Serverd command sequence:

```
CONFIG SECURITYINSPECTION COMMON STATEFUL AsyncReload=1
CONFIG SECURITYINSPECTION ACTIVATE
```

For more information on asynchronous reloading of filter rules, refer to the technical note **Asynchronous reloading of filter rules**.

Improved user experience

Web administration interface

The firewall's web administration interface now makes it possible to simultaneously open a configuration tab and a monitoring tab in the same browser. This makes it easier to check whether the configuration has been correctly applied.

This can be done by clicking on the icon in the **Configuration** and **Monitoring** tab headers.

The SNS theme and user interface have been redesigned for smoother browsing.

TPM

TPM processing traffic has been improved, by removing the need to seal the secrets stored in the TPM with the system's new technical characteristics when changes are made to the firewall's UEFI.

IPsec tunnel monitoring

A search bar is now available in the IPsec VPN monitoring module.

Real-time logs

The **Real-time logs** module makes it possible to view the latest logs stored in memory on firewalls that are not equipped with SD cards.

HTTP protocol

The value of the configuration tokens *AuthorizationBearerBuffer* and *AuthorizationNegotiateBuffer* can now be configured in the HTTP protocol analysis configuration module.

Sending e-mails

The e-mail system has been hardened for enhanced security, and message templates can now be customized in the web administration interface, through the use of variables for each template.

Telemetry

New data reported by the telemetry service

The telemetry service in SNS version 5.0 now reports new data:

- SSD status data:
  - Number of blocks removed from SSD use due to programming or erasing failure,
  - Number of hours SSD has been powered up,
  - Average number of block erasures (number of times the SSD has been completely written),
  - Percentage of remaining lifetime,
  - SSD wear indicator (0 - 100%),
  - Total number of 512 byte sectors written throughout the lifetime of the SSD,
  - Total number of 512 byte sectors read throughout the lifetime of the SSD.
- Data regarding the filter policy:
  - Number of times the filter policy was reloaded since firewall startup,
  - Status of asynchronous filter rule reloading mode.
- Data regarding IPsec tunnels:
  - Number of mobile tunnels configured with a Key-Encapsulation Mechanism (KEM) using an algorithm that is resistant to post-quantum attacks,
  - Number of mobile tunnels set up with a KEM using an algorithm that is resistant to post-quantum attacks,
  - Number of site-to-site tunnels configured with a KEM using an algorithm that is resistant to post-quantum attacks,
  - Number of site-to-site tunnels set up with a KEM using an algorithm that is resistant to post-quantum attacks.

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

Miscellaneous

- Operating system: SNS version 5 is based on FreeBSD 14.
- Intrusion prevention: NPDU and BVLL services are now supported by the BacNet/IP protocol analysis engine.
- The Energy Efficient Ethernet (EEE) feature, associated with 2.5 Gbit/s Ethernet network cards, is now supported.

- The sysObjectID OID (1.3.6.1.2.1.1.2) can now be used to retrieve the firewall model through an SNMP request.

SNS version 5.0.1 Beta bug fixes

System

Syslog - SD-WAN

A parameter has been added to each syslog profile set on the firewall to manage the duration before log sending resumes.

In a configuration that uses SD-WAN and router objects, following a network failure and a switchover to a backup gateway, this parameter makes it possible to set, for each profile, the duration after which the firewall will attempt to send logs to the syslog server again. This will limit the amount of logs that may be lost.

Previously set at 60 seconds, this duration can be adjusted to anywhere between 5 and 600 seconds.

Reports

Support references 85380 - 82777

Enhancements have been made to limit the size of the report database, to prevent it from mistakenly filling up its partition.

Support reference 84256

In configurations that manage host reputation, the CLI/Serverd command `REPORT RESET report=all` now purges the entire report database as expected.

More information on the `REPORT RESET` command.

IPsec VPN

Support reference 85641

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

Support reference 84803

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

Virtual IPsec interfaces (VTI)

Support reference 85770

When the `ennetwork -f` command is run on a configuration containing a tunnel that is based on virtual IPsec interfaces, the IPsec tunnel will no longer be wrongly shut down.

Certificates and PKI

Support reference 85948

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

More information on the `PKI SCEP QUERY` command.

Network card drivers

The default values of some queues that are defined for each network card driver have been increased. This prevents minor packet loss, even though the firewall's CPU load is relatively low.

Filter - NAT

Support references 80798 - 85537

Users now need to double-click on the comment of an unselected NAT or filter rule to edit the comment. In earlier SNS versions, clicking on the comment of an unselected NAT or filter rule would open and close the comment editor almost immediately.

Configuration - Check usage

When a user/user group is found in several LDAP directories listed on the firewall, using the **Check usage** function now only returns results relating to the directory in question.

Configuration - SSH access

Support reference 85101

The use of the "<" and ">" characters between quotes in CLI/Serverd commands that are run in console mode on the firewall over an SSH connection is now correctly interpreted, and no longer causes the "Error in format" error message to appear.

Automatic backups

When the automatic backup module is configured to use a certificate that is signed with the SHA1 algorithm, this certificate is rejected, and a warning message prompts the administrator to generate a new custom certificate that has been signed with secure algorithms.

High availability - Switch optimisation

Support reference 85773

Now, when **Reboot all bridged interfaces** is selected, only bridged interfaces will restart.

LDAPS server

Support reference 85766

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

URL filtering - Extended Web Control (EWC)

Support references 85849 - 86059

The EWC URL filtering service is operational once again, after updating the IP address of the ewc-sns.stormshieldcs.eu server in the service configuration.

CLI/serverd commands

Filter - NAT

Support reference 85566

The documentation and integrated help for the CLI/Serverd command `CONFIG FILTER RULE UPDATE` have been corrected: the *srcport* parameter can represent only a single port or port range, and not a list of ports, as was previously indicated.

More information on the command `CONFIG FILTER RULE UPDATE`.

Virtual machines

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

Support reference 85730

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

Intrusion prevention engine

BIRD dynamic routing

Support reference 84579

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

SIP protocol

The default value for the **Action**/**Level** parameters associated with the sensitive "Anonymous address in SDP connection" alarm (sip:465 alarm) is now **Block**/**Major**. This value was previously set to **Pass**/**Minor** by mistake.

Stealth mode disabled - IPv6 analysis

Support reference 85327

Firewalls on which stealth mode has been disabled no longer crash unexpectedly when IPv6 packets are scanned.

sfctl system commands

Support reference 85757

The analysis of arguments passed to sfctl system commands no longer stops after the first alphabetical character. This behavior could trigger a command that does not match the requested command, but which is similar to it up to the first alphabetical character.

Hardware

Energy Efficient Ethernet (EEE)

EEE can now be enabled on compatible network cards. These cards have the **Enable IEEE 802.3az (EEE)** checkbox in their advanced configuration.

Web administration interface

Administrators - *admin* account

When the private or public key of the super-administrator account (*admin* account) is exported, the result is now a file in text format. This file was previously in csv format.

Protocols - Filtering in the Sandboxing tab

The filtering feature in the Sandboxing tab for HTTP/SMTP/POP3 and IMAP protocols, and in the SSL protocol's certification authority grid, is now operational once again. This regression appeared in SNS version 4.8.0.

Interfaces - Media type

5 Gbit/s has been added to the list of media as a value that can be selected for a network interface.

Compatibility

For more information, see the **Product life cycle guide**.

Limitations and explanations on usage

QoS

The following limitations have been placed on the QoS implemented:

- Maximum bandwidth supported: 1 Gbps,
- Interfaces supported:
  - Ethernet,
  - IPsec,
  - GRETAP,
  - Virtual IPsec (VTI),
  - VLAN.
- Priority Queuing (PRIQ) and Class-Based Queuing (CBQ) are not compatible with one another, and must not be used on the same traffic shaper,
- All thresholds set on queues must be expressed either in absolute values only or percentages only.
- The amount of reserved bandwidth must not exceed the bandwidth assigned to the traffic shaper.

Authentication - TOTP

Support reference 84686

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

Dynamic multicast routing

Dynamic multicast routing implemented in version 5 has the following limitations:

- IGMPv1 is not supported,
- IGMP Snooping is not supported,
- PIM Dense Mode is not supported,
- PIM Sparse-Dense Mode is not supported,
- PIM BiDir is not supported,
- Multicast BGP Extension is not supported,
- MSDP (Multicast Source Discovery Protocol) is not supported,
- AnycastRP is not supported,
- IPv6 and the MLD (Multicast Listener Discovery) protocol are not supported,
- Static multicast routing and dynamic multicast routing cannot be enabled at the same time,
- Dynamic multicast routing tables are not synchronized in HA,

- Bridges and bridged interfaces cannot be selected as interfaces participating in dynamic multicast routing,
- The Cisco AutoRP protocol is not supported,
- SNS firewalls may be included in a Cisco AutoRP infrastructure when Cisco devices are configured to support BSR standards,
- In HA configurations, interfaces that participate in dynamic multicast routing must have a static IP address,
- The intrusion prevention engine does not analyze the PIM protocol,
- The number of interfaces on the firewall that participates in dynamic multicast routing is restricted to 31,
- Source address translation is not supported.

Web services

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

PROFINET RT protocol

Support reference 70045

The network controller used on the following firewall models has been upgraded and allows VLANs with an ID value of 0:

- SN-S-Series-220,
- SN-S-Series-320,
- SN510,
- SN-M-Series-520,
- SN710,
- SN910,
- SN1100,
- SN2100,
- SN3100,
- SN6100,
- SNi40,
- SN-M-Series-720, SN-M-Series-920, SN-L-Series-2200, SN-L-Series-3200, SN-XL-Series-5200 and SN-XL-Series-6200 models equipped with an additional network module.

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.

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/Serverd 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.

Network

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

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

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

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

Bird dynamic routing

In configurations that use BGP with authentication, the "source address <ip>;" directive must be used. For further information on Bird configuration, refer to the Bird v2 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 and version 5, 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 changes to a security policy that is embedded in 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 5.0.1 cannot be restored if the firewall's current version is 4.8.9.

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 v4 to SNS v5, 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 5, 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 tunnels,

- Kerberos authentication,
- 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, mainly 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 more information, refer to the section on Authentication in the SNS user guide.

Users

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

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

Logging out

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

Temporary accounts

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

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

Radius

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

1000Base-LX media

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

Documentation resources

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

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

Installing this version

To update your firewall to SNS version 5.0.1 Beta, we recommend that you carefully follow the procedure below.

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

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

Checking the compatibility of Stormshield Network client applications

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

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

Creating a configuration backup

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

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

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

Updating a high availability firewall cluster

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

Updating the firewall

Update paths

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

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

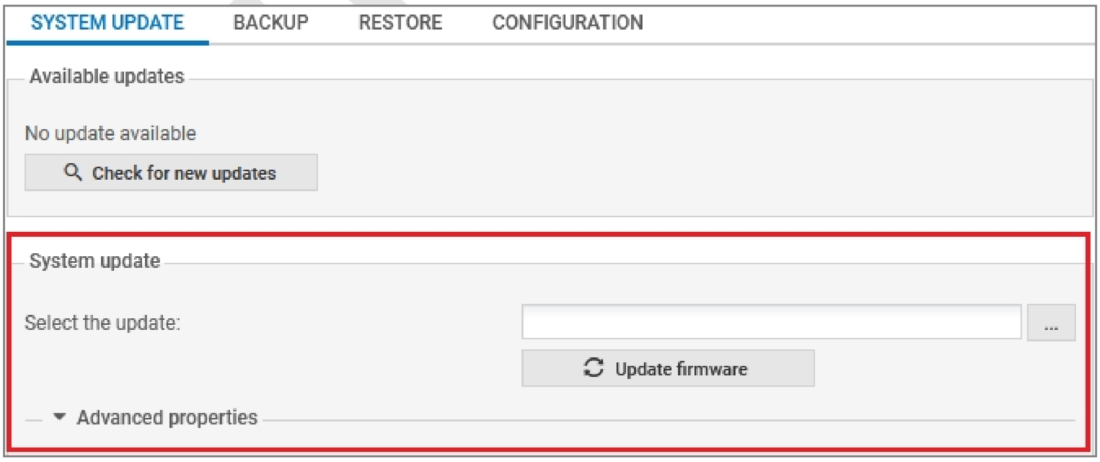
Downloading the update

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

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

Installing the update

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



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

Contact

To contact our Technical Assistance Center (TAC) Stormshield:

- https://mystormshield.eu/

All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under **Technical support** > **Manage cases**.

- +33 (0) 9 69 329 129

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

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