STORMSHIELD

STORMSHIELD NETWORK SECURITY

RELEASE NOTES

Version 4

Document last update: September 3, 2021

Reference: sns-en-release_notes-v4.2.4

Table of contents

Compatibility

Lowest version required

Intermediate updates may be necessary to upgrade firewalls in version 4.2.4.

- From a 2.X version: simply update the firewall beforehand to version 3.7.16 LTSB, then version 3.7.18 LTSB,
- From a 3.X version: simply update the firewall beforehand to version 3.7.18 LTSB, then version 3.11.6 LTSB,
- From a 4.X version: simply update the firewall beforehand to version 4.1.1 or 4.1.2.

Hardware compatibility

SN160(W), SN210(W), SN310, SN510, SN710, SN910, SN1100, SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100
SNi20 and SNi40
Stormshield Network Elastic Virtual Appliances: EVA1, EVA2, EVA3, EVA4, EVAU and VPAYG

Hypervisors

VMware ESXi	Versions 6.5 and 6.7
Citrix Xen Server	Version 7.6
Linux KVM	Red Hat Enterprise Linux 7.4
Microsoft Hyper-V	Windows Server 2012 R2 and 2019

Authentication - Microsoft servers

RADIUS Kerberos Microsoft Active Directory - LDAP(S)	Windows Server 2012 R2 and 2019
SPNEGO	Windows Server 2012 R2, 2016 and 2019

StormshieldNetwork client software

Windows SSO Agent	Version 3.0.1
Linux SSO Agent	Version 3.0.1
SSL VPN client	Version 2.9.1
IPSec VPN Client	Version 6.64.003

SN Real-Time Monitor

SN Real-Time Monitor version 4.0.0 is not compatible with firewalls in version 4.2.1, 4.2.2 and 4.2.4. A specific version of SN Real-Time Monitor compatible with SNS firewalls in version 4.2 will be released later.

Web browsers

In order for the firewall administration interface to operate optimally, you are advised to use the latest versions of Microsoft Edge, Google Chrome and Mozilla Firefox (ESR version - Extended Support Release). For further information on these versions, please refer to the relevant vendors for the life cycles of their products.

Changes to firewall behavior

This section sets out the changes to automatic behavior when SNS firewalls are upgraded to version 4.2.4 from a 3.11.8 LTSB version or higher.

Changes introduced in version 4.2.4

Find out more

- Hardening of operating system - Only shell scripts are allowed, but they must be explicitly called by the interpreter, e.g., sh script.sh instead of ./script.sh.
- Hardening of operating system - For scripts run from the event scheduler (*eventd*), the interpreter must be added for each task described in the configuration file of the event scheduler.
- Hardening of 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 are displayed in the **Messages** widget on the dashboard when the IPSec DR mode is enabled.
- IPSec DR mode - Fixing an anomaly in the implementation of ECDSA based on Brainpool 256 elliptic curves 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.
- Active Update - For clients that use internal mirror sites, Active Update packets hosted on your own servers must be updated so that packets signed by the new certification authority are used.
- Stormshield Management Center agent - On SNS firewalls managed via SMC, 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 storage of all log types on disk, including connections, 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 - The ESN to prevent ESP 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.

- 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.
- 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 - 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.
- 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 in v2.9.1 or higher must be used 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 protocol v1.3 - TLS v1.3 is used for services on the firewall (captive portal, LDAPS, Syslog TLS, Autoupdate, etc.).

Changes introduced in version 4.1.6

Find out more

- After signature certificates are updated, the USB Recovery procedure must be used to install versions lower than 4.1.6 on firewalls 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 the 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 was already possible 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.
- 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.
- Configuration of protected mode - A new setting, stealth mode, gives the firewall the possibility of responding to ICMP requests. This new setting has 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

- 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.

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 names of interfaces has changed for SN160 and SN210(W) firewall models. 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.
- Updates will reinitialize preferences in the web administration interface (e.g.: customized 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 graphical interface has been fully reworked to improve user comfort. It is now easier to switch between **configuration** and **monitoring** modules.

New features in version 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, 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 version 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.

Version 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).

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.

Explanations on usage

PROFINET RT protocol

IX network modules (fiber 2x10Gbps and 4x10Gbps equipped with INTEL 82599 micro-component) and IXL modules (see the list of affected modules) are not equipped with the update that allows PROFINET-RT to be managed.

IPSec VPN

Optimized distribution of encryption/decryption operations

In a configuration with a single IPSec tunnel that several streams of traffic pass through, enabling the mechanism that optimizes encryption and decryption operations could disrupt the sequence of packets and potentially make the recipient reject encrypted packets based on the anti-replay window size 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 restrictions

There are several restrictions 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".

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.

Keepalive IPv6

For site-to-site IPSec tunnels, the additional keepalive option that allows artificially keeping these tunnels up cannot be used with traffic endpoints with IPv6 addresses. In cases where traffic endpoints are dual stack (both IPv4 and IPv6 addresses are used), only IPv4 traffic will benefit from his feature.

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.

A backup configuration cannot be defined for IPSec peers using IKEv2. In order to implement a redundant IKEv2 IPSec configuration, you are advised to use virtual IPSec interfaces and router objects in filter rules (PBR).

SN Real-Time Monitor

SN Real-Time Monitor version 4.0.0 is not compatible with firewalls in version 4.2.1, 4.2.2 and 4.2.4. A specific version of SN Real-Time Monitor compatible with SNS firewalls in version 4.2 will be released later.

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.

4G modems

Support reference 57403

In order to ensure a firewall's connectivity with a 4G USB modem, HUAWEI equipment that supports the HiLink function must be used (e.g.: E8372H-153).

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 graphical 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

With the Bird dynamic routing engine in version 1.6.8, in configurations that use BGP with authentication, the "*setkey no*" option 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

Preferences in the web administration interface

Upgrading to a major firmware release will cause the reinitialization of preferences in the web administration interface (e.g.: customized filters).

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 list of objects 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.

Kaspersky antivirus

The option **Activate heuristic analysis** is not supported on SN160(W), SN210(W) and SN310 firewall models.

Link aggregation (LACP)

Support reference 76432

Link aggregation (LACP) is not compatible with the 40G SFP+ LM4 network module (reference NA-TRANS-QSFP40-SR).

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. Clusters in which one firewall uses 32-bit firmware and the other uses 64-bit firmware are also not allowed.

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,
- Radius or 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.

Instant messaging
NAT is not supported on instant messaging protocols

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).

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).

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`.

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.

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 IPSec Phase 1 negotiation is incompatible with multiple Microsoft Active Directories for the authentication of mobile clients.

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

Multiple directories

Users that have been defined as administrators on the firewall must originate from the default directory.

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 can only log out of a session with 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).

Stormshield Network administration suite

Support reference 28665

The command CLI MONITOR FLUSH SA ALL was initially meant to disable ongoing IPSec tunnels by deleting their SAs (security associations). However, as Bird dynamic routing also uses this type of security association (SA), this command would degrade the Bird configuration, preventing any connections from being set up.

The Bird service must be restarted in order to resolve this issue.

Documentation resources

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

Guides

- Stormshield Network Firewall - User and configuration manual
- Elastic Virtual Appliances - Installation guide
- CLI Serverd - Commands reference guide
- CLI Console / SSH - Commands reference guide
- Stormshield Network Pay As You Go - Deployment guide

Technical notes

Authentication

- SSO configuration: Microsoft SPNEGO
- Configuring "guest" methods
- Stormshield Network SSO Agent for Windows
- Stormshield Network SSO Agent for Linux

Configuration

- Automatic backups
- Basic configuration in command line interface (CLI)
- Complying with regulations on personal data
- Configuring a 3G/4G modem on SNS
- Custom contextual protection signatures
- Filtering HTTPS connections
- Stacking: distribution of traffic among several firewalls
- High availability on SNS
- Identifying industrial protocol commands going through the firewall
- Implementing a filter rule
- Initial configuration via USB key
- Adapting the SES security policy of a workstation to its SNS reputation
- Collaborative security

Hardware

- Secure Return option
- Software Restoration via USB key
- Updating IPMI firmware
- Exchanging a power supply module

Logs

- Description of audit logs

Routing

- BIRD dynamic routing

SNS for Cloud

- EVA on Amazon Web Services
- EVA on Microsoft Azure
- VMWare NSX - SNS firewall as a peripheral router

VPN

- IPSec virtual interfaces
- Integrating NAT into IPSec
- SSL VPN tunnels
- IKEv1 Mobile IPSec VPN - Authentication by pre-shared key
- IKEv2 Mobile IPSec VPN - Authentication by pre-shared key
- IPSec VPN: Authentication by pre-shared key
- IPSec VPN: Certificate-based authentication
- IPSec VPN: Hub and spoke configuration

Videos

- CLI commands and scripts, available on Institute.

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

Downloading this version

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 4.2.4 version of Stormshield Network Security:

1. Log in to MyStormshield with your personal identifiers.
2. In the left panel, select **Downloads**.
3. In the right panel, select the relevant product and version.

Checking the integrity of the binary files

To check the integrity of Stormshield Network Security binary files:

1. Enter one of the following commands and replace `filename` by the name of the file you want to check:
   - Linux operating system: `sha256sum filename`
   - Windows operating system: `CertUtil -hashfile filename SHA256`
2. Compare with hashes provided on MyStormshield personal area, section **Downloads**.

Previous versions of Stormshield Network Security 4

In this section, you will find new features, resolved vulnerabilities and fixes from previous versions of Stormshield Network Security 4.

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

Version 4.2.3 not published

Version 4.2.3 is not available to the public.

Resolved vulnerabilities in version 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

A moderate severity vulnerability was fixed in ClamAV.

Details on this vulnerability can be found on our website 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.

Version 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 version 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).

All SNS MIBs can be downloaded from the MIBS section on Stormshield's official website.

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 version 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.

Version 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 version 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 version 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.

A vulnerability with an overall CVSS score of 5.3 was fixed in ClamAV.

Details on this vulnerability can be found on our website 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.

Version 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”.

Version 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.

Version 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 version 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 version 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.

Version 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.

Version 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 version 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 version 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.

Version 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 version 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 version 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.

Version 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 version 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 version 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.

Version 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 version 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 version 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.

Version 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

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