STORMSHIELD

STORMSHIELD NETWORK SECURITY

RELEASE NOTES

Version 3.11 LTSB

Document last updated: July 21, 2022

Reference: sns-en-release_notes-v3.11.18-LTSB

Table of contents

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

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

LTSB (Long-Term Support Branch) label

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

Compatibility

Update paths

Before updating a firewall to version 3.11.18 LTSB, some intermediate updates may be required, depending on the source version:

From a 2.X version	Update to version 3.11.4 LTSB
From a V / VS-VU firewall	See Migrating a V / VS-VU model virtual firewall to an EVA model

Hardware compatibility

SN160(W), SN210(W), SN310, SN510, SN710, SN910, 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, 6.7 and 7.0
Citrix Xen Server	Version 7.6
Linux KVM	Red Hat Enterprise Linux 7.9
Microsoft Hyper-V	Windows Server 2012 R2 and 2019

Authentication - Microsoft servers

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

StormshieldNetwork client software

Windows SSO Agent	Version 2.1.1
Linux SSO Agent	Version 2.1.1
SSL VPN client	Version 3.1.0
VPN Client Standard	Version 6.87.108
VPN Client Exclusive	Version 7.00.115

Operating systems for SN Real-Time Monitor

Microsoft Windows	Version 10
Microsoft Windows Server	Versions 2012 R2, 2016 and 2022

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.

Public Cloud

Amazon Web Services
Microsoft Azure
3DS OUTSCALE

New features and enhancements in version 3.11.18

System

Synchronization of the object database with DNS servers

Support reference 66537

The automatic synchronization of the object database with DNS servers configured on the SNS firewall can now be enabled/disabled or modified in terms of synchronization frequency.

These operations can only be performed using the following CLI/serverd commands:

- `CONFIG OBJECT SYNC STATE=<0|1>` to disable/enable synchronization respectively,
- `CONFIG OBJECT SYNC UPDATE period=<period>` to change how frequently updates will be launched, between one minute and one day inclusive (e.g., *period=6h5m4s*).

These changes must be confirmed with the command `CONFIG OBJECT SYNC ACTIVATE` to be applied.

Find out more

Intrusion prevention

Multicast IP addresses presented as source addresses

Support reference 84041

A new alarm "Multicast IP src packet" (alarm ip:755), which makes it possible to block by default packets that present a multicast address as a source address, has been added to the intrusion prevention engine.

Resolved vulnerabilities in version 3.11.18 LTSB

Intrusion prevention engine

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

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-009.

ClamAV antivirus

A moderate severity vulnerability was fixed in ClamAV.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-017.

Version 3.11.18 LTSB bug fixes

System

High availability (HA) - Synchronization

Support reference 83721

Anomalies that may cause excessive memory consumption have been fixed in the mechanism that synchronizes the high availability configuration.

Hosts with dynamic IP address resolution used in sub-groups

Support references 84202 - 81951

Whenever a host was:

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

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

Intrusion prevention

TNS protocol - Oracle

Support reference 84341

Analyses of TNS - Oracle client-server communications that undergo packet fragmentation and address translation (NAT) no longer desynchronize traffic due to packets being rewritten.

Recommendations

Before you migrate an existing configuration to version 3 of the firmware, ensure that you have:

- Read the **Release notes of all intermediate versions**,
- Carefully read the section **Known issues** in the Stormshield Knowledge base (use the same login credentials as those for your MyStormshield client area),
- Read the section Explanations on usage carefully,
- **Backed up** the main partition on the backup partition and backed up the configuration.

IMPORTANT

Updating a firewall from a SNS 3.7 LTSB version to a 3.11 LTSB version introduces several technical changes implemented between these two version branches, which may modify the behavior of the updated firewall. Some of these technical changes include:

- **SNS 3.8.0 - Network**: the stricter use of promiscuous mode may cause behavior to change in some configurations (Ethernet interfaces with at least one VLAN on which the MAC address has been forced, disabled Ethernet interfaces with one or several VLANs, Ethernet interfaces with one or several VLANs in a bridge, HA interfaces with one or several VLANs).
  Find out more
- **SNS 3.8.0 - SSL VPN**: as some authentication algorithms are no longer supported for SSL VPN, the configuration of SSL VPN. clients must be edited accordingly.
  Find out more
- **SNS 3.8.0 - IPsec VPN and CRL**: when the *CRLRequired* parameter is enabled in the configuration of a VPN policy, the user must now possess all the CRLs in the certification chain.
- **SNS 3.10.1 - SSL VPN and certificates**: in SSL VPN configurations that use certificates without the *KeyUsage* field, some external services may no longer be able to communicate with the firewall.
  Find out more
- **SNS 3.10.1 - Increased security during firmware updates**: to ensure higher security during firmware updates, *Autoupdate* servers can now only be reached in HTTPS. If an updated firewall contains a specific rule to access this service, this rule must be edited so that it can continue to allow such traffic.
  Find out more
- **SNS 3.10.1 - System**: when time zones are automatically refreshed to observe and end daylight saving time, some time-sensitive authentication processes may stop functioning.
  Find out more

IMPORTANT

Firewalls must not be upgraded from SNS in version 3.10 or 3.11 LTSB to a 4.0 version. This operation is not supported. Some features that are available in SNS versions 3.10 and 3.11 LTSB are only included from SNS version 4.1.1 upwards.

High availability and IPsec VPN (IKEv2)

In version 3.7.x, established IPsec tunnels would occasionally be renegotiated in clustered IPsec VPN configurations when the passive firewall was upgraded to version 3.9.x or higher.

MAC address management

MAC address management has been changed in version 3.8.0 in order to fix issues encountered when certain advanced interface configurations are applied.

As such, Stormshield now applies stricter use of *promiscuous* mode.

These changes may affect the behavior of the following configurations:

- Ethernet interface with at least one VLAN on which the MAC address has been forced [1],
- Disabled Ethernet interface with one or several VLAN(s),
- Ethernet interface with one or several VLANs included in a bridge,
- HA interface with one or several VLANs.

[1] High availability forces MAC addresses on one of the members of the cluster.

If any of these configurations concern you, check that all your network devices reference your firewall's real MAC address.

For further information, please refer to this article in the Stormshield Knowledge Base.

SSL protocol

From version 3.7.0 of the firmware onwards, encryption suites with a weak level of security (suites based on MD5, SHA1 and DES) are no longer available for the SSL protocol that the various firewall components (SSL VPN, SSL proxy, etc.) use.

For configurations that use these encryption suites, algorithms with a higher level of security must be chosen in order to migrate the firewall to an SNS 3.7.0 version or higher. Otherwise, the affected services will not run or will refuse to start.

IPsec VPN

Support reference 66421

Before upgrading the firewall to version 3, check your IPsec VPN configuration:

In the menu **Configuration > VPN > IPsec VPN** > *Identification* tab, check that the email addresses indicated in **Mobile tunnels: Pre-shared keys** are valid, or correct them if necessary.

If an address contains an error (e.g., *product@stormshield* or *product@stormshield.e*), the IPsec policy will fail to activate, returning the error message `Failed to parse PSK list from slotfile`.

EVA (Elastic Virtual Appliances)

You are advised to set the memory of EVAs to at least 2 GB if you use the antivirus and sandboxing features frequently.

Extended Web Control

If synchronous mode has been enabled on the Extended Web Control URL filtering solution (X-CloudURL_Async=0 parameter in the [Config] section of the configuration file ConfigFiles/proxy), it must be disabled before upgrading the firewall to v3. To do so, delete the line containing the *X-CloudURL_Async* parameter.

Updating a cluster with several high availability links

For clusters that implement more than one link dedicated to high availability, ensure that the main link is active before proceeding to upgrade to version 3.

SSO agent authentication method

In configurations using the **SSO Agent** authentication method, the SN SSO Agent must be migrated to a version equal to or higher than 1.4 before migrating the firewall's version.

The "Domain name" field must also be entered in the configuration of the SN SSO Agent BEFORE MIGRATING THE FIREWALL. This domain name must match the actual name of the domain (e.g.: stormshield.eu) so that the SN SSO Agent can run.

Policy-based routing

If the firewall has been reset to its factory settings (*defaultconfig*) after a migration from a 1 version to a 2 version then to a 3 version, the order in which routing will be evaluated will be changed 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).

Filter policies and users

In previous versions of the firmware, the filter policy did not distinguish between users and groups. In version 3, support for multiple directories requires strict checks on users. Migrating a configuration to version 3 of the firmware may therefore generate warnings asking the administrator to re-enter users in the filter policy in order to avoid any ambiguity.

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

Network

4G modems

To ensure the firewall's connectivity with a 4G USB modem, HUAWEI equipment from the following list must be used:

- E3372h-153,
- E8372h-153.

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

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.

In order for RSTP and MSTP to function, the interfaces on which they are applied must have an Ethernet layer. As a result:

- MSTP does not support PPTP/PPPoE modems,
- RSTP supports neither VLANs nor 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 (VLANs, PPTP interfaces, aggregated interfaces [LACP], etc.) are now 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

Since the Bird dynamic routing engine has been upgraded to version 1.6, the "*setkey no*" option must be used in configurations that implement BGP with authentication. 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, a warning message

indicating the row numbers containing errors will inform the user of the need to correct the configuration.

However, if a configuration containing errors is sent to the firewall, it will be applied the next time the Bird service or the firewall is restarted.

System

Support reference 80692

Access to configuration modules

After a firewall is updated, some configuration modules may become inaccessible and an error would occur if major changes were made to the display preferences of modules (e.g. displayed columns or their order) or if a display preference no longer exists in the new version.

To restore access to the configuration modules in question, the default settings of the user preferences must be restored in the **Preferences** module.

Find out more

Support reference 78677

Cookies generated for multi-user authentication

After a new security policy is implemented on mainstream web browsers, multi-user authentication SNSno longer functions when users visit unsecured websites via HTTP.

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

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

Find out more

Support reference 51251

DHCP server

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

Migration

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

Updates to a lower version

Firewalls sold with version 3 firmware are not compatible with older major versions.

Backtracking to a major firmware version older than the firewall's current version would require a prior reset of the firewall to its factory settings (*defaultconfig*). For example, this operation would be necessary in order to migrate a firewall from a 3.0.1 version to a 2.x version.

Support reference 3120

Configuration

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

Restoring backups

Configurations that are backed up on a firewall with a system version higher than the current version cannot be restored. For example, a configuration backed up in 3.0.0 cannot be restored if the firewall's current version is 2.5.1.

Dynamic objects

Network objects with automatic (dynamic) DNS resolution, 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.

Quality of Service

Network traffic to which Quality of Service (QoS) queues have been applied will not fully benefit from enhancements made to the performance of the "fastpath" mode.

Advanced 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).

IPsec VPN

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 3.11.1 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.

Obsolete use of backup peers

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 encourage administrators to modify their configurations.
For this configuration, use virtual IPsec interfaces instead, with router objects or dynamic routing.

IPsec - Mixed IKEv1/IKEv2 policy

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.

Decryption

The IPsec peer distributes data decryption. On multi-processor firewalls, this process is therefore optimized whenever the number of peers is at least equal to the number of the appliance's processors.

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.

PKI

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

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 to authenticate IPsec peers that use 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).

Mobile policy

In mobile IPsec policies containing several peers and using certificate authentication:

- Peers must use the same IKE encryption profile,
- The certificates of the various peers must be issued by the same CA,

Certificates and PKI

SCEP

The SCEP implementation on SNS firewalls has the following characteristics and limitations:

- The **SCEP CertPoll** message, meant to simplify polling requests by sending only the transaction ID, has not been implemented. This request ID is used on the firewall to locate the request that was initially sent and submit it again to the server. This adaptation does not in any way affect the operation of SCEP exchanges.
- The **GetCACaps** operation, which makes it possible to retrieve the list of SCEP features implemented on the server, is not available. This does not in any way affect the management of certificates through SCEP.
- The **GetNextCACert** operation, which makes it possible to retrieve the CA's future certificate before the expiration of the current certificate, has not been implemented. The CA's new certificate can in fact be retrieved through the **GetCACert** SCEP operation when the certificate that was being used up until then has expired.

- The **GetCRL** operation, which retrieves the latest update of the CRL associated with the CA of the SCEP server, has not been implemented. This operation generates unnecessary and excessive activity on the server and the firewall has its own option "Enable regular retrieval of certificate revocation lists (CRL)" (**System** > **Configuration** module > **General settings** tab).
- The draft specification imposes the restriction of the POST method to only SCEP **PKIOperation** operations. On SNS firewalls, this method is used by default for all requests. However, the GET method can be imposed using the "post=off" option for the various SCEP commands available in command line.
- The encryption and authentication algorithms used by default on the firewall are 3DES and SHA-1.

SSL VPN

After the OpenVPN upgrade to version 2.4.4:

- IP address ranges that extend beyond a Class B network (mask /16) must no longer be used.
- Certain TLS algorithms are no longer available.

If your configurations are affected by these restrictions, SSL VPN tunnels can no longer be set up. Error messages will appear explaining how to help you correct your configuration.

IPv6 support

In version 3, 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.

Audit logs

Support reference 60085

Sandboxing

After the firewall has been restarted, a "System error Sandboxing license unavailable" alarm will indicate that the sandboxing license is not available. This alarm appears even when you neither have a sandboxing license nor use sandboxing in your filter rules.

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.

NAT

Support reference 29286

The GRE protocol's state is managed based on source and destination addresses. As such, two simultaneous connections with the same server cannot be distinguished, either from the same client or sharing a common source address (in the case of "map").

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

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 command `monitor flush hostrep ip = host_ip_address`.

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.

Support reference 31715

URL filtering

Authenticated users cannot be filtered within the same URL filter policy. However, particular filter rules may be applied (application inspection) according to users.

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 Active Directory domains
When multiple Active Directory domains are linked by an approval relationship, an Active Directory and SN SSO Agent must be defined in the firewall configuration for each of these domains.

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

Mobile clients cannot be authenticated with multiple Active Directories in phase 1 of the IPsec negotiation.

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

LDAP directory - Microsoft Active Directory
Users are missing from the list of members of their primary group.
This is due to how Microsoft Active Directory works: the user's *memberof* attribute does not in fact contain the user's primary group. Likewise, the user is not included in the *member* attribute of his primary group.

As Stormshield firewalls use the *member* attribute to obtain a group's list of users, they therefore do not appear in the list of members of their primary group.

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".

Conditions of use
The Internet access conditions of use may not display correctly on the captive portal in Internet Explorer v9 with the IE Explorer 7 compatibility mode.

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 out via the authentication portal as the user would need to provide a cookie to log out, 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.

High availability

HA interaction in bridge mode and switches
In a firewall cluster configured in bridge mode, the average failover was observed to last about 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 is not supported on clusters made up of firewalls of different models. 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.

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

SN Real-Time Monitor

File transfer commands (sending and receiving) from the CLI console in SN Real-Time Monitor no longer function in 2.x and higher versions.

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. This issue also arises with the "Reinitialize all tunnels" function, offered in the Real-Time Monitor interface.

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

SN Event Reporter

SN Event Reporter is no longer included in the administration suite from version 3 upwards, and connections from SN Event Reporter to firewalls in version 3 and up will not be supported

Documentation resources

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

Guides

User Guides

- SNS v3.11 LTSB User Manual
- SNS v3.11 LTSB CLI / Serverd Commands Reference Guide
- SNS v3.11 LTSB CLI / SSH Commands Reference Guide

Installation Guides

- Product Presentation and Installation SNS
- Installation and first-time configuration of an SNS firewall Guide
- SNS EVA virtual firewall Deployment Guide
- SNS PAYG virtual firewall Deployment Guide
- Stormshield Network Real-Time Monitor - User and configuration manual

Technical notes

Authentication

- SSO Configuration - Microsoft SPNEGO
- Configuring "Guests" Authentication Methods
- SN SSO Agent for Windows - Installation and Deployment Guide
- SN SSO Agent for Linux - Installation and Deployment Guide

Configuration

- Adapting the SES security policy of a workstation to its SNS reputation
- Automatic backups
- Basic Command Line Interface configurations
- Collaborative security
- Complying with privacy regulations
- Configuring a 3G/4G modem on SNS
- Custom Context-based Protection Signatures
- Filtering HTTPS connections
- Firewall Stacking: service distribution
- Identifying industrial protocol commands going through the firewall
- Implementing a filtering rule
- Initial configuration from USB key

- LACP link aggregation
- Level 2 encapsulation
- Setting up a NAT rule
- SDS Easy - Embedding a SNS PKI in a SDS client

Hardware

- Secure Return option
- Software Recovery via USB key
- SNI20 - Updating the BIOS to version R1.06
- IPMI Firmware update (SN6000 and SN6100)
- Changing a Power Supply Module (SN3000 and SN6000)

Logs

- Description of audit logs V3
- Integrating SNS logs in IBM QRadar

Routing

- Bird dynamic routing V3

SNS for Cloud

- EVA on 3DS OUTSCALE
- EVA on Amazon Web Services
- EVA on Microsoft Azure
- SNS For Cloud - Amazon Web Services
- Deploy SNS For Cloud (2 network interfaces) on Microsoft Azure
- VMWare NSX : SNS Firewall as an edge 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 - Authentication by certificate
- 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 3.11.18 LTSB 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 3

In this section, you will find new features, resolved vulnerabilities and fixes from previous versions of Stormshield Network Security 3.

3.11.17 LTSB			Bug fixes
3.11.16 LTSB			Bug fixes
3.11.15 LTSB		Resolved vulnerabilities	Bug fixes
3.11.14 LTSB			Bug fixes
3.11.13 LTSB		Resolved vulnerabilities	Bug fixes
3.11.12 LTSB	New features		Bug fixes
3.11.11 LTSB		Resolved vulnerabilities	Bug fixes
3.11.10 LTSB			Bug fixes
3.11.9 LTSB		Resolved vulnerabilities	Bug fixes
3.11.8 LTSB		Resolved vulnerabilities	Bug fixes
3.11.7 LTSB	New features	Resolved vulnerabilities	Bug fixes
3.11.6 LTSB	New features	Resolved vulnerabilities	Bug fixes
3.11.5 LTSB			Bug fixes
3.11.4 LTSB			Bug fixes
3.11.3 LTSB	New features	Resolved vulnerabilities	Bug fixes
3.11.2 LTSB			Bug fixes
3.11.1 LTSB	New features	Resolved vulnerabilities	Bug fixes
3.10.3			Bug fixes
3.10.2	New features	Resolved vulnerabilities	Bug fixes
3.10.1	New features	Resolved vulnerabilities	Bug fixes
3.9.2		Resolved vulnerabilities	Bug fixes
3.9.1		Resolved vulnerabilities	Bug fixes
3.9.0	New features		Bug fixes
3.8.1		Resolved vulnerabilities	Bug fixes
3.8.0	New features	Resolved vulnerabilities	Bug fixes
3.7.x LTSB		3.7 LTSB version	
3.6.1	New features		Bug fixes

3.6.0	New features		Bug fixes
3.5.2			Bug fixes
3.5.1			Bug fixes
3.5.0	New features		Bug fixes
3.4.3			Bug fixes
3.4.2		Resolved vulnerabilities	Bug fixes
3.4.1	New features	Resolved vulnerabilities	Bug fixes
3.4.0	New features		Bug fixes
3.3.2		Resolved vulnerabilities	Bug fixes
3.3.1		Resolved vulnerabilities	Bug fixes
3.3.0	New features		Bug fixes
3.2.1	New features	Resolved vulnerabilities	Bug fixes
3.2.0	New features		Bug fixes
3.1.2			Bug fixes
3.1.1	New features		Bug fixes
3.1.0	New features		Bug fixes
3.0.3			Bug fixes
3.0.2			Bug fixes
3.0.1	New features		Bug fixes
3.0.0	New features		

Version 3.11.17 LTSB bug fixes

System

SNMP agent

Support reference 84335

An anomaly in the SNMP agent that could cause the SNS firewall to unexpectedly shut down has been fixed.

IPSec VPN IKEv2 - Mobile peers in config mode

Support reference 84482

Whenever an IPsec IKEv2 tunnel set up with a mobile peer in config mode was abruptly shut down by the remote client, the IP address that was assigned to it would remain locked and unavailable. A parameter has been changed so that users can recover their previous IP address in such scenarios.

Version 3.11.16 LTSB bug fixes

System

Disk monitoring - SNi20 model firewalls

Disk monitoring now functions on SNi20 model firewalls.

High availability

Support reference 84100

In a high availability configuration, when a link is lost on the active node of the cluster, the switch from the active to passive node now takes place faster. This allows the passive node to switch more quickly to an active state, therefore minimizing interruption to network traffic.

Creating interfaces

Support reference 75064

Configurations that contain several hundred interfaces (virtual, VLAN, etc.) no longer cause excessive CPU consumption after network interface configuration files are repeatedly reloaded.

HTTP proxy

Support reference 83607

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

Regular CRL retrieval

Support reference 84431

When the command `PKI CONFIG UPDATE` is used, an incorrect value (such as *Any*) can no longer be entered in the *checkcrlbindaddr* argument.

Outgoing traffic statistics - SSL VPN

Support reference 79814

The counters that counted packets leaving the network interface linked to the SSL VPN were no longer refreshed This anomaly, which first appeared in SNS version 3.7.12, has been fixed.

Resolved vulnerabilities in version 3.11.15 LTSB

OpenSSL

A high severity vulnerability was fixed in OpenSSL.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-008/.

vim file editor

Moderate severity vulnerabilities affecting the *vim* file editor have been fixed.

Details on these vulnerabilities can be found on our website https://advisories.stormshield.eu/2022-004.

ClamAV antivirus

A moderate severity vulnerability was fixed in ClamAV.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-005.

Version 3.11.15 LTSB bug fixes

System

Filter - NAT

Support reference 82567

In some cases, the **TCP (c/s)** connection threshold set in the Quality of Service (QoS) settings in a filter rule were not applied. This issue has been fixed.

Web administration interface

Logs - Audit logs - Alarm details

Support reference 84332

In the modules **Logs - Audit logs > Views > Alarms** and **Logs - Audit logs > Logs - Logs > Alarms**, the **Open help to see details on this alarm** link that can be accessed by right-clicking on an alarm now woks correctly for all alarms.

Version 3.11.14 LTSB bug fixes

System

Proxies

Support reference 79295

The SSL proxy now correctly processes certificates that present both an empty *Subject* field and a filled in *SubjectaltName* field.

SSL VPN Portal

Support reference 82626

On the **Secure access** page of the SSL VPN Portal, links that enable access to servers via the browser have been deleted as they no longer functioned.

IPsec VPN with NAT-T and *Path MTU Discovery* (PMTUD) enabled

Support reference 83292

When the PMTUD option (CLI/Serverd command `CONFIG IPSEC UPDATE slot=<1-10> PMTUD=<0|1>`) was enabled for an IPsec tunnel going through NAT-T, packets with an MTU that was too high would occasionally be generated. Such packets would then be blocked by the network devices that they are supposed to pass through.

NAT - VLANs

Support reference 79759

In a configuration that supports several VLANs on the same physical interface and which implements address translation with ARP publication on the same VLANs, GARP (*Gratuitous ARP*) packets would be wrongly sent to only one of these VLANs. This issue has been fixed.

Resolved vulnerabilities in version 3.11.13 LTSB

SSL VPN

A high severity vulnerability was fixed in the SSL VPN.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2022-003/.

Intrusion prevention engine

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

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-050/.

High availability (HA)

A moderate severity vulnerability was fixed in the high availability mechanism.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-001/.

Version 3.11.13 LTSB bug fixes

System

SNMP Agent

Support reference 81710

Several anomalies that could cause memory leaks in the SNMP agent have been fixed.

Authentication to an LDAPS server

Support reference 84199

The firewall was occasionally unable to authenticate on an LDAPS server when a certificate signed by a CA with a CRL was presented. This issue has been fixed.

Host reputation

Support reference 70473

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

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

Hardware monitoring - Disks

Support reference 84083

The mechanism that analyzes the results of SMART tests has been adapted to stop raising inappropriate alerts on some SSD references.

New features in version 3.11.12 LTSB

High availability and link aggregation

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

Version 3.11.12 LTSB bug fixes

System

IPsec VPN

Support references 83903 - 84062

IPsec VPN tunnels that were set up with certificate authentication would occasionally fail when the private key was protected by the TPM. A "*No private key found for <CN>*" error would then be logged. This issue has been fixed.

Authentication

Support reference 82856

When multiple authentication requests are submitted on a firewall that handles heavy traffic, this would sometimes consume an excessive amount of CPU and cause packet loss. This issue has been fixed.

Filtering and NAT

Support references 81369 - 83651

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

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

Do note that this mechanism is disabled by default.

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.

Intrusion prevention

SSL proxy

Support reference 80792

Since Zoom application traffic is incompatible with the antivirus analysis, its CNs have been added to the CN group *proxyssl_bypass*.

HTTP

Support reference 83553

The HTTP protocol analysis has been optimized to avoid consuming too much memory and inappropriately overloading the firewall.

Resolved vulnerabilities in version 3.11.11 LTSB

Vim file editor

Moderate severity vulnerabilities affecting the Vim file editor have been fixed.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2021-061/,
- https://advisories.stormshield.eu/2021-062/,
- https://advisories.stormshield.eu/2021-063/,
- https://advisories.stormshield.eu/2021-064/.

IPsec VPN

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

Details on these vulnerabilities can be found on our website https://advisories.stormshield.eu/2021-065/.

Version 3.11.11 LTSB bug fixes

System

IPsec VPN

Support reference 83354

Whenever an IPsec policy contained one or several *bypass* rules (in which the peer is *None* and the rule was created to exclude the following rules from the encryption policy), these *bypass* rules were not applied to networks defined by static routes.
This issue was fixed with the addition of an IPsec *bypass* option in the step during which the static route is defined.

Captive portal - External LDAP directory

Support reference 82686

Whenever a user referenced in an external LDAP directory connects to the captive portal, the system event “LDAP unreachable” (event 19) is no longer raised.

Version 3.11.10 LTSB bug fixes

System

SNMP Agent

Support reference 78761

SNMP *informRequest* messages are now considered valid SNMP requests and no longer raise the blocking alarm “Invalid SNMP protocol" (snmp:388).

Support reference 82661

The correct value is now returned in the OID *UCD-SNMP-MIB::memCached.0*.

Disk monitoring

Support references 75125 - 75126 - 83541

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

Support reference 81713

During the initial configuration via USB key, changes to the reference time zone specified in the additional configuration file in CSV format are now correctly applied.

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.

Intrusion prevention

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 issue has been fixed.

SIP

Support references 79839 - 79344

Anomalies in the SIP protocol analysis engine, which could cause the firewall to freeze, have been fixed.

Resolved vulnerabilities in version 3.11.9 LTSB

RTSP, SIP, H323 and MGCP protocol analyses

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/2021-020/.

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/2021-007/.

Proxies

A moderate 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/2021-005/.

DHCP service

A moderate severity vulnerability was fixed in the DHCP service.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-034/.

Curl library

A moderate severity vulnerability was fixed in the *Curl* library.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu/2021-048/.

OpenSSL

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/2021-054/.

Version 3.11.9 LTSB bug fixes

System

System events

Support reference 80426

System event no. 19 "LDAP unreachable" is now activated when there are issues accessing an LDAP directory defined in the firewall configuration.

IPsec VPN

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.

Support reference 82729

Whenever a certificate was identified by a name (DN - Distinguished Name) longer than 128 characters, the firewall would retain only the first 128 characters. The deployment of an IPsec configuration via SMC with such a certificate would therefore fail because the DNs of the certificates do not match.
The maximum supported length is now 204 characters (technical limit).

Support reference 81471

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

Support references 82645 - 83087

In IPsec configurations that use groups containing address ranges, mounted tunnels could be interrupted when such groups were modified, generating *TS_UNACCEPTABLE* errors as a result. This issue has been fixed.

IPsec VPN - Routing

Support reference 80662

When a change of status is applied to a network route associated with an IPsec Security Policy, the service would sometimes shut down unexpectedly and cause the firewall to freeze. This issue has been fixed.

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.

SNMP Agent

Support reference 81710

Issues with memory leaks on SNMP agent have been fixed.

Support reference 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 reference 81710

The mechanism that manages the SNMP alarm table has been enhanced to stop OIDs from being duplicated, as this prevented some alarms from being raised.

CRL verification

Support reference 82370

Whenever a CRL contained an object identified by a fully qualified domain name (FQDN), the DNS resolution of this FQDN would function correctly again when the firewall verified the CRL. This regression appeared in SNS version 3.11.1.

ICMP - IPv6

Support reference 82547

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

Network link aggregation

Support reference 82211

If a link was lost in an aggregate, a switch to a new link could not be made before a 3-second wait, thereby disrupting traffic for 3 seconds. This issue has been fixed.

High availability (HA)

Support reference 82211

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

Support reference 80049

In high availability configurations, after a node switched from active to passive, the passive node would continue to monitor router objects in addition to HA interfaces, generating packet sending errors as a result. This issue has been fixed.

Support reference 80049

In high availability configurations, after the status of a node changed twice (active to passive, then to active again), an anomaly in the communication between several components of the

gateway monitoring mechanism would generate inconsistencies in the status of monitored gateways, and in the update of routes that allow these gateways to be monitored. These issues have been fixed.

Network

Renewing a DHCP lease

Support references 82238 - 82359

When a UNICAST packet originating from port 67 and going to port 68 attempted to pass through the firewall (especially during a DHCP lease renewal), the firewall would occasionally freeze and fail to transmit the packet if the packet's source and outgoing interface are not part of a bridge.

This issue can now be fixed by changing the value of the **UseAutoFastRoute** parameter to **Off** with the following CLI/Serverd command:

```
CONFIG PROTOCOL TCPUDP COMMON IPS CONNECTION UseAutoFastRoute=<On|Off>
```

Find out more

Intrusion prevention

Intrusion prevention engine statistics

Support references 79713 - 82437 - 81466

The mechanism that manages intrusion prevention engine statistics has been optimized to stop potential packet loss when these statistics are recurrently processed on a firewall handling a high network load.

Elastic Virtual Appliances (EVA)

CLI/Serverd commands

Support reference 82637

The CLI / Serverd MONITOR 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.

Resolved vulnerabilities in version 3.11.8 LTSB

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.

ClamAV

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

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu,
- https://advisories.stormshield.eu.

Version 3.11.8 LTSB bug fixes

System

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.

IPsec VPN

Support references 79713 - 81464

Packets would sometimes get lost whenever the keys of IPsec tunnels were renewed. This issue has been fixed.

Regular CRL retrieval

Support reference 81259

The verification of CRLs through the proxy would occasionally not function because the port to reach the proxy was not correctly applied. This issue has 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.

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.

IP address reputation and geolocation service

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.

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.

Network

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.

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.

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.

New features in version 3.11.7 LTSB

IMPORTANT
Firewalls must not be upgraded from SNS in version 3.10.x or 3.11.x LTSB to a 4.0.x version. This operation is not supported.
For further information, refer to Recommendations.

System

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

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 who use internal mirror sites, you must update the packets hosted on your own servers 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.

In a Linux environment, a new version of the *updater.sh* script is available and makes it possible to retrieve all packets signed by the new certification authority.

Find out more

Resolved vulnerabilities in version 3.11.7 LTSB

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.

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.

Version 3.11.7 LTSB bug fixes

System

IPsec VPN

Support reference 80659

When a VPN policy contains many tunnels in which the **Keepalive** option is enabled, this may make the policy exceptionally slow. This anomaly has been fixed.

Support references 81002 - 81013

When the **MakeBeforeBreak** renegotiation scheme was used in IPsec VPN IKEv2 configurations, authenticated users would be deleted from the firewall's table of authenticated users when phase 1 of the VPN tunnel was renegotiated. This anomaly has been fixed.

As a reminder, the **MakeBeforeBreak** renegotiation scheme is enabled by default and can be disabled using the following CLI/serverd commands:

```
CONFIG IPSEC UPDATE slot=<1-10> MakeBeforeBreak=<0|1>
CONFIG IPSEC ACTIVATE
```

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

New features in version 3.11.6 LTSB

IMPORTANT
Firewalls must not be upgraded from SNS in version 3.10.x or 3.11.x LTSB to a 4.0.x version. This operation is not supported.
For further information, refer to Recommendations.

Option to disable stealth mode

Stealth mode has been enhanced with the possibility of disabling it and allowing responses to ICMP requests. This mode can only be changed through the CLI/Serverd command:

```
CONFIG PROTOCOL IP COMMON IPS CONFIG Stealth=<On|Off>
CONFIG PROTOCOL IP ACTIVATE
```

These commands are explained in detail in the CLI SERVERD Commands Reference Guide.

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`.

Update

The hash algorithm of firmware update files has been changed to comply with the highest standards.

Resolved vulnerabilities in version 3.11.6 LTSB

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.

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 3.11.6 LTSB bug fixes

System

Proxies

Support reference 80378 - 77199

Issues with memory leaks in proxies, which would sometimes restart the service unexpectedly, have been fixed.

Support reference 79584

An issue with the management of the SSL context, which could freeze the proxy service, has been fixed.

Support references 79957 - 80108

Configurations that use multi-user authentication would sometimes require several minutes to fully load web pages that embed CSP (content-security-policy) directives. This anomaly has been fixed.

IPsec VPN

Support reference 77960

ESP packets passing through an IPsec tunnel did not keep the DF bit ("Don't fragment") even though the parameter *net.inet.ipsec.dfbit=2* specified the opposite. This anomaly has been fixed.

Find out more

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 (HA)

The errors that occur when the passive member of the cluster is updated are now shown in the firewall's web administration interface.

Filtering and NAT

Support references 79533 - 79636 - 80043 - 80412

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.

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 77779 - 80036

Excessive memory consumption issues that caused the SNMP agent service to unexpectedly shut down have been fixed.

Restoring or deploying configurations via Stormshield Management Center (SMC)

Support reference 80269

When the configuration of a firewall was restored or deployed via Stormshield Management Center (SMC), the restoration or deployment process would wrongly attempt to retrieve the private key of a certificate on the TPM even when the firewall did not have such a module. This would then return the error *tpm file read error*. This anomaly has been fixed.

Network

Link aggregation

Support reference 79805

Whenever two SNS firewalls with an LACP link communicated, traffic was sent from only one link aggregate interface. This anomaly 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.).

This makes it possible to prevent key decryption errors on firewalls equipped with a TPM (SN3100 and SNi20).

Find out more

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.

Web administration interface

NTP client

Support reference 79917

When an NTP server was deleted from the web administration interface; the other NTP servers would lose the *bindaddr* from their configuration. This anomaly has been fixed.

As a reminder, this parameter makes it possible to define the interface through which NTP requests pass.

Find out more

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 be shown in the table after quitting the module. This anomaly has been fixed.

Version 3.11.5 LTSB bug fix

It is highly recommended to apply the 3.7.17 LTSB or 3.11.5 LTSB updates to firewalls in major versions 3.x.x.

As a preventive measure, the certificate used to sign new version updates has been replaced in version 3.11.5 LTSB. 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 3.11.5 LTSB, you must use the USB Recovery procedure. The standard downgrade procedure will not be supported.

Version 3.11.4 LTSB 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 3.11.3 LTSB

IMPORTANT
Firewalls must not be upgraded from SNS in version 3.10.x or 3.11.x LTSB to a 4.0.x version. This operation is not supported.
For further information, refer to Recommendations.

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 - System events

The SNS firewall can now generate a system event when the VPN tunnel fails to set up due to a network issue. This event can be exported through SNMP traps.

Obsolete features

IPsec VPN - Obsolete authentication and encryption algorithms

As some algorithms are obsolete, vulnerable 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.

Resolved vulnerabilities in version 3.11.3 LTSB

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 3.11.3 LTSB bug fixes

IMPORTANT

In some situations, memory leaks may affect the proxy, causing the service to restart unexpectedly. Contact Stormshield support if you think that this issue might affect you.

System

Proxies

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

Issues with memory leaks in proxies, which would sometimes restart the service unexpectedly, have been fixed.

Support references 79304 - 79888

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.

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

TPM

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*).

VPN SSL in portal mode

Support reference 68759

SSL VPN in portal mode now uses a component that is compatible 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.

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.

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.

High availability (HA)

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: SNXXXXXXXXXXXX Command: SYNC FILES failed: Command failed : Command has failed : code 1".

Support references 78758 - 75581

Memory leak issues, especially in the mechanism that manages HA status and role swapping in a cluster, have 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.

Radius authentication

Support reference 76824

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.

SNMP agent

Support reference 74514

The anomalies observed in table indexing, which reflected the hardware status of cluster members in the HA MIB, have been fixed. Returned OIDs did not match the associated MIB, preventing the use of *snmpget* requests to reach these OIDs. Such requests now function correctly.

Automatic backup

Support reference 79807

After a firewall upgrade to a 3.10.x version, then to a 3.11.x version, automatic backups no longer functioned because the network objects that made it possible to reach the automatic backup server were not correctly created.

Network

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.

MTU link aggregation

Support references 78517 - 74507

Aggregated links now use the maximum size of a packet (MTU) configured on their link aggregate (LACP).

Intrusion prevention

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).

sfctl command

Support reference 78769

Using the *sfctl* command with a filter on a MAC address no longer restarts the firewall unexpectedly.

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.

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.

Web administration interface

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.

Version 3.11.2 LTSB bug fixes

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

New features in version 3.11.1 LTSB

IMPORTANT
Firewalls must not be upgraded from SNS in version 3.10.x or 3.11.x LTSB to a 4.0.x version. This operation is not supported.
For further information, refer to Recommendations.

Long-Term Support Branch (LTSB)

SNS version 3.11 is labeled “LTSB” so that it can be considered a version that will be stable over a long term, and will be supported for at least 12 months.

Refer to Compatibility to find out which products are compatible. For more information on the LTSB label, refer to the documents in the section **Product** > **Product Life Cycle** on MyStormshield.

SNi20 model industrial firewalls

Version 3.11.1 LTSB of the SNS firmware ensures compatibility with new SNi20 industrial firewalls.

The features listed below are not available on such firewalls in 3.11.x LTSB versions of the SNS firmware, and are available only from SNS version 4.1.1 onwards:

- Hardware bypass,
- Hardware-secured VPN secrets with the TPM module,
- Link aggregation (LACP),
- Network loop management protocols (RSTP and MSTP).

For more information, refer to the product page for the SNi20 model.

High availability

Shorter failover time when an interface fails

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 is now one second, shortening the interruption to network traffic.

System

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>
```

```
CONFIG NTP ACTIVATE
```

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

Key size of certificates generated by the SSL proxy

The size of keys for certificates generated by the SSL proxy can now be configured.

This parameter can only be modified through *CLI / Serverd* commands:

```
PKI CA CONFIG UPDATE caname=<name> server_size=<size>
```

```
PKI ACTIVATE
```

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

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 checkcrlbindaddr=<bindaddr>
```

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

Authentication

LDAP

Backup LDAP servers can now be configured on ports other than the main LDAP server port.

Certificates and PKI

CRL retrieval

On root authorities that have a built-in certificate revocation list distribution point (CRLDP), CRLs will now be automatically retrieved from these distribution points when an application uses the root authority's certificate.

Obsolete features

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 - Backup peers

As the use of backup peers (referred to as "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 3.11.1 LTSB

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.

NTP service

Vulnerability CVE-2019-8936 was resolved and various fixes were applied with the upgrade of the NTP service to version 4.2.8p14.

FreeBSD

Vulnerabilities CVE-2019-15879 and CVE-2019-15880 relating to cryptodev were fixed after a FreeBSD security patch was applied, to counter the risk of memory corruption by users authenticated on the operating system.

OpenSSH

Vulnerability CVE-2016-8858 was fixed after the OpenSSL software suite was updated.

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

OpenSSL

A vulnerability was fixed after the OpenSSL cryptographic library was updated.

XSS flaw

A vulnerability affecting the **Users > Access privileges** module, *Detailed access* tab in the web administration interface has been fixed.

Version 3.11.1 LTSB 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.

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 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 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 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 IPv4 traffic that was transported in IPv6 IPsec tunnels through virtual interfaces, the firewall would no longer look for return routes among the IPv6 virtual interfaces. Such IPv4 packets are now correctly exchanged at each tunnel endpoint.

IPsec VPN - Logs

Support references 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.

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 anomaly has been fixed.

SSL VPN Portal

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.

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

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.

High availability - link aggregation

In high availability configurations, the mechanism that switches a node from active to passive has been enhanced so that it no longer renegotiates aggregate links (LACP) when:

- The option **Reboot all interfaces during switchover (except HA interfaces)** is enabled (**Configuration > System > High availability** module, under **Advanced properties**, **Swap configuration**),
  - and -
- The **LacpWhenPassive** parameter is enabled with a value of "1" (file */usr/Firewall/ConfigFiles/HA/highavailability Global LACPWhenPassive <0|1>*).

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).

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 - Triggering the failover of a node

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 - Filtering and NAT - Time objects

Support references 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.

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 anomaly has been fixed.

Support reference 75745

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 anomaly has been fixed.

SSL proxy

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 anomaly has been fixed.

Global host objects included in router objects

Support reference 71974

When global host objects included in router objects (local or global) are renamed, the change is correctly applied in the router object concerned.

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 can be used.

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.

TPM

Support reference 76664

When a certificate is revoked, the associated .pkey.tpm file is now properly deleted.

Routers

Support references 75745 - 74524

After a firewall is restarted, the router monitoring service now correctly applies the last known status of these routers.

Automatic backups

Support reference 75051

The mechanism that checks the certificates of automatic backup servers was modified after the expiry of the previous certificate.

Connections from Stormshield Management Center (SMC)

Support reference 76345

During the initial connection from SMC to the web administration interface of a firewall in version 3.7 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.

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 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).

Local storage

Support reference 75301

Firewalls with damaged SD cards (and therefore damaged log storage partitions) would restart in loop. This anomaly has been fixed.

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.

Sandboxing in the proxy

Support reference 77199

The risk of memory leak when the sandboxing engine is used in the proxy has been fixed.

Intrusion prevention

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 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).

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).

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.

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.

Network

Wi-Fi

Support reference 75238

Changes to the access password of a Wi-Fi network hosted by the firewall are now correctly applied.

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.

High availability

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.

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).

Routing

Support reference 77707

Bird dynamic routing

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).

Web administration interface

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 account and of all users and user groups added as administrators. The report previously contained only sessions of the admin account.

Interfaces

Support references 74312 - 76578

When new interfaces were created, their ifnames would sometimes not be correctly assigned (e.g.,vlan0), preventing the interfaces from being created. This issue would arise after interfaces were deleted, releasing their corresponding ifnames as a result, but wrongly leaving the following ifnames to be assigned, even though they were not necessarily free. This anomaly has been fixed.

Certificates and PKI

Support reference 77598

Adding a URI address to the distribution points of certificate revocation lists (CRL) would in some cases create an address for each character entered. This anomaly has been fixed.

3.11.0 Version not released

The 3.11.0 version is not publicly available.

Version 3.10.3 bug fixes

WARNING

- When a firewall that contains an IKEv1 mobile IPsec policy with certificate authentication is upgraded to version 3.10.3, the IKE negotiation engine may switch from *racoon* to *charon*.

  When this occurs, the warning message will appear in the IPsec VPN module: "Combining IKEv1 and IKEv2 peers within the same IPsec policy remains experimental."

  IPsec tunnels that have already been configured will remain operational in theory.

  If your configuration contains such an IPsec policy, we strongly advise you to read this Stormshield Knowledge Base article before you start the upgrade to SNS 3.10.3.
- 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

IPsec VPN

Support references 77264 - 77165 - 77274 - 77246

IPsec policies that were modified on firewalls in version SNS 3.10.x would occasionally be corrupted when they were applied and reloaded, or after the firewall was restarted. This issue has been fixed.

Additionally:

- When an IPsec peer is created, a peer ID no longer needs to be specified in the **Peer ID** field,
- When an IPsec VPN mobile peer with pre-shared key authentication is created, the **Pre-shared key** that this peer needs to use must be specified if a peer ID has been entered in the **Peer ID** field.

New features in version 3.10.2

WARNING
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.

Initial configuration via USB

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.

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.

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.

System

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.

WebGUI file signature

A signature has been added for SNS WebGUI files to strengthen SMC communication mechanisms.

Resolved vulnerabilities in version 3.10.2

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

The vulnerability CVE-2020-7451, which is due to a field that was not properly initialized in the IPv6 header of the TCP network stack, was fixed with the application of a FreeBSD security patch.

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 3.10.2 bug fixes

System

Proxies

Support references 76535 - 75662

Competing access between SSL and HTTP proxy queues would sometimes shut down the proxy manager unexpectedly. This anomaly has been fixed.

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).

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 anomaly has been fixed.

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.

New features in version 3.10.1

WARNING
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.

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. The action applied to the file will then depend on the value given to the "When the antivirus analysis fails" field in the *Analyzing files* tab for FTP, HTTP, POP3 and SMTP protocols. This value is set by default to "Block".

Set by default to 120 seconds, this new parameter can only be modified through the *CLI / Serverd* command:

```
CONFIG ANTIVIRUS LIMITS MaxProcTime=<time>
```

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, it is now possible to assign a weight to each interface in the aggregate in order 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.

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 Gratuitous ARP (GARP) during a switch.

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.

Certificates and PKI

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.

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.

In SNS version 3.10, 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.

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.

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.

Authentication

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).

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.

SSL VPN and certificates

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

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.

Initial configuration via USB

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.

System

The random generator on the kernel named *arc4random* has been upgraded so that it is no longer based on RC4 but on CHACHA20, which is faster and more robust.

The firewall operating system has been upgraded to refresh time zones and daylight saving time.

Hardware

Hardware-based security for VPN secrets on compatible SN3100 models

Ever since revision A3 of SN3100 firewalls, they now offer a trusted platform module (TPM) that secures VPN secrets. With the TPM, a level of security can be added to SN3100 appliances that act as VPN concentrators, which may not necessarily be physically secure. Support for this module begins with this version 3.10.

Serverd Commands

There are now new *CLI / Serverd* commands that operate functions on TPMs and begin with:

```
SYSTEM TPM
```

TPM parameters can also be added to some PKI commands:

```
PKI CERTIFICATE CREATE
```

```
PKI CERTIFICATE PROTECT
```

```
PKI REQUEST CREATE
```

```
PKI SCEP QUERY
```

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

SSH commands

A new *CLI / SSH* command makes it possible to operate the TPM, and begins with:

```
tpmctl
```

It includes the possibility of approving new *PCRs* (*Platform Configuration Registers*) 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 3.10.1

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.

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.

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.

Authentication 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.

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.

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.

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.

Web administration interface

Checks are now conducted 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 3.10.1 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.

IPsec VPN

Support reference 73609

Certificates of IPsec VPN peers are now displayed in the administration interface of the firewall even when they are deployed via SMC.

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.

IPsec VPN (IKEV1 + IKEv2)

Support reference 73584

In configurations that use both IKEv1 and IKEv2 peers, since the 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.

Support reference 74425

A parameter may potentially prevent ResponderOnly mode from running properly whenever Dead Peer Detection (DPD) is enabled. This anomaly has been fixed.

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.

IPsec VPN (IKEv2 / 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.

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.

High availability

When an alias is added to an existing network interface, firewalls in a HA cluster are no longer switched.

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

Firmware can now be updated again via USB key.

Certificate-based authentication

A content check has been applied to some parameters used in the creation of cookies.

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.

SNMP

Support reference 71584

The use of the value *snmpEngineBoots* has changed in order to comply with RFC 3414.

Support reference 72984

When a whitelisted user in the SNMP protocol configuration runs an SNMP operation, the "*Prohibited SNMP user name*" alarm is no longer raised.

SLD daemon

Support references 69577 - 73026

Running the SLD process would sometimes consume an excessive amount of memory resources. This anomaly has been fixed.

Filter - NAT

Support reference 76346

When the “Enable the SYN proxy” option was enabled, it would occasionally generate an error when filter rules were confirmed or edited, making it impossible to use this option. This anomaly has been fixed.

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.

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.

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) would sometimes generate XML errors and prevent 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 anomaly has been fixed; now only the first 1000 items are displayed.

Automatic backups - Cloud Backup

Support reference 73218

Configuration backups could no longer be restored from Cloud Backup since version 3.5.0. This anomaly has been fixed.

Proxy

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 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.

Support reference 66508

The proxy no longer shuts down unexpectedly when an HTTP header analysis fails.

Support references 70598 - 70926

The behavior of the HTTP proxy has been changed so that the SLD process on the firewall will no longer be overwhelmed when too many requests are redirected to the authentication portal.

Support references 70721 - 74552

Memory consumption is now optimized when the proxy is used.

Intrusion prevention

Static routing

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.

SIP

Support references 74771 - 75108

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.

HTTP

The HTTP plugin 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.

TDS protocol

The intrusion prevention engine would occasionally generate false positives during the analysis of TDS (Tabular Data Stream) packets.

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.

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 impossible with the TPM. This anomaly has been fixed.

3.10.0 Version not released

The 3.10.0 version is not publicly available.

Resolved vulnerabilities from version 3.9.2

iconv library update

Vulnerability CVE-2019-5600 has been fixed by the upgrade of the *iconv* library.

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

bzip2 library update

Vulnerabilities (CVE-2016-3189 and CVE-2019-12900) have been fixed by the upgrade of the *bzip2* library.

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

OpenSSL security flaw

Vulnerability CVE-2019-1563 has been fixed by upgrading the OpenSSL cryptographic library.

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

Version 3.9.2 bug fixes

System

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.

Resolved vulnerabilities from version 3.9.1

ClamAV

Vulnerability CVE-2019-13232 has been fixed by the upgrade of the ClamAV antivirus engine.

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

FreeBSD

Vulnerability CVE-2019-5611 has been fixed with the application of a FreeBSD security patch.

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

Version 3.9.1 bug fixes

System

Firewalls with IXL cards

Support reference 74175

The fix below affects firewalls that use IXL cards, in particular:

- Fiber 4x10 Gbps and 2x40 Gbps network extension modules for SN2100, SN3100 and SN6100 models,
- 4x10 G BASE-T modules for SN710, SN910, SN2000, SN2100, SN3000, SN3100 and SN6100,
- Both fiber 10 Gbps onboard ports on SN6100 models.

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.

Support reference 73005

An issue with latency, which could affect firewalls connected using an IXL card on third-party equipment, has been fixed.

Firewalls with IX cards

Support reference 74175

The fix below affects firewalls that use 4x10 Gbps fiber extension modules for SN710, SN210, SN2000, SN3000 and SN6000 (modules also compatible with SN2100 and SN3100).

After the firewall starts up, the automatic media speed detection could fail to be negotiated, and the firewall would consider the network interface offline. The interface could be re-enabled only by physically disconnecting and reconnecting the media. This issue has been fixed, and the available values for IX network cards can now be selected in the **Network** > **Interfaces** module.

Certificate-based authentication

A content checker has been added for the "app" parameter used during the creation of cookies.

Maintenance - Firmware updates

Additional checks have been implemented on the mechanism that searches for available firmware updates and their respective download links.

New features in version 3.9.0

Initial configuration via USB

The mechanism that handles initial configurations via USB drives on firewalls in factory configuration has been improved.

Apart from functions already available in previous firmware versions, such as license imports (files with a ".licence" extension), firmware updates (files with a ".maj" extension), configuration backup imports (files with a ".na" extension), and imports of SMC server connecting packages (files with a ".pack" extension), this mechanism adds functions that import PKCS#12 certificates, import files containing the *admin* super administrator's password, and run files containing additional configuration commands (CSV file) which allow, among other functions, high availability clusters to be built.

Other enhancements

- Improved management of configuration file backups
- Whenever several firmware versions are on the USB drive, only the most recent version will be applied to the firewall as long as it is from the same major version or the next major version.

Restoring a defective cluster node remotely

The improvements to the mechanism mentioned above, which manages initial configurations via USB drives, combined with the possibility of deleting a secondary node from a cluster without having to enter its serial number, make it possible to replace and configure a defective cluster member remotely.

Certificates and PKI

SCEP

SCEP (Simple Certificate Enrollment Protocol) aims to facilitate and automate the secure deployment of certificates within a public key infrastructure.

The first implementation of SCEP on SNS firewalls was based on the IETF Draft Nourse specification. This evolution of the SCEP implementation is based on the IETF Draft Gutmann specification, which followed the Nourse draft.

SCEP uses various types of requests encapsulated in HTTP to perform the following operations:

- Distribution of the public key of the certificate authority (CA) that signs certificates,
- Certificate creation or renewal requests by the PKI administrator,
- Certificate creation or renewal requests by the certificate holder (enrollment),

A "profile" that groups the parameters needed in the various SCEP requests (CA name, etc.) can be called up whenever these commands are run in order to simplify their syntax.

The SCEP implementation also includes the polling mechanism that makes it possible to track the evolution of requests to the server that hosts the CAs whenever it is unable to process requests immediately.

In SNS version 3.9.0, these operations can only be performed using `PKI SCEP` CLI commands. For more information on the syntax of these commands, please refer to the CLI SERVERD Commands Reference Guide.

Hardware

Stormshield Network SN710, SN910, SN2000 and SN3000

SN710, SN910, SN2000 and SN3000 firewall models support Intel XL710 4-port fiber-optic 10 GbE adapters.

High availability

CLI command

The command HA CLUSTER REMOVE accepts the generic "remote" parameter to designate the cluster's secondary node without the need to know its serial number:

```
HA CLUSTER REMOVE serial="remote"
```

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

Stormshield Management Center

SNS version 3.9.0 allows the firewall to embed an SMC connecting package specifying several administration servers as well as the network interfaces on the firewall that need to be used for the link with each SMC server.

Intrusion prevention

SCTP

The intrusion prevention engine handles the analysis of the Stream Control Transmission Protocol (SCTP). This protocol, which is used in signaling networks over IP, handles in particular the concept of *multi-homing* (distribution of traffic to several IP addresses).

Network

DHCP

The internal DHCP server on firewalls includes two advanced options for the configuration of clients via Bootstrap (BOOTP):

- *next-server*: IP address of the TFTP server that hosts the client's configuration file.
- *filename*: name of the configuration file to be retrieved on the server that was declared earlier.

Web administration interface

Logs (Audit logs) - Alarms and system events

The configuration of Alarms or System events can be accessed directly from a row of logs selected in the respective views.

Authentication portal

The link to the SSL proxy's certificate authority (CA) has been added to the authentication portal's logout page.

Filter - NAT

Clicking on **Search in logs** or **Search in monitoring** to search for a rule with an undefined name would display a message indicating that the search for a nameless rule was unsuccessful.

Monitoring

A search field has been added to the following monitoring modules:

- Routing,
- DHCP,
- SSL VPN,
- Black lists / white lists.

Certificates and PKI

New probes regarding the validity dates and statuses of certificate authorities and certificates used in the firewall's configuration have been added to the firewall's health indicator (displayed in the upper banner of the we administration interface).

For more information on these probes, please refer to the SNS User guide v3.

Version 3.9.0 bug fixes

Intrusion prevention

High availability

Support reference 70654

In a configuration such as the following:

- the active firewall would receive, on an interface uninvolved in HA, packets bearing a source address that is an IP address used for the HA link (IP address spoofing attempt),
- Such packets were allowed by a rule in Firewall or IDS mode,
  or
  the action of the "IP address spoofing (type 2)" alarm was forced to "pass",

the firewall cluster would become unstable.

Additional protection mechanisms have been set up to prevent such situations.

DNS protocol

Support references 71390 - 71391

On firewalls using only IPv4, the DNS protocol analyzer would unnecessarily add IPv6 addresses in the host table. This would eventually flood the table on small firewall models. This issue has been fixed.

OPC UA protocol

Support reference 72255

An anomaly during the analysis of the Industrial protocol OPC UA (value of the *SecureChannel* field in an *OPN* packet) would wrongly raise the block alarm "OPCUA invalid protocol". This anomaly has been fixed.

SIP

Support references 71980 - 68971

Some SIP communications would fail after they were put on hold whenever a peer sent *INVITE* packets containing deprecated "c=IN IP4 0.0.0.0" information which the firewall would reject (block alarm "Invalid SIP protocol (SDP)").

This issue was fixed after a new specific alarm was created ("SIP: Anonymous address in the SDP connection"). Such packets are no longer blocked by default, but the alarm can be configured to block them.

TNS protocol - Oracle

Support references 72518 - 71272

Analyses of TNS - Oracle client-server communications that undergo packet fragmentation and address translation (NAT) no longer desynchronize traffic due to packets being rewritten.

DCERPC protocol

Support reference 70716

The risk of memory leak while analyzing the DCERPC protocol has been fixed.

IKE protocol

The SNMP protocol analyzer would wrongly block some valid IKE packets whenever SNMP packets passed through UDP port 500. This issue has been fixed.

System

CLI commands

Support reference 72020

Temporary files created during a PKI update through the CLI command `PKI IMPORT` were not deleted. This anomaly has been fixed.

IPsec VPN

Support reference 71401

IPsec configurations using the AES256-CBC encryption protocol, and in which traffic endpoints exchanged several separate network streams, would cause traffic to be corrupted during the traffic encryption phase. This issue has been fixed.

IPsec VPN (IKEv1 + IKEv2)

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 would not be taken into account. This anomaly has been fixed.

High availability - SNMP

Support reference 71474

For firewalls on which the SNMP agent had never been enabled, the HA configuration synchronizer would wrongly attempt to synchronize this SNMP agent's system ID. This anomaly has been fixed.

High availability - link aggregation

Support references 65863 - 71002

Whenever the weight of a link aggregate was modified in a HA configuration (**High availability** module > **Weight** field or CLI command `CONFIG HA WEIGHT UPDATE`) it would not be applied and would generate a system error. This issue has been fixed.

High availability - SN6000 / SN6100

Support reference 72924

On clusters that handle a large number of connections (tens of thousands) involving several thousand protected hosts, the HA switch would cause connections to be lost. This issue has been resolved by using all processors to restore connections, hosts and active users.

Authentication – SSO Agent

Support reference 71101

The use of the SSO agent authentication method would cause some users to be wrongly registered as administrators. This anomaly has been fixed.

Quality of Service

Support reference 71136

If no reference bandwidth has been defined (**Security policy** > **Quality of Service** > **Maximum bandwidth per interface** > **Total bandwidth** field) a CPU overload would occur on SN160(W), SN210(W) and SN310 firewall models. A value adapted to the firewall model is now defined by default.

Router objects

Support reference 71502

An anomaly in the gateway monitoring mechanism, which occurred whenever a gateway switched from an internal "maybe down" status (pinging failed) to an internal "reachable" status, has been fixed.

FQDN objects

Support reference 69784

The number of IP addresses saved for an FQDN object would be wrongly restricted to 32 entries. This issue has been fixed.

SSL VPN

Support references 66481 - 69424

An anomaly in the counter that counts the number of users connected via SSL VPN would wrongly restrict the number of connections allowed, thereby preventing new valid tunnels from being set up. This anomaly has been fixed.

Filtering and NAT

Support reference 71283

The following error message is now displayed whenever a filter and NAT policy contains an empty port group: The *Group_Name* port group used in this rule is empty.

SN2100 and SN3100 - 1 Gigabit/s interfaces

Support reference 71672

The presence of unconnected 1 Gigabit/s network interfaces would cause the excessive consumption of CPU resources on SN2100 and SN3100 firewall models. This issue has been fixed by updating the driver on these interfaces.

IPsec VPN

Support reference 71858

In IPsec configurations where one tunnel endpoint offered Phase 2 AES and AES_GCM_16 encryption algorithms, and the other endpoint offered only AES_GCM_16, tunnels could not be negotiated. This issue has been fixed.

Captive portal - Conditions of use for Internet access

Support reference 69176

The conditions of use for Internet access displayed on the captive portal, specifically for guest authentication methods, could not be accepted on iOS mobile devices. This issue has been fixed.

SNMP

Support reference 72116

Bandwidth information regarding 10 Gigabit/s interfaces was not correctly reflected in the *ifSpeed* and *ifHighSpeed* OIDs. This anomaly has been fixed.

Support reference 71972

As the snsUptime object is duplicated in the Stormshield-SYSTEM-MONITOR and Stormshield-HA MIBs, requests to this object would not return any results. This object has since been renamed "snsHA Uptime" in the Stormshield-HA MIB to work around this issue.

Support reference 71886

The ranges of values defined for the snsNodeIndex and snsIfIndex objects in the Stormshield-HA MIB were wrong. These anomalies have been fixed.

Support reference 69010

The wrong syntax in the snsQosEntryIndex object (MIB Stormshield-QOS) would prevent some monitoring tools from querying this MIB correctly. This anomaly has been fixed.

SSL proxy

Support reference 72663

The SSL proxy would wrongly consider some certificates invalid and proceed to block access to the corresponding websites. This issue has been fixed.

GRETAP interfaces

Support reference 69981

In configurations using GRETAP tunnels that meet the following conditions:

- One of the tunnel endpoints is an SN310 firewall,
- A VLAN is attached to the GRETAP interfaces that carry the tunnel,
- The GRETAP interface is a member of a bridge,
- The **Keep VLAN IDs** option has been enabled on all interfaces belonging to this bridge.

On SN310 models, outgoing traffic on the physical interface would be corrupted (zero-checksum packets) and rejected by the remote firewall.

Automatic backups

Support reference 72131

During automatic backups to a customized server, if the server's response contained the HTTP 204 return code (*No Content*), this response would be misinterpreted as an error and would generate the system event 87 "Backup failed". However, the backup file would be saved on the server. This misinterpretation of the HTTP 204 return code has been fixed.

Virtual machines

After an EVA has been reset to its factory settings (*defaultconfig*), the initial connection to its web administration interface would result in a failure to load the firewall's configuration. This issue has been fixed.

IPsec logs (IKEv2 only or IKEv1 + IKEv2)

Support reference 73155

Some IPsec log entries (l_vpn file) would not contain the source (src) and destination (dst) fields. This anomaly has been fixed.

Network

VLAN attached to a GRETAP interface

Support reference 72961

On VLANs attached to a GRETAP interface, their MTUs would be set to an incorrect value every time the firewall was restarted. This issue has been fixed.

Web administration interface

Logs

Support reference 71615

Log lines could no longer be copied to the clipboard whenever they were selected. This anomaly has been fixed.

Logs - Geolocation

Whenever a user scrolls over the flag of a source or destination country, the tooltip would display the name of the country or the country code, depending on the log selected. The tooltip now shows both in the format Country name (country code). Do note that the country code is the criterion for filter/search functions.

Notifications

Support reference 59495

The wrong value of the field specifying the interface on which an alarm was raised would be indicated in the HTML report sent by e-mail. This anomaly has been fixed.

Monitoring - SSL VPN tunnels

Support reference 72046

Users would not be able to log off via the right-click menu, and attempting to do so would generate a system error message. This anomaly has been fixed.

Support reference 72048

Searches in the logs of users who have logged on via SSL VPN would not return any results. This issue has been fixed.

System events

Support reference 71337

Whenever a line containing special characters was dragged and dropped to a filter or search zone, these characters would be encoded and distort the filter. This anomaly has been fixed.

Stormshield Network Real-Time Monitor

Support reference 72564

Connecting SN Real-Time Monitor to a firewall that used whitelists/blacklists would cause the monitoring application to immediately shut down. This issue has been fixed.

Resolved vulnerability from version 3.8.1

OpenSSL: Possible disclosure of information

The following vulnerability has been fixed by the update of OpenSSL:

- CVE-2019-1559 (*Unauthorized disclosure of information*).

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

CURL update

The following vulnerabilities have been fixed by the update of CURL:

- CVE-2019-3822,
- CVE-2018-16839,
- CVE-2018-16842,
- CVE-2018-1000120,
- CVE-2018-1000121,
- CVE-2018-1000122,
- CVE-2018-1000300,
- CVE-2018-16890,
- CVE-2017-2629,
- CVE-2017-7468,
- CVE-2017-8816,
- CVE-2017-8817,
- CVE-2017-8818,
- CVE-2017-1000101,
- CVE-2017-1000100,
- CVE-2017-1000254,
- CVE-2016-8619,
- CVE-2016-8618,
- CVE-2016-8616,
- CVE-2016-9586,
- CVE-2016-9594,
- CVE-2016-5419,
- CVE-2016-5420,
- CVE-2016-7167,
- CVE-2016-8622,
- CVE-2016-0755,
- CVE-2016-8615,
- CVE-2016-8624,
- CVE-2016-8625,
- CVE-2016-5421,

- CVE-2015-3236,
- CVE-2015-3237.

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

Version 3.8.1 bug fixes

Network

Wi-Fi

Support reference 71139

WiFi firewall models no longer randomly freeze whenever the Wi-Fi network is enabled.

Protocol

Support reference 71349

If a maximum value is specified for the size of an IP packet (MTU) on a given bridge, and the option **Keep initial routing** has been enabled, this MTU will apply only to this bridge from now on. The interfaces outside the bridge will keep their own MTU values.

Large-scale sending of requests to external IP addresses

Support reference 72329

Infected hosts behind protected interfaces will no longer cause a drastic drop in performance or the sudden shutdown of the firewall whenever they launch SYN flooding attacks to a large number of external IP addresses.

System

High Availability - switch

Support references 71639 - 71681

Whenever the active firewall in the cluster fails, high availability links that freeze would prevent the passive firewall from responding and taking over. This issue has been fixed.

The switch from one cluster node to the other in a configuration that does not have any proxies enabled will no longer cause the *"proxy daemon shutdown"* log to be sent every 5 seconds in system events.

High availability - manual commands

There is no longer any latency in a cluster whenever you restart an active node or when you force the switch to the passive node. These actions now have immediate effect.

SN2100 and SN3100 - 1 Gigabit/s interfaces

Support reference 71672

The presence of unconnected 1 Gigabit/s network interfaces would cause the excessive consumption of CPU resources on SN2100 and SN3100 firewall models. This issue has been fixed by updating the driver on these interfaces.

Firewalls with IXL cards

The two fixes below affect firewalls that use IXL cards, in particular:

- Fiber 4x10Gbps and 2x40Gbps network extension modules for SN2100, SN3100 and SN6100 models,
- 4x10GBASE-T modules for SN710, SN910, SN2000, SN2100, SN3000, SN3100 and SN6100.
- Both fiber 10Gbps onboard ports on SN6100 models.

Whenever the active node is lost in a firewall cluster that uses an IXL card, the other node will now take over immediately. Furthermore, after the switch, traffic will no longer be redirected regularly to the passive firewall.

Issues with traffic control that would stop traffic on firewalls with an IXL card have been fixed.

IPsec VPN

Support reference 71942

The IPsec VPN service would wrongly interpret certain X.509 certificate formats on smartcards, and would restart whenever a user attempted to set up a tunnel. This issue has been fixed.

Support reference 72797

During an IPsec VPN authentication, the list of LDAP groups to which a user belongs will no longer be truncated if it exceeds 250 characters. The full list will now be taken into account within a limit of 4096 characters.

SN310 firewall performance

An issue regarding the regression of performance on SN310 firewall models has been fixed.

Virtual machines

After an EVA has been reset to its factory settings (*defaultconfig*), the right access privileges to the web administration interface will be granted and will no longer prevent the connection.

Support reference 72352

Network packets that can be retrieved via alarms in the web administration interface can now be opened correctly.

New features in version 3.8.0

Virtual machines

Stormshield Network EVA

Version 3.8.0 of the firmware ensures compatibility with new virtual firewalls in the Elastic Virtual Appliance (EVA) range.

These firewalls automatically adapt their limits (number of connections, IPsec tunnels, etc.) according to the amount of memory allocated to the instance. They therefore allow scaling the amount of RAM used and the number of virtual processors (vCPU) according to the following values:

- EVA1: up to 2 GB of RAM and 1vCPU.
- EVA2: up to 3 GB of RAM and 2vCPU.
- EVA3: up to 6 GB of RAM and 4vCPU.
- EVA4: up to 8 GB of RAM and 4vCPU.
- EVAU: up to 64 GB of RAM and 16vCPU.

Whenever the capacity of an EVA's memory is modified, it generates a system event as well as an entry in the system log file (*l_system* file) in order to inform the administrator of any changes to the model, and license as a result.

Do note that in a factory configuration (new installation or reset to factory settings using the command `defaultconfig`), EVAs have two routed network interfaces (not together in a bridge). Furthermore, both of these interfaces are configured in DHCP by default.

For further information on how to install an EVA firewall or on upgrading a V / VS-VU model to an EVA model, refer to the EVA - Installation guide.

V and VS-VU range virtual firewalls support only 3.8.x versions in view of an upgrade to the EVA range.

Instantiation of virtual machines

The creation of virtual machines can be automated using a disk image that was read the first time the virtual firewall was started.

This disk image contains at least one "user-data" file that includes the super-user's password (*admin* account) and the name of the host that needs to be assigned to the firewall. The image may also include a *shell* script (named *script.sh*) or an *nsrpc* script (named *script.nsrpc*) in order to add extra automatic configuration parameters (adding filter rules, etc.).

Hardware

Stormshield Network SN710, SN910, SN2000 and SN3000

These firewall models support cards for 4 copper 10 Gigabit Ethernet ports (only in automatic media detection mode).

Intrusion prevention

The mechanism that detects and blocks SYN Flood attacks that target hosts in the internal network can be extended to protect the firewall's internal services. In this case, the firewall will

generate specific logs that allow logging denial of service attempts by way of such attacks.

To enable this additional protection, implicit rules to the firewall's internal services must be disabled and replaced with equivalent explicit rules.

For more explanations on how to implement this protection, please refer to the relevant article in the Stormshield Knowledge Base.

SSL protocol

An additional action is available for the configuration of the SSL protocol analysis (**Application protection** > **Protocols** > **SSL** > **Proxy** tab): *Delegate to user*.

This action forces the client's browser to present a security alarm in order to inform the user of any potential risks. Users bear the responsibility of disregarding the alarm if they wish to access the requested website anyway.

In such cases, the administrator will be informed when an alarm is raised and a specific entry is written in the alarm log file (*l_alarm*).

The technical note Configuring HTTPS filtering was updated to include the description of this new operating mode.

NTP

The analysis for this protocol has been extended. The NTP protocol configuration module now makes it possible to either analyze or block one or several versions of NTP (v1, v2, v3 and v4). For each version of the protocol analyzed, a dedicated tab offers the possibility of allowing or blocking specific NTP commands.

Protocol whitelist

A whitelist of protocols that do not need to be analyzed by the intrusion prevention engine has been added. This list can only be loaded in command line (**System** > **CLI console** module) using the following command:

```
CONFIG PROTOCOL IP COMMON IPS CONFIG UnanalyzedIpProto="list_of_protocol_numbers"
```

The protocol numbers are available on the IANA website (Internet Assigned Numbers Authority).

Do note that this list contains VRRP (112) and SCTP (132) protocols by default. To show the contents of the list, use the command:

```
CONFIG PROTOCOL IP COMMON SHOW
```

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

Network

MAC address management has been changed in version 3.8.0 in order to fix issues encountered when certain advanced interface configurations are applied.

As such, Stormshield now applies stricter use of *promiscuous* mode.

These changes may affect the behavior of the following configurations:

- Ethernet interface with at least one VLAN on which the MAC address has been forced [1],
- Disabled Ethernet interface with one or several VLAN(s),

- Ethernet interface with one or several VLANs included in a bridge,
- HA interface with one or several VLANs.

[1] High availability forces MAC addresses on one of the members of the cluster.

If any of these configurations concerns you, check that all your network devices use your firewall's real MAC address.

For further information, please refer to this article in the Stormshield Knowledge Base.

System

Trusted certification authorities

The number of built-in root certification authorities on firewalls has been significantly increased. The size of the /var partition on SN210(W), SN310, SN510, SN710 and SNi40 models has therefore been increased as a result.

IPsec VPN

From version 3.8.0 onwards, mobile IPsec policies containing several peers can be built as long as they use the same IKE encryption profile.

In certificate-based authentication, the certificates of the various peers must be issued by the same CA,

IPsec VPN - IKEv2

Support for the OCSP protocol has been introduced in version 3.8.0, to verify certificates used in setting up IKEv2 tunnels.

IPsec VPN (IKEv2 and IKEv1 + IKEv2)

Mobile users (anonymous peers) can simultaneously set up several IPsec tunnels with a firewall by authenticating on different domains (directories). User groups can also be specified on these domains (optional).

A mobile user can therefore simultaneously set up a tunnel to a specific network as a member of the *Administrators* group on the domain Domain1.org, and a tunnel to a particular host as a member of the *Users* group on the domain Domain2.org.

Maintenance

Initialized virtual machines in the V, VS and VU ranges allow the installation of a new initialization pack so that they can be upgraded to virtual machines in the EVA range.

SSL VPN

The level of security implemented during the negotiation and use of SSL VPN tunnels has been raised:

- Stronger authentication and encryption algorithms:
  - SHA256,
  - ECDHE-RSA-AES128-SHA256,
  - AES-256-CBC (except on SN160(W), SN210(W) and SN310 firewalls, which continue to use AES-128-CBC).
- LZ4-based data compression (can be enabled or disabled),

- Strict verification of certificates presented by the server (certificate name and "server" certificates).

If you are not using the Stormshield VPN SSL client, you must:

- Work with OpenVPN clients in a recent version (2.4.x) or OpenVPN Connect (smartphones and tablets),
- Download the configuration of the client again from the captive portal of the firewall that hosts the SSL VPN.

LCD display

On firewalls that have LCD screens on their front panels (SN910 and SN6000), the system command (**System** > **CLI console** module) `CONFIG LCD state=on/off` makes it possible to enable or disable the display of information on the LCD screen.

Stormshield Management Center

After the installation of the connecting package, the addresses for connecting to SMC servers can be managed through the following system commands (**System** > **CLI console** module):

```
config fwadmin contact add | remove | list.
```

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

Logs (Audit logs) - IPsec VPN

The name assigned to an IPsec rule is displayed in the IPsec VPN log file (*l_vpn* file) for better readability. If no name has been assigned to a rule, it will be identified in the log file by an MD5 hash made up of the various components of the rule (local network, remote network, peer, etc.).

Reminder: the name of an IPsec rule can only be defined in command line (**System** > **CLI console** module) with the following commands:

- `CONFIG IPSEC POLICY GATEWAY add,`
- `CONFIG IPSEC POLICY GATEWAY update,`
- `CONFIG IPSEC POLICY MOBILE add,`
- `CONFIG IPSEC POLICY MOBILE update.`

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

Logs (Audit logs) - System events

Two events have been created to track SSH connections to the firewall: one event for successful connections and another for failed connections. These events can be seen in the system event log (*l_system* file).

Proxies

The firewall's proxy supports the *HTTP PATCH* method described in the RFC 5789.

Web administration interface

Right-click pop-up menu

The actions displayed in the toolbar can also be accessed by right-clicking in modules that display data grids:

- System: **Administrators**,
- Network: **Virtual interfaces**, **Routing**, **Multicast routing** and **DHCP**,
- Objects: **Network objects**,
- Users: **Users**, **Access privileges** and **Authentication**,
- Security policy: **Filter - NAT**, **URL filtering**, **SSL filtering** and **SMTP filtering**,
- Application protection: **Host reputation**, (**Hosts** tab) and **Antispam**,
- Notifications: **Monitoring configuration**;

Filter - NAT

A **Protocol** column has been added to the **NAT** tab to facilitate the definition of address translation rules on a full protocol.

Logs - Syslog - IPFIX (Local storage tab)

The field **Action required if storage device is saturated** is no longer available.
If a storage device is full, the most recent logs automatically erase the oldest logs.

Logs (Audit logs)

A "Yesterday" time range has been added to the search criteria in the **Views** and **Logs** modules.

Logs (Audit logs) - Alarms

A pop-up menu (right-click) has been added to alarm logs (**Captured packet** column) to enable the export of the captured network packet in *pcap* format.

Do note that to start capturing packets, the checkbox **Capture the packet that raised the alarm** must be selected in the configuration of the alarm in question (**Application protection** > **Applications and protections** module > **Advanced** column > click on **Configure**).

Logs (Audit logs) - Alarms - Vulnerabilities

A pop-up menu (right-click) has been added to alarm and vulnerability logs in order to display online help for the selected alarm or vulnerability.

Logs (Audit logs) and Monitoring

A tooltip showing additional information appears when the user scrolls over a host or a port:

- Host: Name, IP address, Operating system, Number of vulnerabilities detected, Reputation score, Bytes received, Bytes sent, Incoming throughput, Outgoing throughput, Input interface and MAC address.
- Port: Name, Port number or Port range, Protocol and Comments (if any).

Dashboard

For EVA models, information regarding the amount of memory currently used and the maximum amount of memory that can be used (if the amount of memory allocated to the virtual machine has been increased) has been added to the **Properties** widget in the **Dashboard**.

Resolved vulnerabilities from version 3.8.0

XSS flaw

A vulnerability that could potentially affect command input in the CLI console module of the web administration interface has been fixed.

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

Version 3.8.0 bug fixes

Network

Interfaces

Support reference 69982

The advanced configuration option **Keep VLAN IDs** (for interfaces included in a bridge), which instructs the firewall to accept tagged packets on this interface even when the VLANs concerned have not been explicitly declared, no longer functioned. This issue has been fixed.

Dynamic routing - Router objects

Support references 65524 - 69210 - 70135

Whenever a firewall's default gateway consisted of a router object with load balancing, the dynamic routes that the Bird engine had learned would not be applied. This issue has been fixed.

Static multicast routing

Support reference 70211

A restriction on queue size management in multicast static routing would cause the loss of multicast packets. The size of these queues can now be configured using the command:

```
CONFIG SMCROUTING UPDATE UpcallQueueLimit = <queue_size>
```

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

VLAN attached to a link aggregate

Support references 67337 - 65108

Whenever VLANs were attached to a link aggregate in any of the following configurations:

- Inactive aggregate (configured to accept only traffic bearing the tag of the child VLAN over the aggregate),
- Aggregate with a forced MAC address, even when the VLAN is not in *promiscuous* mode.

Such VLANs would not function. This issue has been fixed.

Support reference 67698

Whenever VLANs attached to a link aggregate were moved to another link aggregate, the MAC address of such VLANs would be forced to 00:00:00:00:00:00 and the VLANs would not function. This issue has been fixed.

Support reference 67516

In a HA cluster with **Periodically send gratuitous ARP requests** option enabled, whenever VLANs attached to a link aggregate were moved to another link aggregate, the MAC address inside the ARP packets would be wrong and the VLANs would not function. This issue has been fixed.

Quality of Service (QoS) - GRE interfaces

Support references 67640 - 69253 - 69316

QoS rules defined in the **Security policy** > **Quality of service** module would never be applied to traffic passing through GRE interfaces. This issue has been fixed.

GRE interfaces

Support reference 71499

It was not possible to set up TCP connections to or from an SNS firewall through a GRE tunnel. This issue has been fixed.

System

Proxies

Support reference 69318

An incident of memory corruption during the use of the SSL proxy would disrupt web access. This issue has been fixed.

Support references 66101 - 64504 - 69005 - 69328

An issue regarding competing access to certain resources used by the OpenSSL module would cause the proxy to freeze. This issue has been fixed.

IPsec VPN

Support reference 70910

In configurations that use virtual IPsec interfaces, an issue with competing access to certain Security Policy parameters would disrupt traffic inside established IPsec tunnels. This issue has been fixed.

IPsec VPN (IKEv1 + IKEv2 or IKEv2 only)

Support reference 70250

An anomaly in the management of Security Associations (SA) during the loss of packets within a tunnel would wrongly generate many child SAs and increase the load on the engine that manages IPsec IKEv2 / IKEv1+IKEv2 tunnels. This anomaly has been fixed.

IPsec VPN - IKEv2

Support reference 70250

In order to prevent the multiplication of inactive child Security Associations (SA) that would increase the load on the engine that manages IPsec IKEv2 tunnels, the maximum lifetime of SAs that no longer send and receive any traffic can be configured using the command (**System** > **CLI Console** module):

```
CONFIG IPSEC PEER NEW
```

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

Captive portal - Sponsorship

Support reference 67894

Whenever the sponsorship authentication method was configured to display a disclaimer page, it would not be displayed during the sponsorship request, and the requester would never see it. This anomaly has been fixed and the disclaimer page is now displayed as soon as a sponsorship request is submitted.

Support reference 70007

An anomaly in the management of sponsorship requests would wrongly cause the detection of a brute force attack and block the requester. This anomaly has been fixed.

Captive portal - SSL VPN - Web administration interface

Support reference 70568

Receiving a non-compliant request could cause the authentication portal management mechanism, SSL VPN and the web administration interface to freeze. This issue has been fixed.

Firewall administration

Support reference 71741

In cases where the administrator password of a firewall was forgotten, if both passwords entered during the password retrieval procedure did not match, the configuration of the firewall would be erased. This issue has been fixed.

Web enrollment

Support reference 54754

Web enrollment with certificate creation was supported only for users logged on to the authentication portal using Mozilla Firefox. This anomaly has been fixed and Microsoft Internet Explorer, Microsoft Edge and Google Chrome are now supported.

High availability and IPsec VPN (IKEv1 + IKEv2 or IKEv2 only)

Support reference 68832

During the reconstruction of a cluster after the physical replacement of the passive firewall, and whenever the quality of the active firewall was lower than the quality of the new passive firewall, established IPsec tunnels would be renegotiated. This issue has been fixed.

High availability - Incident icon

Support references 70506 - 70880

As the high availability (HA) monitoring mechanism takes into account the status of links to router objects, unreachable router objects would wrongly cause the display of an icon indicating an incident on HA links in the firewall cluster. This anomaly has been fixed.

Notifications - E-mail alerts

Support reference 69100

An anomaly in the encoding of the SMTP configuration test e-mail would raise the alarm "Incorrect end of line in SMTP" (blocks packets by default) if the SMTP protocol analysis was enabled. This anomaly has been fixed.

Local storage

Support reference 68506 - 71005

Firewalls with damaged SD cards (and therefore damaged log storage partitions) would restart in loop. This issue has been fixed.

Vulnerability Manager

Support references 58546 - 66338 - 66736 - 68741 - 69083 - 70153 - 66482

The vulnerability management module no longer functioned on SN150, SN160(W), SN210(W) and SN310 firewall models and could cause the firewall to freeze. This issue has been fixed.

USB over Ethernet modem

Support reference 65697

When restarting a U30S or SN200 firewall, the detection of the USB over Ethernet modem would take too long and no IP address would be assigned to the modem. Network services on the firewall therefore needed to be manually rerun (`ennetwork` command). This anomaly has been fixed.

Antispam

Support reference 69307

A flaw in the operation of the domain name blacklist would wrongly classify legitimate e-mails as spam. This anomaly has been fixed.

Filter - NAT

Support references 69146 - 69011

Adding or deleting an inactive filter rule or a rule containing an empty group in front of a rule that uses the proxy (URL filtering, antivirus, sandboxing, etc.) would skew filter rule IDs. This skew would in turn cause web access to malfunction. This issue has been fixed.

Stormshield Management Center

Ever since version 3.6.1 of SNS, the firewall would no longer factor in the fact that a particular network interface has been specified for connections to the SMC server (BindAddr parameter). This issue has been fixed.

URL filtering - Stormshield Management Center

In configurations that use the URL filter database compiled by the *Rectorat de Toulouse* (Academy of Toulouse – refer to the article in the Stormshield knowledge base), and whenever

the administrator was logged on to the firewall via an SMC server, the **Add all predefined categories** button (**Security policy > URL filtering** module) would return an HTTP error message. This anomaly has been fixed.

SSO agent - Nested groups

Support references 66905 - 66350 - 67257 - 69977

Enabling nested groups (**Users** > **Directory configuration** > **Advanced properties**) in a Microsoft Active Directory combined with the SSO agent authentication method would cause excessive memory consumption and could prevent connections to the firewall's web administration interface and captive portal. This issue has been fixed.

Command line

Support reference 68861

The system command `ennetwork -v` would require an argument for which no default value was assigned, unlike what was indicated in command help. This anomaly has been fixed and the value DEBUG is now assigned to this argument whenever no value has been explicitly specified.

SNMP

Support reference 70258

Querying OIDs that correspond to the firewall's network interfaces would cause the firewall's SNMP server to consume too much memory. This anomaly has been fixed.

LDAP directories

Support reference 69872

During the configuration of a Microsoft Active Directory with secure SSL access, an error message "No LDAP configuration" would appear by mistake. Confirming this message and refreshing the screen would remove the directory concerned from the list of directories. This anomaly has been fixed.

Alarms on SN3000 firewalls

Support references 71022 - 71051

On SN3000 firewalls, an alarm indicating a power supply failure would appear on the dashboard even though the firewall would be running properly. This anomaly has been fixed.

Intrusion prevention

SIP

Support reference 68583

The firewall would not take into account the optional fields Record-Route and Route, which can be added by SIP proxies. The addresses and routes indicated in these fields would therefore not be translated when necessary. This anomaly has been fixed.

Support reference 66573

As certain SIP telephones do not specify the network port number used (Contact field in the REGISTER request), the firewall would not correctly redirect incoming REGISTER requests formed in this manner. This anomaly has been fixed.

SNMP

Support reference 68686

Enabling intrusion prevention analysis on the SNMP protocol would cause the excessive consumption of processing resources on the firewall and slow down all network traffic passing through this firewall. This anomaly has been fixed.

LDAP protocol

Support references 71152 - 69806

The analysis of the LDAP protocol would wrongly raise the alarm *ldap_tcp:427* (*Bad LDAP protocol*) and block connections to the target LDAP directory. This anomaly has been fixed.

Support reference 71192

An issue during the analysis of LDAP packets that authenticate via SASL (Simple Authentication and Security Layer) would cause the firewall to freeze. This issue has been fixed.

Software Restoration via USB key

Support reference 68227

SN6000 model firewalls

The internal disk detection method used during a USB recovery would not function on SN6000 firewalls. This anomaly has been fixed.

Web administration interface

Support reference 69237

An issue that slowed down the display of the web administration interface, and which could cause the engine that manages these administration pages to freeze, has been fixed.

Users

Support reference 68972

Displaying users or groups that belong to very large directories (thousands of objects) would sometimes require several minutes or would not even succeed. This issue has been fixed.

Static routing

Support references 65971 - 67347 - 70135

Adding a static route by specifying the destination network first instead of the interface would cause the error message "interface not found" to appear. This issue has been fixed.

Filter - NAT

In a configuration:

- Using several rule separators,
- With a separator placed at the top of the filter or NAT policy.

Whenever all separators were collapsed, deleting the separator at the top would not delete the filter or NAT rules placed under this separator. This anomaly has been fixed.

Administration privileges

Support reference 68691

Users with administration privileges would not be able to modify certain parameters such as DNS or NTP configuration. This anomaly has been fixed.

Administrators

Support references 68888 - 70656

Administrator accounts with names that contained special characters such as uppercase characters would not appear in the list of administrators after being added. This issue has been fixed.

Temporary accounts

The button to export the list of temporary accounts would not function with Microsoft Edge. This issue has been fixed.

Logs - Audit logs

The button to export the contents of audit logs would not function with Microsoft Edge and would log the user off the administration interface. This issue has been fixed.

The hashes of captured network packets (configuration via advanced alarm options) would not be anonymized whenever the administrator only had restricted access to logs. This anomaly has been fixed.

Network objects

Support references 67681 - 68079

After application of the Host or Network filter, the order in which displayed objects were sorted in the IPv4 or IPv6 column would be wrong (sorted by characters that make up the IP address instead of in numerical order). This anomaly has been fixed.

Captive portal

Support reference 68872

In the **Users** > **Authentication** module > **Captive portal** > **Advanced properties** tab, even when a network object has been selected for the **Port on the captive portal** field, this field would show a numerical value and would be wrongly indicated as an anomaly. This issue has been fixed.

Virtual machines

Log partition

Support references 61281 - 69313

On Openstack-based virtualization or hosting platforms (Xen Server, KVM, Cloudwatt, etc.), the virtual firewall's log partition would sometimes not be detected and the **Logs - Audit logs** menu would then be hidden. This issue has been fixed.

Xen Server - "Live migrate" function

Support reference 60867

The use of the Live migrate function, which allows hot-transferring a virtual firewall from a Xen server to another, would cause a system error and make the firewall restart.

Version 3.7 LTSB

Long-Term Support Branch

Version 3.7 LTSB (for Long-Term Support Branch) of SNS has its own set of dedicated Release Notes.

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

For more information, refer to the documents in the section **Product** > **Product Life Cycle** on MyStormshield.

Version 3.7.1 bug fixes

System

Local storage

Support reference 68506

Firewalls with damaged SD cards (and therefore damaged log storage partitions) would restart in loop. This issue has been fixed.

Vulnerability Manager

Support references 58546 - 66338 - 66736 - 68741 - 69083 - 70153

The vulnerability management module no longer functioned on SN150, SN160(W), SN210(W) and SN310 firewall models and could cause the firewall to freeze. This issue has been fixed.

URL filtering - SMC

In configurations that use the URL filter database compiled by the *Rectorat de Toulouse* (Academy of Toulouse – refer to the article in the Stormshield knowledge base), and whenever the administrator was logged on to the firewall via an SMC server, the **Add all predefined categories** button (**Security policy > URL filtering** module) would return an HTTP error message. This anomaly has been fixed.

Captive portal - SSL VPN - Web administration interface

Support reference 70568

Receiving a non-compliant request could cause the authentication portal management mechanism, SSL VPN and the web administration interface to freeze. This issue has been fixed.

Intrusion prevention

TLS protocol

Support reference 70674

The absence of certain encryption suites in the implementation of the TLS 1.3 protocol would raise the "Draft version detected" (ssl:419) alarm, which blocks packets by default. This alarm would prevent connections to websites such as Gmail and Facebook.

The ssl:419 alarm has therefore been modified to detect versions of TLS that the intrusion prevention engine does not manage ("Unsupported version detected") and its default action has been switched to "Pass", except for "High" security inspection profiles.

New features in version 3.7.0

Long Time Support Branch

Version 3.7 has been selected as a Long-Time Support Branch (LTSB) version. Please refer to the *Product Life Cycle* document on Mystormshield for further information.

Hardware

Stormshield Network SN2100, SN3100 and SN6100

Version 3.7.0 of the firmware ensures compatibility with new firewall models SN2100, SN3100 and SN6100. These firewalls support cards for 4 copper 10 Gigabit Ethernet ports (only in automatic media detection mode).

System

SNMP agent

A new OID has been added to the MIBS STORMSHIELD-SYSTEM-MONITOR-MIB and STORMSHIELD-HA-MIB in order to reflect the status of the second power supply unit on SN3000, SN3100, SN6000, SN6100 and SN2100 firewall models (optional redundant power supply). Download them from https://www.stormshield.com/products-services/services/mibs/.

SSL protocol

Encryption suites with a weak level of security (MD5, SHA1 and DES) are no longer available for the SSL protocol used by the various firewall components (SSL VPN, SSL proxy, etc.). Please refer to the Recommendations before updating your firewall to version 3.7.0.

Web administration interface

Audit logs

Clicking on a line in a log or view will automatically display details of the line in a window to the right of the module **Logs / Audit logs**. Buttons now make it possible to hide (») or show («) this window.

Version 3.7.0 bug fixes

Hardware

Support references 70452 - 70242

On standard SN2100 model firewalls (sold by default with a single disk, but eligible for the RAID option) or on models without RAID option, the results of S.M.A.R.T tests would show an alert message regarding the absence of the second disk.

It is therefore recommended that you update the firmware on SN2100 model firewalls to version 3.7.0 in order to stop this message from appearing if you have not subscribed to the RAID option.

System

IPsec VPN - IKEv2 - Mobile tunnels

Support reference 69737

Setting up a very large number of mobile IPsec IKEv2 tunnels (about 17000 tunnels) would cause the SAD (Security Association Database) and SPD (Security Policy Database) to desynchronize, blocking traffic between these tunnels as a result. This issue has been fixed.

Stormshield Management Center

Support reference 68469

Whenever SMC servers set up connections to the web administration interface of a firewall for which the firmware does not appear in the SMC database, the firewall would generate a local archive of this administration interface in order to forward it to the server.

On small firewall models (SN150), such archives could saturate storage space. These archives are now created in memory before being forwarded to the server.

High availability

Support references 69112 - 69141

During the migration of a firewall cluster in an SNS 2.X version to an SNS 3.5.1 version or higher, the firewall that switched to passive after being updated would not switch back to active during the update of the other member of the cluster. This issue has been fixed.

Router objects

Support references 68887 - 69418

Pings from gateways defined in a router object would mistakenly generate an entry in audit logs whenever such gateways switched from an internal "maybe not reachable" status (pinging failed) to an internal "reachable" status. This anomaly has been fixed.

Network

Management of ARP entries

Support references 69450 - 69312

The ARP entry creation service (e.g., creation of a NAT rule with ARP publication) would shut down as soon as there is a failure while creating an entry. This anomaly has been fixed.

Intrusion prevention

TLS protocol

Support reference 68896

The absence of certain encryption suites during the implementation of the TLS 1.3 protocol would raise "Unauthorized cipher level" alarms. This anomaly has been fixed.

ARP protocol

Support reference 69239

After moving a host, without modifying its IP address, from one interface to another within the same bridge, packets going to this host would always be sent to the previous connection interface (the ARP table would not be updated). This anomaly has been fixed.

TCP protocol - Multipath

Support reference 69908

When TCP packets are received with the multipath option size set to zero:

- in a rule in firewall mode,
- in a rule in IDS or IPS mode with the action of the "Multipath TCP" alarm forced to *Allow*,

the firewall would freeze. This issue has been fixed.

Web administration interface

Inactive rules

Support reference 70084

Whenever a filter or NAT rule was set to inactive (**Status** *off*), field values corresponding to this line (**Source**, **Destination**, etc.) would no longer be grayed out. This anomaly has been fixed.

New features in version 3.6.1

Web administration interface

Audit logs

The **Logs - Audit logs** menu contains the **Views** and **Logs** sections by default. To hide the list of all logs, open the **Preferences** menu in the web administration interface and in the **Log preferences** area, uncheck **Show the "Logs" menu**.

Version 3.6.1 bug fixes

System

Maintenance – Updates

Support reference 69771

Whenever a firewall in version 2.x that had never been in version 3.x before was upgraded to version 3.6.0, the firewall would become inoperable. This issue, which is explained in this article in the Stormshield knowledge base, has been resolved.

New features in version 3.6.0

IPsec VPN - AES-GCM encryption algorithm

The AES-GCM encryption algorithm is now available for IPsec VPN encryption profiles, and has the following characteristics:

- It performs both authentication and encryption,
- It is only supported in IKEv2,
- Whenever it is used, the imposed value of the pseudo-random function (PRF) is SHA2 256, in line with the requirements of the "ANSSI Diffusion Restreinte" mode,
- Encryption performance is closely linked to the firewall's hardware capacities.

Firewall health indicator

SNS provides a system of health indicators in the form of colored icons in the upper banner of the web administration interface. The icon appears only when the firewall has a minor (yellow) or major (red) defect.

The indicator takes into account the status of hardware (e.g., CPU, memory, power, disks, etc.) and high availability. More detailed information can be found by scrolling over the icon.

A new MIB, Stormshield Health Monitor, is also available as a way to monitor this health indicator via SNMP. Download it on https://www.stormshield.com/products-services/services/mibs/.

Monitoring

The following modules have been added to the **Monitoring** menu:

- **DHCP monitoring** which shows the list of all the hosts that have obtained an IP address through the firewall's DHCP server.
- **SSL VPN tunnel monitoring** which shows the list of all users connected to the firewall through an SSL VPN tunnel. A button also offers the possibility of renegotiating the selected tunnel.
- **IPsec VPN tunnel monitoring** which shows IPsec policies that have been defined on the firewall and the corresponding tunnels.
- **Black list / white list monitoring** which shows the hosts that have been quarantined (blacklist) and the hosts allowed to pass through the firewall without being monitored by it (whitelist).

Customized warning message

Customized warning messages can now be added to the authentication page of the web administration interface.

System

High Availability

Warning messages relating to high availability are now displayed in the **Hardware monitoring / High availability** view, making it easier to analyze the status of the cluster.

Kaspersky antivirus

The Kaspersky antivirus engine libraries can now be completely deleted from the firewall via the command *serverd CONFIG ANTIVIRUS ERASEKAV [force=<on|off>]*. **Do note that deleting Kaspersky libraries will prevent the proxy from being used in all cases, even when no antivirus has been enabled.**

Antispam

Antispam databases are now updated only when the antispam is used in a security policy. If you select the antispam in a policy, the log *The antispam base is missing. The antispam feature will not run correctly.* will be generated. When this policy is enabled, the antispam databases will be reloaded and run correctly.

IPsec VPN - IKEv2

The **Do not initiate the tunnel (Responder only)** option is now available for IKEv2 peers. This mode is particularly adapted to the hubs of star configurations, in which only peers set up tunnels.

Intrusion prevention

S7 industrial protocol

The table of predefined operations of the S7 industrial protocol has been updated, making it possible to allow or block additional S7 function codes.

Virtual machines

vSphere deployment wizard

IP parameters and the password of the virtual machine administrator can now be entered in the vSphere deployment wizard. This saves the user from having to open the console to enter such information the first time the virtual machine is started up.

Web administration interface

Filtering

When a new rule is created, a predefined rule name is added automatically. This name is used in order to switch from the **Filter and NAT** view to the **Audit logs** or **Monitoring** view.

If you copy and paste a rule with a comment that was automatically generated, this comment will be updated with the relevant date and connected user.

Command line interface

Scripts spanning several lines can now be run in the **Configuration > System > CLI console** field. This command block may, for example, be generated from a recorded sequence of commands (**Record commands** button).

Dragging and dropping objects

The drag and drop function is now available for FQDN and time objects.

Log filtering

Two new filter criteria are available for the *Received* and *Sent* fields: **Higher than 1 MB**, **Higher than 10 MB**, and **Higher than 100 MB**. In particular, they make it possible to identify the connection that uses the largest amount of resources.

Monitoring - New interactive features

The following actions can now be performed by right-clicking in the monitoring views:

- Adding a host to the blacklist,
- Adding a host to the objects base or to a group.

Users and groups

Whenever monitoring is enabled, scrolling over the name of a user displays complementary information about his connection:

- IP address of the user's workstation,
- Country from which the connection originates,
- Reputation of the connecting host's IP address,
- Bandwidth used,
- MAC address of the connecting host,
- Interface on the firewall through which the user's connection was set up.

A **Users** view is now available in the **Logs - Audit logs** menu. It shows the **Authentication** log which sets out users' authentication actions.

Version 3.6.0 bug fixes

System

Proxies

Support reference 67863

The SSL proxy no longer restarts unexpectedly whenever an HTTP CONNECT method is used through SSL. A page now informs the user of this incompatibility and a log is issued for the administrator.

High availability

Support reference 68680

The high availability system is now more stable as memory leak issues have been fixed.

Support reference 66260

Whenever a high availability cluster is created, MAC addresses will no longer be forced on VLAN interfaces. As such, MAC addresses no longer need to be changed after a VLAN is moved to another parent interface.

SSL VPN

Support references 48232 - 68060

OpenVPN has been upgraded from version 2.2.2 to version 2.4.2.

Certain restrictions affect this new version of OpenVPN. Refer to the section Explanations on usage to find out more.

Support reference 68895

The deployment of an SMC configuration no longer causes all SSL VPN tunnels to shut down.

IPsec VPN

Support reference 67803

Firewall resources are now better managed during denial of service attacks on port 500 when IPsec VPN is used with IKEv2.

SPNEGO SSO authentication

Support reference 68533

Whenever SPNEGO authentication has been configured, the user now directly accesses websites without having to go through the authentication portal, even when the website's URL contains a vertical bar (|).

Notifications

Support references 68105 - 68000

E-mail alerts received due to system events or alarms now indicate the right date.

SNMP agent

Support reference 65557

The OIDs *ifSpeed* and *ifHighSpeed* from the IF-MIB MIB now return the right values for 10 Gbps interfaces.

Filter - NAT

Support reference 68255

The firewall would block return packets whenever the NAT rule had the following characteristics:

- Source translated to a virtual IP address that does not physically belong to the firewall,
- Destination translated to an internal (protected) outgoing interface or one that does not belong to a bridge.

This issue, which would generate the alarm *Packet for destination on the same interface*, has been fixed.

Intrusion prevention

Alarms

Support reference 68466

The occurrence of the alarm 351 *Missing mandatory SDP field in RTSP* would cause traffic to be blocked even when the inspection profile has been configured to let packets through. This issue has been fixed.

OPC industrial protocol

The UUID ISystemActivator that OPC clients/servers use to open secondary connections is now supported correctly. The OPC client/server operating mode is no longer disrupted.

Virtual machines

Starting/shutting down virtual machines

Since version 3.5, virtual machines could no longer be shut down or restarted through the **VM > Power** menu in VMware. This issue has been fixed.

VMware Tools alerts

VMware vSphere alerts offering to update VMware Tools on SNS virtual machines no longer appear.

Network

Wi-Fi

Support references 64593 - 65555-66768

A flaw in the Wi-Fi access point driver could cause the firewall to freeze whenever the Wi-Fi network was enabled. This flaw has been fixed.

Support reference 68102

A recurring issue affecting performance and causing traffic to be blocked due to a large number of FQDN objects has been fixed.

Web administration interface

Drag and drop

During drag and drop operations to move up or down rows (e.g., in the filter rule module), the indicator was not in the right position. This issue has been fixed.

Users

Support reference 68133

In the **Detailed access** tab in the **Users > Access privileges** menu, the **User-User group** drop-down list no longer offers the values *Any user@voucher_users.local.domain*, *Any user@sponsored_users.local.domain*, and *Any user@guest_users.local.domain*, which caused invalid domain errors.

Certificates and PKI

Support reference 68688

Certificates created through SMC now appear in the **Objects > Certificates and PKI** view of a firewall's web administration interface and CRL updates are also retrieved.

Monitoring

Support reference 68787

In the **Real-Time** tab in the **Monitoring > Host monitoring** menu, the **Incoming bandwidth** and **Outgoing bandwidth** columns would no longer display the maximum throughput but the current throughput instead.

Version 3.5.2 bug fixes

System

LDAP directory

Support references 69101 - 69035

On SN150, SN200, SN210, SN300 and SN310 firewalls, after an update from a version lower than 3.5.0, the resolution of user groups in an internal LDAP would no longer function. Any authentication method using groups (e.g., captive portal, IPsec VPN, SSL VPN or SSO agent) would fail. This issue has been fixed.

Certificates and PKI

Support reference 68688

Certificates created through SMC now appear in the **Objects > Certificates and PKI** view of a firewall's web administration interface and CRL updates are also retrieved.

Proxies

A case of memory corruption while using the SSL proxy has been fixed.

Network

Support reference 68102

A recurring issue affecting performance and causing traffic to be blocked due to a large number of FQDN objects has been fixed.

Version 3.5.1 bug fixes

System

Proxies

Support references 54298 - 68753 - 65092

Whenever the Kaspersky antivirus database reloaded, an issue would occur when ongoing analyses are paused, potentially disrupting proxy services (HTTP, SSL, SMTP, POP3 and FTP). This issue has been fixed.

Support references 68254 - 67791

Whenever a website presented certificates containing empty *subject* fields, this would disrupt the proxy's service. This issue has been fixed.

IPsec IKEv1

Support reference 68294

As part of the deployment of IPsec configurations via Stormshield Management Center, negotiations between SNS firewalls through IKEv1 tunnels using certificate authentication would fail. This issue, which generated the message "No peer found" in the IPsec log file (*l_vpn* file), has been fixed.

Dashboard

Support references 68866 - 68877

Loading the dashboard would cause excessive memory consumption in the long run. This anomaly has been fixed.

Network

GRETAP interfaces

Support reference 68068

Multicast network packets encapsulated in GRETAP tunnels would wrongly contain a multicast destination MAC address and would not be able to reach their destinations. This issue has been fixed.

Router objects

Support reference 68798

On SN160(W), SN210(W) and SN310 model firewalls, availability tests to the router object that included a main gateway and backup gateway would consider these gateways inactive. This anomaly has been fixed.

Intrusion prevention

IDS / Firewall mode

Support reference 67621

Whenever connections that required packets to be rewritten used a filter rule in IDS or firewall mode, the desychronization of sequence numbers would cause a flood of packets to arrive on the firewall's loopback0 interface, causing it to hang. This issue has been fixed.

New features in version 3.5.0

Intrusion prevention

Sandboxing

Activity reports and sandboxing analysis logs make it possible to access the page describing the malicious file detected on the Stormshield Breach Fighter portal.

Common industrial protocol (CIP)

SNS firewalls now detect and analyze the CIP (Common Industrial Protocol).

CIP encompasses a comprehensive compilation of messages and services for industrial automation applications including monitoring, security, synchronization, movement, configuration and information. It is implemented in particular in the upper layers of the Ethernet/IP protocol. For more detail, please refer to the SNSv3 user and configuration guide.

UMAS industrial protocol

SNS firewalls now detect and analyze UMAS (Unified Messaging Application Services) function codes. The UMAS protocol is an extension of the Modbus protocol and is the intellectual property of Schneider Electric. For more detail, please refer to the SNSv3 user and configuration guide.

NTP

The NTP analysis has been enriched and now has a dedicated control panel that allows, in particular, analyzing or blocking this protocol's modes and operations (NTPv3 and NTPv4). For more detail, please refer to the SNSv3 user and configuration guide.

SSL protocol

When the server presents an unsolicited client certificate, it will raise a new alarm (by default, packets will not be blocked): "SSL: Unexpected client certificate".

Configuration

Firewall name

Firewall names can now be 127 characters long, instead of 15 previously.

Filter - NAT

"IPsec only" option

Two optional conditions have been added in the **Action** panel in the settings of each filter rule in order to allow packets matching this rule only if they are going out through an IPsec tunnel after being processed by the rule:

- **Force source packets in IPsec** for packets going through the rule from the source to the destination,
- **Force return packets in IPsec** for return packets from a connection matching the rule.

This allows, for example, rejecting packets if the IPsec tunnel has not been configured or if it is inactive.

Authentication

Captive portal - Logout page

For every profile on the captive portal (authentication portal), it is possible to enable a page reserved for logging out. Once the user has authenticated, this page will appear instead of the captive portal while the requested web page opens in a new tab.

VPN

IPsec VPN IKEv2

An option has been added to make it possible to prevent a full re-authentication during the renewal of SAs. In this case, only keys will be renewed in order to avoid potentially losing packets during re-authentication.

Security-wise, this option is less safe since the identity of the peer, and in particular the identity of the CRL, is verified only when the tunnel is initialized and no longer during each renewal of the IKE phase.

This option can only be enabled in command line:

```
config ipsec peer update name=Site_Name reauth=0
```

When you enable it, the following warning message will therefore appear: "When the reauthentication option is disabled, authentication components will be verified only during the initial IKE SA negotiation."

Network

DHCP

The maximum number of IP addresses that the DHCP server could distribute used to be set according to the firewall type (S, M, M-VM, L, XL, XL-VM). It is now specific to each model.

Virtual machines

Monitoring - Watchdog

Virtual firewalls are now equipped with a monitoring mechanism (watchdog) that allows them to restart automatically when the firewall is idle for a specified duration.

Notifications

E-mail alerts

The firewall can now verify the identity of the SMTP server through which notification e-mails are sent. This can only be done when encryption has been enabled, and therefore requires the STARTTLS option on the SMTP server. This verification is based on the certificate that the server presents during encryption.

Web administration interface

Bridge and Wi-Fi interface

WiFi interfaces can now be added to or removed from a bridge by dragging and dropping from the **Network** > **Interfaces** configuration module.

E-mail alerts

A button has been added to the **E-mail alerts** parameter to allow sending test e-mails in order to check the firewall's SMTP configuration.

Version 3.5.0 bug fixes

System

High Availability

Support reference 65701 - 65946

An issue regarding competing access to the high availability tracking file would cause the *syncid* field to be deleted from this file. The absence of this field would then make members of the cluster repeatedly synchronize their configurations. This issue has been fixed.

Support reference 66802

Within a cluster in which members are of varying quality or a priority has been defined, resetting the firewall with the highest priority or level of quality would immediately cause it to recover its role as the active firewall without fully synchronizing all information. This issue has been fixed with the addition of a timeout that allows synchronizing before switching roles. Set by default to 15 seconds, this timeout can only be modified in command line with the commands *CONFIG HA CREATE* and *CONFIG HA UPDATE*. Details of these commands can be found in the *CLI SERVERD Commands Reference Guide*.

Support reference 67553

Following a HA swap, network equipment from other vendors may ignore gratuitous ARP requests sent by the new active member of the SNS cluster due to an anomaly in the format of such requests (RFC 5944). This anomaly has been fixed.

Support reference 67776

The high availability quality indicator would be skewed whenever an SD card was inserted into a member of the cluster. This issue has been fixed.

Support reference 67832

An anomaly in the operation of the high availability tracking mechanism, which would cause excessive memory consumption, has been fixed.

Quality of Service

Support reference 67879

During the setup of bandwidth reservation or restriction (CBQ), the actual bandwidth would be much lower than the configured bandwidth restriction. This issue has been fixed.

Configuration – Network parameters

Support reference 58987

Firewalls for which no DNS servers have been declared to perform their own name resolution would restart in loop whenever a firmware update was applied. This issue has been fixed.

Authentication

Support references 64844 - 65776

An anomaly in the way brute force attack attempts were counted would prevent the authentication of legitimate users. This anomaly has been fixed.

Configuration restoration

Support reference 58925

An anomaly in the verification of configuration restoration files' validity has been fixed.

Filter - NAT

Support reference 67922

In rules that group a large number of objects, attempts to add extra objects (source, destination, port, etc.) would cause the web administration interface to disconnect.

Filter - NAT – Global policy

Support reference 66325

Whenever the port in an explicit HTTP proxy was changed, it would not necessarily be applied when global filter rules were generated. This anomaly has been fixed.

Proxies

Support reference 66653

Whenever the proxy sent packets to an ICAP server through a filter rule in firewall mode, it would cause latency issues during web browsing. This issue has been fixed.

Support reference 67713 - 67924

During the initialization of the SMTP proxy's logging mechanism, checks for the existence of an active filter policy would cause the SMTP proxy to freeze.

SSL VPN – UDP

Support reference 67293

The VPN SSL over UDP service would occasionally fail to function with configurations that have several Internet access gateways or several IP addresses on the same interface. To resolve these issues, a field has been added to the **VPN** > **SSL VPN** module, allowing the definition of a listening IP address on the service over UDP.

Support reference 66315

The **Export the configuration file** button would allow exporting archives that contain the server's configuration. Since such archives cannot be used, they have been replaced with an archive containing the client's typical configuration (SSL VPN CA and server certificate, network configuration for the client and the mobile client), similar to the one available on the authentication portal.

Sandboxing

Support reference 57407

After a firewall has been restarted, files would not always be sent for sandboxing analysis (Breach Fighter). This issue has been fixed.

Network

DHCP relay

Support reference 66767

In configurations that use the DHCP relay, enabling WiFI interfaces would prevent the relay of DHCP requests sent from these WiFi interfaces. This issue has been fixed.

Interfaces

Support reference 58822

In a configuration such as the following:

- Several unprotected interfaces are included in a bridge, and
- A static route leaves one of these unprotected interfaces (other than the first).

The first network packets that need to use the static route would be wrongly sent to the bridge's first unprotected interface.

Even though this issue has been fixed, do note that the case described in this configuration is not supported (cf. **Explanations on usage** > **Network** > **Interfaces**).

Intrusion prevention

HTTP

Support reference 65592

Previously, the HTTP headers "Content-Security-Policy" and "Authorization: NTLM" likely to raise the block alarm "Possible buffer overflow in HTTP request/reply" could only be configured in command line. They have since been added to the control panel of the **Maximum size of HTTP headers** (**Application protection** > **Protocols** > **HTTP** > **Advanced properties**).

Support references 65250 - 65820

Using the implicit HTTP proxy while the option **Apply the NAT rule on scanned traffic** (**Application protection** > **Protocols** > **HTTP** > **Go to global configuration** > **Proxy** menu) was enabled would generate a very large number of error messages to the console port (messages such as "XXX already released without rule YYYY"). Attempts to display such a large number of messages would cause excessive CPU consumption and would cause the firewall to freeze.

ICMP

Support reference 65930

The "Invalid ICMP message" alarm would be wrongly raised whenever legitimate ICMP packets were sent over a firewall with declared IPsec tunnels. This anomaly has been fixed.

S7 protocol

Support reference 67764

Since encrypted S7 traffic cannot be analyzed, packets would be wrongly blocked when an alarm is raised ("S7: response without corresponding request" or "S7: invalid protocol"). This anomaly has been fixed.

Fragmented packets

Support references 66850 - 66719

An anomaly in the management of fragmented packets would wrongly cause the first fragment to be blocked. This anomaly has been fixed.

IDS / Firewall mode

Support reference 65120

In a configuration such as the following:

- The firewall used filter rules in IDS or firewall mode, and
- The transparent HTTP proxy was enabled.

An anomaly in the management of address translation could cause a combination of connections presenting the same source IP address and the same source port. This anomaly has been fixed.

Virtual machines

Microsoft Hyper-V

Support references 66627 - 67132

On a Microsoft Hyper-V platform, virtual machines with several network interfaces could encounter issues enabling their last interfaces after restarting. This issue has been fixed.

Notifications

E-mail alerts

Support references 66708 - 66782

Notification e-mails sent through the STARTTLS protocol would be truncated. This anomaly has been fixed.

SNMP agent

Support reference 67726

The OID *hrStorageType* included in the MIB "HOST-RESOURCES-MIB" would no longer return results to SNMP requests. This anomaly has been fixed.

Hardware

Firewall clock

Support reference 58901

Whenever the battery that manages the firewall's clock malfunctioned, it would adopt a random date every time it started up. If this date was earlier than the validity of the appliance's license, the firewall would repeatedly restart. This anomaly has been fixed.

Web administration interface

Wi-Fi network

Support references 65333 - 68006

The web administration interface would wrongly reject the use of special characters (periods, dashes, etc.) in WiFi network names (SSID). This anomaly has been fixed.

Please be reminded that only the " character is prohibited in this field.

IPsec VPN

Support reference 67688

Whenever a peer ID was defined for an IPsec peer, this ID could no longer be deleted via the web administration interface. This issue has been fixed.

QoS monitoring

Support reference 66587

Data displayed in QoS monitoring curves (real time/history) did not match selected queues. This anomaly has been fixed.

Audit logs

Support reference 66838

Whenever a rule name was specified for a filter rule, this name would not appear in the **Rule name** column in connection logs. This anomaly has been fixed.

Support reference 67018

In **Advanced search** mode, dragging and dropping an IP address from the **Source name** or **Destination name** columns into filter criteria would result in an empty page of data. This anomaly has been fixed.

Certificates

Support references 59271 - 66735 - 64509

After the import of a certificate in PKCS12 format (including the full chain of certification), the certificate would not appear in the list of selectable certificates for an IPsec VPN peer. This anomaly has been fixed.

Logs - Syslog - IPFix

Support reference 67475

The progress bar during the formatting of a removable device (SD card) would not disappear after the completion of the operation. This anomaly has been fixed.

Authentication

Support reference 67256

The *sslvpn* interface could no longer be selected in the table matching authentication profiles to interfaces. This anomaly has been fixed.

Support reference 67587 - 67985

Whenever the **Always display advanced properties** checkbox in the firewall's **Preferences** was not selected, the buttons for selecting the proxy configuration file, logo or style sheet (**Authentication** > **Captive portal** > **Advanced properties** tab) would no longer appear in Mozilla Firefox. This anomaly has been fixed.

Support reference 68097

Title

The term *Debug* would systematically appear in the tab of the browser displaying the web administration interface. This anomaly has been fixed.

Network objects

Support reference 68250

When checking the use of a network object, the information displayed would indicate the line number in the filter policy (therefore including separators) instead of the number of the filter rule using the object. This anomaly has been fixed.

Stormshield Network Real-Time Monitor

"Hosts" view

Support reference 67297

Ever since version 3.3 of SNRTM, statistics on internal hosts that pass through a Stormshield v2 firewall would no longer be displayed. This anomaly has been fixed.
Do note that statistics concerning hosts located behind unprotected interfaces are displayed for firewalls with firmware in versions between 3.0 and 3.2.1.

Version 3.4.3 bug fixes

IPsec VPN

IPsec IKEv1

Support reference 68294

As part of the deployment of IPsec configurations via Stormshield Management Center, negotiations between SNS firewalls through IKEv1 tunnels using certificate authentication would fail. This issue, which generated the message "No peer found" in the IPsec log file (*l_vpn* file), has been fixed.

This fix is available only for this version and the following 3.4.x versions. When it is added to a 3.5.x version or a higher version, the relevant version Release Notes will specifically mention it.

System

Quality of Service

Support reference 67879

During the setup of bandwidth reservation or restriction (CBQ), the actual bandwidth would be much lower than the configured bandwidth restriction. This issue has been fixed.

Proxies

Support reference 66653

Whenever the proxy sent packets to an ICAP server through a filter rule in firewall mode, it would cause latency issues during web browsing. This issue has been fixed.

SMTP proxy - SSL proxy

Support reference 68581

During the initialization of the SMTP proxy's logging mechanism, checks for the existence of an active filter policy would cause the SMTP proxy to freeze, and connections through the SSL proxy to slow down. This issue has been fixed.

Intrusion prevention

Fragmented packets

Support references 66850 - 66719

An anomaly in the management of fragmented packets would wrongly cause the first fragment to be blocked. This anomaly has been fixed.

Virtual machines

Microsoft Hyper-V

Support references 66627 - 67132

On a Microsoft Hyper-V platform, virtual machines with several network interfaces could encounter issues enabling their last interfaces after restarting. This issue has been fixed.

Resolved vulnerabilities from version 3.4.2

ClamAV

A set of vulnerabilities has been fixed by upgrading the ClamAV antiviral engine:

- CVE-2012-6706
- CVE-2017-6419
- CVE-2017-11423
- CVE-2018-1000085

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

Version 3.4.2 bug fixes

System

IPsec VPN

Support references 67782 - 67901

IPsec tunnels that rely on certificate-based authentication are now managed differently to prevent such tunnels from being systematically renegotiated whenever a VPN topology is deployed via Stormshield Management Center.

Support reference 67694

Users belonging to groups with names that contain uppercase letters are now taken into account in filter rules relating to traffic encapsulated in IPsec tunnels.

Authentication

Support reference 60425

Enabling the SPNEGO authentication method on an SN150 firewall no longer causes the authentication manager to freeze.

Automatic backups

Support reference 67730

Automatic backups now function correctly again after an upgrade of the firewall to version 3.4. The issue occurred on U500S, U800S, SNi40, SN510, SN710, SN900, SN910, SN2000, SN3000, SN6000, V50, V100, V200, V500, VU, VS5, and VS10 firewall models.

Proxies

Support references 67713 - 67924

SMTP proxy

The SMTP proxy service would unexpectedly restart in some cases. This issue has been fixed.

New features in version 3.4.1

IPsec VPN

In cases where a VPN links two sites, and the internal network of one site overlaps the other site's internal network, local traffic on each site must not go through the encrypted tunnel. This operating mode was not supported in previous versions of SNS.

It can be enabled using CLI commands:

```
CONFIG IPSEC UPDATE slot=<1-10> BypassLocalTraffic=1
CONFIG IPSEC ACTIVATE
```

Stormshield Network Real-Time Monitor

Protection of private data

In the interests of compliance with the European General Data Protection Regulation (GDPR), private data found in logs (e.g., user, machine name, source IP address, etc.) will no longer be displayed systematically in SNRTM's screens. By default, only the super administrator (admin account) will be able to view such data. Other administrators will only be allowed to enable access to private data after they have received an individual and temporary code for access to private data.

Resolved vulnerabilities from version 3.4.1

ClamAV

A set of vulnerabilities has been fixed by upgrading the ClamAV antiviral engine :

- CVE-2017-12374 : ClamAV UAF (use-after-free) Vulnerabilities.
- CVE-2017-12375 : ClamAV Buffer Overflow Vulnerability.
- CVE-2017-12376 : ClamAV Buffer Overflow in handle_pdfname Vulnerability.
- CVE-2017-12377 : ClamAV Mew Packet Heap Overflow Vulnerability.
- CVE-2017-12378 : ClamAV Buffer Over Read Vulnerability.
- CVE-2017-12379 : ClamAV Buffer Overflow in messageAddArgument Vulnerability.
- CVE-2017-12380 : ClamAV Null Dereference Vulnerability.

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

Version 3.4.1 bug fixes

System

Proxies

Support reference 66922

On multi-user hosts connected to firewalls that use authentication and the SSL proxy, using recent versions of Google Chrome and Mozilla Firefox to display the secure version of a website, then the unsecured version, would cause the error page "Too many redirects" to appear. This issue has been fixed.

High Availability

Support reference 65811

An issue with the replication of the internal directory in a cluster has been fixed.

IPsec VPN

Support references 67120 - 67135

An anomaly in the management of routes associated with SAs (Security Associations), which could cause the firewall to freeze when it uses the IPsec IKEv2 tunnel manager, has been fixed.

Support references 67185 - 66902

Peers with the same network parameters (remote gateway) but with different names were prohibited in the same IPsec policy. This behavior prevented the application of certain policies deployed via Stormshield Management Center, and has been modified in order to allow this configuration.

Intrusion prevention

COTP protocol

Support reference 66567

An anomaly in the analysis of the COTP protocol would cause the firewall to either freeze (virtual firewall) or restart (physical firewall). This anomaly has been fixed.

New features in version 3.4.0

Protection of private data

In the interests of compliance with the European General Data Protection Regulation (GDPR), private data found in logs (e.g., user, machine name, source IP address, etc.) will no longer be displayed systematically. By default, only the super administrator (admin account) will be able to view such data. Other administrators will only be allowed to enable *Full access to logs (sensitive data)* mode after they have received an individual and temporary *Code for access to private data*.

Bridge with Wi-Fi interface (experimental)

Wi-Fi interfaces can now be added to bridges. This feature is in an experimental phase, and can only be accessed using the CLI command CONFIG NETWORK INTERFACE and only one SSID is supported per bridge. The address of the bridge is the Wi-Fi interface's MAC address.

System

High Availability

An option has been added, allowing sessions to be synchronized depending on their duration (advanced configuration). Sessions that are shorter than the value specified in the **Minimum duration of connections to be synchronized (seconds)** field will be ignored during a synchronization. This option therefore makes it possible to avoid synchronizing very short connections that may exist in large numbers, such as DNS requests, for example.

IPsec VPN

The "Make-before-break" re-authentication scheme guarantees that the negotiation of a new tunnel is indeed successful before deleting older tunnels. This scheme is now enabled by default. If an issue occurs, the scheme can be disabled using the CLI command CONFIG IPSEC UPDATE slot=xx MakeBeforeBreak=0. Details of this command can be found in the *CLI SERVERD Commands Reference Guide*.

In the *ModeConfig* anonymous user configuration (mobile users), object groups can be selected to define DNS servers.

SSL VPN

The confidentiality level now adapts to the authentication level: the Diffie-Hellman key (confidentiality) is always bigger than or equal to the public key (authentication), with tolerance for a variation of 3 bits.

SSH banner

The welcome banner for SSH connections to the firewall can now be customized. To do so, simply place an *sshd-banner* file containing the desired banner in the *ConfigFiles* folder and run the `enservice` command. Details of this command can be found in the *CLI Console / SSH command reference guide*.

SNMP Agent
Information regarding bandwidth usage for QoS queues can now be collected via SNMP.

BIRD dynamic routing
The BFD (Bidirectional Forwarding Detection) tool is now built into the BIRD dynamic routing module, and is only available for experimentation.

Intrusion prevention

OPC HDA and OPC AE industrial protocols
The industrial protocols OPC HDA (Historical Data Access) and OPC AE (Alarms & Events) are now supported. Events allowed on the network can now be customized and the commands that these protocols use can be monitored.

Oracle TNS, LDAP and HTTP protocols
The analysis of the protocols Oracle TNS (Transparent Network Substrate), LDAP and HTTP have been improved in order to increase the detection rate of malware and attacks.
As the LDAP analysis intercepts LDAP traffic passing through the firewall, ensure that you conduct tests before applying it in your production environment.

A new alarm *Invalid HTTP protocol: strict analysis* has been added to factor in HTTP errors. In the *HIGH* inspection profile used by default in profile 09, the alarm level is Minor, and traffic that raises this alarm is blocked.

TCP protocol
The default duration for which closed connections are kept has been changed from 20 seconds to 2 seconds.

DCE/RPC-based protocols
Among the secondary connections of DCE/RPC-based protocols, the intrusion prevention engine now analyzes the UUID ISystemActivator using the RemoteCreateInstance method (Opnum 4). Address translation is not available for such secondary connections.

Application protection

URL filtering
Block pages can now be configured for URL filtering so that the user is redirected to the authentication portal. This makes it possible to set up a policy that filters unauthenticated users before granting them access to the website after authentication.

Applications and protections
By default, the inspection profile IPS_09 in the **Configuration > Application protection > Applications and protections** module is now based on the *HIGH* alarm model. Furthermore, filter policy 9 has been renamed *(9) Pass all High* and contains a filter rule that uses the new inspection profile IPS_09.
This modification will not be available after a firmware upgrade, only after a new installation or restoration to factory configuration.

Reports

Sandboxing and Security categories

New reports have been added:

- Top most frequently analyzed file types,
- Top hosts that have submitted the most files for sandboxing,
- Top protocols that use sandboxing,
- Top users who have submitted files for sandboxing,
- Detection rate by analytics engine (Sandboxing, Antivirus, AntiSpam).

In order to display these new reports, you will need to disable some others as the number of reports is limited to 30.

Web administration interface

The various pages of the web administration interface can now be added to favorites in the browser.

Dashboard - Sandboxing

The sandboxing widget includes additional information about the status of the connection and submitted file quotas:

- Connected, submitted file quota exceeded,
- Connected, submitted file quota unknown,
- Limited, submitted file quota exceeded,
- Limited, submitted file quota unknown.

Filter - NAT

The number of characters allowed in the source and destination of a filter rule has been increased from 250 to 500, so you can enter a longer list of objects in these fields.

Hardware

Several hardware queues are now automatically allocated to virtual machines that have several virtual CPUs and VMware vmxnet3 interfaces. The multi-queue function can be disabled by adding `pohw.pci.honor_msi_blacklist=1` to the file */boot/loader.conf.custom*. Restart the virtual machine to apply the new configuration.

Version 3.4.0 bug fixes

System

High Availability

Support reference 66789

After a connection is lost with the active node of the cluster, the other node will now take over more efficiently as it leaves minimum impact on network resources.

Support reference 65652

From SNS 3.3.1 onwards, in clusters made up of virtual firewalls, the quality of the high availability link displayed would be 0 even though members of the cluster were communicating correctly. This issue has been fixed.

IPsec VPN - IKEv1

Support reference 66135

In local IPsec policies and global IPsec policies (deployed, for example, via SMC or SNCM), the presence of peers or traffic endpoints that overlap would prevent such policies from being activated. Therefore, local policies relying on mobile peers defined by the **Any** object would overlap any global site-to-site tunnel policy. This issue has been fixed.

IPsec VPN - IKEv2

Support reference 61227

The firewall would not apply user access privileges and refused to authenticate users who present certificates with empty X509v3 Extended Key Usage fields. This issue has been fixed.

Support reference 66862

CRL updates are now correctly applied for VPN tunnels in IKEv2 mode.

Support reference 61100

On SN150 products, existing VPN tunnels in IKEv2 mode would become inoperative after several days, requiring the program or the firewall to be restarted. This issue has been fixed.

Support reference 64048

The number of IKE SAs (Security Associations) for the same IPsec IKEv2 tunnel would increase over time without diminishing the number of unused SAs. The upgrade of the IKEv2 tunnel management engine has fixed this issue.

SSH commands

Support reference 66189

The `autoupdate` command to update all of the firewall's modules no longer raises the following error whenever a module has been configured to not check the signatures of downloaded data:

```
Error=Master file version mismatch! (-1 != 1)
```

Support reference 66137

The SSH command `enwifi` has been improved: it is no longer called up by the `ennetwork -f` command on firewall models without Wi-Fi. Furthermore, the `enwifi -h` command no longer generates inappropriate alarms.

Routing

Support reference 64996

An issue with competing access in configurations that use filter rules in firewall mode as well as policy-based routing (PBR) directives would cause the firewall to freeze. This issue has been fixed.

Support reference 64070

Whenever H323 and TFTP protocols opened a child connection in the opposite direction of the main connection, traffic would not reach its destination if the main connection was associated with a router configured in filter rules (PBR) and/or a return router. This issue has been fixed.

Support reference 67115

A return packet whose initial routing is a static route to a virtual interface (VTI) is now redirected correctly to the return router if the intrusion prevention engine requires it.

Applications and protections

Support reference 61505

Certain actions that were supposed to be performed when alarms were raised by customized context-based protection signatures were not carried out (e.g. sending of e-mails or quarantine). This issue has been fixed.

Audit logs

Support references 66899 - 66797 - 66900

Whenever an internal service corrupted the audit log reporting system, the system would cause all services to hang without making the product restart or making another node in the cluster take over. This issue has been fixed.

Support reference 55251

The name of the user who opened a connection now appears correctly in the connection logs, even if another user has retrieved the same IP address in the meantime.

Support reference 55251

The *logd* daemon that writes logs and generates reports no longer shuts down unexpectedly and no longer causes logs to be lost.

SSL VPN

Support reference 65347

Implicit rules for OpenVPN over TCP and UDP are no longer unnecessarily generated, only depending on the protocol enabled (TCP and/or UDP).

Support references 65392 - 66937 - 65279

In order to resolve malfunctions on SSL VPN over UDP, it is now possible to define the service's listening IP address using the command CONFIG OPENVPN UPDATE udpBindAddr={<firewall_ip_object>|""}. Details of this command can be found in the *CLI SERVERD Commands Reference Guide*.

SPNEGO SSO authentication

Support reference 65439

Whenever SPNEGO authentication has been configured, the user now directly accesses websites without having to go through the authentication portal, even when the website's URL contains an apostrophe.

Proxies

Support references 66014 - 65028 - 65033

In some cases, using the SMTP proxy would cause the service to shut down unexpectedly for all types of connections through the proxy: SMTP, as well as HTTP or SSL. This issue has been fixed.

Maintenance

Support reference 67022

The system report (sysinfo) no longer generates illegitimate errors regarding some of the system's binary files.

Log partition

Support reference 64065

The issue with the corruption of the log partition following a sudden shutdown of SNS has been fixed.

Network

Support reference 64123

The accumulation of unanswered ARP requests could cause the loss of the first packet in communications between two hosts belonging to the firewall's networks. This anomaly, which was problematic for certain monitoring tools, has been fixed.

Intrusion prevention

Antispam

Support reference 66530

Active updates of the antispam engine are now faster and no longer use a disproportionate amount of CPU resources.

Application protection

Inspection profile

Support reference 64042

Whenever a client on the firewall's internal network opens a connection to a server on the Internet and the server's response generates an alarm, the alarm will no longer block the client's IP address, but the server's IP address.

Web administration interface

Filtering

Support reference 64008

The usage counter now appears correctly for all filter and NAT rules.

Support reference 64943

When filter rules are copied and pasted, destination information about *Disk*, *Syslog server* and *IPFIX collector* logs is now saved.

Support reference 66798

The right filter policy is now displayed after a global policy is selected.

Support reference 65057

In the **Security policy > SMTP filter** page, the "?" character can now be entered in the field of the sender's name.

Objects

Support reference 66757

Fixed event time objects that start and end on the same day can now be created again.

Reports

Support reference 65958

The **Reports > Sandboxing > Malicious files blocked** menu now correctly displays the report on files blocked by the Sandboxing engine.

Users

Support reference 65945

If you had an external LDAP directory configured on the firewall, users whose groups contained special characters in their attributes (DN, OU, etc.) would not be correctly applied. This issue has been fixed.

Support reference 66275

The **Configuration > Users > Authentication > Captive portal** tab has been optimized to take into account a large number of interfaces.

Network interfaces

Support reference 64870

The **Configuration > Network > Interfaces** page no longer runs the command relating to Wi-Fi on firewalls without Wi-Fi, and as such no longer generates irrelevant errors.

Protocols

Support reference 66438

In the **Protocols** module, the button that allows adding customized MS-RPC services is now operational.

Monitoring

Support reference 65898

The **Average throughput** column in the **Monitoring > Connection monitoring** menu now shows the correct value for the unit indicated (bits/second).

Support reference 66440

In the interface monitoring configuration, interfaces already on the list can no longer be added, thereby keeping errors to a minimum.

Administrator account password

Support reference 66384

Whenever you change the password of the administrator account, the new password will now be correctly interpreted if it contains spaces.

Login page

Support reference 66027

The help button on the login page that redirected to an unknown page has been deleted.

Virtual machines

Microsoft Azure hosting platform

Support reference 58722

During the initialization of a virtual machine on the Azure platform, the "$" (dollar) character in the administrator password would not be taken into account. The administrator password on the firewall would therefore remain "admin". This issue has been fixed.

Hardware

Support references 65250 - 65820

An exceedingly huge amount of system information would be sent over the serial link, potentially slowing down the firewall and preventing administration via this link. Such information will now no longer be visible by default on the serial link, but only via the `ndmesg`

command. However, you can still modify the `KernelMsg` parameter in the `[Console]` section of the ConfigFiles/system configuration file to display the information again.

Resolved vulnerabilities from version 3.3.2

OpenSSL security flaws

A vulnerability (CVE-2017-3736 - bn_sqrx8x_internal carry bug on x86_64) has been fixed. It was only affecting SNS virtual machines running on processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later, or AMD Ryzen.

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

Version 3.3.2 bug fixes

System

Routing - virtual interfaces

Support reference 66654

Despite a value of 1 in the *PBROverideStatic* field (*/SecurityInspection/common* file), a policy-based routing (PBR) rule intended to direct traffic outside an IPsec tunnel set up between two virtual interfaces (VTIs) would not have priority over a static routing rule. This issue has been fixed.

Proxies

Support reference 66667 - 66533 - 66649 - 66668 - 66699

In configurations that use the SSL proxy, simultaneous web connections from a multi-user machine could cause the proxy to restart in loop. This issue has been fixed.

SSL VPN over UDP

Support reference 65392 - 65323

Implicit rules would not allow access to the UDP-based SSL VPN through dialup interfaces (PPoE, PPTP, PPP or 3G/4G modems). This anomaly has been fixed.

SSL VPN Portal

Support reference 66540

In a configuration such as the following:

- the SSL VPN portal has been enabled to allow access to application servers and web servers;
- users only have access privileges to application servers through the SSL VPN portal and are authenticated on the firewall's captive portal.

Clicking on such users in the **Secure access** menu of the captive portal would cause the firewall's authentication management mechanism to freeze. This issue has been fixed.

Interface aggregates

Support reference 64757

In a configuration containing several interface aggregates, deleting an aggregate other than the last one would cause an internal error to appear in the **Interfaces** widget of the Dashboard. This anomaly has been fixed.

Intrusion prevention

SIP - NAT protocol

Support reference 66121

Whenever the port used for translating SIP packets was higher than the original port, the SDP (Session Description Protocol) field in packets would be truncated. This issue has been fixed.

Resolved vulnerabilities from version 3.3.1

WPA2 Protocol security flaws

The following vulnerabilities have been fixed:

- CVE-2017-13077: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
- CVE-2017-13078: Reinstallation of the group key (GTK) in the 4-way handshake.
- CVE-2017-13079: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
- CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake.
- CVE-2017-13081: Reinstallation of the integrity group key (IGTK) in the group key handshake.
- CVE-2017-13082: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
- CVE-2017-13084: Reinstallation of the STK key in the PeerKey handshake.
- CVE-2017-13086: Reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
- CVE-2017-13087: Reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
- CVE-2017-13088: Reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

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

Version 3.3.1 bug fixes

System

IPsec VPN

Support reference 66135

It is now possible to combine IPsec VPN global policies with some local policies having one identical peer, even if one of the second peers is “Any”. Such configuration no longer returns the `duplicated sainfo` error.

High Availability

Support reference 65652

The quality of the High Availability link was 0 for a cluster with virtual firewalls, even though the communication between the cluster members was working correctly. This issue has been fixed.

Support reference 66515

An error in the management of file synchronization made it impossible to create an HA cluster on model SN310 firewalls. This issue has been fixed.

Web administration interface

Router objects

Support reference 66385

With version 3.3.0, it was no longer possible to create a router object via the menu **Configuration > Objects > Network objects > Add > Router**. This issue has been fixed.

Administrator account password

Support reference 66384

When you modify the password of the administrator account, the new password is now correctly processed if it contains spaces.

New features in version 3.3.0

System

IPsec VPN

IPsec policies can now group peers that use various versions of the IKE protocol with restrictions on the use of the IKEv1 protocol (cf. section **Explanations on usage**). As this feature could not be tested in complex and disparate environments, you are strongly advised to test it out on a test configuration.

It is now possible to define a list of LDAP directories that need to be browsed sequentially in order to authenticate mobile users (certificate or pre-shared key authentication).

Interfaces

Interfaces can now be defined in networks without broadcast addresses (network mask /31 - RFC 3021). Such interfaces are to be used only for point-to-point exchanges.

A "Priority (CoS)" field can be defined for VLAN interfaces. This CoS (Class of Service) priority will then be imposed for all packets sent from this interface.

Global objects

During the deployment of configurations via Stormshield Management Center, additional checks will be performed on global objects used in the firewall's routing instructions.

Authentication by certificate

An advanced option allows user authentication to be enabled on several LDAP directories. When a character string defined by a regular expression is found in a selected field within the certificate that the user presents, the associated LDAP directory will be queried in order to authenticate the user in question and verify his access privileges.

Certificates and PKI

SNS firewalls allow defining separate certificate authorities to sign SCEP exchanges and to sign enrollment certificates. This configuration can only be obtained via the `PKI SCEP QUERY` command *`scep_ca_name`*.

Sandboxing

Additional information is sent whenever files are submitted for sandboxing:

- Version of the firewall's firmware,
- MIME types and the names of all files included in the archives.

Notifications

Version 3.3.0 of the firmware supports the secure sending of e-mails using the SMTP protocol associated with the STARTTLS mechanism.

In the SMTP server's settings, an e-mail address replaces the DNS domain name in order to ensure compatibility with certain external SMTP services (Microsoft Office 365 for example).

Routing - Return routes

MAC addresses no longer need to be specified for network objects corresponding to the gateways selected in return routes. When they are not entered, MAC addresses will be learned

dynamically.

Implicit rules

Since administration tools (Stormshield Management Center and SN Real-Time Monitor) connect to the firewall's web administration port (TCP/443 - HTTPS by default), implicit rules that allow connections to the firewall from the local network to the usual administration port (TCP/1300) are disabled for firewalls in factory settings.
Administrators who use Global Administration, SN Centralized Manager or NSRPC binary files can now create explicit filter rules (recommended method) or manually re-enable these implicit rules.

Audit logs

Connection logs (*l_connection* file) indicate as the destination name (*dstname* field) the SNI (*Server Name Indication*) requested by the client host during TLS negotiation.

Logs relating to IPsec tunnels (*l_vpn* file) specify the name of the user who activated logging as well as his group, if it has been defined.

Centralized administration

The source address that needs to be used for the firewall's connection to its centralized administration server (SMC) can be forced. These settings can only be configured using the command lines `CONFIG FWADMIN UPDATE` and `CONFIG FWADMIN ACTIVATE`. Details of these commands can be found in the *CLI SERVERD Commands Reference Guide*.

SNMP Agent

A new OID that allows reporting the comment assigned to an interface has been added to the Stormshield network interface MIB (STORMSHIELD-IF-MIB).

Intrusion prevention

TCP protocol

The default value of a TCP connection timeout has been set to 3600 seconds (1 hour) for firewalls in factory configuration.

DNS protocol

The intrusion prevention engine analyzes the implementation of the DNS protocol over TCP.

BACnet/IP protocol

The intrusion prevention engine analyzes the industrial protocol BACnet/IP (Building Automation and Control Networks over IP).

Multipath TCP

As the firewall's intrusion prevention engine is not in a position to analyze *multipath TCP* connections, a specific alarm has been added, which blocks such extensions when they are detected ("Multipath TCP").

TDS protocol

The intrusion prevention engine analyzes the TDS (Tabular Data Stream) protocol used for requests sent to Microsoft SQL Server databases.
Note that all traffic streams using the 5000/TCP port are analyzed as TDS protocol.

Facebook Zero protocol

Support reference 64995

As Facebook has implemented the protocol Facebook Zero (based on Google's QUIC protocol), the use of applications such as Facebook Messenger would set off the "Invalid SSL packet" block alarm. A dedicated "Facebook Zero protocol detected" alarm has been created to allow the administrator to identify and allow such connections.

Web administration interface

Saving commands

The upper banner of the administration interface includes a button that allows saving the sequence of commands run during any configuration performed on the firewall. When the saving process is stopped, this command sequence will be displayed so that it can be copied and pasted in a text editor (to be used in an NSRPC script, for example).

This feature can be enabled or disabled in the user preferences of the web administration interface.

Menu display

The display of certain menus is dependent on the activation or availability of related features:

- the **Users and groups** menu only appears if at least one directory has been defined,
- the **Audit logs** menu does not appear on firewalls that are not equipped with storage media,
- the **Reports** menu appears only when reports have been enabled,
- the **My favorites** menu is shown once the first favorite has been defined.

Filtering and NAT

When several cells of a filter policy are modified in succession, the symbol indicating that these cells are in the process of modification (▸) will remain visible until the filter policy is validated.

In certain object selection fields, there is now a button to access a pop-up menu in order to create new objects or modify existing objects from the Filter/NAT module.

User monitoring

New columns have been added, indicating whether the user is allowed to use the SSL VPN portal, set up SSL VPN tunnels or IPsec VPN tunnels.

SN Real-Time Monitor

Hosts monitoring

Support reference 59595

Hosts located behind unprotected interfaces, and which are involved in connections that pass through the firewall, are displayed in the Hosts view in SN Real-Time Monitor.

Version 3.3.0 bug fixes

System

High Availability

Support reference 64234

Reloading a filter policy made up of several hundred rules could temporarily prevent communication between both members of the cluster over their high availability link. Depending on the duration of the interruption, the status of the passive firewall would sometimes switch to active. Restoring the connection between both firewalls would then cause both members of the cluster to attempt a full synchronization of the connection table. This reaction, which imposed an unusually heavy load on the cluster, has been fixed.

Support reference 61400

Information regarding high availability would stop appearing in the dashboard, and clicking on the high availability module would display the error message "Failure when loading high availability information". This issue has been fixed.

Support reference 65614

When an HA link fails during heavy traffic, the high availability mechanism would attempt, unsuccessfully, to recreate this link. This anomaly has been fixed.

Support reference 65925

During the restoration of links between connections, an issue occurring whenever firewall roles were switched in a cluster could cause the firewall to restart. This issue has been fixed.

Dynamic routing

Support reference 65730

On SN150, SN160(W), SN210(W) and SN310 firewalls, the system would not apply routes that the Bird dynamic routing engine had learned. This issue has been fixed.

Configuration

Support reference 54377

Defining a proxy server to allow the firewall to access the Internet (**System** > **Configuration** > **Network settings** tab) would cause the CRL (Certificate Revocation List) verification mechanism to freeze. This issue has been fixed.

Support reference 63972

In the module **System** > **Configuration** > **Network settings** tab, enabling the use of a proxy server to allow the firewall to access the Internet would wrongly require the user to enter a login and password. This anomaly has been fixed.

GRETAP interfaces

Support reference 65589

The MAC addresses associated with packets leaving tunnels set up between GRETAP interfaces were wrong. This issue has been fixed.

Link aggregation

Support reference 65755

A malfunction occurring during the distribution of traffic among physical interfaces that belong to a link aggregate has been fixed.

Filtering and NAT

The filter rule reloading mechanism has been optimized. These enhancements are particularly noticeable in the following cases:

- Firewalls and firewall clusters that manage a very high number of connections,
- Filter policies that group several hundred rules,
- Modifications to alarms relating to several network protocols.

Support reference 64851

Reloading filter rules could cause connections to be deleted, making their child connections orphans. This behavior has been modified to delete child connections as well.

Support reference 64508

Connections that pass through a filter rule that uses a time object could end up being associated with an invalid rule after this time object expired. This behavior has been fixed.

Support reference 64365

Since the act of deploying and then collapsing a filter policy is considered a modification of the filter policy, saving this change would cause the policy to be reloaded. Policies will no longer be reloaded in this context.

Support reference 40421

Rule IDs were the same for all implicit rules (0). Each rule now has its own distinct ID.

Support reference 65227

In a configuration such as the following:

• Policy-based routing (PBR) was used for outgoing traffic with a router configured to perform load balancing by source IP address,

• Implicit rules that could authorize such traffic were disabled,

Sending packets from the firewall using the "tracert -s" network command could cause this firewall to reboot. This issue has been fixed.

Support reference 65990

The SSL inspection rule creation wizard would no longer allow the definition of a source interface. This anomaly has been fixed.

Authentication portal

Support reference 60488 - 60143

The authentication portal (captive portal) would be automatically enabled on all profiles during the migration of configurations from a 2.7 (or 2.x) version to a 3.x version of the firmware. This anomaly has been fixed.

Proxies

Support reference 60134

Access from a multi-user host to websites that use Cross-Origin Resource Sharing (CORS) would not allow the display of external resources on the visited website. This issue has been fixed by integrating the Access-Control-Allow-Origin field into the proxy's response.

Support reference 61499

The size of the cache reserved for the generation of certificates used by the SSL proxy has been increased in order to fix performance issues and reduce the possibility of this proxy freezing.

Support reference 60616 - 64504

In configurations using the HTTP proxy (implicit or explicit proxy) and that are subject to URL filter requests, issues with the management of multiple HTTP requests within a connection (HTTP pipelining) have been fixed.

Support reference 43089

An anomaly in the assignment of inspection profiles for filter rules that use the SSL proxy has been fixed.

NSRPC client

Support reference 64100

The NSRPC client for Microsoft platforms was denied connection to SN160(W), SN210(W) and SN310 model firewalls. This issue has been fixed.

SNMP Agent

Support reference 64135

Sending a large volume of SNMP notifications (*traps*) would cause the firewall's SNMP service to freeze. This issue has been fixed.

Support reference 59492

Non-generic SNMP notifications corresponding to minor or major system events would occasionally not be sent. This anomaly has been fixed.

Support reference 64787

The description of the OID snsHASyncStatus (STORMSHIELD-HA-MIB) was wrong (return codes were inverted for synchronized/unsynchronized statuses). This anomaly has been fixed.

DNS cache

Support reference 58819 - 58633

Whenever the DNS cache was enabled and used by the firewall's protected networks, the creation or modification of a protected interface would not be taken into account in this cache's configuration. This anomaly has been fixed.

SSO Agent

Support reference 59778

Configuring a backup SSO agent without defining a password would cause an error in the authentication portal's management process. This issue has been fixed.

Support reference 59287

The SSO agent installed on Microsoft Windows workstations would send either the FQDN of the Microsoft Active Directory domain (name of the external LDAP directory declared on the firewall) or its NETBIOS name to the firewall. This behavior, which would cause authentication issues, has been modified.

Support reference 61169

The SSO agent installed on Microsoft Windows workstations would send a blank Microsoft Active Directory domain name to the firewall whenever the IP addresses of these workstations changed. This behavior, which would cause authentication issues, has been fixed.

Support reference 64274

The connection between the SSO agent and the firewall would shut down at regular intervals whenever the user group defined in the authentication rule was empty. This anomaly has been fixed.

Support reference 53806

The advanced option "Enable DNS host lookup" allows managing changes to the IP addresses of user workstations and authenticating users who have logged on to hosts that have several IP addresses.

SSL VPN

Support reference 65427 - 65392

Customizations to the UDP listening port on the SSL VPN portal were not applied. This anomaly has been fixed.

SSL VPN Portal

Support reference 60672

Whenever the port used for authentication on the firewall and the SSL VPN portal was modified, the connection to the SSL VPN portal via Java Webstart would fail. This issue has been fixed.

Support reference 59423

Web servers protected by firewalls that were themselves behind NAT (network address translation) equipment could not be contacted via the SSL VPN portal, as the Java client would attempt to connect to the firewalls' private addresses. This behavior has been fixed.

Support reference 60194

The menu that allows selecting the method for loading available applications via the SSL VPN portal would only be available if application servers and web servers were defined. Loading via the Java applet would then be automatically used. This anomaly has been fixed.

IPsec VPN

Support reference 59007

Whenever mobile peers originally defined in IKEv2 with a local ID (optional field), and for which tunnels have been set up, are switched to version 1 of the protocol, this would cause the IKEv1 tunnel management service to restart in loop. This issue has been fixed.

Support reference 64496

The setup of tunnels in mobile mode through virtual tunneling interfaces (VTIs) would fail, as the wrong source interface was assigned (standard IPsec interface instead of the virtual IPsec interface). This issue has been fixed.

IPsec VPN - IKEv1

Support reference 64766

The engine that manages IPsec tunnels in IKEv1 did not automatically apply changes to certificates (renewal) or certificate authorities. This anomaly has been fixed.

IPsec VPN - IKEv2

Support reference 66110

The "Make-before-break" re-authentication scheme that can be used for security associations (SA) would not be taken into account if it had only been defined in global IPsec policies. This anomaly has been fixed.
Do note that this scheme can only be enabled through the configuration file of the active VPN profile (**MakeBeforeBreak** field in the "[Global]" section of the file *ConfigFiles/Global/VPN/xx*).

Automatic backups

Support reference 65510

The Digest authentication method for automatic backups to customized servers would repeatedly fail. This issue has been fixed.

Quality of service

Support reference 59940

During the creation of queues, a maximum bandwidth that was too low would not be taken into account even though no warnings were given. The maximum bandwidth indicated cannot be lower than 100 kbs.

USB key

Support reference 63996

USB drives that were formated according to the FAT32 file system would not be recognized when they were started up on SN150 model firewalls. This anomaly has been fixed.

Wi-Fi network

Support reference 59938

The characters "$" and "!" would not be accepted during the definition of a WPA2 key. This anomaly has been fixed.

Audit logs

Support reference 61232

The message indicating that a power supply module was missing would wrongly appear for both models on an SN6000 model firewall. This anomaly has been fixed.

Support reference 65456

The field representing the IP protocol number for IPFIX would systematically take on the value "0" (zero) in logs. This anomaly has been fixed.

Monitoring - Users view

Support reference 60441

Following a modification to the command in the firmware, the "Remove user from ASQ" pop-up menu no longer functioned. This issue has been fixed.

Intrusion prevention

HTTP

Support reference 59442 - 59639

A whitelist was added to the configuration of the HTTP protocol. This list allows defining response header fields for the server that may exceed 4096 bytes (e.g. the *Content-Security-Policy* field).

Support reference 65504

An issue regarding support for HTTP requests containing a *text/vbscript* type of *content-type* field has been fixed.

EtherNet/IP protocol

Support reference 64012

Whenever the EtherNet/IP protocol was transported over the UDP layer, responses to ListIdentity, ListServices or ListInterfaces requests would be considered inappropriate and blocked by an "EtherNet/IP: invalid protocol" alarm. This anomaly has been fixed.

UDP

Support reference 43718

Whenever the UDP traffic destination server was temporarily unavailable, the many "recipient unavailable" ICMP messages generated as a result would set off the block alarm "'Invalid ICMP message (replay)". A dedicated alarm "ICMP replay (UDP connections)" that can be set to "pass" has been created.

Netbios - CIFS protocol

Support reference 64007

Connections presenting several sequences of unreceived packets, and on which an intrusion prevention scan has already started running, could potentially cause the firewall to freeze.

IPv6

Support reference 59217

ICMP requests (*pings*) sent to an interface on the firewall configured with an IPv6 address would fail and raise the alarm "IP address spoofing (type=1)", which would block traffic. This anomaly has been fixed.

SIP

Support reference 61228

Whenever filter rules for SIP connections were in firewall mode or whenever the "Necessary SDP field missing in the SIP protocol" alarm was set to *Pass*, a SIP connection in which an SDP (Session Description Protocol) field was missing (*media* field, for example) would cause the intrusion prevention engine to freeze for the SIP protocol scan. This issue has been fixed.

Users

Support reference 64493

An issue with competing access to data regarding users would cause attempts to delete users who have already been de-authenticated. This issue, which could potentially cause the firewall to freeze or reboot, has been fixed.

Protocols that generate child connections

Support reference 65583

In configurations that handle large volumes of traffic, an issue regarding competing access on traffic that generates many child connections would occasionally cause firewalls to freeze. The management of such connections has been enhanced and the maximum number of child connections generated for each connection can now be configured.

Web administration interface

DHCP relay

Support reference 51631

Even though bridges cannot be used as listening interfaces for DHCP relays, the web administration interface would suggest bridges in the list of selectable interfaces. This anomaly has been fixed.

Authentication

Support reference 50899

Whenever authentication rules were added, objects created in the wizard could not be directly selected for such rules. This anomaly has been fixed.

Support reference 59996

Changes made to an authentication policy, including policies using the SSO agent and SPNEGO methods, would not be visible in subsequent displays of the same authentication policy. This anomaly has been fixed.

Objects

Support reference 64620

When checking the use of an object, clicking on the link to the NAT/filter policy using it would systematically display the NAT/filter policy currently in use. This anomaly has been fixed.

Network objects

Support reference 59983

When displaying details of a "Ports - port ranges" network object, the name of the object would no longer be modifiable. This anomaly has been fixed.

Filter - NAT

Support reference 60576

The selection of a rule separator located under the lower bar of the last page of rules, therefore implying the use of the window scroll bar, would not function correctly. This anomaly has been fixed.

Directory configuration

Support reference 59694

After having displayed the configuration of an external LDAP directory using a backup server, the backup server field would continue to appear even for LDAP directories that do not use this feature. This anomaly has been fixed.

Audit logs

Support reference 56667

The display of certain columns by group (source name, destination name, source port name, etc.) would not work correctly. This anomaly has been fixed.

Support reference 59272

An anomaly in the creation of advanced filters would allow new filters to be added even if they did not apply to the logs displayed. Moreover, clicking subsequently on the **Add** button of such filters would display the misleading message 'This filter already exists". This anomaly has been fixed.

URL filtering

Support reference 61237

Whenever the names of customized URL filter policies began with the same string of characters, attempting to select any of these policies in a filter rule would systematically select the first of them. This issue has been fixed.

Routing

Support reference 64426

The selection of USB drive/modem devices as gateways for static routes could not be validated. This anomaly has been fixed.

Multi-user objects

Support reference 55877

During connections to the web administration interface using a Microsoft Internet Explorer browser in version 11, multi-user objects added would not be taken into account. This anomaly has been fixed.

Quarantine

Support reference 63949

Whenever a quarantine duration was set to more 49 days, the actual quarantine would last only 17 days and no warning message would be displayed. For technical reasons, the maximum quarantine duration has been restricted to 49 days.

Microsoft Internet Explorer

Support reference 65187

The use of Microsoft Internet Explorer browsers, including version 11, would prevent the display or modification of certain fields in configuration modules. 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 (LTS - Long Term Support version).

SN Real-Time Monitor

Events view

Support reference 63848

Dates displayed in the **Events** view would only be formated in hours and minutes. Seconds have been added to the date.

Users view

Support reference 60441

Following a modification to the command in the firmware, the **Remove user from ASQ** pop-up menu no longer functioned. This issue has been fixed.

Support reference 61017 - 65779

The method displayed for users authenticated via an SSO agent on a firewall in version 3 was wrong (unknown). This anomaly has been fixed.

SSL VPN view

Support reference 64785

The function that makes it possible to shut down an SSL VPN tunnel from the SN Real-Time Monitor interface (**Remove this tunnel** pop-up menu in the **SSL VPN tunnels** tab) was no longer operational with SNS firewalls in version 3. This anomaly has been fixed.

Support reference 64785

Following the migration of firewalls to version 3.2.0, SSL VPN tunnels that were set up on such firewalls could no longer be displayed (**SSL VPN tunnels** tab). This anomaly has been fixed.

Vulnerability Manager view

Support reference 59980

A "No help available" message would appear whenever a detected vulnerability was selected. This anomaly has been fixed.

Active Update view

Support reference 59543

Update information for the "Public IP reputation database" and "Custom context-based signature database" would wrongly display the "No license" warning in the expiration date column. As these features do not require a license, this anomaly has been fixed and "<n/a>" will now appear instead.

Overview

Support reference 59564

The Antivirus column, which would wrongly indicate "Disabled" whenever the Kaspersky antivirus engine was used on the firewall, has been hidden.

Firewall administration

Support reference 64774 - 60480

The menu **Applications** > **Launch administration application** and the automatic connection button (**Overview**) would no longer function with firewalls on which the administration ports have been modified (HTTPS port by default) as the connection URL would be wrong. This issue has been fixed.

Link to the Stormshield knowledge base

Support reference 64117

The link allowing users to log on to the Stormshield knowledge base (*Security KB*) did not work. You will need to modify this link (correct value: https://securitykb.stormshield.eu/) in the **File** > **Preferences** menu > **Miscellaneous** tab and restart the application.

New features in version 3.2.1

System

Updates

Whenever a new firmware version becomes available, a link to download the *Version release notes* of this update will appear in the module **System** > **Maintenance** > **System update** tab and in the **Dashboard** > **Properties** panel.

Resolved vulnerabilities from version 3.2.1

ASN.1 security flaw

A vulnerability (CVE-2017-9023 - Incorrect Handling of CHOICE types in ASN.1 parser and x509 plugin) has been fixed with the upgrade of the IPsec IKEv2 tunnel manager in version 5.5.3. Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

Version 3.2.1 bug fixes

System

CRL verification

Support reference 64074

The firewall no longer performed DNS resolution in order to obtain the address of certificate revocation list distribution points. This issue has been fixed.

Network objects

Support reference 64023

Validating a new network object using the "Create and duplicate" button would deactivate this button as well as the "Create" button for the following object. This anomaly has been fixed.

URL filtering

Support reference 64489

During a connection to an SNS firewall's administration interface via Stormshield Management Center, the request generated by clicking on **Add rules by category** in the **URL filtering** module would not succeed. This anomaly has been fixed.

Intrusion prevention

HTTP

Support reference 61269

Analyzing web pages that use HTML tags containing a large character string to define certain attributes would set off the block alarm "Buffer overflow in HTML attribute". While this reaction is justified, it could potentially cause the firewall to freeze. This issue has been fixed.

Support reference 64941 - 64920

Whenever Web 2.0 scans were enabled (Inspect HTML code and Inspect Javascript code options selected in the Protocols module > HTTP > IPS tab), looking up pages that contained commented VBScript code could cause the firewall to freeze. This issue has been fixed.

New features in version 3.2.0

System

Active Update

For configurations that use customized context-based protection signatures, the **Active Update** module makes it possible to enter the URLs of machines that host such signatures in order for them to benefit from automatic updates.

Filter - NAT

Rules in filter and NAT slots can be exported in CSV (Comma-Separated Values) format.

High Availability

Whenever communication issues arise between members of a cluster even though the active firewall is contactable, the passive firewall will check mutual priorities so that it does not switch to active during a reboot.

A minimum period criterion has been added to the HA mechanism for the selection of connections to be synchronized (*ConnOlderThan*). For example, it allows synchronizing only connections that do not last more than 10 seconds. This parameter can only be modified in command line: `config ha update ConnOlderThan=xx`

SNMP agent

All NETASQ MIBs have been renamed Stormshield (e.g.: STORMSHIELD-SMI-MIB).

Several tables have been added to STORMSHIELD-SYSTEM-MONITOR-MIB in order to provide:

- information on the status of the hardware bypass function (SNi40 industrial firewalls),
- the status of electrical power supplies,
- the temperature of processors,
- the status of disks and the RAID, if applicable.

In a high availability configuration, querying STORMSHIELD-HA-MIB will return information regarding the synchronization status of cluster members, the version number of a deployment via Stormshield Management Center, power supply statuses, the temperature of processors and the status of disks, for both the active and passive firewalls.

Network objects

When the use of network objects is being checked, the name applied to the filter or NAT rule in question will be added to the information displayed.

Access privileges

The command MONITOR USER displays users' access privileges (VPN access, sponsorship, etc.). A link in the user's profile leads directly to the *Detailed access* tab in the **Access privileges** module when the selected user is filtered. These privileges are also available in configuration backups.

Notifications

When a user logs on (web administration interface / Stormshield Management Center / NSRPC) with administration privileges on a firewall, a notification will be sent to other administrators from this firewall.

Directory configuration

User groups may contain other groups. This feature applies to all types of directories supported by SNS firewalls (internal LDAP directory, external LDAP directories, external POSIX LDAP directories and Microsoft Active Directories).

Proxies

Sandboxing now includes Java and Flash files.

SSL VPN

The SSL VPN service supports UDP- or TCP-based connections. In the event a connection over UDP fails, the client will automatically switch to TCP.

This feature requires the use of the SSL VPN Client software in version 2.4 or upwards.

IPsec VPN (IKEv1)

Mobile users can be authenticated using certificates through an external LDAP directory other than the default directory.

IPsec VPN (IKEv2)

Version 3.2.0 of the firmware enables support for the fragmentation mechanism in IKEv2.

Network

Dynamic routing

In the table listing the intrusion prevention system's protected networks, an option has been added in order to automatically inject networks spread by the dynamic routing engine (IPv4 / IPv6).

The configuration of the dynamic routing engine takes into account customized names of network interfaces. Whenever such configurations are restored on devices that do not know these customized names, the system name of the interface will be automatically used.

Wi-Fi network

An option has been added to prevent direct connections between machines connected to the Wi-Fi network managed by the firewall (*AP Isolation*). This option (**Network > Interfaces** module) is enabled by default (public Wi-Fi hotspot configurations); when it is disabled, direct connections between devices connected to the Wi-Fi network will no longer be filtered.

Intrusion prevention

OPC DA protocol

The intrusion prevention system now scans the industrial protocol OPC DA (OPC Data Access).

TDS protocol (Microsoft SQL Server)

The intrusion prevention system scans TDS (Tabular Data Stream) packets used by the Microsoft SQL Server application.

DCE/RPC protocol (Microsoft RPC)

The configuration module for intrusion prevention scans on the DCE/RPC protocol has been modified: UUIDs can now be defined for DCE/RPC services that were not previously defined in a

whitelist of services to allow.

Web administration interface

Audit logs

Alarm logs (*l_alarm* log) specify the names of applications that the intrusion prevention system has detected and that have raised an alarm.

Monitoring

Monitoring data can be printed as graphs.

Reports

The report that shows the highest reputation scores also takes into account internal hosts that are traffic recipients.

A report showing applications that have generated the most alarms can be found in the **Reports > Security** module.

Version 3.2.0 bug fixes

System

Certificates and PKI

Support reference 60548

Whenever an SCEP (Simple Certificate Enrollment Protocol) request was sent to a PKI managed by a Microsoft Windows platform, the authentication phase would fail as the encoding of the password sent was different from the expected encoding (since SCEP is still not covered by any RFC). This anomaly has been fixed.

SNMP agent

Support reference 49523

The OID (Object Identifier) corresponding to the total amount of reserved buffer memory (MIB UCD-SNMP) would wrongly indicate a value that does not correspond to the expected format (32 bits). This issue has been fixed.

Support reference 54961

The unique ID of the SNMP agent would be modified every time the firewall's SNMP service restarted, potentially causing communication errors with monitoring solutions.

Directory configuration

Support reference 58839

Changes to the name of an LDAP directory were not applied in other modules referencing such a directory (e.g.: Filter and NAT). This anomaly has been fixed.

Support reference 57419

In LDAP configurations specifying a backup server, whenever the main server was no longer contactable, LDAP requests in synchronous mode (e.g.: SSL VPN) would not be redirected to the backup server. This issue has been fixed.

Authentication

Support reference 59422

The initial activation of an authentication method would only be applied after its configuration items have been entered and validated twice. This anomaly has been fixed.

Automatic backups

Support reference 59229

Potential communication issues between firewalls and automatic backup servers have been resolved by adding the root Stormshield certificate authority to these servers' trusted authorities.

Filter - NAT

Support reference 59849

Filter rules containing several thousand IP addresses included in groups used in the source or destination could cause the firewall to restart in loop. This issue has been fixed.

Support reference 54522

The "Enable the SYN proxy" option (**Filter - NAT** > **Action** module > **Quality of Service** tab > **Connection threshold** panel > **If threshold is reached** field) would not function to protect servers hidden by address translation. This issue has been fixed.

Address translation

Support reference 58919

To translate the source of traffic sent by the firewall, the destination after translation had to be omitted (removal of *Any* value entered in the **Destination** column in the section **Traffic after translation**). This anomaly has been fixed.

CLI command

Support reference 58853

The command MONITOR FLUSH STATE *X.Y.Z.A* would purge the host and connection table instead of deleting only entries concerning the host X.Y.Z.A. This issue has been fixed.

High availability

Support reference 53958

The status of firewalls' disks is taken into account when calculating the quality of a cluster's members.

Support reference 56613

Instability on the data synchronizer would cause the high availability management service to restart in loop. As a result of this malfunction, the passive firewall could potentially switch to active mode, making both firewalls in the cluster active. This issue has been fixed.

Support reference 56700

Changes made to users' preferences on the active firewall would not be synchronized with the passive firewall. This anomaly has been fixed.

Support reference 57317

Whenever the table of events to be synchronized filled up, the high availability manager would attempt a new full synchronization at the expense of the firewall's performance. This reaction has been modified, so that the mechanism now deletes the oldest events first in order to add the most recent to the queue.

Support reference 58846

In high availability configurations, interfaces that were initially inactive on the main firewall would be indicated as active after the firewall changed its role in the cluster twice (active - passive - active). This anomaly has been fixed.

Support reference 58842

After the roles of firewalls have been switched in a cluster, whenever active connections were restored in incremental mode, the parent-child relationship of these connections (connection traffic / data traffic) would not be kept. In such cases, data traffic for protocols such as FTP would therefore not be forwarded. This issue has been fixed.

Proxies

Support reference 60090

In a configuration for which:

- Web 2.0 scans were disabled (**Inspect HTML code** option unselected in the **IPS** tab of the HTTP protocol),
- The alarm "http:150 additional data at end of reply" was set to "pass",

POST HTTP requests to the proxy could cause the firewall to freeze. This issue has been fixed.

Support reference 56009

Whenever SMTP clients exceeded the amount of sent data allowed, the proxy would send a "552 Data size exceeded" response before wrongly generating an "Invalid SMTP protocol" alarm, causing the connection to end. This anomaly has been fixed.

Support reference 56619

The firewall would attempt to reuse a certificate that has just been deleted. This anomaly, which could cause the proxy to freeze, has been fixed.

IPsec (IKEv2)

Support reference 59900

During the setup of an IKEv2 IPsec tunnel, groups with which a user was associated would not be communicated to the intrusion prevention system. This anomaly has been fixed.

Support reference 59730

During the negotiation of an IKEv2 IPsec tunnel initiated by the firewall, it would send additional IP selectors that devices from other vendors (CheckPint) might not accept, thereby preventing the successful setup of the tunnel. This issue has been fixed.

SSL VPN

Support reference 48993

Whenever the SSL VPN server was reloaded, the configuration meant for the client could be incomplete and would prevent connections to the service. This issue has been fixed.

Support reference 59518

The SSL VPN server would not accept certificates containing spaces or special characters (e.g., apostrophes), and would fail to create the configuration archive that the client was supposed to download. This issue has been fixed.

Support reference 49110

SSL VPN performance has been enhanced with support for UDP in the tunnel setup phase.

PPTP

Support reference 59237

Attempts to set up a PPTP tunnel to a firewall that uses routing by interface could cause the PPTP tunnel manager to freeze. This issue has been fixed.

Network objects - Global objects

Support reference 59511

The feature allowing global objects to be exported to a CSV format did not function. This issue has been fixed.

Logs - Local storage

Support reference 59751

An improvement to the parameters for accessing the SD card on U30S, SN200 and SN300 firewalls has fixed the issue of the firewall restarting unexpectedly.

Network

LACP

Support reference 59545

Changes to the MAC address of an aggregate were not applied to the first physical interface belonging to this aggregate.

IPv6

Support reference 58635

ICMP requests, or network neighborhood discovery requests, sent to an interface configured in IPv6 with a subnet mask equal to /64 would raise an “IP address spoofing (type=1)” alarm (source address from an unprotected interface contacting a protected interface). This issue has been fixed.

Network objects

Support reference 54843 - 56211

During operations on the objects database, all entries in the firewall's ARP table would be systematically erased. Network monitoring solutions could then wrongly assume that certain hosts were uncontactable while rebuilding the table. This behavior has been modified and only permanent entries in this table are deleted during operations on the objects database.

Intrusion prevention

SMB2 protocol

Support reference 58662

An error while reading SMB2 packets during an authentication attempt via SPNEGO would wrongly raise the "Invalid NBSS/SMB2 protocol" alarm. This issue has been fixed.

Ethernet/IP protocol

Support reference 59987

The intrusion prevention module dedicated to scanning the industrial Ethernet/IP protocol would be activated by error on certain streams of UDP traffic, causing them to be blocked. This anomaly has been fixed.

Vulnerability Manager

Support reference 55973 58875

Issues with the intrusion prevention engine freezing have been resolved with the optimization of the vulnerability management mechanism for traffic originating from or going to the firewall.

Intrusion prevention engine queue

Support reference 59366

Whenever the number of connections exceeded the event queue managed by the intrusion prevention engine, the message "HA: Overflow detected while reading ASQ events, resync needed" would be generated in event logs, even though high availability was not enabled on the firewall. This message has been changed to "Overflow detected while reading IPS events, resync needed".

ICMP

Support reference 59712

A parameter setting the maximum global rate of ICMP error packets allowed per core has been added. Set by default to 25000 packet/s, this parameter can be modified in the global ICMP configuration.

Web administration interface

Filter - NAT

When comments are being edited, the use of keyboard shortcuts CTRL+C and CTRL+V would copy and paste a new filter rule instead of the relevant comment. This anomaly has been fixed.

Support reference 54930

After the *dcerpc* protocol was renamed *dcerpc_tcp*, selecting *dcerpc* in the protocol field of a filter rule would cause an error. This issue has been fixed.

Support reference 47826

Moving a collapsed rule separator would not move the filter rules associated with it. This anomaly has been fixed.

Logs - Syslog - IPFIX

Support reference 60007

Whenever the formatting of an SD card failed, the error would not be displayed while the formatting window would continue to be displayed. This issue has been fixed.

Administrators

Support reference 61167

After validating the change of the admin account password, the page would remain frozen on the message "Saving configuration, please wait...". This anomaly has been fixed.

Directory configuration

Support reference 60079

Whenever the name of several directories was derived from the name of the default directory (e.g. mycompany.eu [default] , mycompany.eu.fr, mycompany.eu.org, etc.), all of these directories would be represented as default directories in the **Users > Directory configuration** module.

Monitoring

Monitoring configuration

Support reference 59538 - 59590

Aggregated interfaces could not be selected in the list of interfaces to be monitored. This anomaly has been fixed.

QoS monitoring

Support reference 59322

The QoS monitoring history curve would not display data as the IDs of QoS queues were not taken into account. This anomaly has been fixed.

Hardware

LEDs - SN150

Support reference 58532

The *Online* LED located on the front panel of the SN150 firewall would not light up whenever the appliance started. This anomaly has been fixed.

Version 3.1.2 bug fixes

Intrusion prevention

Custom contextual protection signatures

On SN160(W) and SN210(W) firewalls, the command to validate the customized signatures definition file (`enpattern -t`) did not succeed and generated a high CPU utilization. This problem has been fixed.

New features in version 3.1.1

New models - Wireless networks

Version 3.1.1 of the firmware ensures compatibility with new Wi-Fi firewall models SN160W and SN210W.

These firewalls must therefore be updated after you receive them.

They offer all the features needed for securing Wi-Fi connections.

Wireless network management built into this version is compatible with 802.11 a/b/g/n standards. Two WLAN interfaces, and therefore distinct networks, can be configured on each firewall.

Version 3.1.1 bug fixes

System

Support reference 59936

Automatic backups

Whenever the automatic backup function was enabled, the results of the first backup would not be saved. This would then cause the backup to be wrongly relaunched on a regular basis. This anomaly has been fixed.

Support reference 59296

Authentication

Users logged on via the SSO agent method would be unable to accept sponsorship requests despite being granted the privilege to do so. This issue has been fixed.

Proxies

In configurations without Web 2.0 scans (**Inspect HTML code** option unselected in the **IPS** tab of the HTTP protocol), HTTP POST requests containing data and redirected to an authentication rule could cause the firewall to freeze.

Web administration interface

Support reference 59717 60282

Microsoft Internet Explorer 11 - Mozilla Firefox 51.0.1 or higher

An issue with the slow display of certain pages in the administration interface (e.g., **Network objects**) has been fixed.

New features in version 3.1.0

New models - Wireless networks

Version 3.1.0 of the firmware ensures compatibility with new Wi-Fi firewall models SN160W and SN210W.

These firewalls must therefore be updated after you receive them.

They offer all the features needed for securing Wi-Fi connections.

Wireless network management built into this version is compatible with 802.11 a/b/g/n standards. Two WLAN interfaces, and therefore distinct networks, can be configured on each firewall.

System

Network objects

New objects corresponding to services and service groups used by the Stormshield Endpoint Security solution have been included in the SNS firewall objects database.

IPsec VPN (IKEv2)

Diffie-Hellman DH19 NIST Elliptic Curve Group (256-bits) and DH20 NIST Elliptic Curve Group (384-bits) have been added to the encryption profiles available for IPsec IKEv2 tunnels.

IPsec VPN

A button that allow renaming IPsec peers has been added to the **Peers** tab in the **IPsec VPN** module.

Support reference 56589

Notifications

Object names associated with source and destination IP address have been added to notification reports sent by email.

Certificates and PKI

The period for verifying CRLs (Certificate Revocation Lists) used to be set at 24 hours. It can now be configured for a period ranging from 3600 seconds (1 hour) to 604800 seconds (1 week). The default value is 21600 seconds (6 hours).

These settings can only be modified via the CLI command: `PKI CONFIG UPDATE checkcrlperiod= xxxxx`.

HTTP block page

The return code associated with the HTTP block page (default value: *202 - Accepted*) can be modified using the command: `config protocol http profile proxy urlfilteringindex=X HTTPCodeOnFail=Y`.

High availability

When the quality of the passive firewall changes (e.g., when a link is lost, or when disconnecting from a power supply module), the cluster will send out an SNMP alert (TRAP) in order to warn the administrator. The firewall will also add a message resembling "The quality of

a node in the cluster has been modified: SN910XXXXXXXXXX 12 -> 11" in the system event log (*l_system* log).

In a high availability configuration with a quality factor below 100%, a warning message appears in several cases indicating that the role of a cluster member might change, in particular:

- when an interface in an aggregate is created, added or deleted,
- when a connected interface is disabled,
- when a disconnected interface is enabled,

SSL VPN

The options **Use DNS servers provided by the firewall** (*register-dns*) and **Prohibit use of third-party DNS servers** (*block-outside-dns*), respectively instructing the SSL VPN client to either write the DNS server(s) specified by the Stormshield Network firewall in its configuration or to avoid using third-party DNS servers, can be configured in the **Configuration** > **SSL VPN** module. This feature shortens the time needed for receiving responses to the client's DNS requests, especially for machines running in Microsoft Windows 10.

SSL VPN Portal

The Java Web Start application is now used instead of the standard Java application during connections to the SSL VPN portal.

Global objects

SNS firewalls now support global time objects and router objects, which can therefore be managed and deployed using the Stormshield Management Center solution.

CRL verification and support for BindAddr in the firewall's LDAP requests

In the firewall's LDAP configuration, the BindAddr parameter followed by the firewall's private IP address forces the firewall to present this IP address during LDAP requests to an external directory: LDAP traffic can therefore be encapsulated in an IPsec tunnel in order to encrypt requests to the directory.

This parameter can only be modified in command line: `setconf ConfigFiles/ldap LDAP_Name BindAddr FW_Private_IP`.

Monitoring - Reports - Audit logs

Monitoring

Each line showing a vulnerability detected on a host will now include a link to the page providing details on the vulnerability in question.

New pop-up menus can be opened by right-clicking on a line of data:

- **Hosts monitoring**: you can look for the host in logs, show details about the host, reset its reputation score, add the host to the objects database and/or add it to a group, etc.
- **User monitoring**: you can look for the value in logs, show details about the host on which a user is connected, disconnect the user, etc.
- **Connections monitoring**: you can display a full line, add the source or destination object to the objects database, show details about the host, ping the source or destination, etc.

Intrusion prevention

IEC 60870-5-104 protocol

The intrusion prevention system now scans the industrial protocol IEC 60870-5-104 (IEC 104).

HTTP

A signature context, *vbscript,* has been added to the security inspection for HTTP.

Support reference 54140

The intrusion prevention system now detects cache poisoning attempts on *Squid* web proxies and raises the block alarm *Possible HTTP proxy poisoning*.

SSL Proxy

RC4 and MD5 encryption algorithms, which are considered weak, have been removed from the list of available algorithms for the SSL proxy.

Modbus protocol

An alarm is now generated when the maximum number of Modbus servers with a UMAS reservation has been reached.

IP protocols (except TCP, UDP and ICMP)

Connections that match IP protocols different from TCP, UDP and ICMP (example: GRE) are referenced in connection statistics logs (IPStateMem , -IPStateConn, -IPStatePacket and -IPStateByte fields in the */filterstat* file).

SNi40 industrial firewalls

Hardware bypass

When hardware bypass was enabled, ongoing connections on interfaces included in the bypass were not modified and therefore ended up being shut down since the corresponding network traffic was not received. This reaction has been modified, and such connections will now be kept active until a standard network configuration is adopted again (bypass reset).

Hardware

High availability

As part of the process of resetting the firewall to its factory configuration (*defaultconfig*), the period before the hardware watchdog function is activated will now be 120 seconds compared to the previous 300.

Version 3.1.0 bug fixes

System

Authentication

Support reference 52192

Attempts to log on to the web administration interface via Google Chrome and SSL (certificate) or SPNEGO would not only fail but raise a brute force attack alarm as well. This issue has been fixed.

Support reference 56711

During the configuration of the Sponsorship method, the "Expiry of the HTTP cookie" field would not be automatically set to *Do not use*, thereby causing this authentication method to malfunction. This anomaly has been fixed.

Support reference 56595

Attempts to create new objects through the authentication policy wizard would fail and display a "?" instead of the object name. This issue has been fixed.

Support reference 59731

An encoding anomaly in sponsorship e-mails invalidated the validation link included in such e-mails. This anomaly has been fixed.

Objects

Support reference 58476 - 58944

Router objects and time objects were not retained during partial restorations of a configuration. This anomaly has been fixed.

Support reference 56113

Global objects embedded in a router object were not taken into account. This anomaly has been fixed.

Support reference 53218

Whenever an active and operational dialup (PPoE, PPTP, PPP or L2TP modem) was embedded in a router object, the router object would not retrieve its state and would therefore consider it unreachable. This issue has been fixed.

Support reference 59083

Certificates and PKI

During the renewal of certificates via SCEP (Simple Certificate Enrollment Protocol) using the `SCEP RENEW` command, whenever the Distinguished Names (DN) of such certificates contained more than one attribute of the same type (e.g. OU, CN, O, etc.), only the first occurrence of the attribute would be kept after the operation. This anomaly has been fixed.

Support reference 51618

SSL VPN Portal

Connections to application servers through the SSL VPN portal application no longer functioned in version 3. This issue has been fixed.

SSL VPN

Support reference 58856

The maximum number of SSL VPN tunnels physically allowed on Netasq U model S series firewalls was lower than the expected number of tunnels. This anomaly has been fixed.

Support reference 52972 - 53289

An issue that could prevent new SSL VPN tunnels from being set up (connection blocked at the "GET CONF" stage) has been fixed.

Proxies

Support reference 52034

Whenever a filter rule used the explicit proxy, the authentication rules contained in the filter policy would not take into account this proxy's different listening port (TCP/8080 by default). This anomaly has been fixed.

Support reference 55700

An anomaly regarding the maximum length of a user name and domain that make up an email address has been fixed.

Support reference 54003

The HTTP proxy would mistakenly consider some downloads as partial downloads. This anomaly has been fixed.

Support reference 56464

An anomaly while reading information located behind the domain name specified in the *EHLO* command would wrongly cause the corresponding SMTP traffic to be blocked.

Support reference 52848

After sandboxing an email, the name of the attachment referenced in the logs would be wrong. This issue has been fixed.

Support reference 49996

An anomaly in the management of the Internet Content Adaptation Protocol's (*ICAP*) responses in *Request Modification* (*reqmod*) mode would either cause the overconsumption of memory resources or the HTTP proxy to be blocked.

Support reference 57326

Whenever an e-mail contained a wrong end-of-line command in its data, the connection would be reset only between the client and the firewall while the server would have to wait until the connection timed out. This anomaly has been fixed.

Support reference 58824

Whenever a client sent a RESET command to the mail server, the connection would be reset only between the client and the firewall while the server would have to wait until the connection

timed out. This anomaly has been fixed.

Support reference 56475

Whenever an e-mail contained a sender or recipient address exceeding the size defined by the RFCs (local part or domain name), the proxy would fail to shut down the connection after sending the error message ("553 Localpart too long" or "553 Domain name too long"). This issue has been fixed.

Support reference 59420

The proxy would occasionally refuse to run on a firewall using a filter rule with at least one of its log destination checkboxes unselected (**Advanced properties** tab in the **Action** module in the filter rule editing window). This issue has been fixed.

Support reference 58567

Resetting to factory configuration

The help provided with the reset script (*defaultconfig*) would offer the wrong explanation for the option "–D" (*Only Restore the data partition on G2 hardware*). This anomaly has been fixed (*Only Restore the data partition*).

Support reference 56394

Proxies – SN 910 model firewalls

Limits on the number of connections allowed for proxies (HTTP, SSL, SMTP, POP3 and FTP) on SN910 model firewalls were incorrect. They have been increased in order to match this model's actual performance.

Support reference 57286

IPsec

In configurations that contain a site-to-site IPsec tunnel and an anonymous IPsec policy (nomad users), disabling the site-to-site tunnel (tunnel status *off*) would not delete the peer of the IPsec configuration file. This anomaly, which would cause nomad connections to malfunction, has been fixed.

IPsec (IKEv2)

Support reference 54831

During Phase 1 renegotiations of IPsec tunnels in IKEv2, the IPsec engine would destroy the existing SA (Security Association) as well as child SAs before negotiating the new SA.

Since this could cause significant packet loss, the behavior of the engine has been modified so that it negotiates the new SA first before destroying older ones.

Support reference 59152

An issue that could prevent the setup of IPsec IKEv2 tunnels to SN150 model firewalls has been fixed.

Support reference 59280

The number of IKE SAs for the same IPsec IKEv2 tunnel would increase over time without diminishing the number of unused SAs. This anomaly has been fixed.

High availability

Support reference 56268

Whenever an interface was added to or deleted from an aggregate (LACP), the change was not applied in the quality indicator in the high availability mechanism. This anomaly has been fixed.

Support reference 57056

An optimization in the parameters that detect the loss of an active firewall due to electrical issues (*ConsensusTimeout* parameter) has considerably shortened the time taken for a cluster to switch.

Support reference 56613

After the high availability management engine has been restarted several times by accident, the associated tokens would not be deleted. The token table could then become saturated, therefore preventing other services on the firewall from starting. This issue has been fixed.

Support reference 56478

Instability on the data synchronizer would cause the high availability management service to restart in loop. As a result of this malfunction, the passive firewall could potentially switch to active mode, making both firewalls in the cluster active. This issue has been fixed.

Support reference 50048

Changing roles after the active member of the cluster has been restarted could cause the IPsec tunnels negotiated by both members of the cluster to be desynchronized.

Support reference 54289 - 58842

After the roles of firewalls have been switched in a cluster, whenever active connections were restored, the parent-child relationship of these connections (connection traffic / data traffic) would not be kept. Data traffic for protocols such as FTP would therefore not be transferred. This issue has been fixed.

Support reference 55076

Application protection

In configurations that use the Karspersky antivirus engine, scanning zip bomb files could cause the temporary partition to saturate, leading in turn to a significant CPU load and resulting in an analytical error. This issue has been fixed.

Filter - NAT

Support reference 56570

Whenever the name entered for a filter rule exceeded the maximum length allowed, the length allowed would not be specified in the error message. This anomaly has been fixed and it now indicates that names must not exceed 255 characters.

Support reference 56672

When scrolling over a service group used in a filter rule, the tooltip that sets out all the services included in the group would not appear. This anomaly has been fixed.

Support reference 58535

When scrolling over a service used in a filter rule, incomplete information would be given in the tooltip. This anomaly has been fixed.

Support reference 59297

When scrolling over an *IP address range* network object used in a filter rule, the tooltip would wrongly display the message "Object not found". This anomaly has been fixed.

Support reference 55190

Policy-based routing (PBR)

In a configuration such as the following:

- A static route is applied to a network,
- A filter rule implements policy-based routing (PBR) to the same network for a particular port,
- Address translation is applied when packets leave the firewall,

reloading filter rules would prevent connections matching the PBR rule from being set up.

Support reference 50977

Dynamic DNS

Changes to the firewall's IP address were no longer applied to the Dynamic DNS provider whenever the SSL protocol was used, and the verification of this provider's certificate would even fail. This issue has been fixed.

Support reference 55728

Configuration

Changes made to the name of the firewall (**System** > **Configuration** module) were neither applied to the sender name for email alerts, nor in the SN Real-Time Monitor dashboard. This anomaly has been fixed.

Support reference 56734

System events

The report generated whenever a brute force attack was blocked would not contain the blocked source IP address. This anomaly has been fixed.

Network

Support reference 57328

VLAN

The firewall would not correctly send the last fragment of a UDP packet meant to go through a VLAN to the parent interface of the VLAN. This issue has been fixed.

Virtual interfaces

Support reference 53881

Whenever a GRE virtual interface that was initially created as inactive was assigned an IP address, its change in status would not immediately be applied in the web administration interface. The user would therefore need to change modules before going back to the virtual interface module in order to view this change. This anomaly has been fixed.

Support reference 58685

Outbound throughput statistics of virtual IPsec interfaces would always display a null value. This anomaly has been fixed.

Intrusion prevention

Support reference 57396

For certain streams of traffic that always use the same source port, whenever they passed through a rule in firewall or IDS mode, resetting the first connection would prevent the setup of the connections that immediately follow. These connections would, in fact, have been considered reset as well. This issue has been fixed by allowing the same source port to be reused in firewall and IDS modes (*TCP Closed FastReuse*).

Support reference 53011 - 58465

TeamViewer application

After an upgrade of the TeamViewer application, the IPS scan of traffic relating to this application would wrongly set off an "Unknown SSL protocol" block alarm. This issue has been fixed.

Support reference 53094

RTSP (Real-Time Streaming Protocol)

The intrusion prevention system would wrongly block the *Scale* header in the *Play* method. This anomaly has been fixed.

Support reference 51867

HTTP

In configurations that use policy-based routing (PBR) for HTTP traffic, enabling the **Apply the NAT rule on scanned traffic** option (**Global configuration** of HTTP in the **Application protection** > **Protocols** module) would cause the incorrect routing of packets generated by the proxy.

Support reference 53640

As the *YouTube for Education* filter mechanism is no longer active, it has been replaced with the *Youtube restrictions* mechanism. This new mechanism can be enabled and configured (strict or moderate restriction) in the **IPS** tab in HTTP (**Application protection** > **Protocols** module).

Support reference 58409

SIP

The maximum number of child connections allowed for SIP has been increased in order to allow:

- 127 simultaneous calls on U30S, U70S, SN150, SN160W, SN200, SN210W and SN300 models,
- 127 simultaneous calls on U30S, U70S, SN150, SN160(W), SN200, SN210(W), SN300 and SN310 models,
- 1023 simultaneous calls on other models,

instead of 16 as was previously the case on all models.

Support reference 53886

ICMP

Whenever several ICMP requests were received or sent with the same identifier, the same sequence and different data, the firewall would not take into account reply packets from the first request and would block the requests that follow ("ICMP ECHO paylod modified" alarm). This anomaly has been fixed.

Web administration interface

Support reference 54459

SSL protocol

Whenever a checkbox was selected in the **SSL negotiation** section of a given profile, and such a change was applied, the same checkbox would be selected in all profiles by mistake. This issue has been fixed.

Monitoring - Reports - Audit logs

Support reference 56766

Reports

On firewall models that do not have log partitions (diskless models), an anomaly with the checkbox for enabling reports (**Local storage** tab in the **Notifications** > **Logs - Syslog - IPFIX** module) has been fixed.

Support reference 57247

Monitoring

Whenever reports and history graphs were both disabled (**Notifications** > **Report configuration** module), history graphs covering the past 30 days could not be displayed. This issue has been fixed.

Support reference 53352

Logs

Commands to monitor inactive services on the firewall (*MONITOR POWER*, *MONITOR FWADMIN*,...) were wrongly logged in the *l_server* log file. This anomaly has been fixed.

Support reference 54926

Multicast routing

User accounts holding all administration privileges were unable to apply configuration changes made in the **Network** > **Multicast routing** module (error message "There is nothing to save"). This anomaly has been fixed.

Stormshield Network Real-Time Monitor

Support reference 58502 - 57414

Users

The command to delete users, available via the pop-up menu (right-click) in the **Users** module, no longer worked. This issue has been fixed.

New features in version 3.0.3

System

SNMP

A new OID (Object Identifier) ntqifDrvName corresponding to the system names of network interfaces has been added to the NETASQ-IF-MIB (Management Information Base) .

Directory configuration

The field that defines the name of an LDAP directory has been renamed "Domain name".

Version 3.0.3 bug fixes

System

Authentication

Support reference 58610

Migrating a configuration that uses the "Guest" authentication method together with the customized "e-mail" field would cause an error on the captive portal as this field was not converted properly. This anomaly has been fixed.

Support reference 58816

Attempting to upgrade a configuration with a customized firewall name (**Configuration** module) and the **Use firewall name or certificate CN as FQDN** option selected (**Captive portal** – **Advanced properties** tab in the **Users > Authentication** module in version 2) to version 3 of the firmware would make SPNEGO ineffective.

Directory configuration

Support reference 58512

When migrating configurations that reference external LDAP directories to version 3, such directories would adopt the object name of the LDAP server instead of the domain name. This anomaly, which made the SSO Agent method ineffective, has been resolved and the name of the directory is now made up of the root domain (base DN) declared during its creation.

Support reference 58883

Attempts to migrate to version 3 configurations that reference external LDAP directories with a root domain (DN) containing one or several uppercase letters would render such directories invalid. This issue has been fixed.

Support reference 58825

Filtering and NAT

The display would not refresh during switches from a local filter policy to a global filter policy bearing the same index.

Support reference 58475

SSL VPN portal

The latest versions of the Java client application could prevent connections to servers that can be contacted via the SSL VPN portal as they would reject certificate authorities signed with MD5. This issue has been fixed.

Support reference 58746

Access privileges

The selection of a user in the **Detailed access** tab in the **Access privileges** module would result in his/her identifier being replaced with his/her first and last names. This issue, which caused authentication to malfunction, has been fixed.

Intrusion prevention

Support reference 58572 58589 58742 58553

HTTP

An anomaly in the HTTP security inspection would cause the firewall to hang and the proxy to consume an excessive amount of CPU resources. This anomaly has been fixed.

Web administration interface

Directory configuration

Support reference 58871

Backup servers added to the advanced properties of external directories (Microsoft Active Directory, external LDAPs or PosixAccount LDAPs) would no longer appear after a user browses in the other modules of the web administration interface. This anomaly has been fixed.

Support references 58734 - 58704 - 58900

The web administration interface would not apply changes made to the selection filter of user groups in external directories (**Structure** tab in the directory). This anomaly has been fixed.

Monitoring - Reports - Audit logs

Support reference 58921

User monitoring

When several users were authenticated and connected, refreshing the user monitoring module using the Refresh button would cause the firewall to hang. This issue has been fixed.

Activity Reports

On firewall models that do not have log partitions (diskless models), once the 5 reports allowed were enabled, the corresponding data would not be displayed.

Version 3.0.2 bug fixes

Intrusion prevention

Support reference 57337

SSL protocol

An issue regarding access to websites using CHACHA20 and Poly1305 encryption suites has been fixed following the upgrade of these suites.

System

Support reference 57350 57356

SSL VPN - IPsec VPN

After a migration to SNS v3, connections via the SSL VPN client or IPsec VPN client could fail to function as the *sslvpn* and *ipsec* interfaces were linked to the *Guest* profile. This issue has been fixed and these interfaces will no longer be associated with any profile after a migration.

Support reference 58536

Authentication

A migration to SNS v3 could cause the *Internal* profile of the captive portal to be associated with an unknown interface ("0" interface). This anomaly, which would then prevent these associations from being modified (*Captive portal* tab in the **Configuration > Users > Authentication** module), has been fixed.

Support reference 58433

Proxies

Enabling the DNS cache before a proxy cache could cause the proxy to hang when the firewall is restarted.

Support reference 56184

Filtering

It was impossible to add URLs that were accessible without authentication in a filter rule specifying a redirection to the authentication portal. This issue has been fixed.

High availability

Support reference 58530

In a high availability configuration, the synchronization mechanism could wrongly attempt to enable the hardware *bypass* system reserved for industrial firewalls (SNi40 model). This anomaly, which would generate a synchronization error, has been fixed.

Support reference 58367

The upgrade of a firewall cluster to version 3 could fail during the synchronization of the license file with the passive appliance. This issue has been fixed.

Support reference 58113

Extended Web Control

If the synchronous mode of the Extended Web Control URL filtering solution was enabled on a firewall in version SNS v2, this mode will be automatically disabled in favor of asynchronous

mode during a migration of the firmware to v3.0.2.

Support reference 58496

Automatic backups

Enabling automatic backups in a configuration using several LDAP directories could fail and disable the LDAP module. This issue has been fixed.

Dashboard

Support reference 56635

LDAP configuration

The dashboard of a firewall that does not have a configured LDAP directory would display a misleading message ("LDAP configuration: Disabled. The directory has been configured but the module has not been enabled"). This anomaly has been fixed and the message "No default directory has been configured or enabled" will now appear.

New features in version 3.0.1

SN150 model firewalls

Version 3.0.1 of the firmware ensures compatibility with SN150 firewalls.

Version 3.0.1 bug fixes

Intrusion prevention

Support reference 56973 57355

IDS / Firewall modes

In a configuration that implements filter rules in IDS or Firewall mode and authentication, invalid ICMP traffic that raises alarms which do not block such traffic (*Pass* action) would cause the firewall to hang. This issue has been fixed.

Support reference 56740

Memory resources

Whenever there is a large number of connections, an anomaly in the management of memory resources would cause the firewall to hang then restart. This anomaly has been fixed.

System

Support reference 56964

IPsec tunnels (IKEv2)

Whenever the email address field of a CA used for signing server certificates was filled in, the firewall would refuse to set up IKEv2 IPsec tunnels for which authentication was based on such certificates. This anomaly has been fixed.

Activity Reports

"Host reputation" report

An error in the application of destination host reputations for SSL connections has been fixed.

New features in version 3.0.0

Unified web interface

The unified web interface now covers the administration, monitoring and reporting of Stormshield Network firewalls.

A new monitoring window offers graphs (in real time and with history statistics) on system resources used (memory and CPU), throughput per interface and connected users as well as detailed information on machines (ongoing connections, applications used, vulnerabilities detected, etc).

Many interactive features facilitate the search for incidents and the administration of Stormshield Network firewalls.

Wireless networks

Wireless networks compatible with 802.11 a/b/g/n standards are now supported on the new SN160W and SN210W models.

Every firewall offers all the features needed for securing Wi-Fi connections.

Temporary user management

In order to provide easy Internet access to persons outside the organization or in public places, Stormshield Network products offer advanced features for managing temporary users.

In addition to guest mode, which was already available, version 3 includes "sponsorship" mode and a new portal to create temporary accounts.

The current "guest" portal may be enriched with new fields (first name, last name, e-mail address, etc) that the user will need to enter before accepting the Internet access charter.

Temporary accounts can be created easily thanks to a simplified screen that can only be accessed by persons authorized to create such accounts.

"Sponsorship" mode makes it possible to delegate - to an authorized person - the privilege of accepting or rejecting an Internet access request from a person outside the organization.

Many enhancements allow customizing users' various access portals.

Integration into a multi-domain environment

Users can now be authenticated on several Active Directory domains. It is therefore possible to authenticate users originating from various domains and applying distinct security policies to them.

Multiple directories also offer the possibility of registering firewall administrators in an internal directory and managing unprivileged users in an external directory.

IP geolocation - Country-based filtering

Thanks to the geolocation feature, administrators gain visibility over the source or destination of their network traffic. Security policies can therefore be adapted to filter traffic according to new geographical criteria represented by "Country" or "Continent" objects.

All log files and reports have been enriched with a new item corresponding to the country.

IP Reputation – External host reputation

This feature, which can be combined with geolocation, makes it possible to lower an organization's attack risk.

Public IP addresses with a bad reputation (e.g.: Tor exit nodes) will fall under one of seven categories: Spam, Phishing, Anonymizer, Botnet, Malware, Tor or Scanner. These categories are regularly updated through the Active Update mechanism.

Through his security policy, the administrator can therefore block external machines with bad reputations from attempting to access the organization's network, and prohibit connections from internal workstations to reputedly risky hosts.

Dynamic Host Reputation – Internal host reputation

Security policies can now be assigned based on the reputation of internal hosts.

Reputations, represented by a score, can be calculated dynamically thanks to ratings provided by the inspection engines built into Stormshield firewalls. Whenever our sandboxing solution detects a virus, raises a major alarm or identifies malware, the host's score will automatically be raised.

Administrators can view the history of a host's reputation score in the new "monitoring" module. Other indicators such as the average score of a network and the maximum score, provide addition information to help them define their security policies and act on hosts that require intervention.

This feature requires the use of a SD card if there is no hard disk on the firewall.

"DNS names (FQDN)" objects

In order to refine a security policy, it is now possible to use network objects defined only by their FQDN (IP address(es) automatically retrieved by DNS resolutions) such as "google.com" or "office365.com".

Safe transmission of Syslog traffic through the TLS protocol

The transmission of logs to one or several Syslog servers (maximum 4) via TCP can now be secured through the TLS protocol with client and server certificate authentication.

This secure transmission of Syslog traffic is compatible with the Stormshield Visibility Center solution.

Stormshield Network firewalls support several standardized formats of Syslog messages (RFC3164, RFC5424, RFC5425 and RFC6587).

Possibility of configuring the hash algorithm in the internal PKI and the SSL proxy

The Certificates and PKI module offers the possibility of selecting the hash algorithm (in particular SHA256) used for the certificates of the SSL proxy and the firewall's internal PKI.

IPFIX/Netflow support

Compatibility with Netflow/IPfix collectors allows administrators to easily identify potential network issues.

Customized signatures on the intrusion prevention (IPS) engine

Administrators can now create their own context-based signatures in order to detect applications inside the organization.

SNi40 - Hardware bypass

In order to ensure service continuity in an industrial setting, the SNi40 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.

Importing and exporting the contents of the network objects database

Exporting the objects database in CSV format makes it possible to save the database and reimport it directly into the Stormshield Management Center centralized administration solution.

The structure of the rows that make up the objects database in CSV format is available in the section **Structure of an objects database in CSV format** of the **Stormshield Network Configuration and Administration Manual**.

Official support for KVM and Hyper-V virtualization platforms

Stormshield Network virtual firewalls are available for Microsoft Hyper-V (VHD format) and KVM platforms (Kernel-based Virtual Machine - QCOW2 format). The supported versions of hypervisors are listed in the **Compatibility** section of this document.

Intrusion prevention scans on HTTP traffic with on-the-fly decompression

The intrusion prevention engine is now capable of decompressing HTTP data on the fly in order to perform IPS scans on this protocol. The firewall therefore no longer needs to modify the headers of HTTP packets sent by the client in order to mask compression support (*accept-encoding*). As a result, this mechanism reduces latency and the amount of data needed for transferring HTTP packets, but demands a greater amount of the firewall's resources.

This feature is enabled by default and can be suspended in the HTTP configuration module.

Possibility of adding a constraint on the *Domain name* of the certificate presented by an IPsec peer.

When a certificate authority (CA) is specified in the list of trusted authorities for the establishment of IPsec tunnels, a constraint can be added on the Domain Name (DN) of the certificate presented by the peer in order to strengthen security.

CRL verification and support for *BindAddr* in the firewall's LDAP requests

In the firewall's LDAP configuration, the BindAddr parameter followed by the firewall's private IP address forces the firewall to present this IP address during LDAP requests to an external directory: LDAP traffic can therefore be encapsulated in an IPsec tunnel in order to encrypt requests to the directory.

This parameter can only be modified in command line (setconf ConfigFiles/ldap *LDAP_Name* BindAddr *FW_Private_IP*).

IPS scans of the Ethernet/IP industrial protocol

The intrusion prevention engine now allows filtering (*Analyze / Block*) public command sets for this protocol. A customized list of Ethernet/IP commands that need to be allowed can also be specified.

Intrusion prevention scans for SNMP

SNMP (Simple Network Management Protocol) is a network equipment monitoring protocol. The IPS scan for this protocol has been particularly enriched. It therefore now possible to allow or block SNMP packets according to the version of the protocol (SNMPv1, v2c or v3), create community whitelists/blacklists (SNMPv1 and v2c), identifiers (SNMPv3) or OIDs (*Object Identifier*).

NAT support for Dynamic DNS

The module that sends the public IP address to the dynamic DNS registration service provider now distinguishes the real public IP address presented by a NAT router from the local address. This feature can be enabled by selecting Support address translation (NAT) in the advanced properties of the Dynamic DNS module.

SSL proxy - Support for new encryption algorithms

The SSL proxy supports new encryption algorithms based on elliptic curves (ECDSA algorithm: Elliptic Curve Digital Signature Algorithm).

Systematic verification of unused objects

The **Network objects** module displays the list of objects found in the firewall's database; objects are classified by category (hosts, networks, DNS domain names [FQDN], etc).

A colored symbol appears before each object, dynamically indicating whether the object is being used in the firewall's configuration (green chip) or not (gray chip). Clicking on the "eye" icon located to the right of a green chip will list all the modules using the object in question.

Rule names in IPS logs and active connection logs

The Filter and NAT module makes it possible to assign a name to each rule created. Do note that the "Name" column is hidden by default.

This rule name (*rulename*) is referenced in IPS logs and connection logs. It has the advantage of not changing according to rule criteria (via, interface, etc) or the position of a rule in a filter

policy, unlike rule identifiers (*ruleid*). As such, filter or NAT rules can be easily handled according to their names.

Exporting monitoring data and audit logs

In the same way as report data, the information displayed in audit logs and the data presented in the tables of the monitoring module can also be exported to a file in CSV format.

Sandboxing – Form to report false positives

The interactions offered on audit logs allow warning Stormshield of any wrong categorization following a sandboxing operation. This feature therefore makes it possible to unblock attachments that have been wrongly considered malicious.

Authentication

The maximum length of an identifier has been raised to 255 characters. Moreover, users can now be included in 250 groups (this limit used to be 50 in older versions).

SSL VPN

The SSL VPN Client configuration file now includes register-dns and block-outside-dns options indicating, respectively, for the client to write the DNS server(s) specified by the Stormshield Network firewall to its configuration, and to not use third-party DNS servers. This feature shortens the time needed for receiving responses to the client's DNS requests, especially for machines running in Microsoft Windows 10.

Child connections (active FTP) through virtual IPsec interfaces

Traffic that creates child connections (e.g.: active FTP) is now compatible with the use of virtual IPsec interfaces (VTI).

TCP-based DNS requests

Stormshield Network firewalls automatically switch their DNS requests over to TCP whenever they receive a response exceeding 512 bytes (response with many entries such as dynamic objects and DNS name objects [FQDN]).

Addition of logs in stateful pseudo-connections

Stateful pseudo-connections (GRE, ESP, etc) now generate registrations in connection log files (*l_connection*) and filter statistics files (*l_filterstat*).

Support for generic 3G/4G modems

For generic 3G/4G modems whose characteristics are not automatically recognized, up to two profiles grouping configuration information (model, vendor ID, etc) can be defined, such information having to be manually entered. The various fields to configure are explained in the section **Creating a modem** in the **Stormshield Network Configuration and Administration Manual**.

Strengthening the IPS scan on TCP

The TCP IPS scan has been strengthened in order to detect data in RESET packets and setting off the specific alarm "TCP RST with data". It can now also handle a larger amount of unacknowledged data without setting off alarm no. 84 "TCP data queue overflow".

Other features

- Improvement of the intrusion prevention scan on the SSL protocol with regard to fragmented headers
- Support for Unicode international characters in certificates
- Inclusion of source and destination object names in alarm e-mails
- Addition of the firewall's system name in Shell command prompts

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.

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