STORMSHIELD

STORMSHIELD NETWORK SECURITY

RELEASE NOTES

Version 4

Document last update: December 2, 2020

Reference: sns-en-release_notes-v4.1.2

Table of contents

Version 4.1.2 bug fixes

IMPORTANT
Firewalls that are part of an IPSec x509 topology (certificate-based authentication) deployed via SMC (Stormshield Management Center) **must not be** updated to version 4.1.1 or 4.1.2.
For more information on this topic, refer to this article in the Stormshield knowledge base.

IMPORTANT

In certain conditions, the proxy can be impacted by a memory leak, leading to unwanted restarts of the service. If you believe you have been affected by this problem, please contact Stormshield support.

System

Multi-user authentication

Support reference 78887

After CSP (content-security-policy) directives were implemented in phases on some websites and these directives were verified by mainstream browsers, users who have SNS multi-user authentication would see a degraded display of such websites.

This issue was fixed by adding the firewall's FQDN to the list of websites allowed to use external resources for the sites in question.

Support reference 78677

After the recent implementation of a new security policy on mainstream web browsers, SNS multi-user authentication would longer function. Depending on the web browser used, the error message "Too Many Redirects" or a warning would appear in the browser's web console.

To fix this issue, the authentication cookies that the proxy generates now contain the attributes "SameSite" and "Secure" when HTTPS is used.

When a user visits an unsecured website, i.e., one that uses HTTP, the "Secure" attribute of the cookie cannot be used. The web browser must be manually configured to enable browsing on these websites again.

Find out more

Proxies

Support reference 78190

The mechanism that generates system event and alert notifications has been optimized to no longer excessively increase the CPU load when the number of connections passing through the firewall surges.

Intrusion prevention

RDP/COTP protocols

Support reference 78923

The mechanism that evaluates filter rules in connections that involve RDP/COTP now correctly applies related translation rules again, and no longer wrongly blocks such traffic.

Compatibility

Lowest version required

You need at least version 3.x of Stormshield Network in order to upgrade to 4.1.2.

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 6.0, 6.5 and 6.7
Citrix Xen Server	Version 7.6
Linux KVM	Red Hat Enterprise Linux 7.4
Microsoft Hyper-V	Windows Server 2012 R2

Stormshield Network client software

SSO Agent Windows	Version 2.0
SSO Agent Linux	Version 2.0
SSL VPN client	Version 2.8
IPSec VPN Client	Version 6.64.003

Operating systems for SN Real-Time Monitor

Microsoft Windows	Version 10
Microsoft Windows Server	Version 2012 R2 Version 2016

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.

Recommendations

Before you migrate an existing configuration to version 4 of the firmware, ensure that you have:

- 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

PROFINET RT protocol

Support reference 70045

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

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

SN160, SN210(W) and SN310(W) firewall models - Bird dynamic routing

Since version 4.0.1 of the firmware based on a new version of FreeBSD, the internal name for interfaces has changed for SN160, SN210(W) and SN310(W) firewall models. For configurations based on these firewall models and which use Bird dynamic routing, the dynamic routing configuration must be manually changed to indicate the new network interface names.

EVA (Elastic Virtual Appliances)

You are advised to set the memory of an EVA to 2 GB if you use the antivirus and sandboxing features frequently.

Microsoft Internet Explorer

The use of Microsoft Internet Explorer browsers, including version 11, may adversely affect user experience. You are therefore strongly advised to use the browsers listed in the Compatibility section.

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 4.

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

System

Support reference 78677

Cookies generated for multi-user authentication

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

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

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

Find out more

Preferences in the web administration interface

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

Support reference 51251

DHCP server

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

Updates to a lower version

Firewalls installed with firmware in version 4 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 4.0.1 version to a 3.x version.

Support reference 3120

Configuration

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

Restoring backups

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

Dynamic objects

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

DNS (FQDN) name objects

DNS name objects cannot be members of object groups.

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

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

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

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

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

Filter logs

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

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.

Kaspersky antivirus

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

Link aggregation (LACP)

Support reference 76432

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

IPSec VPN

Obsolete cryptographic algorithms

Several obsolete cryptographic algorithms (md5, hmac_md5, non_auth, blowfish, des, cast128 and null_enc) will be removed from VPN configuration parameters in a future version of SNS. A warning message now appears to encourage administrators to modify their configurations.

Obsolete use of backup peers

The use of backup peers (designated as the “Backup configuration”) is obsolete. A warning message appears to encourage administrators to modify their configurations.
For this configuration, use virtual IPSec interfaces instead, with router objects or dynamic routing.

Interruption of phase 2 negotiations

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

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

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

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

IPSec - 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 firewall's processors.

PKI

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

A CRL can be made mandatory with the use of the "CRLRequired=1" parameter in the CLI command "CONFIG IPSEC UPDATE".

Support reference 37332

DPD (Dead Peer Detection)

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

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

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

Keepalive IPv6

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

IPSec VPN IKEv2

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

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

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

High availability

Migration

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

HA interaction in bridge mode and switches

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

Policy-based routing

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

Models

High availability based on a cluster of firewalls of differing models is not supported. Clusters in which one firewall uses 32-bit firmware and the other uses 64-bit firmware are also not allowed.

VLAN in an aggregate and HA link

Support reference 59620

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

Network

4G modems

Support reference 57403

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

Spanning Tree protocols (RSTP / MSTP)

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

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

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

Interfaces

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

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

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

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

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

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

Bird dynamic routing

With the Bird dynamic routing engine in version 1.6.7, in configurations that use BGP with authentication, the "*setkey no*" option must be used. For further information on Bird configuration, refer to the **Bird Dynamic Routing** Technical Note.

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

Policy-based routing

If the firewall has been reset to its factory settings (*defaultconfig*) after a migration from version 2 to version 3 then to version 4, the order in which routing will be evaluated changes and policy-

based routing [PBR] will take over priority (policy-based routing > static routing > dynamic routing > ... > default route). However, if the firewall has not been reset, the order of evaluation stays the same as in version 1 (static routing > dynamic routing > policy-based routing [PBR] > routing by interface > routing by load balancing > default route).

IPv6 support

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

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

High availability

In cases where the firewall is in high availability and IPv6 has been enabled on it, the MAC addresses of interfaces using IPv6 (other than those in the HA link) must be defined in the advanced properties. Since IPv6 local link addresses are derived from the MAC address, these addresses will be different, causing routing problems in the event of a switch.

Notifications

IPFIX

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

Activity reports

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

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

Intrusion prevention

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.

GRE protocol and IPSec tunnels

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

HTML analysis

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

Instant messaging

NAT is not supported on instant messaging protocols

Support reference 35960

Keep initial routing

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

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

NAT

H323 support

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

Proxies

Support reference 35328

FTP proxy

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

Filtering

Out interface

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

Multi-user filtering

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

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

Geolocation and public IP address reputation

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

Host reputation

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

Support reference 31715

URL filtering

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

Authentication

Captive portal - Logout page

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

SSO Agent

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

Support reference 47378

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

Multiple Microsoft Active Directory domains

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

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

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

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

Multiple directories

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

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

CONNECT method

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

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

Temporary accounts

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

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

Vulnerability management

Support reference 28665

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

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

Stormshield Network administration suite

Support reference 28665

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

Documentation resources

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

Guides

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

Technical notes

- SSO configuration: Microsoft SPNEGO
- Configuring "guest" methods
- Stormshield Network SSO Agent for Windows
- Stormshield Network SSO Agent for Linux
- Automatic backups
- Basic configuration in command line interface (CLI)
- Complying with regulations on personal data
- Configuring a 3G/4G modem on SNS
- Custom contextual protection signatures
- Filtering HTTPS connections
- Stacking: distribution of traffic among several firewalls
- High availability on SNS
- Identifying industrial protocol commands going through the firewall
- Implementing a filter rule
- Initial configuration via USB key
- Adapting the SES security policy of a workstation to its SNS reputation
- Collaborative security
- Collaborative security
- Secure Return option
- Software Restoration via USB key
- Updating IPMI firmware
- Exchanging a power supply module
- Description of audit logs
- BIRD dynamic routing
- EVA on Amazon Web Services
- EVA on Microsoft Azure

- VMWare NSX - SNS firewall as a peripheral router
- IPSec virtual interfaces
- Integrating NAT into IPSec
- SSL VPN tunnels
- IKEv1 Mobile IPSec VPN - Authentication by pre-shared key
- IKEv2 Mobile IPSec VPN - Authentication by pre-shared key
- IPSec VPN: Authentication by pre-shared key
- IPSec VPN: Certificate-based authentication
- IPSec VPN: Hub and spoke configuration

Videos

- CLI commands and scripts, available on Institute.

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

Downloading this version

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 4.1.2 version of Stormshield Network Security:

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

Checking the integrity of the binary files

To check the integrity of Stormshield Network Security binary files:

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

Previous versions of Stormshield Network Security 4

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

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

New features in version 4.1.1

Option to disable protected mode or stealth mode

Improvements have been made to “protected” mode; it can now be disabled, which makes it possible to respond to ICMP requests (option **Enable stealth mode** in the **Application protection** > **Protocols** > **IP protocols** > **IP** module > **Global configuration** tab).

This option allows the firewall to be integrated more easily into existing infrastructures by moderating protected 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 packets have the DF bit ("Don't fragment") and an MTU that is too low: the firewall blocks the packet, sends a response ICMP packet and decrements the TTL ("Time To Live").

Intrusion prevention

Filtering and analysis of IEC61850 protocols

SNS version 4.1 supports the IEC61850 protocol analysis (MMS, Goose and SV) and verifies the compliance of IEC61850 packets that pass through the firewall.

These protocols are used mainly in infrastructures that transport electricity to control, oversee and monitor electrical controllers

RDP protocol

The protocol analysis for RDP traffic has been improved.

HTTP

Protocols derived from HTTP report a specific alarm (alarm 732 "HTTP: invalid upgrade protocol stack") that allows the user to configure alarms an filters more granularly for these protocols.

DHCP client

New DHCP options (60 [vendor-class-identifier], 77 [user-class] and 90 [authsend]) allow SNS firewalls to authenticate on networks of telecoms operators that offer VLAN services. SNS firewalls can therefore be integrated into the operator's network without the need for the PPPOE connection mode.

These options can only be modified through the *CLI / Serverd* command:

```
config network interface update ifname=xxx DHCPVendorClassId="aaa"
DHCPUserClass="bbb" DHCPAuthsend="ccc"
config network interface activate
```

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

Update

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

New SNi20 firewall models

Compatibility

Version 4.1.0 of the firmware ensures compatibility with new SNi20 industrial firewalls.

In order to ensure service continuity in an industrial setting, the SNi20 firewall is equipped with a hardware bypass function, which when enabled, allows network traffic to pass through in the event of a power outage or appliance breakdown.

Hardware-based security for VPN secrets

SNi20 firewalls are equipped with a trusted platform module (TPM) that secures VPN secrets. With the TPM, a level of security can be added to SNi20 appliances that act as VPN concentrators, which may not necessarily be physically secure. Support for this module begins with this version 4.1.0.

SNi20 and SNi40 model firewalls

Link aggregation

Link aggregation (LACP) is now supported on SNi20 and SNi40 firewall models starting from version 4.1.0.

Network loop management protocols

RSTP and MSTP network loop management protocols are now supported on SNi20 and SNi40 firewall models starting from version 4.1.0.

Serverd

To reduce the attack surface on SNS, the Serverd service can be configured to listen only on the firewall's loopback address. This behavior is enabled by default on firewalls in factory configuration,

and can only be modified with the command:

```
CONFIG CONSOLE SERVERDLOOPBACK state=0/1
```

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

IPSec VPN mobile peers

Multiple mobile policies can now be supported simultaneously when peers are distinguished by their logins (ID). These policies can be added in **Configuration > VPN > IPSec VPN**, *Peers* tab.

Using the peer's login (ID) also makes it possible to change the VPN configuration of a particular mobile peer distinguished by its login, without affecting the tunnels of other mobile peers.

Admin account

To change the password of the *admin* user (super administrator), the old password now needs to be entered as well.

IPSec VPN and LDAP groups

During IPSec VPN connections via SSO authentication, the firewall now retrieves the groups associated with users added from the LDAP, so that these groups can be used in filter rules.

SSL VPN and certificates

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

Certification authorities (CAs) and global certificates

Global certificates and certification authorities are now shown and identified as such when the option **Display global policies (Network objects, Certificates, Filtering, NAT and IPSec VPN)** is enabled in the **Preferences** module.

Certificates and PKI

When a certificate is imported in p12 format, the type of certificate (server or user certificate) is now automatically detected.

Certificate enrollment

Stormshield firewalls now support the EST (Enrollment over Secure Transport) certificate enrollment protocol, which is particular due to its use of HTTPS requests secured by the TLS protocol.

The following operations can be performed when EST is set up on Stormshield firewalls:

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

The existing certificate can directly authenticate renewal requests, which no longer require a password, if the EST server allows it.

These operations can only be performed using *CLI / serverd* commands that begin with:

```
PKI EST
```

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

Certificates generation

Certificates can now be generated with new and more efficient algorithms that use elliptic curve cryptography. The following *CLI / Serverd* commands now offer the options of SECP, Brainpool and RSA:

```
PKI CA CREATE
PKI CERTIFICATE CREATE
PKI REQUEST CREATE
PKI CA CONFIG UPDATE
```

The `size` parameter in these commands also needs to be set. Its value must correspond to the selected algorithm:

Algorithm	Sizes allowed
RSA	768, 1024, 1536, 2048 or 4096
SECP	256, 384, or 521
Brainpool	256, 384, or 512

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

High availability

LACP link aggregation

On firewalls containing LACP aggregates, a weight can now be assigned to each interface in the aggregate to calculate the quality of high availability.
Assign the value *1* to the new *LACPMembersHaveWeight* parameter in the following *CLI / Serverd* commands:

```
CONFIG HA CREATE
CONFIG HA UPDATE
```

This will display the interfaces of the aggregate in the **Impact of the unavailability of an interface on a firewall's quality indicator** table in the **High availability** module of the web administration interface.

Without these commands, the default behavior remains the same: the aggregate will be considered a single interface, and the cluster will switch only when all the interfaces in the aggregate are lost.

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

High availability monitoring via SMC

Monitoring of firewalls configured in high availability is now optimized, and gets the value of the **System node name** field.

Loss of network modules

The health status calculation that determines the switch from one node to another in a cluster has been enhanced so that the system will recognize the loss of network modules more easily, even after the firewall is restarted.

NAT rules with ARP publication

In high availability configurations, firewalls may send a Gratuitous ARP (GARP) for all their interfaces in order to maintain traffic routing, so that the network can be informed whenever the location of a MAC address changes.

This operating mode has been improved so that all virtual IP addresses from an **ARP broadcast** of a NAT rule will send a series of Gratuitous ARPs (GARP) during a switch.

Authentication

New SN SSO Agent pour Linux

A new Linux-based SN SSO Agent supports directories that run on non-Windows systems, such as Samba 4. It can be configured in the **Authentication** module in the web administration

interface, and detected through logs exported via Syslog. Exported logs are filtered by regular expressions configured earlier in the interface.

For more information on the configuration and operation of the SN SSO Agent for Linux, refer to the technical note SSO Agent for Linux.

SSO Agent - Syslog

Backup syslog servers can now be configured for the SSO agent authentication method.

Temporary accounts

The password that the firewall automatically generates when a temporary account is created (**User > Temporary accounts**) now meets the minimum password length required in the firewall's password policy (module **System > Configuration** > **General configuration** tab).

LDAP

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

SN6100 firewall - Performance

The configuration of memory occupation has been optimized on the IPS engine of SN6100 appliances.
Details on the performance of SN6100 firewall models are provided in the SN6100 Network Security datasheet.

SNS - SMC synchronization

The synchronization of SNS with SMC has been enhanced to allow smoother data exchange between both products, especially during direct access to the firewall administration interface from SMC.

NTP client

The interface that NTP requests go through can now be configured. The time synchronization daemon on an SNS firewall previously made such requests go through the default interface.

This new parameter can only be modified through the *CLI / Serverd* command:

```
CONFIG NTP SERVER ADD name=<hostname|groupname> bindaddr=<Firewall_obj>
```

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

Network objects

Address range objects now make it possible to configure MAC address ranges.

SSL proxy

The keys generated by the SSL proxy now use the same encryption algorithms as what the certification authority of the SSL proxy uses instead of the algorithms defined by default.

Configuration backups

The algorithm used to derive the passwords that protect configuration backups has been updated to comply with the highest standards.

System

The random kernel generator has been upgraded so that it is now based on a faster, more robust algorithm.

Initial configuration via USB

Bird dynamic routing

Dynamic routing can now be configured by importing *bird.conf* configuration files for IPv4 and *bird6.conf* configuration files for IPv6. The CSV format of the command file has also been enriched for this purpose.

For further information regarding the preparation of *.bird* and *.bird6* files, refer to the technical note Initial configuration via USB key.

setconf operation

In an initial configuration via USB key, the *setconf* command offers a new feature that allows writing lines in sections in addition to writing values in keys (tokens). The CSV format of the command file has been enriched for this purpose.

For further information regarding the *setconf* command, refer to the technical note Initial configuration via USB key.

New *sethostname* operation

A new *sethostname* operation has been added to the initial configuration via USB key, and makes it possible to set the firewall's host name. The CSV format of the command file has been enriched for this purpose.

For further information regarding the *sethostname* operation, refer to the technical note Initial configuration via USB key.

Dashboard

SSO agents and syslog servers are now monitored, and their statuses shown in the dashboard.

LDAP directories

Secure connections to internal LDAP directories are now based on standard protocol TLS 1.2.

Exclusion of the proxy for automatic backups

Automatic backups can now be configured to avoid going through the proxy set on the firewall.

This new parameter can only be modified through the *CLI / Serverd* command:

```
CONFIG AUTOBACKUP SET
```

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

Web administration interface

System node name

A system node name can now be defined for the firewall (**Configuration** > **General configuration** > **Advanced properties** tab).

This name is particularly useful in high availability configurations, as it easily identifies the member of the cluster on which you are connected when you open a session in console mode, for example.

When this system node name is configured, it appears in parentheses in the upper banner of the web administration interface, after the name of the firewall.

Filter - NAT - HTTP cache feature

The *HTTP cache* function can no longer be used in filter rules.

If a firewall used this function in an earlier firmware version, it will automatically be disabled when it is upgraded to version 4.1.0 or higher.

Regular CRL retrieval

The IP address presented by the firewall can now be specified for **Regular retrieval of certificate revocation lists (CRL)**.

This address can only be configured through the CLI / Serverd command:

```
PKI CONFIG UPDATE CHECKBINDADDR=ip_address
```

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

Resolved vulnerabilities in version 4.1.1

FreeBSD

Vulnerabilities CVE-2019-15879 and CVE-2019-15880 relating to *cryptodev* were fixed after a FreeBSD security patch was applied.

JQuery

Support reference 78384

Vulnerabilities (CVE-2020-11022 and CVE-2020-11023) were fixed after the JQuery library was upgraded.

Intel processors

Several vulnerabilities – CVE-2019-11157, CVE-2019-14607 and CVE-2018-12207 – that could affect Intel processors were fixed after a FreeBSD security patch was applied and Intel microcode was updated.

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

Command line

The SNS command line service (serverd) was vulnerable to brute force attacks only through protected interfaces, and only when access to the administration server over port 1300 was allowed in the configuration of implicit rules. This flaw has been fixed.

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

NetBIOS

A vulnerability made it possible to send specially crafted NetBIOS packets through the firewall during NetBIOS sessions to launch denial of service attacks.

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

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.

Certificates and PKI

Additional controls have been set up for operations such as user identities being downloaded or the publication of a certificate in the LDAP directory. These controls block JavaScript code from being run, as malicious users would have been able to inject it into the certificate.

Web administration interface / Captive portal / Sponsorship

Additional controls have been implemented for connections via the web administration interface, the captive portal or sponsorship, to prevent JavaScript code or additional HTML tags from being executed through the optional disclaimer page.

ClamAV antivirus

Vulnerabilities CVE-2020-3327 and CVE-2020-3341 were fixed after the ClamAV antivirus engine was upgraded to version 0.102.3.

Version 4.1.1 bug fixes

System

SSL VPN

Support reference 76762

The **Available networks or hosts** field was wrongly used to calculate the possible number of SSL VPN clients, and therefore skewed the calculation. This issue has been fixed.

SSL VPN Portal

Support reference 77062

Even though a maximum of servers were accessible via the SSL VPN Portal, additional machines could still be declared. This would cause the firewall's authentication engine to restart repeatedly. Now, servers can no longer be created once the limit is reached, which varies according to the firewall model.

Find out more

Support references 77168 - 77132 - 77388

The SLD would occasionally restart and log off all users whenever two users logged in via the SSL VPN portal and accessed the same resource.

Hardware bypass - SNi40 model firewalls

Support reference 78382

On SNi40 industrial firewalls with the hardware bypass function enabled (**Configuration** > **General configuration** tab), an issue that hardware monitoring processes encounter with competing access to the bypass mechanism would sometimes wrongly enable bypass, and provide the wrong status in the firewall's web administration interface. This issue has been fixed.

Directory configuration

Support reference 76576

The default port used to access the backup LDAP server is now the same as the port that the main LDAP server uses.

Monitoring gateways

Support references 71502 - 74524

During the startup sequence of the gateway monitoring mechanism, if any of the gateways used in filter rules switched from an internal "maybe down" status (pinging failed) to an internal "reachable" status, the filter would still consider such gateways disabled. This anomaly has been fixed.

When the status of a gateway changes, it will now be logged as an event.

Support reference 75745

On firewalls that process many connections, and which use configurations with many gateways, replies to pings may take longer to reach the gateway monitoring mechanism. When this occurs,

the mechanism would continuously re-send pings, and restart without sending notifications such as logs or system events. This issue has been fixed.

Support reference 77579

The gateway monitoring mechanism, which would sometimes restart unexpectedly, has been fixed.

Support reference 76802

In some configurations, the process that relied on the gateway monitoring engine would consume an excessive amount of the firewall's CPU resources. This issue has been fixed.

URL filtering - Extended Web Control

Support reference 78169

When a firewall is upgraded to a 4.1.x firmware version, it no longer prevents the generation of URL category groups used by Extended Web Control.

Proxies

Support references 77514 - 76343 - 78378 - 78438 - 78469 - 77896

Issues regarding proxies, which were blocked when the antispam was used together with the Kaspersky antivirus, have been fixed.

Support references 76535 - 75662

Potential competing access between SSL and HTTP proxy queues would sometimes shut down the proxy manager unexpectedly. This issue has been fixed.

Support reference 71870

The proxy daemon no longer shuts down unexpectedly whenever the maximum number of simultaneous connections through the SSL proxy is reached.

Support references 70598 - 70926

The behavior of the HTTP proxy has been changed so that the SLD daemon on the firewall will no longer be overwhelmed when too many requests are redirected to the authentication portal. This new mechanism implements protection against brute force attacks.

SSL proxy

Support references 76022 - 76017

Changes to some parameters (e.g., memory buffers or TCP window sizes) of the SSL proxy, meant to optimize the amount of data exchanged through this proxy, are now correctly applied.

Support reference 77207

An anomaly in the SSL decision-making cache mechanism (decrypt, do not decrypt, etc) that occurs when there are simultaneous connections with the same destination IP addresses with different ports, would occasionally corrupt this cache and freeze the SSL proxy. This anomaly has been fixed.

Support reference 78044

When attempts to connect to an unreachable SSL server resulted in the SSL proxy immediately returning an error message, the firewall would not properly shut down such connections. An

increasing amount of such connections wrongly considered active would then slow down legitimate SSL traffic. This anomaly has been fixed.

SMTP proxy

Support reference 77207

In configurations that use the SMTP proxy in an SMTP filter rule:

- In "Firewall" security inspection mode

  or

- In "IDS" or "IPS" security inspection mode but without SMTP protocol analysis (**Application protection** > **Protocols** > **SMTP** module > **IPS** tab: **Automatically detect and inspect the protocol** checkbox unselected),

when the SMTP server shut down a connection after sending an SMTP/421 server message, the STMP proxy would occasionally freeze. This issue has been fixed.

Local storage

Support reference 75301

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

IPSec VPN IKEv1

Support reference 77679

In IPSec configurations that use mobile peers with certificate authentication, and for which no peer IDs were specified, the message indicating a switch to experimental mode no longer appears by mistake.

Support reference 77358

When IPSec VPN tunnels were set up with remote users (also known as mobile or nomad users), phase 1 of the IKE negotiation would fail because fragmented packets were not correctly reconstructed after they were received. This anomaly has been fixed.

Support reference 65964

The IPSec management engine (*Racoon*) used for IKEv1 policies no longer interrupts the phase 2 negotiation with a peer when another phase 2 negotiation fails with the same peer.

IPSec VPN IKEv2 or IKEv1 + IKEv2

Support reference 74391

When an extremely large CRL – containing several thousand revoked certificates – is automatically reloaded, the IPSec IKEv2 tunnel manager no longer restarts in loop.

Support reference 75303

When the Bird dynamic routing engine (*bird* for IPv4 or *bird6* for IPv6) was restarted too often, it would cause the IKE daemon to malfunction, preventing IPSec VPN tunnels from being negotiated. This anomaly has been fixed.

Support reference 75137

Creating several mobile peers that use the same certificate no longer causes the certificate to be loaded repeatedly. This behavior consumed much more memory unnecessarily when many peers were involved.

Support reference 77722

The presence of the same trusted certification authority with a CRL in both the local IPSec policy and global IPSec policy no longer causes a failure when the IPSec configuration is enabled on the firewall.

Support reference 77097

The management of the authentication process was enhanced for the setup of IPSec VPN tunnels in configurations where several LDAP directories are declared and one or several of these LDAP directories take longer than usual to respond.

These enhancements now make it possible to stop blocking attempts to set up other tunnels during the waiting phase.

IPSec VPN - Virtual interfaces

Support reference 77032

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

IPSec VPN - Logs

Support reference 77366 - 69858 - 71797

Text strings exceeding the maximum length allowed when they are sent to the firewall's log management service are now correctly truncated and no longer contain non-UTF-8 characters. This anomaly would cause a malfunction when logs were read through the web administration interface.

In addition:

- The maximum supported length of a log line is now 2048 characters,
- The maximum supported length of a text field contained in a log line is now 256 characters.

Initial configuration via USB key

Support reference 77603

An anomaly in how special characters (spaces, ampersands, etc.) are managed when CSV files are imported, could prevent some data from being applied (e.g., certificates with names that contain spaces). This anomaly has been fixed.

Antivirus

Support references 77399 - 77369 - 78378 - 78156 - 78579

The antivirus engine no longer freezes at startup, or when its configuration is reloaded in the absence of a Breach Fighter sandboxing license, or when sandboxing is not properly configured.

Network objects

Support reference 77385

When a global network object linked to a protected interface is created, this object will now be correctly included in the *Networks_internals* group.

Restoration of network objects

Support reference 76167

When local or global network objects are restored using a backup file (file with a ".na" extension), the firewall's network routes are reloaded to apply changes that may affect network objects involved in routing.

TPM

Support reference 76664

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

Support reference 76665

When a PEM certificate is imported on the firewall without its private key, the debug command `tpmctl -a -v` no longer wrongly returns a TPM file reading error message (*tpm file read error*).

SNMP agent

Support references 65418 - 71393

SNMP responses such as SNMP_NOSUCHOBJECT, SNMP_NOSUCHINSTANCE and SNMP_ENDOFMIBVIEW are now correctly interpreted and no longer cause SNMP protocol analyses to stop unexpectedly.

Support reference 71584

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

Support references 74522 - 74521

The anomalies observed in table indexing, which reflected the hardware status of cluster members in the HA MIB, have been fixed.

Connection from Stormshield Management Center (SMC)

During the initial connection from SMC to the web administration interface of a firewall in version 4.0.1 or higher, attempts to retrieve the archive containing all the interface data would fail, thereby preventing connections to the firewall from SMC. This anomaly has been fixed.

Reports

In some cases, running the system command *checkdb -C*, which allows the integrity of the report database to be verified, would actually cause it to be deleted. The system that enabled interaction with this database has therefore been enhanced to introduce more thorough verifications, especially in error management.

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

Behavior when the log management service is saturated

Support references 73078 - 76030

When the log management service on the firewall is saturated, it is now possible to define how the firewall manages packets that generate alarms and those intercepted by filter rules that have been configured to log events:

- Block such packets since the firewall is no longer able to log such events,
- Do not block such packets and apply the configuration of the security policy even though the firewall is unable to log such events.

The behavior of the intrusion prevention system can be configured in the firewall's administration interface via **Configuration** > **Application protection** > **Inspection profiles**.

A percentage threshold, above which the firewall will consider that its log management service is saturated, can also be set. Once this percentage is reached, the firewall will apply the configured action to packets that need to be logged.

The threshold can be changed only with the following *CLI / Serverd* commands:

```
CONFIG SECURITYINSPECTION COMMON LOGALARM BlockOverflow=<0|1> BlockDrop=<0-100>
CONFIG SECURITYINSPECTION COMMON LOGFILTER BlockOverflow=<0|1> BlockDrop=<0-100>
```

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

High availability

Support reference 70003

The validity of the license for the **Vulnerability manager** option is now verified before the configuration is synchronized to avoid unnecessarily generating error messages in logs such as "Target: all From: SNXXXXXXXXXXXX Command: SYNC FILES failed: Command failed : Command has failed : code 1".

Support reference 56682

The test process in which nodes in the same cluster confirm the availability of other nodes has been enhanced so that the passive node will not be wrongly switched to active mode, thereby creating a configuration with two active nodes.

High availability - IPSec VPN (IKEv2 policy or IKEv1 + IKEv2 policy)

In high availability configurations that apply IKEv2 or IKEv1+IKEv2 IPSec policies, an anomaly sometimes wrongly detected the replay of ESP sequence numbers and packet loss after two failovers in the cluster. This anomaly has been fixed.

High availability - link aggregation

Support reference 76748

In a high availability configuration, an active node switching to passive mode would no longer wrongly disable VLAN interfaces that belonged to a link aggregate (LACP).

Maintenance - High availability

Support reference 75986

In a high availability configuration, the option that allowed an active partition to be copied to the backup partition from the other member of the cluster is available again (module

System > **Maintenance** > **Configuration** tab).

Filter - NAT - MAC addresses

Support reference 76399

A rule that has a host object as its destination with a forced MAC address (host in a DHCP reservation, for example) now correctly filters traffic that matches it.

High availability - Filtering and NAT - Time objects

Support reference 76822 - 73023 - 76199

To prevent network instability in high availability clusters, the re-evaluation of filter rules is now optimized when there is a change in the status of time objects used in one or several of these rules.

Support reference 76822

The re-evaluation of filter rules has been optimized when time objects used in several rules in the filter policy change their status.

Routers

Support references 75745 - 74524

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

Certificates and PKI

Attempts to import a certificate already found in the firewall's PKI when the "Overwrite existing content" option is unselected, no longer duplicate this certificate on the firewall.

During a connection to a firewall from an SMC server, the firewall now checks that the certificate of the SMC server contains an *ExtendedKeyUsage* field with the attribute *ServerAuth*.

Monitoring certificates and CRLs

Support reference 76169

In a HA cluster, the mechanism that monitors the validity of certificates and CRLs on the passive firewall no longer wrongly generates system events every 10 seconds. Typical events are Passive certificate validity (event 133) or Passive CRL validity (event 135).

In addition, the mechanism that monitors the validity of CRLs now only generates alerts when a CRL exceeds half of its lifetime and is due to expire in less than 5 days.

Firmware updates

The certificate used to sign firmware updates now contains a specific OID monitored by the mechanism that verifies the firewall's update files.

Radius authentication

Support reference 74824

In a configuration that uses Radius server authentication via pre-shared key, selecting another host object in the Server field, then saving this only change no longer causes the initial pre-shared key to be deleted.

Automatic backups

Support reference 75051

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

Support reference 77432

The absence of the "/log" folder no longer prevents automatic backups from functioning properly.

Network interfaces

Support reference 76645

When a bridge is deleted, all occurrences of this bridge will now be correctly removed from configuration files, and no longer prevents new interfaces from being displayed when new network modules are added.

DHCP relay

Support reference 75491

When GRE interfaces are defined on the firewall, selecting “Relay DHCP queries for all interfaces” no longer causes the DHCP relay service to restart in loop.

Network

Bird dynamic routing

Support reference 77707

The *check link* directive used in the *protocol direct* section in the Bird dynamic routing configuration file is now correctly applied for IXL network interfaces (fiber 4x10Gbps and 2x40Gbps network extension modules for SN2100, SN3100 and SN6100 models; 4x10G BASE-T modules for SN710, SN910, SN2000, SN2100, SN3000, SN3100 and SN6100 models; fiber 10Gbps onboard ports on SN6100 models) and IGB network interfaces (SNi20, SNi40, SN2000, SN3000, SN6000, SN510, SN710, SN910, SN2100, SN3100 and SN6100).

Interfaces

Support references 73236 - 73504

On SN2100, SN3100, SN6100 and SNi40 firewall models, packets would occasionally be lost when a cable was connected to:

- One of the management ports (MGMT) on SN2100, SN3100 or SN6100 models,
  or
- One of the interfaces of an SNi40 firewall.

This issue has been fixed by updating the driver on these interfaces.

Wi-Fi

Support reference 75238

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

Hardware monitoring

System events (ID 88 and 111) are now generated when a defective power supply module reverts to its optimal status (when the module is replaced or plugged back in).

Intrusion prevention

TNS protocol - Oracle

Support references 77721 - 71272

Analyses of TNS - Oracle client-server communications that undergo packet fragmentation and address translation (NAT) would desynchronize traffic due to packets being rewritten. This issue has been fixed.

TCP protocol

Support reference 76621

When a threshold was defined for the **Maximum number of simultaneous connections for a source host** in the TCP configuration, and when a TCP-based filter rule blocked an attempted Syn Flood denial of service attack, the packets that raised the alarm were correctly blocked but no alarm would be raised in the corresponding log file (*l_alarm*). This anomaly has been fixed.

RTSP protocol

Support reference 73084

When an RTSP request that uses an RTP/AVP/UDP transport mode passes through the firewall, the RTSP analysis engine no longer deletes the *Transport* field and broadcast channels are set up correctly.

Policy Based Routing (PBR)

Support reference 77489

When a firewall-initiated connection was created, the system would query the intrusion prevention engine to determine the need for policy-based routing, which would lead to issues with competing access and cause the firewall to freeze. This issue has been fixed.

HTTP

The HTTP protocol analysis no longer raises an alarm or blocks traffic when there is an empty field in the HTTP header, especially when SOAP messages are encapsulated in an HTTP request.

Support references 74300 - 76147

When a value is entered in the **Max. length for a HTML tag (Bytes)** field (**Application protection** > **Protocols** > **HTTP** module > **IPS** tab > **HTML/Javascript analyses**), and a packet presents an attribute that exceeds this value, the firewall no longer wrongly returns the error "Possible attribute on capacity (parser data handler (not chunked))" but the error "Capacity exceeded in an HTML attribute".

NTP

Support reference 74654

To improve compatibility with certain vendors, the maximum size of NTP v3 packets considered valid is now set to 120 bytes by default.

Connection counter

Support reference 74110

The mechanism that counts simultaneous connections has been optimized to no longer raise the alarm “Maximal number of connexions per host reached” (alarm tcpudp:364).

DNS protocol

Support reference 71552

Requests to update DNS records are now better managed in compliance with RFC 2136 and no longer trigger the block alarm "Bad DNS protocol" (alarm dns:88).

Quarantine when alarm raised on number of connections

Support reference 75097

When “Place the host under quarantine” is the action set for the alarm “Maximal number of connexions per host reached” (alarm tcpudp:364), the host that triggered this alarm is now correctly added to the blacklist for the quarantine period configured.

Filtering - SIP protocol

Support reference 76009

An error message now appears when there is an attempt to enable a filter rule such as:

- The option **Redirect incoming SIP calls (UDP)** is enabled (**Action** > **Advanced properties**> **Redirection**),
- Two or more destination ports are defined, one relying on ANY as a protocol, and at least another based on UDP or TCP.

Policy-based routing

Support reference 76999

In PBR, when routers were changed directly in filter rules, IPState connection tables (for GRE, SCTP and other protocols) now apply the new router IDs.

Hardware

SN6000 model firewalls

Support references 75577 - 75579

In a few rare cases, a message warning of missing power supply modules would be wrongly sent on SN6000 firewalls equipped with an IPMI module in version 3.54. A mechanism that restarts the IPMI module has been set up to deal with this issue.

This mechanism is disabled by default and does not affect traffic going through the firewall, but temporarily prevents the refreshment of component data. The mechanism needs about five minutes to run its course, the time it takes to restart the IPMI module and to refresh data on components.

This new parameter can only be modified through the *CLI / SSH* command:

```
setconf /usr/Firewall/ConfigFiles/system Monitord EnableRestartIPMI <0|1>
```

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

Virtual machines

EVA on Microsoft Azure

Support reference 76339

The Microsoft Azure Linux Guest Agent log file (file waagent.log) was moved to the "/log" folder on the firewall to avoid saturating the "/var" file system on the firewall.

Web administration interface

Users and groups

Support reference 78413

In directories that have several thousand entries (especially in nested groups), requests to display users and groups for a selection (e.g., the **Filter - NAT** module) could take an unusually long time and cause the display of the module to freeze. This issue has been fixed.

Reports

Support reference 73376

The “Top sessions of Administrators” report now shows all the sessions of the firewall's administrators, i.e., sessions of the *admin* (super administrator) account and of all users and user groups added as administrators. The report previously contained only sessions of the *admin* (super administrator) account

40 Gb/s network modules

The maximum throughput indicated in each interface’s configuration panel is now 40 Gb/s for the network modules concerned.

Protocols

Support reference 75435

The search filter applied to the protocol tree (Application protection > Protocols) now stops being applied after a module is reloaded.

Interface monitoring

Support reference 76162

The theoretical throughput of Wi-Fi interfaces now factors in the standard used (A/B/G/N) and no longer indicates 10 Mb/s systematically.

Hardware monitoring / High availability

The serial number of both members of the cluster now appears in the list of indicators.

LDAP directories

Support reference 69589

Users can now correctly access an external LDAP directory hosted on another Stormshield firewall via a secure connection (SSL) when the option "Check the certificate against a Certification authority" is selected.

Filter - NAT

Support reference 76698

Network objects defined with only a MAC address are now correctly listed as available network objects when a filter rule is being created.

Static routing - Return routes

Support references 77012 - 77013

USB/Ethernet (4G modem) interfaces can now be selected as the routing interface when a static route or return route is added.

Filtering - Implicit rules

Support reference 77095

When the administrator requests to disable all implicit rules, the system command to disable them is now correctly applied.

SSL VPN

Support reference 76588

When the SSL VPN configuration module is opened, the window indicating that the captive portal is not enabled on external interfaces no longer appears by mistake when it is enabled.

Global router objects

Support reference 76552

Double-clicking on a router object now correctly opens the window to edit routers instead of the window for hosts.

Protocols - DNS

Support reference 72583

After the action applied to a DNS registration type is changed, displaying other DNS profiles successively no longer causes an error when the table of DNS registration types and applied actions is refreshed.

User names

Support reference 74102

User names are no longer case-sensitive when they are saved in the tables of the intrusion prevention engine. This guarantees that names are mapped to filter rules based on the names of authenticated users.

Authentication methods

Support reference 76608

During a user's initial access to the Users > Authentication module, the message asking the user to save changes before quitting, even though none were made, will no longer appear.

Version 4.1.0 not published

Version 4.1.0 is not available to the public.

New features in version 4.0.3

IMPORTANT

Firewalls must not be upgraded from SNS in version 3.10.x or higher to a 4.0.x version. This operation is not supported.

For further information, refer to Recommendations.

System

WebGUI file signature

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

Obsolete features and algorithms

Filter - NAT - HTTP cache feature

As the use of the *HTTP cache* function in filter rules will be phased out in a future version of SNS, a warning message now appears to encourage administrators to modify their configurations.

This message appears under the filter grid in the **Checking the policy** field.

IPSec VPN - Obsolete authentication and encryption algorithms

As some algorithms are obsolete and will be phased out in a future version of SNS, a warning message now appears to encourage administrators to modify their configurations. The algorithms in question are:

- Authentication algorithms: *md5*, *hmac_md5* and *non_auth*,
- Encryption algorithms: *blowfish*, *des*, *cast128* and *null_enc*.

This message appears when these algorithms are used in the profiles of IPSec peers.

IPSec VPN - Backup peers

As the use of backup peers (designated as the "Backup configuration") is obsolete and will be phased out in a future version of SNS, a warning message now appears to warn administrators and encourage them to modify their configurations. This message appears under the IPSec policy grid in the **Checking the policy** field.

For this configuration, use virtual IPSec interfaces instead, with router objects or dynamic routing.

Resolved vulnerabilities in version 4.0.3

S7 protocol

The firewall would restart unexpectedly whenever:

- S7 traffic included an exchange containing an invalid request packet followed by an invalid response packet,
  and
- The alarm "S7: invalid protocol" (alarm s7:380) was set to "Pass",
  and
- The option “Log each S7 request” was enabled in the S7 protocol parameters.

This flaw has been fixed.

SIP over TCP protocol

An anomaly, which could result in a SIP session double lock and the sudden shutdown of the SIP over TCP protocol analysis, has been fixed.

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

SNMP

Support reference 76629

Running an SNMP operation when a wrong OID (that does not begin with ".") is added to the blacklist in the SNMP protocol parameters, no longer causes the firewall to reboot in loop.

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

FreeBSD

If a field in the IPv6 header was not properly initialized, it would cause a memory leak that cannot be exploited.

This vulnerability (CVE-2020-7451) was fixed after a security patch was applied to the FreeBSD TCP network stack.

NetBIOS

A vulnerability made it possible to send specially crafted NetBIOS packets through the firewall during NetBIOS sessions to launch denial of service attacks.

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

Version 4.0.3 bug fixes

System

IPSec VPN (IKEv1)

Support reference 75824

Whenever a remote peer switched to its backup peer (designated as the "Backup configuration"), the IKE daemon would sometimes restart unexpectedly and shut down open IPSec tunnels. This anomaly has been fixed.

GRETAP and IPSec

Support reference 76066

The system command *ennetwork -f* no longer makes the firewall reboot in loop in configurations containing GRETAP interfaces that communicate through IPSec tunnels.

SSL VPN

A new certificate, with which Java JAR compiled files can be signed, has been installed and replaces the former certificate due to expire soon (05/24/2020).

SN910 model firewalls

Support reference 76528

After a upgrade of the firewall from an SNS 3.9.x version to an SNS 4.0.x version, the ports of IX interfaces were no longer in the right order on SN910 firewalls equipped with an IX card.

An automatic mechanism has been set up to restore the order of ports.

Daemon shutdown time

Support reference 74990

In some rare cases, a daemon would shut down after a certain duration and prevent the firewall from completing its update. This duration has been shortened to allow the firewall update to run properly.

Network

Wi-Fi network

Support references 73816 - 75634 - 75958

Devices that use *Intel Wireless-N 7260* or *Qualcomm Atheros AR6004 802.11a/b/g/n* Wi-Fi cards would occasionally encounter connectivity issues on the firewall's Wi-Fi. This anomaly has been fixed.

Intrusion prevention

TDS protocol

The analysis of the *Status* field in TDS (Tabular Data Stream) packets no longer wrongly raises the alarm "TDS: invalid protocol" (alarm tds:423).

NB-CIFS protocol

The analysis of NB-CIFS traffic from Microsoft Windows hosts no longer wrongly raises the alarm "Invalid NBSS/SMB2 protocol" (alarm nb-cifs:157).

LDAP protocol

Authentication via SASL (Simple Authentication and Security Layer) now supports the NTLMSSP protocol, and therefore no longer generates errors when analyzing LDAP traffic that uses this protocol.

NTP

NTP packets that present a zero *origin timestamp* no longer wrongly raise the alarm "NTP: invalid value" (alarm ntp:451).

DNS protocol

Support references 72754 - 74272

The DNS protocol analysis has been modified to reduce the number of false positives from the "DNS id spoofing" alarm (alarm dns:38).

Web administration interface

Access to private data (logs)

To get back full access to logs (private data), click directly on the message “Logs: Restricted access” in the upper banner.

Directory configuration

Support reference 76069

When an external LDAP directory is set as the default directory, the name of this directory is no longer wrongly replaced with *NaN* when its parameters are modified.

Interfaces

Support reference 76497

The IP addresses of interfaces 11 and up were replicated on the second interface of the firewall, displaying wrong information as a result. This anomaly has been fixed.

Authentication

During the configuration of the RADIUS authentication method, the “Pre-shared key” fields were not applied. This anomaly has been fixed.

New features in version 4.0.2

IMPORTANT

The update of a firewall from an SNS version 3.10.x and upwards to an SNS version 4.0.x must not be performed and is not supported.

Details are available in Recommendations section.

Stability and performance

The synchronization of SNS with SMC has been enhanced to allow smoother data exchange between both products, especially during direct access to the firewall administration interface from SMC.

Increased security during firmware updates

Security is now tighter during firmware updates. In addition to update packages being protected by signatures to ensure their integrity, Stormshield now also secures communications with the update servers used. These communications now take place in HTTPS and over port 443.

Hardware

SSH commands

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

```
tpmctl
```

It includes a command that allows new *PCRs* (*Platform Configuration Registers*) to be approved after the BIOS or hardware modules are updated.

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

Resolved vulnerabilities in version 4.0.2

Authentication portal (captive portal)

New checks are now conducted during the verification of parameters used in the URL of the firewall's captive portal.

Details on this vulnerability (**CVE-2020-8430**) can be found on our website https://advisories.stormshield.eu.

CLI / Serverd commands

The CLI Serverd command `CONFIG AUTOUPDATE SERVER` has been enhanced so that the use of the "url" parameter is now better monitored.

Libfetch library

The vulnerability **CVE-2020-7450** was fixed after a security patch was applied to the FreeBSD *libfetch* library.

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

Web administration interface

Additional checks are now implemented during the verification of parameters used in the URL of the firewall's web administration interface.

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

Version 4.0.2 bug fixes

System

SSL proxy

Support reference 74927

To prevent compatibility issues with embedded programs or certain browsers, especially in iOS 13 and MacOS 10.15, the size of certificate keys that the SSL proxy generates for SSL connections has been raised to 2048 bits.

Support reference 74427

When the certification authority of the SSL proxy expired, the firewall would sometimes stop attempting to generate new keys unnecessarily for some events, e.g., when reloading the filter policy or network configuration, or when changing the date on the firewall. This would cause excessive CPU usage.

Proxies

Support references 66508 - 71870

In heavy traffic, the proxy would sometimes shut down during a failed HTTP header analysis. This issue has been fixed.

Support reference 71870

The proxy no longer shuts down unexpectedly whenever the SSL proxy is used and the maximum number of simultaneous connections is reached.

Support references 70721 - 74552 - 75874

Memory consumption is now optimized when the proxy is used.

Proxy - URL filtering

Support reference 73516

The connection between the HTTP/HTTPS proxy and the URL filtering engine of the Extended Web Control solution would occasionally be lost; this would display the *URL filtering is pending* page to clients whose connections used the proxy. This issue has been fixed.

Filter - NAT

Support references 76343 - 76231

If several consecutive rules use the same object, they will no longer prevent the filter policy from reloading.

IPSec VPN

Support references 74551 - 74456

An anomaly in the IPSec function **key_dup_keymsg()**, which would generate the error*Cannot access memory at address* and cause the firewall to shut down suddenly, has been fixed.

Support reference 74425

A parameter would occasionally prevent *ResponderOnly* mode from running properly whenever *Dead Peer Detection* (DPD) was enabled. This anomaly has been fixed.

IPSec VPN (IKEv2 / IKEv1 + IKEv2)

Support reference 68796

In configurations that use IKEv2 IPSec policies or which combine IKEv1 and IKEv2, the firewall would sometimes fail to send a network mask to the Stormshield IPSec VPN client when it set up the mobile tunnel in config mode. The network mask that the IPSec client arbitrarily chose would then occasionally conflict with the local network configuration on the client workstation.

The firewall now always sends the network mask /32 (255.255.255.255) to the IPSec VPN client for mobile tunnels in config mode.

Global host objects included in router objects

Support reference 71974

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

Certificates and PKI

Support reference 76048

When certification authorities are imported, spaces in the import path are now correctly interpreted and no longer cause the import to fail.

ANSSI "Diffusion Restreinte" mode

When the ANSSI "Diffusion Restreinte" mode is enabled (**System** > **Configuration** > **General configuration** tab), a mechanism now checks the compatibility of Diffie-Hellmann (DH) groups used in the configuration of IPSec peers with this mode. The list of allowed DH groups has been updated; now only DH 19 and 28 groups must be used.

Excessive memory consumption of the serverd daemon

Support references 76158 - 75155

The memory consumption of the serverd daemon would increase to an excessive extent with the number of remote connections set up via SMC. This issue, which could prevent connections from being set up with the firewall's web administration interface, has been fixed.

Sandboxing

Support reference 76121

When no Sandboxing license has been installed (Stormshield Breach Fighter option) or when the license has expired, the AVD daemon would no longer shut down unexpectedly when users attempt to reload their configuration.

Network

Static routing

Support reference 72938

On the incoming interface of a bridge, policy-based (PBR) routing instructions now take priority over the option to keep initial routing. This new order of priority does not apply to DHCP responses when the IPS automatically adds the option to keep initial routing.

Support reference 72508

Router objects with load balancing that have been configured as the default gateway on the firewall would sometimes override static routes. As a result of this, connections would be initiated from the firewall with the wrong source IP address. This anomaly has been fixed.

Trusted Platform Module (TPM)

Support reference 76181

When the IKE2 / IKEv1+IKEv2 IPSec tunnel manager retrieves the encryption key stored on the TPM, it no longer causes memory leaks.

Intrusion prevention

SIP

Support reference 75997

When a sent SIP packet and its reply contained a field with an anonymous IP address, and the 465 alarm "SIP: anonymous address in the SDP connection" was configured to **Pass**, the firewall would restart unexpectedly. This anomaly has been fixed.

SNMPv3 protocol

Support reference 72984

The SNMP protocol analysis no longer wrongly raises the **Prohibited SNMP user name** alarm (snmp:393) for IDs specified in the whitelist of the SNMPv3 protocol.

Trusted Platform Module (TPM)

Support reference 76181

An anomaly in a function would sometimes cause a shortage of handles, or object identifiers, used for authentication on the TPM, making communication with the TPM impossible. This anomaly has been fixed.

Elastic Virtual Appliances (EVA)

CLIB /B serverd commands

The CLIB / Serverd MONITORB HEALTH command run on an EVA now returns the value *N/A* for absent physical modules (e.g., fan, disk, etc.) instead of *Unknown*, which caused an anomaly on SMC administration consoles.

Web administration interface

Authentication portal (captive portal)

Support reference 76398

The focus of the connection window in the captive portal is no longer set by default on the *Cancel* value. Pressing [Enter] on the keyboard after typing the login and password no longer logs off the user by mistake.

New features in version 4.0.1

Filtering

MAC address filtering

SNS now makes it possible to define and use network objects that are based on MAC addresses only. Such objects can be used in filter policies for level 2 filtering similar to stateful mode.

Industrial protocols

PROFINET support

PROFINET is a set of protocols used in the production, agriculture and transport sectors. PROFINET consists of four main protocols (among others): PROFINET-IO, PROFINET-RT, PROFINET-DCP and PROFINET-PTCP.

You can now filter by these protocols in SNS in order to secure such environments.

Industrial licenses

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

User comfort

New graphical user interface

The SNS version 4.0.1 graphical interface has been fully reworked to improve user comfort. It is now easier to switch between configuration and monitoring modules.

New simplified dashboard

The dashboard has been simplified to provide a clearer view of the status of the firewall. A drill down mechanism enables access to detailed information if it is needed for analyses.

New network configuration panel

The network configuration panel has been simplified to streamline the configuration of interfaces.

New certificate management panel

The certificate management panel has been simplified to facilitate PKI configuration.

New log display panel

The log display panel has been simplified and offers logs in the form of views by specific themes.

New responsive captive portal

The captive portal now has a new responsive design. Its display can be adapted to the size of the screen, so that the captive portal can be used on smartphones or tablets.

Initial installation wizard removed

The initial installation wizard has been removed.

Management

New health indicators
Two new health indicators are available: the first relating to CPU temperature, and the second relating to the administration password if it is too old or is still the default password.

Wi-Fi interface monitoring
Monitoring on Wi-Fi interfaces can now be viewed.

ARPING support
The ARPING command is now available to assist in analyses.

Exporting an identity (containing the private key) or a certificate
You can now export identities (user, server or smart card certificates and the associated private key) or certificates only (user, server or smart card).

Update procedure in cluster mode optimized
The update procedure for clusters has been optimized to prevent update files from being downloaded twice.

Refreshing SSHD configuration
The configuration of the SSHD service has been reworked to ensure compliance with the latest security standards.

Telemetry
A telemetry service is now available on SNS to maintain anonymous statistics regarding the life cycle of SNS firewalls. These statistics serve to improve the quality and performance of future products. The indicators reported in this version are:

- Percentage of CPU use,
- Percentage of memory use,
- Volume of logs generated.

Disabled by default, this service can be enabled/disabled in the module **Configuration** > **General configuration** > **Advanced properties** tab.

Stability and performance

HA mechanisms reworked
High availability synchronization has been simplified to ensure higher stability and better performance.

Proxy mechanisms reworked
The sandboxing features in Breach Fighter have been extracted from the proxy service and now run in a separate service for higher stability.

Improved IPS performance
The IPS connection manager has been enhanced to improve performance.

Simplified DCERPC plugin

The DCERPC plugin has been modified to enable easier configuration.

Overall improved performance

The operating system on SNS firewalls has been upgraded to provide better performance.

ClamAV antivirus

A new parameter in ClamAV makes it possible to restrict the duration of the antivirus analysis. This acts as a new layer of protection against zip bombs. As such, if the length of the analysis implies that the analyzed file contains an overwhelming amount of data, the analysis will be stopped.

Set by default to 120 seconds, this parameter can only be modified through the command:

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

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

Hardware

Hardware-based security for VPN secrets on compatible SN3100 models

Ever since revision A2 of SN3100 model firewalls, they now implement a trusted platform module (TPM) dedicated to securing VPN secrets. With the TPM, an extra level of security can be added to SN3100 appliances that act as VPN concentrators, which may not necessarily be physically secure. This module is supported from version 4.0.1 onwards and can be configured in the interface and in command line.

SN6100 - Seventh and eighth 8x1G modules supported

From SNS version 4.0.1 onwards, eight 8x1G modules can be supported on SN6100 appliances.

Resolved vulnerabilities in version 4.0.1

Certificates and PKI

Additional checks have been implemented when certificates are processed, in order to prevent the execution of JavaScript that can be embedded in specially crafted certificates for malicious purposes. Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

ClamAV

The vulnerability **CVE-2019-15961**, which would enable denial of service attacks through specially crafted e-mails, was fixed with the upgrade of the ClamAV antivirus engine.

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

OpenSSL

Vulnerabilities (CVE-2019-1563, CVE-2019-1547 and CVE-2019-1552) were fixed with the upgrade of the OpenSSL cryptographic library.

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

RTSP protocol

Support reference 70716

A flaw in the IPS analysis of the RTSP protocol with the interleaving function, mainly used by IP cameras, would occasionally cause the appliance to restart. This flaw has been fixed.

Do note that interleaving support is not enabled in factory configuration.

Version 4.0.1 bug fixes

System

IPSec VPN (IKEV1 + IKEv2)

Support reference 73584

In configurations that use both IKEv1 and IKEv2 peers, as UID (LDAP) and CertNID fields used for authentication are applied, user privilege verifications for IPSec tunnel setup are no longer ignored.

Support reference 72290

On firewalls that host IKEv1 and IKEv2 peers, groups belonging to users who set up mobile IKEv1 tunnels with certificate authentication and XAUTH are now taken into account.

Automatic backups - Cloud Backup

Support reference 73218

Configurations backed up in Cloud Backup can now be restored again.

System - Time zone

Support reference 69833

The Europe/Moscow time zone on the system has been updated to fix a time difference of one hour.

Firewalls with IXL cards

For firewalls equipped with IXL cards:

- Fiber 4x10Gbps and 2x40Gbps network extension modules for SN2100, SN3100 and SN6100 models,
- 4x10G BASE-T modules for SN710, SN910, SN2000, SN2100, SN3000, SN3100 and SN6100 models.
- Fiber 10Gbps onboard ports on SN6100 models.

Support reference 73005

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

Support reference 72957

To prevent some negotiation issues relating to the automatic detection of media speed, the available values for IXL network cards can now be selected in the **Network** > **Interfaces** module.

Filter - NAT

The fields **Force source packets in IPSec**, **Force return packets in IPSec** and **Synchronize this connection between firewalls (HA)** were added to the CSV export file in filter and NAT rules.

High availability

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

High availability - IPSec VPN

Support reference 74860

As the SAD's (Security Association Database) anti-replay counters are sent to the passive firewall, sequence numbers are incremented in line with the high availability (HA) mechanism's operating mode.

Whenever the passive firewall detected IPSec traffic in HA configurations (e.g. monitoring frames from virtual IPSec interfaces), it would also send incremented sequence numbers to the active firewall.

As a result of these successive increments, sequence numbers would quickly reach the maximum values allowed. This would then wrongly activate IPSec anti-replay protection and block traffic going through tunnels. This issue has been fixed.

High availability and monitoring

Support reference 73615

A vulnerability to memory leaks has been fixed in high availability configurations with monitoring enabled.

Initial configuration via USB key

Support reference 73923

Firmware can now be updated again via USB key.

Authentication by certificate

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

Reports

Support reference 74730

When the firewall is restarted, an anomaly occurs when the report database is enabled, causing several error messages to appear in the console:

```
checkdb[181]: Missing database file: /var/db/reports/reports.db
enreport: checkdb: Unable to restore the reports database
enreport: Unable to mount the reports database.
```

This anomaly has been fixed.

Serial port - File editors

Support reference 72653

A display bug that occurred during the use of Joe / Jmacs editors via serial link has been fixed.

Intrusion prevention

Support reference 73591

Enabling verbose mode on the intrusion prevention engine that analyzes some protocols (DCE RPC, Oracle, etc.) no longer causes the firewall to suddenly reboot.

Web administration interface

Static routing

Support references 73316 - 73201

In the **Network** > **Routing** module, the IPSec interface can now be selected again during the definition of a static route.

Network objects

Support reference 73404

Accented characters in the comments of network objects no longer prevent the pages of the web administration interface from loading correctly.

DHCP - Server

Support reference 73071

A warning message now appears to indicate that IP address reservations can no longer be added while a display filter is enabled.

DHCP - Relay

Support reference 72951

If network interfaces were specified to relay DHCP requests, they were replaced with the default value (*automatic*) after quitting and displaying the DHCP module again. This anomaly has been fixed.

Special characters

Support references 68883 - 72034 - 72125 - 73404

A bug during the conversion of special characters to UTF-8 (e.g. Asian or accented characters) generated XML errors and prevented affected modules, such as filtering and NAT, from being displayed. This anomaly has been fixed.

Certificates and PKI

Support reference 74111

CRLs containing several thousand revoked certificates would fail to display correctly on some firewall models. This issue has been fixed; now only the first 1000 items are displayed.

SNMP agent

Support reference 74337

During the configuration of the SNMPv3 server, both encryption algorithm buttons would always stay active even after they have been selected. This anomaly has been fixed.

Modbus protocol

Support reference 71166

The firewall would not take into account the information entered in the Allowed UNIT IDs table (**Application protection** > **Protocols** > **Industrial protocols** > **Modbus** > **General settings**). The same information would also not appear in the table after quitting the module.

Contact

To contact our Technical Assistance Center (TAC) Stormshield:

- https://mystormshield.eu/

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

- +33 (0) 9 69 329 129

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

STORMSHIELD

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