STORMSHIELD NETWORK SECURITY

RELEASE NOTES VERSION 3

English version

March 21, 2017

Table of contents

New features in version 3.1.0

System

Network objects

New objects corresponding to services and service groups used by the Stormshield Endpoint Security solution have been included in the SNS firewall objects database.

IPSec VPN (IKEv2)

Diffie-Hellman DH19 NIST Elliptic Curve Group (256-bits) and DH20 NIST Elliptic Curve Group (384-bits) have been added to the encryption profiles available for IPSec IKEv2 tunnels.

IPSec VPN

A button that allow renaming IPSec peers has been added to the **Peers** tab in the **IPSec VPN** module.

Support reference 56589

Notifications

Object names associated with source and destination IP address have been added to notification reports sent by email.

Certificates and PKI

The period for verifying CRLs (Certificate Revocation Lists) used to be set at 24 hours. It can now be configured for a period ranging from 3600 seconds (1 hour) to 604800 seconds (1 week). The default value is 21600 seconds (6 hours).

These settings can only be modified via the CLI command : `PKI CONFIG UPDATE checkcrlperiod= xxxxx`.

HTTP block page

The return code associated with the HTTP block page (default value: *202 - Accepted*) can be modified using the command: `config protocol http profile proxy urlfilteringindex=X HTTPCodeOnFail=Y`.

High availability

When the quality of the passive firewall changes (e.g., when a link is lost, or when disconnecting from a power supply module), the cluster will send out an SNMP alert (TRAP) in order to warn the administrator. The firewall will also add a message resembling "The quality of a node in the cluster has been modified: SN910XXXXXXXXX 12 -> 11" in the system event log (*l_system* log).

In a high availability configuration with a quality factor below 100%, a warning message appears in several cases indicating that the role of a cluster member might change, in particular:

- when an interface in an aggregate is created, added or deleted,
- when a connected interface is disabled,
- when a disconnected interface is enabled,

SSL VPN

The options **Use DNS servers provided by the firewall** (*register-dns*) and **Prohibit use of third-party DNS servers** (*block-outside-dns*), respectively instructing the SSL VPN client to either write the DNS server(s) specified by the Stormshield Network firewall in its configuration or to avoid using third-party DNS servers, can be configured in the **Configuration** > **SSL VPN** module. This feature shortens the time needed for receiving responses to the client's DNS requests, especially for machines running in Microsoft Windows 10.

SSL VPN Portal

The Java Web Start application is now used instead of the standard Java application during connections to the SSL VPN portal.

Global objects

SNS firewalls now support global time objects and router objects, which can therefore be managed and deployed using the Stormshield Management Center solution.

CRL verification and support for BindAddr in the firewall's LDAP requests

In the firewall's LDAP configuration, the BindAddr parameter followed by the firewall's private IP address forces the firewall to present this IP address during LDAP requests to an external directory: LDAP traffic can therefore be encapsulated in an IPSec tunnel in order to encrypt requests to the directory.

This parameter can only be modified in command line: `setconf ConfigFiles/ldap LDAP_Name BindAddr FW_Private_IP`.

Monitoring - Reports - Audit logs

Monitoring

Each line showing a vulnerability detected on a host will now include a link to the page providing details on the vulnerability in question.

New pop-up menus can be opened by right-clicking on a line of data:

- **Hosts monitoring**: you can look for the host in logs, show details about the host, reset its reputation score, add the host to the objects database and/or add it to a group, etc.
- **User monitoring**: you can look for the value in logs, show details about the host on which a user is connected, disconnect the user, etc.
- **Connections monitoring**: you can display a full line, add the source or destination object to the objects database, show details about the host, ping the source or destination, etc.

Intrusion prevention

IEC 60870-5-104 protocol

The intrusion prevention system now scans the industrial protocol IEC 60870-5-104 (IEC 104).

HTTP

A signature context, *vbscript,* has been added to the security inspection for HTTP.

Support reference 54140
The intrusion prevention system now detects cache poisoning attempts on *Squid* web proxies and raises the block alarm *Possible HTTP proxy poisoning*.

SSL Proxy
RC4 and MD5 encryption algorithms, which are considered weak, have been removed from the list of available algorithms for the SSL proxy.

Modbus protocol
An alarm is now generated when the maximum number of Modbus servers with a UMAS reservation has been reached.

Connections in firewall mode
Connections that match a rule in firewall mode are referenced in connection statistics logs (IPStateMem , -IPStateConn, -IPStatePacket and -IPStateByte fields in the */filterstat* file).

SNi40 industrial firewalls

Hardware bypass
When hardware bypass was enabled, ongoing connections on interfaces included in the bypass were not modified and therefore ended up being shut down since the corresponding network traffic was not received. This reaction has been modified, and such connections will now be kept active until a standard network configuration is adopted again (bypass reset).

Hardware

High availability
As part of the process of resetting the firewall to its factory configuration (*defaultconfig*), the period before the hardware watchdog function is activated will now be 120 seconds compared to the previous 300.

Version 3.1.0 bug fixes

This list is not exhaustive and other fixes may have been included in this version.

System

Authentication

Support reference 52192
Attempts to log on to the web administration interface via Google Chrome and SSL (certificate) or SPNEGO would not only fail but raise a brute force attack alarm as well. This issue has been fixed.

Support reference 56711
During the configuration of the Sponsorship method, the "Expiry of the HTTP cookie" field would not be automatically set to *Do not use*, thereby causing this authentication method to

malfunction. This anomaly has been fixed.

Support reference 56595

Attempts to create new objects through the authentication policy wizard would fail and display a "?" instead of the object name. This issue has been fixed.

Support reference 59731

An encoding anomaly in sponsorship e-mails invalidated the validation link included in such e-mails. This anomaly has been fixed.

Objects

Support reference 58476 - 58944

Router objects and time objects were not retained during partial restorations of a configuration. This anomaly has been fixed.

Support reference 56113

Global objects embedded in a router object were not taken into account. This anomaly has been fixed.

Support reference 53218

Whenever an active and operational dialup (PPoE, PPTP, PPP or L2TP modem) was embedded in a router object, the router object would not retrieve its state and would therefore consider it unreachable. This issue has been fixed.

Support reference 59083

Certificates and PKI

During the renewal of certificates via SCEP (Simple Certificate Enrollment Protocol) using the `SCEP RENEW` command, whenever the Distinguished Names (DN) of such certificates contained more than one attribute of the same type (e.g. OU, CN, O, etc.), only the first occurrence of the attribute would be kept after the operation. This anomaly has been fixed.

Support reference 51618

SSL VPN Portal

Connections to application servers through the SSL VPN portal application no longer functioned in version 3. This issue has been fixed.

SSL VPN

Support reference 58856

The maximum number of SSL VPN tunnels physically allowed on Netasq U model S series firewalls was lower than the expected number of tunnels. This anomaly has been fixed.

Support reference 52972 - 53289

An issue that could prevent new SSL VPN tunnels from being set up (connection blocked at the "GET CONF" stage) has been fixed.

Proxies

Support reference 52034

Whenever a filter rule used the explicit proxy, the authentication rules contained in the filter policy would not take into account this proxy's different listening port (TCP/8080 by default). This anomaly has been fixed.

Support reference 55700

An anomaly regarding the maximum length of a user name and domain that make up an email address has been fixed.

Support reference 54003

The HTTP proxy would mistakenly consider some downloads as partial downloads. This anomaly has been fixed.

Support reference 56464

An anomaly while reading information located behind the domain name specified in the *EHLO* command would wrongly cause the corresponding SMTP traffic to be blocked.

Support reference 52848

After sandboxing an email, the name of the attachment referenced in the logs would be wrong. This issue has been fixed.

Support reference 49996

An anomaly in the management of the Internet Content Adaptation Protocol's (*ICAP*) responses in *Request Modification* (*reqmod*) mode would either cause the overconsumption of memory resources or the HTTP proxy to be blocked.

Support reference 57326

Whenever an e-mail contained a wrong end-of-line command in its data, the connection would be reset only between the client and the firewall while the server would have to wait until the connection timed out. This anomaly has been fixed.

Support reference 58824

Whenever a client sent a RESET command to the mail server, the connection would be reset only between the client and the firewall while the server would have to wait until the connection timed out. This anomaly has been fixed.

Support reference 56475

Whenever an e-mail contained a sender or recipient address exceeding the size defined by the RFCs (local part or domain name), the proxy would fail to shut down the connection after sending the error message ("553 Localpart too long" or "553 Domain name too long"). This issue has been fixed.

Support reference 59420

The proxy would occasionally refuse to run on a firewall using a filter rule with at least one of its log destination checkboxes unselected (**Advanced properties** tab in the **Action** module in the filter rule editing window). This issue has been fixed.

Support reference 58567

Resetting to factory configuration

The help provided with the reset script (*defaultconfig*) would offer the wrong explanation for the option "–D" (*Only Restore the data partition on G2 hardware*). This anomaly has been fixed (*Only Restore the data partition*).

Support reference 56394

Proxies – SN 910 model firewalls

Limits on the number of connections allowed for proxies (HTTP, SSL, SMTP, POP3 and FTP) on SN910 model firewalls were incorrect. They have been increased in order to match this model's actual performance.

Support reference 57286

IPSec

In configurations that contain a site-to-site IPSec tunnel and an anonymous IPSec policy (nomad users), disabling the site-to-site tunnel (tunnel status *off*) would not delete the peer of the IPSec configuration file. This anomaly, which would cause nomad connections to malfunction, has been fixed.

IPSec (IKEv2)

Support reference 54831

During Phase 1 renegotiations of IPSec tunnels in IKEv2, the IPSec engine would destroy the existing SA (Security Association) as well as child SAs before negotiating the new SA.

Since this could cause significant packet loss, the behavior of the engine has been modified so that it negotiates the new SA first before destroying older ones.

Support reference 59152

An issue that could prevent the setup of IPSec IKEv2 tunnels to SN150 model firewalls has been fixed.

Support reference 59280

The number of IKE SAs for the same IPSec IKEv2 tunnel would increase over time without diminishing the number of unused SAs. This anomaly has been fixed.

High availability

Support reference 56268

Whenever an interface was added to or deleted from an aggregate (LACP), the change was not applied in the quality indicator in the high availability mechanism. This anomaly has been fixed.

Support reference 57056

An optimization in the parameters that detect the loss of an active firewall due to electrical issues (*ConsensusTimeout* parameter) has considerably shortened the time taken for a cluster to switch.

Support reference 56613

After the high availability management engine has been restarted several times by accident, the associated tokens would not be deleted. The token table could then become saturated, therefore preventing other services on the firewall from starting. This issue has been fixed.

Support reference 56478

Instability on the data synchronizer would cause the high availability management service to restart in loop. As a result of this malfunction, the passive firewall could potentially switch to active mode, making both firewalls in the cluster active. This issue has been fixed.

Support reference 50048

Changing roles after the active member of the cluster has been restarted could cause the IPSec tunnels negotiated by both members of the cluster to be desynchronized.

Support reference 57317

Whenever the table of events to be synchronized filled up, the high availability manager would attempt a new full synchronization at the expense of the firewall's performance. This reaction has been modified, so that the mechanism now deletes the oldest events first in order to add the most recent to the queue.

Support reference 54289 - 58842

After the roles of firewalls have been switched in a cluster, whenever active connections were restored, the parent-child relationship of these connections (connection traffic / data traffic) would not be kept. Data traffic for protocols such as FTP would therefore not be transferred. This issue has been fixed.

Support reference 55076

Application protection

In configurations that use the Karspersky antivirus engine, scanning zip bomb files could cause the temporary partition to saturate, leading in turn to a significant CPU load and resulting in an analytical error. This issue has been fixed.

Filter - NAT

Support reference 56570

Whenever the name entered for a filter rule exceeded the maximum length allowed, the length allowed would not be specified in the error message. This anomaly has been fixed and it now indicates that names must not exceed 255 characters.

Support reference 56672

When scrolling over a service group used in a filter rule, the tooltip that sets out all the services included in the group would not appear. This anomaly has been fixed.

Support reference 58535

When scrolling over a service used in a filter rule, incomplete information would be given in the tooltip. This anomaly has been fixed.

Support reference 59297

When scrolling over an *IP address range* network object used in a filter rule, the tooltip would wrongly display the message "Object not found". This anomaly has been fixed.

Support reference 55190

Policy-based routing (PBR)

In a configuration such as the following:

- A static route is applied to a network,
- A filter rule implements policy-based routing (PBR) to the same network for a particular port,
- Address translation is applied when packets leave the firewall,

reloading filter rules would prevent connections matching the PBR rule from being set up.

Support reference 50977

Dynamic DNS

Changes to the firewall's IP address were no longer applied to the Dynamic DNS provider whenever the SSL protocol was used, and the verification of this provider's certificate would even fail. This issue has been fixed.

Support reference 55728

Configuration

Changes made to the name of the firewall (**System** > **Configuration** module) were neither applied to the sender name for email alerts, nor in the SN Real-Time Monitor dashboard. This anomaly has been fixed.

Support reference 56734

System events

The report generated whenever a brute force attack was blocked would not contain the blocked source IP address. This anomaly has been fixed.

Network

Support reference 57328

VLAN

The firewall would not correctly send the last fragment of a UDP packet meant to go through a VLAN to the parent interface of the VLAN. This issue has been fixed.

Virtual interfaces

Support reference 53881

Whenever a GRE virtual interface that was initially created as inactive was assigned an IP address, its change in status would not immediately be applied in the web administration interface. The user would therefore need to change modules before going back to the virtual interface module in order to view this change. This anomaly has been fixed.

Support reference 58685

Outbound throughput statistics of virtual IPSec interfaces would always display a null value. This anomaly has been fixed.

Intrusion prevention

Support reference 57396

For certain streams of traffic that always use the same source port, whenever they passed through a rule in firewall or IDS mode, resetting the first connection would prevent the setup of the connections that immediately follow. These connections would, in fact, have been considered

reset as well. This issue has been fixed by allowing the same source port to be reused in firewall and IDS modes (*TCP Closed FastReuse*).

Support reference 53011 - 58465

TeamViewer application

After an upgrade of the TeamViewer application, the IPS scan of traffic relating to this application would wrongly set off an "Unknown SSL protocol" block alarm. This issue has been fixed.

Support reference 53094

RTSP (Real-Time Streaming Protocol)

The intrusion prevention system would wrongly block the *Scale* header in the *Play* method. This anomaly has been fixed.

Support reference 51867

HTTP

In configurations that use policy-based routing (PBR) for HTTP traffic, enabling the **Apply the NAT rule on scanned traffic** option (**Global configuration** of HTTP in the **Application protection** > **Protocols** module) would cause the incorrect routing of packets generated by the proxy.

Support reference 53640

As the *YouTube for Education* filter mechanism is no longer active, it has been replaced with the *Youtube restrictions* mechanism. This new mechanism can be enabled and configured (strict or moderate restriction) in the **IPS** tab in HTTP (**Application protection** > **Protocols** module).

Support reference 58409

SIP

The maximum number of child connections allowed for SIP has been increased in order to allow:

- 127 simultaneous calls on U30S, U70S, SN150, SN200 and SN300 models,
- 1023 simultaneous calls on other models,

instead of 16 as was previously the case on all models.

Support reference 53886

ICMP

Whenever several ICMP requests were received or sent with the same identifier, the same sequence and different data, the firewall would not take into account reply packets from the first request and would block the requests that follow ("ICMP ECHO paylod modified" alarm). This anomaly has been fixed.

Web administration interface

Support reference 54459

SSL protocol

Whenever a checkbox was selected in the **SSL negotiation** section of a given profile, and such a change was applied, the same checkbox would be selected in all profiles by mistake. This issue has been fixed.

Monitoring - Reports - Audit logs

Support reference 56766

Reports

On firewall models that do not have log partitions (diskless models), an anomaly with the checkbox for enabling reports (**Local storage** tab in the **Notifications** > **Logs - Syslog - IPFIX** module) has been fixed.

Support reference 57247

Monitoring

Whenever reports and history graphs were both disabled (**Notifications** > **Report configuration** module), history graphs covering the past 30 days could not be displayed. This issue has been fixed.

Support reference 53352

Logs

Commands to monitor inactive services on the firewall (*MONITOR POWER*, *MONITOR FWADMIN*,...) were wrongly logged in the *l_server* log file. This anomaly has been fixed.

Support reference 54926

Multicast routing

User accounts holding all administration privileges were unable to apply configuration changes made in the **Network** > **Multicast routing** module (error message "There is nothing to save"). This anomaly has been fixed.

Stormshield Network Real-Time Monitor

Support reference 58502 - 57414

Users

The command to delete users, available via the pop-up menu (right-click) in the **Users** module, no longer worked. This issue has been fixed.

Compatibility

Lowest version required: Stormshield Network 2.x

Hardware compatibility:

SN150, SN200, SN300, SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN3000 and SN6000

SNi40

NETASQ U30S, U70S, U150S, U250S, U500S and U800S

Stormshield Network and NETASQ Virtual Appliances

Hypervisor compatibility:

VMWare ESX/ESXi: version 5.5 and upwards

Citrix Xen Server: version 6.2 and upwards

Microsoft Hyper-V: Windows Server 2012 and upwards

Linux KVM: Red Hat Enterprise Linux 7.2 and upwards

Lowest versions required for Stormshield Network client software:

SSO Agent: version 1.4 and upwards

SSL VPN Client: version 2.0 and upwards

Software compatibility for the installation of the administration suite (SN Real-Time Monitor and SN Global Administration):

Microsoft Windows 7, 8 and 10

Microsoft Windows Server 2008 and 2012

NOTE

In order for the firewall administration interface to operate optimally, you are advised to use the latest versions of Microsoft Internet Explorer and Mozilla Firefox (LTS version - Long Term Support). 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 3 of the firmware, ensure that you have:

- read the section Known issues carefully,
- read the section Explanations on usage carefully.
- **perfomed a backup** of the main partition on the backup partition and performed a configuration backup

Extended Web Control

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

Updating a cluster with several high availability links

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

SSO agent authentication method

In a configuration using he "SSO Agent" authentication method, the SSO agent has to be migrated to version 1.4 before migrating the firewall's version.

The "domain name" field must also be entered in the configuration of the SSO agent BEFORE MIGRATING THE FIREWALL. This domain name must match the actual name of the domain (e.g.: stormshield.eu) in order to let the SSO agent run.

Policy-based routing

If the firewall has been reset to its factory settings (*defaultconfig*) after a migration from a 1.x version to a 2.x version then to a 3.x version, the order in which routing will be evaluated will be changed and policy-based routing [PBR] will take over priority (policy-based routing > static routing > dynamic routing >...> default route). However, if the firewall has not been reset, the order of evaluation stays the same as in version 1 (static routing > dynamic routing > policy-based routing [PBR] > routing by interface > routing by load balancing > default route).

Filter policies and users

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

Known issues

Intrusion prevention

REGISTER SIP requests that contain asterisks in the Contact field in their headers are not supported. They generate a block alarm "*The SIP request contains an invalid URI (Contact field)*".

System

Support reference 58515 58520 58594 58634

Audit logs - Reports

Migration to version 3 of the firmware deliberately disables the "Top web searches" report. This report is particularly prone to causing the firewall's log service to hang regularly and this instability causes major network traffic disruptions (proxy and security inspections).

The report can however be disabled at the end of the migration process (**Notifications** > **Report configuration** module).

Support reference 58919

Address translation

To translate the source of traffic sent by the firewall, the destination after translation must not be specified. To do so, delete the *Any* value specified in the **Destination** column in the section **Traffic after translation**.

Routing

IPSec interfaces cannot be used for specifying the type of routing in filter rules for IPv6 traffic. This restriction affects interfaces that have been specified directly as well as router objects containing IPSec interfaces.

Filtering

The field corresponding to the name of a filter rule (*rulename*) does not appear in proxy log files.

Support reference 59620

High Availability

Choosing a VLAN that belongs to an aggregate (LACP) used as the main high availability link prevents the high availability mechanism from running on this link. In such configurations, the MAC address assigned to this VLAN on each firewall is 00:00:00:00:00:00.

Hardware

Support reference 58532

The *Online* LED located on the front panel of the SN150 firewall does not light up when the appliance starts.

Explanations on usage

Network

Spanning Tree protocols (RSTP / MSTP)

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

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

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

- MSTP does not support PPTP/PPPoE modems,
- RSTP supports neither VLANs nor PPTP/PPPoE modems.

Interfaces

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

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

On SN150 models, configurations that contain several VLANs included in a bridge will not be supported.

An issue was identified on U30S and SN200 appliances during the creation of several VLANs in a bridge. This issue may potentially cause an error during the transmission of the responses to ARP requests received on these VLANs to other interfaces of the bridge.

Bird dynamic routing

The Bird dynamic routing engine having been upgraded to version 1.6, in configurations implementing BGP with authentication, the "*setkey no*" option must be used. For further information on Bird configuration, please refer to the **Bird Dynamic Routing** Technical Note.

When a Bird configuration file is edited from the web administration interface, the "Apply" action will send this configuration to the firewall. If there are syntax errors, a warning message indicating the row numbers containing errors will inform the user of the need to correct the configuration.

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

IPv6 support

In version 2, the following are the main features that are unavailable for IPv6 traffic:

- IPv6 address translation (NATv6),
- Application inspections (Antivirus, Antispam, HTTP cache, 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.

System

Migration

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

Updates to a lower version

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

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

URL filtering

SN150, SN200, SN300, U30S and U70S models do not allow the use of more than 10 URL filter profiles. On other models, profiles can only be added by editing the URL filter configuration file (ConfigFiles/URLFiltering/slotinfo) in order to add extra sections to it then by creating or downloading the corresponding profiles (11, 12, etc) to the ConfigFiles/URLFiltering folder.

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 has been performed on a firewall whose system version is higher than the current version, it will be impossible to restore this configuration. For example, a configuration backed up in 3.0.0 cannot be restored if the firewall's current version is 2.5.1.

Dynamic objects

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

DNS (FQDN) name objects

DNS name objects cannot be members of object groups.

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

DNS name objects can only be used in filter rules.

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.

Hardware monitoring (watchdog)

SN150 models do not have the hardware monitoring feature (hardware watchdog).

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.

Notifications

IPFIX

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

Activity reports

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

Whether logs are generated by the firewall depends on the type of traffic, which may not necessarily name objects the same way (*srcname* and *dstname*). In order to prevent multiple

representations of the same object in reports, you are advised to give objects created in the firewall's database the same name as the one given through DNS resolution.

Intrusion prevention

GRE protocol and IPSec tunnels

The decryption of GRE traffic encapsulated in an IPSec tunnel would wrongly generate the alarm "*IP address spoofing on the IPSec interface*". The action *Pass* must therefore be configured for this alarm in order for this type of configuration to function.

HTML scan

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 allows keeping the initial routing on an interface is not compatible with the features for which the intrusion prevention engine needs to 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

Support reference 29286

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

H323 support

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

Proxies

Support reference 35328

FTP proxy

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

Filtering

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 command `monitor flush hostrep ip = host_ip_address`.

Support reference 31715

URL filtering

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

IPSec VPN

Decryption

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

PKI

A Certificate Revocation List (CRL) is not required. Even if no CRL is found for the certificate authority (CA), negotiation will be authorized.

Support reference 37332

DPD (Dead Peer Detection)

The VPN feature DPD (Dead Peer Detection) allows checking whether a peer is still up by sending pings.

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 negotiated even before the peer has been identified, and therefore 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

Both versions of the IKE protocol (IKEv1 and IKEv2) currently cannot be used simultaneously in the same IPSec policy.

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).

Authentication

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.

Mobile IPSec clients can only authenticate on the default directory.

Users can only authenticate on the default directory when using SSL certificates and Radius methods.

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 chapter "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 off

Users may only log off from an authentication 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.

High Availability

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 related to the switchover 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. Moreover, clusters in which one firewall uses 32-bit firmware and the other uses 64-bit firmware are not allowed.

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

Stormshield Network administration suite

SN Real-Time Monitor

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

Support reference 28665

The command CLI MONITOR FLUSH SA ALL was initially meant to disable ongoing IPSec tunnels by deleting their SAs (security associations). However, as Bird dynamic routing also uses this type of security association (SA), this command would degrade the Bird configuration, preventing any connections from being set up. This issue also arises with the "Reinitialize all tunnels" function, offered in the Real-Time Monitor interface.

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

SN Event Reporter

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

Documentation

The following technical documentation is available in PDF in the documentation base in the client area. 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
- Stormshield Network virtual firewalls - Installation guide
- Stormshield Network Global Administration - User and configuration manual
- Stormshield Network Real-Time Monitor - User and configuration manual
- CLI Serverd - Commands reference guide
- CLI Console / SSH - Commands reference guide

Technical notes

- Level 2 encapsulation
- Stacking: distribution of traffic among several firewalls
- LACP link aggregation
- Identifying industrial protocol commands going through the firewall
- IPSec virtual interfaces
- SSL VPN tunnels
- Automatic backups
- Customized URL filter database
- Description of audit logs
- Firewall-appliance cloud hybrid mode
- Bird dynamic routing
- Collaborative security
- Stormshield Network Security for Cloud - Amazon Web Services
- Stormshield Network Security for Cloud - Microsoft Azure

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

Hashes

In order to check the integrity of Stormshield Network Security binary files, enter one of the following commands and compare the result with the hashes indicated in the MyStormshield client area, under **Downloads** > **SNS** > **Firmware** or **Software**:

- Linux operating system: `sha256sum filename`
- Windows operating system: `CertUtil -hashfile filename SHA256`

Replace `filename` with the name of the file you want to check.

Contributions from previous versions of Stormshield Network Security 3

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

3.0.3		Bug fixes
3.0.2		Bug fixes
3.0.1	New features	Bug fixes
3.0.0	New features	

New features in version 3.0.3

System

SNMP

A new OID (Object Identifier) ntqifDrvName corresponding to the system names of network interfaces has been added to the NETASQ-IF-MIB (Management Information Base) .

Directory configuration

The field that defines the name of an LDAP directory has been renamed "Domain name".

Version 3.0.3 bug fixes

This list is not exhaustive and other fixes may have been included in this version.

System

Authentication

Support reference 58610

Migrating a configuration that uses the "Guest" authentication method together with the customized "e-mail" field would cause an error on the captive portal as this field was not converted properly. This anomaly has been fixed.

Support reference 58816

Attempting to upgrade a configuration with a customized firewall name (**Configuration** module) and the **Use firewall name or certificate CN as FQDN** option selected (**Captive portal** – **Advanced properties** tab in the **Users > Authentication** module in version 2) to version 3 of the firmware would make SPNEGO ineffective.

Directory configuration

Support reference 58512

When migrating configurations that reference external LDAP directories to version 3, such directories would adopt the object name of the LDAP server instead of the domain name. This anomaly, which made the SSO Agent method ineffective, has been resolved and the name of the directory is now made up of the root domain (base DN) declared during its creation.

Support reference 58883

Attempts to migrate to version 3 configurations that reference external LDAP directories with a root domain (DN) containing one or several uppercase letters would render such directories invalid. This issue has been fixed.

Support reference 58825

Filtering and NAT

The display would not refresh during switches from a local filter policy to a global filter policy bearing the same index.

Support reference 58475

SSL VPN portal

The latest versions of the Java client application could prevent connections to servers that can be contacted via the SSL VPN portal as they would reject certificate authorities signed with MD5. This issue has been fixed.

Support reference 58746

Access privileges

The selection of a user in the **Detailed access** tab in the **Access privileges** module would result in his/her identifier being replaced with his/her first and last names. This issue, which caused authentication to malfunction, has been fixed.

Intrusion prevention

Support reference 58572 58589 58742 58553

HTTP

An anomaly in the HTTP security inspection would cause the firewall to hang and the proxy to consume an excessive amount of CPU resources. This anomaly has been fixed.

Web administration interface

Directory configuration

Support reference 58871

Backup servers added to the advanced properties of external directories (Microsoft Active Directory, external LDAPs or PosixAccount LDAPs) would no longer appear after a user browses in the other modules of the web administration interface. This anomaly has been fixed.

Support references 58734 - 58704 - 58900

The web administration interface would not apply changes made to the selection filter of user groups in external directories (**Structure** tab in the directory). This anomaly has been fixed.

Monitoring - Reports - Audit logs

Support reference 58921

User monitoring

When several users were authenticated and connected, refreshing the user monitoring module using the Refresh button would cause the firewall to hang. This issue has been fixed.

Activity Reports

On firewall models that do not have log partitions (diskless models), once the 5 reports allowed were enabled, the corresponding data would not be displayed.

Version 3.0.2 bug fixes

This list is not exhaustive and other fixes may have been included in this version.

Intrusion prevention

Support reference 57337

SSL protocol

An issue regarding access to websites using CHACHA20 and Poly1305 encryption suites has been fixed following the upgrade of these suites.

System

Support reference 57350 57356

SSL VPN - IPsec VPN

After a migration to SNS v3, connections via the SSL VPN client or IPsec VPN client could fail to function as the *sslvpn* and *ipsec* interfaces were linked to the *Guest* profile. This issue has been fixed and these interfaces will no longer be associated with any profile after a migration.

Support reference 58536

Authentication

A migration to SNS v3 could cause the *Internal* profile of the captive portal to be associated with an unknown interface ("0" interface). This anomaly, which would then prevent these associations from being modified (*Captive portal* tab in the **Configuration > Users > Authentication** module), has been fixed.

Support reference 58433

Proxies

Enabling the DNS cache before a proxy cache could cause the proxy to hang when the firewall is restarted.

Support reference 56184

Filtering

It was impossible to add URLs that were accessible without authentication in a filter rule specifying a redirection to the authentication portal. This issue has been fixed.

High availability

Support reference 58530

In a high availability configuration, the synchronization mechanism could wrongly attempt to enable the hardware *bypass* system reserved for industrial firewalls (SNi40 model). This anomaly, which would generate a synchronization error, has been fixed.

Support reference 58367

The upgrade of a firewall cluster to version 3 could fail during the synchronization of the license file with the passive appliance. This issue has been fixed.

Support reference 58113

Extended Web Control

If the synchronous mode of the Extended Web Control URL filtering solution was enabled on a firewall in version SNS v2, this mode will be automatically disabled in favor of asynchronous mode during a migration of the firmware to v3.0.2.

Support reference 58496

Automatic backups

Enabling automatic backups in a configuration using several LDAP directories could fail and disable the LDAP module. This issue has been fixed.

Dashboard

Support reference 56635

LDAP configuration

The dashboard of a firewall that does not have a configured LDAP directory would display a misleading message ("LDAP configuration: Disabled. The directory has been configured but the module has not been enabled"). This anomaly has been fixed and the message "No default directory has been configured or enabled" will now appear.

New features in version 3.0.1

SN150 model firewalls

Version 3.0.1 of the firmware ensures compatibility with SN150 firewalls.

Version 3.0.1 bug fixes

Intrusion prevention

Support reference 56973 57355

IDS / Firewall modes

In a configuration that implements filter rules in IDS or Firewall mode and authentication, invalid ICMP traffic that raises alarms which do not block such traffic (*Pass* action) would cause the firewall to hang. This issue has been fixed.

Support reference 56740

Memory resources

Whenever there is a large number of connections, an anomaly in the management of memory resources would cause the firewall to hang then restart. This anomaly has been fixed.

System

Support reference 56964

IPSec tunnels (IKEv2)

Whenever the email address field of a CA used for signing server certificates was filled in, the firewall would refuse to set up IKEv2 IPSec tunnels for which authentication was based on such certificates. This anomaly has been fixed.

Activity Reports

"Host reputation" report

An error in the application of destination host reputations for SSL connections has been fixed.

New features in version 3.0.0

Unified web interface

The unified web interface now covers the administration, monitoring and reporting of Stormshield Network firewalls.

A new monitoring window offers graphs (in real time and with history statistics) on system resources used (memory and CPU), throughput per interface and connected users as well as detailed information on machines (ongoing connections, applications used, vulnerabilities detected, etc).

Many interactive features facilitate the search for incidents and the administration of Stormshield Network firewalls.

Temporary user management

In order to provide easy Internet access to persons outside the organization or in public places, Stormshield Network products offer advanced features for managing temporary users.

In addition to guest mode, which was already available, version 3 includes "sponsorship" mode and a new portal to create temporary accounts.

The current "guest" portal may be enriched with new fields (first name, last name, e-mail address, etc) that the user will need to enter before accepting the Internet access charter.

Temporary accounts can be created easily thanks to a simplified screen that can only be accessed by persons authorized to create such accounts.

"Sponsorship" mode makes it possible to delegate - to an authorized person - the privilege of accepting or rejecting an Internet access request from a person outside the organization.

Many enhancements allow customizing users' various access portals.

Integration into a multi-domain environment

Users can now be authenticated on several Active Directory domains. It is therefore possible to authenticate users originating from various domains and applying distinct security policies to them.

Multiple directories also offer the possibility of registering firewall administrators in an internal directory and managing unprivileged users in an external directory.

IP geolocation - Country-based filtering

Thanks to the geolocation feature, administrators gain visibility over the source or destination of their network traffic. Security policies can therefore be adapted to filter traffic according to new geographical criteria represented by "Country" or "Continent" objects.

All log files and reports have been enriched with a new item corresponding to the country.

IP Reputation – External host reputation

This feature, which can be combined with geolocation, makes it possible to lower an organization's attack risk.

Public IP addresses with a bad reputation (e.g.: Tor exit nodes) will fall under one of seven categories: Spam, Phishing, Anonymizer, Botnet, Malware, Tor or Scanner. These categories are regularly updated through the Active Update mechanism.

Through his security policy, the administrator can therefore block external machines with bad reputations from attempting to access the organization's network, and prohibit connections from internal workstations to reputedly risky hosts.

Dynamic Host Reputation – Internal host reputation

Security policies can now be assigned based on the reputation of internal hosts.

Reputations, represented by a score, can be calculated dynamically thanks to ratings provided by the inspection engines built into Stormshield firewalls. Whenever our sandboxing solution detects a virus, raises a major alarm or identifies malware, the host's score will automatically be raised.

Administrators can view the history of a host's reputation score in the new "monitoring" module. Other indicators such as the average score of a network and the maximum score, provide addition information to help them define their security policies and act on hosts that require intervention.

This feature requires the use of a SD card if there is no hard disk on the firewall.

"DNS names (FQDN)" objects

In order to refine a security policy, it is now possible to use network objects defined only by their FQDN (IP address(es) automatically retrieved by DNS resolutions) such as "google.com" or "office365.com".

Safe transmission of Syslog traffic through the TLS protocol

The transmission of logs to one or several Syslog servers (maximum 4) via TCP can now be secured through the TLS protocol with client and server certificate authentication.

This secure transmission of Syslog traffic is compatible with the Stormshield Visibility Center solution.

Stormshield Network firewalls support several standardized formats of Syslog messages (RFC3164, RFC5424, RFC5425 and RFC6587).

Possibility of configuring the hash algorithm in the internal PKI and the SSL proxy

The Certificates and PKI module offers the possibility of selecting the hash algorithm (in particular SHA256) used for the certificates of the SSL proxy and the firewall's internal PKI.

IPFIX/Netflow support

Compatibility with Netflow/IPfix collectors allows administrators to easily identify potential network issues.

Customized signatures on the intrusion prevention (IPS) engine

Administrators can now create their own context-based signatures in order to detect applications inside the organization.

SNi40 - Hardware bypass

In order to ensure service continuity in an industrial setting, the SNi40 firewall is equipped with a hardware bypass function, which when enabled, allows network traffic to pass through in the event of a power outage or appliance breakdown.

Importing and exporting the contents of the network objects database

Exporting the objects database in CSV format makes it possible to save the database and reimport it directly into the Stormshield Management Center centralized administration solution.

The structure of the rows that make up the objects database in CSV format is available in **Appendix B** of the **Stormshield Network Configuration and Administration Manual**.

Official support for KVM and Hyper-V virtualization platforms

Stormshield Network virtual firewalls are available for Microsoft Hyper-V (VHD format) and KVM platforms (Kernel-based Virtual Machine - QCOW2 format). The supported versions of hypervisors are listed in the Compatibility chapter of this document.

Intrusion prevention scans on HTTP traffic with on-the-fly decompression

The intrusion prevention engine is now capable of decompressing HTTP data on the fly in order to perform IPS scans on this protocol. The firewall therefore no longer needs to modify the headers of HTTP packets sent by the client in order to mask compression support (*accept-encoding*). As a result, this mechanism reduces latency and the amount of data needed for transferring HTTP packets, but demands a greater amount of the firewall's resources.

This feature is enabled by default and can be suspended in the HTTP configuration module.

Possibility of adding a constraint on the *Domain name* of the certificate presented by an IPSec peer.

When a certificate authority (CA) is specified in the list of trusted authorities for the establishment of IPSec tunnels, a constraint can be added on the Domain Name (DN) of the certificate presented by the peer in order to strengthen security.

CRL verification and support for *BindAddr* in the firewall's LDAP requests

In the firewall's LDAP configuration, the BindAddr parameter followed by the firewall's private IP address forces the firewall to present this IP address during LDAP requests to an external directory: LDAP traffic can therefore be encapsulated in an IPSec tunnel in order to encrypt requests to the directory.

This parameter can only be modified in command line (setconf ConfigFiles/ldap *LDAP_Name* BindAddr *FW_Private_IP*).

IPS scans of the Ethernet/IP industrial protocol

The intrusion prevention engine now allows filtering (*Analyze / Block*) public command sets for this protocol. A customized list of Ethernet/IP commands that need to be allowed can also be specified.

Intrusion prevention scans for SNMP

SNMP (Simple Network Management Protocol) is a network equipment monitoring protocol. The IPS scan for this protocol has been particularly enriched. It therefore now possible to allow or block SNMP packets according to the version of the protocol (SNMPv1, v2c or v3), create community whitelists/blacklists (SNMPv1 and v2c), identifiers (SNMPv3) or OIDs (*Object Identifier*).

NAT support for Dynamic DNS

The module that sends the public IP address to the dynamic DNS registration service provider now distinguishes the real public IP address presented by a NAT router from the local address. This feature can be enabled by selecting Support address translation (NAT) in the advanced properties of the Dynamic DNS module.

SSL proxy - Support for new encryption algorithms

The SSL proxy supports new encryption algorithms based on elliptic curves (ECDSA algorithm: Elliptic Curve Digital Signature Algorithm).

Systematic verification of unused objects

The **Network objects** module displays the list of objects found in the firewall's database; objects are classified by category (hosts, networks, DNS domain names [FQDN], etc).

A colored symbol appears before each object, dynamically indicating whether the object is being used in the firewall's configuration (green chip) or not (gray chip). Clicking on the "eye" icon located to the right of a green chip will list all the modules using the object in question.

Rule names in IPS logs and active connection logs

The Filter and NAT module makes it possible to assign a name to each rule created. Do note that the "Name" column is hidden by default.

This rule name (*rulename*) is referenced in IPS logs and connection logs. It has the advantage of not changing according to rule criteria (via, interface, etc) or the position of a rule in a filter policy, unlike rule identifiers (*ruleid*). As such, filter or NAT rules can be easily handled according to their names.

Exporting monitoring data and audit logs

In the same way as report data, the information displayed in audit logs and the data presented in the tables of the monitoring module can also be exported to a file in CSV format.

Sandboxing – Form to report false positives

The interactions offered on audit logs allow warning Stormshield of any wrong categorization following a sandboxing operation. This feature therefore makes it possible to unblock attachments that have been wrongly considered malicious.

Authentication

The maximum length of an identifier has been raised to 255 characters. Moreover, users can now be included in 250 groups (this limit used to be 50 in older versions).

SSL VPN

The SSL VPN Client configuration file now includes register-dns and block-outside-dns options indicating, respectively, for the client to write the DNS server(s) specified by the Stormshield Network firewall to its configuration, and to not use third-party DNS servers. This feature shortens the time needed for receiving responses to the client's DNS requests, especially for machines running in Microsoft Windows 10.

Child connections (active FTP) through virtual IPSec interfaces

Traffic that creates child connections (e.g.: active FTP) is now compatible with the use of virtual IPSec interfaces (VTI).

TCP-based DNS requests

Stormshield Network firewalls automatically switch their DNS requests over to TCP whenever they receive a response exceeding 512 bytes (response with many entries such as dynamic objects and DNS name objects [FQDN]).

Addition of logs in stateful pseudo-connections

Stateful pseudo-connections (GRE, ESP, etc) now generate registrations in connection log files (*l_connection*) and filter statistics files (*l_filterstat*).

Support for generic 3G/4G modems

For generic 3G/4G modems whose characteristics are not automatically recognized, up to two profiles grouping configuration information (model, vendor ID, etc) can be defined, such information having to be manually entered. The various fields to configure are explained in the chapter **Creating a modem** in the **Stormshield Network Configuration and Administration Manual**.

Strengthening the IPS scan on TCP

The TCP IPS scan has been strengthened in order to detect data in RESET packets and setting off the specific alarm "TCP RST with data". It can now also handle a larger amount of unacknowledged data without setting off alarm no. 84 "TCP data queue overflow".

Other features

- Improvement of the intrusion prevention scan on the SSL protocol with regard to fragmented headers
- Support for Unicode international characters in certificates
- Inclusion of source and destination object names in alarm e-mails
- Addition of the firewall's system name in Shell command prompts

Contact

To contact our Technical Assistance Center (TAC) Stormshield:

- https://mystormshield.eu/

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

- +33 (0) 9 69 329 129

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