STORMSHIELD

GUIDE

STORMSHIELD NETWORK SECURITY

USER CONFIGURATION MANUAL

Version 5.0.3 EA

Document last updated: November 14, 2025

Reference: sns-en-user_configuration_manual-v5.0.3-EA

Table of contents

WELCOME 7
Recommendations on the operating environment 7
User awareness 13

GETTING STARTED WITH THE SNS FIREWALL 17
Logging in to the firewall web administration interface 17
Understanding the graphical user interface 17

ACCESS PRIVILEGES 19
Default options tab 19
Detailed access tab 19

ACTIVE UPDATE 22
Update 22
Manual update for security databases 22
Advanced properties 22

LOGS - AUDIT LOGS 23
Actions 24
Displaying details of a row of logs 26
Interactive features 26
Logs 30

ADMINISTRATORS 33
Administrators tab 33
Administrator account tab 38
Ticket management tab 38

ANTISPAM 40
General tab 40
Whitelisted domains tab 42
Blacklisted domains tab 43

ANTIVIRUS 44
Settings 44

APPLICATIONS AND PROTECTIONS 45
New alarms 45
View by inspection profile 45
View by context 49

AUTHENTICATION 50
Available methods tab 50
Authentication policy tab 64
Captive portal tab 68
Captive portal profiles tab 70
Transparent or explicit HTTP proxy and multi-user objects 73

BLOCK MESSAGES 76
Antivirus tab 76
Block page tab 77

CERTIFICATES AND PKI 79
Possible operations 79
Adding authorities and identities 81
Revoking an authority, sub-authority or certificate 90
Creating, renewing or removing a CRL 91
Removing the private key of an identity (while keeping the certificate) 92
Defining a default authority or sub-authority 93
Downloading a certificate 93
Downloading an identity 93
Downloading a CRL 94

CLI CONSOLE 95
List of commands 95
Data entry section 95

CONFIGURATION 96
General configuration tab 96
Firewall administration tab 103
Network Settings tab 107

CONFIGURING MONITORING 108
Interval between refreshments 108
Configuring interfaces, QoS queues and web services to be monitored 108

DASHBOARD 110
Network 110
Protections 110
Properties 111
Messages 112
Services 112
Health indicators 113
Pay As You Go 115
Monitoring and configuration modules 116

DHCP 117
General 117
“DHCP server” service 117
“DHCP relay” service 120

DIRECTORIES CONFIGURATION 122
Main window 123
Creating an internal LDAP 123
Connecting to an external LDAP directory 125
Connecting to a PosixAccount external LDAP directory 130
Connecting to a Microsoft Active Directory 135

DNS CACHE PROXY 141
Enable DNS cache 141

DYNAMIC DNS 143
List of dynamic DNS profiles 143
Configuring a profile 143

DYNAMIC ROUTING 146
General tab 146
BIRD v2 tab 147
IPv4 BIRD v1 and IPv6 BIRD v1 tabs 148

E-MAIL ALERTS 150
Notifications tab 150
Recipients tab 151
Templates tab 152
SMTP server tab 154

ENROLLMENT 156
The table 156
Information about the selected enrollment request 156
Advanced properties 157

FILTERING AND NAT 158
Evaluation of filtering and the impact of NAT 158
Policies 158
Filtering tab 161
NAT tab 178

HIGH AVAILABILITY 188
Step 1: Creating or joining a high availability cluster 188
Step 2: Configuring network interfaces 189
Step 3: Cluster's pre-shared key and data encryption 191
Step 4: Summary and finalizing the cluster 192
High availability screen 192

HOST REPUTATION 196
Configuration tab 196
Hosts tab 197

IDENTIFICATION PORTAL 198
Connection 198
The "admin" account, super administrator200
Logging off 200

IMPLICIT RULES 201
Implicit filter rules 201

INSPECTION PROFILES 204
Global configuration 204
Configuring profiles 205

INTERFACES 206
Interfaces 206
Possible operations 206
Bridge interface 207
Ethernet interface 212
Wi-Fi interface (WLAN) 217
VLAN interface 219
Aggregate 224
GRETAP interface 227
PPPoE/PPTP modem interface 229
USB/Ethernet interface (for USB key/modem) 231
Network configuration modes 233

IPSEC VPN 235
Encryption policy – Tunnels tab 236
Peers tab 245
Identification tab 252
Encryption profiles tab 255

IPV6 SUPPORT 260
IPv6 Support 260
Configuration 263
Bridges and interfaces 264
Virtual interfaces 267
Routing 267
DHCP 271
Network objects 274
Filtering 275

LICENSE 277
Firewalls with several models on the same physical platform 277
General tab 277
Local license tab 279

Remote firewall remote_firewall_serial_no. license tab 283

LOGS - SYSLOG - IPFIX 284
Local storage tab 284
Syslog tab 286
IPFIX tab 287

MAINTENANCE 289
System update tab 289
Backup tab 290
Restore tab 292
Configuration tab 293

MONITORING 295
Hardware / High Availability 297
System 300
Interfaces 301
QoS 303
Hosts 304
Web Services 310
Users 310
Connections 315
SD-WAN 319
Dynamic multicast routing 322
DHCP 326
SSL VPN tunnels 327
IPsec VPN tunnels 329
Black list / white list 333
Network captures 333

NETWORK/TIME OBJECTS 338
Possible actions 338
The various types of objects 340

PREFERENCES 351
Parameters tab 351
Display tab 352
Links tab 353

PROTOCOLS 354
Search 354
List of protocols 354
Profiles 354
Global protocol configuration 355
Live Messenger (MSN) 358
Yahoo Messenger (YMSG) 358
ICMP 359
IP 359
SCTP 360
TCP-UDP 360
IEC 61850 GOOSE (IPS) 363
MMS/IEC 61850 MMS 364
IEC 61850 SV (IPS) 366
BACnet/IP 366
CIP (IPS - CIP tab) 366
ETHERNET/IP (IPS tab) 367
IEC 60870-5-104 (IEC 104) 368
MODBUS (IPS) tab 370
OPC AE (IPS) tab 371
OPC DA (IPS) tab 371
OPC HDA (IPS) tab 372
OPC UA 372
PROFINET IO 373
PROFINET RT 374
S7 374
S7 PLUS 375
UMAS (IPS) tab 377
Microsoft RPC (DCE/RPC) protocol 378
NetBios CIFS (IPS tab) 381
NETBIOS EPMAP (IPS) tab 381
NetBios SSN 382
MGCP (IPS tab) 382
RTCP (IPS tab) 383
RTP (IPS tab) 383
RTSP 383
SIP (IPS tab) 385
SOFBUS/LACBUS (IPS) tab 387
DNS (IPS tab) 388
FTP 389
HTTP 396
NTP 404
POP3 408
SMTP 411
SNMP (IPS tab) 415
SSL 416
TFTP (IPS tab) 423
Others 423

REST API 425
General configuration tab 425
API keys tab 426

QUALITY OF SERVICE (QoS) 428
Queues tab 428
Traffic shapers tab 432

REAL-TIME LOGS 434
Log file selection field 434
Log display 434
Possible operations 434

Interactive features 435

RECORDING CONFIGURATION COMMANDS 436

Recording a sequence of configuration commands 436

ACTIVITY REPORTS 437

Possible actions on reports 438
Available reports 439

REPORT CONFIGURATION 445

General 445
List of reports tab 445
List of history graphs tab 446

ROUTING 447

IPv4/IPv6 static route tabs 447
IPv4/IPv6 return routes tab 448

SMTP FILTERING 450

Profiles 450
Rules 450

SNMP AGENT 453

General tab 453
SNMPv3 tab 454
SNMPv1 - SNMPv2c tab 456
MIB and SNMP traps 457

SSL FILTERING 459

Profiles 459
Rules 460

SSL VPN 463

General configuration tab 463
Client workstation verification (ZTNA) tab 466
Windows client workstation verification (ZTNA) tab 467

MULTICAST ROUTING 469

STATIC ROUTING TAB 469
Dynamic routing tab 471

STORMSHIELD MANAGEMENT CENTER 476

Connecting the firewall to the SMC server 476

SYSTEM EVENTS 477

Possible operations 477
List of events 477

TEMPORARY ACCOUNTS 479

Temporary accounts list 479

TRUSTED PLATFORM MODULE (TPM) 482

Initializing the TPM 482
Using certificates with TPM-protected private keys 482
Explanations on usage with the TPM 483

URL FILTERING 484

Profiles 484
Rules 485

USERS 487

LDAP directory tab 487
Microsoft ENTRA ID tab 492

VIRTUAL INTERFACES 496

Creating or modifying IPsec interfaces (VTI) 496
Creating or editing a GRE interface 497
Creating or modifying a loopback interface 499

URL OBJECTS 501

URL tab 501
Certificate names (CN) tab 504
URL database tab 505

WEB SERVICES 506

List of web services tab 506
Groups tab 507
Import custom services tab 509

Wi-Fi 511

General configuration 511
Channel configuration 511

Allowed or prohibited characters 512

Firewall name 512
Admin password of a virtual firewall on Microsoft Azure 512
Login and password 512
Filter - NAT 512
Names of network interfaces 512
Network objects 513
DNS (FQDN) name objects 513
Certificates and PKI 513
LDAP databases 513

IPsec VPN 514
SSL VPN Portal 514
Quality of Service (QoS) 514
E-mail alerts 514
Web services 515
TPM password 515

Structure of an objects database in CSV format 516

Host 516
IP address range 516
DNS name (FQDN) 516
Network 517
Port 517
Port range 517
Protocol 518
Host group, IP address group or network group 518
Service group 518

Structure of the file importing custom web services (CSV format) . 519

WELCOME

Welcome to the Stormshield Network v5.0.3 EA user configuration manual.

This guide explains the features of the web administration interface modules, and provides information on how to configure your Stormshield Network firewall for your network.

The Release Notes contain highly important information. Please refer to them before installing or updating your firewall.

For any questions, or if you wish to report errors, feel free to contact us at documentation@stormshield.eu.

Products concerned

SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320,

SN510, SN-M-Series-520, SN710, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200,

SNi10, SNi20, SNi40, SNxr1200,

EVA1, EVA2, EVA3, EVA4 and EVAU.

Copyright © Stormshield 2025. All rights reserved.

Unauthorized copying, adaptation or translation of this document **prohibited**.

The contents of this document relate to the developments in Stormshield's technology at the time of its writing. With the exception of the mandatory applicable laws, no guarantee shall be made in any form whatsoever, expressly or implied, including but not limited to implied warranties as to the merchantability or fitness for a particular purpose, as to the accuracy, reliability or the contents of the document.

Stormshield reserves the right to revise this document, to remove sections or to remove this whole document at any moment without prior notice.

Recommendations on the operating environment

The installation of an SNS firewall and an SMC server is part of implementing a global security policy. To ensure optimal protection of your assets, resources and information, installing an SNS firewall between your network and the Internet or installing an SMC server to help you to configure them correctly are only the first steps. This is mainly because most attacks come from the inside (accidents, disgruntled employees, dismissed employee having retained internal access, etc.).

The following is a list of security recommendations on how to use the SNS firewall and the SMC server.

IMPORTANT

- Check regularly for the Stormshield security advisories on https://advisories.stomshield.eu and for the latest security information regarding Stormshield products on https://security.stormshield.eu/.
- Always apply updates if they fix security flaws on your Stormshield products. Updates are available on https://mystormshield.eu.

Recommendations

Physical security measures

SNS firewalls and the SMC server are must be installed and stored according to the state of the art regarding sensitive security devices: secured access to the premises, shielded cables with twisted pairs, labeled cables, etc.

Organizational security measures

Super administrator

A particular administrator role, the super administrator, displays the following characteristics:

- The only administrator allowed to log on via the local console on SNS firewalls, and only during the installation of the SNS firewall or for maintenance operations outside of normal production use,
- In charge of defining the profiles of other administrators,
- All access to the premises where the SNS firewalls and the SMC server are stored must be under the super administrator's supervision, regardless the purpose of the access is to conduct operations on the SNS firewall or on other equipment. All operations performed will be this administrator's responsibility.

IMPORTANT
The default password of the super administrator must be changed the very first time the SNS firewall is used.

Password

User and administrator passwords must be chosen in such a way that it will take longer to successfully crack them, by implementing a policy that regulates how they are created and verified (e.g., mix of alphanumeric characters, minimum length, inclusion of special characters, no dictionary words, etc.).

Administrators can change their password in the web administration interface of:

- SNS in **Configuration** > **System** > **Administrators**, **Administrator account** tab,
- SMC in **Maintenance** > **SMC Server** > **Administrators**.

Administrators are aware of these best practices through their duties and are responsible for making users aware of these practices (see the next section User Awareness).

Good information flow control policies

The information flow control policies to be implemented, for equipments on the trusted networks to be protected, are defined as such:

- **Complete**: standard usage scenarios of how equipments are used have all been considered when defining the rules and their authorized limits have been defined,
- **Strict**: only the necessary uses of equipments are authorized,
- **Correct**: rules do not contradict each other,
- **Unambiguous**: the list of rules provides all the relevant elements for direct configuration of the SNS firewall by a qualified administrator.

Cryptographic keys

Cryptographic keys that were generated outside the SNS firewall and injected into it must have been generated according to the general security guidelines defined by the French National Cybersecurity Agency (ANSSI) in the *Référentiel général de sécurité (RGS)* document (in French).

Human agents

Administrators are non-hostile, competent persons with the necessary means for accomplishing their tasks. They have been trained to perform operations for which they are responsible. Their skills and organization mean that:

- Different administrators with the same privileges do not perform contradictory administrative actions (e.g., inconsistent modifications to the information flow control policy),
- Logs are used and alarms are processed within the appropriate time frames.

IT security environment

SNS firewalls

SNS firewalls are installed in compliance with the current network interconnection policy and are the only passage points between the various networks on which the information flow control policy has to be applied. They are sized according to the capacities of adjacent devices or these devices limit the number of packets per second, set slightly below the maximum processing capacities of each SNS firewalls installed in the network architecture.

Besides the application of security functions, SNS firewalls do not provide any network service other than routing and address translation (e.g., no DHCP, DNS, PKI, application proxies, etc.). SNS firewalls are not configured to forward IPX, Netbios, AppleTalk, PPPoE or IPv6 information flows.

SNS firewalls do not depend on external “online” services (DNS, DHCP, RADIUS, etc.) to apply the information flow control policy.

The IT environment provides:

- NTP reliable timestamps,
- Up to date X.509 certificate revocation status, both for peers and administrators,
- A reliable enrolment infrastructure.

SMC server

A traffic control policy must be applied to the SMC server to allow only its administrators and managed SNS firewalls to log in to it.

The virtual machine must be appropriately scaled (RAM, CPU, disk space) to enable administration on SNS firewalls managed by the SMC server. The SMC operating system must never be modified, so that it can meet needs other than those it was designed to meet.

There must be sufficient and available bandwidth at all times between the SMC server and SNS firewalls so that all administration operations can be performed. The administrator must configure and even disable certain features to meet this requirement, otherwise restrict the number of packets per second to give priority to administration traffic.

The production and distribution of connecting packages, which allow the SMC server to manage SNS firewalls, must be managed and entrusted to individuals who are familiar with security requirements. Such packages must only be shared through secure channels (encrypted e-mails, secured USB keys, etc.) between the SMC server and SNS firewalls.

Interconnectivity

Remote administration workstations are secured and kept up to date on all known vulnerabilities affecting operating systems and hosted applications. They are installed in premises with protected access and are dedicated exclusively to the administration of SNS firewalls, the SMC server and the storage of backups.

Network appliances with which the SNS firewall sets up VPN tunnels are subject to restrictions regarding physical access control, protection and control over their configuration, equivalent to the restrictions placed on SNS firewalls.

Workstations on which the VPN clients of authorized users are launched are subject to restrictions regarding physical access control, protection and control over their configuration, equivalent to the restrictions placed on workstations in trusted networks. They are secured and kept up to date on all known vulnerabilities affecting operating systems and hosted applications.

Configurations and usage mode subject to the evaluation of SNS firewalls

The usage mode subject to evaluation has the following characteristics.

- The evaluation covers the Stormshield UTM / NG-Firewall Software Suite installed on all versions of Stormshield firewalls, from the SN210 to SN6100 range, including industrial models SNi20 and SNi40. Certain models do not have large local log storage capacities and have to send events via syslog,
- SNS firewalls have to be stored in a location with secured access. Such measures, as well as organizational procedures for the operating environment, have to guarantee that the only physical access to the SNS firewalls take place under the surveillance of the super administrator,
- The local console is not used in production. Only the super administrator can log on to it, and hypothetically, such interventions are performed only when a decision has been made to make an exception to the operating context – to conduct a maintenance operation or a re-installation,
- Workstations on which the web administration interface will be used are secured, dedicated to such use, and up to date on all patches concerning the respective operating systems and the applications installed on them,
- The Stormshield Network IPsec VPN Client software is not part of the evaluation. Users can use an IPsec VPN client of their choice, however, these client workstations have to be secured as rigorously as remote administration workstations,
- When external services are used by the SNS firewall, they are not part of the evaluation. However, these servers have to be dedicated to such use, and up to date on all patches concerning the respective operating systems and the applications installed on them. External services are:
  - The NTP time servers,
  - The LDAP administrator and IPSec user directory server,
  - The syslog server,
  - The CRL or OCSP server,
  - The SMC server,
  - The EST certificate enrolment server.

- Those configuration parameters must remain in their factory (default) states:
  - CRLs: regularly downloaded from a CRL server,
  - Internal clock: regularly synchronized with NTP servers,
  - NSRPC administration services (port 1300/TCP): restricted to loopback,
  - IPv6 routing feature: even though it is supported, the IPv6 feature is disabled by default and must remain so for the duration of the evaluation,
  - ESP Anti-replay windows, IKE re-authentication and IKE PFS (Perfect Forward Secrecy): activated,
  - Maximum SA lifetimes: 24 hours for IKE SA and 4 hours for IPsec SA.
- Those application analysis functions are the only protocols covered by the certification:
  - FTP over TCP,
  - HTTP over TCP (including WebDAV extensions),
  - SIP over TCP or UDP,
  - SMTP over TCP,
  - DNS over TCP or UDP.

  And industrial protocols:
  - OPC UA over TCP,
  - MODBUS over TCP.

  Others must not be used in the running configuration.
- The following parameters must not be used in filter policy to associate a filter rule with:
  - An application inspection (HTTP, SMTP, POP3 and FTP proxies),
  - A schedule (Time object),
  - The "decrypt" action (SSL proxy),
  - A host reputation,
  - An FQDN object in source or destination (require external DNS services).
- The following features may be used, but are not considered security functions:
  - Address translation (network address translation or NAT),
  - Quality of Service,
  - High availability,
  - Embedded reports,
  - Filtering based on Geolocation and IP Reputation,
  - Filtering based on MAC address (Ethernet level),
  - Active Update.

- The usage mode subject to evaluation excludes the fact that the SNS firewall relies on services other than previously mentioned services. The optional modules provided by Stormshield to manage these services are disabled by default and have to stay that way. Specifically, these are:
  - Modules that allow handling external servers (e.g., Kerberos, RADIUS, etc.),
  - The dynamic routing module,
  - The static multicast routing module,
  - The internal public key infrastructure (PKI),
  - The SSL VPN module (Portal and Tunnel),
  - DNS cache,
  - Antivirus engines,
  - SSH, DHCP, MPD and SNMPD servers,
  - The DHCP client,
  - The DHCP relay,
  - Wifi connection for equipped devices,
  - Host reputation,
  - For SNi40 and SNi20 models: the hardware bypass capabilities,
  - Any custom IPS patterns,
  - FQDN objects (require external DNS services),
  - IPFIX messages,
  - Telemetry,
  - Breathfighter (Sandboxing),
  - Network Vulnerability Manager (SNVM).

  Administration and monitoring tools provide a way of checking at any moment during operation of these modules are disabled.

- The IKE & IPsec cryptographic algorithms implemented must be:

	Standard IPsec	IPsec DR
Identification	Pre-shared key or Certificate with RSA or ECDSA key (1)	Certificate with ECDSA or ECSDSA key (2) (3)
Authentication/Integrity	SHA-2 256 or 384 or 512 bit	SHA-2 256 bit
Key negotiation	Diffie-Hellman groups 14, 15, 16, 17, 18, 20, 21, 28, 29 and 30 (4)	Diffie-Hellman group 19 or 28
Encryption	AES 128 or 192 or 256 bit in CBC or CTR or GCM mode	AES 256 bit in GCM or CTR mode

(1): The smallest size of an RSA key must be 2048 bits, or 3072 bits for use beyond 2030.
(2): The smallest size of a key must be 256 bits.
(3): Although the use of RSA keys is prohibited in a DR environment, an RSA root certificate can be used to sign an intermediate certificate dedicated to IPsec for example, when the certification authority used as the anchor on the firewall is the intermediate certificate.
(4): For use beyond 2030, the smallest group to use must be Diffie-Hellman group 15.

These cryptographic algorithms are needed for compliance with the general security guidelines defined by the French National Cybersecurity Agency (ANSSI) in the *Référentiel général de sécurité (RGS)* document (in French).

Do note that the recommendations on implementing the strengthened IPsec mode called *Diffusion Restreinte (DR) mode* that complies with ANSSI's reference document for IPsec DR are given in the SNS Technical note "IPsec - *Diffusion Restreinte* mode".

User awareness

Administrator management

The Firewall administrator is in charge of instructing users on network security, the equipment which make up the network and the information which passes through it.

Most users in a network are computer novices and even more so in network security. It is thus incumbent upon the administrator or person in charge of network security to organize training sessions or at least programs to create user awareness of network security.

These sessions should be used to state the importance of managing user passwords and the work environment as well as the management of users' access to the company's resources, as indicated in the following section.

Initial connection to the appliance

A security procedure must be followed if the initial connection to the appliance takes place through an untrusted network. This operation is not necessary if the administration workstation is plugged in directly to the product.

Access to the administration portal is secured through the SSL/TLS protocol. This protection allows authenticating the portal via a certificate, thereby assuring the administrator that he is indeed logged in to the desired appliance. This certificate can either be the appliance's default certificate or the certificate entered during the configuration of the appliance (*Authentication* > *Captive portal*).

The name (CN) of the appliance's default certificate is the appliance's serial number and it is signed by two authorities called NETASQ - Secure Internet Connectivity ("O") / NETASQ Firewall Certification Authority ("OU") and Stormshield ("O") / Cloud Services ("OU").

To confirm a secure access, the browser must trust the certification authority that signed the certificate used, which must belong to the browser's list of trusted certification authorities. Therefore to confirm the integrity of an appliance, the NETASQ and Stormshield certification authorities must be added to the browser's list of trusted certification authorities before the initial connection. These authorities are available at http://pki.stormshieldcs.eu/netasq/root.crt and http://pki.stormshieldcs.eu/products/root.crt. If a certificate signed by another authority has been configured on the appliance, this authority will need to be added instead of the NETASQ and Stormshield authorities.

As a result, the initial connection to the appliance will no longer raise an alert in the browser regarding the trusted authority. However, a message will continue to warn the user that the certificate is not valid. This is because the certificate defines the Firewall by its serial number instead of its IP address. To stop this warning from appearing, you will need to indicate to the DNS server that the serial number is associated with the IP address of the Firewall.

NOTE
The default password of the "admin" user (super administrator) must be changed the very first time the product is used, in the web administration interface via the **Administrator** module (**System** menu), under the *Admin account* tab.

This password must be set in line with the best practices described in the following section, under *User password management*.

This password must never be saved in the browser.

User password management

Throughout the evolution of information technologies, numerous authentication mechanisms have been invented and implemented to guarantee that companies' information systems possess better security. The result of this multiplication of mechanisms is a complexity which contributes to the deterioration of company network security today.

Users (novices and untrained users) tend to choose "simplistic" passwords, in general drawn from their own lives and which often correspond to words found in a dictionary. This behavior, quite understandably, leads to a considerable deterioration of the information system's security.

Dictionary attacks being an exceedingly powerful tool is a fact that has to be reckoned with. A study conducted in 1993 has already proven this point. The following is a reference to this study: (http://www.klein.com/dvk/publications/). The most disturbing revelation of this study is surely the table set out below (based on 8-character passwords):

Type of password	Number of characters	Number of passwords	Cracking time
English vocabulary 8 char. and +	Special	250000	< 1 second
Lowercase only	26	208827064576	9-hour graph

Lowercase + 1 uppercase	26/special	1670616516608	3 days
Upper- and lowercase	52	53459728531456	96 days
Letters + numbers	62	218340105584896	1 year
Printable characters	95	6634204312890620	30 years
Set of 7-bit ASCII characters	128	72057594037927900	350 years

Another tendency which has been curbed but which is still happening is worth mentioning: those now-famous post-its pasted under keyboards.

The administrator has to organize actions (training, creating user awareness, etc) in order to modify or correct these "habits".

EXAMPLE

- Encourage your users to choose passwords that exceed 7 characters,
- Remind them to use numbers and uppercase characters,
- Make them change their passwords on a regular basis,
- and last but not least, never to note down the password they have just chosen.

One classic method of choosing a good password is to choose a sentence that you know by heart (a verse of poetry, lyrics from a song) and to take the first letter of each word. This set of characters can then be used as a password.

EXAMPLE
"**S**tormshield **N**etwork, **L**eading **F**rench **m**anufacturer **o**f **F**IREWALL **a**nd **V**PN **a**ppliances…"
The password can then be the following: **SNLFmoFaVa**.

The ANSSI (French Network and Information Security Agency) offers a set of recommendations for this purpose to assist in defining sufficiently robust passwords.

Users are authenticated via the captive portal by default, through an SSL/TLS access that uses a certificate signed by two authorities not recognized by the browsers. It is therefore necessary to deploy these certification authorities used by a GPO on users' browsers. These authorities are by default the NETASQ CA and Stormshield CA, available from the following links:

- http://pki.stormshieldcs.eu/netasq/root.crt.
- http://pki.stormshieldcs.eu/products/root.crt.

For further detail, refer to the previous section **Administrator management**, under *Initial connection to the appliance.*

Work environment

The office is often a place where many people pass through every day, be they from the company or visitors, therefore users have to be aware of the fact that certain persons (suppliers, customers, workers, etc) can access their workspace and by doing so, obtain information about the company.

It is important that the user realizes that he should never disclose his password either by telephone or by e-mail (social engineering) and that he should type his password away from prying eyes.

User access management

To round up this section on creating user awareness of network security, the administrator has to tackle the management of user access. In fact, a Stormshield Network Firewall's authentication mechanism, like many other systems, is based on a login/password system and does not necessarily mean that when the application enabling this authentication is closed, the user is logged off. This concept may not always be apparent to the uninitiated user. As such, despite having shut down the application in question, the user (who is under the impression that he is no longer connected) remains authenticated. If he leaves his workstation for just a moment, an ill-intentioned person can then usurp his identity and access information contained in the application.

Remind users to lock their sessions before they leave their workstations unattended. This seemingly tedious task can be made easier with the use of authentication mechanisms which automate session locking (for example, a USB token).

GETTING STARTED WITH THE SNS FIREWALL

Logging in to the firewall web administration interface

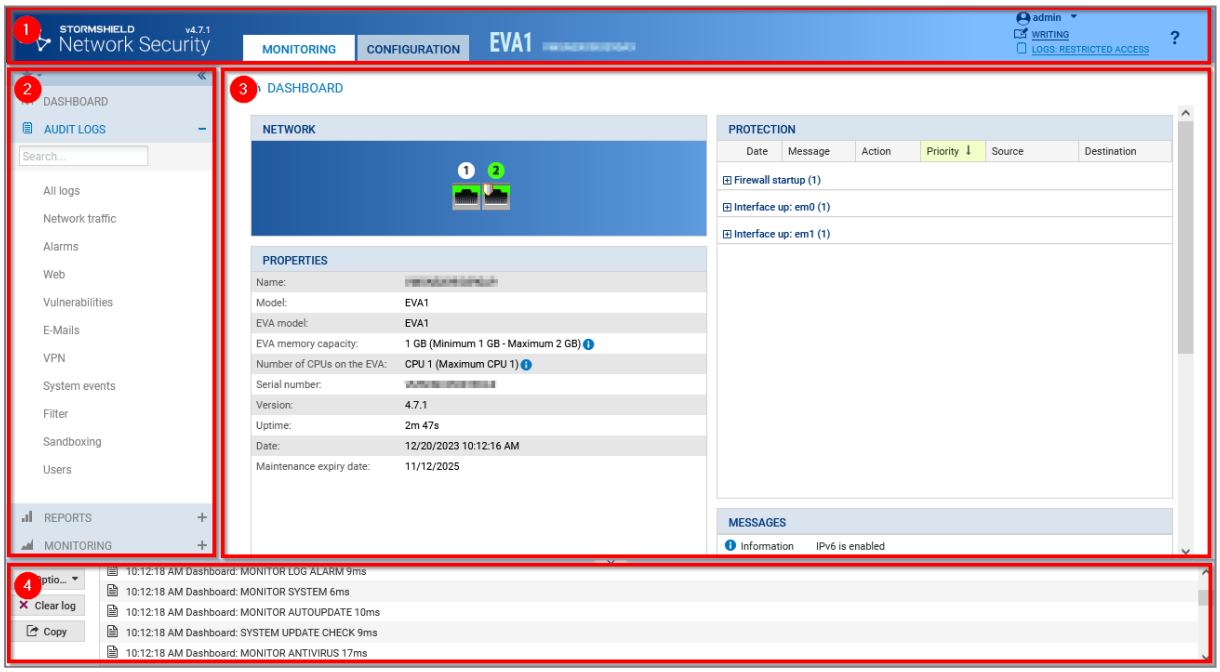
1. In a web browser, enter *https://* followed by the IP address (10.0.0.254 by default) of the firewall. Refer to the Product Life Cycle guide to see the list of supported web browsers.
2. Log in to the firewall web administration interface using your login and password, or the administration login and password.

By default, If you enter the wrong login or password four consecutive times, you will need to wait for a minute before you can authenticate again. If you attempt to authenticate again before the minute is up, the waiting time will be extended by another minute, up to a maximum of 10 minutes. The number of tries and waiting time can be configured. For more information, refer to the Firewall administration tab.

Understanding the graphical user interface

The window consists of 4 zones:

1. The upper banner, which presents the **Monitoring** and **Configuration** views and provides information on the status of the firewall;
2. The menu on the left, which provides access to the various modules on the firewall;
3. The active window of the selected module;
4. The lower window, which shows errors, warnings, commands and notifications.



Upper banner

In the upper banner, the following items are displayed from left to right:

- The version number of your firewall,
- Two tabs that show two firewall views: Monitoring and Configuration,
- The model number of your firewall and its name: scroll over the name to see the serial number,
- A flickering icon that shows whether the status of your firewall requires your attention: scroll over the icon to show monitored items and their status,
- Your user name: click on it to go to your preferences or to log in,
- Your read and write permissions: scroll over the permissions to see more information,
- Your permissions to access logs: if you are in restricted access mode, click on the item to request full access,
- The icon, which opens the page in the online *WELCOME* relating to the module you are viewing.

Left menu

The menu on the left provides access to various modules corresponding to available features. Modules are grouped by category. You can:

- Collapse the menu by clicking on ,
- Expand and collapse categories by clicking on them,
- Set modules as favorites by clicking on the icon that appears by scrolling over the name of a module,
- Quickly access favorite modules by clicking on the icon at the top of the menu.

If modules are grayed out in the menu, this may mean that:

- You have not subscribed to the required license and therefore cannot access them.
- The user account that you used for logging in does not have the necessary permissions to access these modules.

The modules in the menu vary depending on whether you are in **Monitoring** or **Configuration** view.

When you perform searches through the search bar, both the name of the module and its content will be part of the search.

Active window

The content of this window varies according to the module displayed. The other sections in the *WELCOME* describe the various modules and their content.

Lower window

The lower window shows errors, warnings, commands and notifications. You can:

- Show or hide this window by clicking on the arrow in the middle .
- Configure the messages that appear by clicking on **Options**.

ACCESS PRIVILEGES

This module consists of two tabs:

- **Default access**: allows you to define SSL VPN portal, IPsec VPN and SSL VPN access parameters as well as the default sponsorship policy.
- **Detailed access**: grid of rules corresponding to SSL VPN portal, IPsec VPN and SSL VPN access and to users authorized to validate sponsorship requests.

Default options tab

VPN access

IPsec policy	**IPsec VPN** makes it possible to set up secure tunnels (peer authentication, data encryption and/or integrity checking) between two hosts, between a host and a network, or between two networks. This field makes it possible to **Block** users from negotiating IPsec VPN tunnels by default or **Allow** them to do so. Depending on your selection, internal users and user groups will or will not be able to communicate over your private protected IP networks, thereby allowing their data to be transmitted securely.
SSL VPN policy	The SSL VPN makes it possible to set up secure tunnels (peer authentication, data encryption and/or verification of data integrity) between two hosts, between a host and a network, or between two networks. This field makes it possible to Block or Allow users by default from negotiating SSL VPN tunnels in the absence of specific rules. Depending on your selection, internal users and user groups will or will not be able to communicate over your private protected IP networks, thereby allowing their data to be transmitted securely.

Sponsorship method

Sponsorship allows an external user located within the organization to submit a request for limited-duration Internet access from a captive portal.

Sponsorship policy	Sponsorship allows an external user located within the organization to submit a request for limited-duration Internet access from a captive portal. This field makes it possible to Block or Allow users from responding to sponsorship requests submitted from the captive portal by default.

Detailed access tab

Possible operations

Some operations can also be performed by right-clicking in the grid.

Search	Enables searches by whole or partial keywords.
Add	Adds a new detailed access rule. The procedure is explained in the section Add.
Delete	Deletes the selected detailed access rule.
Move up	Places the selected rule above the rule before it in the list.
Move down	Places the selected rule below the following rule in the list.

Add

After clicking on **Add**, define the user or user group for which you want to create the detailed access rule.

User - Group found in the LDAP directory	Makes it possible to add the rule to a user or user group found in the firewall's LDAP directory. Select from the drop-down list the user or user group in question.
User - Group originating from another domain (directory)	Makes it possible to add the rule to a user or user group coming from another domain. For this option, enter the following information: • **User - Group**: choose whether the rule applies to a **User** or a **Group**. • **User - Group name**: type the name of the user or group in question. • **Domain name**: type the domain name in question.

Once the rule is added, it appears in the grid and the user or user group in question can be seen in the **User-user group** column. Added rules are disabled by default and all access is set to **Block** (even if it was configured differently in the **Default access** tab).

Detailed access grid

Status	Shows the configuration status of the detailed access rule for the user or user group. Double-click on it to change its status. **NOTE** The firewall will assess rules in their order of appearance on the screen: one by one from the top down. If Rule 1 applies to a user group, all users involved in the rules that follow and which are part of this same group will receive the configuration in Rule 1.
User-user group	Shows the user or user group affected by the rule.

IPsec	This field makes it possible to **Block** users from negotiating IPsec VPN tunnels or **Allow** them to do so. The **Default** option takes into account the default IPsec policy entered in the **Default access** tab. Depending on your selection, internal users and user groups will or will not be able to communicate over your private protected IP networks, thereby allowing their data to be transmitted securely. **NOTE** The IPsec privilege only applies to tunnels: • With pre-shared key authentication and e-mail address logins, or • With certificate authentication.
SSL VPN	This field makes it possible to **Block** users from negotiating SSL VPN tunnels or **Allow** them to do so. The **Default** option takes into account the default SSL VPN policies entered in the **Default access** tab. Depending on your selection, the internal users and user groups specified will or will not be able to communicate over your private protected IP networks, thereby allowing their data to be transmitted securely.
Sponsorship method	Depending on your selection, users or user groups will or will not be able to validate sponsorship requests submitted from the captive portal. The **Default** option takes into account the default sponsorship policy entered in the **Default access** tab.
Description	Comments describing the user, user group or the rule.

ACTIVE UPDATE

The **Active Update** module consists of a single screen with three separate sections:

- **Update**: for each module, makes it possible to select whether the update must be manual, automatic or disabled.
- **Manual update for security databases**: makes it possible to set manual updates for the configured modules. These modules are updated via an update file downloaded from the MyStormshield website.
- **Advanced properties**: makes it possible to configure the servers used for automatic updates.

Update

Status	Double-click to select the update type for a module. Three choices are possible: • Disabled, • Manual (using the update file downloaded from MyStormshield), • Automatic.
Module	Type of data updated (the list varies according to the license purchased).

Manual update for security databases

To update data configured for manual updates:

1. Download the update file (with *.ssp* extension) from MyStormshield (**Downloads** > **Stormshield Network Security** > **Offline Active Update Data**).
2. Select the file and click on **Update**.
   The file contains all data that can be updated via Active Update, but only data configured for manual updates will be included.

With the **Go to system monitoring** link, you can access the **Monitoring** > **Monitoring** > **System** module, to see the update status and the date on which the modules were last updated.

Advanced properties

Update servers of customized context-based protection signatures

When you use customized context-based protection signatures hosted on one or several internal server(s), enter the URL(s) to access this or these server(s) in order for these signatures to benefit from automatic updates.

Update servers

Stormshield Network update servers are entered by default, but you can customize these addresses to set up internal mirror sites. For further information, refer to the article in the Stormshield Knowledge base *How to create my own autoupdate server for my Stormshield UTMs*.

LOGS - AUDIT LOGS

This menu is not available on firewalls that are not equipped with storage media.

The **Logs - Audit logs** module allows you to read logs generated by appliances and stored locally. These logs are grouped by views, i.e., by alarm, connection, web log, etc. Advanced filters make it possible to analyze logs even deeper.

Private data

For the purpose of compliance with the European GDPR (General Data Protection Regulation), personal data (user name, source IP address, source name, source MAC address) is no longer displayed in logs and reports and have been replaced with the term "Anonymized".

To view such data, the administrator must then enable the "Logs: full access" privilege by clicking on "**Logs: limited access**" (upper banner of the web administration interface), then by entering an authorization code obtained from the administrator's supervisor (see the section **Administrators** > **Ticket management**). This code is valid for a limited period defined at the moment of its creation.

To release this privilege, the administrator must click on "**Logs: full access**" in the upper banner of the web administration interface, then click on "**Release**" in the dialog box that appears.

After a privilege is obtained or released, data must be refreshed.

Please note that every time a "Logs: full access" privilege is obtained or released, it will generate an entry in logs.

Collaborative security

For more collaborative security, in just one click within a view, the level of protection on a host can now be increased. An interactive feature will allow you to add hosts to a pre-set group and assign a strengthened protection profile or specific filter rules to them (quarantine zones, restricted access, etc.).

For further information, please refer to the Technical Note **Collaborative security**.

Storage device: SD / micro SD cards

For SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SNi10 and SNi20 models, you can benefit from full functionality by using an external storage medium such as:

- SD card for SN160(W), SN210(W), SN310 and SNi20 models,
- MicroSD card for SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320 and SNi10 models.

These external media must comply with the following specifications:

SD card	MicroSD card
Class 10 (C10) UHS Class 1 (U1) or **App Performance (A2).** The memory card must be in **SDHC** or **SDXC** standard. The memory card must be in a full-size physical SD format. Only adapters provided with the card must be used.	**Class 10 (C10) UHS Class 1 (U1)** or **App Performance (A2).**The memory card must be in **SDHC** or **SDXC** standard.
Stormshield recommends the use of high-endurance/industrial cards or preferably, those that have a built-in **MLC** flash chip developed by major brands (e.g., SanDisk, Western Digital, Innodisk, Transcend, etc.) and **with at least 32 GB**. The **maximum** memory size supported is **2 TB**.	

> **NOTE**
> Storing logs on an external medium can only be done on an SD card. This service is not compatible with other storage media such as a USB key or an external hard disk.

For more information, refer to the Guide **PRESENTATION AND INSTALLATION OF STORMSHIELD NETWORK PRODUCTS SN Range**, available on Stormshield's Technical Documentation website.

Actions

Toolbar no. 1: period

Time scale	This field allows choosing the period: Last hour, Today, past 7 days, past 30 days and customized duration. • The past hour is calculated up to the minute before the current one. • The Today view covers the current day, from midnight of the day before up to the minute before data is refreshed. • The Yesterday view covers the previous day. • The last 7 and 30 days refer to the period that has ended the day before at midnight. • The customized duration allows you to define a determined period, which covers the whole day except for the current day in which data runs up to the previous minute. The button is a shortcut allowing you to select a **customized duration**.
Refresh	This button allows you to refresh the display of data.

Toolbar no. 2: simple or advanced search

Change search modes using the "**Simple search**" / "**Advanced search**" button.

Simple search mode

In this default search mode, the appliance will search for the value entered in all the fields of the log files displayed.

This search only covers field values, and not field names. For example, to filter blocked connections, enter the value “block” in the search field, instead of “action=block”. For source or destination countries, use the country code (e.g.: fr, en, us, etc.).

(field for entering the search value)	To create the search, enter text in the field or drag and drop the value from a result field. The name of an object can also be dragged and dropped directly into this field from the **Network objects** module.

Advanced search mode

In advanced mode, several search criteria can be combined. All of these criteria have to be met in order to be displayed, as the search criteria are cumulative.

This combination of search criteria can then be saved as a “filter”. Filters will then be saved in memory and can be reset in the **Preferences** module of the administration interface.

(Filter drop-down menu)	Select a filter to launch the corresponding search. The list will suggest filters that have been saved previously and for certain Views, predefined filters. Selecting the entry (New filter) allows the filter to be reinitialized by deleting the selected criteria.
Save	Save as a customized filter the criteria defined in the Filter panel described in the next section. You can save a new filter using the button "Save as" based on an existing filter or a predefined filter offered in certain Views. Once a filter has been saved, it will be automatically offered in the list of filters.
Delete	Delete a customized filter saved earlier.

FILTER panel

You can add a search criterion either by clicking on **Add a criterion**, or by dragging a value from the results field and dropping it in the panel.

The filter creation window allows you to either **apply** or **add** the defined criterion. The **Add** button keeps the window open in order to define several criteria successively before launching the search.

Add a criterion	To add a search criterion, click on this button in order to open a window to edit a criterion, for which you need to enter the 3 following elements: • A **Field** in which the value will be searched. Selecting any will enable searches in all values contained in the logs. • In this list, the translated name of the field is displayed as well as the original name between brackets (token). The main fields are displayed in black and secondary fields in gray, corresponding to the display of the button **Expand all the elements / Collapse elements**. • A sort **Criterion** that will be associated with the value sought. These operators are: equal to, different from, contains, does not contain, starts with and ends with. • A **Value** to look for according to the criteria selected earlier. For source or destination countries, use the country code (e.g.: fr, en, us, etc.).

Once the criterion has been set up, it will be added to this **Filter** panel. The following actions can be done to this criterion:

- Delete using the icon . Deleting a criterion automatically refreshes the search of the modified filter, without this criterion.
- Edit in a window similar to the one during its creation, using the icon . The editing window only allows you to apply the search.

Toolbar no. 3: actions

Expand all the elements / Collapse elements	Displays all fields or only main fields.
Export data	The button allows downloading data in CSV format. The values are separated by commas and saved in a text file. This makes it possible to reopen the file in a spreadsheet program such as *Microsoft Excel.*
Print	The button enables access to the preview window in order to print logs. The *Print* button sends the file to the browser's print module, which allows you to choose whether to print the fie or generate a PDF file.
reset columns	Shows only the columns offered by default the first time the log or view is looked up, or cancels changes to column width.

Information

Above the table displaying the logs, the queried period will be shown, according to the value selected in the drop-down menu in the 1st toolbar. This period is displayed as:

SEARCH FROM - DD/MM/YYYY HH:MM:SS – TO - DD/MM/YYYY HH:MM:SS

Below the log table, the following information will be shown:

- Number of the page displayed,
- Number of logs displayed in the page,
- Period covered by the logs shown in the page,
- The UTM's date and time (information that will be useful if the administrator's workstation does not have the same settings).

Displaying details of a row of logs

Clicking on a row in a log automatically shows the details of the row in a window to the right of the table. Buttons now make it possible to hide (≫) or show (≪) this window.

In this window, click on **Previous** or **Next** to automatically display details of the previous or next row of logs.

The **Copy** button makes it possible to directly copy all fields/values from a row of logs to the clipboard.

Interactive features

Regardless of the display mode (line/grid), the values displayed in the log reading window offer two categories of interactions: ACTION and CONFIGURATION. Right-clicking opens a menu that offers the following actions:

Simple search mode

- **Add this value as a search criterion:** shortcut for creating a criterion that searches for the value in the corresponding field and in the whole view. This search type is the same as dragging and dropping the value.
- **Go to the corresponding security rule**: shortcut to open the Filter and NAT module and highlight the selected rule corresponding to the selected log line.
- **Copy the selected line to the clipboard**: shortcut to copy data from the selected row of logs to the clipboard. The same action is performed when you click on **Copy** under the window displaying details of the selected row.

Advanced search mode

- **Add a criterion for this field/value**: shortcut for creating a criterion that searches for the value in the corresponding field and in the whole view shown. To avoid the repetition of the value sought, the corresponding column will be automatically hidden in the grid view. This search type is the same as dragging and dropping the value.
- **Add a difference criterion to this value**: shortcut for creating a criterion that searches for any value that is different from the one selected in the corresponding field and in the whole view shown.
- **Go to the corresponding security rule**: shortcut to open the Filter and NAT module and highlight the selected rule corresponding to the selected log line.

IP addresses and host objects

- **Search for this value in the "All logs" view** : shortcut to open the "All logs" view filtered by the selected value.
- **Check this host**: shows the filter or NAT rules in which this host is used.
- **Show host details**: opens a window showing additional information about the selected host. The following information is given:
- Public IP address reputation,
- Geolocation,
- Host reputation,
- Classification of the URL (to which the host has connected),
- Vulnerabilities,
- Applications (Internet browsers, mail clients, etc.),
- Services,
- Information (detected operating system, etc.),
- Time taken to respond to the ping and network path (traceroute) to contact the host.
- **Reset this object's reputation score**: by clicking on this menu, the reputation score of the selected object will be reset to zero.
- **Blacklist this object**: makes it possible to place a host, IP address range or network in a blacklist (quarantine). The firewall will therefore reject such selected objects for a specific duration, which can be set in the sub-menu for this action:
- For 1 minute,
- For 5 minutes,

- For 30 minutes,
- For 3 hours.
  Once this duration has lapsed, the object in question will be allowed to go through the firewall again as long as it complies with the active security policy.
- **Show IoCs**: clicking on this menu will redirect you to the Stormshield Security website and show the security details of the selected object:
- IP address,
- Country of origin,
- FQDN
- Reputation category or associated web service if they have been set on the firewall.
- **Add the host to the object base and/or add it to a group:** this option makes it possible to create a host and/or add it to a group from a log file. As such, a host that has been identified as vulnerable can, for example, be added to a group with a strengthened protection profile. (cf. Technical Note **Collaborative security**).
  This option appears on fields that contain IP addresses (source, destination) or object names (source name, destination name). A window will appear, in which you can:
- Save the object in the database if it is an IP address,
- Select the appropriate object if the IP address corresponds to several objects,
- Add it to an existing group. This group may correspond to a quarantine of predefined vulnerable objects.

In addition to the interactions listed above, scrolling over a source IP address or the name of a source host will display a tooltip that shows the following information (if the administrator has obtained the "Full access to logs (private data)" privilege:

- Name of the host if it has been defined in the objects database,
- IP address of the host,
- Host's operating system,
- Number of vulnerabilities detected for the host.

URL

- **Search for this value in the "All logs" view** : shortcut to open the "All logs" view filtered by the selected value.
- **Show host details**: opens a window showing additional information about the selected host. The following information is given:
- Public IP address reputation,
- Geolocation,
- Host reputation,
- Classification of the URL (to which the host has connected),
- Vulnerabilities,
- Applications (Internet browsers, mail clients, etc.),
- Services,
- Information (detected operating system, etc.),
- Time taken to respond to the ping and network path (traceroute) to contact the host.

- **Reset this object's reputation score**: by clicking on this menu, the reputation score of the selected object will be reset to zero.
- **Blacklist this object**: makes it possible to place a host, IP address range or network in a blacklist (quarantine). The firewall will therefore reject connections to and from such selected objects for a specific duration, which can be set in the sub-menu for this action:
- For 1 minute,
- For 5 minutes,
- For 30 minutes,
- For 3 hours.
  Once this duration has lapsed, the object in question will be allowed to initiate or accept connections as long as it complies with the active security policy.
- **Show IoCs**: clicking on this menu will redirect you to the Stormshield Security website and show the security details of the selected object:
- IP address,
- Country of origin,
- FQDN
- Reputation category or associated web service if they have been set on the firewall.
- **Add the host to the Object base and/or add it to a group:** this option allows creating a host and/or adding it to a group from a log file. As such, a host that has been identified as vulnerable can, for example, be added to a group with a strengthened protection profile. (cf. Technical Note **Collaborative security)**.
  This option appears on fields that contain IP addresses (source, destination) or object names (source name, destination name). A window will appear, in which you can:
- Save the object in the database if it is an IP address,
- Select the appropriate object if the IP address corresponds to several objects,
- Add it to an existing group. This group may correspond to a quarantine of predefined vulnerable objects.
- **Add the URL to a group**: this option makes it possible to add a URL to a group from a log file. As such, URLs that have been identified as malicious or undesirable may, for example, be added to a customized group that will be subject to URL filtering.
  This option appears on fields that contain URLs (destination name). A window will appear, enabling:
- URLs to be added to an existing group. This group may correspond to a category of prohibited URLs, for example.

In addition to the interactions listed above, scrolling over a destination URL will display a tooltip that shows the following information (if the administrator has obtained the "Full access to logs (private data)" privilege:

- Domain name,
- Corresponding IP address.

Ports

- **Add the host to the object base and/or add it to a group:** this option makes it possible to create a host and/or add it to a group from a log file. As such, services that have been identified as vulnerable or undesirable may, for example, be added to a group of prohibited services in filter rules.
  This option appears on fields that contain port numbers or service names (source port, destination port, , name of the source port, name of the destination port, etc). A window will appear, enabling:
  - The object to be saved in the database if it is a port number,
  - Add it to an existing group. This group may correspond to a category of prohibited services.

In addition to the interactions listed above, scrolling over a port name will display a tooltip that shows the following information (if the administrator has obtained the "Full access to logs (private data)" privilege:

- Port object name,
- Port number or range of corresponding ports,
- Protocol,
- Comments defined in the port object.

Network packets

- **Export the packet**: this option makes it possible to export the captured packet in *pcap* format in order to analyze it using tools such as Wireshark. To start capturing packets, the checkbox **Capture the packet that raised the alarm** must be selected in the configuration of the alarm in question (**Application protection** > **Applications and protections** module > **Advanced** column > click on **Configure**).

Alarms view

- **Configure the alarm**: shortcut to open the **Applications and Protections - By inspection profile** module with the relevant alarm selected automatically.

System events view

- **Configure the system event**: shortcut to open the **System events** module with the relevant event selected automatically.

Logs

The list of logs (used in thematic views) and the name of the corresponding log file on the firewall are available in the "Description of Audit Log" Technical Note.

The available views are:

- All logs

This view displays all logs: **Administration, Alarms, Authentication, Network connections, Filter, FTP proxy, IPsec VPN, Application Connections, POP3 proxy, SMTP proxy, SSL proxy, System events, HTTP proxy** and **SSL VPN.**

> **NOTE**
> If the user does not have *admin* privileges, the **Administration** log will not be taken into account in this view.

- Network traffic

This view displays **Network connections, Filter, FTP proxy, Application connections, POP3 proxy, SMTP proxy, SSL proxy, HTTP proxy** and **SSL VPN** logs.

Two predefined filters searching for IPv4 traffic and IPv6 traffic are offered.

- Routing

This view displays the **Routing** log corresponding to unicast routing.

- Alarms

This view displays the **Alarms** log according to certain categories; this log only displays logs that do not belong to the filter alarm category.

- Web

This view displays **Network connections, Application connections,** and **HTTP proxy** logs according to certain categories:

- The Network connections logs only display logs whose standard service corresponding to the destination port is HTTP, HTTPS or HTTP_PROXY.
- The Application connections log only displays logs with an associated plugin name that is either HTTP or HTTPS.

A predefined filter that looks for detected viruses is offered.

- E-mails

This view displays **Network connections, Application connections, POP3 proxy** and **SMTP proxy** logs according to certain categories:

- The Network connections logs only display logs whose standard service corresponding to the destination port is SMTP, SMTPS, POP3, POP3S, IMAP or IMAPS.
- The Application connections log only displays logs with an associated plugin name that is either SMTP, SMTPS, POP3, POP3S, IMAP or IMAPS.

Two predefined filters that search for detected viruses (virus=infected) and detected spam (spamlevel entered and different from 0) are offered.

- VPN

This view displays **IPsec VPN, System events** and **SSL VPN** logs according to certain categories.

- System events

This view displays **Alarms** and **System events** logs according to certain categories; the Alarms log only displays logs belonging to the system alarm category.

Two predefined filters that search for Minor (pri = 4) or Major (pri = 1) levels are offered.

- Filtering

This view displays **Alarms** and **Filter** logs according to certain categories; the **Alarms** log displays only logs belonging to the *filter* alarm category.

- Sandboxing

This view displays the **Sandboxing** log.

- Users

This view displays the **Authentication** log.

- Dynamic multicast routing

This view displays the **Dynamic multicast routing** log.

ADMINISTRATORS

This module consists of three tabs:

- **Administrators**: creates administrators by granting administration privileges to users using one of the following authentication methods: LDAP RADIUS, KERBEROS or SSL.
- **Administrator account**: defines the authentication password of the administrator account by exporting the public or private key.
- **Ticket management**: administrators who manage access privileges to personal data can create temporary access tickets for full access to logs.

Administrators tab

This tab consists of a grid containing:

- A taskbar: it shows the various possible operations that can be applied to an administrator.
- The list of users and user groups identified as administrators and their privileges.

> **NOTE**
> The **Administrators** tab can only be accessed by the user connected with the *admin* account.

Possible operations

Some other operations can also be performed by right-clicking in the grid of administrators.

Adding an administrator	Adds a new administrator on the firewall. Several choices are offered depending on the privileges to assign to the new administrator. The procedure is explained in the section Adding an administrator.
Delete	Deletes the selected administrator.
Move up	Places the selected administrator above the previous administrator in the list.
Move down	Places the selected administrator below the following administrator in the list.
Copy privileges	Copies the privileges of the selected administrator.
Paste privileges	Pastes the copied privileges to the selected administrator.
Grant all privileges	Assigns all privileges to the selected administrator.
Switch to advanced/simple view	Changes how privileges are displayed in the grid according to two views: • **Simple view**: default display containing several columns which represent the categories of privileges that an administrator may or may not have. • **Advanced view**: shows all available privileges. Details of the privileges are provided in the section Possible privileges.

Adding an administrator

Several options are available when you click on **Add**:

Administrator without any privileges	This type of administrator has all the basic privileges such as access to the **Dashboard** and to the following modules: • **Licenses,** • **Maintenance,** • **Active Update,** • **High availability** (and its wizard), • **CLI** console, • **Network,** • **Routing,** • **Dynamic DNS,** • **DHCP,** • **DNS proxy cache**, • **Objects**, • **URL categories** (and their groups), • **Certificates and PKI,** • **Authentication** (and its wizard), • **URL filtering,** • **SSL filtering,** • **SMTP filtering,** • **Applications and protections,** • **Inspection profile,** • **Antivirus,** • **Antispam,** • **Block messages,** • **Preferences.** The module **Vulnerability management** can only be accessed with write privileges.
Administrator with read-only access	This type of administrator has the same basic access privileges as the administrator "without privileges" with the following additional privileges: reading of **SNMP** logs, **E-mail alerts, System events** as well as reading privileges for **Filtering** and **VPN**.
Administrator with all privileges	This type of administrator has access to all modules except those in which super-administrator access (*admin* account) is required. **NOTE** There can only be one super-administrator with the following characteristics: • The only administrator authorized to log in via the local console on Stormshield Network appliances, and only during the installation of the firewall or for maintenance operations outside of normal production use. • In charge of defining the profiles of other administrators, • Full access to the premises on which the firewall appliances are stored, and all operations are performed under this administrator's supervision,

Administrator for temporary accounts	This type of administrator can only manage temporary accounts defined on the firewall (creating, modifying and deleting).
Administrator with access to private data	This type of administrator can access all logs by clicking on **Restricted access to logs** in order to enable the **Full access to logs (private data)** privilege without having to enter an access code to view private data.
Administrator without access to private data	For the purpose of compliance with the European GDPR (General Data Protection Regulation), it is now possible to define an administrator with read and write privileges on the firewall but who cannot view private data stored in logs. Nonetheless, the administrator in question can still request and obtain access privileges to such data by entering an authorization code given by his supervisor. This code is valid for a limited period defined at the moment of its creation. To enable **Full access to logs (private data)**, the administrator must click on the link **Restricted access to logs**, then enter the code. Once the administrator's task is complete, this privilege can be released.

Next, define the user or user group to add as an administrator.

User - Group found in the LDAP directory	Makes it possible to add as an administrator a user or user group found in the firewall's LDAP directory. Select from the drop-down list the user or user group in question.
User - Group originating from another domain (directory)	Makes it possible to add as an administrator a user or user group coming from another domain. For this option, enter the following information: • **User - Group**: choose whether you wish to add a **User** or a **Group**. • **User - Group name**: type the name of the user or group in question. • **Domain name**: type the domain name in question.

Once added, the administrator will appear in the grid in the **User-user group** column.

Possible privileges

Privileges are displayed in the grid by two views:

- **Simple view**: default display containing several columns which represent the categories of privileges that an administrator may or may not have. Scroll over the title of a column to find out the exact privileges it holds.
- **Advanced view**: shows all available privileges.

Use the **Switch to advanced/simple view** button to change the display.

The icons in the table mean:

- ✔ : All privileges have been assigned.
- ✖ : All privileges have not been assigned.
- ✔/✖ : Some of the privileges have been assigned.

Double-clicking on the represented icons changes the status of privileges (from “assigned” to “not assigned” for example). Double-clicking on the icon ✔/✖ withdraws the assigned privileges.

> **NOTE**
> Any changes made to an administrator's permissions will only be applied the next time this administrator logs on. If you wish to apply a modification immediately, you will need to force the

disconnection of the administrator in question (for example using the CLI command: `monitor flush user`).

Privileges in simple view

Name	Description	Privileges assigned
System	Permission to perform maintenance operations (backups, restorations, updates, firewall shutdown and reboot, antivirus update, modification of antivirus update frequency and RAID-related operations) Permission to modify Object database	base, console, contentfilter, globalobject, maintenance, modify, object
Network	Permission to modify filter policy configuration and routing configuration (default route, static routes and trusted networks)	base, modify, network, route
Users	Permission to modify users and PKI	base, modify, pki, user
Firewall	Permission to modify VPN configuration, intrusion prevention (IPS) configuration and vulnerability management	modify, base, filter, vpn, asq, pvm, vpn, read, filter_read, globalfilter
Monitoring	Permission to modify logs and the configuration	modify, mon_write, base, log, log_read, report, report_read, privacy, privacy_read
Temporary accounts	Permission to manage temporary accounts for the "Temporary accounts" authentication policy	base, guest_admin

Privileges in advanced view

Name	Description	Privileges assigned
Logs (R)	Reading logs	base, log_read
Filter (R)	Filter policy consultation	base, filter_read
VPN (R)	VPN configuration consultation	base, vpn_read
Access to private data (L)	Permission to view logs containing private data	base, privacy_read
Logs (W)	Permission to modify log configuration	modify, base, log
Filter (W)	Permission to modify filter policy configuration	modify, base, filter

VPN (W)	Permission to modify VPN configuration	modify, base, vpn
Management of access to private data	Permission to create tickets for ad hoc requests for access to private data in logs.	base, privacy
PKI	Permission to modify PKI	base, modify, pki
Monitoring	Permission to view advanced Monitoring	base, modify, mon_write
Content filtering	Permission for URL filtering, Mail, SSL and antivirus management	base, modify, contentfilter
Objects	Permission to modify the object database	base, modify, object
Users	Permission to modify users	base, modify, user
Network	Permission to modify network configuration (interfaces, bridges, dialups, VLANs and dynamic DNS configuration)	base, modify, network
Routing	Permission to modify routing (default route, static routes and trusted networks)	base, modify, route
Maintenance	Permission to perform maintenance operations (backups, restorations, updates, firewall shutdown and reboot, antivirus update, modification of antivirus update frequency, high availability configuration and RAID-related operations).	base, modify, maintenance
Temporary accounts	Permission to manage temporary accounts (**Users > Temporary accounts** module)	base, guest_admin
Intrusion prevention	Permission to modify Intrusion prevention (IPS) configuration	base, modify, asq
Vulnerability management	Permission to modify vulnerability management configuration (Stormshield Network Vulnerability Manager)	base, modify, pvm
Objects (global)	Permission to access global objects	base, modify, globalobject
Filter (global)	Permission to access the global filter policy	base, modify, globalfilter
Activity Reports (W)	Permission to modify Stormshield Network Activity Reports	base, report_read
Activity Reports (R)	Permission to access Stormshield Network Activity Reports	base, report_read
Access to TPM	When the firewall is equipped with a TPM (Trusted Platform Module), this permission makes it possible to initialize the TPM and perform operations on data protected by the TPM (private keys in firewall certificates).	base, modify, tpm
Console (SSH)	Permission to open a remote SSH connection on the firewall.	base, modify, console

The *base* privilege is assigned to all users systematically. With this privilege, the administrator can read the whole configuration except filtering, VPN, logs and content filtering.

The *modify* privilege is assigned to users who have write privileges.

The user logged in as *admin* will obtain the *admin* privilege. This is the only privilege that lets the administrator add or remove administration privileges for other users.

Administrator account tab

In this screen, authentication data can be defined for the administrator account.

NOTES

- The default password of the "admin" user (super administrator) must be changed the very first time the product is used.
- To define an ASCII pre-shared key that is sufficiently secure, you must follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management.

Authentication

Old password	Enter the current password of the admin account so that you can change it.
New password	Enter the new password for the admin account. For the list of allowed and prohibited characters, refer to the section Allowed names.
Confirm password	Confirm the password of the admin account that you have just entered in the previous field
Password strength	This progress bar indicates your password's level of security: "Very Weak", "Weak", "Medium", "Good" or "Excellent". You are strongly advised to use uppercase letters and special characters.

NOTE
Stormshield Network uses asymmetric encryption, i.e., it uses a key pair consisting of a public key to encrypt data, and a private key for decryption. The advantage of using this system is that it removes the hassle of securing keys and allows electronic signatures.

Exports

Administrator's private key	This button saves the private key associated with the admin account on your workstation.
Firewall's public key	This button saves the public key associated with the firewall on your workstation.

Ticket management tab

In this table, administrators with permissions to manage access to personal data can create tickets for temporary access to such data.

The table

This table sets out all information relating to tickets for access to personal data. It contains the following columns:

Ticket ID	This is a randomly generated unique ID and corresponds to the first 4 characters of the code to access private data.
Valid from	Date and time from which ticket and its associated access code become valid.
Valid until	Date and time until which ticket and its associated access code remain valid.
Code for access to private data	Randomly generated code. After clicking on **Restricted access to logs** (upper banner of the web administration interface), the operator must enter this code in order to be able to view the personal data found in logs and reports.

Possible operations

Adding a ticket

To create a temporary ticket for access to personal data found in logs and reports, enter the dates and times to and from which this ticket should be valid.

Valid from	In the calendar, select the first day from which the code for access to private data becomes valid. The default value suggested is the current date. Next, select the time from which it becomes valid (granularity of 30 minutes).
Valid until	In the calendar, select the last day on which the code for access to private data stops being valid. The default value suggested is the current date. Next, select the time after which it stops being valid (granularity of 30 minutes).

Delete

This button allows you to delete a ticket:

1. Select the ticket to delete.
2. Click on **Remove**.

ANTISPAM

The antispam configuration screen consists of 3 tabs:

- **General**: Basic configuration of the Antispam module (activation, SMTP parameters, Reputation-based analysis, etc).
- **Whitelisted domains**: contains the list of domains that must be systematically considered legitimate.
- **Blacklisted domains**: contains the list of domains that must be systematically considered spam senders.

General tab

The antispam module can be enabled by determining the analyses to be enabled. Two options are available on the firewall:

Enable reputation-based analysis (DNS blacklists - RBL)	This option allows validating the sender by comparing against a public list of known spam senders (DNSBL).
Enable heuristic analysis	This option allows examining the contents of the e-mail to determine its impact.

SMTP parameters

The trusted server concerns the SMTP server. By filling in this field, which is optional, e-mails will be analyzed more thoroughly by the **Antispam** module.

SMTP server domain name (FQDN)	This optional field allows defining a "trusted" domain. Mail relayed by a server belonging to the domain indicated will therefore be exempt from the domain scan. This value may be defined for mail relayed by internal servers, for example. SMTP allows mail relay servers to fill in a field indicating their identity. If mail passes through a server belonging to the trusted domain, the earlier servers will be considered legitimate and the scan will only apply to the following servers.
Action	There are 4 possible actions that will allow the SMTP proxy to respond to the remote SMTP server by indicating that the message has been rejected as it is spam : • **Tag as spam (in message subject)**: e-mails will not be blocked but will be tagged as spam. • **Block all spam messages (level 1, 2 or 3)**: the e-mail will be rejected regardless of the level of trust. • **Block spam messages at level 2 or 3**: this option allows defining that beyond the trust threshold of Level 2, an e-mail will be rejected. The thresholds are: "1 – Low", "2 – Medium", "3 – High". • **Block only spam messages at level 3**: this option allows defining that beyond the trust threshold of Level 3 (High), the e-mail will be rejected.

For example, if you set a limit of 100 for the heuristic analysis, e-mails with a score higher than 100 will be considered spam. From 100 to 200, the level of trust will be low, from 200 to 300 it will be moderate and above 300, it will be high. If you have indicated a moderate level of trust for this option, all e-mails of moderate and high level (above 200) will be rejected whereas those from 100 to 200 will be kept.

> **NOTE**
> When several methods of analysis are used simultaneously, the highest score will be assigned.

Advanced properties

The **Antispam** module on the firewall does not delete messages that are identified as spam. However, it modifies messages detected as spam in such a way that the webmail client can process it in the future, for example. There are two ways of tagging messages:

Insert X-Spam headers	When this option is selected, the **Antispam** module will add a header summarizing the result of its analysis to messages identified as spam. The webmail client can then use this antispam header, in "spam assassin" format, to perform the necessary actions on the tagged message.

Reputation-based analysis

The DNS blacklist analysis or *RBL* (*Real-time Blackhole List*) enables identifying the message as spam through RBL servers. The following menus allow configuring the list of RBL servers which will be used for this analysis as well as the level of trust assigned to each of the servers.

List of DNS blacklist severs (RBL)

A table displays the list of RBL servers which the firewall queries to check that an e-mail is not spam. This list is updated by Active Update and cannot be modified, but certain servers can be disabled by clicking on the checkbox at the start of each line (in the **Enabled** column).

The levels indicated in the columns of the table refer to the levels of trust assigned to the server.

You can also configure the RBL servers to which you would like your Firewall to connect. To add a server, click on **Add**. A new line will appear. Up to 50 RBL servers can be defined.

Specify a name for this server (a unique name for the RBL server list), a DNS target (Field: **Domain name** only, which should be a valid domain name), a level of trust (Low, Medium and High) and comments (optional). Click on **Apply**.

To delete a configured server, select it in the list and click on **Delete**.

Some operations listed in the taskbar can be performed by right-clicking on the table of blacklisted servers.

> **NOTE**
> RBL servers in the firewall's native configuration are differentiated from customized servers by a padlock symbol (🔒), which indicates **RBL** servers in native configuration.

Heuristic analysis

The heuristic analysis is based on Vade Secure's antispam engine. Using a set of calculations, this antispam will derive a message's degree of legitimacy.

The antispam module will calculate and assign a score that defines a message's "unwantedness". E-mails that obtain a value exceeding or equal to the threshold set will be considered Advertisement or Spam.

The heuristic analysis will then suggest adding a prefix to the subject of these e-mails, making it possible, for example, to isolate them in a dedicated folder in the Mail Client.

Advertisement

In order to detect advertising e-mails, enable the option **Detect advertising e-mails**.

Add advertisement tag to mail subjects (prefix)	The subjects of e-mails that have been identified as advertisements will be preceded by a string of defined characters. This string is (ADS *) by default, where * represents the assigned level of trust. This score ranges from 1 to 3, a higher number meaning the higher the possibility of the e-mail being an advertisement. Regardless of the character string used, it is necessary to provide for the insertion of the level of trust in this string by using "*". This "*" will thereafter be replaced by the score. The maximum length of the prefix can be 128 characters. E-mails identified as advertisements will be transmitted without being deleted. Please note that double quote characters are not allowed.

Spam

Add spam tag to subject fields (prefix)	The subject of messages identified as spam will be preceded by a string of defined characters. This string is (ADS *) by default, where * represents the assigned level of trust. This score ranges from 1 to 3, a higher number meaning the higher the possibility of the e-mail being spam. Regardless of the character string used, it is necessary to provide for the insertion of the level of trust in this string by using "*". This "*" will thereafter be replaced by the score. The maximum length of the prefix can be 128 characters. E-mails identified as spam will be transmitted without being deleted. Please note that double quote characters are not allowed.
Minimum score for spam definition [1-150] :	The heuristic analysis performed by the **Antispam** module calculates a value that defines a message's "unwantedness". E-mails that obtain a value exceeding or equal to the threshold set will be considered spam. Firewall's default value is 100. This section enables the definition of a threshold to apply. By modifying the score, the minimum value of the 3 trust thresholds will be modified. Furthermore, the higher the calculated value, the higher will be the level of trust that the antispam module assigns to the analysis. Thresholds for the levels of trust cannot be configured in the web administration interface.

Whitelisted domains tab

This section enables the definition of domains from which analyzed messages will be systematically treated as **legitimate**.

Domain name (generic characters accepted: * and ?)	Specify the domain to be allowed. Up to 256 domains can be defined. Click on **Add**. The length of the domain name must not exceed 128 characters. The added domain will then appear in the list of whitelisted domains. To delete a domain or the whole list of domains, click on **Delete**.

Some operations listed in the taskbar can be performed by right-clicking on the table of whitelisted domains.

> **NOTE**
> Blacklisting and whitelisting prevail over DNS blacklist analyses and heuristic analyses. The domain name of the sender is compared against blacklisted and whitelisted domain in succession.

Blacklisted domains tab

This section enables the definition of domains from which analyzed messages will be systematically treated as spam.

Domain name (generic characters accepted: * and ?)	Specify the domain to be blocked. Up to 256 domains can be defined. Click on **Add**. The length of the domain name must not exceed 128 characters. The added domain will then appear in the list of blacklisted domains. Messages that are treated as spam because their domains are blacklisted will have the highest level of trust (3). To delete a domain or the whole list of domains, click on **Delete**.

Some operations listed in the taskbar can be performed by right-clicking on the table of blacklisted domains.

> **NOTE**
> Blacklisting and whitelisting prevail over DNS blacklist analyses and heuristic analyses. The domain name of the sender is compared against blacklisted and whitelisted domain in succession.

ANTIVIRUS

The configuration screen for the Antivirus service consists of two zones:

- Parameters,
- An area relating to sandboxing, available only for the advanced antivirus engine.

Settings

Settings

Inspect archives	This option enables the extraction engine and makes it possible to analyze archives (zip, arj, lha, rar, cab, etc.).
Block password-protected files	This option allows blocking password-protected files.

Sandboxing

This menu is only available (not grayed out) when the advanced antivirus engine has been selected. It also requires the prior subscription of the sandboxing (Breach fighter) option.

Do note that files can be manually submitted on https://breachfighter.stormshieldcs.eu/ for analysis.

After being sandboxed, the file will be assigned a score (maliciousness threshold) evaluated on a scale of 1 to 100. Files with a score of 0 are considered not dangerous. Files with a score of 100 are considered malicious.

Sandboxing threshold above which files will be blocked	From the drop-down list, select the level of maliciousness above which the firewall must block such files. Four levels are available: • Minor (score between 1 and 30) • Suspicious (score between 31 and 70) • Potentially malicious (score between 71 and 99) • Malicious (score of 100)

APPLICATIONS AND PROTECTIONS

In this module, you will be able to manage the configuration of alarms generated by the firewall's applications and protection modules.

> **NOTE**
> Do note that titles of alarms are shown in the language of the firewall (**Firewall language** field in the *General configuration* tab in the **System** > **Configuration** module) instead of the language used during the connection to the web administration interface.

An **inspection profile** (e.g., "IPS_00") is a set of **application profiles** ("tcpudp_00" + "icmp_00" + "modbus(00)" + etc.). An **application profile** contains the configuration of the alarms from a protocol analysis that can be modified in this (see the **Protocol** module). Its other configuration elements can be accessed in the corresponding "**Protocols**" menu.

To configure inspection profiles based on these application profiles, go to the module **Inspection profiles** and click on *Go to profiles*.

The signatures of these alarms are regularly updated via **Active Update** on products under maintenance (*IPS: contextual protection signatures*), and if this database is enabled in the Active Update configuration (module **Configuration/System/Active Update**).

Whether these alarms are raised therefore depends on the configuration of these protocol analyses as well as the security policy applied.

In this module, the alarm configuration is divided into two views:

- By inspection profile (also called " view by configuration")
  Passer en vue par profil d'inspection
- By context (also called "view by protocol")
  Passer en vue par contexte

New alarms

When a new alarm is implemented, an icon appears in the *New* column to attract your attention.

By clicking on *Approve new alarms*, you are confirming that you are aware of all new alarms, or only selected ones. The icons of the alarms in question will then disappear.
Do note that new alarms become operational as soon as they are implemented: the approval serves only to confirm that you have taken note of the new alarms.

This action can also be applied in the View by inspection profile and View by context.

View by inspection profile

Selecting the encryption profile

You can configure up to 10 profiles, with default names of "IPS_00", "IPS_01", etc.

Their names cannot be edited in the **Alarms** module, but in the **Application protection** > **Inspection profiles** menu (*Access profiles* button):

1. Click on **Rename**.
2. Select a profile from the drop-down list.
3. Enter the desired name in the **Profile name** field and add a comment if necessary.
4. Click on **Apply**.

You will see your modified profile in the drop-down list of configurations in the **Applications and Protections** module.

Selecting multiple objects

A multiple selection allows assigning the same action to several alarms. Select several successive alarms using the **Shift** ⇧ key or individually by holding down the **Ctrl** key. You can also remove an item from an existing selection with the **Ctrl** key.

Some column titles have the icon . When you click on it, a menu appears and suggests assigning a setting to several selected alarms (**Action**, **Level**, **New** and **Advanced** columns).

Example: Several lines can be deleted at the same time, by selecting them with the **Ctrl** key and pressing on **Delete**.

You can perform several actions in the profile:

Applying a model

Several templates make it possible to configure the profile of alarms by defining their action (*Allow* or *Block*) and their level (*Ignore, Minor* or *Major*).

The templates **Low, Medium** and **High** are distinguished essentially by the action of the *Protections* alarms, such as alarms relating to peer-to-peer networks or instant messaging. By default, *Applications* alarms allow traffic and *Malware* alarms block it.

The **Internet** template disables alarms that may hinder the typical use of the Internet, usually due to bad practices that are too common to be prohibited. An example of this is an alarm raised when there is a URL containing non-ASCII characters.

By default, the profile **(1) IPS_01** is based on the INTERNET template, since it is intended for traffic with a source address that is part of a protected network (see **Inspection profiles**). Other profiles are configured based on the MEDIUM template that ensures a standard level of security.

Internet	This configuration is adapted to outgoing traffic. Most alarms are configured with the action **Allow** when they do not pose a risk to the internal network.
Low	The least critical alarms are configured with the action **Allow**.
Medium	This template is a compromise between security and excessively strict blocking; it is applied by default to incoming traffic.
High	Most alarms are set to **Block**.

Selection

There are some buttons that allow you to sort the alarms of the inspection profile. These alarms fall under 3 categories: **Applications, Protections** and **Malware**. They can be selected by clicking on either of the 3 buttons with the same name. The button **All** resets the selection.

Applications	This type of alarm is raised when commonly used applications are used. Selecting this makes it possible to prepare an **application security policy**.

Protections	These alarms are raised by the IPS scan: they result from blocked known attacks and the abnormal use of protocols as defined in the **RFC**s.
Malware	These alarms are based on the known signatures of malicious programs, recognized by suspicious types of activity. The examination of hosts at the source of this alarm category is recommended.

Search

This field allows displaying only the alarm(s) containing the letter or word entered. Search results appear instantaneously, in order to filter profiles and contexts more easily, without the need to press [Enter].

Filter

This list contains several protocols and services covered by the alarms. You can sort them and display only the alarms that belong to the following categories:

None	All categories of alarms will be displayed.
BYOD	Traffic generated by mobile devices such as telephones or electronic tablets in bring your own device programs.
Cloud Storage	Applications that offer online data hosting.
E-mail address	Online messaging applications.
Game	Online gaming applications.
Communication	Instant messaging, VoIP or videoconference (Skype, Google talk etc.) applications.
Multimedia	Image, video or online music site.
Peer to peer	Direct file sharing between users.
Remote access	Remote PC control.
Social networks	Online community sites.
Web	Other HTTP/HTTPS-based applications.
Industrial protocols	Alarms relating to filtering and the detection of industrial protocols (PLC command and control, etc.)
DoT/DoH	Alarms relating to DNS over HTTPS (DoH) and DNS over TLS (DoT) requests.

This list may be modified by updating it via Active Update.

The various columns

To display the columns **Signatures, Model** and **Application profile,** click on the arrow that appears when the mouse is rolled over the title of a column and click on the corresponding checkboxes available in the *Columns* menu.

Patterns	Number of variants of the attack or the traffic blocked by the signature that raised the alarm.

Model	Model applied to the inspection profile that configures alarms by setting their action and level. Please refer to the previous chapter **Applying a model**.
Message	Text describing the alarm and its characteristics. When an alarm is selected, a **Help** button will appear. This link will open a help window describing the alarm and summarizing its action and level.
Application profile	Application profile containing the alarm configured in this inspection profile.
Action	When an alarm is raised, the configured action will be applied to the packet that set off the alarm. You can choose to **Allow** or **Block** traffic that causes this alarm.
Level	There are three levels of alarms: **"Ignore", "Minor"** and **"Major".**
New	Allows viewing new alarms, represented by the icon .
Context:id	Alarm name. The icon represents alarms deemed **sensitive**. Refer to the paragraph below for further information.
Advanced	**Send an e-mail**: an e-mail will be sent when this alarm is raised (cf. module **E-mail alerts**) with the following conditions: • **Number of alarms before sending**: minimum number of alarms required before an e-mail is sent, during the period defined hereafter. • **During the period of (seconds)**: period in seconds during which alarms have been raised, before an e-mail is sent. • **Place the machine under quarantine**: the packet that caused the alarm will be blocked with the following parameters. • **for a period of (minutes)**: duration of the quarantine • **Qos applied to traffic**: QoS queues can now be applied to any application traffic that generates alarms. This option therefore allows assigning a bandwidth restriction or lower priority to traffic that caused the alarm to be raised. • **Capture the packet that raised the alarm**: this capture can be viewed when checking alarms (Stormshield Network Realtime Manager or Unified Reporter), using a network sniffer such as *Wireshark*. • **Acknowledgment (ACK) queue**: QoS ACK queues can now be applied to any TCP ACK traffic. This option therefore allows assigning a bandwidth restriction or lower priority to traffic that caused the alarm to be raised. Next, click on **Apply**.

For each of the 10 profiles, you can configure them any way you wish by modifying the parameters described above.

Sensitive alarm

Applying the **Allow** action to an alarm stops protocol analysis on the traffic. As such, you are strongly advised to dedicate a filter rule in Firewall mode (or IDS for logs) to traffic that is affected by the alarm, instead of setting the rule to **Allow** for this type of alarm.

Example of an HTTP 47 sensitive alarm

Microsoft IIS (Internet Information Server) allows managing the application server by using Microsoft technologies. The management of web servers offers the encoding of extended characters using Microsoft's proprietary "%uXXXX" format. Since this encoding is not a standard, intrusion detection systems cannot detect attacks that use this method.

When a user attempts to access a site with a URL containing this type of encoded character and not corresponding to any valid character, the HTTP 47 alarm will be raised – *Invalid %u encoding char in URL*. As this alarm is considered sensitive, access to the site will be blocked.

The *Allow* action applied to an alarm that blocks traffic stops the protocol analysis of this connection (including requests that follow).

In order to maintain protection from this type of attack and simultaneously allow access to this type of server, it is recommended that you dedicate a filter rule in Firewall mode (or *IDS* for logs) to the affected traffic instead of allowing traffic blocked by a *sensitive* alarm to *Allow*. As a reminder, *Firewall* and *IDS* modes allow all types of traffic that raise alarms (with detection for *IDS* mode).

View by context

This view sets out alarms by protocol profiles. The first drop-down list, on the left, allows selecting the protocol context.

For each protocol, you can configure up to 10 configuration files, which can be selected from the second drop-down list (which displays "(00) *protocol*_00")

You can change the name of the file by going to **Application protection** > **Protocols**:

1. Select a configuration from the drop-down list.
2. Click on **Edit** and select **Edit**.
3. Change the name of the profile in the field and add a comment if necessary.
4. Click on **Update**.

You will see your modified profile in the drop-down list of configurations in the **Applications and Protections** module.

You can edit the policy within a profile according to 4 predefined **templates**: **Internet, Low, Medium** and **High**, described in the section "**View by inspection profile**".

AUTHENTICATION

The authentication feature allows the user to identify himself using a login and password or through a seamless process (SSO / certificate). To do so, the feature may use an LDAP (*Lightweight Directory Access Protocol*) database storing user profiles as well as the associated x509 certificate.

Once the authentication is successful, the user's login will be associated with the host from which he has logged on – this information will be stored in the ASQ's user table – and with all IP packets that originate from it for the duration that the user or administrator has specified depending on the method used.

In order to be effective, the methods configured (1st tab) have to be made explicit in the authentication policy rules (2nd tab).

The **Authentication** module contains 4 tabs:

- **Available methods**: this tab offers you the choice of one or several authentication methods and their configuration on the firewall to allow the firewall to apply the security policy. The administrator may also require authentication for the purpose of entering the identity of the host's user in the logs. In this section, you will be able to configure several methods as the authentication policy allows the use of several of these methods that will then be evaluated in order when authentication is processed.
- **Authentication policy**: this tab allows specifying the methods according to the source of the request and defining the order of the authentication methods to apply.
- **Captive portal**: Enables configuration of access to the captive portal from various interfaces, as well as the different information relating to it (SSL access, authentication, proxy). It also allows you to customize the display of the captive portal.
- **Captive portal profiles**: this tab makes it possible to manage several authentication profiles that the captive portal can use. For example, these profiles enable the selection of the type of account used (temporary accounts, users declared in the internal LDAP directory, etc) or allowed authentication durations.

> **NOTE**
> The captive portal has to be enabled for all authentication methods, except for SSO.

For issues relating to **Multi-user networks** and authentication by **transparent or explicit proxies**, please refer to the section Transparent or explicit HTTP proxy and multi-user objects.

Available methods tab

This screen offers the choice of one or several authentication methods and their configuration.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of available methods:

- Delete (the selected method).

Authentication methods

The left column is dedicated to the list of authentication methods. The right column displays the options for setting the selected authentication method.

The **Activate method** button opens a drop-down list that offers a choice of several authentication methods that you can **Disable** if necessary (except the LDAP and TS Agent methods). These methods are:

- LDAP,
- SSL certificate,
- Radius,
- Kerberos,
- Transparent authentication (SPNEGO),
- SSO agent,
- Guest methods
- Temporary accounts,
- Sponsorship method.
- One-time password (TOTP),
- TS agents,
- OIDC/Microsoft Entra ID.

When temporary account management is enabled on the firewall, the Temporary accounts method will automatically appear in the column of authentication methods.

LDAP

Go to the menu **Users** > **Directories configuration** to access the configuration. The configuration of this method is automatic and requires the implementation of an LDAP database.

SSL Certificate (SSL)

After having selected your authentication method from the left column, you may enter information about it in the right column, which sets out the following elements:

List of trusted certificate authorities (CA)

The SSL authentication method accepts the use of certificates that have been signed by a certification authority outside the firewall. This certification authority has to be added in the configuration of the firewall so that it accepts all certificates that have been signed by this authority.

If the certification authority itself is signed by another certification authority, it can then be added to the list of trusted CAs in order to create a “Trusted CA chain”.

If a trusted CA or trusted CA chain is specified in the configuration of SSL authentication, it will be added to the firewall’s internal CA, which is implicitly checked as soon as there is a valid internal root authority on the Firewall.

Add	Adding a certification authority to a list of trusted certification authorities allows the recognition of this authority and the validation of all certificates signed by this certification authority. By clicking on **Add**, then on the icon that appears on the selected line, you will access the CA window (Cf. *Certificates and PKI*). If the certification authority you wish to trust is not in the list of external certificates, click on **Select** in the external certificate window to add this certification authority to the list. Firewalls support **multi-level root authorities** – the certificate of the user to be authenticated is signed by a certification authority, which is itself signed by a higher authority. You can insert the whole certification chain created by this multi-level root authority. In order for the chain to be correctly applied, it is important that you insert every link in the whole chain of authorities between the highest authority you have inserted to the authority just above the user certificate.
Delete	Deletes the selected certification authority.

Certification authority (C.A): This field displays the certificates you wish to trust and which you will use.

It is possible to modify the subject field of the certificate that will be used for finding the user in the LDAP. The LDAP field used for the search can also be modified. By default, the e-mail address is used in both cases. These settings can be configured in CLI.

Advanced properties

You can enable searches in several LDAP directories.

Various criteria can therefore be defined: for a given directory, you can indicate a character string to look for in a specific field in the certificate. This string needs to be defined in the form of a regular expression.

Enable searching in several LDAP directories	Selecting this checkbox enables searches for users in several LDAP directories and provides access to the search criteria grid.

List of search criteria

Each criterion is defined by a certificate field, a regular expression and an LDAP directory.

You can **Add**, **Delete**, or move a criterion **Up** or **Down** the list using the relevant buttons. These criteria are assessed according to the order defined in the grid.

Certificate field	This drop-down list makes it possible to select the specific field in the certificate that will be queried with character strings.
Regular expression	Enter the regular expression that defines the character strings to look for in the certificate's field.
Directory or domain	Select the LDAP directory to query in order to authenticate users if the field defined in their certificates contains a string corresponding to the regular expression.

Radius

RADIUS is a standard authentication protocol running in client-server mode. It allows defining network access for remote users. This protocol is equipped with a server linked to an identification database (e.g. LDAP directory). The firewall can act as a RADIUS client and can therefore send to an external RADIUS server the authentication requests of users wishing to pass through the firewall. The user will only be authenticated on the Firewall if the RADIUS server accepts the authentication request sent by the Firewall.

All RADIUS transactions (communications between the Firewall and the RADIUS server) are themselves authenticated using a pre-shared secret, which is never transmitted over the network. This same secret will be used to encrypt the user password, which will pass through the Firewall and RADIUS server.

After having selected your authentication method from the left column, you can enter information about it in the right column.

Access to the server

When the RADIUS method is selected, enter the information relating to your external RADIUS server and a backup RADIUS server, if there is one.

Server	Select from the drop-down list the object representing the RADIUS server. If this object does not yet exist, you can create it by clicking on the relevant icon. Since RADIUS authentication supports IPv6, the selected object can therefore have an IPv6 address if the firewall is configured to use this protocol.
Port	Port used by the RADIUS server. By default, UDP port 1812 named *RADIUS* is selected. You can set another port by selecting it from the drop-down list or by creating a new object.
Pre-shared key	Key used for encrypting exchanges between the firewall and the RADIUS server.

Backup server

Server	Select from the drop-down list the object representing the backup server. If this object does not yet exist, you can create it by clicking on the relevant icon. Since RADIUS authentication supports IPv6, the selected object can therefore have an IPv6 address if the firewall is configured to use this protocol.
Port	Port used for the backup server. By default, UDP port 1812 named *RADIUS* is selected. You can set another port by selecting it from the drop-down list or by creating a new object.
Pre-shared key	Key used for encrypting exchanges between the firewall and the backup server.

NOTES

- The default timeout allowed to set up a connection to a RADIUS server is set to 3000 milliseconds, i.e., 3 seconds, and the number of tries is set to 1.
- The idle timeout and number of tries to connect to the main and backup RADIUS servers can be configured by using the CLI/Serverd command `CONFIG AUTH RADIUS`. These commands are explained in detail in the CLI SERVERD Commands Reference Guide.

Kerberos

Kerberos is different from other authentication methods. Instead of letting authentication take place between each client host and each server, Kerberos uses symmetrical encryption, the key distribution center (KDC, Key Distribution Center) to authenticate users on a network.

During the authentication process, the Stormshield Network firewall acts as a client which requests authentication on behalf of the user. This means that even if the user has already authenticated with the KDC to open his Windows session, for example, it is still necessary to re-authenticate with this server even if connection information is the same, in order to pass through the Firewall.

After having selected your authentication method from the left column, you may enter information about it in the right column, which sets out the following elements:

Domain name (FQDN)	Domain name assigned to the Active Directory server for the Kerberos authentication method. Defining this domain name allows masking the server's IP address and simplifying the search for it. **Example**: www.company.com: **company.com** represents the domain name, which is more legible than its corresponding IP address: 91.212.116.100.

Access to the server

Server	IP address of the server for the Kerberos authentication method (*Active Directory* for example)
Port	Port used by the server. By default, the port 88 / UDP named Kerberos_udp is selected.

Backup server

Server	Backup IP address of the Active Directory server for the Kerberos authentication method
Port	Port used by the backup server if the main server is no longer available. By default, the port 88 / UDP named Kerberos_udp is selected.

Transparent authentication (SPNEGO)

The SPNEGO method enables Single Sign On to function in web authentication with an external Kerberos authentication server. This means that a user who connects to his domain via a Kerberos-based solution would be automatically authenticated on a Stormshield Network firewall when he accesses the internet (requiring authentication in the filter policy on the Firewall) with a web browser (Microsoft Edge, Firefox, Mozilla).

In order to implement this method, you must first execute the KEYTAB generation script **spnego.bat** on the domain controller. This script is available in the MyStormshield personal area (authentication required), under **Downloads** > **Downloads** > **Stormshield Network Security** > **TOOLS**.

> **REMARK**
> The parameters requested when the script is executed are case-sensitive and must be strictly followed as they cannot be modified later. In the event of an error, a backup of the domain controller has to be restored in order to continue with the installation.

For firewalls that have not been configured in high availability, it is advisable to indicate the serial number of the firewall instead of its name to identify it (this name corresponds to the name indicated in the Stormshield Network script that comes with the installation hardware). The *Service name* will be the serial number preceded by "HTTP/". **Example:** HTTP/VMSNSXXAZ0000000

For firewalls in high availability, since the identifier has to be the same for both appliances, you are advised to use the name of the authentication portal's certificate (CN) entered in the *Captive portal* tab in the **Authentication** module.

SPNEGO can be configured on the firewall with the options explained in the table below:

Service name	This field represents the name of the Kerberos service used by the firewall, obtained after the *spnego.bat* script has been executed.
Domain name	Kerberos server's domain name. This domain name corresponds to the full name of the Active Directory domain. It has to be entered in uppercase.
KEYTAB	This field represents the shared secret, generated when the script is used on Active Directory. This secret has to be provided to the firewall so that it can communicate with Active Directory. It is also provided by the *spnego.bat* script

SSO Agent

With *Single Sign-On* (SSO), users need to authenticate only once to access several services.

The *SSO agent* method requires the installation of the **Stormshield Network SSO Agent** application, a Windows service that allows Stormshield Network firewalls to benefit from transparent authentication on Windows Active Directory. Refer to the technical note **Stormshield Network SSO Agent - Installation and deployment** for instructions on how to install this application.

When users log in to the Windows domain by opening their sessions, they will automatically be authenticated on the firewall. The SSO agent gathers information on the user's identity on the domain by connecting remotely to the event viewer on the domain controller. The SSO agent then relays this information to the firewall through an SSL connection, which updates its table of authenticated users.

From version 3 of the firmware onwards, up to 5 SSO agents can be declared, thereby making it possible to manage authentication on 5 Windows Active Directory domains without approval relationships. These domains must be declared beforehand as external Microsoft Active Directory types of LDAP directories (**Users** > **Directory configuration** module). Additional SSO agents will be named SSO Agent 1, SSO Agent 2, etc.

After having added this method, you can enter the information relating to its configuration.

SSO Agent

Domain name	Select the Microsoft Active Directory corresponding to the domain on which users will be authenticated. This directory must be configured beforehand through the **Directory configuration** module.

SSO Agent	
IP address	IP address of the server for the machine hosting **Stormshield Network SSO Agent**.

Port	By default, the port "agent_ad" is selected, corresponding to port 1301. The protocol used is TCP.
Pre-shared key.	This key is used for SSL encryption in exchanges between the SSO agent (machine hosting **Stormshield Network SSO Agent**) and the firewall. Enter the **pre-shared key** (password) defined during the installation of the SSO agent.
Confirm pre-shared key	Confirm the pre-shared key/password that was typed in the previous field.
Password strength	This field indicates your password's level of security: "Very Weak", "Weak", "Medium", "Good" or "Excellent". The use of uppercase and special characters is strongly advised.

SSO backup agent

The fields for configuring the backup SSO agent are the same as those for the main agent.

Domain controller

You will need to add all the domain controllers that control the selected Active Directory domain. They must be saved in the firewall's object database.

Add a domain controller	Click to select or create the corresponding object. You will need to add all the domain controllers that control the Active Directory domain. They must be saved beforehand in the firewall's object database.

Advanced properties

Select the installation mode used for SSO agent:

- **Windows Active Directory** mode (agent installed on a workstation or on a Windows server),
- **Syslog server** mode (agent installed on a Linux Ubuntu machine).

Common fields to Windows Active Directory mode and Syslog server mode

-

Maximum authentication duration	Define the maximum duration for the session of an authenticated user. After this period, the firewall will delete the user from its table of authenticated users, thereby logging out the user. This duration is to be defined in seconds or minutes. It is set by default to 36000 seconds, or 10 hours.
Refresh user group updates	If the Active Directory has been configured on the firewall (**Directory configuration** module), the firewall will check for possible changes made to **LDAP directory groups**. The firewall will then update its directory configuration then send this information to the SSO agent. This duration defined in seconds, minutes or hours, is set by default to 3600 seconds, or 1 hour.

Disconnection detection	With this option, authenticated users can be deleted when an associated host logs off or when a session is shut down. This test to detect which hosts are connected to the firewall is carried out either by pinging or by the registry database method. If this method is not enabled, the user will only be disconnected after the defined authentication period, even if his session is shut down.
Detection method	Select a log off method from **PING** or **Registry database**: ○ **PING** : the SSO agent tests the accessibility of all hosts authenticated on the firewall every 60 seconds by default. If it gets a *host unreachable* response or no response is received from an IP address after the defined period, the SSO agent will send a logout request to the firewall. The firewall will then will delete the user associated with this IP address from its table of authenticated users, logging the user out of the firewall. ○ **Registry** : the **Registry database (BDR)** is a database used by the Windows operating system to store information about the system's configuration and installed software. This method makes it possible to detect a closed session on a host that is still running. If there is a positive response to the ping, the SSO agent will log in remotely to the host and check in the Registry database the list of users with a session open on the host. This makes it possible to update the firewall's table of authenticated users.
Consider offline after	If a host does not respond to the ping after this period, it will be considered disconnected. The firewall will then delete the user associated with this host from its table of authenticated users. This duration defined in seconds, minutes or hours, is set by default to 5 minutes.
Disconnection detection	With this option, authenticated users can be deleted when an associated host logs off or when a session is shut down. This test to detect which hosts are connected to the firewall is carried out either by pinging or by the registry database method. If this method is not enabled, the user will only be disconnected after the defined authentication period, even if his session is shut down.

Enable DNS host lookup	With this option, you can manage changes to the IP addresses of user workstations and authenticate users who have logged in to hosts that have several IP addresses.

Ignored administration accounts	In the firewall's factory configuration, there is a list of users whose authentication is ignored. These accounts list the usual logins dedicated to the administrator (Administrator and Administrateur by default). This mechanism was set up because the domain controller treats the execution of a service or an application (Run as administrator feature, for example) as an authentication. As SN SSO Agent restricts authentication by IP address, this type of authentication may potentially replace the authentication of the user with an open Windows session. The pre-set list of "Ignored Administrator accounts" allows SN SSO Agent to ignore their authentication. Edit it if necessary.

Additional fields for Syslog server mode

Syslog server configuration

Listening IP address	Enter the IP address of the syslog server.
Listening port	Enter the listening port of the syslog server. The **syslog** network object is suggested by default.
IP address search (reg. expr.)	Enter the regular expression that will be used to search for IP addresses in logs hosted on the syslog server. Example: ([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s\\|
User search (reg. expr.)	Enter the regular expression that will be used to search for user names in logs hosted on the syslog server. Example: JOHN\\([a-zA-Z0-9\.]*)\s will detect entries such as JOHN\john.doe
Message search (reg. expr.)	Enter the regular expression that will be used to search for connection messages in logs hosted on the syslog server. Example: connect|ok will detect entries such as JOHN|connect|ok|sysvol

Backup syslog server configuration

You can specify a backup syslog server

Listening IP address	Enter the IP address of the backup syslog server.

Guest method

This mode allows identification without authentication, for access to a public Wi-Fi network, for example. This method automatically activates the display of the conditions of use for internet access. These conditions can be customized in the *Captive portal* tab. By default, the frequency of this display confirming the authentication is 18 hours and can be modified in the settings for this method (disclaimertime).

When these "guest" users log on, these events will be logged with the addition of source MAC addresses. This identification is checked every 4 hours, and this parameter can be set in the following CLI command:

CONFIG AUTH GUEST (example: state=1 logontime=14400disclaimertime=64800)

> **NOTE**
> In the security policy, the User object to select to match the Guest method is "All".

Display frequency of the Conditions of use for internet access	With this method, the Conditions of use for internet access – commonly known as Disclaimer – are systematically shown to the user. A checkbox to indicate the user's agreement has to be checked before the user can authenticate. These conditions can be customized in the "Captive portal" tab. If the feature has also been enabled in the profiles of the captive portal, this display frequency will be different from the one configured for the other methods.

Temporary accounts

This service enables the management of accounts with a limited validity duration. These accounts are meant to provide temporary public Internet access to persons outside the

organization. Temporary accounts are not saved in the LDAP directory(ies) declared on the firewall.

Default validity duration of a new user account (days)	This field allows setting a validity duration (in days) that will be suggested by default when a new temporary account is created.

The **Go to the list of temporary accounts** link will redirect you to the module **Users** > **Temporary accounts** to allow you to manage (add, modify, delete) these accounts.

Sponsorship method

This mode enables identification without authentication through the captive portal. The sponsored party will need to enter his/her first name and last name and his/her sponsor's email address. The sponsor will then receive an email containing a link to confirm this request. After the request has been validated, the sponsored party will automatically be redirected from the captive portal to the requested web page.

Minimum authentication duration	Define the minimum duration of a session for a sponsored user. This duration is to be defined in minutes, hours or days. It is set by default to 15 minutes.
Maximum authentication duration	Define the maximum duration of a session for a sponsored user. After this duration has lapsed, the firewall will log out the user. This duration is to be defined in minutes, hours or days. It is set by default to 240 minutes, or 4 hours.

This authentication method requires an SMTP server to be configured on the firewall. Click on the link **SMTP server configuration** to access the E-MAIL ALERTS module in which the server can be configured.

TOTP (SNS 2FA)

The 2FA authentication method, which uses time-based one-time passwords (TOTP), increases the security of authentications that the firewall manages.
This additional step to protect access is built into the firewall and does not require any third-party TOTP solution. Users who authenticate with an SNS TOTP only need to use an application on their smartphones or in their browsers to generate TOTPs.

The advantage of this method is that it can be enabled for all types of authentication: captive portal, SSL VPN tunnel, web administration interface, console or SSH connections and IPsec/Xauth VPN tunnels.

NOTE
Since this 2FA method is built into each firewall, users must use as many TOTPs as the number of firewalls to which they must connect.

NOTE
Stormshield strongly recommends that you enable NTP time synchronization for the firewall by selecting **Synchronize firewall time (NTP)**, and by specifying the NTP servers (System module > Configuration > General configuration tab).

Time-based one-time password (TOTP)

Select the authentication methods that the firewall manages and which will use TOTP.
The possible types of authentication are:

- Captive portal,
- SSL VPN tunnels,
- Web administration interface,
- SSH/Console,
- IPsec (Xauth/EAP).

TOTP code settings

This information will be presented on the firewall's captive portal during the user's TOTP enrollment.

Issuer	Specify the issuer of the TOTP (e.g., the name of your company). The default value is Stormshield Network Security.

Customize the TOTP user enrollment message

Message to display (max. 1024 characters)	You can set the message (optional) that will be shown on the firewall's captive portal during the user's TOTP enrollment. Enter this message in the text field within the limit of 1024 characters.

Advanced configuration

> **WARNING**
> If you are using Google Authenticator or Microsoft Authenticator, changing these settings will prevent TOTP authentication from functioning.

Lifetime (s)	Specify the validity period of a TOTP. The user's application will automatically generate a new TOTP when this period expires. The default value is 30 seconds.
Code size	Indicate the length (number of characters) of generated TOTPs. The default value suggested is 6.
Number of valid codes before and after current code	When the time on the firewall and the device that hosts the TOTP code generator (e.g., smart phone or computer) is slightly desynchronized, or to give the user a reasonable time frame to enter the code, this option allows you to specify how many codes generated before or after the currently valid code will be considered valid and accepted for authentication.
Hash algorithm	Select the hash algorithm used when generating TOTPs. The possible values are: • SHA1, • SHA256, • SHA512. The default value is SHA1.

The two buttons found in this section allow you to perform operations on the database of users who have completed TOTP enrollment.	
Reset the TOTP database	Clicking on this button will reset the entire database of users who have completed their TOTP enrollment. Users will then need to start the whole process of TOTP enrollment all over again the next time they authenticate. If you wish to reset the entire TOTP database: 1. Click on **Reset TOTP database**. A warning window will appear. 2. Confirm by clicking on **Continue**. **NOTE** The user must be connected with the *admin* account to reset the TOTP database.
Show TOTP orphans	Orphan users are those found in the TOTP database but cannot be found in the LDAP directories configured on the firewall, and who last used a TOTP at least 3 months ago. This button makes it possible to show orphan users and delete them from the TOTP database (deletes all **TOTP** orphans). If you wish to show the orphan users found in the TOTP database: 1. Click on **Show TOTP orphans**. A selection window appears. 2. In the calendar, select the date on which the orphan users you wish to show last used a TOTP. The default date is 3 months before the current date. The relevant users will be shown. To delete **all** the orphan users listed in this grid: 1. Click on **Delete**. 2. Confirm deleting **all** orphan users by clicking on **OK**. To quit the grid without deleting orphan users, click on **Cancel**.

TS agents

This transparent multi-user authentication method is intended for virtual desktop infrastructures (VDI).
This method relies on exchanges between the SNS firewall and one or several SN TS agents deployed directly on VDI servers (Citrix Virtual Apps and Desktops servers or Microsoft Remote Desktop Services).

Each SNS firewall can manage up to 100 SNS TS agents.

For more information, please refer to the **Technical Note** SN TS Agent - Installation and deployment.

TS agents

Timeout before disconnected users and de-authenticated (sec.)	If users have been accidentally disconnected or have suddenly quit a remote session, this is the length of time after which they will be deleted from the table of authenticated users in the intrusion prevention engine. The default value is 30 seconds. It can be raised to a maximum of 300 seconds (5 minutes).

TS agent list

You can **Add** or **Delete** TA agents by clicking on the respective buttons.

Adding a TS agent

1. Click on **Add**.
   A window containing the various parameters to indicate will appear.
2. Using the cursor, enable (**ON**) or disable (**OFF**) the TS agent being created.

> **NOTE**
> We recommend that you create TS agents by leaving them inactive to avoid generating unnecessary alarms and logs. They will be enabled when the TS agents are deployed on RDS and Citrix servers.

3. Enter the **TS Agent Name**.
4. Select or create the object corresponding to the **TS server** (RDS/Citrix server) on which the TS agent will be installed.
5. Select the communication **Port** between the firewall and the TS agent.
   The object *agent_ts* (TCP/1303) is suggested by default.
6. Set and confirm the **Pre-shared key** used during the communication with the TS agent.
7. Confirm the configuration by clicking on **Apply**.

Removing a TS agent

1. Select a row in the grid that contains the TS agents.
2. Click on **Remove**.
3. Confirm by clicking on **OK**.

Changing the status of a TS agent

To change the status (*on/off*) of a TS agent, double-click in the agent's **Status** column.

Modifying a TS agent

To change one or several parameters of a TS agent, double-click in any column other than the agent's **Status** column.

TS agent grid

Status	Indicates whether communication with the TS agent is enabled (*on*) or disabled (*off*).
Name	TS agent name.
Address	Object corresponding to the server on which the TS agent is installed. The IP address of the server appears when you scroll over this object.

Pre-shared key	The pre-shared key used during the communication with the TS agent is shown when you scroll over this field.
Connection port	Displays the object corresponding to the communication **Port** used between the firewall and the TS agent.

Advanced properties

Ignored administration accounts	For each TS agent configured, administration accounts can be excluded from the TS Agent authentication mechanism. In this case, even when traffic initiated by the selected administrator accounts matches filter rules that allow the TS Agent method, the firewall will block such traffic.

To add an administration account to ignore:

1. Expand the **Advanced properties** section,
2. In the **Ignored administration accounts** grid, click on **Add**,
3. Select a TS Agent configured earlier,
4. Enter the name of the administration account to ignore.

OIDC/Microsoft Entra ID

By using the Microsoft Entra ID authentication/authorization method, based on the OpenID Connect protocol, you can:

- Manage your accounts from a central location: the Microsoft Entra ID directory, known as a *tenant*.
- Monitor in Microsoft Entra who can access the SNS firewall web administration interface,
- Monitor which users/groups are allowed to authenticate over the SNS firewall's captive portal using their Microsoft Entra ID accounts,
- Monitor which users are allowed to connect to the SSL VPN with their Microsoft Entra ID accounts.

This module allows you to:

- Configure your firewall through a wizard, to use the Microsoft Entra ID method, based on your Microsoft Entra ID tenant settings.
- Show/edit the configuration of the Microsoft Entra ID method once it is available on the firewall.

Configuring your firewall to use the Microsoft Entra ID method

The procedure for configuring the Microsoft Entra ID method is detailed in the technical note **Configuring and using OIDC/Microsoft Entra ID authentication**.

Showing/editing the configuration of the Microsoft Entra ID method on your firewall

Open ID Connect/Microsoft Entra ID

Domain name	This is the main domain name as shown in the configuration center of your Microsoft Entra ID tenant (e.g., snsdoc.onmicrosoft.com).

Information about the SNS application on your Microsoft Entra ID tenant:

MS Entra ID service URL	This URL is generated automatically and takes the following form: https://login.microsoftonline.com/<**tenant ID**>/v2.0. The <**tenant ID**> value can be looked up in the configuration center overview of your Microsoft Entra ID tenant (Identity).
Application ID (client).	This value can be viewed in the properties of your SNS application, in the configuration center of your Microsoft Entra ID tenant.
Client secret	This secret was defined when creating your SNS application, in the configuration center of your Microsoft Entra ID tenant.

To find out how to retrieve these values from your Microsoft Entra ID tenant's configuration center, see the technical note **Configuring and using OIDC/Microsoft Entra ID authentication**.

Service URL

This box shows the redirection URLs that you need to enter in your Microsoft Entra ID tenant configuration.

Captive portal	URL generated from the parameters regarding redirection to the captive portal (Configuration > General configuration tab > Advanced configuration section).
SSL VPN	URL generated from the public IP address or FQDN entered in the firewall's SSL VPN configuration (VPN > SSL VPN).
Web administration interface	URL generated from the name of the firewall (Configuration > General configuration tab > General configuration section).

You can also change the duration after which an Entra ID session has to be re-authenticated: this **Maximum duration** of a Microsoft Entra ID session is expressed in days and hours (default value proposed when configuring Microsoft Entra ID on the firewall: 1 day)

Authentication policy tab

The filter table allows you to define the rules of the authentication policy to be applied through the firewall. High-priority rules are placed on top. The firewall executes rules in their order of appearance in the list (rule no. 1, 2 and so on) and stops as soon as it reaches a rule that matches the traffic that it processes. It is therefore important to define rules **from most specific to most general**.

If no rules have been defined in the policy or if the traffic does not match any of the specified rules, the *Default method* will be applied. If this method has not been configured or the action has been set to *Block*, all authentication attempts will be denied.

Actions on the rules of the authentication policy

Search by user...	This field allows searching by user login. The rules assigned to this user appear in the table. **Example**: If you enter “user1” in the field, all rules in the policy with “user1” as their source will appear in the table.

New rule	Inserts a rule – predefined or to be defined – after the selected line. There are 5 possible choices: • **Standard rule**: an authentication wizard will appear when this option is selected. Please refer to the following section to see the options offered in each screen. • **Guest method rule**: this wizard offers to create an authentication rule through the *Guest* method. This method cannot be combined with other methods within the same rule as it does not require authentication. **NOTE** Select "All" as the User object to match the *Guest* method. **NOTE** This method is incompatible with multi-user objects; all users connected in *Guest* mode must have different IP addresses. • **Temporary account rule**: this wizard offers to create an authentication rule through the *Temporary account* method. This method cannot be combined with other methods within the same rule. • **Sponsorship rule**: this wizard offers to create an authentication rule through the *Sponsorship* method. This method cannot be combined with other methods within the same rule as it does not require authentication. • **Separator – rule grouping**: This option allows inserting a separator above the selected line and helps to improve the authentication policy's readability and visibility. It may allow the administrator to prioritize rules, for example, or group those that redirect traffic to different servers. You can collapse or expand the node of the separator in order to show or hide the rule grouping. You can also copy/paste a separator from one location to another.
Delete	Deletes the selected line.
Move up	Places the selected rule before the rule just above it.
Move down	Places the selected rule after the rule just below it.
Cut	Allows you to cut an authentication rule in order to move it.
Copy	Allows you to copy an authentication rule in order to duplicate it.
Paste	Allows you to duplicate an authentication rule after having copied it.

Right-click menu

Some operations listed in the taskbar can be performed by right-clicking on the table of authentication rules:

- New rule (Standard rule, Guest rule, Temporary accounts rule, Sponsorship rule, Separator - rule grouping),
- Delete,
- Cut,
- Copy,
- Paste.

New rule

The authentication policy allows creating rules based on a user or a group of users. It is also possible to target certain traffic by specifying its source. Click on the "**New rule**" button and select "**Standard rule**", "**Guest rule**", "**Temporary account rule**" or "**Sponsorship rule**" to launch the wizard.

Step 1: Action

Action to apply for this rule: select the action to apply when an authentication request matches this rule.

You may choose:

- Allow,
- Block,
- Default (action chosen in the **Default action to apply** section under the authentication policy grid).

Step 2: User authentication

Select the user, user group or leave the default value as "Any user@*default_domain*" where *default_domain* represents the default directory / domain defined on the firewall.
This step is not offered for rules associated with the "**Guest**" or "**Sponsorship**" methods.

Step 3: Source

Click on **Add an interface** or **Add an object** in order to target the source of the traffic affected by the rule. This may be the interface on which your internal network is connected (e.g.: *in* interface) or the object corresponding to the internal networks (e.g.: *Network_internals*).

> **NOTE**
> The SSO agent authentication method cannot be applied with an interface as a criterion. This method is based on authentication events collected by domain controllers, which do not indicate the source of the traffic. A rule combining an interface as the source and the SSO agent method is therefore not allowed.

> **NOTE**
> The choice offered for the interface is the SSL VPN interface, indicating the interface on which users of an SSL VPN tunnel are connected.

Step 4: Authentication methods

This step is not offered for rules associated with the "**Guest**", "**Temporary account**" or "**Sponsorship**" methods.

Click on **Enable a method** and select from the drop-down list the desired authentication methods. The *Default method* selected corresponds to the method selected in the "**Available methods**" tab.

The "Block" entry can also be selected. It will then block authentication attempts on traffic that matches the rule.

One-time password	If you want to add time-based one-time passwords (TOTP) to this authentication method, place the cursor on ON: ON The **One-time password** column will then be selected on the row in the corresponding authentication rule in the authentication policy.

The authentication methods are evaluated **in the order in which they appear on the list** and from top to bottom. As the *SSO agent* method is transparent, it is by definition always applied as a priority.

To **enable** the newly created rule, double-click on *Disabled* in the **Status** column in the authentication rule grid.

Reorganizing rules

Every rule can be dragged and dropped so that the authentication policy can be reorganized easily. The symbol as well as the "Drag and drop to reorganize" tool tip appear when you scroll over the beginning of the rule.

Default action

Default action to apply	Select the action that will be applied: • If the authentication request does not match any of the rules defined in the policy, • For rules set to apply the **Default action**.

Default method

Method to use if no rules match	Select the method that will be applied when the *Default method* is selected in the authentication policy. The methods offered are those added to the table of available methods.

Multi-user objects

This table allows selecting network objects that enable several authentications from the same IP address. For example, applications and data can be accessed from a remote computer (TSE server) by applying user-based filtering.

You can **Add** or **Delete** a multi-user object by clicking on the corresponding buttons.

> **NOTE**
> The SSO method does not allow "**multi user**" authentication.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of multi-user objects:

- Add,
- Remove.

Captive portal tab

For the sake of strengthening security, the connection to the authentication portal and to the Web administration interface is possible only by forcing certain options in the SSL protocol. Version SSLv3 is disabled and the TLS versions enabled, according to the recommendations given by the French Network and Information Security Agency (ANSSI).

The address of the captive or authentication portal is hosted on the firewall and accessible at: **https://<ip_address>/auth**.

The captive portal has to be enabled for all authentication methods, except for the SSO agent.

Captive portal

Authentication profile and interface match

In this grid, a profile from the captive portal can be mapped to an interface on the firewall. It is possible to **Add** or **Delete** a match rule by clicking on the corresponding buttons or by right-clicking in the grid.

Interface	Select the network interface to which a profile from the captive portal will be mapped. This can be an Ethernet interface (in, out, etc.), a modem or an IPsec interface.
Profile	Select the profile to be mapped to the interface. If a warning appears, indicating that the captive portal has been disabled, enable it in the **Captive portal profiles** tab.
Default method or directory	The authentication method or the directory associated with the selected profile will automatically appear.

SSL server

Certificate (private key)	To access the portal via SSL, the firewall's authentication module uses its own certification authority by default; the associated name of the CA is the firewall's serial number. So when users contact the firewall other than by its serial number, they will receive a warning message indicating an inconsistency between what the users are trying to contact and the certificate that the firewall receives. You can choose to use another certificate from another CA imported earlier by choosing it in the selection zone. The icon indicates certificates with a TPM-protected private key. For more information on the TPM, see the section Trusted Platform Module. Users are authenticated via the captive portal by default, through an SSL/TLS access that uses a certificate signed by two authorities that the browsers do not recognize. It is therefore necessary to deploy these certification authorities used by a GPO on users' browsers. These authorities are the NETASQ CA and Stormshield CA, available at the following links: • http://pki.stormshieldcs.eu/netasq/root.crt. • http://pki.stormshieldcs.eu/products/root.crt. For further detail, refer to the chapter User awareness, under **Initial connection to the appliance.**

Conditions of use for Internet access

Conditions of use can be shown whenever users access the Internet. These conditions can be defined by importing them in HTML or PDF format. Users must then accept them by selecting the checkbox before accessing the Internet.

Select the conditions of use for Internet access in HTML format	Imports your version in HTML.
Select the conditions of use for Internet access in PDF format	Imports your version in PDF.
Reinitialize customization of Conditions of use for Internet access	This button allows you to reinitialize the customized Conditions of use for Internet access

> **TIP**
> Remember to enable, in the **Captive portal profiles** tab, the display of the Conditions of use for Internet access in the relevant profile.

Advanced properties

Interrupt connections once the authentication period expires	As soon as the authentication duration expires, connections will be interrupted, even if the user is in the middle of a download.
Proxy configuration file (.pac)	This field allows sending to the firewall the .pac file, which represents the proxy's automatic configuration file (Proxy Auto-Config), to be distributed. Users can retrieve .pac files or check their contents by clicking on the button to the right of the field. Users can indicate in their web browsers the automatic configuration script located at *https://if firewall>/config/wpad.dat.*

Captive portal

Port on the captive portal	This option allows you to specify a listening port other than TCP/443 (HTTPS) defined by default for the captive portal.
Hide the header (logo)	With this option, the header that appears on the captive portal can be hidden. The Stormshield logo appears by default.
Select a logo to display (800x50 px)	You can customize the image that appears in the captive portal's header. The format of the image has to be 800 x 50 px by default.
Select a stylesheet to apply (CSS file)	Import a new style sheet in css, which will override the captive portal's graphics.
Reset	This button resets the custom settings on the captive portal.

Captive portal profiles tab

This window allows you to select a predefined or customizable profile from the captive portal and modify its configuration.

Possible actions

Profile selection field	Select from the drop-down menu the captive portal profile that you wish to configure.
Rename	This button makes it possible to rename the selected profile.
Last modification	Scroll over the icon to display the date and time of the last modification made to the profile from the selected captive portal.

Authentication

Default method or directory	Select the authentication method or LDAP directory (for firewalls that have defined several directories) assigned by default to the authentication profile currently being modified. The methods offered are those defined in the *Available methods* tab. **IMPORTANT** Depending on the authentication method or the default directory selected, some fields in this module cannot be modified.
Enable sponsorship	This option enables the sponsorship method in addition to the authentication method selected by default. This checkbox is automatically selected and grayed out whenever the **Sponsorship** method is selected in the field above.

Conditions of use for Internet access

Enable the display of the conditions of use for Internet access	This option shows the conditions of use when a user accesses the Internet. They must then accept them by selecting the checkbox in order to authenticate. Customize these conditions in the **Captive portal** tab. **NOTE** This option does not apply to the transparent SSO agent authentication method, as it does not require the activation of the authentication portal.
Display frequency of the Conditions	Set the display frequency of the conditions of use for Internet access. This frequency applies to all authentication methods except **Guest** method, which is configured in the **Available methods** tab.

Customized fields on the captive portal (Guest method only)

When **Guest** mode is selected, three numbered fields become available. Up to three input zones can be added to the captive portal when the conditions of use for Internet access are displayed.

The possible values for these fields are: Empty (disables the display of the field on the captive portal), First name, Last name, Telephone number, Email address, Information and Company.

Authentication periods allowed

Minimum duration	Minimum duration for which the user can be authenticated.
Maximum duration	Maximum duration for which the user can be authenticated.
For transparent authentication	For SPNEGO and SSL certificates, set the period during which no transparent reauthentication requests (Kerberos tickets or certificates) will be sent between the captive portal and the client's browser.

Advanced properties

Enable the captive portal	This option allows authentication via a web form from the network interfaces associated with the captive portal profile. The map of the interfaces with the profiles can be consulted in the **Captive portal** tab.
Enable logoff page	This option enables a separate logoff page from the captive portal's authentication page. When users who have not yet authenticated wish to access a website, the authentication page will appear. Once they have authenticated, the requested web page will then open in a new tab while the logoff page appears in the current tab. To log off, simply click on the **Logout** button which appears in the logoff page, or close the tab of this page.
Allow access to the proxy's configuration file (.pac) for this profile	This option allows the publication of the .pac file for users logging in from network interfaces associated with the authentication profile.
Prohibit simultaneous authentication of a user on multiple hosts	This option makes it possible to prevent a user from authenticating on several computers at the same time. Multiple requests are automatically denied.
Expiry of the HTTP cookie	This option makes it possible to configure when the HTTP cookie expires: • **At the end of the authentication period**: the cookie is negotiated only once throughout the whole duration of the authentication. • **At the end of the session:** the cookie will be negotiated every time a request is sent to your web browser. • **Do not use (not recommended - except sponsorship)**: the cookie never expires. This option is not recommended as it compromises authentication security. Configuring an expiry date makes it possible to protect the user from replay attacks, for example. HTTP cookies are negotiated by the web browser, so authentication set up on one browser will not work on another browser. To allow several users to be authenticated from the same IP address, cookies must be used. The IP addresses in question must be entered in the list of **Multi-user objects** in the **Authentication policy** tab, except for the SSO Agent method, which does not support multi-user authentication.

Authentication page

Select a customized message (HTML file)	This option makes it possible to add a customized message containing text and images under the title of the authentication page. This message must be an HTML file so that the firewall can load it.
Reset customization of authentication page	By clicking on this button, the customized message added earlier will be deleted from the authentication page.

User passwords

Users cannot change their passwords	This option does not allow users to change their passwords from the authentication portal.
Users can change their passwords	This option allows users to change their passwords from the authentication portal, at any time with no restrictions on validity.
Users must change their passwords	This option requires users to change their passwords the first time they log in to the authentication portal, and every time the password expires. The validity of a password is specified in days without a specific time.
Lifetime (in days)	This field can be modified if the **Users must change their passwords** option is selected. Indicate the number of days the password stays valid. When the password has reached the end of its lifetime, it expires at midnight. **EXAMPLE** A user changes his password for the first time at 2:00 PM on Monday with a lifetime of 1 day. The password must be changed by 12:00 AM the next day instead of 24 hours later.

User enrollment

The firewall offers web-based user enrollment. If users attempting to log in do not exist in the user database, they may request the creation of their accounts via web enrollment on the captive portal.

Do not allow user enrollment	When this option is selected, users that are not in the user database cannot send account creation requests.
Allow Web enrollment for users	When this option is selected, users that are not in the user database can request the creation of an account by filling in a web form. An administrator must approve or deny the request in the **Configuration** module > **Users** > Enrollment.
Allow web enrolment for users and create their certificates	When this checkbox is selected: • Users that are not in the user database can request the creation of an account and a certificate by filling in a web form. Two requests will then be sent - one for the account, one for the certificate. • Users who are in the user database but who do not have a certificate can request the creation of their certificate. By submitting a request, users set the password for their certificate. An administrator must approve or deny requests in the **Configuration** module > **Users** > Enrollment. The certificate will be signed by the certification authority (CA) chosen by default in the **Configuration** module > **Objects** > **Certificates and PKI** and created based on the settings in the user certificate profile.

Notification of a new enrollment	This option makes it possible to define a user group that will be notified when a new enrollment request is received. By default, the drop-down list will show that no e-mails will be sent. To select a user group, it must first be created in **Configuration** > **Notifications** > **E-mail alerts** > Recipients tab. Once it is created, it can be selected from the drop-down list.

Transparent or explicit HTTP proxy and multi-user objects

Multi-user objects

The *networks of options* allows several authentications from the same IP address (see the option **Multi-user objects**). For example, applications and data can be accessed from a remote computer (TSE server) by applying user-based filtering. This Multi-user application only applies to HTTP and HTTPS traffic.

Below is a brief description of the mechanisms that allow multi-user authentication. The various modes are covered in the following sections.

Cookie mode

Cookie mode makes it possible to use *Multi-user objects*. During the initial connection to every new website visited, the web browser captures authentication data in an authentication cookie that has several attributes. This data is then forwarded in requests that follow, to be intercepted by the firewall, which can then apply its policy.

Only in unsecured HTTP connections, web browsers display an error message instead of the content of queried websites because authentication cookies cannot use the "Secure" attribute together with the "SameSite" attribute.
The web browser must be manually configured to enable browsing on websites queried in HTTP:

- In Google Chrome:
  - Go to chrome://flags/,
  - Set the attribute **Cookies without SameSite must be secure** to **Disabled**,
  - Restart the browser.
- In Firefox:
  - Go to about:config,
  - Set the attribut **network.cookie.sameSite.noneRequiresSecure to false**,
  - Restart the browser.
- In Microsoft Edge:
  - Go to edge://flags/,
  - Set the attribute **Cookies without SameSite must be secure** to **Disabled**,
  - Restart the browser.

Authentication offered by the browser (HTTP code 407)

The *Proxy-Authorization* - HTTP code 407 method can be used only for explicit proxies. The HTTP protocol provides a field dedicated to authentication. The browser will prompt the user to authenticate via a message window and the connection information will be relayed to the firewall via the HTTP header. The security policy can then be applied.

The "Proxy-Authorization" (HTTP 407) authentication method via the browser does not allow the SSL (certificates) and SPNEGO methods as they do not involve the authentication portal, even though it needs to be enabled.

> **NOTE**
> If an object is added to or deleted from the list of *Multi-user objects*, ensure that no authentication process relating to this object has been saved.

Transparent proxy (implicit)

The transparent or implicit proxy filters user requests without any configuration on the client workstation (no proxy declaration in the browser). The firewall's proxy will then intercept and filter all requests in order to allow or deny access to a website, for example.

This mode is recommended as it meets all requirements: authentication of the user according to the selected method, SSL filtering (blocking of websites in HTTPS, for example), etc. While this mode can use all features, it cannot use the transparent authentication *SSO agent* method.

Single user		Multi-user objects (Cookie mode)	
Methods	*Inspections*	*Methods*	*Inspections*
All methods	All inspections	All methods **except SSO agent**	All inspections

Explicit proxy

When a proxy is entered in the browser, two modes of authentication are possible:

- ***Standard* or *Cookie* mode**

This mode is easy to set up thanks to the **Explicit HTTP proxy rule** creation wizard, available in the **Filtering** module. Two rules are generated – one redirects traffic to the explicit HTTP proxy, and the other applies the filter policy. Prescriptions with regard to user authentication have to be stipulated in a rule to be inserted between the two rules that the creation wizard generates, after the redirection to the HTTP proxy and before authorizing traffic via the *Explicit HTTP proxy*.

- **Authentication offered by the browser (HTTP code 407)**

The feature *Proxy-Authorization* - HTTP code 407 can be enabled in the advanced properties of the *HTTP protocol* module (*Proxy* tab) accessible via the menu *Application protection*.

There are however certain restrictions to these modes, as shown in the table below:

Single user				Multi-user objects			
Standard mode		**"Proxy-Authorization" code 407**		**Cookie mode**		**"Proxy-Authorization" code 407**	
Methods	*Inspections*	*Methods*	*Inspections*	*Methods*	*Inspections*	*Methods*	*Inspections*

All methods	All inspections **except on SSL traffic Filtering by user**	• LDAP • RADIUS • Kerberos • SSO Agent Δ passwords in plaintext (encoded in base 64)	All inspections **except on SSL traffic Filtering by user**	All methods **except SSO agent**	All inspections **except on SSL traffic Filtering by user (HTTP only)**	• LDAP • RADIUS • Kerberos Δ passwords in plaintext (encoded in base 64)	All inspections **except on SSL traffic Filtering by user**

Content filtering can only be applied to HTTP traffic.
Filtering by user can be applied to HTTP and HTTPS, except for multi-user networks in *Cookie* mode (HTTP only).

Explicit mode involves HTTP traffic via the CONNECT method. HTTPS traffic is then encapsulated in HTTP and the method for sending requests makes it possible set up a relationship of trust between the client and the server.

BLOCK MESSAGES

The configuration screen for the **Block messages** module comprises 2 sections:

- **The Antivirus** tab: detection of viruses attached to documents, which may arise when sending or receiving e-mails (POP3, SMTP) or through file transfers (FTP).
- The **Block page** tab: page that appears during an attempt to access an HTTP/HTTPS website that the URL and SSL filter rules do not allow.

Antivirus tab

POP3 protocol

Contents of the e-mail	This field allows modifying the text of the message received when a virus is detected in an e-mail. **EXAMPLE** Your Stormshield Network firewall has detected a virus in this e-mail - the embedded antivirus has cleaned it; infected attachments were removed.

SMTP protocol

SMTP error code	Restricted to 3 digits, this field allows defining the error code that the SMTP server will receive when a virus is detected in a sent e-mail. **EXAMPLE** 554
Accompanying message	This field contains the message that will be sent to the SMTP server when a virus is detected. **EXAMPLE** 5.7.1 Virus detected.

FTP protocol

FTP error code	Restricted to 3 digits, this field contains the error code that the user or the FTP server will receive when a virus is detected in a transferred file. **EXAMPLE** 425

Accompanying message	This spot is reserved for the message that will be sent with the error code when a virus is detected while sending / receiving a file to / from an FTP server. **EXAMPLE** Virus detected. Transfer aborted.

Block page tab

This window shows by default the HTTP/HTTPS block page that appears whenever there is an attempt to access a site that URL or SSL filter rules have blocked. In a filter rule, there are 4 versions of block pages to choose from.

By default, a block page consists of an icon and a message clearly explaining why the page has been blocked, and showing for example, to which URL category the unauthorized website belongs.

EXAMPLE
The company's policy does not allow access to this page. It falls under the category: "Games".

The block page can be fully customized as it is in HTML/CSS format. You can choose to display just a logo, a sentence, or a combination of both. Each field on the page can be modified: the logo, font, font size or even the font color.

Each of these 4 customizable HTML pages has multilingual support, meaning that the message that appears can be displayed in several languages. The version of the text displayed when a page is blocked is selected according to the browser's default language.

An e-mail notification to the administrator can also be associated with the page to request the unblocking of access to a website.

Block page tabs

Each of the 4 block pages can be edited directly in the web administration interface. The following operations can also be performed on them:

Rename	Customizes the name of the current block page.
Reset	Resets data to the default block page.
Copy to	Copies the settings of the current block page and applies this template to one of the other block pages.

Editing block pages

You can customize the page by replacing the image displayed on the page. The HTML page also offers multilingual support.

Depending on the language chosen, you can customize the message that appears when the website is blocked, as well as a notification e-mail to the administrator, asking for access to the blocked website to be categorized or unblocked..

The page exists in several languages by default and offers the possibility of adding new languages.

There are variables that can be used to make the information dynamic, such as the categories to which the blocked sites belong.

These variables are:

$host	Queried domain name (e.g.: www.google.com)
$url	Page of the queried domain
$protected_url	Page of the queried domain – encoded in a format that can be processed by the browser or mail client
$user	Name of the authenticated user (if known)
$src	Name of the source or its IP address
$url_group	Name of the category group
$protected_url_group	Name of the category group - encoded in a format that can be processed by the browser or mail client
$cat_group	Name of the URL category
$protected_cat_group	Name of the category - encoded in a format that can be processed by the browser or mail client
$url_rule	Number of the block rule in the URL filter policy
$url_policy	Number of the URL filter policy

To display the full URL, both variables need to be concatenated as follows: **$host$url**

CERTIFICATES AND PKI

PKI or *Public Key Infrastructure* is a cryptographic system based on asymmetric cryptography. It uses signatures and certifies public keys which make it possible to encrypt and sign messages or traffic in order to ensure confidentiality, authentication, integrity and non-repudiation.

The Stormshield Network PKI allows you to generate or import digital identities of trusted authorities (known as CAs or certification authorities), servers or users. With it, you can sign certificates, which contain a public key associated with information that may belong to a user, a server, etc. The aim of Stormshield Network's PKI is to authenticate these entities.

In the rest of this manual, the term "identity" refers to the concept of a digital identity.

When the SSL VPN feature is used, the certification authority "sslvpn-full-default-authority" includes a server identity "openvpnserver" and a user identity "openvpnclient". This allows the client and the Stormshield Network firewall's SSL VPN service to identify each other without relying on an external authority.

The window of the **Certificates and PKI** module consists of three sections:

- At the top of the screen, the various possible operations in the form of a search bar and buttons,
- On the left, the list of authorities, identities and certificates,
- On the right, details regarding the authority, identity or certificate selected beforehand from the list on the left, information regarding the certificate revocation list (CRL), and in the case of a sub-authority, the properties of certificates that were signed by this authority or sub-authority.

The firewall's health indicator (in the upper banner of the web administration interface when there is an issue) uses probes that track validity dates and the statuses of certificates and CRLs of certification authorities used in the configuration. The of the indicator specifies its status:

- For certificates:
  - **Critical**: the certificate has been revoked (by a certification authority) or has expired,
  - **Not critical**: the certificate will expire in less than 30 days or it is not yet valid,
  - **Optimal**: the certificate does not present any critical characteristics.
- For CRLs:
  - **Critical**: the CRL of the CA has expired,
  - **Not critical**: the certificate will expire in less than 30 days or it is not yet valid,
  - **Optimal**: the CRL does not present any critical characteristics.

Possible operations

Enter a filter field

Enter the name of a certificate, identity or authority in the search field to look for it.
All certificates, identities and authorities that match the character string entered will appear.

Example:

If you type “a” in the search bar, the list below it will show all certificates containing an “a”.

Filter

This button allows you to select the type of certificate to display and to view only items that are relevant to you. A drop-down menu offers the following choices:

- "**Filter: All**": displays in the list on the left all existing authorities, identities and certificates,
- "**Filter: Certification authorities**": displays in the list on the left all authorities and sub-authorities,
- "**Filter: User certificates**": displays in the list on the left only user certificates and the authorities on which they depend,
- "**Filter: Server certificates**": displays in the list on the left only server certificates and the CAs on which they depend,
- "**Filter: Smart card certificates**": displays in the list on the left only smart card certificates and the CAs on which they depend,

Add

Add various items to the PKI with this button:

- **Root authority**,
- **Sub-authority**,
- **User identity,**
- **Smart card identity,**
- **Server identity.**

And **Import a file** containing items from the above categories.

For further information on these operations, refer to the sections Adding a root authority, Adding a sub-authority, Adding a user identity, Adding a smart card identity, Adding a server identity and Importing a file.

Refer to the section Allowed names to find out which characters are allowed and prohibited in various fields.

Revoke

Use this button to remove an authority, sub-authority, identity or certificate from the PKI.

For further information on these operations, refer to the section Revoking an authority, sub-authority or certificate.

Actions

The possible actions vary according to the type of object selected in the list on the left:

- Authority or sub-authority: **Create CRL**, **Renew CRL**, **Remove CRL**, **Set as default**.
- User certificate: **LDAP publication**,
- Any identity type (except imported identities): **Remove private key** and **Protect with the TPM**.

For further information on these operations, refer to Creating, renewing or removing a CRL, Removing the private key of an identity, Set as default and Publishing a certificate in the LDAP directory.

Download

With this button, you can download:

- Certificates of authorities and sub-authorities,
- CRLs of authorities and sub-authorities,
- User certificates, smart card certificates and server certificates,
- User identities, smart card identities and server identities.

For further information on these operations, refer to Downloading a certificate, Downloading an identity and Downloading a CRL.

Initializing the TPM (Init. TPM)

This button allows you to initialize the SNS firewall's TPM. For further information regarding the initialization of the TPM, refer to the section Trusted Platform Module.

Check usage

You can look for the features or modules that use the selected certificate, CA of sub-authority selected.

Adding authorities and identities

The **Add** button opens up list of six actions to create certificate authorities, sub-authorities and digital identities.

A digital identity (user, server or smart card identity) consists of:

- The bearer's certificate: identity information (name [FQDN for servers], e-mail address, etc.), bearer's public key, signature and public key of the issuing certification authority
- The bearer's private key.

Adding a root authority or displaying its details

A root authority or “root CA” is an entity that signs, sends and maintains certificates and CRLs (Certificate Revocation Lists).

> **NOTE**
> Once the certification authority has been created, information entered can no longer be changed.

Adding a root authority

1. Click on **Add**.
2. Select **Root authority**.

3. Enter a **CN** (mandatory).
   This is a name that will help you identify your root authority, restricted to 64 characters. It may be the name of an organization, user, server, host, etc.
4. Enter an **ID** (optional).
   Here, you can add a shortcut to your CN, which will be useful for command lines.
5. Enter the attributes of the authority. All this information will appear in the authority certificate and the certificates that it issues.
   - **Organization (O)**: Name of your company (e.g.: Stormshield).
   - **Organizational unit (OU)**: "Branch" of your company (e.g.: Documentation).
   - **Locality (L)**: City in which your company is located (e.g.: Boston).
   - **State or province (ST)**: State or province in which your company is located (e.g.: Massachusetts).
   - **Country (C)**: Select from the list the country in which your company is located (e.g.: USA).
4. Click on **Next**.
5. Enter the password that will protect the root authority, then confirm it.
   A progress bar indicates your password's strength. Combine uppercase and lowercase letters with numbers and special characters for best results.
6. You can enter your **E-mail address** in this field to receive a message confirming that your authority was created.
7. If necessary, change the **Key size (in bits)**.
   Even though large keys are more effective, you are advised against using them with entry-level appliances as this will mean the key will take a long time to be generated.
8. You can also change your authority's **Validity (in days)**.
   This field corresponds to the number of days for which your certification authority, and therefore your PKI, will be valid. This date affects all aspects of your PKI. Indeed, once this certificate expires, all user certificates will expire as well. This value cannot be changed later.
   The value of this field must not exceed 3650 days.
9. Click on **Next**.
10. Where necessary, specify distribution points for certificate revocation lists and click on **Add** to indicate the URL to the CRL.
    All this information will be embedded in the generated CAs and applications that use the certificate will be able to automatically retrieve the CRL in order to check the certificate's validity.
    If there are several distribution points, they will be applied in their order of appearance on the list.
11. Click on **Next**.
    You will be shown a summary of the information you entered.
12. Click on **Finish**.

The authority will automatically be added to the tree of authorities, identities and certificates defined on the firewall.

Displaying details of an authority/editing certificate profiles linked to this authority

Click once on an authority to display its detailed information on the right side of the screen:

"Details" tab

Data about the authority is shown in four frames:

- The duration of its **Validity**: when it was issued and when it expires,
- Its recipient (**Issued for**): subject and details of the authority certificate,
- Its **Issuer**: subject and details of the authority certificate,
- Its **Details**: serial number of the authority, version, encryption and signature algorithms used, key type, key size, and Extended Key Usage (EKU).

"Revocation (CRL)" tab

This tab summarizes information regarding the CRL:

- Its validity, including the date of the last and next updates,
- A grid showing certificates signed by this CA that have been revoked. For each of these revoked certificates, the serial number, revocation date and reason for revocation (optional) are specified.

"Certificate profiles" tab

In this tab, you will see:

- Distribution points that provide the CA's CRL. Distribution points can be added or deleted from this grid.
- Suggested default values for the parameters that are involved when a new sub-authority or certificate is signed by the selected certification authority. These values can be changed.

> **NOTE**
> Changing the values of these parameters does not affect existing sub-authorities or certificates: recreate them if you wish to use the new values for these items.

These parameters are as follows:

- **Key type** (signature algorithm): the default value suggested is **SECP**.
- **Key Size (bits)**: the default value suggested is **256**.
- **Validity (days)**: the default value suggested is **365** days for a certificate, and **3650** days for a CA.
- **CRL validity** duration (only for signing the certificate of a sub-authority): the default value suggested is **30** days (maximum allowed: 3650 days),
- **Checksum**: the default value used is **sha256**,

Adding a root authority or displaying its details

During the creation of a sub-CA, the windows are similar to those for the root CA. The configuration wizard for a sub-CA requires a “parent” reference from which it will copy information.

Adding a sub-authority

1. Click on **Add**.
2. Select **Sub-authority**.
3. Enter a **CN** (mandatory).
   This is a name that will help you identify your root authority, restricted to 64 characters. It may be the name of an organization, user, server, host, etc.
4. Enter an **ID** (optional).
   Here, you can add a shortcut to your CN, which will be useful for command lines.

5. Select the parent authority: a sub-authority can only be used after the identification of its parent authority.
   The authority suggested as the parent for the new sub-authority will be the default authority or the last authority selected before clicking on "**Add > Sub-authority**".
6. Enter the password of the parent authority.
   The icon allows you to view the password in plaintext to check that it is correct.
7. Click on **Next**.
8. Enter the password that will protect the sub-authority, then confirm it.
   A progress bar indicates your password's strength. Combine uppercase and lowercase letters with numbers and special characters for best results.
9. You can enter your **E-mail address** in this field to receive a message confirming that your authority was created.
10. If necessary, change the **Key size (in bits)**.
    Even though large keys are more effective, you are advised against using them with entry-level appliances as this will mean the key will take a long time to be generated.
11. You can also change your authority's **Validity (in days)**.
    This field corresponds to the number of days for which your certification authority, and therefore your PKI, will be valid. The date affects all aspects of your PKI as indeed, once this certificate expires, all user certificates will also expire. This value cannot be changed later. The value of this field must not exceed 3650 days.
12. Click on **Next**.
13. Where necessary, specify distribution points for certificate revocation lists and click on **Add** to indicate the URL to the CRL.
    All this information will be embedded in the generated CAs and applications that use the certificate will be able to automatically retrieve the CRL in order to check the certificate's validity.
    If there are several distribution points, they will be applied in their order of appearance on the list.
14. Click on **Next**.
    You will be shown a summary of the information you entered.
15. Click on **Finish**.

The sub-authority will automatically be added to the tree of authorities and identities defined on the firewall.

Displaying sub-authority details

Click once on the sub-authority to display its detailed information on the right side of the screen.

Displaying details of an authority/editing certificate profiles linked to this authority

Click once on an authority to display its detailed information on the right side of the screen:

"Details" tab

Data about the authority is shown in four frames:

- The duration of its **Validity**: when it was issued and when it expires,
- Its recipient (**Issued for**): subject and details of the sub-authority certificate,
- Its **Issuer**: subject and details of the parent authority certificate,
- Its **Details**: serial number of the sub-authority, version, encryption and signature algorithms used, key type, key size, and Extended Key Usage (EKU).

"Revocation (CRL)" tab

This tab summarizes information regarding the CRL:

- Its validity, including the date of the last and next updates,
- A grid showing certificates signed by this CA that have been revoked. For each of these revoked certificates, the serial number, revocation date and reason for revocation (optional) are specified.

"Certificate profiles" tab

In this tab, you will see:

- Distribution points that provide the CA's CRL. Distribution points can be added or deleted from this grid.
- Suggested default values for the parameters that are involved when a new sub-authority or certificate is signed by the selected certification authority. These values can be changed.

> **NOTE**
> Changing the values of these parameters does not affect existing sub-authorities or certificates: recreate them if you wish to use the new values for these items.

These parameters are as follows:

- **Key type** (signature algorithm): the default value suggested is **SECP**.
- **Key Size (bits)**: the default value suggested is **256**.
- **Validity (days)**: the default value suggested is **365** days for a certificate, and **3650** days for a CA.
- **CRL validity** duration (only for signing the certificate of a sub-authority): the default value suggested is **30** days (maximum allowed: 3650 days),
- **Checksum**: the default value used is **sha256**,

"Details" tab

Data about the sub-authority is shown in four windows:

- The duration of its **Validity**: when it was issued and when it expires,
- Its recipient (**Issued for**): the sub-authority itself,
- Its **Issuer**: its parent authority,
- Its **Details**: serial number of the sub-authority, version, encryption and signature algorithms used, key type, key size, etc.

"Revocation (CRL)" tab

Rounds up information regarding the CRL: its la validity including the last and next update, the table of distribution points and the table of revoked certificates which should contain a serial number, a revocation date and a reason for the revocation (optional).

"Certificate profiles" tab

This tab shows the **Key size (bits)** and **Encryption algorithm** for the certification authority (including the authority's **CRL validity (days)**, restricted to a maximum of 3650 days), user certificates, smart card certificates and server certificates.

These values can be changed later and are suggested by default when a sub-authority is created or when a certificate signed by the selected sub-authority is added.

Adding a user identity or displaying details of such identities

In the configuration wizard, enter the information relating to the user for whom you are creating an identity.

Creating a user identity

1. Click on **Add**.
2. Select **User identity**.
3. Enter a **CN** (mandatory).
   This is a name that will help you identify the user, and is restricted to 64 characters.
4. Enter an **ID** (optional).
   Here, you can add a shortcut to your CN, which will be useful for command lines (e.g., if the CN is a first name+last name pair, the identifier may correspond to the initials of the CN).
5. Enter the **E-mail address** (mandatory) of the user for whom you are creating an identity.
6. Click on **Next**.
7. Select the **Parent authority** that will sign the certificate for the identity.
8. Enter the **Top CA passphrase**.
   The attributes of the authority will be added automatically. They will be found in the user certificate.
9. Click on **Next**.
10. When the firewall has a TPM that has been initialized, select the checkbox **Protect this identity with the TPM** to protect the identity's private key with the TPM.
11. Where necessary, change the duration of the certificate's **Validity (days)**.
    The recommended value is 365 days (suggested by default).
12. The **Key size (bits)** of the certificate can also be changed.
    Even though large keys are more effective, you are advised against using them with entry-level appliances as this will mean the key will take a long time to be generated.
13. If a user that was declared in the LDAP directory indicates the same e-mail address as the one given in step 4, this identity can be automatically associated with the user.
    However, this can only be done if the authority used to generate the certificate is the firewall's default authority. In this case:
    - Select **Publish this identity in the LDAP directory**,
    - Enter the password that will protect the PKCS#12 container of the identity.
14. Click on **Next**.
    You will be shown a summary of the information you entered.
15. Click on **Finish**.

The identity will automatically be added to the tree of authorities, identities and certificates defined on the firewall, under its parent authority.

Displaying identity details

Click once on the identity to display its detailed information on the right side of the screen.

These details are in read-only mode.

"Details" tab

Information about the identity is shown in several frames:

- Its **Usage**: the modules in which the identity certificate is used, and any TPM-protected private key of the identity, if the firewall is equipped with a TPM.

- The duration of its **Validity**: when its certificate was issued and when it expires,
- Its recipient (**Issued for**): subject and details of the user certificate (user's e-mail address),
- Its **Issuer**: subject and details of the server identity's parent authority certificate,
- Its **Details**: serial number of the certificate, version, encryption and signature algorithms used, key type, key size, usage purposes for this identity and its certificate (Extended Key Usage - EKU).

Revocation (CRL) tab

- The URLs of the parent authority's **CRL distribution points**,
- The URLs of **OCSP servers** if OCSP is used in certificate renewal.

Publishing an identity in the LDAP directory

If a user that was declared in the LDAP directory indicates the same e-mail address as the one given for a user certificate, this identity can be associated with the user, if you did not already do so while you were creating the identity.

Do note that this can only be done if the authority used to generate this identity is the firewall's default authority.

In this case:

1. Select the relevant identity by clicking once,
2. Click on the **Actions** menu.
3. Select **LDAP publication**,
4. In the pop-up window that appears, enter the password that will protect the PKCS#12 container of the identity.
5. Click on **Publish certificate**.

Adding a smart card identity or displaying details of such identities

Smart card identities are associated with Microsoft Windows accounts, and therefore associated with a unique user. This user's certificate is signed by a certification authority that provides access to CRLDPs to check the validity of the certificate, then published in an Active Directory (or an LDAP directory). Since the firewall is able to check the user's Windows account against an authentication policy and confirm the information in the corresponding certificate, it can allow smart card-connected users to access your organization's network resources.

Creating a smart card identity

1. Click on **Add**.
2. Select **Smart card identity**.
3. Enter a **CN** (mandatory).
   This is a name that will help you identify the user, and is restricted to 64 characters.
4. Enter an **ID** (optional).
   Here, you can add a shortcut to your CN, which will be useful for command lines (e.g., if the CN is a first name+last name pair, the identifier may correspond to the initials of the CN).
5. Enter the **E-mail address** (mandatory) of the user for whom you are creating an identity.
6. In the **Main user name (Windows)** field, enter the name of the user's Active Directory account.
7. Click on **Next**.
8. Select the **Parent authority** that will sign the certificate.

9. Enter the **Top CA passphrase**.
   The attributes of the authority will be added automatically. They will be found in the smart card certificate.
10. Click on **Next**.
11. When the firewall has a TPM that has been initialized, select the checkbox **Protect this identity with the TPM** to protect the identity's private key with the TPM.
12. Where necessary, change the duration of the certificate's **Validity (days)**.
    The recommended value is 365 days (suggested by default).
13. The **Key size (bits)** of the certificate can also be changed.
    Even though large keys are more effective, you are advised against using them with entry-level appliances as this will mean the key will take a long time to be generated.
14. Click on **Next**.
    You will be shown a summary of the information you entered.
15. Click on **Finish**.

Displaying certificate details

Click once on the identity to display its detailed information on the right side of the screen.

These details are in read-only mode.

"Details" tab

Information about the identity is shown in various frames:

- Its **Usage**: the modules in which the identity certificate is used, and any TPM-protected private key of the identity, if the firewall is equipped with a TPM.
- The duration of its **Validity**: when its certificate was issued and when it expires,
- Its recipient (**Issued for**): subject and details of the smart card certificate (user's e-mail address),
- Its **Issuer**: subject and details of the server identity's parent authority certificate,
- Its **Details**: serial number of the certificate, version, encryption and signature algorithms used, key type, key size, usage purposes for this identity and its certificate (Extended Key Usage - EKU).

Revocation (CRL) tab

- The URLs of the parent authority's **CRL distribution points**,
- The URLs of **OCSP servers** if OCSP is used in certificate renewal.

Adding a server identity or displaying details of such identities

A server identity has to be installed on web or application servers. The certificate corresponding to this identity is used to authenticate the server.

In the case of websites, for example, certificates ensure that the URL and its domain name belong to the right organization.

Adding a server identity

1. Click on **Add**.
2. Select **Server identity**.
3. Enter a **Fully Qualified Domain Name (FQDN)** (mandatory).
   The size limit of this field is 64 characters. E.g.: myserver.mycompany.com.

4. Enter an **ID** (optional).
   Here, you can add a shortcut to your CN, which will be useful for command lines.
5. Click on **Next**.
6. Select the **Parent authority** that will sign the certificate for the identity.
7. Enter the **Top CA passphrase**.
   The attributes of the authority will be added automatically. They will be found in the server certificate.
8. Click on **Next**.
9. When the firewall has a TPM that has been initialized, select the checkbox **Protect this identity with the TPM** to protect the identity's private key with the TPM.
10. Where necessary, change the duration of the certificate's **Validity (days)**.
    The recommended value is 365 days (suggested by default).
11. The **Key size (bits)** of the certificate can also be changed.
    Even though large keys are more effective, you are advised against using them with entry-level appliances as this will mean the key will take a long time to be generated.
12. Click on **Next**.
13. If needed, define aliases for the server. These aliases are in the form of a FQDN.
    E.g.: alias1.mycompany.com
14. Click on **Next**.
    You will be shown a summary of the information you entered.
15. Click on **Finish**.

The identity will automatically be added to the tree of authorities, identities and certificates defined on the firewall, under its parent authority.

Displaying identity details

Click once on the identity to display its detailed information on the right side of the screen.

These details are in read-only mode.

Details tab

Information about the identity is shown in various frames:

- Its **Usage**: the modules in which the identity certificate is used, and any TPM-protected private key of the identity, if the firewall is equipped with a TPM.
- The duration of its **Validity**: when its certificate was issued and when it expires,
- Its recipient (**Issued for**): subject and details of the server certificate,
- Its **Issuer**: subject and details of the server identity's parent authority certificate,
- Its **Details**: serial number of the certificate, version, encryption and signature algorithms used, key type, key size, usage purposes for this identity and its certificate (Extended Key Usage - EKU).
- Its **Aliases**: FQDNs that may have been added when the identity was created.

Revocation (CRL) tab

- The URLs of the parent authority's **CRL distribution points**,
- The URLs of **OCSP servers** if OCSP is used in certificate renewal.

Importing a file

Files that contain one or several of the following items can be imported:

- Certificate(s),
- Private key(s),
- CRL,
- CA,
- CSR (Certificate Signing Request).

Importing a file

1. Click on **Add**.
2. Select **Import a file**.
3. In the **File to import** field, click on the icon to browse your computer and select the file.
4. The firewall will automatically detect the **File format**. If this is not the case, select the appropriate format (**P12**, **DER** or **PEM**).
5. If the file is a PKCS#12 (P12 extension), enter the **Password** that protects the file.
6. Indicate **What to import** from the file (if the file contains several items of different types, you can select only one type).
7. If the items to be imported are already in your PKI, select **Overwrite existing content in the PKI**.
8. When the firewall has a TPM that has been initialized, select the checkbox **Protect this identity with the TPM** to protect the identity's private key with the TPM.
9. Click on **Import**.

If the imported items are authorities, identities or certificates, they will automatically be added to the tree.

When you scroll over these items, the **Type** field in the tool tip will indicate that these are imported items.

Revoking an authority, sub-authority or certificate

The **Revoke** button makes it possible to delete the PKI on authorities and sub-authorities, or add certificates to the CRL of an authority to indicate that such certificates are no longer trusted.

Only the authority set as the default authority on the firewall cannot be revoked.

When a root authority is revoked, its CRL will also removed from the firewall.

When a parent authority or sub-authority is revoked, all these certificates will be revoked and removed during the same operation.

Revoking an authority

1. Select the authority to be revoked from the list on the left.
2. Click on **Revoke**.
3. Enter the **CA passphrase** of the authority or sub-authority.
4. You can select a **Reason** for the revocation in the drop-down list.
   This reason will be shown in the CRL of the parent authority of the revoked entity.
5. Select the **Format of the CRL export file**:
   - Base64 format (PEM),
   - Binary format (DER).

6. Click on **Apply**.
7. Click on the link that appears to download and save the CRL on your workstation.

Revoking a sub-authority or certificate

1. Select the sub-authority to be revoked from the list on the left.
2. Click on **Revoke**.
3. Enter the **CA passphrase** (password of the sub-authority).
4. Enter the **Root CA passphrase** of the parent sub-authority.
5. You can select a **Reason** for the revocation in the drop-down list.
   This reason will be shown in the CRL of the parent authority of the revoked sub-authority.
6. Select the **File format** of the CRL export:
   - Base64 format (PEM),
   - Binary format (DER).
6. Click on **Apply**.
7. Click on the link that appears to download and save the CRL of the sub-authority on your workstation.

Revoking a certificate

1. Select the certificate to be revoked from the list on the left.
2. Click on **Revoke**.
3. Enter the **CA passphrase** (password of the authority that issued the certificate).
4. You can select a **Reason** for the revocation in the drop-down list.
   This reason will be shown in the CRL of the parent authority of the revoked sub-authority.
5. Select the checkbox **Export CRL after revocation** if you wish to keep a copy of the CRL.
6. In this case, select the **File format** of the CRL export:
   - Base64 format (PEM),
   - Binary format (DER).
6. Click on **Apply**.
7. If you have chosen to export the CRL, a window will open with a link to download the CRL export file.

Creating, renewing or removing a CRL

When an authority or sub-authority is added to the PKI, its Certificate Revocation List (CRL) must be created.

Likewise, even though a CRL automatically updates on a regular basis, it may be necessary to renew it manually after revoking certificates that were signed by the authority that owns the CRL.

Creating a CRL

1. In the list on the left, select the authority or sub-authority for which the CRL needs to be created.
2. Click on **Actions**.

3. Select **Create CRL**.
   A dialog box opens.
4. Enter the password of the authority or sub-authority.
5. In the **CRL export** section, check or uncheck **Export CRL after revocation** depending on your requirements.
   If this checkbox is selected, choose the **File format** for the export:

- **Base64 format (PEM)**,
- **Binary format (DER)**.

6. Click on **Apply**.
7. If you have chosen to export the CRL, a window will open with a link to download the CRL export file.

Renewing a CRL

1. In the list on the left, select the authority or sub-authority for which the CRL needs to be renewed.
2. Click on **Actions**.
3. Select **Renew CRL**.
   A dialog box opens.
4. Enter the password of the authority or sub-authority.
5. In the **CRL export** section, check or uncheck **Export CRL after revocation** depending on your requirements.
   If this checkbox is selected, choose the **File format** for the export:

- **Base64 format (PEM)**,
- **Binary format (DER)**.

6. Click on **Apply**.
7. If you have chosen to export the CRL, a window will open with a link to download the CRL export file.

Removing a CRL

1. In the list on the left, select the authority or sub-authority for which the CRL needs to be removed.
2. Click on **Actions**.
3. Select **Remove CRL**.
   A dialog box opens.
4. Confirm by clicking on **OK**.

Removing the private key of an identity (while keeping the certificate)

After an identity - user, server or smart card - has been created on the firewall and issued to the end user (in general, in an encrypted PKCS#12 container), for security and confidentiality reasons, you may want to delete the private key of the identity to avoid keeping a copy on the firewall.

To remove the private key of an identity:

1. Select the identity from the list on the left.
2. Click on **Actions**.
3. Select **Remove private key**.
   A message will appear confirming its removal.

Defining a default authority or sub-authority

To define an authority or sub-authority as the default authority:

1. Select the authority or sub-authority from the list on the left.
2. Click on **Actions**.
3. Select **Set as default**.
   A dialog box opens.
4. Confirm by clicking on **OK**.

Downloading a certificate

The certificate of an authority, sub-authority or identity may be exported with this feature.

The generated file may be in these formats:

- PEM (ASCII format - Base64 encoding),
- DER (binary).

To download a certificate:

1. Select the authority, sub-authority or identity from the list on the left.
2. Click on **Download.**
3. Select **Certificate** then the format of the file.
4. Click on the link to download the file containing the certificate.

Downloading an identity

User, server or smart card identities can be downloaded with this action.

The generated file may be in these formats:

- PEM (ASCII format - Base64 encoding),
- DER (binary),
- P12 (encrypted binary).

To download an identity:

1. Select the identity from the list on the left.
2. Click on **Download.**
3. Select **Identity** then select the format of the export file (PEM, DER or P12).
4. Set the **password** that will protect the private key included in the export file.
5. **Confirm** the password.
   A progress bar will indicate the strength of the password.
6. Click on **Download certificate** (format).
7. Click on the link to download the file containing the identity.

Downloading a CRL

The CRL of an authority or sub-authority may be downloaded with this action.

The generated file may be in these formats:

- PEM (ASCII format - Base64 encoding),
- DER (binary).

To download a CRL:

1. Select the authority or sub-authority from the list on the left.
2. Click on **Download.**
3. Select **CRL** then the format of the file.
4. Click on the link to download the file containing the CRL.

CLI CONSOLE

SNS firewalls provide a command line interface (CLI) that uses a set of proprietary commands. The commands are available via a shell and make it possible to configure and monitor all firewall features.

The CLI shell can be accessed via a secure protocol, NSRPC (*NETASQ Secure Remote Procedure Call*), either locally on the firewall in the **System > CLI Console** module, or remotely from a host by using dedicated Windows and Linux executable files.

The **CLI console** module on the firewall consists of two parts:

- The list of commands in the upper part of the window, which is a text section;
- A data entry section at the bottom of the window.

Commands entered can be saved using the "Save" button located in the upper banner of the web administration interface. This feature must be enabled beforehand in Preferences.

List of commands

By default, the screen shows the main commands that can be executed. Some commands may involve others. To view all commands, run the command of your choice. The list will display the additional commands included in it.

You can also use the `HELP` argument with a command to display help on its arguments. For example:

```
CONFIG HELP
```

To obtain the full list of executable commands, refer to the CLI/Serverd commands reference guide.

Data entry section

In the data entry section, write the command that you wish to execute.

You can browse through the various commands that have already been executed by using the Up/Down buttons on the keyboard. Command history is stored and re-used every time the web application is launched.

Clear display	This button makes it possible to erase the current display on the CLI console.
Launch	This button makes it possible to launch the command that was entered. You can also press Enter on the keyboard to execute the command.
Multiline mode	Select this checkbox to run a command block. This command block may, for example, be generated from a recorded sequence of commands (**Record commands** button).
Stop if error	This checkbox is available only if multiline mode has been enabled. Select this checkbox to interrupt the command sequence as soon as the first error is encountered.

CONFIGURATION

The configuration screen consists of three tabs:

- **General configuration**: defines the firewall's characteristics (name, language, keyboard, etc.), cryptographic settings, date and time, password policy and NTP servers.
- **Firewall administration**: configures access to the firewall's administration interface (listening port, protection from brute force attacks, etc.) and remote access via SSH.
- **Network settings**: enables or disables IPv6, and the configuration of the proxy server and DNS resolution.

General configuration tab

> **NOTE**
> Refer to the section Allowed names to find out which characters are allowed and prohibited in various fields.

General configuration

Firewall name	This name is displayed in the firewall's main window and is used in alarm e-mails sent to the administrator. It can also be used as the DNS name of the captive portal if it was enabled and the option **Use firewall name** was selected. The maximum supported length of the firewall name is 127 characters.
Node name (HA)	This name can be particularly useful in a high availability configuration, as it allows you to easily identify the cluster member to which you are connected (web administration interface or SSH console). By default, this name is not defined (value: **none**).
Firewall language (logs)	Choice of language that the firewall uses for logs, syslog and the CLI configuration. The available languages are: **French** and **English**.
Keyboard (console)	Type of keyboard that the firewall supports. The available languages are: **English, French, Italian, Polish or Swiss.**

Cryptographic settings

Enable regular retrieval of certificate revocation lists (CRL)	If this option is selected, every 6 hours, the firewall will check the validity of each CRL downloaded from the distribution points that were specified in the PKI. When a CRL is close to its expiry date or has expired, an alarm will then be generated.

Enable "*Diffusion Restreinte* (DR)" 2021 version compliance mode

The **Enable "*Diffusion Restreinte* (DR)" 2021 version compliance mode** option forces the firewall to comply with the ANSSI's (French national information security agency) recommendations on the use of coprocessors and cryptographic accelerators on products to be qualified. It is an imperative on networks that fall under the "Restricted" classification.
This mode relies in particular on the use of software versions for asymmetric and symmetric cryptographic algorithms and random key generation algorithms. As for symmetric encryption algorithms, "AES-NI" instructions available on certain products are exempt as they are made up only of "simple acceleration instructions" of certain cryptographic operations.

When "ANSSI Diffusion Restreinte (DR)" mode is enabled in SNS 5.0.3 EA, the following will occur:

- IPsec: only certificate-based authentication is allowed.
- IPsec: the certificates used (from the end user certificate to the common trusted CA) must comply with the following specifications: ECDSA or ECSDSA signature on an SECP or Brainpool curve, SHA256 as the hash algorithm, and key size of 256 bits.
- IPsec: the module will check whether the firewall is using version 2 of the IKE protocol.
- IPsec: the module will check whether the **Peer ID** has been entered.
- IPsec: the module will check whether the encryption algorithms used belong to DH19 and DH28 groups (SECP and Brainpool 256).
- IPsec: the module will check whether the encryption algorithm used is either AES_GCM_16 (AEAD: Authenticated Encryption with Associated Data; AES_GCM_16 is therefore not associated with any authentication algorithm), or AES_CTR, which must be associated with SHA256.
- IPsec: the verification of certificate revocation must be enabled.
- IPsec: the size of the anti-replay window must not be zero.
- IPsec: the Pseudo-Random Function (PRF) algorithm must be SHA256.

> **IMPORTANT**
> If any of the above conditions is not met, the non-compliant IPsec configuration will be disabled and the following message appears:
> "ANSSI 'Diffusion Restreinte' mode disabled the non-compliant IPsec VPN configuration".
> The aim of this message is to prompt the administrator to modify the IPsec policy so that the configuration can be enabled.

- On firewalls equipped with Intel processors, the "ANSSI Diffusion Restreinte (DR)" mode will allow the use of the coprocessor's cryptographic hardware instruction sets. On firewalls equipped with other types of processors, the "ANSSI Diffusion Restreinte (DR)" mode will force such instruction sets to be disabled, causing performance to slow down during encryption.
- The "ANSSI Diffusion Restreinte (DR)" mode restricts the encryption suites that can be used on the authentication portal and on SSL VPN: only AES, SHA256, SHA384 and GCM encryption suites are allowed.

> **NOTE**
> Enabling the "ANSSI Diffusion Restreinte (DR)" mode requires rebooting the firewall.

Password policy

The indicated parameters apply to all passwords and pre-shared keys defined on the firewall (PPTP VPN, IPsec VPN, internal LDAP directory, etc.).

Minimum password length	Indicate the minimum number of characters required for each password defined on the firewall. **NOTE** The value defined by default is 1 for the purpose of compatibility in the event existing configurations are migrated to version 2.
Mandatory character types	Select the mandatory types of characters to be included in each password: • None: the password is not required to contain any alphanumeric or special characters, • Alphanumeric: the password must contain at least an alphabetical character and a number, • Alphabetical and special: the password must contain at least an alphanumeric character and a special character ('#', '@', etc…)
Minimum entropy	Entropy is a parameter that makes it possible to define the required robustness of a password. Higher entropy means that the password must be more robust. When it is defined, it will be factored into the calculation of randomly generated passwords, e.g., for temporary accounts, as well as manually defined passwords. Entropy takes into account the length of the password and the number of different characters in the password. The formula to calculate it is as follows: Entropy = (Length of password)*(Log(Number of different characters in the password)/Log(2)). The entropy value suggested by default is: 20. When its value is 0, entropy will be ignored when passwords are automatically generated or manually defined.

Date/Time settings

Manual mode	With this option, the firewall's date and time can be manually set.
Synchronize with your machine	This option makes it possible to set the firewall's date and time according to your computer's settings.
Synchronize firewall time (NTP)	This option makes it possible to synchronize the firewall's local clock through NTP (*Network Time Protocol*) servers. Complete this configuration by referring to **List of NTP servers** and **List of NTP keys**.
Date	This field appears only if the **Manual mode** option was selected. Select the desired date from the calendar.
Time	This field appears only if the **Manual mode** option was selected. Enter the desired time in *HH:MM:SS* format.
Time zone	Time zone defined for the firewall (GMT by default). The firewall must be restarted if the time zone is changed.

> **NOTE**
> The date and time set on your Stormshield Network firewall are important: they allow you to locate events in the log files. They are also useful in scheduling configurations.

List of NTP servers

> **IMPORTANT**
> The NTP servers used must be compatible with NTPv4.

This grid appears only if the option **Synchronize firewall time (NTP)** was selected.

NTP servers (host or group-address range) (max 15)	Shows the NTP servers used to synchronize the firewall's local clock. To add an NTP server, click on **Add** and select from the drop-down list the object representing the NTP server that you wish to add. If this object does not exist, click on the object creation icon to create it. To delete an NTP server from the list, select it and click on **Delete**.
Authentication key (ID)	You can enter a key if access to an NTP server requires one for authentication. In this field, select an authentication key from the list of NTP keys already created. Each ID is associated with a value representing the NTP authentication key. To create a new key ID, or to view the list of NTP keys already created, refer to **List of NTP keys**.

List of NTP keys

This grid appears only if the option **Synchronize firewall time (NTP)** was selected.

Authentication key (ID)	Shows the list of NTP authentication keys. These IDs can be selected in the **Authentication key (ID)** column in the **List of NTP servers**. To add an NTP key ID, click on **Add** and give it a unique ID between 1 and 15 inclusive. To delete an ID from the list, select it and click on **Delete**.
Value	Shows the value of NTP keys. If you add a new NTP key ID, enter the value of its key in this field (maximum 8 characters). Double-click on an existing value to change it.
Key type	Shows the algorithm used for the NTP key. You can change this option by selecting the desired algorithm from the drop-down list.

Advanced properties

Idle timeout monitoring (*watchdog*)

Idle timeout timer (watchdog)	This device tests the activity of the firewall's system. This test is conducted on the: • Virtual firewall (EVA) software, • Physical firewall hardware and software. The frequency of tests is defined by this timeout. When the system is idle, this watchdog will reboot the firewall and raise a system event (24). To stop monitoring, select **Disable**.

Captive portal

Redirect to the captive portal	This option allows you to choose the name of the firewall used when generating URIs that redirect to the captive portal. There are four possible values: • Use firewall's IP address • Use firewall's name. This refers to the name indicated in the **Firewall name** field in the **General configuration** section or the firewall's serial number if no name was specified in this field. • Use the captive portal's certificate. This refers to the name of the firewall specified in the portal's certificate. • Specify a domain name (FQDN).
Domain name (FQDN)	Enter a fully qualified DNS name for the firewall (e.g.: firewall.company.org). This field can only be accessed when the **Specify a domain name (FQDN)** value was selected in the previous field.

Telemetry

> **NOTE**
> When the administrator who looks up this module is logged in with an account other than the *admin* (super administrator) account, this section will be grayed out and named **Telemetry (require admin privilege)**.

Allow usage data to be sent to Stormshield (anonymous)	When this checkbox is selected, your firewall will send usage data to Stormshield's cloud (over port 443) for statistics (list below). By sending such data, which is **completely anonymous**, you will be helping Stormshield to refine the parameters of the proxy's performance and the dimensions and restrictions on future hardware platforms and SNS versions.

List of usage data for statistics:

- Number of lines generated in each log file,
- Size of each log file,
- CPU consumption,
- Memory use,
- Number of connections managed by the proxy, by protocol,
- Number of degraded connections managed by the proxy, by protocol,
- Maximum number of simultaneous connections managed by the proxy, by protocol,
- Maximum number of simultaneous degraded connections managed by the proxy, by protocol,
- Number of objects in the object database, by type,
- Number of filter and NAT rules,
- Number of simultaneous connections through the firewall,
- Number of hosts known to the firewall,
- Number of authentications by type,
- Number of antivirus scans performed,

- Number of users connected for each authentication method,
- Number of TS agents connected,
- Statistics on memory consumption by sockets,
- Log partition usage information,
- Statistics on memory and CPU consumption by daemons,
- Information on whether the TPM is used,
- Statistics on the PKI (number of CAs, certificates and identities protected by the TPM),
- Number of URLs matching the "Compromised URLs" category,
- Information on whether the Extended Web Control (EWC) URL classification solution is used,
- Number of URL classification requests,
- Number of site-to-site IPsec tunnels configured and enabled in the active IPsec policy,
- Maximum number of site-to-site IPsec tunnels set up,
- Number of mobile IPsec tunnels configured and enabled in the active IPsec policy,
- Maximum number of mobile IPsec tunnels set up,
- Number of IKE v1 IPsec tunnels configured in the active IPsec policy,
- Number of IKE v2 IPsec tunnels configured in the active IPsec policy,
- Number of IPsec tunnels with pre-shared key authentication configured in the active IPsec policy,
- Number of IPsec tunnels with certificate authentication configured in the active IPsec policy,
- Number of IPsec tunnels with certificate and XAUTH authentication configured in the active IPsec policy,
- Number of IPsec tunnels with EAP-GTC authentication configured in the active IPsec policy,
- Number of IPsec tunnels with certificate and EAP-GTC authentication configured in the active IPsec policy,
- Number of entries in the TLS 1.3 cache,
- Number of entries with a timeout error in the TLS 1.3cache,
- Number of times the TLS 1.3 cache was purged after being filled up,
- Number of stop signals indicating that a process ended abnormally,
- Date of the last stop signal indicating that a process ended abnormally,
- SDD status data (number of hours powered up, wear rate, percentage of remaining life,
- Number of filter policy reloads since firewall startup,
- Status of asynchronous filter rule reloading mode,
- Number of mobile IPsec tunnels configured with a Key-Encapsulation mechanism (KEM) using an algorithm that is resistant to post-quantum attacks,
- Number of site-to-site IPsec tunnels configured with a KEM using an algorithm that is resistant to post-quantum attacks,
- Number of mobile IPsec tunnels set up with a KEM using an algorithm that is resistant to post-quantum attacks,
- Number of site-to-site IPsec tunnels set up with a KEM using an algorithm that is resistant to post-quantum attacks
- Number of GET requests on the REST API,
- Number of PUT / POST / DELETE requests on the REST API.

SSH command prompt

System node name	In this field, you can set an additional name that will be concatenated with the name of the firewall. The name of this system node 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 serial number of the firewall.

Bypass - Industrial firewalls

Industrial firewalls (SNi20 and SNi40 models)

To ensure service continuity in an industrial setting, SNi20 and SNi40 model firewalls are equipped with a hardware bypass function. When it is enabled, and if the firewall breaks down, it allows network traffic to pass through without being analyzed.

NOTES

- This mechanism cannot be enabled on firewalls in a high availability configuration,
- This mechanism can only be enabled on the first two interfaces of the firewall.

Operating and enabling bypass mode

Two of the firewall's operating modes are available:

- **Security** mode: this mode prioritizes network security and protection. The bypass mechanism cannot be enabled. This is the firewall's default operating mode.
- **Safety** mode: this mode prioritizes service continuity. The bypass mechanism will be enabled whenever the firewall breaks down or there is a power outage.

Whenever **Safety** mode is enabled, one of three types of bypass may be activated:

- **SystemOff** bypass: activated when the firewall experiences an electrical failure or when there is a power outage.
- **JustOn** bypass: it will be activated when the appliance is restarted and will then be disabled.
- **OnTimer** bypass: when the product has to handle too many connections, this bypass will be activated after a period defined in the configuration of Safety mode. Once the bypass is activated, the firewall administrator can then reset Safety mode.

IMPORTANT
The proper operation of network traffic must be verified immediately after a manual reset. The firewall will not recognize connections initiated during the active bypass phase and will reject them every time.

When bypass is activated, the firewall interfaces in question will be represented as follows:

Enable safety mode	When this option is selected, you will be enabling the firewall's bypass mechanism. All three activation modes will be automatically available.

Safety mode timeout	Select the period after which the **OnTimer** bypass must be activated. The various possible values are: • 1 min • 1 min 30 sec • 2 min • 2 min 30 sec • 3 min • 3 min 30 sec • 4 min
Reset safety mode	When the **OnTimer** bypass is activated, you can click on this button in order to disable it and return the firewall to **Safety** mode.

Firewall administration tab

Access to the firewall's administration interface

Allow the 'admin' account to log in	The *admin* account is the only account with all privileges and can connect without using certificates. Unselect this checkbox to disable the *admin* account's access to the firewall's administration interface. It will still have access to the firewall in SSH or in console mode. **IMPORTANT** This account must be considered "dangerous", given the extent of its configuration possibilities and the access privileges granted to it.
Listening port	This field represents the port on which administrators can access the administration interface (https, tcp/443 by default). You can create an additional listening port by clicking on the relevant icon. The new port must use TCP.
Configure the SSL certificate of the service	Click on this link to modify the certificate presented by the firewall's administration interface and authentication portal.
Maximum idle timeout (for all administrators)	Set the longest idle timeout allowed for all administrator accounts on the firewall before they are logged out. Individual administrator accounts can set a different maximum idle timeout in their preferences as long as it is shorter than the maximum timeout configured.
Enable protection from brute force attacks	Brute force attacks are defined by the repeated attempts to connect to the firewall, by testing all password combinations possible This protection applies to all connections for the purpose of firewall administration - connections to the web administration interface as well as SSH connections. Select this option to enable this protection.

Number of authentication attempts allowed	Maximum number of times an administrator can attempt to connect before being blocked (login/password error or case sensitivity, for example). By default, the number of attempts allowed is limited to 3. This field can only be accessed if the **Enable protection from brute force attacks** option is selected.
Freeze time (minutes)	Duration for which an administrator will not be able to log in the firewall after the number of failed attempts specified above. The duration cannot exceed 60 minutes. This field can only be accessed if the **Enable protection from brute force attacks** option is selected.

Access to firewall administration pages

Add	Select a network object from the drop-down list. It will be treated as an **Authorized administration host** that will be able to log on to the administration interface. This object may be a host, host group, network or address range.
Delete	Select the line to be removed from the list and click on **Delete**.

Disclaimer for access to the administration interface

Warning file	A disclaimer (warning text) can be added to the login page of the firewall's web administration interface, and will appear on the right of the authentication window. Click on **Got it** to enable this authentication window. The file containing the text of the disclaimer can be loaded onto the firewall using the file selector ... For a better layout, the text can be in HTML but must not contain JavaScript. Once the file has been saved on the firewall, its contents can be displayed using the button.
Deleting the warning file	This button allows you to delete the warning file loaded earlier on the firewall.

Remote SSH access

> **NOTE**
> The user must be connected with the *admin* account to modify parameters for remote access via SSH.

Enable SSH access	SSH (Secure Shell) is a protocol that allows users to log in to a remote host via a secure link. Data is encrypted between hosts. SSH also allows commands to be executed on a remote server. Selecting this option will enable access to the firewall via SSH from accounts declared as firewall administrators with the "Console (SSH)" permission and from the *admin* account. When this checkbox is not selected, no accounts can connect to the firewall via SSH. All connection attempts, successful or unsuccessful, will be logged.

Enable password access	When this checkbox is selected, all accounts declared as firewall administrators with the "Console (SSH)" permission and the *admin* account can connect to the firewall via SSH by using their password. When it is unselected, administrators must then use a private/public key pair to authenticate. This field can only be accessed if the **Enable SSH access** option is selected. **IMPORTANT** If the password for one or several administrator accounts allowed to connect via SSH contains non-ASCII characters (e.g., '€', 'à'), refer to the procedure Changing the character set to enable SSH connection with a password that contains non-ASCII characters described at the bottom of this page.
Use the nsrpc shell for administrators other than the admin account	When this checkbox is selected, all accounts declared as firewall administrators with the "Console (SSH)" permission use only the *nsrpc shell* interpreter when they open an SSH session on the firewall. Accessing the firewall in this way allows them to use the *CLI/Serverd* commands according to the privileges that they hold. When this checkbox is unselected, all accounts declared as firewall administrators with the "Console (SSH)" permission use the *nsrpc shell* interpreter by default. This does not apply to the *admin* account and it still benefits from the *shell* interpreter by default. **IMPORTANT** Accessing the *shell* interpreter firewall in this way grants unrestricted access equivalent to *super-administrator* access. Commands used in this type of access are not logged. This field can only be accessed if the **Enable SSH access** option is selected.
Listening port	This field represents the port on which administrators can access the firewall via SSH (ssh tcp/22 by default). You can create an additional listening port by clicking on the relevant icon. The new port must use TCP. This field can only be accessed if the **Enable SSH access** option is selected.

Recommendations

On the firewall

Recommendations:

- Use an ECDSA key to authenticate,
- To use the key past 2030, the lowest accepted group has to be Diffie-Hellman 15,
- Configure the following cryptographic suites in the file *ConfigFiles/System*:

```
[SSHCiphers]
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
aes256-ctr

[SSHKex]
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256

[SSHMACs]
hmac-sha2-256-etm@openssh.com
```

- Do not use *Mac-then-Encrypt* cryptography suites:

```
hmac-sha2-256
hmac-sha2-512
```

On the client workstation that connects to the firewall

We recommend configuring the cryptographic suite ecdsa-sha2-nistp256.

Changing the character set to enable SSH connection with a password that contains non-ASCII characters

If your password contains non-ASCII characters (e.g., '€', 'à'), to connect via SSH to a firewall in SNS version 4, which uses ISO-8859-15 character sets by default to store passwords, proceed as follows.

Option 1: change the character set on the SSH client to adopt ISO-8859-15

Windows workstation using the Putty SSH client

1. Select the session corresponding to the connection to the firewall.
2. Go to the **Windows** > **Translation** menu on the left.
3. In the **Remote Character Set** field, select **ISO-8859-15** as the value.

Unix system using a Gnome terminal

1. Go to the **Preferences** > **Profiles** menu.
2. Click on the "+" button to add a new profile.
3. Name the object (e.g., ISO).
4. In this profile's **Compatibility** tab, change the **Coding** field value to **ISO-8859-15**.
5. In the terminal's main window, right-click and select **Profiles** > *this_new_profile* (ISO in the example) to apply it,

Unix system using any UTF-8 terminal

After you have installed the *luit* utility, run the SSH connection with the following command:

```
luit -encoding ISO8859-15 ssh <login>@<FW_IP_address>
```

Option 2: change the character set on the firewall (the firewall needs to be restarted)

1. Temporarily change the password of the *admin* account to a password that does not contain any non-ASCII characters.
2. Connect to firewall in SSH using this new password.
3. Change the firewall's character set by using the command: `setconf /usr/Firewall/ConfigFiles/language Language PswdCharset UTF-8`.
4. Restart the firewall.
5. Change the password of the *admin* account again, by including non ASCII characters, if you prefer.
6. Check whether SSH connections to the firewall with an SSH client use the UTF-8 character set by default.

Network Settings tab

IPv6 support

ON / OFF	Set the switch to ON to enable IPv6 support on the firewall. To find out about the scope of application of IPv6 support and changes to the various modules in the administration interface, refer to the chapter IPV6 SUPPORT in this guide. **IMPORTANT** As this action is irreversible, you are advised to back up your configuration before enabling support. To revert to IPv4 support only, you will need to reset your configuration to its factory settings before you can restore the backup of this configuration. Reset your configuration by pressing the reset button if your appliance has one, or by using the "defaultconfig" CLI command in console mode.

Proxy server

ON / OFF	Set the switch to ON to enable the use of a proxy when the firewall accesses the Internet for Active Update and License Update services.
Server	This field makes it possible to specify the object corresponding to the server that the firewall will use as a proxy.
Port	This field allows specifying the port used by the firewall to contact the proxy.
ID	This field allows defining an ID that the firewall will use to authenticate with a proxy.
Password	Define a password that the firewall will need in order to access the proxy server.

DNS resolution

List of DNS servers used by the firewall

DNS servers allow the firewall to resolve (find out IP addresses based on a host name) objects or hosts configured in "Automatic" DNS resolution.

Add	When you click on **Add**, a new line will be added to the list of DNS servers. Choose an object from the drop-down list or create a new one.
Delete	Select the DNS server to be deleted and click on **Delete**. Do note that if you delete all the DNS servers defined in the table, the firewall will then use *Root DNS* servers. These servers are found in the DNS configuration file (*/usr/Firewall/Data/dns*).

CONFIGURING MONITORING

Monitoring curves and data are compiled based on logs saved on the firewall. Such logs will then be analyzed.

This screen is divided into 2 sections:

- Top: settings of the various refreshment times
- Bottom: a table listing throughout two tabs the network interfaces and QoS queues to be monitored.

Interval between refreshments

Maximum period displayed (in minutes)	This setting makes it possible to define the data period to be displayed for a curve. This period is expressed in minutes and may take on one of the following values: 15, 30, 45 or 60.
Curve refreshment time (in seconds)	This parameter allows defining the refreshment time of monitoring curves. This period is expressed in seconds and may take on one of the following values: 5, 10, 15 or 20.
Table refreshment time (in seconds)	This parameter allows defining the refreshment time of monitoring data set out on the tables. This period is expressed in minutes and may take on one of the following values: 1, 3, 5, 7 and 10.

Configuring interfaces, QoS queues and web services to be monitored

"Interface configuration" tab

It is possible to **Add** or **Delete** interfaces to be monitored by clicking on the corresponding buttons.

The table contains the following columns:

Name	Select the interface that needs to be monitored. The suggested interfaces are Ethernet, link aggregation, VLAN, Wi-Fi and modem interfaces (dialup).

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of monitored interfaces:

- Add,
- Remove.

"QoS configuration" tab

It is possible to **Add** or **Delete** QoS queues to be monitored by clicking on the corresponding buttons. These queues must be defined beforehand in the **Security policy** > **Quality of service** module.

The table contains the following columns:

Name	Select from the drop-down list the QoS queue that needs to be monitored.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of monitored queues:

- Add,
- Remove.

"Web service configuration" tab

It is possible to **Add** or **Delete** web services (standard or custom) to be monitored by clicking on the corresponding buttons.

The table contains the following columns:

Name	Select the web service that needs to be monitored from the drop-down list.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the grid of monitored web services:

- Add,
- Remove.

DASHBOARD

The dashboard provides an overview of the information relating to your firewall. It can be accessed at any time during the configuration of the firewall by clicking on the **Monitoring** tab in the upper banner, then on **Dashboard** in the menu on the left.

The dashboard consists of several widgets.

Network

The **Network** widget provides a graphical representation of the interfaces on an SNS firewall:

- The number of interfaces available on the firewall is shown (maximum 32),
- The interfaces used appear in green,
- When Safety mode is enabled (bypass mechanism ready to be triggered), interface numbers on bypass segments appear in an orange circle,
- When the bypass mechanism has been triggered, interfaces on bypass segments appear in orange with a two-way arrow that links them:

A tooltip containing information about each interface is available.

The following information is given:

Interface	Name of the in, out or dmz interface used.
Address	IP address(es) and subnet mask.
Network packets	The number of Accepted, Blocked, Fragmented, TCP, UDP and ICMP packets.
Blocked	The number of packets blocked coming from this interface.
Traffic received	The total and individual breakdown of TCP, UDP and ICMP packets received.
Traffic sent	The total and individual breakdown of TCP, UDP and ICMP packets sent.
Current incoming throughput	Current incoming throughput
Current outgoing throughput	Current outgoing throughput
Safety/Bypass mode activated	This value is only available for firewalls equipped with the bypass function and is only shown when Safety mode is enabled. The possible values are "Safety mode enabled" (bypass mechanism not triggered) or "Bypass mode enabled" (bypass mechanism triggered).

Protections

This window contains the list of the latest alarms or system events raised by the firewall. Some columns can be hidden by default.

Date	Date and time of the last alarms raised, arranged from the most recent to least recent.
Message	Comment associated with the selected alarm. **Examples of possible messages** "Invalid ICMP message (no TCP/UDP linked entry)" (minor priority). "IP address spoofing (type=1)" (major priority).
Action	When an alarm is raised, the packet that set off the alarm will be subject to the action configured. The actions are "Block" or "Pass".
ID	Unique alarm ID.
Class	Class associated with the alarm.
Priority	3 levels of priority are possible and can be configured in the module Application Protection > Applications and Protections.
Source interface	Interface on which packets that set off the alarm arrived
Source port	Source port of packets that set off the alarm
Source	IP address that raised the alarm. For the purpose of compliance with the European GDPR (General Data Protection Regulation), IP addresses are now replaced with the term "Anonymized". To view them, you will need to obtain the "Full access to logs (private data)" privilege by clicking on **Logs: restricted access** and refreshing the data in the widget.
Destination Port	Destination port of packets that set off the alarm
Destination	Address of the destination host of the packet that set off the alarm.

Right-clicking on the line of an alarm or system event opens access to its configuration or help page:

Go to alarm configuration	This button shows the alarms in the **Applications and Protections** module. The *Advanced* column in the selected includes the **Advanced options** button, which makes it possible to send an e-mail when an alarm is raised, quarantining the host that caused the alarm to be raised or capturing the blocked packet.
Go to system event configuration	This button shows the system event in the **Notifications** > **System events** module. The *Advanced* column in the selected row includes the *Configure*button, which makes it possible to send an e-mail when an alarm is raised, quarantining the host that caused the alarm to be raised or capturing the blocked packet.
Open help to see details on this alarm	Select the desired alarm and click on this link, which will take you to a help page relating to the message (see above).

Properties

This window displays information relating to your firewall model and firmware version installed on your firewall or firewall cluster.

Name	Name given to the firewall (**Configuration** > **System** > **Configuration, General configuration** tab). This name is the firewall's serial number by default.
Model	Physical firewall model (e.g.: SN 210).

EVA model	This field appears only for virtual firewalls. It indicates the virtual firewall model corresponding to the physical resources allocated to the machine (EVA1, EVA2, EVA3, EVA4 or EVAU).
EVA memory capacity	This field appears only for virtual firewalls. This entry specifies the amount of memory currently allocated to the virtual machine. The minimum and maximum memory values that apply to this model are also indicated in brackets.
Number of CPUs on the EVA	This field appears only for virtual firewalls. This entry specifies the number of virtual processors (vCPU) currently allocated to the virtual machine. The minimum and maximum numbers of virtual processors that apply to this model are also indicated in brackets.
Serial number	Your Stormshield Network firewall's reference.
Version	Firmware version installed on the active partition of the firewall.
Version (passive firewall)	This field appears only when HA is enabled. Firmware version installed on the passive partition of the firewall.
Uptime	Duration for which the firewall has been running uninterrupted.
Date	Firewall date and time in real time.
Maintenance expiry date	Date on which maintenance of the firewall ends.
Maintenance expiry date (passive firewall)	This field appears only when HA is enabled. Date on which maintenance of the passive firewall ends.

Messages

This window lists system-related warnings and alerts.

Services

This window shows the status of some services on the firewall. In general, the color of the icon indicates the status of the service:

- Gray: service not available or not enabled on the firewall,
- Green: service running normally,
- Orange: the status of the service requires your attention,
- Red: the status of the service is critical,

The indicators taken into account for each health indicator are:

Management Center	Status of the connection between the firewall and the Stormshield Management Center server.
Active Update	Date on which the Active Update module was updated.
Sandboxing	Status of the connection to sandboxing servers

Cloud backup	Status of the connection to the Cloud Backup infrastructure when automatic backups are enabled.
Antivirus	Date on which antivirus definitions were updated. When it appears in orange, it means the lightweight antivirus database is being updated.
Reports	Activation status of reports Activation status of history graphs
Syslog server	Status of the connection to syslog servers configured on the firewall. If no syslog servers have been configured, click on this service to go to the corresponding configuration module (**Configuration** > **Notifications** > **Syslog** tab).
SSO Agent	Status of the connection to SSO agents configured on the firewall. If no SSO agents have been configured, click on this service to go to the authentication method configuration module.
Radius	Status of the connection to Radius servers configured on the firewall. If no Radius servers have been configured, click on this service to go to the authentication method configuration module.
TS agents	Status of the connection to TS agents configured on the firewall. If no TS agents have been configured, click on this service to go to the authentication method configuration module.
NTP	Status of the connection to NTP servers configured on the firewall. If the NTP protocol is not used, click on this service to go to the date and time settings module.
Telemetry	Status of the telemetry service. If the telemetry service has not been enabled, click on this service to go to the firewall's general configuration module.
Hostchecking (ZTNA)	Status of the service verifying the compliance of workstations that set up VPN tunnels (ZTNA). There are three possible statuses: • Gray: the ZTNA service has been disabled. • Green: the ZTNA service is enabled and has been configured. • Orange: the ZTNA service is enabled and has been configured in permissive mode. Click on this icon to go to the Client workstation verification (ZTNA) tab in the SSL VPN configuration module.

Health indicators

This window shows the status of the firewall's hardware resources. These statuses are color-coded:

- Gray: the module is not available, installed or enabled on your firewall,
- Green: the health indicators of the module are optimal,
- Orange: the value(s) of one or several indicators in the module require(s) your attention,
- Red: the value(s) of one or several health indicators in the module is/are critical.

Click on a health indicator to go directly to the corresponding monitoring or configuration module.

The indicators taken into account for each health indicator are:

HA link	Status of the link dedicated to HA.
Power supply	Status of the power supply modules if the firewall has any. The value of this field may be one of the following: "Power on", "Power off" or "Not detected" (missing or defective module).
Fan	Status of the fan if the firewall has one.
CPU	Percentage of your processor's use.
Memory	Status of memory used by the firewall. Various types of memory are analyzed: • **Host**: percentage of memory allocated to processing a host. • **Fragmented**: Percentage of memory allocated to processing fragmented packets. • **Connection**: Percentage of memory allocated to processing connections. • **ICMP**: percentage of memory allocated for ICMP. • **Logs**: percentage of memory used for data tracking. • **Dynamic**: percentage of dynamic memory on the intrusion prevention engine.
Disk	Status of the firewall's internal storage medium.
RAID	Status of data redundancy between the firewall's physical disks.
Temperature	Temperature of the firewall This indicator is not available on virtual machines.
Certificates	Validity of certificates and CRLs: • Certificate expiring in fewer than 30 days, • Certificate with a validity period in the future, • Certificate expired, • Certificate revoked, • CRL of a CA that has exceeded half of its lifetime or which will be reaching it in fewer than 5 days, • CRL of an expired CA.

TPM	Status of the TPM if the firewall has one. The value of this field may be one of the following: • Gray: the TPM has not been initialized. • Green: the TPM is initialized, running and protects at least one private key. • Orange: ○ The TPM is initialized, but it not protecting any private key. The value "*The TPM has been initialized, but is not in use*" confirms this status. ○ The TPM sealing policy has been changed. To apply it, reseal the TPM. The value "*TPM sealing required in order to apply the new TPM sealing policy*" confirms this status. • Red: ○ Tests on the TPM do not work (it no longer responds). ○ The TPM can no longer be accessed because the hash values of the trusted PCRs have changed. To refresh them, reseal the TPM. The value "*TPM sealing required in order to recover access to the TPM*" confirms this status. ○ Secure Boot is disabled. A warning in the **Messages** widget in the **Dashboard** confirms that the feature is disabled. Clicking on this indicator will redirect you to the Certificates and PKI module. For more information on sealing the TPM, refer to the technical note Configuring the TPM and protecting private keys in SNS firewall certificates.
SD-WAN	Status of all router objects and their gateways on the firewall. If none of the router objects monitor the status of their gateways, clicking on this indicator will take you to the configuration of network objects.

Pay As You Go

This box appears only on Elastic Virtual Appliances (EVA) that run on a Pay As You Go license model (billed according to usage).

This license model can be used:

- On a standalone basis if you are managing your virtual firewall within your Mystormshield private-access area,
- Through an approved partner who then manages your virtual firewall in his own Mystormshield private-access area.

Virtual machine enrollment	This entry specifies whether the virtual firewall has logged on correctly to the Pay As You Go cloud service in order to retrieve its identity, certificate and license.
Expiry date	Date on which the Pay As You Go license ends.
Web code	Whenever the machine is managed in standalone mode, this web code allows you to register it in your Mystormshield private-access area.
Client ID	This entry may display an optional login chosen when the installation image was imported, or when the partner created this image to identify the owner of the EVA.

Monitoring and configuration modules

The **Monitoring** and **Configuration** tabs in the upper banner make it possible to access the firewall's monitoring and configuration modules respectively. When a tab is opened, the menu on the left enables access to the various modules.

The module menu is laid out in the form of a retractable column (button) that contains several drop-down sections and a list of favorite modules.

Favorite modules

Favorite modules are listed in the drop-down menu under the icon .

To add a module to the list of favorites, click on the icon to the right of the title of the module.

Access to modules

Click on a module to access it. The display at the center of the page will then be refreshed with the contents of the open module.

If certain modules are grayed out in the menus, this may mean that:

- You have not subscribed to the required license and therefore cannot access them.
- The connected user does not have the necessary privileges for accessing these modules.

DHCP

The DHCP module is set out in a single screen, unless IPv6 support has been enabled. If this is the case, the DHCP module will consist of two separate tabs and its settings will be located in the *DHCPv4* tab.

General

ON / OFF	This button makes it possible to enable or disable the use of the DHCP protocol on the firewall (server or relay).

DHCP server	Sends various network parameters to DHCP clients.
DHCP Relay	The DHCP relay mode is to be used when client requests are to be redirected to an external DHCP server.

"DHCP server" service

The "DHCP server" service presents 4 configuration zones:

- **Default settings.** This menu is reserved for the configuration of DNS parameters (domain name, primary and secondary DNS servers) and the default gateway sent to DHCP clients.
- **Address range**. For each range, specify a group of addresses to be allocated to users. The address will be allocated for the duration determined in the advanced configuration.
- **Reservation**. The address allocated by the service stays the same for hosts listed in the column **Reservation**.
- **Advanced properties.** This menu allows enabling or disabling the automatic sending of the proxy configuration files for client hosts (WPAD: Web Proxy Autodiscovery Protocol). Additional servers can also be defined (WINS, SMTP, POP3, etc.) and the duration of the assignment of IP addresses distributed by the DHCP service can be customized.

Default settings

If the DHCP server option has been selected, global parameters can be configured here, such as the **domain name**, **DNS servers**, etc. that client hosts will use.

Domain name	Domain name used by DHCP client hosts for DNS resolution.
Gateway	The default gateway is the host that indicates the routes to use if the client does not know the destination address.
Primary DNS	Select the primary DNS server that will be sent to DHCP clients. This is a host object. If no objects are specified, the firewall's primary DNS server will be sent to them.
Secondary DNS	Select the secondary DNS server that will be sent to DHCP clients. This is a host object. If no objects are specified, the firewall's secondary DNS server will be sent to them.

Address range

In order for a DHCP server to provide IP addresses, an address pool from which the server can pick addresses has to be configured.

Action buttons

To add or delete address ranges, click on **Add** or **Delete**.

Add	Allows adding an address range. Select or create an IPv4 address range (**IP address range** network object).
Delete	Allows deleting one or several address ranges simultaneously.

The table shows the address ranges used by the DHCP server for distributing addresses to clients:

Address range	Select an **IP address range** network object from the drop-down list. The server will pick from this pool to distribute addresses to clients. If none of the firewall's protected interfaces has an IP address in the network hosting this range, a warning message will appear: "No protected interfaces match this address range".
Gateway	This field allows assigning a specific default gateway for DHCP clients. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Default gateway** field in the **Settings** section will then be used as the gateway for DHCP clients.
Primary DNS	This field allows assigning a specific main DNS server to DHCP clients. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Primary DNS** field in the **Default settings** section will then be used as the DNS server for the client.
Secondary DNS	This field allows assigning a specific secondary DNS server to DHCP clients. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Secondary DNS** field in the **Default settings** section will then be used as the DNS server for the client.
Domain name	This field allows indicating a specific domain name that will be used by the DHCP client for its DNS resolution. If no name is specified, the value "Default domain" will be displayed in this column. The domain name indicated in the **Domain name** field in the **Default settings** section will then be used for the client.

WARNING
Address ranges must not overlap. An address range belongs to a single bridge / interface.

Reservation

Even when a server that dynamically distributes IP addresses to clients is used, a specific IP address can be reserved for certain hosts. This configuration resembles static addressing, but nothing is configured on client workstations, thereby simplifying their network configuration.

Action buttons

To add or delete reserved addresses, click on **Add** or **Delete**.

Add	Allows adding a reserved IP address for a specific host network object.
Delete	Allows deleting an IP address reservation. If a reservation is cancelled, the host concerned will be assigned a new random address when it is renewed.

The table displays the host objects for which addresses have been reserved: these objects must always be defined using an IPv4 address and their MAC address. Indeed, the MAC address will be used as the client's unique ID for obtaining or renewing its reserved IP address.

Reservation	This field contains the name of the network object (host) that has a reserved IPv4 address.
Gateway	This field allows assigning a specific default gateway for each DHCP client that has reserved addresses. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Default gateway** field in the **Settings** section will then be used as the gateway for the client.
Primary DNS	This field allows assigning a specific main DNS server to each DHCP client using address reservation. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Primary DNS** field in the **Default settings** section will then be used as the DNS server for the client.
Secondary DNS	This field allows assigning a specific secondary DNS server to each DHCP client using address reservation. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Secondary DNS** field in the **Default settings** section will then be used as the DNS server for the client.
Domain name	This field allows indicating a specific domain name that will be used by the DHCP client for its DNS resolution. If no name is specified, the value "Default domain" will be displayed in this column. The domain name indicated in the **Domain name** field in the **Default settings** section will then be used for the client.

Advanced properties

Other types of servers to be used can be sent to client workstations through the DHCP service.

File name	Name of the boot and configuration file that the client workstation can retrieve at startup.
SMTP Server	The SMTP server is used for sending e-mails. A drop-down list allows selecting the host object that corresponds to this server.
POP3 server	The POP3 server is used for receiving e-mails. A drop-down list allows selecting the host object that corresponds to this server.
Next server	Address of the server that hosts the boot and configuration file for the client workstations specified in the **File name** field.

News Server (NNTP)	This field allows sending the news server's address to DHCP clients. This server provides the NNTP service, which allows clients to read Usenet news.
TFTP Server	The TFTP server is used for booting hosts remotely. This field (option 150: TFTP server address) can be used for starting up network devices such as routers, X-terminals or workstations without hard disks.
Distribute the Web proxy autodiscovery (WPAD) file	If this option has been selected, the DHCP server will distribute the Internet access configuration to DHCP clients through a PAC file (Proxy Auto Configuration). This file must be entered in the authentication settings (*Captive portal* tab in the menu **Configuration**>**Users**>**Authentication**). It can be made accessible from internal and/or eternal interfaces (*Internal interfaces* and *External interfaces* tabs in the menu **Configuration**>**Users**>**Authentication**).
Update DNS server entries	If this option has been selected, DNS servers will be dynamically updated when information contained in the DHCP server is modified.

Assigned lease time

Default (hour)	For the purpose of optimizing network resources, IP addresses are assigned for a limited period. You therefore need to indicate here the default duration for which hosts will keep the same IP address.
Minimum (hour)	Minimum duration for which hosts will keep the same IP address.
Maximum (hour)	Maximum duration for which hosts will keep the same IP address.

"DHCP relay" service

The "DHCP relay" service contains 2 configuration zones:

- **Settings**: this menu allows configuring the DHCP server(s) to which the firewall will relay DHCP requests from client hosts,
- **Listening interfaces on the DHCP relay service**: the network interfaces(s) on which the firewall listens for DHCP client requests.

Settings

DHCP server(s)	The drop-down list allows selecting a host object or group object containing hosts. The firewall will relay client requests to this or these DHCP server(s).

IP address used to relay DHCP queries	The IP address entered as the source in this field will be used for relayed queries. For example, this option would allow local users to benefit from the automatic configuration of the IP parameters of a remote DHCP server through an IPsec tunnel. This address has to belong to the local traffic endpoint in order to be recognized by the tunnel. This option is only available for a DHCPv4 service and via a VPN tunnel whose traffic endpoints have been configured in IPv4. **NOTE** This operating mode is only possible with an external DHCPv4 server; the firewall's DHCP service cannot be used. **NOTE** The tunnel's traffic endpoints have to be configured in IPv4 and the tunnel endpoints can be defined in either IPv4 or IPv6. If nothing is entered, the selection of the address will be automatic (selection of the IP address of the interface in front of the routing).
Relay DHCP queries for all interfaces	If this option has been selected, the firewall will listen for DHCP client requests on all its network interfaces. In this case, the table **Listening interfaces on the DHCP relay service** will be grayed out.

Listening interfaces on the DHCP relay service

In this section, indicate:

- The network interfaces through which the firewall will receive DHCP client requests,
- The network interfaces through which the firewall will contact the external DHCP server(s).

The DHCP relay service on the firewall can also listen on the interface used by the IPsec VPN in order to relay DHCP queries through these tunnels.

Listening interfaces must include the interfaces for listening to the client-side query as well as the interfaces for listening to the server-side response.

The DHCP server has to be configured in such a way that it can distribute IP addresses to clients that pass through the relay.

Action buttons

In order to add or delete listening interfaces, click on **Add** or **Delete**.

Add	Adds a row to the table and opens a drop-down list of the firewall's interfaces in order to select an interface.
Delete	Allows deleting one or several listening or outgoing interfaces.

DIRECTORIES CONFIGURATION

LDAP is a standard protocol that allows managing directories, i.e., accessing user databases on a network through the TCP/IP protocols.

Stormshield Network firewalls embed an internal LDAP database, which stores information relating to users who need to authenticate in order to use the firewall. In addition to this internal directory, the firewall can also be connected to up to four external LDAP bases located on remote hosts.

The Directory configuration module (accessible through the menu **Users > Directory configuration**) contains a wizard in the first page, offering you the choice of a directory and initializing it.

- Connecting to a Microsoft Active Directory
- Connecting to an external LDAP directory
- Connecting to a PosixAccount external LDAP directory
- Creating an internal LDAP

Depending on your selection, the next step will vary, as the configuration of the external LDAP requires more information.

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

Depending on the model of your firewall, a maximum number will determine how many users can be authenticated simultaneously. This restriction is explained in the section Users.

The configuration of each of these directories consists of 3 steps. Select the LDAP database you wish to create by clicking on the relevant option.

For a secure connection (LDAPS) to be set up between the firewall and the directory, the server that hosts the external directory must support and use one of the following cipher suites:

- TLS_AES_128_GCM_SHA256 (0x1301) (TLS1.3),
- TLS_CHACHA20_POLY1305_SHA256 (0x1303) (TLS1.3),
- TLS_AES_256_GCM_SHA384 (0x1302) (TLS1.3),
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b),
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f),
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e),
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9),
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8),
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa),
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c),
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030),
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f),

ECDHE-based cipher suites must use elliptic curves that belong to one of the groups listed below:

- x25519 (0x001d),
- secp256r1 (0x0017),
- x448 (0x001e),

- secp521r1 (0x0019),
- secp384r1 (0x0018).

Main window

This module contains the list of the various directories configured on the firewall.

It is divided into 2 distinct zones:

- Left: the list of directories and action bar.
- Right: details of the configuration and structure of the selected directory.

Possible actions

Add a directory button

Click on this button to launch the wizard that lets you create a new LDAP directory.

Action drop-down list

Scroll down this list to see the various possible actions:

- **Remove** selected directory,
- **Set** the selected directory as the default the **default** directory,
- **Check the connection** to the selected directory,
- **Check usage** of the selected directory in the firewall configuration.

Creating an internal LDAP

This type of directory is hosted by your Stormshield Network multi-function firewall, and your information is stored in it once the LDAP directory is created.

Step 1: Selecting the directory

As indicated above, the LDAP database option has to be selected in order to confirm your choice. This is the first step in the configuration of a directory.

Select the option **Connect to an internal LDAP directory** and click on **Next**.

Step 2: Accessing the directory

In this second step, you will need to enter general information concerning the LDAP database that you wish to create. The information entered here will reappear in your firewall's LDAP directory schema. The name of your directory will be automatically created based on the value of the **Organization** and **Domain** fields.

Organization	Name of your company (e.g.: mycompany).
Domain	The extension of your domain name (e.g.: fr, eu, org, com, etc.).

Password	Defines the password for LDAP administration.
Confirm password	Confirmation of the LDAP administration password that you have just entered in the previous field.
Password strength	This progress bar indicates your password's level of security: "Very Weak", "Weak", "Medium", "Good" or "Excellent". You are strongly advised to use uppercase letters and special characters.
Password hash	Algorithm that encrypts user passwords.

> **NOTE**
> Only the password and hash method can be modified later, after you have configured your internal LDAP.

Click on **Finish** to display the internal LDAP directory screen.

Internal LDAP directory screen

Once the configuration of the LDAP directory is complete, you will arrive at the internal LDAP screen which sets out the following items:

Configuration

Enable user directory	This option allows you to start the LDAP service. If this option is not selected, the module will be inactive.
Organization	This field will contain the name of your company, entered earlier.
Domain	This field will contain your company's domain.
ID	The login that will allow you to connect to the internal LDAP base.
Password	The password allowing the firewall to connect to the directory. This password can be modified.
Confirm password	Confirmation of the LDAP administration password that you have just entered in the previous field.
Password strength	This field indicates your password's level of security: "Very Weak", "Weak", "Medium", "Good" or "Excellent". You are strongly advised to use uppercase letters and special characters.

Access to the internal LDAP

Enable unencrypted access (PLAIN)	Data entered will not be encrypted, but displayed in plaintext.
Enable SSL access (SSL certificate presented by the server)	In order to set up SSL access, you will need to select a certificate server already generated by your root CA, or an imported certificate. The icon indicates certificates with a TPM-protected private key. For more information on the TPM, see the section Trusted Platform Module.

Advanced properties

Use the firewall account to check user authentication on the directory	When this option is selected, the firewall will intercept the authentication request, which is submitted using the account that holds all privileges on the directory: cn=NetasqAdmin. If it is not selected, the request will be submitted in the directory itself.
Allow nested groups	Selecting this option allows you to create groups inside other user groups.
Password hash	Algorithm that encrypts user passwords. A caption will specify whether the algorithm is obsolete.

Connecting to an external LDAP directory

The external LDAP is a directory to which your Stormshield Network multi-function firewall will connect.

Step 1: Selecting the directory

Select the LDAP base of your choice. This is the first step in the configuration of this directory.

Select the option **Connect to an external LDAP directory** and click on **Next**.

Step 2: Accessing the directory

Domain name	Name that identifies the internal LDAP directory when several directories are defined on the firewall. In a configuration containing multiple directories, this name will be needed in addition to the user's login for authentication (login@domain_name). You are therefore strongly advised to enter a DNS domain name in this field. **EXAMPLE** company.com
Server	Select an object corresponding to your LDAP server from the drop-down list. This object must be created prior to this step and must reference the IP address of your LDAP server.
Port	Enter the listening port of your LDAP server. The default port is: 389.
Root domain (Base DN)	Enter the root domain (DN) of your directory. The DN represents the name of an entry, in the form of a path to it, from the top to the bottom of the tree structure. The field can be entered using the name of the Root Domain (DN). **EXAMPLE** LDAP domain is “company.com” so my Root domain (Base DN) should be “dc=company,dc=com”
Read-only access	If this option is selected, you will not be able to perform any actions in write mode on the external LDAP directory.

Anonymous connection	This option makes it possible to log on to the external LDAP directory without entering any username or password. The LDAP server must of course authorize anonymous connections. If this option is selected, the fields **Username** and **Password** will become inactive (grayed out).
ID	An administrator account allowing the firewall to connect to your LDAP server and make changes (reading and writing privileges) to certain fields. We recommend that you create a specific account for the firewall and assign privileges to it only in the necessary fields. **EXAMPLE** cn=id This field will be inactive when the **Anonymous connection** checkbox has been selected.
Password	The password associated with the ID for you to connect to the LDAP server. The key icon ( ) allows you to view the password in plaintext to check that it is correct. This field will be inactive when the **Anonymous connection** checkbox has been selected.
Password hash	Select the algorithm to be used for hashing user passwords.

Click on **Finish** to display the external LDAP directory screen.

External LDAP directory screen

Once the configuration of the LDAP directory is complete, you will arrive at the external LDAP screen which sets out the following items:

"Configuration" tab

The page that appears presents a window that summarizes the information entered for your external LDAP and various services concerning access to your directory.

Remote directory

Enable user directory	This option allows you to start the LDAP service. If this option is not selected, the module will be inactive.
Server	This field contains the name of the server that you entered in the previous page.
Port	This field contains the listening port that you selected in the previous page.
Root domain (Base DN)	The root domain of your directory as it was defined when it was created. **EXAMPLE** dc=company,dc=org
ID	The login name allowing the firewall to connect to your LDAP server.
Password	The password created in the firewall to connect to the LDAP server.

Secure connection (SSL)

For a secure connection (LDAPS) to be set up between the firewall and the directory, the server that hosts the external directory must support and use one of the following cipher suites:

- TLS_AES_128_GCM_SHA256 (0x1301) (TLS1.3),
- TLS_CHACHA20_POLY1305_SHA256 (0x1303) (TLS1.3),
- TLS_AES_256_GCM_SHA384 (0x1302) (TLS1.3),
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b),
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f),
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e),
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9),
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8),
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa),
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c),
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030),
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f),

ECDHE-based cipher suites must use elliptic curves that belong to one of the groups listed below:

- x25519 (0x001d),
- secp256r1 (0x0017),
- x448 (0x001e),
- secp521r1 (0x0019),
- secp384r1 (0x0018).

Enable SSL access	This option makes it possible to check your digital certificate generated by the firewall's root CA. Information is encrypted in SSL. This method uses port 636. Public access to the LDAP is protected by the SSL protocol. **NOTE** If this option is not selected, access will not be encrypted.
Check the certificate with a root certification authority	During a connection to the LDAP database, the firewall will check that the certificate was issued by the certification authority specified below.
Select a trusted Certification Authority	This field allows you to select the CA that will be used to verify the server certificate issued by the LDAP server, to guarantee the authenticity of the connection to this server. **NOTE** This option will be grayed out by default if the two options above were not selected.

Advanced properties

Backup server	This field makes it possible to define a replacement server if the main server cannot be reached. You can select it from the list of objects suggested in the drop-down list.
Port	Enter the listening port of your backup LDAP server, which may be different from the listening port on the main server. The default port is: 389 (ldap).
Use the firewall account to check user authentication on the directory	When this option is selected, the firewall will use the identifier declared during the creation of the directory to verify a user's privileges with the LDAP server when the user authenticates. Otherwise, the firewall will use the user's account to conduct this check.
Do not add the Domain Name (Base DN) to the identifier (ID).	Select this checkbox if you do not want user IDs retrieved by the firewall from this directory to be in login@domain format (e.g., john.doe@mydomain.com if the selected directory manages users from the mydomain.com domain).
Allow nested groups	Select this checkbox if you want groups included in other groups to be imported from the selected directory.

Click on **Apply** to confirm your configuration.

"Structure" tab

Read-only access

User selection filter	When using the firewall in interaction with an external database, only users that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = InetOrgPerson.*
User group selection filter	When using the firewall in interaction with an external database, only user groups that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = GroupOfNames.*

You are accessing the directory in read-only mode. The creation of users and groups will not be allowed: If this option is selected, you will not be able to perform any actions in write mode.

Mapped attributes

Apply a model: This button offers to apply one of three LDAP servers to define your attributes:

- OpenLDAP: LDAP server.
- Microsoft Active Directory (AD): LDAP directory services for Windows operating systems.
- Open Directory: directory of websites under an Open Directory license

External directory attributes	This column represents the value given to the attribute in the external directory. **EXAMPLES** *Cn= COMPANY* *telephoneNumber= +33 (0)3 61 96 30* *mail = salesadmin@company.com*

Advanced properties

Password hash: The password encryption method for new users.

Some authentication methods (such as LDAP) must store the user's password in the form of a hash (result of a hash function applied to the password) which prevents the password from being stored in plaintext.

You must select your desired hash method from the following:

SHA	"Secure Hash Algorithm". This encryption method makes it possible to set up a 160-bit or 160-byte character string (called a "key") which will be used as a reference for identification.
MD5	"Message Digest". This algorithm allows you to check the integrity of data entered, by generating a 128-bit MD5 key. **REMARKS** As this method uses fewer bytes and as such has a lower level of security, it is less robust against attacks.
SSHA	"Salt Secure Hash Algorithm". Based on the same principle as SHA, but contains a password salting function in addition, which consists of adding a bit sequence to the data entered in order to make them less legible. **NOTE** This variant of SHA uses a random value to diversify the password's fingerprint. Two identical passwords will therefore have two different fingerprints. The encryption method is the most secure and strongly recommended.
SMD5	"Salt Message Digest". Based on the same principle as MD5, with the addition of the password salting function.
CRYPT	The password is protected by the CRYPT algorithm, derived from the DES algorithm which allows block encryption using 56-bit keys. This method is not highly advised, as it has a relatively low level of security.
None	No password encryption, meaning it is stored in plaintext. **WARNING** This method is not recommended, as your data will not be protected.

User branch	Enter the name of the LDAP branch for storing users. **EXAMPLE** ou=users
Group branch	Enter the name of the LDAP branch for storing user groups. **EXAMPLE** ou=groups

Certification authority branch	This field defines the location of the CA on the external LDAP base. This location is used especially when searching for the CA used in SSL. **NOTE** This field does not necessarily need to be configured. In this case, to enable SSL authentication, specify the CA in the list of trusted CAs in the SSL configuration (see **Users** > **Authentication** module > **Available methods** tab: the authentication method **Certificate (SSL)** must be added and the CA indicated in the right column "Certification authorities (C.A)").

Click on **Apply** to confirm your configuration.

Connecting to a PosixAccount external LDAP directory

Step 1: Selecting the directory

Select the LDAP base of your choice. This is the first step in the configuration of this directory.

Select the option **Connect to a PosixAccount external LDAP directory** and click on **Next**.

Step 2: Accessing the directory

Domain name	Name that identifies the internal LDAP directory when several directories are defined on the firewall. In a configuration containing multiple directories, this name will be needed in addition to the user's login for authentication (login@domain_name). You are therefore strongly advised to enter a DNS domain name in this field.
Server	Select an object corresponding to your LDAP server from the drop-down list. This object must be created prior to this step and must reference the IP address of your LDAP server.
Port	Enter the listening port of your LDAP server. The default port is: TCP/389 (**ldap** object).
Root domain (Base DN)	Enter the root domain (DN) of your directory. The DN represents the name of an entry, in the form of a path to it, from the top to the bottom of the tree structure. The field can be entered using the name of the Root Domain (DN). **EXAMPLE** AD domain is "company.com" so my Root domain (Base DN) should be "dc=company,dc=com"
Anonymous connection	If this option is selected, the connection to the LDAP directory will not require the use of an identifier and its associated password. In this case, the identifier and password fields will be grayed out.

ID	An administrator account allowing the firewall to connect to your LDAP server and make changes (reading and writing privileges) to certain fields. We recommend that you create a specific account for the firewall and assign privileges to it only in the necessary fields. **EXAMPLE** cn=id
Password	The password associated with the ID for you to connect to the LDAP server. The key icon ( ) allows you to view the password in plaintext to check that it is correct.
Password hash	Select the algorithm to be used for hashing user passwords.

REMARKS
Connections to a *PosixAccount* external directory must be carried out in read-only mode. Users or groups therefore cannot be created from the firewall's web administration interface.

Click on **Finish** to display the external LDAP directory screen.

External LDAP directory screen

Once the configuration of the LDAP directory is complete, you will arrive at the external LDAP screen which sets out the following items:

"Configuration" tab

The page that appears presents a window that summarizes the information entered for your external LDAP and various services concerning access to your directory.

Remote directory

Enable user directory	This option allows you to start the LDAP service. If this option is not selected, the module will be inactive.
Server	This field contains the name of the server that you entered in the previous page.
Port	This field contains the listening port that you selected in the previous page.
Root domain (Base DN)	The root domain of your directory as it was defined when it was created. **EXAMPLE** dc=company,dc=org
ID	The login name allowing the firewall to connect to your LDAP server.
Password	The password created in the firewall to connect to the LDAP server.

Secure connection (SSL)

For a secure connection (LDAPS) to be set up between the firewall and the directory, the server that hosts the external directory must support and use one of the following cipher suites:

- TLS_AES_128_GCM_SHA256 (0x1301) (TLS1.3),
- TLS_CHACHA20_POLY1305_SHA256 (0x1303) (TLS1.3),
- TLS_AES_256_GCM_SHA384 (0x1302) (TLS1.3),
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b),
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f),
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e),
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9),
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8),
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa),
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c),
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030),
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f),

ECDHE-based cipher suites must use elliptic curves that belong to one of the groups listed below:

- x25519 (0x001d),
- secp256r1 (0x0017),
- x448 (0x001e),
- secp521r1 (0x0019),
- secp384r1 (0x0018).

Enable SSL access	This option makes it possible to check your digital certificate generated by the firewall's root CA. Information is encrypted in SSL. This method uses port 636. Public access to the LDAP is protected by the SSL protocol. **NOTE** If this option is not selected, access will not be encrypted.
Check the certificate with a root certification authority	During a connection to the LDAP database, the firewall will check that the certificate was issued by the certification authority specified below.
Select a trusted Certification Authority	This option allows you to select the CA that will be used to verify the server certificate issued by the LDAP server, to guarantee the authenticity of the connection to this server. **NOTE** This option will be grayed out by default if the two options above were not selected.

Advanced properties

Backup server	This field allows you to define a replacement server if the main server fails. You can select it from the list of objects suggested in the drop-down list. By clicking on the button **Test access to the directory** below it, a window will inform you that your main server is functional. Click on **OK**.
Port	Enter the listening port of your backup LDAP server, which may be different from the listening port on the main server. The default port is: 389 (ldap).
Use the firewall account to check user authentication on the directory	When this option is selected, the firewall will use the identifier declared during the creation of the directory to verify a user's privileges with the LDAP server when the user authenticates. Otherwise, the firewall will use the user's account to conduct this check.
Do not add the Domain Name (Base DN) to the identifier (ID).	Select this checkbox if you do not want user IDs retrieved by the firewall from this directory to be in login@domain format (e.g., john.doe@mydomain.com if the selected directory manages users from the mydomain.com domain).
Allow nested groups	Select this checkbox if you want groups included in other groups to be imported from the selected directory.

Click on **Apply** to confirm your configuration.

"Structure" tab

Read-only access

User selection filter	When the firewall is used to interact with an external database, only users that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = InetOrgPerson.*
User group selection filter	When the firewall is used to interact with an external database, only user groups that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = PosixGroup*.

You are accessing the directory in read-only mode. The creation of users and groups will not be allowed: since connections to external POSIX LDAP directories must be in read-only, this option will be automatically selected and grayed out.

Mapped attributes

Apply a model: This button offers to apply one of three LDAP servers to define your attributes:

- OpenLDAP: LDAP server.
- Microsoft Active Directory (AD): LDAP directory services for Windows operating systems.
- Open Directory: directory of websites under an Open Directory license

External directory attributes	This column represents the value given to the attribute in the external directory. For *PosixAccount* LDAP directories, the attribute **Stormshield member** will have the value *memberUid*.

Advanced properties

Password hash: The password encryption method for new users.

Some authentication methods (such as LDAP) must store the user's password in the form of a hash (result of a hash function applied to the password) which prevents the password from being stored in plaintext.

You must select your desired hash method from the following:

SHA	"Secure Hash Algorithm". This encryption method makes it possible to set up a 160-bit or 160-byte character string (called a "key") which will be used as a reference for identification.
MD5	"Message Digest". This algorithm allows you to check the integrity of data entered, by generating a 128-bit MD5 key. **REMARKS** As this method uses fewer bytes and as such has a lower level of security, it is less robust against attacks.
SSHA	"Salt Secure Hash Algorithm". Based on the same principle as SHA, but contains a password salting function in addition, which consists of adding a bit sequence to the data entered in order to make them less legible. **NOTE** This variant of SHA uses a random value to diversify the password's fingerprint. Two identical passwords will therefore have two different fingerprints. The encryption method is the most secure and strongly recommended.
SMD5	"Salt Message Digest". Based on the same principle as MD5, with the addition of the password salting function.
CRYPT	The password is protected by the CRYPT algorithm, derived from the DES algorithm which allows block encryption using 56-bit keys. This method is not highly advised, as it has a relatively low level of security.
None	No password encryption, meaning it is stored in plaintext. **WARNING** This method is not recommended, as your data will not be protected.

User branch	For *PosixAccount* external directories, this field is not available.
Group branch	For *PosixAccount* external directories, this field is not available.

Certification authority branch	This field defines the location of the CA on the external LDAP base. This location is used especially when searching for the CA used in SSL. **NOTE** This field does not necessarily need to be configured but in this case, in order for the SSL authentication method to work, the CA must be specified in the list of trusted CAs in the configuration of the SSL method. (See **Users** > **Authentication** module > **Available methods** tab: the authentication method **Certificate (SSL)** must be added and the CA indicated in the right column "Certification authorities (C.A)")

Click on **Apply** to confirm your configuration.

Connecting to a Microsoft Active Directory

Like internal and external directories, Active Directory offers the same user management features developed by Microsoft, using a *Windows* OS.

Step 1: Selecting the directory

Select the directory of your choice. This is the first step in the configuration of this directory.

Select the option **Connect to a Microsoft Active Directory** and click on **Next**.

Step 2: Accessing the directory

Domain name	Name that identifies the internal LDAP directory when several directories are defined on the firewall. In a configuration containing multiple directories, this name will be needed in addition to the user's login for authentication (login@domain_name). You are therefore strongly advised to enter a DNS domain name in this field.
Server	Select an object corresponding to your LDAP server from the drop-down list. This object must be created prior to this step and must reference the IP address of your LDAP server.
Port	Enter the listening port of your LDAP server. The default port is: 389.
Root domain (Base DN)	Enter the root domain (DN) of your directory. The DN represents the name of an entry, in the form of a path to it, from the top to the bottom of the tree structure. **EXAMPLE** The AD domain is "company.com", so the Root domain (Base DN) is "o=company,dc=com"

Login (user DN)	An administrator account allowing the firewall to connect to your LDAP server and make changes (reading and writing privileges) to certain fields. We recommend that you create a specific account for the firewall and assign privileges to it only in the necessary fields. **EXAMPLE** cn= Administrator,cn=users
Password	The password associated with the ID for you to connect to the LDAP server. The key icon ( ) allows you to view the password in plaintext to check that it is correct.
Password hash	Select the algorithm to be used for hashing user passwords.

Click on **Finish** to display the Microsoft Active Directory screen.

Microsoft Active Directory screen

"Configuration" tab

Once you have completed the configuration of the directory, you will arrive at the Active Directory which sets out the following items:

Enable user directory	This option allows you to start the LDAP service. If this option is not selected, the module will be inactive.
Server	This field contains the name of the server that you entered in the previous page.
Port	This field contains the listening port that you selected in the previous page.
Root domain (Base DN)	The root domain of your directory as it was defined when it was created. **EXAMPLE** o=company,dc=org
ID	The login name allowing the firewall to connect to your LDAP server. **EXAMPLE** cn= Administrator,cn=users
Password	The password created in the firewall to connect to the LDAP server.

Secure connection (SSL)

For a secure connection (LDAPS) to be set up between the firewall and the directory, the server that hosts the external directory must support and use one of the following cipher suites:

- TLS_AES_128_GCM_SHA256 (0x1301) (TLS1.3),
- TLS_CHACHA20_POLY1305_SHA256 (0x1303) (TLS1.3),
- TLS_AES_256_GCM_SHA384 (0x1302) (TLS1.3),
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b),
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f),

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e),
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9),
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8),
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa),
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c),
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030),
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f),

ECDHE-based cipher suites must use elliptic curves that belong to one of the groups listed below:

- x25519 (0x001d),
- secp256r1 (0x0017),
- x448 (0x001e),
- secp521r1 (0x0019),
- secp384r1 (0x0018).

Enable SSL access	This option makes it possible to check your digital certificate generated by the firewall's root CA. Information is encrypted in SSL. This method uses port 636. Public access to the LDAP is protected by the SSL protocol. **NOTE** If this option is not selected, access will not be encrypted.
Check the certificate with a root certification authority	During a connection to the LDAP database, the firewall will check that the certificate was issued by the certification authority specified below.
Select a trusted Certification Authority	This option allows you to select the CA that will be used to verify the server certificate issued by the LDAP server, to guarantee the authenticity of the connection to this server. **NOTE** This option will be grayed out by default if the two options above were not selected.

Advanced properties

Backup server	This field makes it possible to define a replacement server if the main server cannot be reached. You can select it from the list of objects suggested in the drop-down list.
Port	Enter the listening port of your backup LDAP server, which may be different from the listening port on the main server. The default port is: 389 (ldap).

Use the firewall account to check user authentication on the directory	When this option is selected, the firewall will use the identifier declared during the creation of the directory to verify a user's privileges with the LDAP server when the user authenticates. Otherwise, the firewall will use the user's account to conduct this check.
Do not add the Domain Name (Base DN) to the identifier (ID).	Select this checkbox if you do not want user IDs retrieved by the firewall from this directory to be in login@domain format (e.g., john.doe@mydomain.com if the selected directory manages users from the mydomain.com domain).
Allow nested groups	Select this checkbox if you want groups included in other groups to be imported from the selected directory.

Click on **Apply** to confirm your configuration.

"Structure" tab

Read-only access

User selection filter	When using the firewall in interaction with an external database, only users that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = InetOrgPerson.*
User group selection filter	When using the firewall in interaction with an external database, only user groups that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = GroupOfNames.*

You are accessing the directory in read-only mode. The creation of users and groups will not be allowed: If this option is selected, you will not be able to perform any actions in write mode.

Mapped attributes

Apply a model: This button offers to apply one of three LDAP servers to define your attributes:

- OpenLDAP
- Microsoft Active Directory (AD)
- Open Directory

External directory attributes	This column represents the value given to the attribute in the external directory. **EXAMPLES** *Cn= COMPANY* *telephoneNumber= +33 (0)3 61 96 30* *mail = salesadmin@company.com*

Advanced properties

Password hash: The password encryption method for new users.

Some authentication methods (such as LDAP) must store the user's password in the form of a hash (result of a hash function applied to the password) which prevents the password from being stored in plaintext.

You must select your desired hash method from the following:

SHA	"Secure Hash Algorithm". This encryption method makes it possible to set up a 160-bit or 160-byte character string (called a "key") which will be used as a reference for identification.
MD5	"Message Digest". This algorithm allows you to check the integrity of data entered, by generating a 128-bit MD5 key. **REMARKS** As this method uses fewer bytes and as such has a lower level of security, it is less robust against attacks.
SSHA	"Salt Secure Hash Algorithm". Based on the same principle as SHA, but contains a password salting function in addition, which consists of adding a bit sequence to the data entered in order to make them less legible. **NOTE** This variant of SHA uses a random value to diversify the password's fingerprint. Two identical passwords will therefore have two different fingerprints. The encryption method is the most secure and strongly recommended.
SMD5	"Salt Message Digest". Based on the same principle as MD5, with the addition of the password salting function.
CRYPT	The password is protected by the CRYPT algorithm, derived from the DES algorithm which allows block encryption using 56-bit keys. This method is not highly advised, as it has a relatively low level of security.
None	No password encryption, meaning it is stored in plaintext. **WARNING** This method is not recommended, as your data will not be protected.
User branch	Enter the name of the LDAP branch for storing users. **EXAMPLE** ou=users
Group branch	Enter the name of the LDAP branch for storing user groups. **EXAMPLE** ou=groups

Certification authority branch	This field defines the location of the CA on the external LDAP base. This location is used especially when searching for the CA used in SSL. **NOTE** This field does not necessarily need to be configured but in this case, in order for the SSL authentication method to work, the CA must be specified in the list of trusted CAs in the configuration of the SSL method. (See **Users** > **Authentication** module > **Available methods** tab: the authentication method **Certificate (SSL)** must be added and the CA indicated in the right column "Certification authorities (C.A)")

Click on **Apply** to confirm your configuration.

DNS CACHE PROXY

When you send a DNS query to your browser or to an e-mail address, the DNS server will convert the known domain name (e.g. *www.company.com* or *smtp.company.com*) into an IP address and communicate it to you.

The DNS cache proxy allows storing the response and IP address communicated earlier by the server in the firewall's memory. As such, whenever a similar query is sent, the firewall will respond more quickly on behalf of the server and will provide the saved IP address.

The **DNS cache proxy** window consists of a single screen, divided into two sections:

- A table listing the DNS clients allowed to use the cache.
- A drop-down menu allowing the definition of advanced properties.

Enable DNS cache

This option allows the **DNS cache proxy** to run: when a DNS query is sent to the firewall, it will be processed by the DNS cache.

List of clients allowed to used the DNS cache

DNS client [host, network, range, group]:

The clients that appear in the list can send DNS queries through the firewall.

Add	By clicking on this button, a new line will be added to the top of the table. The arrow to the right of the empty field allows adding a DNS client. You may select this client from the object database that appears. This may be a host, network, address range or even a group.
Delete	First, select the DNS client you wish to remove from the list. A window will appear with the following message: "**Remove selected DNS client?**" " You can confirm that you wish to delete or **Cancel** the operation.

> **NOTE**
> In transparent mode, the selected clients will benefit from the DNS cache proxy, while other requests will be subject to filtering.

Advanced properties

Cache size (in bytes):

The maximum size allocated to the DNS cache depends on your firewall's model.

Transparent mode (intercepts all DNS queries sent by authorized clients)	As its name implies, the purpose of this option is to make the Stormshield Network Firewall's DNS service transparent. As such, when this option is enabled, the redirection of DNS traffic to the DNS cache will be invisible to users who will get the impression they are accessing their DNS servers. In transparent mode, all queries will be intercepted, even if they are going to DNS servers others than the firewall. The responses will be saved in memory for a certain duration to avoid resending known requests.
Random querying of domain name servers	If this option is selected, the firewall will select the DNS server at random from the list. (see menu **System**>**Configuration** module/*Network settings* tab/**DNS Resolution** panel).

DYNAMIC DNS

The configuration screen for the Dynamic DNS client consists of 2 sections:

- On the left, the **List of Dynamic DNS profiles**.
- On the right, **DNS resolution**, or the configuration of the profile selected earlier.

List of dynamic DNS profiles

The table that presents the profiles consists of 2 columns:

Status	Double-clicking on this column to enable or disable a profile.
Preview	Indicates the domain name, interface and status of the resolution with regard to the profile.
Associated interface	Indicates the interface associated with the domain name as selected in the domain settings.
Troubleshooting	Indicates whether the DNS was resolved for this profile.

- The **Add** button allows adding a profile.
- The **Delete** button allows deleting a selected profile.
- The **Reset** button allows reinitializing the status of the Dynamic DNS profile.

Configuring a profile

Adding a profile

1. Click on **Add**.
2. Select the desired profile type: **Dyndns provider** or **No-IP provider**.
   The DNS resolution parameters to be applied to this new profile will appear on the right side of the screen.
3. Adapt these parameters by following the instructions in the section **DNS resolution for the profile *Profile_name*.**

Editing a profile

1. In the list of profiles on the left side of the screen: double-click on the profile to be edited.
   The DNS resolution parameters to be applied to this profile will appear on the right side of the screen.
2. Adapt these parameters by following the instructions in the section **DNS resolution for the profile *Profile_name*.**

DNS resolution for the profile *Profile_name*

Domain settings

Domain name	Domain name assigned to the Dynamic DNS client. For example: *myfirewall.dyndns.org*. By using the option **Resolve domain names for all sub-domains (wildcard management)**, you will be able to cover all sub-domains. **EXAMPLE** If you specify **company.dyndns.org** in the **Domain name** field and the option **Resolve domain names for all sub-domains (wildcard management)** has been selected, all sub-domains (commerce.company.dyndns.org, labo.company.dyndns.org, etc.) will be associated with the client.
Interface associated with the domain name	Name of the network interface whose IP address is associated with the domain name. Do note that: • An interface can use only one profile. • A profile can only be used by one interface. • The profile cannot be active if an interface has not been indicated
Resolve domain names for all sub-domains (wildcard management)	Enables or disables the inclusion of sub-domains linked to the domain name. **NOTE** Subscribing to the Wildcard range is necessary in order to benefit from this feature.

Dynamic DNS service provider

This zone allows you to enter the access information for your Dynamic DNS service provider.

Dynamic DNS provider	The name of the DNS service provider selected when the profile was created will be shown (**DynDns** or **No-IP**).
Login (mandatory)	User indicated by the DNS service provider for the authentication of the Dynamic DNS client.
Password (mandatory)	Password indicated by the DNS service provider for the authentication of the Dynamic DNS client.
Dynamic DNS server (mandatory)	Server of the DNS service provider: • *members.dyndns.org* (suggested by default) or *members.dyndns.com* for the **DynDns** service. • *dynupdate.no-ip.com* for the **No-IP** service.
Dynamic DNS service (mandatory)	This option allows you to indicate the service you have subscribed with your DNS service provider: "Dynamic", "Static " or "Customized".

Advanced properties

Access the settings for advanced properties by clicking on the button **Advanced properties**. These allow in particular, renewing registrations and changing addresses.

Renewal frequency (days)	Renewal period of the Dynamic DNS service. Stormshield Network has set this period to 28 days by default. **REMARKS** Excessively frequent renewals will be penalized (by a closure of the account, for example), therefore providers will not allow renewals made less than 26 days (after the first renewal). Also, if an account is not renewed after 35 days, it will be closed. However, the above information is subject to change as it is a provider established operation.
Protocol used for the update	Protocol used during the dynamic DNS service renewal phase. Possible choices are: HTTPS (suggested by default) or HTTP.
Notify the provider	This service, which **DynDNS** charges at a fee, makes it possible to redirect traffic headed for your network to a specific page when your connection is idle.
Support address translation (NAT)	This option allows the firewall to use dynamic DNS services when it is located behind a device that performs address translation.

DYNAMIC ROUTING

BIRD supports the following versions of dynamic routing protocols:

- Rip v2,
- OSPF v2 for IPv4 and OSPF v3 for IPv6,
- BGP v4 for IPv4 and IPv6.

In SNS version 4.8 and higher, the firewall can run the BIRD dynamic routing engine in either version 1 (obsolete) or version 2.

By doing so, a configuration in BIRD v1 can be migrated to BIRD v2 without risk.

The **Dynamic routing** module is organized in three or four tabs, depending on whether the dynamic routing configuration applies to IPv6:

- **General** tab,
- The tab named **BIRD v2** or **BIRD v2 (INACTIVE),** depending on whether BIRD v2 has been enabled,
- The tab named **IPv4 BIRD v1** or **IPv4 BIRD v1 (INACTIVE),** depending on whether IPv4 BIRD v1 has been enabled,
- The tab named **IPv6 BIRD v1** or **IPv6 BIRD v1 (INACTIVE),** depending on whether IPv6 BIRD v1 has been enabled,

General tab

In this tab, you can enable either version of BIRD, and configure dynamic routing, notably in high availability architectures.

General configuration

BIRD v2	Enables or disables the use of the BIRD v2 dynamic routing engine.
IPv4 BIRD v1	Enables or disables the use of the BIRD v1 dynamic routing engine only for IPv4 routes.
IPv6 BIRD v1	Enables or disables the use of the BIRD v1 dynamic routing engine only for IPv6 routes.
IPv4 and IPv6 BIRD v1	Enables or disables the use of the BIRD v1 dynamic routing engine for IPv4 and IPv6 routes.

Advanced properties

Restart dynamic routing when the firewall becomes active (high availability)	In a cluster that implements the OSPF dynamic routing protocol, the active firewall adopts the role of a Designated Router (DR). This option makes it possible to ensure that during a switch the active firewall does not fail to detect that it has inherited the role of OSPF Designated Router. It is enabled by default. This field can only be accessed in the **IPv4 dynamic routing tab**.

Add IPv4 networks distributed via dynamic routing to the table of protected networks	In the table listing the intrusion prevention system's protected networks, this option makes it possible to automatically inject networks propagated by the IPv4 dynamic routing engine.
Add IPv6 networks distributed via dynamic routing to the table of protected networks	In the table listing the intrusion prevention system's protected networks, this option makes it possible to automatically inject networks propagated by the IPv6 dynamic routing engine.

BIRD v2 tab

> **NOTE**
> "**(Inactive)**" is a suffix that is added to the name of the **BIRD v2** tab when version 2 of BIRD has not been enabled in the **General** tab.

Screen description

This screen has been designed to facilitate migration from BIRD v1 to BIRD v2.

It consists of three sections:

- In the upper left part of the screen: the BIRD v2 configuration input window, its toolbar and the configuration verification button;
- In the upper right part of the screen: the window displaying the BIRD v1 configuration;
- In the lower part of the screen: the configuration verification console.

BIRD v2 configuration input window

In this window, changes can be made to the configuration of the BIRD dynamic routing engine.

Verify configuration	By clicking on this button, you will launch a process to verify the configuration: if there are syntax errors, they will be listed in the verification console (error line and column). This verification operation is mandatory before changes to the configuration can be saved.

Possible operations: toolbar

Search	This field can be used to look for a character string in the BIRD v2 configuration. You can choose to make the search case sensitive or not by using the **Aa** button.
Aa	With this button, you can determine whether the search has to be case sensitive or not .
Go back to saved configuration	If you wish to discard changes to the BIRD configuration, use this button to go back to the last version of the configuration that was saved. For optimal benefit, regularly save changes that you make to configurations (**Apply** button).

Copy to clipboard	Use this button to copy selected text to the clipboard to paste it later in an external document, for example.
Go back to configuration suggested by default	Use this button to discard all changes made to the BIRD v2 configuration by restoring the lowest configuration offered on a firewall in factory settings.

BIRD v1 (IPv4 and/or IPv6) configuration display window

When there is a BIRD v1 dynamic routing configuration on the firewall, it will appear in this window, which contains one or two tabs, depending on the IP versions configured in BIRD v1: IPv4 and/or IPv6.

The purpose of this window is to facilitate migration from BIRD v1 to BIRD v2 by allowing configuration items to be copied and pasted directly, while ensuring that no items are forgotten.

Verification console

After having clicked on the **Check configuration** button, the console will show the lines/columns of any syntax errors found in the BIRD v2 configuration.

Errors have to be fixed before the configuration can be saved.

Saving/Applying the configuration

Click on **Apply**, then **Save** to save the configuration: this operation can only be performed if the configuration is valid (without syntax errors).

If the BIRD v2 protocol is enabled, the saved configuration will be automatically applied.

IPv4 BIRD v1 and IPv6 BIRD v1 tabs

> **NOTE**
> "**(Inactive)**" is a suffix that is added to the name of the **IPv4 BIRD v1** and **IPv6 BIRD v1** tabs when the corresponding BIRD version has not been enabled in the **General** tab.

Screen description

The screen consists of two sections:

- In the upper part of the screen: the BIRD v1 configuration input window, its toolbar and the configuration verification button;
- In the lower part of the screen: the configuration verification console.

BIRD v1 configuration input window

In this window, changes can be made to the configuration of the BIRD dynamic routing engine.

Verify configuration	By clicking on this button, you will launch a process to verify the configuration: if there are syntax errors, they will be listed in the verification console (error line and column). This verification operation is mandatory before changes to the configuration can be saved.

Possible operations: toolbar

Search	This field can be used to look for a character string in the BIRD v1 configuration. You can choose to make the search case sensitive or not by using the **Aa** button.
Aa	With this button, you can determine whether the search has to be case sensitive or not .
Go back to saved configuration	If you wish to discard changes to the BIRD configuration, use this button to go back to the last version of the configuration that was saved. For optimal benefit, regularly save changes that you make to configurations (**Apply** button).
Copy to clipboard	Use this button to copy selected text to the clipboard.
Go back to configuration suggested by default	Use this button to discard all changes made to the BIRD v1 configuration by restoring the lowest configuration offered on a firewall in factory settings.

Verification console

After having clicked on the **Check configuration** button, the console will show the lines/columns of any syntax errors found in the configuration.

Errors have to be fixed before the configuration can be saved.

Saving/Applying the configuration

Click on **Apply**, then **Save** to save the configuration: this operation can only be performed if the configuration is valid (without syntax errors).

If the BIRD v1 protocol is enabled, the saved configuration will be automatically applied.

E-MAIL ALERTS

This screen consists of four tabs:

- **Notifications**: enables configuration of modules such as e-mail sending frequency (in minutes), intrusion prevention alarms and system events.
- **Recipients**: makes it possible to create groups that will be used in the mailing policies and in configuration modules in which e-mail sending can be configured.
- **Templates**: makes it possible to preview and modify e-mail templates used when sending notifications to users and administrators.
- **SMTP server**: makes it possible to set the SMTP server that is used to send alerts and system events.

Notifications tab

This tab contains the options and settings associated with sending e-mail alerts.

Enable e-mail notifications	This option enables the configuration of sending alerts by e-mail. The e-mail notification feature requires a mail server that can receive e-mails from the firewall.

E-mail sending frequency (in minutes)

Sending frequency	This option allows you to specify the frequency with which reports will be sent. A report contains all the alarms detected from the previous report. As such, e-mails will be received during certain time slots and not each time an alarm is raised. The default value is 15. **EXAMPLE** With a frequency of 15 minutes, you will be informed by e-mail every 15 minutes of alarms that were raised on the firewall during this period.

Sending notifications for intrusion prevention alarms

Here, you can configure the recipients (e-mail addresses or groups) that will receive intrusion prevention alarms.

The list of alarms will be sent in the body of the e-mail to the specified group, and at the frequency defined in the **Sending frequency** field.

Alarm and event levels	Select the severity of alarms that need to be sent by e-mail: • Configuration specific to each alarm (only alarms with advanced options that enable sending an e-mail will be included in notifications), • Major alarms, • Major and minor alarms.
E-mail recipients (To)	Enter a valid e-mail address or select a group of recipients (groups can be configured in the **Recipients** tab of the same module).

In carbon copy of e-mails (Cc)	Enter a valid e-mail address or select a group of recipients (groups can be configured in the **Recipients** tab of the same module).
In blind carbon copy of e-mails (Cc)	Enter a valid e-mail address or select a group of recipients (groups can be configured in the **Recipients** tab of the same module).

Sending system event notifications

Here, you can configure the recipients (e-mail addresses or groups) that will receive system events.

The list of events will be sent in the body of the e-mail to the specified recipient, and at the frequency defined in the **Sending frequency** field.

Alarm and event levels	Select the severity of system events that need to be sent by e-mail: • Configuration specific to each system event (only system events with advanced configuration that enables sending an e-mail will be included in notifications), • Major events, • Major and minor events.
E-mail recipients (To)	Enter a valid e-mail address or select a group of recipients (groups can be configured in the **Recipients** tab of the same module).
In carbon copy of e-mails (Cc)	Enter a valid e-mail address or select a group of recipients (groups can be configured in the **Recipients** tab of the same module).
In blind carbon copy of e-mails (Cc)	Enter a valid e-mail address or select a group of recipients (groups can be configured in the **Recipients** tab of the same module).

NOTE
The status of system events can be viewed in the **Notifications** > **System events** module.

Recipients tab

In this tab, groups containing recipients can be created. Each recipient is represented by an e-mail address. There are no pre-configured groups. Up to 50 groups can be created. There is no restriction to the number of e-mail addresses in a group.

Once a group is created, it can be used in the notification policies and in configuration modules in which e-mail sending can be configured.

This screen consists of two zones:

- A zone containing the recipient groups,
- A zone containing the members of the selected recipient group.

NOTE
Refer to the section Allowed names to find out which characters are allowed and prohibited in various fields.

Creating a recipients group

1. Click on **Add**.
2. Enter the **Name** that you wish to give to your group.
3. You can add comments regarding this group, by filling in the relevant field.
4. Confirm by clicking on **Apply**.

Adding a recipient to a group

1. Select the group in question beforehand from the zone on the left.
2. In the area on the right, click on **Add**.
3. In the window that appears, add the recipient (user or group) based on two possibilities:
   - If the user (or group) that you want to add is in the firewall's default LDAP directory, select the **User - Group found in the LDAP directory** checkbox and select the user or group from the drop-down list.
   - Otherwise, enter the desired e-mail address directly in the **E-mail address** field.

Deleting a group

1. Select the group that you wish to delete from the zone on the left.
2. Click on **Delete,** then confirm. If the group in question is used in the firewall's configuration, you can: force it to be deleted, check where it is being used, and cancel the operation.

Checking whether a group is in use

The **Check usage** button allows you to check whether a recipient group is used in the various modules of the firewall's configuration.

1. Select the group in question beforehand from the zone on the left.
2. Click on **Check usage**.

Templates tab

Several templates are available, each containing a body that differs according to the message that you wish to send out. This section allows you to use a customized message to send e-mails.

This screen consists of two zones:

- Templates on the left,
- The editing window on the right: subject and body of the e-mail.

Modifying a template (HTML)

Each template has some content called the "body" (like in an HTML page). This consists of unformatted text that may contain simple HTML markers that may finalize the formatting.

These templates can be modified and may contain variables, which will later be replaced with values. For example, a variable may automatically display the user's name.

Do note that the language used for the mail subject and body is the language that is set in the **Firewall language (logs)** field in **Configuration** > **General configuration** tab.

To edit the contents of a template:

Select the template from the list on the left.
An edit window appears on the right.

Make the desired changes.

Two buttons allow you to:

- **Preview** the e-mail **template**,
- **Send a test email**.

If you do not want to keep the changes you have made, you can reset the template to its original layout, by clicking on the **Apply default template** button.

Default templates are categorized and listed below.

Certificate request

- Certificate request accepted.
- Certificate request denied.

User enrollment

- Request to enroll a new user.
- Enrollment request accepted.
- Enrollment request denied.

Sponsorship method

- Sponsorship request.

Variables that can be used in various templates

Variables that are the same across e-mail templates provided by default on the firewall:

Variable	Meaning	E-mail template(s) in question
${Lang}	E-mail language used	All
${SystemNodeName}	Name of firewall system node, if any (firewalls in HA configuration)	All
${Date}	Date on which the e-mail was created	All
${LastName}	Last name of the requester	All
${FirstName}	First name of the requester	All
${URL}	URL to download certificate	Certificate request accepted
${UID}	Requester ID	Certificate request accepted Certificate request denied Enrollment request accepted

${FirewallName}	Firewall name	Request to enroll a new user
${UserIP}	IP address of the user workstation that initiated the request	Request to enroll a new user Sponsorship request
${FirewallFQDN}	Fully qualified name (DNS name) of the firewall	Sponsorship request
${Time}	Sponsored session validity period	Sponsorship request
${AcceptURL}	Sponsorship request acceptance URL	Sponsorship request

Example of a message received by e-mail when a certificate request is accepted

Demande de certificat acceptée

Bonjour John Doe,

Votre demande de certificat vient d'être approuvée.
Votre administrateur a signé votre certificat : **john.doe**
Vous pouvez télécharger votre certificat à partir de l'URL suivante.

Bonne journée.

https://VMSNSX09I0390A9/auth/getcert.html

SMTP server tab

This tab contains all the parameters required to configure the SMTP server that allows e-mail alerts to be sent.

Server	This field determines the host (SMTP server) to which the firewall will send e-mails, by selecting it from the object database. This field is empty by default.
Port	Port on the SMTP server to which e-mails will be sent. A list allows selecting an object, whose default value will be “SMTP”.

Authentication

ID	This entry is disabled if the Authentication option has not been selected. This field allows entering the SMTP username (this entry has to be provided if authentication has been enabled).
Password	This entry is disabled if the Authentication option has not been selected. This field allows entering the SMTP username (this entry has to be provided if authentication has been enabled).

Security

Protocol	Select the object representing the protocol used for authenticating to the e-mail server. The StartTLS protocol is suggested by default.

Certification authority or server certificate	Select the certification authority or server certificate presented by the e-mail server.

Sender's identity

Show e-mail address	Specify the e-mail address that will appear as the sender's address.
Show name	Specify the name that will appear as the sender's name.
Reply to (e-mail address)	Specify the e-mail address to which the recipient can send a reply, if necessary.
Reply to (name)	Specify the name.

Testing the SMTP configuration

This button makes it possible to send a test e-mail to check the firewall's SMTP configuration.

Enter the recipient e-mail address for the test e-mail, then click on **Send**.

ENROLLMENT

The web enrolment service allows “unknown” users in the user database to request the creation of their access accounts (internet, mail server, all services that require authentication) and their certificates.

This module requires at least the use of an LDAP database for user requests and a root CA (internal PKI) for user certificate requests.

> **NOTE**
> To enable users to submit enrollment requests, the captive portal must be configured and allow web enrollment for users. Enrollment can be enabled in **Configuration** > **Users** > **Authentication**, Captive portal profiles tab.

This screen consists of three zones:

- The grid containing user enrollment requests and certificate requests,
- A zone containing information about the selected enrolment request,
- An **Advanced properties** section.

The table

Possible operations

Search	Searches in the enrollment requests received.
Refresh	Refreshes the list of enrollment requests received.
Select all	Selects all the enrollment requests received.
Approve	Approves a user enrollment request or certificate request. Select the line(s) of the requests in question to approve them. When you approve a user enrollment request with a certificate request, you must enter the password of the CA (certification authority) to approve both requests in a single operation.
Reject	Rejects a user enrollment request or certificate request. Select the line(s) of the requests in question to reject them. When you reject a user enrollment request with a certificate request, both requests will be rejected at the same time.

Enrollment requests received

Type	Type of enrollment request received: **User** or **Certificate**.
Name	Name that allows you to identify the user or certificate among the requests received.

Information about the selected enrollment request

This zone displays information about the selected user enrollment request or certificate request. For **Certificate** requests, only the **E-mail address** field appears.

ID	Connection ID that will be created if the user is approved. You can change the format used to generate IDs in the **Advanced properties** section.
Name	User name.
First name	User's first name.
E-mail address	User's e-mail address, If notifications have been configured when an enrollment request is approved or rejected, e-mails will be sent to this address. These notifications can be configured in the **Advanced properties** area.
Description	Description of the user. This field can remain empty if the user did not fill it in during the enrollment request phase.
Telephone number	User's telephone number. This field can remain empty if the user did not fill it in during the enrollment request phase.
Password	Specifies that the user entered a password during the request phase and that the password complies with the password policy set on the firewall.
Certificate request	Specifies whether a certificate creation request was submitted at the same time as the user enrollment request.

Advanced properties

User ID format

Identifier format	Sets the format used to generate connection IDs when a user enrollment request is received: • The format is written in the form: `%F.%L`. • The variable **%F** corresponds to the first name and the variable **%L** to the last name. • The variables **%f** and **%l** change the case of the variables to lowercase. • Variables can contain a number to set a character limit. **EXAMPLES** **%F.%L** results in **FIRSTNAME.LASTNAME** **%f1.%l** results in **f.lastname**

Send an e-mail to the user

when approving/rejecting user's enrollment request	This option makes it possible to send an e-mail to the user to inform him that his user enrollment request has been approved or rejected.
when approving/rejecting user's certificate request	This option makes it possible to send an e-mail to the user to inform him that his certificate request has been approved or rejected.

FILTERING AND NAT

Filtering and **NAT** are condensed in a single module and are part of the **Security policy** menu.

Evaluation of filtering and the impact of NAT

The filter policy is assessed on IP addresses before their modification via NAT, meaning the IP addresses of the network packet before it reaches the firewall. For example, in order to allow access to an internal server from a public network (e.g. the internet), the public address of this server (or the firewall's public address, for example) has to be entered in the *Destination* field of the filter rule.

On rules with a "pass" action and the explicit HTTP service enabled, "decrypt" or "log" does not cancel the execution of he following rules. Rules continue to be evaluated. Filter rules can therefore be added after such rules.

This module consists of 2 tabs, each containing an area reserved for filter policies and NAT policies, and their configuration:

- **Filtering**: this is a set of rules that allow or block certain types of network traffic according to the defined criteria.
- **NAT**: these allow rewriting (or translating) source and destination addresses and ports.

"FastPath" mode

For rules with an inspection in "Firewall" mode, traffic has been optimized and throughput multiplied by a mechanism called *FastPath*. These rules in "Firewall" mode are recommended for simple access control requirements, for example, for specific internal traffic. This may be traffic dedicated to data backups or replication in a datacenter, or reserved for satellite VPN sites' access to a main firewall if it already scans traffic.

This mechanism therefore allows lightening a heavy processing load that the intrusion prevention engine may have by saving connections that are eligible for *FastPath*, meaning that once they have been checked, they no longer need to go through the IPS engine. This optimization is automatic for rules in firewall mode applied to IPv4 traffic, without network translation (NAT) and without scanning the protocol using dynamic connections (FTP, SIP, etc). Rules must also not have the following options or values:

- Quality of service (QoS),
- A connection threshold: TCP with or without protection from synflood (synproxy), UDP, ICMP and application requests
- Rewritten DSCP (DSCP value defined),
- Rule with an unspecified destination port that does not comply with the protocol indicated (onprobe).

This mechanism is compatible with PBR (policy-based routing) and load balancing options. To ensure a full and coherent overview of traffic, connection tracking will examine the table for log generation in particular.

Policies

This section allows you to select and handle **Filter** policies and **NAT** policies.

Selecting the filter policy

The drop-down menu offers 10 pre-configured filter policies, numbered from 1 to 10, from strictest to most permissive:

"Block all (1)"	By default, this filter policy is enabled in factory settings. Only ports used for the management of the firewall will be open (1300/TCP and 443/TCP). All the interfaces of the firewall can also be pinged. All other connections will then be blocked. **NOTE** By selecting this policy, you will only have access to the firewall's administration interface from internal networks (protected networks); this restriction depends on the list of workstations allowed to manage the firewall, defined in the **System** menu, **Configuration** module (*Firewall administration* tab).
"High (2)"	If you select this filter policy, only web, e-mail and FTP traffic and ping requests (echo request) will be allowed from internal interfaces to the outside.
"Medium (3)"	By selecting this policy, intrusion prevention will be applied to outgoing connections, when the threat prevention engine is able to automatically detect the protocol: For example, port 80 is generally used for HTTP traffic. The firewall will therefore consider all traffic on port 80 as HTTP traffic, as this port is defined as the default port for the HTTP protocol (default ports for each protocol are defined in the menu **Application protection**>**Protocols**). However, if another protocol is used (e.g. an SSH tunnel) for traffic going to port 80, the connection will be considered illegitimate and will be blocked as the only protocol allowed is HTTP. **NOTE** All outgoing TCP connections that cannot be analyzed (for which no protocol can be recognized) will be accepted.
"Low (4)"	A protocol analysis will be forced for outgoing connections. **NOTE** All outgoing connections that cannot be analyzed will be allowed.
"Filter 05, 06, 07, 08, 09"	Apart from the five pre-configured policies (**Block all, High, Medium, Low, Pass all**, which can be edited where necessary), there are five blank policies that you can customize.
"Pass all (10)"	This policy allows all traffic to pass through, meaning connections on all protocols and ports are allowed. Application analyses will however be applied. This policy should only be used for testing.

NOTE
You can **Rename** these policies and modify their configuration whenever you wish (see below).

Possible operations

Activate this policy	Click on **Apply** then **Activate now** to immediately activate the policy being edited: parameters saved in this slot will overwrite current parameters and the policy will be applied immediately on the firewall. **IMPORTANT** As Filter and NAT rules belong to the same policy, they will be enabled simultaneously.
Edit	Three operations can be performed on profiles with this function: • **Rename**: by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name of the filter policy and add comments. Once the operation has been performed, click on **Update**. You can also **Cancel** this operation. • **Reinitialize**: Reinitialize: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. • **Copy to**: This option allows you to copy a profile to another, with all the information from the copied profile transferred to the receiving profile. It will also have the same name.
Last modification	Click on this icon to find out the exact date and time of the last modification. The time shown is the time on the appliance instead of on the client workstation.

Selecting multiple objects

A multiple selection allows assigning the same action to several rules. Select several successive alarms using the **Shift** ⇧ key or individually by holding down the **Ctrl** key. You can also remove an item from an existing selection with the **Ctrl** key.

Some column titles have the icon . When you click on it, a menu appears, and suggests assigning the same setting to several selected rules (*Status, Action* and *Inspection type* for filtering).

EXAMPLE
Several lines can be deleted at the same time, by selecting them with the **Ctrl** key and pressing on **Delete**.

Drag & drop

Throughout the entire process of creating and editing rules, you will be able to drag and drop objects, actions and even filter and NAT rules.

You can move any object to wherever you wish in the table, or insert objects from the browser bar on the left (**Objects** field), if they have been created earlier (you can also create them directly in the fields that accept objects).

This feature applies to the search field.

NOTE
Two icons indicate whether the selected object or action can be moved within a particular cell:

- Means that the operation is possible,
- Means that the object cannot be added to the chosen cell.

Filtering tab

Stormshield Network's intrusion prevention technology includes a dynamic packet filtering engine ("stateful inspection") with rule treatment optimization that allows the application of filter policies safely and effectively.

The implementation of filter functions is based on the comparison of the attributes of each IP packet received against the criteria of each rule in the active filter policy. Filtering applies to all packets without any exceptions.

As for the user or user group authorized by the rule, from the moment a user identifies himself and authenticates successfully from a given host, the firewall will take note of it and will attribute this user's login name to all IP packets using this host's address as its source IP address.

As a result, rules which specify user authentication, even without specifying the restrictions placed on authorized users, can only apply to IP packets transmitted from a host on which a user has already authenticated beforehand. A check action (see **Action** column) can be specified in each filter rule.

Filtering consists of two parts. The strip at the top of the screen makes it possible to choose, enable or edit the filter policy, and view its last changes. The filter table is dedicated to the creation and configuration of rules.

Checking the policy in real time

The firewall's filter policy is one of the most important elements for the security of the resources that the firewall protects. Although this policy is constantly changing to adapt to new services, new threats and new user demands, it has to remain perfectly coherent so that loopholes do not appear in the protection provided by the firewall.

The art of creating an effective filter policy is in avoiding the creation of rules that inhibit other rules. When a filter policy is voluminous, the administrator's task becomes even more crucial as the risk increases. Furthermore, during the advanced configuration of very specific translation rules, the multiplicity of options may give rise to the creation of a wrong rule that does not meet the administrator's needs.

To prevent this from happening, the filter rule edit window has a **Configuration validator** field (located under the filter table), which warns the administrator whenever a rule inhibits another or an error has been created on one of the rules.

EXAMPLE

[Rule 2] This rule will never be applied as it is covered by Rule 1.

Actions on filter policy rules

Search	This field makes it possible to perform searches by occurrence, letter or word. **EXAMPLE** If you enter “Network_internal” in the field, all filter rules containing “Network_internal” will be displayed in the table.

New rule

Inserts a predefined line or a blank line after the selected line.
5 choices are available: authentication, SSL inspection and explicit HTTP proxy rules will be defined via a wizard in a separate window:

- **Single rule**: This option makes it possible to create a blank rule that will leave the administrator the possibility of entering different fields in the filter table.
- **Separator – rule grouping**: This option allows inserting a separator above the selected line.
  This separator makes it possible to group rules that apply to traffic going to different servers and helps to improve the filter policy's readability and visibility by indicating a comment.
  Separators indicate the number of grouped rules and the numbers of the first and last rules in the form: "*Rule name* (contains the *total number* of rules, from *first* to *last*)".
  You can collapse or expand the node of the separator in order to show or hide the rule grouping. You can also copy/paste a separator from one location to another.
- **Authentication rule**: The aim of this is to redirect unauthenticated users to the captive portal. By selecting it, an authentication wizard will appear.
  You need to select the **Source** (displays "Network_internal" by default) and the **Destination** (displays "Internet" by default) of your traffic from the drop-down list of objects, then click on **Finish**. As the port cannot be selected, the HTTP port is chosen automatically.
  You can specify as the **Destination** URL categories or groups that are exempt from the rule, and therefore accessible without authentication (the web object *authentication_bypass* contains by default Microsoft update sites). Access to these sites without authentication can therefore also benefit from the firewall's security inspections.
- **SSL inspection rule**: The aim of this wizard is to create rules that inspect the encrypted SSL traffic. You are strongly advised to go through this wizard to generate the two rules needed for the SSL proxy to run correctly.
  You will need to define the **Profile of traffic to be encrypted** by indicating the **Source hosts** ("Network_internal" by default), **Incoming interface** ("any" by default), the **Destination** ("Internet" by default) and the **Destination port** ("ssl_srv" by default) from the drop-down list of objects.
  In order to **Inspect encrypted traffic** through the second zone in the wizard window, you will need to define the configuration of the **Inspection profile**, by selecting one of those you have defined earlier, or leave it in "Auto" mode. This automatic mode will apply the inspection relating to the source of the traffic (cf **Application protection>Inspection profile**).
  You can also enable the **Antivirus** or **Antispam** and select the **URL**, **SMTP, FTP or SSL** filter policies (checks the CN field of the certificate presented).
- **Explicit HTTP proxy rule**: This option enables or disables the explicit HTTP proxy and defines who can access it. You will need to choose a **Host** object and an **Incoming interface** in the **Source** field. Next, define the **Inspection of transmitted traffic** by indicating whether you wish to enable the **Antivirus** and select the **URL filter policies**.

> **NOTE**
> To allow a similar policy on a firewall hosted in the cloud and on a physical firewall, the listening port of an explicit HTTP proxy can be configured on a port other than the default port (8080/TCP).
> Click on **Finish**.

Delete	Deletes the selected line.
Move up	Places the selected line before the line just above it.
Move down	Places the selected line after the line just below it.
Expand all	Expands all rules in the tree.
Collapse all	Collapses all folders in the directory.
Cut	Cuts a filter rule in order to paste it.
Copy	Copies a filter rule in order to duplicate it.
Paste	Duplicates a filtering rule after having copied it.
Search in logs	Whenever a filter rule rule is selected, click on this button to automatically search for the name of the rule in the "All logs" view (**Logs** > **Audit logs** > **Views** module). If the selected rule has not been named, a warning message will indicate that the search cannot be performed.
Search in monitoring	Whenever a filter rule is selected, click on this button to automatically search for the name of the rule in the connection monitoring module.

Advanced	**Reset rules statistics**	Clicking on this button will reinitialize the digital and graphical counters showing how filter rules are used, located in the first column of the table.
	Reset columns	When you click on the arrow on the right in the field containing a column's name (example: **Status**), you will be able to display additional columns or remove columns so that they will not be visible on the screen, by checking or unchecking them.

EXAMPLE
Tick the options "**Name**" and "**Src port**" which are not displayed by default.
By clicking on **reset columns**, your columns will be reset to their original settings, before you selected any additional columns. As such, "**Name**" and "**Src port**" will be hidden again.

NOTE
If you click quickly 10 times on the "Up" button, you will see that the rule moves up but the waiting window will only appear when you leave the button for 2 or 3 seconds. And at the end, only a single command will be executed. Rules can be moved more much fluidly as such.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of filter rules:

- New rule (Single rule, Separator - Rule grouping, Authentication rule, SSL inspection rule, Explicit HTTP proxy rule),
- Delete,

- Cut,
- Copy,
- Paste,
- Search in logs,
- Search in monitoring.

Mathematical comparison

Whenever you come across a drop-down list of objects in the columns (except “Status” and “Action”) a mathematical operator icon will appear ( ). It can only be used if an object other than “**Any**” has been selected.

You can therefore customize the parameters of your traffic using the following icon in 4 different ways:

- “=" (or): the value of the attribute corresponds to what is selected.
- “!=" (or) the value of the attribute is different from what has been selected.
- "<" (or ; can only be used for source ports, destination ports and host reputation scores): the value of the attribute is lower than what has been selected.
- ">" (or ; can only be used for source ports, destination ports and host reputation scores): the value of the attribute is higher than what has been selected.

Adding/modifying objects

Some drop-down lists offer the button, which leads to a pop-up menu:

- **Create an object**: new objects can be created directly from the Filter/NAT module
- **Edit object**: when an object is in a field, it can be edited directly to modify it (name, IP address for a host, adding the object to a group, etc.), except for read-only objects ("**Any**", "**Internet**", etc).

Filter table

This table allows you to define the filter rules to apply.

The firewall will execute rules in their order of appearance on the screen (numbered 1, 2, etc) and will stop once it finds a a rule that matches the IP packet. Place them in the right order so that you obtain a coherent result.

It is therefore important to define rules from the **most restrictive to the most general**.

Reorganizing rules

In every security policy, every rule can be dragged and dropped so that the policy (filter or NAT) can be reorganized easily. The symbol as well as the "Drag and drop to reorganize" tool tip appear when you scroll over the beginning of the rule.

Statistics on the use of rules

In the active security policy, each activated filter and NAT rule also displays a counter that shows the number of times the rule has been used. When scrolling over the icon with a mouse, a tooltip will indicate the exact number of times the rule has been executed. The 4 levels of use correspond to the following values, according to the percentage on the counter of the rule most frequently used:

	0%
	from 0 to 2%
	from 2 to 20% (from 2 to 100% if the counter is lower than 10 000)
	from 20 to 100 %, with a minimum of 10 000 times (otherwise the previous level will be displayed)

To obtain a new indicator, clicking on **Reset rule statistics** will start a new count. This counter will be reinitialized if:

- One of the parameters in the rule has been modified (except for comments),
- Another policy has been enabled,
- The firewall has been restarted.

If no icons are displayed, this means that the information is unavailable.

Status

This column shows the status of the rule: **On** / **Off** . Double-click on it to change its status. By doing this once, you will enable the filter rule. Repeat the operation to disable it.

General tab

General

Status	Select **On** or **Off** to respectively enable or disable the rule being edited.
Comments	You can enter comments in this area; they will be displayed at the end of the rule when the filter policy is displayed.

Advanced properties

Rule name	You can assign a name to the filter rule; this name will be used in logs and facilitates identification of the filter rule during searches in logs or views (**Logs - Audit logs** menu).

Action

This zone refers to the action applied to the packet that meets the selection criteria of the filter rule. To define the various parameters of the action, double-click in the column. A window containing the following elements will appear:

General tab

General

Action	5 different actions can be performed: • **Pass**: The Stormshield Network firewall allows the packet corresponding to this filter rule to pass. The packet stops moving down the list of rules. • **Block**: The Stormshield Network firewall silently blocks the packet corresponding to this filter rule: the packet is deleted without the sender being informed. The packet stops moving down the list of rules. • **Decrypt**: This action decrypts encrypted traffic. Decrypted traffic will continue to move down the list of rules. It will be encrypted again after the analysis (if it is not blocked by any rule). • **Reinit. TCP/UDP:** This option mainly concerns TCP and UDP traffic: For TCP traffic, a "TCP reset" packet will be sent to its sender. For UDP traffic, a "*port unreachable*" ICMP packet will be sent to its sender. As for other IP protocols, the Stormshield Network firewall will simply block the packet corresponding to this filter rule. • If you are editing the global filter policy, a fifth option will appear: "**Delegate**". This option makes it possible to stop comparing the traffic against the rest of the global policy, but to compare it directly with the local policy. If your policy contained rules with the action **Log only**, you will see **log only (deprecated)** whenever you edit these rules.
Log level	The value is set to **Standard (connection log)** by default, so no logs are recorded. Several log levels are possible: • **Standard (connection log)**: No logs will be kept in filter logs if the packet corresponds to this rule. However, ended connections can be logged (connection logs) depending on the connection of the protocol associated with the rule, which is the case in a factory configuration. Do note that this option is not available if you have selected the "Log" action in the previous field. • **Advanced (connection log and filtering log)**: In addition to logs in Standard mode, logs from all traffic that matches this rule will be captured. This option is not recommended on "Deny All" filter rules (except for debugging) as it will then generate a large amount of logs. • **Minor alarm**: As soon as this filter rule is applied to a connection, a minor alarm will be generated. This alarm is recorded in the logs, and can be sent via Syslog (**Logs – Syslog – IPFIX**) or by e-mail (see module **E-mail alerts**). • **Major alarm**: As soon as this filter rule is applied to a connection, a major alarm will be generated. This alarm is recorded in the logs, and can be sent via Syslog (**Logs – Syslog – IPFIX**) or by e-mail (see module **E-mail alerts**). To fully disable logs, you need to disable the **Disk**, **Syslog server** and **IPFIX collector** checkboxes in the **Log destination for this rule** field (**Advanced properties** tab in the rule editing window).
Scheduling	Select or create a time object. You will then be able to define the **period/ day of the year / day of the week / time/ recurrence** when rules will be valid. Objects can be created or modified directly from this field by clicking on

Routing

Gateway – router	This option is useful when specifying a particular router that will redirect traffic matching the rule to the defined router. The selected gateway may be a host or router object. Objects can be created or modified directly from this field by clicking on

IMPORTANT
If routers are specified in filter rules (Policy Based Routing), the availability of these routers will then be tested systematically by sending ICMP *echo request* messages. When a router that has been detected as unreachable is a host object, the default gateway entered in the **Routing** module will be selected automatically. If it is a router object, the action taken will depend on the value selected for the field **If no gateways are available** during the definition of this object (see the section **Network objects**).
For more technical information, refer to the technical support's **Knowledge Base** (article "*How does the PBR hostcheck work*?").

Click on **OK** to confirm your configuration.

Quality of service tab

The **QoS** module, built into Stormshield Network's intrusion prevention engine, is associated with the **Filtering** module in order to provide Quality of Service features.

When a packet arrives on an interface, it will first be treated by a filter rule, then the intrusion prevention engine will assign the packet to the right queue according to the configuration of the filter rule's QoS field.

QoS

Queue	This field offers you the choice of several queues that you have defined earlier in the **Security policy** module, in the **Quality of Service** menu. This operation does not apply (grayed out) to traffic going through the SSL proxy (**Source** menu > **Advanced properties** > **Via** field).
ACK queue	This field offers you the choice of several queues that you have defined earlier for TCP ACK traffic in **Security policy > Quality of Service**. This operation does not apply (grayed out) to traffic going through the SSL proxy (**Source** menu > **Advanced properties** > **Via** field).
Fairness	• **No fairness**: If you select this option, no particular amount of bandwidth will be assigned and each user/host/connection will use it according their needs. • **User fairness**: bandwidth will be distributed evenly between users. • **Host fairness**: bandwidth will be distributed evenly between hosts. • **Connection fairness**: bandwidth will be distributed evenly between connections.

Connection threshold

The Stormshield Network firewall may limit the maximum number of connections accepted per second for a filter rule. The desired number can be defined for protocols corresponding to the rule (TCP, UDP, ICMP and some application requests). This option also allows you to prevent a denial of service which hackers may attempt: you may limit the number of requests per second addressed to your servers.

Once this threshold has been exceeded, received packets will be blocked and ignored.

WARNING
The restriction only applies to the corresponding rule.

EXAMPLE
If you create an FTP rule, only a TCP restriction will be taken into account.

REMARKS
If the option is assigned to a rule containing an object group, the restriction applies to the whole group (total number of connections).

If threshold is reached	• **Do not do anything**: no restrictions will be placed on the number of connections or requests per second (c/s). • **Protect against SYN Flood:** this option makes it possible to protect servers from TCP SYN packet flooding ("SYN flooding") attacks. The SYN proxy instead of the server will respond and will assess the reliability of the TCP request before transmitting it. You can limit the number of TCP connections per second for this filter rule in the field below. • **Raise associated alarm**: Depending on the maximum number of connections per second that you assign to the protocols below, the traffic will be blocked once the defined number has been exceeded. The identifiers of these alarms are: 28 ICMP / 29 UDP / 30 TCP SYN / 253 TCP/UDP.
TCP (c/s)	Maximum number of connections per second allowed for the TCP protocol.
UDP (c/s)	Maximum number of sessions per second allowed for the UDP protocol.
ICMP (c/s)	Maximum number of connections per second allowed for the ICMP protocol.
SCTP (c/s)	Maximum number of connections per second allowed for the SCTP protocol.
Application requests (r/s)	Maximum number of application requests per second allowed for the HTTP and DNS protocol.

Click on **OK** to confirm your configuration.

DSCP

DSCP (*Differentiated Services Code Point*) is a field in the IP packet header. The purpose of this field is to allow services contained in a network architecture to be differentiated. It will specify a mechanism for classifying and controlling traffic while providing quality of service (QoS).

Impose value	By selecting this option, you will enable the field below and allow access to the DSCP service. This option makes it possible to rewrite the packet with the given value, so that the next router will know the priority to apply to this packet.
New DSCP value	In this field, traffic differentiation can be defined. Through this field, it is possible to determine which service a type of traffic belongs to, thanks to a pre-established code. This DSCP service, used in the context of Quality of Service, allows the administrator to apply QoS rules according to the service differentiation that he has defined.

Click on **OK** to confirm your configuration.

Advanced properties tab

Redirection

Service	• **None**: This option means that none of the following services will be used: the user will not go through the HTTP proxy and will not be redirected to the authentication page. • **HTTP proxy:** If you select this option, the HTTP proxy will intercept user connections and scan traffic. This service will be selected when rules are created by the explicit HTTP proxy wizard. • **Authentication**: If you select this option, unauthenticated users will be redirected to the captive portal when they connect. This service will be selected when rules are created by the authentication wizard.
Redirect incoming SIP calls (UDP)	This option allows the Stormshield Network firewall to manage incoming SIP-based communications to internal hosts masked by address translation (NAT).
URLs without authentication	This field becomes accessible if the previous option **Service** redirects traffic to the authentication portal (**authentication** rule). It allows specifying URL categories or groups that are exempt from authentication; the listed sites therefore become accessible without authentication, which is useful for example in accessing update websites. The firewall's security inspections can therefore be applied to such access. There is by default in the URL objects database a URL group named *authentication_bypass* containing Microsoft update websites.

Logs

Log destination for this rule	This option makes it possible to define one or several methods for storing logs generated by the rule: • **Disk**: local storage. • **Syslog server**: the Syslog profile(s) including Filter policy logs must be defined in the *SYSLOG* tab of the menu **Notifications** > **Logs - Syslog - IPFIX**. • **IPFIX collector**: the IPFIX collector(s) must be defined in the *IPFIX* tab of the menu **Notifications** > **Logs - Syslog - IPFIX**. Each log will contain details of connections evaluated through the rule.

Advanced properties

Count	If you select this option, the Stormshield Network firewall will count the number of packets that correspond to this filter rule and generate a report. Volume information on a desired traffic type can therefore be obtained.
Force source packets in IPsec	When this option is selected, for this filter rule, you will force packets from the network or source hosts to go through an active IPsec tunnel to reach their destination.
Force return packets in IPsec	When this option is selected, for this filter rule, you will force return packets (responses) to go through an active IPsec tunnel in order to contact the host that initiated the traffic.
Synchronize this connection between firewalls (HA)	When the firewall belongs to a cluster, this option enables or disables the synchronization of the connection corresponding to the rule between two cluster members. This option is enabled by default.

Click on **OK** to confirm your configuration.

Source

This field refers to the source of the treated packet, and is used as a selection criterion for the rule. Double-click in this zone to select the associated value in a dedicated window.

This window contains three tabs:

General tab

General

User	The rule will apply to the user that you select in this field. You can filter the display of users according to the desired method or LDAP directory by clicking on . Only enabled directories and methods (*Available methods* tab in the **Authentication** module and LDAP directories defined in the **Directory configuration** module) will be presented in this filter list. Depending on the authentication method, several generic users will be suggested: • **"Any user@any"**: refers to any authenticated user, regardless of the directory or authentication method used. • "**Any user@guest_users.local.domain**": refers to any user authenticated via the "Guest" method. • "**Any user@voucher_users.local.domain**": refers to any user authenticated via the "Temporary accounts" method. • "**Any user@sponsored_users.local.domain**": refers to any user authenticated via the "Sponsorship" method. • "**Any user@none**": refers to any user authenticated via a method that does not rely on an LDAP directory (e.g.: Kerberos). • "**Unknown users**": refers to any unknown or unauthenticated user. **NOTE** In order for unauthenticated users to be automatically redirected to the captive portal, at least one rule must be defined, applying to the object "**unknown users**". This rule will also apply when an authentication expires.
Source hosts	The rule will apply to the object or the user (created beforehand in the dedicated menu: **Objects**>**Network objects** that you select in this field. The source host is the host from which the connection originated. You can **Add** or **Delete** objects by clicking on the icon Objects can be created or modified directly from this field by clicking on
Incoming interface	Interface on which the filter rule applies, presented in the form of a drop-down list. By default, the firewall selects it automatically according to the operation and source IP addresses. It can be modified to apply the rule to another interface. This also allows a particular interface to be specified if "Any" has been selected as the source host.

Web Services and IP Reputations

Select a service or an IP reputation category	This field makes it possible to apply the filter rule to hosts with public IP addresses classified under one of the categories below: • **Official web services** (list updated dynamically via Stormshield Active Update), • **Malicious** (list updated dynamically via Stormshield Active Update): ○ **anonymizer**: proxies, IPv4 to IPv6 converters. ○ **botnet**: infected hosts running malicious programs. ○ **exploit**: IP addresses known for having been at the source of vulnerability exploits. ○ **malware**: hosts distributing malicious programs ○ **tor entry node**: inbound endpoint servers of the Tor network. ○ **tor exit node**: outbound endpoint servers of the Tor network. ○ **phishing**: compromised mail servers. ○ **scanner**: hosts that conduct port scanning or launch brute force attacks. ○ **spam**: compromised mail servers. ○ **suspicious**: groups hosts and IP addresses that do not appear very trustworthy, and which are likely to cause false positives. This category is not included in **bad** by default. • **Groups**: ○ Official web services grouped by function (remote access, web conferencing, etc.) or by provider (Apple, Google, etc.), ○ **Bad**: groups all malicious reputation categories except **suspicious**, ○ **Malicious**: groups **bad** and two malicious external URL databases. ○ **Tor nodes**: groups **tor entry nodes** and **tor exit nodes**. **NOTE** Since the reputation of a public IP address may border on two categories (botnet and malware), and this field only allows one category to be selected, you are advised to use the "**bad**" group for optimum protection.

Click on **Ok** to confirm your configuration.

NOTE
Filter rules with a *user@object* source type (except *any* or *unknown@object*), and with a protocol other than HTTP, do not apply to **Multi-user Objects** (**Authentication**> **Authentication policy**). This behavior is inherent in the packet treatment mechanism used by the intrusion prevention engine.

Geolocation/Reputation tab

Geolocation

Select a region	This field allows the filter rule to be applied to hosts with a public IP address belonging to a country, continent or group of regions (group of countries and/or continents) defined beforehand in the **Objects** > **Network objects** module.

Host reputation

Enable filtering based on reputation score	Select this checkbox in order to enable filtering based on the reputation score of hosts on the internal network. To enable host reputation management and to define the hosts affected by the calculation of a reputation score, go to the **Application protection** > **Host reputation** module.
Reputation score	This field makes it possible to select the reputation score above which ( ) or below which ( ) the filter rule will apply to the monitored hosts.

Click on **Ok** to confirm your configuration.

Advanced properties tab

Advanced properties

Source port	This field makes it possible to specify the port used by the source host, if it has a particular value. By default, the "Stateful" module memorizes the source port used and only this port will then be allowed for return packets. Objects can be created or modified directly from this field by clicking on
Via	• **Any**: This option implies that none of the following services will be used – the connection will not go through the HTTP proxy, will not be redirected to the authentication page and will not go through an IPsec VPN tunnel. • **Explicit HTTP proxy**: Traffic originates from the HTTP proxy. • **SSL proxy:** Traffic originates from the SSL proxy. • **IPsec VPN tunnel**: Traffic comes from an IPsec VPN tunnel. • **SSL VPN tunnel**: Traffic comes from an SSL VPN tunnel.
Source DSCP	This field makes it possible to filter by the value of the DSCP field of the packet received.

Authentication

Authentication method	In this field, the application of the filter rule can be restricted to the selected authentication method.

Click on **Ok** to confirm your configuration.

Destination

Destination object used as a selection criterion for the rule. Double-click in this zone to select the associated value in a dedicated window. This window contains two tabs:

General tab

General

Destination hosts	Select the destination host of the traffic from the object database in the drop-down list. You can **Add** or **Delete** objects by clicking on the icon . Objects can be created or modified directly from this field by clicking on .

Web Services and IP Reputations

Select a service or an IP reputation category	This field makes it possible to apply the filter rule to hosts with public IP addresses classified under one of the categories below: • **Official web services** (list updated dynamically via Stormshield Active Update), • **Malicious** (list updated dynamically via Stormshield Active Update): ○ **anonymizer**: proxies, IPv4 to IPv6 converters. ○ **botnet**: infected hosts running malicious programs. ○ **exploit**: IP addresses known for having been at the source of vulnerability exploits. ○ **malware**: hosts distributing malicious programs ○ **tor entry node**: inbound endpoint servers of the Tor network. ○ **tor exit node**: outbound endpoint servers of the Tor network. ○ **phishing**: compromised mail servers. ○ **scanner**: hosts that conduct port scanning or launch brute force attacks. ○ **spam**: compromised mail servers. ○ **suspicious**: groups hosts and IP addresses that do not appear very trustworthy, and which are likely to cause false positives. This category is not included in **bad** by default. • **Groups**: ○ Official web services grouped by function (remote access, web conferencing, etc.) or by provider (Apple, Google, etc.), ○ **Bad**: groups all malicious reputation categories except **suspicious**, ○ **Malicious**: groups **bad** and two malicious external URL databases. ○ **Tor nodes**: groups **tor entry nodes** and **tor exit nodes**. **NOTE** Since the reputation of a public IP address may border on two categories (botnet and malware), and this field only allows one category to be selected, you are advised to use the "**bad**" group for optimum protection.

Click on **OK** to confirm your configuration.

Geolocation/Reputation tab

Geolocation

Select a region	This field makes it possible to apply the filter rule to hosts with a public IP address belonging to a country, continent or group of regions (group of countries and/or continents) defined beforehand in the **Objects** > **Network objects** module.

Host reputation

Enable filtering based on reputation score	Select this checkbox in order to enable filtering based on the reputation score of hosts on the internal network. To enable host reputation management and to define the hosts affected by the calculation of a reputation score, go to the **Application protection** > **Host reputation** module.

Reputation score	This field allows selecting the reputation score above which (>) or below which (<) the filter rule will apply to the monitored destination hosts.

Click on **OK** to confirm your configuration.

Advanced properties tab

Advanced properties

Outgoing interface	This option allows choosing the packet's outgoing interface, to which the filter rule applies. By default, the firewall selects it automatically according to the operation and destination IP addresses. A packet's outgoing interface can be used as a filtering criterion.

NAT on the destination

Destination	If you wish to translate the traffic's destination IP address, select one from the objects in the drop-down list. Otherwise, leave the field empty, i.e. "**None**" by default. **NOTE** As this traffic has already been translated by this option, the other NAT rules in the current policy will not be applied to this traffic. Objects can be created or modified directly from this field by clicking on ≡.
ARP publication on external destination (public)	This option has been added so that an ARP publication can be specified when a filter rule with a NAT operation is used on the destination. It must be enabled if the destination public IP address (before applying NAT) is a virtual IP address and does not belong to the UTM. **NOTE** Another way to set up this publication would be to add the virtual IP address of the affected interface in the **Interfaces** module.

Click on **OK** to confirm your configuration.

Port - Protocol

The destination port represents the port on which the "source" host opens a connection to the "destination" host. The protocol to which the filter rule applies can also be defined in this window.

Port

Destination Port	Service or service group used as a selection criterion for this rule. Double-click on this zone to select the associated object. **EXAMPLES** Port 80: HTTP service Port 25: SMTP service You can **Add** or **Delete** objects by clicking on the icon Objects can be created or modified directly from this field by clicking on .

Protocol

Depending on the protocol type that you choose here, the following field that appears will vary:

Protocol type	Select the desired protocol type. The value of the following fields varies according to your choice. • Automatic protocol detection (default), • Application protocol, • IP protocol. • Ethernet protocol.
Application protocol	The advantage of this choice is being able to apply application analysis on a port other that the default port. When this protocol type is selected: • Application protocol: Select the desired protocol from the drop-down list. • IP protocol: the IP protocols concerned will change according to the selected application protocol.
IP protocol	When this protocol type is selected: • Application protocol: No application analysis. • IP protocol: Select the desired protocol from the drop-down list. Additional fields may appear depending on the protocol selected. • Stateful tracking: Select the checkbox to track the status of IP connections. This option is selected by default for TCP, UDP and ICMP protocols.
Ethernet protocol	When this protocol type is selected, select the desired Ethernet protocol from the drop-down list.

NOTE
For example, connection status tracking (stateful mode) can be enabled for the GRE protocol, which is used in PPTP tunnels. Thanks to this tracking tool, the source (map), destination (redirection) or both (bimap) can be translated.
However, it will be impossible to differentiate 2 connections that share the same source and destination addresses. In concrete terms, this means that when the firewall translates a source N -> 1 (map), only one simultaneous connection to a PPTP server can be made.

Translated port

This section is available when **NAT on the destination** is selected.

Translated destination port	Translated port to which packets are going. Network packets received will be redirected from a given port on a host or a network device to another host or network device. If you wish to translate the traffic's destination port, select one from the objects in the drop-down list. Otherwise, leave the field empty, i.e. "**None**" by default. In this case, the **Destination port** field remains unchanged.

Security inspection

General

Inspection level field

IPS (Detect and block)	If this option is selected, Stormshield Network's IPS (Intrusion Prevention System) will detect and block intrusion attempts, from the Network level to the Application level in the OSI model.
IDS (Detect)	If this option is selected, Stormshield Network's IDS (*Intrusion Detection System*) will detect intrusion attempts on your traffic, without blocking them.
Firewall (Do not inspect)	This option only provides access to basic security functions and will merely filter your traffic without inspecting it.

Inspection profile

Depending on the direction of the traffic, IPS_00 to 09	You can customize the configuration of your security inspection by assigning a predefined policy to it, which will appear in the filter table. Numbered configurations can be renamed in the menu **Application protection** > **Inspection profiles**. The value suggested by default (**Depending on the direction of the traffic**) uses the IPS_00 profile for incoming traffic and the profile IPS_01 for outgoing traffic.

Application inspection

Antivirus	The **On** / **Off** buttons allow you to enable or disable the antivirus in your filter rule. Antivirus analyses will only be run on HTTP, FTP, SMTP, POP3 protocols and on their variants in SSL. They can be configured for each of these protocols in the menu **Application protection** > **Protocols**.
Sandboxing	The **On** / **Off** buttons allow you to enable or disable sandboxing (malicious files) in your filter rule. Do note that Advanced antivirus must be used when this option is enabled. Antivirus analyses will only be run on HTTP, FTP, SMTP, POP3 protocols and on their variants in SSL. They can be configured for each of these protocols in the menu **Application protection** > **Protocols**.
Antispam	The **On** / **Off** buttons allow you to enable or disable the antispam in your filter rule. This analysis is only run on SMTP, POP3 protocols and on their variants in SSL. They can be configured for each of these protocols in the menu **Application protection** > **Protocols**.

URL filtering	To enable this filtering method, select an URL filter profile from the suggested profiles.
SMTP filtering	To enable this filtering method, select an SMTP filter profile from the suggested profiles. Selecting the SMTP filter policy also enables the POP3 proxy in the event the filter rule allows the POP3 protocol.
FTP filtering	The **On** / **Off** buttons allow you to enable or disable FTP filtering in your filter rule, in line with the FTP commands defined in FTP plugin (**Protocols** module).
SSL filtering	To enable this filtering method, select an SSL filter profile from the suggested profiles.

Comments

You can add a description that will allow distinguishing your filter rule and its characteristics more easily.

Comments on new rules indicate the date on which they were created and the user who created them, if the rules were not created by the "admin" account, in the form of "Created on {date} by {login} ({IP address})". This automatic information may be disabled by unselecting the option "Comments about rules with creation date (Filtering and NAT)" found in the Preferences module.

NAT tab

The principle of NAT (*Network Address Translation*) is to convert an IP address to another when passing through the firewall, regardless of the source of the connection. It is also possible to translate ports through NAT.

Checking the policy in real time

The firewall's translation policy is one of the most important elements for the security of the resources that the firewall protects. Although this policy is constantly changing to adapt to new services, new threats and new user demands, it has to remain perfectly coherent so that loopholes do not appear in the protection provided by the firewall.

The art of creating an effective filter policy is in avoiding the creation of rules that inhibit other rules. When a filter policy is voluminous, the administrator's task becomes even more crucial as the risk increases. Furthermore, during the advanced configuration of very specific translation rules, the multiplicity of options may give rise to the creation of a wrong rule that does not meet the administrator's needs.

To prevent this from happening, the filter rule edit window has a **Configuration validator** field (located under the filter table), which warns the administrator whenever a rule inhibits another or an error has been created on one of the rules.

EXAMPLE

[Rule 2] This rule will never be applied as it is covered by Rule 1.

Actions on NAT policy rules

Search	This field makes it possible to perform searches by occurrence, letter or word. **EXAMPLE** If you enter “Any” in the field, all NAT rules containing “Any” will be displayed in the table.

New rule	Inserts a blank line after the selected line, 4 choices are available: • **Single rule**: This option allows creating an inactive NAT rule which will need to be configured. • **Source address sharing rule (masquerading)**: This option allows creating a PAT (Port Address Translation) dynamic NAT rule. This type of rule allows converting multiple IP addresses into one or N IP addresses. The value selected by default is *ephemeral_fw* (corresponding to a port range from 20000 to 59999 inclusive). The source port will also be rewritten. The wizard selects as the destination interface, the interface corresponding to the network of this source after translation. • **Separator – rule grouping**: This option allows inserting a separator above the selected line. This separator makes it possible to group rules that apply to traffic going to different servers and helps to improve the NAT policy's readability and visibility by indicating a comment. Separators indicate the number of grouped rules and the numbers of the first and last rules in the form: "*Rule name* (contains the *total number* of rules, from *first* to *last*)". You can collapse or expand the node of the separator in order to show or hide the rule grouping. You can also copy/paste a separator from one location to another. • **Static NAT rule (bimap):** The principle of static address translation is to convert an IP address (or N public IP addresses) to another (or N private IP addresses) when going through Firewall, whatever the origin of the connection. A wizard window will allow you to map a private IP address to a public (virtual) IP address by defining their parameters. You must also choose from the drop-down lists the **Private** and **virtual** hosts for your IPs, as well as the interface on which you wish to apply them. The **Advanced properties** field makes it possible to restrict the application to a port or port group, and enable ARP publication, which may provision the IP via the firewall's MAC address. You are however advised to restrict access to a port or a port group through a filter rule corresponding to this traffic. This allows adding other criteria to it in order to make this filter more accurate. Click on **Finish** to confirm your configuration. DO note that for an N-to-N bi-map rule, original and translated address ranges, networks or host groups must be of the same size. Bi-directional translation is generally used to allow access to a server from the outside with a public IP address that is not the same as the host's real address The "bi-map" action supports address ranges. Source and translated addresses are used in the following order: the "smallest" address in the source field is translated to the "smallest" address in the translated field. When a virtual IP address is selected, the corresponding interface will be selected automatically. This interface will be used as the source of the redirection rule and as the destination for rules that rewrite the source.
Delete	Deletes the selected line.
Move up	Places the selected line before the line just above it.

Move down	Places the selected line after the line just below it.
Expand all	Expands all rules in the tree.
Collapse all	Collapses all folders in the directory.
Cut	Cuts a NAT filter rule in order to duplicate it.
Copy	Copies a NAT rule in order to duplicate it.
Paste	Duplicates a NAT rule after having copied it.
Search in logs	Whenever a NAT rule is selected, click on this button to automatically search for the name of the rule in the "All logs" view (**Logs** > **Audit logs** > **Views** module). If the selected rule has not been named, a warning message will indicate that the search cannot be performed.
Search in monitoring	Whenever a NAT rule is selected, click on this button to automatically search for the name of the rule in the connection monitoring module.

Advanced	**Reset rules statistics**	Clicking on this button will reinitialize the digital and graphical counters showing how NAT rules are used, located in the first column of the table.
	Reset columns	When you click on the arrow on the right in the field containing a column's name (example: **Status**), you will be able to display additional columns or remove columns so that they will not be visible on the screen, by checking or unchecking them.

> **EXAMPLE**
> Tick the options "**Name**" and "**Src port**" which are not displayed by default.
> By clicking on **reset columns**, your columns will be reset to their original settings, before you selected any additional columns. As such, "**Name**" and "**Src port**" will be hidden again.

> **NOTE**
> If you click quickly 10 times on the "Up" button, you will see that the rule moves up but the waiting window will only appear when you leave the button for 2 or 3 seconds. And at the end, only a single command will be executed. Rules can be moved more much fluidly as such.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of NAT rules:

- New rule (Single rule, Source address sharing rule [masquerading], Separator - Rule grouping, Static NAT rule [bimap]),
- Delete,
- Cut,
- Copy,
- Paste,

- Search in logs,
- Search in monitoring.

Mathematical comparison

Whenever you come across a drop-down list of objects in the columns (except **Status** and **Action**) a mathematical operator icon will appear ( ). It can only be used if an object other than **Any** has been selected.

You can therefore customize the parameters of your traffic using the following icon in 4 different ways:

- "=" (or): the value of the attribute corresponds to what is selected.
- "!=" (or) the value of the attribute is different from what has been selected.
- "<" (or ; used for source and destination ports only): the port number of the traffic is lower than what is selected.
- ">" (or ; used for source and destination ports only): the port number of the traffic is higher than what is selected.

Adding/modifying objects

Some drop-down lists offer the button, which leads to a pop-up menu:

- **Create an object**: new objects can be created directly from the Filter/NAT module
- **Edit object**: when an object is in a field, it can be edited directly to modify it (name, IP address for a host, adding the object to a group, etc.), except for read-only objects ("**Any**", "**Internet**", etc).

NAT table

This table allows you to define the NAT rules to apply. The firewall will assess rules in their order of appearance on the screen: one by one from the top down. Place them in the right order so that you obtain a coherent result. Once it comes upon a rule that corresponds to the request, the will perform the specified action and stop there.

It is therefore important to define rules from the **most restrictive to the most general**.

The NAT table consists of two parts - Original traffic (before translation) and Translated traffic.

Reorganizing rules

Every rule can be dragged and dropped so that the policy (filter or NAT) can be reorganized easily. The symbol as well as the "Drag and drop to reorganize" tool tip appear when you scroll over the beginning of the rule.

Status

This column shows the status of the rule: On /Off . Double-click on it to change its status. By doing this once, you will enable the NAT rule. Repeat the operation to disable it.

> **NOTE**
> Source address translation manages stateless IP protocols (GRE) but with the following restriction:
> if two clients go through the same firewall, they will not be able to connect to the same server at

the same time. Stormshield Network's intrusion prevention engine will block packets received by the second client.
After 5 minutes, the intrusion prevention engine will deem the session too old and will allow the second client to take over.

General tab in the rule editing window

General

Status	Select **On** or **Off** to respectively enable or disable the rule being edited.
Comments	You can enter comments in this area; they will be displayed at the end of the rule when the address translation policy is displayed.

Advanced properties

Rule name	You can assign a name to the NAT rule; this name will be used in logs and facilitates identification of the NAT rule during searches in logs or views (**Logs - Audit logs** menu).

Original source before translation

General tab

General

User	The rule will apply to the user or the user group that you select in this field. There are three choices by default: • **"No user"**: this option clears the user field and stops applying criteria to the rule. • **"Any user"**: refers to any authenticated user. • "**Unknown users**": refers to any unknown or unauthenticated user.
Source hosts	The rule will apply to the object that you select in this field. The source host is the host from which the treated packet originated: it is the sender of the packet. You can **Add** or **Delete** objects by clicking on and **Create** objects by clicking on .
Incoming interface	Interface on which the translation rule applies, presented in the form of a drop-down list. By default, the firewall selects it automatically according to the operation and source and destination IP addresses. It can be modified to apply the rule to another interface. It can be modified to apply the rule to another interface. This also allows specifying a particular interface if "Any" has been selected as the source host.

Click on **OK** to confirm your configuration.

Advanced properties tab

Advanced properties

Source port	This field allows specifying the port used by the source host. By default, the "Stateful" module memorizes the source port used and only this port will then be allowed for return packets.
Source DSCP	This field refers to the DSCP code of the received packet.

Authentication

Authentication method	This field allows restricting the application of the filter rule to the selected authentication method.

Click on **OK** to confirm your configuration.

Original destination before translation

General tab

General

Destination hosts	Select the destination host of the traffic from the object database in the drop-down list.
Destination Port	If you wish to translate the traffic's destination port, select one from the objects in the drop-down list. The object "Any" is selected by default.

You can **Add** or **Delete** objects by clicking on and **Create** objects by clicking on . Click on **Ok** to confirm your configuration.

> **NOTE**
> Load balancing types other than a connection hash can be selected with a destination port range.

Advanced properties tab

Advanced properties

Outgoing interface	This option allows selecting the outgoing interface for the translated traffic. By default, the firewall selects it automatically according to the operation and source and destination IP addresses. It can be modified to restrict the rule to a particular interface.
ARP publication	This option makes the IP address to be published available via the firewall's MAC address.

> **NOTE**
> The ARP publication option is now assigned to the original destination (traffic before translation), whose IP address is indeed published, and not to the translated destination.

Source after translation

General tab

General

Translated source host	The rule will apply to the object that you select in this field. The translated source host refers to the new IP address of the source host, after its translation by NAT.
Translated source port	This field allows specifying the source port used by the source host after translation. By default, the "Stateful" module memorizes the source port used and only this port will then be allowed for return packets. The creation of a *source address sharing* rule (masquerading) assigns the value *ephemeral_fw* to this field.

Select a random translated source port	By selecting this option, the firewall will randomly select the translated source port from the list (e.g.: *ephemeral_fw*). This makes it possible to avoid an anticipation of the following connections as the source ports are assigned consecutively , thereby strengthening security.

Click on **OK** to confirm your configuration.

Advanced properties tab

Load balancing

Load balancing type	This option allows distributing IP addresses of sources that sent the packet after translation. The load balancing method depends on the algorithm used. Several load balancing algorithms are available: • **None**: No load balancing will be carried out. • **Round-robin**: This algorithm allows fairly distributing the load among the various IPs of the selected address range. Each of these source IP addresses will be rotated. • **Source IP hash**: The source address will be hashed in order to choose the address to use from the range. This method allows guaranteeing that a given source address will always be mapped to the same address range. • **Connection hash:** Users can now choose the hash by connection (source IP address + source port + destination IP address + destination) as a load balancing method in their NAT rules. This allows connections from one source to the same server to be distributed according to the source port and source IP address. • **Random:** The firewall randomly selects an address from the selected address range
ARP publication	This option makes the IP address to be published available via the firewall's MAC address.

Click on **OK** to confirm your configuration.

Destination after translation

General tab

General

Translated destination host	This field allows selecting the destination host of the translated packet from the drop-down list of objects.
Translated destination port	This field allows specifying the port used by the destination host.

Click on **OK** to confirm your configuration.

Advanced properties tab

Load balancing types other than a connection hash can be selected with a destination port range.

Load balancing

Load balancing type	This option allows distributing the transmission of packets among several destination IP addresses. The load balancing method depends on the algorithm used. Several load balancing algorithms are available: • **None**: No load balancing will be carried out. • **Round-robin**: This algorithm allows fairly distributing the load among the various IPs of the selected address range. Each of these source IP addresses will be rotated. • **Source IP hash**: The source address will be hashed in order to choose the address to use from the range. This method allows guaranteeing that a given source address will always be mapped to the same address range. • **Connection hash:** Users can now choose the hash by connection (source IP address + source port + destination IP address + destination) as a load balancing method in their NAT rules. This allows connections from one source to the same server to be distributed according to the source port and source IP address. • **Random:** The firewall randomly selects an address from the selected address range
Between ports	This option allows distributing the transmission of packets among several destination ports. The load balancing method depends on the algorithm used. The load balancing algorithms are the same as the ones described earlier.

Click on **OK** to confirm your configuration.

Protocol

Protocol

Depending on the protocol type that you choose here, the following field that appears will vary:

Protocol type	Select the desired protocol type. The value of the following fields varies according to your choice. • Automatic protocol detection (default), • Application protocol, • IP protocol. • Ethernet protocol.
Application protocol	The advantage of this choice is being able to apply application analysis on a port other that the default port. When this protocol type is selected: • Application protocol: Select the desired protocol from the drop-down list. • IP protocol: the IP protocols concerned will change according to the selected application protocol.
IP protocol	When this protocol type is selected: • Application protocol: No application analysis. • IP protocol: Select the desired protocol from the drop-down list. Additional fields may appear depending on the protocol selected.
Ethernet protocol	When this protocol type is selected, select the desired Ethernet protocol from the drop-down list.

Options

Log level	Logging traffic allows facilitating diagnosis and troubleshooting. The results will be stored in the filter log files.
NAT inside IPsec tunnel (before encryption, after decryption)	If the option has been selected, the encryption policy will be applied to the translated traffic. The NAT operation is performed just before encryption by the IPsec module when packets are sent and after decryption when packets are received.

Comments

You can add a description that will allow distinguishing your NAT rule and its characteristics more easily.

Comments on new rules indicate the date on which they were created and the user who created them, if the rules were not created by the "admin" account, in the form of "Created on {date} by {login} ({IP address})". This automatic information may be disabled by unselecting the option "Comments about rules with creation date (Filtering and NAT)" found in the Preferences module.

HIGH AVAILABILITY

This module will allow you to create first of all, a cluster or a group of firewalls. Once this is done, another firewall can be added to join the cluster that you have just initialized.

Do note that only traffic relating to high availability must pass through HA links. The VLAN creation wizard, for example, does not allow selecting HA interfaces to support VLANs in the process of being created.

Stormshield Network's high availability operates in "Active/passive" mode: Consider a cluster containing 2 firewalls. If the firewall considered "active" fails, or if a cable has been disconnected, the second firewall considered "passive" will seamlessly take over. As such, the "passive" firewall becomes "active".

A video from Stormshield Network's WebTV on YouTube will guide you step by step in the configuration of a group of Stormshield Network firewalls (cluster). Click on this link to access the video: Configuring a Stormshield Network firewall cluster.

The configuration of high availability takes place in 4 steps:

- Step 1: Creating a cluster / joining an existing cluster
- Step 2: Configuring network interfaces: the main link and the secondary link (optional)
- Step 3: Defining the cluster's pre-shared key
- Step 4: Summary of the steps and application of configured settings

Once you are done with these 4 steps, a new screen will appear suggesting new configurations within the high availability module.

NOTE
A communication link between members of a cluster has to be set up from a protected interface. The configuration can be changed in the **Interfaces** module.

Step 1: Creating or joining a high availability cluster

Create a cluster	If this option is selected, the firewall will be prepared to receive other firewalls and will add itself to the cluster.

Join a cluster	If this option is selected, the appliance will attempt to connect to the firewall with the IP address defined during the creation of the cluster. As such, this second firewall will retrieve information from the first and synchronize with it. The cluster therefore comprises two firewalls: when the first firewall fails, the second will take over transparently. **NOTE** At the end of the wizard, the appliance will be rebooted. Once the reboot is complete, the appliance will be part of the cluster, and therefore no longer exists as an entity, but as a member of the cluster. **WARNING** If you choose to "join" a cluster, it implies that you have already created one beforehand, and have selected the option "**Create a cluster**" and have performed the necessary configuration to set it up on the first firewall.

WARNING
It is important to avoid creating a cluster twice, as this would mean that you would be setting up two high availability clusters, each containing a firewall, and not a high availability cluster containing 2 firewalls.

NOTE
A member of a cluster can be forced to be the active firewall, even if members of the group have differing firmware versions.

Step 2: Configuring network interfaces

If you have chosen to create a cluster

Configure the main link

Interface	Main interface used for linking both firewalls that make up the cluster. Select it from the list of objects in the drop-down list.
Define name	Define a customized name for the main link.
Define the IP address and network mask	Enter the IP address and subnet mask dedicated to your main link. The format is expressed in address / mask.

Secondary link (optional)

If the firewall does not receive responses on the main link, it will attempt to connect to this secondary link. This will prevent both firewalls from switching to active / active mode if a problem arises on the main link.

Use a second communication link	Select this option in order to enable the fields below it and to define a secondary link for your cluster.
Interface	Secondary interface used for linking both firewalls that make up the cluster. Select it from the list of objects in the drop-down list.
Define name	Define a customized name for your secondary link.
Define the IP address	Enter the IP address for your secondary link.

NOTE
In order for a link to work, both members of the cluster have to use the same interface.
If the nodes of the cluster communicate through an Ethernet interface, the interface has to be reserved solely for this purpose. It will not be supported as the parent interface of a virtual VLAN interface.
The interface that is used for communications between the nodes of a cluster can be isolated in a VLAN. In this case, some of the advanced features relating to the communication of cluster members will not be available.

If you have chosen to join a cluster

This option assumes that a cluster has already been created beforehand, in order for a firewall to be able to join it.
As such, some of the information from the first firewall created will be copied.

Configure the main link

Interface	Main interface used for linking both firewalls that make up the cluster. This has to be the same interface that you had selected during the creation of the cluster on the first firewall.
Define the IP address and network mask	IP address and network mask dedicated to your main link. The format is expressed in address / mask. This address has to belong to the same sub-network as the one defined when creating the cluster on the first firewall.

Secondary link (optional)

If the firewall does not receive responses on the main link, it will attempt to connect to this secondary link. This will prevent both firewalls from switching to active / active mode if a problem arises on the main link.

Use a second communication link	Select this option in order to enable the fields below it and to define a secondary link for your cluster. This option must only be selected if it was also selected during the creation of the cluster on the first firewall.
Interface	Secondary interface used for linking both firewalls that make up the cluster. This has to be the same interface that you had selected during the creation of the cluster on the first firewall.
Define the IP address	IP address for your secondary link. This address has to belong to the same sub-network as the one defined when creating the cluster on the first firewall.

> **NOTE**
> In order for a link to work, both members of the cluster have to use the same interface.

Step 3: Cluster's pre-shared key and data encryption

If a cluster is being created

Pre-shared key

To secure the connection between members of the cluster, you must define a pre-shared key. This key will only be used by firewalls that are joining the cluster for the first time.

New pre-shared key	Define a password/pre-shared key for your cluster.
Confirm	Confirm the password/pre-shared key that you have just entered in the previous field.
Password strength	This progress bar indicates your password's level of security: "Very Weak", "Weak", "Medium", "Good" or "Excellent". You are strongly advised to use uppercase letters and special characters.

Communication between firewalls in the high availability cluster

Encrypt communication between firewalls	By default, communications between the firewalls are not encrypted, since the link used by high availability is a dedicated link. In some architectures, the high availability link is not dedicated, but if you wish to prevent inter-cluster communications from being intercepted, they can be encrypted in AES, for example. **WARNING** 1. Selecting this option can adversely affect the performance of your HA cluster. 2. Only connections, and not their contents, pass through the HA link.
Configurer Unicast synchronization instead of Multicast synchronization	This option makes it possible to configure a unicast synchronization between members of a cluster during the creation of the cluster. It is **required** in order to deploy high availability in environments that do not support the multicast protocol, such as certain cloud hosting platforms.

Swap configuration

Enable link aggregation when the firewall is passive	When this option is enabled in a configuration that uses link aggregation (LACP), aggregates will be enabled even on the passive member of the cluster. This option is enabled by default.

Click on **Next**.

If a cluster exists

IP address of the firewall to contact	Enter the IP address that you had defined in the wizard during the creation of the cluster (IP address of the main or secondary link).
Pre-shared key	Enter the password/pre-shared key that you had defined in the wizard during the creation of the cluster. This icon allows you to view the password in plaintext to check that it is correct.

Step 4: Summary and finalizing the cluster

If a cluster is being created

After having viewed the summary of your configurations, click on **Finish**. The following message will appear:
This firewall is ready to run in high availability. You may now configure another firewall to add it to the cluster.

It also indicates whether the **Deploy the cluster in a Cloud environment** box has been ticked.

Now that your cluster has been created, a new screen will appear when you attempt to access this module.

If a cluster exists

After having viewed the summary of your configurations, click on **Finish**. The following message will appear:
This firewall has to be rebooted in order to add a firewall to the cluster. Join the cluster?

To confirm the configuration, this firewall will join the cluster and synchronize the initial configuration. It will then restart in order to apply the configuration. To access this cluster, you need to connect to the active firewall.

> **NOTE**
> This step may take a long time on entry-level models. Do not unplug the firewall.

High availability screen

Communication between firewalls in the high availability cluster

Main link	Main interface used to link two firewalls that make up the cluster. Select it from the list of objects in the drop-down list.
Use a second communication link	Select this option to enable the fields below it and to define a secondary link for your cluster.
Secondary link	Secondary interface used to link both firewalls that make up the cluster. Select it from the list of objects in the drop-down list.

WARNING
You are advised to use a secondary link when you wish to change the interface used as the main link. Communications between members of the cluster may be disrupted when the link is changed, which may cause the cluster to stop functioning.

Advanced properties

Change the pre-shared key between the firewalls in the high availability cluster

New pre-shared key	In this field, the pre-shared key or the password defined during the creation of the cluster can be changed.
Confirm password	Confirm the password/pre-shared key that you have just entered in the previous field.
Password strength	This progress bar indicates your password's level of security: "Very Weak", "Weak", "Medium", "Good" or "Excellent". You are strongly advised to use uppercase letters and special characters.

Quality indicator

Active firewall if equal

This option designates one firewall as the active firewall in the event both firewalls have the same quality.

The aim of designating an active firewall is to keep as many logs as possible on the same firewall or give priority to the traffic on a specific firewall. If the active firewall fails, or if a cable is accidentally unplugged, the other firewall will take over as the active firewall.

Automatic	If you select this option, no priority will be assigned.
This firewall (<its serial number >)	By selecting this option, you will set this firewall as the active firewall; the second firewall will take over from it if it malfunctions or is unplugged.
The other firewall (remote) (<its serial number >)	By selecting this option, you will set the remote firewall as the active firewall; it will take over if the first firewall malfunctions or is unplugged. **WARNING** Selecting this option will cause the firewalls to swap immediately, or make this firewall the active firewall, logging the user out of the administration interface.

Session synchronization

Enable synchronization based on connection duration	This option makes it possible to activate session synchronization depending on the duration of these sessions. Only connections with durations higher than or equal to the value specified in the **Minimum duration of connections to be synchronized (seconds)** field will be synchronized. Sessions shorter than the specified value will be ignored during synchronization. This option therefore makes it possible to avoid synchronizing very short connections that may exist in large numbers, such as DNS requests, for example.

Minimum duration of connections to be synchronized (seconds)	Specify the minimum duration (in seconds) of connections that need to be synchronized. A value of 0 means this option has been disabled.

Swap configuration

When surrounding appliances change from a cluster to bridge mode, the change is applied faster with this option.

Reboot all interfaces during switchover (except HA interfaces)	If this option is enabled, interfaces on the bridge are reinitialized during the swap to force switches connected to the firewall to renew their ARP tables.
Enable link aggregation when the firewall is passive	When this option is enabled in a configuration that uses link aggregation (LACP), aggregates will be enabled even on the passive member of the cluster.
Periodically send gratuitous ARP requests	If this option is selected, you will send ARP announcements at regular intervals so that the different devices on the network (switches, routers, etc) can update their own ARP tables. **NOTE** Even during the passive stage, the firewall will still send an ARP announcement, regardless of this option.
Frequency (in seconds)	The frequency of ARP requests can be defined in this field, up to a maximum of 9999 seconds.

Force MAC address synchronization	This option lets you choose whether MAC address synchronization should be forced during a cluster failover. The activation or deactivation of this synchronization is immediate. MAC address synchronization is enabled by default on physical firewalls and disabled by default on virtual machines (EVA). It may be necessary to disable this option in configurations using link aggregation (LACP), for example.

Impact of the unavailability of an interface on a firewall's quality indicator

Interface	This column lists all of your firewall's Ethernet interfaces.
Weight [0-9999]	The weight assigns a relative value to the interface. "100" has been set by default for the listed interfaces. They all therefore have the same weighting. This criterion can be modified by selecting the relevant checkbox. E.g. specifying that the "in" interface is more important than the "out" interface and the other interfaces by assigning it a value of 150. **NOTE** Set all unused interfaces to 0 so that they will not affect the quality calculation.

> **NOTE**
> Disabled network interfaces do not appear in the high availability quality calculations.

Next, click on **Apply**.

HOST REPUTATION

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

Using his security policy, the administrator can block the connections of hosts with a bad reputation.

Three criteria are taken into account when calculating a host's reputation:

- minor and major alarms generated by the host,
- the results of the sandboxing analysis of files exchanged by the host,
- the results of the antivirus analysis of files hosted and passing through the host,

Configuration tab

This tab makes it possible to enable host reputation management and define the respective weight of the various criteria involved in the calculation of a reputation.

General

	This button makes it possible to enable or disable host reputation management.

Alarms

Major [0-20]	Adjust the slider in order to define the weight of major alarms raised by a host in the calculation of its reputation.
Minor [0-20]	Adjust the slider in order to define the weight of minor alarms raised by a host in the calculation of its reputation.

Antivirus

Infected [0-100]	Adjust the slider in order to define the weight of infected files detected for a host in the calculation of this host's reputation.
Unknown [0-20]	Adjust the slider in order to define the weight of files that could not be scanned (encrypted files, password-protected files, etc).
Scan failed [0-20]	Adjust the slider in order to define the weight of files for which the antivirus scan failed during the calculation of a host's reputation (corrupted file, corrupted antivirus base, etc.).

Sandboxing

Malicious [0-100]	Adjust the slider in order to define the weight of malicious files detected for a host in the calculation of this host's reputation.
Suspicious [0-100]	Adjust the slider in order to define the weight of suspicious files detected for a host in the calculation of this host's reputation.

Scan failed [0-20]	Adjust the slider in order to define the weight of files for which sandboxing failed during the calculation of a host's reputation (e.g.: corrupted files).

Statistics

Reset scores for all hosts in the database	Clicking on this button will erase the reputation scores of all hosts contained in the reputation database. The scores of all these hosts will then be reset to zero, and will change according to the settings selected in the **Alarms, Antivirus** and **Sandboxing** categories. If "block" filter rules are applied based on reputation scores, hosts will only be blocked after their scores have increased.

Hosts tab

This tab enables the selection of hosts on the internal network for which a reputation needs to be calculated.

Included list

This table enables the definition of hosts for which a reputation needs to be calculated. It is possible to **Add** or **Delete** hosts, host groups, networks or IP address ranges using the relevant buttons.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of monitored hosts:

- **Add**,
- **Remove**.

Advanced properties

Excluded list

This table allows defining the hosts to be excluded from the reputation calculation. It is possible to **Add** or **Delete** hosts, host groups, networks or IP address ranges using the relevant buttons.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of excluded hosts:

- **Add**,
- **Remove**.

IDENTIFICATION PORTAL

For the sake of strengthening security, the connection to the authentication portal and to the Web administration interface is possible only by forcing certain options in the SSL protocol. SSL version v3 is disabled and the TLS versions enabled, in compliance with the recommendations given by the French Network and Information Security Agency (ANSSI).

Connection

In order to configure your Stormshield Network firewall, you need to log onto the web administration interface.

Configuration of a firewall is only accessible to administrators of the product.
The "super admin" user or the administrator who holds all privileges can assign privileges to users and/or user groups in the menu **System** > **Administrators**.

Presentation

The connection module consists of two sections:

- A static section
- A collapsible section: Options

A third, optional panel appears when a **Disclaimer for access to the administration interface** has been configured on the firewall (see **Configuration** > Firewall administration tab).

The information required depends on whether it is the administrator's first connection to the firewall.

ID	This field is reserved for users who have at least basic privileges.
Password	User's password, which he will be asked to enter upon his initial connection. For a default configuration, no passwords need to be entered (empty field).
Authentication with SSL certificate	If this option is selected, the fields **Username** and **Password** will no longer be necessary, and therefore grayed out. The following message will appear: *"Using a certificate will allow you to authenticate automatically. Enable automatic authentication?"*. ". Select **Manual authentication** or **Automatic authentication.** **REMARKS** The automatic connection option can be enabled automatically in the section **Preferences** > **Connection settings** > *Connect automatically with an SSL certificate.*
Log In	Clicking on this button or pressing "Enter" will allow sending connection information to the firewall.

WARNING
The Stormshield Network Firewall is case-sensitive and distinguishes uppercase and lowercase letters, both for the user name as well as for the password.

Options

Language	Language of the web administration interface. When the user chooses a new language for the web interface, the authentication page will reload in the selected language. Available languages are English, French, Polish, Hungarian and German.
Read only	Allows connecting in "read-only" mode. You will then be able to connect to the firewall without modify privileges using an account that ordinarily has such privileges. This allows the user to refrain from using modification privileges if they are not necessary.

REMARKS

- Options are contained in a cookie. Users therefore store their connection preferences on their browsers.
- If the "read only" option has been enabled in a cookie during the connection to the authentication page, to avoid confusion, part of the options will be presented to the user as deployed options.

Error notifications

When a field is empty

If a user attempts to authenticate without having entered the **User** or **Password** field, authentication will not begin and the message "This field should not be empty" will appear.

When "Caps lock" has been enabled

If this button has been enabled when the user enters his password, a warning icon will indicate that "Caps Lock has been enabled".

Authentication failure

When authentication fails, the message *"Authentication has failed"* will appear in red.

REMARKS

Protection from brute force attacks:
When too many requests are sent with the wrong password, the following message will appear: "Protection of authentication from brute force attacks has been enabled. The next authentication attempt will be possible in <number of seconds>".

When TOTP authentication has been enabled

When TOTP is enabled as the authentication method to access the web administration interface, once a valid administrator login (other than the *admin* super administrator account) and password pair is entered, a second window will appear, containing two fields:

- In the first section, a message asks the administrator to enroll for TOTP through the enrollment page on the captive portal if it has not already been done.
- A field in which the TOTP must be entered to fully validate the authentication of the administrator who enrolled for TOTP.

The “admin” account, super administrator

By default, only one user has administration privileges on Stormshield Network products – the “admin” account (whose login is “admin”). This administrator holds all privileges and can perform certain operations such as the modification of a user’s authentication method, for example.

WARNING
The administrator account has the value “admin” as login **and** password by default.

REMARKS
Given the privileges assigned to the “admin” account, Stormshield Network recommends that you use this account only for tests or maintenance operations.
Only the “admin: user can assign administration privileges to other users.

Logging off

The procedure for logging off the firewall is as follows:

1. In the drop-down menu with the name of the connected user (on the top right side of the interface), select **Log off**.
2. Next, click on **Quit** to confirm.
   The administration interface will go back to the connection window.
   If you **Cancel**, the interface will return the user to the main screen, without any impact on how the program runs.

IMPLICIT RULES

Implicit filter rules

This screen shows that it is possible to automatically generate various IP filter rules in order to allow the use of some of the firewall's services. If a service is enabled, the firewall will automatically create the necessary filter rules, without having to create "explicit" rules in the filter policy.

To detect and block SYN Flood attacks against the firewall's internal services, implicit rules applying to the firewall's internal services must be disabled and replaced with equivalent explicit rules. In this case, the firewall will generate specific logs that allow logging denial of service attempts by way of such attacks.

Rule table

The table contains the following columns:

Enabled	Displays the status of the rule. Double-click to enable/disable the implicit rule.
Name	Displays the name of the implicit rule. This name cannot be modified;

The following rules appear in the **Name** column:

- **Allow mutual access to the administration server (port 1300) between the members of a firewall cluster (HA)**: this allows the different members of the HA cluster to communicate with each other.
- **Allow ISAKMP (UDP port 500) and the ESP protocol for IPsec VPN peers**: IPsec VPN peers will be able to contact the firewall through both of these protocols which make it possible to secure data circulating over IP traffic.
- **Allow protected interfaces to access the firewall's DNS service (port 53)**: users can contact the DNS service and therefore use the DNS cache proxy if it has been enabled.
- **Block and reinitialize ident requests (port 113) for modem interfaces (dialup)**.
- **Block and reinitialize ident requests (port 113) for ethernet interfaces**.
- **Allow protected interfaces (serverd) to access the firewall's administration server (port 1300)**: administrators will be able to log in via their internal networks to port 1300 on the firewall. This service is used especially by related Stormshield tools (e.g., Stormshield Network Centralized Management).
- **Allow protected interfaces to access the firewall's SSH port**: enables access to the firewall via SSH in order to log in using command lines from a host located on the internal networks.

- **Allow interfaces associated with authentication profiles (Authd) to access the authentication portal and the SSL VPN**: a rule allowing access to the https service (port 443) will be created for each interface associated with an authentication profile that has enabled the captive portal. Users can then authenticate and access the SSL VPN from the networks corresponding to these interfaces.
- **Allow access to the firewall's web administration server (WebAdmin)**: administrators will be able to log on to the web administration interface.

> **NOTE**
> This rule allows access to the captive portal, and therefore the web administration interface for all users connected from a protected interface. To restrict access to web administration (*/admin/* directory), define one or several hosts in the **System** module > **Configuration** > **Firewall administration** tab. A table will allow you to restrict access to these pages at the web application level.

- **Allow "Bootp" requests with an IP address specified for relaying DHCP requests**: BOOTP service (Bootstrap Protocol) requests to a DHCP server relayed by the firewall are allowed when they use an IP address specified in the configuration of the DHCP relay (option "IP address used to relay DHCP queries"). This option is used for relaying the DHCP queries of remote users through an IPsec tunnel to an internal server.
- **Allow clients to reach the firewall SSL VPN service on TCP and UDP ports**: connections relating to the setup of the SSL VPN tunnel are allowed on TCP and UDP ports.
- **Allow router solicitations (RS) in multicast or directed to the firewall**: if IPv6 support has been enabled on the firewall, IPv6 nodes may send router solicitations (RS) in multicast or to the firewall.
- **Allow requests to DHCPv6 server and DHCPv6 multicast solicitations**: If IPv6 support has been enabled on the firewall, DHCPv6 clients may send solicitation requests to the server or DHCPv6 relay on the firewall.
- **Do not log IPFIX packets in IPFIX traffic**: this rule makes it possible to not include the packets that are needed for running the IPFIX protocol in logs sent to the IPFIX collector(s).
- **Allow IGMP and PIM packets to be received for dynamic multicast routing to function**: with this rule, you do not need to reject IGMP and PIM packets going to the firewall when you configure dynamic multicast routing.
- **Allow certificate analysis requests to be sent to another interface. Useful in TLS 1.3**: this rule makes it possible to transfer certificate analysis requests from one firewall interface to another.
- **Allow access to Extended Web Control resources**: this rule allows requests from the firewall to the URL classification database provider.
- **Allow access to the REST API**: this rule allows requests to the firewall's REST API over the defined port.

> **IMPORTANT**
> The following operations may be risky:
>
> - **Disabling the "Serverd" rule**: in the absence of an explicit rule, this may prevent access with related Stormshield tools that use port 1300 (e.g., Stormshield Network Centralized Management).
> - **Disabling the "WebAdmin" rule**: you will no longer have access to the web administration interface, unless an explicit rule allows it.

Advanced properties

Include outgoing implicit rules for hosted services (indispensable)	This checkbox, selected by default, enables outgoing implicit rules for services hosted by the firewall. Previously, this feature, which was found in earlier versions of the firmware, could only be modified in CLI. **IMPORTANT** These rules are indispensable for the proper operaion of the firewall. They need to be explicitly defined in the filter policy if this checkbox has been unselected.

INSPECTION PROFILES

Global configuration

Default inspection profiles

Profile for incoming traffic	Define the profile to apply to traffic entering the network via the SNS firewall. Incoming traffic represents the traffic from an unprotected interface – such as the Internet – to a protected interface such your local/internal network.
Profile for outgoing traffic	Define the profile to apply to traffic leaving the network via the SNS firewall. Outgoing traffic represents the traffic from a protected interface to an unprotected interface.

New alarms

Apply default model to new alarms	This option is related to the **Application protection** > **Applications and protections** module. When it is enabled, new alarms will be updated automatically and signed with the SNS signature. The following options will then be grayed out. If you wish to apply them manually, unselect the checkbox to edit them.
Action	When an alarm is raised, the configured action will be applied to the packet that set off the alarm. You can choose to **Pass** or **Block** new alarms. You will see the status you applied to the **Application protection** > **Applications and protections** module. New alarms can be found in the "**New**" column.
Level	Three alarm levels are available: "Ignore", "Minor" and "Major".
Packet capture	If this option is selected, the packet that set off the alarm will be captured.

When the log management service is saturated

Block packets that generate an alarm	When the firewall is no longer able to log events because its log management service is saturated, this option makes it possible to block all packets that generate alarms. When this option is disabled, the packets in question are not blocked and will no longer be logged.
Block packets intercepted by a filter rule configured in "Verbose (filtering log)" mode	When the firewall is no longer able to log events because its log management service is saturated, this option makes it possible to block all packets intercepted by a filter rule configured to log events. When this option is disabled, the packets in question are not blocked and will no longer be logged.

Advanced properties

Treat IPsec interfaces as internal interfaces (except virtual IPsec interfaces). Applies to all tunnels: remote networks must be explicitly legitimized.	If this option is selected, IPsec interfaces will become internal - and therefore protected - interfaces. All networks that may go through IPsec tunnels must therefore be validated, and static routes that allow them to be contacted must be declared. Otherwise, the firewall will reject the IPsec traffic. **IMPORTANT** When this checkbox is selected, the option will apply to **all** IPsec tunnels defined on the firewall.

Configuring profiles

Select the application profile associated with the protocol from the drop-down list by clicking on the arrow to the right of the field.

To return to the previous menu, click on "**Go to global configuration**".

INTERFACES

The **Interfaces** module makes it possible to manage, add or delete “network interface” network items. These represent physical or virtual communication devices between the various networks that pass through the firewall.

The module window consists of a grid containing:

- The list of the firewall's interfaces and information about them.
- A taskbar: it shows the various possible operations that can be applied to interfaces.
- The control panel of each interface: appears when an interface is edited.

> **NOTE**
> Refer to the section Allowed names to find out which characters are allowed and prohibited in various fields.

Interfaces

Interface	Name of the interface (in, out, dmz1, etc.). A tool tip displays additional information when you scroll over the interface. The icon shows the interface from which the administrator logged in. The icon shows the interface being edited (open control panel).
Port	Number of the interface’s physical port. For VLANs and modems, the port number of the parent interface appears.
Type	Type of interface (Bridge, Ethernet, etc.). Additional information can be displayed with the type (transfer rate, VLAN ID, etc.).
Status	Special statuses of an interface (disabled, not connected, monitored, etc). When the interface is enabled and connected, this column will be empty.
IPv4 address	IPv4 address of the interface and its mask, or DHCP address if the interface uses dynamic addresses.
IPv6 address	IPv6 address of the interface and its mask, or DHCP address if the interface uses dynamic addresses. This column is hidden by default if IPv6 is not enabled in the firewall’s configuration.
MAC address	Physical interface (MAC) of the interface. This column is hidden by default.
System name	Name of the interface that the firewall operating system sees (em0, vlan0, etc.). This column is hidden by default.
Comments	Comments added during the configuration of the interface (open text field).

Possible operations

Some operations can also be performed by right-clicking in the grid of interfaces. Dragging and dropping on an interface modifies its configuration (its relationships and IP address). An icon indicates whether dragging and dropping is allowed.

Enter a filter	Searches among the firewall's interfaces.

Collapse all	Collapses all interfaces in the tree.
Expand all	Expands all interfaces in the tree.
Refresh displayed data	Refreshes information found in the grid of interfaces.
Edit	Makes it possible to edit the selected network interface or one of the modem profiles.
Add	Adds a new interface. The following sections explain how to add new interfaces or change the configuration of existing interfaces.
Delete	Deletes the selected interface. Some interfaces cannot be deleted.
Monitor	Enables or disables monitoring on the selected the interface. The corresponding graphs are automatically created in **Monitoring** > **Monitoring** > **Interfaces**.
Go to monitoring	Redirects to **Monitoring** > **Monitoring** > **Interfaces**.
Check usage	In the menu on the left, shows the modules in which the interface is used.

Control panel of an interface

Interfaces can be configured in the control panel. Double-clicking on an interface displays it. The contents vary according to the type of interface selected.

- Bridge,
- Ethernet interface,
- Wi-Fi interface,
- VLAN,
- Aggregate,
- GRETAP interface,
- PPPoE/PPTP modem,
- USB/Ethernet interface (USB key/modem).

Bridge interface

Adding a bridge

Adding a bridge without members

1. Click on **Add**.
2. Scroll over **Bridge**.
3. Click on **No members**.
4. Give the new bridge a name, then click on **Apply**.
   The new bridge will be added to the interfaces and its control panel appears.

Adding a bridge that contains selected interfaces

1. Select the interfaces to include in the new bridge beforehand.
2. Click on **Add**.

3. Scroll over **Bridge**.
4. Click on **With *interface_1*, *interface_2* ....**
5. Give the new bridge a name, then click on **Apply**.
   The new bridge will be added to the interfaces and its control panel appears.

Bridge control panel

Double-click on the bridge interface control panel to open it. There are several tabs in the control panel.

General configuration tab

General settings

Name	Name of the interface. This name can be changed.
Comments	Allows you to enter comments regarding the interface.

Address range

> **NOTE**
> The same options must be configured in the **IPv4** and **IPv6 address** fields. The **IPv6 address** field appears only if IPv6 is enabled in the firewall's configuration.

Dynamic IP (obtained by DHCP)	When this option is selected, the IP address of the interface will be defined by DHCP. An **Advanced DHCP properties** zone appears with the following parameters: • **DNS name (optional)**: a fully qualified DHCP host name (FQDN) can be indicated for the DHCP request. If a value is entered in this field and the external DHCP server has the option of automatically updating the DNS server, the DHCP server automatically updates the DNS server with the name of the firewall, its assigned IP address and allocated lease time (field below). • **Requested lease time (seconds)**: in addition to the DNS name, enter the duration for which the IP address is kept before renegotiation. • **Request domain name servers from the DHCP server and create host objects:** select this parameter so that the firewall will retrieve DNS servers from the DHCP server (access provider, for example) that provided its IP address. When this option is selected, two objects will be created: *Firewall_<interface name>_dns1* and *Firewall_<interface name>_dns2.* They can then be used in the configuration of the DHCP service. So if the firewall provides the users on its network with a DHCP service, the users will also benefit from the DNS servers given by the access provider.
Fixed IP (static)	When this option is selected, the IP address of the interface will be static. A grid appears, in which you must add the IP address and its subnet mask. Several IP addresses and associated masks can be added if aliases need to be created, for example. These aliases allow you to use the firewall as a central routing point. As such, an interface can be connected to various sub-networks with a different address range. If you add several IP addresses (aliases) to the same address range, these addresses must all have the same mask. Reloading the network configuration will apply this mask to the first address and a /32 mask to the addresses that follow.

Managing members

At least two interfaces must be selected to make up a bridge. To add or remove members from the bridge, move the interfaces from one section to another by using the arrows, dragging and dropping, or double-clicking on the interface.

Routing configuration tab (IPv6 only)

> **NOTE**
> This tab appears only if IPv6 is enabled in the firewall's configuration.

On each interface, bridge or aggregated interface, router advertisements (RA) can be sent periodically to all IPv6 nodes (*multicast*) of the segment via the local link address or as a response to a router solicitation (RS) from a host on the network.

This advertisement allows an IPv6 node to obtain the following information:

- The address of the default router, in this case, the address of the firewall,
- The prefix(es) used on the link (in 64 bits),
- Indication of the use of SLAAC or DHCPv6 (*Managed*)
- Indication of the retrieval of other parameters via DHCPv6 (*OtherConfig*),
- DNS parameters, if any (RFC4862).

Automatic configuration, which is native in IPv6, is stateless (*StateLess Address AutoConfiguration* - SLAAC), meaning that the server does not choose IP addresses for its clients and does not need to remember them.

For example, a host has a local link address whose uniqueness has been confirmed via NPD DAD (*Neighbor Discovery Protocol – Duplicated Address Detection*). The host will then receive the periodic or solicited RA. If SLAAC information has been specified, the host will then create one or several IPv6 addresses based on the prefix(es) advertised and its interface ID (random or based on the MAC address). The router's IP address (the firewall's address) will then be used as the default gateway.

By default, the routers advertise their presence by broadcasting the first prefix deduced from the interface. By default, DNS servers are those configured for the firewall in the **Configuration** module > **System** > **Configuration**, **Network settings** tab.

> **NOTE**
> If router advertisements have been enabled on a bridge, they will only be broadcast on protected interfaces.

Automatic configuration settings

Automatic detection	If the DHCPv6 service is enabled on the firewall (**Configuration** module > **Network> DHCP**), the firewall will automatically send out router advertisements (RA) on the corresponding interfaces, indicating to IPv6 nodes that they must be auto-configured in DHCPv6 (the options "Managed" and "Other config" will then be enabled by default). If the firewall is acting as a DHCPv6 server, the configured interface must belong to one of the address ranges entered in the DHCPv6 configuration. If the firewall is used as a relay to a DHCPv6 server, the configured interface must belong to the list of the service's listening interfaces. If the DHCPv6 service is inactive, the sending of RAs will be disabled.

Send RA	The firewall's address is sent as the default router. The information relayed by this advertisement will be described further in this manual. This configuration is recommended in order to allow hosts that are directly connected (local link) to use SLAAC.
Disable	No router advertisement (RA) has been sent out. This configuration is recommended in bridge mode if an IPv6 router is directly connected (local link).

Router advertisements (RA)

This zone can be accessed only if the **Send RA** option has been selected.

Announce the prefix extracted from the interface address	The prefix advertised is the prefix configured in the interface's IPv6 address range in the **General configuration** tab. The size of the IPv6 address mask (prefix length – CIDR) must be 64 bits.

Configuration with DHCPv6 server

The DHCPv6 server assigns addresses (Managed)	The advertisement indicates that the IPv6 addresses contacted will be distributed by the DHCPv6 service enabled on the firewall (**Configuration** module > **Network > DHCP**). This service is implemented by the firewall or a relay that is directly connected (local link).
The DHCPv6 server delivers additional options (Other config)	The advertisement indicates that other auto-configuration parameters, such as the addresses of DNS servers or other types of servers, will be issued by the DHCPv6 server (firewall or relay) that is directly connected (local link).

Advanced configuration

DNS settings

This section can be accessed if the option **The DHCPv6 server delivers additional options (Other config)** is not enabled.

Domain name	Default domain name to contact a queried server that does not have a domain.
Primary DNS server	IP address of the primary DNS server. If this field is blank, the address sent will be the address used by the firewall (**Configuration** module > **System > Configuration**, **Network settings** tab).
Secondary DNS server	IP address of the secondary DNS server. If this field is blank, the address sent will be the address used by the firewall (**Configuration** module > **System > Configuration**, **Network settings** tab).

Announced prefixes

This grid can be accessed if the option **The DHCPv6 assigns addresses (Managed)** is not enabled.

Prefixes	Prefix to announce to hosts. We recommend using the interface's prefix as the announced prefix. If the interface specifies several prefixes, this field will indicate the prefix to use.
Autonomous	Instruction to use stateless address auto-configuration (SLAAC): if this option has been selected, the host will then create one or several IPv6 addresses based on the prefix(es) advertised and its interface ID (random and/or based on the MAC address.

On link	This option specifies to the host that all hosts with the same prefix may be contacted directly, without going through the router. In IPv4, such information was deduced from the network mask.
Comments	Allows adding comments for the announced prefix.

Advanced properties tab

Other settings

MTU	Maximum length of frames (in bytes) sent over the physical medium (Ethernet) so that they are sent at one go without fragmentation. This option is not available for interfaces contained in a bridge.
MAC address	Specifies a MAC address for the bridge.
Physical MAC address	This field is not available for bridges.

Loop detection (Spanning Tree)

This section makes it possible to enable a network loop detection protocol (Spanning Tree) on the bridge. This feature is available only on SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200, SNi10, SNi20, SNi40, SNxr1200, EVA1, EVA2, EVA3, EVA4 and EVAU models.

Disable Spanning Tree protocols	Disables the use of Spanning Tree protocols (RSTP and MSTP) in the bridge. This option is enabled by default.
Enable Rapid Spanning Tree Protocol (RSTP)	Enables Rapid Spanning Tree Protocol (RSTP) on the bridge.
Enable Multiple Spanning Tree Protocol (MSTP)	Enables Multiple Spanning Tree Protocol (MSTP) on the bridge. If this option is selected, the MSTP configuration zone appears.

MSTP configuration

This zone appears only if **Enable Multiple Spanning Tree Protocol (MSTP)** is selected. On SNS firewalls, an MSTP configuration can only define one region.

Region name (MSTP region)	Enter the name of the MSTP region in which the firewall is located. It must be the same in the MSTP configuration on all network appliances belonging to this region.
Format selector	This field specifies the information needed to define a region. Its default value is 0, indicating that a region's properties are: • Its name, • Its revision number, • A fingerprint derived from MST instance numbers and VLAN identifiers included in these instances. The format selector must be the same in the MSTP configuration on all network appliances belonging to this region.

Revision number	Select a revision number for the region. The revision number must be the same in the MSTP configuration on all network appliances belonging to this region. **NOTE** To track changes more easily, the revision number may be incremented manually when the configuration of the region changes. In this case, the changed revision number must be applied to all appliances in the affected region.
Common and Internal Spanning Tree (CIST)	Priority assigned to the firewall for traffic involving VLANs that were not declared in any MSTP instances (see grid of **MSTP instances**).

MSTP instances

List of VLAN IDs in the instance	Indicate the various VLAN identifiers (list of identifiers separated by commas) included in the selected instance.
Priority	Set the priority of an MSTP instance in relation to the root bridge. which has the lowest priority. **NOTE** You are advised against declaring the firewall as the root bridge of an MSTP instance. This may create unnecessarily high network traffic on the firewall's interfaces.

Ethernet interface

The parameters of each Ethernet interface can be modified, but none can be added or deleted. When an Ethernet interface is a member of a(n):

- Bridge: some of the fields in the interface's control panel cannot be modified (grayed out) because they are inherited from the bridge.
- Aggregate: only the **Status, Name, Comments** and **Media** fields appear. The other settings are inherited from the configuration of the aggregate.

Ethernet interface control panel

Double-click on the Ethernet interface control panel to open it. There are several tabs in the control panel.

General configuration tab

Status

ON / OFF	Set the switch to **ON/OFF** to enable or disable the interface. Disabled interfaces cannot be used. An interface that has been disabled because it is not in use, or will be deployed later, is an additional security measure against intrusions.

General settings

Name	Name of the interface. This name can be changed.

Comments	Allows you to enter comments regarding the interface.
This interface is	An interface can be: • **Internal (protected)**: when this option is selected, this means that the interface is protected (a shield appears). a protected interface only accepts packets coming from a known address range, such as a directly connected network or a network defined by a static route. This protection includes remembering machines that have logged on to this interface, conventional traffic security mechanisms (TCP) and implicit rules for services offered by the firewall such as DHCP. • **External (public)**: choosing this option indicates that the interface does not benefit from the protection of a protected interface and can therefore receive packets coming from any address range (which are not assigned to internal interfaces). This type of interface is used mainly to connect the firewall to the Internet.

Address range

Address range inherited from the bridge	When this option is selected, the interface becomes part of a bridge. Several parameters, such as the address range, will then be inherited from the bridge. This will unlock the **Bridge** field. Select the parent bridge of the interface in this field.
Dynamic / Static	Selecting this option indicates that the IP address of the interface is dynamic (obtained via DHCP) or static. This will unlock the **IPv4 address** field and **IPv6 address** field if IPv6 was enabled in the firewall's configuration. The same options must be configured in both fields.
Dynamic IP (obtained by DHCP)	When this option is selected, the IP address of the interface will be defined by DHCP. An **Advanced DHCP properties** zone appears with the following parameters: • **DNS name (optional)**: a fully qualified DHCP host name (FQDN) can be indicated for the DHCP request. If a value is entered in this field and the external DHCP server has the option of automatically updating the DNS server, the DHCP server automatically updates the DNS server with the name of the firewall, its assigned IP address and allocated lease time (field below). • **Requested lease time (seconds)**: in addition to the DNS name, enter the duration for which the IP address is kept before renegotiation. • **Request domain name servers from the DHCP server and create host objects:** select this parameter so that the firewall will retrieve DNS servers from the DHCP server (access provider, for example) that provided its IP address. When this option is selected, two objects will be created: *Firewall_<interface name>_dns1* and *Firewall_<interface name>_dns2*. They can then be used in the configuration of the DHCP service. So if the firewall provides the users on its network with a DHCP service, the users will also benefit from the DNS servers given by the access provider.
Fixed IP (static)	When this option is selected, the IP address of the interface will be static. A grid appears, in which you must add the IP address and its subnet mask. Several IP addresses and associated masks can be added if aliases need to be created, for example. These aliases allow you to use the firewall as a central routing point. As such, an interface can be connected to various sub-networks with a different address range. If you add several IP addresses (aliases) to the same address range, these addresses must all have the same mask. Reloading the network configuration will apply this mask to the first address and a /32 mask to the addresses that follow.

Routing configuration tab (IPv6 only)

NOTE
This tab appears only if IPv6 is enabled in the firewall's configuration.

On each interface, bridge or aggregated interface, router advertisements (RA) can be sent periodically to all IPv6 nodes (*multicast*) of the segment via the local link address or as a response to a router solicitation (RS) from a host on the network.

This advertisement allows an IPv6 node to obtain the following information:

- The address of the default router, in this case, the address of the firewall,
- The prefix(es) used on the link (in 64 bits),
- Indication of the use of SLAAC or DHCPv6 (*Managed*)
- Indication of the retrieval of other parameters via DHCPv6 (*OtherConfig*),
- DNS parameters, if any (RFC4862).

Automatic configuration, which is native in IPv6, is stateless (*StateLess Address AutoConfiguration* - SLAAC), meaning that the server does not choose IP addresses for its clients and does not need to remember them.

For example, a host has a local link address whose uniqueness has been confirmed via NPD DAD (*Neighbor Discovery Protocol – Duplicated Address Detection*). The host will then receive the periodic or solicited RA. If SLAAC information has been specified, the host will then create one or several IPv6 addresses based on the prefix(es) advertised and its interface ID (random or based on the MAC address). The router's IP address (the firewall's address) will then be used as the default gateway.

By default, the routers advertise their presence by broadcasting the first prefix deduced from the interface. By default, DNS servers are those configured for the firewall in the **Configuration** module > **System** > **Configuration**, **Network settings** tab.

NOTE
If router advertisements have been enabled on a bridge, they will only be broadcast on protected interfaces.

Automatic configuration settings

Automatic detection	If the DHCPv6 service is enabled on the firewall (**Configuration** module > **Network> DHCP**), the firewall will automatically send out router advertisements (RA) on the corresponding interfaces, indicating to IPv6 nodes that they must be auto-configured in DHCPv6 (the options "Managed" and "Other config" will then be enabled by default). If the firewall is acting as a DHCPv6 server, the configured interface must belong to one of the address ranges entered in the DHCPv6 configuration. If the firewall is used as a relay to a DHCPv6 server, the configured interface must belong to the list of the service's listening interfaces. If the DHCPv6 service is inactive, the sending of RAs will be disabled.
Send RA	The firewall's address is sent as the default router. The information relayed by this advertisement will be described further in this manual. This configuration is recommended in order to allow hosts that are directly connected (local link) to use SLAAC.
Disable	No router advertisement (RA) has been sent out. This configuration is recommended in bridge mode if an IPv6 router is directly connected (local link).

Router advertisements (RA)

This zone can be accessed only if the **Send RA** option has been selected.

Announce the prefix extracted from the interface address	The prefix advertised is the prefix configured in the interface's IPv6 address range in the **General configuration** tab. The size of the IPv6 address mask (prefix length – CIDR) must be 64 bits.

Configuration with DHCPv6 server

The DHCPv6 server assigns addresses (Managed)	The advertisement indicates that the IPv6 addresses contacted will be distributed by the DHCPv6 service enabled on the firewall (**Configuration** module > **Network > DHCP**). This service is implemented by the firewall or a relay that is directly connected (local link).
The DHCPv6 server delivers additional options (Other config)	The advertisement indicates that other auto-configuration parameters, such as the addresses of DNS servers or other types of servers, will be issued by the DHCPv6 server (firewall or relay) that is directly connected (local link).

Advanced properties

DNS settings

This section can be accessed if the option **The DHCPv6 server delivers additional options (Other config)** is not enabled.

Domain name	Default domain name to contact a queried server that does not have a domain.
Primary DNS server	IP address of the primary DNS server. If this field is blank, the address sent will be the address used by the firewall (**Configuration** module > **System > Configuration**, **Network settings** tab).
Secondary DNS server	IP address of the secondary DNS server. If this field is blank, the address sent will be the address used by the firewall (**Configuration** module > **System > Configuration**, **Network settings** tab).

Announced prefixes

This grid can be accessed if the option **The DHCPv6 assigns addresses (Managed)** is not enabled.

Prefixes	Prefix to announce to hosts. We recommend using the interface's prefix as the announced prefix. If the interface specifies several prefixes, this field will indicate the prefix to use.
Autonomous	Instruction to use stateless address auto-configuration (SLAAC): if this option has been selected, the host will then create one or several IPv6 addresses based on the prefix(es) advertised and its interface ID (random and/or based on the MAC address.
On link	This option specifies to the host that all hosts with the same prefix may be contacted directly, without going through the router. In IPv4, such information was deduced from the network mask.
Comments	Allows adding comments for the announced prefix.

Advanced properties tab

Other settings

MTU	Maximum length of frames (in bytes) sent over the physical medium (Ethernet) so that they are sent at one go without fragmentation. This option is not available for interfaces contained in a bridge.
MAC address	Makes it possible to specify a MAC address for an interface, instead of using the address assigned by the firewall (physical MAC address by default). This option is not available for interfaces contained in a bridge.
Physical MAC address	Network card hardware MAC address.

Media

Media	Connection speed of the network. By default the firewall automatically detects the media but you can impose the use of a particular mode by selecting it in the drop-down list. **IMPORTANT** If the firewall is directly connected to an ADSL modem, you are advised to enforce the medium that you wish to use on the interface concerned.

Routing without analysis

This zone appears only if the option **Address range inherited from the bridge** is selected in the **Address range** field in the **General configuration** tab.

Authorize without analyzing	Allows letting IPX (Novell network), Netbios (on NETBEUI), AppleTalk (for Macintosh), PPPoE or Ipv6 packets pass between the bridge's interfaces. No high-level analysis or filtering will be applied to these protocols (the firewall will block or pass).

Interface routing

This zone appears only if the option **Address range inherited from the bridge** is selected in the **Address range** field in the **General configuration** tab.

Keep initial routing	This option will ask the firewall to not modify the destination in the Ethernet layer when a packet goes through it. The packet will be resent to the same MAC address from which it was received. The purpose of this option is to facilitate the integration of firewalls transparently into an existing network, as this makes it possible to avoid the need for modifying the default route of machines on the internal network. This option must be enabled to ensure that a DHCP server located on the interface in question, and which sends unicast responses to requests, runs properly **Known limitations** Features on a firewall that inserts or modifies packets in sessions may fail to function correctly. The affected features are: • Connection reinitialization caused by an alarm, • SYN proxy (enabled in filtering), • Requests to resend packets that were dropped in order to speed up analysis, • Rewriting of packets by application analyses (SMTP, HTTP and web 2.0, FTP and NAT, SIP and NAT).

Keep VLAN IDs	This option enables the transmission of tagged frames without the firewall having to be the VLAN endpoint. The VLAN tag on these frames is kept so that the Firewall can be placed in the path of a VLAN without the firewall interrupting this VLAN. The Firewall runs seamlessly for this VLAN. To use this option, the previous option "**Keep initial routing**" must be enabled.

Energy Efficient Ethernet

Enable IEEE 802.3az (EEE)	This option appears only if the network card driver supports the IEEE 802.3az (EEE) protocol. **NOTE** EEE stands for Energy Efficient Ethernet Select this checkbox to enable mechanisms that allow enabling physical layer transmitters to reduce their power consumption during periods of low data activity.

Wi-Fi interface (WLAN)

Some firewalls build in a Wi-Fi card that makes it possible to configure two WLAN access points to connect wireless equipment over 2.4 GHz or 5 GHz frequency ranges. The parameters of each WiFi interface can be modified, but none can be added or deleted.

Wi-Fi interface control panel

Double-click on a Wi-Fi interface control panel to open it.

Status

ON / OFF	Set the switch to **ON/OFF** to enable or disable the interface. Disabling a Wi-Fi interface makes it unusable even when the Wi-Fi network is enabled in the firewall's configuration. Conversely, if the Wi-Fi interface is enabled but the Wi-Fi network is disabled, the network will be unreachable. Ensure that the settings of Wi-Fi interface parameter coincide with those of the Wi-Fi network parameter (**Configuration** module > **Network** > Wi-Fi).

General settings

Name	Name of the interface. The name assigned by default can be changed. This name is not the network name (SSID).
Comments	Allows you to enter comments regarding the interface.

This interface is	An interface can be: • **Internal (protected)**: when this option is selected, this means that the interface is protected (a shield appears). a protected interface only accepts packets coming from a known address range, such as a directly connected network or a network defined by a static route. This protection includes remembering machines that have logged on to this interface, conventional traffic security mechanisms (TCP) and implicit rules for services offered by the firewall such as DHCP. • **External (public)**: choosing this option indicates that the interface does not benefit from the protection of a protected interface and can therefore receive packets coming from any address range (which are not assigned to internal interfaces). This type of interface is used mainly to connect the firewall to the Internet.

Wi-Fi

Network name	Shows the name of the Wi-Fi network (SSID). This name can be changed if necessary.
Authentication	Shows the type of security used for the authentication of the Wi-Fi network. Three choices are possible: • **Open network**: no authentication. When this option is selected, the **Security key** fields will be hidden. • **WPA** (Wi-Fi Protected Access). • **WPA 2**: WPA 2 is an upgraded form of WPA offering a higher level of security.
Security key	Allows the security key of the Wi-Fi network to be modified or displayed. Click on the button to the right of the field to display it. To modify the key, enter the new key in this field, then confirm it in the **Confirm security key** field. A progress bar will indicate the strength of the security key chosen.
AP Isolation	This feature makes it possible to prohibit devices connected to the Wi-Fi network from communicating directly with one another without going through the firewall. This option is enabled by default in public Wi-Fi hotspot configurations. However, it must be disabled for private Wi-Fi networks that link up, for example, workstations to a network-based printer connected by Wi-Fi.

Address range

Address range inherited from the bridge	When this option is selected, the interface becomes part of a bridge. Several parameters, such as the address range, will then be inherited from the bridge. This will unlock the **Bridge** field. Select the parent bridge of the interface in this field.
Dynamic / Static	Selecting this option indicates that the IP address of the interface is static. A grid appears, in which you must add the IP address and its subnet mask. Several IP addresses and associated masks can be added if aliases need to be created, for example. These aliases allow you to use the firewall as a central routing point. As such, an interface can be connected to various sub-networks with a different address range. If you add several IP addresses (aliases) to the same address range, these addresses must all have the same mask. Reloading the network configuration will apply this mask to the first address and a /32 mask to the addresses that follow.

VLAN interface

Adding a VLAN

Adding a VLAN without members

1. Click on **Add**.
2. Scroll over **VLAN**.
3. Click on **No members**.
   The new VLAN will be added to the interfaces and its control panel appears.

Adding a VLAN that contains selected interfaces

1. Select the interfaces to include in the new VLAN beforehand.
2. Click on **Add**.
3. Scroll over **VLAN**.
4. Click on **With *interface_1*, *interface_2* ....**
   The new VLAN will be added to the interfaces and its control panel appears.

VLAN interface control panel

Double-click on the VLAN interface control panel to open it. There are several tabs in the control panel.

General configuration tab

Status

ON / OFF	Set the switch to **ON**/**OFF** to enable or disable the interface. Disabled interfaces cannot be used. An interface that has been disabled because it is not in use, or will be deployed later, is an additional security measure against intrusions.

General settings

Name	Name of the interface. The name assigned by default can be changed.
Comments	Allows you to enter comments regarding the interface.
Parent interface	Physical name of the interface to which the VLAN is attached.
ID	Identifier for the VLAN, which must be any value between 1 and 4094 inclusive, and must be unique (unless it is a VLAN associated with another bridge in a crossing VLAN).
Priority (CoS)	This CoS (**Class of Service** field) priority will then be imposed for all packets sent by the VLAN.

This interface is	An interface can be: • **Internal (protected)**: when this option is selected, this means that the interface is protected (a shield appears). a protected interface only accepts packets coming from a known address range, such as a directly connected network or a network defined by a static route. This protection includes remembering machines that have logged on to this interface, conventional traffic security mechanisms (TCP) and implicit rules for services offered by the firewall such as DHCP. • **External (public)**: choosing this option indicates that the interface does not benefit from the protection of a protected interface and can therefore receive packets coming from any address range (which are not assigned to internal interfaces). This type of interface is used mainly to connect the firewall to the Internet.

Address range

Address range inherited from the bridge	When this option is selected, the interface becomes part of a bridge. Several parameters, such as the address range, will then be inherited from the bridge. This will unlock the **Bridge** field. Select the parent bridge of the interface in this field.
Dynamic / Static	Selecting this option indicates that the IP address of the interface is dynamic (obtained via DHCP) or static. This will unlock the **IPv4 address** field and **IPv6 address** field if IPv6 was enabled in the firewall's configuration. The same options must be configured in both fields.
Dynamic IP (obtained by DHCP)	When this option is selected, the IP address of the interface will be defined by DHCP. An **Advanced DHCP properties** zone appears with the following parameters: • **DNS name (optional)**: a fully qualified DHCP host name (FQDN) can be indicated for the DHCP request. If a value is entered in this field and the external DHCP server has the option of automatically updating the DNS server, the DHCP server automatically updates the DNS server with the name of the firewall, its assigned IP address and allocated lease time (field below). • **Requested lease time (seconds)**: in addition to the DNS name, enter the duration for which the IP address is kept before renegotiation. • **Request domain name servers from the DHCP server and create host objects:** select this parameter so that the firewall will retrieve DNS servers from the DHCP server (access provider, for example) that provided its IP address. When this option is selected, two objects will be created: *Firewall_<interface name>_dns1* and *Firewall_<interface name>_dns2*. They can then be used in the configuration of the DHCP service. So if the firewall provides the users on its network with a DHCP service, the users will also benefit from the DNS servers given by the access provider.
Fixed IP (static)	When this option is selected, the IP address of the interface will be static. A grid appears, in which you must add the IP address and its subnet mask. Several IP addresses and associated masks can be added if aliases need to be created, for example. These aliases allow you to use the firewall as a central routing point. As such, an interface can be connected to various sub-networks with a different address range. If you add several IP addresses (aliases) to the same address range, these addresses must all have the same mask. Reloading the network configuration will apply this mask to the first address and a /32 mask to the addresses that follow.

Routing configuration tab (IPv6 only)

NOTE
This tab appears only if IPv6 is enabled in the firewall's configuration.

On each interface, bridge or aggregated interface, router advertisements (RA) can be sent periodically to all IPv6 nodes (*multicast*) of the segment via the local link address or as a response to a router solicitation (RS) from a host on the network.

This advertisement allows an IPv6 node to obtain the following information:

- The address of the default router, in this case, the address of the firewall,
- The prefix(es) used on the link (in 64 bits),
- Indication of the use of SLAAC or DHCPv6 (*Managed*)
- Indication of the retrieval of other parameters via DHCPv6 (*OtherConfig*),
- DNS parameters, if any (RFC4862).

Automatic configuration, which is native in IPv6, is stateless (*StateLess Address AutoConfiguration* - SLAAC), meaning that the server does not choose IP addresses for its clients and does not need to remember them.

For example, a host has a local link address whose uniqueness has been confirmed via NPD DAD (*Neighbor Discovery Protocol – Duplicated Address Detection*). The host will then receive the periodic or solicited RA. If SLAAC information has been specified, the host will then create one or several IPv6 addresses based on the prefix(es) advertised and its interface ID (random or based on the MAC address). The router's IP address (the firewall's address) will then be used as the default gateway.

By default, the routers advertise their presence by broadcasting the first prefix deduced from the interface. By default, DNS servers are those configured for the firewall in the **Configuration** module > **System** > **Configuration**, **Network settings** tab.

NOTE
If router advertisements have been enabled on a bridge, they will only be broadcast on protected interfaces.

Automatic configuration settings

Automatic detection	If the DHCPv6 service is enabled on the firewall (**Configuration** module > **Network> DHCP**), the firewall will automatically send out router advertisements (RA) on the corresponding interfaces, indicating to IPv6 nodes that they must be auto-configured in DHCPv6 (the options "Managed" and "Other config" will then be enabled by default). If the firewall is acting as a DHCPv6 server, the configured interface must belong to one of the address ranges entered in the DHCPv6 configuration. If the firewall is used as a relay to a DHCPv6 server, the configured interface must belong to the list of the service's listening interfaces. If the DHCPv6 service is inactive, the sending of RAs will be disabled.
Send RA	The firewall's address is sent as the default router. The information relayed by this advertisement will be described further in this manual. This configuration is recommended in order to allow hosts that are directly connected (local link) to use SLAAC.
Disable	No router advertisement (RA) has been sent out. This configuration is recommended in bridge mode if an IPv6 router is directly connected (local link).

Router advertisements (RA)

This zone can be accessed only if the **Send RA** option has been selected.

Announce the prefix extracted from the interface address	The prefix advertised is the prefix configured in the interface's IPv6 address range in the **General configuration** tab. The size of the IPv6 address mask (prefix length – CIDR) must be 64 bits.

Configuration with DHCPv6 server

The DHCPv6 server assigns addresses (Managed)	The advertisement indicates that the IPv6 addresses contacted will be distributed by the DHCPv6 service enabled on the firewall (**Configuration** module > **Network > DHCP**). This service is implemented by the firewall or a relay that is directly connected (local link).
The DHCPv6 server delivers additional options (Other config)	The advertisement indicates that other auto-configuration parameters, such as the addresses of DNS servers or other types of servers, will be issued by the DHCPv6 server (firewall or relay) that is directly connected (local link).

Advanced properties

DNS Parameters

This section can be accessed if the option **The DHCPv6 server delivers additional options (Other config)** is not enabled.

Domain name	Default domain name to contact a queried server that does not have a domain.
Primary DNS server	IP address of the primary DNS server. If this field is blank, the address sent will be the address used by the firewall (**Configuration** module > **System > Configuration**, **Network settings** tab).
Secondary DNS server	IP address of the secondary DNS server. If this field is blank, the address sent will be the address used by the firewall (**Configuration** module > **System > Configuration**, **Network settings** tab).

Announced prefixes

This grid can be accessed if the option **The DHCPv6 assigns addresses (Managed)** is not enabled.

Prefixes	Prefix to announce to hosts. We recommend using the interface's prefix as the announced prefix. If the interface specifies several prefixes, this field will indicate the prefix to use.
Autonomous	Instruction to use stateless address auto-configuration (SLAAC): if this option has been selected, the host will then create one or several IPv6 addresses based on the prefix(es) advertised and its interface ID (random and/or based on the MAC address.
On link	This option specifies to the host that all hosts with the same prefix may be contacted directly, without going through the router. In IPv4, such information was deduced from the network mask.
Comments	Allows adding comments for the announced prefix.

Advanced properties tab

Other settings

MTU	Maximum length of frames (in bytes) sent over the physical medium (Ethernet) so that they are sent at one go without fragmentation.
Physical MAC address	MAC address of the network interface the VLAN belongs to.

Routing without analysis

This zone appears only if the option **Address range inherited from the bridge** is selected in the **Address range** field in the **General configuration** tab.

Authorize without analyzing	Allows letting IPX (Novell network), Netbios (on NETBEUI), AppleTalk (for Macintosh), PPPoE or Ipv6 packets pass between the bridge's interfaces. No high-level analysis or filtering will be applied to these protocols (the firewall will block or pass).

Routing by interface

This zone appears only if the option **Address range inherited from the bridge** is selected in the **Address range** field in the **General configuration** tab.

Keep initial routing	This option will ask the firewall to not modify the destination in the Ethernet layer when a packet goes through it. The packet will be resent to the same MAC address from which it was received. The purpose of this option is to facilitate the integration of firewalls transparently into an existing network, as this makes it possible to avoid the need for modifying the default route of machines on the internal network. This option must be enabled to ensure that a DHCP server located on the interface in question, and which sends unicast responses to requests, runs properly **Known limitations** Features on a firewall that inserts or modifies packets in sessions may fail to function correctly. The affected features are: • Connection reinitialization caused by an alarm, • SYN proxy (enabled in filtering), • Requests to resend packets that were dropped in order to speed up analysis, • Rewriting of packets by application analyses (SMTP, HTTP and web 2.0, FTP and NAT, SIP and NAT).
Keep VLAN IDs	This option enables the transmission of tagged frames without the firewall having to be the VLAN endpoint. The VLAN tag on these frames is kept so that the Firewall can be placed in the path of a VLAN without the firewall interrupting this VLAN. The Firewall runs seamlessly for this VLAN. To use this option, the previous option "**Keep initial routing**" must be enabled.

Deleting a VLAN

To delete a VLAN:

1. Select the VLAN in the interface directory.
2. Click on **Delete** in the toolbar.
   The message "**Delete this interface?**" will appear.
3. Confirm or cancel the deletion.
   If you confirm the deletion, a check will be performed to see if the interface is in use.

Aggregate

This feature is available only on SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200, SNi10, SNi20, SNi40, SNxr1200, EVA1, EVA2, EVA3, EVA4 and EVAU models. There are several types of aggregates (LACP, Broadcast mode and Redundancy). You can select the desired type in the **Advanced properties** tab.

> **NOTE**
> The use of stackable switches is recommended as this would allow link redundancy between both appliances.

Adding an aggregate

Adding an aggregate without members

1. Click on **Add**.
2. Scroll over **Aggregate**.
3. Click on **No members**.
4. Give the new aggregate a name, then click on **Apply**.
   The new aggregate will be added to the interfaces and its control panel appears.

Adding an aggregate that contains selected interfaces

1. Select the interfaces to include in the new aggregate beforehand.
2. Click on **Add**.
3. Scroll over **Aggregate**.
4. Click on **With *interface_1*, *interface_2* ....**
5. Give the new aggregate a name, then click on **Apply**.
   The new aggregate will be added to the interfaces and its control panel appears.

Aggregate control panel

Double-click on an aggregate control panel to open it. There are several tabs in the control panel.

General configuration tab

Status

ON / OFF	Set the switch to **ON** / **OFF** to enable or disable the aggregate.

General settings

Name	Name of the aggregate. This name can be changed.
Comments	Allows you to enter comments regarding the interface.

This interface is	An interface can be: • **Internal (protected)**: when this option is selected, this means that the interface is protected (a shield appears). a protected interface only accepts packets coming from a known address range, such as a directly connected network or a network defined by a static route. This protection includes remembering machines that have logged on to this interface, conventional traffic security mechanisms (TCP) and implicit rules for services offered by the firewall such as DHCP. • **External (public)**: choosing this option indicates that the interface does not benefit from the protection of a protected interface and can therefore receive packets coming from any address range (which are not assigned to internal interfaces). This type of interface is used mainly to connect the firewall to the Internet.

Address range

Address range inherited from the bridge	When this option is selected, the interface becomes part of a bridge. Several parameters, such as the address range, will then be inherited from the bridge. This will unlock the **Bridge** field. Select the parent bridge of the interface in this field.
Dynamic / Static	Selecting this option indicates that the IP address of the interface is dynamic (obtained via DHCP) or static. This will unlock the **IPv4 address** field.
Dynamic IP (obtained by DHCP)	When this option is selected, the IP address of the interface will be defined by DHCP. An **Advanced DHCP properties** zone appears with the following parameters: • **DNS name (optional)**: a fully qualified DHCP host name (FQDN) can be indicated for the DHCP request. If a value is entered in this field and the external DHCP server has the option of automatically updating the DNS server, the DHCP server automatically updates the DNS server with the name of the firewall, its assigned IP address and allocated lease time (field below). • **Requested lease time (seconds)**: in addition to the DNS name, enter the duration for which the IP address is kept before renegotiation. • **Request domain name servers from the DHCP server and create host objects:** select this parameter so that the firewall will retrieve DNS servers from the DHCP server (access provider, for example) that provided its IP address. When this option is selected, two objects will be created: *Firewall_<interface name>_dns1* and *Firewall_<interface name>_dns2*. They can then be used in the configuration of the DHCP service. So if the firewall provides the users on its network with a DHCP service, the users will also benefit from the DNS servers given by the access provider.
Fixed IP (static)	When this option is selected, the IP address of the interface will be static. A grid appears, in which you must add the IP address and its subnet mask. Several IP addresses and associated masks can be added if aliases need to be created, for example. These aliases allow you to use the firewall as a central routing point. As such, an interface can be connected to various sub-networks with a different address range. If you add several IP addresses (aliases) to the same address range, these addresses must all have the same mask. Reloading the network configuration will apply this mask to the first address and a /32 mask to the addresses that follow.

Managing members

To add or remove members from the aggregate, move the interfaces from one section to another by using the arrows, dragging and dropping, or double-clicking on the interface. An

interface that becomes a member of an aggregate loses its settings to inherit the configuration of the aggregate (except the name and Media settings).

The maximum number of members that an aggregate can contain varies based on its type:

- **LACP**: Maximum 8 members,
- **Broadcast mode**: Maximum 2 members,
- **Redundancy**: 2 members (includes 1 "*Master*" member that must be defined).

The type of aggregate and *Master* member are chosen in the **Advanced properties** tab.

Advanced properties tab

Other settings

MTU	Maximum length of frames (in bytes) sent over the physical medium (Ethernet) so that they are sent at one go without fragmentation. This option is not available for interfaces contained in a bridge.
Physical (MAC) address	Makes it possible to specify a MAC address for an interface instead of using the address assigned by the firewall. If the interface is contained in a bridge, it will have the same MAC address as the bridge.

Aggregate type

LACP	When this option is selected, the aggregate is LACP-based. The LACP (IEEE 802.3ad - Link Aggregation Control Protocol) feature helps improve the firewall's bandwidth while maintaining a high level of availability (link redundancy). Several physical ports on a firewall can be grouped together to be considered a single logical interface. Therefore, by aggregating *n* links, it is possible to set up a link of n times *x* Gbit/s between two appliances. **NOTE** Ensure that the remote appliances are using LACP.
Broadcast mode	When this option is selected, the aggregate is Broadcast mode-based. With this mode, packets can be sent and received over all links included in an aggregate. **NOTE** The device that is connected to the firewall's aggregated interfaces in broadcast mode must support such communications: • Either by having one active interface and a second passive interface (main/backup), • Or by ignoring frames that originate from one of the links.
Redundancy	When this option is selected, the aggregate is redundancy-based. With the redundancy feature, a backup link can be set up in case the main link (*Master*) stops responding.
Main interface	Select the main interface from the drop-down menu. It appears as the *Master* in the list of aggregate members in the **General configuration** tab. This field can only be accessed if it is a **Redundancy** aggregate.

GRETAP interface

Tunnels that use GRETAP interfaces allow encapsulating Level 2 traffic (Ethernet). They can then be used to link sites sharing the same IP address range through a bridge or to transport non-IP protocols over a bridge.

Adding a GRETAP interface

1. Click on **Add**.
2. Click on **GRETAP interface**.
   The GRETAP interface is added to the interfaces and its control panel appears.

GRETAP interface control panel

Double-click on the GRETAP interface control panel to open it. There are several tabs in the control panel.

General configuration tab

Status

ON / OFF	Set the switch to **ON/OFF** to enable or disable the interface. Disabled interfaces cannot be used. An interface that has been disabled because it is not in use, or will be deployed later, is an additional security measure against intrusions.

General settings

Name	Name of the interface. This name can be changed.
Comments	Allows you to enter comments regarding the interface.
This interface is	An interface can be: • **Internal (protected)**: when this option is selected, this means that the interface is protected (a shield appears). a protected interface only accepts packets coming from a known address range, such as a directly connected network or a network defined by a static route. This protection includes remembering machines that have logged on to this interface, conventional traffic security mechanisms (TCP) and implicit rules for services offered by the firewall such as DHCP. • **External (public)**: choosing this option indicates that the interface does not benefit from the protection of a protected interface and can therefore receive packets coming from any address range (which are not assigned to internal interfaces). This type of interface is used mainly to connect the firewall to the Internet.

GRETAP tunnel address

Tunnel source	Select the network object that corresponds to the bridge that supports the GRETAP interface.
Tunnel destination	Select (or create) the network object that corresponds to the public address of the appliance that hosts the remote GRETAP interface.

Address range

Address range inherited from the bridge	When this option is selected, the interface becomes part of a bridge. Several parameters, such as the address range, will then be inherited from the bridge. This will unlock the **Bridge** field. Select the parent bridge of the interface in this field.
Dynamic / Static	Selecting this option indicates that the IP address of the interface is dynamic (obtained via DHCP) or static. This will unlock the **IPv4 address** field.
Dynamic IP (obtained by DHCP)	When this option is selected, the IP address of the interface will be defined by DHCP. An **Advanced DHCP properties** zone appears with the following parameters: • **DNS name (optional)**: a fully qualified DHCP host name (FQDN) can be indicated for the DHCP request. If a value is entered in this field and the external DHCP server has the option of automatically updating the DNS server, the DHCP server automatically updates the DNS server with the name of the firewall, its assigned IP address and allocated lease time (field below). • **Requested lease time (seconds)**: in addition to the DNS name, enter the duration for which the IP address is kept before renegotiation. • **Request domain name servers from the DHCP server and create host objects:** select this parameter so that the firewall will retrieve DNS servers from the DHCP server (access provider, for example) that provided its IP address. When this option is selected, two objects will be created: *Firewall_<interface name>_dns1* and *Firewall_<interface name>_dns2*. They can then be used in the configuration of the DHCP service. So if the firewall provides the users on its network with a DHCP service, the users will also benefit from the DNS servers given by the access provider.
Fixed IP (static)	When this option is selected, the IP address of the interface will be static. A grid appears, in which you must add the IP address and its subnet mask. Several IP addresses and associated masks can be added if aliases need to be created, for example. These aliases allow you to use the firewall as a central routing point. As such, an interface can be connected to various sub-networks with a different address range. If you add several IP addresses (aliases) to the same address range, these addresses must all have the same mask. Reloading the network configuration will apply this mask to the first address and a /32 mask to the addresses that follow.

Advanced properties tab

Other settings

MTU	Maximum length of frames (in bytes) sent over the physical medium (Ethernet) so that they are sent at one go without fragmentation. This option is not available for interfaces contained in a bridge.
Physical (MAC) address	Makes it possible to specify a MAC address for an interface instead of using the address assigned by the firewall. If the interface is contained in a bridge, it will have the same MAC address as the bridge.

Routing without analysis

This zone appears only if the option **Address range inherited from the bridge** is selected in the **Address range** field in the **General configuration** tab.

Authorize without analyzing	Allows letting IPX (Novell network), Netbios (on NETBEUI), AppleTalk (for Macintosh), PPPoE or Ipv6 packets pass between the bridge's interfaces. No high-level analysis or filtering will be applied to these protocols (the firewall will block or pass).

Routing by interface

This zone appears only if the option **Address range inherited from the bridge** is selected in the **Address range** field in the **General configuration** tab.

Keep initial routing	This option will ask the firewall to not modify the destination in the Ethernet layer when a packet goes through it. The packet will be resent to the same MAC address from which it was received. The purpose of this option is to facilitate the integration of firewalls transparently into an existing network, as this makes it possible to avoid the need for modifying the default route of machines on the internal network. **Known limitations** Features on a firewall that inserts or modifies packets in sessions may fail to function correctly. The affected features are: • Connection reinitialization caused by an alarm, • SYN proxy (enabled in filtering), • Requests to resend packets that were dropped in order to speed up analysis, • Rewriting of packets by application analyses (SMTP, HTTP and web 2.0, FTP and NAT, SIP and NAT).
Keep VLAN IDs	This option enables the transmission of tagged frames without the firewall having to be the VLAN endpoint. The VLAN tag on these frames is kept so that the Firewall can be placed in the path of a VLAN without the firewall interrupting this VLAN. The Firewall runs seamlessly for this VLAN. To use this option, the previous option "**Keep initial routing**" must be enabled.

PPPoE/PPTP modem interface

Modem interfaces are used in remote connections when your modem is directly connected to your firewall via an Ethernet port. There are two types of modem interfaces:

- PPPoE modems,
- PPTP modems.

NOTES

- The firewall automatically negotiates the opening of a line and reinitializes the connection in the event of an interruption. When the connection cannot be set up (e.g., issues with the line), the firewall will raise an alarm.
- If your modem needs to be connected to the firewall's USB port, refer to USB/Ethernet interface (for USB sticks /modems).

Adding a modem

1. Click on **Add**.
2. Scroll over **Modem**.
3. Click on **PPPoE** or **PPTP** depending on the interface you wish to create.
   The modem interface is added to the interfaces and its control panel appears.

PPPoE modem interface control panel

Double-click on the modem interface control panel to open it. There are several tabs in the control panel.

General configuration tab

Status

ON / OFF	Set the switch to **ON/OFF** to enable or disable the interface.

General settings

Name	Name given to the modem. This name can be changed.
Comments	Allows you to enter comments regarding the modem.
Modem type	Reminder of the type of modem chosen when the modem was created.

Connectivity

Parent interface	Select the network interface to which the PPPoE modem is connected.

Authentication

ID	Enter the ID used for authentication.
Password	In this field, enter the password used for authentication, then confirm it in the **Confirm** field. A progress bar will indicate the strength of the password entered.

Advanced properties tab

Other settings

Service	Type of PPPoE service used. This option allows distinguishing between several ADSL modems. Leave this field empty by default.
Connectivity	Two choices are given: • **Permanent:** keeps the connection to the Internet permanently active. • **If there is traffic (on demand)**: the Internet connection is set up only when a connection request is received from the internal network. This mode is more economical than a metered connection.

PPTP modem interface control panel

Double-click on the modem interface control panel to open it. There are several tabs in the control panel.

General configuration tab

Status

ON / OFF	Set the switch to **ON/OFF** to enable or disable the interface.

General settings

Name	Name given to the modem. This name can be changed.

Comments	Allows you to enter comments regarding the modem.
Modem type	Reminder of the type of modem chosen when the modem was created.

Connectivity

PPTP address	Enter the internal IP address of the modem.

Authentication

ID	Enter the ID used for authentication.
Password	In this field, enter the password used for authentication, then confirm it in the **Confirm** field. A progress bar will indicate the strength of the password entered.

Advanced properties tab

Other settings

Connectivity	Two choices are given: • **Permanent:** keeps the connection to the Internet permanently active. • **If there is traffic (on demand)**: the Internet connection is set up only when a connection request is received from the internal network. This mode is more economical than a metered connection.

USB/Ethernet interface (for USB key/modem)

USB/Ethernet interfaces are used in remote connections when your modem is directly connected to the firewall's USB port. You can add only one USB/Modem interface on your firewall.

A USB/Ethernet interface is automatically created whenever a *HUAWEI* 4G USB modem that supports the *HiLink* feature is connected to the firewall and then configured. If you are using another USB modem, a modem profile must be configured before a USB/Ethernet interface can be created.

> **NOTE**
> If your modem must be plugged into the firewall's Ethernet port or serial port (PPPoE/PPTP modem), refer to PPPoE/PPTP modem interface.

Modem profile control panel

Click on **Edit** > **Modem profiles** to open the control panel of a modem profile. Two modem profiles can be defined; select one of them.

Status

ON / OFF	Set the switch to ON / OFF to enable/disable the modem profile.

General settings

Name	Enter a name for the modem profile.

Model	Enter the model of the modem for which the profile is being created (open text field).
Vendor ID	ID specific to each modem vendor (*Vendorid* or *VID*). This is a hexadecimal string.
Initial product ID	Product ID (*Productidinit*) after it has been recognized as a USB storage device. This parameter is specific to each modem model.
Target product ID	ID representing the product when it is in modem mode (*ProductId* or *PID*). This parameter is specific to each modem model.
MessageContent for modem mode	This is a character string that allows the firewall to detect the USB device connected as a modem (*ModeSwitchString*).

Advanced configuration

Configuration command port	This is the number of the dedicated serial port for sending configuration commands ("AT" commands) to the modem. The most common value is 0.
Monitoring command port	This is the number of the dedicated serial port for sending monitoring commands ("AT" commands) to the modem. The most common value is 1.
Initialization string no. 1, 2 and 3	These strings are optional and allow you to send "AT" configuration commands to the modem before it is used. **EXAMPLES** *ATZ*: command to reinitialize the modem *AT^CURC=0*: command that allows periodic messages to be disabled)

USB/Ethernet interface control panel (for USB sticks/modems)

Configuring profiles	When no modem profiles are defined or active, a message will prompt you to configure a modem profile. For further information, refer to the section Modem profile control panel

General settings

Name	Name of the interface. Cannot be changed.
Comments	Allows you to enter comments regarding the interface.
This interface is	An interface can be: • **Internal (protected)**: when this option is selected, this means that the interface is protected (a shield appears). a protected interface only accepts packets coming from a known address range, such as a directly connected network or a network defined by a static route. This protection includes remembering machines that have logged on to this interface, conventional traffic security mechanisms (TCP) and implicit rules for services offered by the firewall such as DHCP. • **External (public)**: choosing this option indicates that the interface does not benefit from the protection of a protected interface and can therefore receive packets coming from any address range (which are not assigned to internal interfaces). This type of interface is used mainly to connect the firewall to the Internet.

Address range

Dynamic IP (obtained by DHCP)	When this option is selected, the IP address of the interface will be defined by DHCP. An **Advanced DHCP properties** zone appears with the following parameters: • **DNS name (optional)**: a fully qualified DHCP host name (FQDN) can be indicated for the DHCP request. If a value is entered in this field and the external DHCP server has the option of automatically updating the DNS server, the DHCP server automatically updates the DNS server with the name of the firewall, its assigned IP address and allocated lease time (field below). • **Requested lease time (seconds)**: in addition to the DNS name, enter the duration for which the IP address is kept before renegotiation. • **Request domain name servers from the DHCP server and create host objects:** select this parameter so that the firewall will retrieve DNS servers from the DHCP server (access provider, for example) that provided its IP address. When this option is selected, two objects will be created: *Firewall_<interface name>_dns1* and *Firewall_<interface name>_dns2*. They can then be used in the configuration of the DHCP service. So if the firewall provides the users on its network with a DHCP service, the users will also benefit from the DNS servers given by the access provider.
Fixed IP (static)	When this option is selected, the IP address of the interface will be static. A grid appears, in which you must add the IP address and its subnet mask. Several IP addresses and associated masks can be added if aliases need to be created, for example. These aliases allow you to use the firewall as a central routing point. As such, an interface can be connected to various sub-networks with a different address range. If you add several IP addresses (aliases) to the same address range, these addresses must all have the same mask. Reloading the network configuration will apply this mask to the first address and a /32 mask to the addresses that follow.

Network configuration modes

There are several configuration modes that can be used on your firewall:

- Bridge mode,
- Advanced mode (Router),
- Hybrid mode.

These modes are not visually represented in the web administration interface, and there is no configuration wizard to set them up. There represent the types of configuration that you can apply to your firewall. **Security-wise, all operating modes are equal.**

Bridge mode

Interfaces are part of the address range declared on the bridge. This mode makes it possible to keep the same address range between interfaces.

You can filter traffic later by using interface objects or address ranges depending on your requirements, and protect any part of your network.

The advantages of this mode are:

- Ease of integration of the product since there is no change in the configuration of client workstations (default router, static routes, etc.) and no change in IP address on your network.
- Compatibility with IPX (Novell network), Netbios in Netbeui, Appletalk or IPv6.
- No address translation, therefore time is saved when the firewall processes packets.

This mode is therefore recommended between the external zone and the DMZ. It allows keeping a public address range on the firewall's external zone and on the DMZ's public servers.

Advanced mode (Router)

The firewall operates like a router between its various interfaces. Every enabled interface has an IP address from the network to which it is directly connected. This enables the configuration of translation rules for accessing other zones in the firewall.

This requires some IP addresses to be changed on routers or servers when you move them to a different network (behind a different interface of the firewall).

The advantages of this mode are:

- Address translation between the various networks.
- Only traffic passing from one network to another passes through the firewall (internal network to the Internet, for example). This considerably lightens the firewall's load and returns better response times.
- Item belonging to each zone are easier to differentiate (internal, external and DMZ). The distinction is made by the different IP addresses for each zone. This provides a clearer view of the separations and the configuration to be applied to these items.

Hybrid mode

Some interfaces have the same IP address and others have a separate address. The hybrid mode uses a combination of both modes mentioned earlier. This mode may only be used with Stormshield Network products having more than two network interfaces. You may define several interfaces in bridge mode.

EXAMPLE
Internal zone and DMZ (or external zone and DMZ) and certain interfaces in a different address range. This provides greater flexibility when you integrate the product.

IPSEC VPN

A standard protocol, IPsec (IP Security) enables the creation of VPN tunnels between two hosts, between a host and a network, between two networks and any type of object that supports the protocol.

The services that Stormshield Network's IPsec offers provide access control, integrity in offline mode, authentication of data source, protection against replay, confidentiality in encryption and on traffic. You can for example, create a tunnel between two firewalls, or between the firewall and mobile clients on which VPN clients would be installed.

Recommendations

When you configure an IPsec VPN, you are advised to:

- Configure a static route to the local loopback (*black hole*) to reach remote networks accessible via IPsec VPN tunnels,
- Ensure that the IPsec policy is never enabled, even during transitional phases,
- Ensure that filter rules are always more specific than NAT before IPsec rules,
- Ensure that traffic (source and destination IP addresses) after translation (NAT) matches the IPsec policy,
- Ensure that in the absence of NAT rules, filter rules are always more specific than the IPsec policy.

Optimization of encryption and decryption operations

The IPsec service has a mechanism to optimize the distribution of encryption and decryption operations. Its purpose is to significantly improve IPsec throughput, especially in configurations that contain a single IPsec tunnel.

It offers three configuration modes:

Automatic mode (auto)	This is the default mode, which allows the optimization mechanism to activate automatically and transparently when both of the following conditions are met: • The active IPsec policy has a single active VPN tunnel. • The firewall model supports **Automatic** mode. These models support **Automatic** mode: SN510, SN710, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100 and SNi40. On other models, the optimization mechanism can run only in **Enabled** mode.
Enabled mode (1)	Makes it possible to run the optimization mechanism continuously without any particular conditions. It can be configured on all firewall models. This mode is not recommended when an IPsec policy has many active VPN tunnels. Ensure that using this mode does not affect the general quality of your service.
Disabled mode (0)	Makes it possible to disable the optimization mechanism continuously.

This mode can be configured only with the following CLI/serverd command:

```
CONFIG IPSEC UPDATE slot=<n> CryptoLoadBalance=<0|1|auto>
```

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

IPsec VPN module screen

The IPsec VPN module consists of four tabs:

- **Encryption policy – Tunnels**: create IPsec tunnels between two firewalls (**Site to site – Gateway- Gateway**) or between a Stormshield Network multi-function firewall and a mobile user (**Anonymous – Mobile users**).
  10 blank encryption policies can be configured, activated and edited. The anonymous policy also makes it possible to configure tunnels with another firewall, but which does not have a fixed IP address. It will therefore have the same problem as a "classic" mobile workstation: an unpredictable IP address
- **Peers**: create new peers (remote site or anonymous mobile peer) by entering their IKE profiles, their negotiation method, as well as the specific parameters for each negotiation method.
- **Identification**: list your approved certification authorities in the tunnels using PKI methods as well as the pre-shared keys (PSK) of your mobile tunnels.
- **Encryption profiles**: define your IKE (phase 1) and IPsec (phase 2) encryption profiles, add new ones or set their maximum lifetime (in seconds). You can also define negotiation proposals for authentication and encryption algorithms.

NOTES

- IPsec VPN policies now make it possible to edit their configurations in Global mode. To enable the option, select "Display global policies" in the Preferences module.
- There is no specific privilege for "vpn_global".

Encryption policy – Tunnels tab

IPsec policies can now group peers that use various versions of the IKE protocol with restrictions on the use of the IKEv1 protocol (cf. section ***Explanations on usage*** in ***Release Notes v4***).

Profile bar	The drop-down menu offers 10 IPsec profiles numbered from (01) to (10). To select a profile in order to configure it, click on the arrow to the right of the field.
Activate this policy	Immediately activates the selected IPsec policy: parameters saved in this policy will overwrite current parameters in force.
Actions	This function allows performing 3 operations on profiles: • **Edit**: by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on "Update". This operation can also be canceled. • **Reinitialize**: Deletes all changes made to the profile. The configuration will therefore be lost. • **Copy to**: This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the date and time of the last modification. The time displayed is the appliance's time instead of your workstation's time.
Disable policy	This button allows immediately deactivating the selected IPsec policy.

Site to site (Gateway-Gateway)

This tab will allow a VPN tunnel to be created between two network devices that support IPsec. This procedure is also called: *Gateway to Gateway VPN tunnel.*

Several tutorials show you step by step how to configure a secure connection between your sites. Click on one of the links to access a tutorial:

- IPsec VPN: Authentication by pre-shared key,
- IPsec VPN: Authentication by certificate,
- IPsec VPN: Hub and spoke configuration.

Search	Searches will be performed on the name of the object and its various properties, unless you have specified in the preferences of the application that you would like to restrict this search to object names only.
Add	The **Add** button will be covered in the following section.
Delete	Select the IPsec VPN tunnel to be removed from the grid and click on this button.
Move up	Places the selected line before the line just above it.
Move down	Places the selected line after the line just below it.
Cut	Cuts the selected line to paste it.
Copy	Copies the selected line to duplicate it.
Paste	Duplicates the selected line after it is copied.

Show details	To ease the configuration of the tunnel with a remote device (gateway or mobile client), click on this icon to view information on the IPsec policy: • **Summary**: ○ Rule type: Gateway, ○ IKE version, ○ Peer, ○ Remote gateway, ○ Local network, ○ Remote network. • **Authentication**: ○ Mode: Auto, ○ Type: Certificate or pre-shared key (PSK), • **IKE profiles (phase 1)**: ○ DH by default, ○ Lifetime, ○ Proposals • **IPsec profile (phase2)**: ○ Lifetime, ○ Authentication, ○ Encryption, ○ PFS.
Search in logs	When a name is assigned to the IPsec rule, clicking on this button will run a search by the name of the rule in the IPsec VPN log and show the results.
Search in monitoring	Clicking on this button will open the screen to monitor IPsec tunnels (**Monitoring** tab > **Monitoring** module > **IPsec VPN tunnels**).

REMARKS
Right-clicking anywhere in the grid will display a pop-up menu offering the following actions:

- **Add,**
- **Copy,**
- **Cut,**
- **Paste,**
- **Show details**
- **Delete,**
- **Search in logs,**
- **Search in monitoring.**

Add

In order to configure the tunnel, select the VPN policy in which you wish to set it up. The IPsec VPN policy wizard will guide you through the configuration.

Standard site-to-site tunnel

Here, you will define each of the endpoints for your tunnel as well as for your peer.

Local resources	Host, host group, network or network group that will be accessible via the IPsec VPN tunnel.
Peer selection	This is the object that corresponds to the public IP address of the tunnel endpoint, or of the remote VPN peer. The drop-down list displays "None" by default. You can create peers in the following option or select an existing peer from the list.
Create a peer	Define the parameters for your peer. Several steps are necessary: Step 1: Select the gateway. 1. **Remote gateway**: select the object corresponding to the IP address of the tunnel endpoint from the drop-down list. You can also add gateways using the button . 2. **Name**: you can specify a name for your gateway or keep the peer's original name, which will be prefixed with "Site_" ("Site_<name of object>"). Selecting None as a peer allows generating policies without encryption. The aim is to create an exception to the following rules of the encryption policy. Traffic matching this rule will be managed by the routing policy. 3. **IKE version**: select IKEv1 or IKEv2, depending on the version of the IKE protocol that the peer uses. 4. Click on **Next**. Step 2: Identify the peer. Two choices are possible: • **Certificate** • **Pre-shared Key (PSK)**: 1. Select the desired option. 2. If you have selected **Certificate**, you will need to select it from those you have previously created in the Certificates and PKI module. The certificate to enter here is the one presented by the firewall and not the one presented by the remote site. A certification authority can also be added. 3. If you have selected **Pre-shared key (PSK)**, you will need to define the secret that both peers of the IPsec VPN tunnel will share, in the form of a password to be confirmed in a second field. You can **Enter the key in ASCII characters** (every character in ASCII text is stored in a byte whose 8th is 0) by selecting the relevant option. Unselect the option to view the key in hexadecimal characters (which is based on 16 digits: the letters A to F and numbers 0 to 9). **NOTE** To define an ASCII pre-shared key that is sufficiently secure, you must follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management. 4. Click on **Next**. The screen will show you a window summarizing the configuration that was made, the **Parameters of the remote site** and the **Pre-shared key**. You can also add a backup peer by clicking on the link provided. You will need to define a remote gateway. 5. Click on **Finish**.

Encryption profile	From this drop-down list, you can select the encryption profile to be used from the profiles defined in Encryption profiles tab. Do note that when *Diffusion Restreinte* (DR) mode is enabled on the firewall, only DR-compatible encryption profiles are suggested.
Remote networks	Host, host group, network or network group accessible through the IPsec tunnel with the peer.

Separator (rule grouping)

This option allows inserting a separator above the selected line. This allows the administrator to create a hierarchy for his tunnels according to his needs.

The table

Line	This column indicates the number of the line processed in order of appearance on the screen.
Status	This column shows the status on / off of the tunnel. When a tunnel is created, it is enabled by default. Click twice to disable it.
Name	A name can be given to this IPsec rule so that it will be easier to look for events that involve this rule in logs.
Local network	Select the host, host group, network or network group that will be accessible via the IPsec VPN tunnel, from the drop-down list of objects.
Peer	Configuration of the peer, which can be viewed in the tab of the same name in the IPsec VPN module.
Remote network	Select from the drop-down list of objects, the host, host group, network or network group accessible through the IPsec tunnel with the peer.
Protocol	This option makes it possible to restrict the setup of IPsec tunnels to traffic based on specific protocols: • TCP • UDP • ICMP • GRE • All
Encryption profile	This option allows selecting the protection model associated with your VPN policy, from 3 preconfigured profiles: **StrongEncryption, GoodEncryption and Mobile.** Other profiles can be created or modified in the tab *Encryption profiles*.
Keep alive	The additional **Keepalive** option makes it possible to artificially maintain mounted tunnels. This mechanism sends packets that initialize the tunnel and force it to be maintained. This option is disabled by default to avoid wasting resources, especially in the case of a configuration containing many tunnels set up at the same time without any real need for them. To enable this option, assign a value other than 0, corresponding to the interval in seconds, between each UDP packet sent.
Comments	Description given of the VPN policy.

Checking the policy in real time

The window for editing IPsec policy rules has a "**Check policy**" field (located below the table), which warns the administrator whenever there are inconsistencies or errors in the rules created.

Mobile users

The IPsec VPN has two endpoints: the tunnel endpoint and the traffic endpoint. For anonymous or mobile users, the IP address of the tunnel's endpoint is not known in advance.

As for the IP address of the traffic endpoint, it can either be chosen by the peer ("classic" case) or given by the gateway ("Config mode").

Mobile IPsec policies containing several peers can be built as long as they use the same IKE encryption profile. In certificate-based authentication, the certificates of the various peers must be issued by the same CA,

Add

Select the VPN policy in which you wish to set up a tunnel. Policy creation wizards will guide you in this configuration. If you wish to create the mobile peer through the wizard, please refer to the section "**Creating a mobile peer**" below.

VPN client settings (Config mode) can be defined for mobile users through the *Config mode policy* creation wizard.

New standard mobile policy

This policy makes local networks accessible to authorized users via an IPsec tunnel. In this configuration, remote users log in with their own IP addresses.

1. Specify accessible local resources (hosts, networks, network groups, etc.).
2. Enter the details of the mobile peer to be used.
3. Select the encryption profile to be used from the profiles defined in Encryption profiles tab. Do note that when *Diffusion Restreinte* (DR) mode is enabled on the firewall, only DR-compatible encryption profiles are suggested.

New Config mode policy

This policy with Config mode makes a single local network accessible to authorized users through an IPsec tunnel. With Config mode, remote users log on with an IP address assigned in a set defined as a "Mobile network".

Once it is created, the cell corresponding to the Config mode column will contain an **Edit Config mode (selection)** button, allowing you to enter the parameters of the IPsec Config mode, described in the section **Rule grid**.

You can enter a particular DNS server and specify the domains that this server uses. These indications are indispensable if an Apple® (iPhone, iPad) mobile client is used for example. This feature is paired with Config mode, and is not used by all VPN clients on the market.

Creating a mobile peer

The procedure for creating a peer through these wizards is described below. You can also create it directly from the *Peer* tab.

1. Click on "**Add**" a "**New policy**" (VPN), then on "**Create a mobile peer**" via the mobile IPsec VPN policy wizard.
2. **Name** your mobile configuration.
3. Select the **IKE version** of the protocol that the peer uses.

4. Click on **Next**.
5. Select the authentication method of the peer.

Certificate	If you select this authentication method, you will need to select the **Certificate** (server) to be presented to the peer, from the list of those you have already created previously (**Certificates and PKI module**). You can also enter details about the **Certification authority** (CA) that signed your peer's certificate so that it is automatically added to the list of trusted authorities.
Pre-shared key (PSK)	If you have chosen this authentication method, you will need to edit your key in a table, by providing its ID and its value to be confirmed. To do so, click on **Add**. The ID may be in an IP address (X.Y.Z.W), FQDN (myserver.domain.com), or e-mail address format (firstname.lastname@domain.com). It will then occupy the "Identity" column in the table and the pre-shared key will occupy a column of the same name with its value displayed in hexadecimal. **NOTE** To define an ASCII pre-shared key that is sufficiently secure, you must follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management.
EAP-Generic Token Card (GTC)	The EAP-GTC (Extensible Authentication Protocol - Generic Token Card) method is described in RFC 3748. It is available only for IKEv2 mobile peers. This method is meant to be used with cards that support challenge/response verifications. If you choose this authentication method, you will then need to select the server **Certificate** that the firewall must present to the peer for authentication. You can also enter details about the **Certification authority** (CA) that signed your peer's certificate so that it is automatically added to the list of trusted authorities. The **Groups** grid allows you to directly add user groups to be attached to this peer profile. These groups can either be from the default LDAP directory, or from other domain directories.
Certificate and EAP-Generic Token Card (GTC)	The EAP-GTC (Extensible Authentication Protocol - Generic Token Card) method is described in RFC 3748. It is available only for IKEv2 mobile peers. This method is meant to be used with cards that support challenge/response verifications. If you choose this authentication method, you will then need to select the server **Certificate** that the firewall must present to the peer for authentication. You can also enter details about the **Certification authority** (CA) that signed your peer's certificate so that it is automatically added to the list of trusted authorities. The **Groups** grid allows you to directly add user groups to be attached to this peer profile. These groups can either be from the default LDAP directory, or from other domain directories.

6. Click on **Next**.
7. Check the summary of you mobile configuration and click on **Finish**.
8. Next, enter the local resource, or "**local network**" to which the mobile user will have access.

Other operations can also be performed:

Search	Searches will be performed on the name of the object and its various properties, unless you have specified in the preferences of the application that you would like to restrict this search to object names only.
Delete	Select the IPsec VPN tunnel to be removed from the grid and click on this button.

Move up	Places the selected line before the line just above it.
Move down	Places the selected line after the line just below it.
Cut	Cuts the selected line to paste it.
Copy	Copies the selected line to duplicate it.
Paste	Duplicates the selected line after it is copied.
Show details	To facilitate the configuration of the tunnel with a remote device (gateway or mobile client), click on this icon to view information on a selected rule in the IPsec policy: • **Summary**: ○ Rule type: Mobile peers, ○ IKE version, ○ Peer, ○ Remote gateway: *Any* in the case of mobile peers, ○ Local network, ○ Remote network. • **Authentication**: ○ Mode: Auto, ○ Type: Certificate, Pre-shared key (PSK), EAP-Generic Token Card (GTC) or Certificate and EAP-Generic Token Card (GTC). • **IKE profiles (phase 1)**: ○ DH by default, ○ Lifetime, ○ Proposals • **IPsec profile (phase2)**: ○ Lifetime, ○ Authentication, ○ Encryption, ○ PFS.
Search in logs	When a name is assigned to the IPsec rule, clicking on this button will run a search by the name of the rule in the IPsec VPN log and show the results.
Search in monitoring	Clicking on this button will open the screen to monitor IPsec tunnels (**Monitoring** tab > **Monitoring** module > **IPsec VPN tunnels**).

REMARKS
Right-clicking anywhere in the grid will display a pop-up menu offering the following actions:

- **Add,**
- **Copy,**
- **Cut,**
- **Paste,**
- **Show details**
- **Delete,**

- **Search in logs,**
- **Search in monitoring.**

The table

Line	This column indicates the number of the line processed in order of appearance on the screen.
Status	This column shows the status on / off of the tunnel. When a tunnel is created, it is enabled by default. Click twice to disable it.
Name	A name can be given to this IPsec rule so that it will be easier to look for events that involve this rule in logs.
Local network	Select the host, host group, address range, network or network group that will be accessible via the IPsec VPN tunnel, from the drop-down list of objects.
Peer	Configuration of the peer, which can be viewed in the tab of the same name in the IPsec VPN module.
Remote network	Select from the drop-down list of objects, the host, host group, address range, network or network group accessible through the IPsec tunnel with the peer. **NOTE** When creating a new mobile IPsec VPN policy via the wizard, you will be asked to enter details about the local network, and not the remote network, since the IP address is unknown. The object "Any" will therefore be selected by default.
Domain name	This option makes it possible to specify the domain (LDAP directory) on which the mobile peer must be authenticated. The same user can therefore simultaneously set up several IPsec VPN tunnels and access separate resources by authenticating on several directories.
Group	This option makes it possible to specify the user's group on the authentication domain. The same user can therefore simultaneously set up several IPsec VPN tunnels by authenticating on one or several directories, and accessing separate resources by obtaining the specific privileges for the group in question. The **Domain name** must be specified for this option.
Protocol	This option makes it possible to restrict the setup of IPsec tunnels to traffic based on specific protocols: • TCP • UDP • ICMP • GRE • All
Encryption profile	This option makes it possible to select the protection model associated with your VPN policy, from three preconfigured profiles: **StrongEncryption, GoodEncryption** and Mobile. Other profiles can be created or modified in the tab *Encryption profiles*.

Config mode	This column makes it possible to enable "Config mode", which is disabled by default. This allows the traffic endpoint IP address to be distributed to the peer. **NOTES** 1. If you choose to enable this mode, you will need to select an object other than "Any" as the remote network. 2. With config mode, only one policy can be applied per profile. The **Edit Config mode** button allows you to enter the parameters of the IPsec Config mode: • **DNS server used**: this field determines the host (DNS server) that will be used by mobile clients, for DNS resolutions. You can select it or create it in the object database. This field is empty by default. • **Domains used in Config mode**: the client will use the DNS server selected earlier, only for domains specified in this table. For other domains, the client will continue to use its DNS server(s). Therefore generally internal domain names are involved. **EXAMPLE** In the case of the domain "company.com", if an iPhone attempts to connect to "www.company.com" or "intranet.company.com" it will use the DNS server specified above. However, if it attempts to contact "www.google.fr", it will continue to use its older DNS servers.
Comments	Description given of the VPN policy.
Keep alive	The additional **Keepalive** option makes it possible to artificially maintain mounted tunnels. This mechanism sends packets that initialize the tunnel and force it to be maintained. This option is disabled by default to avoid wasting resources, especially in the case of a configuration containing many tunnels set up at the same time without any real need for them. To enable this option, assign a value other than 0, corresponding to the interval in seconds, between each UDP packet sent.

NOTE
You can only use and create a single mobile (roadwarrior) configuration per IPsec profile. Peers can be applied to all profiles. As a result, only one authentication type can be used at a time for the mobile configuration.

Checking the policy in real time

The window for editing IPsec policy rules has a "**Check policy**" field (located below the table), which warns the administrator whenever there are inconsistencies or errors in the rules created.

Peers tab

This tab consists of two sections:

- Left: the list of site-to-site IPsec VPN peers (**Remote gateways**) and mobile IPsec VPN peers (**Mobile peers**).
- Right: information about the selected peer.

List of peers

Enter a filter	This field allows performing searches on the name of the object and its various properties, by occurrence, letter or word.
Add	Peers can be added to this area. To do so, select the type of peer to create from the drop-down list: • **New remote gateway** (for site-to-site tunnels), • **New mobile peer**.
Action	When you select a peer from the list, expand the **Action** menu to: • **Duplicate** this peer, • **Rename** this peer, • **Delete** this peer, • **Check usage** of this peer in the firewall configuration.

Gateway peer information

Select a peer from the list to display information about it.

Comments	Description given of the local peer.
Remote gateway	Object selected to represent the remote IP address during the creation of the peer via the wizard.
Local address	External interface presented to set up the tunnel with the peer shown.
IKE profile	This option offers three preconfigured profiles as the protection model associated with Phase 1 of your VPN policy: **StrongEncryption**, **GoodEncryption** and **Mobile**. Other profiles can be created or modified in the tab *Encryption profiles*.
IKE version	This option allows selecting the version of the IKE protocol (IKEv1 or IKEv2) that the peer uses.

Identification

Authentication method	This field will show the authentication method selected during the creation of your peer via the wizard. You may modify your choice by selecting another method from the drop-down list. **NOTE** For a "gateway" peer, you have the choice of **Certificate** or **Pre-shared key (PSK)**.

Certificate	If you have chosen certificate-based authentication, this field will display the certificate to display to the peer to set up the IPsec tunnel. The icon indicates certificates with a TPM-protected private key. For more information on the TPM, see the section Trusted Platform Module. If you had opted for the pre-shared key method, this field will not appear.
Local ID (Optional)	This field represents an IPsec VPN tunnel endpoint, and shares the “secret” or the PSK with the “Peer ID”, the other endpoint. You are represented by the “Local ID”. Full Qualified Domain Name) or an e-mail address (user@fqdn). This identifier must be in the form of an IP address, a domain name (FQDN:
Peer ID (Optional)	This field represents an IPsec VPN tunnel endpoint, and shares the “secret” or the PSK with the “Local ID”, the other endpoint. The “Peer ID” represents your peer. The format is the same as the previous field.
Pre-shared key (ASCII)	In this field your PSK appears in the format you had selected earlier when creating the peer via the wizard: ASCII or hexadecimal characters (the format can be selected in the checkboxes below the field if you wish to change formats).
Edit	This button makes it possible to directly edit the pre-shared key that was used to set up the IPsec tunnel with this peer.

Post-quantum pre-shared keys (PPK)

The computing power of quantum computers will very likely allow it to decrypt keys that were negotiated using the Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH) methods, therefore endangering the security of the IKEv2 protocol.

Malicious users would now be able to carry out "store now, decrypt later" attacks, by intercepting IPsec communications and storing them in order to decrypt them later using a quantum computer.

Clients who wish to protect themselves against such attacks can already use post-quantum pre-shared keys (PPK) to protect the exchange of data encryption keys.

To find out more on the use of post-quantum pre-shared keys for the IKEv2 protocol, please refer to RFC 8784.

In line with these recommendations, SNS versions 4.8 and higher offer the option of setting post-quantum pre-shared keys for peers using the IKEv2 protocol with certificate-based authentication.

> **NOTE**
> To be effective, these PPKs must have a sufficiently high entropy (minimum 256 bits according to RFC 8784).

PPK ID	Full Qualified Domain Name) or an e-mail address (user@fqdn). This identifier must be in the form of an IP address, a domain name (FQDN: If this ID matches the ID of a PPK that has already been defined on the firewall (Identification tab in the IPsec VPN module), this PPK will automatically be used. In this case, there is no need to use the **PPK passphrase** field. This field is mandatory if the **PPK required** checkbox has been selected.

PPK passphrase	If the PPK ID entered earlier does not match any PPK defined on the firewall (Identification tab in the IPsec VPN module), click on **Edit** to open the dialog box to enter the password (also called a secret) for this new PPK. This password can either be in ASCII or hexadecimal.
PPK required	If this option is selected, it means that a PPK must be used to set up a tunnel with the peer.

Advanced properties

Do not initiate the tunnel (Responder only)	If this option is selected, the IPsec server will be put on standby. It won't initiate tunnel negotiation. This option is used in the case where the peer is a mobile host.
IKE fragmentation	With this checkbox, IKE fragmentation can be enabled when IKE packets exceed the standard packet size configured on the firewall.
DPD	This field makes it possible to configure the DPD (*Dead Peer Detection*) feature on VPNs, which checks whether a peer is still operational. When DPD is enabled on a peer, requests (*R U there*) are sent to test the availability of the other peer , which will need to acknowledge the requests in order to confirm its availability (*R U there ACK)*. These exchanges are secured via ISAKMP (Internet Security Association and Key Management Protocol) SAs (*Security Associations*). If it is detected that a peer is no longer responding, the negotiated SAs will be destroyed. **IMPORTANT** This feature provides stability to the VPN service on Stormshield Network Firewalls on the condition that the DPD has been correctly configured. Four choices are available for configuring **DPD**: • **Inactive**: DPD requests from the peer are ignored. • **Passive**: DPD requests sent by the peer get a response from the firewall. However, the firewall does not send any. • **Low**: the frequency of DPD packets being sent is low and the number of failures tolerated is higher (*delay* 600, *retry* 10, *maxfail* 5). • **High**: the frequency of DPD packets being sent is high and the number of failures relatively low (*delay* 30, *retry* 5, *maxfail* 3). The value *delay* defines the period after a response is received before the next request is sent. The value *retry* defines the time to wait for a response before sending the request again. The value *maxfail* is the number of requests sent without receiving responses before the peer is considered absent.
DSCP	In this field, you can specify the value of the DSCP field assigned to IKE network packets sent to this peer. Select one of the proposed values or specify a customized DSCP field (integer between 0 and 63 inclusive).

CRL required	When the firewall verifies the peer certificate, it checks to see whether the certificate has an up-to-date CRL; this CRL may be local or hosted on a distribution point. When the firewall does not find an up-to-date CRL, its behavior will be determined by the value assigned to this field: • Not required: the firewall accepts the certificate anyway, • Mandatory: the firewall rejects the certificate, • Auto: the firewall rejects the certificate if the peer is defined as DR-compatible or if DR mode is enabled. It accepts the certificate in all other cases.

NOTE

For every field that contains "Gateway" and the icon , you can add an object to the existing database by specifying its name, DNS resolution, IP address and then clicking on **Apply**.

Mobile peer information

Select a peer from the list to display information about it.

Comments	Description given of the remote peer.
Remote gateway	This field is grayed out for mobile peers.
Local address	External interface presented to set up the tunnel with the peer shown.
IKE profile	This option makes it possible to select the protection model associated with your VPN policy, from three preconfigured profiles: **StrongEncryption**, **GoodEncryption** and **Mobile**. Other profiles can be created or modified in the tab *Encryption profiles*.
IKE version	This option allows selecting the version of the IKE protocol (IKEv1 or IKEv2) that the peer uses.

Identification

Authentication method	This field will show the authentication method selected during the creation of your peer via the wizard. You may modify your choice by selecting another method from the drop-down list. **NOTE** For mobile peers, you have a choice between **Certificate**, **Pre-shared key (PSK)**, **EAP-Generic Token Card (GTC)** or **Certificate and EAP-Generic Token Card (GTC)**.
Certificate	This field appears only if you have chosen authentication via **Certificate**, **EAP-Generic Token Card (GTC)** or **Certificate and EAP-Generic Token Card (GTC)**. It displays the certificate that you present to set up the tunnel with this peer, or suggests that you select it from the drop-down list. The icon indicates certificates with a TPM-protected private key. For more information on the TPM, see the section Trusted Platform Module.

Local ID (Optional)	This field represents an IPsec VPN tunnel endpoint, and shares the “secret” or the PSK with the “Peer ID”, the other endpoint. You are represented by the “Local ID”. Full Qualified Domain Name) or an e-mail address (user@fqdn). This identifier must be in the form of an IP address, a domain name (FQDN: **NOTE** This field can only be accessed if you have selected the **Pre-shared key** authentication method.
Peer ID (Optional)	This field represents an IPsec VPN tunnel endpoint, and shares the “secret” or the PSK with the “Local ID”, the other endpoint. The “Peer ID” represents your peer. The format is the same as the previous field.
Groups	This grid appears only if you have chosen authentication via **EAP-Generic Token Card (GTC)** or **Certificate and EAP-Generic Token Card (GTC)**. It shows the user groups attached to this peer profile, which were defined when the profile was created. You can change the grid to **Add** or **Delete** groups.
Pre-shared key (ASCII)	This field only appears if you have selected the **Pre-shared key (PSK)** authentication method. You can edit this field to view or change your PSK to the format you had selected when you created the peer via the wizard: ASCII or hexadecimal characters (the format can be selected in the checkboxes below the field if you wish to change formats).
Edit	This button makes it possible to directly edit the pre-shared key that was used to set up the IPsec tunnel with this peer.

Post-quantum pre-shared keys (PPK)

The computing power of quantum computers will very likely allow it to decrypt keys that were negotiated using the Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH) methods, therefore endangering the security of the IKEv2 protocol.

Malicious users would now be able to carry out "store now, decrypt later" attacks, by intercepting IPsec communications and storing them in order to decrypt them later using a quantum computer.

Clients who wish to protect themselves against such attacks can already use post-quantum pre-shared keys (PPK) to protect the exchange of data encryption keys.

To find out more on the use of post-quantum pre-shared keys for the IKEv2 protocol, please refer to RFC 8784.

In line with these recommendations, SNS versions 4.8 and higher offer the option of setting post-quantum pre-shared keys for peers using the IKEv2 protocol with certificate-based authentication.

NOTE
To be effective, these PPKs must have a sufficiently high entropy (minimum 256 bits according to RFC 8784).

PPK ID	Full Qualified Domain Name) or an e-mail address (user@fqdn). This identifier must be in the form of an IP address, a domain name (FQDN: If this ID matches the ID of a PPK that has already been defined on the firewall (Identification tab in the IPsec VPN module), this PPK will automatically be used. In this case, there is no need to use the **PPK passphrase** field. This field is mandatory if the **PPK required** checkbox has been selected.
PPK passphrase	If the PPK ID entered earlier does not match any PPK defined on the firewall (Identification tab in the IPsec VPN module), click on **Edit** to open the dialog box to enter the password (also called a secret) for this new PPK. This password can either be in ASCII or hexadecimal.
PPK required	If this option is selected, it means that a PPK must be used to set up a tunnel with the peer.

Advanced properties

Do not initiate the tunnel (Responder only)	This option is grayed out and validated, as a tunnel to a mobile client with an unknown IP address cannot be set up. In this configuration, the firewall is therefore in “responder only” mode.
IKE fragmentation	With this checkbox, IKE fragmentation can be enabled when IKE packets exceed the standard packet size configured on the firewall.

DPD	This field makes it possible to configure the DPD (*Dead Peer Detection*) feature on VPNs, This would allow checking whether a peer is still operational. When DPD is enabled on a peer, requests (*R U there*) are sent to test the availability of the other peer , which will need to acknowledge the requests in order to confirm its availability (*R U there ACK)*. These exchanges are secured via ISAKMP (Internet Security Association and Key Management Protocol) SAs (*Security Associations*). If it is detected that a peer is no longer responding, the negotiated SAs will be destroyed. **IMPORTANT** This feature provides stability to the VPN service on Stormshield Network Firewalls on the condition that the DPD has been correctly configured. Four choices are available for configuring **DPD**: • **Inactive**: DPD requests from the peer are ignored. • **Passive**: DPD requests sent by the peer get a response from the firewall. However, the firewall does not send any. • **Low**: the frequency of DPD packets being sent is low and the number of failures tolerated is higher (*delay* 600, *retry* 10, *maxfail* 5). • **High**: the frequency of DPD packets being sent is high and the number of failures relatively low (*delay* 30, *retry* 5, *maxfail* 3). The value *delay* defines the period after a response is received before the next request is sent. The value *retry* defines the time to wait for a response before sending the request again. The value *maxfail* is the number of requests sent without receiving responses before the peer is considered absent.
DSCP	In this field, you can specify the value of the DSCP field assigned to IKE network packets sent to this peer. Select one of the proposed values or specify a customized DSCP field (integer between 0 and 63 inclusive).
CRL required	When the firewall verifies the peer certificate, it checks to see whether the certificate has an up-to-date CRL; this CRL may be local or hosted on a distribution point. When the firewall does not find an up-to-date CRL, its behavior will be determined by the value assigned to this field: • Not required: the firewall accepts the certificate anyway, • Mandatory: the firewall rejects the certificate, • Auto: the firewall rejects the certificate if the peer is defined as DR-compatible or if DR mode is enabled. It accepts the certificate in all other cases.

Identification tab

Approved certification authorities

This table will allow you to list authorities to identify your peers within the IPsec VPN module.

Add	When you click on this button, a window will open showing the CAs and sub-CAs that you have created earlier. Select the authorities that will enable you to check the identities of your peers, by clicking on **Select**. The CA or sub-CA selected will be added to the table.
Delete	Select the CA to be removed from the list and click on **Delete**.

CA

Below this field, the added and approved certification authorities will be displayed.

Mobile tunnels: pre-shared keys (PSK)

If you had created a mobile peer using the **Pre-shared key (PSK)** authentication method, this table will be pre-entered.

You would have edited a key by assigning it an ID and a value (in hexadecimal or ASCII characters).

Search	Even though the table displays all the pre-shared keys of your mobile tunnels by default, you can search by occurrence, letter or word, so that only the desired keys are displayed.
Add	When you click on this button, a key editor window will appear: you need to provide it with an ID, a value and confirm it. You can choose to edit characters in hexadecimal or ASCII.
Delete	Select the key to be removed from the list and click on **Delete**.

Identity

This column displays the IDs of your pre-shared keys, which may be represented by a domain name (FQDN), an e-mail address (USER_FQDN) or an IP address.

Key

This column displays the values of your pre-shared keys in hexadecimal characters.

NOTES

- An unlimited number of pre-shared keys can be created.
- Deleting a pre-shared key that belongs to an IPsec VPN tunnel will cause this tunnel to malfunction.
- To define an ASCII pre-shared key that is sufficiently secure, you must follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management.

Post-quantum pre-shared keys (PPK)

The computing power of quantum computers will very likely allow it to decrypt keys that were negotiated using the Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH) methods, therefore endangering the security of the IKEv2 protocol.

Malicious users would now be able to carry out "store now, decrypt later" attacks, by intercepting IPsec communications and storing them in order to decrypt them later using a quantum computer.

Clients who wish to protect themselves against such attacks can already use post-quantum pre-shared keys (PPK) to protect the exchange of data encryption keys.

To find out more on the use of post-quantum pre-shared keys for the IKEv2 protocol, please refer to RFC 8784.

In line with these recommendations, SNS versions 4.8 and higher offer the option of setting post-quantum pre-shared keys for peers using the IKEv2 protocol with certificate-based authentication.

NOTE
To be effective, these PPKs must have a sufficiently high entropy (minimum 256 bits according to RFC 8784).

IMPORTANT
If you have created or modified mobile peers earlier to create a PPK for them that had not yet existed, this PPK will not automatically be added to the grid.

Possible operations

Find key	You can search by occurrence, letter or word, so that only the desired keys are displayed.
Add	When you click on this button, a key editor window will appear. You need to enter: • An ID in the form of a domain name (FQDN), an e-mail address or an IP address, • The key value (password) and confirm it. You can enter/edit the key value in hexadecimal or ASCII.
Delete	Select the key to be removed from the list and click on **Delete**.
Edit selection	Select the key to edit and apply the desired changes.
Export the list of PPKs	This button allows you to export the list of PPKs in CSV format, and download it to your workstation.

NOTE
PPKs that are directly created on the peer will not appear in this grid.

Advanced configuration

Enable searching in several LDAP directories (pre-shared key or certificate modes)	When several LDAP directories have been defined, selecting this checkbox will allow the firewall to browse these directories sequentially to authenticate mobile peers. This method is available regardless of the authentication type chosen (pre-shared key or certificate). If this checkbox is not selected, the firewall will only query the directory defined by default.

List of directories

The various directories listed will be queried according to their order in the table.

Add	Clicking on this button will add a line to the table in the form of a drop-down list that allows selecting one of the directories defined on the firewall. This button is grayed out when all of the firewall's directories are selected.
Delete	Select the key to be removed from the list and click on **Delete**.
Move up	This button makes it possible to move the selected directory up the list to raise its priority when the firewall queries the list of directories.
Move down	This button makes it possible to move the selected directory up the list to lower its priority when the firewall queries the list of directories.

Encryption profiles tab

Default encryption profiles

The profiles defined by default in Phase 1 and 2 will be preselected each time a new peer is created.

IKE

Phase 1 of the IKE protocol aims to set up an encrypted and authenticated communication channel between both VPN peers. This “channel” is called ISAKMP SA (different from the IPsec SA). Two negotiation modes are possible: main mode and aggressive mode.

The drop-down list makes it possible to select the protection model associated with your VPN policy, from six pre-configured profiles:

- **DR** (suitable for configurations that are designed to meet *Diffusion Restreinte* mode requirements),
- **StrongEncryption**,
- **GoodEncryption**,
- **Mobile**,
- **PQCEncryption** (for configurations with peers that exclusively use post-quantum encryption standards),
- **PQCTransition** (for configurations that are migrating to post-quantum encryption standards).

Others can also be created by using the **Add** button.

IPsec

Phase 2 of the IKE protocol securely negotiates (through the ISAKMP SA communication channel negotiated in the first phase) the parameters of future IPsec SAs (one incoming, one outgoing).

The drop-down list makes it possible to select the protection model associated with your VPN policy, from six pre-configured profiles:

- **DR** (suitable for configurations that are designed to meet *Diffusion Restreinte* mode requirements),
- **StrongEncryption**,
- **GoodEncryption**,

- **Mobile**,
- **PQCEncryption** (for configurations with peers that exclusively use post-quantum encryption standards),
- **PQCTransition** (for configurations that are migrating to post-quantum encryption standards).

Others can also be created by using the **Add** button.

Table of profiles

This table offers a series of predefined Phase 1 (IKE) and Phase 2 (IPsec) encryption profiles.

Possible operations

Add	By clicking on this button, you will be able to add a **New phase 1 profile (IKE)** or **New phase 2 profile (IPsec)**, which will be displayed in the corresponding column. **Name** the profile. Profiles and their characteristics can also be copied: to do so, select the desired profile and click on the option **Copy selection**, and give it a **Name**.
Actions	In this drop-down menu, one of the following actions can be applied to the selected profile: • **Duplicate** the profile, • **Define the default profile**, • **Delete** the profile, • **Check usage** of the profile.

IKE profile

Depending on the IKE profile added or selected, you will see its characteristics to the right of the screen ("**General**" and "**Proposals**" fields).

General

Comments	Description given to your encryption profile.

Default Diffie-Hellman	This field represents two types of key exchange: if you have selected an **IKE** encryption profile, the **Diffie-Hellman** option will appear. **Diffie-Hellman** allows 2 peers to generate a common secret on each side, without sending sensitive information over the network. In addition, if you have chosen an **IPsec** profile, **PFS** will be offered. **Perfect Forward Secrecy** allows guaranteeing that there are no links between the various keys of each session. Keys are recalculated by the selected Diffie-Hellman algorithm. The higher the number indicating the key size, the higher the level of security. Regardless of what you choose, a drop-down list will suggest that you define the number of bits that allow strengthening security during the transmission of the common secret or password from one peer to another. Encryption algorithms based on elliptic curves (ECDSA algorithm: Elliptic Curve Digital Signature Algorithm) can also be selected. **NOTES** • To define an ASCII pre-shared key that is sufficiently secure, you must follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management. • The longer the password (or "key"), the higher the level of security, but at the same time consumes more resources. • The use of IPsec's PFS function (ISAKMP) is recommended.
Default KEM algorithm	Select the default KEM algorithm for the selected profile. This key encapsulation mechanism makes it possible to share a secret across a public communication network.
Maximum lifetime (in seconds)	Period after which keys will be renegotiated. The default duration of an **IKE** profile is 21600 seconds.

Proposals

This table allows you to modify or add combinations of encryption and authentication algorithms to the pre-entered list of the selected profile.

Add	The default combination suggested is: • **des** encryption algorithm with a "Strength" of 64 bits, • **sha1** authentication algorithm with a "Strength" of 160 bits, Click on the arrow to the right of the respective "Algorithm" columns if you wish to modify them. Each time you add a new line to the table, it will be of the priority level that follows.
Delete	Select the line to be deleted from the list and click on **Delete**.
Move up	Select the line to be moved up the table in order to raise the priority of the corresponding Encryption / Authentication combination.
Move down	Select the line to be moved down the table in order to lower the priority of the corresponding Encryption / Authentication combination.

Encryption

Algorithm	4 choices are offered: • 3des (obsolete), • aes, • aes_gcm_16 (recommended), • aes_ctr. When a preset profile is selected, the recommended choices will automatically be suggested by default. The advantage of the aes_gcm-16 algorithm is that it performs both authentication and encryption. You therefore do not need to choose an authentication algorithm in this case.
Strength	Number of bits defined for the selected algorithm.

Authentication

Algorithm	4 choices are offered: • **sha1** (obsolete), • **sha2_256,** • **sha2_384,** • **sha2_512**.
Strength	Number of bits defined for the selected algorithm.

DH group

Every IKE encryption/authentication proposal listed in this grid can be assigned a DH group other than the **Default Diffie-Hellman group** selected in the **General** section.

If no DH group has been specified for a proposal, the **Default Diffie-Hellman group** in the **General** section will be applied to this proposal.

KEM algorithms

Every IKE encryption/authentication proposal listed in this grid can be associated with a KEM algorithm other than the one selected in the **Default KEM algorithm** field.

IPsec profile

For each IPsec profile added or selected, you will see its characteristics to the right of the screen ("**General**", "**Authentication proposals**" and "**Encryption proposals**" fields).

General

Comments	Description given to your encryption profile.
Maximum lifetime (in seconds)	Period after which keys will be renegotiated. The default duration of an **IPsec** profile is 3600 seconds.

Authentication proposals

This table allows you to modify or add authentication algorithms to the pre-entered list of the selected profile.

Add	The authentication algorithm that appears by default when you click on this button is **hmac_sha256**, with a strength of 256 bits. Click on the arrow to the right of the "Algorithm" column if you wish to modify it. Each time you add a new line to the table, it will be of the priority level that follows.
Delete	Select the line to be deleted from the list and click on **Delete**.
Algorithm	4 choices are offered: • **hmac_sha1** (obsolete), • **hmac_sha256**, • **hmac_sha384**, • **hmac_sha512**.
Strength	Number of bits defined for the selected algorithm.

Encryption proposals

This table allows you to modify or add encryption algorithms to the pre-entered list of the selected profile.

Add	The encryption algorithm that appears by default when you click on this button is **aes_gcm_16 (recommended)**, with a strength of 256 bits. Click on the arrow to the right of the "Algorithm" column if you wish to modify it. Each time you add a new line to the table, it will be of the priority level that follows.
Delete	Select the line to be deleted from the list and click on **Delete**.
Algorithm	4 choices are offered: • **3des** (obsolete), • **aes**, • **aes_gcm_16** (recommended), • **aes_ctr**. The advantage of the aes_gcm-16 algorithm is that it performs both authentication and encryption.
Strength	Number of bits defined for the selected algorithm.

PFS proposals

Add	You can add Diffie-Hellmann groups to be assigned to IPsec encryption/authentication proposals.
Delete	Select the line to be deleted from the list and click on **Delete**.
DH group	After clicking on **Add**, select a Diffie-Hellmann group to add to the list of proposals.

KEM proposals

Add	You can add KEM algorithms to be associated with IPsec encryption/authentication proposals.
Delete	Select the line to be deleted from the list and click on **Delete**.
KEM algorithm	After clicking on **Add**, select a KEM algorithm to add to the list of proposals.

Click on **Apply** once you have completed the configuration.

IPV6 SUPPORT

Support for IPv6, offered in this version, allows firewalls to be integrated into IPv4 and/or IPv6 infrastructures. Network (interfaces and routing), filter, VPN and administration features are compatible with IPv6. This support is optional and can be enabled in the **Configuration** module.

The web administration interface will then be accessible regardless of whether it is in IPv6 or IPv4 as the firewall's network interfaces may have a single static IPv6 address or as a complement to an IPv4 address (double stack). Static routes and gateways can now be defined in IPv6; furthermore, the dynamic routing feature on Stormshield firewalls (Bird6) is also compatible.

The SLAAC mechanism (StateLess Address AutoConfiguration) has been implemented on Stormshield Network firewalls in order to generate Router Advertisements (RA), which allow automatically configuring network hosts by distributing the IPv6 prefixes to be used. These advertisements also allow transmitting DNS parameters (RDNSS support – RFC 6106) and defining the firewall as the default gateway. The firewall's DCHPv6 server or relay service can be used to complete this mechanism, in order to use IPv6 address reservation, for example.

Network objects (hosts, networks and IP address ranges) may have addresses in IPv6, or a hybrid address range. Filter policies can therefore be applied to IPv6 objects and can use the security inspection feature (customizable inspection profiles). However, application inspection features (Antivirus, Antispam and URL, SMTP, FTP and SSL filtering) are not available in this version. Likewise, address translation (NAT) cannot be performed on IPv6 objects.

> NOTE
> For each interface defined in IPv6 and belonging to a bridge, the **routing without analyzing** option in the IPv6 protocol must be **disabled** (*advanced configuration* tab in the **Network**>Interfaces module), in order to allow this traffic to be filtered.

IPsec tunnels are also compatible with IPv6; tunnels can therefore be set up between two IPv6 endpoints and both IPv4 and IPv6 traffic may go through them. Conversely, IPv6 traffic may also go through IPv4 IPsec tunnels.

IPv6 Support

Details of supported features

System

ACL

An internal IPv6 network is automatically integrated into the "Network_internals" group.

Configuration: NTP

Firewalls can synchronize their clocks with a time server (NTP server) configured in IPv6.

IPv4/IPv6 administration server

Firewalls can be administered in the same way from a remote host, whether it has IPv4 or IPv6 addresses (web administration and SSH connections). In order to do so, the server must listen on both protocols.

Active Update

The application protection features provided in Active Update (Antispam, Antivirus, etc.) can retrieve their updates from a mirror server that has an IPv6 address.

High availability (HA)

Sessions set up in IPv4 or IPv6 can be transferred on HA links in IPv4.

CLI commands

IPv6 commands are accessible in the module **Configuration** > **CLI Commands** in the firewall's web administration interface.

Network

Interfaces: double stack

Interfaces on the firewall may have IPv4 and IPv6 addresses simultaneously (double stack).

Interfaces: IPv6 addresses only

It is possible to configure a firewall (or simply one of its interfaces) in IPv6 alone.

Interfaces: router advertisements (RA)

The firewall can send out router advertisements and prefixes (RA: Router Advertisement).

Static routing

IPv6 static routes can be defined on the firewall.

Dynamic routing

The dynamic routing engine handles IPv6 routes (RIP / BGP / OSPF protocols).

DHCPv6

The firewall can take on the role of a DHCPv6 server or relay.

Objects

Network objects

Network objects may have only IPv4 addresses, only IPv6 addresses or both (double stack).

Users

Authentication

Users can log on to the web authentication portal regardless of whether the remote host is in IPv4 or IPv6.

Security policy

Filtering

Filter rules may simultaneously contain IPv4 objects, IPv6 objects and IPv4 and IPv6 objects (double stack).

Filtering: rule coherence checker

The coherence checker also applies to rules that include IPv6 objects.

Filtering: IPS

Protocol scans apply to Level 7 protocols transported over IPv6 (example: HTTP, SMTP, etc.).

tab

Quality of service processing can be applied to IPv6 traffic.

IPv6 implicit rules

Implicit rules specific to IPv6 services (router advertisements, DHCPv6) have been added (these rules are listed in the paragraph **General points** > **Implicit rules**).

Monitoring

Alarms / Logs

Events raised by IPv6 traffic (alarms, etc.) are saved in log files.

VPN

IPsec IKEv1

IPv4 and/or IPv6 traffic can be transported through IPsec tunnels set up between:

- IPv6 tunnel endpoints,
- IPv4 tunnel endpoints.

Notifications

Syslog

Logs can be sent to syslog servers in IPv6.

SNMP server

The SNMP server embeds the MIB-2 in IPv6. It can also generate traps in IPv6.

Unsupported features

In SNS version 5, the following are the main features that are unavailable for IPv6 traffic:

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

General points

Active Update

The firewall's Active Update service can now be used with update servers configured in IPv6. In this case, a mirror server needs to be installed for updates configured in double stack (IPv4 / IPv6): this server will be able to synchronize in IPv4 with Stormshield Active Update servers, and provision its updates to firewalls in IPv6.

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. Indeed, as local IPv6 link addresses are derived from the MAC address, these addresses will be different, causing routing problems during a switch.

Protocols

Enabling IPv6 support does not modify the IP configuration elements (Application protection > Protocols module).

Implicit rules

Implicit rules specific to the use of IPv6 services have been added and can be enabled or disabled. These rules are as follows:

- Allow router solicitations (RS) in multicast mode or to the firewall,
- Allow requests to the DHCPv6 server and DHCPv6 multicast solicitations.

Configuration

IPv6 can be enabled globally on Stormshield Network Firewalls through the *Network parameters* tab in the **Configuration** module.

Network Settings tab

Enable IPv6 support on this Firewall	Clicking on this button enables IPv6 network layers on the firewall, therefore making IPv6 parameters accessible from the various configuration modules (Interfaces, DHCP, Routing, etc.). The firewall must be restarted in order to apply the activation of IPv6. **WARNING** As this action is irreversible, you are advised to back up your configuration before enabling IPv6 support. To return to support for IPv4 addressing only, you will need to reset your firewall to its factory settings before you can restore the backup of this configuration. Reset your configuration by pressing the dedicated button if your appliance has one, or by using the "defaultconfig" CLI command in console mode.

NOTE
Likewise, for each interface with an IPv6 address and belonging to a bridge, the **routing without analyzing** option in the IPv6 protocol must be **disabled** (*advanced configuration* tab in the **Network**>**Interfaces** module), in order to allow this traffic to be filtered.

Bridges and interfaces

Bridges

"General configuration" tab

Address range

IPv6 address

Fixed IP (static)	When this option is selected, the bridge will have a static IPv6 address.
Address/ Mask	IP address assigned to the bridge (all interfaces contained in a bridge have the same IP address). Enter this address and its associated network mask in CIDR notation (example: 2001:db8::70/32), in the field below the checkbox.
Comments	Allows adding comments regarding the bridge's address.

Several IP addresses and associated masks can be defined for the same bridge (when aliases need to be created, for example). These aliases can allow you to use the Stormshield Network firewall as a central routing point. As such, a bridge can be connected to various sub-networks with a different address range. To add or remove them, simply use the **Add** and **Delete** buttons located above the fields in the table.

Several IP addresses (aliases) can be added in the same address range on an interface. In this case, these addresses must all have the same mask.

"Routing configuration" tab

On each interface, bridge or aggregated interface, router advertisements (RA) can be sent periodically to all IPv6 nodes (*multicast*) of the segment via the local link address or as a response to a router solicitation (RS) from a host on the network.

This advertisement allows an IPv6 node to obtain the following information:

- The address of the default router, in this case, the address of the firewall,
- The prefix(es) used on the link (in 64 bits),
- Indication of the use of SLAAC or DHCPv6 (*Managed*)
- Indication of the retrieval of other parameters via DHCPv6 (*OtherConfig*),
- DNS parameters, if any (RFC4862).

Automatic configuration, which is native in IPv6, is stateless (*StateLess Address AutoConfiguration* - SLAAC), meaning that the server does not choose IP addresses for its clients and does not need to remember them.

For example, a host has a local link address whose uniqueness has been confirmed via NPD DAD (*Neighbor Discovery Protocol – Duplicated Address Detection*). The host will then receive the periodic or solicited RA. If SLAAC information has been specified, the host will then create one or several IPv6 addresses based on the prefix(es) advertised and its interface ID (random or based on the MAC address). The router's IP address (the firewall's address) will then be used as the default gateway.

By default, the routers advertise their presence by broadcasting the first prefix deduced from the interface. DNS servers are those configured for the firewall by default (**System**> **Configuration** module).

NOTE
If router advertisements have been enabled on a bridge, they will only be broadcast on protected interfaces.

Automatic configuration settings

Automatic detection	If the DHCPv6 service has been enabled on the firewall (**Network> DHCP**), the firewall will automatically send out router advertisements (RA) on the corresponding interfaces, indicating to IPv6 nodes that they have to be auto-configured in DHCPv6 (the options "Managed" and "Other config" will then be enabled by default). If the firewall is acting as a DHCPv6 server, the configured interface must belong to one of the address ranges entered in the DHCPv6 configuration. If the firewall is used as a relay to a DHCPv6 server, the configured interface must belong to the list of the service's listening interfaces. If the DHCPv6 service is inactive, the sending of RAs will be disabled.
Send RA	The firewall's address is sent as the default router. The information relayed by this advertisement will be described further in this manual. This configuration is recommended in order to allow hosts that are directly connected (local link) to use SLAAC.
Disable	No router advertisement (RA) has been sent out. This configuration is recommended in bridge mode if an IPv6 router is directly connected (local link).

Router advertisements (RA)

Announce the prefix extracted from the interface address	The prefix advertised is the prefix configured in the interface's IPv6 address range (*Configuration* tab). The size of the IPv6 address mask (prefix length – CIDR) must be 64 bits.

Configuration with DHCPv6 server

The DHCPv6 server assigns addresses (Managed)	The advertisement indicates that the IPv6 addresses solicited will be distributed by the DHCPv6 service enabled on the firewall (**Network > DHCP**). This service is implemented by the firewall or a relay that is directly connected (local link).
The DHCPv6 server delivers additional options (Other config)	The advertisement indicates that other auto-configuration parameters such as the addresses of DNS servers or other types of servers, will be delivered by the DHCPv6 server (firewall or relay) that is directly connected (local link).

Advanced properties

DNS settings

Domain name	Default domain name to contact a queried server that does not have a domain.
Primary DNS server	IP address of the primary DNS server. If this field is blank, the address sent will be the address used by the firewall (**System > Configuration**)
Secondary DNS server	IP address of the secondary DNS server. If this field is blank, the address sent will be the address used by the firewall (**System > Configuration**)

Announced prefixes

Even though it is recommended that the announced prefix be the same as the interface's prefix, in the event the interface specifies several, this field will indicate the prefix to use.

Prefixes	Prefix to announce to hosts
Autonomous	Instruction to use stateless address auto-configuration (SLAAC): if this option has been selected, the host will then create one or several IPv6 addresses based on the prefix(es) advertised and its interface ID (random and/or based on the MAC address.
On link	This option specifies to the host that all hosts with the same prefix may be contacted directly, without going through the router. **NOTE** In IPv4, such information was deduced from the network mask.
Comments	Allows adding comments for the announced prefix.

Optional parameters

Certain specific parameters for router advertisements can be configured in CLI, such as the maximum size of a packet sent (MTU) over the link, the validity duration of the prefix(es) used over the link or the field *Router Lifetime*.

For more details and the possible values of these parameters, please refer to the guide "CLI serverd command reference – V1.0" available in your client area.

Ethernet interface in bridge mode

"Advanced properties" tab

Routing without analysis

Authorize without analyzing	Allows IPv6 packets to move between the interfaces of the bridge. No higher analysis or filter will then be applied on this protocol.

IMPORTANT
For each of the interfaces included in a bridge, you must unselect the option **Authorize without analyzing** for IPv6 in order for filtering to be applied on this traffic.

Ethernet interface in advanced mode

"General configuration" tab

To configure an interface in a network that does not belong to a bridge, simply remove it from the tree structure of the bridge by dragging it with the mouse.

During this detachment, the address range window will appear.

IPv4 address range	When this option is selected, the bridge will have an IPv4 address. If this address is static, this has to be indicated (followed by it network mask) in the field below the checkbox. By default, a dynamic address will be assigned to it via DHCP.

IPv6 address range	When this option is selected, the bridge will have a static IPv6 address. Enter this address and its associated network mask in CIDR notation (example: 2001:db8::70/32), in the field below the checkbox.

Once the interface is outside the bridge, you will be able to access the parameters of the interface described in the section **Ethernet interface in bridge mode**.

VLAN

"General configuration" tab

Address range

IPv6 address

Fixed IP (static)	When this option is selected, the VLAN will have a static IPv6 address.
Address/ Mask	IP address assigned to the VLAN. Enter this address and its associated network mask in CIDR notation (example: 2001:db8::70/32), in the field below the checkbox.
Comments	Enables comments regarding the VLAN's address.

"Routing configuration" tab

For options regarding **Automatic configuration settings** and **Router advertisements**, refer to the section **"Router advertisement (RA)" tab** in the **Bridge** menu.

Virtual interfaces

"IPsec interfaces (VTI)" tab

IPv6 address	Indicate the IPv6 address assigned to the IPsec interface.
IPv6 prefix	Indicate the IPv6 prefix associated with the IPsec interface

"Loopback" tab

IPv6 address	Indicate the IPv6 address assigned to the loopback interface.

Routing

The configuration of IPv6 routing is separated into three segments:

- IPv6 static route: allows defining static routes for IPv6 packets. Static routing represents a set of rules defined by the administrator as well as a default route.
- IPv6 BIRD dynamic routing: Allows configuring dynamic routing protocols (RIP, OSPF, BGP) in an IPv6 BIRD engine, in order to allow the firewall to learn routes managed by other appliances.

WARNING : IPv4 DYNAMIC ROUTING
The BIRD6 dynamic routing engine is dedicated to IPv6 dynamic routing. This configuration has to be performed in console mode in the files:
/usr/Firewall/ConfigFiles/Bird/global ([bird6] section) /usr/Firewall/ConfigFiles/Bird/bird6.conf
For more information on the configuration of dynamic routing, please refer to the Technical Note **BIRD Dynamic Routing**, available on Stormshield's Technical Documentation website.

Static routing and dynamic routing run simultaneously; static routing however has priority for transmitting packets over the network.

"IPv6 static routes" tab

Default gateway (router)	The default router is generally the equipment which allows your network to access the Internet. This is the address to which the firewall sends packets that need to go on the public network. If you do not configure a default router, the firewall would not know where to direct packets that have a destination address that differs from the networks directly linked to it. Hosts will therefore not be able to access any other network apart from their own. Click on the button to access the object database and select a host. The "Default gateway" field will be grayed out if a list of gateways has been defined in the advanced configuration zone.

Button bar

Search	Search that covers host, network and group objects.
Add	Adds an "empty" static route. The addition of the route (sending of the command) is applied once the new line is edited and the fields **Destination network (host, network or group object)** and **Interface** are entered.
Delete	Deletes one or several selected routes. Use the keys **Ctrl/Shift + Delete** to delete several routes.
Apply	Sends the configuration of the static routes.
Cancel	Cancels the configuration of the static routes.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of IPv6 static routes:

- Add,
- Remove.

Presentation of the table

The table sets out six fields of information:

Status	Status of the static routes: • **Enabled**: Double-click to enable the route created. • **Disabled**: The route is not functional. The line will be grayed out in order to reflect this.
Destination network (host, network or group object) (Mandatory)	Clicking on this column will open the object database to allow selecting a host, network or group.
Address range	IP address or group of addresses linked to the selected items in the column "Destination network (host, network or group object)". This field is entered automatically.
Interface (Mandatory)	A drop-down list allows selecting the outgoing interface for contacting the destination network. This object may either be an Ethernet interface, VLAN or modem (dialup).
Protected	This column indicates whether the route is protected. Protected routes are added to the object Network_internals. The behavior of the security configuration will take this parameter into account. Hosts that can be contacted via this route will be remembered in the intrusion prevention engine.
Gateway (Optional)	Clicking on this column will open the objects database in order to select a host (router).
(Optional) Comments	Any text.

"IPv6 dynamic routing" tab

This tab makes it possible to enable and configure the IPv6 BIRD dynamic routing engine (Bird6).

Enable dynamic routing (BIRD)	This option activates the use of the routing Bird6 dynamic engine.

The window located under the Bird6 activation option makes it possible to directly enter the configuration of the Bird6 dynamic routing engine.

For further information on how to configure dynamic routing or on migrating from ZebOS to BIRD, please refer to the BIRD Dynamic routing technical note, available on Stormshield's Technical Documentation website.

Advanced properties

Add IPv6 networks distributed via dynamic routing to the table of protected networks	In the table listing the intrusion prevention system's protected networks, this option allows automatically injecting networks spread by the dynamic routing engine (IPv4 / IPv6).

Sending the configuration

Changes made in this window can be confirmed using the "Apply" button.

WARNING
Syntax checks will not be conducted when the configuration is sent to the dynamic routing engine.

"IPv6 return routes" tab

When several gateways are used for load balancing, this tab will allow defining the gateway through which return packets will need to go in order to guarantee the consistence of connections.

REMARK
If the gateway selected from the drop-down list is a host object, this object must specify a MAC address.

Button bar

Add	Adds an "empty" return route. An added route (sending of a command) is effective only if its fields **Gateway** and **Interface** have been entered.
Delete	Deletes the selected route.
Apply	Sends the configuration of the return routes.
Cancel	Cancels the configuration of the return routes.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of IPv6 return routes:

- Add,
- Remove.

Presentation of the table

The table sets out four fields of information:

Status	Status of the static routes: • Enabled: Double-click to enable the route created. • Disabled: The route is not functional. The line will be grayed out in order to reflect this.
Interface (Mandatory)	Drop-down list that allows selecting a Loopback, Ethernet, VLAN, Dialup, GRE or GRETAP interface.
Gateway (Optional)	Clicking on this column will open the objects database in order to select a host or a virtual interface (IPsec). If the object is a host object, it must specify a MAC address.
Comments (Optional)	Any text.

DHCP

DHCP service settings are located within the DHCP IPv6 tab.

General

Enable service: enables the DHCP service in one of 2 specific modes: server or relay.

DHCP server	Sends various network parameters to DHCP clients.
DHCP Relay	The DHCP relay mode is to be used when client requests are to be redirected to an external DHCP server.

"DHCP server" service

The "DHCP server" service presents 4 configuration zones:

- **Default settings** This menu is reserved for the configuration of the DNS parameters sent to DHCP clients (domain name, primary and secondary DNS servers)
- **Address range** For each range, specify a group of addresses to be allocated to users. The allocated address will remain allocated for the duration determined in the advanced configuration.
- **Reservation** The address allocated by the service stays the same for hosts listed in the column **Reservation**.
- **Advanced properties** This menu allows enabling or disabling the automatic sending of the proxy configuration files for client hosts (WPAD: Web Proxy Autodiscovery Protocol). It is also possible to customize the duration of the allocation of IP addresses distributed by the DHCP service.

> **NOTE**
> DHCPv6 can only function with the Router advertisements (RA) mechanism configured on an interface or bridge in the module **Network**>**Interfaces**. These router advertisements indicate that the firewall is presented as the default router.

Default settings

If the DHCP server option has been selected, global parameters can be configured here, such as the **domain name**, **DNS servers**, etc. that client hosts will use.

Domain name	Domain name used by DHCP client hosts for DNS resolution.
Primary DNS server	Select the primary DNS server that will be sent to DHCP clients. This is a host object. If no objects are specified, the firewall's primary DNS server will be sent to them.
Secondary DNS server	Select the secondary DNS server that will be sent to DHCP clients. This is a host object. If no objects are specified, the firewall's secondary DNS server will be sent to them.

Address range

In order for a DHCP server to provide IP addresses, an address pool from which the server can pick addresses has to be configured.

Action buttons

To add or delete address ranges, click on **Add** or **Delete**.

Add	Allows adding an address range. Select or create an IPv6 address range (**IP address range** network object).
Delete	Allows deleting one or several address ranges simultaneously.

The table shows the address ranges used by the DHCP server for distributing addresses to clients:

Address range	Select an **IP address range** network object from the drop-down list. The server will pick from this pool to distribute addresses to clients. If none of the firewall's protected interfaces has an IP address in the network hosting this range, a warning message will appear: "No protected interfaces match this address range".
Primary DNS	This field allows assigning a specific main DNS server to DHCP clients. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Primary DNS** field in the **Default settings** section will then be used as the DNS server for the client.
Secondary DNS	This field allows assigning a specific secondary DNS server to DHCP clients. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Secondary DNS** field in the **Default settings** section will then be used as the DNS server for the client.
Domain name	This field allows indicating a specific domain name that will be used by the DHCP client for its DNS resolution. If no name is specified, the value "Default domain" will be displayed in this column. The domain name indicated in the **Domain name** field in the **Default settings** section will then be used for the client.

WARNING
Ranges must not overlap. An address range belongs to a single bridge/interface.

Reservation

Even when a server that dynamically distributes IP addresses to clients is used, a specific IP address can be reserved for certain hosts. This configuration resembles static addressing, but nothing is configured on client workstations, thereby simplifying their network configuration.

Action buttons

To add or delete reserved addresses, click on **Add** or **Delete**.

Add	Allows adding a reserved IP address for a specific host network object.
Delete	Allows deleting an IP address reservation. If a reservation is cancelled, the host concerned will be assigned a new random address when it is renewed.

The table shows host objects for which addresses have been reserved (each object must contain the reserved IPv6 address), as well as their DUID (DHCP Unique Identifier). The DUID is mandatory as it allows identifying the client host during the assignment or renewal of IP addresses so that it can be assigned the reserved address. It plays a role that is similar to that of a MAC address in DHCP IPv4.

Reservation	This field contains the name of the network object (host) that has a reserved IPv6 address.
DHCP Unique Identifier (DUID)	This field contains the host's unique ID. This ID allows the firewall to identify the client and reassign the reserved IP address to it. On a Windows client workstation, this DUID is entered in the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TCPIP6\Parameters\Dhcpv6DUID
Primary DNS	This field allows assigning a specific main DNS server to each DHCP client using address reservation. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Primary DNS** field in the **Default settings** section will then be used as the DNS server for the client.
Secondary DNS	This field allows assigning a specific secondary DNS server to each DHCP client using address reservation. Select a host network object from the drop-down list. If no objects are selected, the value "default" will be displayed in this column. The host selected in the **Secondary DNS** field in the **Default settings** section will then be used as the DNS server for the client.
Domain name	This field allows indicating a specific domain name that will be used by the DHCP client for its DNS resolution. If no name is specified, the value "Default domain" will be displayed in this column. The domain name indicated in the **Domain name** field in the **Default settings** section will then be used for the client.

Advanced properties

TFTP Server	The TFTP server is used for booting hosts remotely. This field (option 150: TFTP server address) can be used for starting up network devices such as routers, X-terminals or workstations without hard disks. Only servers that have an IPv6 interface will appear in the list.
Distribute the Web proxy autodiscovery (WPAD) file	If this option has been selected, the DHCP server will distribute the internet access configuration to DHCP clients through a PAC Proxy Auto Configuration). This file, which has a ".pac" extension, has to be entered in the authentication settings (*Captive portal* tab in the menu **Configuration**>**Users**>**Authentication**). It can be made accessible from internal and/or external interfaces (*Internal interfaces* and *External interfaces* tabs in the menu **Configuration**>**Users**>**Authentication**).

Assigned lease time

Default (hour)	For the purpose of optimizing network resources, IP addresses are assigned for a limited period. You therefore need to indicate here the default duration for which hosts will keep the same IP address.
Minimum (hour)	Minimum duration for which hosts will keep the same IP address.
Maximum (hour)	Maximum duration for which hosts will keep the same IP address.

"DHCP relay" service

The "DHCP relay" service contains 3 configuration zones:

- **Settings** This menu allows configuring the DHCP server(s) to which the firewall will relay DHCP requests from client hosts.
- **Listening interfaces for DHCP requests** Network interfaces on which the firewall listens for client DHCP requests.
- **Outgoing interfaces on the DHCP relay**. Specify the interfaces through which the firewall will send requests to the DHCP server(s) indicated earlier.

Settings

DHCP server(s)	The drop-down list allows selecting a host object or group object containing hosts. The firewall will relay client requests to this or these DHCP server(s).

Listening interfaces for DHCP requests

Indicate the network interfaces through which the firewall will receive DHCP client requests.

Action buttons

In order to add or delete listening interfaces, click on **Add** or **Delete**.

Add	Adds a row to the table and opens a drop-down list of the firewall's interfaces in order to select an interface.
Delete	Allows selecting one or several listening interfaces.

Outgoing interfaces on the DHCP relay

Indicate the network interfaces through which the firewall will be able to contact the DHCP server(s) in order to send DHCP client requests.

Action buttons

In order to add or delete output interfaces, click on **Add** or **Delete**.

Add	Adds a row to the table and opens a drop-down list of the firewall's interfaces in order to select an interface.
Delete	Allows selecting one or several output interfaces.

Network objects

This module is divided into two sections:

- The action bar, at the top of the screen, allowing objects to be sorted and modified.
- Two columns dedicated to objects: one column listing them, the other displaying their properties.

> **NOTE**
> The creation of objects only allows declaring an object in Global mode if the option "Display global policies (Filter, NAT, IPsec VPN and Objects)" has been enabled in the **Preferences** module.

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

Possible actions

IP version

This button completes the filtering feature and allows choosing the type of objects to display according to the IP version that they use. A drop-down menu will offer you the following choices:

IPv4 and IPv6	This option allows displaying all network objects of the chosen type (host, network, IP address range) in the list on the left, regardless of the IP version used for their address.
IPv4	This option allows displaying all network objects of the chosen type (host, network, IP address range) in the list on the left with addresses exclusively in IPv4.
IPv6	This option allows displaying all network objects of the chosen type (host, network, IP address range) in the list on the left with addresses exclusively in IPv6.

The different types of objects

Computer

Select a host in order to view or edit its properties. Each object of this type must contain a name and DNS resolution method: "Automatic" if the host has been configured with a dynamic IP address; "None (static IP)" if the host has been configured with a static IP address).

IPv6 address	IPv6 address of the selected host. **EXAMPLE** 2001:db8:11a::10 To make it easier to enter the IPv6 address, a drop-down list will suggest all the global prefixes entered on the firewall.

Network

Select a network in order to view or edit its properties. Each object of this type must contain a name, network address and its associated mask.

IPv6 address	IPv6 address of the selected network and its associated mask, in CIDR notation. **EXAMPLE** 2001:db8::/32 To make it easier to enter the IPv6 address, a drop-down list will suggest all the global prefixes entered on the firewall.

Filtering

Network objects (hosts, networks and IP address ranges) may have addresses in IPv6, or in a hybrid mode (IPv4 and IPv6). Filter policies can therefore be applied to IPv6 objects and can use the security inspection feature (customizable inspection profiles).

However, application inspection (Antivirus, Antispam and URL, SMTP, FTP and SSL filtering) and address translation (NAT) features are not available for IPv6 objects in this version (the *NAT* tab is renamed "*NAT IPv4*" when IPv6 is enabled).

"Filtering" tab

Filtering consists of two parts. The strip at the top of the screen allows choosing the filter policy, activating it, editing it and seeing its last modification. The filter table is dedicated to the creation and configuration of rules.

Actions on filter policy rules

The available actions are the same as those for rules including IPv4 or IPv6 objects.

> **REMARK**
> NDP (Neighbour Discovery Protocol) traffic will never be blocked, even in the case of a "block all" filter policy. This concerns NS (Neighbour Solicitation) and NA (Neighbour Advertisement) messages.

In Stormshield Network 1.0, certain actions that can only apply to IPv4 traffic will generate warnings (icon) or errors (icon) in the field "Checking the policy" if IPv6 objects are included in the filter rules.

Standard rule including objects with different IP versions in the source and destination	[Rule X] Source and Destination objects do not use the same IP addressing version (IPv4/IPv6).
Authentication rule including IPv6 objects	[Rule X] Redirection to services will only be performed on IPv4 traffic.
Inspection SSL rule including IPv6 objects	[Rule X] The action "decrypt" will only apply to IPv4 traffic.
Explicit HTTP proxy rule including IPv6 objects	[Rule X] Cannot apply proxy or NAT on IPv6 traffic.
Rule with NAT on the destination including IPv6 objects	[Rule X] NAT on destination will only apply to IPv4 traffic.
Rule including IPv6 objects and using application inspections (Antivirus, Antispam, URL filtering, SMTP filtering, FTP filtering or SSL filtering)	[Rule X] Application inspections will only apply to IPv4 traffic.

LICENSE

The License screen consists of several sections:

- The **General** tab: manual or automatic installation of a license and display of main information.
- **Local license** tab (or in high availability, a serial number such as Local License SN210XX8E4545A5 to distinguish the active firewall from the passive firewall): details of all options in the license and their active value on the firewall.
- An additional **Remote firewall *remote_firewall_serial_no.* license** tab for the passive firewall in a high availability configuration.

Firewalls with several models on the same physical platform

For firewalls that have several models on the same physical platform (SN-XS-Series-170 / SNi10, SN-S-Series-220 / SN-S-Series-320, SN-M-Series-720 / SN-M-Series-920, SN-L-Series-2200 / SN-L-Series-3200 and SN-XL-Series-5200 / SN-XL-Series-6200 firewalls), models can be upgraded by installing a license and restarting the firewall.

For more information, refer to the product installation guide.

General tab

This tab will allow you to automatically or manually install a license.

There are 2 ways to install a license manually:

- By inserting the **License file** in the relevant field. Automatic configuration possible.
- By looking for a new license.

Buttons

- **Search for a new license**: This button is used for finding new licenses or for updating the date of the last check for a license.
  By clicking on this button, a request to search for licenses will be sent to the appliance. If a license is found, a notification will appear in the *General* tab and the user will then have access to the button Install the new license. Licenses are searched for manually. If you prefer an automatic license search, you will need to change the settings in the advanced properties section in this tab.
- **Install the new license**: If the firewall has found a license through the button **Search** for a **new license**, the button **Install the new license** will be enabled. By clicking on it, a download will be launched. Confirm or cancel the download.

Dates

- **Local firewall date**: this date ensures that the firewall's date is correct. Expiry dates are calculated based on this date.
- **Last check for license updates performed on**: date of the last time a request was made manually or automatically to search for licenses.

The Stormshield Network Firewall is sold by default with all features enabled. However, some features (URL filtering, high availability, among others) are optional and not enabled. Certain

options, such as updates, are valid for a limited period. If the expiry date has lapsed, some options will be disabled on the firewall.

Important information about the license

The license configuration window shows you the version of your firewall, information on the hardware and the various options with their expiry dates, if any.

Icons and colors will indicate if an option is approaching its expiry date or has expired.

Installing from a file

You can install your first license here if you do not have internet access or if you wish to manage licenses yourself.

If you choose to use new features or renew certain options, please contact your reseller. A new encrypted file will then be given to you through your private area on Stormshield Network's website.

License file	This field allows you to insert a license that you have retrieved earlier from Stormshield Network's website and activate the configuration on your firewall. The **Install** button validates the installation of the license file on the firewall. Information concerning your firewall will be modified and the new options will be enabled on the firewall.
Install the license on	This field appears only on the active firewall in a high availability configuration. In it, you can select the cluster member on which the license file has to be installed. The **Install** button validates the installation of the license file on the selected firewall. Information about this firewall will be modified and the new options will be enabled on the firewall.

REMARKS
The options that require rebooting the firewall are changes to encryption strength and the addition or removal of network interface cards.
In order to be accessible, these modules, even if they are physically installed, require the installation of the appropriate license following a reboot.

Advanced configuration

Here, you can define how frequently the firewall will look for updates as well as the type of installation (manual or automatic).

Look for license updates	Indicates how frequently searches will be conducted. If a license is found, a notification will appear in the information panel of the *General* tab, which may look like this: "! A new license is available for U30XXA32100950".

Install license after it has been downloaded	• If you select **always manual** (using the button **Install a new license**), the button **Install the new license** will appear whenever a license is suggested. The new license can therefore be compared against the current license in the *License details* tab. If the license is suitable, click on **Install the new license**. A notification will appear, informing you that the current license is up to date. • If you select **automatic when possible (no reboot necessary)**, the appliance will install the license. Do note that there are various notification messages: ○ *"License Update: a new license is available"* will appear when this is clearly the case. Every message is associated with an alarm (*68* in this case). ○ The following can also be seen: *69= "License Update:* Temporary license, registration is necessary" or *71*= "License Update: A new license has been installed" These messages can be seen in SNMP and syslog alarms. To enable the sending of these messages, go to **Notifications**, **Logs-Syslog** or **SNMP Agent**.

Local license tab

This tab displays the current valid license on the firewall to which you are connected (active firewall in a high availability configuration.). In this tab, you can also search for and install a new license file for the firewall.

Buttons

Search for a new license	This button is used for finding new licenses or for updating the date of the last check for a license. **NOTE** In this tab, the button allows searching for licenses for all firewalls in the high availability cluster.
Install the new license	If the firewall has found a license through the button **Search** for a **new license**, the button **Install the new license** will be enabled. By clicking on it, a download will be launched. Confirm or cancel the download. **NOTE** In this tab, the button allows installing the license for the firewall indicated.
Collapse all	This button allows collapsing all the features in the license.
Expand all	This button allows expanding all the features in the license.

Rule grid

Feature	Indicates the features and options of each feature found on the firewall. The features are: “Administration”, “Expiry date”, “Options”, “Global”, “Hardware”, “Limits”, “Network”, “Proxy”, “Services” and “VPN”.
In progress (current license)	Indicates, for each license installed, which options have been enabled for each feature, or the expiry status. A symbol indicates whether a feature is enabled, and another symbol shows that an option has been disabled. Symbols and colors show the difference between an option that is close to expiry (less than 90 days to the expiry date), an expired option and a valid option.
New license	This column appears only if a new license is available but has not yet been installed, and that a reboot would be necessary (in other words, this column will never appear if you have selected in the advanced properties of the *General* tab the option **Install license after it has been downloaded - automatic when possible (no reboot necessary)**. When a new license is available, this column will set out the new values in comparison with the values of the current license indicated in the column “In progress (current license)”. Symbols and colors indicate improvements or declines in value compared to the values of the current license. If the option has not changes, nothing will be indicated.
Manager	Administration possible via the web interface. (Default value: 1).
Monitor	Monitoring possible via Stormshield Network REAL-TIME MONITOR (Default value: 1).
Antispam DNS blacklists (RBL)	Deadline for updating DNSRBL spam databases
ClamAV antivirus	Deadline for updating ClamAV antivirus databases
Express Warranty	Deadline for the Express Warranty. This makes it possible to shorten the client’s waiting time when the product is being repaired.
Industrial	Deadline for the option that enables the analysis of industrial protocols.
License will be valid until	Expiry date of the license.
Contextual protection signatures	Deadline for updating contextual protection signatures (intrusion prevention engine).
Antispam: heuristic engine	Deadline for updating the spam filter heuristic engine.
Sandboxing Breach Fighter	Deadline for file analysis through sandboxing
Internal URL filtering engine (no database updates)	Deadline for updating Stormshield Network’s URL filter databases.
Extended Web Control URL databases	Deadline for updating Stormshield Network Extended Web Control URL filter databases.

Update	Deadline for updating the appliance.
Advanced antivirus	Deadline for updating advanced antivirus databases.
Vulnerability management	Deadline for updating SEISMO vulnerabilities.
Warranty	Deadline for the warranty.
Custom contextual protection signatures	Creates customized signatures for the intrusion prevention engine.
Express Warranty	Express warranty that allows limiting the client's waiting time during the repair of his product.
External directory (LDAP)	Enables or disables the use of an LDAP directory (Default value: 1*)
High availability	Allows defining an active and passive appliance in a high availability cluster. (Master/Slave/None).
Industrial	Enables or disables the analysis of industrial protocols.
PKI	Enables or disables the internal PKI. (Default value: 1)
Vulnerability management	Enables or disables SEISMO. (Default value: 0)
Comments	Comments.
ID	Unique identifier
Temporary	Temporary license (as long as the appliance has not been registered). Default value: 1 (factory settings), 0 once the product has been registered.
Version	Version of the license (checks the compatibility of the format for the license/version of the Firmware). The default value is 9.
Cryptographic card	Presence of an optional cryptographic card. (Default value: depends on the model).
External storage	Presence of an SD card for log storage
Network interfaces	Maximum number of physical interfaces. (Default value: depends on the model).
RAID	Allows channeling date from one hard disk to another when one of them fails.
Connections	Maximum number of connections passing through ASQ. (Default value: 0 (= unlimited)).
Network	Maximum number of networks managed by ASQ. (Default value: 0 (= unlimited)).
Users	Maximum number of users who can authenticate on the appliance. (Default value: 0 (= unlimited)).

Dialup High Availability	Enables or disables the possibility of using dialups to establish high availability links. (Default value: 1).
Interface routing	Allows routing by interface. This option is enabled by default.
Dialup load balancing	Enables or disables load-balancing on dialups. (Default value: 1).
QoS	Enables or disables QoS. (Default value: 1).
Antispam DNS blacklists (RBL)	Enables or disables spam filtering via DNSRBL in the proxy. (Default value: 1).
ClamAV antivirus	Enables or disables the ClamAV antivirus in the proxy. (Default value: 1).
FTP proxy	Enables or disables the FTP proxy. (Default value: 1**).
HTTP proxy	Enables or disables the http proxy (Default value: 1).
ICAP (URL)	Enables or disables the ICAP ReqMod. (Default value: 1).
ICAP (Virus)	Enables or disables the ICAP RespMod. (Default value: 1).
POP3 proxy	Enables or disables the POP3 proxy. (Default value: 1).
SMTP proxy	Enables or disables the SMTP proxy. (Default value: 1).
Sandboxing Breach Fighter	Enables or disables file analysis through proxy-based sandboxing.
Antispam: heuristic engine	Enables or disables the spam filter heuristic engine. (Default value: 0).
Internal URL filtering engine (no database updates)	
Extended Web Control URL databases	Enables or disables URL filtering via Stormshield Network Extended Web Control database in the proxy. (Default value: 0).
Advanced antivirus	Enables or disables the Advanced antivirus in the proxy. (Default value: 0).
Authentication	Enables or disables the user authentication interface.
DHCP	Enables or disables DHCP server/relay service (Default value: 1).
DNS	Enables or disables DNS cache service. (Default value: 1).
Dynamic DNS	Enables or disables the DynDNS client of the DNS update server.
Enrolment	Enables or disables enrolment. (Default value: 1).
Internal LDAP database	Enables or disables the internal LDAP database (Default value: 1).
NTP	Enables or disables NTP synchronization (Default value: 1).
Public directory (LDAP)	Enables or disables public access to the internal LDAP (Default value: 1*).
SNMP	Enables or disables the SNMP agent. (Default value: 1*).

Anonymous IPsec VPN tunnels	Enables or disables the possibility of setting up anonymous tunnels. (Default value: 1*).
PPTP	Enables or disables PPTP tunnels. (Default value: 1*).
SSL VPN	Enables or disables SSL VPN.
Strong Encryption	Enables or disables support for strong algorithms for the encryption of IPsec tunnels. (Default value: 1*).
Number of IPsec VPN tunnels	Maximum number of IPsec tunnels. (Default value: 0 (=unlimited)).

Remote firewall *remote_firewall_serial_no.* license tab

This tab appears only in high availability cluster configurations.

It has exactly the same characteristics as the Local firewall license tab, and makes it possible to search for and install new license files on the remote firewall.

LOGS - SYSLOG - IPFIX

The log configuration screen consists of 3 tabs:

- **Local storage**,
- **Syslog**,
- **IPFIX**.

Local storage tab

Log configuration makes it possible to allocate disk space for each log category on the firewall. In this menu, logging on the firewall can be enabled or disabled.

ON / OFF	Enables or disables logging on the firewall. Logging is disabled by default if the firewall does not have a storage device.

> **NOTE**
> When logging to a local device is disabled, a real-time logging mechanism takes over.
> These logs can then be accessed in **Monitoring** > **Logs - Audit logs** > **Real-time logs**.

Storage device

Storage device	Select the storage device on which logs will be saved: • Firewall's internal storage medium, • SD card for firewalls are equipped with an external storage medium. **NOTE** For more information, refer to the SNS Presentation and installation guide, under **Appendix B: log storage**.
Refresh	Refreshes the list of available storage media.
Format	Formats the selected storage medium.

> **NOTE**
> In a high availability configuration, actions relating to the SD card are only valid for the card inserted into the active firewall. To use an SD card on the passive firewall, you must first switch from passive to active mode in the **Maintenance** module.

Configuring the space reserved for logs

There are several categories under which the firewall logs events detected by log functions, including data relating to capture features.

All categories share the same storage space. You can enable or disable logging for a particular category and modify its disk space quota by assigning a percentage to it.

Rule grid

Enabled	Shows that logging is enabled for a particular log category. Double-click to change the status.
Category	Specifies the name of the log category or family.
%	Shows the percentage of disk space assigned to the log family. Double-click to edit. The total disk space reserved for all log categories is shown at the bottom of the grid: a warning message will appear if it exceeds 100%. However, changes are allowed. If a storage device is full, the most recent logs erase the oldest logs.
Size	Shows the disk space that is assigned to each log category on the storage device. This value varies according to the percentage assigned.

The **Enable all** or **Disable all** buttons make it possible to enable or disable logging in a single action for all log categories.

Confirm changes by clicking on **Apply**.
You must save your changes if the total disk space reserved exceeds 100%.

Log categories

Administration (serverd)	Events relating to the firewall administration server (serverd).
Authentication	Events relating to user authentication.
Network connections	Events relating to connections allowed through and to the firewall. The log is written when the connection ends.
System events	Events directly relating to the system: shutdown and startup of the firewall, system error, etc. Shutting down and starting log functions correspond to shutting down and starting the daemons that generate logs.
Alarms	Events relating to the application of intrusion prevention features.
HTTP proxy	Events relating to HTTP traffic.
Application connections (plugin)	Events relating to processes carried out by ASQ plugins.
SMTP proxy	Events relating to SMTP traffic.
Filter policy	Events relating to the application of filter functions.
IPsec VPN	Events relating to the setup of SAs.
SSL VPN	Events relating to setup of the SSL VPN.
POP3 proxy	Events relating to message sending.
Statistics	Events relating to real-time monitoring.
FTP proxy	Events relating to FTP traffic.
SSL proxy	Events relating to SSL traffic.
Sandboxing	Events relating to file sandboxing if the subscription for this option has been activated.

Network captures	Data obtained from network captures activated on the firewall.
Router statistics	Data obtained from statistics of routers and their gateways.
Dynamic multicast routing	Events relating to dynamic multicast routing.
Routing	Events relating to unicast routing (static routing and dynamic routing [BIRD]).
REST API	

Syslog tab

In the *Syslog* tab, up to four profiles can be configured to send logs to Syslog servers.

To increase the security of sent logs, Syslog servers must be configured with RGS-compliant algorithms.

Syslogs are text files in UTF-8 and follow the WELF standard. The WELF format is a sequence of elements, written in the form of field=value and separated by spaces. Values may be framed by double quotes.

A log corresponds to a line ending with a return carriage (CRLF).

Syslog profiles

Status	Enables or disables the syslog profile by double-clicking.
Name	Displays the name of the syslog profile.

Details

The configuration of the syslog profile selected in the grid on the left can be viewed or modified in this zone.

Name	Name assigned to the syslog profile.
Comments	Comments can be entered in this field.
Syslog server	Select or create a host object corresponding to the syslog server. Groups cannot be selected.
Protocol	Select the protocol used for sending logs to the server: • UDP (possible loss of messages - messages sent in plaintext), • TCP (reliable - messages sent in plaintext), • TLS (reliable - messages encrypted). **NOTE** TLS is recommended.
Port	Port used by syslog server.

Certification authority	This field will only be active when the protocol selected is TLS. Indicate the certification authority (CA) that signed the certificate that the firewall and server will present in order to authenticate mutually.
Server certificate	This field will only be active when the protocol selected is TLS. Select the certificate that the Syslog server will need to present in order to authenticate on the firewall. You cannot select a certificate with a TPM-protected private key.
Client certificate	This field will only be active when the protocol selected is TLS. Select the certificate that the firewall will need to present in order to authenticate on the Syslog server. The icon indicates certificates with a TPM-protected private key. For more information on the TPM, see the section Trusted Platform Module. Ensure that the syslog server has the selected client certificate. You can export the certificate as a P12 file in **Configuration** > **Objects** > **Certificates and PKI**.
Format	Choose the Syslog format to use: • LEGACY (format limited to 1024 character for each Syslog message), • LEGACY-LONG (no limit on message length), • RFC5424 (format compliant with RFC 5424).

Advanced properties

Backup server	This field will only be active when the protocol selected is TLS or TCP. Select or create a host object corresponding to the backup syslog server. Groups cannot be selected.
Backup port	This field will only be active when the protocol selected is TLS or TCP. Port used by the backup syslog server.
Category (facility)	Associates an application system with the logs sent to the syslog server.
Sekoia Intake Key	If you have a subscription allowing you to send data to sekoia.io servers, enter the authentication key provided by Sekoia. This key comprises 32 characters. Erase the key that was entered in this field, and confirm the configuration to disable this service. **NOTE** This field will only be shown when the syslog format RFC 5424 and TLS have been selected.

Logs enabled

In this table, the logs that need to be sent to the syslog server can be selected.

Status	Enables or disables sending the selected log file. Double-click on it to change its status.
Name	Type of logs to be sent (Alarm, Connection, Web, Filter…).

IPFIX tab

The IPFIX (IP Flow Information Export) protocol, derived from Netflow, is a network monitoring protocol that allows gathering information on IP traffic.

Such traffic consists of sending a template describing the type of information sent to the collector. For TCP-based IPFIX traffic, this template will only be sent once the connection is established. When the IPFIX traffic is based on UDP, the template will be sent regularly.

	This button makes it possible to enable or disable the sending of logs to an IPFIX collector.
IPFIX collector	Select or create a host object corresponding to the IPFIX collector. Groups cannot be selected.
Protocol	Select the protocol on which IPFIX traffic will be based (TCP or UDP).

Advanced properties

Port	Choose an object corresponding to the communication port between the firewall and the IPFIX collector. The default value suggested is **ipfix** (port 4739).
Backup IPFIX collector	This field will only be active when the protocol selected is TCP. In this case, a collector can be specified, to which IPFIX messages will be sent in the event the nominal collector is unavailable. 10 minutes after having switched its traffic to the backup collector, the firewall will attempt to contact the nominal collector again. In the event of a failure, the firewall will continue to send its traffic to the backup collector while regularly retrying to contact the nominal collector.
Backup port	This field will only be active when the protocol selected is TCP. This is the listening port of the backup IPFIX collector.

MAINTENANCE

In the **Maintenance** module, you can change settings and conduct the necessary checks to ensure that your appliance runs smoothly.

Through the interface, you can securely configure your firewall, and back up and update your system, as shown in the four following tabs:

- **System update**,
- **Backup**,
- **Restore**,
- **Configuration**.

System update tab

> **NOTE**
> In a high availability (HA) firewall cluster, the procedure is specific and must follow the steps described in the section Updating a cluster in the technical note *High availability on SNS*.

Available updates

If an update is available, it will appear under **Available updates**.

If the update server cannot be accessed, or if you wish to install another version, download it from your personal MyStormshield area by referring to the procedure Downloading the latest available version of a product.

Download this update	This link appears only when a new update is available. Clicking on the link downloads the update (*.maj* file).
Version release notes	This link appears only when a new update is available. Clicking on the link downloads the release notes that apply to the firmware version being suggested for download.
sha1	This link appears only when a new update is available. Clicking on the link displays the SHA1 fingerprint of the update file.
Check for new updates	The firewall will conduct a search for new system updates on *update* servers (**Objects > Network objects**) and will display them on the screen.

System update

Select the update	Click on ... and select the update to install.
Update the firewall	Apply the selected update to your firewall by clicking on this button. **NOTE** Updates to an earlier version are not supported, and may cause instability, requiring the product to be reset.

Advanced configuration

Action

Save the active partition on the backup partition before updating the firewall	If this option is selected, you will back up your system's main partition on the backup partition, in order to keep a record of it. The firewall will restart after the update is complete.
Upload the firmware update and install it	This option allows you to send the update file (.maj) and activate it.
Upload the firmware update only	This option allows you to send the update file (.maj) without activating it. The file can be activated later using the option below **Install the uploaded firmware**.
Install the uploaded firmware	If a file is located on the firewall, this option will allow you to activate it. The version indicated can be found in the field **Update present on the firewall**.

Current version of the system

This field shows the current software version of your product.

Update uploaded on this firewall

This field displays the update that you had selected earlier at the top of this screen.

Backup tab

Through this screen, you can create a manual backup or schedule an automatic backup of the firewall's configuration.

Configuration backup

Backup filename	The suggested name of the backup is **<firewall serial number>_day_month_year.na** by default. This name can be changed if necessary.
Download the configuration backup	Click on this button to save the backup. The file will be saved in *.na* format.

Advanced properties

Password/Confirm	Set a password to protect your backup. You are advised to protect the backup file with a strong password. Keep it in a safe place, as restorations will not be possible without this password, and the file can neither be modified nor reinitialized. Our technical support team will not be able to retrieve or reinitialize it for you.
Password strength	This progress bar indicates your password's level of security: "Very Weak", "Weak", "Medium", "Good" or "Excellent". You are strongly advised to use a combination of upper and lowercase letters, numbers as well as special characters.

TPM password	When the firewall has a TPM that has been initialized, the TPM password must be entered in order to back up the configuration. The backup will contain all private keys of certificates on the firewall, but the TPM-protected private keys that are included will be decrypted. For more information, see the section Trusted Platform Module.

Configuration automatic backup

Automatic configuration backups are made regularly and securely. Information regarding the latest backup is available in the firewall's **Dashboard**, in the **Services** widget.

> **NOTE**
> The firewall must be covered by a valid maintenance contract in order to be eligible for this service.

When the firewall has a TPM that has been initialized, the backup will contain all private keys of certificates on the firewall, and the TPM-protected private keys that are included will be encrypted. For more information, see the section Trusted Platform Module.

ON / OFF	Set the switch to ON to allow a backup of the firewall's configuration to be sent regularly.
Configuration	• **Cloud backup**: these backups are stored in the cloud service infrastructure (your MyStormshield area) using encrypted channels. • **Customized server**: these backups are stored on a custom server (HTTP/HTTPS local or outsourced), depending on the criteria defined below.
Save in the cloud	Click on this button to launch the backup and send it to the cloud (your MyStormshield area), or to your customized server, depending on the option chosen.

Advanced properties

Backup frequency	The automatic backup can be carried out every day, every week (7 days) or every month (30 days).
Password of the backup file	You are advised to protect the backup file with a strong password. Keep it in a safe place, as restorations will not be possible without this password, and the file can neither be modified nor reinitialized. Our technical support team will not be able to retrieve or reinitialize it for you.

Customized server

If you have selected a backup on a customized server, enter its configuration:

Server's URL	Location used for storing backups. This URL is set when the **Backup server**, **Server port**, **Communication protocol** and **Access path** fields have been entered.
Backup server	Selects a customized server. Ensure that the resolution of the selected server corresponds to the one expected.
Backup filename	Enter the name assigned to the backup file.

Server port	Server's listening port for receiving backups.
Communication protocol	Protocol used for sending backups between HTTP and HTTPS. For HTTPS, a certificate needs to be entered so that the firewall can confirm the identity of the server before sending it the backup.
Server certificate	If HTTPS has been chosen, import then select the server certificate in this field, so that the firewall can authenticate it.
Access path	Depending on the sending method selected above, the access path may be a folder (*/directory/*) for WebDAV methods (auth) or a script (*/upload.php*) for the POST method.
Send method	*Basic* and *Digest* modes (RFC 2617) allow the identification of the firewall on the server with the help of a login and password: • **auth basic**: this mode sends the encoded password but in plaintext. It is therefore recommended for use with HTTPS communications. • **auth digest**: this mode allows an identification but without sending the password in plaintext; this mode is more secure than the *basic* mode. It is recommended for use in HTTP communications. • **POST**: as identification via this method is not managed, you are advised to use it with HTTPS communications.
ID	If a sending method with identification is used (*auth basic* or *auth digest*), this user name will allow the server to authenticate the firewall.
Backup password	If a sending method with identification is used (*auth basic* or *auth digest*), this password will allow the server to authenticate the firewall.
POST - control name	If the POST method is used, this field will indicate the control name in the header of HTTP packets.

Restore tab

This window allows you to restore a backup that was made earlier.

Restoring a configuration

Select a backup to restore	In this field, select the *.na* backup file to restore. As a general rule, backups containing TPM-protected private keys of certificates can only be restored on the source firewall. For more information, see the section Trusted Platform Module.
Restore the configuration from the backup file	Click on this button to restore the firewall's configuration from the selected file. You may be asked to reboot your firewall depending on the restored backup. If a reboot is necessary, you will have the choice of rebooting immediately or later.

Advanced properties

Backup password	If you have protected the selected backup with a password, enter it in this field. Backups cannot be restored without this password.

Modules to be restored	Your firewall's configuration can be fully or partially restored. The **Restore all modules of the backup file** checkbox is selected by default. All the modules contained in the backup file can therefore be restored. If you wish to restore only some of the modules in the backup file, unselect **Restore all modules of the backup file**, then individually select the modules you wish to restore.

Restore automatic backup

Date of the latest backup	Date of the latest backup of your configuration, available on the local or external server.
Restore the configuration from the automatic backup	Click on this button to restore the firewall's configuration, using the file selected above. You may be asked to reboot your firewall depending on the restored backup. If a reboot is necessary, you will have the choice of rebooting immediately or later.

Advanced properties

Backup password	If you have protected the selected backup with a password, enter it in this field. Backups cannot be restored without this password.

Configuration tab

System disk

You are currently using this partition	Your firewall's system disk is divided into two partitions, which allow you to back up your data. This section indicates the partition on which the product started up.
Main partition	Version of the firmware installed on the main partition.
Backup partition	Version of the firmware installed on the backup partition.
Upon startup, use the	Choose the partition on which you wish to start the appliance: the main or backup partition. • **Main partition**: if this option is selected, your firewall will use this partition at startup. • **Backup partition**: represents the last partition that you backed up. If this option is selected, your firewall will use this partition at startup.
Back up the active partition	This button allows you to back up the active partition (the one indicated by **You are currently using this partition**) on the other partition.

Maintenance

Reboot the firewall	Click on this button to restart your firewall directly.
Shut down the firewall	Click on this button if you wish to shut down your firewall.

High availability

Make a firewall stay active	In the event both firewalls in your HA cluster are in an active state or start up at the same time, this option allows designating a member that will have priority in staying active. **NOTE** Before defining a remote firewall as the firewall with priority, check that your firewalls are synchronized. This is important as modifications made to the current configuration on the firewall would be lost during the switch.

System report (sysinfo)

Download the system report	This button allows you to obtain various types of information about your firewall in *sysinfo* format. Using this feature, you will be able to find out, for example, the model of the firewall, its serial number, its current status and the status of its memory, etc.

MONITORING

The **Monitoring** module offers data in real time and history graphs (if this option has been enabled in the **Report configuration** module) regarding:

- Hardware and high availability status,
- The use of the firewall's system resources,
- The level of use of network interfaces,
- The level of use of QoS queues,
- Hosts that have gone through the firewall,
- Users authenticated on the firewall,
- Connections made through the firewall,
- The status of routers, SD-WAN routers and network gateways defined on the firewall,
- The DHCP service,
- SSL VPN tunnels set up,
- IPsec VPN tunnels set up,
- The firewall's whitelist/blacklists.
- Captures of network traffic going through the firewall.

Such data is presented in the form of curves or tables. History curves offer four time scales: last hour, day, week or month. These time ranges are calculated in relation to the firewall's date and time settings.

Private data

For the purpose of compliance with the European GDPR (General Data Protection Regulation), personal data (user name, source IP address, source name, source MAC address) is no longer displayed in logs and reports and have been replaced with the term "Anonymized".

To view such data, the administrator must then enable the "Logs: full access" privilege by clicking on "**Logs: limited access**" (upper banner of the web administration interface), then by entering an authorization code obtained from the administrator's supervisor (see the section **Administrators** > **Ticket management**). This code is valid for a limited period defined at the moment of its creation.

To release this privilege, the administrator must click on "**Logs: full access**" in the upper banner of the web administration interface, then click on "**Release**" in the dialog box that appears.

After a privilege is obtained or released, data must be refreshed.

Please note that every time a "Logs: full access" privilege is obtained or released, it will generate an entry in logs.

NOTE
For SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SNi10 and SNi20 models, you can benefit from full functionality by using an external storage medium such as:

- SD card for SN160(W), SN210(W), SN310 and SNi20 models,
- MicroSD card for SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320 and SNi10 models.

The characteristics of these media are specified in the LOGS - AUDIT LOGS section of this guide.

The table

Search	This field allows looking for monitoring graphs or tables using keywords.

Tooltips

Scrolling the mouse over certain types of objects will display their properties in a tooltip. The advantage of this is that it reduces the number of columns to display in a table.

Whenever the administrator has full privileges to access all logs, the properties shown in the tooltip are the following:

Host or IP address

- Name of the host if it has been defined in the objects database,
- IP address of the host,
- Host's operating system (only the internal host),
- Number of vulnerabilities detected for the host,
- Host's reputation score (only the internal host),
- Country in which the host is located (only the external host),
- Number of packets sent,
- Number of packets received,
- Outgoing bandwidth used,
- Incoming bandwidth used,
- Firewall interface through which this host is seen,
- Host's MAC address (only the internal host),

Affected tables :

- Host monitoring: "Hosts" view, "Connections" view,
- User monitoring: "Users" view, "Connections" view,
- Connection monitoring.

Destination Port

- Name of the object corresponding to the port,
- Port number,
- Protocol,
- Comments defined in the port object.

Affected tables :

- Host monitoring: "Hosts" view, "Connections" view,
- User monitoring: "Connections" view,
- Connection monitoring.

User

- Description, if any,
- Connection ID,
- Domain (directory),

- E-mail address,
- Phone number,
- IP address of the connecting host and name of the corresponding host object if it has been defined in the objects database.
- Firewall interface through which this host is seen,
- Incoming bandwidth used,
- Outgoing bandwidth used.

Affected tables :

- User monitoring: "Users" view,
- Connection monitoring.

Interface

- Last name,
- Whether the interface is protected,
- Bridge to which the interface may be attached,
- Incoming bandwidth used,
- Outgoing bandwidth used.

Affected tables :

- Host monitoring: "Hosts" view,
- User monitoring: "Connections" view,
- Connection monitoring.

Hardware / High Availability

"Hardware" tab

This module presents various indicators on the operating status of the firewall or members of the cluster in the form of graphs or tables:

- CPU temperature curve,
- S.M.A.R.T. information and tests on disks,
- RAID status, if any,
- Power supply status,
- Fan status,
- 3G/4G modems connected to the firewall.

Interactive features

For the curve:

- Left-clicking on an indicator listed in the legend allows hiding/showing the corresponding data on the graph,
- Scrolling over a curve with a mouse will display the value of the indicator and corresponding time in a tooltip.

For the table of S.M.A.R.T. information :

- By scrolling over the reference of a disk with a mouse, details of S.M.A.R.T. tests conducted and their results will appear in a tooltip.

"Cluster details" tab

This tab is accessible only when high availability has been configured and enabled. It groups data on the status of high availability for each member of the cluster.

The **Local firewall** column sets out the value of an indicator for the firewall on which the administrator is connected. The **Remote firewall** column sets out the value of this indicator for the remote member of the cluster.

Indicators

Status	This field indicates whether the firewall concerned is active or passive.
Firmware version	Indicates the firmware version on each member of the cluster.
Forced status	The *Active* status is imposed on one of the members of the cluster when you select "This firewall (serial number)" or "The other firewall (serial number)" for the **Quality indicator** field (**System** > **High availability** > **Advanced properties** menu).
Quality indicator	Specifies the quality indicator calculated for high availability. In particular, this indicator takes into account the weight assigned to network interfaces when any of them accidentally become unavailable. A red or green LED will be seen next to the indicator.
Priority	Indicates the priority assigned to the firewall on which the administrator is connected. This priority may be defined in the menu: **High availability** > **Quality indicator** > **Active firewall if equal**. If one of the firewalls is selected, it will have a priority of 50 while the other member of the cluster will be assigned a priority of 0.
Configuration synchronization	Indicates whether the configurations of both members of the cluster are the same. Possible values: *Synchronized* or *Desynchronized*. A green or red LED accompanies this value.
HA link state	Displays the status of the main physical link between members of the cluster: • OK: the link is operational • KO: the link is not functioning (e.g., unplugged cable). • UNKNOWN: the status of the link could not be retrieved.
Backup HA link state	Displays the status of the backup physical link (secondary) between members of the cluster: • OK: a backup link has been defined and is operational. • KO: a backup link has been defined but is not functioning (e.g., unplugged cable). • UNKNOWN: the status of the link could not be retrieved. • N/A: no backup link has been defined in the HA configuration.

Advanced indicators

Retrieving HA data	Indicates, either with a green or red LED, whether the firewall has responded to the request enabling the retrieval of data regarding high availability.
Firewall model	Specifies the firewall model (SN200, SN6000, etc).
Supervisor	In a cluster, one of the firewalls assumes the role of supervisor in order to decide when to synchronize files, for example. This field indicates which of the two firewalls assumes this role.
Version number (data)	This version number is associated with data generated from the intrusion prevention engine and synchronized between both firewalls. It allows detecting incompatibilities when the cluster consists of firewalls in different versions.
Version number (connections)	This version number is associated with the protocol (and not data) used for the synchronization of data generated by the intrusion prevention engine.
Version number (status)	Version number of the algorithm used for determining the status (active/passive) of members of the cluster.
License	Specifies the type of license associated with HA (Master / Slave / None).
Currently connected on	Indicates the cluster member on which the administrator is connected.
Boot partition	Indicates which partition is used when the firewall starts up (main/backup).
Backup partition version	Specifies the firmware version installed on the backup partition.
Backup partition date	Indicates the last time the backup partition was updated.
Firewall last started on	Indicates the last time the firewall was started (format: YYYY-MM-DD HH:MM:SS).
Last synchronization	Indicates the last time the cluster was synchronized (format: YYYY-MM-DD HH:MM:SS).
Last status change	Indicates the last time the firewall's status (active/passive) was changed (format: YYYY-MM-DD HH:MM:SS).
HA service	This refers to the internal status of the HA management service on members of the cluster. The value of this field may be one of the following: • Starting: initial status of the service when the firewall has just restarted. • Waiting_peer: during restart, the firewall goes into passive mode and attempts to contact the other member of the cluster. • Synchronizing: when a firewall has restarted and managed to contact the other member of the cluster, the connection will start synchronizing. • Running: the firewall is active. • Ready: the firewall is passive and ready to switch to active if necessary. • Reboot: before restarting, the firewall informs the other member about it before switching to passive. The status of its service will then be shown as Reboot. • Down: before being shut down, the firewall informs the other member of the cluster about it. The status of its service will then be shown as Down.
HA link IP address	Firewall IP address presented by the interface dedicated to the main HA link.

HA link status changed	Indicates the last time the main HA link's status was changed (format: YYYY-MM-DD HH:MM:SS).
Backup HA link IP address	Firewall IP address presented by the interface dedicated to the backup HA link (N/A if no backup links have been defined in the cluster).
Backup HA link status changed	Indicates the last time the backup HA link's status was changed (format: YYYY-MM-DD HH:MM:SS).
No. of last SMC deployment	Indicates the revision number of the last configuration deployed via Stormshield Management Center (N/A if the firewalls are not managed by an SMC server).

System

"Real time" tab

In this module, various indicators show the firewall's operating status in the form of graphs or tables:

- CPU load (user area, disruptions and system).
- Amount of memory used by internal hosts, fragmented packets, ICMP state, TCP/UDP sessions, IPS data tracking, active services and network sockets.
- CPU consumption of each service enabled on the firewall.
- System information: system date and time, runtime since the last reboot, etc.
- Active Update: name, status (**Never used**/**Failed**/**Disabled**/**Manually updated**/**Updated**/**In progress**) and last update of the firewall's security database.
  An update of all configured modules can be launched so that they can be automatically refreshed (**Run all automatic updates again** button). On modules configured with manual updates (**Updated manually** indicated), this refers to the date of the last *.ssp* file imported.
- SSO agents: name and status (enabled/disabled) of the main agent and backup agent for each SSO Agent method configured (**Configuration** module > **User > Authentication**),
- NTP: server name, status, reason for any alarm raised, date of the firewall's last connection to the server and stratum level of the server in relation to the atomic clock for each configured NTP server (**Configuration** > **Configuration** > **General configuration** tab).
- Syslog servers: name, status (enabled/disabled) and protocol used for each syslog server configured (**Configuration > Notifications** > **Logs - Syslog - IPFIX** module).
- Radius: name, status, port of the main server and backup server (**Configuration** module > **Users > Authentication**).
- TS agents: name, number of users connected via the agent, status and time lapsed since the firewall's last connection to the agent for each TS agent configured (**Configuration > Users > Authentication** module).

Possible operations

Collapse all	Collapses all graphs on the page at once.
Expand all	Expands all graphs on the page at once.
Add a column	Increases the number of columns shown for curves and other information.
Remove a column	Reduces the number of columns shown for curves and other information.

Open monitor configuration	Redirects to the monitoring configuration module (refreshment intervals).

Interactive features

- Clicking on an indicator listed in the legend shows/hides the corresponding data on the graph,
- When you scroll over a curve, the value of the indicator and corresponding time appear in a tooltip.
- Buttons provide direct access to the configuration windows of certain modules.

"History" tab

This tab shows a history graph of the firewall's CPU consumption (user area, disruptions and system).

Possible operations

Time scale	In this field, the time scale can be selected: last hour, views by day, last 7 days and last 30 days. • The last hour is calculated from the minute before the current minute. • The view by day covers the whole day, except for the current day in which data runs up to the previous minute. • The last 7 and 30 days refer to the period that ended the day before at midnight. The button allows the displayed data to be refreshed.
Display the	In a view by day, this field offers a calendar allowing you to select the date.

Interactive features

- Clicking on an indicator listed in the legend shows/hides the corresponding data on the graph,
- When you scroll over a curve, the value of the indicator and corresponding time appear in a tooltip.
- Clicking on the button to the right of each graph will prepare graph data for printing. Comments can be added before you confirm printing (**Print** button).

Interfaces

"Real time" tab

This module presents two indicators in the form of graphs for each interface/aggregate selected in the **Configuration** > **Monitoring configuration** module:

- Bandwidth use (incoming throughput, outgoing throughput),
- Number of connections (TCP, UDP).

Possible operations

Collapse all	The button allows all graphs on the page to be collapsed at once.
Expand all	The button allows all graphs on the page to be expanded at once.
Add a column	This button allows you to increase the number of columns shown for curves and other information. Therefore, information will be grouped in the same column for each active interface.
Remove a column	This button allows you to reduce the number of columns shown for curves and other information.
Configure network interfaces	This link makes it possible to go directly to the network interface configuration module (**Configuration** > **Network** > **Interfaces**).
Open monitor configuration	This link makes it possible to go straight to the configuration module of the network interfaces to be monitored.

Interactive features

- Left-clicking on an indicator listed in the legend allows hiding/showing the corresponding data on the graph.
- When you scroll over a curve, the value of the indicator and corresponding time appear in a tooltip.

"History" tab

This tab sets out history graphs showing bandwidth use and the number of packets accepted/blocked for each monitored interface (exception VLANs).

Possible operations

Time scale	In this field, the time scale can be selected: last hour, views by day, last 7 days and last 30 days. • The last hour is calculated from the minute before the current minute. • The view by day covers the whole day, except for the current day in which data runs up to the previous minute. • The last 7 and 30 days refer to the period that ended the day before at midnight. The button allows the displayed data to be refreshed.
Display the	In a view by day, this field offers a calendar allowing you to select the date.
Collapse	The button allows all graphs on the page to be collapsed at once.
Expand	The button allows all graphs on the page to be expanded at once.
Add a column	This button allows you to increase the number of columns shown for curves and other information. Therefore, information will be grouped in the same column for each active interface.
Remove a column	This button allows you to reduce the number of columns shown for curves and other information.

Interactive features

- Clicking on an indicator listed in the legend shows/hides the corresponding data on the graph,
- When you scroll over a curve, the value of the indicator and corresponding time appear in a tooltip.
- Clicking on the button to the right of each graph will prepare graph data for printing. Comments can be added before you confirm printing (**Print** button).

QoS

"Real time" tab

For each QoS queue selected in the **Configuration** > **Monitoring configuration** module, this module shows bandwidth use (incoming, outgoing) in the form of graphs.

Possible operations

Collapse	The button allows all graphs on the page to be collapsed at once.
Expand	The button allows all graphs on the page to be expanded at once.
Add a column	This button makes it possible to increase the number of columns to be displayed for curves and other information. Therefore, information will be grouped in the same column for each active queue.
Remove a column	This button makes it possible to reduce the number of columns to be displayed for curves and other information.
Go to QoS configuration	This link makes it possible to go directly to the QoS configuration module (**Configuration** > **Security policy** > **Quality of Service**).
Go to monitoring configuration	This link allows going directly to the configuration module of QoS queues to be monitored.

Interactive features

- Clicking on an indicator listed in the legend allows hiding/showing the corresponding data on the graph,
- Scrolling over a curve with a mouse will display the value of the indicator and corresponding time in a tooltip.

“History” tab

This tab sets out history graphs showing bandwidth use for each monitored QoS queue.

Possible operations

Time scale	This field allows selecting the time scale: last hour, views by day, last 7 days and last 30 days. • The last hour is calculated from the minute before the current minute. • The view by day covers the whole day, except for the current day in which data run up to the previous minute. • The last 7 and 30 days refer to the period that has ended the day before at midnight. The button allows the displayed data to be refreshed.
Display the	In the case of a view by day, this field offers a calendar allowing you to select the date.
Collapse	The button allows all graphs on the page to be collapsed at once.
Expand	The button allows all graphs on the page to be expanded at once.
Add a column	This button makes it possible to increase the number of columns to be displayed for curves and other information. Therefore, information will be grouped in the same column for each active queue.
Remove a column	This button makes it possible to reduce the number of columns to be displayed for curves and other information.

Interactive features

- Clicking on an indicator listed in the legend allows hiding/showing the corresponding data on the graph,
- Scrolling over a curve with a mouse will display the value of the indicator and corresponding time in a tooltip.
- Clicking on the button to the right of each graph will prepare graph data for printing. Comments can be added before you confirm printing (**Print** button).

Hosts

"Real time" tab

Hosts

This grid shows all hosts detected by the firewall. Each line represents a host and lists the following data:

Name	Name of the sending host (if declared in objects) or IP address of the host (if not declared).
IP address	IP address of the host.
MAC address	MAC address of the host.
Interface	Interface to which the user belongs.

Reputation	Host's reputation score This column will only contain data when host reputation management has been enabled and the selected host is a monitored host.
Packets	Number of packets exchanged by the selected host.
Bytes in	Number of bytes that have passed through the firewall from the sending host ever since the firewall started running.
Bytes out	Number of bytes that have passed through the firewall towards the sending host ever since the firewall started running.
Incoming throughput	Actual throughput of traffic sent by the source host and passing through the firewall.
Outgoing throughput	Actual throughput of traffic sent to the destination host and passing through the firewall.
Protected	Indicates whether the interface on which the host was detected is a protected interface.
Continent	if the **See all hosts (show hosts behind unprotected interfaces)** checkbox has been selected in the filter, the source continent of the external host will be displayed.
Country	if the **See all hosts (show hosts behind unprotected interfaces)** checkbox has been selected in the filter, the source country of the external host will be displayed.
Reputation category	Indicates the external host's reputation category if it has been classified. **EXAMPLE** Spam, phishing, etc.

Right-click menu

Right-clicking on the name or IP address of a host opens the following pop-up menus:

- Search for this value in the **All logs** view,
- Check usage of this host,
- Show host details,
- Blacklist this object (for 1 minute, 5 minutes, 30 minutes or 3 hours),
- Copy the selected line to the clipboard,
- Copy the current cell to the clipboard,
- Add the host to the objects base and/or add it to a group,
- Show host's connections: displays monitoring of **Connections** by filtering this host,
- Show host reputation: displays the host's reputation history in a new window below the host grid.

Possible actions

Several search criteria can be combined. All of these criteria have to be met in order to be displayed, as the search criteria are cumulative.

This combination of search criteria can then be saved as a “filter”. Filters will then be saved in memory and can be reset in the **Preferences** module of the administration interface.

(Filter drop-down menu)	Select a filter to launch the corresponding search. The list will suggest filters that have been saved previously and predefined filters for certain views. Selecting the entry (New filter) allows the filter to be reinitialized by selecting the criteria selection.

Filter	Click on this button to:
	• Select filter criteria (**Search criterion**). For the "**hosts**" view, the criteria are the following:
	  • By address range or by IP address
	  • By interface
	  • If the reputation score is higher than the value specified with the cursor.
	  • if the **See all hosts (show hosts behind unprotected interfaces)** checkbox has been selected, all hosts detected will be displayed in the table.
	• Save as a customized filter the criteria defined in the Filter panel described in the next section (**Save current filter**). You can save a new filter using the button "Save as" based on an existing filter or a predefined filter offered in certain Views. Once a filter has been saved, it will be automatically offered in the list of filters.
	• **Delete current filter**.

Reset	This button cancels the action of the filter currently in use. If it is a saved customized filter, this action will not delete the filter.
Refresh	This button refreshes data shown on the screen.
Export results	This button makes it possible to download a file in CSV containing information from the table. Once a filter is applied, all results matching this filter will be exported.
Reset columns	This button makes it possible to reinitialize column width and display only columns suggested by default the first time the host monitoring window is opened.

"FILTER ON" panel

You can add a criterion by dragging and dropping the value from the results field into the panel.

	Indicates the date and time of the object's connection.
Connection	Connection ID
Parent connection	Some protocols may generate "child" connections (e.g. FTP) and in this case, this column will list the parent connection ID.
	Communication protocol used for the connection.
	User logged on to the host (if any).
	IP address of the host at the source of the connection
Source name	Name of the object (if any) corresponding to the source host.
	MAC address of the object at the source of the connection
	Number of the source port used for the connection
Source Port Name	Name of the object corresponding to the source port
	IP address of the host to which the connection was set up.

Destination Name	Name of the object (if any) to which the connection was set up.
	Number of the destination port used for the connection
Dest. Port Name	Name of the object corresponding to the destination port
	Name of the interface on the firewall on which the connection was set up.
	Name of the destination interface used by the connection on the firewall.
Average throughput	Average value of bandwidth used by the selected connection.
	Number of bytes sent during the connection.
	Number of bytes received during the connection.
	Connection time.
Last used	Time elapsed since the last packet exchange for this connection.
	ID assigned by the firewall to the router used by the connection
	Name of the router saved in the objects database and used by the connection
Rule type	Indicates whether it is a local, global or implicit rule.
	ID name of the rule that allowed the connection
	This parameter indicates the status of the configuration corresponding, for example, to its initiation, establishment or closure.
Queue name	Name of the QoS queue used by the connection.
Rule name	If a name has been given to the filter rule through which the connection passes, this name will appear in the column.
IPS profile	Displays the number of the inspection profile called up by the rule that filtered the connection.
Geolocation	Displays the flag corresponding to the destination country.
Reputation category	Indicates the external host's reputation category if it has been classified.
Argument	Additional information for certain protocols (e.g.: HTTP).
Operation	Additional information for certain protocols (e.g.: HTTP).
	Select a filter to launch the corresponding search. The list will suggest filters that have been saved previously and predefined filters for certain views. Selecting the entry (New filter) allows the filter to be reinitialized by selecting the criteria selection.
Filter	Click on this button to:
Reset	This button cancels the action of the filter currently in use. If it is a saved customized filter, this action will not delete the filter.
Refresh	This button refreshes data shown on the screen.
Export results	This button makes it possible to download a file in CSV containing information from the table. Once a filter is applied, all results matching this filter will be exported.

Reset columns	This button makes it possible to display only columns suggested by default when the host monitoring window is opened.
	Vulnerability ID
	Indicates the name of the vulnerability.
	Number of hosts affected.
	Indicates the severity level of the vulnerability. There are 4 levels of severity: "**Low**", "**Moderate**", "**High**", "**Critical**".
	Access may be local or remote (via the network). It allows exploiting the vulnerability.
	Indicates whether a workaround exists.
	The alarm level associated with the discovery of this vulnerability.
	The network port on which the host is vulnerable (e.g. 80 for a vulnerable web server).
	Indicates the name of the vulnerable program (e.g.: lighthttpd_1.4.28)
	Indicates the date on which the vulnerability was detected on the host
	Additional information about the vulnerability.
	Name of the application.
	Application family (e.g. Web client).
	Full name of the application including its version number.
	Indicates the port and protocol used by the service (e.g. 80/tcp).
	Indicates the name of the service (e.g.: lighthttpd)
Service	Indicates the name of the service including its version number (e.g. lighthhtpd_1.4.28).
	Additional information about the service detected.
Family	Service family (e.g. Web server).
	Unique identifier of the software program or operating system detected.
	Name of the software program or operating system detected.
	Family to which the detected software belongs (e.g. Operating System).
	The alarm level associated with the discovery of this program.
	Date and time the program or operating system was detected.
	Name and version of the software program or operating system detected (e.g. Microsoft_Windows_Seven_SP1).

"Reputation history" view

This view shows in the form of graphs how the reputation of the selected host has evolved and the impact of the various criteria involved in the calculation of this score (alarms, sandboxing results and antivirus analysis).

Possible operations

Time scale	In this field, the time scale can be selected: last hour, views by day, last 7 days and last 30 days. • The last hour is calculated from the minute before the current minute. • The view by day covers the whole day, except for the current day in which data runs up to the previous minute. • The last 7 and 30 days refer to the period that ended the day before at midnight. The button allows the displayed data to be refreshed.
Display the	In a view by day, this field offers a calendar allowing you to select the date.

Interactive features

Left-clicking on an indicator listed in the legend allows hiding/showing the corresponding data on the graph.

When you scroll over a curve, the value of the indicator and corresponding time appear in a tooltip.

"History" tab

This view shows in the form of graphs how the reputations of hosts have evolved (average reputation and maximum reputation).

Possible operations

Time scale	In this field, the time scale can be selected: last hour, views by day, last 7 days and last 30 days. • The last hour is calculated from the minute before the current minute. • The view by day covers the whole day, except for the current day in which data runs up to the previous minute. • The last 7 and 30 days refer to the period that ended the day before at midnight. The button allows the displayed data to be refreshed.
Display the	In a view by day, this field offers a calendar allowing you to select the date.
Print	This button makes it possible to display the curve in fullscreen mode in order to print it (**Print** button).

Interactive features

Left-clicking on an indicator listed in the legend allows hiding/showing the corresponding data on the graph.

When you scroll over a curve, the value of the indicator and corresponding time appear in a tooltip.

Web Services

"Connection per Web Services" tab

This curve shows how the number of connections made has changed over the past 10 minutes for each of the web services used in the firewall's configuration.

"Incoming per web services" tab

This curve shows how the incoming bandwidth consumed by each of the web services used in the firewall's configuration has changed over the past 10 minutes.

"Outgoing per web services" tab

This curve shows how the outgoing bandwidth consumed by each of the web services used in the firewall's configuration has changed over the past 10 minutes.

Users

"Real time" tab

Users

Name	User name
IP address	IP address of the host to which the user has logged on.
Directory	Name of the LDAP directory used for authenticating the user.
Group	List of groups to which the user belongs.
Timeout	Remaining authentication time for the user's session
Auth. method	Method used for authenticating the user (e.g. SSL)
Client workstation verification (ZTNA)	This column indicates the status of the client with regard to the host/user verification policy. There are four possible values: • **N/A**: when the authentication method is not related to the SSL VPN, • **Disabled**: when no client workstation/user verification policy has been defined, • **Not verified**: this value is shown when permissive mode has been enabled (**Allow tunnels to be set up for clients that are not compatible with ZTNA** checkbox selected), and the SSL VPN client used for setting up the tunnel is not compatible with the client workstation/user verification (third-party SSL VPN client or incompatible SN SSL VPN Client version), • **Compliant**: when the client workstation complies with the criteria defined in the client workstation/user verification policy.
One-time password	A green check means that the user used a TOTP.

Multi-user	Indicates whether the host to which the user has logged on is a multi-user host (e.g. a TSE server).
Administrator	Specifies whether the user has administration privileges on the firewall.
Sponsor	Whenever the user logs on via the Sponsorship method, this column will indicate the name of the person who had validated the connection request.
SSL VPN	A green check in this checkbox means that the user is allowed to set up SSL VPN tunnels using the SN SSL VPN Client.
IPsec VPN	A green check in this checkbox means that the user is allowed to set up one or several IPsec VPN tunnels.

Right-click menu

Right-clicking on the name of the user opens the following pop-up menus:

- Search for this value in logs,
- Log off this user,
- Show host details,
- Copy the selected line to the clipboard,
- Copy the current cell to the clipboard,
- Show user's connections: displays monitoring of **Connections** by filtering this user.

Possible actions

Several search criteria can be combined. All of these criteria have to be met in order to be displayed, as the search criteria are cumulative.

This combination of search criteria can then be saved as a “filter”. Filters will then be saved in memory and can be reset in the **Preferences** module of the administration interface.

(Filter drop-down menu)	Select a filter to launch the corresponding search. The list will suggest filters that have been saved previously and predefined filters for certain views. Selecting the entry (New filter) allows the filter to be reinitialized by selecting the criteria selection.

Filter	Click on this button to:
	• Select filter criteria (**Search criterion**). For the "**users**" view, the criteria are the following:
	  • By address range or IP address (grayed out if a user has been selected in the "users" view).
	  • By directory (allows refining the filter when several LDAP directories have been defined on the firewall)
	  • By authentication method
	  • By one-time password by selecting **TOTP code used** or **No TOTP code used**.
	• Save as a customized filter the criteria defined in the Filter panel described in the next section (**Save current filter**). You can save a new filter using the button "Save as" based on an existing filter or a predefined filter offered in certain Views. Once a filter has been saved, it will be automatically offered in the list of filters.
	• **Delete current filter**.

Reset	This button cancels the action of the filter currently in use. If it is a saved customized filter, this action will not delete the filter.

Refresh	This button refreshes data shown on the screen.
Export results	This button makes it possible to download a file in CSV containing information from the table. Once a filter is applied, all results matching this filter will be exported.
Configure authentication	This link makes it possible to go directly to the authentication parameters (**Configuration** > **Users** > **Authentication** module).
Reset columns	This button makes it possible to reinitialize column width and display only columns suggested by default the first time the host monitoring window is opened.

Date	Indicates the date and time of the object's connection.
Connection	Connection ID
Parent connection	Some protocols may generate "child" connections (e.g. FTP) and in this case, this column will list the parent connection ID.
Protocol	Communication protocol used for the connection.
User	User logged on to the host (if any).
Source	IP address of the host at the source of the connection
Source name	Name of the object (if any) corresponding to the source host.
Source MAC address	MAC address of the object at the source of the connection
Source port	Number of the source port used for the connection
Source Port Name	Name of the object corresponding to the source port
Destination	IP address of the host to which the connection was set up.
Destination Name	Name of the object (if any) to which the connection was set up.
Destination Port	Number of the destination port used for the connection.
Dest. Port Name	Name of the object corresponding to the destination port
Source interf.	Name of the interface on the firewall on which the connection was set up.
Dest. interf.	Name of the destination interface used by the connection on the firewall.
Average throughput	Average value of bandwidth used by the selected connection.
Sent	Number of bytes sent during the connection.
Received	Number of bytes received during the connection.
Duration	Connection time.
Last used	Time elapsed since the last packet exchange for this connection.
Router	ID assigned by the firewall to the router used by the connection
Router name	Name of the router saved in the objects database used by the connection
Rule type	Indicates whether it is a local, global or implicit rule.
Rule	ID name of the rule that allowed the connection

Status	This parameter indicates the status of the configuration corresponding, for example, to its initiation, establishment or closure.
Queue name	Name of the QoS queue used by the connection.
Rule name	If a name has been given to the filter rule through which the connection passes, this name will appear in the column.
IPS profile	Displays the number of the inspection profile called up by the rule that filtered the connection.
Geolocation	Displays the flag corresponding to the destination country.
Reputation category	Indicates the external host's reputation category if it has been classified.
Argument	Additional information for certain protocols (e.g.: HTTP).
Operation	Additional information for certain protocols (e.g.: HTTP).
(Filter drop-down menu)	Select a filter to launch the corresponding search. The list will suggest filters that have been saved previously and predefined filters for certain views. Selecting the entry (**New filter**) allows the filter to be reinitialized by selecting the criteria selection.
Filter	Click on this button to:
Reset	This button cancels the action of the filter currently in use. If it is a saved customized filter, this action will not delete the filter.
Refresh	This button refreshes data shown on the screen.
Export results	This button makes it possible to download a file in CSV containing information from the table. Once a filter is applied, all results matching this filter will be exported.
Reset columns	This button makes it possible to display only columns suggested by default when the host monitoring window is opened.

"FILTER" panel

You can add a criterion by dragging and dropping the value from the results field into the panel.

Product name	Name of the application.
Family	Application family (e.g. Web client).
Details	Full name of the application including its version number.
Port	Indicates the port and protocol used by the service (e.g. 80/tcp).
Service name	Indicates the name of the service (e.g.: lighthttpd)
Service	Indicates the name of the service including its version number (e.g. lighthhtpd_ 1.4.28).
Details	Additional information about the service detected.
Family	Service family (e.g. Web server).

ID	Unique identifier of the software program or operating system detected.
Name	Name of the software program or operating system detected.
Family	Family to which the detected software belongs (e.g. Operating System).
Level	The alarm level associated with the discovery of this program.
Assigned	Date and time the program or operating system was detected.
Details	Name and version of the software program or operating system detected (e.g. Microsoft_Windows_Seven_SP1).

"History" tab

In this tab, you will see history graphs showing the various authentication methods by type:

- Total,
- Captive portal,
- Console,
- IPsec,
- SSL VPN,
- TOTP,
- Web administration interface.

Possible operations

Time scale	In this field, the time scale can be selected: last hour, views by day, last 7 days and last 30 days. • The last hour is calculated from the minute before the current minute. • The view by day covers the whole day, except for the current day in which data runs up to the previous minute. • The last 7 and 30 days refer to the period that ended the day before at midnight. The button allows the displayed data to be refreshed.
Display the	In a view by day, this field offers a calendar allowing you to select the date.

Interactive features

- Clicking on an indicator listed in the legend shows/hides the corresponding data on the graph,
- When you scroll over a curve, the value of the indicator and corresponding time appear in a tooltip.
- Clicking on the button to the right of each graph will prepare graph data for printing. Comments can be added before you confirm printing (**Print** button).

Connections

"Real time" table

This view shows all connections detected by the firewall. Every row represents a connection. The "**Connections**" view displays the following data:

Date	Indicates the date and time of the object's connection.
Connection	Connection ID
Parent connection	Some protocols may generate "child" connections (e.g. FTP) and in this case, this column will list the parent connection ID.
Protocol	Communication protocol used for the connection.
Ethernet protocol	When the communication protocol is part of the following list: • PROFINET-RT, • IEC61850-GOOSE, • IEC61850-SV.
User	User logged on to the host (if any).
Source	IP address of the host at the source of the connection
Source name	Name of the object (if any) corresponding to the source host.
Source IP address (multi-homing)	IP address presented by the host initiating an SCTP connection. Reminder: an appliance that communicates in SCTP may have several IP addresses (*multi-homing*).
Source MAC address	MAC address of the object at the source of the connection
Source port	Number of the source port used for the connection
Source Port Name	Name of the object corresponding to the source port
Destination	IP address of the host to which the connection was set up.
Destination Name	Name of the object (if any) to which the connection was set up.
Destination MAC address	MAC address of the host to which the connection was set up.
Destination IP address (multi-homing)	IP address of the destination host of an SCTP connection. Reminder: an appliance that communicates in SCTP may have several IP addresses (*multi-homing*).
Destination Port	Number of the destination port used for the connection.
Dest. Port Name	Name of the object corresponding to the destination port
Source interf.	Name of the interface on the firewall on which the connection was set up.
Dest. interf.	Name of the destination interface used by the connection on the firewall.
Average throughput	Average value of bandwidth used by the selected connection.
Sent	Number of bytes sent during the connection.

Received	Number of bytes received during the connection.
Duration	Connection time.
Last used	Time elapsed since the last packet exchange for this connection.
Router ID	ID assigned by the firewall to the router used in the connection.
Gateway name	Name of the gateway (making up the router whose ID is specified in the previous column) that the connection uses.
Status of the gateway	Current status of the gateway used for the connection.
Rule type	Indicates whether it is a local, global or implicit rule.
Rule	ID name of the rule that allowed the connection.
Status	This parameter indicates the status of the configuration corresponding, for example, to its initiation, establishment or closure.
Queue name	Name of the QoS queue used by the connection.
Rule name	If a name has been given to the filter rule through which the connection passes, this name will appear in the column.
IPS profile	Displays the number of the inspection profile called up by the rule that filtered the connection.
Geolocation	Displays the flag corresponding to the destination country.
Reputation category	Indicates the external host's reputation category if it has been classified. **EXAMPLE** Spam, phishing, etc.
Argument	Additional information for certain protocols (e.g., HTTP).
Operation	Additional information for certain protocols (e.g., HTTP).

Right-click menu

Right-clicking on the name or IP address of a source or destination host opens the following pop-up menus:

- Search for this value in logs,
- Show host details,
- Reset the reputation score,
- Add the host to the objects base and/or add it to a group.

Right-clicking on the name of the user opens the following pop-up menus:

- Search for this value in logs,
- Log off this user,
- Show host details

Right-clicking on the name of the source or destination opens the following pop-up menus:

- Search for this value in the "All logs" view,
- Show host details,

- Reset this object's reputation score,
- Blacklist this object (for 1 minute, 5 minutes, 30 minutes or 3 hours),
- Add the host to the objects base and/or add it to a group.
- Go to the corresponding security rule

Right-clicking on the name of the source or destination opens the following pop-up menus:

- Go to the corresponding security rule,
- Add the service to the objects base and/or add it to a group.

Right-clicking on the other columns will open the following pop-up menu:

- Go to the corresponding security rule

Possible actions

Several search criteria can be combined. All of these criteria have to be met in order to be displayed, as the search criteria are cumulative.

This combination of search criteria can then be saved as a "filter". Filters will then be saved in memory and can be reset in the **Preferences** module of the administration interface.

(Filter drop-down menu)	Select a filter to launch the corresponding search. The list will suggest filters that have been saved previously and predefined filters for certain views. Selecting the entry (New filter) allows the filter to be reinitialized by selecting the criteria selection.

Filter	Click on this button to:
	• Select filter criteria (**Search criterion**). For the "**connections**" view, the criteria are the following:
	  • By address range, by IP address or by source host.
	  • By interface
	  • By gateway name.
	  • By gateway status.
	  • By source interface
	  • By destination interface
	  • By destination port
	  • By protocol
	  • By user (grayed out if a host has been selected in the "hosts" view).
	  • For a value of exchanged data higher than the value specified with the cursor.
	  • According to the last use of the connection (only saved connections with a last used value lower than the specified value will be displayed).
	  • By rule name
	  • By IPS profile.
	  • By geographic source or destination.
	  • If only the **Display all TCP/UDP connections (shut down, reset connections, etc.)** checkbox is selected, the filter will display all connections regardless of their state as well as the associations in use.
	  • If only the **Display all SCTP associations (reset, currently in use, shutting down and shut down)** checkbox is selected, the filter will display all SCTP associations regardless of their state as well as the connections in use.
	  • Whenever both the **Display all TCP/UDP connections (shut down, reset connections, etc.)** and **Display all SCTP associations (reset, currently in use, shutting down and shut down)** checkboxes are selected, the filter will display all of the firewall's known connections and associations regardless of their state.
	  • If neither the **Display all TCP/UDP connections (shut down, reset connections, etc.)** nor **Display all SCTP associations (reset, currently in use, shutting down and shut down)** checkbox is selected, the filter will display only connections and associations in use.
	• Save as a customized filter the criteria defined in the Filter panel described in the next section (**Save current filter**). You can save a new filter using the button "Save as" based on an existing filter or a predefined filter offered in certain Views. Once a filter has been saved, it will be automatically offered in the list of filters.
	• **Delete current filter**.

Reset	This button cancels the action of the filter currently in use. If it is a saved customized filter, this action will not delete the filter.
Refresh	This button refreshes data shown on the screen.
Export results	This button makes it possible to download a file in CSV containing information from the table. Once a filter is applied, all results matching this filter will be exported.
Reset columns	This button makes it possible to reinitialize column width and display only columns suggested by default the first time the host monitoring window is opened.

"FILTER ON" panel

You can add a criterion by dragging and dropping the value from the results field into the panel.

SD-WAN

"Real time" tab

This grid shows the list of routers used in the firewall's configuration: router objects, default gateway and routers configured in filter rules (PBR: Policy Based Routing) and return routes.

Possible actions

- The **Search** field makes it possible to filter the grid by the name of a router or a gateway. When filtering is applied to the name of a gateway, the router that uses it will appear in the grid.
- The **Collapse** button makes it possible to hide all the gateways that make up the router objects used in the configuration, and show only information regarding these routers.
- The **Expand** button makes it possible to show all the gateways that make up the router objects and all the information relating to routers and gateways.
- The **Refresh** button allows refreshing the display of data in the table.
- The **Export results** button allows downloading a file in CSV format containing all of this information.
- The **Configure routing** link makes it possible to go directly to routing configuration (**Configuration** > **Network** > **Routing** module).
- The **Reset columns** button makes it possible to reinitialize column width and display only columns suggested by default the first time the host monitoring window is opened.

Rule grid

The **Real time** grid displays the following data:

Routers/Gateways	Applies to all routers and gateways. Name of the router or a gateway that makes up a router.
Type	Applies only to gateways. Indicates the type of route in which a gateway is used. The possible values are: • **Policy-based routing**, • **Default route**.

Status	Applies to all routers and gateways. The status of a router is determined by the status of its gateways. The possible values for a main gateway are: • **Active**: gateway in optimal condition and in use, • **Active**: main gateway in a degraded condition and in use, • **Unreachable**: main gateway not responding to pings, • **Not monitored**: no pings have yet been sent for this gateway. The possible values for a backup gateway are: • **Standby**: the backup gateway is in an optimal or a degraded condition, • **Unreachable**: the backup gateway is not responding to pings, • **Not monitored**: no pings have yet been sent for this gateway. The possible values for a router are: • **Functional**: all its gateways are in an **Active** state. • **Functional**: ○ At least one of its gateways is in an **Active** state and all the others are on **Standby**, ○ At least one of its gateways is in an **Active** state and all the others in any other state, ○ All its gateways are in an **Active** state or on **Standby**, ○ At least one of its gateways is on **Standby.** • **Standby**: all other combinations of statuses of gateways that make up the router.
IP version	Applies only to gateways. Version of the IP protocol used in the gateway. The possible values are: • (IPv)**4**, • (IPv)**6**.
IP address	Applies only to gateways. IP address of the gateway (does not exist for a router).
SD-WAN SLA	Applies only to routers. Indicates whether an SLA has been set for the router. The possible values are: • **Enabled**, • **Disabled**.
Detection method	Applies only to routers. Shows the type of pinging to determine the status of a router. The possible values are: • **ICMP**, • **TCP Probe** (***protocol*** *used*).
Main/backup	Applies only to gateways. Indicates whether the gateway is defined as the main gateway or backup gateway in the router.

Last checked	Applies only to gateways. Date and time the gateway was last pinged.
Latency (ms)	Applies to all routers and gateways. For routers: indicates the threshold configured in the object. For gateways, indicates the latency measured during the last ping.
Jitter (ms)	Applies to all routers and gateways. For routers: indicates the threshold configured in the object. For gateways, indicates the jitter measured over a moving period of 10 minutes.
Packet loss	Applies to all routers and gateways. For routers: indicates the threshold configured in the object. For gateways, indicates the packet loss rate measured for a gateway over a moving period of 10 minutes.
Unavailability rate	Applies to all routers and gateways. For routers: indicates the threshold configured in the object. For gateways, indicates the percentage of time spent in an inactive or unreachable status over a moving period of 10 minutes.
SLA status	Applies to all routers and gateways. Indicates whether the router's gateways complied with the defined SD-WAN SLA (when it is enabled in the router object definition). The SLA status of a router is determined by the SLA status of its gateways. The possible values for a gateway are: • Good: the gateway meets all the SLA thresholds defined, • Degraded: the gateway does not meet at least one of the SLA thresholds defined, • Unreachable: the gateway is not responding to pings (ICMP or TCP Probe depending on the detection method chosen). • **Not monitored**: no pings have yet been sent for this gateway. **NOTE** When you scroll over the SLA status of a gateway, a window will show the values of the various metrics measured and defined thresholds. These values are color-coded, making it possible to identify the metrics behind the status of the gateway. The possible values for a router are: • Good: all its gateways have a **Good** SLA status. • Degraded: at least one of its gateways has a **Degraded** SLA status, regardless of the SLA status and its other gateways. • Unreachable: all the gateways on the router have an **Unreachable** SLA status. • **Not monitored**: no pings have yet been sent over the gateways of this router.
Last status change	Applies only to gateways. Time of the last status change and time lapsed since the gateway's status was last changed.
Available since	Applies to all routers and gateways. Time lapsed since the gateway's or router's availability was last changed.

Router ID	Applies only to gateways. Unique gateway ID.
Fairness	Applies only to gateways. Percentage of the gateway used in the router object when load balancing is set.

"Real time chart" tab

No curves are displayed by default the first time the **History** tab is accessed. Select a gateway from the **Select a gateway** drop-down list to display its charts.

Two charts appear for the selected gateway:

- Latency measured for last 10 minutes,
- Status over the same period.

"History" tab

No curves are displayed by default the first time the **History** tab is accessed.

1. **Select a router** from the drop-down list.
   The first router (in alphabetical order) in this router will then be selected automatically and curves relating to this gateway's metrics will be displayed.
2. If you wish to display curves from another gateway, or display the curves from another gateway in addition to the one selected by default, use the **Select a gateway (max. 10)** drop-down list.
   A maximum of 10 gateways can be selected at the same time.

Three graphs appear for each gateway selected:

- Jitter and latency,
- Packet loss rate and unavailability rate,
- Status balancing for the gateway: percentage of time spent in each possible status (Functional, Degraded and Unreachable).

Dynamic multicast routing

Depending on its position in the multicast infrastructure, the firewall may be identified as a:

- *First Hop Router* (FHR): the firewall is connected to a multicast source and sends its multicast traffic to the RP (PIM-SM) or to the destination (PIM-SSM).
- *Middle Hop Router* (MHR): the firewall acts as an intermediary and forwards multicast traffic.
- *Last Hop Router* (LHR): the firewall is connected to multicast receivers and sends subscription/unsubscription requests from these receivers to the RP.

The information shown in the grids described below vary according to the position of the firewall in a given multicast traffic stream.

The firewall may also be required to play specific roles in the multicast infrastructure:

- *Rendez-vous Point* (RP): the RP is contacted to set up the route up to the multicast source (*upstream*), then to transfer received transfer to receivers (*downstream*).
- *BootStrap router*) (BSR): the BSR is elected out of the pool of BSR candidates. Once it is elected, it will gather candidacies for the role of RP, then shares the table of multicast group/RP associations with other routers.

For more information on these roles and election mechanisms, refer to the configuration module in Dynamic multicast routing.

Possible actions

- : click on this button to refresh the data displayed in the dynamic multicast routing monitoring grids.
- : click on this button to change the frequency (in seconds) with which data displayed in the dynamic multicast routing monitoring grids is refreshed. The default value is 30 days.
- : click on this button to collapse all the monitoring grids shown on the screen.
- : click on this button to expand all the monitoring grids shown on the screen.
- : click on this button to directly access the dynamic multicast routing configuration module (**Configuration** > **Network** > **Multicast routing**).

Grids

Multicast routes

This grid shows the multicast routing table that the firewall has learned. The firewall does not necessarily use all routes listed in this grid.

Source	This field indicates the IP address or host object that represents the address of the source of the multicast traffic for the route shown. The value of this source is specified when the firewall meets one of the following conditions: • It is the FHR from the source, • It has been elected as RP (PIM-SM), • It is placed on the route of the *Shortest Path Tree* (*SPT*) when this route is set up. The *any* value appears when the firewall meets one of the following conditions: • It is the RP for the multicast group, and it is informed of subscription requests, • It is the LHR of a receiver (PIM-SM), • It is placed on the route between the LHR and RP.
Group	Indicates the IP address or host object that represents the IP address of the multicast group to which the route applies.
RP address	PIM-SM protocol : Specifies the IP address or host object that represents the IP address of the RP that manages this multicast route. This name is shown in bold when the monitored router itself has been elected as the RP of the selected multicast route. PIM-SSM protocol : No address is entered because the RP role does not exist in this protocol.

Flags	There are several possible values: • SG: when the source has been identified for the multicast route, • CACHE: when the route has been enabled on the monitored firewall, • SPT (only in PIM-SM): ○ When the firewall is the RP, this flag then indicates that the SPT is available, ○ When the firewall is positioned as the LHR: this flag indicates that the traffic passes through the SPT, • WC-RPT: when the firewall is positioned on the route of the LHR (inclusive) on the way to the RP (inclusive), • ASSERTED: when the firewall gains the *PIM assert* mechanism, which makes it possible to eliminate traffic duplicates over a shared segment. Do note that these various values can be combined with one another.
Details	By scrolling over this section, you will see the ongoing timeouts for the mechanisms that run in the PIM SM protocol. The timeouts shown (route expiry [*expiry timer*], end of a traffic transmission when there are no more declared receivers [*register suppression*], etc.) depend on the firewall's position in the multicast infrastructure (first hop, middle hop or last hop), and on its role(s) (RP and/or BSR). RFC 4601 sets out details of these timeouts.

Click on the "+" in a multicast route to obtain further details:

Interface	This column lists the interfaces that are part of the selected multicast route.
Incoming(IIF)	For a given multicast route, the interface that has a check is the interface through which multicast traffic arrives on the firewall.
Outgoing interface list (OIL)	• Joined: a check indicates that this interface has been used for a multicast subscription request. • Pruned: a check indicates that this interface has been used for a multicast unsubscription request. • Leaf: a check indicates that this interface has been directly connected to a receiver. • Asserted: a check indicates that this interface was used in the *PIM assert* mechanism. • Outgoing: a check indicates that this interface has been used to forward multicast traffic.

IGMP group members

> **NOTE**
> Information appears in this grid only when the firewall is positioned as the last hop router in a multicast traffic stream.

By clicking on the title of a column, information in the grid can be sorted by the value in question.

Click on the "+" in a multicast group to obtain the list of receivers that make up the group.

Group	Address or host object that represents the IP address of the group for which the IGMP request was initiated.
Source	Address or host object that represents the IP address of the source of the multicast traffic for the group in question.
Receiver	Address or host object that represents the IP address of the IGMP request initiator.
Interface	Shows the interface through which the firewall received the IGMP request.
Timeout	When this value is reached, this means that the receiver in question no longer listens on the IGMP traffic.

Interfaces/Neighbors

This grid lists all the firewall interfaces that participate in multicast routing, as well as the neighbors of these interfaces. A neighbor is another network device (e.g., router or firewall) that uses the PIM protocol, and which is directly connected to the listed interface.

Some of the information is available only for interfaces, while other information is available for interfaces and their neighbors.

Interface/Neighbor	Shown only for the interface. Name of the firewall interface that participates in multicast routing. The number of neighbors that this interface has is shown in brackets. Click on the interface's "+" symbol to see details about its neighbors.
Status	Shown only for the interface. Indicates whether interface is enabled.
Group	Shown only for the interface. Number of distinct multicast groups contacted by receivers that are connected to the interface.
Address	Shown for the interface and its neighbors. Address or host object that represents the IP address of the interface or of its neighbor.
DR priority	Shown for the interface and its neighbors. Indicates the priority assigned to the interface or to its neighbor as part of the DR election.
DR	Shown for the interface and its neighbors. Indicates whether the interface or its neighbor has been elected as the DR. When the check is followed by an asterisk, this means that it is an interface on the monitored router that was elected as the DR.
IGMP requester	Shown for the interface and its neighbors. A check indicates that the interface or its neighbor acts as the IGMP requester, which has to contact receivers to find out whether they are still listening on certain multicast traffic streams.
Since	Indicates the time lapsed since the discovery of the neighbor.
Expires in	Remaining time before the neighbor disappears, if it has not sent any HELLO messages,

Rendez-vous Points (RP)/Candidates (C-RP)

> **NOTE**
> Data is shown in this grid only when the PIM SM protocol is used (the concept of RPs does not exist in the PIM SSM protocol).

Multicast group	Indicates the address or host/network object that represents the IP address of the multicast group managed by the RP. When the associated RP is a dynamic RP, the number of RP election candidates is indicated in brackets.
RP > C-RP address	On a main line, this field indicates the address or host object that represents the IP address of the designated RP (static RP) or elected RP (dynamic RP) for the multicast group shown. On a dynamic RP, clicking on the "+" displays the list of RP election candidates for the multicast group in question.
Type	Indicates whether it is a static or dynamic (elected) RP.
Priority	Displays the priority assigned to the RP or candidate RP.
Hold-time	Interval between two candidate RP advertisements to the BSR.
Expires in	Expiry period of the candidature if the candidate no longer sends any advertisements to the BSR.

Neighboring bootstrap routers (BSR)/candidates (C-BSR)

> **NOTE**
> Data is shown in this grid only when the PIM SM protocol is used, as the concept of BSRs does not exist in the PIM SSM protocol.

BSR/C-BSR address	References the address of the host object that represents the IP address of the BSR as well as the candidates (C-BSR) advertised by the firewall's neighbors.
Priority	Shows the priority assigned to the C-BSR in the election.
Hash mask length	Shows the size (number of significant bits) used to balance multicast groups among DRs when there is an overlap. The mask is set to 30 by default.
Expires in	This is the remaining time until the next election when the BSR is lost. This value is shown only for the elected BSR.

DHCP

"Real time" table

This table shows the list of all the hosts that have obtained an IP address through the firewall's DHCP server. For each host, the "**DHCP monitoring**" view displays the following data:

IP address	Indicates the IP address assigned to the host. This address comes from one of the address ranges declared in the **Network** > **DHCP** module.
Status	Indicates that the IP address referenced in the table is used (active) or free in the DHCP range.
Lease begins	Indicates the date and time at which the DHCP server assigned an address to the host. This is displayed in YYYY-MM-DD HH:MM:SS.
Lease ends	Indicates the date and time at which the IP address assigned by the firewall's DHCP server will be available again if the host does not send any new requests to renew the lease. The lease duration can be customized in the **Network > DHCP > Advanced properties > Assigned lease time** module. This is displayed in YYYY-MM-DD HH:MM:SS.
MAC address	Indicates the MAC address of the network card bearing the IP address assigned by the firewall's DHCP server.
Host name	Indicates the name of the host to which the IP address was assigned.

Right-click menu

Right-clicking on the name or IP address of a source or destination host opens the following pop-up menus:

- Search for this value in the "All logs" view,
- Check this host,
- Show host details,
- Reset the reputation score,
- Blacklist this object (for 1 minute, 5 minutes, 30 minutes or 3 hours),
- Add the host to the objects base and/or add it to a group.

Possible actions

Refresh	This button refreshes data shown on the screen.
Export results	This button makes it possible to download a file in CSV containing information from the table.
Configure the DHCP service	This link makes it possible to go directly to the configuration of the DHCP service (**Configuration** > **Network** > **DHCP** module).
Reset columns	This button makes it possible to display only columns suggested by default when the host monitoring window is opened.

SSL VPN tunnels

"Real time" grid

This table displays all the hosts connected to the firewall through an SSL VPN tunnel. For each host, the "**SSL VPN tunnel monitoring**" view displays the following data:

User	Connection ID used in setting up the referenced SSL VPN tunnel.

Directory	Directory in which the connected user is defined.
VPN client IP address	IP address assigned to the client workstation to set up the SSL VPN tunnel (this address belongs to the network defined in the **VPN** > **SSL VPN** module > **Network assigned to clients (TCP)** or **Network assigned to clients (UDP)** field.
Client version	This column indicates the SN SSL VPN Client version that was used to set up the tunnel shown. The value indicated for a third-party or incompatible SN SSL VPN client is N/A.
Client workstation verification (ZTNA)	This column indicates the status of the client with regard to the host/user verification policy. There are three possible values: • **Disabled**: when no client workstation/user verification policy has been defined, • **Not verified**: this value is shown when permissive mode has been enabled (**Allow tunnels to be set up for clients that are not compatible with ZTNA** checkbox selected), and the SSL VPN client used for setting up the tunnel is not compatible with the client workstation/user verification (third-party SSL VPN client or incompatible SN SSL VPN Client version), • **Compliant**: when the client workstation complies with the criteria defined in the client workstation/user verification policy.
Real IP address	IP address assigned to the local network of the connected client workstation.
Received	Number of bytes received by the SSL VPN server (firewall) in the tunnel in question.
Sent	Number of bytes sent by the SSL VPN server. (firewall) in the tunnel in question.
Duration	Time lapsed since the tunnel was set up. This value is expressed in hh:mm:ss.
Port	Port used by the client to set up the tunnel.

Right-click menu

Right-clicking on the name of the user opens the following pop-up menus:

- Search for this value in logs,
- Log off this user.

Right-clicking on the IP address of the VPN client or on the real IP address of a host opens the following pop-up menus:

- Search for this value in the "All logs" view,
- Show host details,
- Reset this object's reputation score,
- Blacklist this object (for 1 minute, 5 minutes, 30 minutes or 3 hours).

"Information" grid

This table lists the number of tunnels that have been set up:

- Total number of tunnels (UDP + TCP)
- Number of UDP tunnels
- Number of TCP tunnels

A warning message will appear whenever the number of tunnels set up starts to reach the maximum number of simultaneous tunnels allowed (information available in the SSL VPN module).

Possible actions

Reset this tunnel	This button offers the possibility of forcing the renegotiation of the selected tunnel. The remote client will then be logged off and logged back on automatically.
Refresh	This button refreshes data shown on the screen.
Export results	This button makes it possible to download a file in CSV containing information from the table.
Configure the SSL VPN service	This link makes it possible to go directly to the configuration of the SSL VPN service (**Configuration** > **VPN** > **SSL VPN** module).
Reset columns	This button makes it possible to display only columns suggested by default when the tunnel monitoring window is opened.

IPsec VPN tunnels

This module allows you to view tunnels in active IPsec policies on the firewall (tunnels that have been defined using the native IPsec interface or virtual IPsec interfaces).

Possible actions

Refresh	This button allows data displayed in the table to be refreshed.
Configure the IPsec VPN service	This link makes it possible to go directly to the configuration of the IPsec VPN service (**Configuration** > **VPN** > **IPsec VPN** module).

"Policies" grid

Data shown in the “Policies" table is classified by policy type:

- Site-to-site tunnels,
- Mobile tunnels,
- Exception policies (bypass).

The following information is given:

Type	This is the type of IPsec policy: site-to-site tunnels, mobile tunnels and exception policies (bypass).
Status	A green LED with an “OK” caption, or red LED with a “KO” option, indicates the status of the tunnels in the policy concerned.
Rule name	Name given to the IPsec rule (rule editing window > **General settings** > **Advanced properties** > **Name**).
Source	Name of the object corresponding to the local network
Source address	Host network that initiated the traffic going through the selected IPsec tunnel (traffic endpoint).

Mask	Network mask associated with the source address.
Local gateway	Name of the object corresponding to the local IPsec gateway (local tunnel endpoint).
Local gateway IP address	IP address that the local firewall presents to set up the tunnel.
Local ID	Local ID (optional) specified when the peer was created. If nothing was specified, this refers to the IP address of the local gateway.
Remote gateway	Name of the object corresponding to the remote IPsec gateway (remote tunnel endpoint).
Remote gateway IP address	IP address that the remote firewall presents to set up the tunnel with the local firewall.
Peer	Name of the peer that was used to set up the tunnel.
Peer ID	ID (optional) assigned to the peer. If nothing was specified, this refers to the IP address of the remote gateway.
Remote traffic endpoint	Name of the object corresponding to network of the remote host with which traffic is exchanged in the tunnel.
Remote address	Network of remote hosts that communicate through the selected tunnel (traffic endpoint).
Remote network mask	Network mask associated with the remote address.
Policy	Type of IPsec policy. This field contains two possible values:: • *tunnel*, • *pass*.
Encapsulation	Protocol used to encapsulate data in the tunnel.
IKE version	Version (1 or 2) of the IKE protocol that was used to set up the tunnel.
Lifetime	Maximum lifetime of the tunnel before keys are renegotiated.
PPK protection	Indicates whether the **PPK required** option has been selected for this peer. The possible values shown are: • Mandatory (option selected), • Not required (option not selected).

Right-click menu

Right-clicking on the fields **Type**, **Status**, **Rule name**, **Source network mask**, **Local ID**, **Peer**, **Peer ID**, **Remote network mask**, **Policy type**, **Encapsulation**, **IKE version** or **Lifetime** opens the following right-click menus:

- Go to the logs of this IPsec policy,
- Copy the selected line to the clipboard,
- Go to the configuration of this IPsec policy,
- Go to this peer's configuration.

Right-clicking on the fields **Local gateway, IP address of the local gateway**, **Remote gateway** or **IP address of the remote gateway** opens the following right-click menus:

- Search for this value in the "All logs" view,
- Show host details,
- Blacklist this object (for 1 minute, 5 minutes, 30 minutes or 3 hours),
- Go to the logs of this IPsec policy,
- Copy the selected line to the clipboard,
- Go to the configuration of this IPsec policy,
- Go to this peer's configuration.

Right-clicking on the fields **Source, Source address**, **Remote traffic endpoint** or **Remote address** opens the following right-click menus:

- Search for this value in the "All logs" view,
- Show host details,
- Blacklist this object (for 1 minute, 5 minutes, 30 minutes or 3 hours),
- Go to the logs of this IPsec policy,
- Copy the selected line to the clipboard,
- Add the host to the objects base and/or add it to a group,
- Go to the configuration of this IPsec policy,
- Go to this peer's configuration.

Additional information about a tunnel

Selecting the line of a tunnel displays additional details in the following tables:

- IKE Security Associations (SA),
- IPsec Security Associations (SA).

"IKE Security Associations (SA)" table

Rule name	Name (optional) given to the IPsec VPN rule that corresponds to the tunnel. Reminder: this name makes it possible to search for events relating to the tunnel in IPsec logs.
IKE	Indicates the version of the IKE protocol for the tunnel in question.
Local gateway	Name of the object corresponding to the local gateway (local tunnel endpoint).
Local gateway address	IP address that the local gateway presents to set up the IPsec tunnel in question.
Remote gateway	Name of the object corresponding to the remote gateway (remote tunnel endpoint).
Remote gateway address	IP address that the remote gateway presents to set up the IPsec tunnel in question.
Status	Indicates the state of the IKE SA, e.g., *established*.
Role	Role of the local gateway in setting up the tunnel (*initiator* or *responder*).
Initiator cookie	Temporary identity marker of the initiator of the negotiation. Example: "0xae34785945ae3cbf".

Receiving cookie	Temporary identity marker of the peer of the negotiation. Example: "0x56201508549a6526".
Local ID	Local ID (optional) specified when the peer was created. If nothing was specified, this refers to the IP address of the local gateway.
Peer ID	ID (optional) assigned to the peer. If nothing was specified, this refers to the IP address of the remote gateway.
NAT-T	Indicates whether NAT-T (NAT Traversal - passing the IPsec protocol through a network that performs dynamic address translation) is enabled for this tunnel.
Authentication	Authentication algorithm used for the IKE phase of the tunnel.
Encryption	Encryption algorithm used for the IKE phase of the tunnel.
PRF	PseudoRandom Function negotiated and used for key derivation.
DH	Diffie-Hellman profile used for the tunnel.
Lifetime	Lifetime of the IKE SA (Security Association) lapsed for the tunnel in question.

"IPsec Security Associations (SA)" grid

Status	Indicates the state of the IPsec SA, e.g., *installed/rekeying*.
Local gateway	Name of the object corresponding to the local gateway (local tunnel endpoint).
Remote gateway	Name of the object corresponding to the remote gateway (remote tunnel endpoint).
Bytes in	Amount of data (in bytes) that passed through the tunnel to the local traffic endpoint.
Bytes out	Amount of data (in bytes) that passed through the tunnel to the remote traffic endpoint.
Encryption	Encryption algorithm used for the IPsec phase of the tunnel.
Authentication	Authentication algorithm used for the IPsec phase of the tunnel.
Lifetime lapsed	Lifetime of the IPsec SA lapsed for the tunnel in question.
ESN	Indicates whether the ESN (Extended Sequence Number) option is enabled. This option is only available for IKEv2.
UDP encapsulation	Indicates whether UDP encapsulation of ESP packets is enabled. This encapsulation is automatically forced when DR mode is enabled (**Configuration** > **System** > **Configuration** > **General configuration** tab > **Enable "ANSSI Diffusion Restreinte (DR)" mode**). On firewalls that are not configured in DR mode, this option can be enabled with the token `natt=<auto|force>` in CLI/serverd commands `CONFIG.IPSEC.PEER.NEW` and `CONFIG.IPSEC.PEER.UPDATE`. For more details on these commands, refer to the CLI SERVERD Commands Reference Guide.

Black list / white list

"Real time" table

Black list

This view shows the list of quarantined hosts. Hosts can be quarantined from:

- The pop-up menu available in certain log and monitoring modules,
- The alarm configuration module.

Possible operations:

Delete black list	This button makes it possible to delete the selected blacklist entry from the table.

The "**Black list**" view displays the following data:

Host / Address range	References the blacklisted (quarantined) IP address, name (if the host has been declared in the objects base) or IP address range.
Destination blocked	Indicates the destination (host, network, sub-network, address range) to which traffic from the quarantined host is blocked.
Expiry date	Indicates the date on which the host or address range in question will be released from quarantine.

White list

This view shows the list of hosts allowed to pass through the firewall without any action on its part (no filtering, no IPS analysis). Hosts can only be whitelisted from the command line and the aim of this feature is to not block hosts in production as part of an in-depth analysis of undesirable behavior on the firewall. The "**White list**" view displays the following data:

Host / Address range	References the whitelisted IP address, name (if the host has been declared in the objects base) or IP address range.
Destination blocked	Indicates the destination (host, network, sub-network, address range) to which traffic from the whitelisted host is blocked.
Expiry date	Indicates the date on which the host or address range in question will be released from the whitelist.

Network captures

The network capture tool is based on the tcpdump command line packet analyzer. This module consists of two grids:

- **Captures in progress**: makes it possible to launch network captures, list the ones in progress, stop them and copy their TCPDump filters,
- **Completed captures**: makes it possible to list past captures, download their PCAP files and metadata, delete them and copy their TCPDump filters,

> **NOTE**
> This module can be accessed only if the firewall is equipped with a storage medium on which

captures can be saved (e.g., internal storage or SD card). In addition, administrators must hold write permissions and the **Full access to logs (private data)** privilege or a temporary ticket to access personal data.

Information in local storage

Network captures are stored in the firewall's local storage within the quota of disk space allocated to network captures. If no quota has been allocated or enabled, the module cannot be used and a warning message will appear with two buttons:

- **Configure the allocated disk space**: opens the Logs - Syslog - IPFIX module in which a disk space quota can be allocated to network captures,
- **Reload module**: reloads the module after allocating or enabling the disk space allocated to network captures.

Interactive features

The operations listed in the taskbar of both grids can be performed by right-clicking in the relevant grid. For some actions, a line in the grid must be selected beforehand.

Captures in progress

Possible operations

Refresh list of captures	Refreshes the list of captures in progress and information about them.
Creating a capture	Creates a new capture. The procedure is explained in the following section.
Stop capture	Stops a capture in progress. Select the relevant capture beforehand.
Restart capture	Makes it possible to replay a capture by pre-entering its parameters in the window to create a new capture. Select the relevant capture beforehand.
Copy filter	Copy the capture's TCPDump filter. Select the relevant capture beforehand. This filter can later be used to create a new capture.

Creating a capture

You can launch up to five simultaneous captures but only one at a time per interface. Do note that this may affect the firewall's performance when network captures are in progress. If the disk space used by the captures reaches or exceeds 95%, new captures can no longer be launched. When this threshold is reached, all captures in progress will automatically stop.

To start a capture, click **Create a capture** and choose from:

- **TCPDump filter**: makes it possible to create a capture by manually entering the filter. You must know the format of the TCPDump filters or already have the filter.
- **Filter creation wizard**: creates a capture via a wizard to build a TCPDump filter step by step.

Once the creation window is open, enter the following information:

Interface	Select the interface on which network traffic will be captured. Do note that loopback interfaces cannot be selected for a network capture, to avoid capturing decrypted SSL proxy traffic.

Max. duration (sec)	Specify the maximum duration of the packet capture. This value cannot exceed 172800 seconds, i.e., 48 hours. The capture will automatically stop once the maximum duration is reached, unless another parameter stops the capture before that.
Max. no. of packets	Specify the maximum number of packets that can be captured. This value must not exceed 2147483647. The capture will automatically stop once this number is reached, unless another parameter stops the capture before that.
Packet size limit	You can set a limit for the size of captured packets. Packets that exceed this size will be truncated. A value of 0 makes it possible to capture full packets. This value must not exceed 262144.

TCPDump filter	**If you have selected TCPDump filter**, only the **TCPDump filter** field appears. Enter the filter in the field.
	
	If you have selected Filter creation wizard, several fields will appear. Fill in only the fields needed for your capture.
	• **Transport protocols**: enter the transport protocols (TCP, UDP, ICMP, etc.) involved in the capture.
	• **Network protocols**: enter the network protocols (IP, IP6, ARP, etc.) involved in the capture.
	• **Bimap**: this checkbox is selected by default and makes it possible to to apply the same **Host, MAC address** and **Port** values in the source and destination. Unselect this checkbox to access the **Source** and **Destination** tabs.
	  ◦ **Hosts**: enter the IP addresses of the hosts involved in the capture.
	  ◦ **MAC addresses**: enter the MAC addresses involved in the capture.
	  ◦ **Ports**: enter the ports involved in the capture.
	
	NOTE
	Use the **Equal to** or **Different from** attribute according to what you wish to capture. Click on the icon next to the text zone to change the attribute.

Once you have entered the information, click on **Start** to launch the capture. While it is running, you can quit the **Network captures** module and come back to it later.

NOTE
In high availability (HA) configurations, network captures can only be stopped from the firewall that launched the captures. During the switch from the active firewall to the passive firewall, captures in progress will continue to run until they automatically stop when the **Max. duration (sec) value** is reached.

The table

Interface	Interface on which the capture is currently running.
TCPDump filter	Capture's TCPDump filter.
Max. capture duration	Maximum duration of the packet capture.
Packet size limit	Packet size limit set for the capture.

Number of packets	Number of packets currently captured. The value of this column is not refreshed in real time. Use the **Refresh list of captures** button to refresh the information in the grid.
Max. no. of packets	Maximum number of packets that can be captured.

Completed captures

Possible operations

Refresh list of captures	Refreshes the list of completed captures.
Select all	Selects all the captures in the grid.
Delete	Deletes the selected captures.
Download the PCAP file	Downloads the PCAP file of a capture. Select the relevant capture beforehand, then click on the link to download the file. Multiple PCAP files cannot be downloaded at once in the interface. PCAP files are named according to the format: *serial_ifname_timestamp.pcap*. They are saved on the firewall in the */log/capture* folder.
Download capture metadata	Downloads a capture's metadata. Select the relevant capture beforehand, then click on the link to download the file. The metadata of several captures cannot be downloaded at once in the interface. The files containing the metadata are named according to the format: *serial_ifname_timestamp.txt*. They are saved on the firewall in the */log/capture* folder.
Replay capture	Makes it possible to replay a capture by pre-entering its parameters in the window to create a new capture. Select the relevant capture beforehand.
Copy filter	Copy the capture's TCPDump filter. Select the relevant capture beforehand. This filter can later be used to create a new capture.

> **NOTE**
> In high availability (HA) configurations, files from a network capture can be downloaded or deleted only from the firewall that launched the capture.

The table

Name	Name of the capture's PCAP file.
Interface	Interface on which the packets were captured.
TCPDump filter	Capture's TCPDump filter.
Packet size limit	Packet size limit set for the capture. This column is hidden by default.
Capture size	Size of the capture's PCAP file.
Capture duration	Duration of the packet capture. This duration can either be lower than the **Max. capture duration** if the **Max. no. of packets** is reached earlier, or if the capture was manually stopped.

Max. capture duration	Maximum duration set for the capture.
Start of capture	Date and time the capture started. This column is hidden by default.
End of capture	Date and time capture ended. This column is hidden by default.
Number of packets	Number of packets captured. This number can either be lower than the **Max. no. of packets** if the **Max. capture duration** is reached earlier, or if the capture was manually stopped.
Packets rejected by the kernel	Number of packets that the kernel rejected during the capture. The kernel rejects packets when it is unable to capture all of them, for example when it receives too many packets to process.
Packets rejected by the interface	Number of packets that the interface or its driver rejected during the capture. This column is hidden by default.
Max. no. of packets	Maximum number of packets that could be captured.

NETWORK/TIME OBJECTS

This module groups network objects and time objects. It is divided into two sections:

- The action bar at the top, allowing you to sort and handle objects.
- Two columns dedicated to objects: one column listing them by category, the other displaying their properties.

> **NOTE**
> The creation of objects does not allow declaring an object in Global mode, unless the option "Display global policies (Filter, NAT, IPsec VPN and Objects)" has been enabled in the **Preferences** module.

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

Possible actions

Search	If you are looking for a particular object, enter its name. The search field allows you to list all the network objects with properties that match the keyword(s) or letter(s) entered. **EXAMPLE** If you type the letter "a" in the search bar, the list below it will display all objects containing an "a" in their names or descriptions. You can also refine the search by using the "filter" that lists the various types of objects (see the section on the "Filter" button hereafter). **NOTE** The cross icon in the search field allows you to delete the entry and list all objects by the current filter. **NOTE** When you go to the *Objects* tab in the menu directory on the left, the focus will be on the search field.
Add	When you click on this button, a dialog box will appear, in which you can create an object; indicate its type and other related information in the relevant fields. **REMARK** The object can be defined as a global object when it is created if you select the option "This object is global" in the dialog box. It will then appear when you select the "All objects" or "Network" filter (see below) and will be represented by the following icon .
Delete	Select the object to remove from the list and click on **Delete**.

Check usage	If you click on this button after having selected an event, the results will appear in the module directory.
Export	By clicking on this button (represented by the icon), a window will show the link to download the objects database in CSV format. Click on this link to save the exportable file on your computer.
Import	By clicking on this button (represented by the icon), a window will allow you to select an objects database in the form of a CSV file so that you can import it into the firewall. The fields found in each row in a CSV file are described in the section Structure of an objects database in CSV format. A gauge will show the progress of the database being transferred to the firewall. **NOTE** Objects already found on the firewall will be replaced with the corresponding transferred objects.
Collapse all	This button collapses the object tree.
Expand all	This button expands the object tree.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of network objects:

- **Remove** (selected object),
- **Check usage** (of the selected object).

Filter

This button allows you to select which object types to display. A drop-down menu offers the following choices:

All objects	Represented by the icon , this option makes it possible to display all types of network objects in the list of objects on the left.
Host	Represented by the icon , this option makes it possible to display only host objects in the column on the left.
DNS name (FQDN)	Represented by the icon , this option makes it possible to display only DNS name (FQDN) objects in the column on the left.
Network	Represented by the icon , this option makes it possible to display only network objects.
Address range	Represented by the icon , this option makes it possible to display only IP address and MAC address ranges.

Router	Represented by the icon , this option makes it possible to display only router objects.
Group	Represented by the icon , this option makes it possible to display only network groups.
IP protocol	Represented by the icon , this option makes it possible to display only IP protocols.
Port – port range	Represented by the icon , this option makes it possible to display ports and port ranges.
Port group	Represented by the icon , this option makes it possible to display only port groups.
Time object	Represented by the icon , this option makes it possible to display only time objects.
Region group	Represented by the icon , this option makes it possible to display only geographic groups.

The various types of objects

This section describes the various types of objects that can be defined on the firewall.

Host

Select a host to view or edit its properties. Each host has a name, an IP address and a DNS resolution ("Automatic" or "None (static IP)") by default.

Name of the object	Name given to the object during its creation. This field can be modified, and to save changes, you need to click on **Apply** and **Save**. The icon to the right of the checkbox allows the object's IP address to be obtained, which can be seen in the "IP address" field. To obtain it, the object's full URL must be entered.
IPv4 address	IP address of the selected host.
DNS resolution	The DNS (Domain Name System) resolution matches IP addresses with a domain name. Two choices are possible: • **None (static IP)**: The selected object has a fixed IP address that will be used every time. • **Automatic**: If this option is selected, the firewall will submit DNS requests every 5 minutes in order to determine the IP address of the selected object.

MAC address	Media Access Control address. This address corresponds to the physical address of a network interface or of a network card, allowing the identification of a host on a local network. **EXAMPLE** 5E:FF:56:A2:AF:15.
Comments	Description of the selected host.

DNS name (FQDN)

DNS name objects are dynamic objects that represent DNS (FQDN) names that can be resolved on several IP addresses. These objects can either be defined in IPv4 or IPv6 and can only be used as the source or destination of a filter rule. They cannot be included in groups.

Select a DNS name to view or edit its properties.

Name of the object	Name given to the object during its creation. This field can be modified, and to save changes, you need to click on **Apply** and **Save**.
Default IP address	IP address of the selected object.
Comments	Description of the selected DNS name.

Network

Select a network to view or edit its properties. Each network has a name, IP address and network mask. These objects can either be defined in IPv4 or IPv6.

Name of the object	Name given to the object during its creation. This field can be modified, and to save changes, you need to click on **Apply** and **Save**.
IP address	IP address of the selected network. The address is followed by a "/" and the associated network mask.
Comments	Description of the selected network.

Address range

Select an address range to view or edit its properties.

Object name	Name given to the object when it was created. This field can be edited, and to save changes, click on **Apply** and **Save**.

IPv4 addresses

Start	First IP address of the range.
End	Last IP address of the range.

MAC addresses

Object name	Name given to the object when it was created. This field can be edited, and to save changes, click on **Apply** and **Save**.
Start	First MAC address of the range.
End	Last MAC address of the range.
Comments	Description of the selected MAC address range.

Router

Router objects can be used:

- As the firewall's default gateway,
- As the gateway in static routes (except for router objects involved in load balancing),
- For specifying the type of routing in filter rules (PBR: Policy Based Routing).

Router objects are defined by a name and at least a gateway used. They may contain one or several gateways used and backup gateways. A mechanism that tests the availability of these gateways makes it possible to provide redundancy – if no responses are received from one or several main gateways, one or several backup gateways will then take over. As soon as the main gateway becomes active again, the switch from the backup gateway to the main gateway will be automatic.

Select a router to view or edit its properties.

Properties

Object name	Name given to the router object when it was created.
Comments	Description associated with the router object.

Monitoring

The fields in the **Monitoring** section make it possible to define the method and parameters to use to verify the availability of the router object's gateways.

Detection method	There are two ways to detect the status of gateways: • ICMP: ICMP requests (pings) are sent to gateways, and their statuses are detected based on whether they respond to the pings. • TCP Probe: gateway status is detected by connecting to a TCP service hosted by the gateways that make up the router object. When this method is chosen, an additional field will appear, corresponding to the TCP port of the service to be tested (HTTPS by default).
Port	This field appears only when the TCP Probe detection method is chosen. Select the TCP port to test on the gateways that make up the router object. The *https* port is suggested by default.
Timeout (s)	Indicate the timeout (in seconds) after which a request that has not received a response will be considered a failure.
Interval (s)	Indicate the interval (in seconds) between two requests.

Failures before degradation	Indicate the number of failed requests before the link is declared degraded or the gateway is declared unreachable.

SD-WAN SLA (thresholds)

Select this checkbox to show the restrictions on network metrics (latency, jitter, packet loss, etc.) that the router object's gateway must comply with to guarantee the SLA relating to the router.
Compliance with these values determines the status of the router object's gateways, therefore the status of the router object itself. These statuses are shown in the dashboard, the SD-WAN monitoring module and the Connections monitoring module.

Latency (ms)	This metric represents the amount of time that a data packet needs to go from the source to the destination through a network. Though the term is technically inaccurate, the ms that a ping takes to reach its destination is referred to as "latency". Indicate the maximum accepted latency (in milliseconds) for the router object's gateways. This value must be between 0 and 60000 milliseconds inclusive.
Jitter (ms)	This metric represents how latency changes over time. Indicate the maximum accepted jitter (in milliseconds) for the router object's gateways. This value must be between 0 and 30 milliseconds inclusive.
Packet loss rate (%)	This metric represents the percentage of loss that a message can accept (sending without response). This value must be between 0 and 100 inclusive.
Unavailability rate (%)	This metric represents the percentage of time that a gateway is unavailable or inactive over the period measured. This parameter exists mainly to show statistics regarding the availability of gateways.

NOTE
Prior to configuring a switch when any of the SLA thresholds are not met, we recommend that you check in advance whether these thresholds will not wrongly trigger a switch. To do so, create a router object with the desired SLA thresholds and add it to the end of your security policy in a rule that will never be used. The object will then appear in the **Monitoring** module, which will allow you to ensure that the right SLA thresholds are selected.
We especially recommend this verification when jitter is the only SLA threshold used because it measures even the most minute changes when they occur.

Tables of gateways used and backup gateways

Button bar

Add	Adds a gateway.
Delete	Deletes the selected gateway.
Move to the list of backups/Move to the list of main gateways	Allows switching from one gateway in the main table to the backup table or vice versa.

Both grids contain the following columns:

Gateway	Clicking on a line in this column will open the objects database to select a host that acts as the router.
Weight	Allows a priority to be assigned between the various gateways for the load balancing mechanism. A gateway with a higher weight will therefore be used more often when balancing traffic load.
Test target(s)	Host or host group to test in order to determine the connectivity of the gateway. The value selected may be the gateway itself (**Test the gateway directly**), a host or a group of third-party hosts. The availability test may be disabled for the selected gateway by selecting the value **No availability testing**. **NOTE** We strongly recommend that you use a host group as the test target. **NOTE** If the value **No availability testing** has been selected for all gateways, the function that enables a switch to backup gateways will be disabled.
Comments	Any text.

NOTE
Parameters that define the interval between two availability tests ("frequency"), the maximum waiting time for a response ("wait") and the number of tests to perform before declaring the gateway uncontactable ("tries") can only be configured via CLI command:

```
CONFIG OBJECT ROUTER NEW name=<router name> [tries=<int>]
[wait=<seconds>] [frequency=<seconds>] update=1.
```

The default values suggested are 15 seconds for the "frequency" parameter, 2 seconds for the "wait" parameter and 3 for the "tries" parameter.

Advanced properties

Load balancing	The firewall allows distributed routing between the various gateways used through several methods: • **No load balancing**: only the first gateway defined in the "Used gateways" and "Backup gateways" tables will be used for routing. • **By connection**: all gateways defined in the "Used gateways" table will be used. The load balancing algorithm is based on the source (source IP address, source port) and the destination (destination IP address, destination port) of the traffic. The rate at which the various gateways are used will be related to their respective weights. • **By source IP address**: all gateways defined in the "Used gateways" table will be used. An algorithm allows balancing routing based on the source of the routed traffic. The rate at which the various gateways are used will be related to their respective weights.

Enable backup gateways	• **When all gateways cannot be reached**: the backup gateway(s) will only be enabled when all the gateways used cannot be contacted. • **When at least one gateway cannot be reached**: the backup gateway(s) will be enabled as soon as a gateway used cannot be contacted. This option is grayed out when a single gateway is entered in the table of used gateways. • **When the number of gateways that can be reached is lower than**: the backup gateway(s) will be enabled as soon as the number of contactable gateways used falls below the number indicated. This option is grayed out when a single gateway is entered in the table of used gateways.
Enable all backup gateways when unavailable	If this option is selected, all backup gateways will be enabled as soon as the condition for enabling them has been met. If it is not selected, only the first backup gateway listed will be enabled.
If no gateways are available	Select the behavior that the firewall must adopt if all the gateways defined in the router object cannot be contacted: • **Default route**: the routes (static or dynamic) defined in the firewall's routing table will be applied. • **Do not route**: the firewall will not manage packets passing through.

Apply	Confirms the router's configuration.
Copy	Allows creating a new router object by duplicating the same characteristics as the edited router.
Cancel	Cancels the router's configuration.

Group

In this screen, you will be able to aggregate your objects according to your network topology, for example.

Name of the object	Name given to the object group during its creation. Objects in "read only" mode will be grayed out and cannot be modified.
Comments	Description of the object group.

Edit this group	Clicking on this button triggers a dialog box for adding object(s) to the group. **Object name**: enter the new group name if you wish to change it. Two columns are displayed: • The left column contains the list of all the network objects that you may add to your group. • The right column contains the objects that are already in the group. To add an object to the group, you need to move it from one column to the other: 1. Select the item(s) to add. 2. Click on this arrow . The object will move to the right column and become a part of your group (at the top of the list). To remove an object from the group: 1. Select it in the right column. 2. Click on this arrow . **NOTE** By clicking on the button "Edit this group", you will be able to change the name of the group and add comments to it and also search for objects and include new objects in the group.
Objects in this group	The network objects in your group will be shown in a table. To add or modify objects, refer to the previous field.

Protocol

Name of the object	Name of the selected protocol. This field is grayed out and cannot be modified.
Protocol number	Number associated with the selected protocol and provided by the IANA (Internet Assigned Numbers Authority).
Comments	Description of the selected protocol.

Port – port range

Select a port or port range to view or edit its properties.

Name of the object	Name of the service used. This field is grayed out and cannot be modified.
Port	Number of the port associated with the selected service.
Port range	By selecting this option, you will assign a port range to the selected service and enable the two checkboxes below it.
From	If the Port range checkbox has been selected, this field will be enabled. It corresponds to the first port included in the selected port range.

Up to	If the Port range checkbox has been selected, this field will be enabled. It corresponds to the last port included in the selected port range.
Protocol	Select the IP protocol that your service uses: • **TCP**: Transmission Control Protocol. Transport protocol operating in connected mode and made up of three phases: establishment of the connection, data transfer, end of the connection. • **UDP:** User Datagram Protocol. This protocol allows data to be transferred easily between two entities, each of them having been defined by an IP address and a port number. • **SCTP:** Stream Control Transmission Protocol, is a protocol that is defined in RFC 4960 (an introduction is provided in RFC 3286). As a transport protocol, SCTP is in a certain way equivalent to TCP or UDP. • While TCP is traffic-oriented, (the sequence of bytes contained in a packet does not have a conceptual beginning or end, but belongs to the stream of traffic that makes up the connection), SCTP — like UDP — is message-oriented (it sends messages in a traffic stream with a beginning and an end, which can be segmented over several packets). • **Any protocol**: The selected service can use any IP protocol.
Comments	Description of the selected port or port range.

Port group

This screen will allow you to aggregate your ports by category.

Example

A **"mail"** group that groups "imap", "pop3" and "smtp" ports.

Name of the object	Name given to the port group during its creation.
Comments	Description of the port group.

Edit this group	Clicking on this button triggers a dialog box for adding object(s) to the group. **Object name**: enter the new group name if you wish to change it. Two columns are displayed: • The left column contains the list of all the ports that you may add to your group. • The right column contains the ports that are already in the group. To add a port to the group, you need to move it from one column to the other: 1. Select the item(s) to add. 2. Click on this arrow . The object will move to the right column and become a part of your group (at the top of the list). To remove an object from the group: 1. Select it in the right column. 2. Click on this arrow . **NOTE** By clicking on the button "Edit this group", you will be able to change the name of the group and add comments to it and also search for objects and include new objects in the group.
Objects in this group	The ports in your group will be shown in a table. To add or modify objects, refer to the previous field.

Region group

In this screen, you will be able to aggregate countries or continents in a single group.

Name of the object	Name given to the group of regions during its creation.
Comments	Description of the region group.

Edit this group	This button contains a dialog box for adding countries or continents to the group. By clicking on it, you will be able to change the name of the group and add comments to it and also search for ports and include new countries or continents in the group. Two columns will appear: • The left column contains the list of all the countries or continents that you may add to your group, • The right column contains the countries or continents that are already in the group. To add a country or continent to the group, you need to move it from one column to the other: 1. Select the item(s) to add. 2. Click on this arrow . The object will move to the right column and become a part of your group (at the top of the list). To remove an object from the group: 1. Select it in the right column. 2. Click on this arrow .
Objects in this group	The countries or continents in your group will be shown in a table. To add or modify objects, refer to the previous field.

Time object

Name of the object	Name given to the port group during its creation.
Comments	Description of the port group.
Description	This dynamic field will be entered automatically based on the parameters selected for the definition of the time object. **EXAMPLE** For an ad hoc event: from <*date*> at <*time*> to <*date*> at <*time*>

Fixed event

This field allows defining "From" when the event takes place and until when it will continue. A day has to be defined from the calendar presented.

You will also need to define a time by entering the empty "to" field.

Day of the year

By default, this field indicates the date 01: 01. You can click on **Add a date range** and enter a start date and an end date for your event, by selecting the month and the day.

Day(s) of the week

The days affected by the event are marked with this icon . If you wish to remove a day, click once on it. If you wish to apply an additional day, such as a Saturday, for example, click once

on the checkbox “Sat”. It will then be marked by the same icon described above and your event will affect this day.

Time slots

You can define time slots using these buttons:

- **Add a time slot**, to add a time slot and to define the start and end time of your event.
- To delete it.

New information regarding the time slot(s) will appear in the field **Description**.

PREFERENCES

In the **Preferences** module, you can manage the firewall's web administration interface settings and improve your user experience.

You can access this module in the top right corner, from the drop-down menu with the ID of the connected administrator.

To open this module:

1. Click on the name of the connected administrator (upper right side of the screen).
2. Click on **Preferences**.

Restore default parameters	This button makes it possible to restore user preferences, which include the settings in the **Preferences** module and display settings in the configuration modules, such as columns and their order.

Preferences are organized by 3 tabs:

- **Parameters** tab,
- **Display** tab,
- **Links** tab.

Parameters tab

Connection settings

Connect automatically with an SSL certificate	If this option is selected, you will no longer need to identify yourself, as you will be recognized directly thanks to your SSL certificate.
Log out when idle	A duration can be set for the disconnection from your web interface: • 5 minutes, • 15 minutes, • 30 minutes, • 1 hour, • Always remain connected. **NOTE** If the administrator has set a maximum timeout for all administrator accounts, higher timeouts will not appear in the drop-down menu.

Management interface behavior

Search every field of an object	When you perform a search by letter or by word in the dedicated fields, the engine will check both the names and the comments, to find anything that matches the object of the search.

Disable real-time diagnoses of the security policy	When you create a rule in the security policy, the diagnosis engine will automatically check if rules overlap and if errors have been detected. If this option is selected, a manual search for these possible errors will be implied.
Week starts on Sunday	If this option is selected, Time objects that appear in the menu Objects will begin their weeks on Sunday.
Confirm before applying changes	This option makes it possible to cancel operations if you have made a mistake or if you decide not to continue with your configuration. A confirmation window will appear, allowing you to confirm or cancel your action.

Display tab

Application settings

Always display advanced properties	Every item in advanced properties can be expanded in their respective modules, but are collapsed by default. By selecting this option, you will make them visible on the screen without having to expand them.
Display button to save commands	By selecting this option, the command recording button will appear in the upper banner of the web administration interface. It will therefore be available regardless of the configuration module selected.
Display users at startup of module	If this option is selected, all users will be displayed in the directory on the left.
Display network objects at startup of module	If this option is selected, all network objects will be displayed in the directory on the left.
Display global policies (Network objects, Certificates, Filter, NAT and IPsec VPN)	If this option is selected, during connections to the **Filter and NAT (Security policy)**, **IPsec VPN (VPN) and Objects** modules, the screen will display a drop-down menu offering choices between the local and global policies. The current local security policy is displayed by default.
Apply a default comment to rules (filtering, NAT and IPsec)	If this option is selected, comments created for filter and NAT rules will automatically include the date and time of creation. This option applies to the display of filter, NAT and IPsec policies.
Number of rules per page (filtering, NAT and IPsec)	Depending on the number of existing rules, you can choose to display: • 100 rules per page • 200 rules per page • 500 rules per page • 1000 rules per page By selecting "Automatic", the Stormshield Network engine will try to deduce the number of rules per page, according to your configuration. This option applies to the display of filter, NAT and IPsec policies.

Log settings

Number of lines displayed per page	Depending on the number of rows found in the log files, you can choose to display: • 200 rows per page • 400 rows per page • 600 rows per page • 800 rows per page • 1000 rows per page
Minimum number of characters to start searching (0 to disable)	Indicate the number of characters that need to be entered in the search field in order to automatically filter data based on this value.

Links tab

External links

Online help URL	This URL indicates the address to access Stormshield Network's online help: you will find the directory of the modules in alphabetical order. Click on the module of your choice in order to view the corresponding page.
Alarm online description URL	This address allows you to access a help document that will help you to understand the Alarms module, which appears in the Stormshield Network knowledge base.

PROTOCOLS

This module contains the list of the various protocols that can be configured from your web interface.

It is divided into 2 distinct zones:

- The list of protocols (left column). Some protocols are grouped by theme:
  - Instant messaging,
  - IP protocols (ICMP, IP, SCTP and TCP-UDP),
  - Industrial protocols,
  - Microsoft protocols,
  - VoIP/Streaming.
- Profiles that can be assigned to the protocols and their parameters (right column). This area is enabled after a protocol has been selected in the left column.

Search

The search bar allows locating the protocol to be configured by entering the first few letters of its name. Clicking on the desired protocol allows working directly with it.

List of protocols

Select the protocol that you wish to configure in the list displayed. Once the protocol has been selected, you can start configuring it.

Profiles

Selecting a profile

These **application profiles** contain the configuration of the protocol analysis, which is capable of raising alarms. An **inspection profile** is made up of a set of application profiles per protocol. By default, the inspection profile *IPS_00* contains the **application profiles** *protocole_00*, and so on. These are the **inspection profiles** that will be applied in the filter policy.

For information, in factory configuration the inspection profile *IPS_00* is intended for **internal interfaces**, applied to incoming traffic. The profile meant for **public interfaces** applied to outgoing traffic is the profile *IPS_01*.

The drop-down list offers 10 profiles, numbered from 00 to 09.

Each profile has by default the name of the protocol, accompanied by its number.

EXAMPLES

- http_00
- (1) http_01…

Buttons

Edit	This function allows performing 3 operations on profiles: • **Edit**: by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on "Update". This operation can also be canceled. • **Reinitialize**: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. • **Copy to**: This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the exact date and time of the last modification. If the selected profile has comments, they will be displayed in the tooltip.
Go to global configuration	This option contains the list of default TCP ports. This option is accessible in each protocol except: IP, ICMP, RTP, RTCP. You can **Add** or **Delete** ports by clicking on the respective buttons. Please refer to the following section to find out which settings are offered in the global configuration. **NOTE** The global configuration of SSL and TCP/UDP protocols is carried out differently. They are described in a sub-section under the section **Global protocol configuration**.

Global protocol configuration

The button "Go to global configuration" applies to all the profiles of the selected protocol.

This option is offered for every protocol except IP, RTP, RTCP and S7.

Protocol: list of default TCP or UDP ports

This option defines the list of ports (TCP or UDP) scanned by default by the plugin of the protocol that is being configured. You can **Add** or **Delete** ports by clicking on the respective buttons.

Protocol over SSL: list of default TCP ports

The ports added to the list of secure protocols will first be analyzed by the SSL plugin, then by the plugin of the configured protocol if the traffic is encrypted. You can **Add** or **Delete** ports by clicking on the respective buttons.

This selection is available for the protocols *HTTPS, SMTPS, FTPS, POP3S, OSCAR over SSL, NetBios CIFS over SSL, NetBios SSN over SSL* and *SIP over SSL*.

EXAMPLE
Choosing the HTTPS port in the list "HTTPS: list of default TCP ports" will activate two analyses:

- The HTTPS traffic will be scanned by the SSL plugin.
- The traffic decrypted by the SSL proxy will be analyzed by the HTTP plugin.

Proxy

This option is enabled in the global configuration of the HTTP, SMTP, POP3 and SSL protocols. It applies to all the inspection profiles.

Apply the NAT rule on scanned traffic	By default, traffic scanned by an implicit proxy will be re-sent with the address of the firewall's outgoing interface. If this option is selected for a NAT policy, address translation will be applied to the traffic leaving the proxy analysis. This option will not be applied on translations of the destination.

Global configuration of the TCP/UDP protocol

IPS tab

Denial of Service (DoS)

Max no. of ports per second	In order to avoid port scans, this value is the limit to the number of the various ports (between 1 and 1024) accessible within 1 second for a given protected destination. This number has to be between 1 and 16 ports.
Purge session table every (seconds)	Once the connection/session table is full, the purge of inactive connections will be scheduled. Define the maximum time gap between two purges of the session table between 10 and 172800 seconds to avoid overloading the appliance.

Connection

Allow half-open connections (RFC 793 section 3.4)	This option makes it possible to avoid denials of service that may take place within so-called "normal" connections.

http://tools.ietf.org/html/rfc793#section-3.4

Support

Log every TCP connection	Option to enable log generation for TCP connections
Log every UDP pseudo-connection	Option to enable log generation for UDP connections

Global configuration of the SSL protocol

Proxy tab

Generate certificates to emulate the SSL server

C.A (signs the certificates)	Select the sub-authority used for signing the certificates generated by the SSL proxy. You must first import it in the **Certificate** module (**Object** menu).
Certification authority password	Enter the password of the selected certification authority.
Certificate lifetime (days)	This field indicates the **Validity (days)** of the certificates generated by the proxy.

SSL: list of default TCP ports

This option is offered for the list of default TCP ports. The default ports of the added protocols will be analyzed by the SSL plugin.

Proxy

This option applies to all the inspection profiles. It will not be applied on translations of the destination.

Apply the NAT rule on scanned traffic	By default, traffic scanned by an implicit proxy will obtain the address of the firewall's outgoing interface on its way out. If this option is selected for a NAT policy, address translation will be applied to the traffic leaving the proxy analysis. This option will not be applied on translations of the destination.

Customized certification authorities tab

Add the list of customized CAs to the list of trusted authorities	This option enables the feature for importing certification authorities that are not public. These CAs will be considered trusted authorities. Certificates issued by such customized CAs will therefore be considered trustworthy.

It is possible to **Add** or **Delete** certification authorities by clicking on the respective buttons.

Public certification authorities tab

A public certification authority can be disabled by double-clicking on the status icon, enabled by default. You may also choose to **Enable all** or **Disable all** these public CAs by clicking on the respective buttons.

In order to improve monitoring, these root certification authorities are kept up to date in the firewall's list via **Active Update**.

Trusted certificates tab

These are whitelisted certificates to which content inspection processes (self-signed certificates, expired certificates, etc) defined in the *Proxy* tab in the SSL profile configuration will not be applied.

In this window, you may **Add** or **Delete** trusted certificates by clicking on the relevant button.

IPS tab

Certificate analysis

Certificate cache timeout (TTL)	To optimize the analysis of server certificates, a cache mechanism has been implemented to avoid retrieving a certificate when the intrusion prevention engine already knows it. This mechanism therefore defines how long, in seconds, cache entries will be kept. When a cached certificate reaches the maximum duration, the corresponding entry will be automatically deleted.

Global configuration of the ICMP protocol

IPS tab

IPS	
Maximum global rate of ICMP error packets (packets per second and per core)	Whenever the number of ICMP error packets exceeds this limit (25000 by default), the firewall will ignore additional packets before applying filter rules. This option allows protecting the firewall from Blacknurse attacks.

Live Messenger (MSN)

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

Support	
Disable intrusion prevention	When this option is selected, the scan of the Live Messenger (MSN) protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every Live Messenger query	Enables or disables the generation of logs relating to Live Messenger queries.

Yahoo Messenger (YMSG)

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

Support

Disable intrusion prevention	When this option is selected, the scan of the Yahoo Messenger protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every Yahoo Messenger (YMSG) query	Enables or disables the generation of logs relating to the Yahoo Messenger protocol.

ICMP

"IPS" tab

Session parameters (in seconds)

Session expiration	must be between 2 and 60 seconds.

Support

Ignore ICMP notifications (stateful TCP/UDP)	If this option is selected, you will no longer take into account error messages that could arise in the protocols, such as the accessibility of a service or a host, for example.

IP

"IPS" tab

> **NOTE**
> The IP protocol does not have a profile. Only a global configuration is available.

MTU

Impose MTU limit (force fragmentation)	MTU (Maximum Transmission Unit) represents the maximum size of an IP packet. If this option is selected, the next field will be enabled and you can define your limit.
Maximum MTU value	Define the maximum value of the IP datagram, between 140 and 65535 bytes.

Fragmentation

Minimum fragment size (bytes)	The fragment must be between 28 and 65535 bytes. The default value is 140 bytes.
Session will expire in (seconds)	This period must be between 2 and 30 seconds.

Stealth mode

Enable stealth mode	In stealth mode, the firewall does not respond to detection attempts - ICMP requests in particular - so that it appears invisible. Stealth mode is enabled by default and can be disabled by unselecting this checkbox. **NOTE** Disabling stealth mode will affect packet processing performance. As the firewall must keep a log of each packet so that it can respond to ICMP error messages, stealth mode allows the firewall to save resources that would have been used on logging these packets.

SCTP

SCTP, or Stream Control Transmission Protocol, is a protocol that is defined in RFC 4960 (an introduction is provided in RFC 3286).

As a transport protocol, SCTP is in a certain way equivalent to TCP or UDP.

While TCP is traffic-oriented, (the sequence of bytes contained in a packet does not have a conceptual beginning or end, but belongs to the stream of traffic that makes up the connection), SCTP — like UDP — is message-oriented (it sends messages in a traffic stream with a beginning and an end, which can be segmented over several packets).

"IPS" tab

Specific configuration

Maximum no. of IP addresses per endpoint [1-8]	This parameter defines the maximum number of IP addresses allowed for an SCTP association endpoint (*multi-homing*).

Timeout (seconds)

Association negotiation time [2-60]	Maximum duration allowed for an SCTP association to be fully set up (in seconds). This value has to be between 2 and 60 seconds (default value: 20 seconds).
Idle timeout [30-604800]	Maximum duration for which the state of an idle SCTP association will be kept (in seconds). This value has to be between 30 and 604800 seconds (default value: 3600 seconds).
Association shutdown time [2-60]	Maximum duration allowed for the shutdown phase of an SCTP association (in seconds). This value has to be between 2 and 60 seconds (default value: 20 seconds).

Support

Disable intrusion prevention	When this option is selected, the scan of the SCTP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every SCTP query	Enables or disables the logging of SCTP requests.

TCP-UDP

TCP ensures control of data during their transfer. Its role is to check that IP packets sent are received in good order, without any loss of changes integrity-wise.

UDP may replace TCP in the event of minor problems, as it ensures a more fluid transfer since it does not control each of the transmission stages. For example, it is suitable for streaming applications (audio/video broadcast) for which packet loss is not vital. Indeed, during these transmissions, lost packets are ignored.

Profiles screen

IPS-Connection tab

Inspection

Impose MSS limit	This option allows you to set an MSS (Maximum Segment Size) limit for the inspection of the profile. **NOTE** MSS refers to the amount of data in bytes that a computer or any other communication device can contain in a single unfragmented packet. If this option is selected, you will enable the following field, which would allow you to set your limit.
MSS limit (in bytes)	Define your MSS limit, between 100 and 65535 bytes.
Rewrite TCP sequences with strong random values (arc4).	If this option is selected, TCP sequence numbers generated by the client and server will be overwritten and replaced with the Stormshield Network intrusion prevention engine, which will produce random sequence numbers.
Enable protection from repeated sending of ACK packets	If this option is selected, you are protecting yourself from session hijacking or "ACK" attacks.
Enable automatic adjustment of memory allocated to data tracking	If this option is selected, you will be allowing the firewall to dynamically adjust the memory allocated to data tracking. The maximum value of dynamically allocated memory is equal to the size of the TCP window divided by the MSS limit. When this checkbox is selected, the maximum value becomes 256.
Enable application tracking	This option makes it possible to log application IDs in alarm and connection logs in order to generate reports based on these application IDs.

Protection against denial of service attacks

Connection restrictions

Maximum number of TCP connections per source IP address (0 disables this protection)	This option makes it possible to restrict the number of TCP connections for a single source IP address. When the selected value is 0, no restrictions will be applied. **IMPORTANT** Choosing a number that is too low may prevent certain applications from running or web pages from displaying.
Maximum number of UDP sessions per source IP address (0 disables this protection)	This option makes it possible to restrict the number of UDP sessions for a single source IP address. When the selected value is 0, no restrictions will be applied. **IMPORTANT** Choosing a number that is too low may prevent certain applications from running or web pages from displaying.

Maximum frequency with which initial TCP/UDP packets are received

Maximum number of SYN packets received within the reference interval for a source IP address (0 disables this protection)	This option makes it possible to set the maximum number of TCP connection requests (SYN packets) received from the same source IP address during the reference period set in the **Reference interval for maximum frequency with which initial TCP/UDP packets are received** section. This option makes it possible to protect the firewall from SYN flooding (DDoS) attacks.
Maximum number of new UDP sessions within the reference interval for a source IP address (0 disables this protection)	This option makes it possible to set the maximum number of UDP session requests received from the same source IP address during the reference period set in the **Reference interval for maximum frequency with which initial TCP/UDP packets are received** section. This option makes it possible to protect the firewall from UDP flooding (DoS) attacks.

Reference interval for maximum frequency with which initial TCP/UDP packets are received

Interval during which new TCP connections from the same source address are counted until reaching the threshold set in the calculation of the frequency with which initial TCP packets are received	This option makes it possible to set the reference time to calculate the maximum frequencies of new TCP connections (SYN packets) for the same source IP address. **IMPORTANT** Choosing a number that is too low may prevent certain applications from running or web pages from displaying.
Interval during which new UDP sessions from the same source address are counted until reaching the threshold set in the calculation of the frequency with which initial UDP packets are received	This option makes it possible to set the reference time to calculate the maximum frequencies of new UDP sessions (SYN packets) for the same source IP address. **IMPORTANT** Choosing a number that is too low may prevent certain applications from running or web pages from displaying.

NOTE
To track the values of simultaneous connection counters, use the command: `sfctl -s host -v`.

Timeout (seconds)

Connection opening timeout (SYN)	Maximum time, in seconds, allowed to fully establish the TCP connection (SYN / SYN+ACK / ACK). It has to be between 10 and 60 (default value: 20 seconds).
TCP connection	Maximum duration in seconds for which the state of an idle connection is kept. It has to be between 30 and 604800 (default value: 3600 seconds).

UDP session	Maximum time, in seconds, the state of an idle UDP pseudo-connection is kept. It has to be between 30 and 604800 (default value: 120 seconds).
Connection closing timeout (FIN)	Maximum time, in seconds, allowed for the TCP connection closing phase (FIN+ACK / ACK / FIN+ACK / ACK). This value has to be between 10 and 3600 seconds (default value: 480 seconds).
Closed connections	Number of seconds a closed connection (*closed* state) is kept in the connection table. It has to be between 2 and 60 seconds (default value: 2 seconds).
Small TCP window	To avoid Denial of Service attacks, the counter determine the lifetime of a connection with a small TCP window (lower than 100 byte). This counter is reset when the first small window announcement is received. If no new message is received to increase the window size before this counter expires, the TCP connection will be closed.

Support

Disable the SYN proxy	If this option is selected, you will no longer be protected from "SYN" attacks, as the proxy will no longer filter packets. We advise you to disable this option for debug purposes only.

IEC 61850 GOOSE (IPS)

IEC61850 is a communication standard that protection systems on substations use in the electrical energy industry.

Specifically, IEC 61850 is used in communications between intelligent electronic devices located on distribution substations in a power grid. Intelligent electronic devices, also known as IEDs, essentially include microprocessor-based protective relays, measuring devices, programmable logic controllers, and fault and event recorders. With these devices, power grids can be monitored in real time, therefore making the substation "intelligent".

General settings

Timeout in seconds for Ethernet connection [2-604800]	This value is the period after which IEC 61850 GOOSE connections without responses will be deleted, and must be between 2 and 604800 seconds. The default value is 60 days.

Support

Disable intrusion prevention	When this option is selected, the analysis of the IEC 61850 GOOSE protocol will be disabled and traffic will be allowed if the filter policy allows it.
Log every IEC 61850 GOOSE request	Enables or disables logs that capture IEC 61850 GOOSE requests.

MMS/IEC 61850 MMS

MMS tab

Manage MMS services

Block reserved services	When this option is selected, you will block a particular confirmed service - the service labeled *Reserved service* and associated with ID 79 in the specifications of the IEC61850 protocol.

"Confirmed services" tab

This table lists the standard confirmed MMS services (services that require a reply) predefined on the firewall, classified by service group:

- VMD Support,
- Variable Access,
- Semaphore Management,
- Scattered Access
- Program Invocation Management,
- Operator Communication,
- Journal management,
- File Management,
- Event Management,
- Event Enrollment,
- Event Condition,
- Event Action,
- Domain Management,
- Data Exchange,
- Access Control.

Predefined confirmed standard MMS services are allowed by default (*Allow* action) and this action can be modified for each one of them. The buttons **Block by service set**, **Allow by service set** and **Modify all services** make it possible to modify the action (*Allow/Block*) applied to the selected service set or to all services listed in the table.

"Additional confirmed services" tab

This table lists the additional confirmed MMS services (services that require a reply) predefined on the firewall, classified by service group:

- VMD Support,
- Unit Control,
- Program Invocation Management,
- Event Condition.

Predefined additional MMS services are allowed by default (*Allow* action) and this action can be modified for each one of them. The **Modify all services** button makes it possible to edit the action (*Allow/Block*) applied to all services listed in the table.

Support

Disable intrusion prevention	When this option is selected, the scan of the MMS protocol will be disabled and traffic will be authorized if the filter policy allows it
Automatically detect and inspect the protocol	If the MMS protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

IEC 61850 MMS (IPS) tab

IEC61850 is a communication standard that protection systems on substations use in the electrical energy industry.

Specifically, IEC 61850 is used in communications between intelligent electronic devices located on distribution substations in a power grid. Intelligent electronic devices, also known as IEDs, essentially include microprocessor-based protective relays, measuring devices, programmable logic controllers, and fault and event recorders. With these devices, power grids can be monitored in real time, therefore making the substation “intelligent”.

Manage IEC 61850 services

This table lists the IEC61850 MMS services that have been predefined on the firewall, classified by service group:

- Setting Group Control Block,
- Server,
- Report Control Block,
- Logical Node,
- Logical Device,
- Log Control Block,
- GSSE,
- GOOSE,
- File transfer,
- Data Set,
- Data,
- Control.

IEC61850 MMS services are allowed by default (*Allow* action) and this action can be changed for each one of them. The buttons **Block by service set**, **Allow by service set** and **Modify all services** make it possible to modify the action (*Allow/Block*) applied to the selected service set or to all services listed in the table.

Whitelisted logical nodes

This grid lists the services that do not need the IEC61850 MMS protocol analysis.

Enable whitelist	When this checkbox is selected, you will enable the whitelist so that MMS services to be excluded from the analysis can be added to it.

It is possible to **Add** or **Delete** MMS services to be whitelisted by clicking on the corresponding buttons.

The **Select all** button makes it possible to select all services found in the whitelist to **Delete** them in a single operation.

IEC 61850 SV (IPS)

IEC61850 is a communication standard that protection systems on substations use in the electrical energy industry.

Specifically, IEC 61850 is used in communications between intelligent electronic devices located on distribution substations in a power grid. Intelligent electronic devices, also known as IEDs, essentially include microprocessor-based protective relays, measuring devices, programmable logic controllers, and fault and event recorders. With these devices, power grids can be monitored in real time, therefore making the substation “intelligent”.

General settings

Timeout in seconds for Ethernet connection [2-604800]	This value is the period after which IEC 61850 SV connections without responses will be deleted, and must be between 2 and 604800 seconds. The default value is 60 days.

Support

Disable intrusion prevention	When this option is selected, the analysis of the IEC 61850 SV protocol will be disabled and traffic will be allowed if the filter policy allows it.
Log every IEC 61850 SV request	Enables or disables logs that capture IEC 61850 SV requests.

BACnet/IP

BACnet (Building Automation and Control Networks) is a standardized communication protocol designed for the deployment of building automation and control networks. It is dedicated to the centralized technical management of equipment for ventilation, air conditioning, lighting, access control, and fire safety systems.

CIP (IPS - CIP tab)

Settings

Maximum number of CIP services in a packet	The CIP service code Multiple_Service_Packet makes it possible to encapsulate several CIP commands in the same network packet. This field allows defining the number of commands that can be grouped in a single packet. This value must be between 1 and 65535 seconds (default value: 65535).

Service management

Standard services tab

This list sets out the service IDs and associated standard CIP services that the firewall authorizes by default. The action (*Allow/Block*) applied to each service can be modified by clicking in the **Action** column. The **Select all** button makes it possible to change the action (*Allow/Block*) applied to all services.

Specific services tab

This list sets out the service IDs, specific CIP services and associated class IDs that the firewall authorizes by default. These services are allowed by default (*Allow* action). These services are classified by service group:

- Acknowledge Handler Object,
- Assembly Object,
- Connection Manager Object,
- Connection Object,
- Connection Configuration Object,
- File Object,
- Message Router Object,
- Motion Axis Object,
- Parameter Object,
- S-Analog Sensor Object,
- S-Device Supervisor Object,
- S-Gas Calibration Object,
- S-Partial Pressure Object,
- S-Sensor Calibration Object,
- S-Single Stage Controller Object,
- Time Sync Object.

The buttons **Block by service set**, **Allow by service set** and **Modify all services** make it possible to modify the action (*Allow/Block*) applied to the selected service set or to all CIP services listed in the table.

Customized classes and services

This list makes it possible to filter, for the selected class IDs (between 0 and 65535 inclusive, separated by commas or by a dash to define a range), the CIP service IDs to be authorized (between 0 and 127 inclusive, separated by commas or by a dash to define a range). It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

ETHERNET/IP (IPS tab)

Settings

Max no. of pending requests	Maximum number of requests without responses in a single EtherNet/IP session. This value has to be between 1 and 512 seconds (default value: 10).

Maximum request duration (in seconds)	This value is the period after which EtherNet/IP requests without responses will be deleted. This value has to be between 1 and 3600 seconds (default value: 10).
Maximum message size (bytes)	This value makes it possible to restrict the size allowed for an EtherNet/IP message. It has to be between 24 and 65535 (default value: 65535).

Commands management

Public commands tab

This list sets out the public EtherNet/IP functions allowed by default on the firewall. The action (*Allow/Block*) applied to each command can be modified by clicking in the **Action** column. The **Modify all commands** button makes it possible to change the action (*Allow/Block*) applied to all commands.

Other commands allowed tab

This list makes it possible to allow additional EtherNet/IP commands blocked by default on the firewall. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Support

Disable intrusion prevention	When this option is selected, the scan of the EtherNet/IP protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log each request	Enables or disables the logging of EtherNet/IP requests.
Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

IEC 60870-5-104 (IEC 104)

Settings

Max no. of pending requests	Maximum number of requests without responses in a single session. This value has to be between 1 and 32768 seconds (default value: 12).
Maximum request duration (in seconds)	This value is the period after which requests without responses will be deleted. This value has to be between 1 and 255 seconds (default value: 10).
Maximum message size (bytes)	This value makes it possible to restrict the size allowed for a message. It has to be between 12 and 255 (default value: 255).

Redundancy

The IEC 104 protocol adds the concept of redundancy: a client host sets up a certain number of connections with its server, with only one of these connections active at any given time. This set of connections is called a "redundancy group". Whenever the active connection is disrupted, one of the established connections will immediately take over.

Maximum number of redundancy groups	This is the maximum number of redundancy groups allowed per server.
Maximum number of redundant connections	This is the maximum number of connections that can be set up in a redundancy group.

ASDU management

Public IDs

This table shows the predefined *ASDUs (Application Service Data Units)* on the firewall. ASDUs, represented by their identifiers, are classified by*Type Id*: File transfer, Parameters, Process information and System information.

These public type identifiers are allowed by default (*Allow* action). The buttons **Block by Type ID**, **Allow by Type ID** and **Modify all Type IDs** make it possible to modify the action (*Allow/Block*) applied to the selected *ASDU* set or to all *ASDUs* listed in the table.

Other authorized Type IDs

This list allows additional identifiers to be added. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Support

Disable intrusion prevention	When this option is selected, the scan of the protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log each IEC 60870-5-104 request	Enables or disables the logging of requests.
Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

Advanced settings

Additional cause

An IEC104 packet's Cause of transmission (COT) field makes it possible to specify why the packet was sent.
In addition to the list of COTs predefined in the IEC104 protocol standard, this grid allows you to **Add** (using the button of the same name) **Additional causes** that the IEC 60870-5-104 protocol analysis engine will analyze.

MODBUS (IPS) tab

General settings

Max no. of pending requests	Maximum number of requests without responses in a single session. This value has to be between 1 and 512 seconds (default value: 10).
Maximum request duration (in seconds)	This value is the period after which requests without responses will be deleted. This value must be between 1 and 3600 seconds inclusive (default value: 10).
Support serial gateways	If this option is selected, you will allow protocol scans for Modbus traffic heading to the TCP Modbus gateway to the serial port (in this case, Modbus messages will have fields containing particular values).

Allowed Unit IDs

This list shows the Unit IDs allowed. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Modbus settings

Maximum message size (bytes)	This value makes it possible to restrict the size allowed for a message. It has to be between 8 and 4096 (default value: 260).
Max. number of files	This field allows defining the maximum number of fields allowed for "Read File Record" and "Write File Record" operations in order to protect certain vulnerable automatons beyond a defined number of files.

Managing Modbus function codes

Public operations

This list sets out the public functions allowed by default on the firewall. The buttons **Modify write operations** and **Modify all operations** make it possible to modify the action (*Allow/Block*) applied to the selected function or to all functions.

Other operations allowed

This list allows authorizing additional function codes blocked by default by the firewall. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Managing Modbus addresses

In this panel, the access privileges of Modbus function codes to memory addresses on automatons can be filtered. By default, all Modbus function codes in read and write (1,2,3,4,5,6,15,16,22,23,24) are allowed to access all memory ranges on automatons (0-65535). It is possible to **Add** or **Delete** access rules to or from this list by clicking on the relevant buttons.

This added protection in the firewall makes it possible to define a Modbus profile that specifies the memory ranges on the PLC in which Modbus data can be written.

Support

Disable intrusion prevention	When this option is selected, the scan of the protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log each Modbus request	Enables or disables the logging of requests.
Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

OPC AE (IPS) tab

OPC AE general settings

This table lists the OPC AE (OPC Alarms and Events) services that have been predefined on the firewall. These services are classified by service set:

- Component Categories,
- OPC Events,
- OPC Type Library.

Predefined OPC AE services are allowed (analyzed) by default (*Allow* action). The buttons **Block by service set**, **Allow by service set** and **Modify all services** make it possible to modify the action (*Allow/Block*) applied to the selected service set or to all OPC AE services listed in the table.

OPC DA (IPS) tab

Grid of operations and operation groups

This table lists the OPC DA operations that have been predefined on the firewall. The various types of information for each operation/operation group are:

- **Name**: name of the operation or group of operations.
- **Operation no.**: numerical identifier of the operation in its group.
- **Action**: action applied to the network packet corresponding to the operation (*Allow/Block*)
- **Type**: indicates whether it is a *read* or *write* operation.

Possible operations

Predefined OPC DA operations are allowed by default (*Allow* action). The buttons **Block the selection**, **Allow the selection** and **Modify all write ops** make it possible to change the action (*Allow/Block*) applied to the selected operation, selected operation set or to all OPC DA write operations listed in the grid.

OPC HDA (IPS) tab

OPC HDA general settings

This table lists the OPC HDA (OPC Historical Data Access) services that have been predefined on the firewall. These services are classified by service set:

- Component Categories,
- OPC Browser,
- OPC Client,
- OPC Server
- OPC Type Library.

Predefined OPC HDA services are allowed (analyzed) by default (*Allow* action). The buttons **Block by service set**, **Allow by service set** and **Modify all services** make it possible to modify the action (*Allow/Block*) applied to the selected service set or to all OPC HDA services listed in the table.

OPC UA

OPC UA parameters

Maximum client message size (bytes)	This value makes it possible to restrict the maximum size that an OPC UA client is allowed to send. It has to be between 8192 and 2147483647 (default value: 65535).
Maximum server message size (bytes)	This value makes it possible to restrict the maximum size that an OPC UA server is allowed to send. It has to be between 8192 and 2147483647 (default value: 65535).

Prohibit "None" security mode	If this option is selected, you will prevent the circulation of unencrypted and unsigned OPC UA traffic.

Managing OPC UA services

Public services

This table lists the codes and associated OPC UA services that have been predefined on the firewall. These codes are classified by operation set: Attribute, Discovery, Method, Monitored Item, Node Management, Query, Secure Channel, Session, Subscription and View.

Predefined OPC UA services are allowed by default (*Allow* action). The buttons **Block by service set**, **Allow by service set** and **Modify all services** make it possible to modify the action (*Allow/Block*) applied to the selected service set or to all OPC UA services listed in the table.

Other services allowed

This list allows authorizing additional OPC UA function codes blocked by default by the firewall. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Support

Disable intrusion prevention	When this option is selected, the scan of the OPC UA protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log every OPC UA query	Enables or disables the logging of OPC UA requests.

PROFINET IO

Like FTP, the PROFINET IO protocol may be used to set up several connections for the same traffic stream: a parent connection from the client to the server over the port dedicated to the service, followed by one or several child connections over random ports for data exchange.

When the PROFINET IO protocol is analyzed, the firewall extracts data from the parent connection in order to create child connections (random ports allowed), so that you obtain a connection skeleton that enables dialog.

Connection skeleton settings

Allow creation of skeletons	When this option is selected, the PROFINET IO analyzer will allow parent and child connections to be created.
Allow creation of EPMAP skeletons	When this option is selected, the PROFINET IO analyzer will allow parent and child connections to be created for EPMAP-based transactions.
Expiry date of a skeleton	This parameter determines when a skeleton, which was created by a PROFINET IO connection and has become idle, will be deleted. By default, it is set to 60 seconds.

Managing UUIDs

In this grid, you can manage the action (*Allow/Block*) that will be applied to PROFINET IO service categories defined earlier on the firewall.

This service category is identified by a 16-byte UUID (Universal Unique Identifier). Whenever the user scrolls over each category, a tool tip will display its UUID (Universal Unique Identifier).

An action can be applied to a whole service category, or to all service categories entered in the grid (**Modify all operations** button).

Managing operation numbers

In this grid, you can manage the action (*Allow/Block*) that will be applied to PROFINET IO operations (in read or write mode) defined earlier on the firewall and identified by an operation number.

You can assign an action to an operation, to all operations (**Modify all operations** button) or to all read operations entered in the grid (**Modify write operations** button).

Support

Disable intrusion prevention	When this option is selected, the scan of the PROFINET IO protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log every PROFINET IO query	Enables or disables the logging of PROFINET IO requests.
Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

PROFINET RT

Settings

Timeout in seconds for Ethernet connection [2-604800]	This duration is the period after which idle Ethernet connections will be deleted. This value has to be between 2 and 604800 seconds (default value: 60).

Support

Disable intrusion prevention	When this option is selected, the analysis of the PROFINET RT protocol will be disabled and traffic will be allowed if the filter policy allows it.
Log every Ethernet query	Enables or disables the logging of Ethernet requests.

S7

Settings

Max no. of pending requests	Maximum number of requests without responses in a single session. This value has to be between 1 and 512 seconds (default value: 10).
Maximum request duration (in seconds)	This value is the period after which requests without responses will be deleted. This value has to be between 1 and 3600 seconds (default value: 10).
Maximum message size (bytes)	This value makes it possible to restrict the size allowed for a message. It has to be between 11 and 3837 (default value: 960).

Managing function codes

Predefined operations

This table lists the codes and associated S7 operations that have been predefined on the firewall. These codes are classified by operation set: JOB and USERDATA (from different groups).

Predefined S7 operations are allowed by default (*Allow* action). The buttons **Block by operation set**, **Allow by operation set** and **Modify all operations** make it possible to modify the action (*Allow/Block*) applied to the selected operations set or to all S7 operations listed in the table.

Other operations

Other blocked JOBS

This list makes it possible to prohibit additional S7 function codes or code ranges belonging to the JOB operation set. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Other blocked USERDATA groups

This list makes it possible to prohibit whole sets or ranges of whole sets of USERDATA operations. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Support

Disable intrusion prevention	When this option is selected, the analysis of the S7 protocol will be disabled and traffic will be allowed if the filter policy allows it.
Log each S7 request	Enables or disables the logging of S7 requests.

S7 PLUS

Protocol version

Allow v2 protocol	Selecting this option will allow S7 Plus v2 packets to be analyzed If this checkbox is not selected, S7 Plus v2 packets will always be rejected.
Allow v3 protocol	Selecting this option will allow S7 Plus v3 packets to be analyzed If this checkbox is not selected, S7 Plus v3 packets will always be rejected.

Configuring operations

Start PLC	When this checkbox is selected, the firewall will automatically accept any S7 Plus request to start a PLC.
Set date and time	When this checkbox is selected, the firewall will automatically accept any S7 Plus request to set the date and time on a PLC.
Stop PLC	When this checkbox is selected, the firewall will automatically accept any S7 Plus request to shut down a PLC.
Download a program	When this checkbox is selected, the firewall will automatically accept any S7 Plus request to download programs for a PLC.
Send a program	When this checkbox is selected, the firewall will automatically accept any S7 Plus request to send programs for a PLC.

Managing S7 Plus functions

Standard services tab

This grid lists the codes and corresponding S7 Plus functions that have been predefined on the firewall.

Code	S7 Plus code number according to the Siemens naming system.
Service name	Service name assigned to the S7 Plus code according to the Siemens naming system.
Action	Indicates the action applied to the S7 Plus code. This action can either be **Allow** or **Block.**

Possible operations

Enter a filter	Enter numerical characters to filter the list of codes, or alphabetical characters to filter the list of standard services shown in the grid.
Select all	Selects all the lines shown in the grid so that a single action can be assigned to them (**Allow/Block**) by clicking on the relevant button.
Allow selection	Assigns the **Allow** action to the selected line (or to all lines if **Select all** was used).
Block	Assigns the **Block** action to the selected line (or to all lines if **Select all** was used).

Custom services tab

In this grid, you can manage the custom S7 Plus codes and functions that the firewall will automatically accept.

Possible operations

Enter a filter	Enter numerical characters to filter the list of custom service codes shown in the grid.
Select all	Selects all the lines shown in the grid to **Delete** them in a single action by clicking on the relevant button.
Add	Adds a custom S7 Plus service code in the grid.
Delete	Deletes the selected custom S7 Plus service code or all codes if **Select all** was used.

S7 Plus configuration

Max no. of pending requests	Maximum number of requests without responses in a single session. This value has to be between 1 and 512 seconds (default value: 50).
Max. duration of request(s)	This value is the period after which requests without responses will be deleted. This value has to be between 1 and 3600 seconds (default value: 10).

Support

Disable intrusion prevention	When this option is selected, the analysis of the S7 Plus protocol will be disabled and traffic will be allowed if the filter policy allows it.
Log each S7 Plus request	Enables or disables the logging of S7 Plus requests.

UMAS (IPS) tab

The UMAS (Unified Messaging Application Services) protocol is the intellectual property of Schneider Electric. To ensure the communication between Schneider Electric controllers and software, activate the option sysctl net.link.ether.handle802_3=1 with a command line on the firewalls set up between those elements.

UMAS Parameters

Maximum message size (bytes)	This value makes it possible to restrict the size allowed for a message. It has to be between 10 and 4096 (default value: 1480).
Maximum reservation life time (in seconds, 0 for infinite time)	The reservation mechanism makes it possible to prevent certain behavior-modifying requests from being run at the same time. It is based on a reservation ID that the server randomly defines and returns in the Umas_takePlcReservation response, then uses in the 'Reservation ID' field of commands that the client sends as part of this reservation. Whenever a client reserves a server, reservation requests from other clients will be rejected. Depending on the specifications of the protocol, any unused reservations will be disabled after 50 seconds. Once it has been allocated, a reservation can be used by UMAS requests originating from different TCP connections. Furthermore, the reservation remains valid even after a TCP connection that had been using is shut down, up until its expiration (50 seconds). The value specified in this field therefore makes it possible to shorten the 50-second lifetime set by specifications.

UMAS function codes management

Public operations

This table lists the codes and associated UMAS functions that have been predefined on the firewall. These functions are classified by function group: Application Management, Application download to PLC, Application upload from PLC, Configuration Information requests, Connection Information requests, Debugging, PLC Status commands, PLC Status requests, Read commands, Reservation requests and Write commands.

The **Block by operation set** and **Allow by operation set** buttons make it possible to modify the action (*Allow*/*Block*) that had been applied to the selected operation set.

Other operations allowed

This list allows authorizing additional function codes blocked by default by the firewall. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Support

Disable intrusion prevention	When this option is selected, the scan of the protocol will be disabled and traffic will be authorized if the filter policy allows it.

Microsoft RPC (DCE/RPC) protocol

In order to secure Microsoft RPC traffic based on the DCE/RPC standard, this module allows authorizing or blocking traffic using this protocol, set out in detail by the Microsoft service (Microsoft Exchange, for example).

DCE/RPC (IPS) tab

Like FTP, the DCE/RPC protocol may be used to set up several connections for the same traffic stream: a parent connection from the client to the server over the port dedicated to the service, followed by one or several child connections over random ports for data exchange.

When the DCE/RPC protocol is analyzed, the firewall extracts data from the parent connection in order to create child connections (random ports allowed), so that you obtain a connection skeleton that enables dialog.

Connection skeleton settings

Allow creation of skeletons	When this option is selected, the DCE/RPC analyzer will allow parent and child connections to be created.
Expiry date of a skeleton	This parameter determines when a skeleton, which was created by a DCE/RPC connection and has become idle, will be deleted. By default, it is set to 60 seconds.
Number of skeletons created per address. IP	The number of DCE/RPC skeletons created by the same source IP address can be restricted.

Authentication

Verify user legitimacy	If this option is selected, you will be enabling DCE/RPC user authentication. The DCE/RPC analyzer will then be able to extract the user and compare it against the list of users authenticated on the firewall. When no authenticated user matches the user submitted in the DCE/RPC query, the packet will be blocked.

Microsoft Remote Procedure Call (RPC)

"Predefined MS-RPC services" tab

The DCE/RPC protocol allows remotely hosted procedures to be launched. These services, known as MS-RPC, which have been predefined for the main Microsoft applications, are allowed by default.

These services, classified by category, can be allowed/blocked individually or in groups by selecting several categories using the *Shift* key together with the buttons available in the *Action* menu. The "Modify all operations" button makes it possible to assign the action to all service categories. The "Block by service group" and "Allow by service group" buttons make it possible

to modify the action assigned to a full group of services. Prohibited services will raise the alarm "DCERPC forbidden service".

Whenever the user scrolls over each service, a tooltip will display its UUID (Universal Unique Identifier).

The main Microsoft applications that have predefined MS-RPC services are:

- Distributed File System Replication,
- Microsoft Active Directory,
- Microsoft DCOM,
- Microsoft Distributed Transaction Coordinator service,
- Microsoft Exchange,
- Microsoft File Replication service,
- Microsoft IIS,
- Microsoft Inter-site Messaging,
- Microsoft Messenger,
- Microsoft Netlogon,
- Microsoft Scheduler,
- Microsoft RPC services,
- Windows Management Instrumentation Remote Protocol.

"Customized MS-RPC services" tab

This table allows you to enter the universal unique identifiers (UUID) of MS-RPC services that were not entered in the list of predefined MS-RPC services. Similarly to the first tab, you can assign an action to a service, to all services ("Block by service group" and "Allow by service group" buttons) or to all services entered ("Modify all operations" button).

Support

Disable intrusion prevention	When this option is selected, the analysis of the MS-RPC protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log every MS-RPC query	Enables or disables the logging of MS-RPC requests.
Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

NETBIOS EPMAP (IPS) tab

This protocol allows launching procedures that are remotely hosted (bootstrap) through the distribution of an MS-RPC service's IP address and protocol. The options of this module may restrict the use of these relays. Dynamic connections can be opened on EPMAP (portmapper).

Skeletons

As this protocol is used for relaying access to Microsoft services, the following options allow restricting the services and options relayed by the EPMAP server.

Skeletons can be created only if the address returned in the DCE/RPC response is the same as the server's address	Select this checkbox to allow EPMAP services to create connection skeletons. It is selected by default.
Skeletons can be created only for Microsoft Exchange UUIDs	If this option has been selected, only **Microsoft Exchange** services will be able to create connection skeletons.

OPC AE (IPS) tab

OPC AE general settings

This table lists the OPC AE (OPC Alarms and Events) services that have been predefined on the firewall. These services are classified by service set:

- Component Categories,
- OPC Events,
- OPC Type Library.

Predefined OPC AE services are allowed (analyzed) by default (*Allow* action). The buttons **Block by service set**, **Allow by service set** and **Modify all services** make it possible to modify the action (*Allow/Block*) applied to the selected service set or to all OPC AE services listed in the table.

OPC DA (IPS) tab

Grid of operations and operation groups

This table lists the OPC DA operations that have been predefined on the firewall. The various types of information for each operation/operation group are:

- **Name**: name of the operation or group of operations.
- **Operation no.**: numerical identifier of the operation in its group.
- **Action**: action applied to the network packet corresponding to the operation (*Allow/Block*)
- **Type**: indicates whether it is a *read* or *write* operation.

Possible operations

Predefined OPC DA operations are allowed by default (*Allow* action). The buttons **Block the selection**, **Allow the selection** and **Modify all write ops** make it possible to change the action (*Allow/Block*) applied to the selected operation, selected operation set or to all OPC DA write operations listed in the grid.

OPC HDA (IPS) tab

OPC HDA general settings

This table lists the OPC HDA (OPC Historical Data Access) services that have been predefined on the firewall. These services are classified by service set:

- Component Categories,
- OPC Browser,
- OPC Client,
- OPC Server
- OPC Type Library.

Predefined OPC HDA services are allowed (analyzed) by default (*Allow* action). The buttons **Block by service set**, **Allow by service set** and **Modify all services** make it possible to modify the action (*Allow/Block*) applied to the selected service set or to all OPC HDA services listed in the table.

NetBios CIFS (IPS tab)

NetBios is a protocol that is used for sharing files/printers, generally by Microsoft systems.

NetBIOS CIFS:Maximum size of elements (bytes)

Name of files (SMB2 format)	This number has to be between 1 and 65536 bytes. This file name size (**SMB2 - ioctl referral request**) is set by default to 61640 to protect the system from the vulnerability CVE 2009-2526.

Microsoft RPC (DCE/RPC)

Inspect Microsoft RPC (DCE/RPC) protocol	As the DCE/RPC protocol can be encapsulated in this protocol, this option allows enabling or disabling its inspection.

Authentication

Verify user legitimacy	If this option is selected, you will be enabling user authentication via the CIFS header. The CIFS plugin will therefore be capable of extracting the user ID and comparing it against the list of users authenticated on the firewall. When no authenticated users match, the packet will be blocked.

Support

Disable intrusion prevention	When this option is selected, the scan of the NetBios CIFS protocol will be disabled and traffic will be authorized if the filter policy allows it.
Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

NETBIOS EPMAP (IPS) tab

This protocol allows launching procedures that are remotely hosted (bootstrap) through the distribution of an MS-RPC service's IP address and protocol. The options of this module may restrict the use of these relays. Dynamic connections can be opened on EPMAP (portmapper).

Skeletons

As this protocol is used for relaying access to Microsoft services, the following options allow restricting the services and options relayed by the EPMAP server.

Skeletons can be created only if the address returned in the DCE/RPC response is the same as the server's address	Select this checkbox to allow EPMAP services to create connection skeletons. It is selected by default.
Skeletons can be created only for Microsoft Exchange UUIDs	If this option has been selected, only **Microsoft Exchange** services will be able to create connection skeletons.

NetBios SSN

The screens are the same as for the previous protocol, except that they allow configuring the NetBios SSN protocol, making it possible to exchange messages in connected mode.

MGCP (IPS tab)

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

MGCP session parameters

Maximum command size (bytes)	A command can contain between 32 and 1024 bytes.
Max no. of parameters per command	The number of parameters that can appear in a command has to be between 32 and 1024 bytes.
Maximum SDP parameter size (bytes)	The SDP parameter automatically validates the launch of applications in a session from the client's www or by mail. Its size has to be between 32 and 1024 bytes.
Maximum idle time (seconds)	The maximum idle duration for a session has to be between 60 and 604800 bytes.

Support

Disable intrusion prevention	When this option is selected, the scan of the MGCP protocol will be disabled and traffic will be authorized if the filter policy allows it

RTCP (IPS tab)

RTCP commands

Allowed RTCP commands tab

RTCP commands can be defined in the intrusion prevention module, by clicking on Add. They are limited to 115 characters and can be deleted when needed.

Prohibited RTCP commands tab

RTCP commands can be prohibited in the intrusion prevention module, limited to 115 characters.

Support

Disable intrusion prevention	When this option is selected, the scan of the RTCP protocol will be disabled and traffic will be authorized if the filter policy allows it

RTP (IPS tab)

List of supported RTP codecs

This list contains the RTP codecs supported by default.

You can add codecs by clicking on the appropriate button or remove them from the list by selecting them and clicking on “Delete”.

Support

Disable intrusion prevention	When this option is selected, the scan of the RTP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every RTP query	Enables or disables the logging of RTP requests.

RTSP

RTSP is an application-level communication protocol for media streaming systems. It allows monitoring a media server remotely, offering typical audio/video player features such as “play” and “pause” and allows time-based access.

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

RTSP commands

Allowed RTSP commands tab

Add	Inserts a command in the list of additional commands that require authorization.
Delete	Select the command to remove from the list and click on **Delete**.

Prohibited RTSP commands tab

Add	Inserts a command to the list of additional prohibited commands.
Delete	Select the command to remove from the list and click on **Delete**.

Maximum size of elements (bytes)

RTSP requests	Maximum size of the request and the response. Allows managing memory overflow.
RTSP header	Maximum size of the header. Allows managing memory overflow.
SDP protocol	Maximum size of an SDP line. Allows managing memory overflow.
Content-Type	Maximum size of the « Content-Type » header.

RTSP session settings

Max no. of pending requests	Maximum number of requests without responses in a single RTSP session.
Session timeout (seconds)	Duration of a RTSP session in seconds.
Request timeout (seconds)	Duration of a RTSP request in seconds.

RTSP features

Allow interleaving	If this option is selected, RTSP will be allowed to encapsulate within its own TCP connection RTP/RTCP protocols used for transporting media and usually based on UDP. This may be necessary when UDP traffic is denied.
Allow error messages with content	This option allows accepting error messages containing additional content, in general in HTML.
Allow renegotiation of media transport settings	If this option is selected , the firewall will allow the update of RTP/RTCP transport parameters during a session.

Support

Disable intrusion prevention	When this option is selected, the scan of the RTSP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every RTSP query	Enables or disables the logging of SIP requests.

SIP (IPS tab)

The SIP protocol performs protocol analyses and dynamically authorizes secondary connections. Connections are scanned line by line – the line must be complete before the scan can be launched. For each line containing a header, a check will be performed according to the status of the automaton.

- Verification of the SIP version and the operation, validation of the URI that must be encoded in UTF-8. For requests and responses:

  Line-by-line analysis of the header: validation of the header fields and the extraction of information (e.g. name of the caller and callee), protection from attacks (encoding, buffer overflow, presence and order of mandatory fields, line format, etc).

  Analysis and validation of data presented in the SDP (encoding, buffer overflow, RFC compliance, presence and order of mandatory fields, line format, etc).
- For responses (in addition to the earlier checks): overall consistency of the response with the request.
  The audit feature includes a session group identifier that will enable locating all the connections by conversation, by name of caller and callee and by type of medium used (audio, video, application, data, control, etc).

Automatically detect and inspect the protocol	If the protocol has been enabled, the inspection will be automatically applied to the discovery of the corresponding traffic allowed by the filter.

SIP methods

SIP methods allowed tab

Add	Inserts additional methods that require authorization.
Delete	Select the method to be removed from the list and click on **Delete**.

SIP methods prohibited tab

Add	Inserts additional prohibited methods.
Delete	Select the method to be removed from the list and click on **Delete**.

Maximum size of elements (bytes)

SIP request [64-4096]	Maximum size of the request and the response. Allows managing memory overflow.

SIP header [64-4096]	Maximum size of the header. Allows managing memory overflow.
SDP protocol [64-604800]	Maximum size of an SDP line. Allows managing memory overflow.

SIP session parameters

Max no. of pending requests [1-512]	Maximum number of requests without responses in a single SIP session.
Session timeout (seconds) [60-604800]	Duration of a SIP session in seconds.

SIP protocol extensions

Enable extension INFO (RFC2976)	The INFO extension allows exchanging information during a call in progress. **EXAMPLE** The strength of a peer's Wi-Fi signal. Select this option to enable the extension.
Enable extension PRACK (RFC3262)	Two types of responses are defined by SIP: temporary and permanent. The PRACK extension allows providing a reliable recognition system and guaranteeing a sequenced delivery of temporary responses in SIP. Select this option to enable the extension.
Enable extensions SUBSCRIBE, NOTIFY (RFC3265)	The SIP protocol includes a normalized mechanism to allow any client (a telephone in VoIP being an example of a SIP client) to monitor the status of another device. If client Device A wants to be informed of changes to the status of Device B, it will send a SUBSCRIBE request directly to Device B or to a server that indicates Device B's status. If the SUBSCRIBE request is successful, every time Device B's status changes, Device A will receive a SIP NOTIFY message indicating the change in status or providing information about the event. When one device subscribes to another, it will be informed when an event occurs. **EXAMPLE** Onlining of contacts that it is looking for. Select this option to enable the extension.
Enable extension UPDATE (RFC3311)	The UPDATE extension allows a client to update session parameters even before the session has been set up, such as all media traffic and their codecs. Select this option to enable the extension.

Enable extension MESSAGE (RFC3428)	The MESSAGE extension is an extension of the SIP protocol, allowing the transfer of instant messages. Since the MESSAGE request is an extension of SIP, it inherits all the security and progress features included in this protocol. The contents of MESSAGE requests are in MIME format. Select this option to enable the extension.
Enable extension REFER (RFC3515)	The REFER extension is used in particular for the transfer or redirection of calls. If Peer A tries to contact Peer B who is not available, A will be redirected to Peer C, who will act as B's "referrer". Select this option to enable the extension.
Enable extension PUBLISH (RFC3903)	The PUBLISH extension allows publishing the status of events to a recipient. Select this option to enable the extension.
Enable support for PINT protocol	This extension allows SIP telephones to coexist with non-IP services (fax, etc.). Select this option to enable the extension.
Enable support for Microsoft Messenger (MSN)	This option allows enabling support for Microsoft Windows Messenger.

Support

Disable intrusion prevention	When this option is selected, the scan of the SIP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every SIP request	Enables or disables the logging of SIP requests.

SOFBUS/LACBUS (IPS) tab

The SOFBUS/LACBUS protocols are the intellectual property of LACROIX Sofrel.

SOFBUS/LACBUS are industrial application protocols that are mainly used in water management infrastructures to conduct remote management, i.e., monitoring and controlling industrial sites remotely.

These protocols are encapsulated in the MODBUS protocol, which is also an industrial application protocol that uses TCP as its transport protocol.

Enable SOFBUS/LACBUS analysis in MODBUS packets	Enables or disables the analysis of the SOFBUS/LACBUS protocol in MODBUS packets. The default configuration of the SOFBUS/LACBUS analysis in the firewall complies with LACROIX Sofrel specifications.

Managing Information units (IU) and SOFBUS or LACBUS blocks

The grid lists the Information units (IU) and SOFBUS or LACBUS blocks. Each IU may contain several blocks. Each item has a name, letter, action and type.

IUs and blocks are created by default in the configuration, and can be identified by their type: *Default IU* or *Default block*. These can be found in the technical characteristics provided by LACROIX Sofrel and therefore make up the default configuration. They cannot be renamed, moved or deleted, but the associated action can be changed for: *Allow* or *Block.*

The default configuration can be customized when necessary. The **Add an IU or a block** button makes it possible to add a *Custom IU* or *Custom block* to an existing IU. There are rules regarding the use of letters:

- IU letter: must be in uppercase. No two IUs can have the same letter.
- Block letter: can be uppercase or lowercase. No two blocks in the same IU can have the same uppercase or lowercase letter (case sensitive).

Custom IUs and block can be renamed and moved as long as the rules on the use of letters are followed, but the associated action cannot be changed.

The **Delete** button makes it possible to delete a *Custom IU* or *Custom block*. *Default IUs* and *Default blocks* cannot be deleted.

DNS (IPS tab)

Maximum size of DNS fields (in bytes)

DNS name (query)	This field has to be between 10 and 2048 bytes.

Size of DNS messages

Enable detection of large messages	This checkbox makes it possible to enable (or disable) the option that checks the length of DNS messages in order to generate alarms when messages exceed a specified threshold.
Threshold before "DNS message too large" alarm is raised [0-65535] (in bytes)	Indicate the size above which a DNS message will be considered potentially suspicious and trigger the "DNS message too large" alarm. This size is expressed in bytes.

DNS request parameters (in seconds)

Maximum request duration	This value is the period after which DNS requests without responses will be deleted. It can vary from 1 to 60 seconds, but has been set to 3 seconds by default.

Whitelist of DNS domains (DNS rebinding)

List of domain names

This list contains the allowed domain names (<*www.domainname.fr*>, for example) to be resolved by a server located on an unprotected interface.

You can add codecs by clicking on the appropriate button or remove them from the list by selecting them and clicking on **Delete**.

To prevent false positives, this list contains the domain name of the Windows DNS service by default (msftncsi.com).

DNS registration types

Known types to be prohibited tab

This is a list of the known DNS types (A, A6, AAAA, CNAME, etc) and their associated codes. The firewall allows and analyzes these DNS types by default .

The action (*Allow/ Block*) applied to a DNS type can be changed by clicking on the *Action* column corresponding to this type.

The **Select all** button makes it possible to change the action *(Allow/Block*) applied to all DNS types.

Additional types to be prohibited tab

This list makes it possible to block additional DNS types (identified by their codes). It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Support

Disable intrusion prevention	When this option is selected, the scan of the DNS protocol will be disabled and traffic will be authorized if the filter policy allows it

FTP

The FTP plugin supports the main RFC [RFC959] as well as many extensions.

Enabling this plugin allows the prevention of large families of FTP-based application attacks. This plugin performs various analyses such as the RFC compliance analysis, checks on FTP command parameter size or restrictions on the protocol (SITE EXEC for example). These analyses therefore allow stopping attacks such as FTP Bounce, FTP PASV DoS, Buffer overflow, etc. This plugin is indispensable when allowing FTP traffic to pass through the firewall and to dynamically manage FTP data connections.

IPS tab

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

Authentication

Allow SSL authentication	Enables SSL authentication for the protocol (FTP only). By selecting this option, personal data such as the login and password may be encrypted and therefore, protected.
Do not scan the FTP authentication phase	No data scans will be performed

Size of elements (in bytes)

Imposing a maximum size for elements (in bytes) allows countering buffer overflow attacks.

Username	Maximum number of characters that a user name can contain. This value must be between 10 and 2048 bytes.
User password	Maximum number of characters for the FTP password. This value must be between 10 and 2048 bytes.
Path (directory + filename)	Maximum number of characters of the path taken by the program execution, or the path taken in the directory to reach the FTP file. This value must be between 10 and 2048 bytes.
SITE command	Maximum number of characters that the SITE command can contain (between 10 and 2048 bytes).
Other commands	Maximum number of characters that additional commands can contain (between 10 and 2048 bytes)

Support

Disable intrusion prevention	When this option is selected, the scan of the FTP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every FTP query	Enables or disables the reporting of FTP logs.

Proxy tab

Filter the welcome banner sent by the FTP server	If this option is selected, the server's banner will no longer be sent during an FTP connection.
Block FTP bounce	Allows the prevention of IP address spoofing. By executing the PORT command and by specifying an internal IP address, an external host may access confidential data by exploiting vulnerabilities in an FTP server or a host that is vulnerable to bounces.

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP address of the web client that sent the packet. Otherwise, the firewall's address will be used.

Allowed transfer modes

Between the client and the proxy	When the FTP client sends a request to the server, the proxy will first intercept the request in order to analyze it. From the FTP "client"'s point of view, the proxy corresponds to the server. This option defines the allowed transfer mode. • If **Active only** is specified, the FTP client will determine the connection port to use for transferring data. The FTP server will then initialize the connection from its data port (port 20) to the port specified by the client. • If **Passive only** is specified, the FTP server will determine the connection port to use for transferring data (data connection) and will transmit it to the client. • If **Active and passive** is specified, the FTP client will be able to choose between both transfer modes when configuring the firewall.
Between the proxy and the server	When the proxy has finished scanning the client request, it will transfer it to the FTP server, which will then interpret the proxy as the FTP client. Since the proxy has an intermediary role, it is transparent. The allowed transfer modes are the same as for the previous option.

FTP Commands tab

Proxy

Main commands tab

Command	Name of the command.
Action	3 authorizations possible from "Pass without scanning", "Allow" and "Block".
Command type	Indicates the type of command. "Writing" FTP commands defined in the RFCs can cause changes in the server, such as the deletion of data or even the creation of folders. sThese commands operate in the same way as for "generic" commands – you can allow or prohibit a command or check that the command syntax complies with the RFC in force.

Other commands allowed tab

Where necessary, users can **Add** or **Delete** additional commands up to a limit of 21 characters.

IPS

Allowed FTP commands tab

FTP commands, limited to 115 characters, can be defined in the intrusion prevention module, by clicking on **Add**. They are limited to 115 characters and can be deleted when needed.

Prohibited FTP commands tab

FTP commands, limited to 115 characters, can be prohibited in the intrusion prevention module.

List of generic FTP commands and details of filtering

- **ABOR**: Command that interrupts the transfer in progress. This command does not accept arguments. By default, it will be analyzed to check RFC compliance.
- **ACCT**: Command that specifies the account to be used for connecting. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.
- **ADAT**: Command that sends security data for authentication. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.

- **AUTH**: Command that selects the security mechanism for authentication. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.
- **CCC**: Command that allows unprotected messages.
- **CDUP**: Command that modifies the parent working folder. This command does not accept arguments. . By default, it will be analyzed to check RFC compliance.
- **CONF**: Command that specifies the "confidential" message used for authentication.
- **CWD**: This command modifies the working folder. This command accepts one or several arguments. By default, it will be analyzed to check RFC compliance.
- **ENC**: This command specifies the "private" message used for authentication. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.
- **EPRT**: This command enables the extended active transfer mode. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.
- **EPSV**: This command selects the extended passive transfer mode. This command has to be executed with at most one argument. This command is blocked by default.
- **FEAT**: This command displays the extensions supported by the server and does not accept arguments. The result of this command is filtered by the proxy if filtering has been requested on the FEAT command.
- **HELP**: This command returns the details for a given command. This command has to be executed with at most one argument. By default, it will be analyzed to check RFC compliance.
- **LIST**: This command lists the contents of a data location in a friendly way.
- **MDTM**: This command displays the date of the last modification for a given file. This command accepts one or several arguments. By default, it will be analyzed to check RFC compliance.
- **MIC**: This command specifies the "safe" message used for authentication. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.
- **MLSD**: This command displays the contents of the normalized folder. By default, it will be analyzed to check RFC compliance.
- **MLST**: This command displays the information of the normalized folder. By default, it will be analyzed to check RFC compliance.
- **MODE**: This command specifies the transfer mode. By default, it will be analyzed to check RFC compliance. This command is the object of a greater filter and is only allowed with the arguments S, B, C and Z. If the antivirus analysis has been enabled, only argument S will be allowed.
- **NLST**: This command lists the contents of a data location of the computer in a friendly way. By default, it will be analyzed to check RFC compliance.
- **NOOP**: This command does not do anything and does not accept arguments. By default, it will be analyzed to check RFC compliance.
- **OPTS**: This command specifies the status options for the given command. This command accepts one or several arguments. By default, it will be analyzed to check RFC compliance.
- **PASS**: This command specifies the password used for the connection. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.
- **PASV**: This command selects the passive transfer mode. This command does not accept arguments. By default, it will be analyzed to check RFC compliance.
- **PBSZ**: This command specifies the size of encoded blocks. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.

- **PORT**: This command selects the active transfer mode. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.
- **PROT**: This command specifies the level of protection. By default, it will be analyzed to check RFC compliance. This command is the object of a greater filter and is allowed only with the arguments C, S E and P.
- **PWD**: This command displays the current working folder. This command does not accept arguments. By default, it will be analyzed to check RFC compliance.
- **QUIT**: This command terminates the session in progress and the connection. By default, it will be analyzed to check RFC compliance.
- **REIN**: This command ends the session in progress (initialized with the user). By default, it will be analyzed to check RFC compliance.
- **REST**: This command specifies the offset that the transfer has to catch up with. By default, it will be analyzed to check RFC compliance. This command is the object of a greater filter and is prohibited if the antivirus scan is running. Otherwise, the proxy will check that a single argument is present.
- **RETR**: This command retrieves a given file. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance
- **SITE**: This command executes a command specific to the server. This command accepts only a single argument. By default, it will be analyzed to check RFC compliance.
- **SIZE**: This command displays the transfer size for a given file. This command accepts one or several arguments. By default, it will be analyzed to check RFC compliance.
- **SMNT**: This command modifies the data structure of the system in progress. This command accepts one or several arguments. By default, it will be analyzed to check RFC compliance.
- **STAT**: This command displays the current status. By default, it will be analyzed to check RFC compliance.
- **STRU**: This command specifies the structure of transferred data. By default, it will be analyzed to check RFC compliance. This command is the object of a greater filter and is allowed only with the arguments F, R and P. If the antivirus scan has been enabled, only the argument F will be allowed.
- **SYST**: This command displays the information about the server's operating system. This command does not accept arguments. By default, it will be analyzed to check RFC compliance.
- **TYPE**: This command specifies the type of data transferred. By default, it will be analyzed to check RFC compliance. This command is the object of a greater filter and is allowed only with the arguments ASCII, EBCDIC, IMAGE, I, A, E and L. If the antivirus scan has been enabled, only the arguments ASCII, IMAGE, I and A will be allowed. The option L may be followed by a digital argument. The option L may be followed by a digital argument. The options E, A, EBCDIC and ASCII accept the following arguments: N, C and T.
- **USER**: This command specifies the name of the user for connecting.
- **XCUP**: This command modifies the parent working folder. This command does not accept arguments. By default, it will be analyzed to check RFC compliance.
- **XCWD**: This command modifies the working folder. This command accepts one or several arguments. By default, it will be analyzed to check RFC compliance.
- **XPWD**: This command displays the current working folder. This command does not accept arguments. By default, it will be analyzed to check RFC compliance.

List of FTP modification commands and details of filtering

- **ALLO**: This command allocates the storage space on this server and accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.
- **APPE**: This command adds (or creates) to the data location. This command is the object of a greater filter Indeed, this command is prohibited if the antivirus scan has been enabled (risk of bypass). Otherwise, the presence of at least one argument will be checked for.
- **DELE**: This command deletes a given file and accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.
- **MKD**: This command creates a new folder and accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.
- **RMD**: This command deletes the given folder and accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.
- **RNFR**: This command selects a file that has to be renamed and accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.
- **RNTO**: This command specifies the new name of the selected file and accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.
- **STOR**: This command stores a given file and accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.
- **STOU**: This command stores a given file with a unique name. This command does not accept arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.
- **XMKD**: This command creates a new folder and accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.
- **XRMD**: This command deletes the given folder and accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option "Enable modification commands" has been enabled. Otherwise, the command will be blocked.

FTP Users tab

List of users

Allowed users tab

FTP users can be defined in the intrusion prevention module (limited to 127 characters) by clicking on **Add**. They are limited to 115 characters and can be deleted when needed.

Denied users tab

FTP users can be prohibited in the intrusion prevention module (limited to 127 characters) by clicking on **Add**. They are limited to 115 characters and can be deleted when needed.

Analyzing files tab

Maximum size for antivirus and sandboxing analysis (KB)	In this field, you can set the maximum size used to analyze files, and configure the action to take if the file exceeds the allowed size. **WARNING** When a size limit is manually set for analyzed data, ensure that all values are consistent, as the total memory space corresponds to the resources reserved for all antivirus services. If you define the size limit for data analyzed over FTP as 100% of the total size, no other files can be analyzed at the same time. This option corresponds to the maximum size of files that will be scanned. The default size depends on the firewall model : • SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SN510, SN710, SNi10, SNi20, SNi40, EVA1, EVA2 and EVA3 : 4000 Ko. • SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SNxr1200 and EVA4 : 8000 Ko. • SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200 and EVAU : 16000 Ko.
Analyzing files	This option makes it possible to choose the type of file that needs to be analyzed: “downloaded and sent” files; “downloaded only” or “sent only” files.

Actions on files

When a virus is detected	This field contains two options: "Allow" and "Block". By selecting “Block”, the analyzed file will not be sent. By selecting “Allow”, the antivirus will send the file as is.
When the antivirus scan fails	This option defines the behavior of the antivirus module if the analysis of the file it is scanning fails. **EXAMPLE** The file could not be scanned as it is locked. If **Block** is specified, the file being scanned will not be sent. If **Pass without scanning** is specified, the file being scanned will be sent.
When data collection fails	This option defines the behavior of the antivirus module when certain events occur. It is possible to **Block** traffic when information cannot be retrieved, or **Pass without scanning**.

Sandboxing tab

Sandboxing

Status	This column displays the status (**Enabled**/**Disabled**) of sandboxing for the corresponding file type. Double-click on it to change its status.

Type	The sandboxing option allows scanning four types of files: • **Archive**: these include the main types of archives (zip, arj, lha, rar, cab, etc) • **Office document (Office software)**: all types of documents that can be opened with the MS Office suite. • **Executable**: files that can be run in Windows (files with the extension ".exe",".bat",".cmd",".scr", etc). • **PDF**: files in *Portable Document Format* (Adobe) • **Javascript** (files with a ".js" extension). • **Java** (Java compiled files. E.g.: files with a ".jar" extension). • **Others**.

Actions on files

When known malware has been identified	This field contains two options. By selecting "Block", the analyzed file will not be sent. By selecting "Allow", the file will be sent in its original form.
When sandboxing fails	This option defines the behavior of the sandboxing option if the file scan fails: • If **Block** is specified, the file being scanned will not be sent. • If **Pass without scanning** is specified, the file being scanned will be sent.

HTTP

This plugin allows preventing large families of HTTP-based application attacks. The various analyses that this plugin performs (in particular RFC compliance checks), validation of encoding in URLs or checks on URL size or requests, allow you to block attacks such as Code RED, Code Blue, NIMDA, HTR, WebDav, Buffer Overflow or even Directory Traversal…

Managing buffer overflows is fundamental at Stormshield Network, which is why defining the maximum sizes allowed for HTTP buffers is particularly detailed.

IPS tab

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

Search engine options

Enable search engine filter (Safesearch)	This mechanism allows excluding websites, documents or images that are explicitly inappropriate or undesirable from the results of web searches conducted on the main search engines (Google, Bing, Yahoo)

YouTube content restriction	In this field, the type of restriction to be placed on results of video searches on the YouTube platform can be selected: • "Strict" means that inappropriate videos can be filtered, • "Moderate" will return the most relevant results and may therefore allow the display of inappropriate videos.
Google services and accounts allowed	This option restricts access to Google services and accounts by entering only allowed domains in this list. Enter the domain with which you have signed up to Google Apps, as well as any secondary domains you might have added to it. Users accessing Google services from unauthorized accounts will be redirected to a Google block page. The way this option works is the firewall intercepts SSL traffic toward Google and adds the HTTP header "X-GoogApps-Allowed-Domains" to it, the value of which is the list of allowed domain names, separated by commas. For more information, please refer to the following link: FR https://support.google.com/a/answer/1668854?hl=fr EN https://support.google.com/a/answer/1668854?hl=en **NOTE** SSL inspection has to be enabled in the filter policy for this feature to work.

HTML/JavaScript analyses

Inspect HTML code	Any page containing HTML content that is likely to be malicious will be blocked.
Max. length for a HTML tag (Bytes)	Maximum number of bytes for an attribute of a HTML tag (Min: 128; Max: 65536).
Inspect JavaScript code	In order to prevent malicious content from damaging dynamic and interactive web pages that use JavaScript programming, a scan will be conducted in order to detect them. In the same way as for the option **Inspect HTML code**, if this option is selected, a page containing JavaScript content that is likely to be malicious will be blocked.
Automatically delete malicious content	Instead of prohibiting the TCP connection, the scan will erase the malicious content (e.g. attribute, HTML marker) and allow the rest of the HTML page to pass through. **EXAMPLE OF MALICIOUS BEHAVIOR** Redirection without your knowledge, to a website other than the site you had intended to visit. **NOTE** Selecting this checkbox will disable the **Enable on-the-fly data decompression** option.

Enable on-the-fly data decompression	When HTTP servers present compressed pages, enabling this option will allow decompressing data and inspecting it as and when it passes through the firewall. Since no data will be rewritten, this operation will not cause any additional delay. **NOTE** Selecting this checkbox will disable the **Automatically delete malicious content** option

List of exceptions to the automatic deletion of malicious code (User-Agent)

This list displays the browsers and their data, which will not be automatically deleted by the earlier option mentioned above. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

Authentication

Verify user legitimacy	If this option is selected, you will be enabling user authentication via the HTTP "Authorization" header. The HTTP plugin will therefore be capable of extracting the user and comparing it against the list of users authenticated on the firewall. When no authenticated users match, the packet will be blocked.

Advanced properties

URL: maximum size of elements (in bytes)

Imposing a maximum size for elements (in bytes) allows countering buffer overflow attacks.

URL (domain+path)	Maximum size of a URL, domain name and path inclusive [128 – 4096 bytes]
Per parameter (after the '?' [argument])	Maximum size of a parameter in a URL [128 – 4096 (bytes)]
Full query (URL + parameters)	Maximum number of bytes for the full query: http://URLBuffer ?QueryBuffer [128 – 4096] (bytes)]

URL

Max. nb of parameters (after '?')	Maximum number of parameters in a URL (Min: 0; Max: 512).

HTTP headers: maximum size of elements (in bytes)

Number of lines per client request	Maximum number of lines (or headers) that a request can contain, from the client to the server (Min:16; Max: 512).
Number of ranges per client request	Maximum number of ranges that a response can contain, from the server to the client (Min:0 ; Max: 1024).
Number of lines per server response	Maximum number of lines (or headers) that a response can contain, from the server to the client (Min:16; Max: 512).

Maximum size of HTTP headers (in Bytes)

Authorization field	Maximum number of bytes for the AUTHORIZATION field, including formatting attributes. (Min: 128; Max: 4096).
Content-Type field	Maximum number of bytes for the CONTENTTYPE field, including formatting attributes. (Min: 128; Max: 4096).
Host field	Maximum number of bytes for the HOST field, including formatting attributes. (Min: 128; Max: 4096).
Cookie field	Maximum number of bytes for the COOKIE field, including formatting attributes. (Min: 128; Max: 8192).
Other fields	Maximum number of bytes for other fields, including formatting attributes. (Min: 128; Max: 4096).
Authorization - Bearer field	Maximum number of bytes for the AUTHORIZATION - Bearer field, including formatting attributes. (Min: 128; Max: 4096).
Authorization - Negotiate field	Maximum number of bytes for the AUTHORIZATION - Negotiate field, including formatting attributes. (Min: 128; Max: 4096).
Authorization (NTLM) field	Maximum number of bytes for the AUTHORIZATION (NTLM) field, including formatting attributes. (Min: 128; Max: 4096).
Content-Security-Policy field	Maximum number of bytes for the CONTENT-SECURITY-POLICY field, including formatting attributes. (Min: 128; Max: 65535).

HTTP session parameters (in seconds)

Maximum request duration	Set to 30 seconds by default (Max: 600 seconds).

HTTP protocol extensions

Allow Shoutcast support	This option allows transporting sound over HTTP. **EXAMPLES** Webradio, webtv.
Allow WebDAV connections (reading and writing)	This option allows adding writing and locking features to HTTP, and also allows securing HTTPS connections more easily.

Allowed HTTP commands tab

List of allowed HTTP commands (in CSV format). All commands included may not exceed 126 characters. It is possible to **Add** or **Delete** commands using the respective buttons.

Prohibited HTTP commands tab

List of prohibited HTTP commands (in CSV format). All commands included may not exceed 126 characters. It is possible to **Add** or **Delete** commands using the respective buttons.

Support	
Disable intrusion prevention	When this option is selected, the scan of the HTTP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every HTTP query	Enables or disables the logging of HTTP requests.

Proxy tab

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP address of the web client that sent the packet. Otherwise, the firewall's address will be used.

URL Filtering (Extended Web Control base only)

Allow IP addresses in URLs	This option makes it possible to allow or deny the use of IP addresses in the URL, meaning access to a website by its IP address instead of its domain name. Such a method may be an attempt to bypass URL filtering. If the option has not been selected and the URL queried (containing an IP address) cannot be classified by the URL filtering system, its access will be blocked. However, this option has been designed to be applied after the evaluation of the filter. As a result, internal servers that are contacted by their IP addresses will not be blocked if their access has been explicitly allowed in the filter policy (different from the pass all policy). Such access can be allowed via the firewall's basic Network objects (RFC5735) or the "Private IP" group in the EWC URL database.

Extended web control URL base provider	
Action when classification of URL failed	The choice is either **Allow** or **Block**. If a URL has not been listed in a URL category, this action will determine whether access to the site will be allowed.

> **NOTE**
> Regardless of whether the previous option has been selected, an IP address expressed differently from the format *a.b.c.d* will be systematically blocked.

HTTP protocol extensions

Allow WebDAV connections (reading and writing)	WebDAV is a set of extensions to the HTTP protocol concerning the edition and collaborative management of documents. If this option has been selected, the WebDav protocol will be allowed on the Stormshield Network Firewall.
Allow TCP tunnels (CONNECT method)	The **CONNECT method** builds secure tunnels through proxy servers. If this option has been selected, the **CONNECT** method will be allowed on the Stormshield Network Firewall.

TCP tunnels: List of allowed destination ports

In this zone, specify the types of service that can use the **CONNECT** method.

Destination port (service object)	The **Add** button allows you to add services via the objects database. To **modify** a service, select the line to be modified and make changes. Use the **Delete** button to delete the selected service.

Advanced properties

Protection quality

Check URL encoding	By selecting this option, the filter policy cannot be bypassed.

Traffic sent to the server

Add authenticated user to HTTP header	If the external HTTP proxy requires user authentication, the administrator can select this option to send data regarding the user (collected by the firewall's authentication module) to the external proxy.

Explicit proxy

The explicit proxy allows referencing the firewall's proxy in a browser and sending HTTP requests directly to it.

Enable "Proxy-Authorization" (HTTP 407) 'authentication	The browser will prompt the user to authenticate through a message window and the connection information will be relayed to the firewall via the HTTP header. **NOTE** The "Proxy-Authorization" (HTTP 407) authentication method via the browser does not allow the SSL (certificates) and SPNEGO methods as they do not involve the authentication portal, even though it needs to be enabled. For further information, refer to the help for the **Authentication** module, in the section "Transparent or explicit HTTP proxy and Multi-user networks"

ICAP tab

HTTP response (reqmod)

The ICAP protocol targets mainly web and mail content. It provides HTTP proxies (for web) and SMTP relays (for mail) with an interface.

Send HTTP requests to the ICAP server	Each client request to a website is sent to the ICAP server.

ICAP server

Server	Indicates the ICAP server.
ICAP port	Indicates the ICAP port.
Name of ICAP service	Indicates the name of the service to set up. This information varies according to the solution used, the ICAP server as well as the port used.

Authentication on the ICAP server

Information available on the firewall can be used for performing ICAP services.

Example

It is possible to define in an ICAP server that a certain site is intended for a certain user. In this case, you will be able to filter according to an LDAP ID or an IP address.

Send the username / group name	This option allows using information relating to the LDAP base (especially the logins of authenticated users).
Send client's IP address	This option allows using IP addresses of HTTP clients who send requests to Adapter (object used for translating between the ICAP format and the requested format).

Advanced properties

Whitelist (will not be sent to the ICAP server)

HTTP server (Host – Network – Address range)	Adds hosts, networks or address ranges whose details will not be sent to the ICAP server. These items can be deleted from the list at any time.

Analyzing files tab

Transferring files

Partial download	When a download is incomplete, for example, due to a connection failure during a file download via HTTP, the user can continue to download from where the error occurred, instead of having to download the whole file again. This is called a partial download – the download does not correspond to a whole file. The option **Partial download** defines how the firewall's HTTP proxy reacts to such downloads. • **Block**: partial downloads are prohibited • **Block if file analysis is enabled**: partial downloads are allowed except when the traffic corresponds to traffic that is inspected by a rule with an antivirus scan. • **Allow**: partial downloads are allowed but there will not be any antivirus scan.
File size limit (KB)	When files downloaded off the internet via HTTP get too huge, they can affect internet bandwidth for quite a long stretch of time. To avoid this situation, indicate the maximum size (in KB) that can be downloaded via HTTP.
URLs excluded from the antivirus scan	A URL category or category group can be excluded from the antivirus scan. By default, there is a URL group named *antivirus_bypass* in the object database containing Microsoft update sites.

File filter (MIME type)

Status	Indicates whether a file is active or inactive. Two statuses are available: "Enabled" or "Disabled".

Action	Indicates the action to be taken for the file in question, out of three possibilities: • **Detect and block viruses**: The file will be scanned in order to detect viruses that may have infected the files. These viruses will be blocked. • **Pass without analyzing files** The file can be downloaded freely without any antivirus scans. • **Block**: The download is prohibited.
MIME type	Indicates the file content type. This could be text, an image or a video, to be defined in this field. **EXAMPLES** "text/plain*" "text/*" "application/*"
Maximum size for antivirus scan and sandboxing (KB)	This option corresponds to the maximum size of files that will be scanned. The default size depends on the firewall model: • SN160(W), SN210(W), SN310 and EVA1 : 4000 Ko. • SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320, SN510, SN710, SNi10, SNi20, SNi40, EVA2 and EVA3 : 8000 Ko. • SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SNxr1200 and EVA4 : 16000 Ko. • SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200 and EVAU : 32000 Ko.

Actions on files

When a virus is detected	This field contains two options. By selecting "Block", the analyzed file will not be sent. By selecting "Allow", the antivirus will send the file in its original form.
When the antivirus scan fails	This option defines the behavior of the antivirus module if the analysis of the file it is scanning fails. **EXAMPLE** The file could not be scanned as it is locked. If **Block** is specified, the file being scanned will not be sent. If **Pass without scanning** is specified, the file being scanned will be sent.
When data collection fails	This option defines the behavior of the antivirus module when certain events occur. It is possible to **Block** traffic when information cannot be retrieved, or **Pass without scanning**. **EXAMPLE** If the hard disk has reached its capacity, information will not be downloaded.

Sandboxing tab

Sandboxing

Status	This column displays the status (**Enabled**/**Disabled**) of sandboxing for the corresponding file type. Double-click on it to change its status.
Type	The sandboxing option allows scanning four types of files: • **Archive**: these include the main types of archives (zip, arj, lha, rar, cab, etc) • **Office document (Office software)**: all types of documents that can be opened with the MS Office suite. • **Executable**: files that can be run in Windows (files with the extension ".exe",".bat",".cmd",".scr", etc). • **PDF**: files in *Portable Document Format* (Adobe) • **Java** (Java compiled files. E.g.: files with a ".jar" extension). • **Others**.

Actions on files

When known malware has been identified	This field contains two options: • By selecting **Block**, the analyzed file will not be sent. • By selecting **Allow**, the file will be sent in its original form.
When sandboxing fails	This option defines the behavior of the sandboxing option if the file scan fails. • If **Block** is specified, the file being scanned will not be sent. • If **Pass without scanning** is specified, the file being scanned will be sent.

NTP

Network Time Protocol or NTP is a protocol that allows synchronizing local computer clocks with a reference time, via the information network.

From the very beginning, this protocol was designed to offer synchronization precision of less than a second. Compared to the Time Protocol service, which offers a time service without any infrastructure, the NTP project offers a global and universal synchronization solution that can be used worldwide.

IPS tab

Allow version

Select the checkboxes corresponding to the versions of the NTP protocol that you wish to analyze. The packets corresponding to the unselected versions will raise the alarm "NTP: version denied" and will be blocked by the firewall.

Version 1	By selecting this option, you will be enabling the intrusion prevention analysis for NTP version 1.

Version 2	By selecting this option, you will be enabling the intrusion prevention analysis for NTP version 2.
Version 3	By selecting this option, you will be enabling the intrusion prevention analysis for NTP version 3.
Version 4	By selecting this option, you will be enabling the intrusion prevention analysis for NTP version 4.

General settings

Max no. of pending requests	Maximum number of requests without responses in a single NTP session. This value must be between 1 and 512 seconds (default value: 10).
Maximum request duration (in seconds)	This value is the period after which NTP requests without responses will be deleted. This value must be between 1 and 3600 seconds (default value: 10).

Protection against Time Poisoning attacks

Clock skew threshold allowed (minutes)	This parameter indicates the highest clock skew that an NTP server can send to an NTP client. Beyond the indicated value (20 minutes by default), the client host that sends NTP requests will be considered the target of a Time Poisoning attack and will set off the alarm ntp:463 "NTP: possible poisoning attack" (block alarm by default) . As this protection relies on the firewall's internal clock, ensure that the firewall's clock has been configured correctly (see the Configuration > Date/Time settings module). Setting a value of "0" will disable this protection.

Support

Disable intrusion prevention	When this option is selected, the scan of the NTP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log each request in NTP client mode	Enables or disables the logging of NTP requests.

IPS - NTP v1 tab

Basic configuration

Maximum size of packets (bytes)	Enter the maximum size allowed for NTP v1 packets (default value: 72 bytes).

NTP modes

This list sets out the known NTP v1 modes (active symmetric, passive symmetric, client and server) and the action applied to each one of them.

You can:

- Allow or prohibit modes individually by clicking on their associated action,
- Select all modes with the **Select all** button and apply a common action to them using **Allow** and **Block**.

Advanced properties

Prohibited reference IDs

This list makes it possible to block additional NTP *reference IDs* (LOCL, LCL, etc.):

- Click on **Add** and specify the name of the Reference ID,
- Select a *Reference ID* or all *Reference IDs* with the **Select all** button and click on **Delete**.

IPS - NTP v2 tab

Basic configuration

Maximum size of packets (bytes)	Enter the maximum size allowed for NTP v2 packets (default value: 72 bytes).

NTP modes

This list sets out the known NTP v2 modes (reserved, active symmetric, passive symmetric, client, server, broadcast, NTP control messages and private use) and the action applied to each one of them.

You can:

- Allow or prohibit modes individually by clicking on their associated action,
- Select all modes with the **Select all** button and apply a common action to them using **Allow** and **Block**.

Advanced properties

Prohibited reference IDs

This list makes it possible to block additional NTP *reference IDs* (LOCL, LCL, etc.):

- Click on **Add** and specify the name of the Reference ID,
- Select a *Reference ID* or all *Reference IDs* with the **Select all** button and click on **Delete**.

IPS - NTP v3 tab

Basic configuration

Maximum size of packets (bytes)	Enter the maximum size allowed for NTP v3 packets (default value: 120 bytes).

NTP modes

This list sets out the known NTP v3 modes (reserved, active symmetric, passive symmetric, client, server, broadcast, NTP control messages and private use) and the action applied to each one of them.

You can:

- Allow or prohibit modes individually by clicking on their associated action,
- Select all modes with the **Select all** button and apply a common action to them using **Allow** and **Block**.

Advanced properties

Prohibited reference IDs

This list makes it possible to block additional NTP *reference IDs* (LOCL, LCL, etc.):

- Click on **Add** and specify the name of the Reference ID,
- Select a *Reference ID* or all *Reference IDs* with the **Select all** button and click on **Delete**.

IPS - NTP v4 tab

Basic configuration

Maximum size of packets (bytes)	Enter the maximum size allowed for NTP v4 packets (default value: 72 bytes).

NTP modes

This list sets out the known NTP v4 modes (reserved, active symmetric, passive symmetric, client, server, broadcast, NTP control messages and private use) and the action applied to each one of them.

You can:

- Allow or prohibit modes individually by clicking on their associated action,
- Select all modes with the **Select all** button and apply a common action to them using **Allow** and **Block**.

Advanced properties

Reference ID management

Predefined Reference IDs tab

This list sets out the default Reference IDs (defined in the RFCs) and the action applied to each of them.

You can:

- Allow or prohibit Reference IDs individually by clicking on their associated action,
- Select all Reference IDs with the **Select all** button and apply a common action to them using **Allow** and **Block**.

Custom Reference ID tab

In this list, Reference IDs can also be added or deleted:

- Click on **Add** and specify the name of the Reference ID,
- Select a *Reference ID* or all *Reference IDs* with the **Select all** button and click on **Delete**.

Kiss of death packets

Predefined Reference IDs tab

This list sets out the default Reference IDs (defined in the RFCs) that may be involved in Kiss of Death attacks (DENY, RSTR, RATELCL, etc.) and the action applied to each one of them.

You can:

- Allow or prohibit Reference IDs individually by clicking on their associated action,
- Select all Reference IDs with the **Select all** button and apply a common action to them using **Allow** and **Block**.

Custom Reference ID tab

In this list, Reference IDs that may be involved in Kiss of Death attacks can be added or deleted

- Click on **Add** and specify the name of the Reference ID,
- Select a *Reference ID* or all *Reference IDs* with the **Select all** button and click on **Delete**.

POP3

The aim of the POP3 protocol is to detect connections between a client and e-mail server using the POP3 protocol.

IPS - PROXY tab

Both of these features have been condensed in a single tab for ease of use.

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

Proxy

Mail traffic is based not only on SMTP but also on POP3. This protocol will enable a user to retrieve mail from distant servers onto his workstation using a mail software program. Since this mail server can be located outside the local network or on a separate interface, POP3 traffic passes through and is analyzed by the firewall.

Filter the welcome banner sent by the server	When this option is selected, your mail server's banner will no longer be sent during a POP3 connection. This banner contains information that may be exploited by hackers (server type, software version, etc).

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP address of the web client that sent the packet. Otherwise, the firewall's address will be used.

Support

Disable intrusion prevention	When this option is selected, the analysis of the POP3 protocol will be disabled and traffic will be allowed if the filter policy allows it.
Log each POP3 request	Enables or disables the logging of POP3 requests.

POP3 Commands tab

Proxy

Main commands tab

This menu allows you to authorize or reject POP3 commands defined in the RFCs. You can let commands pass, block them or analyze the syntax and check that the command complies with the current RFCs in force.

Select all button: makes it possible to **Pass without scanning**, **Block** or scan all commands (**Allow**).

Command	Indicates the name of the command.
Action	Allows defining the behavior of the command out of 3 possibilities. Click on the command's action to modify it: • **Allow**: data relating to the command will be scanned in compliance with the RFCs and blocked where necessary. **EXAMPLE** If the name of the USER command does not comply with the RFCs, the packet will not be sent to the server. • **Pass without scanning**: the command will be allowed without being checked. • **Block**: the command will be blocked automatically, and an alarm will be raised to indicate it.

Other commands allowed tab

Command	This field makes it possible to add additional personal commands to **Analyze**.

Analyzing files tab

Maximum size for antivirus and sandboxing analysis (KB)	This option corresponds to the maximum size of files that will be scanned. The default size depends on the firewall model : • SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SN510, SN710, SNi10, SNi20, SNi40, EVA1, EVA2 and EVA3 : 4000 Ko. • SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SNxr1200 and EVA4 : 8000 Ko. • SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200 and EVAU : 16000 Ko.

WARNING
When a size limit is manually set for analyzed data, ensure that all values are consistent, as the total memory space corresponds to the resources reserved for all antivirus services. If you define the size limit for analyzed data on POP3 as 100% of the total size, no other files can be analyzed at the same time.

Action on messages

This zone defines the behavior of the antivirus module when certain events occur.

When a virus is detected	This field contains two options. By selecting **Block**, the analyzed file will not be sent. By selecting **Allow**, the antivirus will send the file in its original form.
When the antivirus scan fails	This option defines the behavior of the antivirus module if the analysis of the file it is scanning fails. **Example** The file could not be scanned as it is locked. If **Block** is specified, the file being scanned will not be sent. If **Pass without scanning** has been specified, the file being scanned will be sent without being checked.
When data collection fails	This option defines the behavior of the antivirus module when certain events occur. It is possible to **Block** traffic when information cannot be retrieved, or **Pass without scanning**.

Sandboxing tab

Sandboxing

Status	This column displays the status (**Enabled**/**Disabled**) of sandboxing for the corresponding file type. Double-click on it to change its status.
File types	The sandboxing option allows scanning four types of attachments: • **Archive**: these include the main types of archives (zip, arj, lha, rar, cab, etc) • **Office document (Office software)**: all types of documents that can be opened with the MS Office suite. • **Executable**: files that can be run in Windows (files with the extension ".exe",".bat",".cmd",".scr", etc). • **PDF**: files in *Portable Document Format* (Adobe) • **Javascript** (files with a ".js" extension). • **Java** (Java compiled files. E.g.: files with a “.jar” extension). • **Others**.
Max. size of sandboxed e-mails (KB)	This field defines the maximum size of e-mails that need to be sandboxed. By default, this value is equal to the one in the **Maximum size for antivirus and sandboxing scan (KB)** field in the *File analysis* tab. This value cannot be exceeded.

Actions on files

When known malware has been identified	This field contains two options. • By selecting **Block**, the analyzed file will not be sent. • By selecting **Allow**, the file will be sent in its original form.
When sandboxing fails	This option defines the behavior of the sandboxing option if the file scan fails: • If **Block** is specified, the file being scanned will not be sent. • If **Pass without scanning** is specified, the file being scanned will be sent.

SMTP

The aim of the SMTP protocol is to detect connection between a client and an e-mail server or between two e-mail servers using SMTP. It allows sending e-mails and is used by Stormshield Vulnerability Manager to detect the version of the client and/or e-mail server in order to report possible vulnerabilities.

IPS tab

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

SMTP protocol extensions

Filter the CHUNKING extension	Allows filtering data transferred from one e-mail address to another. **EXAMPLE** Attachments in e-mails.
Filter Microsoft Exchange Server extensions	Allows filtering additional commands from the Microsoft Exchange Server.
Filter request to change ATRN and ETRN connection direction	Makes it possible to filter data contained in the request to change connection direction, from the client to the server, or from the server to the client. During an SMTP communication, the use of ATRN and ETRN commands allows exchanging the client/server roles.

Maximum size of elements (bytes)

Imposing a maximum size for elements (in bytes) allows countering buffer overflow attacks.

Message header	Maximum number of characters that an e-mail header can contain (e-mail address of the sender, date, type of encoding used, etc.). The values allowed for this field must be between 64 and 4096.
Server response line	Maximum number of characters that the response line from the SMTP server can contain. The values allowed for this field must be between 64 and 4096.
Exchange data (XEXCH50)	Maximum volume of data when transferring files in MBDEF format (Message Database Encoding Format). The values allowed for this field must be between 102400 and 1073741824.
BDAT extension header	Maximum volume of data sent using the BDAT command. The values allowed for this field must be between 102400 and 10485760.
Command line	Maximum volume of data that a command line can contain (excluding the DATA command). The values allowed for this field must be between 64 and 4096.

Support

Disable intrusion prevention	When this option is selected, the scan of the SMTP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every SMTP query	Enables or disables the logging of SMTP requests.

Proxy tab

Filter the welcome banner	When this option is selected, the server's banner will become anonymous during an SMTP connection.

HELO Command

Replace the client's domain name with its IP address	During a basic identification, the client enters its domain name by executing the HELO command. By selecting this option, the domain name will be replaced by the IP address.

Filter domain name

Enable server's domain name filtering	This option allows deleting the domain name of the SMTP server from its response to a HELO command coming from a client. This filter is enabled by default.

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP address of the web client that sent the packet. Otherwise, the firewall's address will be used.

Limits when sending an e-mail

By default, the data size limit for the outgoing mail message (text line) is enabled. Its maximum has been set to 1000 according to the RFC 2821.

Restrict the size of message lines	Sets a limit on the length of the lines in an outgoing message.
Message line [1000-2048 (KB)]	This field indicates the maximum length of a line when sending a message. **REMARKS** Imposing a maximum size for elements (in bytes) allows countering buffer overflow attacks.
Max. no. of recipients	Indicates the maximum number of recipients that a message can contain. The firewall will refuse messages with too many recipients (the refusal will be indicated by an SMTP error). This allows restricting spam.
Maximum size of the message (KB)	Indicates the maximum size of messages passing through the Stormshield Network firewall. Messages exceeding the defined size will be refused by the firewall. The values allowed for this field must be between 0 and 2147483647.

SMTP Commands tab

This menu allows you to authorize or reject SMTP commands defined in the RFCs. You can let commands pass, block them or analyze the syntax and check that the command complies with the current RFCs in force.

Proxy

Main commands tab

Select all button: makes it possible to **Pass without scanning**, **Block** or scan all commands (**Allow**).

Command	Indicates the name of the command.
Action	Indicates the action performed.

Other commands allowed tab

Command	By default, all commands not defined in the RFCs are prohibited. However, some mail systems use additional non-standard commands. You can therefore add these commands in order to let them pass through the firewall. The buttons **Add** and **Delete** allow you to modify the list of commands.

IPS

Allowed SMTP commands tab

List of additional SMTP commands allowed. It is possible to **Add** or **Delete** commands.

Prohibited SMTP commands tab

List of prohibited SMTP commands. It is possible to **Add** or **Delete** commands.

Analyzing files tab

Maximum size for antivirus and sandboxing analysis (KB)	This option corresponds to the maximum size of files that will be scanned. The default size depends on the firewall model : • SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SN510, SN710, SNi10, SNi20, SNi40, EVA1, EVA2 and EVA3 : 4000 Ko. • SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SNxr1200 and EVA4 : 8000 Ko. • SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200 and EVAU : 16000 Ko.

WARNING
When a size limit is manually set for analyzed data, ensure that all values are consistent, as the total memory space corresponds to the resources reserved for all antivirus services. If you define the size limit for analyzed data on SMTP as 100% of the total size, no other files can be analyzed at the same time.

Action on messages

This zone defines the behavior of the antivirus module when certain events occur.

When a virus is detected	This field contains two options: **Allow** and **Block** • By selecting **Block**, the analyzed file will not be sent. • By selecting **Allow**, the antivirus will send the file even if it has been found to be infected.
When the antivirus scan fails	The option **Pass without scanning** defines the behavior of the antivirus module if the analysis of the file it is scanning fails. • If **Block** is specified, the file being scanned will not be sent. • If **Pass without scanning** is specified, the file being scanned will be sent.
When data collection fails	This option defines the behavior of the antivirus module when certain events occur. **EXAMPLES** If the hard disk has reached its capacity, information will not be downloaded. The maximum size that the file can reach for the antivirus scan is restricted (1000KB).

Sandboxing tab

Sandboxing

Status	This column displays the status (**Enabled**/**Disabled**) of sandboxing for the corresponding file type. Double-click on it to change its status.
File types	The sandboxing option allows scanning four types of attachments: • **Archive**: these include the main types of archives (zip, arj, lha, rar, cab, etc) • **Office document (Office software)**: all types of documents that can be opened with the MS Office suite. • **Executable**: files that can be run in Windows (files with the extension ".exe",".bat",".cmd",".scr", etc). • **PDF**: files in *Portable Document Format* (Adobe) • **Javascript** (files with a ".js" extension). • **Java** (Java compiled files. E.g.: files with a “.jar” extension). • **Others**.
Max. size of sandboxed e-mails (KB)	This field defines the maximum size of e-mails that need to be sandboxed. By default, this value is equal to the one in the **Maximum size for antivirus and sandboxing scan (KB)** field in the *File analysis* tab. This value cannot be exceeded.

Actions on files

When known malware has been identified	This field contains two options: • By selecting **Block**, the analyzed file will not be sent. • By selecting **Allow**, the file will be sent in its original form.
When sandboxing fails	This option defines the behavior of the sandboxing option if the file scan fails. • If **Block** is specified, the file being scanned will not be sent. • If **Pass without scanning** is specified, the file being scanned will be sent.

SNMP (IPS tab)

Allow version

SNMPv1	If this option is selected, the firewall will allow packets corresponding to SNMP version 1.
SNMPv2c	If this option is selected, the firewall will allow packets corresponding to SNMP version 2c.
SNMPv3	If this option is selected, the firewall will allow packets corresponding to SNMP version 3.

Allow Empty Field

communityname	If this option is selected, you will be allowing SNMP requests with a blank community field (SNMPv1 - SNMPv2c).
Login	If this option is selected, you will be allowing SNMP requests with a blank ID field (SNMPv3).

SNMP command management

SNMP commands

This list sets out the SNMP functions allowed by default on the firewall. The action (*Allow/Block*) applied to each command can be modified by clicking in the **Action** column. The **Modify all commands** button allows modifying the action applied to all commands.

Community name

Black list tab

This table allows listing communities for which SNMP packets will be systematically blocked. You can **Add** or **Delete** communities by clicking on the respective buttons.

White list tab

This table allows listing communities for which SNMP packets will not undergo content inspection. You can **Add** or **Delete** communities by clicking on the respective buttons.

→ buttons ←

These buttons make it possible to move a community from one table to another.

Identifiers

Black list tab

This table allows listing IDs for which SNMP packets will be systematically blocked. You can **Add** or **Delete** IDs by clicking on the respective buttons.

White list tab

This table allows listing IDs for which SNMP packets will not undergo content inspection. You can **Add** or **Delete** IDs by clicking on the respective buttons.

→ buttons ←

These buttons make it possible to move an ID from one grid to another.

OID

Black list tab

This table allows listing OIDs (Object identifiers) for which SNMP packets will be systematically blocked. You can **Add** or **Delete** OIDs by clicking on the respective buttons.

Whenever an OID is specified in this table, all OIDs originating from it will also be blocked.

Example: adding the OID 1.3.6.1.2.1 to the table will imply that OIDs 1.3.6.1.2.1.1, 1.3.6.1.2.1.2, etc... will also be blocked.

White list tab

This table allows listing OIDs for which SNMP packets will not undergo content inspection. You can **Add** or **Delete** OIDs by clicking on the respective buttons.

Whenever an OID is specified in this table, all OIDs originating from it will not undergo content inspection.

Example: adding the OID 1.3.6.1.2.1 to the table will imply that OIDs 1.3.6.1.2.1.1, 1.3.6.1.2.1.2, etc... will also be whitelisted.

→ buttons ←

These buttons make it possible to move an OID from one table to another.

Support

Disable intrusion prevention	When this option is selected, the scan of the SNMP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every SNMP query	Enables or disables the logging of SNMP requests.
Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

SSL

The SSL (Secure Sockets Layer) protocol, which became Transport Layer Security (TLS) in 2001, is supported in version 3 (1996). Sites that use an older version (which may present security flaws) or that do not support the start of a negotiation in TLS will be blocked.

An ICAP server's validation of HTTPS requests decrypted by the SSL proxy is not supported.

IPS tab

This screen will allow you to confirm the activation of the SSL protocol through the firewall.

Certain options allow reinforcing this protocol's security. For example, negotiations of cryptographic algorithms that are deemed weak can be prohibited, or software applications that use SSL to bypass filter policies can be detected (SKYPE, HTTPS proxy, etc).

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

TLS v1.3

Allow 0-RTT	When this checkbox is selected, the IPS engine allows TLS requests that use 0-RTT (Zero Round Trip Time), which reduces the handshake to zero exchanges in order to improve performance for TLS traffic. 0-RTT allows the client to send application data from the first exchange when the client and server share a pre-shared key, either imported manually or calculated during an earlier handshake.
Unknown values/extensions	Select the type of TLS values or extensions to allow: • RFC TLS 1.3, GREASE (Generate Random Extensions And Sustain Extensibility) or unknown values/extensions, • RFC TLS 1.3 and GREASE values/extensions, • RFC TLS 1.3 and unknown values/extensions (except GREASE), • Only RFC TLS 1.3 values/extensions.
Enable server certificate analysis	When this option is selected, the intrusion prevention engine will attempt to retrieve the server certificate for every TLS v1 traffic stream that passes through the firewall so that any potential security flaws relating to this certificate can be analyzed. **NOTE** To optimize the analysis of server certificates, a cache mechanism makes it possible to avoid retrieving a certificate when the intrusion prevention engine already knows it. This mechanism can be configured in the Global configuration of the SSL protocol, in the **IPS** tab.
When the certificate type is wrong	Select the action applied to analyzed TLS traffic when the retrieved server certificate displays an anomaly: • **Continue analysis**: the intrusion prevention engine continues to analyze the certificate and the protocol analyses on the TLS 1.3 traffic in question. • **Block traffic**: the certificate is rejected, the firewall raises an alarm and blocks the TLS 1.3 traffic in question by shutting down the connection.
When the SNI is missing	Select the action applied to analyzed TLS traffic when the certificate does not have an SNI (Server Name Indication): • **Continue analysis**: the intrusion prevention engine continues to analyze the certificate and the protocol analyses on the TLS 1.3 traffic in question. • **Block traffic**: the certificate is rejected, the firewall raises an alarm and blocks the TLS 1.3 traffic in question by shutting down the connection.

When the CA is not trustworthy	Select the action applied to TLS traffic when the CA that signed the server certificate is not in the list of trusted CAs: • **Continue analysis**: the intrusion prevention engine continues to analyze the certificate and the protocol analyses on the TLS 1.3 traffic in question. • **Block traffic**: the certificate is rejected, the firewall raises an alarm and blocks the TLS 1.3 traffic in question by shutting down the connection.
When the certificate is self-signed	These certificates are used internally and signed by your local server. They allow guaranteeing the security of your exchanges and authenticating users, among other functions. Select the action to perform when you encounter self-signed certificates: • **Continue analysis**: the intrusion prevention engine continues to analyze the certificate and the protocol analyses on the TLS 1.3 traffic in question. • **Block traffic**: the firewall rejects these certificates and matching traffic is blocked.
When the validity date is wrong	The certificates to which this field applies have a validity date before or after the current date, and are therefore not "valid". Select the action to perform when you encounter certificates with validity dates that are wrong: • **Continue analysis**: the intrusion prevention engine continues to analyze the certificate and the protocol analyses on the TLS 1.3 traffic in question. • **Block traffic**: the firewall rejects these certificates and matching traffic is blocked.
When the CRL verification fails	Select the action to perform when the automatic verification of the CRL is unsuccessful. • **Continue analysis**: the intrusion prevention engine continues to analyze the certificate and the protocol analyses on the TLS 1.3 traffic in question. • **Block traffic**: the firewall rejects these certificates and matching traffic is blocked.
When the CRL is invalid	Select the action to perform when the CRL to verify has expired: • **Continue analysis**: the intrusion prevention engine continues to analyze the certificate and the protocol analyses on the TLS 1.3 traffic in question. • **Block traffic**: the firewall rejects these certificates and matching traffic is blocked.
Address used for certificate verification	Select the object that represents the IP address of the firewall to be used for submitting certificate verification requests. If no objects are selected, time the IP address of the interface *Firewall_out* will be used.

SSL negotiation

Allow unsupported encryption methods	Select this option if the encryption algorithm that you wish to use is not supported by the SSL protocol.
Allow unencrypted data after an SSL negotiation	This option allows sending data in plaintext after an SSL negotiation. **WARNING** Allowing data transmission in plaintext poses a security risk.

Authorize signaling cipher (SCSV)	TLS fallback attacks consist of intercepting communications and imposing the weakest cryptographic variant possible. By enabling this option, the firewall will announce a cryptographic pseudo-algorithm that would allow reporting an attempt to launch a fallback attack (RFC 7507).
Encryption levels allowed	The stronger the encryption algorithm used and the more complex the password, the higher the level of security. **EXAMPLE** The AES encryption algorithm with a strength of 256 bits, associated with a password of about ten characters made up of letters, numbers and special characters. Three choices of encryption levels can be authorized: • **Low, medium, high**: for example, DES (64 bits), CAST128 (128 bits) and AES. Regardless of the password's security level, the encryption level will be allowed. • **Medium and high**: Only medium-security and high-security algorithms will be tolerated. • **Only high**: Only strong algorithms and passwords with a high level of security will be tolerated.

Manage SSL extensions

Named extensions tab

This table makes it possible to allow/prohibit the named TLS v1.3 protocol extensions.
All known named extensions (see the IANA's list of TLS extensions) are listed by default: a line in the table therefore contains the ID (between 0 and 56 inclusive), the name of the extension and the action applied to it.

You can:

- Allow or prohibit extensions individually by clicking on their associated action,
- Allow or prohibit a selection of extensions (hold down the Shift key and select consecutive lines or hold down the Ctrl key and select separated lines) and apply a common action to them using **Allow selection** and **Prohibit selection**.
- Select all extensions with the Select all button and apply a common action to them using **Allow selection** and **Prohibit selection**.

A search field also makes it possible to filter the display of extensions.

Blacklisted extension ranges tab

This table contains the known TLS v1.3 extensions to prohibit other than the ones defined in the **Named extensions** tab. The ID of these extensions must be between 57 and 65535 inclusive.

Defined extensions can be added (**Add** button) or deleted (**Delete** button after selecting the line concerned) individually using their IDs (e.g. 59) or extension ranges (e.g. 59-62, 92-1001).

A search field also makes it possible to filter the display of blacklisted IDs.

Unencrypted data detection (plaintext traffic)

Detection method	• **Do not detect**: unencrypted data will not be scanned. • **Inspect all traffic**: all packets received will be scanned by the SSL protocol in order to detect plaintext traffic. • **Sampling (7168 bytes):** only the first 7168 bytes of the traffic will be analyzed in order to detect plaintext traffic.

Support

Disable IPS	When this option is selected, the scan of the SSL protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every SSL query	Enables or disables the logging of SMTP requests.

Application-Layer Protocol Negotiation (ALPN)

Application-Layer Protocol Negotiation (ALPN) is an extension of the Transport Layer Security (TLS) protocol, which negotiates the protocol of the application layer during the TLS handshake.

IANA ALPN tab

In this grid, protocols registered with the IANA and included in the ALPN extension as described in RFC 7301 can be allowed/prohibited.

You can:

- Allow or prohibit protocols individually by clicking on their associated action,
- Select all protocols with the **Select all** button and apply a common action to them using **Allow** and **Block**.

A search field also makes it possible to filter the display of protocols.

ALPN EXCEPTIONS tab

In this grid, ALPN extension protocols that must be excluded from the SSL/TLS protocol analysis can be defined.

You can:

- Add a protocol to be deleted by using the **Add** button.
- Select all excluded protocols and delete them from the grid by using the **Select all** then **Remove** buttons.

A search field also makes it possible to filter the display of protocols.

Proxy tab

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP address of the web client that sent the packet. Otherwise, the firewall's address will be used.

Content inspection

Self-signed certificates	These certificates are used internally and signed by your local server. They allow guaranteeing the security of your exchanges and authenticating users, among other functions. This option determines the action to perform when you encounter self-signed certificates: • **Delegate to user**: this action raises a security alert in the client's web browser. The client will then decide whether to continue the connection to the server concerned. An alarm will be generated and the client's action will be recorded in the logs l_alarm file. • **Continue analysis**: these certificates are accepted without generating any security alerts in the client's web browser. Traffic goes through and is analyzed by the intrusion prevention engine. • **Block**: the firewall rejects these certificates and matching traffic is blocked.
Expired certificates	Expired certificates have validity dates that have lapsed and are therefore not valid. To fix this problem, they must be renewed by a certification authority **WARNING** Expired certificates may pose a security risk. After the expiry of a certificate, the CA that issued it will no longer be responsible for it if it is used maliciously. This option determines the action to perform when you encounter expired certificates: • **Delegate to user**: this action raises a security alert in the client's web browser. The client will then decide whether to continue the connection to the server concerned. An alarm will be generated and the client's action will be recorded in the logs l_alarm file. • **Continue analysis**: these certificates are accepted without generating any security alerts in the client's web browser. Traffic goes through and is analyzed by the intrusion prevention engine. • **Block**: the firewall rejects these certificates and matching traffic is blocked.
Unknown certificates	This option will determine the action to perform when you encounter unknown certificates: • **Delegate to user**: this action raises a security alert in the client's web browser. The client will then decide whether to continue the connection to the server concerned. An alarm will be generated and the client's action will be recorded in the logs l_alarm file. • **Do not decrypt**: these certificates are accepted without generating any security alerts in the client's web browser. Traffic goes through without being analyzed by the intrusion prevention engine. • **Block**: the firewall rejects these certificates and matching traffic is blocked.

Wrong certificate type	This test validates the certificate's type. A certificate is deemed compliant if it is used in the context defined by its signature. Therefore, a user certificate used by a server does not comply. This option will determine the action to perform when you encounter non-compliant certificates: • **Delegate to user**: this action raises a security alert in the client's web browser. The client will then decide whether to continue the connection to the server concerned. An alarm will be generated and the client's action will be recorded in the logs l_alarm file. • **Continue analysis**: these certificates are accepted without generating any security alerts in the client's web browser. Traffic goes through and is analyzed by the intrusion prevention engine. • **Block**: the firewall rejects these certificates and matching traffic is blocked.
Certificate with incorrect FQDN	This option will determine the action to perform when certificates with an invalid domain name are encountered: • **Delegate to user**: this action raises a security alert in the client's web browser. The client will then decide whether to continue the connection to the server concerned. An alarm will be generated and the client's action will be recorded in the logs l_alarm file. • **Continue analysis**: these certificates are accepted without generating any security alerts in the client's web browser. Traffic goes through and is analyzed by the intrusion prevention engine. • **Block**: the firewall rejects these certificates and matching traffic is blocked.
When the FQDN of the certificate is different from the SSL domain name	This option will determine the action to perform when you encounter certificates with domain names (FQDN) that are different from the expected SSL domain: • **Delegate to user**: this action raises a security alert in the client's web browser. The client will then decide whether to continue the connection to the server concerned. An alarm will be generated and the client's action will be recorded in the logs l_alarm file. • **Continue analysis**: these certificates are accepted without generating any security alerts in the client's web browser. Traffic goes through and is analyzed by the intrusion prevention engine. • **Block**: the firewall rejects these certificates and matching traffic is blocked.
Allow IP addresses in SSL domain names	This option allows or denies access to a site based on its IP addresses instead of its SSL domain name.

Support

If decryption fails	This option will determine the action to perform when decryption fails: you can choose to **Block traffic** or **Do not decrypt**. Traffic will not be inspected if the second option is selected.
If classification of certificate fails	The choice is either **Pass without decrypting** or **Block without decrypting**. If a certificate has not been listed in a certificate category, this action will determine whether the traffic will be authorized.

Application-Layer Protocol Negotiation (ALPN)

Application-Layer Protocol Negotiation (ALPN) is an extension of the Transport Layer Security (TLS) protocol, which negotiates the protocol of the application layer during the TLS handshake.

IANA ALPN tab

In this grid, protocols registered with the IANA and included in the ALPN extension as described in RFC 7301 can be allowed/prohibited.

You can:

- Allow or prohibit protocols individually by clicking on their associated action,
- Select all protocols with the **Select all** button and apply a common action to them using **Allow**and **Block**.

A search field also makes it possible to filter the display of protocols.

ALPN EXCEPTIONS tab

In this grid, ALPN extension protocols that must be excluded from the SSL/TLS protocol analysis can be defined.

You can:

- Add a protocol to be deleted by using the **Add** button.
- Select all excluded protocols and delete them from the grid by using the **Select all** then **Remove** buttons.

A search field also makes it possible to filter the display of protocols.

TFTP (IPS tab)

Automatically detect and inspect the protocol	If this protocol is enabled, the inspection function will automatically apply to discover corresponding traffic that filter rules allow.

Maximum size of elements (bytes)

Filename	This number has to be between 64 and 512 bytes.

Support

Disable intrusion prevention	When this option is selected, the scan of the TFTP protocol will be disabled and traffic will be authorized if the filter policy allows it
Log every TFTP query	Enables or disables the generation of logs relating to TFTP queries.

The scan of the option “utimeout” has been added to the TFTP protocol scan.

Others

This section is dedicated to the rest of the protocols that you may encounter but which have not been covered above.

This screen is divided into five columns:

Protocol name	Name given to the protocol

Default port	The name of the port assigned by default. A new port can be created by clicking on to the right of the column.
Default SSL port	Name of the port assigned to the default protocol.
Automatic detection	You can choose to enable or disable automatic protocol detection. As all protocols are enabled by default, double-click on the column to disable the automatic detection of the relevant protocol.
Status	You can choose to enable or disable the selected protocol. As all protocols are enabled by default, double-click on the column to disable the automatic detection of the relevant protocol. Repeat the operation when you wish to re-enable it.

Click on **Apply** to save your changes.

REST API

SNS has a standard REST API with which your SNS firewalls can be used and queried through your own orchestration tools.

Not all SNS features are available yet in the REST API. It will be enriched as new versions are released.

General configuration tab

The REST API is not enabled by default, and only the SNS firewall's super administrator (*admin* account) can enable it.

Authentication over the REST API is secured by API keys that administrators generate. These keys have read/write or read-only privileges as well as a validity period that can be configured.

All operations performed via the REST API are recorded in audit logs.

To make it easier to use this API, OpenAPI documentation is available on the firewall through the address https://<@SNS firewall IP>/docs/papi/v1 or via the link shown in the firewall's web interface.

Documentation can also be found on Stormshield's Technical Documentation website.

Enabling the SNS REST API

Enabling the REST API ON OFF	Set the cursor to **ON** to enable the REST API.

Communication

Server certificate	Select the certificate presented by the firewall when accessing the REST API. The certificate selected by default is the firewall's self-generated certificate (SNS-WebServer-default-authority) for access to the firewall web administration interface.
Port	Select the port to access the firewall's REST API. The default port is the **https** object.

Key lifetimes

Minimum lifetime (in days)	Set the minimum lifetime suggested by default to administrators when they create an API key (30 days by default). The lifetime of an API key generated by an administrator cannot be below this value.
Maximum lifetime (in days)	Set the maximum lifetime suggested by default to administrators when they create an API key (365 days by default). The lifetime of an API key generated by an administrator cannot be above this value.

Logs	
Log authentication failures	Select this checkbox to enable the generation of all logs relating to errors encountered during authentication for API use. These logs are written to the dedicated "l_restapi" log file.
Log all routes:	Select this checkbox to enable the generation of logs relating to all routes used on the REST API. These logs are written to the dedicated "l_restapi" log file.

API keys tab

IMPORTANT
For security reasons, the super administrator (*admin* account) cannot create or regenerate API keys, but can only revoke or delete them.
Only administrator accounts with the specific **API keys** permission are allowed to perform all operations (creation, regeneration, revocation and deletion).
Furthermore, each administrator can only view/edit their own API keys.

Possible operations

Filter	Enter a character string to display only results containing this string.
Status selector	Select the status of the API keys that you wish to display in the grid. The value of this field may be one of the following: • All, • Active, • Expired, • Revoked.

Create	This button allows you to create a new API key. To create a new API key: 1. Click on **Create**. 2. Add comments if necessary. 3. You can change the default **Lifetime (in days)** for this key. 4. Select the **Privileges assigned to the key**: • **Blacklist management - Read-only**: read-only on routes that allow blacklist management, • **Blacklist management - Read/Write**: read/write only on routes that allow blacklist management, • **Same as my privileges** (permissions of the administrator who created the key). 5. Click on **Apply**. The wizard shows you the ID and secret of the created key, in identifier:secret format. Copy them to keep them in a safe place: the secret can no longer be recovered once the key creation is complete. 6. Click on Close. The key is added to the grid.
Regenerate	This button is used to extend the lifetime of the selected API key with the lifetime and privileges that were initially assigned to this key.
Revoke	This button disables the selected API key. This key then becomes unusable and appears grayed out in the grid.
Delete	This button deletes the selected API key. If the key was active, it will first be revoked, and then deleted.
Search in logs	Select one or several API keys, and click on this button to view all log entries that match these keys.
API documentation	Click on this link to access the firewall's embedded REST API documentation.

Rule grid

ID	Displays the unique ID generated when the API key was created.
Owner	Displays the e-mail address of the administrator who owns the key. As a reminder, administrators can only view the keys that they own: only the super administrator can view the keys of all administrators.
Creation date	Shows the date on which the key was created.
Expiry date	Shows the date on which the key will expire: it can be regenerated before this date to extend its lifetime.
Remaining lifetime	Shows the number of days that remain until the key expires.
Status	Shows the status of the key during its lifetime: active, expired or revoked.
Comments	Shows optional comments added when the key was created.
Access privileges	Shows the privileges assigned to the key: the list of privileges varies according to the choice of privileges that were assigned when the key was created.
Last used	Shows the date and time that the key was last used to access the firewall's REST API.

QUALITY OF SERVICE (QoS)

Since the QoS configuration has changed in SNS version 4.3.0, when a configuration that uses QoS is updated to SNS version 4.3.0 or higher, a warning message will appear, indicating that "The QoS configuration must be completed".

IMPORTANT

This is an early access feature in SNS 4.8.

You must refer to the Known issues and Limitations and explanations on usage of SNS 4.8 Release Notes before enabling this feature or upgrading an existing QoS configuration to SNS 4.8.

QoS configurations defined in versions earlier than SNS 4.8 are not automatically valid. Traffic shapers must be set so that these QoS configurations can be enabled after an update to SNS version 4.8.

QoS can be configured through two tabs:

- **Queues** tab: defines traffic shapers and queues.
- **Traffic shapers** tab: assigns traffic shapers and queues to the network interfaces in question.

Queues tab

Queues

The QoS module, built into Stormshield Network's intrusion prevention engine, is associated with the Filtering module in order to provide Quality of Service features.

When a packet arrives on an interface, it will first be processed by a filter rule, then the intrusion prevention engine will assign the packet to the right queue according to the configuration of the filter rule's QoS field.

There are three types of queues on the firewall: Two of them are directly associated with QoS algorithms: PRIQ (Priority Queuing) and CBQ (Class-Based Queuing). The third enables traffic monitoring.

Class-based queue (CBQ)

A scheduling class can be chosen for each filter rule and a bandwidth guarantee or restriction can be assigned to it.

For example, you can associate a scheduling class with HTTP traffic by associating a CBQ to the corresponding filter rule.

Class-based queuing determines the way in which traffic assigned to QoS rules will be managed on the network. Bandwidth reservation mechanisms for this queue type guarantee a minimum service while bandwidth restriction mechanisms enable the preservation of bandwidth when dealing with applications that consume a large amount of resources.

Adding a class-based queue

To add a class-based queue:

1. Click on **Add**.
2. Select **Class Based Queuing (CBQ)**.
   A window appears, allowing you to configure the various properties of the queue: Name, Type, Comments, Bandwidth restrictions;

Details of the properties of a **Class Based Queuing** queue are described below.

Modifying a class-based queue

Name	Name of the queue to be configured.
Type	Bandwidth reservation/limitation queues are indicated as **Class Based Queuing (CBQ)**.
Comments	Related comments (optional).

Bandwidth restrictions

Guaranteed bandwidth	Acting as a service guarantee, this option allows guaranteeing a given throughput and a maximum transfer time. Configured in Kbits/s, Mbits/s, Gbit/s or as a percentage of the reference value, this value is shared between all traffic assigned to this QoS rule. As such, if HTTP and FTP traffic is associated with a queue with a guaranteed minimum of 10Kbits/s, the HTTP+FTP bandwidth will be at a minimum of 10Kbits/s. However, there is no restriction on the HTTP bandwidth being 9Kbits/s and the FTP bandwidth being only 1Kbits/s. **REMARKS** This option is synchronized by default with the option **Guaranteed rev.** By modifying its value, the value will be replicated in **Guaranteed rev**. By modifying the value of **Guaranteed rev.**, the values will be different and therefore desynchronized.
Max bandwidth	Acting as a restriction, this option prohibits bandwidth for the traffic assigned to these queues from being exceeded. Configured in Kbits/s, Mbits/s, Gbit/s or as a percentage of the reference value, this value is shared between all traffic assigned to this QoS rule. As such, if HTTP and FTP traffic is associated with a queue with an authorized maximum of 500Kbits/s the HTTP+FTP bandwidth must not exceed 500Kbits/s. **REMARKS** This option is synchronized by default with the option **Max rev**. By modifying its value, the value will be replicated in **Max rev**. By modifying the value of **Max rev**, the values will be different and therefore desynchronized.

Guaranteed rev.	Acting as a service guarantee, this option makes it possible to guarantee a given throughput and a descending maximum transfer time. Configured in Kbits/s, Mbits/s, Gbit/s or as a percentage of the reference value, this value is shared between all traffic assigned to this QoS rule. As such, if HTTP and FTP traffic is associated with a queue with a guaranteed minimum of 10Kbits/s, the HTTP+FTP bandwidth will be at a minimum of 10Kbits/s. However, there is no restriction on the HTTP bandwidth being 9Kbits/s and the FTP bandwidth being only 1Kbits/s. **REMARKS** If you enter a value higher than the **Max rev.**, the following message will appear: "downward traffic: the minimum guaranteed bandwidth should be lower than or equal to the maximum bandwidth".
Max rev.	Acting as a restriction, this option prohibits bandwidth for the downward traffic, assigned to these queues, from being exceeded. Configured in Kbits/s, Mbits/s, Gbit/s or as a percentage of the reference value, this value is shared between all traffic assigned to this QoS rule. As such, if HTTP and FTP traffic is associated with a queue with an authorized maximum of 500Kbits/s the HTTP+FTP bandwidth must not exceed 500Kbits/s.

REMARKS
If you select "**None**" in the **Guaranteed bandwidth** column and "**Unlimited**" in the **Max. bandwidth** column, no restrictions will be placed on the traffic. In this case, a message will appear, suggesting that you change your queue to a monitoring queue.

The grid of the **Queues** menu displays the various queues that have been configured. Clicking on **Check usage** allows you to display the list of filter rules in which the selected queue is being used.

Deleting a class-based queue

Select the line of the class-based queue to be deleted and click on **Delete**. A message will appear asking you to confirm that you wish to delete the queue.

Monitoring queue

Monitoring queues do not affect how traffic associated with QoS rules is treated.

They enable the registration of throughput and bandwidth information that may be viewed in the **QoS monitoring** module (after being selected in the *QoS configuration* tab in the **Monitoring configuration** module).

Configuration options for Monitoring queues are as follows:

Adding a monitoring queue

To add monitoring queue:

1. Click on **Add**.
2. Select **Monitoring Queuing (MONQ)**.
   A window appears, allowing you to configure the various properties of the queue: Name, Type, Comments.

Details of the properties of a **Monitoring Queuing (MONQ)** queue are described below.

Modifying a monitoring queue

Name	Name of the queue to be configured.
Type	Traffic monitoring queues are indicated as **Monitoring Queuing (MONQ)**.
Comments	Related comments (optional).

Deleting a monitoring queue

Select the line of the monitoring queue to be deleted and click on **Delete.** A message will appear asking you to confirm that you wish to delete the queue.

Priority queue

There are 7 levels of priority. Packets are treated according to the configured priorities.

High priority can be assigned to DNS queries by creating a filter rule and associating it with a PRIQ.

Priority queuing gives certain packets priority during their treatment. This means that packets associated with a **PRIQ** filter rule will be treated before other packets.

The scale of priorities ranges from 0 to 7. Priority 0 corresponds to traffic with the highest priority among **PRIQ** queues. Priority 7 corresponds to traffic with the lowest priority among **PRIQ** queues.

Traffic without QoS rules will be treated before any other **PRIQ** or **CBQ** queues.

Configuration options for PRIQ queues are as follows:

Adding a priority queue

To add a priority queue:

1. Click the **Add** button.
2. Select **Priority Queuing (PRIQ)**.
   A window appears, allowing you to configure the various properties of the queue: Name, Type, Priority, Comments.

Details of the properties of a **Priority Queuing (PRIQ)** queue are described below.

Modifying a priority queue

The table displays the various queues that have been configured. Clicking on **Check usage** allows you to check whether these rules are being used in a filter rule. If this is the case, a menu will appear in the browser bar, showing the rules.

Name	Name of the queue to be configured.
Type	Priority-based queues are indicated as **Priority Queuing (PRIQ)**.
Priority	Defines the priority level of the traffic assigned to the queue. The cells in this column can only be edited for PRIQs. A value from 0 (highest priority) to 7 (lowest priority) can be selected.
Comments	Related comments (optional).

Deleting a priority queue

Select the relevant line in the table of priority queues and click on **Delete**. A message will appear asking you to confirm that you wish to delete the queue.

Available queues

At the end of the queue table, the available number of queues will be indicated for a given firewall model. These values are as follows:

SN160(W), SN210(W), SN310	EVA1, EVA2, EVA3, EVA4, EVAU (16G) SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320 SN510, SN-M-Series-520 SN710, SN-M-Series-720 SN910, SN-M-Series-920 SN1100, SNxr1200 SNi10 SNi20 SNi40	EVAU (32G), EVAU (64G) SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200
20	100	255

Traffic shapers tab

Traffic shaper

This grid lists the traffic shapers that may be assigned to network interfaces to which QoS has been applied.

> **DEFINITION**
> Traffic shaping refers to how the volume of traffic is controlled on a computer network in order to optimize or guarantee performance, lower latency or increase usable bandwidth by delaying packets that meet certain criteria. More specifically, traffic shaping refers to any action on network traffic that imposes an additional delay on these packets so that they comply with a predetermined constraint (contractual or related to a certain type of traffic).

Possible operations

You can **Add** or **Delete** traffic shapers. If you wish to delete a traffic shaper used on a network interface, a warning message will ask you to change the QoS configuration before deleting it.

The traffic shapers displayed can also be filtered by entering a character string in the filter field.

Grid

Name	Name given to the traffic shaper.
Outgoing bandwidth	Indicate the outgoing bandwidth reserved for the traffic shaper. When a traffic shaper is defined for the interface linked to the Internet access router, you are advised to set this value to 95% of the maximum bandwidth on the Internet link.

Unit	Select the outgoing bandwidth unit assigned to the traffic shaper: • Kbit/s, • Mbit/s, • Gbit/s.
Incoming bandwidth	Indicate the incoming bandwidth reserved for the traffic shaper. When a traffic shaper is defined for the interface linked to the Internet access router, you are advised to set this value to 95% of the maximum bandwidth on the Internet link.
Unit	Select the incoming bandwidth unit assigned to the traffic shaper: • Kbit/s, • Mbit/s, • Gbit/s.

Interfaces with QoS

In this grid, you can define the interfaces to which QoS is applied, as well as traffic shaping, queues or queues for TCP ACK traffic to use for each of these interfaces.

Possible operations

You can **Add** or **Delete** Interface/Traffic shaper/Queue/ACK queue associations.

Grid

Interface	Select the interface to which you want to apply QoS.
Traffic shaper	Select one of the traffic shapers defined on the firewall.
Default queue	Select one of the queues defined on the firewall. If you do not wish to assign any particular queue, select *Bypass*.
Default ACK queue	Select one of the queues defined on the firewall. If you do not wish to assign any particular ACK queue, select *Bypass*.

REAL-TIME LOGS

Real-time logging allows firewalls that do not have dedicated storage space (/log partition on hard disk, SD or microSD card) to display logs available in the firewall's memory.

The number of log lines that can be displayed depends on the firewall's memory capacity.

Log file selection field

Select the log file for which you wish to display entries.

The following log files are available:

- Administration,
- Alarms,
- Authentication,
- Application connections,
- Network connections,
- System events,
- Filter policy,
- HTTP proxy,
- SMTP proxy,
- FTP proxy,
- POP3 proxy,
- SSL proxy,
- IPsec VPN,
- SSL VPN,
- Dynamic multicast routing,
- Sandboxing,
- Filter statistics,
- Router statistics,
- Monitoring.

Log display

When a log file is selected, the events contained in the file are displayed in the grid.

The columns found in the grid depend on the log file selected.

Possible operations

Search	Enter a character string in this field to filter by the entries displayed (IP address, protocol, host name, user, etc.).
Refresh	This button refreshes the list of logs that are displayed in the grid.
Refreshment time	This button can be used to change how often the grid is automatically refreshed.

Pause/Resume	Click this button to pause or resume automatic grid refreshment.
Actions	This drop-down list offers three additional actions: • **Show all columns**: the default display selects a certain number of columns, depending on the log file displayed. Click on this action to display all available columns for the selected log. • **Export data**: select this action to download data from the selected log file in CSV format. • **Reset columns**: select this action to return to the default log file display.

Interactive features

Depending on the cell selected, when you right-click on a log line, you can:

- Search for this value in the **All logs** view,
- Check usage of this host,
- Show host details,
- Blacklist this object (for 1 minute, 5 minutes, 30 minutes or 3 hours),
- Copy the selected line to the clipboard,
- Copy the current cell to the clipboard,
- Add the host to the objects base and/or add it to a group.

RECORDING CONFIGURATION COMMANDS

When it has been enabled in your preferences, the button allowing you to record configuration commands will appear on the right side of the upper panel in the web administration interface. It allows you to save all commands sent to the firewall during a configuration sequence so that they can be reused later, for example, in scripts. This sequence may apply to several configuration modules.

The status of this button may be one of the following:

- : no recording in progress.
- : recording in progress.

Recording a sequence of configuration commands

1. Click on to start recording,
2. Perform all the configuration actions that you wish to record,
3. Stop recording by clicking on ,

The **Recorded configuration commands** window will then appear, containing the list of all commands applied sequentially to the firewall. This list can be modified.

4. Select the action to apply to the list of commands:

- **Copy to clipboard**: all commands will be remembered in the workstation's clipboard so that they can be pasted in a text editor,
- **Clear**: all commands will be erased without being remembered,
- **Close**: closes the **Recorded configuration commands** window.

ACTIVITY REPORTS

The **Reports** module offers static reports based on logs saved on the firewall. These reports belong to several categories: Web, Security, Virus, Spam, Vulnerability, Network, Industrial network, Sandboxing, SD-WAN and web services.

Most reports present the Top 10 most frequently occurring values (e.g., Top 10 most frequently blocked websites), while the remaining values are grouped under “Others”. SD-WAN reports are based on metrics and operational statuses obtained when monitoring routers and their gateways.

NOTE
Reports from each category are displayed only if they were enabled in the **Configuration** module > **Logs - Syslog - IPFIX** > Report configuration). If no reports are enabled in the configuration, the **Reports** module will not appear.

Private data

For the purpose of compliance with the European GDPR (General Data Protection Regulation), personal data (user name, source IP address, source name, source MAC address) is no longer displayed in logs and reports and have been replaced with the term "Anonymized".

To view such data, the administrator must then enable the "Logs: full access" privilege by clicking on "**Logs: limited access**" (upper banner of the web administration interface), then by entering an authorization code obtained from the administrator's supervisor (see the section **Administrators** > **Ticket management**). This code is valid for a limited period defined at the moment of its creation.

To release this privilege, the administrator must click on "**Logs: full access**" in the upper banner of the web administration interface, then click on "**Release**" in the dialog box that appears.

After a privilege is obtained or released, data must be refreshed.

Please note that every time a "Logs: full access" privilege is obtained or released, it will generate an entry in logs.

NOTE
For SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SNi10 and SNi20 models, you can benefit from full functionality by using an external storage medium such as:

- SD card for SN160(W), SN210(W), SN310 and SNi20 models,
- MicroSD card for SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320 and SNi10 models.

The characteristics of these media are specified in the LOGS - AUDIT LOGS section of this guide.

Collaborative security

For more collaborative security, based on vulnerability reports generated by Vulnerability Manager, it is now possible in just one click to increase the level of protection on a host that has been identified as vulnerable. Therefore, when critical vulnerabilities are detected, a new

option will allow you to add affected hosts to a pre-set group and assign a strengthened protection profile or specific filter rules to them (quarantine zones, restricted access, etc.).

For further information, please refer to the Technical Note **Collaborative security**.

Possible actions on reports

Time scale	Changes the time scale in the report. Several choices are possible: last hour, views by day, last 7 days and last 30 days. Note: • The last hour is calculated from the minute before the current minute. • The view by day covers the whole day, except for the current day in which data runs up to the previous minute. • The last 7 and 30 days refer to the period that ended the day before at midnight.
Data refresh	Refreshes displayed data.
Display the	This field can only be accessed if the selected time scale is **Views by day**. Select the desired date from the calendar.
Print the report	Opens the print preview window for the report. A comment field can be added to the report that has been formatted for printing. The **Print** button sends the file to the browser's print module, which allows you to choose whether to print the fie or generate a PDF file.
Download the data in CSV format	Allows data to be downloaded in CSV format.
Display the horizontal histogram	Displays data in the form of a horizontal bar graph.
Display the vertical histogram	Displays data in the form of a vertical bar graph.
Display the pie chart	Displays data in the form of a pie chart.
Show/hide legend	Shows or hides the report's legend. Le legend consists of: • A color for each value in the report, • Numbering that specifies the rank of the values in the report, • The name of values, • The amount of values, • The percentage that the value represents in this report. Depending on the report, additional information or interactive features can be added to the legend (e.g., action of an alarm).

Left-clicking on a value in a report will open a menu offering several interactive features. These may be for example, providing additional information on the value, modifying a parameter of the configuration profile or launching a search in the firewall's logs. Some interactive features can only be accessed in some values of some reports.

Available reports

Web reports

The activity analyzed in the Web category is the combined activity for all queried sites, meaning those belonging to the company's internal networks or those hosted on the internet. These reports relate to HTTP and HTTPS traffic.

For reports relating to *Sites*, possible interactions with the elements and the legend are the querying of a URL's category and direct access to the URL. As for the *Top Web searches*, it allows relaunching the search via Google.

Visited Web sites	Top most visited web sites. These values are evaluated by the number of hits sent to the HTTP server, for the download of files needed for displaying web pages.
Visited Web domains	Top most visited web domains. Through a mechanism that aggregates the number of *Websites* queried, the previous report is built according to *web domains*, which makes it possible to avoid dividing them.
Web category consulted	Top most consulted web categories. For this report, the **URL filtering** module has to be enabled. Keep in mind that the sites queries include those belonging to the internal network (category *Private IP Addresses*).
Web sites volume	Top web sites by exchanged volume. This report is based on the volumes of data exchanged, both sent and received.
Web domains volume	Top web domains by exchanged volume. Through a mechanism that aggregates the number of *Websites* queried, the previous report is built according to *web domains*, which makes it possible to avoid dividing them.
Web category volume	Top web categories by exchanged volume. Traffic is scanned against rules on which a **URL filter** has been applied (*Security* inspection). It relates to volumes of data exchanged, both sent and received.
Users volume	Top users by volume exchanged. Authentication must be configured (refer to the section on Authentication in this Guide). It relates to volumes of data exchanged, both sent and received. This report contains sensitive data and therefore the **Full access to logs (sensitive data)** privilege is required in order to view it.
Blocked Web sites	Top most blocked websites. This report relates to sites that have been blocked by the ASQ engine or by **URL filtering** if it has been enabled (*Security inspection*).
Blocked Web domains	Top most blocked web domains. Through a mechanism that aggregates the number of *Websites* queried, the previous report is built according to *web domains*, which makes it possible to avoid dividing them.
Blocked Web categories	Top most blocked web categories. The **URL filtering** inspection is required in order to obtain these categories. This report relates to sites that have been blocked by the ASQ engine or by **URL filtering** if it has been enabled (*Security inspection*).

Web searches	Top web searches. These values relate to requests sent over the search engines Google, Bing and Yahoo. This report contains sensitive data and therefore the **Full access to logs (sensitive data)** privilege is required in order to view it.

Security reports

Alarm reports are based on the alarms in the **Configuration** module > **Application protection** > **Applications and protections** and system events in the **Configuration** module > **Notifications** > **System events**.

For reports relating to alarms, you can modify the action, change the alert level and access help for the selected alarm. These changes can be made to the profile concerned with the traffic that generated the alarm.

Alarms	Top most frequent alarms. This report displays the alarms that are most frequently raised when the firewall analyzes traffic.
Alarms per host	Top hosts generating alarms. Hosts that generate the most alarms are identified by their DNS names (fqdn) or IP addresses if they do not have DNS names. This report contains sensitive data and therefore the **Full access to logs (sensitive data)** privilege is required in order to view it.
Sessions of Administrators	This report lists the largest number of sessions on the firewall's administration interface, regardless of privileges. This number of sessions is counted in relation to the login of the *Administrator* account and in relation to the IP address of the connected host. As such, the same IP address may be listed several times if different accounts have been used to log on to the firewall from the same host.
Alarms by country	Top countries generating alarms. This report sets out the countries that generate the greatest number of alarms, regardless of whether they are the source or destination of network traffic.
Host reputation	Top hosts showing highest reputation scores. This report sets out the hosts on the internal network that have the highest reputation scores, regardless of whether they are the source or destination of network traffic. This report requires the activation of host reputation management. It contains personal data, so the **Full access to logs (sensitive data)** privilege is required in order to view it.
Detection rate by analytics engine (Sandboxing, Antivirus, AntiSpam)	This report shows the distribution of file analyses, between sandboxing, antivirus and antispam scans.

Virus reports

The **Antivirus** inspection is required for these analyses.

Web virus	Top web viruses. This report lists the viruses detected on web traffic (HTTP and HTTPS if the SSL inspection has been enabled). An interactive feature on the graph makes it possible to go to a description of the virus online (http://www.securelist.com).
Email virus	Top mail viruses. This report lists the viruses detected on mail traffic (POP3, SMTP, POP3S and SMTPS if the SSL inspection has been enabled). An interactive feature makes it possible to go to a description of the virus online (http://www.securelist.com).
Senders of email viruses	Top senders of e-mail viruses. Viruses via e-mail detected in the mail traffic of internal networks (SMTP and SMTPS if the SSL inspection has been enabled) are listed by sender. Senders are identified by their authenticated user logins. Authentication must therefore be configured (refer to the section on **Authentication** in this Guide). This report contains sensitive data and therefore the **Full access to logs (sensitive data)** privilege is required in order to view it.

Spam reports

The **Antispam** module has to be enabled. This data is counted by recipient of spam received, by analyzing SMTP, POP3, SMTPS and POP3S traffic if the SSL scan has been enabled.

Spammed users	Top most spammed users. This report counts spam regardless of the level of trust (level 1-Low, 2-Medium and 3-High). The user is identified by the user name of his e-mail address (without the "@" character and the domain name). It contains personal data, so the **Full access to logs (sensitive data)** privilege is required in order to view it.
Spam ratio	Ratio of spam e-mails received. This report is a ratio. Of all e-mails received and analyzed by the **Antispam** module, three percentages are returned. The proportion of spam, regardless of the level of trust (level 1-Low, 2-Medium and 3-High), the proportion of e-mails scanned but with a failure and the proportion of e-mails that are not considered spam.

Network reports

The activity analyzed in the Network category relates to all traffic passing through the firewall, meaning all protocols. Volumes are calculated on data exchanged, both sent and received.

Hosts per volume	Top hosts by volume exchanged. This data volume concerns all hosts, whether they belong to internal or external networks. This report contains sensitive data and therefore the **Full access to logs (sensitive data)** privilege is required in order to view it.
Protocols per volume	Top protocols by volume exchanged. This report sets out the protocols used most often on all data volumes exchanged by all hosts, whether they belong to internal or external networks.

Users volume	Top users by volume exchanged. The data volume concerns authenticated users. Authentication must be configured (refer to the section on **Authentication** in this Guide). This report contains sensitive data and therefore the **Full access to logs (sensitive data)** privilege is required in order to view it.
Protocols per connection	Top most used protocols by connection. The protocols concern only the protocols from the Application layer of the OSI model. This report sets out the protocols used most often on all connections during the specified period.
Source countries	Top countries identified as network traffic source. This report sets out the countries most frequently identified as the source of network traffic going through the firewall.
Destination countries	Top countries identified as network traffic destination. This report sets out the countries most frequently identified as the destination of network traffic going through the firewall.
Client applications detected	Top most frequently detected client applications. This report sets out the applications on the client side most frequently detected by the intrusion prevention engine during the specified period.
Server applications detected	Top most frequently detected server applications. This report sets out the applications on the server side most frequently detected by the intrusion prevention engine during the specified period.
Client applications per exchanged volume	Top client applications by volume exchanged. This report sets out the client applications used most often on all volumes exchanged by all hosts during the specified period.
Server applications per exchanged volume	Top server applications by volume exchanged. This report sets out the server applications used most often on all volumes exchanged by all hosts during the specified period.

Industrial network reports

Activity analyzed in the Industrial network category covers all traffic from industrial protocols passing through the firewall. Volumes are calculated on data exchanged, both sent and received.

MODBUS servers per volume	Top Modbus servers by exchanged volume. This report sets out the most frequently used servers over all volumes exchanged for the industrial protocol MODBUS.
UMAS servers per volume	Top UMAS servers by exchanged volume. This report sets out the most frequently used servers over all volumes exchanged for the industrial protocol UMAS.
S7 servers per volume	Top S7 servers by exchanged volume. This report sets out the most frequently used servers over all volumes exchanged for the industrial protocol S7.
S7+ servers per volume	Top S7+ servers by exchanged volume. This report sets out the most frequently used servers over all volumes exchanged for the industrial protocol S7+.

OPC UA servers per volume	Top OPC UA servers by exchanged volume. This report sets out the most frequently used servers over all volumes exchanged for the industrial protocol OPC UA.
EtherNet/IP servers per volume	Top EtherNet/IP servers per exchanged volume. This report sets out the most frequently used servers over all volumes exchanged for the Ethernet/IP industrial protocol.
IEC 60870-5-104 servers per volume	Top IEC 60870-5-104 servers per exchanged volume. This report sets out the most frequently used servers over all volumes exchanged for the industrial protocol IEC 60870-5-104.

Sandboxing reports

The **Sandboxing** option must be enabled. Data will be taken into account by analyzing HTTP, SMTP, POP3, FTP and HTTPS, SMTPS and POP3S traffic if SSL analysis has been enabled.

Malicious files detected	Top malicious files detected after sandboxing. This report sets out the malicious files most frequently detected by sandboxing.
Malicious files blocked	Top malicious files detected and blocked by sandboxing request. This report sets out the malicious files most frequently blocked by sandboxing.
Most frequently analyzed file types	Top most frequently analyzed file types. This report sets out the types of files most frequently submitted for sandboxing.
Hosts that have submitted the most files for sandboxing	Top hosts that have submitted files for sandboxing. This report shows the hosts on the network that have warranted the highest number of sandboxing analyses. It contains personal data, so the **Full access to logs (sensitive data)** privilege is required in order to view it.
Protocols that use sandboxing the most frequently	Top protocols that use sandboxing. This report shows the network protocols (HTTP, SSL, SMTP, FTP) that have warranted the highest number of sandboxing analyses.
Users who have submitted the most files for sandboxing	Top users who have submitted files for sandboxing This report shows the users that have warranted the highest number of sandboxing analyses. It contains personal data, so the **Full access to logs (sensitive data)** privilege is required in order to view it.

SD-WAN reports

Activity analyzed in the SD-WAN category includes metrics and operational statuses obtained when monitoring routers and their gateways, regardless of whether they are used in the configuration of the firewall (router objects, default gateway, routers configured in filter rules and return routes).

Latency	Routers and gateways with the highest latency. This report shows the gateways of router objects with the highest latency (in ms). Unreachable routers and gateways do not appear in this report.
Jitter	Routers and gateways with the highest jitter. This report shows the gateways of router objects with the highest jitter (in ms). Unreachable routers and gateways do not appear in this report.

Packet loss	Routers and gateways with the highest packet loss rate. This refers shows the gateways of router objects with the highest packet loss rate.
Unavailability	Routers and gateways with the highest unavailability rate. This report shows the gateways of router objects with the highest unavailability rate.
Functional status	Routers and gateways with the highest functional status. This refers shows the gateways of router objects with the highest functional status rate.
Unreachable status	Routers and gateways with the highest unreachable status. This report shows the gateways of router objects with the highest unreachable status rate.
Degraded status	Routers and gateways with the highest degraded status. This refers shows the gateways of router objects with the highest degraded status rate.

Web service reports

The activity analyzed in the Web service category focuses on traffic relating to mainstream web services defined in the configuration of the firewall as well as custom web services.

Web services by exchanged volume	Top web services by exchanged volume. This report presents the web services found in the firewall's configuration and which account for the highest traffic in terms of data volume.
Web services by number of connections	Top web services by number of connections. This report presents the web services found in the firewall's configuration and which account for the highest number of connections recorded.

REPORT CONFIGURATION

In this module, the firewall's static reports and history curves can be enabled. These are based on all traffic processed by the firewall, i.e., all connections passing through all interfaces, internal and external.

General

Static reports	Enables the static reports shown in the **Monitoring** module > Reports. Static reports are compiled based on logs saved on the firewall. In most reports, a list of the top 10 most frequently recurring values is compiled (the rest of the values are filed under "Other"). SD-WAN reports are based on metrics and operational statuses obtained when monitoring routers and their gateways. Data is refreshed every minute and includes a calculation of a new Top 50 over the last few hours and days in order to better represent the recurring values and avoid overloading the database. Data stored on SD cards can be read by other platforms equipped with an SQLite engine.
History curves	Enables history curves shown in the **Monitoring** module > Monitoring. History curves are compiled based on logs saved on the firewall. They offer four time scales: last hour, day, week or month. These time ranges are calculated in relation to the firewall's date and time settings.

List of reports tab

Possible operations

Search	Filters the list of reports by what is entered in the search field.
Categories	Filters the list of reports by the selected category.
Set status	Enables or disables the report selected beforehand in the grid.
Reset the database	Resets the database.

Additional information

Enabled reports	Shows the number of reports enabled.
Database size	Indicates the disk space used by the SQLite database.

Rule grid

Status	Enables or disables the report in question. Some reports require the subscription of a specific option in order to be enabled. **IMPORTANT** Even though the generation of reports does not have priority over other processes, the number of reports enabled or the type of traffic may have a real impact on the performance of the firewall.
Category	Indicates the data category to which the report belongs. The following categories are available: • Web, • Security, • Virus, • Spam, • Network, • Industrial network, • Sandboxing, • SD-WAN, • Web services, • Custom.
Description	Shows a description of the report and the data it contains.
Warning	Displays a warning message if an option or a feature required to build a report has not been enabled.
Private data	Specifies with a symbol that the report contains personal data (source IP address, host name, user name, etc.). Such data can only be viewed if the user holds the **Full access to logs (private data)** privilege.

NOTE
Such data may be sent via Syslog to the Virtual Log Appliance for Stormshield solution in order to build reports or archive them.

List of history graphs tab

Status	Enables or disables the history graph in question.
Description	Shows a description of history graph and the data it contains.
Warning	Shows a warning message if, for example, an option needed for building a graph has not been enabled.

ROUTING

Routing can be configured in several tabs: IPv6 settings can only be accessed if IPv6 is enabled in the firewall's configuration.

- IPv4/IPv6 static routes: enables the definition of static routes. Static routing represents a set of rules defined by the administrator as well as a default route.
- IPv4/IPv6 dynamic routing: makes it possible to configure dynamic routing protocols (RIP, OSPF, BGP) in the BIRD engine, to allow the firewall to learn routes managed by other devices.
- IPv4/IPv6 return routes: when several gateways are used for load balancing, this tab makes it possible to define the gateway through which return packets will need to go in order to guarantee the consistency of connections.

These segments operate simultaneously, static routing having priority over all the rest during the transmission of a packet over the network.

IPv4/IPv6 static route tabs

These tabs correspond to the list of static routes, the maximum number of which varies according to the model of the appliance. Find out more by consulting the product data sheet available at www.stormshield.com.

The **IPv6 Static routes** tab can only be accessed if IPv6 is enabled in the firewall's configuration.

General configuration

Default gateway (router)	The default router is generally the equipment which allows your network to access the Internet. This is the address to which the firewall sends packets that need to go on the public network. Often the default router is connected to the Internet. If you do not configure the default router, the firewall will not be able to let through packets which have a different destination address from those directly linked to the Firewall. You will therefore be able to communicate between hosts on the internal, external or DMZ networks, but not with any other network (including the Internet). To set the default router, select the object that represents it (Host or Router) from the drop-down menu. If this object does not exist, click on the object creation button to create it. Once it has been selected, the hostname will appear on the screen. This option may be grayed out in several main gateways have been defined.

Static routes

Possible operations

Some operations can also be performed by right-clicking in the grid.

Search	Search that covers host, network and group objects.
Add	Adds a row to the grid. The route (sending of the command) is added once the new line is edited and the fields **Destination network (host, network or group object)** and **Interface** are entered.
Delete	Deletes one or several selected routes.

Once the changes have been made:

Apply	Sends the configuration of the static routes.
Cancel	Cancels the configuration of the static routes.

Static routes

Status	Specifies the status of the static routes. Double-click to enable or disable a route.
Destination network (host, network or group object)	Clicking in this column will open the objects database to select a host, network or group. If the object does not exist, click on the object creation button to create it. This field is mandatory.
Interface	The interface that makes it possible to reach the remote network can be selected from a drop-down list. This field is mandatory.
Address range	This column shows the IP address or group of addresses linked to the items in the column **Destination network (host, network or group object)**.
Protected	This column indicates whether the route is protected. A protected route will be added to the object *Network internals*. The behavior of the security configuration will take this parameter into account. Hosts that can be contacted via this route will be remembered in the intrusion prevention engine.
Gateway	Clicking in this column will open the objects database to select a host or router object that is not involved in load balancing. If the desired object does not exist, click on the object creation button to create it. This field is optional. **NOTE** Load balancing is not compatible with static routes. If you select a router that participates in load balancing, a warning message will inform you that the route cannot be enabled.
Comments	Optional field to enter any text.

IPv4/IPv6 return routes tab

When several gateways are used for load balancing, this tab will allow defining the gateway through which return packets will need to go in order to guarantee the consistence of connections.

The **IPv6 Return routes** tab can only be accessed if IPv6 is enabled in the firewall's configuration.

Return routes

Possible operations

Some operations can also be performed by right-clicking in the grid.

Searching...	Search that covers host, network and group objects.

Add	Adds a row to the grid. An added route (sending of a command) is effective only if its fields **Gateway** and **Interface** have been entered.
Delete	Deletes one or several selected routes.

Once the changes have been made:

Apply	Sends the configuration of the return routes.
Cancel	Cancels the configuration of the return routes.

Return routes

Status	Specifies the status of the return route configuration. Double-click to enable or disable a route.
Gateway	Clicking in this column will open the objects database to select a host or a virtual interface (IPsec). If the object is a host object, it must specify a MAC address. This field is optional.
Interface	A drop-down list allows selecting the outgoing interface for the return route. This field is mandatory.
Comments	Optional field to enter any text.

SMTP FILTERING

This module consists of two sections:

- A drop-down menu that lists the various profiles,
- A grid containing SMTP filter rules.

Profiles

The buttons in this strip allow you to configure the profiles associated with SMTP filtering.

Selecting a profile

The drop-down list offers 10 profiles, numbered from 00 to 09.

Each profile is named "MailFilter_" by default, accompanied by its number.

EXAMPLES

- (0) MailFilter_00,
- (1) MailFilter_01 ...

To select a profile, click on the arrow to the right of the field in which "MailFilter_00" is displayed by default, and select the desired profile.

Each profile is configured as follows by default:

State	Action	Sender	Recipient (to,cc,cci)	Comments
On	Pass	*@*	*@*	default rule (pass all)

Buttons

Edit	This function allows performing 3 operations on profiles: • **Rename**: by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on "Update". This operation can also be cancelled. • **Reinitialize**: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. • **Copy to:** This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the exact date and time of the last modification. Comments can also be added.

Rules

The procedure for editing an SMTP filter profile is as follows:

1. Select a profile from the list of URL filter profiles.
2. The table of filters will then appear as well as a screen indicating errors.

Possible operations

The available buttons are:

Add	Inserts a line to be configured after the selected line.
Delete	Deletes the selected line.
Move up	Places the selected line before the line just above it.
Move down	Places the selected line after the line just below it.
Cut	Removes the selected line and moves it to the clipboard.
Copy	Copies the selected line and moves it to the clipboard.
Paste	Pastes the line from the clipboard above the selected line.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of filter rules:

- Add,
- Delete,
- Cut,
- Copy,
- Paste.

The table

The table contains the following columns:

Status	Status of the rule: • If **Enabled**, the rule is used for filtering. • If **Disabled**, the rule is not used for filtering. If this rule is disabled, the line will be grayed out in order to reflect this. **REMARK** The firewall will assess rules in their order of appearance on the screen: one by one from the top down. As soon as it comes across a rule that corresponds to the request, it will perform the specified action and stop there. This means that if the action specified in the rule corresponds to **Block**, all rules below it will also be set to **Block**.
Action	Allows specifying the result of the rule: **Pass** to allow sending and receiving e-mails, **Block** to prohibit them
Sender	Defines the sender of the e-mail. The value “none” can be selected as a sender.
Recipient (to, cc, cci)	Defines the intended recipient of the e-mail.
Comments	Comments relating to the rule.

An e-mail mask may contain the following syntax:

- *: replaces a character string.

> **EXAMPLE**
> *@company.com allows defining all e-mails from the internet domain of the company called COMPANY.

The following can also be seen:

- ? Replaces a character.
- <none>: This value can only be obtained when the **Sender** field is empty, and is used only for mailer daemons. When an e-mail cannot locate its recipient on a remote mail server, the remote mail server will send back an error message, indicating that there is an error regarding the recipient. In this case, the **Sender** field in this error message will be empty.

A rule with the action “Block” can be created to prevent the e-mail from being sent if the sender is unknown.

Errors found in the SMTP filter policy

The screen for editing SMTP filter rules on the firewall has a rule compliance and coherence analyzer which warns the administrator when a rule inhibits another rule or if there is an error in a rule.

This analyzer groups errors during the creation of rules or incoherent rules.

Errors are displayed in the form of a list. By clicking on an error, the rule concerned will automatically be selected.

SNMP AGENT

IMPORTANT
To keep up to date with the recommendations in RFC2578, and to resolve a compatibility issue with some monitoring applications, all SNMP tables in which the first index was set to 0 have been duplicated to new tables in which the first index is set to 1.

These new SNMP tables (index starting at 1) are now used by default, and older tables are tagged as obsolete. The older tables will be phased out in a future SNS version.

When upgrading to SNS version 5 or higher from a firewall that used the older tables, a warning appears, prompting the administrator to enable new SNMP tables by following this procedure:

1. Connect to the firewall in SSH/Console mode (*admin* or administrator account with Console [SSH] permissions),
2. Edit the section [Config] in the ConfigFiles/snmp configuration file and set the configuration token IndexStartAt1 to "1",
3. Run the SNMP agent using the command *ensnmp*.

The screen for configuring the **SNMP** service consists of three tabs:

- **General**: tab that is displayed by default when users click on the SNMP menu in the tree on the left, and which makes it possible to enable the module, and alarm and system notifications, which will be integrated into the available MIBs (Management Information Base) (lookup and sending of traps).
- **SNMPv3**: Recommended version as it is equipped with more secure tools (security tools such as authentication, encryption, timing control, etc.).
- **SNMPv1 – SNMPv2c**: Version for which the SNMP request contains a name called “Community”, which is used as an ID and transmitted over the network in plaintext.

General tab

This tab allows configuring the system, meaning the host and its administrator. It contains notifications (alarms and system events) which will be integrated into the available MIBs.

	Enables or disables the SNMP agent.

It is however possible to configure the data for this screen even if the module has not been enabled.

SNMPv3 (recommended)	Enables SNMP version 3, the recommended version as it is equipped with more secure tools (security tools such as authentication, encryption, timing control, etc.) Since December 2002, a new standard has been introduced for SNMP, providing a significant advance in security. The configuration requires the following parameters: SNMPv3 offers authentication and encryption methods and resolves certain security issues from earlier versions.

SNMPv1/v2c	Enables versions v1/v2c of SNMP. V1 is the first version of the protocol. The only check made by this version concerns the "Community" character string. Version v2C is a version that improves the types of operations in SNMPv2p and uses "Community" character string security from SNMPv1.
SNMPv1/v2c and SNMPv3	Enables all three versions of SNMP.

Configuration of MIB-II information

Location (sysLocation)	Alphanumeric information regarding the location of the monitored item. This location can be a country, city, server room, etc. Example: France.
Name	Makes it possible to assign a significant name to the SNMP agent on the firewall.
Contact (sysContact)	E-mail address, telephone number, etc. of the contact person when issues arise. E.g., *admin@company.com*

Sending of SNMP alerts (traps)

Intrusion prevention alarms	By selecting: • **Do not send**: you will not receive alarms from the intrusion prevention system. • **Send only major alarms**: you will receive major alarms from the intrusion prevention system. • **Send major and minor alarms:** you will receive major and minor alarms from the intrusion prevention system.
System events	By selecting: • **Do not send**: you will not receive system events from the intrusion prevention system. • **Send only major alarms**: you will receive major system events from the intrusion prevention system. • **Send major and minor alarms**: you will receive major and minor system events from the intrusion prevention system.

NOTE
SNMP can now be configured so that the name of the firewall instead of its serial number is used for SysName.

SNMPv3 tab

The options **Enable the agent SNMPv3 (recommended)** or **SNMPv1/v2c and SNMPv3** make it possible to enable the SNMP v3 module.

Connection to the SNMP agent

Username	Username used for the connection and for looking up MIBs on the firewall.

Authentication

Password	Password of the user who will look up MIBs. This password must comply with the firewall's general password policy defined in the **Password policy** section in the **Configuration** module (*General configuration* tab), and contain at least 8 characters.

Algorithm	The algorithm currently in use appears. A caption will specify whether it is obsolete.
	To use SHA256, use the following CLI/serverd commands:
	`CONFIG SNMP ACCESS USERV3 username=<username> authtype=SHA256 authpass=<passphrase>`
	`CONFIG SNMP ACTIVATE`

Encryption (optional)

Password	SNMP packets are encrypted in DES or AES, and an encryption key can be defined. By default the authentication key will be used. **WARNING** **You are strongly advised to use a specific key.**

Algorithm	The algorithm currently in use appears.
	AES-128 is used by default.
	To change the algorithm, use the following CLI/Serverd command sequence:
	`CONFIG SNMP ACCESS USERV3 username=<username> authtype=<authtype> authpass=<passphrase> privtype=<privtype> privpass=<passphrase>`
	`CONFIG SNMP ACTIVATE`
	More information on the command `CONFIG SNMP ACCESS USERV3`.

Sending SNMPv3 alerts (traps)

Sending traps to hosts takes place in two parts, with the list of hosts on the left, and details on a selected host on the right.

List of SNMP servers

In this screen, you can configure the stations that need to contact the firewall when it needs to send an SNMP trap (event). If no stations (hosts) are specified, the firewall will not send any messages.

A wizard will guide you through the configuration of the hosts.

By clicking to the right of a host name, the objects database will appear, allowing you to select a host.

Server [Name of destination server (object)]

The parameters in the configuration of SNMP v3 events are as follows:

Port	Port used for sending data to the host (*snmptrap* by default).

Username (securityName)	Name of the user allowed to send traps on the management workstation. Do note that when the server ID below has not been entered (engineID), this user name (securityName) has to be the same as the name used for logging in to the SNMP agent.
ID (engineID)	Hexadecimal string created by the management station in order to give the user a unique identification such as 0x0011223344. The engine ID has to be made up of a minimum of 5 bytes and a maximum of 32 bytes. Do note that if this field is empty, the SNMP agent has to be configured to receive an identifier that changes, as it will be automatically generated every time the service restarts.
Security level	Several levels of security are available for the version of the SNMP protocol: • **None**: no security. The sections "Security Level: authentication" and "Security level: Encryption" are grayed out. • **Authentication, no encryption**: authentication of traps without encryption. • **Authentication and encryption**: if the encryption password is not defined, the authentication password will be used for encryption.

Authentication settings

Password	User's password
Algorithm	Two authentication methods are available, MD5 (hash algorithm that calculates a 128-bit digest) and SHA1 (hash algorithm that calculates a 160-bit digest). By default MD5 will be used for authentication.

Encryption settings

Password	SNMP packets are encrypted in DES or AES-128, and an encryption key can be set. By default the authentication key will be used. **WARNING** **You are strongly advised to use a specific key.**

SNMPv1 - SNMPv2c tab

The option **Enable SNMPv1/v2c** or **SNMPv1/v2c** and **SNMPv3** allows enabling the SNMP v1 and v2c modules.

Connection to the SNMP agent

Community	The first versions of the SNMP protocol are not secured. The only field necessary is the community name. By default VPN suggests the name "public". **WARNING** We advise against using it for security reasons. If you wish to indicate several communities, separate them with commas.

Sending of SNMPv2c alerts (traps)

List of SNMP servers

Destination server (object)	Host that receives traps, ("Host" object).
Port	Port used for sending traps to this host (object type: service). By default, *snmptrap*.
Community	Indicates the community.

Sending of SNMPv1 alerts (traps)

By default, the list of hosts that receive v1 traps will be minimized to point the user to version v2c.

List of SNMP servers

Computer	Host that receives traps, ("Host" object).
Port	Port used for sending traps to this host (object type: service). By default, *snmptrap*.
Community	Indicates the community.

MIB and SNMP traps

The Simple Network Management Protocol (SNMP) allows you to monitor all hosts installed on your network. SNMP alerts (traps) and data listening (MIB) can be configured using the **SNMP Agent** module in the firewall's web administration interface.

In it, you can configure the workstations to which the firewall must send traps, and configure access to those that gather data. This manager allows you to communicate with the SNMP agent on a firewall and to obtain, manage and monitor data from any firewall through the network. The SNMP agent authorizes read-only access to supervisors that comply with SNMP versions v1, v2c, and v3.

To configure data tracking and receive Stormshield *traps*, you must first download MIBs (text files that describe a list of SNMP objects that the supervisor uses). These MIBs therefore provision data that the supervisor may need in order to interpret SNMP traps, events and request messages sent to the firewall.

Downloading MIBs

Download MIBs from your MyStormshield personal area (authentication required): in **Downloads** > **Downloads** > **Stormshield Network Security** > **SNMP MIB** > MIB corresponding to your SNS version.

Stormshield Network MIB

The following is the list of Stormshield Network MIBs, the corresponding CLI/Serverd commands and console commands.

STORMSHIELD-SMI-MIB is the top-level MIB of all MIBs.
STORMSHIELD-VPN-MIB is the top-level MIB of *VPNIKESA*, *VPNSA* and *VPNSP*.

Stormshield Network MIB	Contents	CLI/Serverd	Console
STORMSHIELD-ALARM-MIB	Triggered alarms		sfctl -s log
STORMSHIELD-ASQ-STATS-MIB	IPS statistics		sfctl –s stat
STORMSHIELD-AUTHUSERS-MIB	Authenticated users	MONITOR USER	sfctl -s user
STORMSHIELD-AUTOUPDATE-MIB	Status of modules updated by Active Update	MONITOR AUTOUPDATE	
STORMSHIELD-HA-MIB	Information on high availability	HA INFO	hainfo
STORMSHIELD-HEALTH-MONITOR-MIB	Health status of firewalls	MONITOR HEALTH	
STORMSHIELD-HOSTS-MIB	Table of protected hosts	MONITOR HOST	sfctl -s host
STORMSHIELD-IF-MIB	Status of interfaces seen by IPS	MONITOR INTERFACE	sfctl -s global
STORMSHIELD-IPSEC-STATS-MIB	IPsec statistics		ipsecinfo
STORMSHIELD-MODEL-MIB	Firewall models		
STORMSHIELD-OVPNTABLE-MIB	Clients connected to the SSL VPN	MONITOR OPENVPN LIST	
STORMSHIELD-POLICY-MIB	Filter policy	MONITOR POLICY	slotinfo
STORMSHIELD-PROPERTY-MIB	Information returned by the "SYSTEM PROPERTY" command	SYSTEM PROPERTY SYSTEM IDENT SYSTEM LANGUAGE	
STORMSHIELD-QOS-MIB	Information on QoS	MONITOR QOS	sfctl -s qos
STORMSHIELD-ROUTE-MIB	Table of routers	MONITOR ROUTE	sfctl -s route
STORMSHIELD-SERVICES-MIB	Status of firewall services	MONITOR SERVICE	dstat
STORMSHIELD-SYSTEM-MONITOR-MIB	IPS resource usage counters	MONITOR STAT	
STORMSHIELD-VPNIKESA-MIB	Table of negotiated IKE SAs	MONITOR GETIKESA	
STORMSHIELD-VPNSA-MIB	Table of SAs	MONITOR GETSA	showSAD
STORMSHIELD-VPNSP-MIB	Table of SPs	MONITOR GETSPD	showSPD

SSL FILTERING

This module allows filtering access to secure web sites. It also makes it possible to allow or prohibit web sites or certificates that pose risks.

This module consists of two sections:

- A drop-down menu that lists the various profiles,
- A grid containing SSL filter rules.

NOTE
To set up a URL/SSL filter policy, you are advised to operate in blacklist mode, i.e., explicitly group the URL categories to be prohibited in a custom URL group. A URL/SSL filter rule will then be applied to this group with a *block* action. This rule must then be placed above the rule that allows all the other categories.

Profiles

The buttons in this strip allow you to configure the profiles associated with SSL filtering.

Selecting a profile

The drop-down list offers 10 profiles, numbered from 00 to 09.

Each profile is named "SSLFilter_" by default, accompanied by its number.

EXAMPLES

- (0) SSLFilter_00,
- (1) SSLFilter_01…

To select a profile, click on the arrow to the right of the field in which "Default00" is displayed by default, and select the desired profile.

Each profile is configured as follows by default:

State	Action	URL-CN	Comments
On	Decrypt	any	default rule (decrypt all)

Buttons

Edit	This function allows performing 3 operations on profiles: • **Rename**: by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on "Update". This operation can also be cancelled. • **Reinitialize**: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. • **Copy to:** This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the exact date and time of the last modification. Comments can also be added.
URL database provider	This link redirects to the module that allows configuring the URL database provider (**Objects** / **URL** module / *URL database* tab).

Rules

The procedure for editing an SSL filter profile is as follows:

1. Select a profile from the list of SSL filter profiles.
2. The table of filters will then appear as well as a screen indicating errors.

> **NOTE**
> To set up a URL/SSL filter policy, you are advised to operate in blacklist mode, i.e., explicitly group the URL categories to be prohibited in a custom URL group. A URL/SSL filter rule will then be applied to this group with a *block* action. This rule must then be placed above the rule that allows all the other categories.

Possible operations

A multiple selection allows assigning the same action to several rules. Select several successive alarms using the **Shift** ⇧ key or individually by holding down the **Ctrl** key. You can also remove an item from an existing selection with the **Ctrl** key.

Some column titles have the icon . When you click on it, a menu appears and suggests assigning a setting to several selected rules (*Status* and *Action*).

> **EXAMPLE**
> Several lines can be deleted at the same time, by selecting them with the **Ctrl** key and pressing on **Delete**.

The available buttons are:

Add	Inserts a line to be configured after the selected line.
Delete	Deletes the selected line.

Move up	Places the selected line before the line just above it.
Move down	Places the selected line after the line just below it.
Cut	Removes the selected line and moves it to the clipboard.
Copy	Copies the selected line and moves it to the clipboard.
Paste	Pastes the line from the clipboard above the selected line.
Add all predefined categories	This button makes it possible to create as many filter rules as the number of URL categories in the selected URL base at once. All rules created in this way are enabled and the associated action by default is *Decrypt*.
Purge rules	This button is useful for EWC SSL filter policies that were created before SNS version 4.7.1 EA, and which were migrated when the URL database provider was changed (SNS 4.7.1 EA or higher). It deletes rules using categories that no longer have an equivalent in the URL database of the current provider as of SNS version 4.7.1 EA.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of filter rules:

- Add,
- Delete,
- Cut,
- Copy,
- Paste.

Rule grid

The table contains the following columns:

Status	Status of the rule: • If **Enabled**, the rule is used for filtering. • If **Disabled**, the rule is not used for filtering. If this rule is disabled, the line will be grayed out in order to reflect this. **REMARKS** The firewall will assess rules in their order of appearance on the screen: one by one from the top down. As soon as it comes across a rule that corresponds to the request, it will perform the specified action and stop there. This means that if the action specified in the rule corresponds to **Block**, all rules below it will also be set to **Block**.

Action	Allows specifying the operation to perform: • If **Pass without decrypting** is specified, access to the requested CN will be allowed without a prior SSL analysis. • If **Block without decrypting** is specified, access to the requested CN will be denied, without any SSL analysis being applied. The connection will be shut down. • If **Decrypt** is specified, the protocol analysis will be applied to the decrypted traffic, as well as on the proxy, if a rule has been created for it. • If BlockPage_XX is specified, access to the requested CN will be denied, without any SSL analysis being applied. The connection will be shut down and the user will see the selected block page (BlockPage_XX). These block pages can be edited and customized in Block page tab of the BLOCK MESSAGES module.
URL-CN	This action applies according to the value of this column. It may contain a group or URL category, as well as a group of certificate names.
Comments	Comments relating to the rule.

Errors found in the SSL filter policy

The screen for editing SSL filter rules on the firewall has a rule compliance and coherence analyzer which warns the administrator when a rule inhibits another rule or if there is an error in a rule.

This analyzer groups errors during the creation of rules or incoherent rules.

Errors are displayed in the form of a list. By clicking on an error, the rule concerned will automatically be selected.

SSL VPN

SSL VPN allows remote users to securely access a company's resources - internal or otherwise - via the SNS firewall. An SSL VPN client must be installed on the user's workstation or mobile device before a VPN tunnel can be set up with the SNS firewall.

Several VPN clients are compatible with the SSL VPN service on the SNS firewall. Stormshield's SSL VPN client (SN SSL VPN Client) has a connection mode that allows it to automatically and securely retrieve its VPN configuration, unlike OpenVPN Connect, on which the VPN configuration must be manually integrated.

Enabling the SSL VPN service

Enable SSL VPN ON OFF	Enables or disables VPN SSL on the SNS firewall.

Configuring the SSL VPN service

Three tabs allow you to respectively configure:

- The general settings of the SSL VPN service,
- The policy verifying the compliance (ZTNA) of SSL VPN clients. Zero trust network access (ZTNA) consists of trusting users and devices only after they have been verified.
- The policy verifying the compliance (ZTNA) of Microsoft Windows client workstations.

> **NOTE**
> If the LZ4 compression feature in the SSL VPN service is enabled, a warning message will automatically appear when the module opens, encouraging you to disable the feature. You are strongly advised to disable it for security reasons. If you ignore this warning, a message will be displayed until it is disabled. To disable it, use the CLI Serverd commands:
> `CONFIG OPENVPN UPDATE compress=0` then `CONFIG OPENVPN ACTIVATE`.

Do note that in order to set up SSL VPN tunnels, the **Authentication, Access privileges** and **Filter - NAT** modules must also be configured. For more information, refer to the technical note Configuring and using the SSL VPN on SNS firewalls.

General configuration tab

Enable client workstation verification (ZTNA) ON OFF	Set the selector to **ON** to enable the verification of client workstation compliance. When it is enabled: • Compatible SSL VPN clients can set up SSL VPN tunnels with the firewall **only if all** the criteria defined in the policy have been met, • Incompatible SSL VPN clients cannot set up SSL VPN tunnels with the firewall, **unless** permissive mode has been enabled.

Network settings

Public IP address (or FQDN) of the UTM used	Indicate the IP address that users must use to reach the SNS firewall in order to set up VPN tunnels. You can indicate either an IP address or FQDN. • For IP addresses: they must be public, and therefore accessible over the Internet, • For FQDNs: they must be declared on the DNS servers that the workstation uses when it is outside the corporate network. If you have a dynamic public IP address, you can use the services of a provider such as *DynDNS* or *No-IP* dynamic, and then configure this FQDN in the Dynamic DNS module.
Available networks or hosts	Select the object representing the networks or hosts that will be reached through the VPN tunnel. This object makes it possible to automatically set on the workstation the routes needed to reach resources that can be accessed via the VPN. Filter rules (in the Filter - NAT module) will be necessary to more granularly allow or prohibit traffic between remote workstations and internal resources. You may also need to set static routes for access to the network assigned to VPN clients on corporate network devices located between the SNS firewall and the internal resources provided.
Network assigned to clients (UDP) **Network assigned to clients (TCP)**	Select the object corresponding to the network that has been assigned to VPN clients in UDP and TCP. The network mask must not be smaller than **/28**. If you assign two networks, VPN client will always choose the UDP network first to ensure better performance. Choosing the network or sub-networks: • The assigned network must not belong to any existing internal networks, or networks declared by a static route on the SNS firewall. Since the interface used for the SSL VPN is protected, the firewall would then detect an IP spoofing attempt and block the corresponding traffic. • To avoid routing conflicts, select less commonly used sub-networks (such as 10.**60**.**77**.0/24) as many filtered Internet access networks (public Wi-Fi, hotels, etc) or private local networks already use the first few reserved address ranges.
Maximum number of simultaneous tunnels allowed	The number appears automatically. This number corresponds to the lowest value, either the number of tunnels allowed on the SNS firewall, or the number of sub-networks available for VPN clients. For sub-networks, this shows the total number of IP addresses, minus 3.

DNS settings sent to client

Domain name	Enter the domain name assigned to the SSL VPN clients so that they can resolve their host names.
Primary DNS server **Secondary DNS server**	Select the object representing the DNS server to be assigned.

Advanced properties

Enable DCO kernel acceleration	Select the checkbox to enable the DCO (Data Channel Offload) kernel acceleration feature. This option is enabled by default in factory configuration. This feature transfers the encryption/decryption of data packets passing through SSL VPN tunnels to the operating system kernel. This increases the performance of **UDP-based tunnels** and enables the SSL VPN service to process the setup of many more UDP tunnels. This feature is not compatible with **TCP-based tunnels**. **NOTE** When the checkbox is selected, if the encryption suite used by the SSL VPN service is incompatible with the DCO kernel acceleration feature, a window appears, encouraging you to use the AES-256-GCM encryption suite. Accept the change to enable the feature.
Public IP address of the UTM for the SSL VPN (UDP)	In either of the following cases, you need to select the object representing the IP address used for setting up UDP SSL VPN tunnels: • The IP address used for setting up the SSL VPN tunnels (UDP) is not the main IP address of the external interface. • The IP address used for setting up the SSL VPN tunnels (UDP) belongs to an external interface that is not linked to the default gateway of the firewall.
Port (UDP) **Port (TCP)**	The listening ports of the SSL VPN service can be changed. Note: • Some ports are reserved for the SNS firewall's internal use only and cannot be selected, • Port 443 is the only port below 1024 that can be used, • If you change any of the default ports, the SSL VPN could become inaccessible from networks (hotels or public WiFi) on which Internet access is filtered.
Interval before key renegotiation (in seconds)	You can change the length of time (14400 seconds by default, or 4 hours) after which the keys used by the encryption algorithms will be renegotiated. During this operation: • The SSL VPN tunnel will not respond for several seconds, • If multifactor authentication is used, the user will need to enter a new OTP, or approve the new connection on the third-party application (in push mode), in order to stay connected. It would be helpful to set an interval that corresponds to the average length of a workday, such as 28800 seconds (8 hours).
Use DNS servers provided by the firewall	You can instruct VPN clients to include the DNS servers retrieved via the SSL VPN in the workstation's (Windows only) network configuration. If DNS servers are already defined on the workstation, they may be queried.
Prohibit use of third-party DNS servers	You can instruct VPN clients to exclude the DNS servers that have already been defined in the workstation's (Windows only) configuration. Only DNS servers sent by the SNS firewall can be queried.

Scripts to run on the client

In Windows, the Stormshield SSL VPN client can run *.bat* scripts when an SSL VPN tunnel is opened or closed. In these scripts, you can use:

- Windows environment variables (**%USERDOMAIN%**, **%SystemRoot%**, etc.),
- Variables relating to the Stormshield SSL VPN client: **%NS_USERNAME%** (user name used for authentication) and **%NS_ADDRESS%** (IP address assigned to the SSL VPN client).

Script to run when connecting	Select the script to run when the VPN tunnel is opened. Example of a script that makes it possible to connect the Z: network drive to the shared network: `NET USE Z: \\myserver\myshare`
Script to run when disconnecting	Select the script to run when the VPN tunnel is closed. Example of a script that makes it possible to disconnect the Z: network drive from a shared network: `NET USE Z: /delete`

Certificates

Select the certificates that the SNS firewall's SSL VPN service and the Stormshield SSL VPN client must present to set up a tunnel. They must be issued from the same certification authority. The default suggestions are the certification authority dedicated to the SSL VPN, and a server certificate and a client certificate created when the firewall was initialized.

Server certificate	Select the desired certificate. The icon indicates certificates with a TPM-protected private key. For more information on the TPM, see the section Trusted Platform Module.
Client certificate	Select the desired certificate. Client certificates with a TPM-protected private key cannot be selected as the private keys of such certificates must be available in plaintext (unencrypted) in the VPN configuration that is distributed to VPN clients.

Configuration

Export the configuration file	Click on this button to export the SSL VPN configuration in *.ovpn* format.

Client workstation verification (ZTNA) tab

A policy can be set up to verify the compliance of client workstations (ZTNA) that set up SSL VPN tunnels with the SNS firewall. With this verification, workstations or users that do not comply with the criteria in the policy will not be able to set up SSL VPN tunnels with the SNS firewall.

This use case requires the Stormshield SSL VPN client in version 4.0 or higher on each workstation in the corporate network.

Stormshield SSL VPN client version

Select the checkbox to enable the settings section of the required versions.

Allow a version range (at least v4.0.0)	Select this option if you have a varied pool of Stormshield SSL VPN clients, and wish to allow several versions of the client to set up tunnels with the firewall. You must then enter the **Lowest version** of Stormshield SSL VPN clients that are allowed to set up tunnels. You can enter the **Highest version** or leave this field empty to allow all versions equal to or higher than the lowest specified version.

Allow only one version	Select this option to exclusively allow one Stormshield SSL VPN client version. You must then enter the exact version of Stormshield SSL VPN clients that are allowed to set up tunnels.

Allow tunnels to be set up for the following additional clients

Stormshield SSL VPN clients for (Linux or macOS)	Select the option if you have client workstations with a Linux or Mac Stormshield SSL VPN client (available soon). By doing so, specific Windows criteria will not be applied to these workstations, and you will not need to adapt your criteria to them.
SSL VPN clients incompatible with ZTNA	Select the checkbox to enable permissive mode, which allows SSL VPN clients that are incompatible with the client workstation verification feature to set up tunnels with the SNS firewall. With this permissive mode, it is possible to: • Progressively update a pool of Stormshield SSL VPN clients to a compatible version, • Continue using third-party SSL VPN clients.

Customized message for incompatible workstations

If an SSL VPN tunnel fails to set up because the workstation or user is non-compliant, the Stormshield SSL VPN Client displays the default message "For more information, please contact support" in English, French and German.

In the text entry section, you can change the message, or delete it if you do not wish to display an additional message. Do note that as automatic translation mechanisms have not been set up: you will need to have the message translated with your own means.

You can reset the additional message that you have written by clicking on **Go back to messages suggested by default**.

Windows client workstation verification (ZTNA) tab

Windows client workstations are verified based on different criteria. Do note that if you select several criteria from those described below, the SSL VPN client has to meet all the defined criteria to be allowed to set up tunnels with the firewall.

Client workstation antivirus enabled and up to date	The workstation must be equipped with an active antivirus program **with** the latest antivirus database updates. This information is based on the status of the antivirus recognized by the Windows Security center. Third-party antiviruses are therefore supported as long as the Windows Security center recognizes their status.
Active firewall on the client workstation	The Windows firewall must be running on the workstation, and the *domain network*, *private network* and *public network* profiles must be enabled. If a profile is disabled, the criterion will be considered non-compliant.
SES installed on the client workstation	In infrastructures that have deployed SES Evolution, the SES agent must be installed on the workstation. Do note that the configuration and status of the SES agent are not taken into account.

Prohibit users holding administration privileges on the client workstation	Users who hold administrator privileges on the workstation cannot set up tunnels with the SNS firewall.

Check the Windows 10/Windows 11 version (build number)

Select the checkbox to enable the settings section of the required Windows 10 and Windows 11 versions. Two tabs are available, depending on the Windows version in question.

Allow a version range (builds)	When this option is selected, you have to enter the **Lowest version** that the workstation must run (by default 10000 for Windows 10 and 20000 for Windows 11). You can enter the **Highest version** that the workstation must run, or leave this field empty to allow all versions equal to or higher than the lowest specified version.
Allow only one version	When this option is selected, you have to enter the exact Windows version of workstations that are allowed to set up tunnels.

Membership in a company domain

Ensure that the host is connected to a company domain	When this option is selected, you have to add to the grid the domains of the workstations that are allowed to set up tunnels. Do note that this criterion is not related to the configuration of directories on the firewall.
Ensure that the user belongs to a company domain	When this option is selected, you have to add to the grid the domains of users who are allowed to set up tunnels. With this criterion, the user's full name, including the domain, will be verified. As such, even if the workstation is connected to a domain, local users on the workstation will not be able to set up tunnels. Do note that this criterion is not related to the configuration of directories on the firewall.

MULTICAST ROUTING

Multicast routing is a technology that aims to preserve bandwidth by delivering a single information flow to several recipients, potentially in a very large number (several thousands). With IP multicast, simultaneous content can be delivered by using the least bandwidth possible and without overloading either the sender or receivers.

This distribution method is an advantage for applications such as video-conferencing, e-learning, stock market quotes, or video on demand.

> **NOTE**
> Static or dynamic multicast routing has priority over all other types of routing (static routing, dynamic routing, routing in a bridge, policy-based routing, etc).

	This switch makes it possible to enable or disable multicast routing. Static routing **or** dynamic routing must then be selected. **IMPORTANT** Static multicast routing and dynamic multicast routing cannot be enabled simultaneously.
Static routing	With this radio button, static multicast routing and its configuration tab can be enabled.
Dynamic routing	With this radio button, dynamic multicast routing and its configuration tab can be enabled.

STATIC ROUTING TAB

Possible operations on rules in the static multicast routing policy

In this grid, you can set the rules in the multicast routing policy that will be applied on the firewall. High-priority rules are placed on top. The firewall executes rules in their order of appearance in the list (rule no. 1, 2 and so on) and stops as soon as it reaches a rule that matches the traffic that it processes.

Add	Inserts a line after a selected line; a routing rule creation wizard will then open automatically.
Delete	Deletes the selected line.
Move up	Places the selected rule before the rule just above it.
Move down	Places the selected rule after the rule just below it.
Cut	Cuts a routing rule in order to move it.
Copy	Copies a routing rule in order to duplicate it.
Paste	Duplicates a routing rule after having copied it.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the grid of multicast static routes:

- Add,
- Delete,
- Up,
- Down,
- Cut,
- Copy,
- Paste.

New rule

Step 1: selecting the multicast group and the source interface

Select the multicast object containing allowed multicast IP addresses as well as the multicast traffic source (source interface) for this routing rule.

The multicast group must contain a host, network, IP address range or group containing exclusively multicast IP addresses (within the range 224.0.0.0 - 239.255.255.255 inclusive).

Step 2: selecting the destination interfaces

Click on **Add** to target the destination of the traffic affected by the multicast routing rule. You can add as many destination interfaces as necessary in the rule.

A multicast packet matching the rule (packet originating from an address contained in the multicast group and being presented by one of the declared source interfaces) will be sent to all destination interfaces.

Rule grid

The grid sets out the list of static multicast routing rules and their statuses:

Status	Status of the static multicast route: • on: the route is in operation. • off: the route is not in operation. Double-click to enable the route.
Source interface	Displays the multicast group and the associated source interface in the following form: multicast_group@source_interface.
Destination interfaces	Displays the list of destination interfaces of the multicast traffic specified in the routing rule creation wizard.
Comments	Displays any comments that may have been entered when the rule was added.

Dynamic routing tab

Definitions

- Multicast source: source sender (e.g., video camera).
- Multicast receiver: receiver of multicast traffic (subscribed to the multicast group).
- Multicast group: multicast address (private, public, SSM).
- (S,G) - multicast (Source, Group): source IP address and multicast group address pair.
- IGMP (*Internet Group Management Protocol*): protocol used by a multicast receiver to subscribe to or unsubscribe from a multicast group.
- PIM (*Protocol Independent Multicast*): family of multicast IP routing protocols.
- PIM-SM (*PIM Sparse Mode*): version of PIM that builds a distribution tree. This is a scalable version of the protocol, making it possible to manage multiple sources. The distribution tree can be:
  - In shared mode, by going through a Rendez-vous Point (Shared Tree or RPT),
  - Set up by recalculating the shortest path tree (SPT), through unicast routing.
- PIM-SSM (*PIM Source-Specific Multicast*): version of PIM in which receivers know the source. When the receiver subscribes, the source IP address and multicast group address pair will be formed directly. This protocol is easier to set up than PIM-SM (no RP involved), but requires IGMPv3 and is meant for a more restricted application type.
- RP (*Rendez-vous Point*): role held by a PIM-SM router. The RP is contacted to discover and indicate the multicast source.
  The SNS firewall can play this role.
- BSR (*BootStrap Router*): role held by a PIM router. The BSR is elected from a list of candidates. Once it is elected, it will gather candidacies for the role of RP, then shares the table of multicast group/RP associations with other routers.
  The SNS firewall can play this role.

Interfaces & candidate rendez-vous points (dynamic RPs)

This section defines all the interfaces involved in dynamic multicast routing:

- Source and/or destination interfaces using the IGMP protocol,
- IGMP protocol versions that these interfaces can accept for source advertisements or receiver subscriptions and unsubscriptions,
- Interfaces used by a firewall acting as a candidate dynamic rendez-vous point (RP) and associated multicast groups,
- Interfaces used by a firewall acting as a candidate bootstrap router (BSR).

To allow packets originating from these protocols going to the firewall's interfaces, the Allow IGMP and PIM packets to be received for dynamic multicast routing to function implicit filter rule must be enabled. It is enabled by default.

Possible operations

Select all	Selects all the lines shown in the grid to delete them in a single action.
Add	Inserts a line after a selected line to add an interface.

Delete	Deletes the selected line.
Edit selection	This button makes it possible to edit the selected line.

Rule grid

Interface	Interface involved in multicast routing: • Interface used for IGMP announcements (subscription or unsubscription requests from multicast receivers). Example: *in* and *out* interface on the firewall. • Interfaces used for RP candidacies (C-RP). You are advised to use local loopback interfaces that have been defined for this purpose. These interfaces must have routable IP addresses.
IGMP version	Versions of the IGMP protocol that this interface can accept for subscription or unsubscription requests from multicast receivers. Possible choices are: • **IGMP v2 only,** • **IGMP v2 and IGMP v3.**
DR priority	The Designated Router (DR) is the border router (last router encountered before a multicast source or multicast receiver) that forwards subscription requests to the RP. DRs are elected. Indicate the priority assigned to the firewall in its candidacy to act as the DR for a given multicast group. **IMPORTANT** The interface with the **lowest** priority number will have the highest priority among all candidates. If both interfaces have the same priority, the interface with the highest IP address will have priority.
C-RP (Candidate Rendez-vous Point)	Select this checkbox to enable the firewall's candidacy to the role of RP for the associated multicast group.
Priority C-RP (Candidate Rendez-vous Point)	**IMPORTANT** The interface with the **lowest** priority number will have the highest priority among all candidates. If both interfaces have the same priority, the interface with the highest IP address will have priority.
Multicast groups	Specify the multicast group associated with the C-RP.

Adding an interface

NOTE
Bridges and bridged interfaces cannot be selected as multicast interfaces.

To add an interface to the list of interfaces participating in dynamic multicast routing:

1. Select the line in the grid under which you want to create a new entry.
2. Click on **Add**.
3. Select the interface.
4. Select the IGMP protocol version allowed for this interface: **IGMP v2 only** or **IGMP v2 and IGMP v3**.

> **NOTE**
> If you wish to use the PIM-SSM protocol, you must choose **IGMP v2 and IGMP v3** because only IGMP v3 is compatible with this protocol.

5. Specify the priority assigned to this interface.
   This concept of priority is important in an architecture with multiple access, in which several SNS firewalls or routers manage dynamic multicast routing over the same local network. In fact, priority makes it possible to elect the Designated Router (DR), which will then send requests to the RP via the interface with the highest priority.

> **NOTE**
> The interface with the lowest priority number will have the highest priority in routing multicast traffic.
> If both interfaces have the same priority, the interface with the highest IP address will have priority.

6. If you want the firewall to participate in RP elections with this interface, select **Be a candidate for the Rendez-vous Point (RP)**. In this case, complete the configuration by selecting:
   - A C-RP (Candidate Rendez-vous Point) priority,
   - One or several multicast groups for which the firewall will act as the RP, if it is elected.

Possible interactions

Some operations listed in the taskbar can be performed by right-clicking on the grid of interfaces:

- Add,
- Delete,
- Edit selection

PIM-SM settings

Be a candidate for the Bootstrap Router (BSR) role

The presence of a Bootstrap Router (BSR) is essential in a configuration that uses dynamic Rendez-vous Points (RPs), as it manages the RP election process:

- Collects candidacies from C-RPs,
- Elects RPs for each multicast group,
- Announces the RPs in charge of the various multicast groups.

When a a BSR is already configured on the network, the SNS firewall cannot be a candidate to this role.

If you want the SNS firewall to be eligible for election as a BSR, use this grid:

Address	Select the network interface on the firewall that will be used as the firewall's identifier in the election mechanism. It may be an interface on the firewall (example: *Firewall_out*), but you are advised to use local loopback IP addresses that have been specifically defined for such a purpose, as they do not depend on physical interfaces that may have varying statuses. This interface must have been declared in the interfaces involved in multicast routing. Loopback interfaces can be defined in **Network** > **Virtual interfaces** > **Loopback** tab. More information on creating loopback interfaces.
Priority	This concept of priority is important in an architecture for which several devices are BSR candidates - the device that has the interface with the highest priority will be elected. **IMPORTANT** The interface with the **highest** number will have the highest priority. If both interfaces have the same priority, the interface with the highest IP address will have priority.

Static Rendez-vous Points (RP)

NOTE
Multicast groups must be very thoroughly managed (no address overlaps tolerated) so that the RP election mechanism can be used while static RPs are being defined.

If you wish to define static Rendez-vous Points (without going through an election mechanism), use this grid.

Possible operations:

- To add a static RP definition, click on **Add**, then fill in the two fields below:

Range	Multicast address range (multicast group) that the static RP will manage. This may be a group of addresses or a range that includes the multicast IP addresses of videosurveillance cameras, for example. This range may either be an existing custom range defined in the firewall's network objects, or can be created directly from this grid.
Address	IP address of the RP in charge of the specified multicast group. It may be an interface on the firewall (example: *Firewall_out*), but you are advised to use local loopback IP addresses that have been specifically defined for such a purpose, as they do not depend on physical interfaces that may have varying statuses. This interface must have been declared in the interfaces involved in multicast routing. Loopback interfaces can be defined in **Network** > **Virtual interfaces** > **Loopback** tab. More information on creating loopback interfaces.

IMPORTANT
Every static RP entry (IP address) has to be identical on all devices involved in the multicast routing of the range in question.

- To delete a static RP definition, select the corresponding line and click on **Delete**.
- To delete all static RP definitions, click on **Select all**, then on **Delete**.

NOTE
There is a disadvantage to using static RPs: there is no redundancy if the RP in charge of the specified multicast group is down.

Advanced configuration

Interval between two Hello messages	Interval (in seconds) between two Hello packets sent to other devices that manage the PIM protocol. The default value is 30 seconds.
Interval between two IGMP requests	Interval (in seconds) between two requests for the purpose of gathering subscription requests from multicast receivers or detecting ended subscriptions. The default value is 5 seconds.

STORMSHIELD MANAGEMENT CENTER

If you have installed the Stormshield Management Center centralized administration server, this panel will allow you to install the connecting package in order to connect your firewall to the SMC server.

> **IMPORTANT**
> If you have logged on via the web administration interface to a firewall connected to an SMC server, "**Managed by SMC**" will be displayed in the upper panel. By default, the account used only has read-only access privileges.
> You are strongly advised against directly modifying the configuration of a firewall administered by an SMC server, except in an emergency (SMC server uncontactable, for example).
> This is because any changes made directly to the configuration via the web administration interface on a firewall connected to an SMC server may be overwritten when a new configuration is sent from the SMC server.
> For more information on implementing SMC, refer to the SMC installation guide and the SMC administration guide.

Connecting the firewall to the SMC server

Select the connecting package	Choose the SMC connecting package from the centralized administration server.

Buttons

Install the package: When a connecting package has been selected, this button will download and install it on the firewall.

Connection settings

Once the package has been installed, information regarding the connection to the server will then be displayed (IPv4/IPv6 address of the server, connection validity, verification frequency for this connection, timeout before the server's response, timeout before reconnection).

> **NOTE**
> For more information on Stormshield Management Center centralized administration, refer to the SMC installation guide and SMC administration guide.

TPM

When the firewall is equipped with a TPM, this section makes it possible to protect the private key in the certificate that is used for communications with the SMC server. Click on **Protect the SMC agent** to enable this protection.

If the firewall is already connected to an SMC server during the initialization of the TPM, the private key of the certificate that is used for communications with the SMC server will be automatically protected.

For more information on the TPM, see the section Trusted Platform Module.

SYSTEM EVENTS

In this module, you will be able to configure the alarm level of the various system events that may occur (attacks, update failures, invalid CRLs, etc).

It consists of a single screen, listing events by number and in alphabetical order, with the possibility of searching for a particular event.

Possible operations

There are two actions you can perform in this section.

Search

This field allows you to search by occurrence, letter or word. You can as such filter elements in the list in order to view only those you need.

Example

If you enter "CRL" in the field, all messages containing this term will be displayed in the table.

Restore the default configuration

This button will allow you to cancel all changes you have made earlier in the system event configuration.

When you click on this button, a confirmation message will appear, allowing you to confirm or cancel the action.

List of events

The screen consists of three columns, as well as a help page at the end of the line for each event type.

ID	This field shows the number that identifies the event. It cannot be edited.
Level	This column shows the default alarm levels assigned to events. There are 4 levels, which you can modify by selecting the desired level from the drop-down list. This list appears when you click on the downward arrow on the right: • **Ignore**: no logs on the event will be kept. • **Minor**: as soon as the event in question is detected, a minor alarm will be generated. This alarm is transferred to the logs, and can be sent by Syslog (Logs – Syslog) or by e-mail (see module E-mail alerts). • **Major:** as soon as the event in question is detected, a minor alarm will be generated. This alarm is transferred to the logs, and can be sent by Syslog (Logs – Syslog) or by e-mail (see module E-mail alerts). • **Log:** the Stormshield Network firewall does not do anything. This is useful when you wish to log only certain types of traffic without applying any particular action.

Message (language depends on the firewall language)	This field shows the name of the system event and its characteristics (cannot be edited). **NOTE** By clicking on the arrow on the right side of the column header, you can invert the order in which events appear.
Open help	When you select an event from the list by clicking on it, a **Show help** link appears. Clicking on this link will take you to the Stormshield Network knowledge base, providing more details on the information relating to the event.
Configure	When you select an event from the list by clicking on it, a **Configure** link appears. By clicking on it, an advanced configuration window will appear: **Send an e-mail**: an e-mail will be sent when this alarm is raised (cf. module **E-mail alerts**) with the following conditions: • **Number of alarms before sending**: minimum number of alarms required before an e-mail is sent, during the period defined below. • **During the period of (seconds)**: period in seconds during which alarms have been raised, before an e-mail is sent. **Place the machine under quarantine**: the packet that caused the alarm will be temporarily blocked with the following parameters: • **For a period of (minutes)**: duration of the quarantine.

NOTE
When you change the alarm level of an event, don't forget to click on **Apply** at the bottom of the page, in order to confirm your action.

TEMPORARY ACCOUNTS

This service enables the management of accounts with a limited validity duration. These accounts are meant to provide temporary public Internet access to persons outside the organization. Temporary accounts are not saved in the LDAP directory(ies) declared on the firewall.

These accounts consist of the following information:

- First name (mandatory),
- Last name (mandatory),
- E-mail address (optional),
- Company (optional),
- Date from which the account will be valid (mandatory),
- Date until which the account will be valid (mandatory),
- Connection ID automatically made up of the first name and last name separated by a period,
- Automatically generated password.

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

The **Temporary account** is used to manage (creating / modifying / deleting) temporary accounts.

Temporary accounts list

Whenever the "Temporary accounts" authentication method is disabled, this module will ask you to go to the **Authentication** module to enable it.

Once it is enabled, this module will allow you to manage temporary accounts: add, delete, modify, print information, export the list of accounts.

The table

This table sets out all information relating to temporary accounts created on the firewall. It contains the following columns:

Username	Connection ID of the temporary user. It will be automatically created by concatenating the first name and last name separated by a period. Example: john.doe
First name	First name associated with the account.
Last name	Last name associated with the account.
E-mail address	E-mail address associated with the account.
Company name:	Company associated with the account.
From	This is the date from which the temporary account will be valid.
Up to	This is the date until which the temporary account will be valid.
Password	The password associated with the temporary account. The firewall automatically generates this password.

Possible operations

Refresh

When several persons are authorized to create temporary accounts, clicking on this button will refresh the list of accounts and allow viewing all entries.

Add user

To create a temporary account, enter at least the user's first name, last name and the start and end dates for the account's validity.

First name	First name associated with the account.
Last name	Last name associated with the account.
E-mail address	E-mail address associated with the account.
Company name:	Company associated with the account.
From	In the calendar, select the first day of the temporary account's validity. The default value suggested is the current date.
Up to	In the calendar, select the last day of the temporary account's validity. The default value suggested takes into account the start date and the default duration specified in the *Configuration* tab.

REMARK
The ID associated with the account will be automatically created using the first name and last name separated by a period (example: john.doe). Once the account has been created, this ID can no longer be modified.

In order to confirm the creation of the account, click on **Create account**.

The following window will provide a summary of the account information as well as the generated password. This information can then be printed using the **Print** button in this window.

Remove

This button allows deleting a temporary account:

1. Select the user to remove.
2. Click on **Remove**.

Modify user

This button allows you to modify certain parameters of a temporary account:

- First name,
- Last name,
- E-mail address,
- Company,
- Valid from,
- Valid until,

Only the account ID (permanent after the creation of the account) and password cannot be modified here.

1. Select the account that you wish to modify.
2. Click on **Modify user**.
3. After having modified the relevant parameters, click on **Apply**.
   The following window will provide a summary of the account information that can you can **Print** unless the beneficiary of the temporary account has modified the initial password. In this case, the account settings can only be printed after the password has been reinitialized;

Generate a new password

This button allows generating a new password associated with the selected temporary account.

1. Select the account for which you wish to generate a new password.
2. Click on **Generate a new password.**
   A window will provide a summary of the account information as well as the new associated password, which you can **Print**.

Export

This button allows exporting the list of temporary accounts in CSV. You will then be able to open this export file in a text editor in order to customize it.

Print selection

This button allows printing the information of a temporary account unless the beneficiary of the temporary account has modified the initial password. In this case, the account settings can only be printed after the password has been reinitialized;

TRUSTED PLATFORM MODULE (TPM)

The trusted platform module (TPM) found on some SNS firewalls offers hardware storage that increases the security of certificates stored on the SNS firewall.

If the SNS firewall is equipped with a TPM, a "TPM" indicator will appear in the Health indicators widget in the **Dashboard**. See the list of firewall models that are equipped with a TPM on the Stormshield website at Our Stormshield Network Security firewalls.

In order to use the TPM and protect private keys in certificates, the TPM must be initialized in advance.

Initializing the TPM

To initialize the TPM, the administrator must hold the **TPM access (W)** privilege. Only the *admin* account can assign this privilege in **Configuration** > **System** > **Administrators**, Administrators tab, **Switch to advanced view** button.

To initialize the TPM:

1. Go to **Configuration** > **Objects** > **Certificates and PKI**.
2. Click on **Init. TPM**.
3. If Secure Boot has not been enabled, a warning will appear. You are advised to enable Secure Boot before initializing the TPM, but this can be done later. Do note, however, that TPM protection is incomplete as long as the Secure Boot feature is not enabled.
4. In the **Set password** window, set the TPM administration password:
   - It must comply with the password policy set on the SNS firewall,
   - We recommend generating it randomly with a length of at least 64 characters.
   - **It must be kept in a secure and protected location.** If you misplace the TPM password, you will not be able to reinitialize it, and Stormshield is not in a position to recover the password.
5. Select the features for which the private keys of the certificates used will be protected. Features that do not use certificates in their configuration cannot be selected. You can also leave all checkboxes unchecked and protect private keys in SNS firewall certificates later.
6. Click on **Finish**.

The TPM is initialized and the mechanism that derives the symmetric key is used to generate the symmetric key, regardless of whether the SNS firewall is a member of a high availability cluster. If the SNS firewall is part of a high availability cluster, the TPM on the passive firewall will be automatically initialized.

For more information on the initialization of the TPM, refer to the technical note Configuring the TPM and protecting private keys in SNS firewall certificates.

Using certificates with TPM-protected private keys

The TPM-based security mechanism applies to certificates in the cases below: Refer to the sections in these modules for details on how to use certificates with protected private keys in the configuration of SNS firewalls.

In these modules, the icon indicates certificates with a TPM-protected private key.

- IPsec VPN (Configuration > VPN > IPsec VPN module),
- SSL VPN (Configuration > VPN > SSL VPN module),
- SSL/TLS decryption for the web administration interface and captive portal (Configuration > Users > Authentication module),
- Communications with the SMC server (Configuration > System > Management Center module),
- Sending of logs to a syslog server (Configuration > Notifications > Logs - Syslog - IPFIX module),
- Internal LDAP (Configuration > Users > Directory configuration module).

For more information on protecting certificate private keys with the TPM, refer to the technical note Configuring the TPM and protecting private keys in SNS firewall certificates..

Explanations on usage with the TPM

- There are several particularities regarding the encryption status of protected private keys that are included in the configuration backup file (Configuration > Maintenance > Backup module):
  - For manual backups, protected private keys are included decrypted as the TPM password has to be entered,
  - For automatic backups, private keys are included, but remain encrypted.
- Backups containing encrypted private keys can **only** be restored on the original firewall. Encrypted private keys cannot be decrypted on another SNS firewall as the symmetric key is assumed to be different.
- During the initial configuration of an SNS firewall via USB key, the init and p12import operations allow you to interact with the TPM.
- The status of the TPM can be applied to the calculation of the high availability (HA) quality factor.

For more information on these use cases, refer to the section Explanations on usage when the TPM is initialized, in the technical note *Configuring the TPM and protecting private keys in SNS firewall certificates*.

URL FILTERING

This module consists of two sections:

- A drop-down menu that lists the various profiles,
- A grid that centralizes URL filter rules.

> **NOTE**
> To set up a URL/SSL filter policy, you are advised to operate in blacklist mode, i.e., explicitly group the URL categories to be prohibited in a custom URL group. A URL/SSL filter rule will then be applied to this group with a *block* action. This rule must then be placed above the rule that allows all the other categories.

Profiles

The buttons in this strip allow you to configure the profiles associated with URL filtering.

Selecting a profile

The drop-down list offers 10 profiles, numbered from 00 to 09. Each profile is named "URLFilter_" by default, accompanied by its number.

> **EXAMPLES**
> - (0) URLFilter_00,
> - (1) URLFilter_01 ...

To select a profile, click on the arrow to the right of the field in which "Default00" is displayed by default, and select the desired profile. Each profile is configured as follows by default:

State	Action	URL category or group	Comments
On	Pass	any	default rule (decrypt all)

Buttons

Edit	This function allows performing 3 operations on profiles: • **Rename**: by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on "Update". This operation can also be cancelled. • **Reinitialize**: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. The profile becomes "active" again thanks to the **Pass** action applied to all URL categories or their groups. • **Copy to:** This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.

Last modification	This icon allows finding out the exact date and time of the last modification. Comments can also be added.
URL database provider	This link redirects to the module that allows configuring the URL database provider (**Objects** / **URL** module / *URL database* tab).

Rules

The procedure for editing a URL filter profile is as follows:

1. Select a profile from the list of URL filter profiles.
2. The filter table will then appear with a screen listing all errors found in the policy.

> **NOTE**
> To set up a URL/SSL filter policy, you are advised to operate in blacklist mode, i.e., explicitly group the URL categories to be prohibited in a custom URL group. A URL/SSL filter rule will then be applied to this group with a *block* action. This rule must then be placed above the rule that allows all the other categories.

Possible operations

A multiple selection allows assigning the same action to several rules. Select several successive alarms using the **Shift** ⇧ key or individually by holding down the **Ctrl** key. You can also remove an item from an existing selection with the **Ctrl** key.

Some column titles have the icon . When you click on it, a menu appears and suggests assigning a setting to several selected rules (*Status* and *Action*).

Example: Several lines can be deleted at the same time by selecting them with the Ctrl key held down, then by clicking on **Delete**.

The available buttons are:

Add	Inserts a line to be configured after the selected line.
Delete	Deletes the selected line.
Move up	Places the selected line before the line just above it.
Move down	Places the selected line after the line just below it.
Cut	Removes the selected line and moves it to the clipboard.
Copy	Copies the selected line and moves it to the clipboard.
Paste	Pastes the line from the clipboard above the selected line.
Add all predefined categories	This button makes it possible to create as many filter rules as the number of URL categories in the selected URL base at once. All rules created in this way are enabled and the associated action by default is a redirection to the block page BlockPage_00.
Clean up rules	This button is useful for EWC URL filter policies that were created before SNS version 4.7.1 EA, and which were migrated when the URL database provider was changed (SNS 4.7.1 EA or higher). It deletes rules using categories that no longer have an equivalent in the URL database of the current provider as of SNS version 4.7.1 EA.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of filter rules:

- Add,
- Delete,
- Cut,
- Copy,
- Paste.

Rule grid

The table contains the following columns:

Status	Status of the rule: • **Enabled**, the rule will be active when this filter policy is selected. • **Disabled**, the rule will not be operational. The line will be grayed out in order to reflect this. **REMARKS** The firewall will assess rules in their order of appearance on the screen: one by one from the top down. As soon as it comes across a rule that corresponds to the request, it will perform the specified action and stop there. This means that if the action specified in the rule corresponds to **Block**, all rules below it will also be set to **Block**.
Action	Allows specifying the result of the rule: **Pass** to allow the site, **Block** to prohibit access and directly shut down the connection without displaying a block message. It is possible to **Block and redirect to a block page** in order to prohibit access and display one of the 4 available HTML block pages. These pages can be customized in the menu **Notifications**, **Block messages** module and *HTTP block pages* tab.
URL category or group	The name of a URL category or a group of categories created earlier. By clicking on this field, a drop-down list will prompt you to select a URL category or a category group, taken from the objects database. The group <Any> corresponds to any URL, even if it does not belong to any URL category or group.
Comments	Comments relating to the rule.

Errors found in the URL filter policy

The screen for editing URL filter rules on the firewall has a rule compliance and coherence analyzer which warns the administrator when a rule inhibits another rule or if there is an error in a rule.

This analyzer groups errors during the creation of rules or incoherent rules.

Errors are displayed in the form of a list. By clicking on an error, the rule concerned will automatically be selected.

USERS

The user authentication service requires user accounts to be created:

- On the firewall in an internal LDAP directory,
- In an external LDAP directory (Microsoft Active Directory, LDAP or PosixAccount LDAP),
- In a provider directory such as Microsoft Entra ID.

LDAP directory tab

This tab displays the users and groups that are defined in the directories configured on the firewall.

To access data on a user or group in order to display or edit it, select the user or group in the CN grid (left side of the screen): the relevant information appears in the column on the right.

Refer to the section Allowed names to find out which characters are allowed and prohibited in various fields.

Rule grid

This grid consists of one to three columns:

- The **CN** column, displayed by default, which includes user and group names in *identifier@directory* format,
- The **DN** column, hidden by default, which displays the *Distinguished Name* of the user or group (CN, OU, O and DC fields describe the user or group in its reference directory),
- The **TOTP** column, hidden by default, which contains a green tick for each user authenticated by a TOTP (*Time-based One Time Password*) method.

Details of a user

Account tab

ID (cannot be modified)	Connection ID of the selected user.
Last name (cannot be modified)	Last name of the selected user
First name (cannot be modified)	First name of the selected user
E-mail address	E-mail address of the selected user.
Phone number	Telephone number of the selected user
Description	Description of the selected user.

Create or update password	By clicking on this link, you will be able to create the user's authentication password in a specific window, which also displays the level of security. **NOTE** To allow users to change their own passwords, go to the **Users** module > **Authentication** > **Captive portal profiles** tab > **Advanced properties** section > **User passwords**.

TOTP

This section appears only when the selected user authenticated on the firewall with a TOTP.

TOTP code to be verified	In this field, enter the TOTP used to connect to services on the firewall that use TOTP authentication to verify its validity.
Reset enrollment	When you click on this button, the user's TOTP enrollment will be reset: the next time this user connects to services on the firewall that use TOTP authentication, he or she will need to start the whole process of TOTP enrollment all over again. **NOTE** Users with administration privileges cannot be deleted from the TOTP database.

Certificate tab

This tab allows you to:

- Display the user's x509 certificate when it exists and has been published in the LDAP directory,
- Create the user's identity when it does not exist in the PKI,
- Delete the user's certificate from the LDAP directory.

Since the PKI does not have a certification authority by default, you will need to create one in order to manage user's certificates: go to the **Objects** module > **Certificates and PKI** > **Add** button > **Add a root authority.**

This certificate will be useful in two cases: SSL authentication and VPN access to the firewall with a mobile IPsec client. This certificate can also be used by other applications.

Member of these groups tab

This tab allows including the user in one or several groups:

1. Click on **Add**.
   A new line will appear at the top of the table.
2. Select the arrow to the right of the field.
   A drop-down menu will display the list of existing groups.
3. Click on the desired group, and confirm your selection by clicking on **Apply**.
   The user is added to the table.

To remove a group, select it and click on **Delete**.

The maximum number is 50 groups per user.

Details of a group

Details

Name of the group (cannot be modified)	Name of the selected group.
Description	Description of the selected group.

The grid below the **Details** frame shows the users that belong to the selected group.

To add a user to the group:

1. Click on **Add**.
   A new line will appear at the top of the table.
2. Select the arrow to the right of the field.
   A drop-down menu displays the list of users found in the directory.
3. Click on the desired user, and confirm your selection by clicking on **Apply**.
   The user is added to the table.
4. Click on **Apply** to save the changes.

To remove a user from the group, select it and click on **Delete**.

Possible operations

Search bar

To search for a user or user group, enter all or part of the user's first name, last name and/or login: all users and/or user groups with names that contain the characters entered will be displayed.

> **EXAMPLE**
> If you type “a” in the search bar, the list below it will show all users and/or user groups with first names and/or last names containing an “a”.

Filter

This button allows you to select the type of CN to display. A drop-down menu offers the following choices:

Groups and users	Represented by the icon , this option makes it possible to display users and user groups in the list.
Users	This option is represented by the icon , which makes it possible to display only users in the list.
Groups	This option is represented by the icon , which makes it possible to display only user groups in the list.

Directory filter

When several directories are configured on the firewall, this button filters the display of users and/or groups according to the directory selected.

Add user

1. To create a user, click on **Add a user**, then select the relevant directory.
2. Enter at least the user's **ID** and **Last name,** and assign a **Password**.
   To associate a certificate with this user, you will need to indicate a valid e-mail address.
   The following are the various fields that are available when creating a user:

Account

ID (login)	User's login. This field is mandatory.
Name	User name. This field is mandatory.
First name	User's first name.
Mail	User's e-mail address, This will be useful for creating certificates for the user.
Phone number	User's telephone number
Description	Description of the user

> **NOTE**
> The fields "ID", "First name" and "Last name" cannot be modified after the user is created.

Authentication password

Password	Enter the user's password. This field is mandatory.
Confirm password	Enter the password again. This field is mandatory.
Password strength	A gauge indicating the robustness of the password will appear.

3. Click on **Next**, then select any available groups in the reference directory that you wish to assign to the user.
4. Click on **Finish** to confirm the creation of the user.

Add group

1. To create a group, click on **Add a group**, then select the relevant directory.
2. Enter at least the **Group name**.
   The following are the various fields that are available when creating a group:

Details

Group name	Give your group a name in order to identify it in the grid. This field is mandatory. **NOTE** You will not be able to change the name of the group after you have created it.

Description	You can provide a description of the group and modify the contents of the description whenever necessary. This field is optional but you are advised to fill it in.

Members	
Initial member	Select the first member to be added to the group. This field is mandatory: new groups cannot be empty.

3. Click on **Create** to confirm the creation of your user.

Deleting users or groups

Groups or users that do not have certificates issued by the firewall's PKI

1. Select the user or group to be deleted.
2. Click on **Remove**.
   A window will appear with the message "*Delete the user <name of user>?*".
3. Select **Yes** to proceed.

Users who have certificates issued by the firewall's PKI

1. Select the user to remove.
2. Click on **Remove**.
   A window will appear with the message "*Delete the user <name of user>?*".
3. Enter the **CA passphrase** (password of the authority that issued the certificate).
4. Select the checkbox **Export CRL after revocation** if you wish to keep a copy of the CRL.
5. In this case, select the **File format** of the CRL export:
   - Base64 format (PEM),
   - Binary format (DER).
6. Click on **Apply**.
7. If you have chosen to export the CRL, a window will open with a link to download the CRL export file.

Check usage

Represented by the icon , this button will show you which groups users belong to, as well as where the user or group is used in the rest of the configuration.

EXAMPLE
Filtering:

1. Select the user or group for which you wish to check usage.
2. Click on **Check usage**.
   The menu directory on the left will show you the user/group (via its ID) in the tab *Users and groups*, and displays the list of groups to which this user belongs, as well as its use in the configuration of the firewall.

Reset user's TOTP enrollment

This button is enabled only when the selected user authenticated on the firewall with a TOTP.

When you click on this button, the user's TOTP enrollment will be reset: the next time this user connects to services on the firewall that use TOTP authentication, he or she will need to start the whole process of TOTP enrollment all over again.

> **NOTE**
> Users with administration privileges cannot be deleted from the TOTP database.

Access privileges module

This shortcut makes it possible to display the user's access privileges directly in the **Users > Access privileges** module.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of users/groups (CN table):

- Deleting (the user or the selected group),
- Checking usage (of the user or the selected group),
- Resetting the selected user's TOTP enrollment.

Microsoft ENTRA ID tab

This tab lists the security groups and application roles that are associated with the SNS application in Microsoft Entra ID.

Rule grid

Security groups/Application roles	This column lists the names of the security groups and application roles that were defined on the firewall.

UID	This column lists the unique identifiers (UIDs) that describe each security group or application role. A security group's UID must comply with the identity provider's requirements. For Microsoft Entra ID, the required format is a string consisting of five blocks of characters separated by dashes (-). The character block structure is as follows: • First block: eight alphanumeric characters. • Second, third and fourth blocks: four alphanumeric characters. • Fifth block: eight alphanumeric characters. EXAMPLE e620fcd3-1522-47f9-9f9b-6a5764c1f1f9 The UID of an application role must comply with the identity provider's requirements. For Microsoft Entra ID, the required format is a set of words separated by dots (.). EXAMPLES SNS.Config.All.Write SNS.VPNSSL My.Own.Role
Description	The description is optional, but you are advised to add one for each security group or application role.

Possible operations

Search bar

To search for a group or role, enter all or part of its name, UID and description: all security groups and/or application roles that contain the characters entered will be displayed.

Select all

This button is used to select all the entries in the grid, in order to apply a common action such as **Delete**.

Adding a security group or application role

1. Click on **Add,** then select the type of item to add (**Security group** or **Application role**).
2. Enter the **Security group name** or the **Application role name**.
3. Enter the **UID** of the item according to the identity provider's requirements (see the description of UIDs in Rule grid).
4. Add a description if necessary (recommended).
5. Click on **Apply** to add the item.

Deleting a security group or application role

1. Select the item to remove.
2. Click on **Remove**.

> **WARNING**
> You will not be asked to confirm.

Edit

Select the item to be edited: you can then change its name and/or UID.

Check usage

Represented by the icon , this button indicates whether security groups or application roles are being used in the firewall configuration.

Importing security groups

Security groups can be imported through a CSV file generated by exporting groups from your Microsoft Entra ID tenant management space, or through a file that you created.

The structure of the header line should be as follows:

```
id,displayName,groupType,membershipType,source,mail,securityEnabled,mailEnabled,isAssignableToRole,onPremisesSyncEnabled
```

With the following values for each log line:

id	Specify the UID of the security group according to the identity provider's requirements (see the description of UIDs in Rule grid).
displayName	Enter the name (any text) of the security group.
groupType	Specify that this is a security group by indicating (without quotation marks): "Security".
membershipType	Specify the value (without quotation marks): "Assigned".
source	Specify the value (without quotation marks): "Cloud".
mail	Leave empty.
securityEnabled	Specify the value (without quotation marks): "True".
mailEnabled	Specify the value (without quotation marks): "False".
isAssignableToRole	Specify the value (without quotation marks): "False".
onPremisesSyncEnabled	Leave empty.

> **EXAMPLE**
> id,displayName,groupType,membershipType,source,mail,securityEnabled,mailEnabled,isAssignableToRole,onPremisesSyncEnabled
> 518afc56-071b-4c5b-ab34-ac78f07d6dac,SNS Authentication,Security,Assigned,Cloud,,True,False,False,

Configure auth.

This shortcut provides direct access to the **Authentication** module, to configure the OIDC/Microsoft Entra ID method.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the user/group grid (CN grid):

- Add an item,
- Delete the selected item,
- Edit the selected item,
- Check usage of the selected item.

VIRTUAL INTERFACES

The **Virtual interfaces** module allows managing, adding or deleting virtual network elements. Depending on their nature, these virtual interfaces can be used in a dynamic routing configuration (loopback interfaces), or to set up tunnels (GRE interfaces) or routed tunnels (IPsec interfaces).

The window for configuring virtual interfaces consists of 3 tabs:

- IPsec interfaces (VTI),
- GRE interfaces,
- Loopback.

> **NOTE**
> Please refer to the section Allowed names to find out which characters are allowed and prohibited in various fields.

Creating or modifying IPsec interfaces (VTI)

These interfaces make it possible to set up routed IPsec tunnels. The virtual IPsec interface acts as a traffic endpoint and all packets routed to this interface will then be encrypted. Such configurations may make it possible, for example, to make QoS traffic pass through a dedicated IPsec tunnel: high-priority traffic will then take a specific tunnel while other traffic will go through a second tunnel.

To create or modify a virtual IPsec interface, click on the *IPsec interfaces (VTI)* tab.

Button bar

Enter a filter	This field makes it possible to search for an interface by entering a sequence of characters included in its name.
Add	Adds a new interface. An added interface (sending of a command) is effective only if its fields **Name**, **IP address** and **Network** mask have been entered.
Delete	Deletes one or several selected interfaces. Use the keys Ctrl/Shift + Delete to delete several interfaces.
Check usage	Represented by the icon , this button indicates whether the selected interface is being used elsewhere in the configuration.
Apply	Applies the configuration of the IPsec interfaces.
Cancel	Cancels the configuration of the IPsec interfaces.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of virtual IPsec interfaces:

- Add,
- Delete,

- Check usage.

Presentation of the table

The grid presents, in the form of columns, the information that is defined when creating a virtual IPsec interface:

Status	Status of the interfaces: • Enabled: Double-click to enable the created interface. • Disabled: The interface is not in operation. The line will be grayed out in order to reflect this.
Name (mandatory)	Name the IPsec interface. **NOTE** Please refer to the section Allowed names to find out which characters are allowed and prohibited in various fields.
IPv4 address and mask (mandatory)	Enter the IP address/network mask pair that describes the virtual interface created. The mask format can be decimal (e.g., 255.255.255.252) or CIDR (e.g., %30). Since virtual IPsec interfaces are meant for setting up point-to-point tunnels, a network that allows assigning two addresses is sufficient in theory.
Protected	This column is hidden by default. If you wish to show it: 1. Scroll over the column header, 2. Click on the drop-down menu that appears to the right of the column header, 3. Select **Column** > **Protected**. When the column is shown, double-click on the corresponding cell to change the interface type: • Protected • Public
Comments (optional)	Any text.

Creating or editing a GRE interface

The GRE protocol allows encapsulating IP traffic in a point-to-point IP tunnel. This allows, for example, routing networks from one site to another through a GRE tunnel without having to declare this routing method on all routers in between.

GRE tunnels are not encrypted natively: they merely encapsulate. GRE traffic can however be made to go through an IPsec tunnel.

To create or modify a virtual GRE interface, click on the *GRE interfaces* tab.

Button bar

Search	Search that covers interfaces.
Add	Adds a new interface. An added interface (sending of a command) is effective only if its fields **Name**, IP address, Network mask, Tunnel source and Tunnel destination have been entered.
Delete	Deletes one or several selected interfaces. Use the keys Ctrl/Shift + Delete to delete several interfaces.
Check usage	Represented by the icon , this button indicates whether the selected interface is being used elsewhere in the configuration.
Apply	Applies the configuration of the IPsec interfaces.
Cancel	Cancels the configuration of the IPsec interfaces.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of GRE interfaces:

- Add,
- Delete,
- Check usage.

Presentation of the table

The grid presents, in the form of columns, the information that is defined when creating a virtual GRE interface:

Status	Status of the interfaces: • Enabled: Double-click to enable the created interface. • Disabled: The interface is not in operation. The line will be grayed out in order to reflect this.
Name (mandatory)	Name the GRE interface.
IPv4 address and mask (mandatory)	Enter the IP address/network mask pair that describes the virtual interface created. The mask format can be decimal (e.g., 255.255.255.252) or CIDR (e.g., %30).

Protected	This column is hidden by default. If you wish to show it: 1. Scroll over the column header, 2. Click on the drop-down menu that appears to the right of the column header, 3. Select **Column** > **Protected**. When the column is shown, double-click on the corresponding cell to change the interface type: • Protected • Public
Tunnel source (mandatory)	Select the outgoing interface of traffic using the tunnel. In general, this would be the firewall's "out" interface or a bridge.
Tunnel destination (mandatory)	Select the object representing the tunnel's remote endpoint. This is a host object that presents the public IP address of the remote firewall.
Comments(optional)	Any text.

Creating or modifying a loopback interface

Loopback interfaces may be used, for example, in dynamic routing configurations.

To create or modify a loopback interface, click on the "Loopback" tab.

Button bar

Search	Search that covers interfaces.
Add	Adds an "empty" interface. An added interface (sending of a command) is effective only if its fields **Name** and IP address have been entered.
Delete	Deletes one or several selected interfaces. Use the keys Ctrl/Shift + Delete to delete several interfaces.
Check usage	Represented by the icon , this button indicates whether the selected interface is being used elsewhere in the configuration.
Apply	Sends the configuration of the IPsec interfaces.
Cancel	Cancels the configuration of the IPsec interfaces.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of loopback interfaces:

- Add,
- Delete,
- Check usage.

Presentation of the table

The table sets out four fields of information:

Status	Status of the interfaces: • Enabled: Double-click to enable the created interface. • Disabled: The interface is not in operation. The line will be grayed out in order to reflect this.
Name(mandatory)	Give the loopback interface a name.
IPv4 address (mandatory),	Enter the IP address assigned to the loopback interface created.
Comments(optional)	Any text.

URL OBJECTS

In this module, you can:

- Create custom URL categories and custom groups of URL categories,
- Create custom categories of certificate names (CN) and custom CN groups,
- Set the URL database provider that provides dynamic URL categories.

For a specific category, e.g. "banks", that groups the most frequently visited bank URLs, a rule can be created in the **Configuration** > **Security policy** > **URL filtering** module to block access to it. Therefore, when a user attempts to connect to a website in this category, a block page will appear with an error message.
Block pages can be customized in **Configuration** > **Notifications** > **Block messages** ⇒ **HTTP Block page** tab.

> **NOTE**
> In filter policies, it is better to use dynamic categories provided by URL databases, as they are richer and perform better than custom URL lists.

This module consists of three tabs:

- **URL**: makes it possible to group URLs by category (e.g., *shopping*, *pornography or videogames*). Each of these categories groups together a certain number of website URLs, which may be blocked or allowed, depending on the desired action. Also allows the creation of URL or certificate category groups from the customized or dynamic categories (URL database).
- **Certificate name (CN)**: makes it possible to create categories to recognize the certificates assigned to secure websites, for use in SSL filtering. Also allows the creation of CN category groups.
- **URL database**: defines the URL database provider used. **Internal URL filtering engine (no database updates)** is selected by default.
  You need to associate this engine with custom URL categories or URL bases maintained by third parties, such as :
  - French URL filtering database provided by the Rectorat de Toulouse (Académie de Toulouse), following the method described in the Stormshield Knowledge Base (authentication required),
  - Polish URL filtering database provided by Dagma, using the following method: https://stormshield.pl/pomoc/baza-wiedzy/item/zmiana-klasyfikacji-url-na-rozszerzona-klasyfikacje-dedykowana-dla-polskiego-rynku).

Refer to the section Allowed names to find out which characters are allowed and prohibited in various fields.

URL tab

This tab provides an overview of:

- Predefined URL categories such as *antivirus_bypass* and *authentication_bypass*,
- Custom URL categories,
- URL category groups.

Possible operations

Enter a filter	Type a character string in the field: only items that contain this character string will appear in the **URL categories** and **URL category group** grids. Erase the character string to display all items once more.
Select all	Select all URL categories and all URL category groups to **Delete** them.
Add	Create a new URL category or a new URL category group. By selecting one of these two items in the drop-down menu, a new line appears in the corresponding grid, allowing you to indicate the name of the category or category group, as well as comments, if necessary.
Delete	Deletes the selected item (URL category or category group). If this item is in use in the firewall configuration, a warning message will ask you to confirm the operation.
Check usage	Checks whether the selected item is used in the firewall's configuration. The results of the check are shown in the module tree.
Check URL classification	Checks whether a URL belongs to a defined URL category. Custom and dynamic categories will be searched. This will help to determine whether a URL needs to be added to a category. Enter the desired URL in the text zone, then press **Enter**. A **URL categories** panel appears, displaying the categories that contain this URL.

URL category grid

The grid includes the following:

URL category	Name of the URL category.
Usage	• A ● symbol indicates that this URL category is used in the firewall's configuration (URL/SSL filtering or filtering), • A ● symbol indicates that this URL category is not used in the firewall's configuration.
Number of items	Indicates the number of URLs included in the URL category.
Comments	Displays any comments that may have been added when the URL category was created.

> **NOTE**
> The number of characters for a URL category is restricted to 255.

Editing a URL category

By double-clicking on a URL category, its content will appear on the right side of the screen.

The following actions can be performed in the grid:

Group name	Change the name of the URL category.
Comments	Add or change the comments associated with this URL category.

Enter a filter	Type a character string in the field: only items that contain this character string will appear in the grid. Erase the character string to display all items once more.
Select all	Makes it possible to select all the URLs in a category to **Delete** them.
Add	Adds a URL to a category. Clicking on this button creates a new line, allowing you to enter the URL and add comments if necessary. The URL may contain the wildcards ***** and **?**.
Delete	Deletes a URL from a category. Select the URL in question, then click on the button.

The grid includes the following:

URL	Name of the URL. It may contain the wildcards ***** and **?**.
Comments	You can add a comment in this field to describe each URL listed.

The list of **Characters allowed** and syntax restrictions apply only to URLs. The following wildcards can be used:

*****	replaces a character string. **EXAMPLES** ***.company.com**/ makes it possible to include all sub-domains of company.com (e.g. mail.company.com or www.company.com) as well as all elements that follow the slash "/". ***.exe** makes it possible to include all URLs ending with "*.exe*".
?	replaces a single character. **EXAMPLE** **???**.company.com includes **www**.company.com or **ftp**.company.com but not **www1**.company.com.

URL category group grid

This grid appears only when the first group of URL categories has been created.

The grid includes the following items:

URL category group	Name of the URL category group.
Usage	• A ● symbol indicates that this URL category group is used in the firewall's configuration (URL/SSL filtering or filtering), • A ● symbol indicates that this URL category group is not used in the firewall's configuration.
Number of items	Indicates the number of URL categories included in the group.
Comments	Shows comments that may have been added when group was created.

NOTE
The number of characters for a URL category group is restricted to 255.

Editing a URL category group

By double-clicking on a URL category group, its content will appear on the right side of the screen.

The following actions can be performed in the grid:

Group name	Change the name of the URL category group.
Comments	Add or change the comments associated with the group.
Enter a filter	Type a character string in the field: only items that contain this character string will appear in the grid. Erase the character string to display all items once more.
Select all	Makes it possible to select all the categories in a group to **Delete** them.
Add	Adds a URL category to the group. Clicking on this button creates a new line, allowing you to select the URL category.
Delete	Deletes a URL category from the group. Select the URL category in question, then click on the button.

The grid includes the following:

Objects in this group	Name of URL categories that make up the group.

Certificate names (CN) tab

In this screen, custom certificate name categories can be created, and may be useful in SSL filtering (**Configuration** > **Security policy** > **SSL filtering** module).

The screen is split into two parts - one for custom certificate name categories, and the other for certificate names added to a category.

CN category grid

The following operations can be performed:

Enter a filter	Type a character string in the field: only items that contain this character string will appear in the **CN categories** and **CN category group** grids. Erase the character string to display all items once more.
Select all	Select all CN categories and all CN category groups to **Delete** them.
Add	Create a new CN category or a new CN category group. Clicking on this button creates a new line, allowing you to name the category and add comments if necessary.
Delete	Deletes an existing category. Select the category in question, then click on the button. If the category is in use, a warning message will ask you to confirm the operation.
Check usage	Checks whether a category is being used in a configuration. Select the category in question, then click on the button. The results of the check are shown in the module tree.

The grid includes the following:

Certificate name category (CN)	Name of the category.
Comments	Description of the category.

> **NOTE**
> The number of characters for certificate name categories is restricted to 255.

CN category group grid

By double-clicking on a CN category group, its content will appear on the right side of the screen.

The following actions can be performed in the grid:

Add	Adds a certificate name to a category. Clicking on this button creates a new line, allowing you to name the certificate and add comments if necessary. The name can contain a wildcard (*) as long as it is placed at the beginning of a URL and followed by a dot.
Delete	Deletes a certificate name from a category. Select the name of the certificate in question, then click on the button.

The grid includes the following:

Certificate name (CN):	Name of the certificate. It can contain a wildcard (*) as long as it is placed at the beginning of a URL and followed by a dot.
Comments	You can add a comment in this field to describe each name.

The list of **Characters allowed** and syntax restrictions apply only to certificate names. Wildcards (*) can be used to replace any character sequence, but must be placed at the beginning of a URL followed by a dot.

> **EXAMPLE**
> ***.company.com** makes it possible to include all sub-domains of company.com (e.g. mail.company.com or www.company.com).

URL database tab

This tab displays the name and description of the URL categories in the URL database used by the firewall. This URL database is available only if you have subscribed to the option. It is hosted in the supplier's cloud.

WEB SERVICES

This module presents the web services that are defined on the firewall. They will be used in the filter policy. Two types are available:

- Web service objects distributed by Stormshield (**List of web services** tab): these are downloaded automatically via Active Update.
  These are web services from mainstream vendors, e.g., Google Drive, Logmein or Microsoft Azure.
  They can be grouped in predefined and custom groups (**Groups** tab).
- Custom web services objects (**List of web services** tab): defined by the administrator and imported on the firewall through a CSV file (**Import custom services** tab). They can be grouped in custom groups (**Groups** tab).

List of web services tab

This tab provides an overview of the web services defined on the firewall. The web services grid consists of two sections:

- The list of web service objects distributed by Stormshield,
- The list of custom web service objects.
  This list appears only if a custom database has been imported.

Web services distributed by Stormshield

These are the most common online web services (Microsoft Office 365, Logmein, Sharepoint, Webex, etc.).
They are automatically imported and updated through Active Update.

Each web service is made up of public IP addresses and/or FQDNs.

The following are a web service's characteristics:

Name	Name given to the group.
Usage	When the color of the icon is: • Green: the web service in question belongs to a service group or is used in the firewall's configuration. • Black: the group in question does not belong to any service group and is not used in the firewall's configuration.

When you scroll over a web service, a tooltip shows its properties:

- **Name**: name of the web service, e.g., Microsoft Office 365,
- **Description**: the contents of the service, e.g., IP addresses and domains to reach Microsoft Office 365 online services,
- **Read only**: indicates whether the service can be renamed or deleted. Web services distributed by Stormshield are always in read-only mode,
- **Revision number**: this number is incremented every time Active Update retrieves a new version of content from the web service in question,
- **Revised on**: this is the date when Active Update last retrieved a content update from the web service in question,

- **URL**: specifies the addresses with which the service's FQDN lists or public IP addresses can be looked up with the provider.

Custom web services

This list appears only when custom web services have been imported via a CSV file (**Import custom services** tab).

When you scroll over a web service, a tooltip shows its properties:

- **Name**: name of the web service, e.g., MyCustomWebService,
- **Description**: corresponds to the optional comments added for the service in the import file,
- **Read only**: indicates whether the service can be renamed or deleted. Customized services are always in read-only mode. Only the full database of custom web services can be deleted,
- **Revision number**: this number is specified manually in the CSV import file,
- **Revised on**: this date is specified manually in the CSV import file,
- **No. of IPv4 addresses**: indicates the number of IPv4 addresses that define the web service,
- **No. of IPv6 addresses**: indicates the number of IPv6 addresses that define the web service,
- **No. of FQDNs**: indicates the number of FQDNs that define the web service.

Possible operations

Enter a filter	Enter a sequence of letters found in the name of the web services you are looking for, to restrict the display to these services.
Export custom database	Click on this button to export all custom web services to a CSV file for download.
Delete custom database	Click on this button to delete the whole custom web service database.
Check usage	Click on this to check whether a web service listed in the grid is used in the firewall's configuration: 1. Select the web service. 2. Click on **Check usage**. The configuration modules that use this web service are shown in the menu on the left.

Groups tab

This tab consists of two separate parts:

- The list of web service groups on the left side of the screen,
- The properties and members of the selected group on the right side of the screen.

List of groups grid

This grid contains:

- Predefined groups containing web service objects that are distributed by Stormshield (cloud computing, Microsoft, etc.),
- Custom groups, if any, meant to contain official and custom web services. Such groups are manually created by the administrator.

The following are a group's characteristics:

Name	Name given to the group.
Usage	When the color of the icon is: • Green, the group in question is used in the firewall's configuration. • Black, the group in question is not used in the firewall's configuration.
Number of members	Shows the number of web services that make up the group.
Comments	Shows optional comments entered when the group was created or edited (only for custom groups).

When you scroll over a group, a tooltip shows its properties:

- **Name**: the name of the group, e.g., Microsoft,
- **Read only**: indicates whether the group can be renamed or deleted. Web service object groups distributed by Stormshield are always in read-only mode,
- **Members of the group**: lists the web services included in the group.

Possible operations on the List of groups grid

Enter a filter	Enter a sequence of letters found in the name of the web service groups you are looking for, to restrict the display to these groups.
Select all	By clicking on this button, all service groups found in the grid will be selected.
Add	This button makes it possible to create a new blank custom group: 1. Click on **Add**. 2. Enter the **Group name** (no spaces allowed). 3. Add **Comments** if necessary. 4. Click on **Apply**.
Rename	This action is allowed only for custom groups. 1. Select the custom group that you wish to rename. 2. Click on **Rename**. 3. Enter the new **Group name**. 4. Click on **Apply**.
Delete	This action is allowed only for custom groups. 1. Enter the custom group(s) that you want to delete (select several by pressing [Ctrl]). 2. Click on **Remove**. 3. Confirm by clicking on **OK**.

Check usage	This button allows you to check whether a web service group listed in the grid is used in the firewall's configuration: 1. Select the group. 2. Click on **Check usage**. The configuration modules that use this group are shown in the menu on the left.

Editing the properties and members of a service group

Double-click on the group you want to edit. Only custom groups can be edited.

The properties and members of the selected group will appear on the right side of the screen.

Group properties

Comments	Enter comments for the group if necessary. These comments are immediately applied (they appear automatically in the service group grid).

Members of the group grid

Enter a filter	Enter a sequence of letters found in the names of the web service group members you are looking for, to restrict the display to these members.
Select all	By clicking on this button, all members found in the group will be selected so that a common action can be applied to all of them (**Delete**).
Add	This button makes it possible to add web services (official and custom) or web service groups to the custom group being edited: 1. Click on **Add**. The list of web services and service groups defined on the firewall appears. Services already in the group will be highlighted in yellow and the checkbox next to their name is selected. **NOTE** Groups containing a service already in the group being edited cannot be added. 2. Select the checkboxes next to the Web services or groups that you want to add. Changes are applied immediately.
Delete	This action is allowed only for custom groups. 1. Enter the web services or web service groups that you want to delete from the group being edited (select several by pressing [Ctrl]). 2. Click on **Remove**. Changes are applied immediately.

Import custom services tab

In this tab, custom web services can be imported from a CSV file.
The structure that this CSV file must follow is described in Structure of the file importing custom web services (CSV format).

Import

> **IMPORTANT**
> When a custom database is successfully imported, it **deletes and replaces** the existing custom database. When this occurs, ensure beforehand that the import file used contains all the custom web services that you wish to keep, otherwise they will be lost.

1. Use the **Select database to import (.csv file)** field to choose an import file saved on your workstation.
2. Next, click on **Import database**.
   Depending on the result of the import operation, additional information may be shown in this section:
   - If the operation is successful, the "Custom list of imported web services fully operational" message appears,
   - In the event of failure:
     - The reason for the failure is given, e.g., "Failed to generate BitGraph files from CSV import: invalid format of some data in the CSV file",
     - The number of the line in question in the CSV file and the contents of this line, e.g., "An error occurred on line1: MyWebService1,,2022/01/19,12.2,My first".

Information about the last import

After a successful import, this section shows a summary of the imported data:

Last custom web service import	Date and time of the last successful import.
Number of custom web services	Number of web services imported via the CSV file.
Total no. of IPv4 addresses	Number of entries imported with an IPv4 address.
Total no. of IPv6 addresses	Number of entries imported with an IPv6 address.
Total no. of FQDNs	Number of entries imported with an FQDN.

Wi-Fi

The WI-Fi Network module makes it possible to enable the Wi-Fi network. It also sets out some of this network's physical parameters.

> **NOTE**
> The parameters set out in this screen are the same for both access points available on the firewall.

Enable Wi-Fi: enables or disables the use of the Wi-Fi network on the firewall

General configuration

Scheduling	Select the time object that defines the Wi-Fi network's availability period.
Mode	Select the Wi-Fi network standard that needs to be managed by the firewall: • 802.11a (5 GHz frequency - shorter range), • 802.11b (2.4 GHz frequency - wider range), • 802.11g (2.4 GHz frequency - improved version of the "b" standard - wider range), • 802.11a/n (high throughput [channel aggregation] based on the "a" standard - 5 GHz frequency), • 802.11g/n. (high throughput [channel aggregation] based on the "g" standard - 2.4 GHz frequency),

Channel configuration

Country	Select the country in which the firewall has been installed. This choice will determine the available communication channels as well as the signal strength for these channels, depending on the country's local regulations.
Channel	Select the channel used by the firewall's Wi-Fi network. The channels offered depends on the selected country in the previous field.
Tx power	This field makes it possible to set the Wi-Fi network's transmission strength for the selected channel. Depending on the country selected and the associated local regulations, the strength offered may differ.

Access point configuration: clicking on this link will redirect you to the Interface modules in order to configure the necessary WLAN interfaces (network name, authentication type, etc);

Allowed or prohibited characters

This section lists the characters that are allowed or prohibited in the various items found in the configuration of your firewall.

Firewall name

- The name of the firewall must not exceed 127 characters (**allowed** characters):

```
<alphanum> - _ .
```

Admin password of a virtual firewall on Microsoft Azure

- Password (**prohibited** characters):

```
" ' ` \ $ ( )
```

Login and password

- Login (**prohibited** characters):

```
" <tab> & ~ | = * < > ! ( ) [ ] / \ $ % ? ' ` <space> : ; @ + ,
```

- Password (**prohibited** characters):

```
" <tab>
```

Filter - NAT

- Comments and rule separators (**prohibited** characters):

```
< > "
```

Names of network interfaces

- The name of an interface must not exceed 15 characters. It cannot contain the following words if they are immediately followed by numbers (e.g., ethernet0, dialup123):

```
loopback ethernet wifi dialup vlan bridge agg ipsec sslvpn gretun gretap
```

- The name of an interface must not begin with any of the following prefixes:

```
firewall network serial loopback
```

- The name of an interface must not be any of the following reserved words:

```
ipsec dynamic sslvpn any protected notprotected blackhole
```

- The name of an interface must not contain the following characters (**prohibited** characters):

```
@ " # <tab> <space> [ ] < >
```

Network objects

- The name of a network object must not exceed 255 characters (**prohibited** characters):

```
<tab> <space> ! " # , = @ [ \ | ]
```

- Names must not contain any of the following **prohibited** prefixes:

```
Firewall_ Network_ ephemeral_ Global_
```

- The following names are **prohibited**:

```
any internet none anonymous broadcast all
```

> **NOTE**
> Object names are not case sensitive.

- Comments must not contain any of the following characters (**prohibited** characters):

```
" # @ < >
```

DNS (FQDN) name objects

- Names must not exceed 255 characters (**allowed** characters):

```
<alphanum> . -
```

Certificates and PKI

- Certification authority names (**prohibited** characters):

```
/ <tab> " ` % :
```

- Certificate names (**prohibited** characters):

```
/ <tab> " ` % :
```

- Short name of a certificate or certification authority (**prohibited** characters):

```
/ <tab> " ` % : \
```

LDAP databases

- User names in the LDAP database (**prohibited** characters):

```
" <tab> , ; & ~ | = * < > ! ( ) \
```

- User IDs (**prohibited** characters):

```
" <tab> & ~ | = * < > ! ( ) \ $ % ? ' ` <space>
```

> **WARNING**
> In external directories such as Microsoft Active Directory, user IDs must comply with the above criteria **as well as** the criteria imposed by Microsoft.

- Group names in the LDAP database (**prohibited** characters):

```
<tab> <space> & ~ | = * < > ! ( ) \ $ % ! ' " `
```

- LDAP database paths: Base DN, CA Dn, etc. (**prohibited** characters):

```
" & ~ | * < > ! ( )
```

IPsec VPN

- Names of IPsec peers (**prohibited** characters):

```
# = @ [ \ ]
```

- Names of IPsec rules (**prohibited** characters):

```
. , : { } [ ] = " # \n <tab> <space>
```

SSL VPN Portal

- Server names and aliases (**allowed** characters):

```
<alphanum> - _ . :
```

- Prefix of the URL's root directory (**allowed** characters):

```
<alphanum> - _
```

Quality of Service (QoS)

QoS queues

- Names must not exceed 31 characters (**prohibited** characters):

```
@ [ ] # ! \ " | = <space> <tab>
```

- Names must not contain any of the following reserved expressions:

```
internet any any_v4 any_v6 firewall_ network_ broadcast anonymous none all
original
```

Traffic shapers

- Names must not exceed 15 characters (**prohibited** characters):

```
@ [ ] # ! \ " | = <space> <tab>
```

E-mail alerts

- E-mail addresses - domain names (**allowed** characters):

```
<alphanum> ! # $ % & \ * + - / = ? _ ` { } | ~ .
```

- Recipient group names (**prohibited** characters):

```
<tab> <space> ! " # , = @ [ \ | ]
```

- IDs used for authentication on the server (**prohibited** characters):

```
<tab> <space> " \ < >
```

- Passwords used for authentication on the server (**prohibited** characters):

```
<tab> <space> " \
```

- Sender names and *ReplyTo* (**prohibited** characters):

```
< > ; , "
```

Web services

- Web service names must not exceed 40 characters (**allowed** characters):

```
<alphanum>
```

TPM password

- Passwords must not exceed 240 characters (**prohibited** characters):

```
" <tab>
```

Structure of an objects database in CSV format

For each type of object that can be imported or exported, this section defines the structure of a row that makes up the objects database in CSV format.

These objects can be imported/exported in **Objects** > NETWORK/TIME OBJECTS.

All fields are separated by commas on each row in the file. Optional empty fields will be included between two commas.

Host

- Type of object (mandatory): **host**,
- Name (mandatory): text string using only accepted characters (see Allowed names),
- IPv4 address (mandatory),
- IPv6 address (optional),
- DNS resolution: **static** or **dynamic**,
- MAC address (optional),
- Comments (optional): text string between quotes.

EXAMPLES

```
host,dns1.google.com,8.8.8.8,2001:4860:4860::8888,,,"Google Public DNS Server"
host,AD_Server,192.168.65.12,,static,,""
```

IP address range

- Type of object (mandatory): **range**,
- Name (mandatory): text string using only accepted characters (see Allowed names),
- First IPv4 address in the range (mandatory),
- Last IPv4 address in the range (mandatory),
- First IPv6 address in the range (optional),
- Last IPv6 address in the range (optional),
- Comments (optional): text string between quotes.

EXAMPLE

```
range,dhcp_range,10.0.0.10,10.0.0.100,,,""
```

DNS name (FQDN)

- Type of object (mandatory): **fqdn**,
- Name (mandatory): text string using only accepted characters (see Allowed names),
- IPv4 address (mandatory),
- IPv6 address (optional),
- Comments (optional): text string between quotes.

EXAMPLE
fqdn,www.free.fr,212.27.48.10,,""

Network

- Type of object (mandatory): **network**,
- Name (mandatory): text string using only accepted characters (see Allowed names),
- IPv4 address (mandatory),
- Network mask (mandatory),
- IPv6 address (optional),
- Length of the IPv6 prefix (optional): indicated in number of bits,
- Comments (optional): text string between quotes.

EXAMPLES
network,IANA_v6_doc,,,,2001:db8::,32,""
network,rfc5735_private_2,172.16.0.0,255.240.0.0,12,,,""

Port

- Type of object (mandatory): **service**,
- Name (mandatory): text string using only accepted characters (see Allowed names),
- Protocol (mandatory): TCP, UDP or Any,
- Port (mandatory): port used by the service,
- First port in the range: empty field
- Last port in the range: empty field
- Comments (optional): text string between quotes.

EXAMPLE
service,bgp,tcp,179,,"Border Gateway Protocol"

Port range

- Type of object (mandatory): **service**,
- Name (mandatory): text string using only accepted characters (see Allowed names),
- Protocol (mandatory): TCP, UDP or Any,
- Port: empty field,
- First port in the range (mandatory): number of the first port used by the port range,
- Last port in the range (mandatory): number of the last port used by the port range,
- Comments (optional): text string between quotes.

EXAMPLE
service,MyPortRange,tcp,2000,2032,""

Protocol

- Type of object (mandatory): **protocol**,
- Name (mandatory): text string using only accepted characters (see Allowed names),
- Protocol number (mandatory): standardized number available from the IANA (Internet Assigned Numbers Authority),
- Comments (optional): text string between quotes.

EXAMPLE
protocol,ospf,89,"Open Shortest Path First"

Host group, IP address group or network group

- Type of object (mandatory): **group**,
- Name (mandatory): text string using only accepted characters (see Allowed names),
- Group components (mandatory): list of elements included in the group (list between quotes - components separated by commas),
- Comments (optional): text string between quotes.

EXAMPLE
group,IANA_v6_reserved,"IANA_v6_6to4,IANA_v6_doc,IANA_v6_linklocal_unicast,IANA_v6_teredo,IANA_v6_multicast,IANA_v6_uniquelocal",""

Service group

- Type of object (mandatory): **servicegroup**,
- Name (mandatory): text string using only accepted characters (see Allowed names),
- Group components (mandatory): list of elements included in the group (list between quotes - components separated by commas),
- Comments (optional): text string between quotes.

EXAMPLE
servicegroup,ssl_srv,"https,pop3s,imaps,ftps,smtps,jabbers,ldaps","SSL Services"

Structure of the file importing custom web services (CSV format)

For each custom web service that can be imported or exported, this section defines the structure of a row that makes up the CSV file.

These services can be imported/exported in **Objects** > WEB SERVICES:

- **Import custom services** tab to import,
- **List of web services** tab to export (**Export custom database** menu).

All fields are separated by commas on each row in the file. Optional empty fields will be included between two commas:

- Name of the service (mandatory): text string using only accepted characters (see Allowed names),
- Public IPv4/IPv6 address (mandatory) or FQDN (mandatory),

> **NOTE**
> Private IP addresses are not allowed.

- Date of last revision (optional),
- Revision number (optional),
- Comments (optional): any text.

> **IMPORTANT**
> The CSV file must contain a blank line after the last entry.

> **EXAMPLE**
> CustomWebService1,john.doe.org,2022/01/19,12.2,My first webservice with FQDN
> CustomWebService2,1.2.3.4,,,My second webservice with IP address
> CustomWebService3,5.6.7.8,2022/01/19,15,My third webservice

Do note that for web services relying on several IP addresses or several FQDNs the line that describes this web service must be duplicated as many times as the number of addresses or FQDNs that the service contains.

> **EXAMPLE**
> CustomWebService1,john.doe.org,2022/01/19,12.2,First FQDN for my first webservice
> CustomWebService1,foo.bar.org,2022/01/19,12.2,Second FQDN for my first webservice
> CustomWebService1,1.2.3.4,2022/01/19,12.2,IP address for my first webservice

documentation@stormshield.eu

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

Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.