GUIDE

STORMSHIELD NETWORK SECURITY

USER CONFIGURATION MANUAL

Version 3

Date: July 29, 2019

Reference: sns-en-user_configuration_manual-v3.9.1

Table of contents

WELCOME 11
Recommendations on the operating environment 11
Introduction 11
Security watch 12
Physical security measures 12
Organizational security measures 12
Human media 13
IT security environment 13
User awareness 15
Administrator management 15
User password management 16
Work environment 17
User access management 17

ACCESS PRIVILEGES 19
"Default options" tab 19
SSL VPN Portal 19
IPSEC 19
SSL VPN 19
Sponsorship 20
"Detailed access" tab 20
Possible operations 20
Interactive features 20
Configuration table 20
"PPTP" tab 22
Interactive features 22

ACTIVE UPDATE 23
Automatic updates 23
Advanced properties 23
Update servers of the URL database 23
Update servers of customized context-based protection signatures 23
Update servers 23

LOGS - AUDIT LOGS 24
Personal data 24
Collaborative security 24
Storage device: SD Card 24
Logs 25
Actions 25
Displaying details of a row of logs or a view 27
Interactive features 27
Views 31
Logs 32

ADMINISTRATORS 34
"Administrators" tab 34
Interactive features 34
Possible operations 34
Table of privileges 35
"Admin account" tab 38
"Ticket management" tab 39
The table 39
Possible operations 39

ANTISPAM 41
"General" tab 41
SMTP parameters 41
Advanced properties 42
"Whitelisted domains" tab 43
Interactive features 44
"Blacklisted domains" tab 44
Interactive features 44

ANTIVIRUS 45
Antivirus engine 45
Settings 45
Analysis of ClamAV files 45
Analysis of Kaspersky files 45
Sandboxing 46

APPLICATIONS AND PROTECTIONS 47
View by inspection profile 47
Selecting the configuration profile 47
The various columns 49
View by context 50

AUTHENTICATION 52
"Available methods" tab 52
Interactive features 52
Authentication methods 53
"Authentication policy" tab 59
Actions on the rules of the authentication policy 60
Interactive features 61
New rule 61
"Captive portal" tab 62
Captive portal 63
SSL server 63
Conditions of use for Internet access 63
Advanced properties 64
"Captive portal profiles" tab 64
Possible actions 64
Authentication 65
Conditions of use for Internet access 65
Authentication periods allowed 65
Advanced properties 65
Transparent or explicit HTTP proxy and multi-user objects 67

Multi-user objects 67
Transparent proxy (implicit) 68
Explicit proxy 68

BLOCK MESSAGES 70

Antivirus tab 70
POP3 protocol 70
SMTP protocol 70
FTP protocol 70
“HTTP block page” tab 70
Block page tabs 71
Editing block pages 71

CERTIFICATES AND PKI 73

Possible operations 73
Search bar 73
Filter 73
Add 74
Delete 74
Action 74
Download 75
Check usage 76
Adding authorities and certificates 76

CLI CONSOLE 84

List of commands 84
Data entry zone 85

CONFIGURATION 86

“General configuration” tab 86
General configuration 86
Cryptographic settings 86
Password policy 87
Date/Time settings 88
Hardware 88
Advanced properties 90
“Firewall administration” tab 90
Access to the firewall’s administration interface 90
Access to firewall administration pages 91
Disclaimer for access to the administration interface 91
Remote SSH access 91
“Network settings” tab 92
IPv6 support 92
Proxy server 92
DNS resolution 92

CONFIGURATION OF MONITORING 93

Interval between refreshments 93
Configuration of interfaces and QoS queues to be monitored 93
"Interface configuration" tab 93
"QoS configuration" tab 93

DASHBOARD 95

The module configuration menu 95
My favorites 95
Configuration 95
The dynamic area: widgets 96
Network 97
Alarms 97
Resources 98
License 98
Hardware 98
Properties 99
New applications 100
Services 100
Active Update 101
Interfaces 101
High availability 101
Stormshield Management Center 101
Sandboxing 102

DHCP 103

General 103
“DHCP server” service 103
Default settings 103
Address range 103
Reservation 104
Advanced properties 105
“DHCP relay” service 106
Settings 106
Listening interfaces on the DHCP relay service 106

DIRECTORIES CONFIGURATION 108

Main window 108
"Add a directory" button 108
"Action" list 108
Creating an internal LDAP 108
Step 1: Selecting the directory 109
Step 2: Accessing the directory 109
Internal LDAP directory screen 109
Connecting to an external LDAP directory 110
Step 1: Selecting the directory 110
Step 2: Accessing the directory 110
External LDAP directory screen 111
Connecting to a PosixAccount external LDAP directory 114
Step 1: Selecting the directory 114
Step 2: Accessing the directory 114
External LDAP directory screen 115
Connecting to a Microsoft Active Directory 117

Step 1: Selecting the directory 117
Step 2: Accessing the directory 117
Microsoft Active Directory screen 118

DNS CACHE PROXY 121
Enable DNS cache 121
List of clients allowed to used the DNS cache 121
Advanced properties 121

DYNAMIC DNS 123
List of dynamic DNS profiles 123
Configuring a profile 123
DNS resolution 123
Dynamic DNS service provider 123
Advanced properties 124

E-MAIL ALERTS 125
"Configuration" tab 125
Enable e-mail notifications 125
SMTP server 125
E-mail sending frequency (in minutes) 126
Intrusion prevention alarms 126
System events 126
"Recipients" tab 127
Creating a group 127
Deleting a group 127
Check use 128
"Templates" tab 128
Editing the template (HTML) 128
Vulnerability manager 128
Certificate request 129
User enrollment 129
List of variables 129
Example of a report received by e-mail regarding alarms 129

ENROLMENT 130
The enrolment table 130
Possible operations 130
User enrolment and certificate requests 130
Advanced properties 131

FILTERING AND NAT 132
Evaluation of filtering and the impact of NAT 132
"FastPath" mode 132
Policies 132
Selecting the filter policy 133
Possible operations 134
Selecting multiple objects 134
Drag & drop 134
"Filtering" tab 134
Actions on filter policy rules 135
Interactive features 137
Filter table 138
"NAT" tab 150
Actions on NAT policy rules 151
Interactive features 153
NAT table 154

HIGH AVAILABILITY 159
Step 1: Creating or joining a high availability cluster 159
Step 2: Configuring network interfaces 160
If you have chosen to create a cluster 160
If you have chosen to join a cluster 160
Step 3: Cluster's pre-shared key and data encryption 161
If a cluster is being created 161
If a cluster exists 162
Step 4: Summary and finalizing the cluster 162
If a cluster is being created 162
If a cluster exists 162
High availability screen 163
Communication between firewalls in the high availability cluster 163
Advanced properties 163

HOST REPUTATION 165
"Configuration" tab 165
General 165
"Hosts" tab 166
Included list 166
Advanced properties 166

IDENTIFICATION PORTAL 167
Connection 167
Presentation 167
Logging off 168

IMPLICIT RULES 170
Implicit filter rules 170
Rule table 170
Advanced properties 171

INSPECTION PROFILES 172
Security inspection 172
Global configuration for each profile 172
Configuring profiles 173

IPSEC VPN 174

"Encryption policy – Tunnels" tab .. 174
Site to site (Gateway-Gateway) 175
Anonymous – Mobile users 178
"Peers" tab 181
List of peers 181
Peer information 182
"Identification" tab 187
Approved certificate authorities 187
Mobile tunnels: pre-shared keys 188
Advanced configuration 188
"Encryption profiles" tab 189
Default encryption profiles 189
Table of profiles 189

INTERFACES 193

Operating mode between interfaces 193
Advanced mode 193
Bridge mode or transparent mode 193
Hybrid mode 194
Link aggregation (LACP) – SN510, SN710, SN910, SN2000, SN3000 and SN6000 194
Conclusion 194
Presentation of the configuration screen 194
Directory of interfaces 195
Toolbar 196
Creating a bridge 196
Identifying the bridge 196
Address range 197
Modifying a bridge 197
"General" tab 197
"Advanced properties" tab 198
"Bridge members" tab 200
Deleting a bridge 200
Modifying an Ethernet interface (in bridge mode) 200
"Configuration of the interface" tab .. 200
"Advanced properties" tab 202
Modifying an Ethernet interface (advanced mode) 204
Creating or modifying a Wi-Fi interface (WLAN) 204
"Configuration of the interface" tab .. 204
Creating a VLAN 205
VLAN attached to a single interface (VLAN endpoint) 206
VLAN attached to 2 interfaces (crossing VLAN) 206
Adding a VLAN 208
Modifying a VLAN 208
"Configuration of the interface" tab .. 208
"Advanced properties" tab 209
Deleting a VLAN 211
Creating a modem 211
Step 1 211
Customized 3G/4G modem profile 212
Step 2 213
Modifying a modem 213
PPPoE modem 213
PPTP Modem 214
PPP Modem 215
3G/4G modem 215
Deleting a modem 216
General remarks on configuring modems 216
Creating a USB stick / modem 216
Modifying a USB/Ethernet interface 217
"Configuration of the interface" tab 218
Creating a GRETAP interface 219
Modifying a GRETAP interface 219
"Configuration of the interface" tab 219
"Advanced properties" tab 221
Converting an interface to link aggregation (LACP) 222
"Link aggregation (LACP)" Tab 223
Configuring an aggregated link 223

LICENSE 225

"General" tab 225
Buttons 225
Dates 225
Important information about the license 225
Installing from a file 226
Advanced properties 226
"License details" tab 227
Buttons 227
The table 227

LOGS - SYSLOG - IPFIX 230

"Local storage" tab 230
Configuration of the space reserved for logs 231
"Syslog" tab 232
Table of Syslog profiles 232
Configuring a profile 232
"IPFIX" tab 233
Advanced properties 234

MAINTENANCE 235

"Configuration" tab 235
System disk 235
Maintenance 235
High availability 235
System report (sysinfo) 236

"Backup" tab 236
Configuration backup 236
Configuration automatic backup 236
"Restore" tab 238
Restore configuration 238
Automatic backup restoration 238
"System update" tab 239
Advanced properties 239

MONITORING 241

Private data 241
The table 242
Tooltips 242
Hardware / High Availability 243
"Hardware" tab 243
"Cluster details" tab 244
System 246
"Real time" tab 246
"History" tab 246
Interfaces monitoring 247
"Real time" tab 247
"History" tab 247
QoS 248
"Real time" tab 248
"History" tab 249
Hosts 249
"Real time" tab 249
"History" tab 255
Users 256
"Real time" tab 256
Connections 261
"Real time" table 261
Routing 264
"Real time" tab 264
DHCP 264
"Real time" table 264
SSL VPN tunnels 265
"Real time" table 265
"Information" table 266
IPSec VPN tunnels 266
"Policies" table 266
"Tunnels" table 267
Black list / white list 268
"Real time" table 268

NETWORK OBJECTS 269

Possible actions 269
Interactive features 270
Filter 270
The various types of objects 271
Host 271
Network 271
IP address range 271
Port – port range 272
IP protocol 272
Group 272
Port group 273
Router 273
Region group 275
DNS name (FQDN) 276
Time object 276
Fixed event 276
Day of the year 277
Day(s) of the week 277
Time slots 277

PPTP SERVER 278

General configuration 278
Parameters sent to PPTP clients 278
Advanced configuration 278
Traffic encryption 278

PREFERENCES 279

Logon settings 279
Application settings 279
Management interface behavior 280
External links 280
Log settings 280

PROTOCOLS 281

Search 281
List of protocols 281
Profiles 281
Selecting a profile 281
Buttons 282
Global protocol configuration 282
Global configuration of the TCP/UDP protocol 283
Global configuration of the SSL protocol 283
Global configuration of the ICMP protocol 284
ICQ – AOL IM (OSCAR) 284
Profiles screen 284
Live Messenger (MSN) 285
Profiles screen 285
Yahoo Messenger (YMSG) 285
Profiles screen 285
ICMP 285
"IPS" tab 285
IP 286
"IPS" tab 286
SCTP 286
"IPS" tab 286
TCP-UDP 287
Profiles screen 287

BACnet/IP 288
Service management 288
Support 289
CIP 289
Settings 289
Service management 289
ETHERNET/IP 290
EtherNet/IP settings 290
EtherNet/IP command management 290
Support 290
IEC 60870-5-104 (IEC 104) 291
Settings 291
Redundancy 291
ASDU management 291
Support 291
MODBUS 292
General settings 292
Modbus settings 292
Managing Modbus function codes 292
Managing Modbus addresses 292
Support 293
OPC AE 293
Service management 293
OPC DA 293
Services management 293
OPC HDA 293
Service management 293
OPC UA 294
OPC UA parameters 294
Managing OPC UA services 294
Support 294
S7 294
Settings 294
Managing function codes 295
Support 295
UMAS 295
UMAS Parameters 295
UMAS function codes management 296
Support 296
MS-RPC protocol 296
NetBios CIFS 297
Profiles screen 297
EPMAP protocol 298
NetBios SSN 298
MGCP 298
Profiles screen 298
RTCP 299
“IPS” tab 299
RTP 299
“IPS” tab 299
RTSP 299
RTSP commands 300
Maximum size of elements (bytes) 300
RTSP session settings 300
RTSP features 300
Support 300
SIP 300
SIP commands 301
Maximum size of elements (bytes) 301
SIP session parameters 301
SIP protocol extensions 302
Support 302
DNS 303
Profiles screen 303
FTP 304
“IPS” tab 304
“Proxy” tab 304
“Commands FTP” tab 305
« FTP Users » tab 309
“Analyzing files” tab 309
"Sandboxing" tab 310
HTTP 310
“IPS” tab 311
“Proxy” tab 313
“ICAP” tab 314
“Analyzing files” tab 315
"Sandboxing" tab 316
NTP 317
POP3 320
“IPS - PROXY” tab 320
“POP3 Commands” tab 320
“Analyzing files” tab 321
"Sandboxing" tab 322
SMTP 322
“IPS” tab 322
“Proxy” tab 323
“SMTP Commands” tab 324
“Analyzing files” tab 324
"Sandboxing" tab 325
SNMP 326
Allow version 326
Allow Empty Field 326
SNMP command management 326
Community name 326
Identifiers 326
OID 327
Support 327
SSL 327
“IPS” tab 327
“Proxy” tab 329
TFTP 331
Profiles screen 331
Others 331

QUALITY OF SERVICE (QoS) 332
Network traffic 332
Bandwidth reservation or limitation (CBQ) 332
Queues 332
Class-based queue (CBQ) 333
Monitoring queue 334
Priority queue 335
Available queues 335
Examples of application and usage recommendations 335
RECORDING CONFIGURATION COMMANDS 338
Recording a sequence of configuration commands 338
ACTIVITY REPORTS 339
Personal data 339
Collaborative security 339
Storage device: SD Card 339
Activity Reports 340
Possible operations 340
Interactions 341
Reports 342
REPORT CONFIGURATION 348
"General" menu 348
Table of reports and history graphs 348
"List of reports" tab 348
"List of history graphs" tab 349
ROUTING 350
“Static routes” tab 350
Button bar 350
Interactive features 351
Presentation of the table 351
“Dynamic routing” tab 351
Advanced properties 352
Sending the configuration 352
“Return routes” tab 352
Button bar 352
Interactive features 352
Presentation of the table 353
SMTP FILTERING 354
Profiles 354
Selecting a profile 354
Buttons 354
Rules 354
Possible operations 355
Interactive features 355
The table 355
Errors found in the SMTP filter policy 356
SNMP AGENT 357
“General” tab 357
Configuration of MIB-II information 357
Sending of SNMP alerts (traps) 357
“SNMPv3” tab 358
Connection to the SNMP agent 358
Authentication 358
Encryption (optional) 358
Sending of SNMPv3 alerts (traps) 358
“SNMPv1 - SNMPv2c” tab 359
Connection to the SNMP agent 359
Sending of SNMPv2c alerts (traps) 360
Sending of SNMPv1 alerts (traps) 360
MIBS and Traps SNMP 360
Stormshield Network SNMP event and alert (traps) format 360
Management information bases (MIBs) 362
SSL FILTERING 376
Profiles 376
Selecting a profile 376
Buttons 376
Rules 377
Possible operations 377
Interactive features 377
The table 377
Errors found in the SSL filter policy 378
SSL VPN 379
Network settings 379
DNS settings sent to client 380
Advanced properties 380
Used certificates 381
Configuration 381
SSL VPN Portal 382
“General” tab 382
Advanced properties 383
“Web servers” tab 383
Adding a web server 383
Adding an OWA web server 385
Adding a Lotus Domino web server 386
“Application servers” tab 386
Configuration with an application server 386
Configuration with a Citrix server 387
Deleting a server 387
“User profiles” tab 388
Operating principle 388
Configuring a profile 388

SSL VPN services on the Stormshield Network web portal 389
Accessing your company's web sites via an SSL tunnel 389
Accessing your company's resources via an SSL tunnel 389

MULTICAST ROUTING 390
Actions on multicast routing policy rules in IPv4 390
Interactive features 390
New rule 390
The table 391

STORMSHIELD MANAGEMENT CENTER 392
Attaching the firewall to SMC 392
Buttons 392

SYSTEM EVENTS 393
Possible operations 393
Search 393
Restore the default configuration 393
List of events 393
System alarms list 394

TEMPORARY ACCOUNTS 398
Temporary accounts list 398
The table 398
Possible operations 399

URL FILTERING 401
Profiles 401
Selecting a profile 401
Buttons 401
Rules 401
Possible operations 402
Interactive features 402
The table 402
Errors found in the URL filter policy 403

USERS 404
Possible operations 404
Search bar 404
Filter 405
Interactive features 405
Creating a group 405
Creating a user 406
Delete 406
Check usage 406
List of users (CN) 407
"Account" tab 407
"Certificate" tab 407
"Member of these groups" tab 407

VIRTUAL INTERFACES 408
Creating or modifying an IPSec interface (VTI) 408
Button bar 408
Interactive features 408
Presentation of the table 409
Creating or modifying a GRE interface 409
Button bar 409
Interactive features 410
Presentation of the table 410
Creating or modifying a loopback interface 410
Button bar 410
Interactive features 411
Presentation of the table 411

VULNERABILITY MANAGEMENT 412
General configuration 412
List of monitored network objects 413
Advanced configuration 414
Exclusion list (unmonitored objects) 414

WEB OBJECTS 415
"URL" tab 415
URL category table 415
URL table 416
"Certificate name (CN)" tab 417
"Groups of categories" tab 417
Table of groups 417
"URL database" tab 418

Wi-Fi 419
General configuration 419
Channel configuration 419

IPv6 Support 420
IPv6 Support 420
Details of supported features 420
Unsupported features 422
General points 422
Configuration 423
Network Settings tab 423
Interfaces 423
Modifying a bridge 423
Creating a bridge 426
Modifying an Ethernet interface (in bridge mode) 426
Modifying an Ethernet interface (advanced mode) 427
Creating a VLAN 427

Modifying a VLAN 428
Virtual interfaces 428
"IPSec interfaces (VTI)" tab 428
"Loopback" tab 428
Routing 428
"IPv6 static routes" tab 429
"IPv6 dynamic routing" tab 430
"IPv6 return routes" tab 430
DHCP 431
General 431
"DHCP server" service 431
"DHCP relay" service 434
Network objects 435
Possible actions 435
The different types of objects 435
Filtering 436
"Filtering" tab 436

Allowed or prohibited names 438

Firewall name 438
Login and password 438
Comments (prohibited characters) 438
Rules separators (prohibited characters) 438
Interface names 438
Objects 438
DNS (FQDN) name objects 439
Certificates 439
Users 439
IPSEC VPN 439
SSL VPN 439
E-mail alerts 439

Structure of an objects database in CSV format 440

Host 440
IP address range 440
DNS name (FQDN) 440
Network 441
Port 441
Range port 441
Protocol 441
Host group, IP address group or network group 442
Service group 442

WELCOME

Welcome to the Stormshield Network v3.9.1 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.

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

Products concerned

SN160(W), SN210(W), SN310,

SN510, SN710, SN910,

SN2000, SN2100, SN3000, SN3100, SN6000, SN6100,

SNi40,

VS5, VS10, V50, V100, V200, V500, VU (only in upgrades to an EVA model).

EVA1, EVA2, EVA3, EVA4 and EVAU.

Copyright © Stormshield 2020. All rights reserved.

Any copying, adaptation or translation of this material without prior authorization is **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

DEFINITION

The common criteria evaluate (on an Evaluation Assurance Level or EAL scale of 1 to 7) a product's capacity to provide security functions for which it had been designed, as well as the quality of its life cycle (development, production, delivery, putting into service, updates).

Introduction

The installation of a Firewall often comes within the scope of setting up a global security policy. To ensure optimal protection of your assets, resources or information, it is not only a matter of installing a Firewall between your network and the Internet. This is namely because the majority of attacks come from the inside (accidents, disgruntled employees, dismissed employee having retained internal access, etc.). And one would also agree that installing a steel security door defeats its purpose when the walls are made of paper.

Backed by the Common Criteria, Stormshield Network advises taking into consideration the recommendations of use for the Administration Suite and Firewall product stated below. These recommendations set out the usage requirements by which to abide in order to ensure that your Firewall operates within the context of the common criteria certification.

Security watch

Please regularly check Stormshield security advisories published on https://advisories.stomshield.eu.

Always update your firewall if it allows fixing a security flaw. Updates are available here: https://mystormshield.eu.

Physical security measures

Stormshield Network Firewall-VPN appliances must be installed and stored in compliance with 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

The default password of the "admin" user (super administrator) must be changed the very first time the product is used. The wizard will prompt the user to change his password during the initial installation, in the *Administration of the appliance* window. In the web administration interface, this password can be changed in the **Administrator** module (**System** menu), under the *Administrator account* tab.

The definition of this password must observe the best practices described in the following section, under *User password management*.

A particular administrative role – that of the super-administrator – has the following characteristics:

- Only the super-administrator is permitted to connect via the local console on NETASQ firewall-VPN appliances, and only when installing the Firewall or for maintenance operations, apart from actual use of the equipment.
- He is in charge of defining the profiles of other administrators,
- All access to the premises where the appliances are stored has to be under his supervision, regardless of whether the access is due to an intervention on the appliance or on other equipment. He is responsible for all interventions carried out on appliances.

User and administrator passwords have to be chosen in such a way that successful attempts at cracking them will take longer. This can be assured with the implementation of a policy regulating their creation and verification.

Example

Combination of letters and numbers, minimum length, addition of special characters, words which are not taken from ordinary dictionaries, etc.

Administrators are attuned to these best practices in the course of their functions and have the responsibility of directing users' awareness to these practices (Cf. Next section: User Awareness).

For equipment in "trusted" networks which have to be protected, the control policy for traffic to be implemented should be defined in the following manner:

- **Complete**: the standard scenarios of how equipment is used have all been considered when defining the rules and their authorized limits have been defined.
- **Strict**: only the necessary uses of the equipment are authorized.
- **Correct**: rules do not contradict each other.
- **Unambiguous**: the wording of the rules provides a competent administrator with all the relevant elements for direct configuration of the appliance.

Human media

Administrators are non hostile, competent persons with the necessary means for accomplishing their tasks. They have been trained to launch operations for which they are responsible. In particular, their skills and organization imply that:

- Different administrators having the same rights will not perform administrative actions which conflict.
- Logs are used and alarms are processed within the appropriate time frames.

Example

Incoherent modifications to the control policy for traffic.

IT security environment

Stormshield Network firewall-VPN appliances must be installed in accordance with the current network interconnection policy and are the only passageways between the different networks on which the control policy for traffic has to be applied. They are scaled according to the capacities of the adjacent devices or these devices restrict the number of packets per second, positioned slightly below the maximum treatment capacities of each firewall-VPN appliance installed in the network architecture.

Besides applying security functions, NETASQ firewall-VPN appliances do not provide any network service other than routing and address translation.

Example

no DHCP, DNS, PKI, application proxies, etc.*

Stormshield Network appliances are not configured to forward IPX, Netbios, AppleTalk, PPPoE or IPv6 information flows.

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

Remote administration workstations are secured and kept up to date on all known vulnerabilities affecting operating systems and hosted applications. They are installed in protected premises and are exclusively dedicated to the administration of firewall-VPN appliance and the storage of backups.

Network devices that the firewall uses to establish VPN tunnels are subject to constraints relating to physical access, protection and control of their configuration. These constraints are equivalent to those faced by the TOE’s firewall-VPN appliances.

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.

** These services are available on firewalls but are not part of the scope of evaluation of the common criteria.*

Evaluated configurations and usage

The usage of the environment being evaluated must possess the following characteristics:

- Certificates and CRLs are distributed manually (importing).
- The usage mode subject to evaluation excludes the fact that the TOE relies on services other than PKI, DNS and DHCP servers and proxies. The optional modules provided by Stormshield Network to manage these services are disabled by default and have to stay that way. Specifically, these are:
  - the internal public key infrastructure (PKI),
  - User authentication module,
  - SSL VPN module (Portal and Tunnel),
  - antivirus engine (ClamAV or Kaspersky),
  - Active Update module,
  - Dynamic routing module (BIRD dynamic routing service),
  - DNS cache (DNS/Proxy cache),
  - SSH, DHCP, MPD and SNMPD servers (SSH server, DHCP server and SNMP agent),
  - DHCP client (DHCP server),
  - NTP daemon (NTP client),
  - DHCP relay,
  - Cloud backup service.
- Even though it is supported, the IPv6 feature is disabled by default and must remain so for the duration of the evaluation.
- IPSec administrators and users are managed by the internal LDAP directory. The evaluation of such usage excludes the fact that external LDAP clients outside the scope of the firewall-VPN appliance's network can connect to this base.
- Audit logs – depending on the model – are either stored locally or sent by Syslog.
- The ability provided by the filter policy to associate each filter rule with an application inspection (HTTP, SMTP, POP3 and FTP proxies) and a schedule falls outside the scope of this evaluation and must not be used.
- The option of associating a "decrypt" action (SSL proxy) with a filter rule in the filter policy falls outside the scope of this evaluation and must not be used.

Cryptographic algorithms needed for compliance with the RGS (General Security Guidelines defined by ANSSI, the French Network and Information Security Agency) and used for the evaluation

Algorithm	Key size
Diffie-Hellman	2048, 3072, 4096

Algorithm	Key size
RSA	2048, 4096

Algorithms	Fingerprint size
HMAC-SHA1	160
HMAC-SHA2	256, 384, 512
SHA2	256, 384, 512

Algorithms	Key size
AES	128, 192, 256
Triple DES	168
Blowfish	128 to 256
CAST	128

The Perfect Forward Secrecy (PFS) option performs a new Diffie-Hellman key exchange during IKE Phase 2. This allows ensuring that in the event a key has been stolen, the next or previous keys cannot be deduced, thereby preventing the whole IPSec exchange from being decrypted, apart from the segment of the communication protected by the corrupted key. You are strongly advised to leave PFS enabled in order to comply with the RGS, which is the scenario that has been chosen for the evaluation.

The security of the connection to the authentication portal and administration interface has been strengthened, as per the recommendations of the ANSSI (*French Network and Information Security Agency*). These connections have to go through certain versions of the SSL/TLS protocol. Version SSLv3 has been disabled to make way for TLS versions. The use of AES encryption suites with Diffie-Hellman has also been imposed. As Internet Explorer in version 6, 7 and 8 does not support this configuration, you are advised to use a higher version of this browser. This configuration must not be disabled in order to stay within the scope of the evaluation.

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 ("0") / NETASQ Firewall Certification Authority ("OU") and Stormshield ("0") / Cloud Services ("OU").

To confirm a secure access, the browser must trust the certificate authority that signed the certificate used, which must belong to the browser's list of trusted certificate authorities. Therefore to confirm the integrity of an appliance, the NETASQ and Stormshield certificate authorities must be added to the browser's list of trusted certificate 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. The wizard will prompt the user to change his password during the initial installation, in the *Administration of the appliance* window. In the web administration interface, this password can be changed in the **Administrator** module (**System** menu), under the *Administrator account* tab.

The definition of this password must observe 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. For 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 certificate 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, please 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).

ACCESS PRIVILEGES

This module consists of 3 tabs:

- *Default access*: This tab allows you to define SSL VPN portal, IPSec VPN and SSL VPN access parameters as well as the default sponsorship policy.
- *Detailed access*: Table of rules corresponding to SSL VPN portal, IPSec VPN and SSL VPN access and access to users authorized to validate sponsorship requests.
- *PPTP server*: Allows adding and listing users who have access to PPTP VPN via their logins, and creating passwords to enable them to log on.

"Default options" tab

SSL VPN Portal

SSL VPN Portal profiles (see menu **VPN>SSL VPN Portal** module) represent the set of web and application servers that you wish to list in order to assign them to your users or user groups.

SSL VPN portal profile	In this field, the default SSL VPN Portal profile can be defined for users. Prior to this, ensure that you have already restricted access to servers defined in the configuration of the SSL VPN in the menu **VPN**>**SSL VPN Portal**>\User profiles tab (see SSL VPN Portal document). The drop-down list will display the following options: • Block: Users will not have access to the SSL VPN Portal. • Allow: The user will have access to all SSL VPN Portal profiles created previously. ---------- <Name of user1 profile>: the user will have access only to this SSL VPN Portal profile. <Name of user2 profile>: the user will have access only to this other SSL VPN Portal profile.

Click on **Apply** to confirm your configuration.

IPSEC

IPSec VPN enables the establishment of secure tunnels (peer authentication, data encryption and/or integrity checking) between two hosts, between a host and a network, or between two networks.

IPSec policy	In this field, it is possible to **Block** or **Allow** users the privilege of negotiating IPSec VPN tunnels by default. 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.

Click on **Apply** to confirm your configuration.

SSL VPN

The SSL VPN allows setting up a secure tunnel (peer authentication, encryption and/or verification of data integrity) between two hosts, between a host and a network, or between two

networks.

SSL VPN policy	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.

Click on **Apply** to confirm your configuration.

Sponsorship

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

Default sponsorship policy	This field makes it possible to Block or Allow users from responding to sponsorship requests submitted from the captive portal by default.

Click on **Apply** to confirm your configuration.

"Detailed access" tab

Possible operations

- **Add** button: Inserts a line to be configured after the selected line.
- **Delete** button: Deletes the selected line.
- **Up** button: Places the selected line before the line just above it.
- **Down** button: Places the selected line after the line just below it.

A search field in which keywords/letters can be entered will allow you to find relevant users.

Interactive features

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

- Add,
- Delete.

Configuration table

This table allows assigning access privileges to your users or user groups, with regards to **SSL VPN** and **IPSec VPN** parameters.

The table contains the following columns:

Status	Status of the access privilege configuration for the user or user group: Enabled: Double-click anywhere in the column to enable the created rule. Disabled: The rule is not in operation. 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. They are numbered likewise on the left side of the column. If Rule 1 affects a user group, all users involved in the rules that follow and which are part of this same group will be subject to its configuration. **Example**: If in Rule 1, you deny a user group authentication and/or access to the **SSL VPN** and if the user in Rule 2 can authenticate via the LDAP and has a particular SSL VPN profile but is part of the group, this user will be blocked, and will have neither access to authentication nor to the SSL VPN.
User-user group	Whenever a new line is added to the table, you can select the user of the user group you wish to configure. To do so, click on the arrow to the right of the column, which will display a drop-down list offering you a choice of several CNs created earlier, in the menu **Users**\Users module. **NOTE** It is also possible to add users who are not in the LDAP database, for example, for the KERBEROS and RADIUS methods.
SSL VPN Portal	This column allows you to assign a particular SSL VPN profile to a user or user group, configured beforehand in the menu **VPN\SSL VPN module***User profiles* tab. You may also select the Default option, which will take into account the default SSL VPN profile entered in the previous tab (Default options). If you select Deny, the user or user group will not have access to any SSL VPN profiles, contrary to the option All profiles, which will provide access to all web and application servers that have been enabled in the user profiles.
IPSEC	In this field, it is possible to **Block** or **Allow** users the privilege of negotiating IPSec VPN tunnels. 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. **REMARK** The IPSec privilege only concerns tunnels: • with pre-shared key authentication and e-mail address logins, or • with certificate authentication.
SSL VPN	In this field, it is possible to **Block** or **Allow** users the privilege of negotiating SSL VPN tunnels. 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	Depending on your selection, users or user groups will or will not be able to validate sponsorship requests submitted from the captive portal.
Description	Comments describing the user, user group or the rule.

REMARK

When you add lines to the table without having set up any rules, the columns **Authentication**, **SSL VPN** and **IPSEC** will be set to "Deny" by default, even if you have

configured them differently in the Default options tab.

You therefore need to click on the option “Default” using the arrow to the right of each column if you wish to retrieve changes made earlier.

“PPTP” tab

This tab allows listing users who have access to the **PPTP VPN**, providing them with a secure and encrypted connection for their login.

Interactive features

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

- Add,
- Delete,
- Change password.

The following actions can be performed:

Add	When you click on this button, a new line will be added to the table and will display the drop-down list of users created earlier in the menu **Users\Users module**: To ensure that the operation is valid, you will need to enter the user's password in the window that appears. **NOTE** It is possible to enter a user that does not exist in the firewall's user database, as the PPTP is separate from the LDAP module.
Delete	To delete a user, select the line containing the user to be removed from the list of PPTP logins, then click on **Delete**.
Change password	Select the line containing the user whose password you wish to modify, and enter the new data in the window that appears.

NOTE

A login consisting only of uppercase letter can be entered.

ACTIVE UPDATE

The **Active Update** configuration window consists of a single screen. This screen is divided into 2 sections:

- **Automatic updates**: allows activating an update module.
- **Advanced properties** – **Update servers**: allows defining update servers.

Automatic updates

On	Enables or disables (Enabled/ Disabled buttons), by a simple click, updates via Active Update for the type of update selected.
Module	Type of update. (The list of modules varies according to the license purchased).

NOTES

In the event of a failed update, the system will automatically backtrack. Simply double-click to allow (**"Allow all"** button) or prohibit (**"Block all"**) all updates.

Advanced properties

Update servers of the URL database

If the **Stormshield Network URL database** has been selected as the URL database provider (menu **Object** > **Web objects**, **URL database** tab), servers other than Stormshield Network servers can be entered. This allows you to update the Stormshield Network URL database through internal mirror sites or import your own URL database.

URL	Update files are retrieved on one of the servers defined by the user. 4 URLs are defined by default. To add a URL, click on **Add**; the following URL will be added by default: http://update.1.stormshield.eu/1. Replace this with your own URL and click on **Apply**. To delete a URL from the list, select it and click on **Delete**.
Update frequency	Indicates the frequency with which dynamic URL lists, ASQ contextual signatures and the antispam configuration are updated. The frequency is indicated as 3 hours, and can be modified in console mode.

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 (made easy with views by types of alarms, connections, web logs, etc) generated by appliances and stored locally. Advanced filters allow these logs to be thoroughly analyzed.

Personal 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 "Full access to logs (sensitive data)" privilege by clicking on "**Restricted access to logs**" (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 "**Full access to logs (sensitive data)**" 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 "Full access to logs (sensitive data)" privilege is obtained or released, it will generate an entry in logs.

Collaborative security

For more collaborative security, based on views and audit logs, it is now possible in just one click to increase the level of protection on a host. 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 Card

The **External log storage on SD card** feature is available on SN160(W), SN210(W) and SN310 firewall models. This feature is offered with a subscription to the “External storage” option.

The type of SD card must be at least **Class 10** and compliant with the **SDHC or SDXC standard**.

Only the SD format is compatible: Micro SD or Nano SD cards fitted with an adapter are not supported. The maximum memory 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 Guides **PRESENTATION AND INSTALLATION OF NETASQ PRODUCTS U SERIES – S Models** or **PRESENTATION AND INSTALLATION OF STORMSHIELD NETWORK PRODUCTS SN Range,** available on the Stormshield Technical Documentation website.

Logs

To prevent the display of this module in the firewall's web administration interface, unselect the **Show the "Logs" menu** checkbox (Preferences > **Log preferences** menu);

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 or a view

Clicking on a row in a log or view 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

ACTION:

- **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 log or view. This search type is the same as dragging and dropping the value.

CONFIGURATION:

- **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

ACTION:

- **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 log or view. 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 log or view.

CONFIGURATION:

- **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

ACTION:

- **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.

CONFIGURATION:

- **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.

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 privilege for full access to logs):

- 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.

URLs

ACTION:

- **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.

CONFIGURATION:

- **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 allows adding 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 privilege for full access to logs):

- Domain name,
- Corresponding IP address.

Ports

CONFIGURATION:

- **Add the service to the objects base and/or add it to a group:** this option allows creating a service and/or adding 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 privilege for full access to logs):

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

Network packets

ACTION

- **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

CONFIGURATION

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

System events view

CONFIGURATION

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

Views

- 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, Vulnerabilities, 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.

- 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.

Three predefined filters that search for Application (classification=1), Malware (classification=2) or Protection (classification=0) vulnerabilities are offered.

- 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.

- Vulnerabilities

This view displays the **Vulnerabilities** log.

Two predefined filters that search for Client (targetclient=1) and Server (targetserver=1) vulnerabilities are 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; the System events log only displays logs for which the reference message is PPTP.

- 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 only displays logs belonging to the filter alarm category.

- Sandboxing

This view displays the **Sandboxing** log.

- Users

This view displays the **Authentication** log.

Logs

The list of logs displayed in the menu and the name of the corresponding log file is shown below:

Administration	l_server
Alarms	l_alarm
Authentication	l_auth
Network connections	l_connection
Filtering	l_filter
FTP proxy	l_ftp
IPSec VPN	l_vpn
Application connections (plugin)	l_plugin
POP3 proxy	l_pop3
SMTP proxy	l_smtp
SSL proxy	l_ssl
System events	l_system
Vulnerabilities	l_pvm
HTTP proxy	l_web
SSL VPN	l_xvpn
Sandboxing	l_sandboxing

NOTE

If the user does not have *admin* privileges, the **Administration** log will not be accessible.

NOTE

If the time on the firewall is changed, a yellow line indicating this change will be shown for each log queried. This line is logged when the change is made.

As a result, the period displayed may no longer correspond to the expected number of hours. For example, if the time on the firewall has been moved back by one hour, the log for the past day will show logs for the past 25 hours. Likewise, if a search is launched for a common time, the search will be conducted in all logs, meaning before and after the change of time on the firewall.

ADMINISTRATORS

This module consists of 3 tabs:

- ***Administrators***: allows creating administrators by granting administration privileges to users using one of the following authentication methods: LDAP RADIUS, KERBEROS or SSL.
- ***Admin account***: allows defining the authentication password of the administrator account by exporting the public or private key.
- ***Ticket management*** : administrators with the privilege to manage access to private data can create tickets for temporary access to such data.

"Administrators" tab

The window for this tab is divided into 3 sections:

- A taskbar (top): displays the various possible operations that can be performed (**Add an administrator**, **Delete**, **Copy privileges** etc.).
- The list of users and user groups identified as admin (left).
- The table of administrator privileges (right).

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.

Once the administrator's task is complete, he can release this privilege.

Interactive features

Some operations listed in the section "Possible operations" can be performed by right-clicking on the table of administrators:

- Add an administrator,
- Delete (an administrator),
- Copy privileges,
- Paste privileges,
- Grant all privileges.

Possible operations

You will be able to create your table of administrators from your LDAP database as well as their respective privileges.

Adding an administrator

Administrator without any privileges	This type of administrator has all the basic privileges such as access to the **Dashboard** and to the following modules: **License, Maintenance, Active Update**, **High availability** and its wizard, CLI console, **Network, Routing, Dynamic DNS, DHCP, DNS cache proxy**, **Objects, URL categories** and their groups, **Certificates and PKI**, **Authentication** and its wizard, **URL filtering, SSL** and **SMTP, Applications and protections, Inspection profiles, Antivirus, Antispam, Block messages,** and 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 the Administrators and Admin account tabs in the **Administrators** module. **REMARK** There can only be one "superadministrator" with the following characteristics: • The only administrator authorized to log on 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. • He is in charge of defining the profiles of other administrators, • Full access to the premises on which the firewall appliances are stored, and all interventions are performed under his 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	Such administrators 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	Such administrators can access all logs that do not contain private data. To enable the **Full access to logs (private data)** privilege, he must click on **Restricted access to logs** and enter the access code given to him in order to access private data.

Once you have imported your administrator, he will appear in the list "**User-user group**" to the left of the screen.

The following operations can be performed on this administrator.

Delete	Select the administrator to be removed from the list and click on **Delete**.
Move up	Places the administrator above the administrator before him in the list.
Move down	Places the administrator below the administrator after him in the list.
Copy privileges	Select the administrator whose privileges you wish to copy and click on this button.
Paste privileges	Select the administrator to whom you wish to assign the same privileges as the administrator from whom the privileges have been copied and click on this button.
Grant all privileges	Regardless of the privileges assigned to the selected administrator, by clicking on this button.

Table of privileges

Your interface is in "**simple view**" by default. The table displays 5 columns, which represent 5 categories of privileges to which an administrator may or may not be affiliated: **System, Network, Users, Firewall** and **Monitoring**.

The icons in the table mean:

: All privileges have been assigned.

: All privileges have not been assigned.

: Some of the privileges have been assigned.

By switching to "**advanced view**" using the icons or (depending on the length of your screen), the table will display the details of the privileges by category. To find out the exact privileges corresponding to each column, see the bubble that appears when the mouse passes over each column header.

Example

If you are at the top of the **System** column, you will see the access privileges it includes, in this case, **"Maintenance"** and "Objects".

NOTE

Double-clicking on the represented icons changes the status of privileges (from "assigned" to "not assigned" for example). Double-clicking on this icon will assign the privileges, and this icon will be displayed instead.

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`).

The list of privileges that can be assigned in simple view are:

Privileges in simple view

Name	Description	Privileges assigned
System	Privilege to perform maintenance operations (backups, restorations, updates, Firewall shutdown and reboot, antivirus update, modification of antivirus update frequency and RAID-related actions in the monitor) Privilege to modify Object database	modify, base, maintenance, object
Network	Privilege to modify filtering policy configuration and routing configuration (default route, static routes and trusted networks)	modify, base, filter, route
Users	Privilege to modify Users and PKI	modify, base, user, pki
Firewall	Privilege to modify VPN configuration, Intrusion prevention (IPS) configuration and vulnerability management	modify, base, vpn, asq, pvm
Monitoring	Privilege to modify configuration from Stormshield Network Realtime Monitor and log configuration	modify, base, log, maintenance
Temporary accounts	Privilege to manage temporary accounts for the "Temporary accounts" authentication policy	modify,base,voucher

Privileges in advanced view

Name	Description	Privileges assigned
Logs (R)	Log consultation	base, log_read
Filter (R)	Filter policy consultation	base, filter_read
VPN (R)	VPN configuration consultation	base, vpn_read
Access to private data (L)	Privilege to view logs containing private data	base, log_read, report_read, privacy_read
Logs (W)	Privilege to modify log configuration	modify, base, log
Filter (W)	Privilege to modify filter policy configuration	modify, base, filter
VPN (W)	Privilege to modify VPN configuration	modify, base, vpn
Management of access to private data	Privilege to create tickets for ad hoc requests for access to private data in logs.	base, log_read, modify, privacy, privacy_read, report_read
PKI	Privilege to modify PKI	modify, base, pki
Monitoring	Privilege to modify configuration from Stormshield Network Realtime Monitor	modify, base, mon_write
Content filtering	Privilege for URL filtering, Mail, SSL and antivirus management	modify, base, contentfilter
Objects	Privilege to modify Object database	modify, base, object
Users	Privilege to modify Users	modify, base, user

Network	Privilege to modify network configuration (interfaces, bridges, dialups, VLANs and dynamic DNS configuration)	modify, base, network
Routing	Privilege to modify routing (default route, static routes and trusted networks)	modify, base, route
Maintenance	Privilege to perform maintenance operations (backups, restorations, updates, Firewall shutdown and reboot, antivirus update, modification of antivirus update frequency and RAID-related actions in Stormshield Network Realtime Monitor)	modify, base, maintenance
Temporary accounts	Privilege to manage temporary accounts (**Users > Temporary accounts** module)	modify, base, voucher
Intrusion prevention	Privilege to modify Intrusion prevention (IPS) configuration	modify, base, asq
Vulnerability Manager	Privilege to modify vulnerability management configuration (Stormshield Network Vulnerability Manager)	modify, base, pvm
Objects (global)	Privilege to access global objects	modify, base, globalobject
Filter (global)	Privilege to access the global filter policy	modify, base, globalfilter
Reports (W)	Privilege to modify Reports	base, report_read
Reports (R)	Privilege to access Reports	modify, base, report, report_read

The *base* privilege is assigned to all users systematically. This privilege allows reading the whole configuration except filtering, VPN, logs and content filtering.

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

The user who has logged on as *admin* will obtain the *admin* privilege. This is the only privilege that allows giving other users administration privileges or removing them.

"Admin account" tab

This screen allows the definition of authentication data for the *admin* account.

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

NOTE

The default password of the "admin" user (super administrator) must be changed the very first time the product is used.

NOTE

To define an ASCII pre-shared key that is sufficiently secure, it is absolutely necessary to follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management.

Password	Defines the password for the admin account. **REMARK** Must not contain the character ".

Confirm passphrase	Confirms the password of the admin account which you have just entered in the previous field.
Mandatory 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.

NOTE

Stormshield Network uses asymmetrical encryption, meaning that it uses a key pair consisting of a public key, used for encrypting data, and a private key, used for decryption. The advantage of using this system is that it removes the problem of securely transmitting the key and allows electronic signatures.

Export private key	By clicking on this button, you will save the private key associated with the admin account on your workstation.
Export firewall's public key	By clicking on this button, you will save the public key associated with the firewall on your workstation.

"Ticket management" tab

In this table, administrators with the privilege to manage access to private data can create tickets for temporary access to such data.

The table

This table sets out all information relating to tickets for access to private 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 private data found in logs and reports.

Possible operations

Add a ticket

To create a temporary ticket for access to private 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).

Remove

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).
Activate 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**: e-mails will not be blocked but will be tagged as spam. • **Block all spam messages**: the e-mail will be rejected regardless of the level of trust. • **Block all spam messages at Level 2 or higher**: 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 Level 3 spam messages**: 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.

REMARK

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

Advanced properties

The **Antispam** module on Stormshield Network UTM appliances 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**.

NOTE

RBL servers in Stormshield Network's native configuration are differentiated from customized servers by a padlock symbol (), which indicates **RBL** servers in Stormshield Network's native configuration.

Reminder: **Active Update** only updates the list of these servers.

Interactive features

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

- Add,
- Remove.

Heuristic analysis

The heuristic analysis is based on VadeRetro'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. **WARNING** 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. **WARNING** Double quote characters are not allowed.
Minimum score for spam definition [1-5000] :	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. Stormshield Network's default value is 200. 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**. The procedure for adding an authorized domain is as follows:

Domain name (generic characters accepted: * and ?)	Specify the domain to be allowed. Click on **Add**. 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**.

NOTE

The antispam module will NEVER treat messages from whitelisted domains as spam.

Interactive features

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

- Add,
- Remove.

"Blacklisted domains" tab

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

The procedure for adding a domain to be blocked is as follows:

Domain name (generic characters accepted: * and ?)	Specify the domain to be blocked. Click on **Add**. 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**.

GENERAL REMARKS

The antispam module will treat as spam all messages from blacklisted domains.

Interactive features

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

- Add,
- Remove.

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.

For each of these lists, up to 256 domains can be defined. The same domain name cannot appear more than once in the same list. A domain name can appear in either the whitelist or the blacklist.

Domain names can contain alphanumeric characters, as well as "_", "-" and ".". Wildcard characters "*" and "?" are also allowed. The length of the domain name must not exceed 128 characters.

ANTIVIRUS

The configuration screen for the Antivirus service consists of 3 zones:

- Selection of the antivirus engine
- Parameters
- An area relating to sandboxing, available only for the Kaspersky analysis engine.

Antivirus engine

The drop-down list allows migrating between antivirus solutions (ClamAV or Kaspersky). When the choice of an antivirus is made, the following message will appear:

"The antivirus database has to be fully downloaded before the antivirus can be changed. During this interval, the antivirus scan will fail." Click on **Switch engines** to confirm your selection.

Once the database has been downloaded, the antivirus will be enabled.

Settings

Analysis of ClamAV files

The types of files that need to be scanned by the Stormshield Network firewall antivirus service are configured in this menu.

Analyze compressed executable files	This option enables the decompression engine (Diet,Pkite, Lzexe, Exepack, etc.).
Analyze archives	This option enables the extraction engine and allows scanning archives (zip, arj, lha, rar, cab…)
Block encrypted or password-protected files	This option allows blocking files that are encrypted or protected by a password.
Block unsupported file formats	This option allows blocking file formats that the antivirus is unable to scan.

Analysis of Kaspersky files

Inspect archives	This option enables the extraction engine and allows scanning archives (zip, arj, lha, rar, cab, etc.)
Block password-protected files	This option allows blocking password-protected files.
Activate heuristic analysis	Heuristic analysis is a method used to detect new viruses as well as new variants of known viruses, and is based on the assumed behavior of a program in order to determine whether such a program is a virus. This method is not to be confused with statistical analysis, which operates by looking up a repository of known viruses. Heuristic analysis therefore makes it possible to detect viruses that have not yet been referenced in an antivirus engine vendor's repository. This option is not supported on SN160(W), SN210(W) and SN310 firewall models.

Sandboxing

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

Note that it is possible to manually submit a file to https://breachfighter.stormshieldcs.eu/ for this file to be scanned.

After undergoing sandboxing, the file will be assigned a score (maliciousness threshold) evaluated on a scale of 1 to 100. Files with a score of 0 are therefore considered not dangerous. Files with a score above 0 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 your alarms generated by the firewall's applications and protection modules.

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** (*IPS_00*) is a set of **application profiles** (*default00* – See the module **Protocols**). An **application profile** contains the configuration of the alarms from a protocol scan that can be modified in this module. Its other configuration elements can be accessed in the corresponding "**Protocols**" menu.

To configure inspection profiles according to 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** for 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 scans as well as the security policy applied.

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

- "view by inspection profile" (also called " view by configuration")

- "view by context" (also called "view by protocol")

View by inspection profile

Selecting the configuration profile

You can configure up to 10 profiles, bearing by default the names "IPS_00", "IPS_01" etc. These names cannot be modified in the Alarms module but in the menu **Application protection\Inspection profile** (*Go to profiles* button):

1. Select a configuration from the drop-down list.
2. Click on "Edit" and select "Rename".
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.

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).

Example: Several lines can be deleted at the same time by selecting them with the Ctrl key held down, then by clicking on **Delete**.

You can perform several actions in the profile:

Applying a model

Several templates allow configuring 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".

New alarms

Approve new alarms	If this option is selected, all new alarms represented by the icon will be accepted. This allows validating the action and alarm level set by default.

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**.
Protection	These alarms are raised by the ASQ 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 applications.

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 section **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 packet that set off the alarm will be subject to the action configured. You can choose to **Allow** or **Block** traffic that causes this alarm.
Level	Three alarm levels are available: **"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. To remove a packet from quarantine, use Stormshield Network Realtime Monitor. • **for a period of (minutes)**: duration of the quarantine **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*. **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. 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

The action Allow on an alarm stops the protocol scan on the traffic. You are therefore strongly advised to dedicate a filter rule in Firewall mode (or IDS for logs) for traffic affected by the alarm instead of setting 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 scan 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 profiles, which can be selected from the second drop-down list (which displays "default")

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

1. Select a configuration from the drop-down list.
2. Click on "Edit" and select "Rename".
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 modify the policy within a profile according to 4 predefined **templates**: INTERNET, LOW, MEDIUM and HIGH, described in the section "**View by inspection profile**".

The "new" status of alarms can be removed by clicking on **Approve new alarms** described in the previous section. You can also **Search** in alarms by typing letters or words in the appropriate field.

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 button **Add a method** opens a drop-down list that offers a choice of 8 authentication methods that you can **Delete** if necessary. These methods are:

- LDAP
- SSL Certificate (SSL)
- Radius
- Kerberos
- Transparent authentication (SPNEGO)
- SSO Agent
- Guest method
- Temporary accounts
- Sponsorship method

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\Directory 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 certificate authority you wish to trust is not in the list of external certificates, click on **Select** in the external certificate window to add this certificate authority to the list. Firewalls support **multi-level root authorities** – the certificate of the user to be authenticated is signed by a certificate 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 certificate authority.

Certificate 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 (SSL authentication)	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.

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.
Domain or directory	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 Stormshield Network firewall can act as a

RADIUS client and can therefore address authentication requests for users wishing to pass through the Firewall, to an external RADIUS server. 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 may enter information about it in the right column, which sets out the following elements:

Access to the server

When the RADIUS method is selected, RADIUS authentication will be enabled. This menu will allow you to specify information relating to the external RADIUS server used and a backup RADIUS server. For each of them, the configuration requires the following information:

Server	IP address of the RADIUS server.
Port	Port used by the RADIUS server. By default, the port 1812 / UDP named RADIUS is selected.
Pre-shared key	Key used for encrypting exchanges between the firewall and the RADIUS server.

Backup server

Server	IP address of the backup server.
Port	Port used by the backup server if the main server is no longer available. By default, the port 1812 / UDP named RADIUS is selected.
Pre-shared key	Key used for encrypting exchanges between the firewall and the backup server.

REMARK

The firewall will attempt to connect twice to the "main" RADIUS server, and in the event of failure, will attempt to connect twice to the "backup" RADIUS server. If the backup RADIUS server responds, it will become the main RADIUS server. After 600 seconds, a new switch will take place, and the original "main" RADIUS server will become the "main" server again.

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 (Internet Explorer, 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 your **secure area**, in the Knowledge Base (article *"Where can I find the last version of the "spnego.bat" script?"*).

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/U70XXAZ0000000

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

Single Sign-On (SSO) allows a user 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 a seamless authentication on Windows Active Directory. Please refer to the technical note **Stormshield Network SSO Agent - Installation and deployment** for instructions on how to install this application.

When a user logs on to the Windows domain by opening his session, he will automatically be authenticated on the firewall. The principle is as follows: the SSO agent gathers information on the identification of a user 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.
Pre-shared key 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 have to 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 have to be saved beforehand in the firewall's object database. **NOTE** The firewall manages a single domain, as only a single directory can be configured.

Advanced properties

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	This option allows deleting authenticated used 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 period defined hereafter, the SSO agent will send a logoff 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 allows, for example, detecting a closed session on a host that is still running. In the event of a positive response to the ping, the SSO agent will log on remotely to the host and check in the Registry database the list of users with a session open on the host. This allows updating the firewall's table of authenticated users.
Consider as disconnected 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	This option allows deleting authenticated used 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	This option allows managing changes to the IP addresses of user workstations and authenticating users who have logged on to hosts that have several IP addresses.

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.
Go to the list of temporary accounts	This shortcut 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 off the user. This duration is to be defined in minutes, hours or days. It is set by default to 240 minutes, or 4 hours.

"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 2 possible choices. • **Standard rule**: an authentication wizard will appear when this 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** The User object to select to match the *Guest* method is "All". **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 line before the line just above it.
Move down	Places the selected line after the line 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.

Multi-user objects	Defines one or several network objects authorized to allow several authentications on the same IP address. Click on "Add an object" and select from the drop-down list a host, network, IP address range or a group. **NOTE** The SSO method does not allow "**multi user**" authentication. Please refer to the last section **Transparent or explicit HTTP proxy and multi-user objects**.

Interactive features

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: User authentication

Select the user or group concerned or leave the default value at "All". This step is not offered for rules associated with the "**Guest**" or "**Sponsorship**" methods.

Step 2: Authentication 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 3: Authentication methods

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

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

The “Block” entry can also be selected. It will as such block any authentication attempt on traffic affected by the rule.

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 new rule, double-click on the status “**Disabled**”.

Default method	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.

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 start of the rule.

Multi-user objects

This table allows selecting network objects that enable several authentications from the same IP address. This allows, for example, accessing applications and data 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.

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).

As these options are not supported in Internet Explorer versions 6, 7 and 8, you are advised to use a higher version of this browser. Nonetheless, this mode may be disabled via command line in the CLI (CONFIG AUTH HTTPS sslparanoiac=0 / CONFIG AUTH ACTIVATE).

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

This table allows associating an authentication profile (profile of the captive portal) defined earlier with an interface on the firewall. It is possible to **Add** or **Delete** a match rule by clicking on the corresponding buttons.

Interactive features

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

- Add,
- Remove.

Interface	Select the network interface with which a profile of the captive portal must be associated. This can be an Ethernet interface (in, out ...), a modem or an IPSec interface.
Profile	Select the profile to be associated with the network interface. If the **Enable captive portal** checkbox was not selected in the chosen profile, the name of the profile will follow the icon
Default method or directory	The authentication method or the directory associated with the selected profile will automatically appear.

SSL server

Certificate (private key)	By default, the CA that the firewall's authentication module uses is the firewall's own CA, and the name associated with this CA is the product's serial number. Thus, when a user attempts to contact the firewall other than by its serial number, it will receive a warning message indicating incoherence between what the user is trying to contact and the certificate it is receiving. By clicking on the icon , the CA configuration screen will appear (server certificate) and you can select a CA that was imported earlier. 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 certificate 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, please refer to the section **Welcome > User awareness**, under *Initial connection to the appliance*.

Conditions of use for Internet access

Conditions of use for internet access can be displayed for the user. He will need to select the checkbox indicating his agreement to the terms before being able to authenticate.

This option can be enabled in the "Available methods" tab (**Guest** method) or "Captive portal profiles" tab (other methods). You can customize these conditions by entering, for example, the name of your company.

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.

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)	This option makes it possible to hide the Stormshield Network banner (this is the Stormshield logo by default) when the user authenticates on the captive portal, for confidentiality reasons.

Select a logo to display (800x50 px)	You can select the image that will appear 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 portal's graphics.

The "**Reset**" button allows you to go back to the original versions of the visual identity (logo and style sheet) and the default *Conditions of use for internet access*.

"Captive portal profiles" tab

This window allows you to select a predefined or customizable authentication profile and to modify its configuration.

Possible actions

Rename	This button makes it possible to rename the selected profile.
Enable sponsorship	If this option is selected, you can enable 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 by default.

Scroll over the icon to display the date and time of the last modification made to the profile of the selected captive portal.

Authentication

Default method or directory	This field allows selecting the authentication method or LDAP directory (in the case of a firewall that has defined several directories) assigned by default to the authentication profile currently being modified. The methods offered are those defined in the *Available methods* tab.
Enable sponsorship	If this option is selected, you can enable 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 by default.

Conditions of use for Internet access

Enable the display of the conditions of use for Internet access	Through this option, *Conditions of use for Internet access*, also known as a *Disclaimer*, can be shown to the user. The user must indicate his agreement to the terms by selecting the relevant checkbox before being able to authenticate. These conditions can be customized in the "Captive portal" tab.

NOTE

This option to display the Conditions of use for internet access 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	This display frequency concerns all authentication methods expect Guest method (see the *Available methods* tab).

Customized fields on the captive portal

When Guest mode is selected, three numbered fields become available. They allow adding up to three input zones 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, in minutes or in hours (up to 24 hours).
Maximum duration	Maximum duration for which the user can be authenticated, in minutes or in hours (up to 24 hours).
For transparent authentication	For SPNEGO and SSL certificates, this means 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	By selecting this option, you will enable the **Authentication** module and allow authentication via a web form from the network interfaces associated with the authentication profile.

Enable logoff page	By selecting this option, you will be enabling 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	By selecting this option, you will allow the publication of the .pac file for users logging on 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. By enabling this option, his multiple requests will automatically be denied.

Expiry of the HTTP cookie

Managing cookies for user authentication on the firewalls allows securing authentication by preventing replay attacks for example, given that the connection cookie is necessary in order to be considered authenticated.

Cookies are indispensable for allowing several users to authenticate from the same IP address. These IP addresses have to be entered in the list of **Multi-user objects** (*Authentication policy* tab).

NOTE

This option affects all methods except the SSO agent, which does not support multi-user authentication.

The web browser negotiates cookies, therefore if authentication is carried out with Internet Explorer, it will not be effective with Firefox or other web browsers.

At the end of the authentication period	The HTTP cookie expires by default **At the end of the authentication period**, meaning that it is negotiated only once throughout the whole duration of the authentication.
When a session is shut down	The cookie will be negotiated every time a request is sent to your web browser.
Do not use (not recommended)	It is possible to function without using the HTTP cookie, but this option is not recommended as it compromises the security of the 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 in the form of 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	By selecting this option, users will not be able to change their authentication passwords on the Stormshield Network Firewall.
Users can change their passwords	By selecting this option, users will be able to change their authentication passwords from the authentication portal, at any time with no restrictions on validity.

Users must change their passwords	By selecting this option, users will need to change their authentication passwords on the Stormshield Network Firewall on their first connection to the Firewall's authentication portal, and then for each time the password expires. This duration is specified in days without a specific time. The field **Lifetime (days)** appears below, allowing you to indicate the number of days the password will remain valid. **NOTE** If the user password is valid for 1 day and that the password was initialized for the first time at 2.00 p.m. on 25 November 2010, the password has to be changed from 12.00 midnight on 26 November 2010 and not 24 hours later.

User enrolment

Stormshield Network offers web-based user enrolment. If the user attempting to connect does not exist in the user database, he may request the creation of his account via web enrolment.

For certificate requests (CSR) by the user, they will be signed by the certificate authority (CA) chosen by default in the menu Certificates and PKI.

Do not allow user enrolment	If this option is selected, no "unknown" users will be able to register or create accounts with the LDAP directory.
Allow web enrolment for users	A user account has to be created in order for this option to be functional. If this option is selected, any user who attempts to connect and who does not exist in the user database will be able to request the creation of his account by filling in a web form. The administrator will then be able to confirm or deny his request.
Allow web enrolment for users and create their certificates	If this option is selected, users will not only be able to request the creation of their accounts if they do not exist in the user database, but they will also be able to request the creation of a certificate.

Notification of a new enrolment

This option allows new enrolled users to be informed of the creation of their accounts in the user database.

Do not send any e-mail	By default, the drop-down list will show that no e-mails will be sent to the administrator to inform him of enrolment requests. You can also define a group of users to whom enrolment requests will be sent in the menu **Notifications\E-mail alerts** *Recipients* tab. Once this group has been created, it will automatically be included in the drop-down list and will be able to receive requests if you select it.

Transparent or explicit HTTP proxy and multi-user objects

Multi-user objects

The list of networks of options allows several authentications from the same IP address (see the option **Multi-user objects**). This allows, for example, accessing applications and data from a remote computer (TSE server) applying filtering by user. 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

Multi-user objects have been made possible thanks to the *Cookie mode*; in which authentication information is saved in a *cookie* by the browser during the first connection to each new queried website. This information is forwarded in requests that follow to be intercepted by the firewall, which will then be able to apply its policy.

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. Using Stormshield Network Realtime Monitor, check the use of this object in the *User* module and delete the authentication of any authenticated users by right-clicking on them – action "Delete user from ASQ".

Transparent proxy (implicit)

The transparent or implicit proxy allows filtering user requests without any configuration on the client workstation (no proxy declaration in the browser). As such, the firewall's proxy will 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. The use of this mode provides the benefits of all the features but nonetheless 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, offered 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 allows setting 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 HTTP block page* tab: page that appears during an attempt to access a website that has not been allowed by the filter rules.

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.

"HTTP block page" tab

This window presents by default the HTTP block page that is displayed during an attempt to access a site that has been blocked by URL filter rules. 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. 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 these 4 block pages can be configured in the drop-down menu **Modify**. The entries are:

Modify	Allows customizing the HTTP block page by modifying the HTML code. Clicking on this button opens up **two dedicated tabs** below the block window. These tabs allow the use of a **simplified editor** or an **HTML editor**, covered in detail in the following section.
Rename	Allows customizing the name of the current block page.
Reset	Allows resetting to the default data of the block page.
Copy to	Allows copying the settings of the current block page and applying this model 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 chosen language, it is possible to customize the message displayed when the website is blocked, as well as a notification e-mail to the administrator to request a categorization or unblocking of access to the blocked website.

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

There are variables that allow making 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**

Simplified editor

Simplified editing uses a WYSIWYG interface and allows importing an image.

Actions on the table

Add	Creates a new version of the HTML page. By clicking on this button, a new line appears, allowing you to indicate the language and the other information to display.
Delete	Deletes an existing version. Select the line to be deleted and click on this button.
Modify image	This button allows customizing the block page by importing an image. Only JPG, GIF and PNG formats are accepted.
Default language	This field selects the version of the page to display, in the event the browser does not have a specified default language or if the language specified in the browser is not one of the languages of the page.

The table

Each line corresponds to a language of the HTML page message and a version of the e-mail notification to the administrator (request to unblock access).

Language ID	Language of the message to be displayed by the HTML page. This field has to be a two-character identifier of a valid country (ISO 3166-1 alpha-2) so that the browser can detect it.
Page title	Title displayed in the browser's window or tab
Block message	Clicking on the cell opens an editing window: a text box allows entering the version of the block page's message. This field allows entering HTML tags to format the text.
Contact e-mail	Clicking on the cell opens an editing window: the name of an e-mail link can be entered at the end of the message. If this field is empty, no e-mails will appear on the page. The preview field allows you to see the e-mail that will be sent if a mail client has been installed on the host. The information to enter is the e-mail address of one or two recipients, the subject of the e-mail and the message. A box will show the variables that can be used.

HTML editor

The text box allows copying all the HTML code of the block page in order to modify it. Code from a customized HTML page can also be pasted.

Images embedded in the HTML page have to be encoded in base64 and contained in the image tag.

This code embeds various versions of the page's message and information about the e-mail notification.

CERTIFICATES AND PKI

PKI or *Public Key Infrastructure* is a cryptographic system (based on asymmetric cryptography). It uses signature mechanisms and certifies public keys (by associating a key to a user) which allow encrypting and signing messages as well as traffic in order to ensure confidentiality, authentication, integrity and non-repudiation.

The Stormshield Network PKI allows generating and issuing certificate authorities (CAs) as well as certificates. These contain a key pair associated with information that may belong to a user, a server, etc. The aim of Stormshield Network's PKI is to authenticate these elements.

When the SSL VPN feature is used, the CA (certificate authority) "SSL VPN-full-default-authority" includes a server certificate "openvpnserver" and a user certificate "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 3 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 and certificates.
- On the right, details regarding the certificate authority selected beforehand from the list on the left, as well as information regarding the CRL and the configuration of the CA or sub-CA.

Whenever you scroll over a certificate or a CA used in the firewall's configuration, the validity period of the item being scrolled over will appear in color in the following cases:

- Certificate expiring in fewer than 30 days (expiration date in orange),
- Certificate with a validity period in the future (start date in orange),
- Expired certificate (expiration date in red),
- Revoked certificate (end of validity period in red),
- CRL of a CA that has exceeded half of its lifetime or which will be reaching it in fewer than 5 days (expiration date in orange),
- CRL of an expired CA (expiration date in red),

Possible operations

Search bar

Enter the name of the particular certificate or CA you are looking for if it exists.

The search field will list all certificates and CAs with names that correspond to the keywords entered.

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 will offer you the following choices:

All	Represented by the icon , this option allows displaying all existing authorities and certificates in the list on the left.
Certificate authorities	Represented by the icon , this option allows displaying all existing authorities and sub-authorities in the list on the left.
User certificates	Represented by the icon , this option allows displaying only user certificates and the CA that they depend on.
Server certificates	Represented by the icon , this option allows displaying only server certificates and the CA that they depend on.
Smartcard certificates	Represented by the icon , this option allows displaying only Smartcard certificates and the CA that they depend on.

Add

The **Certificates and PKI** module window makes it possible to **Add** several types of authorities:

For each of them, a wizard will appear so that the authority's properties can be defined.

To find out which characters are allowed or prohibited in various fields, please refer to section Allowed names.

NOTE

You can now add CRLDPs (Certificate Revocation List Distribution Points) for CAs imported via the GUI.

Delete

This button relates to the left column. Select the item from the list of CAs, sub-CAs or certificates that you wish to remove and click on **Delete**.

Action

This button relates to the left column. Select a CA, sub-CA or certificate from the list and click on the **Action** button. The possible actions vary according to the type of object selected.

Actions on a CA or sub-CA

Create or renew a CRL	A CRL (Certificate Revocation List) is a list of certificate IDs that have been revoked or are no longer valid and are no longer trustworthy. The certificate authority signs this list in order to prevent it from being modified by unauthorized parties. This action allows creating or renewing a CRL for the selected CA or sub-CA. You need to enter the password that protects the authority, and then click on **Create or renew a CRL**.
Remove the CRL	This action allows deleting the CRL for the selected CA or sub-CA. **REMARK** This action is not available (grayed-out option) when the CA or sub-CA does not have a CRL.
Set as default	This action allows defining the certificate authority used by default on the Firewall.

Actions on a certificate

Delete private key	This action allows deleting a certificate's private key. When the certificate is used in the firewall's configuration, you will be asked to confirm the deletion. It will then be possible to: • Cancel the deletion (click on **Cancel**), • Display configuration elements in which the certificate is used (click on **Check certificate use**), • Confirm the deletion of the private key (click on **Confirm deletion**). **REMARK** This action is not available (grayed-out option) when the selected certificate does not have a private key.
LDAP publication	This action allows publishing a user's certificate in the LDAP directory. To do so, the e-mail address specified in the creation wizard for this certificate must be the same as the one used in the user's properties in the firewall directory. When the user has a private key, you will be asked to enter a password to protect this certificate and its private key in a directory. Next, confirm this password. A gauge will indicate the password's level of security: "Very weak", "Weak", "Moderate", "Good" or "Excellent". You are strongly advised to use a combination of uppercase and lowercase letters, numbers and special characters.

Download

This button allows you to download CAs, sub-CAs and certificates, by selecting them from the list on the left.

1. A window will open offering you the following options:

"**Open with – Browse**"

or

"**Save file**"

A certificate import wizard will then appear, if you have selected "Open with". It helps to copy certificates, list of trusted certificates and CRLs from your hard disk to the certificate library.

A certificate sent by a CA is a confirmation of your identity and contains information used in protecting your data and establishing secure network connections.

2. Click on **Next** and select the file to import.
3. Next, enter the password. Two options are available:
   - Enable increased protection for private keys. You will be asked to enter the private key each time an application uses it, if you enable this option.
   - Tag this key as exportable. This will allow you to transport your keys later.
4. Click on **Next**, and you will access the certificate library. Windows may automatically select the certificate library, or you can specify the location of the certificate.

   Two options are available:
   - Automatically select the certificate library according to the type of certificate.
   - Add all certificates to the following library: select the location by clicking on "**Browse**".
5. Click on **Next**, you will reach the end of the certificate import wizard which summarizes the parameters that you have configured.

6. Click **Finish**. A "Security warning" screen may appear and ask you to confirm the installation of your certificate (this will depend on your OS configuration).

The 'downloads' menu will also offer the export of a certificate revocation list (CRL) in PEM or DER format.

NOTE

Any issues encountered during this procedure are beyond Stormshield Network's competence.

Check usage

You can look for the features or modules that use the selected certificate.

Adding authorities and certificates

The **Add** button has a drop-down list offering 6 options that will enable the creation of an authority or a certificate, via a wizard.

Adding a root authority

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

You will need to define the properties of the authority you wish to add:

WARNING

This information cannot be modified after the creation of the authority is confirmed.

CN	Enter a name that would allow you to identify your root authority, limited to a maximum of 64 characters. This name may refer to an organization, a user, a server, a host, etc. **Example** Stormshield Network **NOTE** This field has to be entered in order to continue the configuration.
Identifier	Even though this field is not mandatory, you can indicate here a shortcut to your CN, which will come in handy for your command lines. **Example** If you had selected a first name and last name for your CN, the ID may indicate just the initials.

Select the parent CA (if necessary)

Selecting a parent authority involves first entering the authority's attributes in the fields below.

Parent CA	Even though a CA is made up of certificates, it can also involve sub-CAs that depend on it. A sub-CA can only be used after the identification of its "**Parent authority**" or CA.

Password for the parent CA	Define a password if you wish to indicate that you are indeed in charge of the parent CA.

Certificate authority attributes

During this step, you will need to enter general information regarding the authority that you wish to implement. The information entered will be found in your CA's certificate and in your users' certificates.

NOTE

For sub-CAs, these data are already pre-entered. And unless you modify the configuration, not all of this information can be modified later.

Organization (O)	Name of your company (e.g.: COMPANY).
Organizational Unit (OU)	"Branch" of your company (e.g.: INTERNAL).
Locality (L)	City in which your company is located (e.g.: Villeneuve d'Ascq).
State or province (ST)	State or province in which your company is located (e.g.: Nord).
Country (C)	Select from the list the country in which your company is located (e.g.: France).

Click on **Next**.

Next, you will need to secure access to your authority.

In this step of the PKI configuration wizard, you will need to enter a password that will allow you to protect your certificate authority's private key.

WARNING

You are advised against choosing passwords that are too easy. We recommend that you mix uppercase and lowercase letters with numbers and special characters.

Certificate authority password

Password (min. 8 char)	Enter a password of at least 8 characters in order to protect access to your CA. **WARNING** The firewall will not save this password. If you forget your password, you will need to reinitialize the PKI and as such, you will lose the configuration parameters that you had defined for it.
Confirm password	Type your password again in this field in order to confirm it.
Mandatory 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.

E-mail address

Entering your e-mail address in this field will allow you to receive a message confirming that your authority has been created.

Key size (bits)

When you create a CA, you need to select the size of the key that the firewall will generate in order to allow traffic encryption. The larger the key, the more secure it is.

4 key sizes (in bits) are available:

1024	If you select this key size, the password generated for your authority will be 1024 bits. **NOTE** This number corresponds to 1024 characters visible in the console on your workstation.
1536	If you select this key size, the password generated for your authority will be 1536 bits.
2048	If you select this key size, the password generated for your authority will be 2048 bits.
4096	If you select this key size, the password for your authority should not exceed 4096 bits. **WARNING** Even though large keys are more effective, you are advised against using this key with entry-level appliances as this will mean the key will take a long time to be generated.

NOTE

The computation of big keys may slow down your Stormshield Network appliance.

Validity (days)

This field corresponds to the number of days for which your certificate authority and consequently 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 modified later.

NOTE

The value of this field must not exceed 3650 days.

Click on **Next**.

In this step of the wizard, you will need to enter the configuration regarding the distribution of the CRL (*Certification Revocation List*). This information will be embedded in the generated CAs and will allow applications that use the certificate to automatically retrieve the CRL in order to check the certificate's validity.

You can now manage your certificate revocations in the table that appears on the screen and enter the URLs that act as distribution points for revoked (invalid) certificates.

Add	When you click on this button, a new line will appear allowing you to enter a URL as a distribution point for certificate revocation lists. The first URL you enter will be numbered "1" and so on for the URLs that follow. The firewall will process items in the CRL according to their order of appearance on the screen.
Delete	Select the line to delete and click on this button to remove it from the list.
Move up	Move your URL up one line in the order of priority in the table by clicking on this button. Repeat this operation until your URL reaches the number you wish to assign to it.
Move down	Bring down your URL one or several places in the list using this button.

The following window sets out a summary of the information in your certificate.

Click **Finish**.

You will now see in the left column of the **Certificates and PKI** screen the CA that you have just created, represented by the icon (which represents the default CA).

By clicking on the relevant CA, detailed information about it will be displayed on the right side of the screen in 3 tabs:

"Details" tab

This tab contains 4 sections setting out data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer**" and its "**Fingerprint**" (information about the CA and its version).

"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).

The maximum lifetime of certificates has been increased to ten years.

"Properties" tab

This tab presents the **Key size (bits)**, the **Validity (days)** and the **Encryption algorithm** for the certification authority (including the **CRL validity (days)** for the CA, limited to a maximum of 3650 days), user certificates, Smartcard certificates and server certificates.

Adding a sub-CA

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.

The CA selected as a reference for the sub-CA will be the default CA, or the last CA selected before clicking on "**Add a sub-CA**".

You will need to enter a CN and an ID to begin with. Next, enter the password of the parent authority in the field "Password for the parent CA".

The icon allows you to view the password in plaintext to check that it is correct.

Click on **Next**.

The screen that follows will ask for the password of your CA and a confirmation.

You can also enter your **E-mail address**, **Key size (in bits)**, as well as the duration of your sub-CA's **Validity (in days)**.

You will then see a summary of the information entered.

NOTE

To view your sub-CA in the list to the left, expand the parent CA to which it is attached.

Click **Finish**.

By clicking on the relevant sub-CA, detailed information about it will be displayed on the right side of the screen in 3 tabs:

"Details" tab

These 4 sections will contain the same data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer**" and its "**Fingerprint**" (information about the product and its version).

"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).

"Properties" tab

This tab presents the **Key size (bits)** and the **Validity (days)** for the certification authority (including the **CRL validity (days)** for the CA, limited to a maximum of 3650 days), user certificates, Smartcard certificates and server certificates.

Adding a user certificate

In the configuration wizard, the administrator will specify information relating to the user for whom he wishes to create a certificate, by entering the user's e-mail address.

Once the certificate has been generated and published by the administrator, the user will receive a confirmation e-mail that his certificate has been created and will be able to use it for logging on (if the e-mail sending option has been enabled).

NOTE

The user certificate also depends on a parent CA, and will therefore select the default CA. Click on the button **Add a user certificate**.

Name (CN) (mandatory)	Enter your user's name, limited to a maximum of 64 characters. **NOTE** This field has to be entered in order to continue the configuration.
Identifier	Even though this field is not mandatory, you can indicate here a shortcut to your CN, which will come in handy for your command lines. **Example** If you had selected a first name and last name for your CN, the ID may indicate just the initials.
E-mail address (mandatory)	In this field, enter the e-mail address of the user for whom you wish to create a certificate.

Next, you will need to specify various options for your user certificate.

The field "**Validity**" is set by default to 365 days, and the field **Key size** to 2048 bits.

NOTE

To view your certificate created in the list to the left, expand the parent CA to which it is attached.

Publication in LDAP directory

You can choose to associate the user certificate with your LDAP database by selecting the option "**Publish this certificate in the LDAP directory**".

If this option is selected, the certificate can be directly linked to its user if this user exists in the LDAP database and consequently make the **Authentication** process easier.

For this, the e-mail address specified during the creation of the user certificate in the wizard has to be the same as the address used in the user profile in the firewall's user database.

Password of the published PKCS#12 container (min. 8 char)	The PKCS#12 container is a file format that allows storing the private key and the user certificate as well as the CA's certificate. Enter a password in order to protect the data for the 3 items mentioned above.
Confirm password	Type your password again in this field in order to confirm it.
Mandatory 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.

Click **Next**.

The following windows set out the information about the pre-selected parent CA as well as a summary of the data in the user certificate.

Click **Finish**.

By clicking on the relevant certificate, detailed information about it will be displayed on the right side of the screen in a single tab:

"Details" tab

These 4 sections will contain the same data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer**" and its "**Fingerprint**" (information about the product and its version).

Adding a Smartcard certificate

The Smartcard certificate is linked to a *Microsoft Windows* account associated with a user and a certificate. It allows signing and issuing certificates that allow the authentication of registered users in the Active Directory (see document on **Directory configuration (LDAP)\Connection to a Microsoft Active Directory),** and also in your LDAP database.

NOTE

Each user will be assigned a Windows account. Consequently, each user is assigned a Smartcard certificate. The CA used must have defined CRLDPs.

Name (CN) (mandatory)	Enter a name for the Smartcard certificate, limited to a maximum of 64 characters.
Identifier	Even though this field is not mandatory, you can indicate here a shortcut to your CN, which will come in handy for your command lines. **Example** If you had selected a first name and last name for your CN, the ID may indicate just the initials.
E-mail address (mandatory)	In this field, enter the e-mail address of the user for whom you wish to create a certificate.
Main user name (Windows)	Enter the name of the owner of the Windows account for whom you wish to create a Smartcard certificate.

Proceed in the same way as for adding a user certificate:

Specify the various options for your Smartcard certificate. The field "**Validity**" is set by default to 365 days, and the field **Key size** to 1024 bits.

You can then "**Publish this certificate in the LDAP directory**" by selecting the relevant option, and define a password that you will confirm for the PKCS#12 container.

After having clicked on **Next**, select a parent CA for your certificate and enter its password. You will see a summary of the data that was entered.

Click **Finish**.

By clicking on the relevant certificate, detailed information about it will be displayed on the right side of the screen in a single tab:

"Details" tab

These 4 sections will contain the same data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer**" and its "**Fingerprint**" (information about the product and its version).

Adding a server certificate

The server certificate is installed on a web server and allows providing a link between them.

In the case of a website, it allows checking that the URL and its DN (domain name) belong to the stated company.

Define the properties of the server certificate through the wizard.

Fully Qualified Domain Name (FQDN)	The FQDN represents the full name of a host in a URL, such as HOST (e.g. *www*) and a domain name (such as *company.com*). **Example** www.company.com
Identifier	Even though this field is not mandatory, you can indicate here a shortcut to your CN, which will come in handy for your command lines. **Example** Stormshield Network (owner of the FQDN)

Proceed in the same way as for adding a user certificate or a Smartcard certificate:

Specify the various options for your server certificate. The field "**Validity**" is set by default to 365 days, and the field **Key size** to 2048 bits.

You can then "**Publish this certificate in the LDAP directory**" by selecting the relevant option, and define a password that you will confirm for the PKCS#12 container.

After having clicked on **Next**, select a parent CA for your certificate and enter its password. You will see a summary of the data that was entered.

Click **Finish**.

By clicking on the relevant certificate, detailed information about it will be displayed on the right side of the screen in a single tab:

"Details" tab

These 4 sections will contain the same data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer**" and its "**Fingerprint**" (information about the product and its version).

Importing a file

By clicking on this button, you can import a file (containing your certificate) through the configuration wizard.

This will save you the hassle of having to go through the steps of creating the CA, sub-CA or certificates.

File to import

By clicking on the icon , to the right of the field, you will be able to browser your computer or your web browser to look for a certificate (if you have created one earlier).

File format

3 file formats are suggested:

- **Base64 format** (**PEM** - Privacy-enhanced Electronic Mail), It allows encoding X509 certificates in Base64. A PEM-type certificate may look like this:

-----BEGIN CERTIFICATE-----
MIIDdzCCAuCgAwIBAgIBBzANBgkqhkiG9w0BAQQFADCBpDELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAkdFMQ8wDQYD
VQQHEwZHZW5IdmExHTAbBgNVBAoTFFVuaXZlcnNpdHkgb2YgR2VuZXZhMSQwIgYDVQQLExtVTkIHRSBDZXJ0aWZpY
2FOZSBBdXRob3JpdHkxETAPBgNVBAMTCFVuaUdIIENBMR8wHQYJKoZIhvcNAQkBFhB1bmluZWNhQHVuaWdlLmNoMB
4XDTk5MTAwNDE2MjI1N1oXDTAwMTAwMzE2MjI1N1owgbExCzAJBgNVBAYTAkNIMQswCQYDVQQIEwJHRTEPMA0GA1
UEBxMGR2VuZXZhMR0wGwYDVQQKExRVbmI2ZXJzaXR5IG9mIEdlbmV2YTEeMBwGA1UECxMVRGI2aXNpb24gSW5mb
3JtYXRpcXVlMRowGAYDVQQDExFBbGFpbiBldWdlbnRvYmxlcjEpMCcGCSqGSIb3DQEJARYaQWxhaW4uSHVnZW50b2J
sZXJAdW5pZ2UuY2gwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALIL5oX/FR9ioQHMOaXxfDELkhPKkw8jc6l7BtSY
Jk4sfqvQYqvOMt1uugQGkyIuGhP2djLj6Ju4+KyKKQVvDJIu/R1zFX1kkqOPt/A2pCLkisuH7nDsMbWbepOhDTVNELoKVoVIA
azwWMFIno2JuHJgUcs5hWskg/azqI4d9zy5AgMBAAGjgakwgaYwJQYDVR0RBB4wHIEaQWxhaW4uSHVnZW50b2JsZXJAd
W5pZ2UuY2gwDAYDVR0TAQ0BAUwAwIBADBcBglghkgBhvhCAQ0ETxZNVU5JR0VDQSBjbGIIbnQgY2VydGlmaWNhdGUsI
HNIZSBodHRwOi8vdW5pZ2VjYS51bmInZS5jaCBmb3IgbW9yZSBpbmZvcm1hdGIvbnMwEQYJYIZIAYb4QgEBBAQDAgSwM
A0GCSqGSIb3DQEBBAUAA4GBACQ9Eo67A3UUa6QBBNJYbGhC7zSjXiWySvj6k4az2UqTOCT9mCNnmPR5I3Kxr1GpWT
oH68LvA30inskP9rkZAksPyaZzjT7aL//phV3ViJfreGbVs5tiT/cmigwFLeUWFRvNyT9VUPUov9hGVbCc9x+v05uY7t3UMeZejj
8
zHHM+
-----END CERTIFICATE----

The markers "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" frame the block of lines (the number of which is variable), each being 64 characters-long [A-Za-z0-9/+].
It is a format which is often transmitted by e-mail because this format is resistant to distortions caused by mail software.

The PEM file is a text file which contains this type of information.
Likewise, a CRL file type contains chains of coded characters in Base64 framed by markers like "-----BEGIN X509 CRL-----" and "-----END X509 CRL-----".
As for the private key file, it contains character strings encoded in Base64 framed by markers like: "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----".

- **Binary format** (**DER** - Distinguished Encoding Rules), containing the user's certificate in binary format.
- **Container** (**PKCS#12**), containing the private key and the user certificate as well as the CA's certificate. Furthermore, it is encrypted.

File password (if PKCS#12)

Define a password for the PKCS#12 file, if this is the format you have chosen (the same as for publishing the user certificate in the LDAP).

The icon allows you to view the password in plaintext to check that it is correct.

Items to import

Given that each file format contains different items, you can choose to import a file or part of it through the following choices.
All: Imports all items contained in your files.

Or select only the following:
Certificate(s) Private key (s) CRL Certification authority (CA) Request(s)

Overwrite existing content in the PKI

If you select this option, contents similar to the items above will be overwritten in the PKI, in favor of new certificates/private keys/CAs and requests.

Click **Next**. You will see a summary of the data regarding the import of your file (its name, format and items to import).

Click on **Finish**.

CLI CONSOLE

This module will allow you to view executable commands on your appliance's CLI (Command Line Interface) console.

You can access it from the menu **System** > **CLI**.

This module consists of two sections:

- the list of commands in the upper part of the window, which is a text zone
- a data entry zone at the bottom of the window

To obtain the full executable commands, refer to the guide **CLI Serverd Commands reference Guide** available in your secure area, under the section *Documentation*.

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

The window displays by default the 16 main executable commands that are part of the "HELP" category.

NOTE

By entering the "HELP" command in the data entry zone that we will see later, the list that summarizes the main commands will appear again.

The following are the visible commands:

AUTH	Used with the aim of avoiding spoofing, this command allows the user or the administrator to authenticate in total security.
CHPWD	Allows redefining the password if necessary.
CONFIG	Allows accessing the firewall's configuration features, which group 38 implicit commands (ACTIVATE CONFIG, ANTISPAM CONFIG etc., cf "Data entry zone").
GLOBALADMIN	Allows obtaining information about the system and consists of two implicit commands: GETINFOS and GETSTATUS.
HA:	Allows accessing high availability features, grouping 8 commands.
HELP	This command, as indicated earlier, allows displaying the list of main executable commands.
LIST	Displays the list of connected users, by showing user privileges (by level) and privileges for the session in progress (SessionLevel).
LOG	Allows viewing the Stormshield Network multifunction firewall's activity logs, groups 6 commands.
MODIFY	This command is a specific privilege that allows the user to modify the configuration of a module, in addition to reading privileges.
MONITOR	Allows accessing features relating to MONITOR, contains 20 commands.
NOP	Does not perform any action and while preventing the server from logging off.
PKI	Allows displaying or downloading the PKI, groups 7 commands.
QUIT	Allows logging off.
SYSTEM	Groups 20 commands relating to the system.
USER	Groups 12 commands relating to the user.
VERSION	Allows displaying the version of the server.

Data entry zone

When you go to the **CLI** module, the area in which commands are entered is the main focus.

To the right of it, there are two buttons and a checkbox, which allow modifying certain actions:

Launch	This button allows launching the command that was entered manually. The command will also be launched when the user presses "Enter". **NOTE** In the field for editing commands, you can browse through the various commands that have already been launched, using the Up/Down buttons. Command history is stored and re-used each time the web application is launched.
Clear display	This button allows erasing the list of commands displayed above it (cf. "List of commands"). To view them again, enter the HELP command in the data entry zone and click on "Launch".
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 becomes available only when multiline mode has been enabled. If this option is selected, the command sequence will be interrupted as soon as the first error is found.
Raw format	If this option is selected, the launch of the command will display the line of code in its raw form between markers.

NOTE

Most commands displayed in the list at the top of the page involve others. To view all these commands, proceed as follows:

1. Enter the command of your choice in the text entry zone.
2. Click on "Launch".
3. Depending on the command you have selected, the list will display the additional commands included in it.

Example

If you enter the CONFIG command, all commands relating to it will appear on the screen.

To use one of these commands, enter "CONFIG" in the data entry zone, followed by a space and the desired command, such as: "CONFIG HA".

CONFIGURATION

The configuration-administration screen consists of 3 tabs:

- *General configuration*: definition of the firewall's settings (name, language, keyboard), date and time settings and NTP servers.
- *Firewall administration*: configuration of access to the firewall's administration interface (listening port, SSH etc.)
- *Network settings*: Ipv6 activation, configuration of the proxy server and DNS resolution.

"General configuration" tab

The **General configuration** tab allows the following parameters to be modified:

General configuration

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

Firewall name	This name is used in alarm e-mails sent to the administrator and is displayed in the firewall's main window. It can also be used as the DNS name of the captive portal if it has been enabled and the option "Use firewall name or certificate CN as FQDN" has been selected. The maximum supported length of the firewall name is 127 characters.
Firewall language (logs)	Choice of language, between **French** and **English**. This language is used for logs, syslog and the CLI configuration.
Keyboard (console)	Type of keyboard that the firewall supports. 5 layouts are available: **English**, **French**, **Italian**, **Polish** and **Swiss**.

Cryptographic settings

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

Enable "ANSSI Diffusion Restreinte (DR)" mode	The **Enable "ANSSI Diffusion Restreinte (DR)" mode** option forces the firewall to abide by the ANSSI's (French national information security agency) guidelines on the use of coprocessors and cryptographic accelerators on products for which qualification is sought. It is an imperative on networks that fall under the "Restricted" classification. This mode relies in particular on the use of software versions for asymmetrical and symmetrical cryptographic algorithms and random key generation algorithms. As for symmetrical cryptographic 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 3.9.1, the following will occur: • IPSec: the module will check whether the firewall is using version 2 of the IKE protocol. If this is not the case, a warning will appear, prompting the administrator to change the IPSec configuration. • IPSec: the module will check whether the encryption algorithms used belong to DH19 and DH20 groups (ECP 256 and ECP384). If this is not the case, a warning will appear, prompting the administrator to change the IPSec configuration. • IPSec: the module will check whether the encryption algorithm used is AES_GCM_16 (associated by default with SHA256 authentication). • On firewalls equipped with Intel processors, the "ANSSI Diffusion Restreinte (DR)" mode will impose 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. Do note as well that the firewall must be rebooted in order to enable the "ANSSI Diffusion Restreinte (DR)" mode.

Password policy

The indicated parameters will apply to all passwords and pre-shred keys defined on the firewall (VPN PPTP, IPSec VPN, internal LDAP directory, etc.). The parameters are:

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…)

NOTE

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

Date/Time settings

Date	Firewall's date. Select the date from the calendar. This field will be grayed out if NTP configuration has been enabled.
Time	Firewall's time. This field will be grayed out if NTP configuration has been enabled.
Synchronize with your machine	By clicking on this button, the firewall will synchronize its time with your computer's time. This field will be grayed out if NTP configuration has been enabled.
Time zone	Time zone defined for the firewall (GMT by default). **WARNING** The firewall has to be restarted if the time zone is changed.
Synchronize firewall time (NTP)	NTP (Network Time Protocol) is a protocol that allows synchronizing the local clock on your computers with a time reference via your network. If this option is selected, your firewall will automatically be synchronized with the local time.

NOTE

The date and time to which your Stormshield Network firewall is set are important: – they allow you to locate events in the log files. They are also useful in the scheduling of configurations.

List of NTP servers

This table will only be accessible if you have selected the option **Synchronize firewall time (NTP).** If you have not done so, the list of NTP servers will be grayed out.

NTP servers (host or group-address range) (max 15)	The NTP server represents the remote clock with which your firewall will be synchronized. You can **Add** or **Delete** servers by clicking on the relevant buttons. When you click on **Add**, a new line will be added to the list of NTP servers. You may select an object from the drop-down list or create one by clicking on . It will then be possible to create a host, an IP address range or a group. Click on **Apply** after you have entered the data for the new object.
Password (ASCII)	Even though this is optional, you can enter a password for your NTP server which you can use for authentication.

Hardware

The option for monitoring hardware activity **Watchdog** is available on all physical **"S" model firewalls in the U Series**.

Other Firewalls in the **U Series** can benefit from this tool, which can improve diagnoses and help. This mechanism is implemented by default but has to be enabled via the BIOS system. Please refer to the technical support department's Knowledge Base for the full procedure.

Hardware monitoring timeout (watchdog)	This device tests the activity of the firewall's system. 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.

Industrial firewalls only (SNi40 models)

In order to ensure service continuity in an industrial setting, the SNi40 firewall is equipped with a hardware bypass function, which when enabled, allows making network traffic pass through without being scanned.

NOTE

This mechanism can only be enabled on the first two interfaces of the firewall.

Two of the firewall's operating modes are offered:

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

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

- **SystemOff** bypass: it will be activated when the appliance 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 has been 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 systematically reject them.

When bypass is activated, the first two interfaces of the firewall 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
Resetting 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.

Advanced properties

Redirect to the captive portal	This option allows choosing 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 **NOTE** 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 has been specified in this field. • Use the captive portal's certificate **NOTE** 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 is only accessible when the "Specify a domain name (FQDN)" value has been selected in the **Redirect to the captive portal** field.

"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. It can connect without using certificates. This option has to be selected if you wish to keep this privileged access. **WARNING** This account is to be considered "dangerous", in view of the extent of its configuration possibilities and the access privileges granted to it.
Listening port	This field represents the port on which you can access the administration interface (https, tcp/443 by default). **NOTE** You can create an additional listening port by clicking on . **WARNING** The object can only be a "TCP" object (not "UDP").
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.
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 If this option is selected, you will prevent such attacks and enable the configuration of the two fields that follow, in order to restrict connection attempts.

Number of authentication attempts allowed	Maximum number of connection attempts before blocking the user (login/password error or case sensitivity, for example). By default, the number of attempts allowed is limited to 3.
Freeze time (minutes)	Duration for which you will not be able to log on the firewall after the number of failed attempts specified above. The duration of the freeze may not exceed 60 minutes.

Access to firewall administration pages

Add a server	Select a server from the drop-down list of objects. This server 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 for the firewall's web administration interface, which will then appear in a frame located above the login and password fields. 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

Enable SSH access	SSH (Secure Shell) is a protocol that allows logging on to a remote host via a secure link. Data from host to host are encrypted. SSH also allows the execution of commands on a remote server. Select this option if you wish to connect remotely and securely in console mode. **NOTE** By selecting this option, you will enable the configuration of the two fields below it.
Enable password access	The password in question corresponds to the password for the “admin” account, as it is the only account that is able to connect in SSH. The “admin” will need to enter it in order to access the firewall via a remote host. You may also use a private/public key pair to authenticate.
Listening port	This field represents the port on which you will be able to access the administration interface (ssh tcp/22 by default). **NOTE** You can create an additional listening port by clicking on . **WARNING** The object can only be a “TCP” object (not “UDP”).

"Network settings" tab

IPv6 support

Enable IPv6 support on this Firewall	Enables support for IPv6 on the firewall. To find out which modules support IPv6 and what changes have been made to the various modules in the administration interface, please refer to the section **Enabling IPv6** in this guide. **WARNING** 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

The firewall uses a proxy to access the Internet	Select this option to enable the fields below it and to allow the firewall to use an HTTP proxy in order to access the Internet securely. This field is used by ActiveUpdate and LicenceUpdate.
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.
Identifier	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	Clicking on this button will add a new line to the table and will allow you to select a DNS server from the drop-down list.
Delete	Select the line to be removed from the table and click on **Delete**.
Move up	Moves the selected line above the previous line.
Move down	Moves the selected line below the next line.

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).

CONFIGURATION OF 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.

Configuration of interfaces and QoS queues 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 the Ethernet interfaces 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.

DASHBOARD

The dashboard provides an overview of the information concerning your firewall. It is represented by this icon and is divided into 2 sections:

- The module configuration menu on the left, containing 6 collapsible tabs that can be personalized according to your needs: *Configuration, Network objects, Users and groups, Audit logs, Reports* and *Monitoring.* A search bar is available for these 6 modules.
- A dynamic area at the center, containing 13 modules or widgets:
  - Network
  - Alarms
  - Resources
  - License
  - Hardware
  - Properties
  - New applications
  - Active Update
  - Services
  - Interfaces
  - High availability
  - Sandboxing
  - Stormshield Management Center

By default, each one of these windows is updated dynamically. The most recent components are downloaded automatically and are displayed on the screen.

The module configuration menu

This retractable column (button) is divided into 4 collapsible sections. They will allow you to personalize your interface and configure your modules.

My favorites

This section only appears when at least one module has been added to the list of favorites. It is closely linked to the “pin” icon: .

When you come across this icon at the top right of each module, select it if you want it to be added to your favorites.

Configuration

This section is presented as a tree of menus and their modules, replaced with a keyword search bar.

9 sub-menus are available (click on them to expand):

- Dashboard
- System (containing 8 modules: Configuration, Administrators, License, Maintenance, Active Update, High availability, Management Center, CLI console)
- Network (containing 7 modules: Interfaces, Virtual interfaces, Routing, Multicast routing, Dynamic DNS, DHCP, DNS cache proxy)
- Objects (containing 3 modules: Network objects, Web objects, Certificates and PKI)
- Users (containing 6 modules: Users, Temporary accounts, Access privileges, Authentication, Enrollment, Directory configuration)
- Security policy (containing 6 modules: Filtering and NAT, URL filtering, SSL filtering, SMTP filtering, Quality of service, Implicit rules)
- Application protection (containing 7 modules: Applications and Protections, Protocols, Inspection profiles, Vulnerability manager, Host reputation, Antivirus, Antispam)
- VPN (containing 4 modules: IPSec VPN, SSL VPN, SSL VPN portal, PPTP server)
- Notifications (containing 7 modules: Logs - Syslog - IPFIX, SNMP agent, E-mail alerts, System events, Block messages, Report configuration, Monitoring configuration)

NOTE

If certain modules are grayed out, this means that you have not subscribed to the required license and therefore cannot access them.

This can also mean that the connected user does not have the necessary privileges for accessing these menus

The icon » allows personalizing the display of your directory:

This provides a partial view of your directory, displaying only the menus.

This provides a full view of your directory, displaying the menus and their modules.

The dynamic area: widgets

In this area, you will be able to view certain updates on your firewall such as the latest alarms raised or the expiry dates of your licenses.

13 windows are shown, each with a toolbar at the top right corner, including the full dashboard module.

The possible actions that can be performed with these tools are:

Enlarge	Represented by the icon , this tool allows adding a column to the dashboard module and enlarging the window for widgets.
Reduce	Represented by the icon , this tool allows deleting a column from the dashboard module and minimizing the window for widgets.
Close	Represented by the icon , this tool allows closing your widget.
Refresh	Represented by the icon , this tool allows you to refresh the data on the dashboard or the widget concerned.
Open	Represented by the icon , this tool opens the module associated with the widget you are browsing and as such, closes the dashboard.

Dashboard configuration	Represented by the icon , this tool allows you to select the **Components** you wish to display on the dashboard, through a series of checkboxes. You can also configure the **Update frequency** of the widgets: "Manual only" (you will need to click on the "Refresh" ( ) icon systematically) , "Every minute" or "Every 5 minutes".
Add to favorites	Represented by the icon , this tool allows you to add the Dashboard module to "**My favorites**" in the directory on the left (see section The module configuration menu).

Network

This window displays the model of your Stormshield Network multifunction firewall as well as the number of interfaces available on it (32 maximum).

The interface(s) used appear(s) in green. When the bypass mechanism is enabled (industrial firewalls only) and has been activated, the first two interfaces of the firewall will be represented as follows:

A tooltip containing information about each interface is available.

The following information is given:

Name	Name of the interface used ("in", "out" or "dmz"), accompanied by its IP address 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
xx mode activated	This value is only available for industrial firewalls and is only shown when bypass has been enabled and the "Safety" operating mode has been selected. The possible values are "Safety mode enabled" (bypass not activated) or "Bypass mode enabled" (bypass activated).

Alarms

This window contains the list of the last 50 alarms raised by the firewall.

Date	Date and time of the last alarms raised, arranged from the most recent to least recent.
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".
Priority	3 levels of priority are possible and can be configured in the module Application Protection > Applications and Protections.
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 **Full access to logs** and refreshing the data in the widget.
Destination	Address of the intended destination before the alarm was raised.

Message	Comment associated with the selected alarm. **Examples of possible messages** "Invalid ICMP message (no TCP/UDPlinked entry)" (minor priority). "IP address spoofing (type=1)" (major priority).

When the row of the alarm is selected, the following buttons will appear:

Configure	This button shows the alarms in the **Applications and Protections** module. The *Advanced* column in the selected row will offer the *Modify* button, which allows sending an e-mail when an alarm is raised, quarantining the host that caused the alarm to be raised or capturing the blocked packet.
Online help	Select the desired alarm and click on this link, which will take you to a help page relating to the message (see above).

This section of the dashboard will contain a button allowing you to "Clear screen", or delete information logs.

Resources

This window provides a graphic view of hardware resources relating to your firewall.

Space used	Percentage of space used for the firewall's logs.
CPU	Percentage of your processor's use.
Temperature	Temperature of your appliance. This information is not available on virtual machines.
Memory	Memory used by your appliance: **Host**: percentage of memory allocated by hosts (bytes). **Fragmented**: percentage of memory allocated by fragments (or folders that are too big and fragmented – in bytes). **Connection**: percentage of memory allocated for various connections (bytes). **ICMP**: percentage of memory allocated for ICMP (bytes). **Logs**: percentage of memory used for DataTracking. **Dynamic**: memory in which a computer puts its data while they are processed.

NOTE

The graph that used to display the dynamic memory consumed now displays the highest value between the dynamic memory and memory allocated to processes. This explains why the value is higher than those of earlier versions.

License

The widget offers a view of Licenses of warranty and options by expiry date.

Those options are : Update (firmware), Contextual protection signatures, Vulnerability Manager, ClamAV Antivirus, Kaspersky Antivirus, Stormshield Network URL databases, Extended Web Control URL databases, Antispam DNS blacklists (RBL), Antispam: heuristic engine, License expiry.

Hardware

This window sets out the various hardware data of your appliance.

USB key	Presence or absence of a USB key on the system (secure configuration for the module **System > Maintenance**).
SD Card	Presence or absence of an SD card for storing logs that would allow reports and monitoring curves to be generated.
3G/4G modem	Presence or absence of a 3G/4G modem.
Operating mode	On industrial firewalls, indicate the mode selected for hardware bypass (for further information on how bypass works, please refer to the section *General configuration tab* in the **Configuration** module. The value of this field may be one of the following: "Security", "Safety", "Bypass" (the bypass mechanism is activated" or "Not detected" (default value for non-industrial firewalls). When the mouse is rolled over this row, details of the bypass status will be displayed (SystemOff, JustOn, RunTime, RunTimeWatchdogTimer).
Internal disk	Status of the internal disk. An alarm will appear if the disk is defective. Scrolling over this row with a mouse will display the list of tests performed and their results.
Removable disk	Status of the removable disk if the firewall has one. An alarm will appear if the disk is defective. Scrolling over this row with a mouse will display the list of tests performed and their results.
RAID	Status of the RAID (redundant set of independent or low-value hard disks) and of its disks, if the option is available on the hardware. An alarm will appear if a disk is defective or missing.
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).

Properties

This window shows the data essential to the configuration of your firewall.

Warning

This box shows available update version and warnings that the administration interface has raised concerning the firewall's configuration.

Update Available	This entry indicates whether a new version of the firmware is available. If this is the case, a link bearing the name of the available version will allow the user to download it. To install it, go to the **Maintenance** module, *System update* tab.
Release Notes	When a new firmware version is available, this link will enable the user to download the version release notes applicable to the firmware version offered for download.

EVA

This box appears only on Elastic Virtual Appliance (EVA) models.

Model	This entry specifies whether it is an EVA firewall with a standard license or a firewall with a Pay As You Go license model.
Model being used	This entry specifies the virtual machine model applied (EVA1, EVA2, EVA3, EVA4 or EVAU).
Limits applied	This entry specifies the amount of memory and the number of virtual processors (vCPU) currently allocated to the EVA.
Maximum limits	This entry specifies the amount of memory and the maximum number of virtual processors (vCPU) that can be allocated to this EVA model.

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 in order to identify the owner of the EVA.

Properties

Serial number	Your Stormshield Network Firewall's reference.
Date	Date and time in real time.
Backup partition	Absence or presence of a backup partition on your system (cf Menu **System**>**Maintenance** module >*Configuration* tab).
Uptime	Duration for which the firewall has been running uninterrupted.
Stormshield Network Activity Reports	Status of report generation.

Policy

Filtering	Profile applied for the filter and NAT policy. A "Collapse/Expand" button has been added for filter rules.
VPN	Status of the VPN on your network.

Dynamic DNS

Status of the dynamic DNS client.

New applications

This component shows the new signatures installed on the appliance via Active Update that allow raising Applications alarms.

Services

Services	List of the various services available on the appliance.
Uptime	Duration for which the service has been running uninterrupted.
Load	Status of the service.

Active Update

Name of the object	Name of the listed module.
Status	Whether the module is up to date.
Last update	Date and time of the last update.

Interfaces

Name of the object	Name of the in, out or dmz interface.
Type	This may be a physical interface (ethernet), VLAN, or modem (dialup)
Address	IP address and subnet mask of the interface.
Incoming throughput	Incoming traffic in KB.
Outgoing throughput	Outgoing traffic in KB.

Disabled interfaces are displayed in the **Dashboard**.

High availability

Status	Indicates whether high availability has been enabled, and if this is not the case, whether it has been reinitialized.
Configuration	Indicates whether both firewalls in the cluster have a synchronized configuration.
Last synchronization	Date on which the configuration was last synchronized.
Last switch	Date on which both members of the cluster changed statuses (active/passive)
Serial number	Shows the serial numbers of both members of the cluster.
Status	Indicates the status of each member of the cluster (**Active** or **Passive**)
License	Specifies the type of high availability license of each member of the cluster (e.g.: **Master**).
Quality	Indicates the quality of the link between members of the cluster.
Version	Firmware version of each member of the cluster.

Additional information can be displayed such as **Authentication certificate not defined** when both firewalls in the cluster do not present the same certificate.

Stormshield Management Center

If you have installed the Stormshield Management Center centralized administration server, this panel will allow you to display the characteristics of the firewall's connection to the SMC server.

IMPORTANT

If you have logged on via the web administration interface to a firewall attached to an SMC server, "**Managed by SMC - Emergency mode**" 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 attached to an SMC server may be overwritten when a new configuration is sent from the SMC server.

Status of the service	Indicates the status of the connection between the firewall and the SMC server.
IP address	IP address of the SMC server.
Logged on/ Logged off since	Specifies the time/date from which the firewall has been logged on to or logged off from the SMC server.
Last deployment number	Indicates the number of the last deployment carried out by the SMC server on the firewall.
Last configuration update	Indicates the last date on which the configuration was sent from the SMC server to the firewall.

Sandboxing

If your firewall has the sandboxing option, this panel will allow you to show the status of the connection to the service as well as the latest scan statistics.

Status of the service	Indicates the status of the connection between the firewall and the Stormshield sandboxing servers. The various possible values are: • Connected: the firewall has a Sandboxing license and the analysis infrastructure in the cloud is contactable. • Unreachable: the firewall has a Sandboxing license but the analysis infrastructure in the cloud is uncontactable. • Restricted access: the firewall has a sandboxing license, the analysis infrastructure in the cloud is contactable, the quota for the number of files that the firewall can send has not been exceeded, but a rather large number of submitted files has been analyzed with a low priority. • Connected, submitted file quota exceeded: the firewall has a sandboxing license, the analysis infrastructure in the cloud is contactable, but the quota for the number of files that the firewall can send has recently been exceeded. Files beyond this quota will be analyzed with a low priority. • Connected, submitted file quota unknown: the firewall has a sandboxing license, the analysis infrastructure in the cloud is contactable, but the quota for the number of files that the firewall can send cannot be determined. • Restricted access, submitted file quota exceeded: the firewall has a sandboxing license, the analysis infrastructure in the cloud is contactable, the quota for the number of files that the firewall can send has recently been exceeded, and a rather large number of submitted files has been analyzed with a low priority. • Restricted access, submitted file quota unknown: the firewall has a sandboxing license, the analysis infrastructure in the cloud is contactable, the quota for the number of files that can be sent cannot be determined, and a rather large number of submitted files has been analyzed with a low priority.
Criticality of the last malicious file detected	This indicator will only be displayed when a file scanned by sandboxing has been deemed malicious. It will then be presented in the form of a score ranging from the detection threshold of a malicious file (set by default to 80) to 100.
Nature of the last malicious file detected	This indicator will only be displayed when a file scanned by sandboxing has been deemed malicious. In this case, it will set out the nature of the malware (e.g.: "variant of Win32/SNS.Test").
Last malicious file detected on	This indicator will only be displayed when a file scanned by sandboxing has been deemed malicious. In this case, it will set out the date and time the malware was detected (format: YYYY-MM-DD HH:MM:SS).

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

	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.

Main window

This module contains the list of the various directories configured on the firewall.

It is divided into 2 distinct zones:

- The list of directories and action buttons (left column).
- Tabs setting out the configuration and structure of the selected directory.

"Add a directory" button

Clicking on this button will launch the wizard to create a new LDAP directory.

"Action" list

When this list is expanded, it is possible to **Delete** a directory, **Set as default**, **Check connection** to a directory or **Check usage** of a directory in the firewall's 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	Confirmation of the LDAP administration password that you have just entered in the previous field.
Mandatory 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.

NOTE

Only the password 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 starting 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.
Username	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	Confirmation of the LDAP administration password that you have just entered in the previous field.
Mandatory 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.

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 enabling the identification of the internal LDAP directory when several directories have been 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 has to 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 of a DN** The 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).

Username	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. **NOTE** 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.

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 starting 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 had entered in the previous page.
Port	This field contains the listening port that you had 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
Username	The login name allowing the firewall to connect to your LDAP server.
Password	The password created in the firewall for connecting to the LDAP server.

Secure connection (SSL)

Enable SSL access	This option allows checking 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 against a Certification Authority	During a connection to the LDAP database, the firewall will check that the certificate has been issued by the Certification Authority specified below.
Certificate authority	This option allows selecting the CA which will be used for verifying the server certificate issued by the LDAP server, in order to ensure the authenticity of the connection to this server. Click on the magnifying glass icon ( ) to search for the corresponding CA. **NOTE** This option will be grayed out by default if the previous option **Check that the name of the server matches the FQDN in the SSL certificate** was not selected.

Advanced properties

Backup server	This field allows defining a replacement server in the event the main server cannot be contacted. You can select it from the list of objects suggested in the drop-down list.
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 in order to verify a user's privileges with the LDAP server when the user authenticates. Otherwise, the firewall will use the user's account to perform this verification.

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 you 3 choices of LDAP servers, which you will apply to define your attributes:

- OpenLDAP: LDAP server.
- Microsoft Active Directory (AD): LDAP directory services for Windows operating systems.
- Open Directory: directory of websites under license of 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) have to store the user's password in the form of a hash (result of a hash function applied to the password) which will avoid having to store the password in plaintext.

You have to select your desired hash method from the following:

SHA	"Secure Hash Algorithm". This encryption method allows establishing 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 checking the integrity of data entered, by generating a 128-bit MD5 key. **REMARK** 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 you are strongly advised to use it.
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** Configuring this field is not absolutely necessary but in this case, in order for the SSL authentication method to work the CA has to be specified in the list of trusted CAs in the configuration of the SSL method. (See menu **Users\Authentication** module**Available methods** tab: the authentication method **Certificate (SSL)** has to be added and the CA indicated in the right column "Certificate 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 enabling the identification of the internal LDAP directory when several directories have been 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 has to 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 of a DN** 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.
Username	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. **NOTE** The key icon ( ) allows you to view the password in plaintext to check that it is correct.

REMARK

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 starting 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 had entered in the previous page.
Port	This field contains the listening port that you had 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
Username	The login name allowing the firewall to connect to your LDAP server.
Password	The password created in the firewall for connecting to the LDAP server.

Secure connection (SSL)

Enable SSL access	This option allows checking 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 against a Certification Authority	During a connection to the LDAP database, the firewall will check that the certificate has been issued by the Certification Authority specified below.
Certificate authority	This option allows selecting the CA which will be used for verifying the server certificate issued by the LDAP server, in order to ensure the authenticity of the connection to this server. Click on the magnifying glass icon ( ) to search for the corresponding CA. **NOTE** This option will be grayed out by default if the previous option **Check that the name of the server matches the FQDN in the SSL certificate** was not selected.

Advanced properties

Backup server	This field allows defining a replacement server in the event 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**.
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 in order to verify a user's privileges with the LDAP server when the user authenticates. Otherwise, the firewall will use the user's account to perform this verification.

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 match 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 match 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 you 3 choices of LDAP servers, which you will apply to define your attributes:

- OpenLDAP: LDAP server.
- Microsoft Active Directory (AD): LDAP directory services for Windows operating systems.
- Open Directory: directory of websites under license of Open Directory

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) have to store the user's password in the form of a hash (result of a hash function applied to the password) which will avoid having to store the password in plaintext.

You have to select your desired hash method from the following:

SHA	"Secure Hash Algorithm". This encryption method allows establishing 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 checking the integrity of data entered, by generating a 128-bit MD5 key. **REMARK** 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 you are strongly advised to use it.

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** Configuring this field is not absolutely necessary but in this case, in order for the SSL authentication method to work the CA has to be specified in the list of trusted CAs in the configuration of the SSL method. (See menu **Users\Authentication** module**Available methods** tab: the authentication method **Certificate (SSL)** has to be added and the CA indicated in the right column "Certificate authorities (C.A)")

Click on **Apply** to confirm your configuration.

Connecting to a Microsoft Active Directory

Like the internal and external directories, Active Directory offers the same user management features that have been 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 enabling the identification of the internal LDAP directory when several directories have been 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 has to 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 of a DN** AD domain is "company.com" so my Root domain (Base DN) should be "dc=company,dc=com"
Identifier	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. **NOTE** The key icon ( ) allows you to view the password in plaintext to check that it is correct.

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 starting 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 had entered in the previous page.
Port	This field contains the listening port that you had 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
Identifier	The login name allowing the firewall to connect to your LDAP server.
Password	The password created in the firewall for connecting to the LDAP server.

Secure connection (SSL)

Enable SSL access	This option allows checking 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 against a Certification Authority	During a connection to the LDAP database, the firewall will check that the certificate has been issued by the Certification Authority specified below.

Select a trusted Certificate Authority	This option allows selecting the CA which will be used for verifying the server certificate issued by the LDAP server, in order to ensure the authenticity of the connection to this server. Click on the magnifying glass icon ( ) to search for the corresponding CA. **NOTE** This option will be grayed out by default if the two options above were not selected.

Advanced properties

Backup server	This field allows defining a replacement server in the event the main server cannot be contacted. You can select it from the list of objects suggested in the drop-down list.
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 in order to verify a user's privileges with the LDAP server when the user authenticates. Otherwise, the firewall will use the user's account to perform this verification.

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 you 3 choices of LDAP servers, which you will apply 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) have to store the user's password in the form of a hash (result of a hash function applied to the password) which will avoid having to store the password in plaintext.

You have to select your desired hash method from the following:

SHA	"Secure Hash Algorithm". This encryption method allows establishing 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 checking the integrity of data entered, by generating a 128-bit MD5 key. **REMARK** 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 you are strongly advised to use it.
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** Configuring this field is not absolutely necessary but in this case, in order for the SSL authentication method to work the CA has to be specified in the list of trusted CAs in the configuration of the SSL method. (See menu **Users\Authentication** module**Available methods** tab: the authentication method **Certificate (SSL)** has to be added and the CA indicated in the right column "Certificate 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:

State	Double-clicking on this allows enabling or disabling the profile.
Overview	Indicates the domain name, interface and status of the resolution with regards to the 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

DNS resolution

Domain name (mandatory)	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. For 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. **NOTE** • 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 (mandatory)	DNS service provider. Currently, two DNS service providers are supported: **DynDNS** and **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. The object to specify in this field must be named: "members.dyndns.org" or “members.dyndns.com” in order to run with DynDNS.
Dynamic DNS service (mandatory)	This option allows you to indicate the service you have subscribed with the DNS service provider from among the following: "dynamic DNS", "custom", and "static DNS".

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. **REMARK** 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 and HTTP.
Notify the provider	This service, which **DynDNS** charges at a fee, enables redirecting traffic headed for your network to a specific page when your connection is inactive.
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.

E-MAIL ALERTS

The screen consists of three sections:

- Configuration tab: allows proceeding to the basic settings of module, such as SMTP server settings, e-mail sending frequency (in minutes), intrusion prevention alarms and system events.
- Recipients tab: allows defining groups that will be used in the mailing policies but also in other configuration modules in which e-mails need to be sent.
- Templates tab: allows viewing and modifying e-mail formats, used when sending notifications to users and administrators.

"Configuration" tab

This tab contains all the necessary parameters for configuring e-mail alerts.

It consists of the following elements:

Enable e-mail notifications

This option enables the configuration of alerts. If it is disabled, none of the configuration items will be accessible as the firewall will not send ay e-mails. This option is disabled by default.

REMARK

The e-mail notification feature requires a mail server that can receive e-mails from the firewall.

SMTP server

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".
E-mail address	Specifies the e-mail address of the sender and makes it possible to ensure compatibility with external SMTP services such as Microsoft Office 365. The sender's e-mail address suggested by default starts as follows: '<firewall_name>@'.
Authentication	A login and password can now be defined for sending e-mails via the firewall. This checkbox allows you to enable the authentication of the firewalls when sending e-mail alerts.
Identifier	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).
Testing the SMTP configuration	This button makes it possible to send a test e-mail to check the firewall's SMTP configuration. After having clicked on **Test the SMTP configuration**, enter the e-mail address of the recipient for the test e-mail in the window that opens, then click on Send.

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.

Intrusion prevention alarms

Here, you may select a group to notify of intrusion prevention alarms.

The list of alarms will be sent in the body of the e-mail to the specified group.

The frequency for sending alarm reports can be modified in the field "Sending frequency" in the menu **E-mail sending frequency (in minutes).**

Example

If you define a frequency of 15 minutes in the field Sending frequency, you will be informed by e-mail every 15 minutes of alarms that were raised on the firewall during this period.

Do not send any e-mails	No e-mails regarding alarms will be sent to a specific recipient. This option is selected by default, and used to enable e-mail notifications in order to approve certificate requests, for example, without necessarily generating e-mails for alarms.
Send according to alarm and event settings	Only intrusion prevention and system event alarms for which the **Send an e-mail** checkbox has been selected will activate the sending of an e-mail.
Send only major alarms	If this option is selected, the group selected in the next field will receive major alarms, which will act as a configured e-mail notification (**Applications and Protections** module / *Advanced* column).
Message recipient	Selection of the group that will receive major intrusion prevention alarms.
Send major and minor alarms	If this option is selected, the group selected in the next field will receive major and minor intrusion prevention alarms, which will act as a configured e-mail notification (**Applications and Protections** module / *Advanced* column).
Message recipient	Selection of the group that will receive major and minor intrusion prevention alarms.

System events

Like the previous field, a group can also be notified of system events.

The frequency for sending system events can be modified, likewise, in the field **Sending frequency** in the menu **E-mail sending frequency (in minutes)**.

Do not send any e-mails	No e-mails regarding system events will be sent to a specific recipient. This option is selected by default, and used to enable e-mail notifications in order to approve certificate requests, for example, without necessarily generating e-mails for system events.
Send only major alarms	If this option is selected, the group selected in the next field will receive major system events, which will act as a configured e-mail notification (**Applications and Protections** module / *Advanced* column).
Message recipient	Selection of the group that will receive major system events.

Send major and minor alarms	If this option is selected, the group selected in the next field will receive major and minor system events, which will act as a configured e-mail notification (**Applications and Protections** module / *Advanced* column).
Message recipient	Selection of the group that will receive major and minor system events.

REMARK

The status of system events can be viewed in a module of the same name: In the menu, go to **Notifications>System events**.

"Recipients" tab

This screen consists of 2 views:

- Recipient groups
- Select a group

Each group contains a certain number of e-mail addresses

Up to 50 groups can be created.

There are no pre-configured groups. You may add new groups and comments, and delete groups.

Each group must contain at least one e-mail address. There is no restriction to the number of e-mail addresses in a group.

Next, you will be able to select a group to which detailed or simplified vulnerability reports can be sent, in the menu **Application protection** > **Vulnerability manager.**

Creating a group

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

1 Click on the button **New recipient group**. A new line will appear in the list and you will be asked to enter the name that you wish to give the group.

2 You can add comments regarding this group, by filling in the field in "Comments" column.

To add a recipient, go to the selected group. Its name will appear on the right in the field **Recipients of group**: **<groupname>.** Next, click on **Add new recipient to group**. A screen will appear, allowing you to indicate either the recipient's e-mail address or the user or the group he belongs to if it exists in the object database. Any e-mail address can be entered, but the format of the address will be checked.

Deleting a group

1 Select the line to delete.

2 Click on the button Remove. The message "Delete the group <group name>?" will appear. By clicking on "Yes", the group will be deleted from the list.

REMARK

Groups can be deleted only if the group is not being used in another configuration on the firewall.

If you wish to delete a group that is active in another module, a pop-up window will appear with the following options: force deletion, check where the group is being used, or cancel.

Check use

The **Check use** button allows checking if a group of e-mail is used in the different modules of the firewall's configuration.

1. Select the line to check.
2. Click on the button **Check use** in order to check.

"Templates" tab

This section allows you to use a customized message for sending out e-mails. Six templates are available, each of them containing a body that differs according to the message that you wish to send out.

Editing the 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 keywords which will later be replaced with values. For example, a keyword may automatically display the user's name.

To modify contents, click on the button **Edit**.

The screen will be split into two parts:

- Top: preview of the e-mail template
- Bottom: Editing window

2 buttons allows you to modify the message's body:

Insert a variable	This button allows you to select variables that will later be replaced with real values when the message is sent.
Apply default template	Allows resetting the template to its initial presentation. When you click on this button, the following message will appear: *"Reset the contents of this template to its default values?"*

Vulnerability manager

- Vulnerability detection (detailed): detailed vulnerability report template, applied by default.
- Vulnerability detection (summary): simple vulnerability report template, applied by default.

Certificate request

- Accept the certificate request: e-mail template specifying that the certificate request has been approved by the administrator.
- Reject the certificate request: e-mail template specifying that the certificate request has been rejected by the administrator.

User enrollment

- Accept the user request: e-mail template specifying that the enrolment request has been approved by the administrator.
- Reject the user request: e-mail template specifying that the enrolment request has been rejected by the administrator.

List of variables

E-mail templates dedicated to vulnerability detection:

- Mail subject ($Title)
- Subtitle ($SubTitle)
- Message summary ($MailSummary)
- Vulnerability summary ($VulnsSummary)
- Affected hosts ($HostsByVuln)
- Vulnerable applications ($VulnsByProduct)
- Message footer ($Footer)

E-mail templates used for certificate requests and user enrolment requests.

- User's last name ($LastName)
- User's first name ($FirstName)
- Date of the enrolment request ($Date)
- User ID ($UID)
- URL for downloading the certificate ($URL)

Example of a report received by e-mail regarding alarms

Type	Minor
Action	Block
Date	2010-10-11 15:08:32
Interface	dmz2
Protocol	tcp
Source	10.2.18.5:55987 (ed:ephemeral_fw_tcp)
Destination	66.249.92.104:80 (www.google.com)
Description	SQL injection prevention: suspicious instruction OR in the URL

ENROLMENT

Stormshield Network's 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.

The **Enrolment** module consists of 3 zones:

- The table containing user enrolment requests and certificate requests on the left
- Information relating to the user or to the selected certificate on the right
- Advanced properties

The enrolment table

Possible operations

Validate	When a user sends an enrolment or a certificate request, the request will appear in this table. To validate a user's request, go to the relevant line and click on **Validate**. **NOTE** If a user submits an enrolment request with a certificate request, the validation of the user request implies the validation of the certificate as well (checkboxes selected simultaneously).
Reject	You can also reject users' requests for enrolment or for certificates by selecting the corresponding line and clicking on **Reject**.
Ignore	This button allows you to cancel an approval or a rejection. This avoids having to use the **Cancel** button and erasing operations in progress.
Refresh	This button allows refreshing the list of enrolment and certificate requests. As such, recent requests will be added automatically to the table pending approval or rejection.

User enrolment and certificate requests

Type	This column indicates the type of request the user has created: an enrolment request is represented by "**User**" while certificate requests are represented by "**Certificate**".
CN User	Name that allows identifying the user or the certificate.
E-mail address	E-mail address of the user, which will allow him to receive an approval or a rejection of his enrolment or certificate request.

Summary

Information regarding the selected user/certificate is displayed here.

Identifier	User's login
Name	User's last name
First name	User's first name
E-mail address	User's e-mail address, which will be useful for sending him a response regarding his enrolment or certificate request.

Description	Description of the user
Telephone number	User's telephone number
Password	User's password
Certificate request	Indicates whether the user requested a certificate during his enrolment request.

NOTE

For certificate requests, only the e-mail address will appear in the field on the right.

Advanced properties

User identifier format for empty ID fields

Identifier format	Define a default character string for connection IDs. **NOTE** The format is written in the form: **%F.%L** The variables that define the identifier are: **F** being the first name, **L** being the last name. The variable **f** changes the case of the value to lowercase and **F** changes it to uppercase. Likewise for **l** and **L**. The form **f1** makes it possible to select only the first character. **example**: for the values *Firstname* and *Lastname*, **%f1.%l** will produce **f.lastname**
Example	Illustrated example of a user ID. **Example:** JOHN.SMITH

NOTE

The desired number of characters for the first name and/or last name can be defined by indicating the number after the F and/or the L.

%F1%L

JSMITH

E-mails

Send an e-mail to the user:

when approving/rejecting user's enrolment request

This option allows sending an e-mail to the user to inform him that his enrolment request has been approved or rejected.

when approving/rejecting user's certificate request

This option allows sending 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 manipulate **Filter** policies and **NAT** policies.

Selecting the filter policy

The drop-down menu offers 10 pre-configured filter policies, number from 1 to 10:

"Block all (1)"	By default, this filter policy is enabled in the factory settings. Only ports corresponding to the administration of the appliance will be open (1300/TCP and 443/TCP). Pinging all the interfaces of the appliances is also allowed. All other connections will then be blocked. **REMARK** 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 administer 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, to the extent that the protocol can be automatically detected by the threat prevention engine: 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. **REMARK** All outgoing TCP connections that cannot be scanned (for which no protocol can be recognized) will be accepted.
"Low (4)"	A protocol scan will be forced for outgoing connections. **REMARK** All outgoing connections that cannot be scanned will be allowed.
"Filter 05, 06, 07, 08, 09"	Apart from the 5 pre-configured policies (**Block all, High, Medium, Low, Pass all**, which can be edited where necessary), there are 5 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 scans 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	Immediately activates the policy being edited. Parameters saved in this slot will overwrite current parameters in force and the policy will be applied immediately on the firewall. **WARNING** As Filter and NAT rules belong to the same policy, they will be enabled simultaneously.
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 of the filter policy and add comments. Once the operation has been performed, click on "Update". This operation can also be cancelled. • **Reinitialize**: 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. 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 a 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 creation and edition of 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.

REMARK

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 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.

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 **Check policy** 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 allows performing 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 allows creating 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 allows 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 will 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, and 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 allows enabling the explicit HTTP proxy and defining 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 policy on a firewall hosted in the cloud to be similar to a policy on physical appliance, 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.
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 ticking or unticking 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.

Explanations regarding symbols appearing in the configuration of filter rules

Mathematical comparison

Each time 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

Certain 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 matched 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 rebooted.

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 menu in the filter 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 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 allows decrypting the 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 sixth 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 **none** 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. **NOTE** This option is not available if you have selected the "Log" action in the previous field. **Verbose (filter log)**: If you select this option, a log from each connection matching the rule will be added to the filter logs. 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** of rule validity. 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 allow directing traffic that corresponds to 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 uncontactable 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 **Quality of service** module, in the **Security policy** menu.
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 its 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.

REMARK

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 allows protecting 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 connections per second allowed for the UDP protocol.
ICMP (c/s)	Maximum number of connections per second allowed for the ICMP 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 allowing differentiating services contained in a network architecture. 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 allows rewriting the packet with the given value, so that the next router will know the priority to apply to this packet.
New DSCP value	This field allows defining traffic differentiation. 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

Redirect

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 web 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 will generate a report. It will therefore be possible to obtain volume information on a desired traffic type.
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.

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 specifying a particular interface if "Any" has been selected as the source host.

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 applying 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.

Public IP address reputation

Select a reputation category

This field allows applying the filter rule to hosts whose public IP addresses have been classified in one of the predefined reputation categories:

- **anonymizer**: proxies, IPv4 to IPv6 converters.
- **botnet**: infected hosts running malicious programs.
- **malware**: hosts distributing malicious programs
- **phishing**: compromised mail servers.
- **scanner**: hosts that conduct port scanning or launch brute force attacks.
- **spam**: compromised mail servers.
- **tor exit node**: endpoint servers of the Tor network.
- **Bad**: groups all of the above categories.

> **NOTE**
> Since the reputation of a public IP address may border on two categories (botnet and malware), and this field only allows selecting one category, you are advised to use the "**bad**" group for optimum protection.

Other host categories are also available to facilitate the setup of filter rules for Microsoft Online solutions:

- **Exchange online**: servers that host the corporate mail application.
- **Microsoft Identity and authentication**: authentication servers used for accessing Microsoft Office 365.
- **Office 365**: servers that host the Microsoft Office 365 storage and office tools solution.
- **Office online**: servers that host the free online office tools solution Microsoft Office 365.
- **Sharepoint online**: servers that host the online collaborative solution Microsoft Sharepoint.
- **Skype Enterprise Online**: servers that host the professional version of the instant messaging solution Skype.
- **Microsoft**: groups all categories of machines that host Microsoft services online.

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 hosts.

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, 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 allows filtering according to the value of the DSCP field of the packet received.

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.

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 . Objects can be created or modified directly from this field by clicking on .

Click on **Ok** to confirm your configuration.

"Geolocation/Reputation" tab

Geolocation

Select a region	This field allows applying 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.

Public IP address reputation

Select a reputation category

This field allows applying the filter rule to destination hosts whose IP addresses have been classified in one of the predefined reputation categories:

- **anonymizer**: proxies, IPv4 to IPv6 converters.
- **botnet**: infected hosts running malicious programs.
- **malware**: hosts distributing malicious programs
- **phishing**: compromised mail servers.
- **scanner**: hosts that conduct port scanning or launch brute force attacks.
- **spam**: compromised mail servers.
- **tor exit node**: endpoint servers of the Tor network.
- **Bad**: groups all of the above categories.

NOTE
Since the reputation of a public IP address may border on two categories (botnet and malware), and this field only allows selecting one category, you are advised to use the "Bad" group for optimum protection.

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. Filtering by a packet's outgoing interface is possible.

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	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 type

Depending on the protocol type that you choose here, the following field that appears will vary:

Automatic protocol detection (default)	If this option is selected, a field with the same name will appear below with the following data: Application protocol: Based on default port or content IP protocol: All
Application protocol	The advantage of this choice is being able to apply an application analysis on a port other that the default port. If this option is selected, a field with the same name will ask you to choose: Application protocol: Select the desired protocol from the drop-down list. IP protocol: All
IP protocol	If this option is selected, the field will offer a drop-down list of the various IP protocols.

NOTE

The status of IP connections can be tracked for protocols other than TCP, UDP or ICMP.

Status tracking (stateful)	If you select "IP Protocol", a "stateful" option will be available. This option is selected by default for any IP protocol other than TCP, UDP, ICMP and IGMP.

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.

For the **translation of a selected destination**, an additional option is available:

Translated port

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

Inspection type

General

Inspection level

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**. **NOTE** 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. **NOTE** 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. **NOTE** Enabling this option requires the use of the Kaspersky antivirus. **NOTE** 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. **NOTE** 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**.
HTTP Cache	**On**/ **Off** buttons allow you to enable or disable the HTTP cache in your filter rule. This feature makes it possible to memorize all types of resources when visiting websites, so that they do not need to be downloaded again from the internet during new visits, even for different clients. However, this mode is recommended only for internet links with low bandwidth or for which access is restricted to a limited number of websites. This feature is available only for models equipped with a hard disk. **NOTE** This option only applies to HTTP and HTTPS traffic if SSL inspection has been enabled. The total amount of data that can be memorized is 100 MB on the disk and 1MB in RAM. The maximum size of a resource that can be memorized is 32 KB. The tracking of memorized resources and cache management can be viewed in Realtime Monitor (Dashboard).
URL filtering	To enable this filtering method, select a URL filter profile from the suggested profiles.
SMTP Filtering	To enable this filtering method, select an SMTP filter profile from the suggested profiles. **NOTE** 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, corresponding to 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 **Check policy** 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 allows performing 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 allows 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. • **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 allows restricting the application to a port or port group, and enabling 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. **NOTE** For an N-to-N bi-map rule, original and translated address ranges, networks or host groups have to 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 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 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.
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.

GENERAL NOTE:

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.

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.

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 menu in the NAT 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 traffic (before translation)

By clicking in the column "Source" a configuration window will appear:

Source before translation (original)

"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 allows clearing the user field and to no longer apply any criteria for 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.

Destination before translation (original)

"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.

Traffic after translation

Source after translation

"General" tab

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

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 type

Depending on the protocol type that you choose here, the following field that appears will vary:

Automatic protocol detection (default)	If this option is selected, a field with the same name will appear below with the following data: Application protocol: Based on default port or content IP protocol: All
Application protocol	The advantage of this choice is being able to apply an application analysis on a port other that the default port. If this option is selected, a field with the same name will ask you to choose: Application protocol: Select the desired protocol from the drop-down list. IP protocol: All
IP protocol	If this option is selected, the field will offer a drop-down list of the various IP protocols.

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 make it possible to break down your NAT rule and its characteristics.

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 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

To secure the connection between members of the cluster, you will need to define a pre-shared key.

This key will only be used by firewalls that are joining the cluster for the first time.

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.
Mandatory 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.

Communication between firewalls in the high availability cluster

Encrypt communication between firewalls	By default, communication between the firewalls is not encrypted, based on the principle that the link used by high availability is a dedicated link. In some architectures, the high availability link is not dedicated, and if you wish to prevent inter-cluster communications from being read, they can be encrypted (in AES, for example). **WARNINGS** 1. Selecting this option can degrade the performance of your high availability cluster. 2. Only connections, and not their contents, pass through the high availability link.

Click **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.

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 for linking both 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 in order to enable the fields below it and to define a secondary link for your cluster.
Secondary link	Secondary interface used for linking 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. Changing the link may indeed cause interruptions to communications between members of the cluster, which may lead to a nonoperational cluster.

Advanced properties

Modifying the pre-shared key between firewalls in the high availability cluster

New pre-shared key	This field allows modifying the pre-shared key or the password defined during the creation of the cluster.
Confirm	Confirm the password/pre-shared key that you have just entered in the previous field.
Mandatory 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.

Quality indicator

Active firewall if equal

This option allows favoring one firewall as the active firewall in the event both firewalls have the same quality.

The aim of favoring an active firewall is to keep as many logs as possible on the same firewall or to favor 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 and 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 this firewall as the active firewall and the second firewall will take over from it if it malfunctions or is unplugged. **WARNING** Selecting this option will cause the firewalls to swap immediately, or switch from this firewall as the active firewall, causing a disconnection from 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 considered. 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)	Reboot interfaces in a bridge during the swap If this option is enabled, interfaces on the bridge are reinitialized at the time of the switch in order to force switches connected to the firewall to renew their ARP tables.
Enable link aggregation when the firewall is passive	If this option is selected, you will be enabling link aggregation on the firewall even if it has become passive in 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 (switch, 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)	This field enables defining the frequency of ARP requests in seconds, to a maximum of 9999 seconds.

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 allows giving the interface a relative value. "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** It may be useful to 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. Version SSLv3 is disabled and the TLS versions enabled, according to the recommendations given by the French Network and Information Security Agency (ANSSI).

As these options are not supported in Internet Explorer versions 6, 7 and 8, you are advised to use a higher version of this browser. Nonetheless, this mode may be disabled via command line in the CLI (CONFIG AUTH HTTPS sslparanoiac=0 / CONFIG AUTH ACTIVATE).

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 2 sections:

- A static section
- A collapsible section: options

The information required depends on whether it is the administrator's first connection to the firewall.

User	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.** **REMARK** 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 username as well as for the password.

Additional Options

Language	Language of the web-based graphical 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. As such, you will be able to log onto the firewall without modification privileges using an account that ordinarily has such privileges. This allows the user to refrain from using modification privileges if they are not necessary.

REMARK

- Options are contained in a cookie. The user therefore stores his connection preferences on his browser.
- 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 be launched 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.

REMARK

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>".

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.

REMARK

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 Click on at the top right side of the interface. The window “Quit?” will appear with the following message: “**You are about to be disconnected** ". Click on **Quit** or on **Cancel** if you do not wish to log off.

2 By clicking on **Quit**, the interface will return to the connection window. Cancelling will return the user to the main screen, without any effect to the execution of the program.

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.

Rule table

The table contains the following columns:

On	Status of the rule: **Enabled/ Disabled:** Click on the field to enable/disable the creation of one or several implicit riles. The rule **Allow external (unprotected) interfaces (Authd_ext) to access the authentication portal and the SSL VPN** has been disabled by default.
Name	Name of the implicit rule: this name cannot be modified.

The following rules appear in the "**Name**" column:

- **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.
- **Block and reinitialize ident requests (port 113) for modem interfaces (dialup)**.
- **Block and reinitialize ident requests (port 113) for ethernet interfaces**.
- **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.
- **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 access to the PPTP server**: users can contact the firewall via PPTP to access the server, if it has been enabled.
- **Allow protected interfaces (serverd) to access the firewall's administration server (port 1300)**: administrators will be able to log on via their internal networks to port 1300 on the firewall. This service is used especially by Stormshield Network Real-Time Monitor.
- **Allow protected interfaces to access the firewall's SSH port**: allows opening access to the firewall via SSH in order to log on using command lines from a host located on the internal networks.

- **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 that allow securing data circulating over IP traffic.
- **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 menu **System**\ **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 the HTTPS port**: Connections relating to the setup of the SSL VPN tunnel are allowed on the HTTPS port.
- **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 queries 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).

WARNINGS

The following actions may be dangerous:

- **Disabling the "Serverd" rule**: in the absence of an explicit rule, may cause users to no longer have access to tools using port 1300, namely Stormshield Network RealTime Monitor, GlobalAdmin, Stormshield Network Centralized Management and Stormshield Network Event Analyzer.
- **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

The inspection profile module consists of 2 screens:

- A zone dedicated to the default configuration and a collapsible menu for advanced properties.
- A zone for associating application profiles, accessible by clicking on "**Go to profiles**".

Security inspection

Global configuration for each profile

Default configuration

Configuration for incoming traffic	Define the profile to apply for incoming traffic on the network via the Stormshield Network Firewall. Incoming traffic represents the traffic of an unprotected interface (such as the internet) to a protected interface (your local/internal network).
Configuration for outgoing traffic	Define the profile to apply for outgoing traffic on the network via the Stormshield Network Firewall. Outgoing traffic represents the traffic of a protected interface (such as the internet) to an unprotected interface.

New alarms

Apply the default model to new alarms	This option is related to the **Application protection\Alarms** module. By enabling it, new alarms will be updated automatically and will be issue with the Stormshield Network signature. The three options that follow will be grayed out if you have chosen an automatic configuration. If you wish to apply them yourself, unselect the option and define the parameters in the fields that follow.
Action	When an alarm is raised, the packet that set off the alarm will be subject to the action configured. You can choose to **Pass** or **Block** new alarms. You will notice the status you have applied to the **Application protection\Alarms** module. New alarms can be found in the column "**New**".
Level	Three alarm levels are available: **"Ignore", "Minor"** and **"Major"**.
Packet capture	By selecting this option, the packet that set off the alarm will be captured.

Advanced properties

Apply translation operations (NAT) before IPSec VPN	This option means that the IP addresses will be modified before the encryption performed by the IPSec VPN.

Treat IPSec interfaces as internal interfaces	If this option is selected, IPSec interfaces will become internal - and therefore protected - interfaces. All networks that are able to go through IPSec tunnels must therefore be legitimized and static routes allowing 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

This screen consists of 2 sections:

- A zone for editing various possible profile configurations
- A zone for associating protocol 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"**.

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.

IPSec VPN policies now allow editing their configurations in Global mode. To enable the option, select "Display global policies" in the Preferences module.

NOTE

There is no specific privilege for "vpn_global".

The IPSec VPN module consists of 4 tabs:

- *Encryption policy – Tunnels*: this tab allows creating your 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 allows configuring 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*: here, you can 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*: this tab allows listing your approved certificate authorities in the tunnels using PKI methods as well as the pre-shared keys (PSK) of your mobile tunnels in two tables.
- *Encryption profiles*: here, 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.

"Encryption policy – Tunnels" tab

From version 2 of the firmware onwards, Stormshield Network firewalls support IPSec tunnels based on IKEv1 or IKEv2 protocols.

Peers that use different versions of the IKE protocol can now be defined in the same IPSec policy.

Profile bar	The drop-down menu offers 10 IPSec profiles numbered from (1) 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 slot will overwrite current parameters in force.

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**: 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 creating a VPN tunnel between two network devices that support IPSec. This procedure is also called: *Gateway to Gateway VPN tunnel* or *Gateway to Gatewaytunnel*

Some How To's will guide you step by step in the configuration of a secure connection between your sites. Click on one of the the links to access to these How To's:

- IPSec VPN: Authentication by pre-shared key,
- IPSec VPN: Authentication by certificate,
- IPSec VPN: Hub and Spoke Configuration.

The Add button will be covered in the following section.

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 table 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	Cut the selected line in order to paste it.
Copy	Copy the selected line in order to duplicate it.
Paste	Duplicate the selected line after having copied it.

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.

Site to site tunnel

Here, you will define each of the endpoints for your tunnel as well as for your peer.

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 an IKEv1 peer	Define the parameters for your peer. Several steps are necessary: 1 Selecting the gateway:

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 .

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.

Click on **Next**.

2 Identifying the peer:

2 choices are possible, identification via **Certificate** or by **Pre-shared key** (PSK). Select the desired option.

1. 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 certificate authority can also be added.

2. 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, it is absolutely necessary to follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management.

Click on **Next**.

3 Finish creating the peer:

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.

Click on **Finish**.

Create an IKEv2 peer	The steps are the same as the ones in creating an IKEv1 peer.
Local network	Host, host group, network or network group that will be accessible via the IPSec VPN tunnel.
Remote network	Host, host group, network or network group accessible through the IPSec tunnel with the peer.

Star configuration

This procedure consists of directing several VPN tunnels to a single point. It allows, for example, linking agencies to a central site.

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.
Remote sites	Define the parameters for your remote sites: select your peer from the list of those already created or click on the icon » to create a new one and select the remote networks from the objects in the drop-down list. You can **Add** or **Delete** peers by clicking on the relevant buttons.
Treat IPSec interfaces as internal interfaces checkbox (applies to all tunnels).	If this option is selected, IPSec interfaces will become internal - and therefore protected - interfaces. All networks that are able to go through IPSec tunnels must therefore be legitimized and static routes allowing them to be contacted must be specified. 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. If you have selected this option by mistake in the IPSec VPN tunnel installation wizard, it can be disabled by unselecting **Treat IPSec interfaces as internal interfaces (applies to all tunnels - remote networks will need to be explicitly legitimized)** found in the *Advanced properties* panel in the **Application protection > Inspection profiles** module.
Create policies without encryption (none) for internal networks	This option allows automatically generating policies without encryption (none) dedicated to internal networks (*Network_internals* to *Network_internals*). If the policy already exists, a warning message will appear indicating that these policies have already been created.

Click on **Finish**.

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 treated in order of appearance on the screen.
State	This column shows the status **On**/**Off** of the tunnel. When you create tunnels, they are active by default. Click twice to disable them.
	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: • - Tunnel endpoints: local object / remote object • - Traffic endpoints: local object / destination object • Authentication: Mode / Type / Certificate / Pre-shared key • - Encryption profiles (phase 1 & 2): algorithms, Diffie Hellman group, lifetime This information can be selected, and can therefore be copied.

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.
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*.
Comments	Description given of the VPN policy.

The additional option **Keepalive** allows artificially maintaining 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.

This option is only valid for **site-to-site tunnels**. It can be enabled by selecting the value *Keepalive* in the *Columns* menu, which appears when you move the mouse over the header of the columns in the table.

Keepalive	To enable this option, assign a value other than 0, corresponding to the interval in seconds, between each UDP packet sent.

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.

Example: *[gateway policy at line 2] - Different IKE versions cannot be used in the same IPSec policy.*

Anonymous – 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").

Note that from version 3.8.0 onwards it is possible to build a nomad IPSec policy including several peers if those peers use the same IKE encryption profile. When authenticating with certificates, all peers'certificates must be issued from 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.

It is possible to define VPN client settings (Config mode) for mobile users through the *Config mode policy* creation wizard.

New Policy

This policy makes local networks accessible to authorized users via an IPSec tunnel. In this configuration, remote users log on with their own IP addresses.

Enter the details of the mobile peer to be used. Then add the accessible local resources to the list.

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 a **Modify** button, allowing you to enter the parameters of the IPSec Config mode, described in the section **The table**.

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 the button "**Add**" a "**New policy**" (VPN), then on "**Create a mobile peer**" via the mobile IPSec VPN policy wizard.
2. Name your mobile configuration, and click on **Next**.
3. 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 **Certificate authority** (CA) that signed your peer's certificate so that it is automatically added to the list of trusted authorities.
Hybrid	If you select this hybrid method, you will need to provide the **Certificate** (server) to be presented to the peer and probably its CA. The server is authenticated by certificate in Phase 1, and the client by XAuth immediately after Phase 1.
Certificate and XAuth (iPhone)	This option allows mobile users (roadwarriors) to connect to your company's VPN gateway via their mobile phones, using a certificate in Phase 1. The server is also authenticated by certificate during this Phase 1. Additional authentication of the client is carried out by XAuth after Phase 1. **NOTE** This is the only mode compatible with iPhones.
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 (monserver.domain.com), or e-mail address format (toto.dupont@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, it is absolutely necessary to follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management.

Click on **Next**.

4. Check the summary of you mobile configuration and click on Finish.
5. 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 table 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.

The table

Line	This column indicates the number of the line treated in order of appearance on the screen.
State	This column shows the status **On**/**Off** of the tunnel. When you create tunnels, they are active by default. Click twice to disable them.
	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: • - Tunnel endpoints: local object / remote object • - Traffic endpoints: local object / destination object • Authentication: Mode / Type / Certificate / Pre-shared key • - Encryption profiles (phase 1 & 2): algorithms, Diffie Hellman group, lifetime This information can be selected, and can therefore be copied.
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.
Encryption profile	This option allows selecting the protection model associated with your VPN policy, from the choice of 3 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 activate "Config mode", which is disabled by default. This allows distributing the traffic endpoint IP address to the peer **NOTES** 1. If you choose to activate 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** button allows entering the parameters of the IPSec Config mode:

DNS Server	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.
List of 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.

REMARK

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.

Example: *[gateway policy at line 2] - Different IKE versions cannot be used in the same IPSec policy.*

"Peers" tab

This tab consists of two sections:

- Left: the list of IPSec VPN and mobile IPSec VPN peers.
- Right: Information about the selected peer.

List of peers

Search in peers	This field allows performing searches on the name of the object and its various properties, by occurrence, letter or word.

Filter	3 choices are possible: You can view "**All peers**" in the lists, including gateways and mobile users. You can also choose to view only "**Gateways**" or only "**Mobile peers**".
Add	Peers can be added to this area. To do so, select the type of peer to create from the drop-down list: a "**New remote site**", a "**New IKEv2 remote site**", a "**New anonymous (mobile) peer**" or a "**New anonymous IKEv2 (mobile) peer**". You can also "**Copy from the selection**" – the copied peer will be duplicated. To do this, click on the peer to be copied and enter its new name in the window that appears.
Delete	Select the peer to be deleted from the list and click on **Delete**.
Rename	Select the peer from the list and click on Rename.
Name	Name given to the peer during the creation phase.

Peer information

"Gateway" peer

Comments	Description given of the local peer.
Remote address	Object selected to represent the remote IP address during the creation of the peer via the wizard.
Backup configuration	This field indicates whether you have defined a backup configuration during the creation of the peer. "None" will appear by default if you have not created any. However, you can define one by selecting it in the drop-down list containing your other remote peer.
IKE profile	This option allows selecting the protection model associated with Phase 1 of your VPN policy, from the choice of 3 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 a "gateway" peer, you have the choice of **Certificate** or **Pre-shared key (PSK)**.
Certificate	If you have chosen the certificate authentication method, this field will display your certificate. If you had opted for the pre-shared key method, this field will be grayed out.

Local ID (Optional)	This field represents an IPSec VPN tunnel endpoint, sharing the "secret" or the PSK with the "Peer ID", the other endpoint. You are represented by the "Local ID". This identifier must be in the form of an IP address, a domain name (FQDN: Full Qualified Domain Name) or an e-mail address (user@fqdn).
Peer ID (Optional)	This field represents an IPSec VPN tunnel endpoint, sharing 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).
Confirm	Confirmation of you pre-shared key (PSK).

Advanced properties

Negotiation mode	In IPSec, 2 negotiation modes are possible: main mode and aggressive mode. They have particular influence over Phase 1 of the IKE protocol (authentication phase). This mode is automatically determined according to the configuration parameters; aggressive mode is used only in the case of an anonymous configuration by pre-shared keys. This mode can nonetheless be modified by CLI. **Main mode**: In this mode, Phase 1 takes place in 6 exchanges. The remote host can only be identified by its IP address with pre-shared key authentication. In PKI mode, the identifier is the certificate. Main mode guarantees anonymity. **Aggressive mode**: In this mode, Phase 1 takes place in 3 exchanges between the Firewall and the remote host. Peer identities can either be an IP address, an FQDN or an e-mail address but not a certificate. Authentication is carried out with pre-shared keys. Aggressive mode does not guarantee anonymity. **WARNING** The use of the aggressive mode + pre-shared keys (especially for VPN tunnels to mobile workstations) may be less safe than other modes in the IPSec protocol. Stormshield Network recommends using the main mode and especially main mode + certificates for tunnels to mobile workstations. In fact, the Firewall's internal PKI is capable of providing the certificates needed for such use. **NOTE** To define an ASCII pre-shared key that is sufficiently secure, it is absolutely necessary to follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management.

Backup mode	The backup mode is the switch mode for the IPSec failover – if a server becomes unreachable, another will take over transparently. When the tunnel switches to the backup peer, two choices are possible: "**temporary**" mode: once the main peer becomes contactable again, the tunnel will switch back to it. "**permanent**" mode: the tunnel stays on the backup peer as long as it is operational, even if the main peer is contactable again. **NOTE** This field can only be edited in expert mode (CLI). Please refer to the article in the technical support's Knowledge Base for further information (How can I modify the backup mode for a specific IPSec peer?).
Local address	Object selected as the local IP address used for IPSec negociations with this peer. This field is set to "Any" by default, corresponding to the automatic choice of interface, based on the outing table.
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.
DPD	This field allows configuring the DPD (*Dead Peer Detection*) VPN feature. 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 , who will need to acknowledge the requests in order to validate his availability (*R U there ACK)*. These exchanges are secured via ISAKMP (Internet Security Association and Key Management Protocol) SAs. If it is detected that a peer is no longer responding, the negotiated SAs will be destroyed. **WARNING** 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.

NOTE

For each 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**.

When the negotiation mode (main or aggressive) has been imposed, it will be preserved when the configuration of an IPSec peer is modified.

Peer (nomad/"mobile peer")

Comments	Description given of the remote peer.
Remote gateway	This field is grayed out for mobile peers.
Backup configuration	This field is grayed out for mobile peers.
IKE profile	This option allows selecting the protection model associated with your VPN policy, from the choice of 3 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)**, **Hybrid**, **Certificate** and **XAuth (iPhone).**
Certificate	If you have chosen the **Certificate**, **Hybrid** or **Certificate** and **XAuth** authentication method, this field will display your certificate or will suggest that you select it from the drop-down list. If you had opted for the pre-shared key method, this field will be grayed out.
Local ID (Optional)	This field represents an IPSec VPN tunnel endpoint, sharing 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.
Click here to edit the PSK list	By clicking on this link, you will switch to the "Identification" tab in the IPSec VPN module. You can add you **Approved certificate authorities** as well as your **Mobile tunnels: pre-shared keys**.

Advanced properties

Negotiation mode

In IPSec, 2 negotiation modes are possible: main mode and aggressive mode. They have particular influence over Phase 1 of the IKE protocol (authentication phase).

Main mode: In this mode, Phase 1 takes place in 6 exchanges. The remote host can only be identified by its IP address with pre-shared key authentication.
In PKI mode, the identifier is the certificate. Main mode guarantees anonymity.

Aggressive mode: In this mode, Phase 1 takes place in 3 exchanges between the Firewall and the remote host. The remote host can be identified by an IP address, FQDN or e-mail address but not by a pre-shared key certificate. Aggressive mode does not guarantee anonymity.

NOTE
Stormshield Network automatically configures the use of certificate, hybrid or XAuth authentication methods in main mode.
If the client wishes to use the PSK, he has to use the aggressive mode.

WARNING
The use of the aggressive mode + pre-shared keys (especially for VPN tunnels to mobile workstations) may be less safe than other modes in the IPSec protocol. Stormshield Network therefore recommends the use of main mode for mobile peers, either with authentication by certificate or by using hybrid mode. In an authentication by certificate, the firewall's internal PKI is fully capable of providing the certificates needed for such use.

NOTE
To define an ASCII pre-shared key that is sufficiently secure, it is absolutely necessary to follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management.

Backup mode

The backup mode is the switch mode for the IPSec failover – if a server becomes unreachable, another will take over transparently.

Nonetheless, the field is grayed out here as the backup configuration cannot be applied to a mobile configuration.

NOTE
This field can only be edited in expert mode (CLI). Please refer to the article in the technical support's Knowledge Base for further information (*How can I modify the backup mode for a specific IPSec peer?*).

Local address

Object selected as the local IP address used for IPSec negociations with this peer. This field is set to "Any" by default.

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.

DPD

This field allows configuring the DPD (*Dead Peer Detection*) VPN feature. 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 , who will need to acknowledge the requests in order to validate his availability (*R U there ACK)*.

These exchanges are secured via ISAKMP (Internet Security Association and Key Management Protocol) SAs.
If it is detected that a peer is no longer responding, the negotiated SAs will be destroyed.

WARNING
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.

"Identification" tab

Approved certificate authorities

This table will allow you to list the authorities in order 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 certificate authorities will be displayed.

Mobile tunnels: pre-shared keys

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.

REMARKS

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.

NOTE

To define an ASCII pre-shared key that is sufficiently secure, it is absolutely necessary to follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management.

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 values defined in Phase 1 and 2 will be preselected each time a new peer is created.

IKE (Phase 1) encryption profile

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 allows choosing the protection model associated with your VPN policy, from 3 pre-configured profiles: **StrongEncryption**, **GoodEncryption**, and **Mobile**. Others may also be created.

IPSec (Phase 2) encryption profile

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 allows choosing the protection model associated with your VPN policy, from 3 pre-configured profiles: **StrongEncryption**, **GoodEncryption**, and **Mobile**. Others may also be created.

Table of profiles

This table offers a series of predefined Phase 1 and Phase 2 encryption profiles.

Add	By clicking on this button, you will be able to add a **Phase 1 profile (IKE)** or **Phase 2 profile (IPSec)**, which will be displayed in the "Type" column. You can give it any "Name" you wish. It is also possible to copy a profile and its characteristics: to do so, select the desired profile and click on the option **Copy selection**, and give it a name.
Delete	Select the encryption profile to be deleted from the list and click on **Delete**.

IKE profiles

For each 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.

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. **NOTE** To define an ASCII pre-shared key that is sufficiently secure, it is absolutely necessary to follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management. **REMARK** The longer the password (or "key"), the higher the level of security, but at the same time consumes more resources. **NOTE** The use of IPSec's PFS function (ISAKMP) is recommended.
Maximum lifetime (in seconds)	Period beyond which keys will be renegotiated. The default duration of an **IKE** profile is 21600 seconds, and 3600 seconds for an **IPSec** profile.

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	6 choices are offered: **des**, **3des**, **blowfish, cast128**, **aes** and **aes_gcm_16**. 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	5 choices are offered: **sha1, md5, sha2_256, sha2_384, sha2_512**.
Strength	Number of bits defined for the selected algorithm.

IPSec profiles

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.
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. **NOTE** To define an ASCII pre-shared key that is sufficiently secure, it is absolutely necessary to follow the same rules for user passwords set out in the section **Welcome**, under the section User awareness, sub-section User password management. **REMARK** The longer the password (or "key"), the higher the level of security, but at the same time consumes more resources. **NOTE** The use of IPSec's PFS function (ISAKMP) is recommended.
Lifetime (in seconds)	Period beyond which keys will be renegotiated. The default duration of an **IKE** profile is 21600 seconds, and 3600 seconds for an **IPSec** profile.

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_sha1**, with a "Strength" of 160 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	6 choices are offered: **hmac_sha1, hmac_md5, hmac_sha256, hmac_sha384, hmac_sha512** or **non_auth.**
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 **des**, with a "Strength" of 64 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	6 choices are offered: **des**, **3des**, **blowfish, cast128**, **aes**, **aes_gcm_16** or **null_enc**. 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.

Click on **Apply** once you have completed the configuration.

INTERFACES

The Interfaces module allows you to manage, add and delete network elements called network interfaces that represent physical or virtual communication devices between the various networks that pass through the appliance.

Bridges comprise 3 tabs, interfaces consist of 2 tabs (Ethernet and VLANs) and modems take up only 1 tab.

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

Operating mode between interfaces

How interfaces on the firewall interact can be configured according to three different modes:

- Advanced mode (Router)
- Bridge mode (or transparent mode)
- Hybrid mode

Advanced mode

In advanced mode: each interface has a different IP address and the network that has been assigned to it is in the same address class. This enables the configuration of translation rules for accessing other zones in the firewall.

With this configuration mode, the Firewall operates like a router between its different interfaces.

This involves certain IP address changes on the routers or servers when you move them to a different network (behind a different interface of the Firewall).

The advantages of this mode are:

- possibility of address translation from one address class to another.
- only traffic passing from one interface 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.
- better distinction between the different elements belonging to each zone (internal, external and DMZ). The distinction is made by the different IP addresses for each zone. This enables a clearer view of the separations and the configuration to be applied on these elements.

Bridge mode or transparent mode

In transparent (bridge) mode: interfaces are part of the address range declared on the bridge.

The transparent or "bridge" mode, allows keeping the same address range between interfaces.

It simulates a filtering bridge: in other words, all the network traffic crosses it.

However, you can subsequently filter traffic across by using interface objects or address ranges according to your needs and therefore protect any part of your network.

There are many advantages to this mode:

- 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-saving as far as firewall packet treatment is concerned.

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.

Hybrid mode

In hybrid mode: some interfaces have the same IP address and others have a distinct 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 transparent mode

Example

Internal zone and DMZ (or external zone and DMZ) and certain interfaces in a different address range. As such, you have greater flexibility when integrating the product.

Link aggregation (LACP) – SN510, SN710, SN910, SN2000, SN3000 and SN6000

The LACP (IEEE 802.3ad - Link Aggregation Control Protocol) or Aggregation of links allows improving the appliance's bandwidth while maintaining a high level of availability (link redundancy).

Several physical ports on an appliance can be grouped together to be considered a single logical interface. Therefore, by aggregating *x* links, it will be possible to set up a link of *x* times 1 Gbps or 10 Gbps between two appliances.

This feature is only available on SN510, SN710, SN910, SN2000, SN3000 and SN6000 models.

NOTE

Ensure that the remote appliances are using LACP.

Conclusion

The choice of a mode is made only where network interface configuration is concerned. The configuration of the firewall is then the same for all modes.

Security-wise, all operating modes are equal. The same things are filtered and attack detection is identical.

Presentation of the configuration screen

The interface configuration window consists of 3 sections:

- **The directory of interfaces**: the appliance's interfaces are presented sorted in the following order: Bridge, Interface, VLAN, Modem according to the selected view. Clicking on an interface allows viewing its configuration. It is also possible to use the search engine to look for a specific interface. (Example: by typing "br", all bridges will be displayed).
- **The configuration panel (central panel)**: by clicking on an interface in the directory, its configuration will appear in this panel.
- **The toolbar**: this bar allows:
  - Adding or deleting interfaces (bridge, modem),
  - Expanding or collapsing the folders in the interface directory,

- Selecting one of 3 views: “Mixed view” which is the default view and which corresponds to a logical representation of the interfaces (that is, bridges first (they make up the root node), interfaces, VLANs (attached to the interface or the bridge), then modems). “Group by physical port” and “Group by address range” allow filtering according to the desired interface and checking its use.

Directory of interfaces

The appliance's interfaces are indicated in the directory.

Drag & Drop

Dragging and dropping an interface modifies its configuration (its relationships and address range). If a drag & drop operation is authorized, a green tick will appear. Otherwise, if the move is prohibited, a red circle will be indicated.

When an interface is detached from a bridge, a window will appear, allowing the address range to be entered.

The following moves are allowed:

Bridge/Interface	From	To
Ethernet Interface	Bridge	Root
Ethernet Interface	Bridge	Another bridge
Ethernet Interface	Root	Bridge
VLAN	Ethernet Interface	Another Ethernet interface
VLAN	Ethernet Interface	Bridge
VLAN	Bridge	Another bridge
VLAN	Bridge	Ethernet Interface
Modem (PPPoE)	Interface	Another interface

Searching for interfaces

An interface can be found more easily with the search field.

Name, Address, Type, Comments, Hostname (DHCP), Physical MAC address, Gateway (routing by interface). Searches are possible in the following fields of the interfaces:

Example: you can search for an interface by indicating its name or even the address of its gateway.

To validate a search, simply click on **Enter**. To delete a search, click on the cross to the right of the search field.

Identifying interfaces

Each interface has its own icon for quicker visual identification. This icon also allows identifying whether the interface has been enabled or disabled. If it has been disabled, the icon and the name of the interface will be grayed out.

Ethernet interfaces have a real name (ex: "Out") and a technical name (ex: "0"). The physical port is displayed in brackets after the name of the interfaces.

Toolbar

Add	This button allows you to open the bridge, VLAN, modem or GRETAP interface creation wizard. It also allows converting an interface into a link aggregate.
Delete	This button allows you to delete an interface that was previously selected in the interface directory. Ethernet interfaces cannot be deleted.
Collapse	This button allows collapsing all folders in the interface directory.
Expand	This button allows expanding all folders in the interface directory.
Mixed view	3 views are suggested: Mixed view, Group by physical port (interfaces are grouped by port. For each port, interfaces and VLANs are indicated), **Group by address range** (interfaces are separated according to their address range. If the interface contains an address + an alias, in this case, it will appear twice in the directory).
Show all	6 filter options are available: **Bridge, Interface, VLAN, Modem (Dialup),** GRETAP interface, **Show all**.
Check usage	If you click on this button after having selected an interface, the results will appear in the directory of modules. If you delete an interface, a check will be performed in order to warn the user about configurations that use the interface he wishes to delete. If the interface is in use, the following message will appear: "Warning, *this interface/bridge is being used by one or several modules. Removing it will make the firewall unstable*." You can either force the deletion, check its usage or cancel. If the check does not turn up any results, the message: "**Delete this interface?**" will appear.

NOTE

An external 3G modem can now be connected to the USB port.

NOTE

Renaming an interface does not migrate references to it especially in configuration items that use generated objects such as "Network_in". A warning message appears when an interface is renamed.

Creating a bridge

Bridges can be created using a wizard that allows you to create the interface easily.

Click on **Add** in the toolbar and select "**Add a Bridge**". The bridge creation wizard will then appear.

NOTE

The number of bridges to create depends on your firewall model.

Identifying the bridge

Name	Name of the interface. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the interface.

Address range

Fixed IP (static)	By selecting this option, the bridge will have a static address range. In this case, its IP address and the mask of the sub-network to which the bridge belongs, have to be indicated.
Dynamic IP (obtained by DHCP)	By selecting this option, the interface will be defined by DHCP. In this case, a DHCP hostname that is the name of a server for the connection (FQDN) must be indicated. This optional field does not identify the DHCP server but the firewall. If this field has been entered and the external DHCP server has the option of automatically updating the DNS server, the DHCP server will automatically update the DNS server with the name and the IP address provided by the firewall as well as the allocated time (mandatory). This name consists of 6 bytes in hexadecimal separated by : The period during which the IP address is kept before renegotiation must also be indicated.

Click on **Next** at the bottom of the screen. The bridge creation screen will appear (Step 2).

Select the interfaces for which you wish to create a bridge. The list of "Available interfaces" shows all the Ethernet and VLAN interfaces already in the configuration. At least two interfaces have to be selected in order to make a bridge, either by using arrows or by dragging and dropping between both lists or by double-clicking on the interface. Click on **Finish** to confirm the creation.

Modifying a bridge

To modify the parameters of a bridge, click on its name in the left side of the window. Three tabs allow the modification of the bridge's parameters.

"General" tab

Name (mandatory)	Name of the interface. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the interface.

Bridge members

Physical ports	List of Ethernet ports in the bridge (Example: (Port2)
Interfaces (physical and logical)	List of interfaces contained in the bridge (Example: in)

Address range

Dynamic IP (obtained by DHCP)	The assigned IP address can be matched to a domain name via a DNS service provider (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This option is used when your firewall does not have a static IP address (e.g., your service provider, or DHCP renews its IP address regularly). This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. *The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module.* This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the "DHCP" zone in the *Advanced properties* tab will be enabled.
Fixed IP (static)	Your firewall has a static (fixed) IP address.

List of the bridge's IP addresses

This table appears if the option Fixed IP (static) has been selected.

IP address	IP address assigned to the bridge. (All interfaces contained in the bridge will have the same IP address).
Net Mask	Network mask of the sub-network to which the bridge belongs. The various interfaces that are part of the bridge have the same IP address so all networks connected to the firewall are part of the same address range. The network mask provides the firewall with information about the network to which it belongs.
Comments	Allows adding comments regarding the bridge's address.

Here, several associated IP addresses and network masks may be defined for the same bridge (the need to create aliases, for example). These aliases may allow you to use this 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. Reloading the network configuration will apply this mask on the first address and a mask /32 on the following addresses.

"Advanced properties" tab

MTU	Maximum length (in bytes) of frames transmitted on the physical support (Ethernet) so that they are sent at one go (without fragmentation).
Physical (MAC) address	**Warning** This option is not accessible for firewalls in high availability. This window allows you to specify a MAC address for an interface instead of using the address assigned by the firewall. This allows you to better facilitate the integration of the Stormshield Network firewall in transparent mode into your network (by specifying your router's MAC address instead of having to reconfigure all the workstations using this MAC address). When the MAC address is assigned to the bridge, all interfaces contained in this bridge will then have the same MAC address. This address consists of 6 bytes in hexadecimal separated by :

DHCP

NOTE

This field will be indicated as "disabled" if the option Dynamic IP (obtained by DHCP) was not selected in the *General* tab, and options will be grayed out.

DNS name (optional)	Name of the DNS server (FQDN) for the connection. This optional field does not identify the DHCP server but the firewall. If this field has been entered and the external DHCP server has the option of automatically updating the DNS server, the DHCP server will automatically update the DNS server with the name and the IP address provided by the firewall. This name consists of 6 bytes in hexadecimal separated by ":"
Requested lease time (seconds)	Period during which the IP address is kept before renegotiation.

Request domain name servers from the DHCP server and create host objects	If this option is selected, the firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address. Two objects will be dynamically created in the object database upon the selection of this option: 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.

Loops detection (Spanning Tree)

This section allows activating the use of a network loop detection protocol (Spanning Tree) on the selected bridge. This feature is only available on SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100 models.

Disable Spanning Tree protocols	This option disables the use of Spanning Tree protocols (RSTP and MSTP) in the bridge. It is selected by default.
Enable Rapid Spanning Tree protocol (RSTP)	This option allows activating the Rapid Spanning Tree protocol on the bridge.
Enable Multiple Spanning Tree protocol (MSTP)	This option allows activating the Multiple Spanning Tree protocol on the bridge.

When MSTP is enabled, additional fields need to be filled in:

Region name (MSTP region)	Indicate the name of the MSTP region in which the firewall is located. The name of the region has to be the same in the MSTP configuration on all network appliances belonging to this region.
Format selector	This field specifies the information needed for defining a region. Its default value is 0, indicating that a region's properties are: • Its name, • Revision number, • Fingerprint calculated based on MST instance numbers and VLAN identifiers included in these instances. The format selector has to 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 has to be the same in the MSTP configuration on all network appliances belonging to this region. **NOTE** In order to ensure that modifications can be tracked 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 for the affected region..

REMARK

On Stormshield Network firewalls, an MSTP configuration can only define one region.

Table of MSTP instances

This table allows defining the various instances declared in the MSTP configuration:

Instance	This unique identifier is incremented automatically whenever an instance is added to the MSTP configuration.

VLAN IDs	Indicate the various VLAN identifiers (list of identifiers separated by commas) included in the selected instance.
Priority	This field allows setting 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.

"Bridge members" tab

Another way to include interfaces in a bridge, apart from dragging and dropping, is to use the panel in this tab. (bridge members).

To move an available interface to the bridge, drag and drop it or use the red arrow in between both tables or double-click on the interface you wish to move.

To remove an interface from a bridge, do the exact opposite.

Deleting a bridge

To delete a bridge, select it in the interface directory, then click on **Delete** in the toolbar. The message *"Delete this interface?"* will appear.

Confirm or cancel the deletion.

If you confirm the deletion, a check will be performed to see if the interface is in use.

NOTE

Deleting a bridge disables the interfaces that it contained and also disables their switch to a configuration in DHCP.

Modifying an Ethernet interface (in bridge mode)

If an interface is in a bridge, it will be represented as a child node in relation to the bridge. Thus, a bridge may contain several child nodes.

You can change the parameters of each interface, whether or not it belongs to the bridge. To do so, select an interface located inside or outside a bridge on the left-hand side of the window. Two tabs will then appear:

NOTE

Ethernet interfaces cannot be added or deleted.

"Configuration of the interface" tab

Name (mandatory)	Name given to the bridge interface. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the interface.
Physical port	Name of the physical port (example: in (port 2)).

VLANs attached to the interface	List of VLANs attached to the selected interface. The appliance does not need to be systematically rebooted whenever a VLAN is deleted.
Color	Color assigned to the interface.
This interface is	An interface can either be "internal (protected)" or "external (public)". If you select "internal (protected)", you are indicating that this interface is protected. This protection includes the memorization of 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 (see the section *Implicit rules*). Protected interfaces are represented by a shield ( ). If you select "external (public)", you are indicating that this part of the network is linked up to the internet. In most cases, the external interface, linked up to the internet, has to be in external mode. The shield icon disappears when this option is selected.

Address range

None (interface disabled)	By selecting/unselecting this option, the interface will be enabled/disabled. By disabling an interface, it becomes unusable. In terms of use, this may correspond to an interface to be used in the near or distant future, but which is not active. An interface which has been disabled because it is not in use is an example of an additional security measure against intrusions.
Dynamic IP (obtained by DHCP)	The assigned IP address can be matched to a domain name via a DNS service provider (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This option is used when your firewall does not have a static IP address (e.g., your service provider, or DHCP renews its IP address regularly). This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. *The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module.* This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the "DHCP" zone in the *Advanced properties* tab will be enabled.
Address range inherited from the bridge	If the interface is part of a bridge, the address range of the bridge can be retrieved.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and the mask of the sub-network to which the interface belongs, have to be indicated.

Here, several associated IP addresses and network masks may be defined for the same bridge (the need to create aliases, for example). These aliases may allow you to use this 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. Reloading the network configuration will apply this mask on the first address and a mask /32 on the following addresses.

"Advanced properties" tab

MTU

Maximum length (in bytes) of frames transmitted on the physical support (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

WARNING
This option is not accessible for firewalls in high availability.

This window allows you to specify a MAC address for an interface instead of using the address assigned by the firewall. This allows you to better facilitate the integration of the Stormshield Network firewall in transparent mode into your network (by specifying your router's MAC address instead of having to reconfigure all the workstations using this MAC address).

If the interface is contained in a bridge, it will have the same MAC address as the bridge.

NOTE
This field is grayed out as the interface belongs to a bridge. It can neither be modified nor deleted.

DHCP

NOTE

This option will be indicated as "disabled" if the option **Dynamic IP (obtained by DHCP)** was not selected in the *Configuration of the interface* tab and the options will be grayed out.

DNS name (optional)

Name of the DNS server (FQDN) for the connection.

This optional field does not identify the DHCP server but the firewall. If this field has been entered and the external DHCP server has the option of automatically updating the DNS server, the DHCP server will automatically update the DNS server with the name and the IP address provided by the firewall.

This name consists of 6 bytes in hexadecimal separated by :

Requested lease time (seconds)

Period during which the IP address is kept before renegotiation.

Request domain name servers from the DHCP server and create host objects

If this option is selected, the firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address.

Two objects will be dynamically created in the object database upon the selection of this option: 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.

NOTE
This option will be disabled if the option **Dynamic IP (obtained by DHCP)** was not selected in the *Configuration of the interface* tab

Bridge – Routing without analysis

NOTE

This option will be indicated as "disabled" if the option **Address range inherited from the bridge** was not selected in the *Configuration of the interface* tab and the options will be

grayed out.

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).

Bridge – Routing by interface

NOTE

This option will be indicated as "disabled" if the option **Address range inherited from the bridge** was not selected in the *Configuration of the interface* tab and the options will be grayed out.

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. These cases are: • The reinitialization of connections induced by an alarm, • The SYN proxy (enabled in filtering), • Requests to resend packets dropped in order to speed up a scan, • Rewriting of packets by application scans (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. This option requires the activation of the previous option "**Keep initial routing**".
Gateway address	This field is used for routing by interface. All packets that arrive on this interface will be routed via a specified gateway.

Media

Media	Connection speed of the network. By default the firewall detects this automatically but you can enforce the use of a particular mode. The different speeds available are: "Automatic detection", "10 Mb Half duplex", "10 Mb Full duplex", "100 Mb Half duplex", "100 Mb Full duplex", "1 Gb Half duplex", "1 Gb Full duplex". **WARNING** 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.

Interface's bandwidth (for information only)

Bandwidth	Defines the throughput on an interface. This is an automatic entry that is not compulsory: it is used for monitoring in the calculation of bandwidth.

Modifying an Ethernet interface (advanced mode)

To configure an interface in a network which is not part of a bridge you need to take it out of the bridge directory using the mouse. You may then configure the interface parameters.

During this detachment, the address range window will appear.

Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and network mask must be indicated.
Dynamic IP (obtained by DHCP)	By selecting this option, the interface will be defined by DHCP. In this case, a DHCP hostname and a lease time must be indicated.

Once the interface is outside the bridge, you will be able to access the parameters of the interface described in the section "**Modifying an Ethernet interface (in bridge mode)**".

Creating or modifying a Wi-Fi interface (WLAN)

Interfaces corresponding to the firewall's access points (WLAN) are listed in the left section of the **Interfaces** window. Select an interface in order to modify its parameters. A tab will appear:

NOTE

WLAN interfaces cannot be added or deleted.

"Configuration of the interface" tab

Name (mandatory)	Name given to the WLAN interface. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the interface.
VLANs attached to the interface	List of VLANs attached to the selected interface.
Color	Color assigned to the interface.
This interface is	An interface can either be "internal (protected)" or "external (public)". If you select "internal (protected)", you are indicating that this interface is protected. This protection includes the memorization of 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 (see the section *Implicit rules*). Protected interfaces are represented by a shield ( ). If you select "external (public)", you are indicating that this part of the network is linked up to the internet. In most cases, the external interface, linked up to the internet, has to be in external mode. The shield icon disappears when this option is selected.

Wi-Fi

Network name	Enter the name assigned to the Wi-Fi network that the firewall manages (SSID).
Authentication	Select one of the three authentication mechanisms that allow connecting to the Wi-Fi network that the firewall manages: • Open network (no authentication). **NOTE** When this option is selected, the **Security key** field will become inactive (grayed out). • WPA (Wi-Fi Protected Access). • WPA 2 (WPA 2 is an upgrade to WPA offering a higher level of security).
Security key	Enter the security key (password) needed for logging on to the Wi-Fi network.
Access point 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. It 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

None (interface disabled)	By selecting/unselecting this option, the interface will be enabled/disabled. By disabling an interface, it becomes unusable. In terms of use, this may correspond to an interface to be used in the near or distant future, but which is not active. An interface which has been disabled because it is not in use is an example of an additional security measure against intrusions.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and the mask of the sub-network to which the interface belongs, have to be indicated.

Here, several associated IP addresses and network masks may be defined for the same bridge (the need to create aliases, for example). These aliases may allow you to use this 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. Reloading the network configuration will apply this mask on the first address and a mask /32 on the following addresses.

Creating a VLAN

VLANs are configured via a wizard that allows you to create the interface easily.

Select the interface or the bridge for which you wish to associate a VLAN. Then click on **Add** and **Add a VLAN**.

Select the type of VLAN you wish to create.

VLAN attached to a single interface (VLAN endpoint)	Stormshield Network firewalls can be placed at the end of VLANs to add or remove a VLAN tag. The firewall carries out the filtering and takes care of communications between the VLANS and the networks connected to the other firewall interfaces. The firewall recognizes the VLANs as belonging to virtual interfaces, which enables them to be fully integrated into the company's security system. If you select this option, by clicking on **Next**, the screen for Step 2 will appear. The creation process takes place in 2 steps.
VLAN attached to 2 interfaces (crossing VLAN)	This option allows creating a crossing VLAN, meaning a bridge containing 2 VLANs with the same ID. If you select this option, by clicking on **Next**, the screen for Step 3 will appear

VLAN attached to a single interface (VLAN endpoint)

VLAN identification

Parent interface	Select the interface to which the VLAN will be attached.
Name	Enter a unique name for your VLAN (Cf. section Allowed names).
Comments	You may also enter a description.
Color	Color assigned to the VLAN.
VLAN IDs	This field allows specifying the value to be associated with the VLAN in packets passing through the network. This tag identifies the VLAN and is used at the Ethernet level. It must be unique and be any value between 1 and 4094 inclusive.
Priority (CoS)	This CoS (Class of Service field) priority will then be imposed for all packets sent by the VLAN.
This interface is	Determine whether the VLAN should be defined as an external or internal (protected) interface.

Address range

Dynamic IP (obtained by DHCP)	Select this option to give the VLAN a dynamic address.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and network mask must be indicated.

Click on **Finish**.

VLAN attached to 2 interfaces (crossing VLAN)

When configuring VLANs for bridges, the same tag can be used for two VLAN interfaces , making the Firewall appear transparently on the network. This method requires the use of one VLAN interface per physical interface.

Unlike the option **Keep VLAN IDs** (cf. in the *advanced properties of an Ethernet interface*) which makes the firewall fully transparent to the VLAN and which prevents the use of features which would interrupt VLAN traffic, such as proxies, this method of keeping the VLAN tag between several interfaces on the same bridge allows the use of all firewall features.

VLAN identification

Name	Enter a unique name for your VLAN

VLAN IDs	This field allows specifying the value to be associated with the VLAN in packets passing through the network. This tag identifies the VLAN and is used at the Ethernet level.
Color	Color assigned to the VLAN.

VLAN address range

Use an existing bridge	By selecting this option, you will need to select from the drop-down list the bridge to which VLANs will be attached.
Create a new bridge	If this option is selected, a wizard will allow creating a new bridge which will contain both interfaces.
Dynamic IP (obtained by DHCP)	The assigned IP address can be matched to a domain name via a DNS service provider (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This option is used when your firewall does not have a static IP address (e.g., your service provider, or DHCP renews its IP address regularly). This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module. This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the "DHCP" zone in the *Advanced properties* tab will be enabled.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and the mask of the sub-network to which the interface belongs, have to be indicated.

Click on **Next**.

Identification of the incoming VLAN

Name (mandatory)	Unique name for your VLAN. This field is pre-entered with the name indicated in the Name field in Step 3 suffixed with "1".
Interface (mandatory)	Select the interface to which the VLAN will be attached.
This interface is	If "internal (protected)" is selected, this indicates that the interface is private. Addresses of **internal** interfaces cannot be used as destinations for packets coming from unprotected interfaces, except if they have been translated. **NOTE** You will notice that "internal (protected)" implies being on a protected interface. Therefore the options "internal (protected)" and "external (public)" are incompatible. If you select "**external (public)**" this indicates that this section of the network is connected to the internet. In most cases, the external interface, linked up to the internet, has to be in external mode. The interface's security, represented by a shield ( ), disappears when this option is checked.
Priority (CoS)	This CoS (Class of Service field) priority will then be imposed for all packets sent by the VLAN.
Use the same priority for the outgoing VLAN	When this checkbox is selected, an identical value will be automatically assigned to the **Priority (CoS)** field in the properties of the outgoing VLAN.

Click on **Next** again.

Identification of the outgoing VLAN

Name (mandatory)	Unique name for your VLAN. This field is pre-entered with the name indicated in the Name field in Step 3 suffixed with "2".
Interface	Enter a unique name for your VLAN
This interface is	If "internal (protected)" is selected, this indicates that the interface is private. Addresses of **internal** interfaces cannot be used as destinations for packets coming from unprotected interfaces, except if they have been translated. **NOTE** You will notice that "internal (protected)" implies being on a protected interface. Therefore the options "internal (protected)" and "external (public)" are incompatible. If you select "**external (public)**" this indicates that this section of the network is connected to the Internet. In most cases, the external interface, linked up to the internet, has to be in external mode. The interface's security, represented by a shield ( ), disappears when this option is checked.
Priority (CoS)	This CoS (Class of Service field) priority will then be imposed for all packets sent by the VLAN. This priority may be different from the one assigned to the incoming VLAN.

The following screen summarizes the configuration that you have just created.

Adding a VLAN

If you wish to create a new VLAN and you have reached the maximum number of dynamic VLANs possible, a pop-up window will appear to allow you to add others. This number can also be modified manually by going to **System\Configuration\Network\Available VLANs (max 128).**

Modifying a VLAN

"Configuration of the interface" tab

Name (mandatory)	Name given to the VLAN. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the VLAN.
Parent interface	Physical name of the interface to which the VLAN is attached.
Color	Color assigned to the VLAN.
VLAN IDs	Identifier for the VLAN which may 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 either be "internal (protected)" or "external (public)". If you select "internal (protected)", you are indicating that this interface is protected. This protection includes the memorization of 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 (see the section *Implicit rules*). Protected interfaces are represented by a shield ( ). If you select "external (public)", you are indicating that this part of the network is linked up to the internet. In most cases, the external interface, linked up to the internet, has to be in external mode. The shield icon disappears when this option is selected.

Address range

None (interface disabled)	By selecting/unselecting this option, the interface will be enabled/disabled. By disabling an interface, it becomes unusable. In terms of use, this may correspond to an interface to be used in the near or distant future, but which is not active. An interface which has been disabled because it is not in use is an example of an additional security measure against intrusions.
Dynamic IP (obtained by DHCP)	The assigned IP address can be matched to a domain name via a DNS service provider (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This option is used when your firewall does not have a static IP address (e.g., your service provider, or DHCP renews its IP address regularly). This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. *The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module.* This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the "DHCP" zone in the *Advanced properties* tab will be enabled.
Address range inherited from the bridge	If the interface is part of a bridge, the address range of the bridge can be retrieved. This zone will be grayed out if the interface does not belong to a bridge.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and the mask of the sub-network to which the interface belongs, have to be indicated.

Here, several associated IP addresses and network masks may be defined for the same bridge (the need to create aliases, for example). These aliases may allow you to use this 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. Reloading the network configuration will apply this mask on the first address and a mask /32 on the following addresses.

"Advanced properties" tab

MTU	Maximum length (in bytes) of frames transmitted on the physical support (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	**Warning** This option is not accessible for firewalls in high availability. This window allows you to specify a MAC address for an interface instead of using the address assigned by the firewall. This allows you to better facilitate the integration of the Stormshield Network firewall in transparent mode into your network (by specifying your router's MAC address instead of having to reconfigure all the workstations using this MAC address). If the interface is contained in a bridge, it will have the same MAC address as the bridge. **NOTE** This field is grayed out as the interface belongs to a bridge.

DHCP

NOTE

This option will be indicated as "disabled" if the option **Dynamic IP (obtained by DHCP)** was not selected in the *Configuration of the interface* tab and the options will be grayed out.

DNS name (optional)	Name of the DNS server (FQDN) for the connection. This optional field does not identify the DHCP server but the firewall. If this field has been entered and the external DHCP server has the option of automatically updating the DNS server, the DHCP server will automatically update the DNS server with the name and the IP address provided by the firewall. This name consists of 6 bytes in hexadecimal separated by :
Requested lease time (seconds)	Period during which the IP address is kept before renegotiation.
Request domain name servers from the DHCP server and create host objects	If this option is selected, the firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address. Two objects will be dynamically created in the object database upon the selection of this option: 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. **NOTE** This option will be disabled if the option **Dynamic IP (obtained by DHCP)** was not selected in the *Configuration of the interface* tab

Routing without analyzing

NOTE

This option will be indicated as "disabled" if the option **Address range inherited from the bridge** was not selected in the *Configuration of the interface* tab and the options will be grayed out.

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

NOTE

This option will be indicated as "disabled" if the option **Address range inherited from the bridge** was not selected in the *Configuration of the interface* tab and the options will be grayed out.

Preserve VLAN 802.1p priority	This option forces the firewall to keep 802.1p (Quality of Service) priority for packets coming from the VLAN and passing through the firewall to an IPSec tunnel or another interface on the firewall, for example.
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. These cases are: • The reinitialization of connections induced by an alarm, • The SYN proxy (enabled in filtering), • Requests to resend packets dropped in order to speed up a scan, • Rewriting of packets by application scans (SMTP, HTTP and web 2.0, FTP and NAT, SIP and NAT).
Gateway address	This field is used for routing by interface. All packets that arrive on this interface will be routed via a gateway.

Interface's throughput (for information only)

Bandwidth	Defines the throughput on an interface. This is an automatic entry that is not compulsory: it is used for monitoring in the calculation of bandwidth.

Deleting a VLAN

To delete a VLAN, select it in the interface directory, then click on **Delete** in the toolbar. The message "**Delete this interface?**" will appear.

Confirm or cancel the deletion.

If you confirm the deletion, a check will be performed to see if the interface is in use.

Creating a modem

Modem interfaces are used in remote connections when your modem is directly connected to the firewall (serial port or Ethernet). The firewall accepts all modem types (ADSL, ISDN, RTC, ...).

New modem interfaces can be created thanks to the wizard. The maximum number of available modems on your firewall depends on the model.

In the menu **Network\Interfaces** click on **Add** and select "Add un modem"

Step 1

Identification du modem

Name	Enter a name (mandatory).
Comments	Description to identify the Dialup connection.
Color	Color assigned to the remote connection.

Configuring the modem

Select the type of dialup from PPPoE, PPTP, PPP or 3G/4G. The configuration window varies according to the selected dialup.

PPPoE	Select the network interface used for the modem
PPTP	Enter the IP address of the modem.
PPP	Enter the telephone number used for dialing.
3G/4G	Fill in the following fields: • **Access point name**: this information varies according to each access provider and is given to you when your 3G/4G subscription begins. • **Number to dial**: this is the number that the modem needs to dial in order to connect to the access provider's network. The default value suggested is *99# • **IP address of the remote server**: your access provider will give you this address. • **PIN code of the SIM card**: information that comes together with your SIM card. • **USB modem**: by default, the value *Automatic detection* will be suggested. If your modem is not automatically recognized, choose one of the two "customized modem" profiles then click on **Modem configuration**.
Query domain name servers and create associated host objects	If this option is selected, the firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address. Two objects will be dynamically created in the object database upon the selection of this option: 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.
Define the maximum size of TCP packets (MSS) to prevent them from being fragmented. This limit will be applied to all profiles.	If this option is selected, the firewall will automatically adapt the size of packets exchanged through the modem so that they will not be fragmented.

Customized 3G/4G modem profile

If your 3G/4G modem is not automatically recognized, select one of the two customized profiles and fill in the following fields:

Enable: this checkbox will allow taking into account the modem's customized settings.

Name	Enter a name to identify the customized settings.
Model	Enter the model of the modem.
Vendor ID	ID specific to each modem vendor (hexadecimal string).
Initial product ID	Product ID after it has been recognized as a USB storage device. 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.
Target product ID	ID representing the product when it is in modem mode. This parameter is specific to each modem model.
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	This string is optional and allows sending "AT" configuration commands to the modem before it is used. Example: "ATZ" (command to reinitialize the modem), "AT^CURC=0" (command which allows disabling periodic messages).
Initialization string no. 2	This string is optional and allows sending "AT" configuration commands to the modem before it is used. Example: "ATZ" (command to reinitialize the modem), "AT^CURC=0" (command which allows disabling periodic messages).
Initialization string no. 3	This string is optional and allows sending "AT" configuration commands to the modem before it is used. Example: "ATZ" (command to reinitialize the modem), "AT^CURC=0" (command which allows disabling periodic messages).

Authentication

Identifier	Enter the user's ID (mandatory).
Password	Enter the password (mandatory).

Once Step 1 has been configured, click on Next.

Step 2

Routing: use the gateway obtained by the modem

Select whether you wish to define the modem as a gateway.

To the list of main gateways	The host Firewall_<name of modem>_peer will be added to the main gateways. If there is no main gateway, a window will appear asking if you wish to define a main gateway (default router).
To the list of backup gateways	The host Firewall_<name of modem>_peer will be added to the secondary gateways.
Do not add (configure later)	The modem has not been defined as a gateway.

Modifying a modem

PPPoE modem

Use this modem	By selecting this option, you will enable the modem.
Name (mandatory)	Name given to the modem. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the modem.
Modem type	Indicates the type of modem chosen in the creation phase.
Color	Color assigned to the modem.

Authentication

Identifier	Name used for authentication
Password	Password used for authentication. If you click on the key icon to the right of the field, the password will appear in plaintext for 5 seconds.

Connectivity

The modem is connected to the interface	Indicates the modem's connection interface.
Query domain name servers and create associated host objects	If this option is selected, the firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address. Two objects will be dynamically created in the object database upon the selection of this option: 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.

Advanced properties

Service	Type of PPPoE service used. This option allows distinguishing between several ADSL modems. Leave this field empty by default.
Connection	Connection when there is traffic (on demand) establishes a connection with the internet only when a connection request is made by the internal network (this is more economical than in the case of a link that is charged by duration). The Permanent connection keeps the connection to the internet permanently active.

PPTP Modem

Use this modem	By selecting this option, you will enable the modem.
Name (mandatory)	Name given to the modem. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the modem.
Modem type	Indicates the type of modem chosen in the creation phase.
Color	Color assigned to the modem.

Authentication

Identifier	Name used for authentication
Password	Password used for authentication. If you click on the key icon to the right of the field, the password will appear in plaintext for 5 seconds.

Connectivity

PPTP address	Internal IP address of the ADSL modem.
Query domain name servers and create associated host objects	If this option is selected, the firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address. Two objects will be dynamically created in the object database upon the selection of this option: 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.

Advanced properties

Connection	Connection when there is traffic (on demand) establishes a connection with the internet only when a connection request is made by the internal network (this is more economical than in the case of a link that is charged by duration). The Permanent connection keeps the connection to the internet permanently active.

PPP Modem

Use this modem	By selecting this option, you will enable the modem.
Name (mandatory)	Name given to the modem. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the modem.
Modem type	Indicates the type of modem chosen in the creation phase.
Color	Color assigned to the modem.

Authentication

Identifier	Name used for authentication
Password	Password used for authentication. If you click on the key icon to the right of the field, the password will appear in plaintext for 5 seconds.

Connectivity

Number to dial	**Phone number of the access provider.**
Query domain name servers and create associated host objects	If this option is selected, the firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address. Two objects will be dynamically created in the object database upon the selection of this option: 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.

Advanced properties

Initialization strong	String of characters used optionally for initializing the connection.
Connection	Connection when there is traffic (on demand) establishes a connection with the internet only when a connection request is made by the internal network (this is more economical than in the case of a link that is charged by duration). The Permanent connection keeps the connection to the internet permanently active.

3G/4G modem

Use this modem	By selecting this option, you will enable the modem.
Name (mandatory)	Name given to the modem. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the modem.
Modem type	Indicates the type of modem chosen in the creation phase.
Color	Color assigned to the modem.

Authentication

Identifier	Name used for authentication
Password	Password used for authentication. If you click on the key icon to the right of the field, the password will appear in plaintext for 5 seconds.

Connectivity

Access point name	This information varies according to each access provider and is given to you when your 3G/4G subscription begins.
Number to dial	This is the number that the modem needs to dial in order to connect to the access provider's network.
Default IP address of the remote server	Your access provider will give you this address.
PIN code of the SIM card	Information that comes with your SIM card

Advanced properties

Connection	Connection when there is traffic (on demand) establishes a connection with the internet only when a connection request is made by the internal network (this is more economical than in the case of a link that is charged by duration). The Permanent connection keeps the connection to the internet permanently active.
USB modem	This is the configuration mode selected when the modem was created (Automatic detection or customized profile)

Deleting a modem

To delete a modem, select it in the interface directory, then click on **Delete** in the toolbar. The message "**Delete this interface?**" will appear.

Confirm or cancel the deletion.

If you confirm the deletion, a check will be performed to see if the interface is in use.

General remarks on configuring modems

The firewall automatically negotiates the opening of a line and reinitializes the connection in the event of an interruption. In the event the connection is impossible (problem with the line), the firewall will raise an alarm.

Creating a USB stick / modem

USB/Modem interfaces are used in remote connections when your modem is directly connected to the firewall (USB port).

Certain parameters (*access point, number to dial, etc.*) must be entered directly via the administration interface of the USB stick/modem.

The USB/Ethernet interface associated with the USB stick/modem is created via a wizard.

In the menu **Network\Interfaces** click on **Add** and select "Add a USB stick/modem"

Identification of the USB stick / modem

Name	Enter a name for this modem (mandatory).
Comments	Description to identify the 4G connection.
Color	Color assigned to the remote connection.

This interface is	An interface can either be “internal (protected)” or “external (public)”. If you select “internal (protected)”, you are indicating that this interface is protected. This protection includes the memorization of 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 (see the section *Implicit rules*). Protected interfaces are represented by a shield ( ). If you select “external (public)”, you are indicating that this part of the network is linked up to the internet. In most cases, the external interface, linked up to the internet, has to be in external mode. The shield icon disappears when this option is selected.

Address range

IPv4 address	This field offers by default the value *Dynamic IP (DHCP)* so that the USB/Ethernet interface associated with the key automatically retrieves an IPv4 address. You can also specify the IP address and subnet mask associated with this key (e.g.: 10.10.10.10/24 or 10.10.10.10 255.255.255.0).

Modem parameters

If your USB stick/modem is not automatically recognized (**Automatic detection** option), select one of the two customized profiles and fill in the following fields:

Enable: this checkbox will allow taking into account the modem's customized settings.

Name	Enter a name to identify the customized settings.
Model	Enter the model of the modem.
Vendor ID	ID specific to each modem vendor (hexadecimal string).
Initial product ID	Product ID after it has been recognized as a USB storage device. 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.
Target product ID	ID representing the product when it is in modem mode. This parameter is specific to each modem model.
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	This string is optional and allows sending "AT" configuration commands to the modem before it is used. Example: "ATZ" (command to reinitialize the modem), "AT^CURC=0" (command which allows disabling periodic messages).
Initialization string no. 2	This string is optional and allows sending "AT" configuration commands to the modem before it is used. Example: "ATZ" (command to reinitialize the modem), "AT^CURC=0" (command which allows disabling periodic messages).
Initialization string no. 3	This string is optional and allows sending "AT" configuration commands to the modem before it is used. Example: "ATZ" (command to reinitialize the modem), "AT^CURC=0" (command which allows disabling periodic messages).

Modifying a USB/Ethernet interface

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.

The parameters of this type of interface can be modified by selecting it in the left section of the window. A tab will appear:

NOTE

A second USB/Ethernet interfaces cannot be added.

"Configuration of the interface" tab

Name (mandatory)	Name associated with the USB/Ethernet interface (see warning in the introduction of the **Interfaces** section).
Comments	Allows you to enter comments regarding the interface.
Color	Color assigned to the interface.
This interface is	An interface can either be "internal (protected)" or "external (public)". If you select "internal (protected)", you are indicating that this interface is protected. This protection includes the memorization of 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 (see the section *Implicit rules*). Protected interfaces are represented by a shield ( ). If you select "external (public)", you are indicating that this part of the network is linked up to the internet. In most cases, the external interface, linked up to the internet, has to be in external mode. The shield icon disappears when this option is selected.

Modem parameters

USB modem	This field allows selecting the modem's automatic detection mode or one of the customized profiles created earlier.

Address range

Dynamic IP (obtained by DHCP)	The assigned IP address can be matched to a domain name via a DNS service provider (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This option is used when your firewall does not have a static IP address (e.g., your service provider, or DHCP renews its IP address regularly). This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. *The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module.* This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the "DHCP" zone in the *Advanced properties* tab will be enabled.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and the mask of the sub-network to which the interface belongs, have to be indicated.

Here, several associated IP addresses and network masks may be defined for the same interface (the need to create aliases, for example). These aliases may allow you to use this Stormshield Network firewall as a central routing point. As such, a USB/Ethernet interface 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. Reloading the network configuration will apply this mask on the first address and a mask /32 on the following addresses.

Creating a 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.

GRETAP interfaces are configured via a wizard that allows you to create the interface easily.

Click on **Add** and **Add a GRETAP** interface. The following screen appears:

Global configuration

Name	Enter a unique name for your GRETAP interface.
Color	Color assigned to the GRETAP interface.

Interface configuration

Create a disabled GRETAP interface	If this option is selected, the GRETAP interface will be inactive and located outside the bridges defined on the firewall. This option allows preparing a GRETAP configuration before using it in a production environment.
Use an existing bridge	A drop-down list allows selecting the bridge to which the GRETAP interface will be attached.

Configuring the GRETAP tunnel

Tunnel source	Select the outgoing interface of traffic using the tunnel. In general, this would be the "out" interface of the bridge to which the GRETAP interface belongs.
Tunnel destination	Select the object representing the tunnel's remote endpoint. This is a host object that presents the public IP address of the remote firewall.

Modifying a GRETAP interface

A GRETAP interface is represented as a child node in relation to the bridge. A bridge may contain several child nodes.

You can change the parameters of each GRETAP interface. To do so, select a GRETAP interface located inside a bridge on the left-hand side of the window. Two tabs will then appear:

"Configuration of the interface" tab

Name (mandatory)	Name given to the GRETAP interface. (See warning in the introduction to the section on **Interfaces**)
Comments	Allows you to enter comments regarding the interface.
VLANs attached to the interface	List of VLANs attached to the selected interface. The appliance does not need to be systematically rebooted whenever a VLAN is deleted.
Color	Color assigned to the interface.

This interface is	An interface can either be “internal (protected)” or “external (public)”. If you select “internal (protected)”, you are indicating that this interface is protected. This protection includes the memorization of 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 (see the section *Implicit rules*). Protected interfaces are represented by a shield ( ). If you select “external (public)”, you are indicating that this part of the network is linked up to the internet. In most cases, the external interface, linked up to the internet, has to be in external mode. The shield icon disappears when this option is selected.

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

None (interface disabled)	By selecting/unselecting this option, the interface will be enabled/disabled. By disabling an interface, it becomes unusable. In terms of use, this may correspond to an interface to be used in the near or distant future, but which is not active. An interface which has been disabled because it is not in use is an example of an additional security measure against intrusions.
Dynamic IP (obtained by DHCP)	The assigned IP address can be matched to a domain name via a DNS service provider (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This option is used when your firewall does not have a static IP address (e.g., your service provider, or DHCP renews its IP address regularly). This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. *The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module.* This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the “DHCP” zone in the *Advanced properties* tab will be enabled.
Address range inherited from the bridge	If the interface is part of a bridge, the address range of the bridge can be retrieved.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and the mask of the sub-network to which the interface belongs, have to be indicated.

Here, several associated IP addresses and network masks may be defined for the same bridge (the need to create aliases, for example). These aliases may allow you to use this 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. Reloading the network configuration will apply this mask on the first address and a mask /32 on the following addresses.

"Advanced properties" tab

Physical (MAC) address	Since the GRETAP interface is contained in a bridge, it will have the same MAC address as the bridge. **NOTE** This field is grayed out when the interface belongs to a bridge. It can neither be modified nor deleted.

DHCP

NOTE

This option will be indicated as "disabled" if the option **Dynamic IP (obtained by DHCP)** was not selected in the *Configuration of the interface* tab and the options will be grayed out.

DNS name (optional)	Name of the DNS server (FQDN) for the connection. This optional field does not identify the DHCP server but the firewall. If this field has been entered and the external DHCP server has the option of automatically updating the DNS server, the DHCP server will automatically update the DNS server with the name and the IP address provided by the firewall. This name consists of 6 bytes in hexadecimal separated by :
Requested lease time (seconds)	Period during which the IP address is kept before renegotiation.
Request domain name servers from the DHCP server and create host objects	If this option is selected, the firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address. Two objects will be dynamically created in the object database upon the selection of this option: 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. **NOTE** This option will be disabled if the option **Dynamic IP (obtained by DHCP)** was not selected in the *Configuration of the interface* tab

Routing without analyzing

NOTE

This option will be indicated as "disabled" if the option **Address range inherited from the bridge** was not selected in the *Configuration of the interface* tab and the options will be grayed out.

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

NOTE

This option will be indicated as "disabled" if the option **Address range inherited from the bridge** was not selected in the *Configuration of the interface* tab and the options will be grayed out.

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. These cases are: • The reinitialization of connections induced by an alarm, • The SYN proxy (enabled in filtering), • Requests to resend packets dropped in order to speed up a scan, • Rewriting of packets by application scans (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. This option requires the activation of the previous option "**Keep initial routing**".
Gateway address	This field is used for routing by interface. All packets that arrive on this interface will be routed via a specified gateway.

Interface's throughput (for information only)

Backup appliance	Defines the debit on an interface. This is an automatic entry that is not compulsory: it is used for monitoring in the calculation of bandwidth.

Converting an interface to link aggregation (LACP)

This feature is only available on SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100 models.

The LACP (IEEE 802.3ad - Link Aggregation Control Protocol) feature allows improving the appliance's bandwidth while maintaining a high level of availability (link redundancy). Several physical ports on an appliance can be grouped together to be considered a single logical interface. Therefore, by aggregating *x* links, it will be possible to set up a link of *x* times 1 Gbps or 10 Gbps between two appliances.

NOTE

Ensure that the remote appliances are using LACP.

NOTE

The use of stackable switches is recommended as this would allow link redundancy between both appliances.

Click on **Add** in the toolbar and select **Convert to link aggregation (LACP)**.

An interface that is already in use in the configuration cannot be converted in aggregate form.

An interface converted in aggregate form becomes a virtual interface, allowing aggregation to be viewed and configured. The physical interface of this converted interface then becomes similar to any other interface added to the aggregate. These members are called “aggregated links”.

An interface converted in aggregate form keeps its settings. The converted interface will then have an additional tab called “Link aggregation (LACP)”. On the other hand, an interface that becomes an aggregate link loses its settings to inherit the configuration of the aggregate (except the name and Media settings).

Depending on the extension modules installed, the maximum possible aggregate is half of the total number of interfaces on the model. The maximum number of aggregated links is 8 interfaces, regardless of the model.

"Link aggregation (LACP)" Tab

Another way to include interfaces in an aggregation, apart from dragging and dropping, is to use the panel in this tab (Link aggregation (LACP)).

To move an available interface (interface that is not being used in the configuration) to the link aggregation, drag and drop it or use the red arrow in between both tables or double-click on the interface you wish to move.

To remove an interface from an aggregation, do the exact opposite.

Configuring an aggregated link

Enable aggregated interface	If this option is selected, the interface will become an “aggregated link”. All of these interfaces will then be considered one single logical interface. If this option is not selected, the interface will be disabled and rendered unusable. In terms of use, this may correspond to an interface to be used in the near or distant future, but which is not active. An interface which has been disabled because it is not in use is an example of an additional security measure against intrusions.

Name	Name of the interface. (See warning in the introduction to the section on **Interfaces**)
Physical port	List of Ethernet ports in the aggregation (Example: (Port2)
Aggregated to the interface	Name of the virtual, i.e., “aggregated” interface.

Media

Media	Connection speed of the network. By default the firewall detects this automatically but you can enforce the use of a particular mode. The different speeds available are: "Automatic detection", "10 Mb Half duplex", "10 Mb Full duplex", "100 Mb Half duplex", "100 Mb Full duplex", "1 Gb Half duplex", "1 Gb Full duplex". **Warning** 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.

LICENSE

The License screen consists of several sections:

- The *General* tab: manual or automatic installation of a license and display of main information.
- The *License details* tab (or in the case of high availability, a serial number such as Local License U70XXADA913500 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 tab per passive appliance in the case of high availability.

"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 allows ensuring 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 button **Install the license** file will validate the installation of the license file on the appliance. Information concerning your firewall will be modified and the new options will be enabled on the firewall.

REMARK

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 properties

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. Note : There are several different notifications: *"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, syslog and RealTime Monitor alerts as well as in Stormshield Network Event Analyzer logs. To enable the sending of these messages, go to the menu **Notifications**, **Logs-Syslog** or **SNMP Agent**.

"License details" tab

This tab displays the current valid license of the appliance to which you are connected.

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.

The table

Feature	Indicates the features and options of each feature found on the firewall. The features are: "Administration", "Date", "Flags", "Global", "Hardware", "Limit", "Network", "Proxy", "Service" and "VPN". The options relating to the features are explained in detail in the next section.
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.

Administration

Manager	Administration possible via the web interface. (Default value: 1).
Monitor	Monitoring possible via Stormshield Network REAL-TIME MONITOR (Default value: 1).

Date

Antispam	Deadline for updating DNSRBL spam databases
Antivirus	Deadline for updating ClamAV antivirus databases

ExpressWarranty	Deadline for the ExpressWarranty. This allows limiting the client's waiting time during the repair of his product.
NotAfter	Expiry date of the license.
NotBefore	Earliest date for using the license
ASQ	Deadline for updating ASQ patterns.
SPAMVendor	Deadline for updating the spam filter heuristic engine.
URLFiltering	Deadline for updating Stormshield Network's URL filter databases.
URLVendor	Deadline for updating Stormshield Network Extended Web Control URL filter databases.
Update	Deadline for updating the appliance.
VirusVendor	Deadline for updating Kaspersky antivirus databases.
VulnBase	Deadline for updating SEISMO vulnerabilities.
Warranty	Deadline for the warranty.

Flags

Clone	Enables/disables management/presence of the backup partition. (Default value: 1).
CustomPattern	Allows customizing ASQ models.
ExpressWarranty	Express warranty that allows limiting the client's waiting time during the repair of his product.
ExternalLDAP	Enables or disables the use of an LDAP directory (Default value: 1*)
HAState	Allows defining an active and passive appliance in a high availability cluster. (Master/Slave/None).
PKI	Enables or disables the internal PKI. (Default value: 1)
PVS	Enables or disables SEISMO. (Default value: 0)

Global

Comment	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.

Hardware

CryptCard	Presence of an optional cryptographic card. (Default value: depends on the model).
Networkif	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.

Limit

Conn	Maximum number of connections passing through ASQ. (Default value: 0 (= unlimited)).
Network	Maximum number of networks managed by ASQ. (Default value: 0 (= unlimited)).
User	Maximum number of users who can authenticate on the appliance. (Default value: 0 (= unlimited)).

Network

HADialup	Enables or disables the possibility of using dialups to establish high availability links. (Default value: 1).

HybridMode	Enables or disables hybrid mode on interfaces (mix of interfaces, bridges, VLANs, etc). (Default value: 1*).
InterfaceRoute	Allows routing by interface. This option is enabled by default. See the Menu: **Configuration** > **Network** > **Interfaces** / *Advanced properties* tab/ **Bridge: routing by interface** (Default value: 1).
LBDialup	Enables or disables load-balancing on dialups. (Default value: 1).
QoS	Enables or disables QoS. (Default value: 1).
VLAN	Enables or disables VLANs (Default value: 1).

Proxy

Antispam	Enables or disables spam filtering via DNSRBL in the proxy. (Default value: 1).
Antivirus	Enables or disables the ClamAV antivirus in the proxy. (Default value: 1).
FTPProxy	Enables or disables the FTP proxy. (Default value: 1**).
HTTPProxy	Enables or disables the http proxy (Default value: 1).
ICAPURL	Enables or disables the ICAP ReqMod. (Default value: 1).
ICAPVirus	Enables or disables the ICAP RespMod. (Default value: 1).
IMAPProxy	Enables or disables the IMAP proxy (which does not exist on UTMs). (Default value: 1).
POP3Proxy	Enables or disables the POP3 proxy. (Default value: 1).
SMTPProxy	Enables or disables the SMTP proxy. (Default value: 1).
SpamVendor	Enables or disables the spam filter heuristic engine. (Default value: 0).
URLFiltering	Enables or disables URL filtering via Stormshield Network's database in the proxy. (Default value: 1).
URLVendor	Enables or disables URL filtering via Stormshield Network Extended Web Control database in the proxy. (Default value: 0).
VirusVendor	Enables or disables the Kaspersky antivirus in the proxy. (Default value: 0).

Department

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).
DynDNS	Enables or disables the DynDNS client of the DNS update server.
Enrolment	Enables or disables enrolment. (Default value: 1).
LDAPBase	Enables or disables the internal LDAP database (Default value: 1).
NTP	Enables or disables NTP synchronization (Default value: 1).
PublicLDAP	Enables or disables public access to the internal LDAP (Default value: 1*).
SNMP	Enables or disables the SNMP agent. (Default value: 1*).

VPN

Anonymous	Enables or disables the possibility of setting up anonymous tunnels. (Default value: 1*).
PPTP	Enables or disables PPTP tunnels. (Default value: 1*).
SSL	Enables or disables SSL VPN.
StrongEnc	Enables or disables support for strong algorithms for the encryption of IPSec tunnels. (Default value: 1*).
Tunnels	Maximum number of IPSec tunnels. (Default value: 0 (=unlimited)).

This tab works in the same way as the local license tab.

LOGS - SYSLOG - IPFIX

The log configuration screen consists of 3 tabs:

- *Local storage*
- *Syslog*
- *IPFIX*

"Local storage" tab

The configuration of logs allows allocating disk space for each type of log on the firewall. This menu also allows modifying the firewall's behavior when saving these logs.

This screen is divided into 2 sections:

- Top: a menu setting out the various options
- Bottom: a table

NOTE

This tab will be grayed out if the firewall is a model that does not have a hard disk. In this case, when the module is opened, the *Syslog* tab will appear.

This button makes it possible to enable or disable log storage on the hard disk or on an SD card (S series firewalls).

Storage device

You have the option of using as a storage medium:

- Your firewall's internal hard disk – **6 GB internal support** option
- An **SD card** for firewalls in the "S" Series and by subscribing to the "external storage" option.

NOTE

For more information, refer to the Guides **PRESENTATION AND INSTALLATION OF NETASQ PRODUCTS U SERIES – S Models** or **PRESENTATION AND INSTALLATION OF STORMSHIELD NETWORK PRODUCTS SN Range,** available on Stormshield's Technical Documentation website.

When storage device is saturated, the most recent logs will erase the oldest logs.

Refresh Refreshes the list of storage media

Format Formats the storage medium in a specific format

Whenever the medium is full (no more space available), logs will automatically be rotated, so the most recent logs will erase the oldest ones.

NOTE

When the firewall is in high availability, actions relating to the SD card are only valid for the card inserted into the active firewall. To perform operations on the passive firewall's SD card, you will need to switch the remote firewall to active mode using the **Maintenance** module, then go back to the menu **Logs–Syslog** to be able to make changes to the SD card.

Configuration of the space reserved for logs

The firewall manages a certain number of log files intended for collecting events detected by the log functions. The files involved in security events are:

- **Alarms**: events relating to the application of intrusion prevention features (l_alarm),
- **Authentication**: events relating to user authentication (l_auth),
- **Network connections**: events relating to connections through and to the firewall (l_connection),
- **Filter policy**: events relating to the application of filter functions (l_filter),
- **FTP proxy**: events relating to FTP traffic (l_ftp),
- **Statistics:** events relating to real-time monitoring (l_monitor),
- **Application connections (plugin)**: events relating to the treatment of ASQ plugins (l_plugin),
- **POP3 proxy:** events relating to message sending (l_pop3),
- **Vulnerability manager:** events relating to the application for consulting vulnerabilities on the Stormshield Network Vulnerability Manager network (l_pvm),
- **Sandboxing**: events relating to the sandboxing of files if this option has been subscribed and enabled (l_sandboxing),
- **Administration (Serverd)**: events relating to the firewall administration server: "serverd" (l_server),
- **SMTP proxy**: events relating to SMTP traffic (l_smtp),
- **System events**: this is the log in which events directly relating to the system are logged: shutdown/startup of the firewall, system error, etc. Shutting down and starting log functions correspond to shutting down and starting the daemons that generate logs (l_system),
- **IPSec VPN**: events relating to the establishment of SAs (l_vpn),
- **HTTP proxy**: events relating to HTTP traffic (l_web),
- **SSL VPN**: events relating to the establishment of the SSL VPN (l_xvpn),
- **SSL proxy**: events relating to SSL traffic (l_ssl),

The files share a common storage area with other log files.

For each log menu (Alarms, Authentication, Network connections, Filter policy, FTP proxy, Statistics, Application connections (plugin), POP3 proxy, Applications and vulnerabilities (SEISMO), Server, SMTP proxy, System events, IPSec VPN, HTTP proxy, SSL VPN), you can restrict the size of the log file by selecting the size of the file as a percentage of the total space reserved for log files.

The table sets out the following columns:

On	Allows enabling/disabling the log file. If this line is unselected, the percentage will be 0. In this case, the type of log will not be stored on the disk. If the line is selected, the default percentage indicated will be 1%.
Family	Name of the log file
Percentage	Current percentage of space occupied. By clicking in a box, the percentage can be modified.
Disk space quota	Proportion of the disk space that each file occupies on the disk, which varies according to the percentage specified.

The total percentage is shown at the bottom right side of the table. If the total exceeds 100%, a warning line will be indicated in red at the bottom of the table. (Example: *"Warning, incorrect distribution:* 113% of the available space has been reserved). Modifications are however allowed.

By clicking on **Apply**, the following message will appear: "The total disk space reserved for logs exceeds this model's capacity. Apply this configuration?". ". You can force the save or cancel,.

NOTE

These files can be copied on the Stormshield Network EVENT ANALYZER solution in order to create reports or archive them.

"Syslog" tab

The *Syslog* tab allows configuring up to 4 profiles for sending logs to Syslog servers.

You can send logs to the Stormshield Visibility Center (SVC) server, Stormshield's monitoring solution, in Syslog format. Please refer to the *SVC administration guide* that you will find on the Stormshield Technical Documentation website.

Logs are in UTF-8 text format following 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).

Table of Syslog profiles

The table that presents the profiles consists of 2 columns:

State	Double-clicking on this allows enabling or disabling the profile.
Profile	Displays the name of the Syslog profile

Configuring a profile

Details

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).
Certification authority	This field will only be active when the protocol selected is TLS. Indicate the certificate 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.
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.

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 TCP or TLS. In this case, a server can be specified, to which Syslog messages will be sent in the event the nominal server is unavailable. 10 minutes after having switched its traffic to the backup server, the firewall will attempt to contact the nominal server again. In the event of a failure, the firewall will continue to send its traffic to the backup server while regularly retrying to contact the nominal server.
Backup port	This field will only be active when the protocol selected is TCP or TLS. This is the listening port of the backup Syslog server.
Category (facility)	Number added to the beginning of a log line. It can be used to differentiate several firewalls appliances when they send their logs to the same Syslog server.

Logs enabled

This table allows selecting the type of logs that need to be sent to the Syslog server.

Status	Makes it possible to enable the sending of the selected log file.
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. Four templates are defined by default: • IPv4 connections without address translation (NAT), • IPv4 connections with NAT, • IPv6 connections, • alarms. These templates define whether information contained in alarm (l_alarm), connection (l_connection), intrusion prevention plugin (l_plugin), or packet filtering (l_filter) log files will be sent.
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

The **Maintenance** module will allow you to modify settings and perform the necessary checks to ensure that your appliance runs smoothly.

It is possible, via the interface, to set up a secure configuration of your firewall, to back up and update your system, as the 4 following tabs show:

- UPDATING THE system
- Save
- Restore
- Configuration

"Configuration" tab

System disk

This refers to the system disk of your Stormshield Network multifunction firewall.

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.

Upon startup, use the: select the product's startup partition – the main or backup partition.

Main partition	If this option is selected, your firewall will use this partition at startup.
Backup partition	The backup partition represents your last backed up partition. Select this option if you wish to use it when your firewall starts up.
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 will allow 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.

"Backup" tab

Configuration backup

Through this screen, you will be able to create a comprehensive backup of your firewall's configuration in the form of files, and protect access to it.

Backup filename	The name of the backup will correspond to "<firewall serial number>_day_month_year.na" by default, but can be modified. You are however advised to use the ".na" extension for the name of this file.
Download	The file will be saved in .na format (Stormshield Network ARCHIVES). Click on this button to save it.

Advanced properties

Password	Define a password to protect your backup.
Confirm	Confirm the password of your backup, entered in the previous field.
Mandatory password strength.	This field 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.

Configuration automatic backup

Regular backups of your configuration are now offered with the "Cloud backup" service. These backups can be saved on a local or outsourced HTTP/HTTPS server or within the infrastructure offered by the **Stormshield Network Cloud backup** service.

These regular backups are saved in a secure environment.

NOTE

You are advised to protect the backup file with a password that must be kept in a safe place, as technical support will not be able to retrieve or reinitialize it if it is forgotten.

Information regarding the latest automatic backup is also available in the **Dashboard**'s *Properties*.

NOTE

The firewall must be covered by a valid maintenance contract in order to be eligible for this service.

Automatic Database Backup	When selected, this checkbox allows a backup of your firewall's configuration to be sent regularly.

The various parameters of the service are:

Backup server selection	**Cloud backup**	These backups are stored in the cloud service infrastructure using encrypted channels.
	Customized server	These backups are stored on a customized server, depending on the criteria defined below.
Server's URL	Location used for storing backups. This URL is defined by the resolution of the Cloud server or customized server selected below combined with the access path indicated hereafter.	
Backup server	Selects a customized server. Ensure that the resolution of the selected server corresponds to the one expected.	
Name of the backup file	Enter the name of the backup file that will be sent to your server. You are advised to use the ".na" extension for the name of this file.	
Server port	Server's listening port for receiving backups.	
Communication protocol	Protocol used for sending backups, which may be HTTP or HTTPS. For HTTPS, a certificate needs to be entered so that the firewall may confirm the identity of the server.	
Server certificate	If HTTPS has been chosen, import then select the server certificate in this field, so that the firewall can authenticate it. The aim of this is for the firewall to confirm the identity of the server before sending it the backup.	
Access path	Depending on the sending method selected above, this access path for data on the server 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.
User name (auth)	If a sending method with identification is used (*auth basic* or *auth digest*), this user name will allow the server to authenticate the firewall.	
Password (auth)	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.	

Depending on whether you have chosen *Cloud auto-backup* or a backup on a customized server, you will be able to select the following parameters:

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	If you wish to do so, you can encrypt your configuration file with a password. You are advised to use a complex password. **IMPORTANT** You are advised to keep your password in a safe place, as files cannot be restored without it. Furthermore, after the backup, you will not be able to change or reinitialize it.
Change the password	This button allows displaying a window to edit the password. This new password will only be valid for subsequent backups.

"Restore" tab

Restore configuration

This window allows you to restore a backup that was made earlier.

Select a backup to restore:

Select a backup file	Click on the button to the right of the field ( ) in order to insert the backup file to be restored in .na format.
Restore the configuration from the backup file	Next, click on this button in order to proceed to the restoration of 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 in the previous tab, Backup, enter it in this field.

Modules to be restored: it is possible to perform a partial or full restoration of your firewall's configuration.

Restore all modules of the backup file	This option is selected by default. If you choose to keep it that way, all modules contained in the backup file will be restored.

If you wish to restore only some of the modules of the backup file, unselect the option above in order to enable the following fields.

Select the configurations you wish to restore from:

- Network (interface, routing and dynamic DNS)
- SMTP Filtering
- URL filtering
- SSL filtering
- Web objects
- Global modules
- Secure configuration
- Active Update
- Services (SNMP, DHCP server),
- IPS Inspection profiles
- Network objects
- Filtering and NAT
- IPSec VPN
- LDAP directory

Automatic backup restoration

Date of the latest backup	Date of the latest backup of your configuration, available on the local or external server.

Advanced properties

Backup password	If you have protected the selected backup with a password in the previous tab (Backup), enter it in this field, otherwise any restoration of the file will be impossible.

"System update" tab

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: Updating a Stormshield Network firewall cluster.

Available updates:

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.

Select the update:

Select an update file	Select the firewall update to be installed and insert it in the field using the button ... . The SHA1 fingerprint of the update file is displayed when you click on the link with its name. When a new firmware version is available, the **Release Notes** link will enable the user to download the version release notes applicable to the firmware version offered for download.
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 appliance will reboot and update the firewall version
Update firmware	Apply the selected update on your appliance by clicking on this button.

NOTE

In case of High availability cluster, if you choose installation on both firewalls, the upgrade will be applied only to the remote firewall, to prevent your network from becoming inaccessible. Proceed as follows to enable this upgrade on your active firewall:

1. Ensure that the upgrade of the passive firewall on the **Dashboard** (Hardware component) screen is complete.
2. Go back to the **Maintenance** module, *System upgrade* tab and select "This firewall" as the Firewall to be upgraded,
3. In advanced properties, select the option "Enable the firmware downloaded earlier" then click on Upgrade the firewall.

A switch will take place and your passive Firewall will become active.

Advanced properties

Action

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. **NOTE** If a file is present, the version indicated will be present 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.

MONITORING

The **Monitoring** module offers graphs and data in real time (history graphs may be added to these 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,
- routes 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.

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 "Full access to logs (sensitive data)" privilege by clicking on "**Restricted access to logs**" (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 "**Full access to logs (sensitive data)**" 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 "Full access to logs (sensitive data)" privilege is obtained or released, it will generate an entry in logs.

NOTE

For SN160(W), SN210(W) and SN310 models, you can obtain the full feature by using an external storage medium such as an SD card and by subscribing to the "external storage" option (refer to the module **Logs – Syslog**). Only the SD format is compatible: Micro SD or Nano SD cards fitted with an adapter are not supported.

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

This module presents various indicators on the firewall's operation in the form of graphs or tables:

- CPU load,
- Memory use,
- CPU consumption of each service enabled on the firewall,
- System date and time,
- Uptime since the last startup.

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.
Remove a column	This button makes it possible to reduce the number of columns to be displayed for curves and other information.
Go to monitoring configuration	This link allows you to go directly to the monitoring configuration module (refreshment intervals).

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 shows a history graph of the firewall's CPU consumption.

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.

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).

Interfaces monitoring

"Real time" tab

This module presents two indicators in the form of graphs for each network interface 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 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 interface.
Remove a column	This button makes it possible to reduce the number of columns to be displayed 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**).
Go to monitoring configuration	This link allows going directly to the configuration module of 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.
- 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 and the number of packets accepted/blocked for each monitored interface (except for VLANs).

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 interface.
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).

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

This screen consists of 2 views:

- A view listing the hosts
- A view listing Connections, Vulnerabilities, Applications, Services, Information and Reputation history relating to the selected host.

"Hosts" view

This view shows all hosts detected by the firewall. Every row represents a host.

The "Hosts" view displays 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 logs,
- Check usage of this host,
- 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.

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 for certain Views, predefined filters. 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.

"Connections" view

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	Certain 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 and 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. 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 a line in this view 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 for certain Views, predefined filters. 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 or IP address (grayed out if a host has been selected in the "hosts" view).
	  • By interface
	  • By source interface
	  • By destination interface
	  • By destination port
	  • By protocol
	  • By user
	  • 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 filter rule name
	  • By IPS profile.
	  • By geographic source or destination.
	  • If the **See all connections (closed or reinitialized connections, etc.)** checkbox has been selected, all connections will be displayed in the table, regardless of their status.
	• 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 display only columns suggested by default when 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.

"Vulnerabilities" view

For a selected host, this tab will describe the vulnerabilities detected. Each vulnerability can then later be viewed in detail. Scrolling over a vulnerability will display a link to a page providing a description of the vulnerability.

The "Vulnerabilities" view displays the following data:

Identifier	Vulnerability ID
Name	Indicates the name of the vulnerability.
Family	Number of hosts affected.
Severity	Indicates the severity level of the vulnerability. There are 4 levels of severity: "**Low**", "**Moderate**", "**High**", "**Critical**".

Exploit	Access may be local or remote (via the network). It allows exploiting the vulnerability.
Workaround	Indicates whether a workaround exists.
Level	The alarm level associated with the discovery of this vulnerability.
Port	The network port on which the host is vulnerable (e.g. 80 for a vulnerable web server).
Service	Indicates the name of the vulnerable program (e.g.: lighthttpd 1.4.28)
Assigned	Indicates the date on which the vulnerability was detected on the host
Details	Additional information about the vulnerability.

Right-click menu

Right-clicking on the name of the vulnerability opens the following pop-up menus:

- Search for this value in logs,
- Add the host to the objects base and/or add it to a group.

"Application" view

For a selected host, this tab will describe the applications detected.

The "**Application**" view displays the following data:

Product name	Name of the application.
Family	Application family (e.g. Web client).
Details	Full name of the application including its version number.

Right-click menu

Right-clicking on the name of the product opens the following pop-up menus:

- Search for this value in logs,
- Add the host to the objects base and/or add it to a group.

"Services" view

For a selected host, this tab will describe the services detected.

The "**Services**" view displays the following data:

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).

"Information" view

This tab provides information relating to a given host.

The "**Information**" view displays the following data:

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).

Right-click menu

Right-clicking on the name opens the following pop-up menus:

- Search for this value in logs,
- Add the host to the objects base and/or add it to a group.

"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	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.

Interactive features

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.

"History" tab

This view shows in the form of graphs how the reputation of the selected host has evolved (average reputation and maximum reputation).

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.
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.

Scrolling over a curve with a mouse will display the value of the indicator and corresponding time in a tooltip.

Users

"Real time" tab

This screen consists of 2 views:

- A view listing the users authenticated on the firewall.
- A view listing Connections, Vulnerabilities, Applications, Services and information regarding the selected user.

"Users" view

This view shows all the users authenticated on the firewall. Every row represents a user.

The "**Users**" view displays the following data:

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.
Expiry date	Remaining authentication time for the user's session
Auth. method	Method used for authenticating the user (e.g. SSL)
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 Portal	A green check in this checkbox means that the user is allowed to log on to the SSL VPN portal in order to access web servers.
SSL VPN Portal - Java applet	A green check in this checkbox means that the user is allowed to log on to the SSL VPN portal in order to access application servers via a Java applet.
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 SSL 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

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 deleting the selected criteria.

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
	• 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 configuration of authentication (**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.

"FILTER" panel

You can add a criterion by dragging and dropping the value from the results field into the panel.

"Connections" view

This view shows all connections detected by the firewall for a selected user. 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.
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. 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 of the source or destination host opens the following pop-up menus:

- 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 or by IP address
	  • By interface
	  • 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 the **See all connections (closed or reinitialized connections, etc.)** checkbox has been selected, all connections will be displayed in the table, regardless of their status.
	• 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 display only columns suggested by default when 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.

"Vulnerabilities" view

This tab describes the vulnerabilities detected on the host on which the selected user is connected.

The "**Vulnerabilities**" view displays the following data:

Identifier	Vulnerability ID
Name	Indicates the name of the vulnerability.
Family	Number of hosts affected.
Severity	Indicates the level of severity on the host(s) affected by the vulnerability. There are 4 levels of severity: "**Low**", "**Moderate**", "**High**", "**Critical**".
Exploit	Access may be local or remote (via the network). It allows exploiting the vulnerability.
Solution	Indicates whether a workaround exists.

Level	The alarm level associated with the discovery of this vulnerability.
Port	The network port on which the host is vulnerable (e.g. 80 for a vulnerable web server).
Service	Indicates the name of the vulnerable program (e.g.: lighthttpd_1.4.28)
Assigned	Indicates the date on which the vulnerability was detected on the host
Details	Additional information about the vulnerability.

Right-click menu

Right-clicking on the name of the vulnerability opens the following pop-up menus:

- Search for this value in logs,
- Add the host to the objects base and/or add it to a group.

"Application" view

This tab describes the applications detected on the host on which the selected user is connected.

The "**Application**" view displays the following data:

Product name	Name of the application.
Family	Application family (e.g. Web client).
Details	Full name of the application including its version number.

Right-click menu

Right-clicking on the name of the product opens the following pop-up menus:

- Search for this value in logs,
- Add the host to the objects base and/or add it to a group.

"Services" view

This tab describes the services detected on the host on which the selected user is connected.

The "**Services**" view displays the following data:

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).

"Information" view

This tab describes the information relating to the host on which the selected user is connected.

The "**Information**" view displays the following data:

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).

Right-click menu

Right-clicking on the name of the product opens the following pop-up menus:

- Search for this value in logs,
- Add the host to the objects base and/or add it to a group.

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.
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 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 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. 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 deleting the selected criteria.

Filter	Click on this button to:
	• Select filter criteria (**Search criterion**). For the "**connections**" view, the criteria are the following:
	  • By address range or by IP address
	  • By interface
	  • 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.

Routing

"Real time" tab

This view 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. The "**Connections**" view displays the following data:

Type	Indicates the type of route in which the gateway is used (e.g. PBR, DefaultRoute, etc)
Name	Name of the router or gateways that make up a router object.
Status	Indicates the status of each gateway. There are three possible values: • **Active**: when the gateway is in use, • **On standby**: when it is a backup gateway, • **Not reachable**: the gateway is not responding to pings
IP version	IP version used on the gateway (4 or 6).
IP address	IP address of the gateway.
Main/backup	Indicates whether the gateway is in use (main) or is a backup gateway.
Last checked	Date and time the gateway was last pinged.
Last status change	Date and time the gateway's status was last changed (main/backup).
Active	Indicates whether the gateway is available for use.
Available since	Time elapsed since the gateway's availability was last changed.
Default gateway	Indicates whether the router is used as the firewall's default gateway.
Default gateway last changed on	Date and time the default gateway was last changed
Router ID	Router's unique identifier
Fairness	Indicates the percentage of the gateway used in the router object.

Possible actions

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.

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" table

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.
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" table

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 set up 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" table

The "Policy" table displays the following data:

Filter	The Search field enables data to be filtered according to alphanumeric characters that belong to any column in the table.

Hide established tunnels to display only policies with issues.	This button makes it possible to hide IPSec tunnels that have been correctly set up. Only tunnels that cannot be successfully set up remain displayed.
ID	This system ID allows you to link security policies (SP) to security associations (SA).
Local network	Network of local hosts that communicate through the selected tunnel (traffic endpoint).
Local network name	Name of the object corresponding to the local network
Local gateway	IP address that the local firewall presents to set up the tunnel (tunnel endpoint).
Local gateway name	Name of the object corresponding to the local gateway.
Direction	Direction of network traffic in the tunnel.
Remote gateway	IP address that the remote firewall presents to set up one or several tunnels with the local firewall (tunnel endpoint).
Remote gateway name	Name of the object corresponding to the remote gateway.
Remote network	Network of remote hosts that communicate through the selected tunnel (traffic endpoint).
Remote network name	Name of the object corresponding to the local network
Lifetime	Lifespan of the configured VPN policy.
Status	A green or red LED indicates whether a tunnel has been set up.

Right-click menu

Right-clicking on the address or name of a network (local or remote) opens the following pop-up menus:

- Search for this value in the "All logs" view,
- Show host details

Right-clicking on the address or name of a gateway (local or remote) opens the following pop-up menus:

- Search for this value in the "All logs" view.

"Tunnels" table

The "Tunnels" table displays the following data:

Display only tunnels matching the selected policy	If this checkbox is selected, only tunnels matching the selected policy in the "Policies" table will be displayed.
Local gateway	IP address that the local firewall presents to set up the selected tunnel (tunnel endpoint).
Local gateway name	Name of the object corresponding to the local gateway.
Remote gateway	IP address that the remote firewall presents to set up the selected tunnel (tunnel endpoint).
Remote gateway name	Name of the object corresponding to the remote gateway.
Lifetime	Life span of the SA (Security Association) for the tunnel concerned.
Bytes	Number of bytes exchanged in the selected tunnel.
Status	Indicates the status of the tunnel. (Example: Mature).
Encryption	Name of the encryption algorithm
Authentication	Name of the authentication algorithm

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,
- SN Real-Time Monitor.

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 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 whose properties 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 deleting the entry and listing all objects according to the current filter.

NOTE
When you go to the *Objects* tab in the menu directory on the left, the focus will now be on the search field.

Add

When you click on this button, a dialog box will appear, offering to create an object, by indicating its type and the information relating to it in the relevant fields.

REMARK
The object can be defined as a "global" object at the moment of its creation 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 download link of 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 in order to import it into the firewall. The fields that make up a row in a CSV file are set out in the section Structure of an objects database in CSV format. A gauge will allow you to view the progress of the transfer of the database to the firewall. **NOTE** Objects already found on the firewall will be replaced with the corresponding transferred objects.
Collapse all	This button allows expanding all folders in the interface directory.
Expand all	This button allows collapsing all folders in the interface directory.

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 object).

Filter

This button allows selecting which object types to display. A drop-down menu will offer you the following choices:

All objects	Represented by the icon, this option allows displaying all types of network objects in the list of objects on the left.
Host	Represented by the icon, this option allows displaying only “host” objects in the column on the left.
DNS name (FQDN)	Represented by the icon, this option allows displaying only “DNS name (FQDN)” objects in the column on the left.
Network	Represented by the icon, this option allows displaying only “network” objects.
IP address range	Represented by the icon, this option allows displaying only IP address ranges.
Router	Represented by the icon, this option allows displaying only router objects.
Group	Represented by the icon, this option allows displaying only network groups.
IP protocol	Represented by the icon, this option allows displaying only IP protocols.
Port – port range	Represented by the icon, this option allows displaying ports and port ranges.
Port group	Represented by the icon, this option allows displaying only port groups.
Time object	Represented by the icon, this option allows displaying only time objects.
Region group	Represented by the icon, this option allows displaying only geographic groups.

The various types of objects

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.

Network

Select a network to view or edit its properties. Each network has a name, IP address and network mask.

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**.
Comments	Description of the selected network.
IP address	IP address of the selected network. The address is followed by a "/" and the associated network mask.

IP address range

Select an IP address range 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**.
Start	First IP address of the range.
End	Last IP address of the range.
Comments	Description of the selected IP address range.

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.

IP protocol

Name of the object	Name of the selected IP protocol. This field is grayed out and cannot be modified.
Protocol number	Number associated with the selected IP protocol and provided by the IANA (Internet Assigned Numbers Authority).
Comments	Description of the selected IP protocol.

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	This button contains a dialog box for adding objects to the group. Two columns will appear: 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, select it in the right column and 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.

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	This button contains a dialog box for adding ports 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 ports in the group. Two columns will appear: 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, select it in the right column and 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.

Router

Router objects can be used:

- As the firewall's default gateway,
- For specifying the type of routing in filter rules (PBR: Policy Based Filtering).

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.

Select a router to view or edit its properties.

Name of the object	Name given to the router object when it was created.
Comments	Description associated with the router object.

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.
Apply	Sends 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.

Tables of gateways used and backup gateways

Both of these tables contain the following columns:

Host (Mandatory)	Clicking on this column will open the objects database to allow selecting a host that acts as the router.
Device(s) for testing availability (Mandatory)	Host or host group to ping 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** If the value **No availability testing** has been selected for all gateways, the function enabling a switchover to backup gateways will then be disabled.
Weight	Allows assigning a priority 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.
(Optional) 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.

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, select it in the right column and 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 countries or continents in your group will be shown in a table. To add or modify objects, refer to the previous field.

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**.
IP address	IP address of the selected object.
Comments	Description of the selected DNS name.

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**.

PPTP SERVER

The screen for configuring the PPTP server consists of 2 zones:

- **General configuration**: Activation of the PPTP server, selection of the address pool.
- **Advanced properties**: Traffic encryption.

Setting up the server is very quick and simple, and takes place in three steps:

- The IP addresses of PPTP clients (object).
- Encryption parameters.
- The DNS server and WINS server.

General configuration

Enable PPTP server	Enables the configuration of the **PPTP** server on the firewall. This can be done by selecting the option **Enable PPTP server**.
IP addresses of PPTP clients (object) (mandatory)	Once the PPTP server has been enabled, a pool of private IP addresses must be created. The firewall will then assign available IP addresses from the pool to clients who connect in **PPTP**. A host group must be created, containing reserved addresses or an address range from the object database.

Parameters sent to PPTP clients

DNS Server	The field **DNS server** allows sending the IP address of the DNS server to the client.
WINS server	The field **WINS server** allows sending the IP address of the WINS server to the client.

REMARK

The characters "_", "-", and "." are allowed for PPTP user names

Advanced configuration

Traffic encryption

The possible encryption parameters are:

Do not encrypt	This will disable the field **Accept only encrypted traffic and allow the following algorithms** as well as the MPPE offered.
Accept only encrypted traffic and allow the following algorithms	Allows the connection only if the client encrypts data.
40-bit MPPE	Allows the use of the 40-bit MPPE encryption protocol.
56-bit MPPE	Allows the use of the 56-bit MPPE encryption protocol.
128-bit MPPE	Allows the use of the 128-bit MPPE encryption protocol.

PREFERENCES

This module is accessible via the button in the top row of the interface.

It will allow you to manage the parameters of your web interface.

Depending on your selection of options, you will be able to save time and browse more easily.

Logon 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 You can also choose to "Always remain connected".
Systematically display the last active module at startup	If this option is selected, every time you log on, you will be redirected to the last module displayed before you were disconnected.

Application settings

Always display advanced properties	The elements of advanced properties can be expanded in every module that has them, 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 (Filter, NAT and IPsec VPN)	If this option is selected, during connections to the **Filter and NAT (Security policy)** and **IPsec VPN (VPN)** 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.
Comments about rules with creation date (Filtering and NAT)	If this option is selected, comments created for filter and NAT rules will automatically include the date and time of creation.

Display the security policy	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.

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 allows cancelling your actions if you have made a wrong move or if you decide not to continue with your configuration. A confirmation window will appear, allowing you to confirm or cancel your action.

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.
Administration suite URL	This URL allows you to download the Stormshield Network administration suite: Monitor, Reporter, and GlobalAdmin.

Log settings

Show the "Logs" menu	This checkbox allows the **Logs** menu to be displayed in the **Logs - Audit logs** module. This menu is hidden by default.
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.

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:
  - IP protocols (ICMP, IP, SCTP and TCP-UDP),
  - Instant messaging,
  - 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 scan, 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: • **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. 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.

Secure protocol: 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 set off two successive scans:

- 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 in the case of a NAT policy, address translation will be applied to the traffic leaving the proxy scan. 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 for enabling log generation for TCP connections.
Log every UDP pseudo-connection	Option for enabling 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).
Certificate authority password	Enter the password of the selected certificate 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 in the case of a NAT policy, address translation will be applied to the traffic leaving the proxy scan. This option will not be applied on translations of the destination.

Customized certificate authorities

Add the list of customized CAs to the list of trusted authorities	This option enables the feature for importing certificate 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** certificate authorities by clicking on the corresponding buttons.

Public certificate authorities

A public certificate 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 corresponding buttons.

In order to improve monitoring, these root certificate authorities are kept up to date in the firewall's list via **Active Update**.

Trusted certificates

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.

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.

ICQ – AOL IM (OSCAR)

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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 every OSCAR query	Enables or disables the generation of logs relating to OSCAR queries.

Live Messenger (MSN)

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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 has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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	This value has to 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

MTU

Impose MTU limit (force fragmentation)	MTU (Maximum Transmission Unit) represents the maximum size of an IP packet. If this option is selected, you will enable the next field and 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 has to be between 140 and 65535 bytes.
Session will expire in (seconds)	This period has to be between 2 and 30 seconds.

NOTE

The IP protocol does not have a profile.

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 analysis of the SCTP protocol will be disabled and traffic will be allowed 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"

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.

Protection against denial of service attacks

Maximum number of simultaneous connections for a source host (0 disables protection)	This option allows restricting the number of simultaneous connections for a single source host. When the selected value is 0, no restrictions will be applied. **WARNING** Choosing a number that is too low may prevent certain applications from running or web pages from displaying.
Maximum number of new connections for a source host in the interval defined (0 disables protection)	This option allows restricting the number of new connections initialed by a source host within a defined interval. When the selected value is 0, no restrictions will be applied. **WARNING** Choosing a number that is too low may prevent certain applications from running or web pages from displaying.
Interval during which new connections are limited	Define the reference interval to calculate the number of new connections allowed for each source host. This value has to be between 1 and 3600 seconds.

Timeout (in 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 time, in seconds, the state of an idle connection is kept (default value: 1800 seconds).
UDP connection	Maximum time, in seconds, the state of an idle UDP pseudo-connection is kept. It has to be between 30 and 3600 (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 10 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.

BACnet/IP

Service management

"Confirmed services" tab

This table lists the IDs and associated confirmed BACnet/IP services (services that require a reply) that have been predefined on the firewall. These codes are classified by service set (*Service choice*): Alarm and Event, File Access, Object Access, Remote Device Management, Virtual Terminal et Security.

Predefined confirmed BACnet/IP services are allowed by default (*Analyze* action) and this action can be modified for each one of them. The buttons **Block by service set**, **Analyze by service set** and **Modify all services** allow modifying the action (*Analyze / Block*) applied to the selected service set or to all BACnet/IP services listed in the table.

Other confirmed services

This list allows authorizing additional confirmed BACnet/IP service IDs 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.

"Unconfirmed services" tab

This table lists the IDs and associated unconfirmed BACnet/IP services (services that do not require a reply) that have been predefined on the firewall.

Predefined unconfirmed BACnet/IP services are allowed by default (*Analyze* action) and this action can be modified for each one of them. The **Modify all services** button allows modifying the action (*Analyze / Block*) applied to all BACnet/IP types listed in the table.

Other unconfirmed services

This list allows authorizing additional unconfirmed BACnet/IP service IDs 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 BACnet/IP protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log every BACnet/IP query	Enables or disables the logging of BACnet/IP requests.

CIP

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 has to 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 (*Analyze / Block*) applied to each service can be modified by clicking in the **Action** column. The **Modify all services** button allows modifying the action (*Analyze / 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 (*Analyze* action). These services are classified by service group: Acknowledge Handler Object, Assembly Object, Connection

Configuration Object, Connection Manager Object, Connection 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 and Time Sync Object.

The buttons **Block by service set**, **Analyze by service set** and **Modify all services** allow modifying the action (*Analyze / 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

EtherNet/IP settings

Max. number 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 (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).

EtherNet/IP command management

Public commands

This list sets out the public EtherNet/IP functions allowed by default on the firewall. The action (*Analyze / Block*) applied to each command can be modified by clicking in the **Action** column. The **Modify all commands** button allows modifying the action (*Analyze / Block*) applied to all commands.

Other commands allowed

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 every EtherNet/IP query	Enables or disables the logging of EtherNet/IP requests.
Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

IEC 60870-5-104 (IEC 104)

Settings

Maximum number 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 (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*: System information, Settings and Process information.

These public type identifiers are allowed by default (*Analyze* action). The buttons **Block by Type ID set**, **Analyze by Type ID set** and **Modify all Type IDs** allow modifying the action (*Analyze / Block*) applied to the selected *ASDU* set or to all *ASDU*s 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 has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

MODBUS

General settings

Max. number 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 (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).

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** allows modifying the action (*Scan/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 therefore allows defining a Modbus profile that specifies the memory ranges on the automaton 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 has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

OPC AE

Service management

Predefined services

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 and OPC Type Library.

Predefined OPC AE services are allowed by default (*Analyze* action). The buttons **Block by service set**, **Analyze by service set** and **Modify all services** allow modifying the action (*Analyze / Block*) applied to the selected service set or to all OPC AE services listed in the table.

OPC DA

Services management

Predefined services

This table lists the OPC DA services that have been predefined on the firewall. These services are classified by service set: Componet Categories, OPC Client, OPC Group, OPC Server and OPC Type Library.

Predefined OPC DA services are allowed by default (*Analyze* action). The buttons **Block by service set**, **Analyze by service set** and **Modify all services** allow modifying the action (*Analyze / Block*) applied to the selected service set or to all OPC DA services listed in the table.

OPC HDA

Service management

Predefined services

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 and OPC Type Library.

Predefined OPC HDA services are allowed by default (*Analyze* action). The buttons **Block by service set**, **Analyze by service set** and **Modify all services** allow modifying the action (*Analyze / 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 code	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 (*Analyze* action). The buttons **Block by service set**, **Analyze by service set** and **Modify all services** allow modifying the action (*Analyze / Block*) applied to the selected service set or to all OPC UA services listed in the table.

Other allowed services

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.

S7

Settings

Maximum number 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 (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 (*Analyze* action). The buttons **Block by operation set**, **Analyze by operation set** and **Modify all operations** allow modifying the action (*Analyze* / *Block*) applied to the selected operation set or to all S7 operations listed in the table.

Other operations

Other blocked JOBS

This list allows prohibiting 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 allows prohibiting 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 scan of the S7 protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log each S7 request	Enables or disables the logging of S7 requests.

UMAS

The UMAS (Unified Messaging Application Services) protocol is the intellectual property of Schneider Electric.

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 function group** and **Analyze by function group** buttons make it possible to modify the action (*Analyze* / *Block*) that had been applied to the selected function group.

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.

MS-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).

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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 applications can be allowed/blocked individually or in groups by selecting several services using the Shift key together with the buttons available in the Action menu. The **Modify all operations** button allows assigning the action to all services. The "Block by service group" and "Allow by service group" buttons allow modifying 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 RPC services
- Microsoft Scheduler

"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 scan of the MS-RPC protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log every DCE/RPC query	Enables or disables the logging of MS-RPC queries.
Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

NetBios CIFS

NetBios is a protocol that is used for sharing files/printers, generally by Microsoft systems.

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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.

EPMAP protocol

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).

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

Dynamic connections

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.

Allow dynamic opening of MS RPC services connections	This option allows MS RPC services to open connections without having to authorize them explicitly with a filter rule.
Block services provided by other servers than the EPMAP server	If this option has been selected, only services relayed by the connection's recipient EPMAP server will be authorized.
Only relay to Microsoft Exchange services	If this option has been selected, only Microsoft Exchange services will be relayed by the EPMAP server.

Support

Disable intrusion prevention	When this option is selected, the scan of the EPMAP protocol will be disabled and traffic will be authorized if the filter policy allows it

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

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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

Allowed RTCP commands

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

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 generation of logs relating to the RTP queries.

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.

RTSP commands

Allowed RTSP commands

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

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. number 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 request	Enables or disables the logging of SIP requests.

SIP

The SIP protocol performs protocol analyses and dynamically authorizes secondary connections. Connections are scanned line by line – the line has to 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): general coherence of the response in relation to 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 commands

Allowed SIP commands

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 SIP commands

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)

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 Device A client wishes 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 is aware of Device B's status. If the SUBSCRIBE request is successful, each time Device B's status changes, Device A will receive a SIP NOTIFY, a message indicating the change in status or presenting 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.

DNS

Profiles screen

"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)

This list contains the allowed domain names (<www.ofdomain.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**.

DNS registration types

Known types to be prohibited

This is a list of the known DNS types (A, A6, AAAA, CNAME, etc) and their associated codes. By default, these DNS types are allowed and scanned by the firewall.

The action (*Analyze* / *Block*) applied to a DNS type can be modified by clicking on the *Action* column corresponding to this type.

The **Modify all operations** button allows modifying the action (*Analyze* / *Block*) applied to all DNS types.

Additional types to be prohibited

This list allows blocking 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

"IPS" tab

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.

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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 each FTP request	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.

Authorized 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 allows defining the authorized 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 authorized transfer modes are the same as for the previous option.

"Commands FTP" tab

Proxy

Main commands

Modify write commands button: This button allows you to Pass without scanning, Block or Scan the syntax and check that the command complies with the RFCs in force, for write commands.

Modify all commands button: This button allows you to Pass without scanning, Block or Scan the syntax and check that the command complies with the RFCs in force, for generic commands as well as modification commands.

Command	Name of the command.
Action	3 authorizations possible from "Pass without scanning", "Scan" 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. These commands operate in the same way as for "generic" commands – you can authorize or prohibit a command or check that the command syntax complies with the RFC in force.

Other commands allowed

Additional commands, limited to 21 characters, can be added and deleted when necessary.

IPS

Authorized FTP commands

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 FTP commands

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, a scan will be performed to check RFC compliance.
- **ACCT**: Command that specifies the account to be used for connecting. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **ADAT**: Command that sends security data for authentication. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **AUTH**: Command that selects the security mechanism for authentication. This command accepts only a single argument. By default, a scan will be performed 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, a scan will be performed 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, a scan will be performed to check RFC compliance.
- **ENC**: This command specifies the “private” message used for authentication. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **EPRT**: This command enables the extended active transfer mode. This command accepts only a single argument. By default, a scan will be performed 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. It 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, a scan will be performed 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, a scan will be performed to check RFC compliance.

- **MIC**: This command specifies the "safe" message used for authentication. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **MLSD**: This command displays the contents of the normalized folder. By default, a scan will be performed to check RFC compliance.
- **MLST**: This command displays the information of the normalized folder. By default, a scan will be performed to check RFC compliance.
- **MODE**: This command specifies the transfer mode. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It 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, a scan will be performed to check RFC compliance.
- **NOOP**: This command does not do anything. It does not accept arguments. By default, a scan will be performed to check RFC compliance.
- **OPTS**: This command specifies the status options for the given command. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance.
- **PASS**: This command specifies the password used for the connection. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **PASV**: This command selects the passive transfer mode. This command does not accept arguments. By default, a scan will be performed to check RFC compliance.
- **PBSZ**: This command specifies the size of encoded blocks. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **PORT**: This command selects the active transfer mode. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **PROT**: This command specifies the level of protection. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It 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, a scan will be performed to check RFC compliance.
- **QUIT**: This command terminates the session in progress and the connection. By default, a scan will be performed to check RFC compliance.
- **REIN**: This command terminates the session in progress (initialized with the user). By default, a scan will be performed to check RFC compliance.
- **REST**: This command specifies the offset with which the transfer has to catch up. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It 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, a scan will be performed to check RFC compliance.
- **SIZE**: This command displays the transfer size for a given file. This command accepts one or several arguments. By default, a scan will be performed 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, a scan will be performed to check RFC compliance.
- **STAT**: This command displays the current status. By default, a scan will be performed to check RFC compliance.
- **STRU**: This command specifies the structure of transferred data. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It 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, a scan will be performed to check RFC compliance.
- **TYPE**: This command specifies the type of data transferred. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It 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, a scan will be performed to check RFC compliance.
- **XCWD**: This command modifies the working folder. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance.
- **XPWD**: This command displays the current working folder. This command does not accept arguments. By default, a scan will be performed to check RFC compliance.

List of FTP modification commands and details of filtering

- **ALLO**: This command allocates the storage space on this server. It 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. It 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. It 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. It 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. It 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. It 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. It 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. It 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. It 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

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

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 scan (KB)	In this field, the maximum size used for scanning files can be determined. You can also configure the action to perform if the file exceeds the authorized size. **WARNING** When manually defining a size limit for analyzed data, ensure that all values are coherent. The total memory space corresponds to a common space for all the resources reserved for the Antivirus service. If you define the size limit for analyzed data on FTP as 100% of the total size, no other files can be analyzed at the same time. The default size depends on the firewall model: • S model (SN160(W), SN210(W) and SN310): 4000 Ko. • M model (SN510, SN710 and SNi40): 4000 Ko. • L model (SN910): 8000 Ko. • XL model (EVA1, EVA2, EVA3,EVA4, EVAU, SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100): 16000 Ko.
Analyzing files	This option allows choosing the type of file that needs to be scanned: "downloaded and sent" files; "downloaded only" or "sent only" files.

Actions on files

When a virus is detected	This field contains 2 options. "Pass" and "Block". By selecting "Block", the analyzed file will not be sent. By selecting "Pass", 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 has been locked. If **Block** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been 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 retrieval fails, 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 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). • **Flash** (files with the extension ".swf"). • **Java** (compiled java files. Example: files with a ".jar" extension).
Max size of scanned files (KB)	This field allows defining the maximum size of files 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 2 options. By selecting "Block", the analyzed file will not be sent. By selecting "Pass", 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** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been 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 has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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 allows restricting access to Google services and accounts by entering only authorized 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 an unauthorized account 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 authorized 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).
CONTENTTYPE 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 others field, including formatting attributes. (Min: 128; Max: 4096).

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

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

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 each HTTP request	Enables or disables the logging of POP3 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)

Action when classification of URL failed	The choice is either **Pass** or **Block**.If a URL has not been listed in a URL category, this action will determine whether access to the site will be authorized.
Allow IP addresses in URLs	An option allows authorizing or denying 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 authorized in the filter policy (different from the pass all policy). Such access can be authorized via the firewall's basic Network objects (RFC5735) or the "Private IP" group in the EWC URL database.

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 authorized in the Stormshield Network Firewall.
Allow TCP tunnels (CONNECT method)	The **CONNECT method** allows building secure tunnels through proxy servers. If this option has been selected, the **CONNECT** method will be authorized in 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 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** allows defining the behavior of the firewall's HTTP proxy towards this type of download. • **Block**: partial downloads are prohibited • **Block if antivirus has been enabled**: partial downloads are allowed except if the traffic corresponds to traffic that is inspected by a rule with an antivirus scan. • **Pass**: partial downloads are authorized but there will not be any antivirus scan.
File size limit [0-2147483647(KB)]	When files downloaded off the internet via HTTP get too huge, they can deteriorate the internet bandwidth for quite a long stretch of time. To avoid this situation, indicate the maximum size (in KB) that can be downloaded by 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. 2 positions are available: "Enabled" or "Disabled".
Action	Indicates the action to be taken for the file in question, out of 3 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 being performed. • **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 and sandboxing scan (KB)	This field corresponds to the maximum size of files that will be scanned. The default size depends on the firewall model: • S model (SN160(W), SN210(W) and SN310): 4000 Ko. • M model (SN510, SN710 and SNi40): 8000 Ko. • L model (SN910): 16000 Ko. • XL model (EVA1, EVA2, EVA3,EVA4, EVAU, SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100): 32000 Ko.

Actions on files

When a virus is detected	This field contains 2 options. By selecting "Block", the analyzed file will not be sent. By selecting "Pass", 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 has been locked. If **Block** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been 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 retrieval fails, 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.

File types	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). • **Flash** (files with the extension ".swf"). • **Java** (compiled java files. Example: files with a ".jar" extension).
Max size of scanned files (KB)	This field allows defining the maximum size of files 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 2 options. By selecting "Block", the analyzed file will not be sent. By selecting "Pass", 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** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been 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

Analyzed and allowed versions

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. number of pending requests	Maximum number of requests without responses in a single NTP session. This value has to be between 1 and 512 seconds (default value: 10).
Maximum request duration (seconds)	This value is the period after which NTP requests without responses will be deleted. This value has to 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. Above the indicated value (default value: 20 minutes), 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) .

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

General 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.

The action (*Analyze* / *Block*) applied to each mode can be changed by double-clicking in the corresponding action column.

Advanced properties

Prohibited reference IDs

This list makes it possible to block additional NTP reference IDs (LOCL, LCL, etc.) by specifying their names. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

"IPS - NTP v2" tab

General 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.

The action (*Analyze* / *Block*) applied to each mode can be changed by double-clicking in the corresponding action column.

Advanced properties

Prohibited reference IDs

This list makes it possible to block additional NTP reference IDs (LOCL, LCL, etc.) by specifying their names. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

"IPS - NTP v3" tab

General configuration

Maximum size of packets (bytes)	Enter the maximum size allowed for NTP v3 packets (default value: 72 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.

The action (*Analyze / Block*) applied to each mode can be changed by double-clicking in the corresponding action column.

Advanced properties

Prohibited reference IDs

This list makes it possible to block additional NTP reference IDs (LOCL, LCL, etc.) by specifying their names. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

"IPS - NTP v4" tab

General 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.

The action (*Analyze / Block*) applied to each mode can be changed by double-clicking in the corresponding action column.

Advanced properties

Reference ID management

This table allows blacklisting or whitelisting additional NTP Reference IDs (LOCL, LCL, etc.).

Click on **Block All** to move all predefined NTP Reference IDs from the whitelist to the blacklist.

Reference IDs can also be added or deleted:

- Click on **Add** and specify the name of the Reference ID,
- Select a Reference ID and click on **Delete**.

Kiss of death packets

This table allows blacklisting or whitelisting additional Reference IDs that may be involved in Kiss of Death attacks (DENY, RSTR, RATELCL, etc.).

Click on **Block All** to move all predefined NTP Reference IDs from the whitelist to the blacklist.

Reference IDs can also be added or deleted:

- Click on **Add** and specify the name of the Reference ID,
- Select a Reference ID 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.

IPS

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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 scan of the POP3 protocol will be disabled and traffic will be authorized if the filter policy allows it.
Log each POP3 request	Enables or disables the logging of POP3 requests.

"POP3 Commands" tab

Proxy

Main commands

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.

Modify all commands button:allows authorizing, rejecting or checking all commands.

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: • **Scan**: 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 authorized, without being checked. • **Block**: the command will be blocked automatically, and an alarm will be raised to indicate it. • **Javascript** (files with a ".js" extension).

Other commands allowed

Command	This field allows adding additional personal commands.

"Analyzing files" tab

Maximum size for antivirus and sandboxing scan (KB)	This field corresponds to the maximum size of files that will be scanned. The default size depends on the firewall model: • S model (SN160(W), SN210(W) and SN310): 4000 Ko. • M model (SN510, SN710 and SNi40): 4000 Ko. • L model (SN910): 8000 Ko. • XL model (EVA1, EVA2, EVA3,EVA4, EVAU, SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100): 16000 Ko.

Warning

When manually defining a size limit for analyzed data, ensure that all values are coherent. The total memory space corresponds to a common space for all the resources reserved for the Antivirus service. 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 2 options. By selecting "Block", the analyzed file will not be sent. By selecting "Pass", 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 has been locked. If **Block** has been 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 retrieval fails, 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). • **Flash** (files with the extension ".swf"). • **Java** (compiled java files. Example: files with a ".jar" extension).
Max. size of sandboxed e-mails (KB)	This field allows defining 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 2 options. By selecting **Block**, the analyzed file will not be sent. By selecting **Pass**, 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** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been 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 SEISMO 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 has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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 connection direction (ATRN, ETRN)	Allows filtering 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 [64 – 4096]	Maximum number of characters that an e-mail header can contain (e-mail address of the sender, date, type of encoding used, etc.)
Server response line [64 – 4096]	Maximum number of characters that the response line from the SMTP server can contain.
Exchange data (XEXCH50)[102400 – 1073741824]	Maximum volume of data when transferring files in MBDEF format (Message Database Encoding Format).
BDAT extension header [102400 – 10485760]	Maximum volume of data sent using the BDAT command.
Command line [64 – 4096]	Maximum volume of data that a command line can contain (excluding the DATA command).

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 each SMTP request	Enables or disables the logging of SSL 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. **REMARK** 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 [0 – 2147483647 (KB)]	Indicates the maximum size of messages passing through the Stormshield Network firewall. Messages exceeding the defined size will be refused by the firewall.

"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

The button **Modify all commands** allows authorizing, rejecting or checking all commands.

Command	Indicates the name of the command.
Action	Indicates the action performed.

Other commands allowed

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

List of additional authorized SMTP commands. It is possible to **Add** or **Delete** commands.

Prohibited SMTP commands

List of prohibited SMTP commands. It is possible to **Add** or **Delete** commands.

"Analyzing files" tab

Maximum size for antivirus and sandboxing scan (KB)	The default size depends on the firewall model: • S model (SN160(W), SN210(W) and SN310): 4000 Ko. • M model (SN510, SN710 and SNi40): 4000 Ko. • L model (SN910): 8000 Ko. • XL model (EVA1, EVA2, EVA3,EVA4, EVAU, SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100): 16000 Ko.

WARNING

When manually defining a size limit for analyzed data, ensure that all values are coherent. The total memory space corresponds to a common space for all the resources reserved for the Antivirus service. 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 2 options. "Pass" and "Block". By selecting "Block", the analyzed file will not be sent. By selecting Pass, the antivirus will send the file event 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** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been 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). • **Flash** (files with the extension ".swf"). • **Java** (compiled java files. Example: files with a ".jar" extension).
Max. size of sandboxed e-mails (KB)	This field allows defining 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 2 options. By selecting **Block**, the analyzed file will not be sent. By selecting **Pass**, 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** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been specified, the file being scanned will be sent.

SNMP

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 showing a blank community (SNMPv1 - SNMPv2c).
Username	If this option is selected, you will be allowing SNMP requests showing a blank ID (SNMPv3).

SNMP command management

SNMP commands

This list sets out the SNMP functions allowed by default on the firewall. The action (*Analyze* / *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

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

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

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

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 table to another.

OID

Black list

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

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 each SNMP request	Enables or disables the logging of SNMP requests.
Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

SSL

"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).

WARNING

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.

Internet Explorer in version 7 or 8 does not enable by default, support for the protocol TLS 1.0. For security reasons, you are advised to enable TLS 1.0 support via an Active Directory object that defines host configurations (group policy object or GPO).

An ICAP server's validation of HTTPS requests decrypted by the SSL proxy is not supported.

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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.

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 SSL 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.

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 | 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 certificate 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 | 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 | 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 **Pass without decrypting**. 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**. If a certificate has not been listed in a certificate category, this action will determine whether the traffic will be authorized.

TFTP

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules.

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.
State	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.

QUALITY OF SERVICE (QoS)

The configuration window for quality of service consists of a single screen.

Network traffic

An important element of Quality of Service is the resolution of a major issue – the high rate of packet loss over the internet. When a packet is lost before it reaches its destination, the resources involved in its transmission will be wasted. In certain cases, this can even lead to severe congestion which may completely paralyze the systems.

The need for the stability and "real time" of videoconferencing applications is no longer the case today. The optimized control of congestion and the management of data queues has become a major challenge in Quality of Service.

Stormshield Network Firewalls employ two algorithms for congestion management – **TailDrop** and **BLUE**. However, Stormshield Network recommends the use of BLUE for managing congestion.

Treatment when full This option allows defining the congestion treatment algorithm, which aims to prevent slowdowns.

REMARK

The Default queue setting has been removed from the web administration interface, as it could enable QoS on all of the firewall's interfaces. This option has been kept as an advanced property via the serverd command line.

This option allows selecting the default queue from the choice of defined queues. More precisely, this option allows choosing how the default traffic (which does not correspond to any queue) will be treated in relation to the rest of the traffic. By default, this traffic type has priority over traffic treated by QoS ("Top priority"), but it is possible to subject the traffic to a certain queue by selecting it from this drop-down list.

Bandwidth reservation or limitation (CBQ)

Total bandwidth The reference value in Kbits/s or en Mbits/s allows indicating a reference on which bandwidth restrictions, indicated in percentage in the configuration of queues, will be based.

IMPORTANT

This value will restrict all traffic subject to QoS. The sum of all traffic passing through QoS will not be able to exceed this value and any excess network packets will be eliminated. It is therefore very important to set a reference value suited to the throughput of the network interface in question.

"ACK" and "low delay" packets are treated with a higher default priority (in order to speed up the transfer of data through limited bandwidth).

Queues

The QoS module embedded in Stormshield Network's intrusion prevention engine is associated with the Filter module in order to provide Quality of Service functions.

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.

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, click on the button **Add a queue**, then select **Class-based queue (CBQ)**. A line will be added to the table in which you will be able to make your changes.

Modifying a class-based queue

Name	Name of the queue to be configured.
Type	Type of queue (from monitoring (MONQ), priority (PRIQ), reservation/limitation (CBQ)).
Priority	Defines the priority level of the traffic assigned to the queue. The cells in this column can only be edited for PRIQs. It is possible to select a value from 1 (highest priority) to 7 (lowest priority).
Bp min	Acting as a service guarantee, this option allows guaranteeing a given throughput and a maximum transfer time. Configured in Kbits/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. **REMARK** This option is synchronized by default with the option **Min inv**. By modifying the value of this option, this value will be replicated in **Min inv**. By modifying the value of **Min inv**, the values will be different and therefore desynchronized.
Bp max	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. **REMARK** This option is synchronized by default with the option **Min inv**. By modifying the value of this option, this value will be replicated in **Min inv**. By modifying the value of **Min inv**, the values will be different and therefore desynchronized.

Min inv.	Acting as a service guarantee, this option allows guaranteeing a given throughput and a maximum transfer time. Configured in Kbits/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. **REMARK** If you enter a value higher than the **Max inv.**, the following message will appear: "downward traffic: the minimum guaranteed bandwidth should be lower than or equal to the maximum bandwidth".
Max inv.	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.
Color	Color to differentiate the queue.
Comments	Related comments.

REMARK

If you select "0" in the "Minimum bandwidth" column and "Unlimited" in the "Maximum 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 table in the menu Class-based queuing displays the various queues that have been configured. Clicking on **Check usage** allows you to view (in the browser bar on the left) 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 a monitoring queue, click on **Add** a queue, then select **Monitoring queue (MONQ).**

Modifying a monitoring queue

Name	Name of the queue to be configured.
Type	Type of queue from **CBQ**, **PRIQ** or **MONQ**).
Color	Color to differentiate the queue.
Comments	Related comments.

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 1 to 7. Priority 1 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 class-based queue click on the button **Add a queue**, then select **Priority queue (PRIQ)**.

A line will be added to the table in which you will be able to make your changes.

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	Type of queue from **CBQ**, **PRIQ** or **MONQ**).
Priority	Defines the priority level of the traffic assigned to the queue. The cells in this column can only be edited for PRIQs. It is possible to select a value from 1 (highest priority) to 7 (lowest priority).
Color	Color to differentiate the queue.
Comments	Related comments.

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:

SN160w, SN210w, SN310	SN510, SN710, SN910	SN2000, SN2100, SN3000, SN3100, SN6000, SN6100
20	100	255

Examples of application and usage recommendations

Example 1: Prioritization of DNS traffic

DNS queries, based on UDP, lose a large number of packets due to the definition of UDP – which does not provide mechanisms for managing transmission errors – and the overwhelming presence of TCP traffic that drowns out UDP traffic in the mass of TCP packets.

To preserve such traffic, and in particular DNS traffic, the creation of a PRIQ QoS rule is recommended. This rule will help to diminish frequent packet loss, as well as latency that may occur on this type of traffic, which requires high responsiveness (this is the precise reason for DNS queries being done on UDP).

Defining the QoS rule for DNS

Name	Type	Priority	Bp min	Bp max	Min inv.	Max inv.	Color	Comments
Priority queue (1 item)								
QoS_DNS		1						Prioritization of DNS traffic

Using the QoS rule in the filter policy

To view QoS in the *Filtering* tab, in the Filtering and NAT module, double-click on the Action column once you have set up your filter rule (see the document on Filtering and NAT or go to the menu Security Policy\Filtering and NAT module\Action column).

Effects on traffic

- Decreases the number of lost packets if the rule has level 1 priority (and is the only such rule).
- Reduces latency.

Example 2: Restricting HTTP traffic

HTTP traffic consumes more bandwidth from the internet link and local network than any other type of internet traffic. Heavy use of the internet may cause congestion of network traffic and decrease in overall performance, making it bothersome to use the network.

We recommended limiting HTTP traffic using a CBQ QoS rule that defines the maximum throughput allowed. Fortunately, the situation can be remedied. This rule will allow preserving the network's bandwidth and reducing the impact of using the internet on the network's overall performance.

Defining the QoS rule for HTTP

Name	Type	Priority	Bp min	Bp max	Min inv.	Max inv.	Color	Comments
Class-based queue (1 item)								
QoS_HTTP			0kb	512kb	0kb	512kb		Restriction on HTTP traffic

Using the QoS rule in the filter policy

To view **QoS** in the **Filtering** tab, in the **Filtering and NAT** module, double-click on the Action column once you have set up your filter rule (see the document on Filtering and NAT or go to the menu **Security Policy****Filtering and NAT** module\Action column).

Effects on traffic

- Lowers the risk of network congestion.
- Reduces the impact of traffic on the network's overall performance.

Example 3: Guaranteeing a minimum level of service

Some applications (e.g. VoIP) require a level of service with the guarantee of compliance. Failure to comply would result in the suspension of the service (e.g. VoIP conversations can no longer be held). Other applications and their impact on the network's general performance may disrupt the progress of obtaining the required service level.

To ensure the maintenance of the required service level, we recommend that you create a CBQ QoS rule that defines a minimum guaranteed throughput. It will guarantee a service level for specified traffic irrespective of the impact of other traffic on the network's overall performance and without defining the bandwidth restriction for these other types of traffic.

Defining the QoS rule for VoIP

Name	Type	Priority	Bp min	Bp max	Min inv.	Max inv.	Color	Comments
Class-based queue (1 item)								
QoS_VoIP			1kb	0kb	100kb	0kb		Guarantee of a minimum level of service

Using the QoS rule in the filter policy

To view **QoS** in the **Filtering** tab, in the **Filtering and NAT** module, double-click on the Action column once you have set up your filter rule (see the document on Filtering and NAT or go to the menu **Security Policy****Filtering and NAT** module\Action column).

Effects on traffic

- Guarantees bandwidth for a specified traffic type.
- Introduces a maximum data transfer time for the service.

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

This menu only appears when reports have been enabled on the firewall (**Report configuration** module).

The **Reports** module presents "Top 10" reports in the categories of **Web, Security, Viruses, Vulnerabilities** and **Spam**. As such, you will be able to view how the internet access is used, which attacks your firewall has blocked as well as the vulnerable hosts on your corporate network. Many interactive features allow you to directly fine-tune your firewall's configuration.

Personal 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 "Full access to logs (sensitive data)" privilege by clicking on "**Restricted access to logs**" (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 "**Full access to logs (sensitive data)**" 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 "Full access to logs (sensitive data)" privilege is obtained or released, it will generate an entry in logs.

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**.

Storage device: SD Card

The **External log storage on SD card** feature is available on all models in the S and SN ranges, except for SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100 models. This feature is offered with a subscription to the "External storage" option (see the **Logs - Syslog** module).

The type of SD card must be at least **Class 10** and compliant with the **SDHC standard**. The maximum memory supported is 2 TB for SN160(W), SN210(W) and SN310 firewall models.

Only the SD format is compatible: Micro SD or Nano SD cards fitted with an adapter are not supported.

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 Guides **PRESENTATION AND INSTALLATION OF NETASQ PRODUCTS U SERIES – S Models** or **PRESENTATION AND INSTALLATION OF STORMSHIELD NETWORK PRODUCTS SN Range,** available on the Stormshield Technical Documentation website.

Activity Reports

These reports are displayed in the form of bar graphs or pie charts and offer four time scales: the last hour, day, week or month. These time ranges are calculated in relation to the firewall's date and time settings.

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 refreshing the display of data.
Display the	In the case of a view by day, this field offers a calendar allowing you to select the date.

The button allows you to access 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 choosing to print or to generate a PDF file.

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.*

	Displays data in the form of a horizontal bar graph
	Displays data in the form of a vertical bar graph
	Displays data in the form of a pie chart

The analyzed period is then displayed.

Legend

A table made up of 6 columns summarizes the description of the data displayed. The information shown is as follows:

- Numbering indicates the rank according to the value,
- A letter and a color allow referencing the value when text is too long to be displayed in full (graphs in vertical bars or pie charts),
- The full name of the data type is displayed,

- The column displays the percentage that the data type represents for this list,
- The column displays the quantity value,
- This column contains a status button that displays or hides data. The category "Others" – representing data other than those in the Top 10 – is hidden by default. The status Hidden/Shown is kept in the preferences of the application.

Depending on the reports, extra columns can be added to the legend table offering certain information or interactions in relation to the values displayed (e.g.: action of an alarm).

Interactions

Left-clicking on a value in a report will open a menu offering several interactions. These may be for example, providing additional information on the value, modifying a parameter of the configuration profile or launching a search in the Logs section.

All items in a diagram allow the action **Search for this value in logs**: this search is conducted in the **Logs** section on all logs by keeping the monitored period with the value of the element selected in the report as a search criterion. This action is offered for all values except for certain specific searches listed below.

If it is an **IP address**, the possible actions will be:

- Add the host to the object base: through a dialogue window, the host can be added to the Object base and added to a group created earlier. The aim of this is to apply a particular filter policy to the object (quarantine zone).

* Please refer to the Technical Note "Collaborative security" on how to create a policy with a remediation zone.

A **domain name** allows the following additional actions:

- URL access: this action displays the URL in a new tab.
- Display the URL Category: this action displays in a window the category to which the domain belongs.
- Add the URL to a group: this action will display a window that allows adding the URL directly to an existing URL group.

The following are the particular interactions of the various reports:

WEB: Top web searches report

Execute this search via Google: this action launches a Google keyword search in a new tab.

SECURITY: Top most frequent alarms report

- **Set action to (Allow/Block)**: this modification will be made to the profile relating to the traffic that raised the alarm.
- **Set level to (Major/ Minor / Ignore)**: this modification will be made to the profile relating to the traffic that raised the alarm.
- **Open help**: this link redirects to the help page of the alarm raised or the vulnerability detected.
- **Search for this value in logs**: this search is conducted in the Logs section, on all logs and by keeping the monitored period.

VULNERABILITIES

Top most vulnerable hosts report

- Click to display the remaining vulnerabilities of this host: the remaining vulnerabilities for this host at this exact moment will be displayed. Indeed, a vulnerability that may have been reported at a given moment may have been resolved by the time it is read in the reports. You can also confirm the current status of vulnerabilities in Realtime Monitor.
- Search for this host in the vulnerabilities log: this search is conducted in the Logs section, on all logs and by keeping the monitored period.

Top client vulnerabilities and Top server vulnerabilities report

- View hosts having this vulnerability: hosts concerned at this exact moment and their version of the application or the vulnerable service are displayed. Indeed, a vulnerability that may have been reported at a given moment may have been resolved by the time it is read in the reports. You can also confirm the current status of vulnerabilities in Realtime Monitor.
- Open help: this link redirects to the help page of the alarm raised or the vulnerability detected.
- Search for this value in logs: this search is conducted in the Logs section, in the Vulnerabilities view and by keeping the monitored period.

Reports

WEB

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.

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.

Top most visited web domains

Through a mechanism that aggregates the number of *web servers* queried, the previous report is built according to *web domains*, which makes it possible to avoid dividing them..

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*).

Top web sites by exchanged volume

This report is based on the volumes of data exchanged, both sent and received.

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..

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.

Top users by volume exchanged,

Authentication has to be configured (refer to the section Authentication in this Guide). It relates to volumes of data exchanged, both sent and received.

This report contains private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

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*).

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..

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*).

Top web searches

These values relate to requests sent over the search engines Google, Bing and Yahoo.

This report contains private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

SECURITY

The *Alarms* reports are based on the **Applications and protections** alarms (*Application protection* menu) and **System events** (*Notifications* menu).

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.

Top most frequent alarms,

This report displays the alarms that are raised most frequently when the firewall scans traffic.

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 private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

Top administrator sessions

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.

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.

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 private data and therefore the **Full access to logs (private 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.

VIRUSES

The **Antivirus** inspection is required for these analyses.

Top web viruses

This report lists the viruses detected on web traffic (HTTP and HTTPS if the SSL inspection has been enabled). An interaction on the graph allows going to a description of the virus online (http://www.securelist.com).

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 interaction on the graph allows going to a description of the virus online (http://www.securelist.com).

Top senders of e-mail viruses

Viruses by e-mail detected on 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 has to be configured (refer to the section Authentication in this Guide).

This report contains private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

VULNERABILITIES

Vulnerabilities can be listed by host. The *Vulnerability management* module has to be enabled.

By default, these reports concern vulnerabilities that have been detected on internal networks as the object *network_internals* is defined by default in the list of network elements being monitored (see the **Vulnerability management** module in the administration interface). The analysis therefore covers hosts belonging to internal networks, identified by a DNS name (fqdn) or the IP address if there is no DNS name.

For further detail on profiles and vulnerability families, please refer to the section **Vulnerability management** in this guide.

Top most vulnerable hosts

This report shows the list of the most vulnerable hosts in the network with regard to the number of vulnerabilities detected without taking into account their severity.

It contains private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

Top Client vulnerabilities

This report shows all vulnerabilities detected with a *Client* target, with a level of severity of either “3” (High) or “4” (Critical). These include vulnerabilities that have both *Client* and *Server* targets.

Top Server vulnerabilities

This report shows all vulnerabilities detected with a *Server* target, with a level of severity of either "2" (Moderate), "3" (High) or "4" (Critical). These include vulnerabilities that have both *Client* and *Server* targets.

Top most vulnerable applications

This report shows the top 10 most detected vulnerabilities on the network by product regardless of severity.

NETWORK

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.

Top hosts by volume exchanged

This data volume concerns all hosts, whether they belong to internal or external networks.

This report contains private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

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.

Top users by volume exchanged

The data volume concerns authenticated users. Authentication has to be configured (refer to the section **Authentication** in this Guide).

This report contains private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

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.

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.

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.

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.

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.

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.

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.

SPAM

The **Antispam** module has to be enabled. These data are counted by recipient of spam received, by analyzing SMTP, POP3, SMTPS and POP3S traffic if the SSL scan has been enabled.

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 private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

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.

Industrial networks

Activity scanned 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.

Top Modbus servers by exchanged volume

This report sets out the most frequently used servers over all volumes exchanged for the industrial protocol MODBUS.

Top UMAS servers by exchanged volume

This report sets out the most frequently used servers over all volumes exchanged for the industrial protocol UMAS.

Top S7 servers by exchanged volume

This report sets out the most frequently used servers over all volumes exchanged for the industrial protocol S7.

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.

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.

Sandboxing

The **Sandboxing** option must be enabled. Data will be taken into account by analyzing HTTP, SMTP, POP3, FTP and HTTPS, SMTPS, POP3S if the SSL scan has been enabled.

Top malicious files detected after sandboxing

This report sets out the malicious files most frequently detected by sandboxing.

Top malicious files detected and blocked by sandboxing request

This report sets out the malicious files most frequently blocked by sandboxing.

Top most frequently analyzed file types

This report sets out the types of files most frequently submitted 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 private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

Top protocols that use sandboxing

This report shows the network protocols (HTTP, SSL, SMTP, FTP) that have warranted the highest number of sandboxing analyses.

Top users who have submitted files for sandboxing

This report shows the users that have warranted the highest number of sandboxing analyses. It contains private data and therefore the **Full access to logs (private data)** privilege is required in order to view it.

REPORT CONFIGURATION

These reports are compiled based on logs saved on the firewall. These logs are analyzed and the most frequently recurring values are stored within a database. The top 10 and 11th value corresponding to "Others" is therefore based on these values.

Data is refreshed every minute. The refreshment includes a calculation of a new Top 50 over the last few hours and days in order to better represent the recurrent values and to avoid overloading the database.

Data stored on SD cards can be read by other platforms equipped with an SQLite engine.

Reports are based on all traffic processed by the firewall, meaning for connections passing through all interfaces, internal and external.

WARNING

Even though the generation of reports does not have priority over other treatments, the number of reports enabled or the type of traffic may have a real impact on the performance of the appliance (*Dashboard*: CPU and memory).

This module also allows enabling history graphs available in the **Monitoring** module.

This screen is divided into 2 sections:

- Top: the options that make it possible to enable report management and/or history graphs.
- Bottom: table listing all reports and history graphs that may be selected in two tabs.

NOTE

Certain reports or history graphs require some features (such as antivirus, vulnerability management or authentication) to be enabled. Please refer to the monitoring module to find out which features are required and the possible interactions.

"General" menu

Enable reports	This option makes it possible to enable reports calculated based on logs stored on the hard disk or on an SD card (S series firewalls).
Enable history graphs	This option allows enabling history graphs that can be viewed in the **Monitoring** module.

Table of reports and history graphs

"List of reports" tab

The table sets out the following columns:

Status	Allows enabling/disabling the report in question.

Category of contact	Indicates the data category to which the report belongs. The report can be viewed in a menu bearing the name of this category in the **Reports** module. The report categories are the following: • Network • Industrial networks • Sandboxing • Spam • Security • Virus • vulnerability • Web
Description	The name of the report as it appears in the **Reports** module.
Warning	A warning message may appear if, for example, an option needed for building a report has not been enabled.
Private data	The symbol appears on the line in the report containing private data (source IP address, host name, user name, etc.). This means that the user will need to obtain the **Full access to logs (private data)** privilege in order to view the corresponding report.

At the bottom right of the table, the disk space used by the SQLite database will be shown.

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

The table sets out the following columns:

Status	Allows enabling/disabling the report in question.
Description	Specifies the type of history graph.
Warning	A warning message may appear if, for example, an option needed for building a graph has not been enabled.

ROUTING

Routing can be configured in three sections:

- Static route: Enables the definition of static routes. Static routing represents a set of rules defined by the administrator as well as a default route.
- Bird dynamic routing: Allows configuring dynamic routing protocols (RIP, OSPF, BGP) in a Bird engine, in order to allow the firewall to learn routes managed by other appliances.
- Return routes: 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.

These segments operate simultaneously, static routing having priority over all the rest during the transmission of a packet over the network.

"Static routes" tab

This tab corresponds to the list of static routes, the maximum number of which varies according to the model of the appliance:

SN160(W)	SN210(W)	SN310	SN510	SN710	SN910	SN2000 SN2100	SN3000 SN3100	SN6000 SN6100
512	512	512	2048	2048	5120	10240	10240	10240

Default gateway (router)	The default router is generally the equipment which allows your network to access the Internet. The Stormshield Network Firewall sends all packets which have to exit on the public network to this address. Often the default router is connected to the Internet. If you do not configure the default router, the Stormshield Network Firewall will not be able to let through packets which have a different destination address from those directly linked to the Stormshield Network Firewall. You will be able to communicate between hosts on the internal, external or DMZ networks, but not with any other network (including the Internet). Router objects can now be selected as the default gateway. 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.

Button bar

Search	Search that covers host, network and group objects.
Add	Adds an "empty" static route. An added route (sending of a command) is effective only if its fields **Destination network (host, network or group object)** and **Interface** have been 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 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 objects database in order to select a host, network or group.
Address range	IP address or group of addresses linked to the items in the column "Destination network (host, network or group object)".
Interface (Mandatory)	Drop-down list that allows selecting an interface from Ethernet, VLAN, dialup and IPSec.
Protected	This column indicates whether the route is protected. A protected route will be added to the object "Network internal". 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).
Color (Optional)	A window will appear, allowing the selection of an interface color (used in Stormshield Network REAL-TIME MONITOR).
(Optional) Comments	Any text.

"Dynamic routing" tab

Bird supports the following versions of dynamic routing protocols:

- Ripv2,
- OSPFv2 for IPv4 and OSPFv3 for IPv6,
- BGPv4 for IPv4 and IPv6.

This tab allows enabling and configuring the Bird dynamic routing engine.

Enable dynamic routing (Bird)	This option enables the use of the Bird dynamic routing engine when it is selected.

The window below this checkbox allows you to enter the configuration of the Bird dynamic routing engine directly.

NOTE

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 the Stormshield Technical Documentation website.

Advanced properties

Restart dynamic routing when the firewall becomes active (high availability)	In a cluster implementing the OSPF dynamic routing protocol, the active firewall would have the role of OSPF DR (Designated Router). 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.
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 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

Once the configuration has been sent to the firewall, and if there are syntax errors, a message indicating the row numbers containing errors will inform the user of the need to correct the configuration.

"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 return routes:

- Add,
- Remove.

Presentation of the table

The table sets out four fields of information:

Status	Status of the return 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)	A drop-down list allows selecting the outgoing interface for the return route.
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.
(Optional) Comments	Any text.

SMTP FILTERING

This module consists of 2 zones:

- A zone for profiles,
- A zone for 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 "Default" by default, accompanied by its number.

Examples:

- Defaut00
- (1) Default01 ...

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	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

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 directory on the left and which allows enabling the module and alarm and system notifications which will be integrated into the available(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.

The option **Enable the agent** allows enabling the module. It is however possible to configure the data for this screen even if the module has not been enabled.

SNMPv3 (recommended)	Enables version 3 of SNMP, 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 et 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.
Contact (sysContact)	E-mail address, telephone number, etc of the contact person in case problems arise. Example: *admin@mycompany.com*

Sending of SNMP alerts (traps)

Intrusion prevention alarms	**Do not send**: by selecting this option, you will not receive ASQ alarms. By selecting **send only major alarms**, you will be able to receive major ASQ alarms. By selecting **send major and minor alarms**, major and minor ASQ alarms will be sent.
System events	**Do not send**: by selecting this option, you will not receive system alarms. By selecting **send only major alarms**, you will be able to receive major system alarms. By selecting **send major and minor alarms, major and minor** system alarms will be sent.

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 et SNMPv3** allow enabling 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	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 (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 two encryption methods possible are DES and AES. By default DES is used for encryption.

Sending of SNMPv3 alerts (traps)

Sending traps to hosts consists of 2 parts, with the list of hosts on the left and details of 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 station. **NOTE** When the server's ID below has not been entered (engineID), this user name (securityName) has to be the same as the name used for logging on 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. **NOTE** If this field is empty, the SNMP agent has to be configured to receive an identifier that changes as it will be automatically generated each time the service starts.
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 defined. By default the authentication key will be used. **Warning** **You are strongly advised to use a specific key.**
Algorithm	The two encryption methods possible are DES and AES-128. By default AES-128 is used for encryption.

"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.

MIBS and Traps SNMP

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 your firewall's web administration interface.

In this module, you will be able to configure the workstations to which the firewall has to send SNMP events and alerts (traps) or to 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 to receive Stormshield traps, you must first group data from Stormshield Network's information base (these MIBs are available on Stormshield Network's website, at the address indicated in the section on Stormshield Network MIBs). MIB data are files in text format that describe a list of SNMP objects used by the supervisor. These MIBs therefore provision data that the supervisor would need in order to interpret SNMP traps, events and query messages sent to the firewall.

The values of Stormshield Network MIB traps are described in the following section.

Stormshield Network SNMP event and alert (traps) format

SNMPv2-MIB traps

http://www.net-snmp.org/docs/mibs/snmpMIB.html#notifications

coldStart NOTIFICATION-TYPE

STATUS current

DESCRIPTION "A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered."

::= { snmpTraps 1 }

warmStart NOTIFICATION-TYPE

STATUS current

DESCRIPTION"A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered."

::= { snmpTraps 2 }

authenticationFailure NOTIFICATION-TYPE

STATUS current

DESCRIPTION"An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated."

::= { snmpTraps 5 }

Traps managed by DISMAN-EVENT-MIB

To obtain the list of traps that are sent, you will need to use the MIB **DISMAN-EVENT-MIB**.

http://www.net-snmp.org/docs/mibs/dismanEventMIB.html

The tables **mteTriggerTable** and **mteEventNotificationTable** are the most useful.

Example of how to use an SNMP MIB lookup tool:

snmpwalk -v 2c -c public -M +/usr/local/share/snmp/mibs/ -m ALL 192.168.4.250 mteEventNotificationTable

....

DISMAN-EVENT-MIB::mteEventNotification."_snmpd"."_linkDown' = OID: IF-MIB::linkDown

DISMAN-EVENT-MIB::mteEventNotification."_snmpd"."_linkUp' = OID: IF-MIB::linkUp

....

To find out the conditions that trigger a trap, use **mteTriggerTable**

(based on IF-MIB::ifOperStatus)

...

The following are the most useful traps:

IF-MIB::linkDown

IF-MIB::linkUp

You will find the descriptions of **IF-MIB::linkDown** and **IF-MIB::linkUp** at: http://www.net-snmp.org/docs/mibs/IF-MIB.txt

linkDown NOTIFICATION-TYPE

OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }

STATUS current

DESCRIPTION "A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus."

::= { snmpTraps 3 }

linkUp NOTIFICATION-TYPE

OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }

STATUS current

DESCRIPTION "A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus."

::= { snmpTraps 4 }

Stormshield Network Traps

.1.3.6.1.4.1.11256.1.5

Stormshield Network traps are defined in the file **MIB STORMSHIELD-ALARM-MIB.txt**

time	.0.1.1
srcif	.0.1.2
src	.0.1.5
dst	.0.1.6
msg	.0.1.11

time	.1.1.1
srcif	.1.1.2
src	.1.1.4
dst	.1.1.5
msg	.1.1.10

NOTE

The notification "snsAMessage" contains the message associated with the alarm or the system event. Documentation on alarms is available online in the security KB, or accessible via the administration interface, in the System events module when you click on the *Show help* link for each event.

The descriptions of system alarms are also given in the section **SYSTEM EVENTS** > **List of events**.

Management information bases (MIBs)

Stormshield Network MIBs

Here is the list of fields of Stormshield Network MIBs, CLI commands corresponding and console commands.

The links can be downloaded from: https://www.stormshield.com/products-services/services/mibs/

STORMSHIELD-SMI-MIB: Mib as a whole

STORMSHIELD-ALARM-MIB: Table of alarms

.1.3.6.1.4.1.11256.1.5

==> Contents of logs

Contains 2 tables :

Alarms

time	.0.X.1
srcif	.0.X.2
dstif	.0.X.3
proto	.0.X.4
src	.0.X.5
dst	.0.X.6
srcport	.0.X.7
dstport	.0.X.8
srcname	.0.X.9
dstname	.0.X.10
msg	.0.X.11

ICMP alarms

time	.1.X.1
srcif	.1.X.2
dstif	.1.X.3
src	.1.X.4
dst	.1.X.5
type	.1.X.6
code	.1.X.7
srcname	.1.X.8
dstname	.1.X.9
msg	.1.X.10

STORMSHIELD-HA-MIB: Information on high availability

.1.3.6.1.4.1.11256.1.11

==> (CLI) HA INFO

==> (console) hainfo

General information

NbNode	.1.0
NbDeadNode	.2.0
NbActiveNode	.3.0
NbHALinks	.5.0
NbFaultyHALinks	.6.0
HASyncStatus	.8.0
HAFwAdminRevision	.9.0

Table of HA members

FwSerial	.7.X.2
Online	.7.X.3
Model	.7.X.4
Version	.7.X.5
HALicence	.7.X.6
HAQuality	.7.X.7
HAPriority	.7.X.8
HAStatusForced	.7.X.9
HAActive	.7.X.10
Uptime	.7.X.11

Tracking of power supply modules

NodePowerSupplyPowered	.10.X.2
NodePowerSupplyStatus	.10.X.3

Tracking of disks

NodeDiskName	.11.X.2
NodeDiskSmartResult	.11.X.3
NodeDiskIsRaid	.11.X.4
NodeDiskRaidStatus	.11.X.5
NodeDiskPosition	.11.X.6

Tracking of processors

NodeCpuTemp	.12.X.2

STORMSHIELD-POLICY-MIB: Filter policy

.1.3.6.1.4.1.11256.1.8.1

==> (CLI) MONITOR POLICY

==> (console) slotinfo

Name	.X.2
Slot_Name	.X.3
Partition	.X.4
Sync	.X.5

STORMSHIELD-AUTHUSERS-MIB: Table of authenticated users

.1.3.6.1.4.1.11256.1.2.1

==> (CLI) MONITOR USER

==> (console) sfctl -s user

AuthIpAddr	.X.1
AuthTimeout	.X.2
AuthUserName	.X.3
AuthUsersDomain	.X.4

STORMSHIELD-HOSTS-MIB: Tables of protected hosts

.1.3.6.1.4.1.11256.1.3.1

==> (CLI) MONITOR HOST

==> (console) sfctl -s host

HostIpAddr	.X.1
HostName	.X.2
Interface	.X.3
Packet	.X.4
Bytes	.X.5
CurrThroughput	.X.7

MaxThroughput	.X.8
InBytes	.X.9
OutBytes	.X.10
InCurrThroughput	.X.11
OutCurrThroughput	.X.12
InMaxCurrThroughput	.X.13
OutMaxCurrThroughput	.X.14

STORMSHIELD-PROPERTY-MIB: Information returned by the "SYSTEM PROPERTY" command

.1.3.6.1.4.1.11256.1.0

==> (CLI) SYSTEM PROPERTY, SYSTEM IDENT, SYSTEM LANGUAGE

Model	.1.0
Version	.2.0
SerialNumber	.3.0
SystemName	.4.0
SystemLanguage	.5.0
NbEther	.6.0
NbVlan	.7.0
NbDialup	.8.0
NbPPTP	.9.0
NbSerial	.10.0
NbLoopback	.11.0
Watchdog	.12.0
Led	.13.0
Clone	.14.0
HADialup	.15.0

STORMSHIELD-SYSTEM-MONITOR-MIB: ASQ resource usage counters

.1.3.6.1.4.1.11256.1.10

==> (CLI) MONITOR STAT

General information

Date	.1.0
UpTime	.2.0
Mem	.3.0
StatTime	.4.0

Tracking of disks

DiskEntryDiskName	.5.X.2
DiskEntrySmartResult	.5.X.3
DiskEntryIsRaid	.5.X.4
DiskEntryRaidStatus	.5.X.5
DiskEntryPosition	.5.X.6

Tracking of power supply modules

PowerSupplyPowered	.6.X.2
PowerSupplyStatus	.6.X.3

Tracking of processors

CpuTemp	.7.X.2

Tracking of hardware bypass

Bypassl2CAddress	.8.X.2
BypassSystemOff	.8.X.3
BypassJustOn	.8.X.4
BypassRunTime	.8.X.5
BypassWatchdog	.8.X.6

STORMSHIELD-AUTOUPDATE-MIB: Status of various modules updated by Active Update

.1.3.6.1.4.1.11256.1.9.1

==> (CLI) MONITOR AUTOUPDATE

AutoupdateSubsys	.X.2
AutoupdateState	.X.3
AutoupdateLast	.X.4

STORMSHIELD-IF-MIB: Status of interfaces seen by ASQ

.1.3.6.1.4.1.11256.1.4.1

==> (CLI) MONITOR INTERFACE

ifUserName	.X.2
ifName	.X.3
ifAddr	.X.4
ifMask	.X.5
ifType	.X.6
ifColor	.X.7
ifMacThroughput	.X.8
ifCurThroughput	.X.9
ifMaxThroughput	.X.10
ifPktAccepted	.X.11
ifPktBlocked	.X.12
ifPktFragmented	.X.13
ifPktTcp	.X.14
ifPktUdp	.X.15
ifPktIcmp	.X.16
ifTotalBytes	.X.17
ifTcpBytes	.X.18
ifUdpBytes	.X.19
ifIcmpBytes	.X.20
ifTcpConn	.X.21
ifUdpConn	.X.22
ifTcpConnCount	.X.23
ifUdpConnCount	.X.24
ifInCurThroughput	.X.25
ifOutCurThroughput	.X.26

ifInMaxThroughput	.X.27
ifOutMaxThroughput	.X.28
ifInTotalBytes	.X.29
ifOutTotalBytes	.X.30
ifInTcpBytes	.X.31
ifOutTcpBytes	.X.32
ifInUdpBytes	.X.33
ifOutUdpBytes	.X.34
ifInIcmpBytes	.X.35
ifOutIcmpBytes	.X.36
ifProtected	.X.37
ifDrvName	.X.38

STORMSHIELD-SERVICES-MIB: Status of firmware services

.1.3.6.1.4.1.11256.1.7.1

==> (CLI) MONITOR SERVICE

==> (console) dstat

ServicesName	.X.2
ServicesState	.X.3
ServicesUpTime	.X.4

STORMSHIELD-VPNSA-MIB: Table of negotiated IPSEC SA

.1.3.6.1.4.1.11256.1.1.1

==> (CLI) MONITOR GETSA

==> (console) showSAD

VPNSAIndex	.X.1
VPNIPSrc	.X.2
VPNIPDst	.X.3
VPNType	.X.4
VPNMode	.X.5
VPNSpi	.X.6
VPNPeerSpi	.X.7
VPNReqID	.X.8
VPNEnc	.X.9
VPNAuth	.X.10
VPNState	.X.11
VPNLifeTime	.X.12
VPNBytes	.X.13
VPNMaxLifeTime	.X.14
VPNMaxBytes	.X.15

STORMSHIELD-ASQ-STATS-MIB: Table of ASQ statistics

.1.3.6.1.4.1.11256.1.12

==> no CLI command

==> (console) sfctl –s stat

SPD Statistics

ASQStatsStatefulPktBlocked	.1.1
ASQStatsStatefulPktBlockedAsync	.1.2
ASQStatsStatefulPktBlockedSynProxy	.1.3
ASQStatsStatefulPktAccepted	.1.4
ASQStatsStatefulLogged	.1.5
ASQStatsStatefulLogOverflow	.1.6
ASQStatsStatefulFilterOverflow	.1.7
ASQStatsStatefulAlarmOverflow	.1.8
ASQStatsStatefulSeismoFacts	.1.9
ASQStatsStatefulSeismoOverflow	.1.10
ASQStatsStatefulMinorAlarm	.1.11
ASQStatsStatefulMajorAlarm	.1.12
ASQStatsStatefulPktFragmented	.1.13
ASQStatsStatefulInBytes	.1.14
ASQStatsStatefulOutBytes	.1.15
ASQStatsStatefulNatFailures	.1.16
ASQStatsStatefulFlowConflicts	.1.17
ASQStatsStatefulFlowFailures	.1.18
ASQStatsStatefulInterfaceMute	.1.19
ASQStatsStatefulTcpPkt	.1.20
ASQStatsStatefulTcpInBytes	.1.21
ASQStatsStatefulTcpOutBytes	.1.22
ASQStatsStatefulTcpConn	.1.23
ASQStatsStatefulTcpNatConnSrc	.1.24
ASQStatsStatefulTcpNatConnDst	.1.25
ASQStatsStatefulTcpNoNatConnSrc	.1.26
ASQStatsStatefulTcpNoNatConnDst	.1.27
ASQStatsStatefulTcpSmallWindowRst	.1.28
ASQStatsStatefulTcpEmptyDupAckBlk	.1.29
ASQStatsStatefulUdpPkt	.1.30
ASQStatsStatefulUdpInBytes	.1.31
ASQStatsStatefulUdpOutBytes	.1.32
ASQStatsStatefulUdpConn	.1.33
ASQStatsStatefulUdpNatConnSrc	.1.34
ASQStatsStatefulUdpNatConnDst	.1.35
ASQStatsStatefulUdpNoNatConnSrc	.1.36
ASQStatsStatefulUdpNoNatConnDst	.1.37
ASQStatsStatefulIcmpPkt	.1.38
ASQStatsStatefulIcmpInBytes	.1.39
ASQStatsStatefulIcmpOutBytes	.1.40
ASQStatsStatefulHttpTimeoutRst	.1.41
ASQStatsStatefulNatUnusable	.1.42

SAD statistics

ASQStatsGlobalTimeSinceReset	.2.1

STORMSHIELD-IPSEC-STATS-MIB: Table of IPSEC statistics

.1.3.6.1.4.1.11256.1.13

==> no CLI command

==> (console) ipsecinfo

SPD Statistics

IPSECStatsSPDIn	.1.1
IPSECStatsSPDOut	.1.2

SAD statistics

IPSECStatsSADLarval	.2.1
PSECStatsSADMature	.2.2
IPSECStatsSADDying	.2.3
IPSECStatsSADDead	.2.4

STORMSHIELD-ROUTE-MIB: Table of routers

.1.3.6.1.4.1.11256.1.14.1

==> (CLI) MONITOR ROUTE

==> (console) sfctl -s route

RouteType	.X.2
RouteIPVersion	.X.3
RouteRouterName	.X.4
RouteGatewayName	.X.5
RouteGatewayAddr	.X.6
RouteGatewayType	.X.7
RouteLastCheck	.X.8
RouteState	.X.9
RouteStateLastChange	.X.10
RouteActive	.X.11
RouteActiveLastChange	.X.12
RouteSysDefaultGateway	.X.13
RouteSysDefaultGatewayLastChange	.X.14
RouteRtid	.X.15
RouteUsagePrct	.X.16

STORMSHIELD-HEALTH-MONITOR-MIB: Table of the firewall's health status

.1.3.6.1.4.1.11256.1.16

==> (CLI) MONITOR HEALTH

GlobalHealth	.1
FirewallIndex	.2.1.1
SerialHealth	.2.1.2
HaModeHealth	.2.1.3
HaLinkHealth	.2.1.4
PowerSupplyHealth	.2.1.5
FanHealth	.2.1.6
CpuHealth	.2.1.7
MemHealth	.2.1.8
DiskHealth	.2.1.9
RaidHealth	.2.1.10

Other standard MIBs

Links to various MIBs are given below.

The SNMP agent only supports listed fields and sub-sets.

SNMPv2-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMPv2-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpMIB.html

rfc=http://www.ietf.org/rfc/rfc3418.txt

system.*.0

sysORTable

snmp.*.0

setSerialNo.0

SNMP-FRAMEWORK-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-FRAMEWORK-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpFrameworkMIB.html

rfc=http://www.ietf.org/rfc/rfc3411.txt

snmpEngine.*.0

SNMP-TARGET-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-TARGET-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpTargetMIB.html

rfc=http://www.ietf.org/rfc/rfc3413.txt

snmpTargetSpinLock.0

snmpTargetAddrTable

snmpTargetParamsTable

snmpUnavailableContexts.0

snmpUnknownContexts.0

SNMP-NOTIFICATION-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-NOTIFICATION-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpNotificationMIB.html

rfc=http://www.ietf.org/rfc/rfc3413.txt

snmpNotifyTable

snmpNotifyFilterProfileTable

snmpNotifyFilterTable

nlmConfig.*.0

nlmStats.*.0

NOTIFICATION-LOG-MIB

mibfile=http://www.net-snmp.org/docs/mibs/NOTIFICATION-LOG-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/notificationLogMIB.html

rfc=http://www.ietf.org/rfc/rfc3014.txt

SNMP-USER-BASED-SM-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-USER-BASED-SM-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpUsmMIB.html

rfc=http://www.ietf.org/rfc/rfc3414.txt

usmStats.*.0

usmUserTable

SNMP-VIEW-BASED-ACM-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-VIEW-BASED-ACM-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpVacmMIB.html

rfc=http://www.ietf.org/rfc/rfc3415.txt

vacmContextTable

vacmSecurityToGroupTable

vacmAccessContextTable

vacmViewSpinLock.0

vacmViewTreeFamilyTable

SNMP-USM-DH-OBJECTS-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-USM-DH-OBJECTS-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpUsmDHObjectsMIB.html

rfc=http://www.ietf.org/rfc/rfc2786.txt

usmDHPublicObjects.*.0

usmDHUserKeyTable

IF-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IF-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ifMIBObjects.html

rfc=http://www.ietf.org/rfc/rfc2863.txt

ifNumber.0

ifTable

ifXTable

RFC1213-MIB

mibfile=http://www.net-snmp.org/docs/mibs/RFC1213-MIB.txt

rfc=http://www.ietf.org/rfc/rfc1213.txt

atTable

IP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ip.html

rfc=http://www.ietf.org/rfc/rfc4293.txt

ip.*.0

icmp.*.0

ipAddrTable

ipRouteTable

ipNetToMediaTable

ipNetToPhysicalTable

IPV6-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IPV6-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ipv6MIB.html

rfc=http://www.ietf.org/rfc/rfc2465.txt

ipv6MIBObjects.?.0

ipv6Interfaces

ipv6IfTable

ipv6IfStatsTable

IPV6-TCP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IPV6-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ipv6TcpMIB.html

rfc=http://www.ietf.org/rfc/rfc2452.txt

ipv6TcpConnTable

IPV6-UDP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IPV6-UDP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ipv6UdpMIB.html

rfc=http://www.ietf.org/rfc/rfc2465.txt

ipv6UdpTable

IPV6-ICMP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IPV6-ICMP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ipv6IcmpMIB.html

rfc=http://www.ietf.org/rfc/rfc2466.txt

ipv6IfIcmpTable

TCP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/TCP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/tcp.html

rfc=http://www.ietf.org/rfc/rfc4022.txt

tcp.*.0

tcpConnTable

UDP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/UDP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/udp.html

rfc=http://www.ietf.org/rfc/rfc4113.txt

udp.*.0

udpTable

IF-INVERTED-STACK-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IF-INVERTED-STACK-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ifInvertedStackMIB.html

rfc=http://www.ietf.org/rfc/rfc2864.txt

HOST-RESOURCES-MIB

mibfile=http://www.net-snmp.org/docs/mibs/HOST-RESOURCES-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/host.html

rfc=http://www.ietf.org/rfc/rfc2790.txt

hrSystem.*.0

hrMemorySize

hrStorageTable

hrDeviceTable

hrProcessorTable

hrNetworkTable

hrPrinterTable

hrDiskStorageTable

hrPartitionTable

hrFSTable

hrSWRunTable

hrSWRunPerfTable

hrSWInstalled.*.0

hrSWInstalledTable

DISMAN-EVENT-MIB

mibfile=http://www.net-snmp.org/docs/mibs/DISMAN-EVENT-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/dismanEventMIB.html

rfc=http://www.ietf.org/rfc/rfc2981.txt

mteTriggerTable

mteTriggerDeltaTable

mteTriggerExistenceTable

mteTriggerBooleanTable

mteTriggerThresholdTable

mteObjectsTable

mteEventTable

mteEventNotificationTable

DISMAN-SCHEDULE-MIB

mibfile=http://www.net-snmp.org/docs/mibs/DISMAN-SCHEDULE-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/schedMIB.html

rfc=http://www.ietf.org/rfc/rfc3231.txt

schedLocalTime.0

schedTable

AGENTX-MIB

mibfile=http://www.net-snmp.org/docs/mibs/AGENTX-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/agentxMIB.html

rfc=http://www.ietf.org/rfc/rfc2742.txt

NET-SNMP-AGENT-MIB

mibfile=http://www.net-snmp.org/docs/mibs/NET-SNMP-AGENT-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/netSnmpAgentMIB.html

nsModuleTable

nsCacheTable

nsConfigDebug.*.0

nsDebugTokenTable

nsConfigLogging

nsLoggingTable

netSnmpExampleScalars

netSnmpIETFWGTable

netSnmpHostsTable

nstAgentModules

NET-SNMP-VACM-MIB

mibfile=http://www.net-snmp.org/docs/mibs/NET-SNMP-VACM-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/netSnmpVacmMIB.html

nsVacmAccessTable

UCD-DISKIO-MIB

mibfile=http://www.net-snmp.org/docs/mibs/UCD-DISKIO-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ucdDiskIOMIB.html

UCD-DLMOD-MIB

mibfile=http://www.net-snmp.org/docs/mibs/ucdDlmodMIB.html

desc=http://www.net-snmp.org/docs/mibs/ucdDlmodMIB.html

SCTP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SCTP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/sctpMIB.html

rfc=http://www.ietf.org/rfc/rfc3873.txt

sctpStats

sctpParameters

sctpAssocTable

sctpAssocLocalAddrTable

sctpAssocRemAddrTable

sctpLookupLocalPortTable

sctpLookupRemPortTable

sctpLookupRemHostNameTable

sctpLookupRemPrimIPAddrTable

sctpLookupRemIPAddrTable

SSL FILTERING

SSL filtering is now integrated into the new security policy on Stormshield Network multi-function firewalls. 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 2 zones:

- A zone for profiles,
- A zone for SSL filter rules.

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 "Default" by default, accompanied by its number.

Examples:

- Defaut00
- (1) Default01…

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	Pass without decrypting	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 (**Web Objects** 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.

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*.

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 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.
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 enables remote users to safely access internal corporate resources using communications encrypted in SSL. The use of SSL VPN requires the installation of an SSL VPN client installed on the workstation or on any type of mobile terminal (Windows, IOS, Android, etc.).

SSL VPN tunnels may be based on UDP or TCP protocols. Whenever a UDP-based tunnel fails, the connection will switch to TCP.

If the VPN client that has been provided is used, only the IP address of the firewall and its authentication information (login/password) will be needed for the connection. If an OpenVPN client is used, the client must retrieve configuration details from the authentication portal ("Personal data" menu) before inserting them into the client

In addition to the settings in this module, the **Authentication** section must define the method and allow the user in its policy. A filter rule must also specify 'Via SSL VPN tunnel' as the source (advanced configuration) in order to authorize traffic.

For further information, please refer to the Technical note **SSL VPN tunnels** available in your secure-access area.

This module consists of a single configuration screen split up into 4 zones:

- Enable the service
- **Network settings:** this zone contains elements for configuring the SSL VPN server, networks or contactable hosts, as well as the network assigned to clients.
- **DNS settings sent to client**: this zone contains the DNS configuration elements that will be sent to the client.
- **Advanced configuration**: an area for customizing the lifetime before SSL renegotiation, defining scripts to be executed where necessary when logging on to/off from the client and selecting client and server certificates for setting up the SSL tunnel.

This button makes it possible to enable or disable the SSL VPN server on the firewall.

Network settings

UTM IP address (or FQDN) used	Indicate the public IP address of the IPS-Firewall (or an FQDN associated with this address. Example: sslserver.company.com) through which clients will be able to contact the SSL VPN server.
Available networks or hosts	Indicate which network and hosts will be visible to clients. All packets from the client going towards these networks will go through the SSL tunnel. This object can either be a "network", "machine" or "group" object (containing several networks and/or hosts). It can be created directly in this window by clicking on The value of this field is "Network_internals" by default, offering connectivity with all networks protected by the firewall. **REMARK** This is only a network routing concept. Filter rules must be created to allow or block traffic between the remote client network and internal resources.

Network assigned to clients (UDP)	Select a "network" object ("IP address range" or "Group" objects are not accepted). Each client that sets up a UDP-based tunnel will be assigned an IP address belonging to this network. This network must be different from the one assigned to the clients of TCP-based tunnels. The object can be created directly in this window by clicking on the icon **IMPORTANT** In order to prevent routing conflicts on client workstations during the connection to the SSL VPN, select for your clients sub-networks that are less commonly used instead (example: 10.60.77.0/24, 172.168.38.0/24, etc.). Many filtered Internet access networks (public Wi-Fi, hotels, etc) or private local networks precisely use the first few address ranges reserved for these uses (example: 10.0.0.0/24, 192.168.0.0/24).
Network assigned to clients	Select a "network" object ("IP address range" or "Group" objects are not accepted). Each client that sets up a TCP-based tunnel will be assigned an IP address belonging to this network. This network must be different from the one assigned to the clients of UDP-based tunnels. The object can be created directly in this window by clicking on the icon **IMPORTANT** In order to prevent routing conflicts on client workstations during the connection to the SSL VPN, select for your clients sub-networks that are less commonly used instead (example: 10.60.77.0/24, 192.168.38.0/24, etc.). Many filtered Internet access networks (public Wi-Fi, hotels, etc) or private local networks precisely use the first few address ranges reserved for these uses (example: 10.0.0.0/24, 192.168.0.0/24).
Maximum number of simultaneous tunnels allowed	Depending on the size of the network chosen for clients and the model of the firewall, the number of tunnels that can be set up simultaneously will be indicated. This number corresponds to the minimum of the two following values: • A quarter of the number of IP addresses includes in the selected client network (example: 63 for a Class C network). Each SSL tunnel takes up 4 IP addresses. • The maximum number of tunnels allowed on the IPS-Firewall used.

DNS settings sent to client

Domain name	Domain name assigned to the client to allow him to perform DNS resolutions.
Primary DNS server	Primary DNS server assigned to the client.
Secondary DNS server	Secondary DNS server assigned to the client.

Advanced properties

UTM IP address for the SSL VPN (UDP)	Enter the public IP address of the IPS-Firewall through which clients will be able to contact the SSL VPN server over UDP.
Port (UDP)	Select or create the object corresponding to the UDP port that will be used to set up tunnels.
Port (TCP)	Select or create the object corresponding to the TCP port that will be used to set up tunnels. This port will also be used as a backup mechanism if tunnels cannot be set up via UDP.

Interval before key renegotiation (in seconds)	Period beyond which leys will be renegotiated. The default value is 14400 seconds, or 4 hours.
Use DNS servers provided by the firewall	If this option is selected, the SSL VPN client will include the DNS servers retrieved via the SSL VPN in the workstation's network configuration. If DNS servers have already been defined on the workstation, they may be queried.
Prohibit use of third-party DNS servers	If this option is selected, the SSL VPN client will exclude DNS servers already defined in the workstation's configuration. Only DNS servers sent by the firewall can be queried. These DNS servers must be contactable through an SSL VPN tunnel.
Script to run when connecting	Select a script that the client will execute locally when connecting to the SSL tunnel (example: connecting a disk to a remote shared network).
Script to run when disconnecting	Select a script that the client will execute locally when disconnecting from the SSL tunnel (example: disconnecting a disk from a remote shared network).

NOTE

Only client hosts running under Windows and with the Stormshield Network client can use the executable script service. The format of files must be ".bat".

NOTE

All Windows environment variables can be used in connection/disconnection scripts (example: %USERDOMAIN%, %SystemRoot%, etc.).

Two environment variables relating to the SSL VPN tunnel can also be used:

- %NS_USERNAME%: the user name used for authentication,
- %NS_ADDRESS%: the IP address assigned to the client.

Used certificates

Server certificate	Select the certificate submitted by the server to set up the SSL tunnel. By default, the server certificate suggested is the one created during the initialization of the firewall. It is issued by the CA dedicated to the default SSL VPN.
Client certificate	Select the certificate submitted by the client to set up the SSL tunnel. By default, the client certificate suggested is the one created during the initialization of the firewall. It is issued by the CA dedicated to the default SSL VPN. This certificate is the same for all clients. They can be authenticated once the SSL connection has been established.

IMPORTANT

If you choose to create your own CA, you will need to use two certificates signed by it. If this CA is not a root authority, both certificates have to be issued by the same sub-authority.

Configuration

Download the configuration file	Click on this button to obtain an archive containing the SSL VPN server's configuration file.

SSL VPN Portal

Stormshield Network's SSL VPN allows your mobile or static users to connect to your company's resources securely.

The SSL VPN configuration screen consists of 4 tabs:

- **General**: Allows enabling the module, selecting the access type and configuring advanced properties.
- *Web servers*: Stormshield Network's SSL VPN allows securing access to your HTTP servers (Intranet, webmail,...) while avoiding the need to manage multiple HTTP servers. Furthermore, for mobile users, it allows masking information about your internal network, the only visible IP address being your firewall's.
  Stormshield Network's SSL VPN automatically rewrites HTTP links found in web pages that your users visit. This allows browsing between your various servers, if they have been configured, or prohibiting access to certain servers. When a web link in a page points to an unconfigured server, the link will be redirected to the Stormshield Network SSL VPN start page.
- *Application servers*: This section shows the servers that have been configured for access to resources other than web-based resources (telnet, mail, etc)
  Stormshield Network's SSL VPN enables securing any protocol based on a single TCP connection (POP3, SMTP, telnet, remote access, etc). For protocols other than HTTP, the client that allows secure connections is a Java applet, which will open an encrypted tunnel. All packets exchanged between the client workstation and the firewall are encrypted.
  Stormshield Network'S SSL VPN does not impose any client installations on your users' workstations and natively supports operating systems that have Java installed (Windows, Linux, MAC OS-X,...).
  You only need to configure the servers which you intend to allow your users to access. These servers will be added dynamically to the list of authorized servers the next time your users load the java applet.
  The java applet opens listening ports on the client workstation, and client tools will need to connect to these ports in order to pass through the secure tunnel set up between the applet and the firewall. It is necessary to ensure that the chosen port is accessible to the user (where privileges are concerned) and that there is no conflict with another port used by another program. These servers will be added dynamically. These can be used for control purposes and/or transparent authentications on the source of requests.
- *User profiles*: If you wish to restrict access to servers defined in the SSL VPN configuration, you need to define profiles that contain the list of authorized servers, then assign them to users.

"General" tab

Enable SSL VPN: Allows enabling SSL VPN and choosing from three options offers in the table below.

Access only to web servers	Use of the SSL VPN module to access web-based resources. Enables the *Web servers* tab.
Access only to application servers	Use of the SSL VPN module to access resources on a TCP connection. Enables the *Application servers* tab.
Access to both web and application servers	Use of the SSL VPN module to access web-based and TCP-based resources. Enables both the *Web servers* and *Application servers* tabs.

Advanced properties

Access to servers via SSL VPN

Prefix for the URL root directory	Stormshield Network's SSL VPN technology enables masking the real addresses of servers to which users are redirected, by rewriting all URLs contained in HTTP pages visited. These URLs will then be replaced by a prefixed followed by 4 digits. This field enables defining the prefix to be used.
HTTP header for user ID	This field's value will be sent to the web server in the HTTP header of outgoing queries, along with the user's login. This value can be used for checks and/or transparent authentication on the source of the queries. In the event the server to which HTTP traffic is redirected requests authentication, a login can be defined in the header of the HTTP packet. This login may be useful in indicating, for example, that this traffic arriving on the server come from the firewall and can be accepted by the server without authentication.

Client workstation configuration

Command executed at startup	This command, which is executed when the applet is launched, allows the administrator to define actions to perform before displaying the applet. For example, this command may launch a script (installed on a server) which will modify the parameters of the user's mail account in such a way that when the applet is launched, SMTP and POP traffic will be automatically redirected, all without the user's intervention.
Command executed during shutdown	This command, which is launched when the applet is shut down, allows the administrator to define actions to perform before shutting down the applet. For example, this command may launch a script (installed on a server) which will modify the parameters of the user's mail account in such a way that when the applet is shut down, SMTP and POP traffic will no longer be automatically redirected, all without the user's intervention.

"Web servers" tab

This section groups the servers configured for access to web resources.

The number of web servers that can be configured varies according to the appliance model:

Model	Max. no. of HTTP servers	Max. no. of other servers
SN160(W), SN210(W), SN310	64	64
SN710	128	128
SN910	256	256
SN2000, SN2100, SN3000, SN3100, SN6000, SN6100	512	512

Adding a web server

To add a web access server, the procedure is as follows:

1 Click on **Add** then select one of the suggested servers. A screen containing server names will appear.

2 Enter a name for this server. (The field can be left empty. Allowed characters: numbers, letters, spaces, -, _, and dots.)

3 This server's configuration then appears. The different parameters are explained below.

Destination server	The object corresponding to the server accessible to the user can be specified in this field. **WARNING** Make sure that you use an object whose name is identical to the **FQDN** name of the server it refers to. If this is not the case, (e.g. object name: webmail, FQDN name: www.webmail.com), Firewall queries to this server may be refused.
Port	The port on the server accessible to the user can be specified in this field. Port 80 is defined for HTTP.
URL: access path	This URL enables going directly to the specified page.
URL used by SSL VPN	Link calculated based on 3 fields: **Destination server, Port** and **URL: access path.** (Example: http://destination server/URL: access path).
Name of the link on the user portal	The defined link appears on the Stormshield Network web portal. When the user clicks on this link, he will be redirected to the corresponding server.

Advanced properties

Enable URL whitelist	Only links that the SSL VPN module has rewritten can be accessed through SSL VPN. If, on an authorized site, there is a link to an external website whose server has not been defined in SSL VPN configuration, the authorized site will not be accessible via SSL VPN. If the white list has been activated, it will enable access to URLs which have not been rewritten through the field **Do not rewrite URLs in the category**. For example, for webmail SSL VPN access, if you wish to allow users to quit the SSL VPN by clicking on the links contained in their e-mails, you need to add a whitelist containing "*". **WARNING** If the user clicks on a link in the whitelist, it will no longer be protected by the Stormshield Network SSL VPN module.
Don't show this server on the user portal (access via another server only)	All servers configured in SSL VPN are listed on the Stormshield Network authentication portal by default. However, it may be necessary for servers to be accessible only through another server, so in this case, the option Don't show this server on the user portal has to be selected. When this option is selected during the configuration of a server, this server can be accessed via SSL VPN, but will not be on the direct-access list. A link to this server is needed in order to access it. An application can use several servers but have only one entry point, so only one link in the menu of the portal.
Deactivate NTLM	Some web servers may request authentication before the transfer of data between the server and the user. This method can be disabled for servers that do not support this authentication method for traffic passing through the firewall.

Rewrite \"User-Agent\" field (force OWA compatibility mode)	The "User-Agent" field in the header of an HTTP request contains the identifier for the web browser used. For example, on Internet Explorer: Mozilla/4.0 (compatible; MSIE 6.0 ...). Rewriting the "User-Agent" value therefore allows modifying the HTTP request in such a way that it gives the impression of coming from a different browser type. This option is particularly useful in basic mode of Outlook **Web Access** (OWA). In fact, **OWA** in premium mode (a very advanced mode), uses Webdav, an extension of HTTP. Since not all types of network equipment support these extensions (the SSL VPN module on firewalls supports OWA in premium mode), the transmission of such traffic may give rise to compatibility issues, especially on the internet. Instead of all users (internal and external) having to use a more basic mode of OWA, the option **Rewrite User-Agent** enables using "premium" OWA internally (compatibility with premium mode is easy to obtain) and using "basic" mode by passing through SSL VPN (for mobile users, via internet). Since "old" web browsers do not support these extensions, OWA therefore automatically operates in basic mode when it encounters the "User-Agent" on these browsers.
Rewrite OWA Premium mode specific code	If this option has been selected, you will enable the specific rewriting rules that allow supporting Outlook Web Access in premium mode.

Lotus Domino Web Access version 7.0.4 runs through SSL VPN tunnels. There is therefore no need to enable specific rewriting rules that would allow supporting Lotus Domino web applications.

Alternative URLs for this server (alias)

Server alias	Aliases allow indicating to the SSL VPN module that the server is known by several names and/or IP addresses. If a mail server is defined as the object "webmail.intranet.com" to which the alias "192.168.1.1" is assigned, the user will be redirected to the mail server whether he visits the link "http://webmail.intranet.com" or "http://192.168.1.1". Clicking on **Add** will display a line that will allow you to add a new alias.

Adding an OWA web server

The SSL VPN module on Stormshield Network Firewalls supports OWA (Outlook Web Access) Exchange 2003, 2007 and 2010 servers.

"Premium" mode can only be used in Windows with Internet Explorer 5 and higher. It is based on web technologies such as html, css and javascript but also on Microsoft proprietary technologies such as htc, xml and activeX.

In Exchange 2003, the links are absolute links, regardless of whether they are in HTML pages, javascripts, in XML data, or in XSL sheets, such as "http://www.company.com/index.htm".

It is therefore possible to add HTTP servers (with specific preset options for perfect compatibility with OWA) to the list of web-access servers.

To add an HTTP server-OWA, the procedure is as follows:

1 Click on **Add** then select OWA Web server 2003 (Premium mode) or OWA Web server 2007 – 2010 (premium mode). The following screen appears:

2 Enter a name for this server. (The field can be left empty. Allowed characters: numbers, letters, spaces, -, _, and dots.)

3 The preset options for an OWA 2003 premium server are: HTTP port, the field **URL: access path** with "exchange" indicated, the field **Enable URL whitelist** enabled, the field **Do not rewrite URLs in the category** with the URL group "vpnssl_owa" indicated, the field **Deactivate NTLM** and the field **Rewrite OWA Premium mode specific code**.

For an OWA 2007-2010 server, the pre-entered fields are: HTTP port, the field **URL: access path** with "owa" indicated, the field **Enable URL whitelist** with the URL category "vpnssl_owa" indicated, and the field **Rewrite OWA Premium mode specific code.**

Other options that have not been entered have to be configured in the same way as for a "normal" web-access server.

Adding a Lotus Domino web server

The SSL VPN module on Stormshield Network Firewalls supports Lotus domino servers.

An HTTP server can be added to the list of web access servers with certain options specifically pre-entered for compatibility with Lotus Domino.

The procedure for adding an HTTP-Lotus Domino server is as follows:

1 Click on **Add** then select **Lotus Domino web server**.

2 Enter a name for this server. (The field can be left empty. Allowed characters: numbers, letters, spaces, -, _, and dots.)

The following field is pre-entered option for Lotus domino servers: "http" port

"Application servers" tab

Configuration with an application server

The procedure for adding a server to access resources other than web-based resources is as follows:

1 Click on **Add** then select **Application server**.

2 Enter a name for this server. (The field can be left empty. Allowed characters: numbers, letters, spaces, -, _, and dots.)

3 This server's configuration then appears. The different parameters are explained below.

Destination server	This field allows specifying the object corresponding to the server that the user will be able to access.
Port	The port on the server accessible to the user can be specified in this field.

User workstation settings

Listening IP address (local)	Local address of the client.

Port	The JAVA applet uses this port, located on the remote workstation, to redirect encrypted traffic going to the Stormshield Network Firewall. The user must possess certain privileges on this port (to open it, for example), therefore make sure that the host's local administration rights are modified as well. Also, the specified port must be free on all hosts wishing to connect to the associated server via the portal.

Advanced properties

Enable Citrix compatibility	Enables compatibility with the Citrix web authentication portal and access via the web browser. This option is useless if the Citrix fat client is used.
Command executed at startup	This command, which is executed when the server is launched, allows the administrator to define actions to perform before displaying the server. For example, this command may execute a script (installed on a server) that will check the activity of the antivirus installed on the user's host before granting him access to the server.

Configuration with a Citrix server

1 Step 1: Creating an object for the Citrix server

Go to the object database in order to create a host and select a host.

2 Step 2: Configuring an application server

In the SSL VPN module, select the tab *Application servers*. Click on Add then select Citrix server. Give your server a name. The Citrix configuration screen will then appear.

Select the Citrix server created earlier in the objects database. (Cf. Step1)

3 Step 3: Configuring a web server

Select the tab *Web servers*.

Click on Add then select "web server ". Give your server a name. The web server configuration window will then appear:

As for the URL: access path, indicate CitrixAccess/auth/login.aspx (if it is the version Presentation Server 4.0).

4 Sending the configuration

Click on Apply.

5 Accessing the web portal

Open the web browser then identify yourself (https://your firewall's IP address or its name).

Go to "Secure access" then select "Pop up secure-access window" from the drop-down list.

WARNING

It is important for the Stormshield Network SSL VPN applet to operate as a background task.

Next, select **Portal access**\Portal then enter your username, password and domain.

Deleting a server

To delete a server, the procedure is as follows:

1 Select the server to remove

2 Click on the button **Remove**.

WARNING

When a server is removed from the list of configured SSL VPN servers, it will automatically be removed from the profiles to which it belonged.

"User profiles" tab

Operating principle

All servers configured in the SSL VPN module are listed on the Stormshield Network authentication portal by default. As such, users who have the right to access SSL VPN features on the firewall have access to all the servers configured by the administrator. The concept of using profiles enables determining which users will have access to which servers configured in SSL VPN.

Configuring a profile

Adding a profile

The procedure for adding a profile to the list of available SSL VPN profiles is as follows:

1. Click on **Add**, then specify the name of the profile.
2. From the list of "Accessible web servers" and "Accessible application servers", select the servers that will be accessible to users that belong to this profile.
3. Click on **Apply** to activate the configuration.

WARNING

Profiles cannot be created if there is not at least 1 configured SSL VPN server.

Deleting a profile

The procedure for deleting a profile is as follows:

1. Select the profile you wish to delete.
2. Click on the button **Remove**.

Using a profile

Profiles can be used in 2 ways – either as a default profile in SSL VPN configuration, or assigned to one or several users as the specific profile of these users.

Using a profile as a default profile

The procedure for using a profile as the default profile in SSL VPN configuration (users who do not have a specific profile will be assigned this default profile) is as follows:

1. Create a profile in SSL VPN\User profiles,
2. Define the profile to be used as the default profile (name of the profile and associated servers) in the configuration menu Users\VPN Access privileges \default access \SSL VPN.

Using a profile as the specific profile for one or several users

The procedure for using a profile as the specific profile for one or several users (regardless of the list of servers defined by the default profile, these users will possess a list of specific servers) is

as follows:

1 Define the profile to be used as the specific profile (name of the profile and associated servers) in **User profiles** in the SSL VPN module, then click on Apply to apply the changes.

2 In the module **Users**\VPN Access privileges \VPN access, select the user from the "SSL VPN" column, select the profile defined earlier and click on Apply.

SSL VPN services on the Stormshield Network web portal

When authentication is enabled on the firewall (module **Users\Authentication***General*, select "Enable the captive portal"), then you will be able to access Stormshield Network's SSL VPN features.

To access **SSL VPN** features, the procedure is as follows:

1 Open the web browser.

2 Indicate the URL "https:// firewall_address" in the address bar.

3 The firewall authentication page will appear; you need to log in.

4 If the you have the privileges to use VPN features, the Secure access menu will appear, enabling access to SSL VPN features.

When the authentication duration expires or access to the SSL VPN is denied, the user will be redirected to the transparent authentication page (SSO) if this method is available.

Accessing your company's web sites via an SSL tunnel

This menu displays the list of websites the administrator has configured and to which users have access.

The other methods of secure access enable accessing other secure sites configured by the administrator.

Accessing your company's resources via an SSL tunnel

This menu displays the list of other servers the administrator has configured and to which users have access.

> **WARNING**
>
> No links are available on this page. However, this window must be kept open throughout the duration of the connection (the window can be reduced), otherwise the connection will be lost.

To access resources the administrator has configured, it has to be indicated to the client software (e.g. a mail client) that the server to which he has to connect to retrieve mail is no longer the usual mail server. An address like "127.0.0.1: Listening_port" where "Listening_port" is the port specified on the server configuration, has to be indicated.

The listening port for each configured server will be displayed on the Stormshield Network web portal page.

MULTICAST ROUTING

Multicast routing allows distributing network traffic from one source to several destinations. The source and destinations will then be placed in a "multicast group".

This type of routing is used for tele-seminar applications (no interaction with recipients), teleconferences (each member of the group can be a traffic source), routing table distribution for the RIPv2 protocol, remote network booting (BOOTP protocol), etc.

IMPORTANT

Static multicast routing has priority over all other types of routing (static routing, dynamic routing, routing in a bridge, policy-based routing, etc).

This button makes it possible to enable or disable multicast static routing.

Actions on multicast routing policy rules in IPv4

The table allows you to define the rules in the multicast routing policy to 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	This button allows inserting 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 line before the line just above it.
Move down	Places the selected line after the line just below it.
Cut	Allows you to cut a routing rule in order to move it.
Copy	Allows you to copy a routing rule in order to duplicate it.
Paste	Allows you to duplicate a routing rule after having copied it.

Interactive features

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

The table

The table sets out the list of static multicast routing rules and their statuses:

Status	Status of the static multicast route: Enabled: Double-click to enable the route created. Disabled: The route is not functional.
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.

STORMSHIELD MANAGEMENT CENTER

If you have installed the Stormshield Management Center centralized administration server, this panel will allow you to install the attachment 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 attached 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 attached to an SMC server may be overwritten when a new configuration is sent from the SMC server.

Attaching the firewall to SMC

Select the attachment package. Choose the SMC attachment package from the centralized administration server.

Buttons

Install the package: When an attachment package has been selected, this button will download and install it on the firewall.

Once the package has been installed, information regarding the attachment 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, please refer to the *Stormshield Management Center administration guide*.

SYSTEM EVENTS

In this module, you will be able to define in your configurations 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.

Username	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 concerned 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 concerned 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	**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. **Quarantine host:** the packet that caused the alarm will be blocked with the following parameters. To remove a packet from quarantine, use Stormshield Network Realtime Monitor. • **for a period of (minutes)**: duration of the quarantine

GENERAL NOTE

When you modify 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.

System alarms list

ID	Name	Description
1	System shutdown	System shutdown
2	Authentication failed for	Authentication failed for
3	Connection terminated for	Connection terminated for
4	20% left in log file	20% left in log file
5	Connection established for	Connection established for
6	IPsec phase 1 failed	IPsec phase 1 failed
7	IPsec phase 2 failed	IPsec phase 2 failed
8	IPsec pre-shared key not found	IPsec pre-shared key not found
9	Firewall startup	Firewall startup
10	HA: Mode change	HA: Mode change
11	HA: Peer lost	HA: Peer lost
12	Invalid CRL	Invalid CRL
13	Invalid Certificate	Invalid Certificate
14	log partition has changed	log partition has changed
15	System error	System error
16	User denied in IPSEC negotiation	User denied in IPSEC negotiation

17	Antivirus: update failed	Antivirus: Update failed
18	Antivirus: update successful	Antivirus: Update successful
19	LDAP unreachable	LDAP unreachable
20	DNS error	DNS error
21	Certificate Revocation List is expired	Certificate Revocation List is expired
22	Certificate Revocation List expires in less than 3 days	Certificate Revocation List expires in less than 3 days
23	RAID alert:	RAID alert:
24	Watchdog has rebooted firewall	Watchdog has rebooted firewall
25	System date corrupted at boot	System date corrupted at boot
26	System updated	System updated
27	System date has been changed	System date has been changed
28	Many authentication failures	Many authentication failures
29	Backup dialup(s) activated	Backup dialup(s) activated
30	Client connection on local PPTP server established for	Client connection on local PPTP server established for
31	Client connection on local PPTP server terminated for	Client connection on local PPTP server terminated for
32	Authentication failed on local PPTP server for	Authentication failed on local PPTP server for
33	No PPPoE peer has answered for	No PPPoE peer has answered for
34	Your release is old, check that you are up to date.	Your release is old, check that you are up to date.
35	This dynamic DNS client configuration has been tagged invalid:	This dynamic DNS client configuration has been tagged invalid:
36	This dynamic DNS client configuration has bend successfully updated:	This dynamic DNS client configuration has bend successfully updated:
37	Interface up:	Interface up:
38	Interface down:	Interface down:
39	Server switched:	Server switched:
40	Custom event:	Custom event:
41	Active Update: update successful	Active Update: Update successful
42	Active Update: update failed	Active Update: Update failed
43	Active Update: your license has expired	Active Update: your license has expired
44	Antivirus failed:	Antivirus failed:
45	Too many Authentication failures:	Too many Authentication failures:
46	DHCP interface got a new IP address:	DHCP interface got a new IP address:
47	DHCP interface has released its IP address:	DHCP interface has released its IP address:
48	Restoring configuration from USB token:	Restoring configuration from USB token:
49	Installation of the secure configuration:	Installation of the secure configuration:
50	USB error:	USB error:
51	Activation error:	Activation error:
52	The event returned an unhandled error code:	The event returned an unhandled error code:
53	The following slot activation did not succeed:	The following slot activation did not succeed:
54	System was not properly halted	System was not properly halted

55	DNS cache is cycled too quickly	DNS cache is cycled too quickly
56	Get CRL failed	Get CRL failed
57	Invalid CRL	Invalid CRL
58	Invalid QoS queue in the filtering slot	Invalid QoS queue in the filtering slot
59	Configuration has been modified	Configuration has been modified
60	Configuration has been validated	Configuration has been validated
61	L2TP:	L2TP:
62	Error while validating configuration	Error while validating configuration
63	Invalid password for configuration	Invalid password for configuration
64	HA: PVM database sync failure	HA: PVM database sync failure
65	Globalgen : hardware configuration file created	Globalgen : hardware configuration file created
66	Problem reported on hard disk:	Problem reported on hard disk:
67	Network: Unexpected media type change	Network: Unexpected media type change
68	License Update: A new license is available	License Update: A new license is available
69	License Update: Temporary license, need to register	License Update: Temporary license, need to register
70	License Update: Download error	License Update: Download error
71	License Update: New license installed	License Update: New license installed
72	License Update: New license installed: need reboot	License Update: New license installed: need reboot
73	License: a feature has expired :	License: a feature has expired :
74	License: remaining days before expiration of	License: remaining days before expiration of
75	This address is banned from webadmin access : bruteforcing detection	This address is banned from webadmin access : bruteforcing detection
76	IPsec failover: peer is dead, switching to other peer	IPsec failover: peer is dead, switching to other peer
77	LDAP Base backend LDBM not supported. Ldap restore not performed	LDAP Base backend LDBM not supported. Ldap restore not performed
78	The webadmin portal is under brute force attack	The webadmin portal is under brute force attack
79	Configuration Migration:	Configuration Migration:
80	Patterns database is corrupted, you should try to update it with the force option	Patterns database is corrupted, you should try to update it with the force option
81	HA: Can't synchronize reports: Some firewalls have a log disk while others don't	HA: Can't synchronize reports: Some firewalls have a log disk while others don't
82	Remote host reachable:	Remote host reachable:
83	Remote host unreachable:	Remote host unreachable:
84	Aggregated link up:	Aggregated link up:
85	Aggregated link down:	Aggregated link down:
86	Backup successful	Backup successful
87	Backup failed	Backup failed
88	Power:	Power:
89	Connection error with agentAD:	Connection error with agentAD:
90	Topology change	Topology change
91	Malicious file has been detected, hash:	Malicious file has been detected, hash:
92	Remote service is no longer reachable:	Remote service is no longer reachable:

93	Remote service is reachable:	Remote service is reachable:
94	An error occurred loading a proxy functionality:	An error occurred loading a proxy functionality:

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** module contains 2 tabs:

- **Configuration**: this tab allows you to enable temporary account management and define a default validity duration for accounts,
- **List of temporary accounts**: this tab allows creating/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**. 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;

URL FILTERING

This module consists of 2 zones:

- A zone for profiles,
- A zone for URL filter rules.

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 "Default" by default, accompanied by its number.

Examples:

- Defaut00
- (1) Default01 ...

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 (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. 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 (**Web Objects** 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.

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.

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: **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. **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 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 category 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.

REMARK

The characters "[ ]" and "{}" are no longer allowed in URLs (Internet Explorer 7 and 8).

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 the creation of user accounts at the firewall level. To access the features of this module, you must first create or configure your LDAP base (see document *Directory configuration* or module **Users\Directory configuration**).

The accounts contain all the information relating to these users:

ID

- Name
- First name
- E-mail address (optional)
- Phone number (optional)
- Description (optional)

The Users screen consists of 2 parts:

- A banner showing the various options
- The list of **CNs** (or users) in the left column, accompanied by information about them in the right column.

These are the tables indicating the maximum number of users that can be authenticated simultaneously according to the model of your firewall:

Model - SN range	SN160(W)	SN210(W)	SN310	SN510	SN710
Max. no. of users	15	30	50	100	200

Model - SN range	SN910	SN2000	SN2100	SN3000	SN3100	SN6000	SN6100
Max. no. of users	500	1,000	2,000	2,500	4,000	15,000	15,000

Model - V range	EVA1	EVA2	EVA3	EVA4	EVAU
Max. no. of users	50	100	200	500	6,000

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

Possible operations

Search bar

Enter the name of the particular user or user group you are looking for.

The search field will list all users and/or user groups with first names, last names and/or logins that correspond to the keywords entered.

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 will offer you the following choices:

Groups and users	Represented by the icon , this option allows displaying all users and user groups in the list of CNs on the left.
Users	Represented by the icon , this option allows displaying only users in the left column.
Groups	Represented by the icon , this option allows displaying only user groups in the left column.

Interactive features

Some operations listed in the taskbar can be performed by right-clicking on the table of users / groups (CN table):

- Adding users,
- Adding groups,
- Deleting (the user or the selected group),
- Checking usage (of the user or the selected group).

Creating a group

The **Users** module allows you to enter information about the group you wish to create in the right column.

Group name	Give your group a name in order to identify it in the list of CNs. **REMARK** 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.

CN

Filter (search bar)	You can enter a character string in order to filter the list of members, or clear the field to see the whole list.
Add	Users can be added to a group in 2 ways: When you click on **Add**, a new line will appear at the top of the table. Expand the list of existing users with the help of the arrow on the right and select the user you wish to add to the group. You can also drag and drop users by importing them from the list of CNs in the left column.
Delete	To remove a member of the group, select it and click on **Delete**. When a user is deleted, the administrator will be prompted to revoke his certificate.

To confirm the creation of your group and to save changes made, click on **Apply**.

Creating a user

To create a user, enter at least a login and a name. To associate a certificate with this user, you will need to indicate a valid e-mail address.

ID	User's login
Name	User's last name
First name	User's first name
Mail	User's e-mail address, This will be useful for creating certificates.
Phone number	User's telephone number
Description	Description of the user

REMARK

The fields "ID", "First name" and "Last name" cannot be modified after the user is created.

To confirm the creation of your user and to save changes made, click on **Apply**.

A window that allows creating a password for this user will then appear:

Password	Enter the user's password.
Confirm password	Confirm password
Mandatory password strength.	A gauge indicating the strength of the password will appear.

Click on **Apply** in this window to confirm the creation of the password.

REMARK

The creation of the user's password is not mandatory. Simply click on **Cancel** in the window to skip this step.

Delete

This button allows deleting a user or a group:

1. Select the user or group to be deleted.
2. A window will appear with the message "Delete the user <name of user>?". Select **Yes** to proceed.

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.

List of users (CN)

If you wish to access a user's data, select the user in the list of CNs on the left. The information concerning this user will appear in the right column.

"Account" tab

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 the user to modify his password himself, go to the menu **Users**\ **Authentication** module*Internal (or external) interfaces* tab**User passwords** and select the option Users can change their passwords.
Access privileges	This shortcut makes it possible to display the user's access privileges directly in the **Users > Access privileges** module.
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
Mail	E-mail address of the selected user.
Telephone number	Telephone number of the selected user
Description	Description of the selected user.

"Certificate" tab

This tab will allow you to manage the user's x509 certificate.

Since the PKI does not have a certificate authority by default, you will need to create one in order to manage user's certificates: go to the menu **Objects**\ **Certificates and PKI**\ Add\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. Click on the group of your choice. It will be added to your table.

To remove a group, select it and click on **Delete**.

A user attached to several departments, for example, may belong to numerous groups. The maximum number is 50 groups per user.

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

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

Creating or modifying an IPSec interface (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 allow, for example, making 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

Search	Search that covers interfaces.
Add	Adds an "empty" 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	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 virtual IPSec interfaces:

- Add,
- Delete,
- Check usage.

Presentation of the table

The table sets out five 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 IPSec interface a name. **NOTE** Please refer to the section Allowed names to find out which characters are allowed and prohibited in various fields.
IPv4 address (mandatory),	Enter the IP address assigned to the virtual interface created.
IPv4 mask (mandatory),	The default value suggested is 255.255.255.252. Since virtual IPSec interfaces are meant for setting up point-to-point tunnels, a network that allows assigning two addresses is sufficient in theory. This value may however be customized.
Protected	Double-click on this cell to modify the interface type: Protected Public
Comments (optional)	Any text.

Creating or modifying 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 an "empty" 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	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 GRE interfaces:

- Add,
- Delete,
- Check usage.

Presentation of the table

The table sets out seven 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 GRE interface a name.
IPv4 address (mandatory),	Enter the IP address assigned to the virtual interface created.
IPv4 mask (mandatory),	The default value suggested is 255.255.255.252. Since virtual GRE interfaces are meant for setting up point-to-point tunnels, a network that allows assigning two addresses is sufficient in theory. This value may however be customized.
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.

VULNERABILITY MANAGEMENT

In this menu, you will be able to configure your policy for managing vulnerabilities that may appear on your network.

You can assign a detection profile to a host, network, group or address range. There are 12 pre-configured profiles by default.

The configuration of vulnerability management therefore simply consists of:

- Linking network objects to detection profiles and
- Deciding which recipients will receive vulnerability reports.

The **Vulnerability management** configuration screen comprises 2 zones:

- A **General configuration** zone: it contains a checkbox for enabling the module and various items for the general configuration.
- **Advanced properties:** an area for determining data lifetime and excluded objects.

WARNING

The index of applications is based on the IP address of the host initiating the traffic.

A single IP address shared by several users can create a heavy load on the module. This happens for example, when an http proxy, a TSE server or a router that performs dynamic NAT from the source, is used. It is therefore recommended that these shared IP addresses be placed in the exclusion list.

General configuration

Enable application and vulnerability detection

If this option is selected, vulnerability detection will be enabled and the relevant information will be visible in Stormshield Network REAL-TIME MONITOR.

REMARK

During the update (if you have purchased the license), the Vulnerability management module will be enabled by default. Alarms will be raised according to the default configuration: monitor all vulnerabilities for all internal hosts.

WARNING

Remember to update the vulnerability database in System\Active Update. Without a database that is up to date, the service may not run correctly.

Vulnerability detection relies on the analysis of network traffic. This allows detecting an application and/or a flaw, from the moment the user first uses the network.

Send simple reports to

Group of e-mail addresses to which summary reports will be sent.

These reports are brief and contain a summary of the vulnerabilities by product and the hosts affected.

Send detailed reports to	Group of e-mail addresses to which comprehensive reports will be sent. Detailed reports contain a summary of vulnerabilities, as well as their detailed descriptions (family, client, possibility of remote exploitation) and a link to their references in the Stormshield Network knowledge base, which generally includes instructions regarding the bug fix to apply.

REMARK

E-mail address groups can be configured in the menu: **Notifications\E-mail alerts** *Recipients* tab.

List of monitored network objects

The list of monitored objects is displayed in the table together with the detection profiles assigned to them.

Network object (host or group – network – address range)	Selects the network object to which monitoring applies. This object will be scanned by the Stormshield Network Vulnerability Manager engine which will rely on the rules contained in the associated detection profile. The type of object linked to the profile can only be a host, host group, network or address range. **WARNING** The list of monitored objects will be applied in order. This means that if a network object appears several times in this list, only the first detection profile will be applied. **REMARK** Objects can be created within the column using the button on the far right of the field in a new line.
Detection profile	Allows selecting a profile to restrict the applications to be monitored. The profile can be selected in the drop-down list of the column, which appears by clicking on the arrow on the right, when you add a new line to the table. (See **Add** button below)

Several actions can be performed in this table:

Add	This button allows you to add a network object and a profile associated with this object in the list of monitored objects. By clicking on this button, a blank line will appear in the table.
Delete	Select the object-profile pair to be deleted, then click on this button. **WARNING** You will not be asked to confirm the deletion of the profile.
Move up	Allows raising the priority of the association between a network object and a profile.
Move down	Allows lowering the priority of the association between a network object and a profile.

Below is the list of profiles and vulnerability families that will be detected and reported:

SERVERS	CLIENT APPLICATIONS AND OPERATING SYSTEMS	CLIENTS	TOOLS
Servers: SSH Servers –HTTP Servers / Web – Database Servers – FTP Server – Mail Servers and Operating Systems **Servers – critical flaws**: SSH-Web-Apps-DB-DNS-Web Server-FTP Server-Misc-Mail Server-P2P-OS	**Client applications and operating systems (OS)** **Client applications and operating systems (OS) – critical flaws**	**Mail client**: Client, Mail (Thunderbird, Outlook, e-mail …)	**Security tools**: Antivirus, Security tools and Vulnerability scanner or Network scanner
FTP Servers		**Browsers and other web clients**: Web clients, RSS feed readers	**Administration tools**: Administration client FTP, SSH etc.
Mail servers			
Web servers: web/HTTP content servers			
Database servers (SQL)			

"All known applications" profile

This profile allows assigning to an object (host, group, network or address range), the detection of all client/server and operating system vulnerabilities detected by the Stormshield Network Vulnerability Manager.

Advanced configuration

Data lifetime (days) [1 – 30]: Duration for which data (application, vulnerability) will be kept without traffic or updates detected.

Exclusion list (unmonitored objects)

Network object (host or group – network – address range)

Once objects have been associated with their profiles, one or several objects can be excluded from the analysis.

As such, regardless of the configuration of the monitored objects, the members of this exclusion list will not be monitored.

Objects to be excluded can be selected in this table by clicking on **Add**.

WARNING

The application inventory carried out by Stormshield Network Vulnerability Manager is based on the IP address of the host that initiates traffic in order to index applications.

For hosts that have an IP address shared by several users, for example an HTTP proxy, a TSE server or even a router that performs dynamic NAT on the source may cause a significant load on the module. You are therefore advised to place the addresses of these hosts in an exclusion list (unsupervised elements).

WEB OBJECTS

There are two types of URL and certificate categories: customized categories (entered manually by the administrator) and dynamic categories. The URL database provider that provides dynamic URL categories is Stormshield Network by default.

This module offers the creation of customized URL or certificate categories, and groups that may contain customized and dynamic categories. This module also allows entering the URL database provider.

For a given category, e.g. “banks”, which contains the most frequently visited URLs of banks, a rule can be created in **URL filtering** (**Security policy**\URL filtering) to block access.

Therefore, when you attempt to connect to your bank’s website, a block page will appear, with an error message. (See the module **Notifications****Block messages***HTTP block page*).

REMARK

In filter policies, it is better to use dynamic categories provided by URL databases, as they are richer and perform better than customized URL lists.

This module consists of 4 tabs:

- *URL*: Allows grouping URLs by category (e.g.: “shopping”, “pornography”, “videogames”). Each of these categories groups together a certain number of website URLs, which may be blocked or allowed, depending on the desired action.
- *Certificate (CN)*: Allows creating categories to recognize the certificates assigned to secure websites, for use in SSL filtering.
- *Groups of categories*: Offers the creation of URL or certificate category groups from the customized or dynamic categories (URL database).
- *URL database*: Depending on le type of option subscribed, the available URL lists are updated by different providers (Stormshield Network or Stormshield Network Extended Web). Stormshield Network’s URL lists are offered by default.

To find out which characters are allowed or prohibited in various fields, please refer to the section Allowed names.

“URL” tab

This tab provides an overview of customized categories and their classified URLs.

URL category table

The URL category screen consists of 2 parts: a first part for URL customized categories and a second part for the URLs.

When configuring these categories, you can perform the following actions:

Add a customized category	Creates a new category. By clicking on this button, a new line will appear, allowing you to indicate the name of the category and comments if necessary.
Delete	Deletes an existing category. Select the line to be deleted and click on this button. A following message will appear and if the category is in use, the message will inform you and ask you what you wish to do.

Check usage	Allows checking if the selected category is used in a configuration. When you click on this button, a panel will appear in the module directory to indicate the modules that use the URL of this category.
Check URL classification	Allows checking whether a URL belongs to a category. This search will be conducted in the customized and dynamic categories as well. This will help to determine if it needs to be added to a category. When you click on this button, a panel will appear at the bottom of the tab and display the categories that contain this URL.

The table sets out the elements indicated below:

URL group	Name of the URL category.
Comments	Description of the URL category.

REMARK

The number of characters for a URL category is restricted to 255.

URL table

Format

The list of **Characters allowed** and the following syntax indications are valid only for URLs. URL categories are not affected by format restrictions.

A URL mask may contain wildcards and use the following syntax:

*	replaces a character string. **Example:** *.company.com allows defining the internet domain of the company called COMPANY.
?	replaces a character. **Example:** ???.company.com is equivalent to www.company.com or to ftp.company.com but not to www1.company.com.

A URL mask can contain a full URL (**example**: www.company.com*) or keywords contained in the URL (**example**: *mail*).

You can also filter file extensions:

Example: the URL mask '*.exe' will filter executable files.

URL table

The following actions may be carried out in the configuration of URL categories:

Add a URL	Adds a URL to a category. First, select the category to which you wish to add a URL in the left column, then click on this button.
Delete	Deletes a URL from a category. First, select the category from which you wish to delete a URL in the left column, then click on this button.

The table sets out the elements indicated below:

Name of the URL	Name of the URL. Wildcards may be used.
Comments	You can add a comment in this field to describe each URL listed.

"Certificate name (CN)" tab

This screen offers the creation of certificate name categories, which may be useful for SSL filtering (see the module **Security policy\SSL filtering**). It consists of 2 parts: one for categories, one for certificates.

As for the buttons, the screen layout is similar to the layout in the *URL* tab. The list on the right contains the names of certificates (CN) and any associated comments.

The only difference regards the meta-characters (wildcards) which have additional syntax indications:

The characters "*" and "?" are only allowed at the beginning and followed by a "."
Example: *.company.com

NOTE

The number of characters for CN categories is restricted to 255.

"Groups of categories" tab

Table of groups

This screen allows creating groups of URL or certificate categories.

- A **URL category group** may contain customized or dynamic URL categories (URL database).
- A **Certificate category group** may contain customized or dynamic certificate categories (URL database).

It consists of 2 parts: one of the groups, and a second for the contents of the groups.

Search	The search field allows you to find category groups by letter or with keywords.
Filter	This button allows selecting which object types to display. A drop-down menu allows you to display only URL category groups or Certificate category groups.
Add	Creates a new group. A window appears when you click on this button, allowing you to choose between creating a URL category group or a Certificate category group. Indicate the name of the group and comments in the relevant field. The left column lists the customized categories (URLs or certificates) and the known dynamic categories (URL database). Select the categories to integrate into the group in the left column and copy them using the arrows in the right column listing the objects contained in the group.
Delete	Deletes an existing group. Select the line to be deleted and click on this button. A confirmation message will appear and if the group is in use, a warning message will ask you again what you wish to do.
Check usage	Allows checking whether the group selected earlier is being used in a configuration. When you click on this button, a panel will appear in the tree structure of the modules and indicate the modules that use this group.

Details

The fields in this section allow editing the name of the group and adding comments, if any.

The table summarizes all the customized or dynamic categories contained in the group selected in the left column. The button **Edit this group** shows a window similar to the creation window, allowing categories to be added to or deleted from the group.

"URL database" tab

This tab allows changing the URL categories provider/certificate name.

According to the type of option subscribed (**See Stormshield Network's current pricing policy**), the available URL lists are updated dynamically by a URL database provider. When a "standard" maintenance service is subscribed, by default, **Stormshield Network** URL lists will be suggested.

The new provider **Extended Web Control** offers a URL database hosted in the cloud. The advantage of this URL filter is its higher quality compared to the embedded solutions.

If you have subscribed to the option **Stormshield Network EWC**, in order to enable the URL filter feature on Extended Web Control URL lists, select the entry from the list of suggested providers.

URL database provider By default, **Stormshield Network**'s URL database will be selected.

Updates for Stormshield Network URL lists can be downloaded from the **Active Update** module. This module allows you to modify the addresses of update servers if a mirror site is used.

A box below the drop-down list displays the information concerning the URL categories of the provider currently in use (names of categories and their descriptions).

NOTE

If the provider has been changed, a warning message will appear, informing the user that any URL filter policy using a category from the current provider will cease to operate. During the migration, you are advised to apply a URL filter policy that does not involve URL categories that are about to be deleted. This is due to different category names according to the URL databases.

Likewise, older URL filter policies with rules containing **Extended Web Control** categories have to be rewritten with the categories from the Stormshield Network Extended Web Control database.

If the servers are temporarily inaccessible, a page will indicate that the query mechanism for the classification of the site will be automatically relaunched.

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);

IPv6 Support

Support for IPv6, offered in this new 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 NEXUS 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. They can also be looked up in the SN Real-Time Monitor application.

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 version 1.0, the following are features that will not be available for IPv6 traffic:

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

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.

Interfaces

Modifying a bridge

"Configuration of the interface" tab

IPv6 address range

In Stormshield Network version 1.0, IPv6 addresses assigned to the bridge must be static addresses.

IP address	IP address assigned to the bridge. (All interfaces contained in the bridge will have the same IP address).
Net Mask	Mask of the network to which the bridge belongs. The various interfaces belonging to the bridge have the same IP address: all networks connected to the firewall are therefore part of the same address range.
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.

"Router Advertisement (RA)" 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.

Router advertisement

Send RA if DHCPv6 enabled	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 advertisement settings

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.

Creating a bridge

Address range

IPv4 address	When this option is selected, the bridge will have an IPv4 address. If this address is static, this has to be indicated in the field below the checkbox along with its network mask. By default, a dynamic address will be assigned to it via DHCP.
IPv6 address	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.

Modifying an Ethernet interface (in bridge mode)

Address range

Hybrid resolution	When this option is selected, the interface must have at least an IPv4 address (dynamic or static) and an IPv6 address (static). In this case, you will need to indicate these IP addresses and their associated network mask in the tables "IPv4 address range" and "IPv6 address range".

IPv6 address range

IP address	IP address assigned to the interface.
Net Mask	Mask of the sub-network to which the interface belongs. The network mask provides the firewall with information about the network to which it belongs.
Comments	Allows adding comments on the address range of the interface.

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.

"Advanced properties" tab

Routing without analyzing

Authorize without analyzing	Allows IPv6 packets to move between the interfaces of the bridge. No higher scan 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.

Modifying an Ethernet interface (advanced mode)

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	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	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 "**Modifying an Ethernet interface (in bridge mode)**".

Creating a VLAN

VLAN attached to a single interface (VLAN endpoint)

Address range

IPv4 address	When this option is selected, the VLAN will have an IPv4 address. If this address is static, this has to be indicated in the field below the checkbox along with its network mask. By default, a dynamic address will be assigned to it via DHCP.
IPv6 address	When this option is selected, the VLAN 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.

VLAN attached to 2 interfaces (crossing VLAN)

VLAN address range

Use an existing bridge	When this option is selected, you will need to select from the drop-down list the bridge to which the VLAN will be attached.
Create a new bridge	When this option is selected, a wizard will allow you to create a new bridge containing both of the interfaces to which the VLAN is attached.
IPv4 address	When this option is selected, the VLAN will have an IPv4 address. If this address is static, this has to be indicated in the field below the checkbox along with its network mask. By default, a dynamic address will be assigned to it via DHCP. This option is only available if you have chosen to create a new bridge.
IPv6 address	When this option is selected, the VLAN 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. This option is only available if you have chosen to create a new bridge.

Modifying a VLAN

"Configuration of the interface" tab

Address range	
Hybrid resolution	When this option is selected, the interface must have at least an IPv4 address (dynamic or static) and an IPv6 address (static). In this case, you will need to indicate these IP addresses and their associated network mask in the tables "IPv4 address range" and "IPv6 address range".

"Router Advertisement (RA)" tab

For options regarding Router advertisements, please refer to the paragraph "Router advertisement (RA)" tab in the menu **Modifying a Bridge**.

"Advanced properties" tab

For advanced VLAN configuration options please refer to the paragraph "Advanced configuration" tab in the menu **Modifying an Ethernet interface (in bridge mode)**.

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).
Color (Optional)	A window will appear, allowing the selection of an interface color (used in Stormshield Network REAL-TIME MONITOR).
(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 eternal 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, HTTP cache, URL filtering, SMTP filtering, FTP filtering or SSL filtering)	[Rule X] Application inspections will only apply to IPv4 traffic.

Allowed or prohibited names

These are the characters allowed or prohibited on items saved on your firewall:

Firewall name

Firewall name must contain less than 127 characters. Allowed characters are:

```
<alphanum> - _ .
```

Login and password

- Login (prohibited characters):

```
" <tab> & ~ | = * < > ! ( ) \ $ % ? ' ` <space>
```

- PPTP login (allowed characters):

```
<alphanum> - _ .
```

- Password (prohibited characters):

```
" <tab> <space>
```

Comments (prohibited characters)

```
" # @ < >
```

Rules separators (prohibited characters)

```
>
```

Interface names

- Names of interfaces may not 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
```

- Names must not begin with the following prefixes:

```
firewall network serial loopback
```

- Names must not be a reserved word:

```
Ipsec dynamic sslvpn any protected notprotected
```

- Names must not contain the following characters:

```
@ " # <tab> <space>
```

Objects

- Prohibited characters:

```
<tab> <space> | ! " # , = @ [ \ ]
```

- Prohibited prefixes:

```
Firewall_ Network_ ephemeral_ Global_
```

- Prohibited names:

```
any internet none anonymous broadcast all
```

DNS (FQDN) name objects

Prohibited characters:

```
*
```

Certificates

Certificate Authority name (prohibited characters):

```
` " : _ [ / ]
```

Users

- User name in the database (prohibited characters):

```
<tab> " , ; & ~ | = * < > ! ( ) \
```

- Name of the group in the User database (prohibited characters):

```
<tab> <space> & ~ | = * < > ! ( ) \ $ % ! ' " `
```

- LDAP database path: DN, CA Dn and consort (prohibited characters):

```
" & ~ | * < > ! ( )
```

IPSEC VPN

Name of the IPSec peer (prohibited characters):

```
# = @ [ \ ]
```

SSL VPN

- Web server login (allowed characters):

```
<alphanum> - _ . :
```

- Prefix of the URL's root directory: (allowed characters):

```
<alphanum> - _
```

E-mail alerts

Name of e-mail groups (prohibited characters):

```
<tab> <space> | ! " # , = @ [ \ ]
```

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.

All fields are separated by commas. Optional empty fields will be included between two commas.

Host

- Type of object (mandatory): **host**,
- Name (mandatory): text string using only accepted characters (see section 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 section 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 section 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 section 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 section 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"

Range port

- Type of object (mandatory): **service**,
- Name (mandatory): text string using only accepted characters (see section 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 section 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 section 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 section 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"

STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2020. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.