Stormshield Network Security

UTM / NG-Firewall Software Suite

Version 4

EAL4+ Security Target

Document version: 4.8

Reference: SN_ASE_sectarget_v4

Date: 07/08/2023

TABLE OF CONTENTS

TABLE OF ILLUSTRATIONS

1 ST INTRODUCTION

The aim of this section is to provide accurate identification and reference information for this document and the product being evaluated. Tis section also provides an overview of the features on the Stormshield appliance and specify the scope and limits of the evaluation.

1.1 ST Reference

Title:	Stormshield Network Security UTM / NG-Firewall Software Suite version 4 EAL4+ Security Target
Reference of the ST:	SN_ASE_sectarget_v4
Version of the ST:	4.8

1.2 TOE Reference

Target of evaluation:	UTM / NG-Firewall Software Suitefor Stormshield appliances
Version of the TOE:	4.3.12.2 (S, M, XL)
Security assurance package:	EAL4 augmented with ALC_FLR.3.

1.3 TOE Overview

Stormshield Network Security UTM / NG-Firewalls are appliances that provide security features allowing the interconnection between one or several trusted networks and an **uncontrolled network**, without compromising the level of security of the trusted networks.

The main features of the Stormshield UTM / NG-Firewall Software Suite, which equips these appliances, consist of two main groups:

- the firewall feature grouping: filtering, attack detection, bandwidth management, security policy management, audit, accountability and strong authentication of administrators,
- the VPN (Virtual Private Network: encryption and authentication) feature implementing [ESP] in IPSec tunnel mode and securing the transmission of confidential data between remote sites, partners or mobile salespersons.

ASQ (Active Security Qualification) is a real-time intrusion prevention technology embedded in all Stormshield appliances in the Stormshield Network Security range. Based on a multi-layer analysis, ASQ detects and prevents the most sophisticated attacks without affecting the performance of the Stormshield appliance and considerably lowers the number of false positives. This technology is backed up by alarm features which can be fully customized.

In order to offer strong authentication features for administrators, the Stormshield UTM / NG-Firewall integrates a user database and offers authentication services with it.

Via an intuitive and user-friendly graphical interface, the Stormshield Web Manager administration tool allows installing and configuring Stormshield appliances, and offers simplified monitoring and reporting features.

1.4 TOE Description

1.4.1 IT security characteristics of the TOE

1.4.1.1 Overview

The process of securing the interconnection between trusted networks belonging to an organization and an **uncontrolled network** requires the organization's ISS manager to define an **internal security policy**, summarizing or referencing the "laws, regulations and practices that govern how assets, especially sensitive information, are managed, protected and shared" in the organization [ITSEC].

The internal security policy may impose technical requirements on the network and restrictions on physical, personnel-related or organizational measures in its operating environment. The **Stormshield UTM / NG-Firewall Software Suite,** in the context of the evaluation, aims to meet the technical requirements of information flow control through advanced filter functions and VPN encryption features.

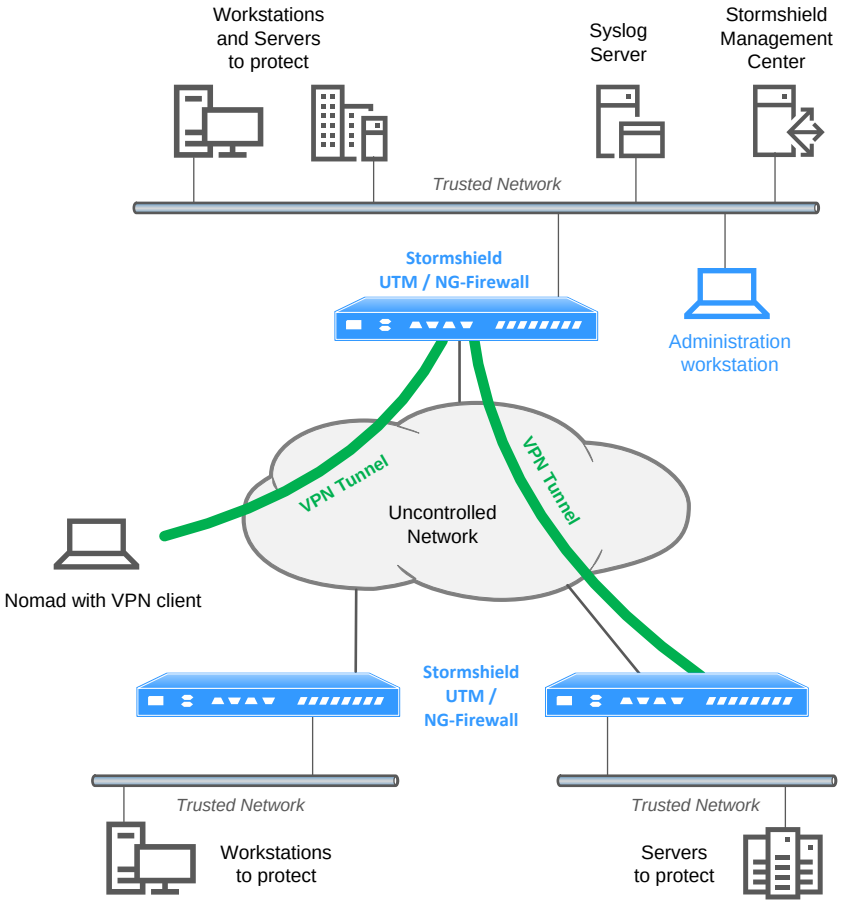


Illustration 1: Example of use of the TOE.

In the network infrastructure example shown above, Stormshield appliances are deployed to the boundary between a **trusted network** and an **uncontrolled network**. They protect workstations and the servers connected to the trusted networks, by controlling information flows that passes through this boundary.

They also implement VPN tunnels on the uncontrolled portion of the network where such information flows are transmitted, between both appliances as well as between an appliance and a mobile workstation equipped with a VPN client connected to the uncontrolled network.

Remote administration workstations can log on to the uncontrolled network or to a trusted network.

1.4.1.2 Roles

Different roles may use or manage the TOE:

- A **user** is a person using IT resources on trusted networks protected by the TOE from other trusted networks or from an uncontrolled network.
- An **IPSec User** is a user acting as a VPN Peer with a mobile client.
- An **administrator** is a person qualified who has the ability to enable, disable, modify the behavior of the security functions of the Stormshield appliance, or to read logs, as defined in is profile.
- An **auditor** is an administrator qualified to perform security audit operations and audit log management.
- The **super-administrator** is an authorized administrator who has full privileges over the configuration of the Stormshield appliance: he is the only person allowed to log on using the local console and to define the profiles of other administrators. He accomplishes this task during installation or maintenance phases.

1.4.1.3 Information flow control

The above set of requirements is the reason that UTM products exist. The internal security policy must enable one to deduce:

- which **entities** (**users** or IT agents) are entitled to set up information flows with which other entities, in what is called the **filter policy**.
- from among the streams of authorized information flows, which ones require the protection of confidentiality and integrity, and the nature of such protection (protocols and encryption algorithms), in what is called the **encryption policy**.

Depending on each case, the rules of this **encryption and filter policy**, also known as the **information flow control policy**, can be expressed in more or less sophisticated criteria: source and destination IP addresses, number of the IP protocol used, source/destination TCP/UDP port, SCTP associations.

The Stormshield UTM / NG-Firewall Software Suite provides the following **filter features**:

- Filtering of traffic between appliances (*stateful inspection*) based on characteristics at the IP and transport level: IP protocol number, source and destination IP addresses, source and destination ports.
- Traceability of information flows to entities that initiated it through the generation of audit data.

The **encryption functions** are the ones provided in standard by ESP in IPSec tunnel mode [ESP, IPSec] associated with the protocol for negotiating security settings and IKE session keys ([IKEv2]):

- Confidentiality of the contents of information flows;
- Anonymity of traffic endpoint devices;
- Integrity of traffic contents: integrity of packets, protection against replay, authentication of the sender of the encrypted packet;
- Mutual authentication of tunnel endpoints (i.e. the portion of information flows on which encryption has been applied).

The interoperability of the VPN module of Stormshield UTM / NG-Firewall Software Suite allows interconnecting disparate IPSec encryption systems.

Both of these large functional sets are completed by **alarm features** that the administrator can define based on all the security events that the firewall is likely to detect (events relating to filtering and encryption, or raised by the ASQ engine (cf. §2.1.3), low-level system events (shutdown/startup of the appliance, hardware errors, etc).

1.4.1.4 Protection against attacks coming from Internet

Monitoring information flows between several trusted networks and the uncontrolled network makes it possible to deny obvious attempts to set up illicit information flows with respect to the information flow control policy.

However, even within the limits of an information flow control policy adapted to the network and correctly implemented in firewall, there remains the following possibilities for attackers that have access to the uncontrolled network:

- Bypassing the information flow control policy implemented by the firewall,
- And/or “attacking” devices in the trusted networks by taking advantage of particularities and errors in the design and implementation of the network protocols (IP, TCP, UDP, SCTP, application protocols).

The effects of such attacks may include:

- An intrusion, meaning unauthorized access to a service, or to functions in an appliance’s operating system;
- Blocking or restarting an appliance, causing a denial of service;
- Flooding of network equipment, causing a denial of service;
- Divulgation of the topology and/or technical details of equipment on the trusted network with the aim of obtaining additional unauthorized access from the first successful intrusion.

To counter this risk, the Stormshield UTM / NG-Firewall Software Suite offers an **intrusion prevention function**, based on **ASQ technology**. This technology includes a dynamic scan at the IP, transport and application levels, with rule optimization allowing the swift and secure application of information flow control policy. It enables:

- The detection of attacks without connection contexts, for example:
  - IP spoofing by mapping the source IP address to the interface on which packets are received,
  - Counterfeit packets such as ‘xmas tree’ (all TCP options enabled) or ‘land’ (the source and destination addresses are identical) which aim to cause breakdowns on the target appliances,
  - Fragment overlaps with the purpose of causing breakdowns on target appliances or bypassing the information flow control policy,
  - Buffer overflow attempts at the application level;
- The detection of attacks with a connection context, such as:
  - The use of incorrect or exceeded TCP sequence numbers,
  - Brute force attacks on FTP passwords;
- The detection of global attacks requiring the characteristics of many distinct streams of information flows to be cross-referenced, for example:
  - Flooding of resources on servers, by sending an excessive amount of requests to open unacknowledged TCP connections (*SYN flooding*),
  - Attempts to probe the internal topology of trusted networks with nmap or queso utilities.

Appendix B, §8 contains an exhaustive list of attacks currently handled by the ASQ filter engine.

1.4.1.5 Risks of improper use

The definition of a **flow control policy**, as well as the operation of an appliance (audits, reactions to alarms, etc.) are generally complex tasks requiring specific skills and presenting risks of errors.

These risks make it preferable to separate administrative roles in order to guarantee that only persons who are qualified to carry out certain operations are those specifically qualified and trained to do so. This is why Stormshield UTM / NG-Firewall Software Suite **controls access to administrative security operations** based on privileges defined through administrator profiles.

A **configuration backup and restoration function** reduces the risk of errors by making it possible to keep configuration templates that address well-defined issues, and to backtrack in the event of an error.

The **quality of documentation** concerning operation and the **ease of use** of interfaces also have an impact on this type of risk.

1.4.1.6 Protection of the TOE itself

Assuming that the security functions of the TOE are effective in implementing the network security policy and countering attacks, and are correctly configured, the only solution for beating an attack is to modify the behavior of the TOE:

- Either by disabling the security functions or by modifying their configuration, through a local or remote attack exploiting vulnerabilities that may allow bypassing the function that monitors access to administration operations, without the need for special privileges;
- Or by obtaining legitimate **administrator** access (by colluding with an **administrator**, by guessing his password, etc.).

To counter this risk, measures have to be taken for the physical and logical security of Stormshield appliances as well as remote administration workstations (premises with controlled access, prohibition from using a local console during production, etc.). The function to monitor access to administrative operations mentioned in §2.1.4 is supported by **administrators' strong authentication mechanisms based on: mutual authentication by X.509 certificate (TLS) or login/password authentication (TLS).** Moreover, since remote administration can be done from an uncontrolled network, the Stormshield UTM / NG-Firewall Software Suite provides a **function that protects the confidentiality and integrity of administration sessions** based on cryptographic encryption operations. These functions make up a distinct set of IPSec encryption functions and are therefore provided in all cases.

1.4.2 Perimeter of the TOE:

1.4.2.1 Logical limits of the TOE

The following illustration outlines the logical limits of the TOE and TSF:

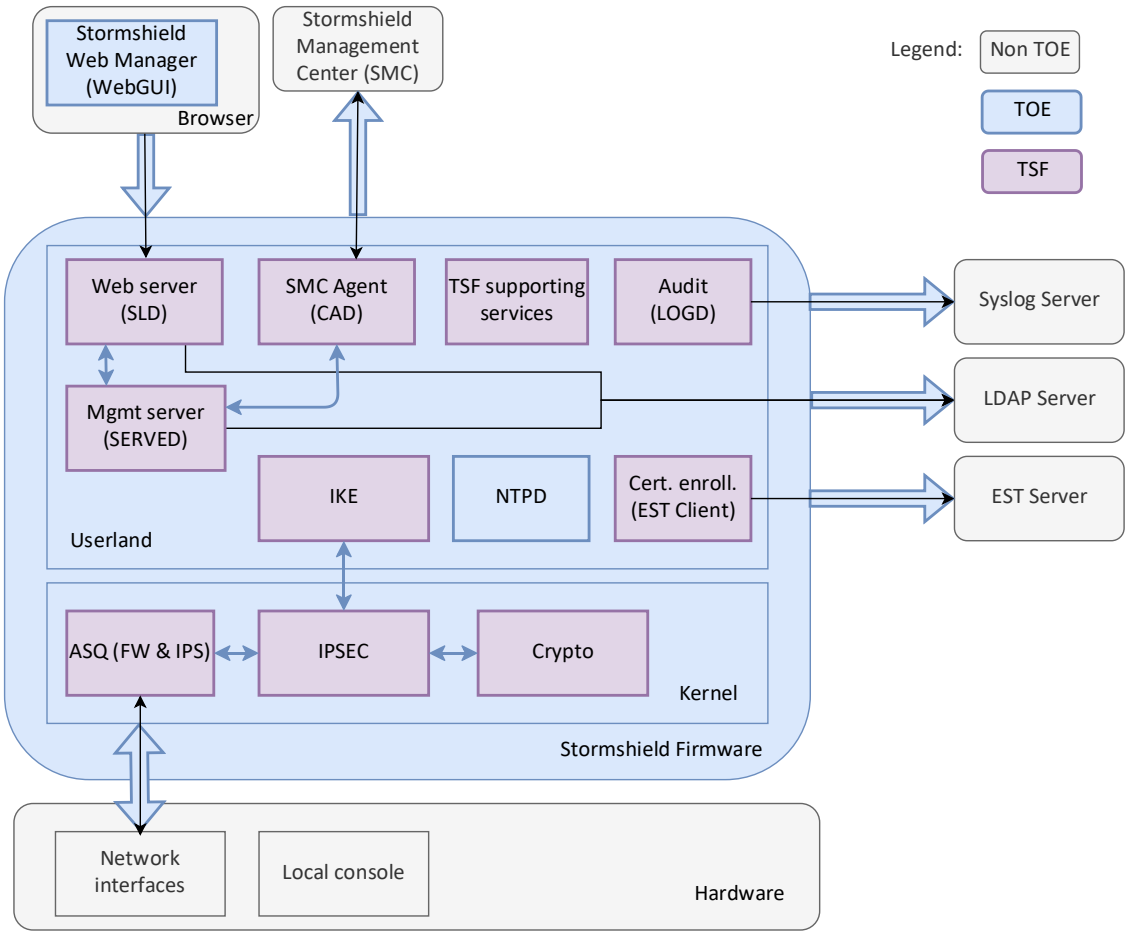


Illustration 2: Logical limits of the TOE and TSF

WebGUI	Graphical administration interface running as an Javascript application in a Web browser
SLD	HTTPS server who expose a set of API allowing WebGUI to manage and monitor the appliance.
CAD	TLS Client connected to central management (SMC), and relay configuration operations.
SERVERD	Internal administration service for management and monitoring commands.
ASQ	Kernel module in charge of firewalling and protocol analysis
IKE	IKE service, in charge to establish IPSEC security associations (SA)
IPSEC	Kernel module in charge of encrypt and decrypt IPSEC flows
CRYPTO	Kernel module in charge of cryptographic operations
LOGD	Agent in charge to write audit records on system disk and sends them in TLS to syslog server.

Cert. Enroll	Agent in charge to request EST server for certification enrollment and renewal.
TSF supporting services	Several internal services supporting previously presented TSF subsystems.

The following are outside the scope of the evaluation:

- the hardware section of appliances, administration workstations and mobile workstations.
- the VPN client software used on the mobile workstation,
- the Stormshield Management Center,
- The Syslog Server,
- The CRL/OCSP Server,
- The LDAP Server,
- The EST Server.

1.4.2.2 Architecture and interfaces of the TOE

A TOE in operation is a product distributed over several Stormshield appliances, and one or several remote administration workstations. The figure below illustrates the interfaces existing between these components as well as with other IT entities outside the TOE and users.

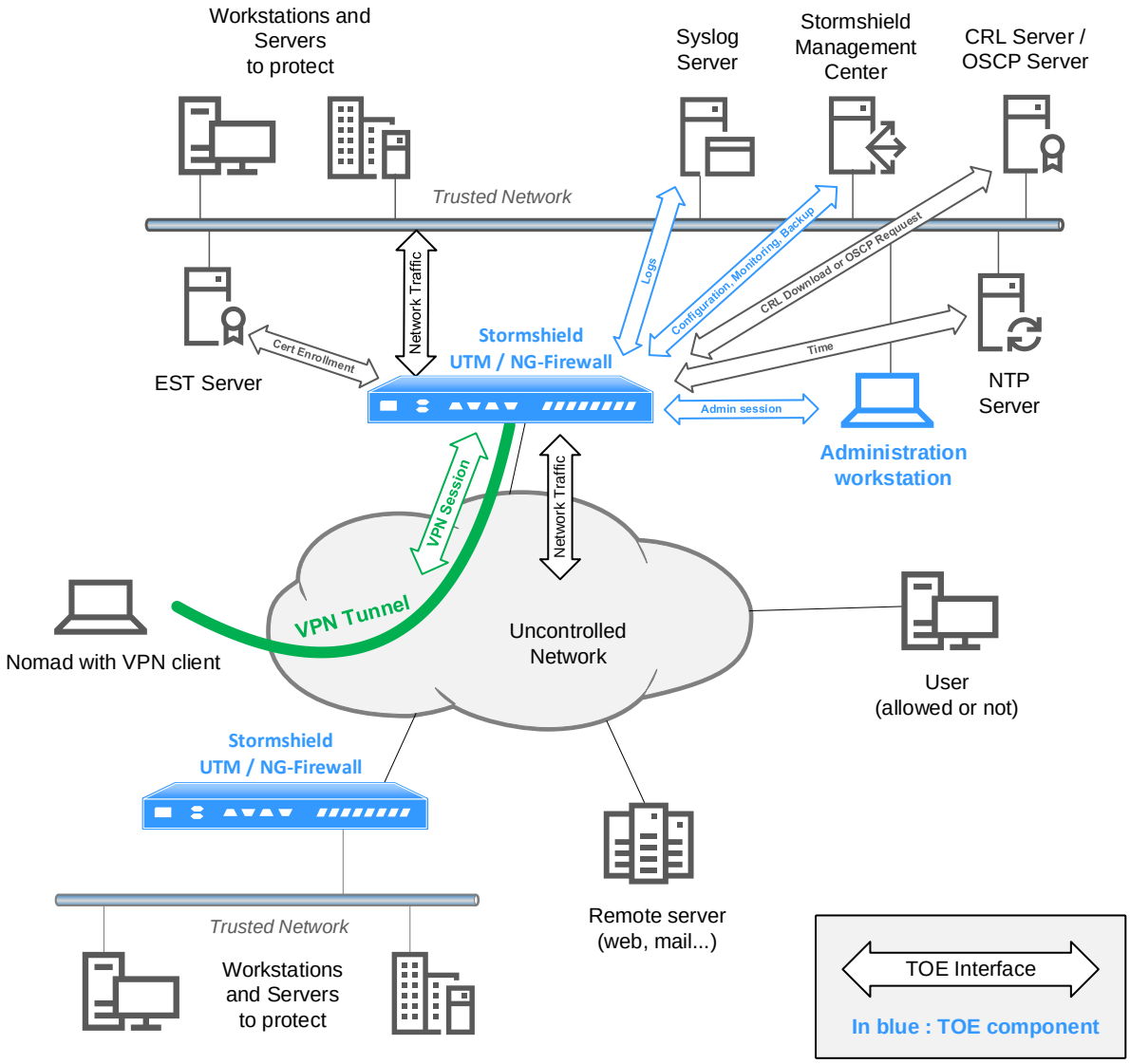


Illustration 3: Components and interfaces of the TOE.

1.4.2.3 Physical interfaces

The physical interfaces of the TOE are made up, according to platforms, of the following components:

- RJ45 connectors;
- RS-232 serial interface;
- HDMI port and USB port.
- SD-Card drive

1.4.3 Evaluation environment

1.4.3.1 Configurations and usage modes subject to the evaluation

The usage mode subject to evaluation has the following characteristics:

- The evaluation covers the Stormshield UTM / NG-Firewall Software Suite installed on all versions of Stormshield appliances, from the SN210 to SN6100 range, the suite existing in 3 distinct compilations (S, M and XL build) according to the appliance's position in the range. Certain models do not have large local log storage capacities and have to send events via syslog.
- Stormshield appliances have to be stored in a location with secured access. Such measures, as well as organizational procedures for the operating environment, have to guarantee that the only physical access to the Stormshield appliances take place under the surveillance of the **super-administrator**.
- The local console is not used in production. Only the super-administrator can log on to it, and hypothetically, such interventions are performed only when a decision has been made to make an exception to the operating context – to conduct a maintenance operation or a re-installation.
- Workstations on which the Stormshield Web Manager will be launched are secured, dedicated to such use, and up to date on all patches concerning the respective operating systems and the applications installed on them.
- The VPN client software is not part of the evaluation; besides, users can use an IPSec client of their choice. However, these client workstations have to be secured as rigorously as remote administration workstations.
- When external services are used by the TOE, they are not part of the evaluation. However, these servers have to be dedicated to such use, and up to date on all patches concerning the respective operating systems and the applications installed on them.

  External services are:
  - The NTP time servers.
  - The LDAP administrator and IPSec user directory server.
  - The SYSLOG server.
  - The CRL or OCSP server.
  - The SMC centralized management server.
  - The EST certificate enrolment server.
- Those configuration parameters must remain in their factory (default) states:
  - CRLs: regularly downloaded from a CRL server.
  - Internal TOE clock: regularly synchronised with NTP servers.
  - NSRPC administration services (port 1300/TCP): restricted to loopback.
  - IPv6 routing feature: disabled.
  - ESP Anti-replay windows, IKE re-authentication and IKE PFS (Perfect Forward Secrecy): activated.
  - Maximum SA lifetimes: 24 hours for IKE SA and 4 hours for IPSEC SA.
- Those application analysis functions are the only protocols covered by the certification:
  - FTP over TCP,
  - HTTP over TCP (including WEBDAV extensions),
  - SIP over TCP or UDP,
  - SMTP over TCP,
  - DNS over TCP or UDP,
  - and industrial protocols:
    - OPC UA over TCP,
    - MODBUS over TCP.

  Others must not be used in the running configuration.

- The following parameters must not be used in filter policy to associate a filter rule with:
  - an application inspection (HTTP, SMTP, POP3 and FTP proxies).
  - a schedule falls (Time object).
  - the “decrypt” action (SSL proxy).
  - a host reputation.
  - an FQDN object in source or destination (require external DNS services).
- The following features may be used, but are not considered security functions:
  - Address translation (network address translation or NAT).
  - Quality of Service.
  - The high availability module.
  - The feature for viewing embedded reports.
  - Filtering based on Geolocalisation and IP Reputation.
  - Filtering based on MAC address (Ethernet level).
  - Active Update.
- The IKE & IPSEC cryptographic algorithms implemented must be:

	standard IPSec	**IPSec DR**
Identification	Pre-shared key or Certificate with RSA or ECDSA key	Certificate with ECDSA or ECSDSA key Certificate with RSA Key only for Root CA.
Authentication/Integrity	SHA-2 256 or 384 or 512 bit	SHA-2 256 bit
Key negotiation	Diffie-Hellman group 14, 15, 16, 17, 18, 19, 20, 21, 28, 29, 30	Diffie-Hellman group 28
Encryption	AES 128 or 192 or 256 bit in CBC or CTR or GCM mode	AES 256 bit in GCM or CTR mode

- The usage mode subject to evaluation excludes the fact that the TOE relies on services other than previously mentioned services. The optional modules provided by Stormshield to manage these services are disabled by default and have to stay that way[1]. Specifically, these are:
  - modules that allow handling external servers (e.g.: Kerberos, RADIUS, etc),
  - the dynamic routing module,
  - the static multicast routing module,
  - the internal public key infrastructure (PKI),
  - the SSL VPN module (Portal and Tunnel),
  - DNS cache,
  - antivirus engine,
  - SSH, DHCP, MPD and SNMPD servers,
  - the DHCP client,
  - the DHCP relay,
  - Wifi connection for equipped devices,
  - Host reputation,
  - For SNi40 and SNi20 models: the hardware bypass capabilities,
  - Any custom IPS patterns,
  - FQDN objects (require external DNS services),
  - IPFIX messages,
  - Telemetry,
  - Breathfighter (Sandboxing),

[1] Administration and monitoring tools provide a way of checking at any moment during operation, that this is indeed the case.

- Network Vulnerability Manager (SNVM).

1.4.3.2 Test platform used during the evaluation

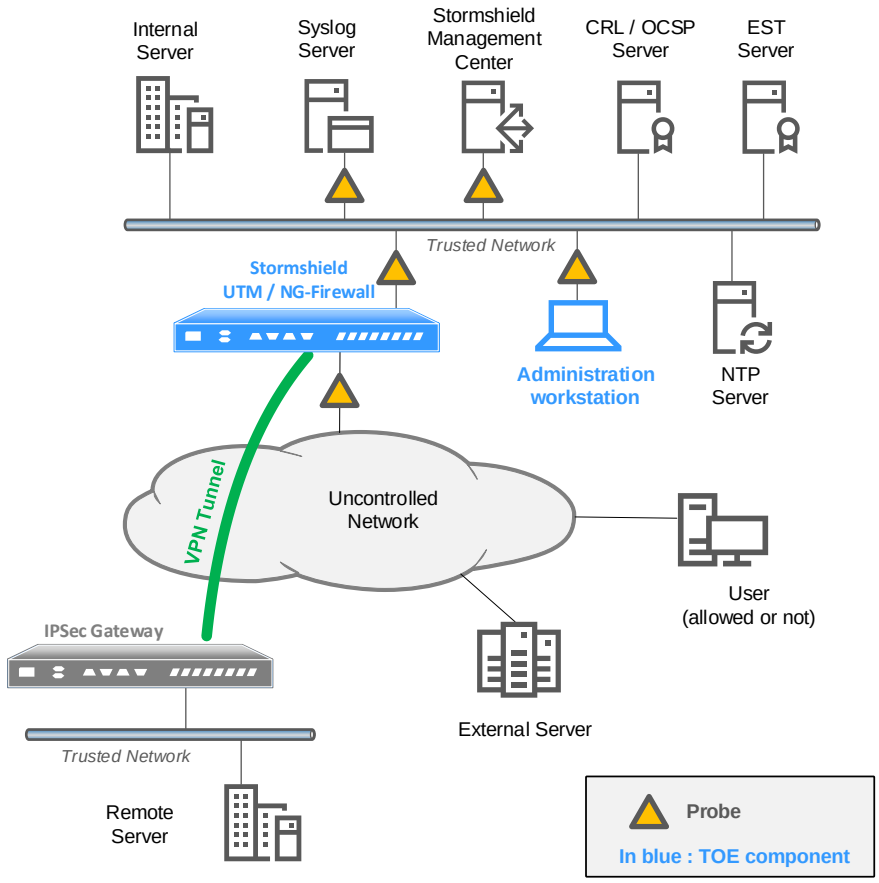


Illustration 4: Test platform used during the evaluation.

The Stormshield appliances under evaluation are the following models:

- SN210 and SN310 (entry-level),
- SN510, SN710, SN910 and SN1100 (mid-range),
- SN2000, SN2100, SN3000, SN3100, SN6000 and SN6100 (high-end),
- SNi40 and SNi20 (industrial models).

The operating system of the remote administration workstation is a Professional edition 64-bit Microsoft Windows 10 with all the latest patches published by Microsoft.

The web browser used for Stormshield Web Manager is Mozilla Firefox 80 or higher.

The software on workstations and servers comprises representative mass market products (e.g. browsers, mail clients, web servers) and applications that have been specifically developed for the purpose of compliance or penetration testing (scripts, attack programs, etc). The mobile client workstation is also equipped with the Stormshield Network Security VPN client (not subject to evaluation).

Laptops equipped with “probe” programs are used for listening on information flows in order to gauge the compliance of the Stormshield appliance’s behaviour at the network interface level, and for conducting penetration testing by counterfeiting packets. They may be connected at various points on the network.

1.4.3.3 Minimum characteristics of operating platforms

The **Stormshield Firmware** uses the following “open-source” components with updated patches under evaluation conditions:

- FreeBSD in version 11.3
- Strongswan in version 5.9.5
- OpenLDAP in version 2.4.58
- OpenSSL in version 1.1.1t
- Ntpd in version 4.2.8p14
- Libevent in version 2.1.8
- Libcurl in version 7.78
- libwebsockets in version 4.2.1

For the remote administration workstation hosting Stormshield Web Manager

- CPU with a minimum of 2 GHz;
- 2 GB of RAM;
- 100 or 1000 Mbps Ethernet network card;
- Mozilla Firefox 102.9.0 or higher.

1.5 Applicable and reference documents

1.5.1 TOE Guides

[User Guide]	SNS - MANUEL D'UTILISATION ET DE CONFIGURATION Version 4.3.12.2, ref: sns-frmanuel_d'utilisation_et_de_configuration-v4.3.12.2, 21/06/2023
[Install GUIDE]	SNS - PRÉSENTATION ET INSTALLATION PRODUITS ref: sns-fr-GammeSN_guide_installation-2021, version 1.0, 10/2021
[SMC Admin Guide]	SMC - GUIDE D'ADMINISTRATION Version 3.3.3, ref: SMC-guide_d_administration-v3.3.3, 15/06/2023
[SMC Install Guide]	SMC - GUIDE D'INTALLATION Version 3.3.3, ref: SMC-guide_d_installation-v3.3.3, 15/06/2023
[CLI Commands]	SNS - CLI CONSOLE / SSH COMMANDS REFERENCE GUIDE Version 4, ref: sns-en-cli_console_ssh_commands_reference_guide-v4, 06/04/2022
[Serverd Commands]	SNS - CLI SERVERD COMMANDS REFERENCE GUIDE Version 4, ref: sns-encli-serverd_commands_reference_guide-v4, 06/04/2022
[SNS Logs]	SNS - DESCRIPTION DES JOURNAUX D'AUDIT (LOGS) Version 4, ref: sns-frdescription des_journaux_d_audit_note_technique-v4, 06/04/2022
[USB Restore]	SNS - RESTAURATION LOGICIELLEPAR CLÉ USB ref: sns-fr-restauration_logicielle_cle_USB_note_technique, 09/02/2022
[Indus Protocols]	SNS - IDENTIFIER LES COMMANDES DE PROTOCOLES INDUSTRIELS TRAVERSANT LE FIREWALL ref: sns-fridentifier_ commandes_protocoles_industriels_note_technique, 09/12/2019

1.5.2 Common Criteria references

[CC-01] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 - Part 1: Introduction and general model, CCMB-2017-04-001, April 2017.

[CC-02] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 - Part 2: Security functional components CCMB-2017-04-002, April 2017.

[CC-03] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 - Part 3: Security assurance components CCMB-2017-04-003, April 2017.

[CEM-04] Common Criteria - Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 – Evaluation Methodology CCMB-2017-04-004, April 2017.

[PP-MDM] Protection Profile for Mobile Device Management, National Information Assurance Partnership, Version: 4.0 - 2019-04-25

[FP-TLS] Functional Package for Transport Layer Security (TLS), National Information Assurance Partnership, Version: 1.1 - 2019-02-12

1.5.3 Reference for the Standard Qualification

[QUALIF-STD]	General Security Baseline Qualification process of a security product – standard level - Version 1.2.
[RGS-CRYPTO]	ANSSI-PG-083 Cryptographic mechanisms Guide Rules and recommendations regarding the choice and size of cryptographic mechanisms - Version 2.0004 2020-01-01
[RGS-GC]	General Security Baseline Version 2.0 Appendix B2 Management of cryptographic keys Rules and recommendations regarding the management of keys used in cryptographic mechanisms - Version 2.00 June 8 2012
[RGS-AUTH]	General Security Baseline Appendix B3 Authentication Rules and recommendations regarding authentication mechanisms Version 1.00 January 13 2010
[IPSEC DR]	Note Crypto Référentiel IPsec DR 2021-03-16

1.5.4 RFCs and other standards supported

[IP]	P. Almquist, Type of Service in the Internet Protocol Suite, RFC 1349, July 1992.
[ICMP]	Postel, J., Internet Control Message Protocol - DARPA Internet Program Protocol Specification, RFC 792, USC/Information Sciences Institute, September 1981.
[IGMP]	Cain, B., Deering, S., Kouvelas, I., Fenner, B. and A. Thyagarajan, *Internet Group Management Protocol, Version 3*, RFC 3376, October 2002.
[UDP]	Postel, J., *User Datagram Protocol*, STD 6, RFC 768, August 1980.
[TCP]	Postel, J., *Transmission control protocol*, STD 7, RFC 793, September 1981.
[IPSec]	Kent, S. and R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.
[ESP]	Kent, S., *IP Encapsulating Security Payload (ESP)*, RFC 4303, December 2015.
[IKE-MODP]	T. Kiniven, M. Kojo; More Modular (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), RFC 3526, May 2003.
[IKE-ECP]	D. Fu, J. Solinas Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2, RFC 5903, June 2010
[IKE-BEC]	D. Harkins: Brainpool Elliptic Curves for the Internet Key Exchange (IKE) Group Description Registry, RFC 6932, May 2013
[ECDSA]	D. Fu, J. Solinas, IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA), RFC 4754, January 2007
[IKEv2]	Kaufman, Hoffman, Nir, Eronen, Kivinen, Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7427, October 2014.
[FTP]	Postel, J. and J. Reynolds, *File Transfer Protocol (FTP)*, STD 9, RFC 959, October 1985.
[FTP-security]	Allman, M., Ostermann, S., *FTP Security Considerations*, RFC 2577, May 1999
[FTP-feature]	Hethmon, P., Elz, R., Feature negotiation mechanism for the File Transfer Protocol, RFC 2389, August 1998

[FTP-IPV6] Allman, M., Ostermann, S. and C. Metz, *FTP Extensions for IPv6 and NATs*, RFC 2428, September 1998.

[HTTP] Fielding, R., Gettys, J., Mogul, J., Frysyk, H., Masinter, L., Leach, P. and T. Berners-Lee, *Hypertext Transfer Protocol -- HTTP/1.1*, RFC 2616, June 1999.

[WEBDAV] Goland, Y., Whitehead, E., Faizi, A., Carter, S. and D. Jensen, *HTTP Extensions for Distributed Authoring - WEBDAV*, RFC 2518, February 1999.

[WEBDAV-extensions] Clemm, G., Amsden, J., Ellison, T., Kaler, C. and J. Whitehead, *Versioning Extensions to WebDAV (Web Distributed Authoring and Versioning)*, RFC 3253, March 2002.

[DNS-1] Mockapetris, P., *Domain names - Concepts and Facilities*, STD 13, RFC 1034, November 1987.

[DNS-2] Mockapetris, P., *Domain Names - Implementation and Specification*, STD 13, RFC 1035, November 1987.

[RIP-1] Hedrick, C., *Routing Information Protocol*, RFC 1058, Rutgers University, June 1988.

[RIP-2] Malkin, G., *RIP Version 2*, STD 56, RFC 2453, November 1998.

[DSCP] K. Nichols, Differentiated Services Field, RFC 2474, December 1998.

[MGCP] F. Andreasen and B. Foster, Media Gateway Control Protocol, RFC 3435, January 2003.

[SIP] *Session Initiation Protocol*, RFC 3261, June 2002.

[RTP] RTP: A Transport Protocol for Real-Time Applications, RFC 3550, July 2003.

[RTCP] Real Time Control Protocol (RTCP) attribute in SDP, RFC 3605, October 2003.

[TLS12] *The Transport Layer Security (TLS) Protocol – Version 1.2*, RFC 5246, August 2008.

[TLS13] *The Transport Layer Security (TLS) Protocol – Version 1.3*, RFC 8446, August 2018.

[TLS-AES] P. Chown, Advanced Encryption Standard (AES) Ciphersuites Transport Layer Security (TLS), RFC 3268, June 2002.

[DH] Rescorla, *Diffie-Hellman Key Agreement Method*, RFC 2631, June 1999.

[RSA] RSA Laboratories. PKCS #1 v2.1: RSA Encryption Standard. June 2000.

[AES] NIST, FIPS PUB 197, *Advanced Encryption Standard (AES)*, November 2001.

[AES-CBC-256] NIST, SP800-38A, Recommendation for Block Cipher Modes of Operation

[AES-GCM-256] Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol, RFC 5282, August 2008

[HMAC] Krawczyk, H., Bellare, M. and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, RFC 2104, February 1997.

, April 1992.

[SHA] NIST, FIPS 180-1, *Secure Hash Standard*, April 1993.

[SHA2] NIST, FIPS 180-2, *Secure Hash Standard*, February 2004.

[DSA] NIST, FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[Brainpool] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010

[ECSDSA] ISO/IEC 14888-3 :2016 - Information technology – Security techniques – Digital signatures with appendix – Part 3 : Discrete logarithm based mechanisms”

[SMB2] MS-SMB2, Server Message Block (SMB) Version 2 Protocol Specification, December 30, 2010

[OPC-UA]	IEC 62541 - OPC Unified Architecture Specification Release 1.01 February 9, 2009
[MODBUS)	MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b3
[SCTP]	RFC 4960, Stream Control Transmission Protocol, R. Stewart, Ed. September 2007.
[EST]	RFC 7030, Enrollment over Secure Transport, October 2013.
[CSR]	RFC 2986, PKCS #10: Certification Request Syntax Specification, Version 1.7, November 2000
[CMS]	RFC 5652, Cryptographic Message Syntax (CMS), September 2009
[CMC]	RFC 5273, Certificate Management over CMS (CMC): Transport Protocols, June 2008

1.6 Glossary

TOE
Target of Evaluation

ST
Security Target.

IT
Information technology.

EAL
Evaluation Assurance Level.

SFR
Security Functional Requirement.

TSF
TOE Security Functionality

CEM
Common Evaluation Methodology for information technology security

CC
Common Criteria for the evaluation of security.

RGS
General Security Baseline (*Référentiel Général de Sécurité*).

Administrator
Personnel qualified to perform certain administrative security operations and responsible for the proper execution of such operations.

Auditor
Administrator qualified to perform security audit operations and audit log management and responsible for the proper execution of such operations.

ECDH
Elliptic Curve Diffie-Hellman

Entity
IT agent or human user likely to set up information flows with other entities.

Stormshield appliance
Stormshield Network Security equipment placed at the boundary between the uncontrolled network and one or several trusted networks, dedicated to the implementation of the information flow control policy. This is the device on which the core of the Stormshield software suite's security functions run.

IPSec Security Association (IPSec SA)
One-way connection at the transport level that implements security services on the information flow that it transports. From the point of view of an entity participating in a VPN tunnel, an IPSec SA may be incoming or outgoing. Outgoing SAs are used for encapsulating and protecting outgoing IP datagrams, while incoming SAs are used for decapsulating and monitoring incoming IP datagrams.

Traffic / tunnel endpoints
In the case of a VPN tunnel, traffic endpoints are entities that make up the endpoints of information flows partially passing through the tunnel, as opposed to tunnel endpoints which are devices between which the tunnel was set up. In encrypted ESP in tunnel mode, the confidentiality of IP address of traffic endpoints is protected from attackers who are able to listen on information flows on the network segments where the tunnel has been set up. These attackers will only be able to see the IP addresses of tunnel endpoints.

VPN peer
Remote entity that makes up the other endpoint of the tunnel.

Local/remote entity
In the case of a VPN tunnel, local entities are traffic endpoints whose traffic reaches the Stormshield appliance encapsulated in ESP, and which need to be so before being re-sent to the other traffic endpoint via the VPN peer. Remote entities are those whose traffic reaches the Stormshield appliance via the VPN peer and are encapsulated in ESP.

Local console
Terminal physically connected to a Stormshield appliance, used for performing installation or maintenance operations on this appliance's firmware.

Security administration operations
Operations performed on Stormshield appliances, under the responsibility of an **administrator** in the scope of the internal security policy of the organization using trusted networks. These operations may be governed by the internal security policy (e.g. audit revenues) or by the need to maintain the TOE in nominal operating conditions (e.g. modification of the configuration of the information flow control function, audit log purge, shutdown/restart of the appliance). Typically, their purpose is to modify the behavior of the TOE's security functions.

Filter policy
Set of technical rules describing which entities are entitled to set up information flows with which entities. This arises from the concatenation of **implicit rules**, the **global filter policy**, and the **local filter policy**.

Global filter policy
Set of technical rules describing which entities are entitled to set up information flows with which entities. This set is defined by an administrator with the objective of coherence in the **filter policy** for a set of Stormshield appliances.

Local filter policy
Set of technical rules describing which entities are entitled to set up information flows with which entities. This set is defined by an administrator with the aim of adjusting the **global filter policy** according to specific needs for a Stormshield appliance.

Implicit rule
Set of rules automatically generated by the Stormshield appliance in order to ensure the proper running of services that an administrator has configured and started.

Encryption policy
Set of technical rules describing the encryption processes to apply to certain types of information flows for the purpose of protecting their confidentiality and integrity.

Information flow control policy
Set of technical rules comprising the filter policy and the encryption policy.

Pseudo-connection
1º) Set of UDP datagrams associated with the same application exchange
2) Set of ICMP messages associated with a request/response exchange in the context of use of this protocol (e.g.: 'echo request' / 'echo reply').

SCTP association
Protocol relationship between SCTP endpoints, composed of the two SCTP endpoints and the protocol state information (endpoints addresses for multi-homing, verification tag, association cookie and association state).

Trusted network
A network is considered trusted if, due to the fact that it is under the control of the TOE operator, the internal security policy does not imply that there is a need to be protected from information flows originating from it, but on the contrary, implies that there is a need to protect information flows going to it.

Uncontrolled network
A network is considered uncontrolled if it is not under the control of the TOE operator, meaning that users need to be protected from information flows set up with devices from this network (the internet, for example).

Remote administration workstation
Workstation connected to a trusted or uncontrolled network, dedicated to administration operations relating to the security of one or several Stormshield appliances through secure administration sessions.

Super-administrator
Administrator possessing full privileges over the configuration of Stormshield appliances, the only person allowed to log on using the local console, to define the profiles of other administrators, and who must accomplish this task only outside operating phases (i.e. installation or maintenance).

User
Person using IT resources on trusted networks protected by the TOE from other trusted networks or from the uncontrolled network.

IPSec User
User acting as a VPN Peer with a mobile client.

Data table
Set of tables containing data (interfaces, etc) needed for the proper operation of the TOE. The Stormshield appliance automatically fills in these tables when it runs normally.

Incoming IP packet
Incoming IP packet that needs to be compared against the **filter policy**. As a result, this refers to an IP packet that does not belong to a connection or **pseudo-connection** detected and allowed earlier.

Knowledge base
Set of control points, defined by **TOE** version, allowing the proper operation of the **intrusion prevention function**.

Active Update
Service enabling the automatic and regular update of the signature bases of various modules using such bases in order to optimize their effectiveness. This includes in particular IPS and NVM (Seismo), Antivirus, Antispam, URL filter signatures, etc.

2 CONFORMANCE CLAIMS

The aim of this section is to provide appropriate statements regarding compliance with the Common Criteria and other applicable baselines.

2.1 CC Conformance Claim

The applicable version of the Common Criteria is version 3.1 revision 5 of April 2017.

The security functions of the target of evaluation are “Strictly Compliant with Part 2 extended of the Common Criteria” with the introduction of:

- the FMT_MTD.BRS component.
- two security functions for certificate enrollment (FIA_X509_EXT.4 and FCS_HTTPS_EXT.1) inspired from [PP-MDM].
- a security function for TLS (FCS_TLSC_EXT.1) inspired from [FP-TLS].

2.2 PP Claim, Package Claim

There are no Protection Profile claims.

This Security Target claims to be conformant to the Assurance Packet EAL4 augmented with ALC_FLR.3.

These components are defined in CC Part 3.

2.3 Conformance Rationale

The security assurance measures implemented on the target of evaluation are “Strictly Compliant with Part 3 of the Common Criteria”.

No statement of compliance for any Protection Profile or any other security requirement package other that the package selected has been made.

The security assurance package selected is an extension of the augmented EAL4 package of the ALC_FLR.3 component.

This package of assurance requirements includes all the assurance requirements needed in for the standard qualification [QUALIF-STD].

3 SECURITY PROBLEM DEFINITION

The purpose of this section is to describe the security issue that the TOE must address in the form of a set of threats that the TOE must counter and rules of the security policy that the TOE must satisfy. This specification is made subject to assumptions on the security characteristics of the environment in which the TOE is expected to be used as well as on its expected usage mode.

3.1 Typographical convention

For a better understanding of the following paragraphs, we will explain the typographical conventions used for naming assumptions, threats, policies and objectives:

- **A**ssumptions on the security environment of the TOE have names beginning with the following prefixes:
  - AH. Prefix for **A**ssumptions relating to **H**uman agents,
  - AP. Prefix for **A**ssumptions relating to **P**hysical measures,
  - AO. Prefix for **A**ssumptions relating to **O**rganizational security measures,
  - AIT. Prefix for **A**ssumptions relating to the **IT** security environment**.**
- **T**hreats on the security environment of the TOE or the security of the TOE itself have names beginning with the prefix **T.**
- The organization's security Policies have names beginning with the prefix **P.**

3.2 Identification of sensitive assets

3.2.1 Assets protected by the TOE

The Stormshield UTM / NG-Firewall contributes to the protection of the following sensitive assets, subject to a proper and feasible definition of the information flow control policy to be implemented globally in the information system (cf. AO.GOOD_PCFI):

- UA.APPLI: Application services offered by servers of trusted networks (confidentiality, integrity and availability);
- UA.PROGRAMS_CONFIG: Programs launched on devices in trusted networks (servers, browsers, etc.), and the configuration of such programs (integrity and confidentiality);
- UA.FLOWS: The contents of information flows passing through the uncontrolled network, for which the implementation of the VPN is possible (confidentiality and integrity);
- UA.TOPOLOGY: Information about the network's topology (confidentiality), against probe attempts based on the use of internet protocols contrary to best practices.

3.2.2 Assets belonging to the TOE

With the aim of protecting these external sensitive assets, the various components of the Stormshield UTM / NG-Firewall Software Suite also protect their own confidentiality and integrity security settings during exchanges between each other (administration sessions).

Furthermore, sensitive assets of the TOE comprise data relating to the security functions of the TOE (TSF-Data).

TSF-Data is made up of:

- TA.CONFIGURATION: configuration settings of the TOE (confidentiality),
- TA.POLICIES: data control policies implemented by the TOE (confidentiality),
- TA.CONTEXTS : contexts of use (confidentiality, integrity and availability),
- TA.LOGS: records of events of the TOE (confidentiality, integrity),
- TA.CREDENTIALS: authentication data of IPSec administrators and users (confidentiality).

3.3 Threats and rules of the security policy

The threats and rules of the security policy follow the plan taken for the description of the TOE's IT security characteristics.

The various threat agents are:

- internal attackers: entities belonging to the trusted network
- external attackers: entities not belonging to the trusted network

Administrators are not considered hackers.

3.3.1 Information flow control

P.FILTERING

The TOE must apply the **filter policy** defined by the **administrator**. This policy is expressed in terms of authorization or rejection of information flows according to their characteristics at the IP level (source and destination address, type of IP protocol) and transport (source and destination TCP or UDP port, or SCTP associations).

P.VPN

The TOE must apply the encryption policy defined by the administrator. This policy is expressed in terms of:

1. the application of the encryption function on information flows according to their characteristics at the IP level (source and destination address, type of IP protocol),
2. conditions under which IPSec sessions are established (pre-shared key or certificate, expected identity of the VPN peer),
3. ESP parameters used (authentication and encryption algorithms of frames and length of associated keys).

P.AUDIT_ALARM

The TOE must:

1. Generate filter (including information flows and denials) and encryption events that the administrator has deemed sensitive and for appliances that are able to record events, it must provide the means to attribute them later in an audit to the entities that initiated them;
2. Raise security alarms for filter, encryption, contextual analysis events (cf. P.ANALYSIS) or events relating to the activity of Stormshield appliance firmware, specified as such by the administrator.

P.CRYPTO

Key management and the cryptographic and authentication mechanisms used in the TOE have to comply with the ANSSI baseline ([RGS_CRYPTO], [RGS_CLES], [RGS_AUTH] and [IPSEC DR]) with regard to the standard resistance level.

3.3.2 Protection against Internet attacks

P.ANALYSIS

The TOE must analyze information flows passing through Stormshield appliances, detect and destroy it where necessary without forwarding the following types of information flows, which may be potentially dangerous for the receiving entity:

1. Information flows that may expose the network topology (e.g.: route recording option),
2. Information flows valid in respect to Internet protocols but which are incompatible with certain best practices (e.g.: ICMP redirect),
3. Information flows that may cause software issues on destination appliances,
4. Information flows that may flood communication and processing capacities on destination appliances.

T.IP_SPOOFING

An unauthorized entity on the uncontrolled network bypasses information flow control policies by counterfeiting the source IP address of packets that it sends in order to usurp the identity of an entity on the authorized network.

3.3.3 Risks of improper use

T.IMPROPER_USE

The security functions of the TOE do not behave in harmony with the internal security policy (cf.1.4.1.1), due to the fact that an administrator does not correctly exercise the responsibilities associated with his role, either by incorrectly configuring the TOE or by acting in a manner that is contrary to his responsibilities or to proper usage. This would allow a hacker to exploit a vulnerability or poor configuration in order to access assets protected by the TOE on the trusted network.

P.BACKUP_RESTORATION

The TOE must provide a way to back up its configuration, and to restore it later for the purpose of easing the administrator's job. The backup operation can be triggered either from Stormshield Web Manager or from Stormshield Management Center. The TOE ensures the confidentiality and integrity of the configuration transmitted over the network.

3.3.4 Protection of the TOE itself

T.ILLEGAL_ADMIN

An external or internal attacker manages to perform illegal administration operations by bypassing the information flow policies, usage contexts, authentication data of administrators as well as the configuration settings of the TOE.

T.ADMIN_USURP

An external or internal attacker manages to establish an administration session on a Stormshield appliance by usurping the identity of an administrator after repeated random attempts, or by analyzing intercepted authentication sequences. Threatened assets affect administrators' authentication data.

T.ILLEGAL_ADMIN_SESSION

An external or internal attacker reads, modifies or deletes the contents of an administration session set up between a Stormshield appliance and a remote administration workstation using an administrator account. The assets threatened are information flow control policies and usage contexts.

Note: T.ADMIN_USURP and T.ILLEGAL_ADMIN_SESSION are requirements (non-exhaustive) that allow the threat T.ILLEGAL_ADMIN to be carried out.

T.AUDIT

An external or internal attacker prevents security events from being generated by depleting the TOE's storage or sending capacity for these events, with the purpose of masking a hacker's illegal actions.

This entity may also either read or modify security events during their transmission to a centralised log server.

3.4 Assumptions

3.4.1 Assumptions on physical security measures

AP.PROTECT_APPLIANCES

Stormshield appliances are installed and stored according to the state of the art regarding sensitive security devices: premises with protected access, shielded twisted pair cables, labeling of cables, etc.

3.4.2 Assumptions on organizational security measures

AO.SUPER_ADMIN

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

1. The super-administrator is the only administrator allowed to log on via the local console on Stormshield appliances, and only during the installation of the TOE or for maintenance operations, and not during production;
2. He is in charge of defining the profiles of other administrators;
3. All access to the premises in which Stormshield appliances are stored must be under his watch, whether the cause for such access is an intervention on the appliances or on other equipment. All interventions on Stormshield appliances shall be conducted under his responsibility.

AO.PASSWORD

The passwords of IPSec administrators and users must be chosen in a way that delays attacks aiming to crack them, via a password creation and/or control policy (e.g.: mix of alphanumeric characters, minimum length, inclusion of special characters, no dictionary words, etc).

Administrators have been made aware of these best practices in exercising their function and it is their responsibility to create awareness in IPSec users.

AO.GOOD_PCFI

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

1. full: standard usage scenarios have all been considered during the definition of rules and their authorized limits have been defined,
2. strict: only the necessary usage scenarios have been authorized,
3. correct: rules do not contradict each other,
4. unambiguous: the list of rules provides all the relevant elements for the direct configuration of the TOE by a qualified administrator.

AO.CRYPTO_EXT

Cryptographic keys that were generated outside the TOE and injected into it must be generated according to the recommendations in the ANSSI's baseline ([RGS-CRYPTO] and [RGS-GC]) with regard to the standard resistance level,

3.4.3 Assumptions relating to human agents

AH.PERSONNEL

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:

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

3.4.4 Assumption on the IT security environment

AIT.INTERPOSITION

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

AIT.STRICT_USAGE

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

AIT.AUTONOMOUS

The TOE does not depend on external “online” services (DNS, DHCP, RADIUS, etc.) to apply the information flow control policy.

AIT.PROTECT_WORKSTATIONS

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

AIT.PROTECT_VPN_PEER

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

AIT.PROTECT_VPN_CLIENTS

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.

AIT.TIMESTAMPS

The IT environment provides through NTP reliable timestamps.

AIT.REVOCATION_LIST

The IT environment provides up to date X.509 certificate revocation status, both for peers and administrators.

AIT.ENROLLMENT

The IT environment provides a reliable enrollment infrastructure.

4 SECURITY OBJECTIVES

The aim of this section is to concisely present the expected response to the security issue, in the form of security objectives. Security objectives are normally classified as security objectives for the TOE and as security objectives for the environment. The rationale for security objectives must show that the security objectives for the TOE and for the environment are linked to the identified threats that need to be countered or to the rules of the security policy and assumptions that need to be satisfied by each objective.

4.1 Typographical convention

For a better understanding of the following paragraphs, we will explain the typographical conventions used for objectives:

- Security **O**bjectives for the TOE have names beginning with the prefix **O.**
- Security **O**bjectives for the **E**nvironment of the TOE have names beginning with the **OE**.

4.2 Overview

The presentation of security objectives for the TOE follows the plan for the description of the TOE's IT security characteristics and the threats and rules of the security policy.

The rationale for each security objective of the TOE is provided immediately after the description of the objective, instead of in a separate section. A table summarizing this rationale is provided at the end of this section.

With regard to security objectives O.PCAOA, O.PCAOA_I&A_ADMIN and O.RESIST_AUTH_ADMIN, it is important to note that the control policy for access to security administration operations contributes to both:

- The prevention of improper use, by allowing the separation of administration tasks adapted to the responsibility and skills of each administrator to be implemented, governed by the restrictions of the organization using the trusted networks,
- The protection of the TOE itself, since it prevents illegal administration operations.

As such, these three objectives cover the issues described in §4.5 as well as §4.6.

All of the assumptions mentioned in the description of the TOE's security environment must be considered components of the security objectives for the environment. When security objectives for the environment comprising the assumptions specifically support security objectives of the TOE, these assumptions are directly indicated in the rationale for the security objectives of the TOE concerned. When security objectives for the environment directly counter threats, or when their support is generalized, this will be presented at the end of this section (§4.7).

4.3 Information flow control objectives

O.PCFI_FILTERING

The TOE must provide information flow control between the networks connected to it, by filtering information flows according to the rules configured by the **administrators** based on the following characteristics:

- The source interface of the information flow,
- The destination interface of the information flow,
- Machines at the traffic endpoints,
- Type of IP protocol,
- For ICMP: type of message,
- For TCP, UDP and SCTP: type of service,
- Type of DSCP service.

Rationale: O.PCFI_FILTERING is mainly dedicated to the satisfaction of the P.FILTERING policy.

O.PCFI_APPLICATION_CONTEXT

The TOE must maintain tracking contexts of application sessions for which “child” connections are necessary, and must allow opening child connections relating to these sessions only when the context requires it.

Note: The most common case of a “child connection” is in FTP data connections, whose characteristics (destination port) cannot be known in advance and is the result of the contents of the command session.

Rationale: O.PCFI_APPLICATION_CONTEXT supports O.PCFI_FILTERING in order to cover the P.FILTERING policy. During an applicative session, the characteristics of child connections result from the product of the session’s contents. If there is no tracking on these contents, in case of doubt, the filter policy should authorize all the possible variations of these characteristics so that the application protocols considered may function. This objective therefore allows applying the most restrictive filter policy possible.

O.PCFI_ENCRYPTION

The TOE must provide VPN services on information flows exchanged with certain remote devices in order to ensure the initial enrollment of the TOE, the mutual authentication of endpoints, as well as the confidentiality and integrity of such information flows.

Rationale: O.PCFI_ENCRYPTION is mainly dedicated to the satisfaction of the P.VPN policy.

In order to effectively support this objective, potential hackers have to be deterred from accessing the VPN session keys for the purpose of violating the P.VPN policy for this encrypted information flow (by decrypting it thereafter, or modifying it, replaying it or inserting data into it). This protection is ensured:

- *On the TOE side, by AP.PROTECT_APPLIANCES which prevents physical access to appliances,*
- *On the VPN peer side by AIT.PROTECT_VPN_PEER and AIT.PROTECT_VPN_CLIENTS, depending on whether the VPN clients are static network devices or mobile clients.*

The application of an encryption policy is the most effective way to counter IP address spoofing (T.IP_SPOOFING), by imposing strong authentication on entities at information flow endpoints. Cf. O.IPS_ATTACK_DETECTION for cases in which the setup of an encryption policy is not feasible for countering this threat.

O.LAA_PCFI[2]

[2] ‘LAA’ = logging, audit and alarms.

The TOE must:

- Log events relating to the application of the information flow control policy (filtering and encryption),
- Allow auditing logs of these events, and
- Raise alarms to the administrator when events that have been specified by the administrator as critical have been detected.

Rationale: O.LAA_PCFI is mainly dedicated to the satisfaction of the policy P.AUDIT_ALARM. It covers the aspect "recording of filter and encryption events deemed sensitive by the administrator" (P.AUDIT_ALARM.1).

O.CRYPTO

The TOE must implement cryptographic functions and manage cryptographic keys in compliance with the requirements for the standard level of robustness in the ANSSI's cryptographic baselines [RGS_CRYPTO], [RGS_CLES] and [RGS_AUTH].

The use of a built-in cryptographic coprocessor is disabled for IPSec DR, except for models based on an Intel processor.

Rationale: O. CRYTPO is mainly dedicated to the satisfaction of the P.CRYPTO policy. By covering the requirement of compliance with the RGS, it also contributes to the safe implementation of the P.VPN encryption policy and countering the T.ILLEGAL_ADMIN threat.

4.4 Objectives of protection against Internet attacks

O.IPS_ATTACK_DETECTION

The TOE must be able to analyze packets associated with information flows as well as the application requests/commands/responses included in this information flow, in order to detect and *block attacks on devices in trusted networks.*

Rationale: O.IPS_ATTACK_DETECTION is mainly dedicated to the satisfaction of the policy P.ANALYSIS. The detection of attacks covers in particular the correlation between the IP addresses of incoming packets and the interface on which they are presented, thereby making it possible to counter IP address spoofing attempts (T.IP_SPOOFING) conducted with addresses not included in the range associated with the receiving interface.

Note: All information flows allowed to pass through the TOE are analyzed, even those whose destination is the TOE.This is a particular case and is not the reason for O.IPS_ATTACK_DETECTION.

O.IPS_RFC_COMPLIANCE

The TOE must be able to analyze packets associated with information flows as well as the application requests/commands/responses included in this information flow, in order to detect and block packets and application information flows that do not comply with the RFCs.

Rationale: O.IPS_RFC_COMPLIANCE is dedicated to the satisfaction of the policy P.ANALYSIS, particularly to prevent contraventions of best practices (P.ANALYSIS.2).

O.LAA_IPS

The TOE must:

- Log events relating to the detection of potential intrusions,
- Allow auditing logs of these events, and
- Raise alarms to the administrator when events that have been specified by the administrator as critical have been detected.

Rationale: O.LAA_IPS is mainly dedicated to the satisfaction of the policy P.AUDIT_ALARM. It covers the aspects of this policy specifically associated with the recognition of potential intrusions. This objective supports O.IPS_ATTACK_DETECTION and O.IPS_RFC_COMPLIANCE by providing a way to consequently control the effectiveness of the intrusion prevention function's configuration, and to recognize possible false positives for what they are.

4.5 Improper use prevention objectives

O.PCAOA

The TOE must monitor administrators' access to security administration operations according to their individual privileges associated with various administration tasks.

Rationale: O.PCAOA is dedicated to:

- *The prevention of T.IMPROPER_USE, since it allows implementing the separation of tasks adapted to each administrator's responsibility and skills,*
- *The prevention of illegal administration operations (T.ILLEGAL_ADMIN), since it allows preventing certain illegal administration operations (for which access control is technically feasible, cf. O.LAA_PCAOA).*

O.PCAOA_I&A_ADMIN

The TOE must require administrators to be identified and authenticated before granting them access to the security administration function.

Rationale: O.PCAOA_I&A_ADMIN provides a way to base the access control specified by O.PCAOA and the accountability specified by O.LAA_PCAOA on the identity of administrators, in order to counter T.IMPROPER_USE and T.ILLEGAL_ADMIN.

O.LAA_PCAOA

The TOE must: log events relating to security administration operations performed by each authorized administrator,

- allow auditing and attributing logs of these events, and
- log and raise alarms to the administrator when events that have been specified by the administrator as critical have been detected, in particular attempts to open unauthorized administration sessions.

Rationale: In many operating contexts, it is not preferable or technically possible to prevent administrators from performing certain security administration operations, but rather to train them and foster a sense of responsibility with regard to the effects of these operations, while ensuring consequently that they perform them sensibly. This is the context in which O.LAA_PCAOA, with the support of AH.PERSONNEL, completes O.PCAOA when the prevention of T.IMPROPER_USE and T.ILLEGAL_ADMIN cannot be carried out by controlling technical access to security administration operations.

O.BACKUP_RESTORATION

The TOE must provide means to back up the current configuration of its security functions, and to restore it subsequently. The TOE ensures confidentiality and integrity of the configuration transmitted over the network.

Rationale: O.BACKUP_RESTORATION contributes to the prevention of improper use (T.IMPROPER_USE) by making it possible to keep and restore configuration templates that have been validated with regard to well-defined security issues, and to backtrack in the event of an error. This objective is dedicated to the satisfaction of the policy P.BACKUP_RESTORATION.

4.6 Protection objectives of the TOE

O.RESIST_AUTH_ADMIN

The TOE must provide authentication mechanisms that prevent the reuse of data originating from the authentication of administrators that have been authorized to log on remotely and/or the counterfeiting of authentication data allowing a hacker to spoof the identity of an authorized administrator.

Rationale: O.RESIST_AUTH_ADMIN is dedicated to the prevention of the threat T.ADMIN_USURP, which is a possible requirement for the execution of T.ILLEGAL_ADMIN.

O.PROTECT_LOGS

The TOE able to locally store logs must be able to implement file rotation functions for security event log files, shut down the logging of such events or fully block information flows when potential file saturation arises.

The TOE can also centralise logs onto a log server and ensures confidentiality and integrity of events transmitted over the network.

Rationale: O.PROTECT_LOGS is dedicated to the prevention of the threat T.AUDIT. It supports the objectives O.LAA_PCFI, O.LAA_IPS and O.LAA_PCAOA to counter violations of the P.AUDIT_ALARM policy and to counter the threats T.IMPROPER_USE and T.ILLEGAL_ADMIN.

O.PROTECT_ADMIN_SESSIONS

The TOE must provide mechanisms that allow protecting the contents of remote administration sessions from hackers' attempts to view, alter or delete data.

Rationale: O.PROTECT_ADMIN_SESSIONS is dedicated to the prevention of the threat T.ILLEGAL_ADMIN_SESSION, which is a possible requirement for the execution of T.ILLEGAL_ADMIN.

4.7 Security objectives for the environment

OE.PROTECT_APPLIANCES

Objective making it possible to ensure the reality of the assumption AP.PROTECT_APPLIANCES.

Rationale: This security objective is dedicated to the prevention of the physical aspect of T.ILLEGAL_ADMIN. It eliminates the possibilities of performing illegal security administration operations from local access to Stormshield appliances in the absence of the super-administrator.

OE.SUPER_ADMIN

Objective making it possible to ensure the reality of the assumption AO.SUPER_ADMIN.

Rationale:

1. *The result of centralizing the ability to carry out the installation or maintenance of Stormshield appliances in the power of the super-administrator (AO.SUPER_ADMIN.1) is the guarantee of the overall proper operation of the TOE's security functions. AO.SUPER_ADMIN.1 therefore supports all security objectives specified for the TOE to counter threats and satisfy the rules of the security policy.*
2. *The result of centralizing the ability to implement the policy of separating administration tasks in the power of the super-administrator (AO.SUPER_ADMIN.2) is the guarantee of the proper operation of the security functions dedicated to O.PCAOA and O.LAA_PCAOA. AO.SUPER_ADMIN.2 therefore supports these security objectives specified for the TOE to counter the threats T.IMPROPER_USE and T.ILLEGAL_ADMIN.*

3. *Furthermore, the fact that all interventions in the premises where the Stormshield appliances are stored are carried out under the supervision and responsibility of the super-administrator (AO.SUPER_ADMIN.3) eliminates the possibilities of performing illegal security administration operations from local access to Stormshield appliances in the presence of the super-administrator. AO.SUPER_ADMIN.3 therefore complements AP.PROTECT_APPLIANCES to counter T.ILLEGAL_ADMIN.*

OE.PASSWORD

Objective making it possible to ensure the reality of the assumption AO.PASSWORD.

Rationale: This security objective supports O.PCAOA_I&A_ADMIN to counter T.IMPROPER_USE and T.ILLEGAL_ADMIN by guaranteeing that administrators' identification / authentication function cannot be circumvented by obtaining the password of an authorized administrator.

OE.GOOD_PCFI

Objective making it possible to ensure the reality of the assumption AO.GOOD_PCFI.

Rationale: This security objective is dedicated to the prevention of T.IMPROPER_USE.

OE.CRYPTO_EXT

Objective making it possible to ensure the reality of the assumption AO.CRYPTO_EXT.

Rationale: by imposing the condition that the operational environment provides the keys complying with the RGS, this objective contributes to the satisfaction of the policy P.CRYPTO. It also supports a safe implementation of the encryption policy P.VPN. and contributes to countering T.ILLEGAL_ADMIN.

OE.PERSONNEL

Objective making it possible to ensure the reality of the assumption AH.PERSONNEL.

Rationale: This security objective is dedicated to the prevention of T.IMPROPER_USE.

OE.INTERPOSITION

Objective making it possible to ensure the reality of the assumption AIT.INTERPOSITION.

Rationale: This security objective supports all the security objectives specified to counter the threats and to satisfy the rules of the security policy associated with information flow control and protection from Internet attacks, since it allows preventing the bypass of security functions dedicated to these objectives by prohibiting the setup of information flows subject to the PCFI but which, owing to the fact that it does not pass through any StormShield appliances, would not be subject to these security functions.

OE.STRICT_USAGE

Objective making it possible to ensure the reality of the assumption AIT.STRICT_USAGE.

Rationale: This security objective is dedicated to the prevention of T.ILLEGAL_ADMIN. It eliminates the possibility of performing illegal security administration operations, or of modifying the behavior of Stormshield appliances in any other way, through unauthorized access based on possible vulnerabilities on software launched on the appliances and not subject to the evaluation. The prohibition of protocols other than IP (AppleTalk, IPX, etc.) allows preventing the bypass of the information flow control policy in a manner similar to OE.INTERPOSITION.

OE.AUTONOMOUS

Objective making it possible to ensure the reality of the assumption AIT.AUTONOMOUS.

Rationale: This security objective eliminates the risk of bypassing security functions through the intrusion or substitution of external devices on which the TOE may depend in order to carry out its functions. It therefore supports all the security objectives specified for the TOE to counter threats and satisfy the rules of the security policy.

OE.PROTECT_WORKSTATIONS

Objective making it possible to ensure the reality of the assumption AIT.PROTECT_WORKSTATIONS.

Rationale: This security objective is dedicated to the prevention of T.ILLEGAL_ADMIN.

OE.PROTECT_VPN_PEER

Objective making it possible to ensure the reality of the assumption AIT.PROTECT_VPN_PEER.

Rationale: This security objective supports O.PCFI_ENCRYPTION to satisfy P.VPN by guaranteeing that the focus of the encryption policy (protection of the confidentiality and integrity of information flows) cannot be bypassed by retrieving session keys on remote devices.

OE.PROTECT_VPN_CLIENTS

Objective making it possible to ensure the reality of the assumption AIT.PROTECT_VPN_CLIENTS.

Rationale: This security objective supports O.PCFI_ENCRYPTION to satisfy P.VPN by guaranteeing that the focus of the encryption policy (protection of the confidentiality and integrity of information flows) cannot be bypassed by retrieving session keys on remote devices

OE.TIMESTAMPS

Objective making it possible to ensure the reality of the assumption AIT.TIMESTAMPS.

Rationale: This security objective supports O.LAA_PCFI, O.LAA_IPS and O.LAA_PCAOA to satisfy P.AUDIT_ALARM by providing reliable timestamps.

OE.REVOCATION_LIST

Objective making it possible to ensure the reality of the assumption AIT.REVOCATION_LIST.

Rationale: This security objective supports O.PCFI_ENCRYPTION and O.PCAOA_I&A_ADMIN to satisfy P.VPN, T.IP_SPOOFING, T.IMPROPER_USE and T.ILLEGAL_ADMIN by providing up to date revocation status to X.509 authentication mechanism.

OE.ENROLLMENT

Objective making it possible to ensure the reality of the assumption AIT.ENROLLMENT.

Rationale: This security objective supports O.PCFI_ENCRYPTION to satisfy P.VPN by providing a reliable enrollment infrastructure.

4.8 Rationale of security objectives

The way security objectives prevent threats and satisfy rules in the security policy is expressed in the “Rationale” sections that accompany the description of each security objective. The link between security objectives and threats or rules of the security policy is summarized below.

		P.FILTERING	P.VPN	P.AUDIT_ALARM	P.ANALYSIS	P.CRYPTO	T.IP_SPOOFING	T.IMPROPER_USE	P.BACKUP_RESTORATION	T.ILLEGAL_ADMIN	T.ADMIN_USURP	T.ILLEGAL_ADMIN_SESSION	T.AUDIT
O.PCFI_FILTERING		X											
O.PCFI_APPLICATION_CONTEXT		S											
O.PCFI_ENCRYPTION			X				X						
O.LAA_PCFI				X									
O.CRYPTO			S			X				S			
O.IPS_ATTACK_DETECTION					X		X						
O.IPS_RFC_COMPLIANCE					X								
O.LAA_IPS				X	S		S						
O.PCAOA								X		X			
O.PCAOA_I&A_ADMIN								X		X			
O.LAA_PCAOA								X		X			
O.BACKUP_RESTORATION								X	X				
O.RESIST_AUTH_ADMIN										X	X		
O.PROTECT_LOGS				S				S		S			X
O.PROTECT_ADMIN_SESSIONS										X		X	
OE.PROTECT_APPLIANCES										X			
OE.SUPER_ADMIN	1	S	S	S	S		S	S	S	S	S	S	S
	2							S		S			
	3									S			
OE.PASSWORD								S		S			
OE.GOOD_PCFI								X					
OE.CRYPTO_EXT			S			X				S			
OE.PERSONNEL								X					
OE.INTERPOSITION		S	S	S	S		S						
OE.STRICT_USAGE		S	S	S	S		S			X			
OE.AUTONOMOUS		S	S	S	S		S	S	S	S	S	S	S
OE.PROTECT_WORKSTATIONS										X			
OE.PROTECT_VPN_PEER			S										
OE.PROTECT_VPN_CLIENTS			S										
OE.TIMESTAMPS				X									
OE.REVOCATION_LIST			S				S	S		S			
OE.ENROLLMENT			S										

Legend:

X: the objective is dedicated to the prevention of the threat / the satisfaction of the rule of the security policy.

S: the objective supports other objectives to prevent threats / satisfy rules of the security policy.

4.9 Links between assumptions and the security objectives for the environment

The table below shows the link between the security assumptions for the environment and the associated objectives.

	AP.PROTECT_APPLIANCES	AO.SUPER_ADMIN	AO.PASSWORD	AO.GOOD_PCFI	AO.CRYPTO_EXT	AH.PERSONNEL	AIT.INTERPOSITION	AIT.STRICT_USAGE	AIT.AUTONOMOUS	AIT.PROTECT_WORKSTATIONS	AIT.PROTECT_VPN_PEER	AIT.PROTECT_VPN_CLIENTS	AIT.TIMESTAMPS	AIT.REVOCATION_LIST	AIT.ENROLLMENT
OE.PROTECT_APPLIANCES	X														
OE.SUPER_ADMIN		X													
OE.PASSWORD			X												
OE.GOOD_PCFI				X											
OE.CRYPTO_EXT					X										
OE.PERSONNEL						X									
OE.INTERPOSITION							X								
OE.STRICT_USAGE								X							
OE.AUTONOMOUS									X						
OE.PROTECT_WORKSTATIONS										X					
OE.PROTECT_VPN_PEER											X				
OE.PROTECT_VPN_CLIENTS												X			
OE.TIMESTAMPS													X		
OE.REVOCATION_LIST														X	
OE.ENROLLMENT															X

Legend:

X: the objective is linked to the security assumption for the environment.

5 SECURITY REQUIREMENTS

The aim of this section is to set out the security requirements for information technologies, which arise from the refinement of security objectives, as well as an Rationale demonstrating that this refinement has been correctly carried out.

The security requirements comprise the security requirements for the TOE and the security requirements for the environment, which, if satisfied, will guarantee that the TOE can meet its security objectives.

The CC divides security requirements into two categories: functional requirements and assurance requirements. Functional requirements relate to functions of the TOE that specifically contribute to IT security and which guarantee the desired behavior in terms of security. Assurance requirements relate to actions that the developer needs to perform, the evidence to produce and the actions to be taken by the evaluator.

5.1 Introduction

5.1.1 Overview

The TOE's security functional requirements are divided into the following function sub-sets:

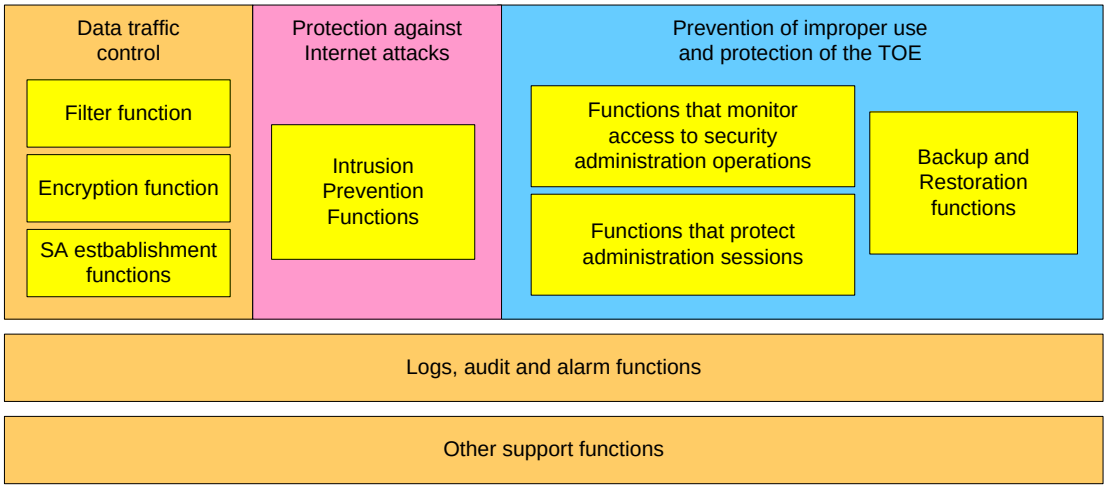


Illustration 5: *Functional subsets of the TOE.*

5.1.2 Typographical conventions

In order to present security requirements in a way that makes them easy to read and use, they have been drafted by transposing Common Criteria concepts (such as "TSF" or "subjects" and "objects") in terms corresponding to the product, in the form of operations assigning, selecting and refining the Common Criteria. The operations have not been identified in the text of this section's requirements, only the names that result from their application have been indicated in bold.

However, only the wording extracted from [CC-02] and [CC-03] has prescriptive value and acts as a reference. Furthermore, operations performed have to be accurately identified. Appendix C, §9, has been specially drafted for this purpose and makes up the element of proof to be taken into account as set out in the IT security requirements.

The extended security requirements have been drafted in the same manner in this chapter. Appendix D, §10, sets out these extended security requirements in a format similar to the one in [CC-02].

Format for labeling security requirements:

- Security Assurance Requirements have the same labels as the ones used in [CC-03];

- Security Functional Requirements have labels in the following format:

  F*CC_FFF.component.<iteration>n*

  - F*CC* is the three-letter acronym of the class;
  - *FFF* is the three-letter acronym of the family;
  - *component* is the component's identifier: either a number for components extracted from [CC-02], or a three-letter acronym for extended security requirements;
  - *iteration* is a label that allows identifying the various iterations of the same component inside various functional sets;
  - *n* is the item number.

5.1.2.1.1 IKE protocol:

The TOE implements versions 1 and 2 of the IKE negotiation protocol. But only version 2 is in the scope of evaluation.

5.1.3 Presentation of security data

5.1.3.1 Attributes of IP packets concerned by filter and encryption rules

- The receiving interface of the packet;
- The destination interface of the packet;
- The source and destination IP address of the packet and, based on that, the packet's source and destination machine or, for SCTP packet, one of the endpoint IP addresses in case of multi-homed endpoints;
- The IP protocol number;
- The value of the DSCP field;
- The ESP security index;
- The source and destination TCP/UDP/SCTP port or the type of ICMP message.

5.1.3.2 Concept of slots

The behavior of security functions is described with the help of "*slots*", which are an abstract representation that administrators of the Stormshield appliance's configuration files will be able to interpret. Slots describe well-defined security behaviors that can be saved and reused. They can be enabled on demand

In the scope of the evaluation, we will focus on two types of slots: filter slots and encryption slots (also known as "VPN slots"):

- A filter slot is a list of filter and address translation rules. The filter policy applied is a sequence of two filter slots – the global filter slot then the local filter slot. During operation, there is always at least one active local filter slot.
- An encryption slot is a set of VPN tunnels.

5.1.3.3 Parameters of filter rules

- Rule ID;
- (criterion) The receiving interface of IP packets covered by the rule;
- (criterion) The destination interface of IP packets covered by the rule;
- (criterion) The machine(s) or, for SCTP, in case of multi-homing, the endpoint primary path at the source of the information flows covered by the rule;
- (criterion) the IP protocol(s), DSCP field, TCP/UDP services or types of ICMP messages of information flows covered by the rule;

- (criterion) The machine(s) or, for SCTP, in case of multi-homing, the endpoint primary path of the destination of the information flows covered by the rule;
- The action: ‘none’, ‘pass’, ‘block’, ‘reinitialize’, ‘delegate’;
- The generation of an audit log and the alarm level assigned, if any;
- The Quality of Service policy associated with the information flows covered by the rule;
- The maximum rate of open connections / pseudo-connections / associations associated with the rule;
- The profile of Internet attacks associated with connections covered by the rule.

5.1.3.4 Parameters of a connection / pseudo connection / association

- (criterion) The source IP address, destination IP address;
- (criterion) The type of protocol (TCP, UDP, SCTP, ICMP or IP if none of previous);
- (criterion) For TCP, UDP and SCTP: source and destination ports;
- (criterion) For ICMP: the ‘type’ and ‘code’ fields of the ICMP message;
- (optional criterion) For IP: the DSCP field;
- For UDP and ICMP: the age of the pseudo-connection;
- For TCP: the status of the connection, windows (for the purpose of rejecting packets that do not conform).
- For SCTP: the status of the association, the source and destination IP addresses for multi-homed association, the verification tag and the association cookie.

5.1.3.5 Characteristics of IPSec users

- The user’s login name;
- Information about the user (last name, first name, telephone number, e-mail address, etc.);

5.1.3.6 Privileges of IPSec users

- The user’s login name;
- The fact that the user is authorized to authenticate (a user can be revoked without deleting his account).

5.1.3.7 Parameters of VPN tunnels

A VPN tunnel consists of a trusted path (the IKE SA) between the Stormshield appliance and a VPN peer, as well as a set of encryption rules to be applied to information flows that have to pass through the tunnel. The application of these rules requires the negotiation and establishment of security contexts that are IPSec SAs.

The VPN tunnel settings are the following:

- The local interface on which the tunnel has to be set up;
- The IP address of the other tunnel endpoint (the VPN peer);
- The mutual authentication mechanism: pre-shared key (PSK) or certificates (PKI);
- In an authentication by certificate: the X509 certificate presented by the StormShield appliance;
- In an authentication by pre-shared key: the IP address of the Stormshield appliance;
- The encryption rules associated with the tunnel;
- The current IKE SA pair associated with the VPN tunnel;

5.1.3.8 Parameters of an IKE SA

- The VPN peer;
- The current age of the SA;
- Its lifetime;
- The effective authentication algorithm and its key;
- The effective encryption algorithm and its key;

5.1.3.9 Encryption rule (SPD entry)

- (criterion) The local machine(s) covered by the rule;
- (criterion) The remote machine(s) covered by the rule;
- (criterion) The type of protocol covered by the rule;
- The acceptable proposals during the SA negotiation:
  - Authentication algorithms and key sizes;
  - Encryption algorithms and key sizes;
  - SA lifetime.
- The current IPSec SA pairs associated with the rule.

5.1.3.10 Parameters of an IPSec SA

- (criterion) The SPI (*Security Parameter Index*) ;
- The current age of the SA;
- Its lifetime;
- Whether it is incoming or outgoing;
- The effective authentication algorithm and its key;
- The effective encryption algorithm and its key;

5.1.3.11 Characteristics of VPN peers managed by the Stormshield appliance

- Either an X509 certificate or a CA (with the associated CRL or OSCP server) in an authentication by certificate;
- Or the login (IP address), associated with a pre-shared key;
- Or the login associated with the user's password.

5.1.3.12 Profile of Internet attacks

- Name;
- The associated action: block or let the packet through (not always configurable);
- The desired alarm level: ignore, minor or major.

5.1.3.13 Profile of system events

- Name;
- The desired alarm level: ignore, minor, major or system

5.1.3.14 Characteristics of administrators

- The administrator’s login name;
- Information about the administrator (last name, first name, telephone number, e-mail address, etc.);
- The fact that the administrator is authorized to authenticate (an administrator can be revoked without deleting his account);

- The authentication mechanism[3].

5.1.3.15 Administrator privileges

- The administrator's login name;
- The group to which the administrator belongs;
- The list of the administrator's privileges.

Administrators are managed in the LDAP Server used for non-administrator users, but they are assigned an explicit administrator role as well as a profile built from a modification privilege ('M') and privileges associated with various domains of security management. The details of various privileges are provided in Appendix A, §7.

The privileges assigned to administrators and IPSec users are managed in distinct files in a local database.

The term 'auditor" is used to refer to administrators tasked with performing audits and managing audit logs. These auditors are administrators with the 'L' privilege.

5.2 Security requirements for the TOE

This section sets out the refinement of the TOE's functional requirements. The formal description of these requirements is given in Chapter 9, The extended functional requirement is described in Chapter 10. To ensure traceability, the titles of the functional requirements concerned are indicated here in square brackets (e.g.: [FDP_IFC.2.1]).

5.2.1 Information flow control requirements

5.2.1.1 Filter function

5.2.1.1.1 FDP_IFC.2 – Full filtering of information flows

[FDP_IFC.2.1]
The filter function must apply the **filter policy** to **incoming IP packets**.

[FDP_IFC.2.2]
The filter function must guarantee that **all incoming IP packets** are covered by the **filter policy**.

Rationale: FDP_IFC.2 supports FDP_IFF.1.Filtering to satisfy O.PCFI_FILTERING, by defining the filter policy and requiring that it applies to all incoming IP packets.

5.2.1.1.2 FDP_IFF.1.Filtering – Filter function

[FDP_IFF.1.Filtering.1]
The filter function must apply the **filter policy** according to the following types *of security attributes of **Incoming IP packets**:*

a. The receiving interface,

b. The destination interface,

c. The source and destination IP address of the packet and, based on that, the source and destination host of the packet,

d. The IP protocol number,

e. The value of the DSCP field,

f. If the protocol is TCP or UDP: the source and destination port,

g. If the protocol is ICMP: the message's 'type' and 'code' fields,

h. If the protocol is SCTP: the source and destination port.

[3] Mandatory login / password (TLS) or Certificate (TLS) in the usage mode subject to evaluation.

[FDP_IFF.1.Filtering.2]

The filter function must authorize **an incoming IP packet** if the following rules apply:

a. Prior to the application of the filter rules, the packet is compared against all connections / pseudo-connections / associations currently set up and having been allowed by the filter rules;

b. If the packet corresponds to one of these connections / pseudo-connections / associations, it can pass through without being subject to filter rules;

c. Otherwise, the packet will be allowed if the action of the first applicable filter rule is 'pass'.

[FDP_IFF.1.Filtering.3]

The filter function must apply **the following complementary rules:**

a. the only purpose of filter rules with a 'none' action is to generate audit logs and are not taken into account in packet filtering.

b. the only purpose of filter rules with a 'delegate' action is to skip the evaluation of the end of the global filter slot to go back to the beginning of the local slot and are not taken into account in packet filtering.

FDP_IFF.1.Filtering.4]

The filter function must explicitly authorize **an incoming IP packet** according to the following rules:

a. Sessions associated with protocols requiring child connections are tracked so that these child connections will be authorized according to the status of the main session;

b. The firewall can generate implicit filter rules together with the configuration of other security functions. These are rules corresponding to:

i. The remote administration of the firewall,

ii. VPN setup.

[FDP_IFF.1.Filtering.5]

The filter function must explicitly prohibit **an incoming IP packet** according to the following rules:

a. The action of the first applicable filter rule is 'block' or 'reinitialize';

b. No filter rules have allowed the packet to pass through.

Rationale: FDP_IFF.1.Filtering is dedicated to the satisfaction of the objective O.PCFI_FILTERING. Point FDP_IFF.1.Filtering.4.a also covers the objective O.PCFI_APPLICATION_CONTEXT.

5.2.1.2 Encryption function

5.2.1.2.1 FDP_IFC.1 – Encryption of information flows

[FDP_IFC.1.1]

The encryption function must apply the **encryption policy** to **incoming ESP datagrams and outgoing IP datagrams covered by an encryption rule**.

Rationale: FDP_IFC.1 supports FDP_UCT.1, FDP_UIT.1 and FDP_IFF.1.Encryption to satisfy O.PCFI_ENCRYPTION, by defining the encryption policy.

5.2.1.2.2 FDP_UCT.1 – Confidentiality of the contents of information flows

[FDP_UCT.1.1]

The **encryption function** must apply the **encryption policy** to be able to **send and receive IP datagrams** in a way that protects them from unauthorized disclosure.

Rationale: FDP_UCT.1 is dedicated to the satisfaction of the "confidentiality" aspect of the objective O.PCFI_ENCRYPTION.

5.2.1.2.3 FDP_UIT.1 – Integrity of the contents of information flows

[FDP_UIT.1.1]

The encryption function must apply the **encryption policy** to be able to **send and receive IP datagrams** in a way that protects them from **modification, insertion or replay** errors.

[FDP_UIT.1.2]

The encryption function must be able to determine when receiving **incoming ESP datagrams** whether they any **modification, insertion or replay** has taken place.

Rationale: FDP_UIT.1 is dedicated to the satisfaction of the "integrity" aspect of the objective O.PCFI_ENCRYPTION.

5.2.1.2.4 FDP_IFF.1.Encryption – Encryption function

[FDP_IFF.1.Encryption.1]

The encryption function must apply the encryption **policy** according to the following types of security attributes of incoming **ESP datagrams and outgoing IP datagrams covered by an encryption rule:**

Incoming ESP datagrams:

a. Security Parameter Index (*SPI*),

Outgoing IP datagrams:

b. Either the source and destination IP addresses and IP protocol of the packet, and based on that, the packet's source and destination machine,

c. or the virtual tunnel outgoing interface (VTI).

[FDP_IFF.1.Encryption.2]

The encryption function must authorize **an incoming ESP packet** if the following rules apply:

a. an incoming ESP datagram can be attached to an active incoming IPSec SA,

b. the packet encapsulated in the ESP datagram corresponds to the criteria of the encryption rule associated with the IPSec SA.

[FDP_IFF.1.Encryption.3]

The encryption function must apply **the following complementary rules:**

a. on outgoing IP datagrams, use the effective authentication and encryption algorithms specified by the outgoing IPSec SA associated with the first applicable encryption rule.

b. launch a renegotiation attempt if an outgoing IP datagram is covered by an encryption rule without an active IPSec SA and no other attempt is in progress. The datagram will be destroyed.

[FDP_IFF.1.Encryption.4]

(not applicable).

[FDP_IFF.1.Encryption.5]

(not applicable).

Rationale: FDP_IFF.1.Encryption supports FDP_UCT.1, FDP_UIT.1 and FTP_TRP.1.Peer to satisfy O.PCFI_ENCRYPTION:

- *by guaranteeing that the encryption function is applied to outgoing IP datagrams covered by the encryption policy,*
- *by directing the incoming ESP datagrams to the integrity and decryption control processes specified by the applicable incoming IPSec SA,*
- *by turning to the use of the trusted path if the outgoing IP datagram is covered by an encryption rule without an applicable outgoing IPSec SA.*

5.2.1.3 SA establishment function

5.2.1.3.1 FTP_TRP.1.Peer – Trusted path with VPN peers

[FTP_TRP.1.Peer.1]

The SA establishment function must provide a communication channel between the **Stormshield appliance and VPN peers** that is logically distinct from the other communication channels and which guarantees the identification of its endpoints and the protection of transferred data from **modification or disclosure**.

[FTP_TRP.1.Peer.2]

The SA establishment function must allow the **Stormshield appliance and VPN peers** to initiate communication via the trusted path. **The establishment of the trusted path corresponds to IKE_SA of the IKE protocol.**

[FTP_TRP.1.Peer.3]

The SA establishment function must require the use of the trusted path for:

- **the initial mutual authentication of tunnel endpoints (IKE_SA),**
- **the negotiation of IPSec SAs (CHILD_SA)**.

Rationale: FTP_TRP.1.Peer is dedicated to the satisfaction of the "mutual authentication of endpoints" aspect of the objective O.PCFI_ENCRYPTION.

5.2.1.3.2 FIA_UAU.5.Peer – Multiple authentication mechanisms of VPN peers

[FIA_UAU.5.Peer.1]

The SA establishment function must provide the **following authentication mechanisms** to participate in the authentication of the **VPN peer of a given tunnel, in the context of an initial mutual authentication of the endpoints of this tunnel during IKE_SA:**

- **X509 certificates,**
- **pre-shared key.**

[FIA_UAU.5.Peer.2]

The SA establishment function must authenticate the announced identity of any **VPN peer** according to the **authentication mechanism specified for the VPN tunnel**.

Rationale: FIA_UAU.5.Peer supports FTP_TRP.1.Peer to satisfy the objective O.PCFI_ENCRYPTION.

5.2.1.3.3 FPT_TDC.1 – Negotiation of IKE and IPSec SAs

[FPT_TDC.1.1]

The SA establishment function must offer the possibility of **negotiating IKE and IPSec SA parameters during the establishment of VPN tunnels between the Stormshield appliance and VPN peers**.

[FPT_TDC.1.2]

The SA establishment function must use the **following rules** to **negotiate IKE or IPSec SA parameters with VPN peers:**

a. If the Stormshield appliance is the initiator, propose the parameters of the IKE or IPSEC SA, and accept the responses that are as strict as one of the proposals made;

b. If the Stormshield appliance is the responder, accept only proposals that are as strict as one of the local proposals.

Rationale: FPT_TDC.1 supports:

- *Firstly FTP_TRP.1 to satisfy the "mutual authentication of endpoints" aspects of the objective O.PCFI_ENCRYPTION, by allowing the negotiation of parameters that will enable mutual authentication,*
- *And FDP_UCT.1 and FDP_UIT.1 to satisfy the "confidentiality" and "integrity" aspects of the objective O.PCFI_ENCRYPTION by allowing the negotiation of encryption and authentication algorithm parameters.*

5.2.1.4 Enrollment function

5.2.1.4.1 FIA_X509_EXT.4 – Alternate X.509 Enrollment

[FIA_X509_EXT.4.1]
The **enrollment function** shall use the Enrollment over Secure Transport (EST) protocol as specified in RFC 7030 to request certificate enrollment using the simple enrollment method described in RFC 7030 Section 4.2.

[FIA_X509_EXT.4.2]
The **enrollment function** shall be capable of authenticating EST requests using an existing certificate and corresponding private key as specified by RFC 7030 Section 3.3.2.

[FIA_X509_EXT.4.3]
The **enrollment function** shall be capable of authenticating EST requests using HTTP Basic Authentication with a username and password as specified by RFC 7030 Section 3.2.3.

[FIA_X509_EXT.4.4]
The **enrollment function** shall perform authentication of the EST server using an Explicit Trust Anchor following the rules described in RFC 7030, section 3.6.1.

[FIA_X509_EXT.4.7]
The **enrollment function** shall generate a Certificate Request Message for EST as specified in RFC 2986 and be able to provide the following information in the request: public key and Common Name, Organization, Organizational Unit, Country.

Rationale: FIA_X509_EXT.4 is dedicated to the satisfaction of the initial enrollment necessary to implement O.PCFI_ENCRYPTION.

5.2.1.4.2 FCS_HTTPS_EXT.1 HTTPS Protocol

[FCS_HTTPS_EXT.1.1]
The **enrollment function** shall implement the HTTPS protocol that complies with RFC 2818.

[FCS_HTTPS_EXT.1.2]
The **enrollment function** shall implement HTTPS using TLS as specified in FCS_TLSC_EXT.1.

Rationale: FCS_HTTPS_EXT.1 supports FIA_X509_EXT.4 to satisfy the initial enrollment necessary to implement O.PCFI_ENCRYPTION, by providing secure applicative communication with EST Server.

5.2.1.4.3 FCS_TLSC_EXT.1 TLS Client Protocol

[FCS_TLSC_EXT.1.1]
The **enrollment function** shall implement TLS 1.2 (RFC 5246) or TLS 1.3 (RFC

8446) and **no other version** supporting the following ciphersuites:

- TLS_AES_128_GCM_SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- TLS_CHACHA20_POLY1305_SHA256
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- TLS_AES_256_GCM_SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-CHACHA20-POLY1305-SHA256
- no other ciphersuite.

[FCS_TLSC_EXT.1.2]

The **enrollment function** shall verify that the presented identifier matches the reference identifier according to RFC 6125.

[FCS_TLSC_EXT.1.5]

The **enrollment function** shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [selection: secp256r1, secp384r1, secp521r1, BrainpoolP256r1 BrainpoolP384r1 BrainpoolP512r1] and no other curves.

Rationale: FCS_TLSC_EXT.1 supports FCS_HTTPS_EXT.1 to satisfy the initial enrollment necessary to implement O.PCFI_ENCRYPTION, by providing secure network communication with EST Server.

5.2.1.5 Log, audit and alarm function

5.2.1.5.1 FAU_GEN.1 – Generation of audit data

[FAU_GEN.1.1]

The log function must be able to generate an audit log of the following auditable events:

Startup and shutdown of the **log function**,

and the **auditable events set out in the table in chapter 5.2 (after FAU_GEN.1.2)**

[FAU_GEN.1.2]

The log function must record at least the following information in each audit log:

date and time of the event,

type of event,

source IP address,

result (success or failure) of the event,

alarm level (if it is one),

for each type of log event, the complementary audit information listed in the table below:

Component	*Auditable events*	*Audit information*
FDP_IFF.1.Filtering	Application of a filter rule for which the generation of an audit log has been specified.	• Name of the receiving interface, • Name of the destination interface, • Action applied.

		• rule ID, • Type of protocol, • ICMP type, • Source port • IP address and destination port,
FTP_TRP.1.Peer and FPT_TDC.1	Attempt to establish an IKE and IPSec SA	• IKE phase (1 or 2), • If failure: reason for the failure (if possible).
FAU_STG.3	Limit exceeded	•
FAU_SAA.4	Detection of potential internet attack	• Name of the receiving interface, • Action applied. • Attack name • Type of protocol, • ICMP type, • Source port • IP address and destination port,
FMT_SMR.1, FMT_MOF.1, FMT_MTD.1, FTP_TRP.1.Admin	Accomplishment of a security administration operation (including attempts to open administration sessions)	• Type of operation, • Parameters, • Administration session ID,

Rationale: FAU_GEN.1 is dedicated to the satisfaction of the "log" aspects (point 1) of the objectives O.LAA_PCFI, O.LAA_IPS and O.LAA_PCAOA. For events associated with FDP_IFF.1.Filtering and FAU_SAA.4, the result (success or failure) associated with the event corresponds to the action that the Stormshield appliance has applied.

5.2.1.5.2 FAU_GEN.2 – User identification

[FAU_GEN.2.1]

For any audit event resulting from the actions of identified **administrators**, the log function must be able to associate this **auditable event linked to security administration operations** with the identity of the **administrator** who caused this event.

Rationale: FAU_GEN.2 is dedicated to the satisfaction of "accountability" aspects (point 2) of the objective O.LAA_PCAOA.

5.2.1.5.3 FAU_SAR.1 – Audit review

[FAU_SAR.1.1]

The audit function has to offer **auditors** the ability to read **all audit information** from **log files**.

[FAU_SAR.1.2]

The audit function must present **log files** in a way that would allow the **auditor** to interpret them.

Rationale: FAU_SAR.1 is dedicated to the satisfaction of the "audit" aspects (point 2) of the objectives O.LAA_PCFI, O.LAA_IPS and O.LAA_PCAOA.

5.2.1.5.4 FAU_STG.3 – Action in the event of possible loss of audit data

[FAU_STG.3.1]

The log function must carry out **a file rotation: the most recent audit logs erase the oldest audit logs if the existing log file (excluding the use of Syslog) exceeds 20 MB.**

Rationale: FAU_STG.3 is dedicated to the satisfaction of the objective O.PROTECT_LOGS. It does not apply to a TOE that is unable to log events locally.

5.2.2 Requirements of protection from Internet attacks

5.2.2.1 Intrusion prevention function

5.2.2.1.1 FAU_SAA.4 – Heuristics of complex attacks

[FAU_SAA.4.1]

The intrusion prevention function must be able to maintain a **knowledge base**[4]of signature events and event sequences that may indicate a **potential Internet attack**:

[FAU_SAA.4.2]

The intrusion prevention function must be able to compare **the status of the various contexts associated with each incoming and outgoing IP packet against types of attacks in the knowledge base**.

[FAU_SAA.4.3]

The intrusion prevention function must be able to indicate a **potential internet attack** when **the status of one or several contexts associated with an incoming IP packet** corresponds to a **type of attack in the knowledge base**.

Rationale: FAU_SAA.4 is dedicated to the satisfaction of the objective O.IPS_ATTACK_DETECTION as well as the implementation of compliance with the RFCs specified by O.IPS_RFC_COMPLIANCE.

5.2.2.1.2 FAU_ARP.1.IPS – Automatic response to potential internet attacks

[FAU_ARP.1.IPS.1]

Upon the detection of an **Internet attack potentially conveyed by an incoming IP packet**, the intrusion prevention function must:

a. apply to the packet the action associated with the type of attack,

b. if an alarm level has been specified for this type of attack, generate an audit log for the event, by assigning this level of alarm to it.

Rationale: FAU_ARP.1.IPS supports FAU_SAA.4 for the satisfaction of the objective O.IPS_ATTACK_DETECTION and for the implementation of compliance with the RFCs specified by O.IPS_RFC_COMPLIANCE. Furthermore, FAU_ARP.1.IPS is specifically dedicated to point 3 of the objective O.LAA_IPS.

5.2.3 Requirements of prevention of improper use

5.2.3.1 Function for the control of access to security administration operations

5.2.3.1.1 FMT_SMF.1 – Security administration function

[FMT_SMF.1.1]

The security administration function must be able to perform the following security administration functions:

a. The function for the control of access to security administration operations;

b. The administration session protection function

c. The audit function

d. The backup/restoration function

Rationale: FMT_SMR.1 supports FMT_MOF.1 and FMT_MTD.1 to satisfy the objective of controlling access to administration operations specified by O.PCAOA. It also ensures the implementation of FTP_ITT.1, FAU_SAR.1 and FMT_MTD.BRS

[4] The knowledge base is a set of controls; the controls in the scope of evaluation are listed in Appendix B – Attacks HANDLED BY ASQ.

5.2.3.1.2 FMT_SMR.1 – Role of the security administrator

[FMT_SMR.1.1]

The function for the control of access to security administration operations must manage the **"administrator" and "super administrator"** roles**.**

[FMT_SMR.1.2]

The function for the control of access to security administration operations must be able to associate roles with users **according to the following rules:**

a. There is only one super-administrator, distinct from other administrators, and who possess all privileges;

b. Administrators are persons to whom this role has been explicitly assigned.

Rationale: FMT_SMR.1 supports FMT_MOF.1 and FMT_MTD.1 to satisfy the objective of controlling access to administration operations specified by O.PCAOA. FMT_SMR.1 also supports FTP_TRP.1.Admin to satisfy the objective O.PCAOA_I&A_ADMIN.

5.2.3.1.3 FDP_ACC.2 – Control of full access to security administration operations

[FDP_ACC.2.1]

The function for the control of access to security administration operations must apply the **policy controlling access to security administration operations** to all security administration operations **performed by the administrator**.

[FDP_ACC.2.2]

The function for the control of access to security administration operations must guarantee that all security administration operations **performed by the administrator** are covered by **the policy controlling access to security administration operations**.

Rationale: FDP_ACC.2 supports FMT_MOF.1 and FMT_MTD.1 to satisfy the objective of controlling access to administration operations specified by O.PCAOA, by guaranteeing that the policy controlling access to administration operations is applied to all operations.

5.2.3.1.4 FMT_MOF.1 – Administration of the behavior of security functions

[FMT_MOF.1.1]

The function for the control of access to security administration operations must restrict the ability to **enable**, **disable**, **perform** or **modify the security functions in the table below** to **administrators, according to the privileges below:**

Security functions	*Operations / necessary privileges*
Filter function	Enable/Disable: (F or GF) +M
Encryption and SA establishment function	Enable/Disable: V+M
Backup function	Perform: Ma
Restoration function	Perform: Ma+M

Rationale: FMT_MOF.1 is dedicated to the satisfaction of the objective O.PCAOA. This component covers the administration tasks that set off security functions.

5.2.3.1.5 FMT_MTD.1 – Administration of security data

[FMT_MTD.1.1]

The function for the control of access to security administration operations must restrict the ability to **read**, **modify** or **delete the security functions in the table below** to **administrators, according to the privileges below:**

Security data	*Operations / necessary privileges*
Characteristics of IPSec users and administrators	Read: all administrators Modify: U+M
Assignment of the administrator role and administrative privileges to a user	Read: super-administrator Modify: A+M
Configuration of interfaces and network routes	Read: all administrators Modify interfaces: N+M Modify routes: R+M

Objects describing the network topology: machines, networks, protocols and predefined services	Read: all administrators Modify: (O or GO) +M
Filter slots: contents	Read: F Modify: F+M
Global filter slots: contents	Read: GF Modify: GF+M
Encryption slots: contents	Read: V Modify: V+M
Log files of security events	Read (and audit): L Erase: L+M
Monitoring data	Read (and audit): L Modify: L+MW
Log and alarm parameters including profiles of system events.	Read: all administrators Modify: *+M
Dynamic analysis parameters, including profiles of Internet attacks	Read: As Modify: As+M
Configuration backup and restoration	Backup: Ma Restoration: Ma+M
Time base	Read: all administrators Modify: Ma+M

Rationale: FMT_MTD.1 is dedicated to the satisfaction of the objective O.PCAOA. This component covers administrative tasks that consist of modifying security data.

5.2.3.2 Backup and restoration function

5.2.3.2.1 FMT_MTD.BRS – Backup and restoration of security data

[FMT_MTD.BRS.1]

The backup/restoration function must be able to back up **security data** on the **administration workstation's hard disk.**

[FMT_MTD.BRS.2]

The backup/restoration function shall allow restoration of **security data** saved on the **administration workstation's hard disk.**

Rationale: FMT_MTD.BRS is dedicated to the satisfaction of the objective O.BACKUP_RESTORATION. Resorting to this explicit component was necessary as the components of [CC-02] do not allow specifying the backup or restoration of security data.

5.2.4 TOE protection requirements

5.2.4.1 Administration session protection function

5.2.4.1.1 FPT_ITT.1 – Basic protection of the contents of administration sessions

[FPT_ITT.1.1]

The administration session protection function must protect **the contents of administration sessions** from **disclosure and modification** when they are sent between **administration workstation and the Stormshield appliance**.

Rationale: FPT_ITT.1 is dedicated to the satisfaction of the objective O.PROTECT_ADMIN_SESSIONS.

5.2.4.1.2 FTP_TRP.1.Admin – Trusted path for remote administration

[FTP_TRP.1.Admin.1]

The administration session protection function must provide a communication channel between **administrators and the Stormshield appliance** that is logically distinct from the other communication channels and which guarantees the identification of its endpoints and the protection of transferred data from **modification or disclosure**.

[FTP_TRP.1.Admin.2]

The administration session protection function must allow **administrators** to initiate communication via the trusted path.

[FTP_TRP.1.Admin.3]

The administration session protection function must require the use of the trusted path for:

a. the initial mutual authentication of the administrator and the Stormshield appliance,

b. remote security administration operations.

Rationale: FTP_TRP.1.Admin is dedicated to the satisfaction of the objective O.PCAOA_I&A_ADMIN. Furthermore, it supports FPT_ITT.1 to satisfy O.PROTECT_ADMIN_SESSIONS by providing the means to protect administration sessions.

5.2.4.1.3 FIA_UAU.5.Admin – Authentication mechanism for administrators

[FIA_UAU.5.Admin.1]

The administration session protection function must provide **the TLS protocol** to participate in the authentication of the **administrator**.

[FIA_UAU.5.Admin.2]

The administration session protection function must authenticate the announced identity of any **administrator** according to the **TLS protocol (login / password or X.509 certificate)**.

Rationale: FIA_UAU.5.Admin supports FTP_TRP.1.Admin to satisfy the objective O.PCAOA_I&A_ADMIN. The strength of mechanisms associated with TLS protocols enables the satisfaction of the objective O.RESIST_AUTH_ADMIN. Protection against replay and counterfeiting of authentication data is guaranteed by the exclusive use of CipherSuite TLS_DHE_RSA_WITH_AES_128_CBC_SHA (cf. [TLS-AES])

5.2.4.1.4 FTP_TRP.1.LDAP – Trusted path with LDAP server

[FTP_TRP.1.LDAP.1]

The secure LDAP communication function must provide a communication channel between **a LDAP server and the Stormshield appliance** that is logically distinct from the other communication channels and which guarantees the identification of its endpoints and the protection of transferred data from **modification or disclosure**.

[FTP_TRP.1.LDAP.2]

The secure LDAP communication function must allow **the TSF** to initiate communication via the trusted path.

[FTP_TRP.1.LDAP.3]

The secure LDAP communication function must require the use of the trusted path for **the initial mutual authentication of the Syslog server and the Stormshield appliance.**

Rationale: FTP_TRP.1. LDAP *is dedicated to the protection of confidentiality and integrity of requests transmitted to a LDAP server in order to identify and authenticate administrators (O.PCAOA_I&A_ADMIN).*

5.2.4.1.5 FIA_UAU.5.LDAP – Authentication mechanism for LDAP server

[FIA_UAU.5.LDAP.1]

The secure LDAP communication function must provide **the TLS protocol** to participate in the authentication of the **LDAP server**.

[FIA_UAU.5.LDAP.2]

The secure LDAP communication function must authenticate the announced identity of **the LDAP server** according to the **TLS protocol (with a X.509 certificate)**.

Rationale: FIA_UAU.5.LDAP supports FTP_TRP.1.LDAP to satisfy the objective of protection of communication with a LDAP server in order to identify and authenticate administrators (O.PCAOA_I&A_ADMIN).

5.2.4.1.6 FTP_TRP.1.Management – Trusted path with Management Center

[FTP_TRP.1.Management.1]

The secure management communication function must provide a communication channel between **Stormshield Management Center and the Stormshield appliance** that is logically distinct from the other communication channels and which guarantees the identification of its endpoints and the protection of transferred data from **modification or disclosure**.

[FTP_TRP.1.Management.2]

The secure management communication function must allow **the TSF** to initiate communication via the trusted path.

[FTP_TRP.1.Management.3]

The secure management communication function must require the use of the trusted path for:

a. the initial mutual authentication of the Management Center and the Stormshield appliance,

b. Backup operations:

Rationale: FTP_TRP.1.Management is dedicated to the protection of confidentiality and integrity of data exchanged with a Management Center while a backup operation (O.BACKUP_RESTORATION).

5.2.4.1.7 FIA_UAU.5.Management – Authentication mechanism for Management Center

[FIA_UAU.5.Management.1]

The secure management communication function must provide **the TLS protocol** to participate in the authentication of the **Management Center**.

[FIA_UAU.5.Management.2]

The secure management communication function must authenticate the announced identity of **the Management Center** according to the **TLS protocol (with a X.509 certificate)**.

Rationale: FIA_UAU.5.Management supports FTP_TRP.1.Management to satisfy the objective of protection of communication with a Management Center (O.BACKUP_RESTORATION).

5.2.4.1.8 FTP_TRP.1.Syslog – Trusted path with Syslog server

[FTP_TRP.1.Syslog.1]

The secure syslog communication function must provide a communication channel between **a Syslog server and the Stormshield appliance** that is logically distinct from the other communication channels and which guarantees the identification of its endpoints and the protection of transferred data from **modification or disclosure**.

[FTP_TRP.1.Syslog.2]

The secure syslog communication function must allow **the TSF** to initiate communication via the trusted path.

[FTP_TRP.1.Syslog.3]

The secure syslog communication function must require the use of the trusted path for **the initial mutual authentication of the Syslog server and the Stormshield appliance.**

Rationale: FTP_TRP.1.Syslog is dedicated to the protection of confidentiality and integrity of events transmitted to a Syslog server (O.PROTECT_LOGS).

5.2.4.1.9 FIA_UAU.5.Syslog – Authentication mechanism for Syslog server

[FIA_UAU.5.Syslog.1]

The secure syslog communication function must provide **the TLS protocol** to participate in the authentication of the **Syslog server**.

[FIA_UAU.5.Syslog.2]

The secure syslog communication function must authenticate the announced identity of **the Syslog server** according to the **TLS protocol (with a X.509 certificate)**.

Rationale: FIA_UAU.5.Syslog supports FTP_TRP.1.Syslog to satisfy the objective of protection of communication with a Syslog server (O.PROTECT_LOGS).

5.2.5 Cryptographic supporting security requirements

5.2.5.1 Cryptographic supporting functions

5.2.5.1.1 FCS_COP.1 – Cryptographic function

[FCS_COP.1.Key_preparation]

The cryptographic function must prepare keys according to the cryptographic algorithm **specified below** and with the cryptographic key sizes **specified below**, in compliance with the **standards set out below**.

Algorithm	*Key size*	*Ref. of the standard*	*Requirements supported*
Diffie-Hellman	2048, 3072, 4096	[DH], [IKE-MODP], [IKEv2], [TLS12], [TLS13]	FIA_UAU.5.Peer. FIA_UAU.5.Admin FIA_UAU.5.Manager FIA_UAU.5.Syslog FIA_UAU.5.LDAP
ECDH	256, 384, 512, 521	[DH], [IKE-ECP], [IKE-BEC], [IKEv2], [TLS12], [TLS13]	

[

[FCS_COP.1.Signature]

The cryptographic function must sign and verify signature according to the cryptographic algorithm **specified below** and with the cryptographic key sizes **specified below**, in compliance with the **standards set out below**.

Algorithm	*Key size*	*Ref. of the standard*	*Requirements supported*
RSA	2048, 4096	[RSA]	FIA_UAU.5.Peer (X509) FIA_UAU.5.Admin FIA_UAU.5.Manager FIA_UAU.5.Syslog FIA_UAU.5.LDAP
ECDSA	256,384,512, 521	[DSA], [ECDSA]	
ECSDSA	256	[DSA], [ECSDSA], [IPSEC DR]	

[FCS_COP.1.Hashing]

The cryptographic function must conduct one-to-one hashing according to the cryptographic algorithms **specified below** and with the cryptographic key sizes **specified below**, in compliance with the **standards set out below.**

Algorithms	*Key size*	*Ref. of the standard*	*Requirements supported*
SHA2	256, 384, 512	[SHA2]	FTP_TRP.1.Peer FIA_UAU.5.Peer FIA_UAU.5.Admin FIA_UAU.5.Manager FIA_UAU.5.Syslog FIA_UAU.5.LDAP

[FCS_COP.1.Encryption_VPN]

The cryptographic function must perform symmetrical **encryption/decryption of ESP packets** according to the cryptographic algorithms **specified below** and with the cryptographic key sizes **specified below**, in compliance with the **standards set out below**.

Algorithms	*Key size*	*Ref. of the standard*	*Requirements supported*
AES	128, 192, 256	[AES] [IPSEC DR] (modes GCM et CTR)	FTP_TRP.1.Peer, FDP_UCT.1

[FCS_COP.1.Integrity_VPN]

The cryptographic function must check the integrity **of ESP paquets** according to the cryptographic algorithm **specified below** and with the cryptographic key sizes **specified below**, in compliance with the **standards set out below**.

Algorithm	*Key size*	*Ref. of the standard*	*Requirements supported*
HMAC-SHA2	256, 384	[HMAC], [SHA2]	FDP_UIT.1

[FCS_COP.1.Encryption_sessions]

The cryptographic function must perform symmetrical **encryption/decryption of administration sessions** according to the cryptographic algorithm **specified below** and with the cryptographic key sizes **specified below**, in compliance with the **standards set out below**.

Algorithm	*Key size*	*Ref. of the standard*	*Requirements supported*
AES	128, 256	[AES]	FPT_ITT.1

[FCS_COP.1.Integrity_sessions]

The cryptographic function must check the integrity **of administration sessions** according to the cryptographic algorithm **specified below** and with the cryptographic key sizes **specified below**, in compliance with the **standards set out below**.

Algorithm	*Key size*	*Ref. of the standard*	*Requirements supported*
HMAC-SHA2	256, 384	[HMAC], [SHA2]	FPT_ITT.1

Rationale: FCS_COP.1 satisfies the objective O.CRYPTO by specifying the cryptographic mechanisms that comply with the RGS and supports all requirements specified in the right column for the satisfaction of their respective security objectives.

5.2.5.1.2 FCS_CKM.1 - Cryptographic key generation

[FCS_CKM.1]

The cryptographic key generation function shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **specified below** and with the cryptographic key sizes **specified below**, in compliance with the **standards set out below**.

Algorithm	*Key size*	*Ref. of the standard*	*Requirements supported*
Diffie-Hellman	2048, 3072, 4096	[DH], [IKE-MODP], [IKEv2], [TLS12], [TLS13]	FIA_UAU.5.Admin FIA_UAU.5.LDAP FIA_UAU.5.Peer FIA_UAU.5.Manager FIA_UAU.5.Syslog FCS_TLSC_EXT.1
ECDH	256, 384, 512, 521	[DH], [IKE-ECP], [IKE-BEC], [IKEv2], [TLS12], [TLS13]	FIA_UAU.5.Admin FIA_UAU.5.LDAP FIA_UAU.5.Peer FIA_UAU.5.Manager FIA_UAU.5.Syslog FCS_TLSC_EXT.1
RSA	2048, 4096	[RSA]	FIA_X509_EXT.4
ECDSA	256,384,512, 521	[DSA], [ECDSA]	FIA_X509_EXT.4
HMAC-SHA2	256, 384, 512	[HMAC], [SHA2]	FTP_TRP.1.Peer FIA_UAU.5.Peer FIA_UAU.5.Admin FIA_UAU.5.LDAP FIA_UAU.5.Manager FIA_UAU.5.Syslog FDP_UIT.1 FCS_TLSC_EXT.1
AES	128, 192, 256	[AES] [IPSEC DR] (modes GCM et CTR)	FTP_TRP.1.Peer FDP_UCT.1 FIA_UAU.5.Admin FIA_UAU.5.LDAP FIA_UAU.5.Manager FIA_UAU.5.Syslog FCS_TLSC_EXT.1

Rationale: FCS_CKM.1 satisfies the objective O.CRYPTO by specifying the cryptographic mechanisms that comply with the RGS and supports all requirements specified in the right column for the satisfaction of their respective security objectives.

5.2.5.1.3 FCS_CKM.4 - Cryptographic key destruction

[FCS_CKM.4]

The cryptographic key destruction function shall destroy cryptographic keys by overwriting them with zeros.

Rationale: FCS_CKM.4 satisfies the objective O.CRYPTO by specifying the cryptographic methods that comply with the RGS and supports all requirements specified in the right column for the satisfaction of their respective security objectives.

5.3 Security assurance requirements for the TOE

This section presents the selected package of assurance requirements.

The level of assurance that the TOE aims for is an augmented EAL4 level for the components ALC_FLR.3 associated with expertise in the implementation of the cryptography described in [QUALIF-STD].

The table below provides details of the coverage of assurance requirement dependencies.

Components		Comment
ADV_ARC.1	Security architecture description	EAL4
ADV_FSP.4	Complete functional specification	EAL4
ADV_IMP.1	Implementation representation of the TSF	EAL4
ADV_TDS.3	Basic modular design	EAL4
AGD_OPE.1	Operational user guidance	EAL4
AGD_PRE.1	Preparative procedures	EAL4
ALC_CMC.4	Production support, acceptance procedures and automation	EAL4
ALC_CMS.4	Problem tracking CM coverage	EAL4
ALC_DEL.1	Delivery procedures	EAL4
ALC_DVS.1	Identification of security measures	EAL4
ALC_FLR.3	Systematic flaw remediation	+
ALC_LCD.1	Developer defined life-cycle model	EAL4
ALC_TAT.1	Well-defined development tools	EAL4
ASE_CCL.1	Conformance claims	EAL4
ASE_ECD.1	Extended components definition	EAL4
ASE_INT.1	ST introduction	EAL4
ASE_OBJ.2	Security objectives	EAL4
ASE_REQ.2	Security requirements	EAL4
ASE_SPD.1	Security problem definition	EAL4
ASE_TSS.1	TOE summary specification	EAL4
ATE_COV.2	Analysis of coverage	EAL4
ATE_DPT.1	Testing: basic design	EAL4
ATE_FUN.1	Functional testing	EAL4
ATE_IND.2	Independent testing – sample	EAL4
AVA_VAN.3	Focused vulnerability analysis	EAL4

5.4 Security requirements rationale

5.4.1 Satisfaction of security objectives

The satisfaction of security objectives is expressed in the “Rationale” sections that come with the description of each security requirement. The link between requirements and security objectives is summarized below.

“S”: The requirement supports the objective, “X”: The requirement enforces the objective

	O.PCFI_FILTERING	O.PCFI_APPLICATION_CONTEXT	O.PCFI_ENCRYPTION	O.LAA_PCFI	O.CRYPTO	O.IPS_ATTACK_DETECTION	O.IPS_RFC_COMPLIANCE	O.LAA_IPS	O.PCAOA	O.PCAOA_I&A_ADMIN	O.LAA_PCAOA	O.BACKUP_RESTORATION	O.RESIST_AUTH_ADMIN	O.PROTECT_LOGS	O.PROTECT_ADMIN_SESSIONS
FDP_IFC.2	S														
FDP_IFF.1.Filtering	X	X													
FDP_IFC.1			S												
FDP_UCT.1			X												
FDP_UIT.1			X												
FDP_IFF.1.Encryption			S												
FTP_TRP.1.Peer			X												
FIA_UAU.5.Peer			S												
FPT_TDC.1			S												
FIA_X509_EXT.4			S												
FCS_HTTPS_EXT.1			S												
FCS_TLSC_EXT.1			S												
FAU_GEN.1				X				X			X				
FAU_GEN.2											X				
FAU_SAR.1				X				X			X				
FAU_STG.3														X	
FAU_SAA.4						X	X								
FAU_ARP.1.IPS						S	S	X							
FMT_SMF.1									S		S	S			S
FMT_SMR.1									S	S					
FDP_ACC.2									S						
FMT_MOF.1									X						
FMT_MTD.1									X						
FMT_MTD.BRS												X			
FPT_ITT.1															X
FTP_TRP.1.Admin										X					S
FIA_UAU.5.Admin										S			X		
FTP_TRP.1.LDAP										S					
FIA_UAU.5.LDAP										S					
FTP_TRP.1.Management												S			
FIA_UAU.5.Management												S			
FTP_TRP.1.Syslog														S	
FIA_UAU.5.Syslog														S	
FCS_COP.1.Key_preparation			X		X					X			S		S

FCS_COP.1.Signature			X		X					X			X		S
FCS_COP.1.Hashing			X		X										
FCS_COP.1.Encryption_VPN			X		X										
FCS_COP.1.Integrity_VPN			X		X										
FCS_COP.1.Encryption_sessions					X					X					X
FCS_COP.1.Integrity_sessions					X					X			S		X
FCS_CKM.1			S		X					S			S		S
FCS_CKM.4			S		X					S			S		S

5.4.2 Mutual support and non contradiction

All dependencies have been satisfied or the inability to satisfy them has been justified. Security requirements therefore make up a set of dependencies that mutually support each other and do not present any contradiction.

5.4.3 Satisfaction of the dependencies of SFRs

The table below summarizes the dependencies of security requirement components and justifies how they have been satisfied or why they have not been satisfied.

Component	*Dependencies*	*Satisfaction*
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1.Filtering
FDP_IFF.1.Filtering	FDP_IFC.1	FDP_IFC.2
	FMT_MSA.3	The security attributes of IP packets are deduced from the contents of IP and transport headers. Under these conditions, the concept of the “restrictive value of attributes” is not clear and in any case these attributes are not under the control of the TSF. The dependency is therefore not applicable.
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1.Encryption
FDP_UCT.1	FTP_ITC.1 | FTP_TRP.1	FTP_TRP.1.Peer
	FDP_ACC.1 | FDP_IFC.1	FDP_IFC.1
FDP_UIT.1	FTP_ITC.1 | FTP_TRP.1	FTP_TRP.1.Peer
	FDP_ACC.1 | FDP_IFC.1	FDP_IFC.1
FDP_IFF.1.Encryption	FDP_IFC.1	FDP_IFC.1
	FMT_MSA.3	The security attributes of IP packets are deduced from the contents of IP and transport headers. Under these conditions, the concept of the “restrictive value of attributes” is not clear and in any case these attributes are not under the control of the TSF. The dependency is therefore not applicable.
FTP_TRP.1.Peer	None	
FIA_UAU.5.Peer	None	
FPT_TDC.1	None	
FIA_X509_EXT.4	FCS_HTTPS_EXT.1 FCS_TLSC_EXT.1 FCS_CKM.1	Yes
FCS_HTTPS_EXT.1	FCS_TLSC_EXT.1	Yes
FCS_TLSC_EXT.1	None	
FAU_GEN.1	FPT_STM.1	This dependency is satisfied by the IT environment (see OE.TIMESTAMPS).
FAU_GEN.2	FAU_GEN.1	Yes
	FIA_UID.1	The administrator is unable to perform any sort of administrative operation without being authenticated. The authentication function is therefore the only operation that can be carried out during a connection to the administration server. The dependency is therefore not applicable.

Component	*Dependencies*	*Satisfaction*
FAU_SAR.1	FAU_GEN.1	Yes
FAU_STG.3	FAU_STG.1	Audit logs can only be deleted or modified with the “admin” account and only via the local console. There is no administration function to perform these operations. The dependency is therefore not applicable.
FAU_SAA.4	None	
FAU_ARP.1.IPS	FAU_SAA.1	FAU_SAA.4
FMT_SMR.1	FIA_UID.1	The administrator is unable to perform any sort of administrative operation without being authenticated. The authentication function is therefore the only operation that can be carried out during a connection to the administration server. The dependency is therefore not applicable.
FDP_ACC.2	FDP_ACF.1	All access to administration operations are controlled by a set of administration privileges. These privileges are grouped by functional category. It is therefore impossible to allow or deny access to a particular element in a functional category. The dependency is therefore not applicable.
FMT_MOF.1	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_MTD.1	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_SMF.1	None	
FMT_MTD.BRS	FMT_MTD.1	Yes
	FMT_SMF.1	Yes
FPT_ITT.1	None	
FTP_TRP.1.Admin	None	
FIA_UAU.5.Admin	None	
FTP_TRP.1.LDAP	None	
FIA_UAU.5.LDAP	None	
FTP_TRP.1.Management	None	
FIA_UAU.5.Management	None	
FTP_TRP.1.Syslog	None	
FIA_UAU.5.Sylog	None	
FCS_COP.1.Key_preparation	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Not applicable: the operation is a key generation method.
	FCS_CKM.4	Yes
FCS_COP.1.Signature	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Not applicable as it is outside the scope of the TOE. The administrator downloads certificates on the Stormshield appliance.
	FCS_CKM.4	Yes
FCS_COP.1.Hashing	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Not applicable as there is no secret used
	FCS_CKM.4	Not applicable as there is no secret used
FCS_COP.1.Encryption_VPN	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Satisfied by FCS_CKM.1
	FCS_CKM.4	Yes
FCS_COP.1.Integrity_VPN	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Satisfied by FCS_CKM.1
	FCS_CKM.4	Yes

Component	*Dependencies*	*Satisfaction*
FCS_COP.1.Encryption_sessions	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Satisfied by FCS_CKM.1
	FCS_CKM.4	Yes
FCS_COP.1.Integrity_sessions	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Satisfied by FCS_CKM.1
	FCS_CKM.4	Yes
FCS_CKM.1	FCS_CKM.2 | FCS_COP.1 | FCS_CKM.4	Satisfied by FCS_CKM.4|
FCS_CKM.4	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Satisfied by FCS_CKM.1

5.4.4 Satisfaction of SAR dependencies

The assurance level of the evaluation that is the focus of this security target is a standard augmented qualification of the component ALC_FLR.3.

All dependencies are satisfied.

6 EXTENDED COMPONENTS DEFINITION

This Security Target defines security functional requirements that are not included in CC Part 2.

Those new requirements implement:

- Backup and restoration function (FMT_MTD.BRS),
- Certificate enrollment (FIA_X509_EXT.4, FCS_HTTPS_EXT.1 and FCS_TLSC_EXT.1).

They are defined in section 11- Appendix D – Extended security Requirement.

7 TOE SUMMARY SPECIFICATIONS

The aim of this section is to provide a high-level definition of IT security functions that are supposed to satisfy security functional requirements, and of security assurance measures taken to satisfy security assurance requirements.

7.1 IT security functions

The presentation of IT security functions follows the plan taken for the description of the TOE's security functional requirements.

7.1.1 Filter function

ASQ technology includes a dynamic packet filter engine (*stateful inspection*) with rule optimization allowing the safe and quick application of the **filter policy**. The implementation of the filter function is based on the comparison of the attributes of each IP packet received against the criteria of each rule in the active filter slot. Filtering applies to all packets without any exceptions. The criteria of filter rules are:

- The receiving or destination interface of IP packets covered by the rule;
- The machine(s) at the source of the information flows covered by the rule;
- The IP protocol(s), DSCP field, TCP/UDP/SCTP services or types of ICMP messages of information flows covered by the rule;
- The destination machine(s) of information flows covered by the rule;

The attributes of IP packets that are compared against the first four criteria above are obviously taken from Ethernet, IP, ICMP, UDP, TCP or SCTP frame headers.

Each filter rule may specify a control action and logging action. The latter is described in §6.1.4. There are five possible values for the control action:

- 'pass': the packet is accepted and not compared against the rules that follow;
- 'block': the packet is destroyed without the sender's knowledge and will not be compared against the rules that follow in the filter policy;
- 'reinitialize': the packet is destroyed and:
  - For TCP: a TCP RST signal will be sent to the sender;
  - For UDP: an ICMP unreachable signal will be sent to the sender;
  - For SCTP: no signal sent to the sender.
- none: the packet is compared against the rules that follow (used only for specifying a logging action).
- 'delegate': the packet is compared against filter rules in the local slot (used for getting out of the evaluation of the global filter policy in order to allow delegating a subset of it to a local administrator via the local filter slot). This action is only available for rules in the global slot.

If no filter rule applies to the packet, or if the only ones that do have specified 'none' for the control action, the packet is destroyed without the sender's knowledge and will not be compared against the rules that follow in the filter policy.

It is important to note that, strictly speaking, for a set of IP packets linked to the same exchange at the transport layer (TCP connection, UDP or ICMP pseudo-connection, SCTP association), the Stormshield appliance only compares the initial packet from the exchange against rules of the current filter slot. Upon receiving any IP packet, prior to the application of rules from the current filter slot, the packet will be compared against currently established connections / pseudo-connections / associations. If the attributes and parameters of the packet correspond to the criteria and status of one of these connections / **pseudo-connections / associations**, it will be allowed to pass through without being subject to the filter rules. This mechanism allows in particular managing two-way exchanges (especially TCP connections), four-way exchanges and multihoming (especially SCTP associations) without having to define a filter rule in both directions on the firewall.

The firewall generates implicit filter rules together with the configuration of other security functions. This refers to the rules corresponding to: remote firewall administration and the setup of VPNs. At the same time, dynamic filter rules are also generated for protocols requiring child connections.

The filter policy is the result of a sequence of implicit rules, filter rules contained in the global filter policy (if there is one) then filter rules contained in the local filter policy.

Do note that at any moment while the Stormshield appliance is running, there is always an active **filter policy**.

Rationale: the filter function satisfies FDP_IFC.2 and FDP_IFF.1.Filtering.

7.1.2 Encryption function

The encryption function on the Stormshield appliance implements IPSec ESP to provide authentication and encryption services for datagrams exchanged with a VPN peer (or another Stormshield appliance) with equivalent features.

The authentication algorithms supported by the Stormshield appliance are: HMAC-SHA2 (256, 384, 512 bits).

The encryption algorithms supported by the Stormshield appliance are: AES (128, 192 or 256 bits)

The Stormshield appliance implements ESP in tunnel mode. This means that the encryption function may not necessarily be implemented on end-to-end traffic, but only on a portion of the network that supports the information flows, physically marked off by VPN peers, typically the uncontrolled network. On this portion, the IP datagrams that need to be protected are fully encrypted, signed and encapsulated in ESP datagrams whose source and destination IP addresses are the ones used for VPN peers. Therefore, the IP addresses of real traffic endpoint hosts will be inaccessible to hackers listening on the uncontrolled network. VPN peers are called tunnel endpoints, as opposed to real traffic endpoint hosts located “behind” VPN peers from the viewpoint of the uncontrolled network, and which are called traffic endpoints.

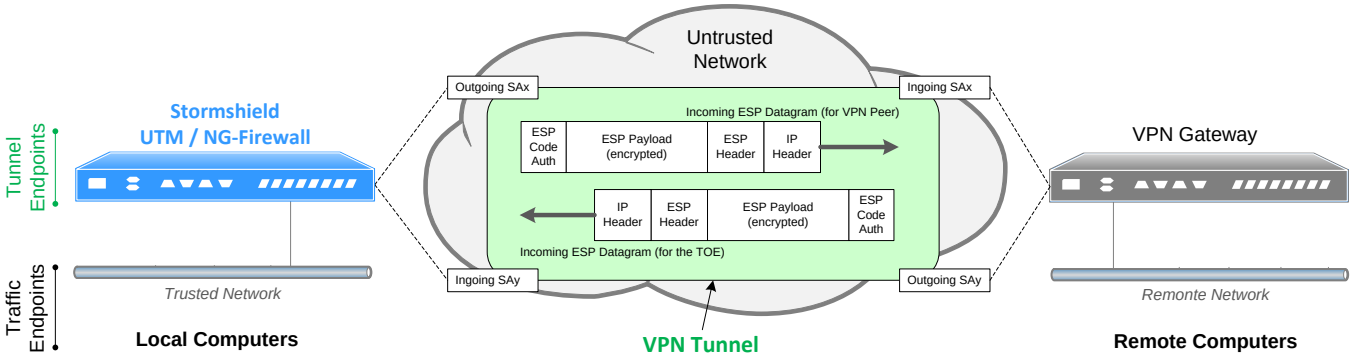


Illustration 6: ESP in tunnel mode.

In ESP, each datagram exchanged between two given VPN peers is attached to a one-way connection that implements security services, called the Security Association or SA. Each ESP datagram possesses a Security Policy Identifier or SPI which identifies the IPSec SA to which it is attached.

An IPSec SA specifies the encryption and authentication algorithms to be applied to the datagrams that it covers, as well as the associated secret keys. From the point of view of a VPN peer, an IPSec SA may either be incoming our outgoing.

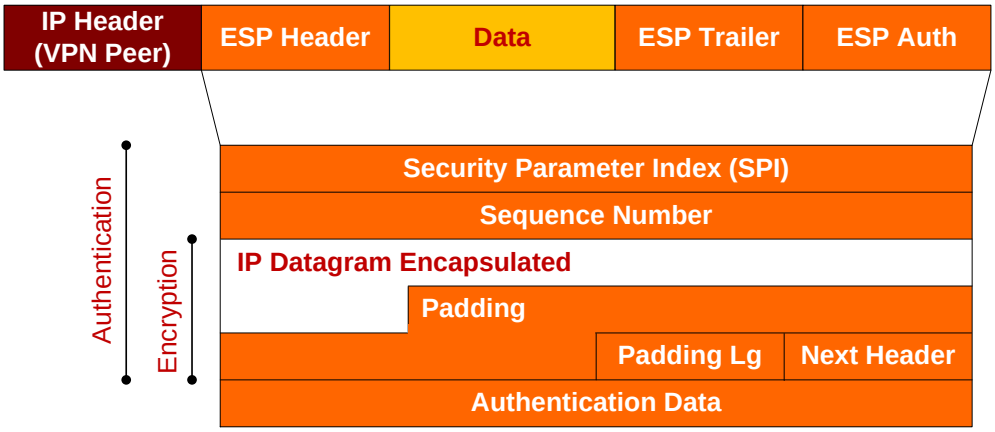


Illustration 7: Contents of an ESP datagram

For a given two-way exchange (e.g.: a TCP connection), VPN peers set up a pair of IPSec SAs (one for each direction), each IPSec SA being outgoing for one peer and incoming for the other. The setup of IPSec SA pairs is the focus of a specific functional security set (cf. IKE phase2: setup of the IPSEC SA at §).

An IPSec SA has a configurable lifetime that needs to be renegotiated after it expires. The VPN peer can also push for the re-negotiation of the IPSec SA by applying other criteria (e.g.: volume of data exchanged).

At any given moment, the Stormshield appliance is able to manage a multitude of IPSec SA pairs. It is relatively easy to find the incoming IPSec SA associated with an incoming ESP datagram (thanks to the security index), but for each outgoing IP datagram IP, the selection of the outgoing IPSec SA requires the comparison of the datagram's attributes against the criteria of each rule in the active encryption slot. The criteria of encryption rules[5] are:

- The machine(s) at the source of the information flows covered by the rule;
- The IP protocol(s);
- The host(s) at the destination of the information flows covered by the rule.

Unlike the encryption function, if the outgoing IP datagram does not match any rule, it will continue checking against the other rules in the stack. It will then be subject to the filter function. Another difference: at any given moment, it is possible to not have any active encryption slot.

Every encryption rule is usually associated with an IPSec SA pair. If the outgoing IP datagram matches an encryption rule that has a valid outgoing IPSec SA, the processes of this IPSec SA will be applied to the datagram. Otherwise, the outgoing IPSec SA will be negotiated (or re-negotiated). If the negotiation fails, the packet will be destroyed.

The authenticity of incoming ESP datagrams is monitored before they are decrypted. Once they are decapsulated, the attributes of the IP packet obtained will also be checked to ensure that they do indeed comply with the criteria of the encryption rule associated with the IPSec SA.

It is important to note that we referred to IP or ESP "datagrams" throughout this section. Indeed, in fragmentation, outgoing IP packets or incoming ESP packets are reassembled before the application of the encryption function.

[5] Encryption rules can be considered to correspond to *Security Policy Database* entries in RFC 2401 [IPSec], apart from the fact that SPD, such as it is defined in the RFC, thoroughly covers encryption and filter rules.

Application Note: DES (56 bits) and HMAC-MD5 (128 bits) algorithms are also supported but are excluded from the usage mode subject to evaluation. Likewise CAST and Blowfish algorithms can be configured with key sizes lower than 128 bits, but this deviates from the usage mode subject to evaluation.

Rationale: the encryption function satisfies FDP_IFC.1, FDP_UCT.1, FDP_UIT.1 and FDP_IFF.1.Encryption.

The use of HMAC-SHA2 algorithm for the IPSec SA's confidentiality services satisfies the section FCS_COP.1.Integrity_VPN which supports FDP_UIT.1.

The use of AES algorithm for the IPSec SA's confidentiality services satisfies the section FCS_COP.1.Encryption_VPN which supports FDP_UCT.1.

The random generation of keys satisfies FCS_CKM.1 and their destruction satisfies FCS_CKM.4.

7.1.3 SA establishment function

7.1.3.1 CHILD_SA: establishment of IPSec SAs

The establishment of an IPSec SA between two VPN peers requires a phase to negotiate key parameters and establishment in order to ensure that both tunnel endpoints consistently apply the encryption rule associated with the IPSec SA. The negotiation of IPSec SAs is issued from CHILD_SA of the IKE protocol [IKEv2].

The authentication algorithms that can be negotiated are:

- SHA2 (256, 384 and 512 bits),
- ECDSA with the curve SECP256R1
- ECDSA with the curve Brainpoolp256r1
- ECSDSA with the curve SECP256r1
- ECSDSA with the curve Brainpoolp256r1

The key exchange algorithms that can be negotiated are:

- Diffie-Hellman (DH) with regular groups [IKE-MODP]:
  - group 14 - MODP 2048 bits,
  - group 15 - MODP 3072 bits,
  - group 16 - MODP 4096 bits,
  - group 17 - MODP 6144 bits,
  - group 18 - MODP 8192 bits,
- ECDH with NIST Elliptic Curve Groups [IKE-ECP]:
  - group 19 – ECP 256 bits,
  - group 20 – ECP 384 bits,
  - group 21 – ECP 521 bits,
- ECDH with Brainpool Elliptic Curve Groups [IKE-BEC]:
  - group 28 – Brainpool 256 bits,
  - group 29 – Brainpool 384 bits,
  - group 30 – Brainpool 512 bits,

The encryption algorithms that can be negotiated are AES (128, 192 or 256 bits.

As the responder, the Stormshield appliance selects a response that is at least as strict as its local proposals.

A Child SA expires after a configurable lifetime.

Application Note: the administrator may configure other policies, but they are excluded from the usage mode subject to evaluation.

Rationale: proposal-response messages satisfy FPT_TDC.1 regarding IPSec SAs. The IKE SA constitutes a trusted path (cf. IKE phase1: establishment of IKE SAs and mutual authentication at §SA establishment function) whose use, through CHILD_SA, for the negotiation of IPSec SAs satisfies FTP_TRP.1.Peer.3.b.

The use of the Diffie-Hellman algorithm satisfies FCS_COP.1.Key_preparation regarding the section of this requirement which supports FIA_UAU.5.Peer.

The SHA2 algorithm is used, in compliance with RFC 2409, to generate the secret keys of the IPSec SA and authentication codes, which satisfies the section FCS_COP.1.Hashing which supports FTP_TRP.1.Peer. This algorithm is also used for the integrity services of the IKE SA (cf. §SA establishment function), which satisfies the section FCS_COP.1.Integrity_Sessions which supports FTP_TRP.1.Peer.1.

The AES algorithm is used for the confidentiality services of the IKE SA (cf. §SA establishment function), which satisfies the section FCS_COP.1.Encryption_Sessions which supports FTP_TRP.1.Peer.1.

The random generation of keys satisfies FCS_CKM.1 and their destruction satisfies FCS_CKM.4.

7.1.3.2 IKE_SA: establishment of IKE SAs and mutual authentication

The establishment of an IKE SA between two VPN peers requires the mutual authentication of VPN peers. This is followed by the phase in which the parameters and the establishment of secret keys for authentication, encryption and derivation of the IKE SA are negotiated, in order to sure that both tunnel endpoints consistently apply the communication protection rule.

A IKE SA expires after a configurable lifetime.

Application Note: RSA and Diffie-Hellman algorithms with keys strictly lower than 2048 bits is also supported but excluded from the usage mode subject to evaluation.

Rationale: the trusted path specified by the component FTP_TRP.1.Peer is implemented by IKE_SA, which satisfies the element FTP_TRP.1.Peer.2. Mutual authentication, which guarantees the identification of endpoints (element FTP_TRP.1.Peer.1), is established at the end of the last pass in each mode. The confidentiality and integrity services (element FTP_TRP.1.Peer.1) are effective after the fifth message in main mode. The use of the trusted path for the initial mutual authentication of VPN peers satisfies FTP_TRP.1.Peer.3.a.

Both authentication mechanisms are those specified by FIA_UAU.5.Peer.

Proposal-response messages satisfy FPT_TDC.1 regarding IKE SAs.

The use of the Diffie-Hellman algorithm satisfies FCS_COP.1.Key_preparation regarding the section of this requirement which supports FIA_UAU.5.Peer.

In X509 mode:

- *the private key is either imported (and thus reliable according OE.CRYPTO_EXT) or generated by the TOE and enrolled through FIA_X509_EXT.4, FCS_HTTPS_EXT.1 and FCS_TLSC_EXT.1.*
- *the use of the RSA, ECDSA or ECSDSA algorithms satisfies FCS_COP.1.Signature.*

The SHA2 algorithm is used, in compliance with RFC 2409, to generate the secret keys and authentication codes, which satisfies the section FCS_COP.1.Hashing which supports FIA_UAU.5.Peer. This algorithm is also used for the integrity services of the IKE SA, which satisfies the section FCS_COP.1.Integrity_Sessions which supports FTP_TRP.1.Peer.1.

The AES algorithm is used for the confidentiality services of the IKE SA, which satisfies the section FCS_COP.1.Encryption_Sessions which supports FTP_TRP.1.Peer.1.

Mutual authentication satisfies FCS_COP.1.Signature. The destruction of negotiated keys satisfies FCS_CKM.4.

7.1.4 Log and audit function

7.1.4.1 Log function

The Stormshield appliance – depending on the model – may or may not store audit events locally. Where local storage is not possible, the Stormshield appliance will manage a certain number log files meant for collecting events detected by the log function. The files involved in security events are:

- Filter: events relating to the application of the filter function;
- VPN: events relating to the establishment of SAs;
- Alarms: events relating to the application of the intrusion prevention function;
- Administration: events relating to the authentication of administrators and security administration operations;
- System: startup/shutdown of the log function. More generally: this is the log that will record events relating directly to the system: startup/shutdown of the appliance, system errors, etc. shutting down and starting the log function correspond to shutting down and starting the daemons that generate logs.

All log files share a global storage space. The administrator who has '*+M' privileges may specify the maximum percentage that each of the log files can occupy in this total space. When the maximum limit is reached, the most recent logs will erase the oldest logs.

When logs are centralized via Syslog, the server is duly authenticated and data transmitted is protected in confidentiality and integrity.

Rationale: the log function satisfies FAU_GEN.1 and FAU_GEN.2. The detailed justification of the satisfaction of each requirement placed on audit information saved in each type of log will be provided during the evaluation. Limits on the size of log files and the associated actions satisfy the requirement FAU_STG.3 for these files. Protection of Syslog communications is ensured by FTP_TRP.1.Syslog and FIA_UAU.5.Syslog.

Mutual authentication satisfies FCS_COP.1.Signature. The destruction of negotiated keys satisfies FCS_CKM.4.

The encryption of Syslog *sessions satisfies FCS_COP.1.Encryption_sessions. Their integrity control satisfies FCS_COP.1.Integrity_sessions.*

7.1.4.2 Audit function

The audit function allows the auditor to display the events stored in each log file by:

Selecting from periods predefined in relation to the current date ('today', 'this week, etc.) or defined manually;

Sorting (ascending/descending order) by the value of each field in recorded security events;

Rationale: the audit function satisfies FMT_SMF.1.c, FAU_SAR.1.

7.1.5 Intrusion prevention function

ASQ technology includes an intrusion prevention system (IPS) allowing the detection of attacks:

Without context, meaning that they use only one IP packet;

With connection context, meaning that they involve the analysis of several packets associated with the same TCP connection / UDP or ICMP pseudo-connection;

or with a global context, meaning that they require the contexts of several TCP connections / UDP or ICMP pseudo-connections to be cross-referenced.

A plugin-based technology allows carrying out checks at the application level with the aim of implementing RFC compliance, adhesion to best practices and the prevention of known attacks on application servers.

Details of potential attacks detected are provided in Appendix B, §8. For each of these attacks, the administrator with 'As+M' privileges may define whether incriminated packets have to be sent or destroyed and whether there is a need to generate a security event possessing a level of alarm automatically saved in the 'Alarms' log.

Rationale: the intrusion prevention system satisfies the requirements of FAU_SAA.4. Appendix B, §8 associates each potential attack with six types listed in FAU_SAA.4.1. The indication of a potential attack (FAU_SAA.4.3) may be represented by an action on the incriminated packet (which satisfies FAU_ARP.IPS.1.a) and/or the generation of an alarm (which satisfies FAU_ARP.IPS.1.b).

7.1.6 Function controlling access to administration operations

In order to allow several persons to access the Stormshield appliance, the super-administrator may assign reading or writing privileges to users defined in an external LDAP over TLSbase, which makes them administrators. The privileges are defined in a local database (the LDAP Server manages only users and groups).All administration privileges are listed in Appendix A §7

The particular privilege BASE (B) serves as an explicit administrator role. Users who do not have the 'B' privilege are not considered administrators and cannot open administration sessions.

The MODIFY (M) privilege complements all other privileges assigned to an administrator in order to allow him to read and modify security data.

There is a second data modification privilege reserved for Monitoring (MW). This privilege allows administrators to perform operations without interfering with an administrator who has the M privilege and is logged on to the Stormshield appliance at the same time.

For each basic security administration operation, the necessary privileges are defined in detail (details are given during the examination of the high-level design). All security administration operations performed by administrators are therefore covered by the access control policy that these privileges implement.

The account whose login is 'admin' is always defined by default and is not managed in the LDAP base. This account is called the "super-administrator". It possesses all privileges as well as a special ADMIN (A) privileges, and is the only one able to perform certain operations (creating a user and assigning administration privileges to him, restoring the configuration, etc.)

Application Note: Please be reminded that in the usage mode that is the focus of the evaluation, the super-administrator is not supposed to log on to the Stormshield appliance during production except for the promotion of a user to administrator.

Rationale: the privilege system described above satisfies the requirements of FMT_SMF.1.a, FMT_MTD.1 and FMT_MOF.1. The fact that all security administration operations are subject to access control satisfies FDP_ACC.2. The definition of administrators and super-administrator given above satisfies FMT_SMR.1.1. The association of the 'admin' account with the super-administrator satisfies FMT_SMR.1.2.a. The need to assign the 'B' privilege explicitly to administrators satisfies FMT_SMR.1.2.b.

Mutual authentication satisfies FCS_COP.1.Signature. The destruction of negotiated keys satisfies FCS_CKM.4.

The encryption of administration *sessions satisfies FCS_COP.1.Encryption_sessions. Their integrity control satisfies FCS_COP.1.Integrity_sessions.*

7.1.7 Backup and restoration function

The administrator with the 'Ma' privilege can back up in a file on the administration workstation either the full configuration or a sub-set. Such a backup can also be triggered from a Stormshield Management Center.

Sub-sets may be one of the following examples:

- The network configuration of the Stormshield appliance (addresses of the Firewall, routers, etc); ;
- Objects (hosts, networks, services and each group);

- The filter rules.

The backup file is protected in confidentiality and integrity when transmitted over the network.

Restoring the configuration from a backup requires modification (M) privileges in addition to maintenance (Ma) privileges.

The backup file may also be secured by encryption. In this case, the restoration of the backup requires the restitution of the encryption key.

Rationale: the backup and restoration function satisfies FMT_SMF.1.d and FMT_MTD.BRS. Protection of communications with Management Center is ensured by FTP_TRP.1.Management and FIA_UAU.5.Management.

Mutual authentication satisfies FCS_COP.1.Signature. The destruction of negotiated keys satisfies FCS_CKM.4.

The encryption of backup sessions satisfies FCS_COP.1.Encryption_sessions. Their integrity control satisfies FCS_COP.1.Integrity_sessions.

7.1.8 Administration session protection function

7.1.8.1 Encryption and authentication of administration sessions

Sessions set up between the administration tool (Web Manager) and the Stormshield appliance are encrypted with the AES 128 to 256 bit algorithm. The confidentiality of their contents is protected.

The integrity of the contents of administration sessions is monitored with the help of the HMAC-SHA2 algorithm, with a key length of 256 or 384 bits.

The authentication and encryption keys of remote administration sessions are derived from the session key set up during the establishment of a TLS channel, whether it is with or without mutual authentication by X.509 certificate (Web Manager).

Note - the exact list of TLS cypher suites available is:

- TLS_AES_128_GCM_SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- TLS_CHACHA20_POLY1305_SHA256
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- TLS_AES_256_GCM_SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-CHACHA20-POLY1305-SHA256

Rationale: the AES 128/256 bit encryption of administration sessions satisfies FPT_ITT.1 and FCS_COP.1.Encryption_sessions. The integrity control by HMAC-SHA2 256/384 bits satisfies FPT_ITT.1 and FCS_COP.1.Integrity_sessions. The need for the administrator to authenticate by login / password through the TLS protocol, or to authenticate by X.509 certificate through the TLS protocol satisfies FMT_SMF.1.b, FTP_TRP.1.Admin.3.b.

Mutual authentication satisfies FCS_COP.1.Signature. The destruction of negotiated keys satisfies FCS_CKM.4.

7.1.8.2 Authentication of administrators and preparation of the encryption key by the TLS protocol

The TLS protocol [TLS] allows a “client” (in our case: administration tools such as Web Manager) to authenticate a “server” (the Stormshield appliance) and to authenticate (optional) with the same server. In both cases, the TLS protocol also allows negotiating a session key used for protecting later exchanges.

When the profile of each administrator is being created, the authentication method that will be used can be specified (login / password or X.509 certificate)

Application Note: further detail is given in RFC 2246 [TLS]. In Web Manager's use of the TLS protocol, the connection is set up by the web browser on the administration workstation which is out of scope. Likewise the TLS protocol itself is outside the scope of this evaluation.

Rationale: the trusted path between the administrator and the Stormshield appliance specified par FTP_TRP.1.Admin is implemented by the TLS protocol, as specified by FIA_UAU.5.Admin. In this protocol, the authentication initiative returns to the administrator, which satisfies FTP_TRP.1.Admin.2. Mutual authentication, which guarantees the identification of endpoints (element FTP_TRP.1.Admin.1), is established in the TLS protocol (when X.509 certificates are used) or after the TLS connection has been set up (if a login/password has been used). The use of the trusted path for the initial mutual authentication of the administrator and the Stormshield appliance satisfies FTP_TRP.1.Admin.3.a and FMT_SMF.1.b

The use of the Diffie-Hellman algorithm with ephemeral keys with 2048-bit entropy satisfies FCS_COP.1.Key_preparation regarding the section of this requirement which supports FIA_UAU.5.Admin.

7.1.9 Certificate enrollment

X.509 certificates and CA have expiration dates. A CA could also decide to revoke a certificate before due date for external reasons. This is why certificate management always include revocation and certificate renewal methods. EST is such management protocol, based on HTTPS.

The EST implementation supports the following operations:

- CA public key distribution.
- Certificate enrollment.
- Certificate renewal.

On initial enrollment, the TOE supports HTTP basic auth: credentials must be supplied to the EST server.

On renewal, The TOE supports Mutual TLS auth (along additional HTTP basic auth if necessary), however we restrict the TLS client certificate to the one to be renewed.

Before any EST operation, in order to be able to communicate with the server, one has to install the TLS CA as a trust anchor. This is done by obtaining the certificate out-of-bounds. It is the most sensitive operation as it establishes trust.

After this step:

- Client asks for the EST CA (the one signing the enrolled certificates) through the "cacerts" operation.
- Client prepares a CSR and sends it as POST on the /simpleenroll URL. The request is authenticated via HTTP Basic, whose credentials are known out-of-bounds.
- In case of a renewal, the client sends the same kind of CSR but on the /simplereenroll URL. There's usually no need for HTTP Basic credentials at this point since the previously enrolled certificate is used as client certificate during the TLS handshake.

Rational: the X509 enrollment satisfies FIA_X509_EXT.4, FCS_HTTPS_EXT.1 and FCS_TLSC_EXT.1

The random generation of keys satisfies FCS_CKM.1 and their destruction satisfies FCS_CKM.4.

Mutual authentication with EST Server satisfies FCS_COP.1.Signature.

The encryption of enrollment sessions satisfies FCS_COP.1.Encryption_sessions. Their integrity control satisfies FCS_COP.1.Integrity_sessions.

7.1.10 Cryptographic supporting functions

The cryptographic function is presented with functional security sub-sets that it supports, as well as the justification of the various basic requirements specified by FCS_COP.1.

8 APPENDIX A – ADMINISTRATION PRIVILEGES

This section aims to list all administration privileges on the Stormshield appliance that could be assigned to users, as defined in FMT_MOF.1.1 and FMT_MTD.1.1

Privileges regarding functions or security data:

- **ADMIN (A)**: super-administrator (“admin” login)
- **BASE (B)**: minimum administration, all access necessary for administration
- **LOG (L)**: access to log files and the audit function.
- **LOG_READ (LR)**: access log files and the audit function in read-only mode.
- **FILTER (F)**: access to filter slots.
- **FILTER_READ (FR)**: access to filter slots in read-only mode.
- **GLOBALFILTER (GF)**: access to the filter slots of the global configuration.
- **VPN (V)**: access to VPN slots, pre-shared keys, certificate (Stormshield appliance).
- **VPN_READ (VR)**: access to VPN slots, pre-shared keys, certificate (Stormshield appliance) in read-only mode.
- **OBJECT (O)**: adding and deleting objects (network configuration).
- **GLOBALOBJECT (GO)**: adding and deleting objects of the global configuration.
- **USER (U)**: user management.
- **NETWORK (N)**: management of the network configuration (interfaces, bridges, dialups, VLANs, etc)
- **ROUTE (R)**: management of routing (default route, static routes, trusted networks)
- **ASQ (As)**: consultation of the ASQ stateful engine’s configuration
- **MAINTENANCE (Ma)**: access to maintenance operations
- **MODIFY (M)**: modification of security data including configuration.
- **MON_WRITE (MW)**: modification of data reserved for Monitoring.
- **CONTENT_FILTER (CF)**: definition of application filter policies (url, smtp, antispam, antivirus, and ssl).
- **TPM (TPM)**: When the firewall is equipped with a TPM, initialization of the TPM and operations on data protected by this TPM (certificates, keys, etc).

Other privileges that do not concern security functions or data:

- **PKI:** management of the internal PKI (issuance, revocation, etc)
- **HA:** high availability (internal, prohibited to users).
- **PVM:** vulnerability management (consultation, modification)
- **REPORT (R)**: access to embedded rapports.
- **REPORT_READ (RR)**: access to embedded rapports in read-only mode.
- **PRIVACY**: access to logs containing personal data.
- **PRIVACY_READ**: access to logs containing personal data in read-only mode.

9 APPENDIX B – ATTACKS HANDLED BY ASQ

This section aims to list all attacks that the ASQ filter engine handles to enforce FAU_SAA.4.1.

Level of analysis	*Attack name*	*Id*
IP	IP loopback address spoofing	0
	IP address spoofing	1
	Broadcast Packet	2
	Multicast Packet	3
	Address from experimental class	4
	Bad IP options	5
	Unknown IP options	6
	Unanalyzed IP protocol	7
	Unknown internal network host	8
	Oversized fragment	9
	Overlapped fragment	10
	Multicast address with TCP	18
	Land style attack	21
	Source routing	23
	Detection of the filter policy	26
	Possible port scan	27
	Zero sized fragment received	33
	Tiny fragment	57
	Port probe	63
	IP address spoofing on bridge	70
	Broadcast address with TCP	71
	Filter alarm	72
	"Link local" addresses (RFC 3330)	83
	Broadcast address used in source address	89
	Possible attack on resources	91
	Invalid IP protocol	92
	Blacklisted address	93
	Whitelisted address	94
	Packet for destination on the same interface	95
	Wrong IP checksum	96
	Quality of service drop	101
	IP fragment analyze	102
	IP address spoofing on IPSec interface	108
	Fragment with DF bit set	175
	Connection lost	210
TCP	Invalid TCP option	14
	Unknown TCP option	15
	Wrong TCP sequence number	16
	Wrong TCP checksum	17
	Xmas tree attack	20
	Nmap OS probe	24
	Queso OS probe	25
	Possible TCP SYN flooding	29

Level of analysis	*Attack name*	*Id*
	Port 0 used as service	34
	Windows OOB data bug	35
	Possible small MSS attack	36
	Misplaced TCP option	58
	TCP data evasion	65
	TCP data queue overflow	84
	Interactive connection detection	85
	Invalid TCP packet for current connection state	97
	Invalid TCP protocol	98
	Datatracking problem	99
	Unauthorized protocol detected	110
	Urgent unauthorized data in TCP information flows	162
	Desynchronization of TCP information flows	211
	Managed by synproxy	212
	Desynchronization status of TCP information flows	213
	Cisco WAN information flow optimizer detected	247
	Possible TCP request flooding	253
	RFC 2385 MD5 signature for TCP	302
	Number of connections allowed per host reached	364
	Number of connections allowed per host per interval reached	365
UDP	Possible UDP flooding	29
	UDP port loopback	31
	Port 0 used as service	34
	Invalid UDP checksum	73
	Datatracking problem	99
	Invalid UDP protocol	100
	Unauthorized protocol detected	110
	Possible UDP request flooding	253
SCTP	SCTP: invalid protocol	475
	SCTP: invalid packet for current association state	476
	SCTP: invalid chunk	477
	SCTP: unsupported option	478
	SCTP: multi-homing max ip reached	479
	SCTP: unknown association	480
	SCTP: invalid length	481
	SCTP: possible flooding	482
ICMP	Unknown ICMP type	11
	ICMP reply without request	12
	ICMP redirect	22
	Possible ICMP flooding	28
	XProbe OS probe	66
	Invalid ICMP message	67
	ICMP 'timestamp' request	68
	ICMP 'mask' request	69
	Invalid ICMP checksum	75
	Possible small MTU attack	81
	ICMP 'information' request	103
	Allowed by ICMP analyze	107
	Modification of ECHO ICMP data	109
	Protocol not analyzed in an ICMP message	112
IGMP	Unknown IGMP type	19
	Non-multicast address in IGMP query	61
	Invalid IGMP packet	62
	Invalid IGMP checksum	74
DNS	DNS label recursion	32

Level of analysis	*Attack name*	*Id*
	DNS id spoofing	38
	DNS zone change	39
	DNS zone update	40
	DNS cache poisoning	60
	Bad pointer in packet	86
	Possible buffer overflow using DNS string	87
	Bad DNS protocol	88
	Contradictory DNS query field	151
	Targeted DNS spoofing	152
	Possible 'DNS rebinding' attack	154
	Duplicated DNS response	159
	DNS NS Type not allowed	163
	DNS Tunneling possible	164
FTP	Possible FTP bounce attack	37
	FTP PASV insertion attack	41
	Unknown FTP command	42
	Buffer overflow on FTP USER/PASSWORD	43
	Buffer overflow on FTP command	44
	Brute force attack on FTP password	45
	Command execution using SITE EXEC	46
	FTP PASV DoS	59
	Invalid FTP Protocol	76
	Invalid PORT command	123
	User not allowed	313
	Blacklisted user	314
HTTP	Invalid %u encoding char in URL	47
	Evasion using %u encoding char in URL	48
	Invalid escaped char in URL	49
	Escaped NULL char in URL	50
	Escaped percent char in URL	51
	Evasion using UTF-8 encoding	52
	Invalid HTTP protocol	53
	Possible buffer overflow on URL	54
	Possible buffer overflow on HTTP request	55
	Tunneling using CONNECT method	56
	Multiple slashes in URL	78
	Directory self-reference	79
	Directory traversal	80
	Bad UTF-8 encoding in URL	82
	Possible malicious code in HTTP header	90
	Directory traversal outside root folder	124
	Bounce by redirect	148
	304 response with data	149
	Additional data at end of reply	150
	HTTP parameter pollution attempt	160
	Unicode character to change reading direction in HTTP URL	161
	Unable to inflate compressed data	165
	Unsupported HTTP compression	166
	Unknown HTTP compression	169
	Malicious compressed HTTP content	170
	Possible HTTP proxy poisoning	172
	Invalid HTTP protocol: strict analysis	173
	Too many HTTP headers in request	232
	Unexpected HTTP/1.1 response for this User-Agent	242
	Decoding of HTML field failed, invalid code	243

Level of analysis	*Attack name*	*Id*
	Recursion detected in decoding of HTML field	244
	HTTP redirection to local file	249
	Too many ranges in HTTP request	251
	Malformed ranges in HTTP request	252
	Compressed HTTP content	254
	The URL contains non-ASCII "8bit in request" characters	256
	RFC 2817 method TLS UPGRADE detected	300
	RFC 6455 method WebSocket UPGRADE detected	301
	Capacity exceeded in an HTML attribute	303
	Unsupported HTTP document encoding SIP	367
SIP	Invalid SIP protocol	131
	Overflow in SIP protocol	132
	Possible malicious code in SIP header	133
	Missing necessary SIP header	134
	Spoofed SIP request	135
	Missing necessary SDP field in the SIP protocol	136
	Invalid SIP expires field	137
	Bad UTF-8 encoding in the SIP protocol	138
	SIP operation limit exceeded	139
	Missing purpose parameter in the SIP protocol	140
	Bad Via field in the SIP protocol	141
	Binary packet in the SIP protocol	142
	Invalid value in SIP Max-Forward header	153
	Missing SIP Max-Forwards header	248
	The SIP request contains an invalid "Contact field" "From field" URI	306
SMTP	Invalid SMTP protocol	121
	Invalid characters in SMTP header	122
	Overflow in the SMTP protocol	217
	Invalid parameters for the SMTP BDAT command	218
	Empty SMTP command line or response	219
	Invalid base64 data in an AUTH SMTP command SMTP	220
	SMTP DATA command with parameters	221
	SMTP command not supported by the server	223
	SMTP BDAT command disabled	224
	Exchange Server SMTP commands disabled	225
	SMTP EXPN command used	226
	SMTP VRFY command used	227
	SMTP TURN, ATRN, ETRN commands disabled	228
	Forbidden SMTP command found	229
	SMTP message with too many header bytes	230
	SMTP subject header contains non-ASCII characters	231
	Brute force attack on SMTP authentication	255
	Sending of e-mail through an anonymous SMTP connection	305
	SMTP bad line ending	315
	User not found for this inbound connection SMTP	366
MODBUS	MODBUS: invalid header or function code	368
	MODBUS: invalid PDU	369
	MODBUS: message length greater than the authorized limit	370
	MODBUS: response without corresponding request	371
	MODBUS: maximal number of pending requests reached	372
	MODBUS: the retransmitted request does not match with the original version	373
	MODBUS: function code denied	374
	MODBUS: Unit Id denied	406
	MODBUS: memory access denied	418

Level of analysis	*Attack name*	*Id*
OPCUA	OPCUA: invalid protocol	396
	OPCUA: service denied	397
	OPCUA: message length greater than the authorized limit	398
	OPCUA: invalid message length	399
	OPCUA: security mode 'None' forbidden	400

10 APPENDIX C – IDENTIFICATION OF OPERATIONS PERFORMED ON IT SECURITY REQUIREMENTS

This section aims to accurately identify the operations performed on IT security requirements, as required by ASE_REQ.2.3C. It must be considered "the list of IT security requirements provided as part of the ST", required by ASE_REQ.2.1D,

10.1 Introduction

In addition to the four types of operations defined in the Common Criteria (cf. [CC-01], § C.4, p. 77), two additional types of modifications to the original version of IT security requirements have been introduced:

Systematic refinement: this refers to a uniform refinement of all the elements of a component;

Layout: this refers to the transformation of the grammatical structure of an element, to make it more legible, or to delete superfluous text without changing the meaning of the element in any way. This corresponds to the concept of *editorial refinement* set out in [CC-01], § C4.4, p. 80.

The security requirements specified in section 5.2 are expressed in order to make their comprehension easier. This section 9 provides a formal description of those requirements.

In the identification of operations, refinements that consist of substituting one term with another, assignments and selections are identified by the symbol ":=". Refinements that consist of adding text are identified by the symbol "+". Format changes are identified by the symbol "→" for substitutions and "⌫" for deletions.

Iterations are identifiable with the help of labels, as explained in §5.1.2.

IT security requirements are presented as follows:

- For each component used, the systematic refinements made to the elements of this component,
- For each element of the component:
  - The original text of the element in English, as extracted from [CC-02] or [CC-03],
  - The list of operations performed on the element.

10.2 Security requirements for the TOE

This section presents the functional requirements of the TOE according to a formal description. The link to chapter 5 is made by maintaining the same title for the functional requirements concerned.

10.2.1 Information flow control requirements

10.2.1.1 Filter function

10.2.1.1.1 FDP_IFC.2 – Full filtering of information flows

Systematic refinement	*The TSF*:= the filter function

FDP_IFC.2.1 *The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.*

Assignment	*information flow control SFP*:= the filter policy
Assignment	*list of subjects and information*:= devices on networks interconnected by the Stormshield appliance (*subjects*) and IP packets (*information*)
Refinement	*all operations that cause that information to flow to and from subjects covered by the SFP*:= all transfers (*operations*) of IP packets between devices on networks interconnected by the Stormshield appliance
Layout	devices on networks interconnected by the Stormshield appliance, IP packets and all transfers of IP packets between the devices on networks interconnected by the Stormshield appliance → Incoming IP packets

FDP_IFC.2.2 *The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.*

Refinement + layout	*all operations that cause any information in the TOE to flow to and from any subject in the TOE:*= all transfers of packets and devices on networks interconnected by the Stormshield appliance → all Incoming IP packets
Refinement	*an information flow control SFP*:= the filter policy

10.2.1.1.2 FDP_IFF.1.Filtering – Filter function

Systematic refinement	*The TSF*:= the filter function
Systematic refinement	*information flow between a controlled subject and controlled information via a controlled operation*:= Incoming IP packets

FDP_IFF.1.1 *The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].*

Assignment	*information flow control SFP*:= the filter policy
Refinement + layout	*subject and information*:= devices on networks interconnected by the Stormshield appliance (*subjects*), IP packets (*information*) → Incoming IP packets
Assignment	*list of subjects and information controlled under the indicated SFP, and, for each, the security attributes* := a. The receiving interface, b. The destination interface, c. The source and destination IP address of the packet and, based on that, the source and destination host of the packet, d. The IP protocol number, e. The value of the DSCP field, f. If the protocol is TCP or UDP: the source and destination port, g. If the protocol is ICMP: the 'type' and 'code' fields of the message, h. If the protocol is SCTP: the source and destination port.

FDP_IFF.1.2 *The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].*

Assignment	*for each operation, the security attribute-based relationship that must hold between subject and information security attributes* := a. Prior to the application of filter rules, the packet is compared against all connections / pseudo-connections currently established and having been authorized by the filter rules; b. If the packet corresponds to one of these connections / pseudo-connections, it will be allowed to pass through without being subject to filter rules; c. Otherwise, the packet will be allowed if the action of the first applicable filter rule is 'pass'.

FDP_IFF.1.3 *The TSF shall enforce the [assignment: additional information flow control SFP rules].*

Assignment	*additional information flow control SFP rules* := the following complementary rules: a. The filter rules whose action is 'none' serve only to generate audit logs and are not taken into account in packet filtering. b. the only purpose of filter rules with a 'delegate' action is to skip the evaluation of the end of the global filter slot to go back to the beginning of the local slot and are not taken into account in packet filtering.

FDP_IFF.1.4 *The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].*

Assignment	*rules, based on security attributes, that explicitly authorise information flows* := a. Sessions associated with protocols requiring child connections are tracked so that these child connections will be authorized according to the status of the main session; b. The firewall can generate implicit filter rules together with the configuration of other security functions. This refers to the rules corresponding to: i. the remote administration of the firewall, ii. VPN establishment.

FDP_IFF.1.5 *The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].*

Assignment	*rules, based on security attributes, that explicitly deny information flows* := a. The action of the first applicable filter rule is 'block' or 'reinitialize'; b. No filter rule has allowed the packet.

10.2.1.2 Encryption function

10.2.1.2.1 FDP_IFC.1 – Encryption of information flows

Systematic refinement	*The TSF*:= the encryption function

FDP_IFC.1.1 *The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].*

Assignment	*information flow control SFP*:= the encryption policy
Assignment + layout	*list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*:= VPN peers and traffic endpoints (TOE side and VPN peer side) (*subject*), incoming ESP datagrams and outgoing IP datagrams covered by an encryption policy (*information*), reception of incoming ESP datagrams originating from VPN peers and sending of outgoing IP datagrams covered by an encryption policy (*operations*)→ incoming ESP datagrams and outgoing IP datagrams covered by an encryption rule

10.2.1.2.2 FDP_UCT.1 – Confidentiality of the contents of information flows

Systematic refinement	*The TSF*:= the encryption function

FDP_UCT.1.1 *The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to be able to [selection: transmit, receive] user data in a manner protected from unauthorised disclosure.*

Assignment	*access control SFP(s) and/or information flow control SFP(s)*:= the encryption policy
Selection	*transmit, receive*:= *transmit and receive*
Refinement	*user data*:= IP datagrams

10.2.1.2.3 FDP_UIT.1 – Integrity of the contents of information flows

Systematic refinement	*The TSF*:= the encryption function

FDP_UIT.1.1 *The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to be able to [selection: transmit, receive] user data in a manner protected from [selection: modification, deletion, insertion, replay] errors.*

Assignment	*access control SFP(s) and/or information flow control SFP(s)*:= the encryption policy
Selection	*transmit, receive*:= *transmit and receive*
Refinement	*user data*:= IP datagrams
Selection	*modification, deletion, insertion, replay*:= *modification, insertion, replay*

FDP_UIT.1.2 *The TSF shall be able to determine on receipt of user data, whether [selection: modification, deletion, insertion, replay] has occurred.*

Refinement	*user data*:= incoming ESP datagrams
Selection	*modification, deletion, insertion, replay*:= *modification, insertion, replay*

10.2.1.2.4 FDP_IFF.1.Encryption – Encryption function

Systematic refinement	*The TSF*:= the encryption function

FDP_IFF.1.1 *The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].*

Assignment	*information flow control SFP*:= the encryption policy
Refinement + layout	*subject and information*:= VPN peers and traffic endpoints (TOE side and VPN peer side) (subject), incoming ESP datagrams and outgoing IP datagrams covered by an encryption policy (information)→ incoming ESP datagrams and outgoing IP datagrams covered by an encryption rule
Assignment	*list of subjects and information controlled under the indicated SFP, and for each, the security attributes*:=Incoming ESP datagrams: a. The Security Parameter Index (SPI), Outgoing IP datagrams: b. Either the source,destination IP addresses and IP protocol of the packet and, based on that, the source and destination host of the packet, c. or the virtual tunnel outgoing interface (VTI).

FDP_IFF.1.2 *The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].*

Refinement	*information flow between a controlled subject and controlled information via a controlled operation*:= incoming ESP packet
Assignment	*for each operation, the security attribute-based relationship that must hold between subject and information security attributes* := a. an incoming ESP datagram can be attached to an active incoming IPSec SA, b. the packet encapsulate in the ESP datagram corresponds to the criteria of the encryption rule associated with the IPSec SA.

FDP_IFF.1.3 *The TSF shall enforce the [assignment: additional information flow control SFP rules].*

Assignment	*additional information flow control SFP rules*:= the following complementary rules: a. on outgoing IP datagrams, use effective authentication and encryption algorithms specified by the outgoing IPSec SA associated with the first applicable encryption rule. b. launch a renegotiation attempt if an outgoing IP datagram is covered by an encryption rule without an active IPSec SA. The datagram will be destroyed if the negotiation fails.

FDP_IFF.1.4 *The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].*

Assignment	*rules, based on security attributes, that explicitly authorise information flows*:= No rule
Layout	From the element

FDP_IFF.1.5 *The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].*

Assignment	*rules, based on security attributes, that explicitly deny information flows*:= No rule
Layout	From the element

10.2.1.3 SA establishment function

10.2.1.3.1 FTP_TRP.1.Peer – Trusted path with VPN peers

Systematic refinement	*The TSF*:= the SA establishment function

FTP_TRP.1.1 *The TSF shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].*

Selection	*remote, local*:= *remote*
Refinement	*Itself* := the StormShield appliance
Refinement	*remote users*:= VPN peers
Assignment	*other types of integrity or confidentiality violation*:= none
Selection	*modification, disclosure, none*:= modification or disclosure

FTP_TRP.1.2 *The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path.*

Selection	*the TSF, local users, remote users*:= *the TSF and remote users*
Refinement	*the TSF and remote users*:= the Stormshield appliance and VPN peers
Refinement	*communication via the trusted path:*= the establishment of the trusted path corresponds to IKE_SA.

FTP_TRP.1.3 *The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].*

Selection	*initial user authentication, [assignment: other services for which trusted path is required]* := *a. initial user authentication,* *other services for which trusted path is required]*
Refinement	***initial user authentication*:= the initial mutual authentication of tunnel endpoints (phase 1 of the IKE protocol)**
Assignment	***other services for which trusted path is required*:= the negotiation of IPSec SAs (CHILD_SA)**

10.2.1.3.2 FIA_UAU.5.Peer – Multiple authentication mechanisms of VPN peers

Systematic refinement	*The TSF*:= the SA establishment function

FIA_UAU.5.1 *The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.*

Assignment	*list of multiple authentication mechanisms* := the following authentication mechanisms: X509 certificates, pre-shared keys
Refinement	*user*:= the VPN peer of a given tunnel, in the scope of the initial mutual authentication of this tunnel's endpoints during IKE_SA.

FIA_UAU.5.2 *The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].*

Assignment + layout	*rules describing how the multiple authentication mechanisms provide authentication*:= rules of the authentication mechanism specified for the VPN tunnel → the authentication mechanism specified for the VPN tunnel
Refinement	*user*:= VPN peer

10.2.1.3.3 FPT_TDC.1 – Negotiation of IKE and IPSec SAs

Systematic refinement	*The TSF*:= the SA establishment function

FPT_TDC.1.1 *The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product.*

Assignment	*list of TSF data types*:= parameters of IKE and IPSec SAs
Refinement	*consistently interpret parameters of IKE and IPSec SAs*:= negotiate the parameters of IKE and IPSec SAs
Refinement	*when shared between the TSF and another trusted IT product*:= when establishing VPN tunnels between the Stormshield appliance and VPN peers

FPT_TDC.1.2 *The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product.*

Assignment	*list of interpretation rules to be applied by the TSF*:= the following rules: a. If the Stormshield appliance is the initiator, propose the parameters of the IKE or IPSEC SA, and accept the responses that are as strict as one of the proposals made; b. If the Stormshield appliance is the responder, accept only proposals that are as strict as one of the local proposals.
Refinement	*interpreting the TSF data from another trusted IT product*:= negotiate IKE or IPSEC SA parameters with VPN peers

10.2.1.4 Enrollment function

10.2.1.4.1 FIA_X509_EXT.4 – Alternate X.509 Enrollment

Systematic refinement	*The TSF*:= the enrollment function

FIA_X509_EXT.4.1 *The TSF shall use the Enrollment over Secure Transport (EST) protocol as specified in RFC 7030 to request certificate enrollment using the simple enrollment method described in RFC 7030 Section 4.2.*

Refinement	*The TSF*:= the enrollment function

FIA_X509_EXT.4.2 *The TSF shall be capable of authenticating EST requests using an existing certificate and corresponding private key as specified by RFC 7030 Section 3.3.2.*

Refinement	*The TSF*:= the enrollment function

FIA_X509_EXT.4.3 *The TSF shall be capable of authenticating EST requests using HTTP Basic Authentication with a username and password as specified by RFC 7030 Section 3.2.3.*

Refinement	*The TSF*:= the enrollment function

FIA_X509_EXT.4.4 *The TSF shall perform authentication of the EST server using an Explicit Trust Anchor following the rules described in RFC 7030, section 3.6.1..*

Refinement	*The TSF*:= the enrollment function

FIA_X509_EXT.4.7 *The TSF shall generate a Certificate Request Message for EST as specified in RFC 2986 and be able to provide the following information in the request: public key and* [selection: device-specific information, Common Name, Organization, Organizational Unit, Country].

Refinement	*The TSF*:= the enrollment function
Selection	device-specific information, Common Name, Organization, Organizational Unit, Country := Common Name, Organization, Organizational Unit, Country

10.2.1.4.2 FCS_HTTPS_EXT.1 HTTPS Protocol

Systematic refinement	*The TSF*:= the enrollment function

FCS_HTTPS_EXT.1.1 *The TSF shall implement the HTTPS protocol that complies with RFC 2818.*

Refinement	*the TSF*:= the enrollment function

FCS_HTTPS_EXT.1.2 *The TSF shall implement HTTPS using TLS as specified in FCS_TLSC_EXT.1.*

Refinement	*the TSF*:= the enrollment function

10.2.1.4.3 FCS_TLSC_EXT.1 TLS Client Protocol

Systematic refinement	*The product*:= the enrollment function

FCS_TLSC_EXT.1.1 *The product shall implement [selectionTLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446)] supporting the following ciphersuites:*

- *TLS_AES_128_GCM_SHA256*
- *ECDHE-ECDSA-AES128-GCM-SHA256*
- *ECDHE-RSA-AES128-GCM-SHA256*
- *DHE-RSA-AES128-GCM-SHA256*

- *TLS_CHACHA20_POLY1305_SHA256*
- *ECDHE-ECDSA-CHACHA20-POLY1305*
- *ECDHE-RSA-CHACHA20-POLY1305*
- *TLS_AES_256_GCM_SHA384*
- *ECDHE-ECDSA-AES256-GCM-SHA384*
- *ECDHE-RSA-AES256-GCM-SHA384*
- *DHE-RSA-AES256-GCM-SHA384*
- *DHE-RSA-CHACHA20-POLY1305-SHA256*

o no other ciphersuite].

Refinement	*the product*:= the enrollment function
Selection	*TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446):= TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446) and no other version*

FCS_TLSC_EXT.1.2 *The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.*

Refinement	*the product*:= the enrollment function

FCS_TLSC_EXT.1.5 *The product shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [selection: secp256r1, secp384r1, secp521r1] and no other curves.*

Refinement	*the product*:= the enrollment function
Selection	*secp256r1, secp384r1, secp521r1*:= secp256r1, secp384r1, secp521r1
Refinement	secp256r1, secp384r1, secp521r1:= secp256r1, secp384r1, secp521r1, BrainpoolP256r1 BrainpoolP384r1 BrainpoolP512r1

10.2.1.5 Log, audit and alarm function

10.2.1.5.1 FAU_GEN.1 – Generation of audit data

Systematic refinement	*The TSF*:= the log function

FAU_GEN.1.1 *The TSF shall be able to generate an audit record of the following auditable events:*

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection: choose one of: minimum, basic, detailed, not specified] level of audit; and

c) [assignment: other specifically defined auditable events].

Selection	*minimum, basic, detailed, not specified* := *not specified*
Layout	From Item b)
Assignment	*other specifically defined auditable events*:= auditable events listed in the table in chapter 5.2 after FAU_GEN.1.2
Refinement	*audit functions:= log function*

FAU_GEN.1.2 *The TSF shall record within each audit record at least the following information:*

a) Date and time of the event, type of event, subject identity (if applicable) and the outcome (success or failure) of the event; and

b) *For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information]*

Refinement	*subject identity*:= source IP address
Assignment	*other audit relevant information*:= alarm level (if it is an alarm), complementary audit information listed in the table in chapter 5.2
Layout	‘‘Factoring’ of “alarm level (if it is an alarm)”

10.2.1.5.2 FAU_GEN.2 – User identification

Systematic refinement	*The TSF*:= the log function

FAU_GEN.2.1 *For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.*

Refinement	*user* := administrator
Refinement	*auditable event*:= auditable event linked to security administration operations

10.2.1.5.3 FAU_SAR.1 – Audit review

Systematic refinement	*The TSF*:= the audit function

FAU_SAR.1.1 *The TSF shall provide [assignment: authorised users] with the capability to read [assignment: list of audit information] from the audit records.*

Assignment	*authorised users*:= auditors
Assignment	*list of audit information*:= all audit information
Refinement	*audit records*:= log files

FAU_SAR.1.2 *The TSF shall provide the audit records in a manner suitable for the user to interpret the information.*

Refinement	*audit records*:= log files
Refinement	*user*:= auditor

10.2.1.5.4 FAU_STG.3 – Action in the event of possible loss of audit data

Systematic refinement	*The TSF*:= the log function

FAU_STG.3.1 *The TSF shall [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit].*

Assignment	*actions to be taken in case of possible audit storage failure* := Rotate files: the most recent audit logs erase the oldest audit logs, b.
Refinement	*audit trail*:= an existing log file (excluding the use of Syslog)
Assignment	*pre-defined limit*:= exceeds 20 MB.

10.2.2 Requirements of protection from Internet attacks

10.2.2.1 Intrusion prevention function

10.2.2.1.1 FAU_SAA.4 – Heuristics of complex attacks

Systematic refinement	*The TSF*:= the intrusion prevention function

FAU_SAA.4.1 *The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the enforcement of the SFRs.*

Refinement	*internal representation*:= knowledge base
Layout	*the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the enforcement of the SFRs.* *→ the following signature events and event sequences of known intrusion scenarios [assignment: list of system events or sequences of system events whose occurrence are representative of known penetration scenarios] that may indicate a potential violation of the enforcement of the SFRs.*
Assignment	*list of system events or sequences of system events whose occurrence are representative of known penetration scenarios* := the attacks listed in Appendix B – Attacks HANDLED BY ASQ
Refinement	*potential violation of the enforcement of the SFRs*:= potential internet attack

FAU_SAA.4.2 *The TSF shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of [assignment: information to be used to determine system activity].*

Refinement	*signature events and event sequences*:= types of attacks in the knowledge base
Assignment	*information to be used to determine system activity*:= incoming and outgoing IP packets
Refinement	*the record of system activity discernible from an examination of incoming and outgoing IP packets*:= the status of one or several contexts associated with each incoming and outgoing packet

FAU_SAA.4.3 *The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when system activity is found to match a signature event or event sequence that indicates a potential violation of the enforcement of the SFRs.*

Refinement	*potential violation of the enforcement of the SFRs*:= potential internet attack
Refinement	*system activity*:= the status of one or several contexts associated with an incoming packet
Refinement	*signature event or event sequence that indicates a potential violation of the enforcement of the SFRs*:= type of attack in the knowledge base

10.2.2.1.2 FAU_ARP.1.IPS – Automatic response to potential internet attacks

Systematic refinement	*The TSF*:= the intrusion prevention function

FAU_ARP.1.1 *The TSF shall take [assignment: list of actions] upon detection of a potential security violation.*

Assignment	*list of actions* := a. apply to the packet the action associated with the type of attack, b. if an alarm level has been specified for this type of attack, generate an audit log for the event, by assigning this level of alarm to it
Refinement	*potential security violation*:= internet attack potentially conveyed by an incoming IP packet

10.2.3 Requirements of prevention of improper use

10.2.3.1 Function for the control of access to security administration operations

10.2.3.1.1 FMT_SMF.1 – Security administration function

Systematic refinement	*The TSF*:= the security administration function

FMT_SMF.1.1 *The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].*

Assignment	*list of management functions to be provided by the TSF* := a. The function for the control of access to security administration operations; b. The administration session protection function c. The audit function d. The backup/restoration function

10.2.3.1.2 FMT_SMR.1 – Role of the security administrator

Systematic refinement	*The TSF*:= The function for the control of access to security administration operations

FMT_SMR.1.1 *The TSF shall maintain the roles [assignment: the authorised identified roles].*

Assignment	*the authorised identified roles*:= “administrator” and “super administrator”

FMT_SMR.1.2 *The TSF shall be able to associate users with roles.*

Refinement	+ according to the following rules: a. There is only one super-administrator, distinct from other administrators, and who possess all privileges; b. Administrators are persons to whom this role has been explicitly assigned

10.2.3.1.3 FDP_ACC.2 – Control of full access to security administration operations

Systematic refinement	*The TSF*:= The function for the control of access to security administration operations

FDP_ACC.2.1 *The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.*

Assignment	*access control SFP*:= the policy controlling access to security administration operations
Assignment	*list of subjects and objects*:= administrators (subjects), data and security functions (objects)
Refinement	*all operations among subjects and objects covered by the SFP*:= all security administration operations
Layout	administrators, data and security functions and all security administration operations → all security administration operations performed by the administrator

FDP_ACC.2.2 *The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.*

Refinement + layout	*all operations between any subject controlled by the TSF and any object controlled by the TSF*:= all security administration operations between administrators and data and security functions→ all security administration operations performed by the administrator
Refinement	*an access control SFP*:= the policy controlling access to security administration operations

10.2.3.1.4 FMT_MOF.1 – Administration of the behavior of security functions

Systematic refinement	*The TSF*:= The function for the control of access to security administration operations

FMT_MOF.1.1 *The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorised identified roles].*

Selection	*determine the behaviour of, disable, enable, modify the behaviour of:= disable, enable, modify the behaviour of*
Refinement	*modify the behaviour of*:= perform, modify
Assignment	*list of functions*:= the security functions in the table below
Assignment	*the authorised identified roles*:= administrators
Refinement	According to the privileges below

10.2.3.1.5 FMT_MTD.1 – Administration of security data

Systematic refinement	*The TSF*:= The function for the control of access to security administration operations

FMT_MTD.1.1 *The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles].*

Selection	*change_default, query, modify, delete, clear, [assignment: other operations]* := *query, modify, clear*
Assignment	*list of TSF data*:= the security functions in the table below
Assignment	*the authorised identified roles*:= administrators
Refinement	+ according to the privileges below

10.2.3.2 Backup and restoration function

10.2.3.2.1 FMT_MTD.BRS – Backup and restoration of security data

Systematic refinement	*The TSF*:= The backup/restoration function

FMT_MTD.BRS.1 The TSF shall be able to back up [assignment: list of TSF data] into a storage device.

Assignment	*list of TSF data*:= security data
Refinement	*a storage device*:= administration workstation's hard disk

FMT_MTD.BRS.2 The TSF shall allow restoration of TSF data backed up into a storage device.

Refinement	*TSF data*:= security data
Refinement	*a storage device*:= administration workstation's hard disk

10.2.4 TOE protection requirements

10.2.4.1 Administration session protection function

10.2.4.1.1 FPT_ITT.1 – Basic protection of the contents of administration sessions

Systematic refinement	*The TSF*:= the administration session protection function

FPT_ITT.1.1 The TSF shall protect TSF data from [selection: disclosure, modification] when it is transmitted between separate parts of the TOE.

Refinement	*TSF data*:= the contents of administration sessions
Selection	*disclosure, modification* := *disclosure, modification*
Refinement	*separate parts of the TOE*:= the administration workstation and the Stormshield appliance

10.2.4.1.2 FTP_TRP.1.Admin – Trusted path for remote administration

Systematic refinement	*The TSF*:= the administration session protection function

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].

Refinement	*itself* := the Stormshield appliance
Selection	*remote, local* := *remote*
Refinement	*remote users*:= administrators
Assignment	*other types of integrity or confidentiality violation* := none
Selection	*modification, disclosure, none* := modification or disclosure

FTP_TRP.1.2 The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path.

Selection	*the TSF, local users, remote users* := *remote users*
Refinement	*remote users* := administrators

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].

Selection	*initial user authentication, [assignment: other services for which trusted path is required]* := *initial user authentication, [assignment: other services for which trusted path is required]*
Refinement	*initial user authentication*:= the initial mutual authentication of the administrator and the Stormshield appliance
Assignment	*other services for which trusted path is required*:= remote security administration operations

10.2.4.1.3 FIA_UAU.5.Admin – Authentication mechanism for administrators

Systematic refinement	*The TSF*:= the administration session protection function

FIA_UAU.5.1 *The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.*

Assignment	*list of multiple authentication mechanisms* := the TLS protocol
Refinement	*user*:= administrator

FIA_UAU.5.2 *The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].*

Refinement	*user*:= administrator
Assignment + layout	*rules describing how the multiple authentication mechanisms provide authentication*:= rules of the TLS protocol (login / password or X.509 certificate) → TLS protocol (login / password or X.509 certificate)

10.2.4.1.4 FTP_TRP.1.LDAP – Trusted path with LDAP server

Systematic refinement	*The TSF*:= the secure LDAP communication function

FTP_TRP.1.1 *The TSF shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].*

Refinement	*itself* := the Stormshield appliance
Selection	*remote, local* := *remote*
Refinement	*remote users*:= LDAP server
Assignment	*other types of integrity or confidentiality violation* := none
Selection	*modification, disclosure, none* := modification or disclosure

FTP_TRP.1.2 *The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path.*

Selection	*the TSF, local users, remote users* := *the TSF*

FTP_TRP.1.3 *The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].*

Assignment	*other services for which trusted path is required*:= none
Selection	*initial user authentication, none*:= *initial user authentication,*
Refinement	*initial user authentication*:= the initial mutual authentication of the LDAP server and the Stormshield appliance

10.2.4.1.5 FIA_UAU.5.LDAP – Authentication mechanism for LDAPServer

Systematic refinement	*The TSF*:= the secure LDAPcommunication function

FIA_UAU.5.1 *The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.*

Assignment	*list of multiple authentication mechanisms* := the TLS protocol
Refinement	*user*:= LDAP server

FIA_UAU.5.2 *The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].*

Refinement	*user*:= LDAP Server
Assignment + layout	*rules describing how the multiple authentication mechanisms provide authentication*:= rules of the TLS protocol (login / password or X.509 certificate) → TLS protocol (with a X.509 certificate)

10.2.4.1.6 FTP_TRP.1.Management – Trusted path with Management Center

Systematic refinement	*The TSF*:= the secure management communication function

FTP_TRP.1.1 *The TSF shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].*

Refinement	*itself* := the Stormshield appliance
Selection	*remote, local* := *remote*
Refinement	*remote users*:= Management Center
Assignment	*other types of integrity or confidentiality violation* := none
Selection	*modification, disclosure, none* := modification or disclosure

FTP_TRP.1.2 *The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path.*

Selection	*the TSF, local users, remote users* := *the TSF*

FTP_TRP.1.3 *The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].*

Selection	*initial user authentication, [assignment: other services for which trusted path is required]* := *initial user authentication, [assignment: other services for which trusted path is required]*
Refinement	*initial user authentication*:= the initial mutual authentication of the Management Center and the Stormshield appliance
Assignment	*other services for which trusted path is required*:= backup operations

10.2.4.1.7 FIA_UAU.5.Management – Authentication mechanism for Management Center

Systematic refinement	*The TSF*:= the secure management communication function

FIA_UAU.5.1 *The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.*

Assignment	*list of multiple authentication mechanisms* := the TLS protocol
Refinement	*user*:= Management Center

FIA_UAU.5.2 *The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].*

Refinement	*user*:= Management Center
Assignment + layout	*rules describing how the multiple authentication mechanisms provide authentication*:= rules of the TLS protocol (login / password or X.509 certificate) → TLS protocol (with a X.509 certificate)

10.2.4.1.8 FTP_TRP.1.Syslog – Trusted path with Syslog server

Systematic refinement	*The TSF*:= the secure syslog communication function

FTP_TRP.1.1 *The TSF shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].*

Refinement	*itself* := the Stormshield appliance
Selection	*remote, local* := *remote*
Refinement	*remote users*:= Syslog server
Assignment	*other types of integrity or confidentiality violation* := none
Selection	*modification, disclosure, none* := modification or disclosure

FTP_TRP.1.2 *The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path.*

Selection	*the TSF, local users, remote users* := *the TSF*

FTP_TRP.1.3 *The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].*

Assignment	*other services for which trusted path is required*:= none
Selection	*initial user authentication, none*:= *initial user authentication,*
Refinement	*initial user authentication*:= the initial mutual authentication of the Syslog server and the Stormshield appliance

10.2.4.1.9 FIA_UAU.5.Syslog – Authentication mechanism for Syslog Server

Systematic refinement	*The TSF*:= the secure syslog communication function

FIA_UAU.5.1 *The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.*

Assignment	*list of multiple authentication mechanisms* := the TLS protocol
Refinement	*user*:= Syslog server

FIA_UAU.5.2 *The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].*

Refinement	*user*:= Syslog Server
Assignment + layout	*rules describing how the multiple authentication mechanisms provide authentication*:= rules of the TLS protocol (login / password or X.509 certificate) → TLS protocol (with a X.509 certificate)

10.2.5 Cryptographic supporting security requirements

10.2.5.1 Cryptographic supporting functions

10.2.5.1.1 FCS_COP.1 – Cryptographic function

Systematic refinement	*The TSF*:= the cryptographic function

FCS_COP.1.Key_preparation *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Assignment	*list of cryptographic operations*:= key preparation
Assignment	*cryptographic algorithm*:= the cryptographic algorithm ⌫ specified below
Assignment	*cryptographic key sizes*:= cryptographic key sizes ⌫ specified below
Assignment	*list of standards*:= standards set out below

FCS_COP.1.Signature *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Assignment	*list of cryptographic operations*:= signature and signature verification
Assignment	*cryptographic algorithm*:= the cryptographic algorithm ⌫ specified below
Assignment	*cryptographic key sizes*:= cryptographic key sizes ⌫ specified below
Assignment	*list of standards*:= standards set out below

FCS_COP.1.Hashing *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Assignment	*list of cryptographic operations*:= one-to-one hashing
Assignment	*cryptographic algorithm*:= cryptographic algorithms ⌫ specified below
Assignment	*cryptographic key sizes*:= cryptographic key sizes ⌫ specified below
Assignment	*list of standards*:= standards set out below

FCS_COP.1.Encryption_VPN *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Assignment	*list of cryptographic operations*:= symmetrical encryption/decryption of ESP packets
Assignment	*cryptographic algorithm*:= cryptographic algorithms ⌫ specified below
Assignment	*cryptographic key sizes*:= cryptographic key sizes ⌫ specified below
Assignment	*list of standards*:= standards set out below

FCS_COP.1.Integrity_VPN *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Assignment	*list of cryptographic operations*:= checking the integrity of ESP paquets
Assignment	*cryptographic algorithm*:= the cryptographic algorithm ⌫ specified below
Assignment	*cryptographic key sizes*:= cryptographic key sizes ⌫ specified below
Assignment	*list of standards*:= standards set out below

FCS_COP.1.Encryption_sessions *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Assignment	*list of cryptographic operations*:= symmetrical encryption/decryption of administration sessions
Assignment	*cryptographic algorithm*:= the cryptographic algorithm ⌫ specified below
Assignment	*cryptographic key sizes*:= cryptographic key sizes ⌫ specified below
Assignment	*list of standards*:= standards set out below

FCS_COP.1.Integrity_sessions *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Assignment	*list of cryptographic operations*:= checking the integrity of administration sessions
Assignment	*cryptographic algorithm*:= the cryptographic algorithm ⌫ specified below
Assignment	*cryptographic key sizes*:= cryptographic key sizes ⌫ specified below
Assignment	*list of standards*:= standards set out below

10.2.5.1.2 FCS_CKM.1 – Cryptographic key generation

Systematic refinement	*The TSF*:= the cryptographic key generation function

FCS_CKM.1 *The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Assignment	*cryptographic key generation algorithm*:= the cryptographic *key generation* algorithm ⌫ specified below
Assignment	*cryptographic key sizes*:= cryptographic key sizes ⌫ specified below
Assignment	*list of standards*:= standards set out below

10.2.5.1.3 FCS_CKM.4 – Cryptographic key destruction

Systematic refinement	*The TSF*:= the cryptographic key destruction function

FCS_CKM.4 *The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].*

Refinement	*"in accordance with a specified cryptographic key destruction method":= by*
Assignment	*cryptographic key destruction method*:= overwriting them with zeros
Refinement	*that meets the following: [assignment: list of standards]:= none*

11 APPENDIX D – EXTENDED SECURITY REQUIREMENTS

This section aims to set out the extended security requirements with the purpose of complementing existing requirements in part 2 and 3 of the Common Criteria.

11.1 Introduction

The extended security requirement set out in this security target is functional.

11.2 FMT_MTD - Management of TSF data

Component levelling

Backup and restoration of TSF data specifies the capacity to spare the configuration of the TSF, or part of it, into a separate storage device, and to restore it thereafter.

Management: FMT_MTD.BRS

a) Managing the group of roles that can perform backup.

b) Managing the group of roles that can perform restoration.

Audit: FMT_MTD.BRS

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Use of the backup functions.

b) Basic: Use of the restoration functions.

FMT_MTD.BRS Backup and restoration of TSF data

Hierarchical to: no other component.

Dependencies: FMT_MTD.1: Management of TSF data
FMT_SMF.1: Specification of Management Functions

FMT_MTD.BRS.1 The TSF shall be able to back up [assignment: list of TSF data] into a storage device.

FMT_MTD.BRS.2 The TSF shall allow restoration of TSF data backed up into a storage device.

Application notes

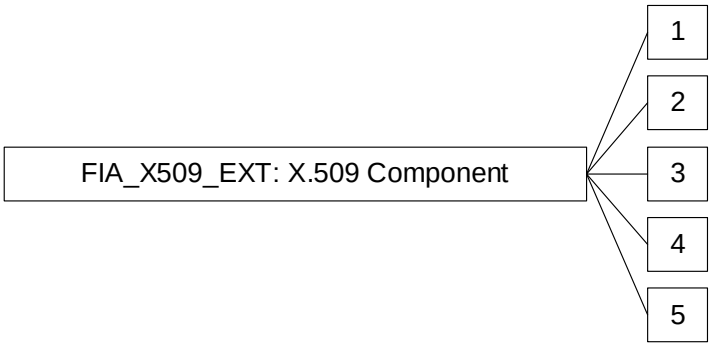
Operations

Assignment:

In FMT_MTD.BRS.1, the PP/ST author should specify the TSF data that can be backed up. In particular, it should be specified whether partial backup is possible.

11.3 FIA_X509_EXT: X509 Component

Component levelling



FIA_X509_EXT.4 Alternate X.509 Enrollment provides an X.509 enrollment method over EST as specified in RFC 7030.

Management: FIA_X509_EXT.4

a) Initiate certificate request.

Audit: FIA_X509_EXT.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Generation of Certificate Enrollment Request, with:

- Issuer and Subject name of EST Server.
- Method of authentication.
- Issuer and Subject name of certificate used to authenticate.
- Content of Certificate Request Message.

b) Basic: Success or failure of enrolment, with:

- Issuer and Subject name of added certificate
- or reason for failure.

FIA_X509_EXT.4 - Alternate X.509 Enrollment

FIA_X509_EXT.4.1

The TSF shall use the Enrollment over Secure Transport (EST) protocol as specified in RFC 7030 to request certificate enrollment using the simple enrollment method described in RFC 7030 Section 4.2.

FIA_X509_EXT.4.2

The TSF shall be capable of authenticating EST requests using an existing certificate and corresponding private key as specified by RFC 7030 Section 3.3.2.

FIA_X509_EXT.4.3

The TSF shall be capable of authenticating EST requests using HTTP Basic Authentication with a username and password as specified by RFC 7030 Section 3.2.3.

FIA_X509_EXT.4.4

The TSF shall perform authentication of the EST server using an Explicit Trust Anchor following the rules described in RFC 7030, section 3.6.1.

FIA_X509_EXT.4.7

The TSF shall generate a Certificate Request Message for EST as specified in RFC 2986 and be able to provide the following information in the request: public key and [selection: device-specific information, Common Name, Organization, Organizational Unit, Country].

Application Note: The public key referenced is the public key portion of the public-private key pair generated by the TOE as specified in FCS_CKM.1.

11.4 FCS_HTTPS_EXT.1 HTTPS Protocol

Component levelling

FCS_HTTPS_EXT: HTTPS Protocol	1

FCS_HTTPS_EXT.1 HTTPS Protocol provides an HTTPS implementation that complies with RFC 2818.

Management: FCS_HTTPS_EXT.1

There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Failure of the certificate validity check, with:
  - Issuer Name and Subject Name of certificate.
  - [selection: User's authorization decision, No additional information]..

FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

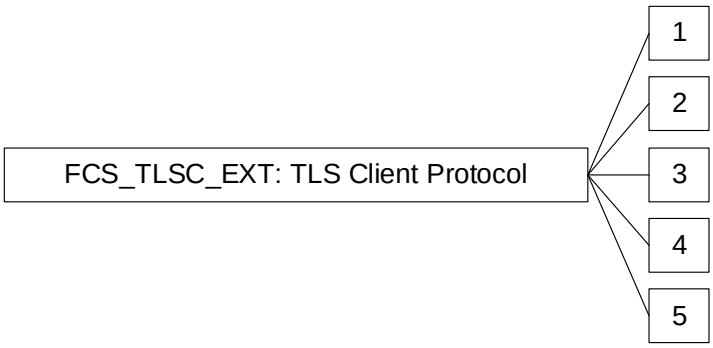
FCS_HTTPS_EXT.1.2

The TSF shall implement HTTPS using TLS as specified in FCS_TLSC_EXT.1.

Application Note: Validity is determined by the certificate path, the expiration date, and the revocation status in accordance with RFC 5280.

11.5 FCS_TLSC_EXT.1 TLS Client Protocol

Component levelling



FCS_TLSC_EXT.1 TLS Client Protocol provides a TLS client implementation that complies with RFC 2818.

Management: FCS_TLSC_EXT.1

There are no management activities foreseen.

Audit: FCS_TLSC_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Failure to establish a TLS session, with:
  - Reason for failure.
- Basic: Failure to verify presented identifier, with:
  - Presented identifier and reference identifier.

FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1

The product shall implement [selection TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446)] supporting the following ciphersuites:

- TLS_AES_128_GCM_SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- TLS_CHACHA20_POLY1305_SHA256
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- TLS_AES_256_GCM_SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-CHACHA20-POLY1305-SHA256

o no other ciphersuite].

FCS_TLSC_EXT.1.2

The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.5

The product shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [selection: secp256r1, secp384r1, secp521r1] and no other curves.