



STORMSHIELD



Stormshield Network Security

UTM / NG-Firewall Filtering Function

Version 2.2

EAL4+ Security Target

Document version : 2.5

Référence : SN_ASE_ciblesec_filter_v2

Date: 19/05/2016

**DOCUMENT TRACKING**

Version	Author	Date	Modifications
0.1	Ludovic FLAMENT	22/08/2008	Initial version of the document
0.2	Ludovic FLAMENT	26/08/2008	Update following vetting by Boris MARECHAL
1.0	Ludovic FLAMENT	11/09/2008	Comments following the preparation phase
1.1	Ludovic FLAMENT	13/10/2008	Integration of comments from the CESTI (SA-FdC01-ASE)
1.2	Ludovic FLAMENT	30/10/2008	Integration of comments from the CESTI (SA-FdC02-ASE)
1.3	Ludovic FLAMENT	27/03/2009	Integration of comments from the CESTI (SA-FdC12-ASE)
1.4	Ludovic FLAMENT	20/02/2012	Update to version 9.1
1.5	Ludovic FLAMENT	22/02/2012	AVA_VAN correction
1.6	Ludovic FLAMENT	24/05/2012	Update following remarks from ANSSI
1.7	Ludovic FLAMENT	09/07/2012	Update following remarks from CESTI
2.0	Thierry MIDY	08/04/2015	Names and diagrams updated with "Stormshield Network Security" Update of the evaluation platform
2.1	Thierry MIDY	03/07/2015	Minor corrections
2.2	Thierry MIDY	14/09/2015	Update following remarks from CESTI Update of TOE version to 2.2
2.3	Thierry MIDY	29/02/2016	Update of TOE version to 2.2.4
2.4	Thierry MIDY	24/03/2016	Update of TOE version to 2.2.5
2.5	Thierry MIDY	25/03/2016	Update of TOE version to 2.2.6 and test plateform



CONTENTS

- 1 INTRODUCTION 6**
 - 1.1 Identifying the security target..... 6
 - 1.2 Statements of compliance..... 6
 - 1.3 Summary of the Stormshield appliances features 6
 - 1.4 Applicable and reference documents 7
 - 1.4.1 Common Criteria references 7
 - 1.4.2 RFCs and other standards supported 7
 - 1.5 Glossary 7
- 2 DESCRIPTION OF THE TARGET OF EVALUATION 10**
 - 2.1 IT security characteristics of the TOE..... 10
 - 2.1.1 Overview..... 10
 - 2.1.2 Information flow control 10
 - 2.1.3 Protection against log saturation 10
 - 2.1.4 Risks of improper use..... 11
 - 2.1.5 Protection of the TOE itself 11
 - 2.2 Physical limits of the TOE 12
 - 2.2.1 Appliances that comprise the TOE..... 12
 - 2.2.2 Minimum characteristics of operating platforms..... 12
 - 2.3 Logical limits of the TOE 13
 - 2.4 Architecture and interfaces of the TOE 13
 - 2.5 Configurations and usage modes subject to the evaluation..... 14
 - 2.6 Test platform used during the evaluation..... 15
- 3 SECURITY ENVIRONMENT OF THE TARGET OF EVALUATION..... 16**
 - 3.1 Typographical convention..... 16
 - 3.2 Identification of sensitive assets..... 16
 - 3.2.1 Assets protected by the TOE 16
 - 3.2.2 Assets belonging to the TOE..... 16
 - 3.3 Threats and rules of the security policy 17
 - 3.3.1 Information flow control 17
 - 3.3.2 Risks of improper use..... 17
 - 3.3.3 Protection of the TOE itself 17
 - 3.4 Assumptions..... 18
 - 3.4.1 Assumption on physical security measures 18
 - 3.4.2 Assumption on organizational security measures..... 18
 - 3.4.3 Assumption relating to human agents 18
 - 3.4.4 Assumption on the IT security environment..... 18
- 4 SECURITY OBJECTIVES..... 19**
 - 4.1 Typographical convention..... 19
 - 4.2 Overview 19
 - 4.3 Information flow control objectives 19
 - 4.4 Security objectives for the environment 20
 - 4.5 Rationale of security objectives 21
- 5 IT SECURITY REQUIREMENTS 22**
 - 5.1 Introduction 22
 - 5.1.1 Typographical conventions..... 22
 - 5.1.2 Presentation of security data..... 22
 - 5.2 Security requirements for the TOE..... 24
 - 5.2.1 Information flow control requirements 24



- 5.3 Security assurance requirements for the TOE..... 26**
- 5.4 Security requirements rationale 27**
 - 5.4.1 *Satisfaction of security objectives 27*
 - 5.4.2 *Mutual support and non contradiction 27*
 - 5.4.3 *Satisfaction of the dependencies of SFRs 27*
 - 5.4.4 *Satisfaction of SAR dependencies 28*
- 6 TOE SUMMARY SPECIFICATIONS..... 29**
- 6.1 IT security functions 29**
 - 6.1.1 *Filter function 29*
 - 6.1.2 *Audit data generation function 30*
- 7 APPENDIX – IDENTIFICATION OF OPERATIONS PERFORMED ON IT SECURITY REQUIREMENTS..... 31**
- 7.1 Introduction 31**
- 7.2 Security requirements for the TOE..... 31**
 - 7.2.1 *Information flow control requirements 31*



TABLE OF ILLUSTRATIONS

Illustration 1: Example of use of the TOE. 12

Illustration 2: Components and interfaces of the TOE. 13

Illustration 3: Test platform used during the evaluation. 15

1 INTRODUCTION

The aim of this section is to provide accurate identification and reference information for this document and the product being evaluated, as well as the appropriate statements regarding compliance with the Common Criteria and other applicable baselines. It also provides an overview of the features on the Stormshield appliance.

1.1 Identifying the security target

<u>Title:</u>	Security Target - UTM / NG-Firewall Filtering Function - version 2.2 EAL4+ Security Target
<u>Reference of the ST:</u>	SN_ASE_ciblesec_filter_v2
<u>Version of the ST:</u>	2.5
<u>Target of evaluation:</u>	Filtering Function of UTM / NG-Firewall Firmware
<u>Version of the TOE:</u>	2.2.6 (S, M, L, XL)
<u>Security assurance package:</u>	Augmented EAL4 for ALC_FLR.3.

1.2 Statements of compliance

The applicable version of the Common Criteria is version 3.1 revision 4 of July 2009.

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

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 than the package selected has been made.

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

1.3 Summary of the Stormshield appliances features

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 network(s).

The main features of the Stormshield Network Security UTM / NG-Firewalls Firmware, which equips these appliances, consist of two main groups:

- the NG-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 Applicable and reference documents

1.4.1 Common Criteria references

- | | |
|----------|--|
| [CC-01] | Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 – Part 1: Introduction and general model, CCMB-2012-09-001, September 2012. |
| [CC-02] | Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 – Part 2: Security functional components CCMB-2012-09-002, September 2012. |
| [CC-03] | Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 – Part 3: Security assurance components CCMB-2012-09-003, September 2012. |
| [CEM-02] | Common Criteria - Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 – Evaluation Methodology CCMB-2012-09-004, September 2012. |

1.4.2 RFCs and other standards supported

- | | |
|--------|---|
| [DSCP] | K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, RFC 2474, December 1998. |
| [ESP] | Kent, S. and R. Atkinson, <i>IP Encapsulating Security Payload (ESP)</i> , RFC 2406, November 1998. |
| [ICMP] | Postel, J., Internet Control Message Protocol - DARPA Internet Program Protocol Specification, RFC 792, USC/Information Sciences Institute, September 1981. |
| [IP] | P. Almquist, Type of Service in the Internet Protocol Suite, RFC 1349, July 1992. |
| ITSEC] | <i>Critères d'évaluation de la sécurité des systèmes informatiques</i> Commission des Communautés Européennes, version 1.2, juin 1991. |
| [TCP] | Postel, J., <i>Transmission control protocol</i> , STD 7, RFC 793, September 1981. |
| [UDP] | Postel, J., <i>User Datagram Protocol</i> , STD 6, RFC 768, August 1980. |

1.5 Glossary

TOE

Target of Evaluation

ST

Security target

IT

Information technology

EAL

Evaluation Assurance Level.

SFR

Security Functional Requirement

TSF

TOE Security Function

CEM

Common Evaluation Methodology for information technology security

CC

Common Criteria for the evaluation of security.

Administrator

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

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 **filter policy**. This is the device on which the core of the Stormshield Firmware's security functions run.

Local console

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

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 filter 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.

Pseudo-connection

1^o) 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').

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).

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**.

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.



2 DESCRIPTION OF THE TARGET OF EVALUATION

The aim of this section is to expand on the concepts that will be used later in presenting the security issues addressed by the TOE, the security objectives and security requirements of the TOE. It will also serve to specify the scope and limits of the evaluation.

2.1 IT security characteristics of the TOE

2.1.1 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 Firmware**, in the context of the evaluation, aims to meet the technical requirements of information flow control through advanced filter features.

2.1.2 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**.

Depending on individual cases, the rules of such **filter policies** may be expressed in more or less sophisticated criteria: source and destination IP addresses, number of the IP protocol used, source/destination TCP/UDP port, time of the day and day of the week, **user** identity, prior authentication, etc.

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

- Filtering of information flows between appliances, based on IP and transport characteristics: IP protocol number, source and destination IP addresses, source and destination TCP/UDP ports.
- Traceability of information flows to entities that initiated it through the generation of audit data.

2.1.3 Protection against log saturation

Monitoring information flows between trusted networks and the **uncontrolled network** makes it possible to deny obvious attempts to establish information flows considered illicit with respect to the **filter policy**.

Attempts to establish information flows can be logged in order to allow future audits. Protection against flooding caused by the writing of such logs is implemented, which consists in blocking such flows once they can no longer be logged.

Flows that need to be logged would therefore be unable to pass through the **filter feature** following a log flooding attempt.

2.1.4 *Risks of improper use*

The definition of a **filter 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.

The greatest risk is the definition of a wrong **filter policy**. Indeed, the fact that a **filter policy** has been incorrectly defined may create possibilities for attacks. Such risks can be countered by the fact that the **administrator** defining the **filter policy** is presumed to be a qualified non-hostile person who has been trained in performing such tasks.

The “**super-administrator**”, who acts only during installation and maintenance phases, and is the only person authorized to connect to the **local console**.

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

2.1.5 *Protection of the TOE itself*

Assuming that the security functions of the TOE are effective in implementing the network security policy, 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 filter function 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 (premises with controlled access, prohibition from using a **local console** during production, etc.).

2.2 Physical limits of the TOE

2.2.1 Appliances that comprise the TOE

A platform operating the TOE is made up of **Stormshield appliances** on which the **Stormshield UTM / NG-Firewall Firmware** runs. These appliances implement the filter functions (the TOE) between the various sub-networks linked to their interfaces,

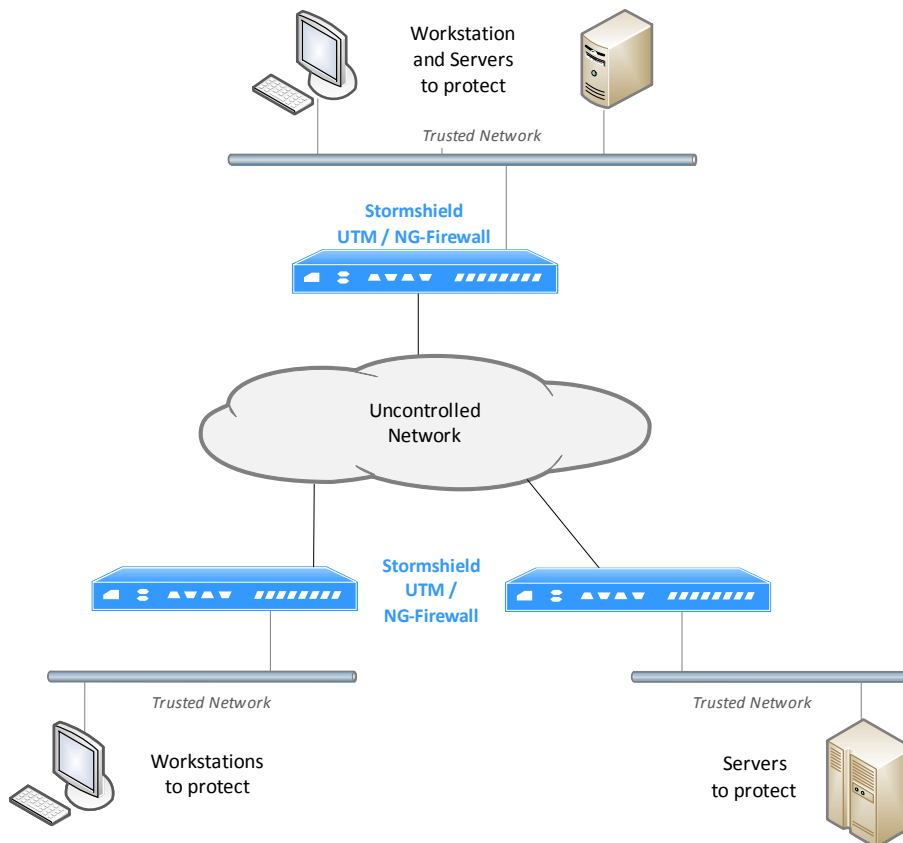


Illustration 1: Example of use of the TOE.

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

2.2.2 Minimum characteristics of operating platforms

Stormshield appliances are fully packaged by Stormshield. They are developed around the FreeBSD 9.3 kernel, with up-to-date patches that are adapted and refined by Stormshield.

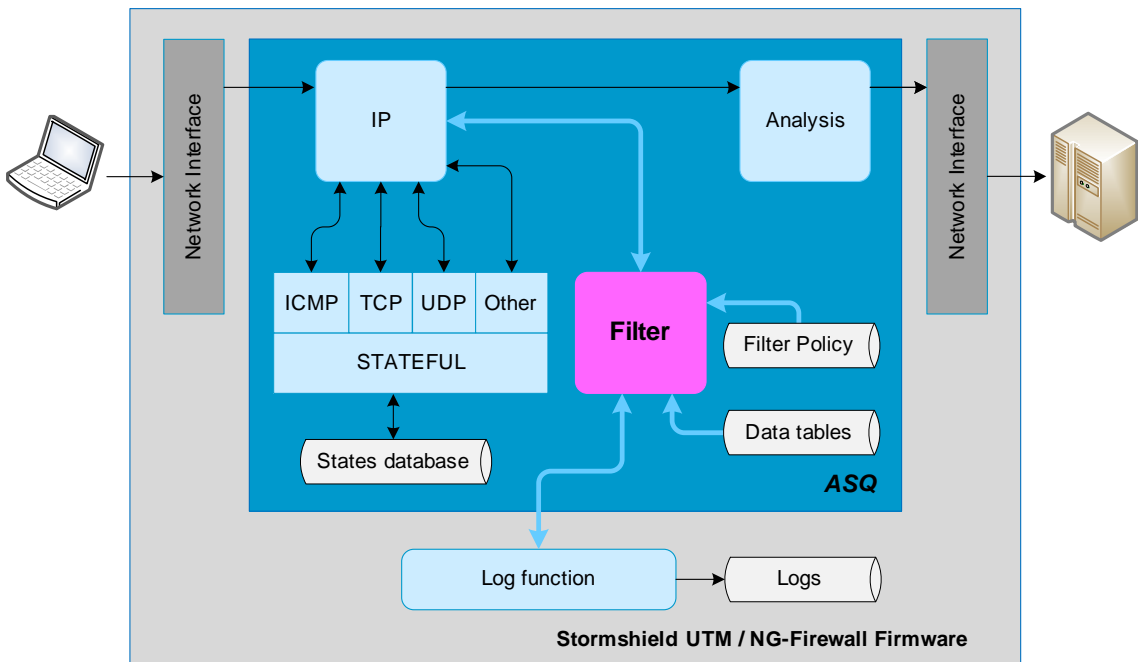
Take note that only the software portion, and not the hardware, is subject to evaluation.

2.3 Logical limits of the TOE

The perimeter of the evaluation covers the **"Filter"** function included in the ASQ module in version 2.2 of the **Stormshield UTM / NG-Firewall Firmware**, which is installed on Stormshield appliances from the SN150 to the SN6000 ranges (S, M, L and XL builds).

2.4 Architecture and interfaces of the TOE

A TOE in operation is a software element included on Stormshield appliances. The figure below sets out the TOE in its environment.



Caption:






-  Software suite containing the TOE
-  Software environment of the TOE
-  TOE
-  External interface
-  Logical link

Illustration 2: Components and interfaces of the TOE.

2.5 Configurations and usage modes subject to the evaluation

The usage mode subject to evaluation has the following characteristics:

- The evaluation covers the **filter function** on the Stormshield UTM / NG-Firewall Firmware which is installed on all versions of Stormshield appliances. The Firmware is available in 4 distinct compilations (S, M, L and XL builds) according to the appliance's position in the product range.
- 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 **filter policy** used by the **filter function** has been correctly configured and installed. These actions are performed by a trained, qualified and non-hostile **administrator**.
- **Data tables** (tables of interfaces, groups of source IPs, groups of destination IPs) used by the **filter function** have been correctly initialized and filled in by the Stormshield appliance.
- Software modules in the **filter function**'s environment and the environment itself have been correctly configured and are operational.
- 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;
- The usage mode subject to evaluation excludes the fact that the TOE relies on the services provided by version 2.2 of the Stormshield UTM / NG-Firewall Firmware or outside of it.

2.6 Test platform used during the evaluation

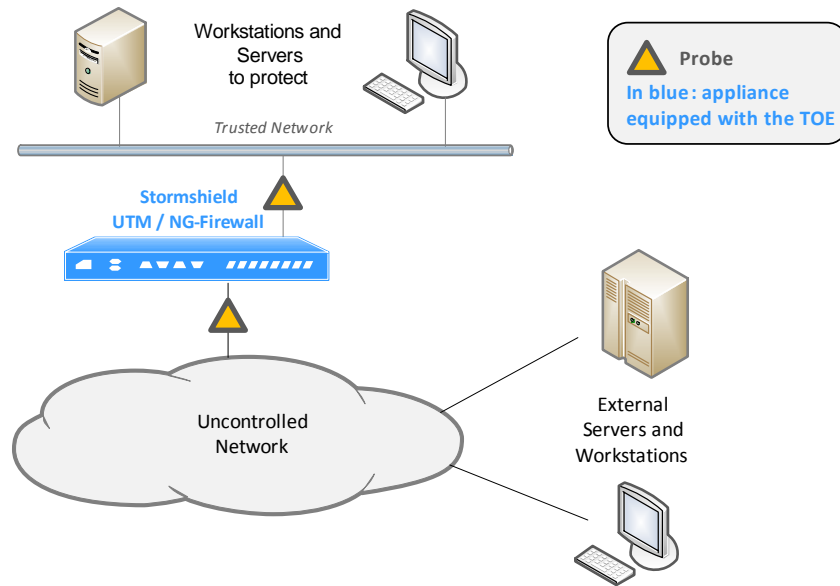


Illustration 3: Test platform used during the evaluation.

The Stormshield appliance is an SN200 or SN910.

Laptops equipped with “probe” programs are used for listening on information flows in order to gauge the compliance of the Stormshield appliance’s behavior at the network interface level. They may be connected at various points on the network.

These laptops will also be used for conducting penetration testing by counterfeiting packets.

3 SECURITY ENVIRONMENT OF THE TARGET OF EVALUATION

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 convention used for naming assumptions, threats and policies:

- Assumptions 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.
- Threats 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 **filter policy** to be implemented globally in the information system (cf. AO.GOOD_PF):

- Application services offered by servers of trusted networks (confidentiality, integrity and availability);
- Programs launched on devices in trusted networks (servers, browsers, etc.), and the configuration of such programs (integrity and confidentiality);
- Network topology information (confidentiality), against probe attempts.

3.2.2 Assets belonging to the TOE

In the purpose of protecting these sensitive assets, the software environment that interacts with the TOE correctly meets its objectives (e.g.: confidentiality and integrity of the configuration).

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

TSF-Data is made up of:

- the **filter policy** that the TOE uses,
- data tables,
- logged data of security events.

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).

P.AUDIT

The TOE must log filter events (including information flows and denials) that the **administrator** has deemed sensitive.

3.3.2 Risks of improper use

T.IMPROPER_USE

The security functions of the TOE do not behave in harmony with the internal security policy (cf. §2.1.1), 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**.

3.3.3 Protection of the TOE itself

T.ILLEGAL_ADMIN

An **entity** belonging or not to the **trusted network** manages to perform illegal administration operations that would undermine the filter policy and associated data tables.

T.AUDIT_LOSS

An **entity** belonging or not to the **trusted network** prevents security events from being logged by depleting the TOE's capacity for logging these events, with the purpose of masking an external hacker's illegal actions.

3.4 Assumptions

3.4.1 Assumption 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 Assumption on organizational security measures

AO.GOOD_PF

The **filter policy** to be implemented, for all appliances on the trusted networks to be protected, are defined as such:

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

3.4.3 Assumption 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 competence allows them to build a coherent **filter policy** that complies with the state of the art in the field as defined in §3.3.2.

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 **filter 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.INTEGRITY

The software environment that interacts with the TOE is considered safe and trusted and cannot be used as a means to corrupt the TOE or its configuration.

AIT.LOG

Version 2.2 of the Stormshield UTM / NG-Firewall Firmware provides the TOE with a secure log service that formats, timestamps and records audit data.

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 convention 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.

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 (§4.4).

4.3 Information flow control objectives

O.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 and UDP: type of service,
- Type of DSCP service.

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



O.AUDIT

The TOE must:

request the generation of audit data relating to events that have to do with the application of the **filter policy**, in view of processing them with the log function that will format, timestamp and save them.

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

O.AUDIT_LOSS

The TOE must:

make it possible to prohibit traffic for which a request to generate audit data is required even when it cannot be performed.

Rationale: O.AUDIT_LOSS is mainly dedicated to the prevention of the threat T.AUDIT_LOSS.

4.4 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 T.ILLEGAL_ADMIN. It eliminates the possibilities of performing **illegal security administration operations** from local access to Stormshield appliances.*

OE.GOOD_PF

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

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

OE.PERSONNEL

Objective making it possible to ensure the reality of the assumption AO.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 satisfy the rules of the security policy associated with information flow control, since it allows preventing the bypass of security functions dedicated to these objectives by prohibiting the setup of information flows subject to the **filter policy** 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 **filter policy** in a manner similar to OE.INTERPOSITION.*



OE.INTEGRITY

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

Rationale: This security objective supports the implementation of the policies P.FILTERING and P.AUDIT by ensuring that software and other services running on the product outside the scope of the TOE are reliable and allow the TOE to be correctly executed.

OE.LOG

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

Rationale: This security objective supports the implementation of the policy P.AUDIT by ensuring that audit data is generated and saved. It also participates in countering the threat T.AUDIT_LOSS by reporting to the TOE each time there is a request to save audit data or a specific error when logs are saturated.

4.5 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.AUDIT	T.AUDIT_LOSS	T.ILLEGAL_ADMIN	T.IMPROPER_USE	AP.PROTECT_APPLIANCES	AO.GOOD_PF	AH.PERSONNEL	AIT.INTERPOSITION	AIT.STRICT_USAGE	AIT.INTEGRITY	AIT.LOG
O.FILTERING	X											
O.AUDIT		X										
O.AUDIT_LOSS			X									
OE.PROTECT_APPLIANCES				X		X						
OE.GOOD_PF					X		X					
OE.PERSONNEL					X			X				
OE.INTERPOSITION	S	S							X			
OE.STRICT_USAGE	S	S		X						X		
OE.INTEGRITY	S	S									X	
OE.LOG		S	S									X

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.



5 IT 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 IT 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 *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, §7, 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.

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:

FCC_FFF.component.n

- FCC 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;
- n is the item number.

5.1.2 *Presentation of security data*

Attributes of IP packets concerned by filter 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;
- The IP protocol number;
- The value of the DSCP field;
- The source and destination TCP/UDP port or the type of ICMP message.

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) (name, IP address, port) 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 destination machine(s) (name, IP address, port, name associated with the port) of 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 associated with the rule;
- The profile of Internet attacks associated with connections covered by the rule.

Data tables

In the following description of data tables, we will only set out the information from various tables that is essential to the proper operation of the TOE.

Interface table

- Interface's unique identifier;
- Number of valid IP addresses on the interface;
- List of valid IP addresses on the interface.

Table of source IP groups

- Group's unique identifier;
- Name of the group;
- Number of IP addresses contained in the group;
- List of IP addresses contained in the group.

Table of destination IP groups

- Group's unique identifier;
- Name of the group;
- Number of IP addresses contained in the group;
- List of IP addresses contained in the group.

Profile of audit logs

- indicates the group of the rule that activated logging;
- identifier of the rule that activated logging;
- internal name of the source machine's interface;
- name of the object representing the source machine's interface;
- internal name of the destination machine's interface;
- name of the object representing the destination machine's interface;
- type of network protocol (tcp or udp);
- name of the associated plugin, otherwise the name of the standard service corresponding to the destination port;
- IP address of the source machine;
- name of the object corresponding to the IP address of the source machine;
- service's source port number;



- name of the object corresponding to the source port;
- IP address of the destination machine;
- name of the object corresponding to the IP address of the destination machine;
- service's destination port number;
- name of the object corresponding to the destination port;
- behavior associated with the filter rule.

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 7, 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

Filter function

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 to satisfy O.FILTERING, by defining the **filter policy** and requiring that it applies to all **incoming IP packets**.*

FDP_IFF.1 – Filter function

[FDP_IFF.1.1]

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,**

[FDP_IFF.1.2]

The filter function must authorize an **incoming IP packet** if the **action of the first applicable rule is 'pass'**.

[FDP_IFF.1.3]

The filter function must apply 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 filter rules whose action is 'delegate' serve only to skip the evaluation of the end of the global filter policy to go back to the beginning of the local filter policy and are not taken into account in packet filtering.



[FDP_IFF.1.4]

The filter function must explicitly authorize an incoming IP packet if implicit filter rules have been associated with it.

[FDP_IFF.1.5]

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 rule has allowed the packet.**

Rationale: FDP_IFF.1 is dedicated to the satisfaction of the objective O.FILTRAGE.

Audit data generation function

FAU_GEN.1 – Generation of audit data

[FAU_GEN.1.1]

The **audit data generation function** must be able to request the logging of the following auditable event:

Application of a filter rule for which the generation of an audit log has been specified.

[FAU_GEN.1.2]

The **audit data generation function** must be able to request the logging of the following information in each audit log:

- a. **IP address and source port,**
- b. **IP address and destination port,**
- c. **names of source and destination interfaces,**
- d. **identifier of the Stormshield appliance,**
- e. **protocol type and ICMP,**
- f. **rule ID,**
- g. **action applied**

Rationale: FAU_GEN.1 is dedicated to the satisfaction of the audit data generation aspects of the objective O.AUDIT.

Refinement: The TOE is only concerned with part of the requirement, in particular, using the Firmware's logging service, which is itself outside the scope of the TOE.

Refinement of FAU_GEN.1.1: The log function, which is outside the scope of the TOE, logs its startup and shutdown. However, the audit data generation function does not have an actual concept of starting up and shutting down.

Refinement of FAU_GEN.1.2: The log function, which is outside the scope of the TOE, has a timestamping mechanism, which is itself outside the scope of the TOE.

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

[FAU_STG.3.1]

The filter function must **block incoming IP packets that need to be logged according to the filter policy** if the **amount of logs** exceeds the **following number of elements to be logged**:

- a. **S build: 100**
- b. **M build: 256**
- c. **L build: 512**
- d. **XL build: 1024**

Rationale: FAU_STG.3 is dedicated to the satisfaction of the objective O.AUDIT_LOSS.



5.3 Security assurance requirements for the TOE

This section sets out the refinement of the TOE’s assurance requirements. The formal description of these requirements is given in Chapter 7.

The level of assurance that the TOE aims for is an augmented EAL4 for the component ALC_FLR.3

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

Components		Comments
ADV_ARC.1	Security architecture description	EAL4
ADV_FSP.4	Formal 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.

	O.FILTERING	O.AUDIT	O.AUDIT_LOSS
FDP_IFC.2	S		
FDP_IFF.1	X		
FAU_GEN.1		X	
FAU_STG.3			X

X: the security requirement meets the objective.
S: the security requirement supports the objective.

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	Yes
FDP_IFF.1	FDP_IFC.1	Yes, via 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.
FAU_GEN.1	FPT_STM.1	Not applicable. The requirement FAU_GEN.1 relating to the preparation of recording logs with timestamps is outside the scope of the TOE.
FAU_STG.3	FAU_STG.1	Not applicable. The requirement FAU_STG.3 relating to the protection of log recordings is outside the scope of the TOE.



5.4.4 *Satisfaction of SAR dependencies*

The level of assurance that this security target aims for is EAL4+ (or augmented EAL4) for the component ALC_FLR.3, which does not have any dependencies.

The dependencies required by the CC pour assurance components included in the EAL4 package have all been preserved.



6 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.

6.1 IT security functions

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

6.1.1 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 **incoming IP packet** received against the criteria of each rule in the **filter policy**. Filtering applies to all **incoming IP packets**. 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 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 **user** or **user group** allowed by the rule.

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

Each filter rule may specify a control action and audit data generation action. The latter is described in §6.1.2.

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 a TCP RST (for TCP) or ICMP unreachable (for UDP) signal will be sent to the sender;
- 'none': the packet is compared against the rules that follow (used only for specifying an audit data generation action).
- 'delegate': the packet is compared against filter rules in the **local filter policy** (allows going through the evaluation of the **global filter policy** in order to allow delegating a subset of it to a local **administrator** via the **local filter policy**). This action is only available for rules in the **global filter policy**.

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**), the Stormshield appliance only compares the initial packet from the exchange against rules of the current **filter policy**. Upon receiving any IP packet, prior to the application of rules from the **filter policy**, the packet will be compared against currently established connections / **pseudo-connections**. If the

attributes and parameters of the packet correspond to the criteria and status of one of these connections / **pseudo-connections**, 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) without having to define a filter rule in both directions on the firewall.

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

6.1.2 **Audit data generation function**

The Stormshield appliance simultaneously manages several log files meant for gathering events detected by the log function. More specifically, there is a file dedicated to logging events relating to the application of the filter function (Filter file).

The audit data generation function (subset of the TOE) sends logging requests to the log function (which is outside the scope of the TOE) through a message queue that has a set capacity for the number of elements to log according to appliance builds:

- S build: 100
- M build: 256
- L build: 512
- XL build: 1024

When these capacities are exceeded, the filter function will block traffic in order to prevent logs from being lost.

The audit data generation function provides the following information to the log function:

- IP address and source port,
- IP address and destination port,
- names of source and destination interfaces,
- identifier of the Stormshield appliance,
- protocol type and ICMP,
- rule ID,
- action applied.

Rationale: the audit data generation function satisfies FAU_GEN.1. Limits on the size of the message queue and the associated actions satisfy the requirement FAU_STG.3.



7 APPENDIX – 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.2.3.C. It must be considered “the list of OT security requirements provided as part of the ST”, required by ASE_REQ.2.1D,

7.1 Introduction

In addition to the four types of operations defined in the Common Criteria (cf. [CC-01], § C.2, 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.

Les opérations ont été effectuées sur le texte anglais original des exigences de sécurité des TI, mais elles ont pour effet de remplacer ces termes anglais par des termes français, et/ou à ajouter des termes français à un patron original en anglais. Malgré leur difficulté d’emploi, ces exigences en « franglais » constituent en tout état de cause l’élément de preuve requis par l’élément ASE_REQ.2.1D, alors que les exigences énoncées au §5.2 du présent document ne sont qu’une reformulation du contenu de cette section, fournie dans le but de faciliter la compréhension de l’énoncé des exigences de sécurité des TI.

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 §5.1.1.

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.

7.2 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.

7.2.1 Information flow control requirements

Filter function

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	<i>information flow control SFP:= the filter policy</i>
Assignment	<i>list of subjects and information:= devices on networks interconnected by the Stormshield appliance (subjects) and IP packets (information)</i>
Refinement	<i>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</i>
Layout	<i>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</i>

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	<i>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</i>
Refinement	<i>an information flow control SFP:= the filter policy</i>

FDP_IFF.1 – Filter function

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

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	<i>information flow control SFP:= the filter policy</i>
Refinement + layout	<i>subject and information:= devices on networks interconnected by the Stormshield appliance (subjects), IP packets (information) → Incoming IP packets</i>
Assignment	<i>list of subjects and information controlled under the indicated SFP, and, for each, the security attributes :=</i> <ol style="list-style-type: none"> 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.

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 := 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 filter rules whose action is 'delegate' serve only to skip the evaluation of the end of the global filter policy to go back to the beginning of the local filter policy 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 := if there are implicit filter rules associated with this incoming IP packet
------------	--

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.
------------	--

Audit data generation function

FAU_GEN.1 – Generation of audit data

Systematic refinement	The TSF:= the audit data generation 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 := application of a filter



rule for which the generation of an audit log has been specified.

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	<i>subject identity</i> := source IP address, and identity of the user (if known)
Assignment	<i>other audit relevant information</i> := the following complementary audit information: a. IP address and source port, b. IP address and destination port, c. names of source and destination interfaces, d. identifier of the Stormshield appliance, e. protocol type and ICMP, f. rule ID, g. action applied.

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

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].

Refinement	<i>The TSF</i> := the filter function
Refinement	<i>audit trail</i> := amount of logs
Assignment	<i>actions to be taken in case of possible audit storage failure</i> := block incoming IP packets that need to be logged according to the filter policy.
Assignment	<i>pre-defined limit</i> := the following number of elements to be logged: a. S build: 100 b. M build: 256 c. L build: 512 d. XL build: 1024