Direction centrale de la sécurité des systèmes d'information

Protection Profile
IP Interconnection Firewall

Version	:	3.0f
Date	:	June 2008
Classification	:	Public
Reference	:	PP-FWIP

Courtesy Translation

Courtesy translation of the protection profile registered and certified by the French Certification Body under the reference DCSSI-PP-2008/02.

Document history

Version	Date	Status	Modifications
2.0	July 2005	Reference document for launching the evaluation	
2.0a	September 2005	Reference document for launching the evaluation after proofreading and factoring in comments	See document *PP-FWIP-2_0-Fiche-Commentaires-Réponses DCSSI-ARKOON.doc.*
2.0b	September 2005	Reference document for launching the evaluation	"Sensitive data" became "Sensitive assets" Factoring in of remote administration and of the integrity of data exchanged with the TOE via FPT_TDC.
2.1	October 2005	Reference document for launching the evaluation	Update of audit levels.
2.2	March 2006	Document revised following the recommendations of the MELEZE_APE_1.1 evaluation report	
3.0	April 2008	Reference document for validation	Update of the "IP interconnection firewall" protection profile from Common Criteria version 2.3 to version 3.1r2. Modification of the remote administration function at the DCSSI's request.
3.0a	April 2008	Reference document for launching the evaluation	Factoring in of the DCSSI's comments following validation proofreading.
3.0b	May 2008	Reference document for evaluation	Deletion of OSP.EAL & O.EAL at the DCSSI's request.
3.0c & 3.0d	May 2008	Reference document for evaluation	Factoring in of comments made in the ETR.
3.0e & 3.0f	June 2008	Reference document for evaluation	Factoring in of comments made in the review file of the APE report, issued by the DCSSI.

Table of contents

Figures

Tables

1 Introduction

1.1 Protection profile reference

Title:	Protection Profile - IP Interconnection Firewall
Author:	FIDENS
Version:	3.0f

1.2 Context

This PP has been drawn up under the aegis of the *Direction Centrale de la Sécurité des Systèmes d'Information* (DCSSI).

The aim is to provide an administrative framework for the certification of IP interconnection firewalls to meet the requirements of the public and private sectors with a view to qualification.

The update of this protection profile from Common Criteria version 2.3 to version 3.1r2 was carried out by FIDENS. The previous version of this protection profile was drawn up by ARKOON.

1.3 General overview of the Target of Evaluation (TOE)

Note: a detailed description of the TOE can be found in Appendix A.

1.3.1 TOE type

This protection profile (PP) presents the security objectives and the functional and assurance requirements for a Target of Evaluation (TOE) for a firewall used to filter data flow within the scope of IP network interconnection.

This firewall is a hardware device placed between an IP network to be protected and another IP network. This device can be managed locally or from a remote administration workstation.

Application note

If a software client designed to manage and monitor the firewall is delivered with this firewall, this software client must be included in the scope of the TOE.

1.3.2 Usage and major security features of the TOE

This TOE is designed to support the security policy governing the interconnection of a protected network with another network. Its purpose is to maintain the protected network's

security level after interconnection, and to protect it from attack from the other network by controlling flow transiting to and from this network.

The main functions or the TOE involve:

- The application of a filtering policy
- The audit and the logging of data flows and of the implementation of the filtering policy

The implementation of this filtering policy is based on filtering rules to ensure:

- Non-contextual filtering: the filtering action (acceptance, blocking, rejection, with logging or otherwise) is determined according to the content of a network packet;
- Contextual filtering: following an initial non-contextual filtering, the TOE establishes a context and appropriate filtering rules according to the nature of the identified data flow (origin, destination, protocols, etc.). Knowledge of this context allows the TOE not only to gain in performance, but also to increase the pertinence and accuracy of filtering.

TOE filtering features, contextual or otherwise, concern only data flow over IP and take into consideration network and transport layers.

Moreover, for it to operate correctly, the TOE implements the following services:

- Filtering policy management:
  - Filtering policy definition
  - Filtering rules access control
- Protection of administrative and monitoring operations:
  - Local authentication of administrators
  - Assistance in the protection of remote administration flow
  - Protection of monitoring flow
- Audit of administration and monitoring operations:
  - Audit and logging of administrative operations
  - Generation of security alarms
  - TOE supervision
- Protection of access to TOE configuration parameters (network configuration parameters, authentication data, access rights)

1.3.3 Specific conditions and security specificities of the TOE

This PP was drafted in accordance with the expectations and recommendations of the [QUA-STD] document. This document defines the standard level as being an initial level of robustness corresponding to a product able to withstand an attacker with a basic attack potential as defined by the Common Criteria.

A security target (ST) claiming conformance to the PP may have additional features that are not covered by this PP: IP encryption, authentication server, anti-virus gateway, etc. These additional features and their implementation must not conflict with the requirements of this

PP. During the drafting of a security target claiming conformance to this protection profile, these features may be expressed and, where necessary, reference may be made to all other relevant protection profiles (e.g. [PP-CIP]).

1.3.4 Hardware and software environment

TOE administration and monitoring security is dependent on its environment, particularly the workstations used for the purposes of remote administration.

This environment shall:

- Be built around trusted remote administration workstations
- Contribute to the security of data transfer between remote administration workstations and the TOE

2 Conformance claims

2.1 Conformance of this protection profile

2.1.1 Conformance with the Common Criteria

This protection profile conforms with:

- Part 2 of the Common Criteria, Version 3.1, Release 2, dated September 2007 (see [CC2])
- Part 3 of the Common Criteria, Version 3.1, Release 2, dated September 2007 (see [CC3])

No recourse has been made to extension or interpretation.

2.1.2 Conformance with an assurance package

This PP defines a set of assurance requirements corresponding to the EAL3 package augmented with the following components:

- ALC_FLR.3
- AVA_VAN.3

This level of security assurance conforms with the DCSSI reference document *Processus de qualification d'un produit de securite - niveau standard*, see [QUA-STD]).

2.1.3 Conformance with a protection profile

This protection profile is not dependent on any other protection profile.

2.2 Conformance of security targets and protection profiles

This PP requires "**demonstrable**" conformance of the PP or ST claiming conformance to this PP.

Application notes detail which assumptions can be partially or completely transformed into an OSP by the STs and PPs in conformity with this PP. These application notes are shown for the assumptions concerned.

3 Security problem definition

3.1 Assets

Each asset description outlines the types of protection required (entitled Protection).

3.1.1 Assets protected by the TOE

When the type of protection (entitled *Protection*) is followed by "(opt.)", for optional, this means that although protection shall be provided by the TOE, it is not systematically applied by the TOE.

D.PROTECTED_NETWORK_DATA

The TOE helps to protect the user information and service assets of the protected network by filtering flows likely to access or to modify these assets.

Protection: confidentiality (opt.), integrity (opt.) or availability (opt.)

3.1.2 Sensitive assets of the TOE

D.FILTERING_POLICY

Processing (filtering and security controls) to be carried out by the firewall on IP packets is determined according to filtering policies and connection contexts.

This includes the audit policy of user flows.

Protection:

- authenticity when the policies (and their contexts) travel from the place the administrator defines them remotely to the firewall
- integrity of policies (and contexts) stored on the firewall
- coherence between the defined policy (and its context) and that applied
- confidentiality

D.DATA_FLOW_AUDIT

Data generated by the audit policy for logging the data flow processed by the firewall.

Protection: integrity

D.CONFIGURATION_PARAMETER

Among others, firewall configuration parameters include:

- the internal IP addresses of protected networks and routing tables (network configuration)
- authentication and integrity data
- access rights
- the audit policy for administrative operations

Protection: confidentiality and integrity

D.ADMIN_AUDIT

Data generated by the audit policy for logging administrative operations carried out on the TOE.

Protection: integrity

D.ALARMS

Security alarms generated by the TOE to warn about or identify a possible security violation.

Protection: integrity

3.2 Threats

The standard level qualification policy applies to products destined for the general public aimed at ensuring the security of restricted data which are not "defence-classified data". Consequently, a certain number of threats are not taken into account in the rest of the PP, like for example the theft of equipment (which shall be detected by organisational measures) or denial of service.

The various threats agents are:

- internal attackers: any authorised user of the protected network
- external attackers: any person external to the protected networks

In compliance with A.ADMIN, administrators are not considered as potential attackers of the TOE.

3.2.1 Threats impacting the operation of the TOE

T.MALFUNCTION

An attacker places the TOE into a state of malfunction, as a result of which the services offered by the TOE may become unavailable or its state untrusted.

Threatened assets: D.PROTECTED_NETWORK_DATA, D.FILTERING_POLICY, D.DATA_FLOW_AUDIT, D.CONFIGURATION_PARAMETER, D.ADMIN_AUDIT, D.ALARMS

3.2.2 Threats to the filtering policy

T.FILTERING_POLICY_ALTERATION

An attacker illegally modifies the filtering policy and/or connection contexts.

Threatened asset: D.FILTERING_POLICY

T.FILTERING_POLICY_DISCLOSURE

An attacker illegally retrieves the filtering policy and/or connection contexts.

Threatened asset: D.FILTERING_POLICY

3.2.3 Threats to configuration parameters

T.PARAMETER_ALTERATION

An attacker illegally modifies the configuration parameters of the TOE.

Threatened asset: D.CONFIGURATION_PARAMETER

T.PARAMETER_DISCLOSURE

An attacker illegally gains access to TOE configuration parameters.

Threatened asset: D.CONFIGURATION_PARAMETER

3.2.4 Threats to the audit trail

T.FLOW_AUDIT_ALTERATION

An attacker illegally modifies or deletes flow audit event records.

Threatened asset: D.DATA_FLOW_AUDIT

3.2.5 Threats to alarms

T.ALARM_ALTERATION

An attacker illegally modifies or deletes alarms when they are returned by the TOE to the security administrator.

Threatened asset: D.ALARMS

3.2.6 Threats to the administration audit trail

T.ADMIN_AUDIT_ALTERATION

An attacker illegally modifies or deletes administration audit event records.

Threatened asset: D.ADMIN_AUDIT

3.2.7 Threats to all assets during the reuse of the TOE

T.CONTEXT_SWITCHING

An attacker or an administrator of a new protected network becomes aware, as a result of direct access to the TOE, of the TOE's sensitive assets during a change in the usage context (using the firewall with a new network, maintenance, etc).

Threatened assets: D.PROTECTED_NETWORK_DATA, D.FILTERING_POLICY, D.DATA_FLOW_AUDIT, D.CONFIGURATION_PARAMETER, D.ADMIN_AUDIT, D.ALARMS

3.3 Organisational security policies

The organisational security policies presented in this section make it possible to define the services provided by the TOE for the information system and the constraints to be satisfied for security products to achieve Standard level Qualification from the SGDN/DCSSI.

3.3.1 Policies relative to the provided services

OSP.FILTERING_POLICY_APPLICATION

The TOE shall apply the filtering policy defined by the security administrator on the basis of the security policy of the information system.

In contextual mode, the TOE shall be able to establish and apply filtering rules based on the characteristics of the processed flows (e.g. origin, destination, applied protocol).

The TOE shall also allow the current filtering rules to be viewed.

OSP.FLOW_AUDITING

The TOE shall track the flows it processes in such a way as to:

- record as a minimum the events generated when a flow is rejected
- enable the administrator to put the recorded events into chronological order
- enable the administrator to attribute an event to a particular user
- enable audit logs to be viewed and the recorded events to be selected in order to guarantee the relevance of the filtering policy and its correct instantiation at the level of the firewall

OSP.ROLES

The TOE shall make it possible to define different security officer, security administrator, auditor, system and network administrator roles.

It shall also provide an audit trail of actions undertaken by these roles.

3.3.2 Policies taken from applicable regulations

OSP.CRYPTO

The DCSSI cryptography reference document ([CRYPTO]) shall be respected for the management of keys (generation, destruction, usage and distribution) and for the cryptography functions used in the TOE for the standard level of resistance.

3.4 Assumptions

3.4.1 Assumptions concerning the expected usage of the TOE

A.AUDIT

It is assumed that the auditor regularly consults the audit events generated by the TOE. The memory storing these audit events is managed in such a way that administrators do not lose events.

A.ALARM

It is assumed that the security administrator analyses and processes the security alarms generated and returned by the TOE.

3.4.2 Assumptions concerning the environment in which the TOE is used

A.ADMIN

Administrators are non-hostile persons. They have the necessary resources for undertaking their tasks, are trained to carry out the operations for which they are responsible and follow the administration manuals and procedures.

As a result of this hypothesis, these administrators are not considered attackers as far as the threats identified in this document are concerned.

A.SECURE_SITE

Equipments containing TOE services (firewall), administration equipments and media containing sensitive TOE assets (paper, diskettes, back-ups, etc.) shall be located in secured premises to which there is controlled access that is restricted to administrators.

Equipments that do not contain sensitive assets may be located in non-secure premises: e.g. in the event of changes in a firewall's usage context.

A.CONFIGURATION_CONTROL

The administrator has resources for controlling the hardware and software configuration of the TOE in relation to a reference state or to reproduce a trusted state.

This assumption extends to the control of the "Filtering policy" sensitive asset when the TOE cannot guarantee its integrity alone.

A.TRUSTED_ADMIN_WS

The workstations used by administrators to manage the TOE remotely are trusted.

4 Security objectives

4.1 Security objectives for the TOE

4.1.1 Objectives for security services provided by the TOE

O.FILTERING_POLICY_APPLICATION

The TOE shall apply the filtering policy specified by the administrator and the filtering rules established by the TOE (contextual mode). This policy can concern both user flows and administration flows.

O.POLICY_VISUALISATION

The TOE shall enable security administrators to view unitarily the filtering policy and connection contexts present on the firewall.

O.POLICY_CONSISTENCY

In the event of remote administration, the TOE shall guarantee coherence between filtering policy definition and policies applied on the firewall.

O.FLOW_AUDIT

The TOE shall log the flows it processes in such a way as to:

- record as a minimum the events generated when a flow is rejected
- enable the administrator to put the recorded events into chronological order
- enable the administrator to attribute an event to a particular user
- enable audit records to be viewed and the recorded events to be selected in order to guarantee the relevance of the filtering policy and its correct instantiation at the level of the firewall

O.ROLES

The TOE shall enable various roles to be defined and associate users' roles in a trusted manner.

4.1.2 Security objectives for operating the TOE

4.1.2.1 Protection of the filtering policy

O.FILTERING_POLICY_PROTECTION

The TOE shall control access (consultation, modification) to the filtering rules and to connection contexts on the firewall.

4.1.2.2 Audit and alarms

Flows

O.FLOW_AUDIT_PROTECTION

The TOE shall control access on the firewall (consultation, modification) to the flow audit trail it records and shall enable an auditor to detect the loss of flow audit events (by using a counter for example).

Administration events

O.ADMIN_AUDIT

The TOE shall generate audit trails of operations carried out by firewall administrators. The TOE shall make it possible to visualise this audit trail.

The generation of audit trails shall make it possible to impute recorded administration events.

O.ADMIN_AUDIT_PROTECTION

The TOE shall control access on the firewall (consultation, modification) to the administration audit trail it records and shall enable an auditor to detect the loss of administration audit events (by using a counter for example).

Alarms

O.ALARM

The TOE shall generate security alarms in the event of an infringement of the TOE's sensitive assets.

O.ALARM_PROTECTION

The TOE shall control access on the firewall (consultation, modification) to the security alarms (for local or remote security administrators) that it generates and shall enable a security administrator to detect the loss of security alarms (by using a counter for example).

4.1.2.3 Protection of remote administration

O.ADMIN_FLOW_PROTECTION

The TOE shall contribute to guaranteeing the authenticity, integrity and confidentiality of remote administration flows. Confidential protection is not systematically applied if the data contained in the flows is not confidential.

The TOE shall also help protect flows from replay.

4.1.2.4 Configuration of the TOE

O.PARAMETER_PROTECTION

The TOE shall control access on the firewall (consultation, modification) to configuration parameters, access rights, authentication data and elements for managing the integrity of administration flows.

4.1.2.5 Monitoring of the TOE

O.TOE_MONITORING

The TOE shall allow the system and network administrator to consult its operational status.

O.MONITOING_IMPACT

The TOE shall guarantee that the monitoring service does not endanger its sensitive assets.

4.1.2.6 Reuse of the TOE

O.TOE_REUSE

The TOE shall provide a feature enabling it to make its sensitive assets unavailable before changes are made to its usage context: new usage, maintenance, etc.

4.1.2.7 Identification and authentication of administrators

O.ADMIN_AUTHENTICATION

The TOE shall ensure the identification and authentication of TOE administrators who connect to the TOE locally or from a remote administration workstation.

4.2 Security objectives for the operational environment

4.2.1 Security objectives for the design of the TOE

OE.CRYPTO

The DCSSI cryptography reference document ([CRYPTO]) shall be followed for the design and operation of the TOE, for the management of keys (generation, destruction, usage and distribution) and the cryptography functions used in the TOE for the standard level of resistance.

4.2.2 Security objectives for TOE usage

4.2.2.1 Physical environment

OE.SECURE_SITE

Equipment containing TOE services (firewall), administration equipments and media containing sensitive TOE assets (paper, diskettes, back-ups, etc.) shall be located in secured premises to which there is controlled access that is restricted to administrators.

4.2.2.2 TOE administration

OE.ADMIN

Administrators shall be trained for the tasks they must carry out on the TOE and be trustworthy.

OE.TRUSTED_ADMIN_WS

Workstations used by administrators to manage the TOE remotely shall be trusted.

They shall contribute to guaranteeing the authenticity, integrity and confidentiality of remote administration flows. Confidential protection is not systematically applied if the data contained in the flows are not confidential.

They shall also help protect flows from replay.

4.2.2.3 Management of audit trails and alarms

OE.AUDIT_ANALYSIS

The auditor shall regularly analyse audit events recorded by the TOE and act accordingly. The memory storing audit events is managed in such a way that administrators do not lose events.

Furthermore, audits shall be recorded and archived to limit the impact of accidental or intentional deletion.

OE.ALARM_PROCESSING

The security administrator shall analyse and process security alarms generated and returned by the TOE.

4.2.2.4 TOE control

OE.TOE_INTEGRITY

The administrator has resources for controlling the hardware and software configuration of the TOE in relation to a reference state or to reproduce a trusted state.

This objective extends to the control of the “Filtering policy” sensitive asset when the TOE cannot guarantee its integrity alone.

4.3 Rationale

4.3.1 Coverage of threats

4.3.1.1 Threats to the operation of TOE services

T.MALFUNCTION

In order to guard against threats, the TOE shall carry out:

- no action

In order to protect itself, the TOE shall carry out:

- no action

In order to detect a threat occurrence, the TOE shall:

- offer a monitoring service (O.TOE_MONITORING) while not exposing its sensitive assets (O.MONITOING_IMPACT)

In order to limit threat impact, the TOE shall:

- be able to be restored to a previously validated state (OE.TOE_INTEGRITY)

4.3.1.2 Threats to the filtering policy

T.FILTERING_POLICY_ALTERATION

In order to guard against threats, the TOE shall:

- be deployed in secure premises (OE.SECURE_SITE)
- be used by trustworthy administrators (OE.ADMIN)
- be managed from trusted workstations (OE.TRUSTED_ADMIN_WS)

In order to protect itself, the TOE shall:

- enable administration flows to be filtered (O.FILTERING_POLICY_APPLICATION)
- provide controlled access to its sensitive assets (O.FILTERING_POLICY_PROTECTION)
- protect remote administration flows (O.ADMIN_FLOW_PROTECTION)
- authenticate the TOE administrator (O.ADMIN_AUTHENTICATION)

In order to detect a threat occurrence, the TOE shall:

- generate audit trails and alarms (O.ADMIN_AUDIT, O.FLOW_AUDIT and O.ALARM) The security administrator shall analyse and process these alarms (OE.ALARM_PROCESSING)

In order to limit threat impact, the TOE shall:

- be able to be restored to a previously validated state (OE.TOE_INTEGRITY)

T.FILTERING_POLICY_DISCLOSURE

In order to guard against threats, the TOE shall:

- be deployed in secure premises (OE.SECURE_SITE)
- be used by trustworthy administrators (OE.ADMIN)
- be managed from trusted workstations (OE.TRUSTED_ADMIN_WS)

In order to protect itself, the TOE shall:

- enable administration flows to be filtered (O.FILTERING_POLICY_APPLICATION)
- provide controlled access to its sensitive assets (O.FILTERING_POLICY_PROTECTION)
- protect remote administration flows (O.ADMIN_FLOW_PROTECTION)
- authenticate the TOE administrator (O.ADMIN_AUTHENTICATION)

In order to detect a threat occurrence, the TOE shall:

- generate audit trails and alarms (O.ADMIN_AUDIT, O.FLOW_AUDIT and O.ALARM) The security administrator shall analyse and process these alarms (OE.ALARM_PROCESSING)

In order to limit threat impact, the TOE shall carry out:

- no action

4.3.1.3 Threats to configuration parameters

T.PARAMETER_ALTERATION

In order to guard against threats, the TOE shall:

- be deployed in secure premises (OE.SECURE_SITE)
- be used by trustworthy administrators (OE.ADMIN)
- be managed from trusted workstations (OE.TRUSTED_ADMIN_WS)

In order to protect itself, the TOE shall:

- enable administration flows to be filtered (O.FILTERING_POLICY_APPLICATION)
- provide controlled access to its sensitive assets (O.PARAMETER_PROTECTION)
- protect remote administration flows (O.ADMIN_FLOW_PROTECTION)
- authenticate the TOE administrator (O.ADMIN_AUTHENTICATION)

In order to detect a threat occurrence, the TOE shall:

- generate audit trails and alarms (O.ADMIN_AUDIT, O.FLOW_AUDIT and O.ALARM) The security administrator shall analyse and process these alarms (OE.ALARM_PROCESSING)

In order to limit threat impact, the TOE shall:

- be able to be restored to a previously validated state (OE.TOE_INTEGRITY)

T.PARAMETER_DISCLOSURE

In order to guard against threats, the TOE shall:

- be deployed in secure premises (OE.SECURE_SITE)
- be used by trustworthy administrators (OE.ADMIN)
- be managed from trusted workstations (OE.TRUSTED_ADMIN_WS)
- be reused when there is a change of context (O.TOE_REUSE)

In order to protect itself, the TOE shall:

- enable administration flows to be filtered (O.FILTERING_POLICY_APPLICATION)
- provide controlled access to its sensitive assets (O.PARAMETER_PROTECTION)
- protect remote administration flows (O.ADMIN_FLOW_PROTECTION)
- authenticate the TOE administrator (O.ADMIN_AUTHENTICATION)

In order to detect a threat occurrence, the TOE shall:

- generate audit trails and alarms (O.ADMIN_AUDIT, O.FLOW_AUDIT and O.ALARM) The security administrator shall analyse and process these alarms (OE.ALARM_PROCESSING)

In order to limit threat impact, the TOE shall carry out:

- no action

4.3.1.4 Threats to flow audit trails

T.FLOW_AUDIT_ALTERATION

In order to guard against threats, the TOE shall:

- be deployed in secure premises (OE.SECURE_SITE)
- be used by trustworthy administrators (OE.ADMIN)
- be managed from trusted workstations (OE.TRUSTED_ADMIN_WS)

In order to protect itself, the TOE shall:

- enable administration flows to be filtered (O.FILTERING_POLICY_APPLICATION)
- provide controlled access to its sensitive assets (O.FLOW_AUDIT_PROTECTION)
- protect remote administration flows (O.ADMIN_FLOW_PROTECTION)
- authenticate the TOE administrator (O.ADMIN_AUTHENTICATION)

In order to detect a threat occurrence, the TOE shall:

- enable the loss of audit records to be detected (O.FLOW_AUDIT_PROTECTION)

In order to limit threat impact, the TOE shall:

- rely on audit trail recording and archiving measures (OE.AUDIT_ANALYSIS)

4.3.1.5 Threats to alarms

T.ALARM_ALTERATION

In order to guard against threats, the TOE shall:

- be deployed in secure premises (OE.SECURE_SITE)
- be used by trustworthy administrators (OE.ADMIN)
- be managed from trusted workstations (OE.TRUSTED_ADMIN_WS)

In order to protect itself, the TOE shall:

- enable administration flows to be filtered (O.FILTERING_POLICY_APPLICATION)
- provide controlled access to its sensitive assets (O.ALARM_PROTECTION)
- protect remote administration flows (O.ADMIN_FLOW_PROTECTION)
- authenticate the TOE administrator (O.ADMIN_AUTHENTICATION)

In order to detect a threat occurrence, the TOE shall:

- enable the detection of the loss of alarms (O.ALARM_PROTECTION)

In order to limit threat impact, the TOE shall carry out:

- no action

4.3.1.6 Threats to administration audit trails

T.ADMIN_AUDIT_ALTERATION

In order to guard against threats, the TOE shall:

- be deployed in secure premises (OE.SECURE_SITE)
- be used by trustworthy administrators (OE.ADMIN)
- be used from trusted workstations (OE.TRUSTED_ADMIN_WS)

In order to protect itself, the TOE shall:

- enable administration flows to be filtered (O.FILTERING_POLICY_APPLICATION)
- provide controlled access to its sensitive assets (O.ADMIN_AUDIT_PROTECTION)
- protect remote administration flows (O.ADMIN_FLOW_PROTECTION)
- authenticate the TOE administrator (O.ADMIN_AUTHENTICATION)

In order to detect a threat occurrence, the TOE shall:

- enable the loss of audit records to be detected (O.ADMIN_AUDIT_PROTECTION)

In order to limit threat impact, the TOE shall:

- rely on audit trail recording and archiving measures (OE.AUDIT_ANALYSIS)

4.3.1.7 Threats to all assets during the reuse of the TOE

T.CONTEXT_SWITCHING

In order to guard against threats, the TOE shall:

- provide a feature rendering its sensitive assets unavailable before changes are made to its usage context: new usage, maintenance, etc. (O.TOE_REUSE)

In order to protect itself, the TOE shall carry out:

- no action

In order to detect a threat occurrence, the TOE shall carry out:

- no action

In order to limit threat impact, the TOE shall carry out:

- no action

4.3.2 Coverage of organisational security policies (OSP)

OSP.FILTERING_POLICY_APPLICATION

This OSP is defined directly in terms of objectives for security services provided by the TOE: O.FILTERING_POLICY_APPLICATION, O.POLICY_VISUALISATION and finally O.POLICY_CONSISTENCY when the filtering policy is not managed directly on the firewall, but at a remote administration workstation.

OSP.FLOW_AUDITING

This OSP is defined directly in terms of objective for security services provided by the TOE (O.FLOW_AUDIT).

OSP.ROLES

This OSP is defined directly in terms of:

- the roles management objective O.ROLES
- the audit objective of actions carried out by administrators O.ADMIN_AUDIT

OSP.CRYPTO

This OSP is defined directly in terms of the product design objective OE.CRYPTO.

4.3.3 Coverage of assumptions

A.ADMIN

This assumption is supported by OE.ADMIN, which imposes the training of administrators for their tasks.

A.SECURE_SITE

This assumption is supported by OE.SECURE_SITE, which imposes the location of TOE equipments and media containing TOE sensitive assets in a secure place.

A.AUDIT

This assumption is expressed by OE.AUDIT_ANALYSIS.

A.ALARM

This assumption is expressed by OE.ALARM_PROCESSING.

A.CONFIGURATION_CONTROL

This assumption is expressed by OE.TOE_INTEGRITY.

A.TRUSTED_ADMIN_WS

This assumption is expressed by OE.TRUSTED_ADMIN_WS.

4.3.4 Coverage tables with security objectives

4.3.4.1 Coverage of threats

Threats	Security objectives	Rationale
T.MALFUNCTION	O.TOE_MONITORING, OE.TOE_INTEGRITY, O.MONITOING_IMPACT	Section 4.3.1
T.FILTERING_POLICY_ALTERATION	OE.SECURE_SITE, OE.ADMIN, OE.TRUSTED_ADMIN_WS, OE.TOE_INTEGRITY, OE.ALARM_PROCESSING, O.ADMIN_AUTHENTICATION, O.FILTERING_POLICY_PROTECTION, O.ADMIN_FLOW_PROTECTION, O.FILTERING_POLICY_APPLICATION, O.ADMIN_AUDIT, O.FLOW_AUDIT, O.ALARM	Section 4.3.1
T.FILTERING_POLICY_DISCLOSURE	OE.SECURE_SITE, OE.ADMIN, OE.TRUSTED_ADMIN_WS, OE.ALARM_PROCESSING, O.ADMIN_AUTHENTICATION, O.FILTERING_POLICY_APPLICATION, O.FILTERING_POLICY_PROTECTION, O.ADMIN_FLOW_PROTECTION, O.ADMIN_AUDIT, O.FLOW_AUDIT, O.ALARM	Section 4.3.1
T.PARAMETER_ALTERATION	OE.SECURE_SITE, OE.ADMIN, OE.TRUSTED_ADMIN_WS, OE.ALARM_PROCESSING, O.ADMIN_AUTHENTICATION, O.FILTERING_POLICY_APPLICATION, O.PARAMETER_PROTECTION, O.ADMIN_AUDIT, O.FLOW_AUDIT, O.ALARM, OE.TOE_INTEGRITY, O.ADMIN_FLOW_PROTECTION	Section 4.3.1
T.PARAMETER_DISCLOSURE	OE.SECURE_SITE, OE.ADMIN, OE.TRUSTED_ADMIN_WS, OE.ALARM_PROCESSING, O.ADMIN_AUTHENTICATION, O.TOE_REUSE, O.FILTERING_POLICY_APPLICATION, O.PARAMETER_PROTECTION, O.ADMIN_AUDIT, O.FLOW_AUDIT, O.ALARM, O.ADMIN_FLOW_PROTECTION	Section 4.3.1
T.FLOW_AUDIT_ALTERATION	OE.SECURE_SITE, OE.ADMIN, OE.TRUSTED_ADMIN_WS, O.ADMIN_AUTHENTICATION, O.FILTERING_POLICY_APPLICATION, OE.AUDIT_ANALYSIS, O.FLOW_AUDIT_PROTECTION, O.ADMIN_FLOW_PROTECTION	Section 4.3.1
T.ALARM_ALTERATION	OE.SECURE_SITE, OE.ADMIN, OE.TRUSTED_ADMIN_WS, O.ADMIN_AUTHENTICATION, O.FILTERING_POLICY_APPLICATION, O.ADMIN_FLOW_PROTECTION, O.ALARM_PROTECTION	Section 4.3.1
T.ADMIN_AUDIT_ALTERATION	OE.SECURE_SITE, OE.ADMIN, OE.TRUSTED_ADMIN_WS, O.ADMIN_AUTHENTICATION, O.FILTERING_POLICY_APPLICATION, OE.AUDIT_ANALYSIS, O.ADMIN_FLOW_PROTECTION, O.ADMIN_AUDIT_PROTECTION	Section 4.3.1
T.CONTEXT_SWITCHING	O.TOE_REUSE	Section 4.3.1

Table 1 Threats to security objectives

Security objectives	Threats
O.FILTERING_POLICY_APPLICATION	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE, T.FLOW_AUDIT_ALTERATION, T.ALARM_ALTERATION, T.ADMIN_AUDIT_ALTERATION
O.POLICY_VISUALISATION	
O.POLICY_CONSISTENCY	
O.FLOW_AUDIT	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE
O.ROLES	
O.FILTERING_POLICY_PROTECTION	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE
O.FLOW_AUDIT_PROTECTION	T.FLOW_AUDIT_ALTERATION
O.ADMIN_AUDIT	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE
O.ADMIN_AUDIT_PROTECTION	T.ADMIN_AUDIT_ALTERATION
O.ALARM	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE
O.ALARM_PROTECTION	T.ALARM_ALTERATION
O.ADMIN_FLOW_PROTECTION	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE, T.FLOW_AUDIT_ALTERATION, T.ALARM_ALTERATION, T.ADMIN_AUDIT_ALTERATION
O.PARAMETER_PROTECTION	T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE
O.TOE_MONITORING	T.MALFUNCTION
O.MONITOING_IMPACT	T.MALFUNCTION
O.TOE_REUSE	T.CONTEXT_SWITCHING, T.PARAMETER_DISCLOSURE
OE.TRUSTED_ADMIN_WS	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE, T.FLOW_AUDIT_ALTERATION, T.ALARM_ALTERATION, T.ADMIN_AUDIT_ALTERATION
O.ADMIN_AUTHENTICATION	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE, T.FLOW_AUDIT_ALTERATION, T.ALARM_ALTERATION, T.ADMIN_AUDIT_ALTERATION
OE.CRYPTO	
OE.SECURE_SITE	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE, T.FLOW_AUDIT_ALTERATION, T.ALARM_ALTERATION, T.ADMIN_AUDIT_ALTERATION
OE.ADMIN	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE, T.FLOW_AUDIT_ALTERATION, T.ALARM_ALTERATION, T.ADMIN_AUDIT_ALTERATION
OE.AUDIT_ANALYSIS	T.FLOW_AUDIT_ALTERATION, T.ADMIN_AUDIT_ALTERATION
OE.ALARM_PROCESSING	T.FILTERING_POLICY_ALTERATION, T.FILTERING_POLICY_DISCLOSURE, T.PARAMETER_ALTERATION, T.PARAMETER_DISCLOSURE

Security objectives	Threats
OE.TOE_INTEGRITY	T.MALFUNCTION, T.FILTERING_POLICY_ALTERATION, T.PARAMETER_ALTERATION

Table 2 Security objectives to threats

4.3.4.2 Coverage of assumptions

Assumptions	Security objectives for the environment	Rationale
A.ADMIN	OE.ADMIN	Section 4.3.3
A.SECURE_SITE	OE.SECURE_SITE	Section 4.3.3
A.AUDIT	OE.AUDIT_ANALYSIS	Section 4.3.3
A.ALARM	OE.ALARM_PROCESSING	Section 4.3.3
A.CONFIGURATION_CONTROL	OE.TOE_INTEGRITY	Section 4.3.3
A.TRUSTED_ADMIN_WS	OE.TRUSTED_ADMIN_WS	Section 4.3.3

Table 3 Assumptions to security objectives for the environment

Security objectives for the environment	Assumptions
OE.CRYPTO	
OE.SECURE_SITE	A.SECURE_SITE
OE.ADMIN	A.ADMIN
OE.TRUSTED_ADMIN_WS	A.TRUSTED_ADMIN_WS
OE.AUDIT_ANALYSIS	A.AUDIT
OE.ALARM_PROCESSING	A.ALARM
OE.TOE_INTEGRITY	A.CONFIGURATION_CONTROL

Table 4 Security objectives for the environment towards assumptions

4.3.4.3 Coverage of organisational security policies

Organisational security policies	Security objectives	Rationale
OSP.FILTERING_POLICY_APPLICATION	O.FILTERING_POLICY_APPLICATION, O.POLICY_CONSISTENCY, O.POLICY_VISUALISATION	Section 4.3.2
OSP.FLOW_AUDITING	O.FLOW_AUDIT	Section 4.3.2
OSP.ROLES	O.ROLES, O.ADMIN_AUDIT	Section 4.3.2
OSP.CRYPTO	OE.CRYPTO	Section 4.3.2

Table 5 Organisational security policies towards security objectives

Security objectives	Organisational security policies
O.FILTERING_POLICY_APPLICATION	OSP.FILTERING_POLICY_APPLICATION
O.POLICY_VISUALISATION	OSP.FILTERING_POLICY_APPLICATION
O.POLICY_CONSISTENCY	OSP.FILTERING_POLICY_APPLICATION
O.FLOW_AUDIT	OSP.FLOW_AUDITING
O.ROLES	OSP.ROLES
O.FILTERING_POLICY_PROTECTION	
O.FLOW_AUDIT_PROTECTION	
O.ADMIN_AUDIT	OSP.ROLES
O.ADMIN_AUDIT_PROTECTION	
O.ALARM	
O.ALARM_PROTECTION	
O.ADMIN_FLOW_PROTECTION	
O.PARAMETER_PROTECTION	
O.TOE_MONITORING	
O.MONITOING_IMPACT	
O.TOE_REUSE	
O.ADMIN_AUTHENTICATION	
OE.CRYPTO	OSP.CRYPTO
OE.SECURE_SITE	
OE.ADMIN	
OE.TRUSTED_ADMIN_WS	
OE.AUDIT_ANALYSIS	
OE.TOE_INTEGRITY	

Table 6 Security objectives towards organisational security policies

5 Extended components definition

Not applicable.

6 IT security requirements

6.1 Definitions

The diagram below shows the interactions between elements defined in the Security Functional Requirements (SFR).

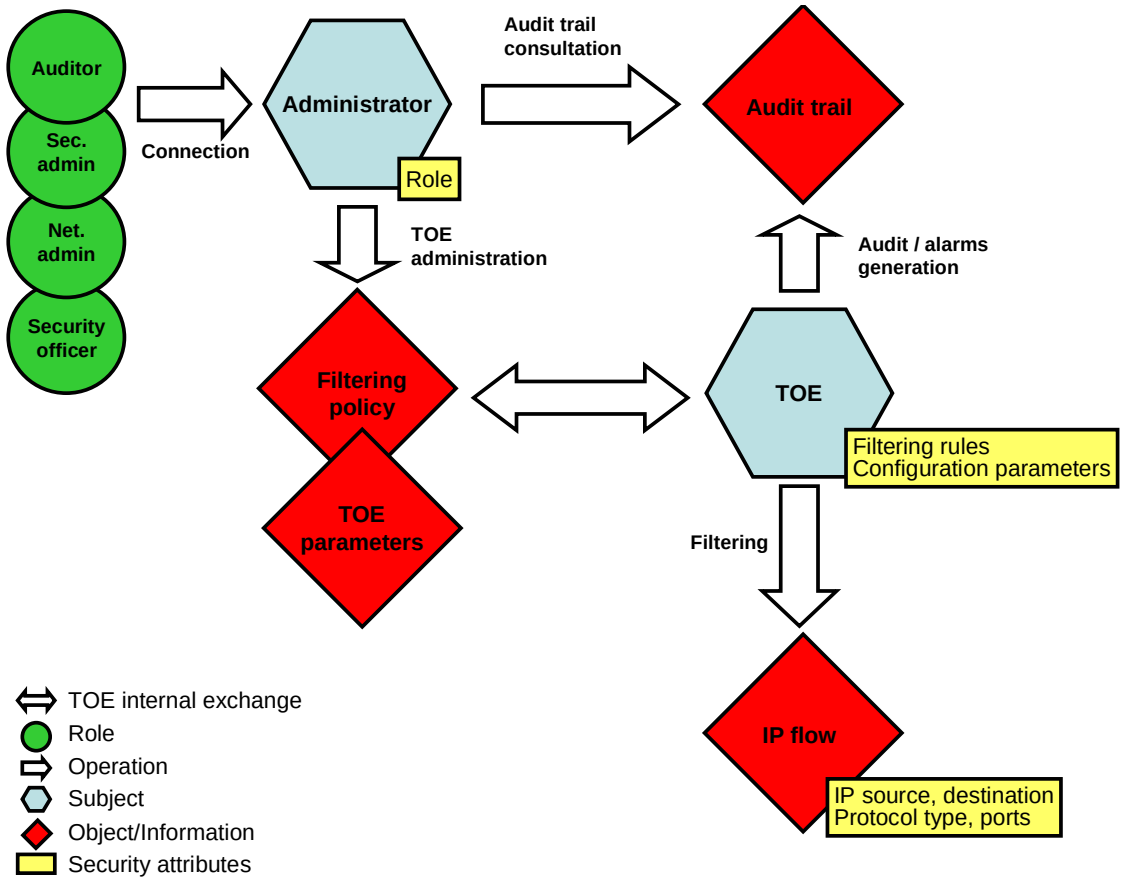

Figure 1: illustration of the interaction between elements defined in the SFRs

These elements are listed below.

Subjects

- The TOE
- Administrators

Objects

- Filtering policy rules
- Sensitive assets of the firewall
- Audit trails
- TOE parameters

Informations

- User IP flows
- TCP, UDP and ICMP application flows
- Administration flows

Operations

Operations regarding the control of flows:
- Application of the filtering policy

Operations regarding access to filtering policy rules:
- Reading, inserting, modifying and deleting

Operations regarding access to sensitive assets (the objects) of the firewall:
- Deletion

Security attributes

- Source and destination IP addresses of IP packets
- Protocol types
- Communication ports
- Administrators' role (security officer, security administrator, system and network administrator, auditor)
- TOE configuration parameters

External entities

- Remote administration workstations

6.2 TOE security functional requirements

6.2.1 Services provided by the TOE

6.2.1.1 Flow filtering

FDP_IFC.2-flow_filtering Complete information flow control

FDP_IFC.2.1-flow_filtering

The TSF shall enforce the **filtering policy (and the rules relating to connection contexts in contextual mode)** on:

subjects:

- **the TOE**

information:

- **user IP flows**
- **TCP, UDP and ICMP application flows**
- **administration flows**

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2-flow_filtering

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.

FDP_IFF.1-flow_filtering Simple security attributes

FDP_IFF.1.1-flow_filtering

The TSF shall enforce the **filtering policy (and the rules relating to connection contexts in contextual mode)** based on the following types of subject and information security attributes:

Subject security attributes:

- **filtering rules**
- **TOE configuration parameters used in filtering rules**

Information security attributes:

- **source and destination IP addresses of IP packets**
- **types of protocol**
- **communication ports**

Application note:

STs in conformity with this PP must specify the configuration parameters used.

FDP_IFF.1.2-flow_filtering

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **IP packet attributes processed respect the criteria defined in the filtering policy and/or the filtering rules relating to the connection context in contextual mode**

FDP_IFF.1.3-flow_filtering

The TSF shall enforce **no additional rules**.

FDP_IFF.1.4-flow_filtering

The TSF shall explicitly authorise an information flow based on the following rules:

- **a filtering rule explicitly authorises the transfer of the IP packet**

FDP_IFF.1.5-flow_filtering

The TSF shall explicitly deny an information flow based on the following rules:

- **a filtering rule explicitly forbids the transfer of the IP packet**
- **no filtering rule has authorised the transfer of the IP packet**

FMT_SMF.1-filtering_policy_visualisation Specification of management functions

FMT_SMF.1.1-filtering_policy_visualisation

The TSF shall be capable of performing the following management functions:

- **viewing of the filtering policy and connection contexts present on the firewall**

6.2.1.2 Flow audit

FAU_GEN.1-flow_audit Audit data generation

FAU_GEN.1.1-flow_audit

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 **not specified** level of audit; and

c) **As a minimum, the events generated when a flow is rejected**

Non-editorial refinement:

The level of detail of the audit trail (minimal, basic, detailed) depends on the audited event. Appendix A summarises minimal audit trails required and shows the associated level of auditing.

Application note:

STs in conformity with this PP must state, where applicable, the other audited events.

FAU_GEN.1.2-flow_audit

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, **the information enabling an auditor to detect the loss of flow audit events (a counter for example)**

Overall refinement:

The recorded logs must notably enable administrators to check the relevance of the filtering policy and its correct instantiation at the level of the firewall.

FAU_GEN.2-flow_audit User identity association

FAU_GEN.2.1-flow_audit

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.

Non-editorial refinement:

'User identity' is understood to mean the IP address of the issuers of flows.

FIA_UID.2-flow User identification before any action

FIA_UID.2.1-flow

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Overall refinement:

'User' is understood to mean the issuers and recipients of flows processed by the firewall identified by their IP addresses.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1
The TSF shall be able to provide reliable time stamps.

Overall refinement:

The expected reliability of the time reference is such that only the TOE administrator is allowed to modify it, as the time reference must be reliable between two updates by the administrator.

FAU_SAR.1-flow_audit Audit review

FAU_SAR.1.1-flow_audit
The TSF shall provide **auditors** with the capability to read **the audit trails of flows processed by the firewall** from the audit records.

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

FAU_SAR.3-flow_audit Selectable audit review

FAU_SAR.3.1-flow_audit
The TSF shall provide the ability to apply **methods of sorting, ordering and searches** of audit data based on **the data and time** and **[assignment: criteria selected by the auditor]**.

Application note:

STs in conformity with this PP must detail these criteria and the logical relationships used.

6.2.1.3 Role management

FMT_SMR.1 Security roles

FMT_SMR.1.1
The TSF shall maintain the roles**:**

- **security officer**
- **security administrator**
- **system and network administrator**
- **auditor**

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

Application note:

A same person can have several roles. In the case of the firewall, for example, a same person may be both security administrator and system and network administrator. These roles can be performed locally on the firewall or remotely via an administration workstation.

FIA_UID.2-administrator User identification before any action

FIA_UID.2.1-flow

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Overall refinement:

In this context, 'users' are administrators; not to be confused with the possibility offered by some firewalls of linking filtering with network user identification/authentication.

FIA_UAU.2-administrator User authentication before any action

FIA_UAU.2.1-administrator

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Overall refinement:

This requirement relates to the authentication of administrators managing the firewall.

Non-editorial refinement:

The authentication mechanism shall be compliant with [AUTH].

6.2.2 Operation of the TOE

6.2.2.1 Protection of the filtering policy

FDP_ACC.1-filtering_rules Subset access control

FDP_ACC.1.1-filtering_rules

The TSF shall enforce the **filtering rules access policy** on:

- **subjects: administrators**
- **objects: filtering policy rules**
- **operations: reading, inserting, modifying and deleting**

FDP_ACF.1-filtering_rules Security attribute based access control

FDP_ACF.1.1-filtering_rules

The TSF shall enforce the **filtering rules access policy** to objects based on the following:

- **subjects: administrators on the basis of their role**
- **objects: filtering policy rules**

FDP_ACF.1.2-filtering_rules

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **insertion, modification and deletion (complete or in part) of the filtering rules are only authorised for the security administrator role**

- **the reading of filtering rules and connection contexts is only authorised for the security administrator role**

FDP_ACF.1.3-filtering_rules

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

Application note:

STs in conformity with this PP must indicate the additional rules used or state "no additional rules".

FDP_ACF.1.4-filtering_rules

The TSF shall explicitly deny access of subjects to objects based on the **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.

Application note:

STs in conformity with this PP must indicate the additional rules used or state "no additional rules".

Application note:

These access rules shall be developed by the author of the security target to take into account the firewall's ability to adapt rules itself according to connection contexts (contextual mode).

6.2.2.2 Audit and alarms

Protection of flow audit trails

FAU_STG.1-flow_audit_trail Protected audit trail storage

FAU_STG.1.1-flow_audit_trail

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2-flow_audit_trail

The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

Administration events

FAU_GEN.1-admin_audit Audit data generation

FAU_GEN.1.1-admin_audit

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 **minimal or basic** level of audit **defined in Appendix B with the associated level of audit**; and

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

Application note:

The author of the security target shall detail the other events requiring audit according to the functional requirements selected. These shall be determined according to Part 2 of the Common Criteria, which states the type of event to be audited for each of the components for the level of detail chosen in FAU_GEN.1.1.

FAU_GEN.1.2-admin_audit

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, **information enabling an auditor to detect the loss of administration audit events (a counter for example)**

FAU_GEN.2-admin_audit User identity association

FAU_GEN.2.1-admin_audit

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.

FAU_SAR.1-admin_audit Audit review

FAU_SAR.1.1-admin_audit

The TSF shall provide **the auditors** with the capability to read **the administration audit event data** from the audit records.

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

FAU_SAR.3-admin_audit Selectable audit review

FAU_SAR.3.1-admin_audit

The TSF shall provide the ability to apply **methods of sorting, ordering and searches** of audit data based on **criteria selected by the auditor**.

Application note:

STs in conformity with this PP must detail these criteria and the logical relationships used.

FAU_STG.1-admin_audit_trail Protected audit trail storage

FAU_STG.1.1-admin_audit_trail

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2-admin_audit_trail

The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

Alarms

FAU_SAA.1-alarm Potential violation analysis

FAU_SAA.1.1-alarm

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2-alarm

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of **audit events** known to indicate a potential security violation;

b) **other events**

Application note:

STs in conformity with this PP must detail events indicating a potential violation of the security policy.

FAU_ARP.1-alarm Security alarms

FAU_ARP.1.1-alarm

The TSF shall **at a minimum send an alert to the security administrator** upon detection of a potential security violation.

Application note:

STs in conformity with this PP must state, where appropriate, additional implemented actions.

6.2.2.3 Protection of remote administration

The following requirements contribute to establishing a trusted channel between the TOE and a remote administration workstation.

FTP_ITC.1-remote_administration Inter-TSF trusted channel

FTP_ITC.1.1-remote_administration

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2-remote_administration

The TSF shall permit **[selection: another trusted IT product]** to initiate communication via the trusted channel.

Non-editorial refinement:

'Another trusted IT product' describes a remote administration workstation.

Application note:

STs in conformity with this PP must detail the method used.

FTP_ITC.1.3-remote_administration
The TSF shall initiate communication via the trusted channel for **[assignment: administration or monitoring of the TOE].**

FPT_ITI.1-remote_administration Inter-TSF detection of modification

FPT_ITI.1.1-remote_administration
The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: **[assignment: detection of modifications, deletions, insertions in administration data]**.

Application note:

STs in conformity with this PP must state the anomalies taken into consideration and the detection methods used.

FPT_ITI.1.2-remote_administration
The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform **[assignment: ignore the data and issue an alert]** if modifications are detected.

FPT_RPL.1-remote_administration Replay detection

FPT_RPL.1.1-remote_administration
The TSF shall detect replay for the following entities: **[assignment: administration data received via a remote administration workstation].**

Application note:

STs in conformity with this PP must detail the methods used.

FPT_RPL.1.2-remote_administration
The TSF shall perform **[assignment: ignore the data and issue an alert] when replay is detected.**

FPT_ITC.1-remote_administration Inter-TSF confidentiality during transmission

FPT_ITC.1.1-remote_administration
The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Application note:

STs in conformity with this PP must detail the methods used.

FPT_TDC.1-remote_administration Inter-TSF basic TSF data consistency

FPT_TDC.1.1-remote_administration
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.

Application note:

STs in conformity with this PP must detail data shared with a remote administration workstation requiring interpretation.

FPT_TDC.1.2-remote_administration

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.

Application note:

STs in conformity with this PP must detail these interpreting rules.

6.2.2.4 Configuration of the TOE

FMT_SMF.1-TOE_configuration Specification of management functions

FMT_SMF.1.1-TOE_configuration

The TSF shall be capable of performing the following management functions:

- **configuration of TOE parameters (identification and authentication data, access rights, system time, etc.)**
- **configuration of system and network parameters**
- **configuration of the filtering policy**

FMT_MTD.1-configuration_parameter Management of TSF data

FMT_MTD.1.1-configuration_parameter

The TSF shall restrict the ability to **query and modify system time and system and network configuration parameters** to **system and network administrators**.

FMT_MTD.1-security_officer Management of TSF data

FMT_MTD.1.1-security_officer

The TSF shall restrict the ability to **modify identification and authentication data and access rights** to the **security officer**.

FMT_MTD.1-auditor Management of TSF data

FMT_MTD.1.1-auditor

The TSF shall restrict the ability to **query identification and authentication data and access rights** to **auditors**.

6.2.2.5 Monitoring of the TOE

FMT_SMF.1-monitorig Specification of management functions

FMT_SMF.1.1-monitorig

The TSF shall be capable of performing the following management functions:

- **monitoring of the firewall status**

FPT_ITC.1-monitorig Inter-TSF confidentiality during transmission

FPT_ITC.1.1-monitorig

The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Overall refinement:

Data exported outside TOE control is data strictly required for monitoring, and transmitted to monitoring equipment. This data must not contain confidential information, unless such information is protected.

Application note:

STs in conformity with this PP must detail the used mechanisms.

6.2.2.6 Reuse of the TOE

FDP_RIP.1-TOE_reuse Subset residual information protection

FDP_RIP.1.1-TOE_reuse

The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **all sensitive assets (filtering policies, configuration parameters, audits trails, alarms).**

FDP_ACC.1-TOE_reuse Subset access control

FDP_ACC.1.1-TOE_reuse

The TSF shall enforce the **sensitive asset access policy** on:

- **subjects: administrators**
- **objects: sensitive assets of the firewall**
- **operations: deletion**

Application note:

The TOE must provide a deletion operation for sensitive assets in the event of reuse.

FDP_ACF.1-TOE_reuse Security attribute based access control

FDP_ACF.1.1-TOE_reuse

The TSF shall enforce the **sensitive asset access policy** to objects based on the following:

- **subjects: administrators on the basis of their role**
- **objects: sensitive assets of the firewall**

FDP_ACF.1.2-TOE_reuse

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **deletion (complete or in part) of sensitive assets is only authorised for the security officer role.**

FDP_ACF.1.3-TOE_reuse

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

Application note:

STs in conformity with this PP must indicate the additional rules used or state "no additional rules".

FDP_ACF.1.4-TOE_reuse

The TSF shall explicitly deny access of subjects to objects based on the **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.

Application note:

STs in conformity with this PP must indicate the additional rules used or state "no additional rules".

6.3 Security assurance requirements for the TOE

A TOE with a ST in conformity with this PP shall be evaluated according to EAL3 augmented by ALC_FLR.3 and AVA_VAN.3 components, corresponding to the assurance package provided for the standard level qualification of a security target (see [QUA-STD]), defined by the "QS" column of the following table:

Assurance class	Assurance family	Assurance Components by Evaluation Assurance Level							
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	**QS**
Development	ADV_ARC		1	**1**	1	1	1	1	**1**
	ADV_FSP	1	2	**3**	4	5	5	6	**3**
	ADV_IMP				1	1	2	2	
	ADV_INT					2	3	3	
	ADV_SPM						1	1	
	ADV_TDS		1	**2**	3	4	5	6	**2**
Guidance documents	AGD_OPE	1	1	**1**	1	1	1	1	**1**
	AGD_PRE	1	1	**1**	1	1	1	1	**1**
Life-cycle support	ALC_CMC	1	2	**3**	4	4	5	5	**3**
	ALC_CMS	1	2	**3**	4	5	5	5	**3**
	ALC_DEL		1	**1**	1	1	1	1	**1**
	ALC_DVS			**1**	1	1	2	2	**1**
	ALC_FLR								**3**
	ALC_LCD			**1**	1	1	1	2	**1**
	ALC_TAT				1	2	3	3	
Security Target evaluation	ASE_CCL	1	1	**1**	1	1	1	1	**1**
	ASE_ECD	1	1	**1**	1	1	1	1	**1**
	ASE_INT	1	1	**1**	1	1	1	1	**1**
	ASE_OBJ	1	2	**2**	2	2	2	2	**2**
	ASE_REQ	1	2	**2**	2	2	2	2	**2**
	ASE_SPD		1	**1**	1	1	1	1	**1**
	ASE_TSS	1	1	**1**	1	1	1	1	**1**
Tests	ATE_COV		1	**2**	2	2	3	3	**2**
	ATE_DPT			**1**	2	3	3	4	**1**
	ATE_FUN		1	**1**	1	1	2	2	**1**

Assurance class	Assurance family	Assurance Components by Evaluation Assurance Level							
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	**QS**
	ATE_IND	1	2	**2**	2	2	2	3	**2**
Vulnerability assessment	AVA_VAN	1	2	2	**3**	4	5	5	**3**

Table 7 Requirements for the standard level qualification of a ST

Application note: STs in conformity with this PP must respect the assurance package required for the standard level qualification.

6.4 Rationale

6.4.1 Security requirements / Security objectives

6.4.1.1 Coverage of TOE security objectives

Objectives for security services provided by the TOE

O.FILTERING_POLICY_APPLICATION

This objective is expressed by the following requirements:

- FDP_IFF.1-flow_filtering, which allows for the definition of minimal rules to be respected by the filtering policy
- FDP_IFC.2-flow_filtering, which demands that the TOE apply this filtering policy

O.POLICY_VISUALISATION

This objective is expressed by the FMT_SMF.1-filtering_policy_visualisation requirement, which requires the visibility of filtering rules and connection contexts.

O.POLICY_CONSISTENCY

This objective is expressed by FPT_TDC.1-remote_administration, which ensures coherence between the filtering policy defined for the remote administration workstation and the firewall.

O.FLOW_AUDIT

This objective is expressed by FAU_GEN.1-flow_audit, which calls for the generation of event logs for flows processed by the firewall, and FAU_GEN.2-flow_audit, according to which it must be possible to attribute events to the issuers of these flows. In order to carry out the latter, flows must be identified without fail (FIA_UID.2-flow). Because the dates of audited events are recorded, the TOE must also be equipped with a reliable clock (FPT_STM.1).

The ability to consult the audit trails of flows processed by the firewall is expressed by FAU_SAR.1-flow_audit and FAU_SAR.3-flow_audit.

O.ROLES

The objective is expressed by the FMT_SMR.1 requirement, which requires the TOE to manage the various roles (administrators). In order to manage these roles, administrators must, without fail, be identified (FIA_UID.2-administrator) and authenticated (FIA_UAU.2-administrator).

Security objectives for TOE operation

Protection of the filtering policy

O.FILTERING_POLICY_PROTECTION

This objective is expressed by the filtering policy access rules (FDP_ACC.1-filtering_rules and FDP_ACF.1-filtering_rules).

Audit and alarms

Flows

O.FLOW_AUDIT_PROTECTION

This objective is expressed by FAU_STG.1-flow_audit_trail, which requires the integrity protection of audit events records. The risk of record loss occurring as a result of insufficient memory is not dealt with in this protection profile on account of the associated A.AUDIT assumption.

Administration events

O.ADMIN_AUDIT

This objective is expressed by FAU_GEN.1-admin_audit, which calls for the generation of event logs for firewall administration events, and FAU_GEN.2-admin_audit, according to which it must be possible to attribute events to administrators. Administrators must be identified without fail (FIA_UID.2-administrator). Because the dates of audited events are recorded, the TOE must also be equipped with a reliable clock (FPT_STM.1).

The ability to consult these firewall administration event audit trails is expressed by FAU_SAR.1-admin_audit and FAU_SAR.3-admin_audit.

O.ADMIN_AUDIT_PROTECTION

This objective is expressed by FAU_STG.1-admin_audit_trail, which requires the integrity protection of administration event records.

Alarms

O.ALARM

This objective is expressed by FAU_ARP.1-alarm, which requires a security alarm to be set off when a potential security violation is detected, and by FAU_SAA.1-alarm, which indicates the rules used for detecting potential violations.

O.ALARM_PROTECTION

This objective is expressed by FAU_STG.1-admin_audit_trail and FAU_STG.1-flow_audit_trail, which ensure integrity of the event records.

Protection of remote administration

O.ADMIN_FLOW_PROTECTION

This objective is expressed by the following protection requirements:

- FTP_ITC.1-remote_administration and FPT_ITI.1-remote_administration require that the TOE be capable of establishing a trusted channel enabling the control of the integrity of administration data shared with a remote site

- FPT_RPL.1-remote_administration requires that the TOE ensure protection against the replay of data shared with remote sites within the context of remote administration and monitoring operations
- FPT_ITC.1-remote_administration requires that the TOE ensure the confidentiality of administration data exported to a remote site
- FPT_TDC.1-remote_administration requires data to be interpreted in order to ensure coherence between the remote administration workstation and the TOE, and outlines how interpretation rules should be defined for mechanisms ensuring TSF data coherency
- FIA_UID.2-administrator and FIA_UAU.2-administrator require that administrators be identified and authenticated without fail for them to carry out administrative operations

Configuration of the TOE

O.PARAMETER_PROTECTION

This objective is expressed by the following protection requirements:

- for network configuration parameters: FMT_MTD.1-configuration_parameter
- for access rights and authentication data: FMT_MTD.1-security_officer for security administrators and FMT_MTD.1-auditor for auditors

The configuration functionality of these parameters is covered by FMT_SMF.1-TOE_configuration.

Monitoring of the TOE

O.TOE_MONITORING

This objective is expressed by FMT_SMF.1-monitorig, which requires the provision of a service indicating the status of the firewall.

O.MONITOING_IMPACT

This objective is expressed by requirement FPT_ITC.1-monitorig, which requires the protection of data exported outside the control of the firewall if it contains confidential information.

Reuse of the TOE

O.TOE_REUSE

This objective is expressed by the following requirements:

- FDP_RIP.1-TOE_reuse, which requires that the TOE be able to make unavailable the content of resources corresponding to TOE sensitive assets
- FDP-ACC.1-TOE_reuse and FDP_ACF.1-TOE_reuse, which require access rules for the deletion operation of sensitive assets

O.ADMIN_AUTHENTICATION

This objective is expressed by the following requirements:

- FIA_UID.2-administrator and FIA_UAU.2-administrator, which require that administrators be identified and authenticated without fail for them to carry out administrative operations

6.4.2 Coverage tables of security objectives and security requirements

Security objectives	Functional requirements for the TOE	Rationale
O.FILTERING_POLICY_APPLICATION	FDP_IFF.1-flow_filtering, FDP_IFC.2-flow_filtering	Section 6.3.1
O.POLICY_VISUALISATION	FMT_SMF.1-filtering_policy_visualisation	Section 6.3.1
O.POLICY_CONSISTENCY	FPT_TDC.1-remote_administration	Section 6.3.1
O.FLOW_AUDIT	FAU_GEN.1-flow_audit, FAU_GEN.2-flow_audit, FPT_STM.1, FIA_UID.2-flow, FAU_SAR.1-flow_audit, FAU_SAR.3-flow_audit	Section 6.3.1
O.ROLES	FMT_SMR.1, FIA_UID.2-administrator ; FIA_UAU.2-administrator	Section 6.3.1
O.FILTERING_POLICY_PROTECTION	FDP_ACC.1-filtering_rules, FDP_ACF.1-filtering_rules	Section 6.3.1
O.FLOW_AUDIT_PROTECTION	FAU_STG.1-flow_audit_trail	Section 6.3.1
O.ADMIN_AUDIT	FPT_STM.1, FAU_GEN.2-admin_audit, FAU_GEN.1-admin_audit, FAU_SAR.1-admin_audit, FAU_SAR.3-admin_audit, FIA_UID.2-administrator	Section 6.3.1
O.ADMIN_AUDIT_PROTECTION	FAU_STG.1-admin_audit_trail	Section 6.3.1
O.ALARM	FAU_ARP.1-alarm, FAU_SAA.1-alarm	Section 6.3.1
O.ALARM_PROTECTION	FAU_STG.1-flow_audit_trail, FAU_STG.1-admin_audit_trail	Section 6.3.1
O.ADMIN_FLOW_PROTECTION	FTP_ITC.1-remote_administration ; FPT_ITI.1-remote_administration ; FPT_RPL.1-remote_administration ; FPT_ITC.1-remote_administration ; FPT_TDC.1-remote_administration ; FIA_UID.2-administrator ; FIA_UAU.2-administrator	Section 6.3.1
O.PARAMETER_PROTECTION	FMT_MTD.1-configuration_parameter, FMT_MTD.1-security_officer, FMT_SMF.1-TOE_configuration, FMT_MTD.1-auditor	Section 6.3.1
O.TOE_MONITORING	FMT_SMF.1-monitorig	Section 6.3.1
O.MONITOING_IMPACT	FPT_ITC.1-monitorig	Section 6.3.1
O.TOE_REUSE	FDP_RIP.1-TOE_reuse, FDP_ACC.1-TOE_reuse, FDP_ACF.1-TOE_reuse	Section 6.3.1
O.ADMIN_AUTHENTICATION	FIA_UID.2-administrator ; FIA_UAU.2-administrator	Section 6.3.1

Table 8 Rationale of security objectives to the functional requirements for the TOE

Functional requirements for the TOE	Security objectives
FDP_IFC.2-flow_filtering	O.FILTERING_POLICY_APPLICATION
FDP_IFF.1-flow_filtering	O.FILTERING_POLICY_APPLICATION
FMT_SMF.1-filtering_policy_visualisation	O.POLICY_VISUALISATION
FTP_ITC.1-remote_administration	O.ADMIN_FLOW_PROTECTION
FPT_ITI.1-remote_administration	O.ADMIN_FLOW_PROTECTION

Functional requirements for the TOE	Security objectives
FPT_RPL.1-remote_administration	O.ADMIN_FLOW_PROTECTION
FPT_ITC.1-remote_administration	O.ADMIN_FLOW_PROTECTION
FPT_TDC.1-remote_administration	O.POLICY_CONSISTENCY ; O.ADMIN_FLOW_PROTECTION
FAU_GEN.1-flow_audit	O.FLOW_AUDIT
FAU_GEN.2-flow_audit	O.FLOW_AUDIT
FIA_UID.2-flow	O.FLOW_AUDIT
FPT_STM.1	O.FLOW_AUDIT, O.ADMIN_AUDIT
FAU_SAR.1-flow_audit	O.FLOW_AUDIT
FAU_SAR.3-flow_audit	O.FLOW_AUDIT
FMT_SMR.1	O.ROLES
FIA_UID.2-administrator	O.ROLES, O.ADMIN_AUDIT ; O.ADMIN_FLOW_PROTECTION ; O.ADMIN_AUTHENTICATION
FIA_UAU.2-administrator	O.ROLES ; O.ADMIN_FLOW_PROTECTION ; O.ADMIN_AUTHENTICATION
FDP_ACC.1-filtering_rules	O.FILTERING_POLICY_PROTECTION
FDP_ACF.1-filtering_rules	O.FILTERING_POLICY_PROTECTION
FAU_STG.1-flow_audit_trail	O.FLOW_AUDIT_PROTECTION, O.ALARM_PROTECTION
FAU_GEN.1-admin_audit	O.ADMIN_AUDIT
FAU_GEN.2-admin_audit	O.ADMIN_AUDIT
FAU_SAR.1-admin_audit	O.ADMIN_AUDIT
FAU_SAR.3-admin_audit	O.ADMIN_AUDIT
FAU_STG.1-admin_audit_trail	O.ADMIN_AUDIT_PROTECTION, O.ALARM_PROTECTION
FAU_SAA.1-alarm	O.ALARM
FAU_ARP.1-alarm	O.ALARM
FMT_SMF.1-TOE_configuration	O.PARAMETER_PROTECTION
FMT_MTD.1-configuration_parameter	O.PARAMETER_PROTECTION
FMT_MTD.1-security_officer	O.PARAMETER_PROTECTION
FMT_MTD.1-auditor	O.PARAMETER_PROTECTION
FMT_SMF.1-monitorig	O.TOE_MONITORING
FPT_ITC.1-monitorig	O.MONITOING_IMPACT
FDP_RIP.1-TOE_reuse	O.TOE_REUSE
FDP_ACC.1-TOE_reuse	O.TOE_REUSE
FDP_ACF.1-TOE_reuse	O.TOE_REUSE

Table 9 Rationale of functional objectives for the TOE to security objectives

6.4.3 Dependencies of functional security requirements

Requirements	CC dependencies	Satisfied dependencies
FIA_UAU.2-administrator	(FIA_UID.1)	FIA_UID.2-administrator
FDP_IFC.2-flow_filtering	(FDP_IFF.1)	FDP_IFF.1-flow_filtering
FDP_IFF.1-flow_filtering	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2-flow_filtering
FMT_SMF.1-filtering_policy_visualisation	No dependencies	
FAU_GEN.1-flow_audit	(FPT_STM.1)	FPT_STM.1
FAU_GEN.2-flow_audit	(FAU_GEN.1) and (FIA_UID.1)	FAU_GEN.1-flow_audit, FIA_UID.2-flow
FIA_UID.2-flow	No dependencies	
FPT_STM.1	No dependencies	
FAU_SAR.1-flow_audit	(FAU_GEN.1)	FAU_GEN.1-flow_audit
FAU_SAR.3-flow_audit	(FAU_SAR.1)	FAU_SAR.1-flow_audit
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2-administrator
FIA_UID.2-administrator	No dependencies	
FIA_UAU.2-administrator	(FIA_UID.1)	FIA_UID.2-administrator
FDP_ACC.1-filtering_rules	(FDP_ACF.1)	FDP_ACF.1-filtering_rules
FDP_ACF.1-filtering_rules	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1-filtering_rules
FTP_ITC.1-remote_administration	No dependencies	
FPT_ITI.1-remote_administration	No dependencies	
FPT_RPL.1-remote_administration	No dependencies	
FPT_ITC.1-remote_administration	No dependencies	
FPT_TDC.1-remote_administration	No dependencies	
FMT_SMF.1-TOE_configuration	No dependencies	
FMT_MTD.1-configuration_parameter	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1-TOE_configuration
FMT_MTD.1-security_officer	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1-TOE_configuration
FMT_MTD.1-auditor	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1-TOE_configuration
FMT_SMF.1-monitorig	No dependencies	
FPT_ITC.1-monitorig	No dependencies	
FDP_RIP.1-TOE_reuse	No dependencies	
FDP_ACC.1-TOE_reuse	(FDP_ACF.1)	FDP_ACF.1-TOE_reuse
FDP_ACF.1-TOE_reuse	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1-TOE_reuse
FAU_STG.1-flow_audit_trail	(FAU_GEN.1)	FAU_GEN.1-flow_audit
FAU_GEN.1-admin_audit	(FPT_STM.1)	FPT_STM.1

Requirements	CC dependencies	Satisfied dependencies
FAU_GEN.2-admin_audit	(FAU_GEN.1) and (FIA_UID.1)	FIA_UID.2-administrator, FAU_GEN.1-admin_audit
FAU_SAR.1-admin_audit	(FAU_GEN.1)	FAU_GEN.1-admin_audit
FAU_SAR.3-admin_audit	(FAU_SAR.1)	FAU_SAR.1-admin_audit
FAU_STG.1-admin_audit_trail	(FAU_GEN.1)	FAU_GEN.1-admin_audit
FAU_SAA.1-alarm	(FAU_GEN.1)	FAU_GEN.1-flow_audit, FAU_GEN.1-admin_audit
FAU_ARP.1-alarm	(FAU_SAA.1)	FAU_SAA.1-alarm

Table 10 Functional requirement dependencies

6.4.3.1 Rationale for unsatisfied dependencies

Dependency FMT_MSA.3 of FDP_IFF.1-flow_filtering is not supported. Within the context of this protection profile, there are no set restrictive values for the attributes on which the filtering policy is based. However, there is no restriction on a product doing so.

Dependency FMT_MSA.3 of FDP_ACF.1-filtering_rules is not supported. The protection profile does not require that the TOE predefine default values for security attributes controlling access to the filtering policy.

Dependency FMT_MSA.3 of FDP_ACF.1-Biens_sensibles is not supported. The protection profile does not require that the TOE predefine default values for security attributes controlling access to sensitive assets.

6.4.4 Conformity with a PP

Not applicable.

6.4.5 Extended components

Not applicable.

Appendix A Additional descriptions of the TOE

A.1 Functionalities of the TOE

The main functionality of the TOE is to provide the system with the capacity to restrict the flow of information to or from a protected network in order to protect the resources of that network against attacks from other networks (via the interconnection where the TOE is implemented):

- Application of a filtering policy
- Audit/logging of IP flows

Moreover, the TOE requires the following services if it is to function correctly:

- Management of the filtering policy
- Protection of administrative operations
- Audit of administrative and monitoring operations
- Protection of access to TOE parameters

A.1.1 Services provided by the TOE

Application of the filtering policy

The TOE is a firewall offering filtering functionalities for data flows between IP networks based on rules allowing for the implementation of the security policy of the information system concerned. In order to benefit from optimal filtering, the security policy must be coherent and unambiguous. Two types of filtering exist:

- Non-contextual filtering: the filtering action (acceptance, blocking, rejection, with logging or otherwise) is determined according to the content of a network packet;
- Contextual filtering: following an initial non-contextual filtering, the TOE establishes a context and appropriate filtering rules according to the nature of the identified data flow (origin, destination, protocols, etc.). Knowledge of this context allows the TOE not only to gain in performance, but also to increase the pertinence and accuracy of filtering.

TOE filtering features, contextual or otherwise, concern only IP data flow and take into consideration network and transport layers.

Audit/logging of IP flows

This service makes it possible to track all IP flows processed by the TOE. It also enables the definition of events to be tracked and their consultation.

A.1.2 Services required for the TOE to function correctly

A.1.1.1 Management of filtering policies

Definition of filtering policies

Only security administrators are authorised to define the filtering policy. They specify filtering rules for the sending or the receiving of data: acceptance, rejection and level of control.

A filtering policy can be defined locally, at the local firewall administration level, and remotely on a remote administration workstation, in which case the policy is delivered to the firewall. Coherence between the policy defined by the security administrator and that located on the firewall shall be guaranteed to ensure that the implemented filtering policy is indeed that which is expected and defined by the security administrator.

Protection of access to filtering policies

This service makes it possible to monitor the various types of access (modification, consultation, etc.) to the filtering policy and to security context rules in contextual mode and according to the role of the authenticated person.

A.1.1.2 Protection of administrative operations

The firewall can be administered locally or remotely. Local administration is administration carried out directly on the machine containing the firewall services, whereas remote administration is administration carried out via a LAN or WAN.

Authentication of administrators

This service makes it possible to authenticate all administrators carrying out administrative operations on the firewall.

Protection of remote administration flows

This service makes it possible to protect the authenticity (including therefore the coverage of replay attacks) of data flows shared between the firewall and the administration workstation for carrying out remote administrative operations. This service also makes it possible, where applicable, to protect the confidentiality of administration flows. Such protection concerns security-related administration flows (filtering policy) and system and network administration flows (configuration parameters).

A.1.1.3 Audit and monitoring

Audit / logging of administrative operations

This service makes it possible to track administrative operations carried out by the administrator on the firewall, such as modifications to the filtering policy. It also enables the definition of events to be tracked and their consultation.

Generation of security alarms

This service enables security alarms to be generated to indicate major firewall malfunctions. It also allows a security administrator to define the alarms to be generated and the method of transmission and consultation of these alarms.

Monitoring of the TOE

This service enables a system and network administrator to check the availability status of the firewall (working status, level of use of resources, etc.).

A.1.1.4 Protection of access to configuration parameters

This service makes it possible to protect the confidentiality and integrity of firewall configuration parameters (from an attack through the network). These parameters include, among others, network configuration parameters (topological data concerning protected networks), authentication data and access rights.

A.1.3 Roles

The TOE, in its operational environment, directly or indirectly handles the roles described below. These are 'logical' roles, the attribution of which to distinct or indistinct persons is covered by the security policy of the organisation implementing the TOE.

Security officer

Security officers configure roles and access to administration tools and functions. They manage authentication resources for gaining access to administration tools or to the firewall.

Security administrator

Administrators (either local or remote) of the firewall. They define the filtering policy that the firewall shall apply. They define audit events to be logged and security alarms to be generated. They also analyse, process and delete security alarms generated.

Auditor

Auditors analyse and manage audit events relating to IP flow activity and administrative operations.

System and network administrator

Administrators responsible for the information system on which the firewall is located. They are responsible for maintaining the TOE in an operational state (including software and hardware maintenance).

They configure firewall network parameters and system parameters relating to the operational network contexts to be taken into account: they define the overall network topology, but do not define the filtering policy applied by the firewall.

It is also their role to control the status of the firewall.

Protected network user

A user of a protected network connected to another network via the firewall. By using applications, this user can send / receive information to / from another network via their network's firewall.

Unless a specific distinction is made, the administrator role in this document includes the following roles: security officer, security administrator, auditor and system and network administrator.

A.2 Architecture of the TOE

This section presents the TOE architecture in two different aspects: the physical aspect and the functional aspect.

A.2.1 Physical architecture

Figure 2 shows an example of a physical interconnection architecture for a network protected by a firewall, an architecture on the basis of which the TOE shall be evaluated.

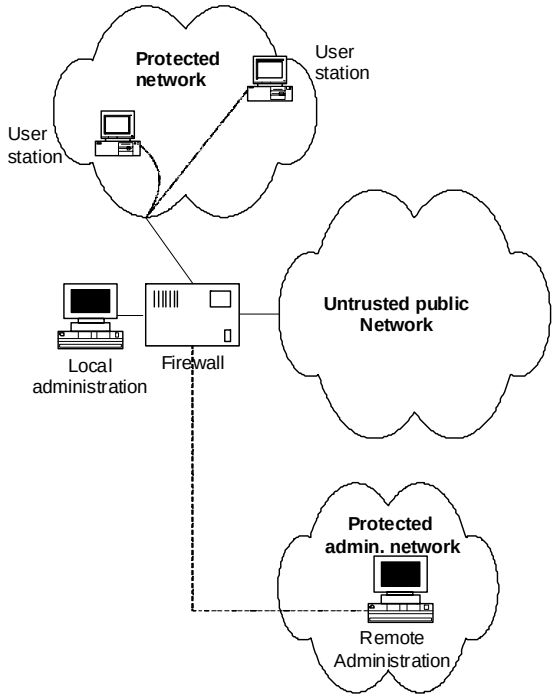

Figure 2: Example of a possible firewall interconnection architecture

As Figure 2 illustrates, the firewall has four logical external interfaces: an interface to the protected network, an interface to the public network, a local administration interface and a remote administration interface.

The firewall alone therefore ensures the interconnection between the protected network and the public network. It may however be inserted within a wider IP network interconnection structure (see [PB-INT]) and allow the protected network to be separated into several sub-networks, notably by providing a specific interface to a DMZ-type sub-network. The impact of this possibility must be studied specifically by the author of the security target.

A.2.2 Functional architecture

The diagrams in this section show the elements that make up the TOE at the functional level. These elements are greyed in the diagrams. Assets appear in italics. The other elements are outside the scope of the TOE.

These diagrams are for illustrative purposes and present an abstract overview of the TOE's functional architecture. The layout of the services shown in these diagrams does not therefore necessarily correspond to a given implementation.

Figure 3 presents the functionalities related to role management.

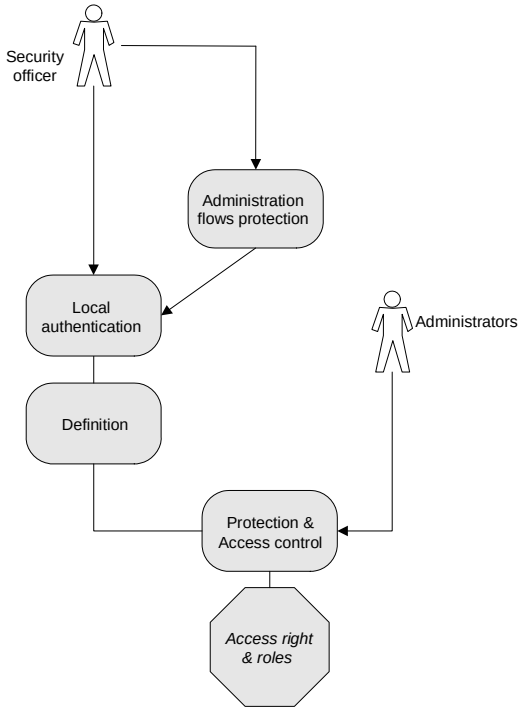

Figure 3: Role management

Figure 4 presents the functionalities relating to filtering policy management and rules governing connection contexts (in contextual mode). All the services are part of the TOE, except the remote authentication of the security administrator. The 'protection of administration flows' service includes both the service protecting the authenticity of remote administration flows and that offering protection against the replay of administration flows. This is also the case in the following diagrams.

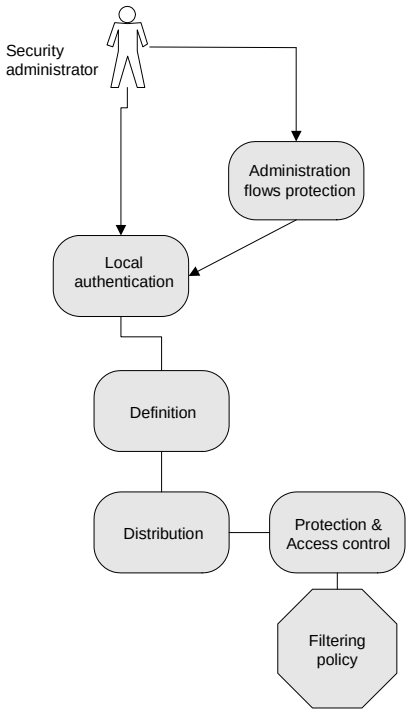

Figure 4: Filtering policy management

Figure 5 presents the functionalities relating to the application of the filtering policy and rules governing connection contexts (in contextual mode).

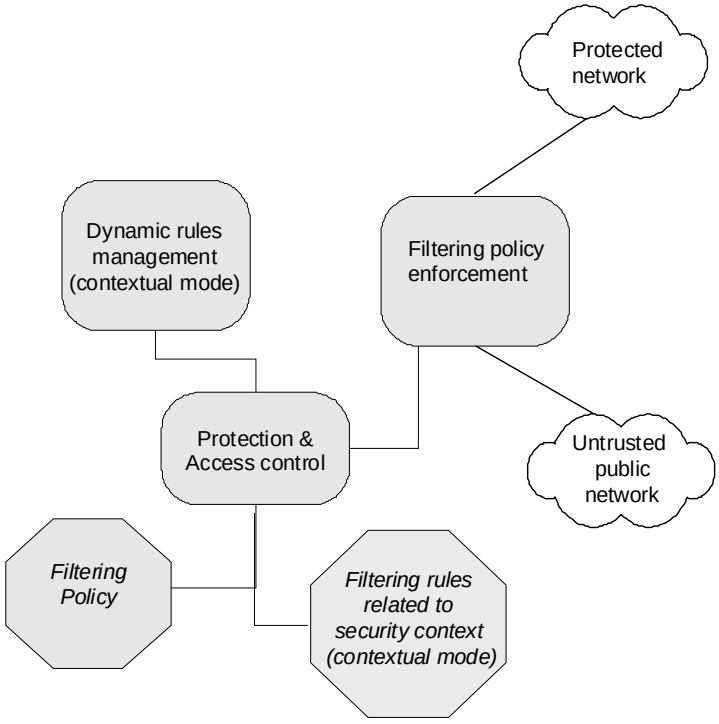

Figure 5: Application of the filtering policy

Regarding firewall configuration, the remote authentication of the system and network administrator is not part of the TOE (Figure 6). This diagram does not present all TOE services with read access to configuration parameters as they are too numerous. These services include, among others, local authentication services, the application of the filtering policy and all services consulting access rights and internal IP addresses for their own needs.

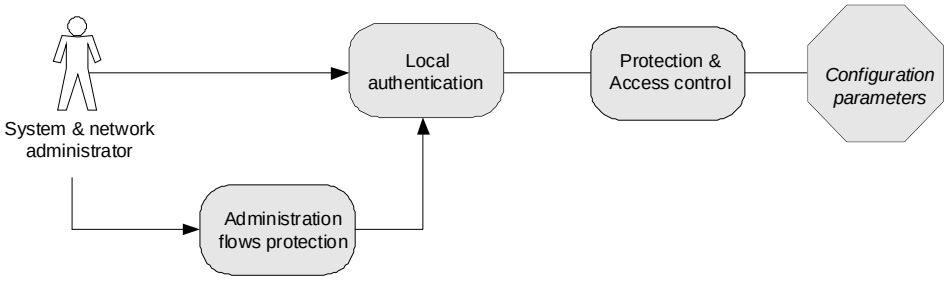

Figure 6: Configuration of the firewall

Regarding audit management, the remote authentication of the system and network administrator and of the auditor is not part of the TOE (Figure 7).

In practice, the definition of events to be audited (audit policy) is covered by:

- the definition of the filtering policy for events relating to user flows
- the definition of configuration parameters concerning events relating to administrative operations

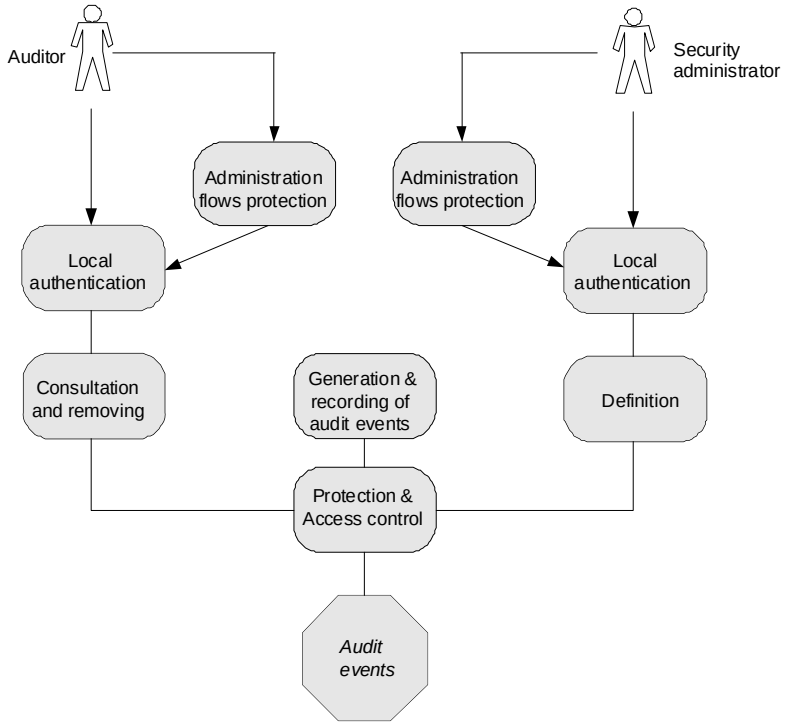

Figure 7 Audit management

Regarding security alarms, the remote authentication of the security administrator and the processing of alarms are not part of the TOE (Figure 8).

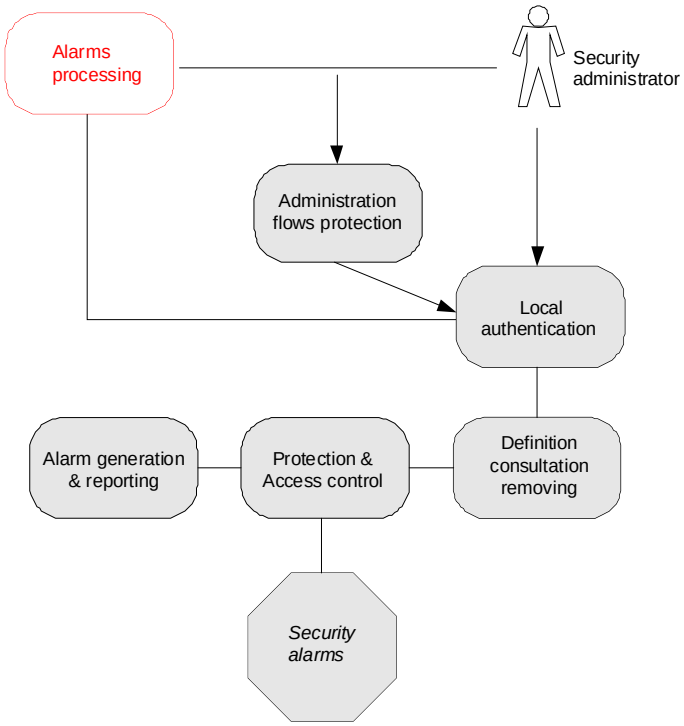

Figure 8 Security alarm management

Regarding monitoring, the remote authentication of the system and network administrator is not part of the TOE (Figure 9).

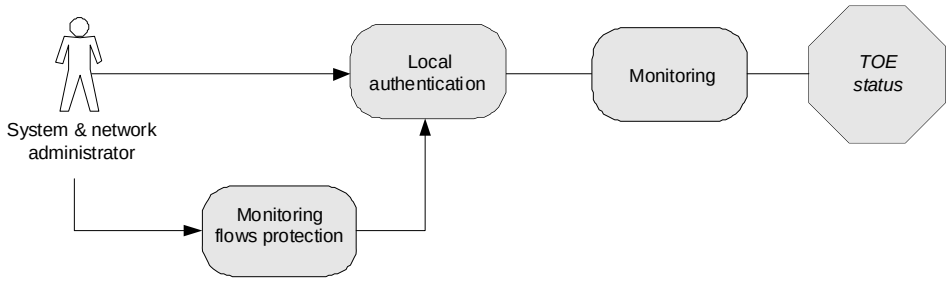

Figure 9 Monitoring of the TOE

Appendix B Minimal audit trails and associated level

For each functional requirement defined in Part 2 of the CC v3.1r2, it is recommended to take into account some of the audit trails of the FAU_GEN requirements. The table below summarises these recommendations for the functional requirements included in PP-FWIP, and establishes the applicable audit level.

PP-FWIP Requirement	**Part 2 CC Recommendation**	**Retained level**
FDP_IFC.2-flow_filtering	N/A	N/A
FDP_IFF.1-flow_filtering	a) Minimal: Decisions to permit requested information flows. b) Basic: All decisions on requests for information flow. c) Detailed: The specific security attributes used in making an information flow enforcement decision. d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	Basic
FMT_SMF.1-filtering_policy_visualisation	a) Minimal: Use of the management functions.	Minimal
FAU_GEN.1-flow_audit	N/A	
FAU_GEN.2-flow_audit	N/A	
FIA_UID.2-flow	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Basic
FPT_STM.1	a) Minimal: changes to the time; b) Detailed: providing a timestamp.	Minimal
FAU_SAR.1-flow_audit	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.3-flow_audit	a) Detailed: the parameters used for the viewing.	-
FMT_SMR.1	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	Minimal
FIA_UID.2-administrator	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Basic
FIA_UAU.2-administrator	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	Basic
FDP_ACC.1-filtering_rules	N/A	
FDP_ACF.1-filtering_rules	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Basic
FAU_STG.1-flow_audit_trail	N/A	
FAU_GEN.1-admin_audit	N/A	
FAU_GEN.2-admin_audit	N/A	
FAU_SAR.1-admin_audit	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.3-admin_audit	a) Detailed: the parameters used for the viewing.	-

PP-FWIP Requirement	Part 2 CC Recommendation	Retained level
FAU_STG.1-admin_audit_trail	N/A	
FAU_SAA.1-alarm	a) Minimal: Enabling and disabling of any of the analysis mechanisms; b) Minimal: Automated responses performed by the tool.	Minimal
FAU_ARP.1-alarm	a) Minimal: Actions taken due to potential security violations.	Minimal
FTP_ITC.1-remote_administration	a) Minimal: Failure of the trusted channel functions. b) Minimal: Identification of the initiator and target of failed trusted channel functions. c) Basic: All attempted uses of the trusted channel functions. d) Basic: Identification of the initiator and target of all trusted channel functions.	Minimal
FPT_ITI.1-remote_administration	a) Minimal: the detection of modification of transmitted TSF data. b) Basic: the action taken upon detection of modification of transmitted TSF data.	Basic
FPT_RPL.1-remote_administration	a) Basic: Detected replay attacks. b) Detailed: Action to be taken based on the specific actions.	Detailed
FPT_ITC.1-remote_administration	N/A	
FPT_TDC.1-remote_administration	a) Minimal: Successful use of TSF data consistency mechanisms. b) Basic: Use of the TSF data consistency mechanisms. c) Basic: Identification of which TSF data have been interpreted. d) Basic: Detection of modified TSF data.	Basic
FMT_SMF.1-TOE_configuration	a) Minimal: Use of the management functions.	Minimal
FMT_MTD.1-configuration_parameter	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1-security_officer	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1-auditor	a) Basic: All modifications to the values of TSF data.	Basic
FMT_SMF.1-monitorig	a) Minimal: Use of the management functions.	Minimal
FPT_ITC.1-monitorig	N/A	
FDP_RIP.1-TOE_reuse	N/A	
FDP_ACC.1-filtering_rules	N/A	
FDP_ACF.1-filtering_rules	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Basic

Appendix C Definitions and acronyms

A.3 Acronyms

CC Common Criteria

EAL Evaluation Assurance Level.
An assurance package, consisting of assurance requirements drawn up from CC Part 3, representing a point on the CC predefined assurance scale.

IP Internet Protocol.

IT Information Technology.

OSP Organisational Security Policies.
A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment.

PP Protection Profile.
An implementation-independent statement of security needs for a TOE type.

SF Security Function.
A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

SFP Security Function Policy.
a set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.

ST Security Target.
An implementation-dependent statement of security needs for a specific identified TOE.

TOE Target of Evaluation.
A set of software, firmware and/or hardware possibly accompanied by guidance.

TSF TOE Security Functionality.
A set consisting of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

A.4 Definitions

Administrator

Users authorised to manage all or part of the TOE. They may have particular privileges enabling them to modify the TOE security policy.

Authentication

A security measure for checking the stated identity.

Mutual authentication

Security measure enabling each pair of entities to authenticate the other entity of the pair.

Operational environment

TOE environment when in use.

Filtering policy

Security policy defined for managing interconnection data flows.

Filtering rules relating to connection contexts

Filtering rules established by the TOE, following an initial non-contextual filtering, based on the nature of the identified flow (origin, destination, application protocol, etc.). Knowledge of this context allows the TOE to free itself from explicit filtering rules thereby improving performance.

Editorial refinement

Refinement according to which a minor modification is made to a requirement item, for example the reformulation of a phrase to respect syntax. In no case shall this modification change the significance of the requirement.
This term is defined in [CC1].

Non-editorial refinement

Refinement to achieve greater precision or to limit the set of acceptable implementations for a requirement item.

Overall refinement

Non-editorial refinement concerning all the requirement items of a same component.

Protected network

A network internal to an entity (such as a business or department) that must be protected from flows arriving from the outside, and for which outgoing flows must be controlled. This network is regarded as being trusted.

Public network

A network accessible by any entity or person, and that cannot be considered trusted.

Appendix D References

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2006, Version 3.1, Release 1, CCMB-2006-09-001
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, September 2007, Version 3.1, Release 2, CCMB-2007-09-002
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, September 2007, Version 3.1, Release 2, CCMB-2007-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2007, Version 3.1, Release 2, CCMB-2007-09-004
[CRYPTO]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level (regularly updated version) http://www.ssi.gouv.fr/fr/sciences/publications
[CRYPTO_GESTION]	Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard http://www.ssi.gouv.fr/fr/sciences/publications
[AUTH]	Authentification - Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard http://www.ssi.gouv.fr/fr/sciences/publications
[PB-INT]	Problématique d'interconnexion des réseaux IP (Issues relating to the interconnection of IP networks), Version 1.9, March 2004, Premier Ministre, Secrétariat général de la défense nationale, Direction Centrale de la Sécurité des Systèmes d'Information, Sous-direction scientifique et technique, Laboratoire Technologies de l'Information
[PP-CIP]	Profil de Protection - Chiffreur IP - Version 1.5, 3 February 2005 Reference: PPnc/0502 - SGDN/DCSSI
[QUA-STD]	Processus de qualification d'un produit de sécurité - niveau standard - version 1.1 - 18 March 2008, DCSSI, N°549/SGDN/DCSSI/SDR

Appendix E Index