Common Criteria

Common Criteria
for Information Technology
Security Evaluation

CONFIGURABLE SECURITY GUARD (CSG)

PROTECTION PROFILE

Version 3.3

99/03/04

ecf

Evaluation et Certification Française

Registered by the French Certification Body under the reference PP/9906

Table of Contents

1. INTRODUCTION

1.1. PP IDENTIFICATION

TITLE :	Configurable Security Guard V3.3 - CSG V3.3
REGISTRATION :	PP/9906
KEYWORDS :	TCP/IP, Application Protocols (FTP, SMTP, HTTP, TELNET, SQL), Filtering, Audit, Covert Channels, Tunnelling, Authentication, Encipherment, Signature.

1.2. PP OVERVIEW

The purpose of this Protection Profile consists in defining a set of security and assurance requirements for a trusted filtering device which interconnects two networks (local or wide) with different levels of sensitivity as depicted in the following figure :

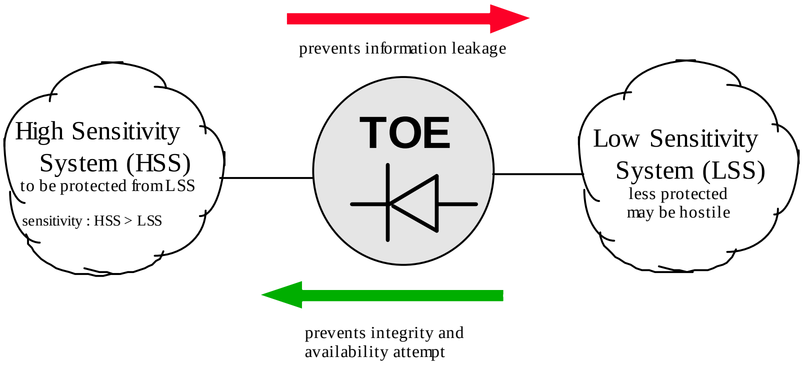
prevents information leakage
High Sensitivity System (HSS)
to be protected from LSS
sensitivity : HSS > LSS
TOE
Low Sensitivity System (LSS)
less protected
may be hostile
prevents integrity and availability attempt

Figure 1-1 : The TOE as a logical and physical boundary device between two systems

This PP describes a TOE (Target Of Evaluation) that provides incoming and outgoing traffic filtering functions to protect the High Sensitivity System (HSS) from Low Sensitivity System (LSS). This selective filtering avoids intrusion (prevents integrity and availability of HSS) from LSS to HSS and allows the controlled leakage of information from HSS to LSS. The HSS is a local area network while LSS could be a local or wide area network (e.g. INTERNET).

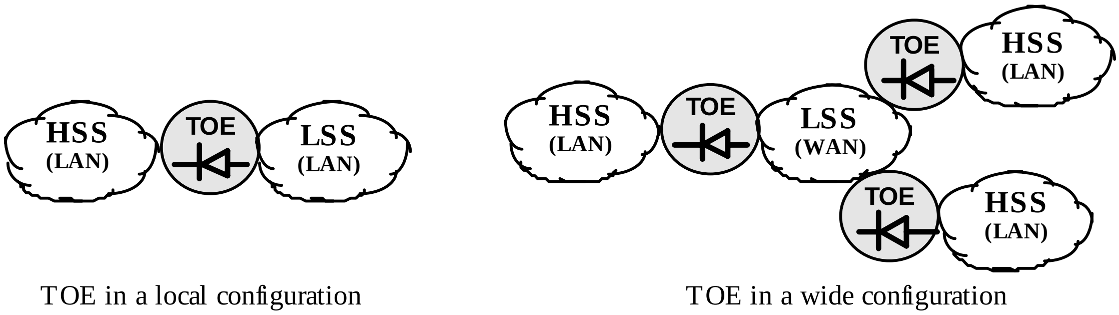

Figure 1-2 : Multiple configurations of the TOE

The security filtering functions realised by the TOE are based on the control of TCP/IP and application protocols (file transfer, messaging system, ...). Moreover, the TOE implements also tunnelling (authentication, encipherment and signature) to interconnect local networks through a wide area network. Finally, security policy violations are detected by the TOE and audited by trusted staff.

This PP is compliant with Common Criteria V2.0.

1.3. RELATED PP

Configurable Security Guard V2.0 - CSG V2.0

1.4. REFERENCES

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1 : Introduction and General Model. CCIB-98-026, version 2.0, May 1998.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2 : Security functional requirements. CCIB-98-027, version 2.0, May 1998.

[CC2A] Common Criteria for Information Technology Security Evaluation, Part 2 : Annexes : CCIB-98-027A_A, version 2.0, May 1998.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3 : Security assurance requirements. CCIB-98-028, version 2.0, May 1998.

2. TOE DESCRIPTION

The purpose of the TOE is to connect two networks with different levels of sensitivity called the HSS (High Sensitivity System) and the LSS (Low Sensitivity System) in a way that the TOE maintains the security policy of HSS.

The TOE is a Firewall designed to be the only interconnection point (physical and logical) between HSS and LSS. As shown in the following figures, two configurations are allowed : HSS is a local area network and LSS is either a local (Fig 2-1) or a wide area network (Fig 2-2) :

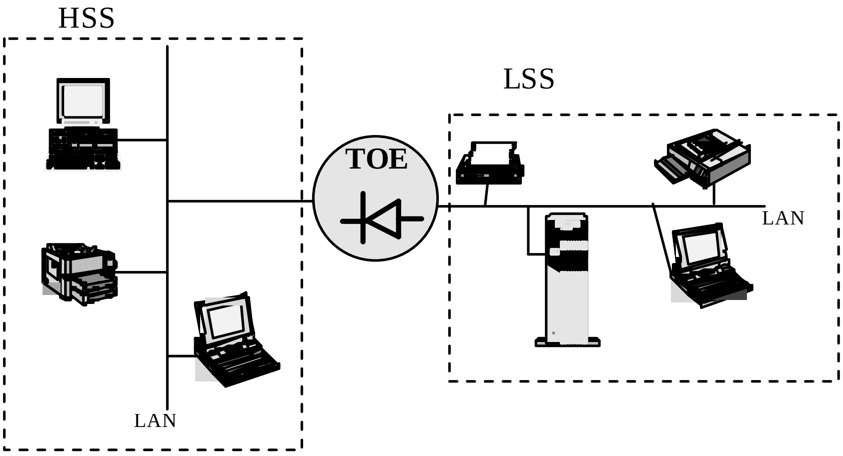

Figure 2-1 : The TOE in a local network configuration

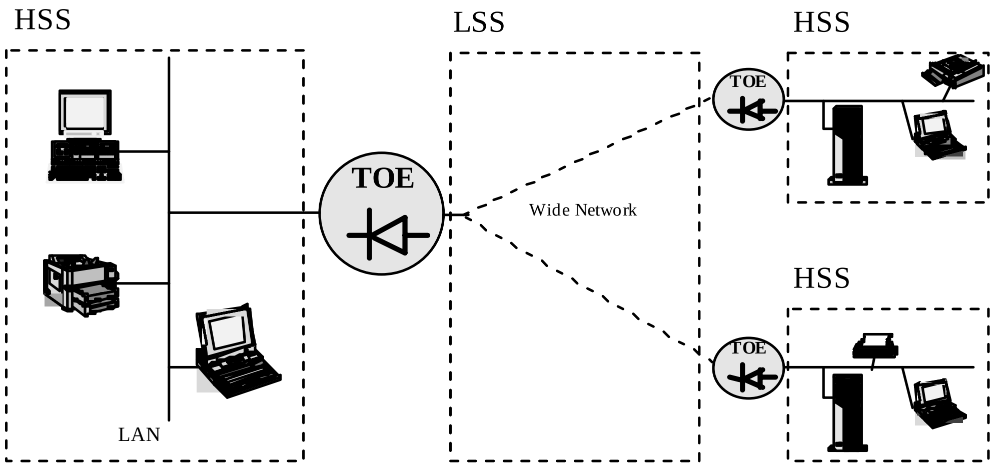

Figure 2-2 : The TOE in a wide network configuration

To be compliant with the operational environment, the communication model addressed by the TOE is the INTERNET communication model. The following figure points out this communication stack :

Application SQL, FTP, SMTP, TELNET, HTTP
Transmission TCP / UDP
Interconnection IP (ICMP)
Physical Ethernet

Figure 2-3 : The TOE communication model

In such a context, to prevent intrusions from LSS and data leakage from HSS, the TOE must filter each communication layer of the model. Thus, the TOE must filter :

- the lower layer protocols of the model :
  - the interconnection protocol IP (internet protocol),
  - the transmission protocol TCP (transmission control protocol),
- the higher layer protocols of the model :
  - the messaging protocol SMTP (simple mail transfer protocol),
  - the file transfer protocol FTP (file transfer protocol),
  - the database access protocol SQL (standard query language),
  - the web protocol HTTP (hyper text transfer protocol),
  - the virtual terminal protocol Telnet (terminal network).

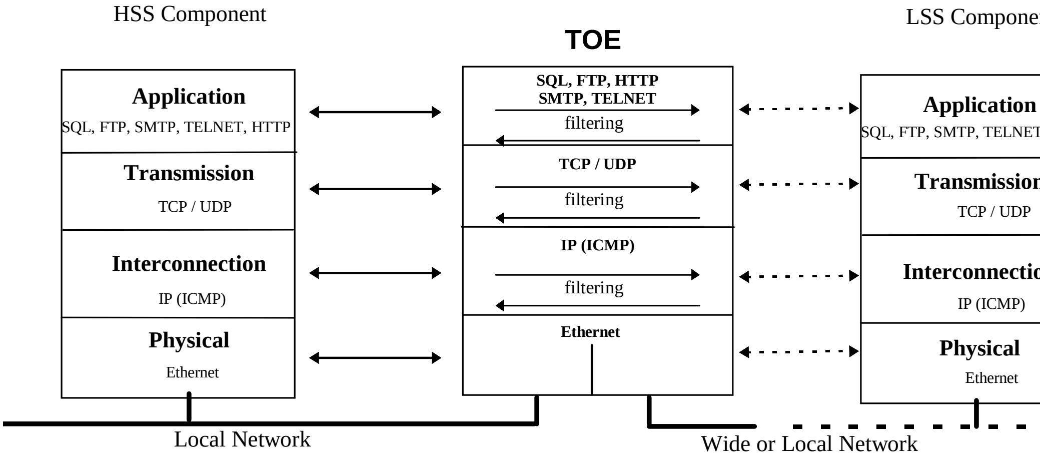

Figure 2-4 : Filtering principles of the TOE

Additionally, in the wide network configuration, the TOEs have to protect inter-TOE communication from WAN threats (data tampering, ...) as depicted in the following figure :

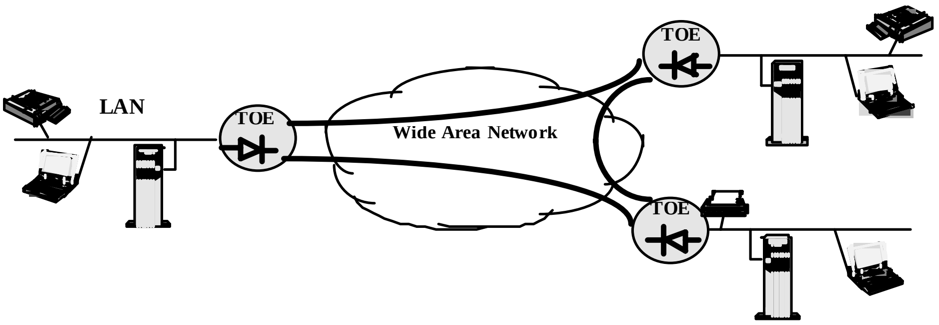

Figure 2-5 : Inter-TOE communications

Trusted path (realised by authentication, encipherment and signature functions) between widely interconnected TOEs allows secured communications. Each TOE has its own security policy and the global security policy consistency (cryptology consistency for example) must be maintained by the global security supervisor.

Additionally, the TOE provides accountability and audit functionality which allow security policy violation detection.

3. SECURITY ENVIRONMENT

3.1. METHODOLOGY APPROACH

The methodology approach used to realise this PP is the following :

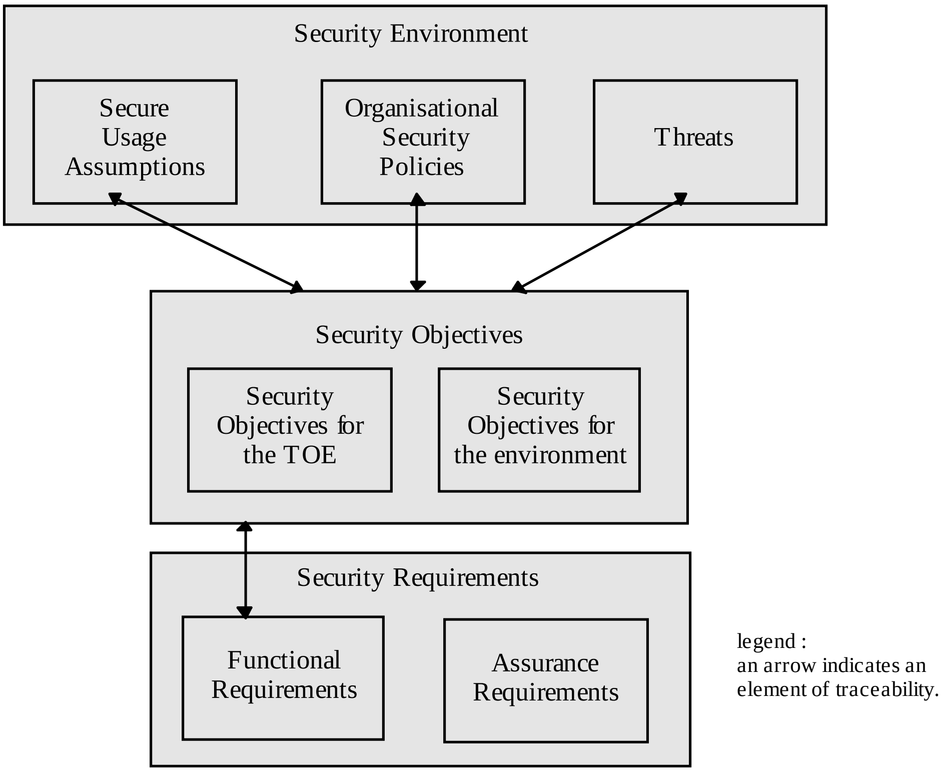
Security Environment
Secure Usage Assumptions
Organisational Security Policies
Threats
Security Objectives
Security Objectives for the TOE
Security Objectives for the environment
Security Requirements
Functional Requirements
Assurance Requirements
legend :
an arrow indicates an element of traceability.

Figure 3-1 : Methodology approach

3.2. SUMMARY

Compliant firewalls are intended for use in very sensitive commercial and defence environments. This is why a compliant firewall provides a high level of assurance and a very full set of security functions.

3.3. Secure Usage Assumptions

3.3.1. Physical Assumptions

A.PHY_ACCESS
[All configurations]

The access to the TOE is limited to authorised personnels (Security Officer, TOE Operator and TOE Administrator). Thus, the TOE is stored in an access controlled room.

A.PHY_SINGLE
[All configurations]

The TOE is the unique and single access between HSS and LSS. There is no other connection (e.g. modem).

3.3.2. Organisational Assumptions

There is no organisational assumption.

3.3.3. Staff Assumptions

A.STAFF_TRAINED
[All configurations]

The authorised personnels are well trained to perform their role.

A.STAFF_NOEVIL
[All configurations]

The authorised personnels (Security Officer, the TOE Operator and the TOE Administrator) and the Global Security Supervisor are non-hostile and trusted to perform their role correctly.

3.4. THREATS

The threats addressed in this section concern :

- intrusion/overloading on/of HSS from LSS [all configurations],
- information leakage from HSS to LSS [all configurations],
- information tampering during TOE to TOE communication [WAN configuration only],
- threats on the TOE itself [all configurations].

3.4.1. THREATS ADDRESSED BY THE TOE

T.INTRUSION

[All configurations]

An hostile person, connected to LSS, accesses to HSS resources and realises intelligent actions :

- access (read/write/erase) to sensitive information (sensitive user data of workstations and servers, configuration data of bridges / routers / HUBs, ...) ;
- access to unauthorised services (private applications, CPU/disk of mainframe, ...).

T.OVERLOADING

[All configurations]

An hostile entity, connected to LSS, accesses to HSS local network and can overload HSS (servers, printers and network devices, the LAN itself, bridges / routers / HUBs, ...). This kind of threat only consists in attacking the availability of HSS resources (via high traffic of IP datagrams or multiple TCP connection requests) whereas T.INTRUSION considers HSS resources integrity and confidentiality attacks.

T.PROBING

[All configurations]

An hostile entity, connected to LSS, tries to deduce the HSS network topology to prepare a further attack. The hostile entity can use probes (via ping-pong ICMP requests or TCP connection requests) to test IP address masks.

T.LEAKAGE

[All configurations]

An authorised entity, connected to HSS, accesses intentionally or not (with a destination error) to LSS and can :

- disclose sensitive information (sensitive user data, topology information [IP route recording], ...) ;
- access unauthorised LSS services (e.g. internet services).

This threat can use direct channels (a file, a mail, ...) or covert channels (TCP/IP or application covert channels).

T.TAMPERING

[WAN configuration]

An hostile entity, connected on the WAN, can have access to the information exchanged between TOEs. The hostile entity can :

- hijack a session with a TOE (on an established TCP connection) ;
- replay information (authentication sequence, ...) ;
- modify the information ;
- disclose the information (user data, authorised HSS IP address, ...) ;
- destroy the information.

T.TOE_INTRUSION

[All configurations]

An hostile entity, connected on LSS or HSS, can have a remote access on the TOE. This allows the hostile entity to :

- modify the security policy (by changing the TOE filtering parameters, ...) in a passing or blocking way ;
- disclose / modify / destroy the TOE secret and sensitive elements.

3.4.2. THREATS ADDRESSED BY THE OPERATING ENVIRONMENT

T.TOE_BAD_OPE

[All configurations]

An hostile, negligent or careless authorised personnel can exceed his rights :

- bad installation of the TOE ;
- poor TOE configuration ;
- ignoring audit ;
- ...

In such a context, the TOE does not implement a valid security policy.

T.TOE_PHYSICAL

[All configurations]

An hostile intruder may have physical access to the TOE and can :

- modify the physical TOE’s connections and make the TOE passing or blocking ;
- destroy the TOE ;
- steal sensitive information (passwords / keys on a stolen hard disk).

In such a context, the TOE does not implement a valid security policy.

3.5. ORGANISATIONAL SECURITY POLICIES

P.ROLE

[All configurations]

For the TOE, there are three authorised personnels roles :

- the Security Officer who is in charge of the TOE security management, administration, operations including creation, deletion or modification of local operator accounts, definition of a minimum default level of security stringency, definition of a minimum default level of audit (logged events), security audit, integrity verification ;
- the TOE Operator who is in charge of the effective enforcement of the security policy (entry and update of filtering parameters, entry and update of the lists of HSS and LSS authorised users,...);
- the TOE Administrator (or « system engineer ») is in charge of the TOE IT management (hardware and software administration, operation of the TOE computing environment including creation or modification of software releases, maintenance, ...)

These previous roles will be enforced only after a personnel identification and authentication procedure.

P.WAN_ROLE

[WAN configuration]

This element of security policy includes a new role for the consistency of the global security policy (consistency of secret elements shared between the different TOEs, ...). This new role consists in a ***global security supervisor***. This role does not allow any access to the TOE.

P.AUDIT

[All configurations]

The security relevant events (internal to the TOE or due to the communication flows) must be detected and registered. The audit trail analysis is executed in order to hold the authorised personnels accountable for their actions and to trace attack attempts from networks.

Only the Security Officer and the TOE Operator are allowed to analyse the audit trail. The Security Officer analyses the internal events due to the TOE and the TOE Operator the events due to the communication flows.

P.CONFIG

[All configurations]

The configuration modification (filtering policy) of the TOE must be possible during an acceptable time in operational terms by the authorised personnels. These modifications can be predefined and stored in a timetable.

P.NO_BYPASS

[All configurations]

There must be no way to bypass the security policy enforced by the TOE.

4. SECURITY OBJECTIVES

4.1. SECURITY OBJECTIVES FOR THE TOE

O.ACCESS_CTL

[All configurations]

The TOE must provide controlled access between the connected networks by filtering the accesses through rules defined by the TOE Operator. The direct channel (e.g. FTP) as well as the covert channel (e.g. TCP header) must be controlled and filtered by the TOE.

For certain kind of applications, filtering can be previously completed by user authentication.

The filtering rules are based on the identity of the users, the type of application, the commands used with their options, and the data flow control.

O.AUDIT

[All configurations]

All the security relevant events must be recorded and utilised. This means to record the following information :

- the security relevant operations performed directly on the TOE by the Security Officer, the TOE Operator and the TOE Administrator ; these events are then analysed by the Security Officer.
- the security relevant communication flows (with header information) treated by the TOE ; these events are then analysed by the TOE Operator.

O.FLOW_CTL

[All configurations]

The HSS must be protected against overload attacks. The TOE must provide a control over the throughput, the number of connection requests and the frequencies of connection requests.

O.MASK_TOPO

[All configurations]

The HSS must be protected against probing attack from LSS. The topology of the HSS network must not be guessed.

O.TOE_I&A

[All configurations]

Only the authorised personnels (Security Officer, TOE Operator and TOE Administrator) can locally access to the TOE. Thus the TOE must identify and authenticate the personnels before performing any other action.

O.TOE_ACCESS_CTL

[All configurations]

The TOE must prevent authorised personnels to access operation and object which are not allowed to their role. The Security Officer must define a minimum level of filtering and accountability.

To enforce this objective, the data in the TOE must be protected.

O.TUNNEL_PROTECT

[WAN configuration]

The TOE must be able to protect the tunnel established when several TOEs are communicating. The TOE must ensure that the data exchanged are secured in terms of confidentiality and integrity.

O.MANAGEMENT

[All configurations]

The authorised personnels must be able to perform all the functions due to their role. The TOE must be sure that any modifications in administrative functions are valid.

O.TOE_CONFIG
[All configurations]

The configuration modifications of the TOE must be possible during an acceptable time in operational terms.

O.TOE_NOREMOTE
[All configurations]

No remote access to the TOE is allowed.

Only local access for administration and configuration are allowed on the TOE.

O.NO_BYPASS
[All configurations]

They must be no way to bypass the security functions enforced by the TOE security policy defined by the security officer.

4.2. Security Objectives for the environment

O.PHY_ACCESS
[All configurations]

The TOE must be protected against unauthorised physical access.

O.PHY_SINGLE
[All configurations]

The TOE must be the unique and single access between HSS and LSS.

O.STAFF_TRAINED
[All configurations]

The authorised personnels must be well trained to perform their role.

O.STAFF_NOEVIL
[All configurations]

The Security Officer, the TOE Operator, the TOE Administrator and the Global Security Supervisor must be non-hostile and trusted to perform their role correctly.

5. IT SECURITY REQUIREMENTS

5.1. TOE IT SECURITY REQUIREMENTS

5.1.1. FUNCTIONAL REQUIREMENTS

5.1.1.1. SYNTHESIS OF FUNCTIONAL REQUIREMENTS

The following tables show the different security requirements chosen for this PP :

Security Audit		
FAU_ARP.1	=>	Security alarms
FAU_GEN.1	=>	Audit data generation
FAU_GEN.2	=>	User identity association
FAU_SAA.1	=>	Potential violation analysis
FAU_SAR.1	=>	Audit review
FAU_SAR.3	=>	Selectable audit review
FAU_SEL.1	=>	Selective audit
FAU_STG.2	=>	Guarantees of audit data availability

User Data Protection		
FDP_ACC.2	=>	Complete access control
FDP_ACF.1	=>	Security attribute based access control
FDP_IFC.2	=>	Complete information flow control
FDP_IFF.1	=>	Simple security attributes
FDP_IFF.3	=>	Limited illicit information flows
FDP_ITT.1	=>	Basic internal transfer protection
FDP_RIP.1	=>	Subset residual information protection

Identification and authentication		
FIA_AFL.1	=>	Authentication failure handling
FIA_ATD.1	=>	User attribute definition
FIA_SOS.1	=>	Verification of secrets
FIA_SOS.2	=>	TSF generation of secrets
FIA_UAU.1	=>	Timing of authentication
FIA_UAU.4	=>	Single-use authentication mechanisms
FIA_UAU.5	=>	Multiple authentication mechanisms
FIA_UID.2	=>	User identification before any action
FIA_USB.1	=>	User-subject binding

Security management		
FMT_MOF.1	=>	Management of security functions behaviour
FMT_MSA.1	=>	Management of security attributes
FMT_MSA.2	=>	Secure security attributes
FMT_MSA.3	=>	Static attribute initialisation
FMT_MTD.1	=>	Management of TSF data
FMT_MTD.2	=>	Management of limits on TSF data
FMT_REV.1	=>	Revocation
FMT_SMR.2	=>	Restrictions on security roles
FMT_SMR.3	=>	Assuming roles

Protection of the TOE Security Functions		
FPT_AMT.1	=>	Abstract machine testing
FPT_ITC.1	=>	Inter-TSF confidentiality during transmission
FPT_ITI.1	=>	Inter-TSF detection of modification
FPT_RPL.1	=>	Replay detection
FPT_RVM.1	=>	Non-bypassability of the TSP
FPT_SEP.1	=>	TSF domain separation
FPT_STM.1	=>	Reliable time stamps
FPT_TST.1	=>	TSF testing

TOE Access		
FTA_LSA.1	=>	Limitation on scope of selectable attributes
FTA_TSE.1	=>	TOE session establishment

Trusted Path / Channels		
FTP_ITC.1	=>	Inter-TSF trusted channel
FTP_TRP.1	=>	Trusted path

Table 5-1 : Summary of functional requirements

5.1.1.2. SECURITY AUDIT (FAU)

FAU_ARP.1 => Security alarms

FAU_ARP.1.1 : The TSF shall take [**the least disruptive actions**] upon detection of a potential security violation.

Refinement :

a) The least disruptive action is to generate an alarm to the security officer or to the TOE operator and to destroy the threat vector (e.g. TCP connection, local session for administration or configuration).

b) The TOE operator or the security officer selects which security events must be defined as an alarm. Once detected, the alarm would be urgently treated by the operator or the security officer.

c) As defined in P.AUDIT, the internal events are linked with the security officer and the events due to communication flow to the TOE operator.

FAU_GEN.1 => Audit data generation

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

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

b) All auditable events for the [**detailed**] level of audit; and

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

Refinement :

a) The following table gives the auditable events.

b) The ST author shall add auditable events.

The following tables give the auditable events :

Legend :

normal -> event issues from CC part 2,
bold -> additional auditable event defined by the PP author

Class FAU	Security Events
FAU_ARP.1	• Actions taken due to imminent security violations.
FAU_GEN.1	• none
FAU_GEN.2	• none
FAU_SAA.1	• Enabling and disabling of any of the analysis mechanisms, • Automated responses performed by the tool.
FAU_SAR.1	• Reading of information from the audit records.
FAU_SAR.3	• The parameters used for the viewing.
FAU_SEL.1	• All modifications to the audit configuration that occur while the audit collection functions are operating.
FAU_STG.2	• none

Class FDP	Security Events
FDP_ACC.2	• none
FDP_ACF.1	• All requests to perform an operation on an object covered by the SFP, • The specific security attributes used in making an access check.
FDP_IFC.2	• none
FDP_IFF.1	• All decisions on requests for information flow, • The specific security attributes used in making an information flow enforcement decision, • Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).
FDP_IFF.3	• All decisions on requests for information flow, • The use of identified illicit information flow channels, • The specific security attributes used in making an information flow enforcement decision, • Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material), • The use of identified illicit information flow channels with estimated maximum capacity exceeding a specified value.
FDP_ITT.1	• All attempts to transfer user data, including the protection method used and any errors that occurred.
FDP_RIP.1	• none

Class FIA	Security Events
FIA_AFL.1	• The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).

Class FIA	Security Events
FIA_ATD.1	• none
FIA_SOS.1	• Rejection or acceptance by the TSF of any tested secret, • Identification of any changes to the defined quality metrics.
FIA_SOS.2	• id FIA_SOS.1
FIA_UAU.1	• All use of the authentication mechanism, • All TSF mediated actions performed before authentication of the user.
FIA_UAU.4	• Attempts to reuse authentication data.
FIA_UAU.5	• The result of each activated mechanism together with the final decision on authentication.
FIA_UID.2	• All use of the user identification mechanism, including the user identity provided.
FIA_USB.1	• Success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject).

Class FMT	Security Events
FMT_MOF.1	• All modifications in the behaviour of the functions in the TSF.
FMT_MSA.1	• All modifications of the values of security attributes.
FMT_MSA.2	• All offered and rejected values for a security attribute, • All offered and accepted secure values for a security attribute.
FMT_MSA.3	• Modifications of the default setting of permissive or restrictive rules, • All modifications of the initial values of security attributes.
FMT_MTD.1	• All modifications to the values of TSF data.
FMT_MTD.2	• All modifications to the limits on TSF data, • All modifications in the actions to be taken in case of violation of the limits.
FMT_REV.1	• All attempts to revoke security attributes, • **Immediate revocation (reason, date/time, ...).**
FMT_SMR.2	• Modifications to the group of users that are part of a role, • Unsuccessful attempts to use a role due to the given conditions on the roles, • Every use of the rights of a role.
FMT_SMR.3	• Explicit request to assume a role.

Class FPT	Security Events
FPT_AMT.1	• Execution of the tests of the underlying machine and the results of the tests.
FPT_ITC.1	• **Confidentiality error (crypto error).**
FPT_ITI.1	• The detection of modification of transmitted TSF data, • The action taken upon detection of modification of transmitted TSF data, • **Integrity error (crypto error).**
FPT_RPL.1	• Detected replay attacks, • Action to be taken based on the specific actions.
FPT_RVM.1	• none

FPT_SEP.1	• none
FPT_STM.1	• Changes to the time, • Providing a timestamp.
FPT_TST.1	• Execution of the TSF self tests and the results of the tests, • **Integrity failure/success**. Refinement : integrity failure or success information could be useful if the administrator is not the security officer.

Class FTA	Security Events
FTA_LSA.1	• All attempts at selecting a session security attributes, • Capture of the values of each session security attributes.
FTA_TSE.1	• All attempts at establishment of a user session, • Capture of the value of the selected access parameters (e.g. location of access, time of access).

Class FTP	Security Events
FTP_ITC.1	• All attempted uses of the trusted channel functions, • Identification of the initiator and target of all trusted channel functions.
FTP_TRP.1	• All attempted uses of the trusted path functions, • Identification of the user associated with all trusted path invocations, if available.

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

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

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

Refinement :

a) The ST author shall define the other audit relevant informations.

FAU_GEN.2 => User identity association

FAU_GEN.2.1 : The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAA.1 => Potential violation analysis

FAU_SAA.1.1 : 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 TSP.

FAU_SAA.1.2 : The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;

b) [assignment: *any other rules*].

Refinement :

a) The ST author shall define the subset of auditable events.

b) The ST author shall define the other rules.

FAU_SAR.1 => Audit review

FAU_SAR.1.1 : The TSF shall provide [**the TOE operator**] with the capability to read [**filtering events**] from the audit records.

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

FAU_SAR.1 => Audit review

FAU_SAR.1.1 : The TSF shall provide [**the security officer**] with the capability to read [**security events**] from the audit records.

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

FAU_SAR.3 => Selectable audit review

FAU_SAR.3.1 : The TSF shall provide the ability to perform [**searches and sorting**] of audit data based on [

a) Time and date of event;

b) User or IP @ that caused the event;

c) Multiple criteria with logical relationships as specified by the ST author].

Refinement :

a) The ST author shall define other criteria with relationships.

FAU_SEL.1 => Selective audit

FAU_SEL.1.1 : The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [**object identity and/or user identity and/or subject identity and/or host identity and/or event type**]

b) [assignment: *list of additional attributes that audit selectivity is based upon*].

Refinement :

a) The ST author shall specify the additional attributes.

FAU_STG.2 => Guarantees of audit data availability

FAU_STG.2.1 : The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 : The TSF shall be able to [**prevent**] modifications to the audit records.

FAU_STG.2.3 : The TSF shall ensure that [assignment: *metric for saving audit records*] audit records will be maintained when the following conditions occur: [**audit storage exhaustion or failure or attack**].

Refinement :

a) The ST author shall specify the metric for saving audit records.

5.1.1.3. USER DATA PROTECTION (FDP)

FDP_ACC.2 => Complete access control

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

FDP_ACC.2.2 : The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Refinement :

a) The TSF shall ensure that all objects and operations within the TSC are controlled by the access control SFP. The operations on objects are operations from an operator (subject) on a TOE element (object) [e.g. a file].

FDP_ACF.1 => Security attribute based access control

FDP_ACF.1.1 : The TSF shall enforce the [**TOE internal access control policy**] to objects based on [assignment: *security attributes, named groups of security attributes*].

Refinement :

a) The ST author shall precise the security attributes and groups.

FDP_ACF.1.2 : The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

Refinement :

a) The ST author shall precise the different rules.

FDP_ACF.1.3 : 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*].

Refinement :

a) The ST author shall define the rules that explicitly authorise access of subjects to objects.

FDP_ACF.1.4 : 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*].

Refinement :

a) The ST author shall define the rules that explicitly deny access of subjects to objects.

FDP_IFC.2 => Complete information flow control

FDP_IFC.2.1 : The TSF shall enforce the [**TOE filtering policy**] on [**communication flows**] and all operations that cause that information to flow to and from subjects covered by the SFP.

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

FDP_IFF.1 => Simple security attributes

FDP_IFF.1.1 : The TSF shall enforce the [**TOE filtering policy**] based on the following types of subject and information security attributes: [

a) **network origin identity of the communication flow (e.g., IP address) ;**
b) **network destination identity of the communication flow (e.g., IP address) ;**
c) **user origin identity of the communication flow (user name) [for authentication] ;**
d) **user destination identity of the communication flow (user name or IP address) ;**
e) **sender authentication data (e.g., password) ;**
f) **type of application (e.g., FTP, SQL, HTTP, SMTP, TELNET,...) ;**
g) **type of application command requested (e.g., FTP « get », SQL « select »,...) ;**
h) **format of the commands (e.g., lowercase, uppercase, length of commands, ...);**
i) **date / time of the access ;**
j) **correctness and filtering of communication (TCP/IP) and application protocols (see g.)**
k) **number, frequency and throughput of communication flow ;**
l) **IP address translation ;**
m) **any other multiple attributes will be specified by the ST author.**]

Refinement :

a) An example of user name could be a directory name (e.g., DNS name ; URL ...), a messaging name (e.g., user@domain.com) ...

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

Refinement :

a) The ST author shall precise the different operations and associated rules.

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

Refinement :

a) The ST author shall precise the additional rules.

FDP_IFF.1.4 : The TSF shall provide the following [assignment: *list of additional SFP capabilities*].

Refinement :

a) The ST author shall precise the additional capabilities.

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

Refinement :

a) The ST author shall define the rules that explicitly authorise information flows.

FDP_IFF.1.6 : The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

Refinement :

a) The ST author shall define the rules that explicitly deny information flows.

FDP_IFF.3 => Limited illicit information flows

FDP_IFF.3.1 : The TSF shall enforce the [**TOE filtering policy**] to limit the capacity of [**illicit data intrusion or sensitive data leakage]** to a **[acceptable throughput**].

Refinement :

a) The information flow control SFP is the covert channels eradication or limitation.

b) The ST author shall specify for each INTERNET layer the limitation of covert channels (sequential and storage covert channels ; covert channels acceptable throughput : e.g. 100 b/s max).

c) For each layer of figure 2-3 (INTERNET model) the maximum capacity shall be given by the ST author.

FDP_ITT.1 => Basic internal transfer protection

FDP_ITT.1.1 : The TSF shall enforce the [**TOE internal access control policy**] to prevent the [**disclosure and modification**] of user data when it is transmitted between physically-separated parts of the TOE.

FDP_RIP.1 => Subset residual information protection

FDP_RIP.1.1 : The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**allocation of the resource to**] the following objects: [**some objects linked to the disk or memory**].

Refinement :

a) The ST author shall define which objects will be made unavailable.

5.1.1.4. IDENTIFICATION AND AUTHENTICATION (FIA)

FIA_AFL.1 => Authentication failure handling

FIA_AFL.1.1 : The TSF shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [**security officer's or TOE operator's authentication, network users' authentication or TOE to TOE authentication**].

FIA_AFL.1.2 : When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**take the following actions :**

- **for security officer's or TOE operator's authentication, all the operator's login are disabled, except the TOE administrator's one and an alarm is generated.**
- **for network users, the user's login is disabled and an alarm is generated.**
- **for TOE to TOE authentication, an alarm is generated.**]

Refinement :

a) The number of unsuccessful authentication attempts must be defined by the ST author.

b) The range for the number of unsuccessful authentication attempts is [1;5].

FIA_ATD.1 => User attribute definition

FIA_ATD.1.1 : The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

Refinement :

a) The ST author shall define the list of security attributes.

b) For this requirement, a user can be a HSS or LSS network user or an authorised administrator (security officer, TOE operator or TOE administrator).

FIA_SOS.1 => Verification of secrets

FIA_SOS.1.1 : The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

Refinement :

a) The defined quality metric shall be identified by the ST author.

FIA_SOS.2 => TSF Generation of secrets

FIA_SOS.2.1 : The TSF shall provide a mechanism to generate secrets that meet [assignment: *a defined quality metric*].

FIA_SOS.2.2 : The TSF shall be able to enforce the use of TSF generated secrets for [assignment: *list of TSF functions*].

Refinement:

a) The defined quality metric shall be identified by the ST author.

b) The list of TSF functions using secrets shall be identified by the ST author.

FIA_UAU.1 => Timing of authentication

FIA_UAU.1.1 : The TSF shall allow [**no action**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 : The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement :

a) For this requirement, the user is an authorised administrator (security officer, TOE operator or TOE administrator) or a TOE's process for TOE to TOE authentication (tunnelling in WAN configuration).

FIA_UAU.1 => Timing of authentication

FIA_UAU.1.1 : The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 : The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement :

a) For this requirement, the user can be a HSS or LSS network user.

b) The list of TSF mediated actions shall be identified by the ST author.

FIA_UAU.4 => Single-use authentication mechanisms

FIA_UAU.4.1 : The TSF shall prevent reuse of authentication data related to [**passwords and cryptographic authentication codes**].

Refinement :

a) One time passwords will be used for network users ; cryptographic authentication codes will be used for TOE to TOE authentication.

FIA_UAU.5 => Multiple authentication mechanisms

FIA_UAU.5.1 : The TSF shall provide [**one time password, cryptographic mechanisms and usual password**] to support user authentication.

FIA_UAU.5.2 : The TSF shall authenticate any user's claimed identity according to the [**rule defined in the refinement**].

Refinement :

a) For network users, the authentication mechanism must be one time password.

b) For TOE to TOE authentication (tunnelling in WAN configuration), the authentication mechanism must be cryptographic. In this case, the user is a TOE's process reacting on behalf of network users.

c) For the authorised personnels, the authentication mechanism must be usual password.

FIA_UID.2 => User identification before any action

FIA_UID.2.1 : The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Refinement :

a) The users are :

- HSS or LSS network users ;
- the TOE itself on behalf of the users (for TOE to TOE authentication in WAN configuration) ;
- authorised personnels : the TOE operator, the security officer or the TOE administrator (cf. P.ROLE).

FIA_USB.1 => User-subject binding

FIA_USB.1.1 : The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

5.1.1.5. SECURITY MANAGEMENT (FMT)

FMT_MOF.1 => Management of security functions behaviour

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

Refinement :

a) This table completes the three operations of this requirement. Each line is an iteration of the component.

- « Operation » is for [selection: *determine the behaviour of, disable, enable, modify the behaviour of*],
- « Function » is for [assignment: *list of functions*],
- « Role » is for [assignment: *the authorised identified roles*].

Operation	Function	Role
determine the behaviour of	function which permits the TSF to ignore or prevent the occurrence of auditable actions, except those taken by the authorised administrator, in the event of audit storage exhaustion.	security officer

FMT_MSA.1 => Management of security attributes

FMT_MSA.1.1 : The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

Refinement :

a) This table completes the four operations of this requirement. Each line is an iteration of the component.

- « Control » is for [assignment: *access control SFP, information flow control SFP*]
- « Operation » is for [selection: *change_default, query, modify, delete,* [assignment: *other operations*]],
- « Attribute » is for [assignment: *list of security attributes*],
- « Role » is for [assignment: *the authorised identified roles*].

Control	Operation	Attribute	Role
information flow control SFP	modify	TOE communication flow filtering parameters	TOE administrator or TOE operator
information flow control SFP	query	TOE communication flow filtering parameters	security officer or TOE operator or TOE administrator

FMT_MSA.2 => Secure security attributes

FMT_MSA.2.1 : The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 => Static attribute initialisation

FMT_MSA.3.1 : The TSF shall enforce the [**TOE internal access control policy and the TOE filtering policy**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 : The TSF shall allow the [**security officer**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 => Management of TSF data

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

Refinement :

a) This table completes the three operations of this requirement. Each line is an iteration of the component.

- « Operation » is for [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]],
- « Data » is for [assignment: *list of TSF data*],
- « Role » is for [assignment: *the authorised identified roles*].

Operation	Data	Role
empty	the audit trail	TOE Operator or Security Officer
display	which events are being audited	all
add, modify or delete	the rules for monitoring the audited events	all
maintain	the parameters that control the audit storage capability	TOE administrator
display and modify	the TOE access parameters (user-id, users' passwords, frequencies of connection, …)	all
initialise and modify	user data related to one time password mechanisms and cryptographic mechanisms	TOE operator or TOE administrator
manage	the authentication data	all
manage	the user identities	all
define	default subjects security attributes	security officer or TOE administrator
install	the TSF	TOE administrator
configure	the TSF	all
manage	the lists of users, subjects, objects and other resources for which revocation is possible	all
manage	the time	TOE administrator

FMT_MTD.2 => Management of limits on TSF data

FMT_MTD.2.1 : The TSF shall restrict the specification of the limits for [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

FMT_MTD.2.2 : The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment: *actions to be taken*].

Refinement :

a) This table completes the three operations of this requirement. Each line is an iteration of the component.

- « Data » is for [assignment: *list of TSF data*],
- « Role » is for [assignment: *the authorised identified roles*],
- « Action » is for [assignment: *actions to be taken*].

Data	Role	Action
audit trail	security officer	generate an alarm to the security officer or the TOE operator and prevent audit data loss (FMT_MOF.1)

FMT_REV.1 => Revocation

FMT_REV.1.1 : The TSF shall restrict the ability to revoke security attributes associated with the [**users or objects**] within the TSC to [**security officer, TOE operator and TOE administrator**].

FMT_REV.1.2 : The TSF shall enforce the rules [assignment: *specification of revocation rules*].

Refinement :

a) The ST author shall identify the revocation rules.

FMT_SMR.2 => Restrictions on security roles

FMT_SMR.2.1 : The TSF shall maintain the roles: [**security officer, TOE operator and TOE administrator**].

Refinement :

a) These three roles are defined in P.ROLE.

FMT_SMR.2.2 : The TSF shall be able to associate users with roles.

FMT_SMR.2.3 : The TSF shall ensure that the conditions [assignment: *conditions for the different roles*] are satisfied.

Refinement :

a) The ST author shall identify the conditions for the different roles.

FMT_SMR.3 => Assuming roles

FMT_SMR.3.1 : The TSF shall require an explicit request to assume the following roles: [**security officer, TOE operator and TOE administrator**].

5.1.1.6. PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)

FPT_AMT.1 => Abstract machine testing

FPT_AMT.1.1 : The TSF shall run a suite of tests [**during initial start-up and at the request of an authorised user**] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Refinement :

a) For this requirement, the authorised user is the security officer or the TOE administrator.

FPT_ITC.1 => Inter-TSF confidentiality during transmission

FPT_ITC.1.1 : The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

FPT_ITI.1 => Inter-TSF detection of modification

FPT_ITI.1.1 : The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [**a hash coding (ciphered within inter-TOE communication flows)**].

FPT_ITI.1.2 : The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.

Refinement :

a) The ST author shall define the actions to be taken if modifications are detected.

FPT_RPL.1 => Replay detection

FPT_RPL.1.1 : The TSF shall detect replay for the following entities: [**user authentication messages**].

Refinement :

a) The users are :
   - HSS or LSS network users ;
   - the TOE itself on behalf of the users (for TOE to TOE authentication in WAN configuration).

FPT_RPL.1.2 : The TSF shall perform [assignment: *list of specific actions*] when replay is detected.

Refinement :

a) The ST author shall precise the list of specific actions to be taken (e.g. TCP connection broken).

FPT_RVM.1 => Non-bypassability of the TSP

FPT_RVM.1.1 : The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 => TSF domain separation

FPT_SEP.1.1 : The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 : The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 => Reliable time stamps

FPT_STM.1.1 : The TSF shall be able to provide reliable time stamps for its own use.

FPT_TST.1 => TSF testing

FPT_TST.1.1 : The TSF shall run a suite of self tests [**during initial start-up and at the request of the authorised user**] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 : The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 : The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Refinement :

a) The authorised users can be the security officer or the TOE administrator.

5.1.1.7. TOE ACCESS (FTA)

FTA_LSA.1 => Limitation on scope of selectable attributes

FTA_LSA.1.1 : The TSF shall restrict the scope of the session security attributes [**role**], based on [**user identification**].

Refinement :

a) For this requirement, the user can be the security officer, the TOE operator or the TOE administrator.

FTA_TSE.1 => TOE session establishment

FTA_TSE.1.1 : The TSF shall be able to deny session establishment based on [**an ID or an authentication code**].

Refinement :

a) For this requirement, the session establishment only concerns administrators.

5.1.1.8. TRUSTED PATH / CHANNEL (FTP)

FTP_ITC.1 => Inter-TSF trusted channel

FTP_ITC.1.1 : The TSF shall provide a communication channel between itself and a remote 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 : The TSF shall permit [**the TSF and the remote trusted IT product**] to initiate communication via the trusted channel.

FTP_ITC.1.3 : The TSF shall initiate communication via the trusted channel for [**the TSF involved in the tunnelling security (authentication, encipherment, signature)**].

FTP_TRP.1 => Trusted path

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

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

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

Refinement :

a) For this requirement, local users are authorised personnels : the TOE operator, the security officer or the TOE administrator (cf. P.ROLE).

b) As only local communication is chosen, the remote access is forbidden.

c) The ST author can define other services for which trusted path is required.

5.1.2. Assurance Requirements

The evaluation assurance level requested is **EAL5**. There is no assurance augmentation component.

The minimum strength level requested for the TOE security functions realised by a probabilistic or permutational mechanism is **SOF-medium**.

6. Application Notes

To improve the TOE security, it is suggested to enforce the following recommendations :

- it is suggested that the security relevant TOE internal data (TOE's parameters) should be logically and physically separated from communication flows in transit in the TOE ;
- it is suggested that before passing filtering treatments, HSS communication flows in transit should be logically isolated from LSS communication flows ;
- it is suggested that the Security Officer and the TOE Operator come from different hierarchy in order to make the compromising of the authorised people more difficult ;
- it is suggested to make the TOE transparent for users (except for authentication) and protocol networks.

The ST shall specify whether these suggestions are enforced or not.

7. Rationale

7.1. Security Objectives Rationale

7.1.1. Secure Usage Assumptions

The table below shows the traceability between assumptions and objectives for the environment :

Assumptions	*Objectives for the environment*
A.PHY_ACCESS	O.PHY_ACCESS
A.PHY_SINGLE	O.PHY_SINGLE
A.STAFF_TRAINED	O.STAFF_TRAINED
A.STAFF_NOEVIL	O.STAFF_NOEVIL

Table 7-1 : Secure usage assumptions

A.PHY_ACCESS Physical access to the TOE.
[All configurations]

Counter-Measures *O.PHY_ACCESS* covers this assumption as it requires the TOE to be protected against unauthorised physical access.

A.PHY_SINGLE Unique access between HSS and LSS.
[All configurations]

Counter-Measures *O.PHY_SINGLE* covers this assumption as it requires the TOE to be the unique access between the two networks.

A.STAFF_TRAINED Authorised staff well trained.
[All configurations]

Counter-Measures *O.STAFF_TRAINED* covers this assumption as it requires the authorised personnels to be well trained to perform their role.

A.STAFF_NOEVIL Authorised staff non-hostile.
[All configurations]

Counter-Measures *O.STAFF_NOEVIL* covers this assumption as it requires the authorised personnels to be non-hostile and trusted to perform their role correctly.

7.1.2. Threats to be addressed by the TOE

The table below shows the traceability between threats and objectives for the TOE or for the environment :

Threats	*Objectives for the TOE*	*Objectives for the environment*
T.INTRUSION	O.ACCESS_CTL	O.PHY_SINGLE
T.OVERLOADING	O.FLOW_CTL	O.PHY_SINGLE
T.PROBING	O.MASK_TOPO	O.PHY_SINGLE
T.LEAKAGE	O.ACCESS_CTL	O.PHY_SINGLE
T.TAMPERING	O.TUNNEL_PROTECT	
T.TOE_INTRUSION	O.TOE_NOREMOTE	

Table 7-2 : Threats to be addressed by the TOE

T.INTRUSION [All configurations]	Intrusion from LSS to an HSS machine.
COUNTER-MEASURES	*O.ACCESS_CTL* counters this threat by filtering and controlling (the authorised network addresses for example) all the communication flows. The objective concerns the direct channels as well as the covert channels. *O.PHY_SINGLE* is the condition to assure that the TOE could not be bypassed. This objective assures that all the communication flows are treated by the TSFs associated to O.ACCESS_CTL.
T.OVERLOADING [All configurations]	Overloading of an HSS machine or the whole HSS network.
COUNTER-MEASURES	*O.FLOW_CTL* counters this threat as it requires HSS to be protected against overload attacks (limitation on the number of TCP requests, on the TCP connection frequencies and the throughput). *O.PHY_SINGLE* is the condition to assure that the TOE could not be bypassed.
T.PROBING [All configurations]	Deduction of HSS topology from LSS.
COUNTER-MEASURES	*O.MASK_TOPO* counters this threat as it requires HSS topology to be protected against probing attack from LSS. *O.PHY_SINGLE* is the condition to assure that the TOE could not be bypassed (filtering of TCP/IP protocols (e.g. ICMP); IP addresses translation).
T.LEAKAGE [All configurations]	Access to LSS from HSS to disclose sensitive information or access to unauthorised LSS services (through direct or covert channels).
COUNTER-MEASURES	*O.ACCESS_CTL* counters this threat by filtering and controlling all the communication flows. The objective concerns the direct channels as well as the covert channels (control on IP addresses, type of protocol...). *O.PHY_SINGLE* is the condition to assure that the TOE could not be bypassed.
T.TAMPERING [WAN configuration]	Access to the sensitive information exchanged between remote TOEs.
COUNTER-MEASURES	*O.TUNNEL_PROTECT* counters this threat by protecting the tunnel established when several TOEs are communicating (TOE to TOE authentication, encipherment and signature).

T.TOE_INTRUSION
[All configurations]

Remote access to the TOE from LSS or HSS.

COUNTER-MEASURES

O.TOE_NOREMOTE counters this threat by forbidding remote access to the TOE (elimination of TOE connecting protocols servers on the TOE, e.g. telnetd, ftpd, ...).

7.1.3. THREATS TO BE ADDRESSED BY THE OPERATING ENVIRONMENT

The table below shows the traceability between threats and objectives for the TOE or for the environment :

Threats	*Objectives for the TOE*	*Objectives for the environment*
T.TOE_BAD_OPE	O.TOE_ACCESS_CTL	O.STAFF_TRAINED O.STAFF_NOEVIL
T.TOE_PHYSICAL		O.PHY_ACCESS

Table 7-3 : Threats to be addressed by the operating environment

T.TOE_BAD_OPE
[All configurations]

An hostile, negligent or careless authorised personnel can exceed his rights.

COUNTER-MEASURES

O.STAFF_TRAINED counters this threat as it assumes the authorised personnels to be well trained. This helps to avoid TOE utilisation errors due to negligent behaviour.

O.STAFF_NOEVIL counters this threat as it assumes the authorised personnels to be non hostile.

O.TOE_ACCESS_CTL helps to counter this threat as it requires the TOE to prevent the authorised personnels to access operations and objects which are not allowed to their role.

T.TOE_PHYSICAL
[All configurations]

Physical intrusion to the TOE.

COUNTER-MEASURES

O.PHY_ACCESS counters this threat as it requires the TOE to be protected against unauthorised physical access. The room where the TOE is stored must be accessible only by authorised personnels.

7.1.4. POLICIES TO BE ADDRESSED BY THE TOE

The table below shows the traceability between policies and objectives for the TOE or for the environment :

Policies	*Objectives for the TOE*	*Objectives for the environment*
P.ROLE	O.MANAGEMENT O.TOE_I&A O.TOE_ACCESS_CTL	
P.WAN_ROLE	O.MANAGEMENT	
P.AUDIT	O.AUDIT O.TOE_I&A O.TOE_ACCESS_CTL	
P.CONFIG	O.TOE_CONFIG O.TOE_I&A O.TOE_ACCESS_CTL	O.STAFF_TRAINED
P.NO_BYPASS	O.NO_BYPASS	

Table 7-4 : Policies to be addressed by the TOE

P.ROLE
[All configurations]

There are three kinds of authorised personnels and each has a well defined role. These roles will be enforced after identification and authentication.

RESPONSE ELEMENTS

O.MANAGEMENT assures that the authorised personnels can perform the functions due to their role.

O.TOE_I&A assures that the authorised personnels are identified and authenticated before performing any action.

O.TOE_ACCESS_CTL assures that the authorised personnels access only to operations and objects allowed to their role according to the TOE internal access control policy.

P.WAN_ROLE
[WAN configuration]

This element includes a new role for the consistency of the global security policy.

RESPONSE ELEMENTS

O.MANAGEMENT assures that the new role defined can be performed.

P.AUDIT
[All configurations]

The security relevant events must be detected and registered. The audit trail is analysed to hold the authorised personnels accountable for their actions and to detect potential failure of filtering policy (e.g. attacks from LSS networks on HSS network). Only the authorised people can analyse the audit trail.

RESPONSE ELEMENTS

O.AUDIT assures that the security events are recorded and utilised.

O.TOE_I&A assures that the authorised personnels are identified and authenticated before performing any action (analyse the audit trail).

O.TOE_ACCESS_CTL assures that the authorised personnels access only to operations and objects allowed to their role.

P.CONFIG

[All configurations]

The configuration modification of the TOE must be possible during an acceptable time in operational terms by the authorised personnels.

RESPONSE ELEMENTS

O.TOE_CONFIG assures that the configuration modification of the TOE is possible during an acceptable time in operational terms.

O.TOE_I&A assures that the authorised personnels are identified and authenticated before they can modify the TOE.

O.TOE_ACCESS_CTL assures that the authorised personnels access only to operations and objects allowed to their role.

O.STAFF_TRAINED assumes that the authorised personnels are well trained.

P.NO_BYPASS

[All configurations]

The TSP must not be bypassable.

RESPONSE ELEMENTS

O.NO_BYPASS assures that all the TSP can not be bypassed. This assures that the TSP is well respected.

7.1.5. COMPLETENESS OF THE OBJECTIVES

7.1.5.1. OBJECTIVES FOR THE TOE

The following table depicts the traceability between objectives for the TOE, threats and policies :

Objectives for the TOE	*Threats*	*Policies*
O.ACCESS_CTL	T.INTRUSION T.LEAKAGE	
O.AUDIT		P.AUDIT
O.FLOW_CTL	T.OVERLOADING	
O.MASK_TOPO	T.PROBING	
O.TOE_I&A		P.ROLE P.AUDIT P.CONFIG
O.TOE_ACCESS_CTL	T.TOE_BAD_OPE	P.ROLE P.AUDIT P.CONFIG
O.TUNNEL_PROTECT	T.TAMPERING	
O.MANAGEMENT		P.ROLE P.WAN_ROLE
O.TOE_CONFIG		P.CONFIG
O.TOE_NOREMOTE	T.TOE_INTRUSION	
O.NO_BYPASS		P.NO_BYPASS

Table 7-5 : Completeness of the objectives for the TOE

O.ACCESS_CTL
[All configurations]

The TOE must provide controlled access between HSS and LSS by filtering the accesses (over direct and covert channels as well).

JUSTIFICATION

This security objective is necessary to counter T.INTRUSION and T.LEAKAGE threats as it requires the TOE to control the accesses and so can prevent any unauthorised access from LSS to HSS or from HSS to LSS.

O.AUDIT
[All configurations]

All the security events must be recorded and utilised.

JUSTIFICATION

This security objective is necessary to assure the P.AUDIT policy as it requires that all security events have to be recorded and utilised.

O.FLOW_CTL
[All configurations]

The HSS resources must be protected against overload attacks.

JUSTIFICATION

This security objective is necessary to counter T.OVERLOADING threat as it requires HSS resources to be protected against overload attacks.

O.MASK_TOPO
[All configurations]

The HSS topology must be protected against probing attacks from LSS.

JUSTIFICATION

This security objective is necessary to counter T.PROBING threat as it requires HSS topology to be protected against probing attacks.

O.TOE_I&A
[All configurations]

Only the authorised personnels can directly access to the TOE.

JUSTIFICATION

This security objective is necessary to assure the P.ROLE policy as it restricts the access to the TOE only to the Security Officer, the TOE Operator and the TOE Administrator.

It helps to assure the P.AUDIT policy as it restricts the access to the TOE to at the most three roles among which the Security Officer. It allows to identify the authorised personnels and to associate them with the actions they perform.

It helps to assure the P.CONFIG policy as it restricts the access to the TOE to only the authorised personnels.

O.TOE_ACCESS_CTL
[All configurations]

The TOE must prevent the authorised personnels not to act in accordance with their role.

JUSTIFICATION

This security objective is necessary to counter T.TOE_BAD_OPE and to assure P.ROLE, P.AUDIT and P.CONFIG policies as it requires the TOE to prevent the authorised personnels not to act in accordance with their role.

O.TUNNEL_PROTECT
[All configurations]

The TOE must protect the tunnel established when several TOEs are communicating.

JUSTIFICATION

This security objective is necessary to counter T.TAMPERING threat as it prevents any access to the channel established when several TOEs are communicating and so to the data exchanged.

O.MANAGEMENT
[All configurations]

The authorised personnels must be able to perform all the functions due to their role.

JUSTIFICATION

This security objective is necessary to assure P.ROLE and P.WAN_ROLE policies as it gives the authorised personnels the ability to perform their role.

O.TOE_CONFIG
[All configurations]

The configuration modification of the TOE must be possible during an acceptable time in operational terms.

JUSTIFICATION

This security objective is necessary to assure the P.CONFIG policy as it requires the configuration modification of the TOE to be possible during an acceptable time in operational terms.

O.TOE_NOREMOTE
[All configurations]

No remote access to the TOE is allowed, only local accesses are authorised.

JUSTIFICATION

This security objective is necessary to counter T.TOE_INTRUSION threat as it requires the TOE to be non accessible through remote access.

O.NO_BYPASS
[All configurations]

The TSP must not be bypassed.

JUSTIFICATION

This security objective is necessary to assure the P.NO_BYPASS policy as it requires the TSP to not be bypassable.

7.1.5.2. OBJECTIVES FOR THE ENVIRONMENT

The table below shows the traceability between objectives for the environment and threats, policies and assumptions :

Objectives for the environment	*Threats*	*Policies*	*Assumptions*
O.PHY_ACCESS	T.TOE_PHYSICAL		A.PHY_ACCESS
O.PHY_SINGLE	T.INTRUSION T.OVERLOADING T.PROBING T.LEAKAGE		A.PHY_SINGLE
O.STAFF_TRAINED	T.TOE_BAD_OPE	P.CONFIG	A.STAFF_TRAINED
O.STAFF_NOEVIL	T.TOE_BAD_OPE		A.STAFF_NOEVIL

Table 7-6 : Completeness of the objectives for the environment

O.PHY_ACCESS
[All configurations]

The TOE must be protected against unauthorised physical access.

JUSTIFICATION

This security objective is necessary to counter T.TOE_PHYSICAL threat as it requires the TOE to be protected against unauthorised physical access.

This security objective is necessary to cover A.PHY_ACCESS as it requires the TOE to be stored in an access controlled room to limit physical access to the TOE.

O.PHY_SINGLE
[All configurations]

The TOE must be the unique and single access between HSS and LSS.

JUSTIFICATION

This security objective is necessary to cover A.PHY_SINGLE as it requires the TOE to be the unique access between the two networks.

Thos security objective is necessary to counter the threats T.INTRUSION, T.OVERLOADING, T.PROBING and T.LEAKAGE as it requires the TOE to be the unique access between HSS and LSS. It also prevents an hostile person to communicate from LSS to HSS without crossing the TOE.

O.STAFF_TRAINED
[All configurations]

The authorised personnels must be trained to perform their role.

JUSTIFICATION

This security objective is necessary to counter A.STAFF_TRAINED as it requires the authorised personnels to be well trained to do their job.

This security objective is necessary to counter T.TOE_BAD_OPE threat as it requires the authorised personnels to be well trained to perform their role.

This security objective is necessary to assure P.CONFIG as it requires the authorised personnels to be well trained. They also can change configuration of the TOE during an acceptable time in operational terms.

O.STAFF_NOEVIL
[All configurations]

The authorised personnels must be non-hostile.

JUSTIFICATION

This security objective is necessary to counter A.STAFF_NOEVIL as it requires the authorised personnels to be non-hostile people and trusted to perform their role correctly.

This security objective is necessary to counter T.TOE_BAD_OPE threat as it requires the authorised personnels to be non-hostile.

7.1.6. SYNTHESIS

The table below shows a synthetic traceability between objectives, assumptions, threats and policies :

	A.PHY_ACCESS	A.PHY_SìNGLE	A.STAFF_TRAINED	A.STAFF_NOEVIL	T.INTRUSION	T.OVERLOADING	T.PROBING	T.LEAKAGE	T.TAMPERING	T.TOE_INTRUSION	T.TOE_BAD_OPE	T.TOE_PHYSICAL	P.ROLE	P.WAN_ROLE	P.AUDIT	P.CONFIG	P.NO_BYPASS
O.ACCESS_CTL					X			X									
O.AUDIT															X		
O.FLOW_CTL						X											
O.MASK_TOPO							X										
O.TOE_I&A													X		X	X	
O.TOE_ACCESS_CTL											X		X		X	X	
O.TUNNEL_PROTECT									X								
O.MANAGEMENT													X	X			
O.TOE_CONFIG																X	
O.TOE_NOREMOTE										X							
O.NO_BYPASS																	X
O.PHY_ACCESS	X											X					
O.PHY_SINGLE		X			X	X	X	X									
O.STAFF_TRAINED			X								X					X	
O.STAFF_NOEVIL				X							X						

Table 7-7 : Synthetic traceability between assumptions & threats & policies and objectives for the TOE & for the environment

The completeness of security objectives is assured by the following elements :

- all threats, policies and assumptions are covered by at least one security objective ;
- all security objectives cover at least one threat, one policy or one assumption ;
- all the security objectives work together to form an integrated and effective whole.

7.2. SECURITY REQUIREMENTS RATIONALE

7.2.1. SECURITY AUDIT

FAU_ARP.1	**Security alarms**
JUSTIFICATION	The component is included to directly support O.AUDIT as it requires the TSF to generate an alarm to the authorised personnels upon detection of a possible security violation and as it requires the TSF to take actions to terminate the security violation. This component contributes to O.ACCESS_CTL, O.FLOW_CTL, O.MANAGEMENT, O.MASK_TOPO, O.TOE_I&A, O.TOE_ACCESS_CTL, O.TUNNEL_PROTECT as it is an implicit need for all these objectives.

FAU_GEN.1	**Audit data generation**
JUSTIFICATION	The component is included to directly support O.AUDIT as it requires the creation and maintenance of an audit trail. This component contributes to O.ACCESS_CTL, O.FLOW_CTL, O.MANAGEMENT, O.MASK_TOPO, O.TOE_I&A, O.TOE_ACCESS_CTL, O.TUNNEL_PROTECT as it is an implicit need for all these objectives.

FAU_GEN.2	**User identity association**
JUSTIFICATION	The component is included to directly support O.AUDIT as it requires the TSF to associate the auditable events with the individual identities who activate them. This component contributes to O.ACCESS_CTL, O.FLOW_CTL, O.MANAGEMENT, O.MASK_TOPO, O.TOE_I&A, O.TOE_ACCESS_CTL, O.TUNNEL_PROTECT as it is an implicit need for all these objectives.

FAU_SAA.1	**Potential violation analysis**
JUSTIFICATION	The component is included to directly support O.AUDIT as it requires the TSF to indicate a potential violation of the TSP based upon a set of rules. This component contributes to O.ACCESS_CTL, O.FLOW_CTL, O.MANAGEMENT, O.MASK_TOPO, O.TOE_I&A, O.TOE_ACCESS_CTL, O.TUNNEL_PROTECT as it is an implicit need for all these objectives.

FAU_SAR.1	**Audit review**
JUSTIFICATION	The component is included to directly support O.AUDIT as it requires the TSF to provide audit tools to read the audit trail (filtering events) and as it requires the audit trail to be understandable by the authorised personnels (TOE Operator).

FAU_SAR.1 — **Audit review**

JUSTIFICATION

The component is included to directly support O.AUDIT as it requires the TSF to provide audit tools to read the audit trail (security events) and as it requires the audit trail to be understandable by the authorised personnels (Security Officer).

FAU_SAR.3 — **Selectable audit review**

JUSTIFICATION

The component is included to directly support O.AUDIT as it requires the TSF to provide audit review tools for audit trail analysis.

FAU_SEL.1 — **Selective audit**

JUSTIFICATION

The component is included to directly support O.AUDIT as it defines the attributes the TSF will use to include or exclude auditable events.

FAU_STG.2 — **Guarantees of audit data availability**

JUSTIFICATION

The component is included to directly support O.AUDIT as it requires the audit trail to remain unaffected even in the case of audit storage exhaustion, failure and attack.

7.2.2. USER DATA PROTECTION

FDP_ACC.2 — **Complete access control**

JUSTIFICATION

The component is included to directly support O.ACCESS_CTL and O.TOE_ACCESS_CTL as it requires that all accesses to the objects will be mediated by the access control.

It contributes to O.MASK_TOPO as the access control allows to watch over some probing attacks.

It contributes to O.FLOW_CTL as it is an implicit need for this objective.

FDP_ACF.1 — **Security attribute based access control**

JUSTIFICATION

The component is included to directly support O.ACCESS_CTL, O.FLOW_CTL and O.MASK_TOPO as it provides the rules which shall be used to mediate the access between subjects and objects.

In the case of O.MASK_TOPO, the access control allows to watch over some probing attacks.

The component is included to support O.ACCESS_CTL, O.FLOW_CTL and O.TOE_ACCESS_CTL as it grants or denies access based on security attributes.

FDP_IFC.2 **Complete information flow control**

JUSTIFICATION

The component is included to directly support O.FLOW_CTL and O.ACCESS_CTL as it requires the TSF to enforce the TOE filtering policy on the communication flows. This component allows the limitation of flows based on : limitation of TCP connection number, limitation of TCP connection frequencies and limitation of communication throughput.

FDP_IFF.1 **Simple security attributes**

JUSTIFICATION

The component is included to directly support O.ACCESS_CTL as it requires the TSF to enforce the TOE filtering policy using a list of types of subject and of object security attributes.

This component contributes to O.FLOW_CTL and O.MASK_TOPO as it is necessary to enforce the list of types of subject and of object security attributes linked to these objectives..

FDP_IFF.3 **Limited illicit information flows**

JUSTIFICATION

The component is included to directly support O.ACCESS_CTL as it requires the SFP to limit the capacity of illicit information flows.

This component contributes to O.FLOW_CTL as the methods used to control illicit information flows contribute to the flow control.

FDP_ITT.1 **Basic internal transfer protection**

JUSTIFICATION

The component is included to directly support O.TOE_ACCESS_CTL as it requires user data to be protected when transmitted between parts of the TOE.

FDP_RIP.1 **Subset residual information protection**

JUSTIFICATION

The component is included to directly support O.TOE_ACCESS_CTL as it requires the TSF to ensure that any residual information content of any resources being allocated to a defined subset of the objects in the TSC is unavailable.

7.2.3. IDENTIFICATION AND AUTHENTICATION

FIA_AFL.1 **Authentication failure handling**

JUSTIFICATION

The component is included to directly support O.TOE_I&A and O.TUNNEL_PROTECT as it requires the TSF to provide the security officer with the ability to specify action to be taken on authentication failure.

This component contributes to O.ACCESS_CTL when an authentication is required for some kind of applications (when it is possible according to the protocols used).

FIA_ATD.1 **User attribute definition**

JUSTIFICATION

The component is included to contribute to O.ACCESS_CTL, O.FLOW_CTL, O.TOE_ACCESS_CTL, as it is an implicit need for all these objectives. It requires that user security attributes are uniquely associated with each individual user.

The user can be the network users and the authorised personnels.

FIA_SOS.1 **Verification of secrets**

JUSTIFICATION

The component is included to contribute to O.TOE_I&A and O.TUNNEL_PROTECT as it is an implicit need for all these objectives. It requires the TSF to verify that secrets meet defined quality metrics.

This component contributes to O.ACCESS_CTL when an authentication is needed (when it is possible according to the protocols used).

FIA_SOS.2 **TSF generation of secrets**

JUSTIFICATION

The component is included to contribute to O.TOE_I&A and O.TUNNEL_PROTECT as it is an implicit need for all these objectives. It requires the TSF to be able to generate secrets that meet defined quality metrics .

This component contributes to O.ACCESS_CTL when an authentication is needed (when it is possible according to the protocols used).

FIA_UAU.1 **Timing of authentication**

JUSTIFICATION

The component is included to directly support O.TOE_I&A and O.TUNNEL_PROTECT as it requires the TSF to perform the authentication of any authorised personnel or TOE's process (for tunnelling in WAN configuration) claimed identity before performing any other TSF-mediated actions on behalf of that authorised personnel or process.

FIA_UAU.1 **Timing of authentication**

JUSTIFICATION

The component is included to directly support O.ACCESS_CTL as it requires the users to be successfully authenticated before performing some actions (when authentication is needed)

FIA_UAU.4 **Single-use authentication mechanisms**

JUSTIFICATION

The component is included to directly support O.TOE_I&A as it requires an authentication mechanism that operates with single-use authentication data.

This component is included to directly support O.ACCESS_CTL when an authentication is needed (when it is possible according to the protocols used).

FIA_UAU.5	**Multiple authentication mechanisms**
JUSTIFICATION	The component is included to directly support O.ACCESS_CTL, O.TUNNEL_PROTECT and O.TOE_I&A as it defines the types of authentication mechanisms to be used.

FIA_UID.2	**User identification before any action**
JUSTIFICATION	The component is included to directly support O.ACCESS_CTL, O.TOE_I&A and O.TUNNEL_PROTECT as it requires that each user have a unique identity. This component contributes to O.AUDIT as it allows to know who made what.

FIA_USB.1	**User-subject binding**
JUSTIFICATION	The component is included to directly support O.ACCESS_CTL, O.FLOW_CTL and O.TOE_ACCESS_CTL as it requires the TSF to associate the appropriate user security attributes with subjects acting on behalf of that user.

7.2.4. SECURITY MANAGEMENT

FMT_MOF.1	**Management of security functions behaviour**
JUSTIFICATION	The component is included to directly support O.AUDIT and O.MANAGEMENT as it requires the Security Officer to define the actions to be taken in the event of audit storage exhaustion.

FMT_MSA.1	**Management of security attributes**
JUSTIFICATION	The component is included to directly support O.MANAGEMENT as it provides the authorised personnels with the ability to query and/or modify the security attributes. This component is included to directly support O.TOE_CONFIG as it allows the possibility to modify the configuration of the TOE.

FMT_MSA.2	**Secure security attributes**
JUSTIFICATION	This component contributes to O.MANAGEMENT and O.TOE_CONFIG as it ensures that only secure values are accepted for security attributes.

FMT_MSA.3	**Static attribute initialisation**
JUSTIFICATION	The component is included to directly support O.TOE_ACCESS-CTL and O.ACCESS_CTL as it requires that the default values for security attributes are restrictive and only modifiable by the authorised personnels. This component is included to support O.TOE_CONFIG as it allows the possibility to modify the configuration of the TOE.

FMT_MTD.1	**Management of TSF data**
JUSTIFICATION	The component is included to support O.TOE_CONFIG, O.AUDIT, O.ACCESS_CTL, O.TOE_I&A and O.TOE_ACCESS_CTL as it provides the authorised personnels with the ability to modify the TOE configuration, to manage the audit trail, to define the filtering rules, to manage the authentication data and to define the TOE access parameters. The component is included to support O.MANAGEMENT as it defines the tasks the authorised personnels can perform.

FMT_MTD.2	**Management of limits on TSF data**
JUSTIFICATION	The component is included to directly support O.AUDIT and O.MANAGEMENT as it requires the TSF to provide the security officer with the ability to define limits to control audit trail saturation.

FMT_REV.1	**Revocation**
JUSTIFICATION	The component is included to contribute to O.ACCESS_CTL, O.FLOW_CTL, O.TOE_ACCESS_CTL and O.TUNNEL_PROTECT as it provides the possibility to immediately revoke security attributes.

FMT_SMR.2	**Restrictions on security roles**
JUSTIFICATION	The component is included to support O.MANAGEMENT as it defines the three roles needed for TOE management.

FMT_SMR.3	**Assuming roles**
JUSTIFICATION	The component is included to support O.MANAGEMENT and O.TOE_ACCESS_CTL as it requires an explicit action to assume administrative roles. It prevents an unauthorised user to perform administrative functions.

7.2.5. PROTECTION OF THE TOE SECURITY FUNCTIONS

FPT_AMT.1	**Abstract machine testing**
JUSTIFICATION	The component is included to directly support O.MANAGEMENT as it provides the authorised personnels with the ability to test underlying abstract machine.

FPT_ITC.1	**Inter-TSF confidentiality during transmission**
JUSTIFICATION	The component is included to directly support O.TUNNEL_PROTECT as it requires the TSF to ensure that data transmitted between TSFs are protected from disclosure while in transit.

FPT_ITI.1	**Inter-TSF detection of modification**
JUSTIFICATION	The component is included to directly support O.TUNNEL_PROTECT as it provides the ability for the remote TOE to detect modification of transmitted TSF data.

FPT_RPL.1	**Replay detection**
JUSTIFICATION	The component is included to contribute to O.ACCESS_CTL and O.TUNNEL_PROTECT as it requires the TSF to be able to detect the replay of identified entities.

FPT_RVM.1	**Non-bypassability of the TSP**
JUSTIFICATION	The component is included to directly support O.NO_BYPASS as it requires non-bypassability for all SFPs in the TSP.

FPT_SEP.1	**TSF domain separation**
JUSTIFICATION	The component is included to directly support O.TOE_ACCESS_CTL as it provides a distinct protected domain for the TSF and a separation between subjects within the TSC.

FPT_STM.1	**Reliable time stamps**
JUSTIFICATION	The component is included to support O.AUDIT as it requires the TSF to provide a reliable time stamp, which is necessary to have a valid audit trail.

FPT_TST.1	**TSF testing**
JUSTIFICATION	The component is included to directly support O.TOE_ACCESS_CTL and O.MANAGEMENT as it requires the TSF to be able to verify the integrity of the TSF executable code and of the TSF data.

7.2.6. TOE ACCESS

FTA_LSA.1	**Limitation on scope of selectable attributes**
JUSTIFICATION	The component is included to directly support O.TOE_ACCESS_CTL as it limits the scope of attributes for a session, based on user identification.

FTA_TSE.1	**TOE session establishment**
JUSTIFICATION	The component is included to directly support O.TOE_ACCESS_CTL as it provides the ability to deny session establishment on conditions defined by the authorised personnels.

7.2.7. TRUSTED PATH / CHANNEL

FTP_ITC.1 **Inter-TSF trusted channel**

JUSTIFICATION The component is included to directly support O.TUNNEL_PROTECT as it requires the TSF to provide a trusted communication channel between itself and another TSF.

FTP_TRP.1 **Trusted path**

JUSTIFICATION The component is included to directly support O.TOE_NOREMOTE as it provides a communication path between a local user and the TSF; and so it implies that the remote access is not chosen.

7.3. SYNTHESIS OF SECURITY REQUIREMENTS RATIONALE

	O.ACCES_CTL	O.AUDIT	O.FLOW_CTL	O.MASK_TOPO	O.TOE_I&A	O.TOE_ACCESS_CTL	O.TUNNEL_PROTECT	O.MANAGEMENT	O.TOE_CONFIG	O.TOE_NOREMOTE	O.NO_BYPASS
FAU_ARP.1	x	x	x	x	x	x	x	x			
FAU_GEN.1	x	x	x	x	x	x	x	x			
FAU_GEN.2	x	x	x	x	x	x	x	x			
FAU_SAA.1	x	x	x	x	x	x	x	x			
FAU_SAR.1		x									
FAU_SAR.3		x									
FAU_SEL.1		x									
FAU_STG.2		x									

	O.ACCES_CTL	O.AUDIT	O.FLOW_CTL	O.MASK_TOPO	O.TOE_I&A	O.TOE_ACCESS_CTL	O.TUNNEL_PROTECT	O.MANAGEMENT	O.TOE_CONFIG	O.TOE_NOREMOTE	O.NO_BYPASS
FDP_ACC.2	x		x	x		x					
FDP_ACF.1	x		x	x		x					
FDP_IFC.2	x		x								
FDP_IFF.1	x		x	x							
FDP_IFF.3	x		x								
FDP_ITT.1						x					
FDP_RIP.1						x					
FIA_AFL.1	x				x		x				
FIA_ATD.1	x		x			x					
FIA_SOS.1	x				x		x				
FIA_SOS.2	x				x		x				
FIA_UAU.1	x				x		x				
FIA_UAU.4	x				x						
FIA_UAU.5	x				x		x				
FIA_UID.2	x	x			x		x				
FIA_USB.1	x		x			x					
FMT_MOF.1		x						x			
FMT_MSA.1								x	x		
FMT_MSA.2								x	x		
FMT_MSA.3	x					x			x		
FMT_MTD.1	x	x			x	x		x	x		
FMT_MTD.2		x						x			
FMT_REV.1	x		x			x	x				
FMT_SMR.2								x			
FMT_SMR.3						x		x			
FPT_AMT.1								x			
FPT_ITC.1							x				
FPT_ITI.1							x				
FPT_RPL.1	x						x				
FPT_RVM.1											x
FPT_SEP.1						x					
FPT_STM.1		x									
FPT_TST.1						x		x			

	O.ACCES_CTL	O.AUDIT	O.FLOW_CTL	O.MASK_TOPO	O.TOE_I&A	O.TOE_ACCESS_CTL	O.TUNNEL_PROTECT	O.MANAGEMENT	O.TOE_CONFIG	O.TOE_NOREMOTE	O.NO_BYPASS
FTA_LSA.1						x					
FTA_TSE.1						x					
FTP_ITC.1							x				
FTP_TRP.1										x	

7.4. Rationale for Assurance Requirements

Considering that this PP addresses firewalls which are intended for use in a very sensitive commercial and defence environment, a high level of assurance is requested. EAL5 (Evaluation Assurance Level 5) and SOF-medium have been chosen for these reasons.

7.5. Consistency of the Security Requirements

The consistency of the security requirements can be proved if :

- all dependencies among the IT security requirements included in the PP are satisfied,
- the set of IT requirements together forms a mutually supportive whole,
- the set of IT requirements together forms an internally consistent whole.

7.5.1. Functional Security Requirements Dependencies

Legend :

FAU_SAA.1	Ok	=>	the component FAU_SAA.1 is included in the PP
FIA_UID.1	Ok - included in FIA_UID.2	=>	FIA_UID.2 is included in the PP and is hierarchical to FIA_UID.1
AVA_CCA.1	Ok - included in EAL5	=>	AVA_CCA.1 is included in EAL5 and also in the PP.

Components	***Dependencies***	***Comments***
FAU_ARP.1	FAU_SAA.1	Ok
FAU_GEN.1	FPT_STM.1	Ok
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Ok Ok - included in FIA_UID.2
FAU_SAA.1	FAU_GEN.1	Ok
FAU_SAR.1	FAU_GEN.1	Ok
FAU_SAR.3	FAU_SAR.1	Ok
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Ok Ok
FAU_STG.2	FAU_GEN.1	Ok

Components	***Dependencies***	***Comments***
FDP_ACC.2	FDP_ACF.1	Ok
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Ok - included in FDP_ACC.2 Ok
FDP_IFC.2	FDP_IFF.1	Ok
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Ok - included in FDP_IFC.2 Ok
FDP_IFF.3	AVA_CCA.1 FDP_IFC.1	Ok - included in EAL5 Ok - included in FDP_IFC.2
FDP_ITT.1	[FDP_ACC.1 or FDP_IFC.1]	Ok - included in FDP_ACC.2 Ok - included in FDP_IFC.2
FDP_RIP.1	-	

Components	***Dependencies***	***Comments***
FIA_AFL.1	FIA_UAU.1	Ok
FIA_ATD.1	-	
FIA_SOS.1	-	
FIA_SOS.2	-	
FIA_UAU.1	FIA_UID.1	Ok - included in FIA_UID.2
FIA_UAU.4	-	
FIA_UAU.5	-	
FIA_UID.2	-	
FIA_USB.1	FIA_ATD.1	Ok

Components	***Dependencies***	***Comments***
FMT_MOF.1	FMT_SMR.1	Ok - included in FMT_SMR.2
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1	Ok - included in FDP_ACC.2 Ok - included in FDP_IFC.2 Ok - included in FMT_SMR.2
FMT_MSA.2	ADV_SPM.1 [FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	Ok - ADV_SPM.3 included in EAL5 Ok - included in FDP_ACC.2 Ok - included in FDP_IFC.2 Ok Ok - included in FMT_SMR.2

Components	Dependencies	Comments
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Ok Ok - included in FMT_SMR.2
FMT_MTD.1	FMT_SMR.1	Ok - included in FMT_SMR.2
FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	Ok Ok - included in FMT_SMR.2
FMT_REV.1	FMT_SMR.1	Ok - included in FMT_SMR.2
FMT_SMR.2	-	
FMT_SMR.3	FMT_SMR.1	Ok - included in FMT_SMR.2

Components	Dependencies	Comments
FPT_AMT.1	-	
FPT_ITC.1	-	
FPT_ITI.1	-	
FPT_RPL.1	-	
FPT_RVM.1	-	
FPT_SEP.1	-	
FPT_STM.1	-	
FPT_TST.1	FPT_AMT.1	Ok

Components	Dependencies	Comments
FTA_LSA.1	-	
FTA_TSE.1	-	

Components	Dependencies	Comments
FTP_ITC.1	-	
FTP_TRP.1	-	

All dependencies are satisfied.

7.5.2. ASSURANCE SECURITY REQUIREMENTS DEPENDENCIES

EAL5 is constituted with a complete set of assurance requirements. All dependencies for these requirements are satisfied.

7.5.3. SATISFACTION OF THE MUTUAL SUPPORT

The following analysis shows how the security requirements defend each other against the following forms of indirect attacks, by which the intent of the security requirement could be defeated :

- bypassing attacks, which involve an attacker exploiting interfaces to the TOE that do not enforce the security requirements
- tampering (or corruption) attacks, which involve attacks on the integrity of data used by the security requirements
- de-activation attacks, including mis-configuration of the TSF.

	Requirement providing protection against		
Requirement	Bypassing	Tampering	De-activation
FAU_ARP.1	FPT_RVM.1	FMT_MTD.1	FAU_GEN.1 FAU_SAA.1
FAU_GEN.1	FPT_RVM.1	FAU_STG.2 FMT_MTD.1	FAU_STG.2

Requirement	Requirement providing protection against		
	Bypassing	Tampering	De-activation
FAU_GEN.2	FPT_RVM.1 FIA_UID.2	FMT_MSA.1 FMT_MTD.1	N/A
FAU_SAA.1	FPT_RVM.1	FMT_MTD.1	FAU_GEN.1
FAU_SAR.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FAU_SAR.3	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FAU_SEL.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	FAU_GEN.1
FAU_STG.2	FPT_RVM.1	FMT_MTD.1	N/A
FDP_ACC.2	FPT_RVM.1 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	N/A
FDP_ACF.1	FPT_RVM.1 FDP_ACC.2	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2
FDP_IFC.2	FPT_RVM.1 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	N/A
FDP_IFF.1	FPT_RVM.1 FDP_IFC.2	FMT_MSA.1 FMT_MTD.1	FDP_IFC.2
FDP_IFF.3	FPT_RVM.1 FDP_IFC.2	FMT_MSA.1 FMT_MTD.1	FDP_IFC.2
FDP_ITT.1	FPT_RVM.1 FDP_ACC.2 FDP_IFC.2	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2 FDP_IFC.2
FDP_RIP.1	N/A	FMT_MTD.1	N/A
FIA_AFL.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	FIA_UAU.1
FIA_ATD.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FIA_SOS.1	FPT_RVM.1	FMT_MTD.1	N/A
FIA_SOS.2	FPT_RVM.1	FMT_MTD.1	N/A
FIA_UAU.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FIA_UAU.4	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FIA_UAU.5	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FIA_UID.2	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FIA_USB.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FMT_MOF.1	FPT_RVM.1 FIA_UAU.1	FMT_MTD.1	N/A
FMT_MSA.1	FPT_RVM.1 FIA_UAU.1	FMT_MTD.1	N/A
FMT_MSA.2	FPT_RVM.1 FIA_UAU.1	FMT_MTD.1	N/A

	Requirement providing protection against		
Requirement	Bypassing	Tampering	De-activation
FMT_MSA.3	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2 FDP_IFC.2
FMT_MTD.1	FDP_ACC.2 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2
FMT_MTD.2	FDP_ACC.2 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2
FMT_REV.1	FDP_ACC.2 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2
FMT_SMR.2	FPT_RVM.1 FIA_USB.1	FMT_MSA.1 FMT_MTD.1	N/A
FMT_SMR.3	FMT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FPT_AMT.1	FMT_RVM.1	FMT_MTD.1	N/A
FPT_ITC.1	FMT_RVM.1	FMT_MTD.1	N/A
FPT_ITI.1	FMT_RVM.1	FMT_MTD.1	FDP_IFC.2
FPT_RPL.1	FMT_RVM.1	FMT_MTD.1	FDP_IFC.2
FPT_RVM.1	N/A	FMT_MTD.1	N/A
FPT_SEP.1	N/A	FMT_MTD.1	N/A
FPT_STM.1	N/A	FMT_MTD.1	N/A
FPT_TST.1	N/A	FMT_MTD.1	N/A
FTA_LSA.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FTA_TSE.1	FPT_RVM.1 FIA_USB.1	FMT_MSA.1 FMT_MTD.1	N/A
FTP_ITC.1	FPT_RVM.1	FPT_AMT.1 FPT_TST.1	N/A
FTP_TRP.1	FPT_RVM.1	FPT_AMT.1 FPT_TST.1	N/A

In the above table, « N/A » signifies « Not Applicable », i.e. the attack is not relevant to the security requirement as stated. In general :

- bypassing attacks are « N/A » if the requirement defines an invariant property of the TOE (e.g. FPT_SEP.1) or if the decision to invoke the functionality resides with the user rather than the TOE (e.g. FPT_TST.1).
- tampering attacks are « N/A » if the correct behaviour of the stated security requirement is not dependent on the integrity of any data.
- de-activation attacks are « N/A » if the security requirement as stated is not dependent on the configuration of the TSF.

Bypassing attacks are prevented by :

- FPT_RVM.1 which ensures non-bypassability for all security functions,
- FIA_UAU.1 which ensures authentication of users before any security action,
- FIA_UID.2 which ensures identification of users before any other action,
- FIA_USB.1 which ensure the association between the user's security attributes and a subject acting on the user's behalf,
- FDP_ACC.2 which ensures access control on all operations,
- FDP_IFC.2 which ensures flow control on all operations.

Tampering attacks are prevented by :

- FMT_MSA.1 which ensures protection of security attributes,

- FMT_MTD.1 which ensures protection of TSF data,
- FAU_STG.2 which ensures protection of the audit trail,
- FPT_AMT.1 which ensures secure operation of the TOE,
- FPT_TST.1 which ensures integrity of the TOE.

De-activation attacks are prevented by :

- FAU_GEN.1 which records all auditable events,
- FAU_SAA.1 which ensures detection of security violation,
- FAU_STG.2 which ensures protection of the audit trail,
- FDP_ACC.2 which ensures access control on all operations,
- FDP_IFC.2 which ensures flow control on all operations,
- FIA_UAU.1 which ensures authentication of users before any security action.

7.5.4. SATISFACTION OF THE INTERNAL CONSISTENCY

The set of security requirements forms a internally consistent whole if there are not two requirements which are incoherent. All dependencies between components is analysed to prove the components are coherent.

Legend for the following tables :

grey square	=>	relation already analysed
cc	=>	no inconsistency between components because no operation has been completed and the two components are in the same class or there is a dependency among them (dependency from CC part 2)
o	=>	relation which will be analysed
x	=>	no relation between the two components

7.5.4.1. FAU <=> FAU

	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1	FAU_SAR.3	FAU_SEL.1	FAU_STG.2
FAU_ARP.1		o	x	o	x	x	x	x
FAU_GEN.1			x	o	o	o	o	x
FAU_GEN.2				x	x	x	x	x
FAU_SAA.1					x	x	x	x
FAU_SAR.1						x	x	x
FAU_SAR.3							x	x
FAU_SEL.1								x
FAU_STG.2								

FAU_GEN.1 ↔ **FAU_ARP.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1**

JUSTIFICATION FAU_GEN.1 stores in the audit trail informations which are managed or generated by the other components. There is no inconsistency between these components.

FAU_ARP.1 ↔ **FAU_SAA.1**

JUSTIFICATION

FAU_SAA.1 defines the rules used to detect potential violation of the TSP and FAU_ARP.1 defines what to do upon a potential security violation. These components are complementary and there is no inconsistency between them.

7.5.4.2. FAU <=> FDP

	FDP_ACC.2	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.3	FDP_ITT.1	FDP_RIP.1
FAU_ARP.1	x	x	x	x	x	x	x
FAU_GEN.1	x	o	x	o	o	o	x
FAU_GEN.2	x	x	x	x	x	x	x
FAU_SAA.1	x	x	x	x	x	x	x
FAU_SAR.1	o	x	x	x	x	x	x
FAU_SAR.3	x	x	x	x	x	x	x
FAU_SEL.1	x	x	x	x	x	x	x
FAU_STG.2	x	x	x	x	x	x	x

FAU_GEN.1 ↔ **FDP_ACF.1, FDP_IFF.1, FDP_IFF.3, FDP_ITT.1**

JUSTIFICATION

FAU_GEN.1 stores in the audit trail informations which are managed or generated by the other components. There is no inconsistency between these components.

FAU_SAR.1 ↔ **FDP_ACC.2**

JUSTIFICATION

FDP_ACC.2 provides access control which permits to restrict access to the audit trail to the security officer and the TOE Operator (FAU_SAR.1). There is no inconsistency between these two components.

7.5.4.3. FAU <=> FIA

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_SOS.2	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UID.2	FIA_USB.1
FAU_ARP.1	x	x	x	x	x	x	x	x	x
FAU_GEN.1	o	x	o	o	o	o	o	o	o
FAU_GEN.2	x	x	x	x	x	x	x	o	x
FAU_SAA.1	x	x	x	x	x	x	x	x	x
FAU_SAR.1	x	x	x	x	x	x	x	x	x
FAU_SAR.3	x	x	x	x	x	x	x	x	x
FAU_SEL.1	x	x	x	x	x	x	x	o	x
FAU_STG.2	x	x	x	x	x	x	x	x	x

FAU_GEN.1 ↔ **FIA_AFL.1, FIA_SOS.1, FIA_SOS.2, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UID.2, FIA_USB.1**

JUSTIFICATION FAU_GEN.1 stores in the audit trail informations which are managed or generated by the other components. There is no inconsistency between these components.

FAU_GEN.2 ↔ **FIA_UID.2**

JUSTIFICATION FIA_UID.2 provides the identity of the users, which will be used by FAU_GEN.2 for the audit. These components are complementary and there is no inconsistency between them.

FAU_SEL.1 ↔ **FIA_UID.2**

JUSTIFICATION FIA_UID.2 provides the identity of the users, which will be used by FAU_SEL.1 to select auditable events. These components are complementary and there is no inconsistency between them.

7.5.4.4. FAU <=> FMT

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SMR.2	FMT_SMR.3
FAU_ARP.1	x	x	x	x	o	x	x	o	x
FAU_GEN.1	o	o	o	o	o	o	o	o	o
FAU_GEN.2	x	x	x	x	x	x	x	x	x
FAU_SAA.1	x	x	x	x	o	x	x	x	x
FAU_SAR.1	x	x	x	x	o	x	x	x	x
FAU_SAR.3	x	x	x	x	o	x	x	x	x
FAU_SEL.1	x	x	x	x	o	x	x	x	x
FAU_STG.2	x	x	x	x	o	x	x	x	x

FAU_ARP.1 ↔ **FMT_MTD.1**

JUSTIFICATION

FAU_ARP.1 defines what to do upon detection of a security violation and FMT_MTD.1 provides the authorised personnels the ability to modify these actions. These components are complementary and there is no inconsistency between them.

FAU_ARP.1 ↔ **FMT_SMR.2**

JUSTIFICATION

FAU_ARP.1 defines what the authorised personnels have the ability to do. These attributions are coherent with the definition of the roles in FMT_SMR.2. There is no inconsistency between these two components.

FAU_GEN.1 ↔ **FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1, FMT_SMR.2, FMT_SMR.3**

JUSTIFICATION

FAU_GEN.1 stores in the audit trail informations which are managed or generated by the other components. There is no inconsistency between these components.

FMT_MTD.1 ↔ **FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.2**

JUSTIFICATION

FMT_MTD.1 defines who can do operations defined in the other components. There is no inconsistency between these components.

7.5.4.5. FAU <=> FPT

	FPT_AMT.1	FPT_ITC.1	FPT_ITI.1	FPT_RPL.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FPT_TST.1
FAU_ARP.1	x	x	x	x	x	x	x	x
FAU_GEN.1	o	o	o	o	x	x	o	o
FAU_GEN.2	x	x	x	x	x	x	x	x
FAU_SAA.1	x	x	x	x	x	x	x	x
FAU_SAR.1	x	x	x	x	x	x	x	x
FAU_SAR.3	x	x	x	x	x	x	x	x
FAU_SEL.1	x	x	x	x	x	x	x	x
FAU_STG.2	x	x	x	x	x	x	x	x

FAU_GEN.1 ↔ **FPT_AMT.1, FPT_ITC.1, FPT_ITI.1, FPT_RPL.1, FPT_STM.1, FPT_TST.1**

JUSTIFICATION FAU_GEN.1 stores in the audit trail informations which are managed or generated by the other components. There is no inconsistency between these components.

7.5.4.6. FAU <=> FTA

	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1	FAU_SAR.3	FAU_SEL.1	FAU_STG.2
FTA_LSA.1	x	o	x	x	x	x	x	x
FTA_TSE.1	x	o	x	x	x	x	x	x

FAU_GEN.1 ↔ **FTA_LSA.1, FTA_TSE.1**

JUSTIFICATION FAU_GEN.1 stores in the audit trail informations which are managed or generated by the other components. There is no inconsistency between these components.

7.5.4.7. FAU <=> FTP

	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1	FAU_SAR.3	FAU_SEL.1	FAU_STG.2
FTP_ITC.1	x	o	x	x	x	x	x	x
FTP_TRP.1	x	o	x	x	x	x	x	x

FAU_GEN.1 ↔ **FTP_ITC.1, FTP_TRP.1**

JUSTIFICATION

FAU_GEN.1 stores in the audit trail informations which are managed or generated by the other components. There is no inconsistency between these components.

7.5.4.8. FDP <=> FDP

	FDP_ACC.2	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.3	FDP_ITT.1	FDP_RIP.1
FDP_ACC.2		o	x	x	x	o	x
FDP_ACF.1			x	x	x	x	x
FDP_IFC.2				o	x	x	x
FDP_IFF.1					x	x	x
FDP_IFF.3						x	x
FDP_ITT.1							x
FDP_RIP.1							

FDP_ACC.2 ↔ **FDP_ACF.1**

JUSTIFICATION

FDP_ACF.1 completes FDP_ACC.2 by giving the list of attributes on which the access control will be based. There is no inconsistency between these two components.

FDP_ACC.2 ↔ **FDP_ITT.1**

JUSTIFICATION

FDP_ACC.2 provides FDP_ITT.1 access control which permits to prevent disclosure and modification of user data. These components are complementary and there is no inconsistency between them.

FDP_IFC.2 ↔ **FDP_IFF.1**

JUSTIFICATION FDP_IFF.1 completes FDP_IFC.2 by giving the list of attributes on which the flow control will be based. There is no inconsistency between these two components.

7.5.4.9. FDP <=> FIA

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_SOS.2	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UID.2	FIA_USB.1
FDP_ACC.2	x	x	x	x	x	x	x	x	x
FDP_ACF.1	x	x	x	x	x	x	x	x	x
FDP_IFC.2	x	x	x	x	x	x	x	x	x
FDP_IFF.1	x	x	x	x	x	x	x	x	x
FDP_IFF.3	x	x	x	x	x	x	x	x	x
FDP_ITT.1	x	x	x	x	x	x	x	x	x
FDP_RIP.1	x	x	x	x	x	x	x	x	x

7.5.4.10. FDP <=> FMT

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SMR.2	FMT_SMR.3
FDP_ACC.2	o	o	x	o	o	x	x	x	x
FDP_ACF.1	o	o	x	o	o	x	x	x	x
FDP_IFC.2	x	o	x	o	o	x	x	x	x
FDP_IFF.1	x	o	x	o	o	x	x	x	x
FDP_IFF.3	x	x	x	x	x	x	x	x	x
FDP_ITT.1	x	x	x	x	x	x	x	x	x
FDP_RIP.1	x	x	x	x	x	x	x	x	x

FDP_ACC.2 ↔ **FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1**

JUSTIFICATION These four components provide access control rules which will be used by FDP_ACC.2. There is no inconsistency between these components.

FDP_ACF.1 ↔ **FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1**

JUSTIFICATION These four components provide access control rules which will be used by FDP_ACF.1. There is no inconsistency between these components.

FDP_IFC.2 ↔ **FMT_MSA.1, FMT_MSA.3, FMT_MTD.1**

JUSTIFICATION These three components provide flow control rules which will be used by FDP_IFC.2. There is no inconsistency between these components.

FDP_IFF.1 ↔ **FMT_MSA.1, FMT_MSA.3, FMT_MTD.1**

JUSTIFICATION These three components provide flow control rules which will be used by FDP_IFF.1. There is no inconsistency between these components.

7.5.4.11. FDP <=> FPT

	FPT_AMT.1	FPT_ITC.1	FPT_ITI.1	FPT_RPL.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FPT_TST.1
FDP_ACC.2	x	x	x	x	x	x	x	x
FDP_ACF.1	x	x	x	x	x	x	x	x
FDP_IFC.2	x	x	x	x	x	x	x	x
FDP_IFF.1	x	x	x	x	x	x	x	x
FDP_IFF.3	x	x	x	x	x	x	x	x
FDP_ITT.1	x	x	x	x	x	x	x	x
FDP_RIP.1	x	x	x	x	x	x	x	x

7.5.4.12. FDP <=> FTA

	FDP_ACC.2	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.3	FDP_ITT.1	FDP_RIP.1
FTA_LSA.1	x	x	x	x	x	x	x
FTA_TSE.1	x	x	x	x	x	x	x

7.5.4.13. FDP <=> FTP

	FDP_ACC.2	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.3	FDP_ITT.1	FDP_RIP.1
FTP_ITC.1	x	x	x	x	x	x	x
FTP_TRP.1	x	x	x	x	x	x	x

7.5.4.14. FIA <=> FIA

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_SOS.2	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UID.2	FIA_USB.1
FIA_AFL.1		x	x	x	o	x	x	x	x
FIA_ATD.1			x	x	x	x	x	x	x
FIA_SOS.1				cc	x	x	x	x	cc
FIA_SOS.2					x	x	x	x	cc
FIA_UAU.1						x	x	x	x
FIA_UAU.4							o	x	x
FIA_UAU.5								x	x
FIA_UID.2									x
FIA_USB.1									

FIA_AFL.1 ↔ **FIA_UAU.1**

JUSTIFICATION

FIA_UAU.1 requires the authorised personnels and the users in some cases to be successfully authenticated before doing anything else and FIA_AFL.1 defines what to do in case of successive authentication failures. There is no inconsistency between these two components.

FIA_UAU.4 ↔ **FIA_UAU.5**

JUSTIFICATION

The authentication mechanisms listed in the two components are coherent. There is no inconsistency between these two components.

7.5.4.15. FIA <=> FMT

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SMR.2	FMT_SMR.3
FIA_AFL.1	x	x	x	x	o	x	x	x	x
FIA_ATD.1	x	x	x	x	o	x	x	x	x
FIA_SOS.1	x	x	x	x	o	x	x	x	x
FIA_SOS.2	x	x	x	x	o	x	x	x	x
FIA_UAU.1	x	x	x	x	o	x	x	x	x
FIA_UAU.4	x	x	x	x	o	x	x	x	x
FIA_UAU.5	x	x	x	x	o	x	x	x	x
FIA_UID.2	x	x	x	x	o	x	x	x	x
FIA_USB.1	x	x	x	x	o	x	x	x	x

FMT_MTD.1 ↔ **FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_SOS.2, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UID.2, FIA_USB.1**

JUSTIFICATION FMT_MTD.1 restricts to authorised personnels the management of parameters or rules used by the other components. There is no inconsistency between these components.

7.5.4.16. FIA <=> FPT

	FPT_AMT.1	FPT_ITC.1	FPT_ITI.1	FPT_RPL.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FPT_TST.1
FIA_AFL.1	x	x	x	x	x	x	x	x
FIA_ATD.1	x	x	x	x	x	x	x	x
FIA_SOS.1	x	x	x	x	x	x	x	x
FIA_SOS.2	x	x	x	x	x	x	x	x
FIA_UAU.1	x	x	x	x	x	x	x	x
FIA_UAU.4	x	x	x	o	x	x	x	x
FIA_UAU.5	x	x	x	x	x	x	x	x
FIA_UID.2	x	x	x	x	x	x	x	x
FIA_USB.1	x	x	x	x	x	x	x	x

FIA_UAU.4 ↔ **FPT_RPL.1**

JUSTIFICATION FPT_RPL.1 shall detect replay for authentication and is coherent with FIA_UAU.4 which shall prevent reuse of authentication data. There is no inconsistency between these two components.

7.5.4.17. FIA <=> FTA

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_SOS.2	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UID.2	FIA_USB.1
FTA_LSA.1	x	x	x	x	x	x	x	x	x
FTA_TSE.1	x	x	x	x	x	x	x	x	x

7.5.4.18. FIA <=> FTP

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_SOS.2	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UID.2	FIA_USB.1
FTP_ITC.1	x	x	x	x	x	x	x	x	x
FTP_TRP.1	x	x	x	x	x	x	x	x	x

7.5.4.19. FMT <=> FMT

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SMR.2	FMT_SMR.3
FMT_MOF.1		x	x	x	x	o	x	o	x
FMT_MSA.1			o	x	x	x	x	o	x
FMT_MSA.2				o	o	x	x	x	x
FMT_MSA.3					x	x	x	o	x
FMT_MTD.1						x	o	o	x
FMT_MTD.2							x	o	x
FMT_REV.1								o	x
FMT_SMR.2									o
FMT_SMR.3									

FMT_SMR.2 ↔ **FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1**

JUSTIFICATION

All these components define what the three operators have the ability to do. These attributions are coherent with the definition of the three roles in FMT_SMR.2. There is no inconsistency between these components.

FMT_MOF.1 ↔ **FMT_MTD.2**

JUSTIFICATION

These two components are complementary and contribute to prevent audit data loss in the event of audit storage exhaustion. There is no inconsistency between these two components.

FMT_MSA.2 ↔ **FMT_MSA.1, FMT_MTD.1, FMT_MSA.3**

JUSTIFICATION

FMT_MSA.2 verify that the values for security attributes are always valid. FMT_MSA.2 is complementary with the other components. There is no inconsistency between these components.

FMT_MTD.1 ↔ **FMT_REV.1**

JUSTIFICATION

FMT_REV.1 provide the administrators the ability to revoke security attributes and FMT_MTD.1 provide the administrators the ability to manage the revocation rules. There is no inconsistency between these two components.

FMT_SMR.2 ↔ **FMT_SMR.3**

JUSTIFICATION

The three roles identified in these two components are identical. There is no inconsistency between these two components.

7.5.4.20. FMT <=> FPT

	FPT_AMT.1	FPT_ITC.1	FPT_ITI.1	FPT_RPL.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FPT_TST.1
FMT_MOF.1	x	x	x	x	x	x	x	x
FMT_MSA.1	x	x	x	x	x	x	x	x
FMT_MSA.2	x	x	x	x	x	x	x	x
FMT_MSA.3	x	x	x	x	x	x	x	x
FMT_MTD.1	x	x	x	o	x	x	o	x
FMT_MTD.2	x	x	x	x	x	x	x	x
FMT_REV.1	x	x	x	x	x	x	x	x
FMT_SMR.2	x	x	x	x	x	x	x	x
FMT_SMR.3	x	x	x	x	x	x	x	x

FMT_MTD.1 ↔ **FPT_RPL.1, FPT_STM.1**

JUSTIFICATION FMT_MTD.1 restricts to administrators the management of parameters or rules used by the other components. There is no inconsistency between these components.

7.5.4.21. FMT <=> FTA

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SMR.2	FMT_SMR.3
FTA_LSA.1	x	x	x	x	x	x	x	x	x
FTA_TSE.1	x	x	x	x	o	x	x	x	x

FMT_MTD.1 ↔ **FTA_TSE.1**

JUSTIFICATION FMT_MTD.1 restricts to administrators the management of parameters or rules used by FTA_TSE.1. There is no inconsistency between these two components.

7.5.4.22. FMT <=> FTP

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SMR.2	FMT_SMR.3
FTP_ITC.1	x	x	x	x	o	x	x	x	x
FTP_TRP.1	x	x	x	x	o	x	x	x	x

FMT_MTD.1 ↔ **FTP_ITC.1, FTP_TRP.1**

JUSTIFICATION FMT_MTD.1 restricts to administrators the management of parameters or rules used by the other components. There is no inconsistency between these components.

7.5.4.23. FPT <=> FPT

	FPT_AMT.1	FPT_ITC.1	FPT_ITI.1	FPT_RPL.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FPT_TST.1
FPT_AMT.1		x	x	x	x	x	x	o
FPT_ITC.1			x	x	cc	cc	cc	x
FPT_ITI.1				x	x	x	x	x
FPT_RPL.1					x	x	x	x
FPT_RVM.1						cc	cc	x
FPT_SEP.1							cc	x
FPT_STM.1								x
FPT_TST.1								

FPT_AMT.1 ↔ **FPT_TST.1**

JUSTIFICATION These two components are complementary and permit to demonstrate the correct operation of the TSF. There is no inconsistency between these two components.

7.5.4.24. FPT <=> FTA

	FPT_AMT.1	FPT_ITC.1	FPT_ITI.1	FPT_RPL.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FPT_TST.1
FTA_LSA.1	x	x	x	x	x	x	x	x
FTA_TSE.1	x	x	x	x	x	x	x	x

7.5.4.25. FPT <=> FTP

	FPT_AMT.1	FPT_ITC.1	FPT_ITI.1	FPT_RPL.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FPT_TST.1
FTP_ITC.1	x	x	x	x	x	x	x	x
FTP_TRP.1	x	x	x	x	x	x	x	x

7.5.4.26. FTA <=> FTA

	FTA_LSA.1	FTA_TSE.1
FTA_LSA.1		x
FTA_TSE.1		

7.5.4.27. FTA <=> FTP

	FTP_ITC.1	FTP_TRP.1
FTA_LSA.1	x	x
FTA_TSE.1	x	x

7.5.4.28. FTP <=> FTP

	FTP_ITC.1	FTP_TRP.1
FTP_ITC.1		x
FTP_TRP.1		

7.5.4.29. CONCLUSION

The set of IT security requirements together forms a mutually supportive and internally consistent whole.