ARKOON FAST360 6.0

Version 6.0/9

Common Criteria Security Target

Level EAL3+

Document version :	3.1
Référence :	ST_ARKOON_FAST360_60
Date:	2015-10-13

Table of contents

List of figures

Liste of tables

References

[AUTH] Référentiel général de sécurité (RGS)
Annexe B3 Authentification
Règles et recommandations concernant les mécanismes d'authentification
Version 1.00 du 13 janvier 2010

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

[CC] Common Criteria for Information Technology Security Evaluation, version 2.3
- Part 1: Introduction and general model, ref. CCMB-2005-08-001
- Part 2: Security functional requirements, ref. CCMB-2005-08-002
Part 3: Security assurance requirements, ref. CCMB-2005-08-003

[CRYPTO] Référentiel général de sécurité (RGS) Version 2.0
Annexe B1 Mécanismes cryptographiques
Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques
Version 2.03 du 21 février 2014

[GC] Référentiel général de sécurité (RGS) Version 2.0
Annexe B2 Gestion des clés cryptographiques
Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques
Version 2.00 du 8 juin 2012

[PP_CIP] Profil de protection Chiffreur IP, version 1.5, February 3, 2005.

[PP_FWIP] Profil de protection Firewall d'interconnexion IP, version 2.2, March 10, 2006.

[QS] Référentiel général de sécurité
Processus de qualification d'un produit de sécurité – Niveau Standard
Version 1.2.

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

[SHA256] FIPS 180-2, Secure Hash Standard (SHS), August 2002

Glossary

Common Criteria [CC] glossary

OSP Organisational Security Policy: Security policy of the environment of the product or system to evaluate. This policy can impact its security functions.

SOF Strength Of Function: Intrinsic resistance level of a function against attacks.This level is different from the TOE global resistance level (level defined by the AVA_VLA component) which takes into account attacks affecting TOE functions or making them ineffective.

ST Security Target: this document

TOE Target Of Evaluation: Product or system evaluated by the present security target which constitutes the specifications.

TSF TOE Security Functions: Product or system subset to evaluate which enables the achievement of the security functional requirements.

TOE glossary

Administrator User allowed to manage all or part of the TOE. He or she can have specific privileges which allow to modify the TOE security policy.

Security background Security parameters negociated between two VPN components allowing to know which security characteristics shall be used to apply the given VPN security policy. These parameters include the cryptographic algorithms, the key sizes, etc.

Filtering policy Security policy defined for managing the flows within an interconnection. This policy is applied by the TOE firewall. The term *firewall security policy* can also be used.

Security policy TOE security policy, including the TOE firewall filtering policies and the VPN security policies of the TOE VPN component.

VPN security policy Unidirectional security policy defined between two given VPN components. This policy specifies the security services to apply on data which pass from one VPN component through the other.

External network Network accessible to any entity or anyone which is not considered as safe. The term *public network* can also be used.

Internal network Internal network of an entity (a company or a department for example) which shall be protected from incoming flows and for which outcoming flows shall be controlled. This network is considered as safe. The term *protected network* can also be used. The TOE firewall is the interface between an internal network and an external network.

Private network Internal network of an entity (a company or a department for example) for which the confidentiality, the integrity and the authenticity of the communications with other private networks through a public network shall be protected. The TOE VPN component service protects the communications between two private networks.

Acronyms

Common Criteria [CC] acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organisational Security Policy
PP	Protection Profile
SF	Security Function
SFR	Security Functional Requirement
SFP	Security Function Policy
SOF	Strength Of Function
ST	Security Target
TOE	Target Of Evaluation
TSP	TOE Security Policy
TSF	TOE Security Functions

TOE acronyms

DMZ	Demilitarized Zone
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSEC	IP Security Protocol
LAN	Local Area Network
NAT	Network Address Translation
OS	Operating System
PC	Personal Computer
SMTP	Simple Mail Transfer Protocol

Conventions

The list below describes the prefixes used for the different property identified in this security target.

D.FW.	TOE sensitive assets relating to the firewall of the TOE
D.VPN.	TOE sensitive assets relating to the VPN service of the TOE
A.FW.	Hypothesis relating to the firewall of the TOE
A.VPN	Hypothesis relating to the VPN service of the TOE
T.FW.	Threats relating to the firewall of the TOE
T.VPN.	Threats relating to the VPN service of the TOE
OSP.FW	Organization security policies relating to the firewall of the TOE
OSP.VPN	Organization security policies relating to the VPN service of the TOE

1. INTRODUCTION

1.1 Identification of the document

Title	ARKOON FAST360 6.0
Reference	ST_ARKOON_FAST360_60
Version	3.1
Author(s)	Arkoon, Oppida
Date	2015-10-13
Product	Arkoon FAST360 6.0/9
Identification CC	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (ISO 15408)
Assurance level	Evaluation Assurance Level 3 (EAL3) enhanced with the components ALC_FLR.3 and AVA_VLA.2
Strenght of function (SOF)	SOF-high

The present document constitutes the security target of the product Arkoon FAST360 version 6.0/9.

This document defines the security requirements which shall be met by the evaluated product (the target of evaluation, TOE). These requirements are functional or relates to evaluation tasks.

The security target describes as well how the evaluated product meets these requirements.

1.2 Organization of the document

Chapter 1 is the introduction of the document.

Chapter 2 describes in a natural language the services provided by the evaluated product (TOE) and its architecture.

Chapter 3 describes the operating conditions defined for the evaluated product including the security services provided by the product and the threats the product will have to handle.

Chapter 4 describes the security goals the product and its operating environment shall reach particularly to provide the required security services and stop the identified threats.

Chapter 5 describes the security requirements to be met to reach these security goals: functional requirements and assurance requirements.

Chapter 6 describes the functionalities of the evaluated product designed to meet the functional requirements and the measures implemented to meet the assurance requirements.

Chapter 7 explains if the evaluated product meets also the requirements specified in a protection profile (PP).

Chapter 8 gathers all the technical overviews demonstrating that security goals and requirements are totally able to face all threats and that functionalities of the product meet functional requirements.

1.3 Compliance with the Common Criteria

The applicable version of the Common Criteria is version 2.3, August 2005 [CC].

The security functions provided by the TOE are compliant with Part 2 of the Common Criteria [CC]

The security assurance measures implemented on the TOE are compliant with Part 3 of the Common Criteria [CC].

The security assurance package selected is EAL3 augmented with FLC_FLR.3 and AVA_VLA.2 components.

The strength level of security functions aimed is “SOF-high”.

This security target complies with the protection profile [PP_FWIP].

This target cannot comply with the protection profile [PP_CIP] because [PP_CIP] complies with the version 2.2 of Common Criteria and this document shall comply with the version 2.3 of Common Criteria. However all hypothesis, threats, organizational security policies, security objectives for the TOE, security objectives for the environment of the TOE and functional security requirements defined by [PP_CIP] are included in this target.

2. DESCRIPTION OF THE TOE

2.1 Overview

Arkoon FAST360 appliances are designed to protect a computer network from most of the threats.

Based on the patented FAST technology (Fast Applicative Shield Technology), FAST 360 appliances incorporate firewalling, VPN/IPSEC server, real-time intrusion detection and prevention, antivirus, antispyware, authentication server, etc.

Arkoon's range of FAST360 appliances provides platforms with performance level scaled to meet the needs of everyone.

Arkoon Management Tools are provided with any ARKOON network security appliance and enable to manage (Arkoon Manager) and supervise (Arkoon Monitoring) the network security policy in a centralized way.

They enable to configure and supervise a set of Arkoon FAST360 appliances from only one administration console. They are suitable for large multi-site configurations especially thanks to additional functionalities like the "master/slave" architecture which allows automatically dispatching the configurations and automating the update processes.

2.1.1 FAST firewall

Thanks to the FAST technology, FAST360 appliances enable a « real-time » application monitoring (layers 5 to 7) and a stateful monitoring (layers 3 and 4) of internet flows without altering the network performances.

FAST360 appliances filtering service stops attacks by checking the conformity of more than 20 mostly used protocols (HTTP, SMTP, FTP, POP3, IMAP4, NNTP, DNS, RTSP, H323, Netbios, SSL, etc.) to the RFC. It applies rules detecting an unusual use of these protocols and limits some potentially intrusive commands or parameters of the protocols.

The FAST firewall is equipped with an applicative decoding technology allowing analysing the packets circulating on the network. This technology decodes the application protocol used, checks the conformity of the communication to the application protocol norm (RFC) and is able to separate the different elements of the application protocol in this communication (commands, parameters, data, etc.).

It is proactive against unknown attacks because it enables to detect and stop attacks breaking application protocols as well as attacks which do not comply with the protocols guidelines defined by the security administrator (usage rules).

The FAST technology combines a very high level of security with outstanding performances which enables to manage rates higher than 25 Gbits/s, 3 millions of simultaneous connections and more than 40 000 new connections per second.

2.1.2 FAST VPN

FAST360 appliances incorporate a VPN/IPSEC server supporting the « Lan to Lan » and « Host to Lan » communication applications or the protection of WiFi networks with very high levels of performances (up to 1 Gbits/s in AES and 25 000 simultaneous tunnels).

The VPN module is based on the IPSec norm which guarantees the interoperability with the solutions of the market and supports more particularly the 3DES, AES 128/192/256 and Blowfish encryption algorithms. Thanks to the NAT-Traversal functionality, it is compatible with address translation systems. It supports strong authentication systems (USB key, smart card, biometrics, etc.) and uses the authentication methods with shared key and X509 certificate. These certificates can be generated either by the Certification Authority which Arkoon provides by default on the appliances, or by an external PKI.

2.2 Architecture

The Common Criteria evaluation only assesses the software part of the TOE and not the equipments.

2.2.1 System architecture

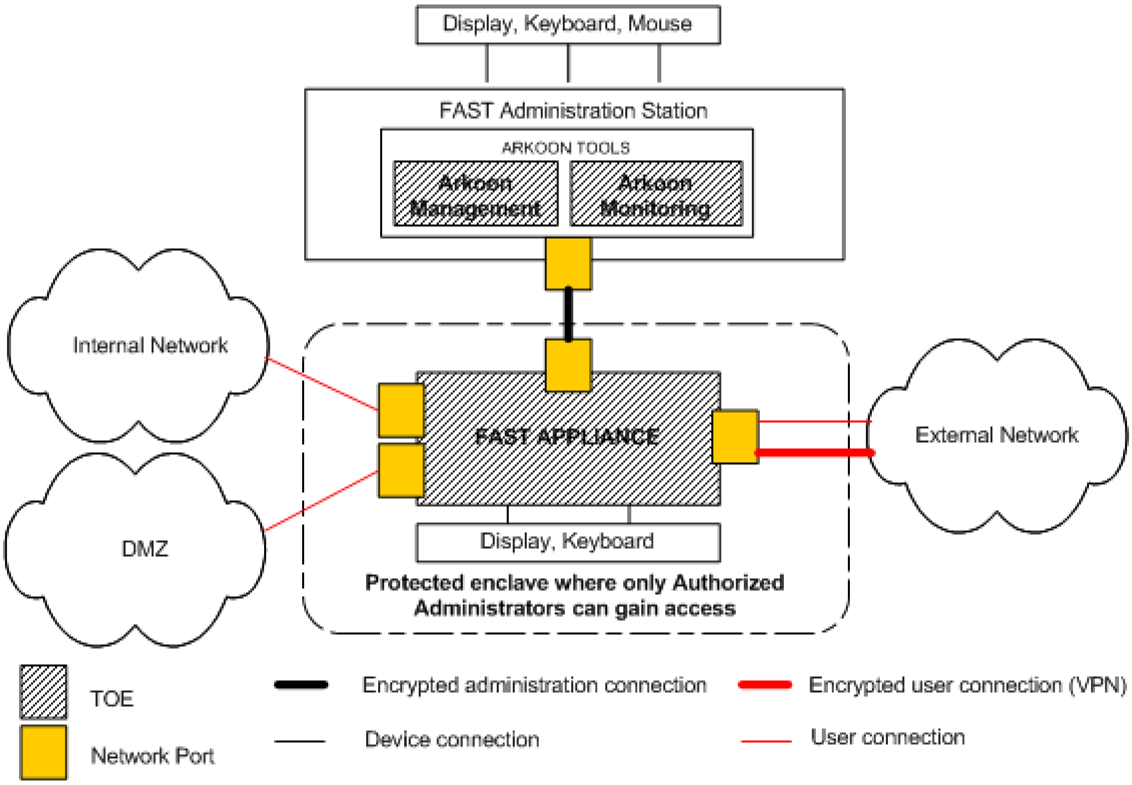

Figure 1 : Interfaces of the TOE

The TOE has four network interfaces:

1. an administration interface: this interface connects the TOE to the administration station through an administration network and enables the remote administration of the TOE.
2. an external network interface: this interface connects the TOE to the external network considered as not safe (Internet for example).
3. an internal network interface: this interface connects the TOE to the internal network, that is to say the network protected by the TOE.
4. a DMZ network interface: connects the TOE to a DMZ network, that is to say a network on which only the machines which shall be visible from the external network can be found.

The TOE can be managed by remote control through an administration station where Arkoon Tools are installed (Arkoon Management and Arkoon Monitoring). Arkoon Tools enable administrators to be authenticated by the TOE and the TOE protects the confidentiality, integrity and authenticity of the administration operations.

The TOE administration operations are only performed from the administration network interface. The administration flows never pass through another network interface of the TOE (external, internal, DMZ).

Administrators can also manage the TOE thanks to a minimum local administration service via a screen and a keyboard directly connected to the appliance.

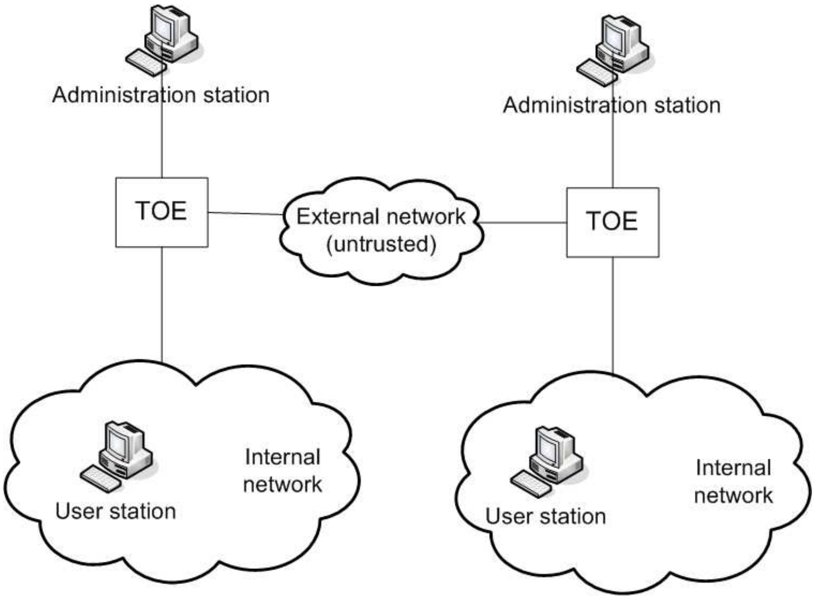

Figure 2: Architecture of the evaluation of the TOE

As shown in the above figure, this is how the TOE will be configured during its evaluation: two TOE connected via an external network (not safe) through their external interface. Each TOE is managed by its own administration station (connected to the administration interface of the TOE) where Arkoon Management and Arkoon Monitoring are installed.

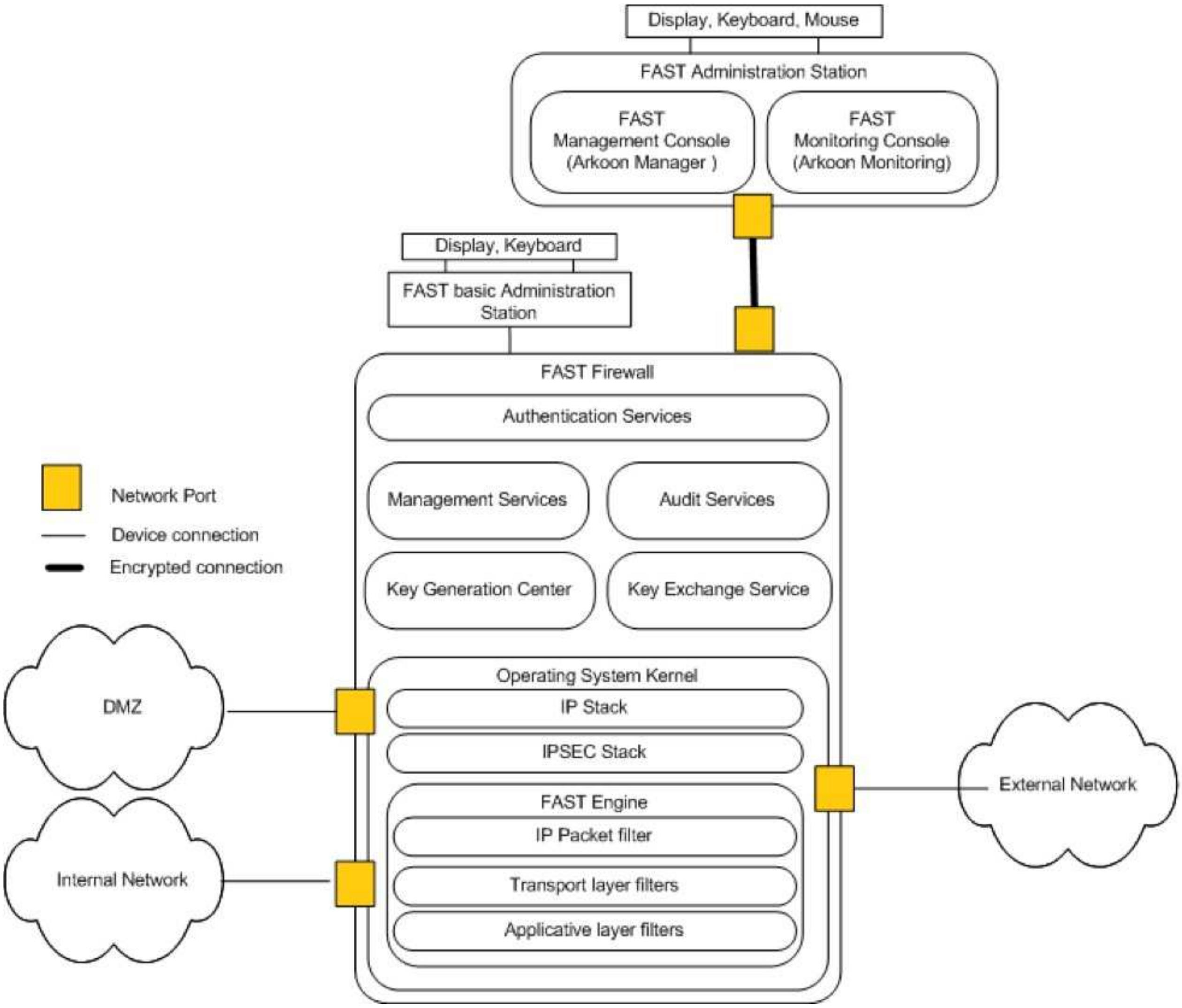

Figure 3: Internal architecture of the TOE

The TOE includes the following elements:

- **FAST Management Console**: software installed on the remote administration station enabling TOE security administrators to authenticate and perform administration operations on the TOE.
- **FAST Monitoring Console**: software installed on the remote administration station enabling system and network administrators to configurate network parameters and to supervise the status of the TOE.
- **Authentication services**: enable the authentication of remote administration stations and of TOE administrators (local and remote).
- **Management services**: provide different administration rights according to each administration roles. There are seven administration roles: security officer, security administrator, network and system administrator and supervisor, auditor, security supervisor and role all permissions.
- **Audit services**: enable to record all the events in logs: administration operations, flows managed by the TOE firewall, flows managed by the VPN component, etc.
- **Key Generation Center**: enables the TOE to generate its own cryptographic keys (this element is out of the scope of the evaluation (refer to 2.2.2)).

- **Key exchange service (IKE)**: in order to generate the symmetric cryptographic keys used by the IPSec stack, the key exchange service establishes a secured connection between two machines communicating through a hostile network.This service implements the IKE norm (Internet Key Exchange) and therefore interacts with all the IKE key exchange services of the market.
- **Operating System Kernel**: main part of the operating system. It manages the hardware and software resources and enables all the components to communicate.
- **IP Stack**: module responsible for forwarding IP packets by applying routing rules.
- **IPSEC Stack**: this module ensures the authenticity, confidentiality and protection against data replay of an IP communication between two machines. It receives symmetric and cryptographic keys negociated by the IKE key exchange service, stores them during their lifetime and uses them to apply the encryption policy on flows. This module implements the IPSec norm and is able to interact with all the IPSec products of the market.
- **FAST Engine**: this mechanism is the heart of the FAST360 technology and sets up the rules which accept or deny a new connection. By applying filtering rules and submiting flows to specialized modules for each protocols, it provides a set of services like monitoring sessions and limiting the number of established or pending connections.
- **IP Packet filter**: FAST module in charge of IP filtering. It provides specific IP mechanisms like limiting the number of connections, translating addresses (NAT) and managing IP options.
- **Transport Layer filters**: FAST modules in charge of filtering TCP and UDP transport layer protocols. They guarantee that the packets received respect the constraints defined by the norms of these protocols. For example, a mechanism supervises TCP packets sequencing.
- **Applicative layer filters**: the activation of these modules is configured in the filtering policy. They enable to analyze the conformity of a flow to an applicative protocol (HTTP, FTP, SMTP, DNS) and to filter it according to the applicative policy configured by the security administrator.

2.2.2 Limits of the scope of the evaluation

The TOE includes the following elements:

1. **FAST Administration Station** (refer to Figure 1)

   This element includes two softwares: FAST Management Console and FAST Monitoring Console. The scope of the evaluation only includes modules enabling the authentication and protection (confidentiality, integrity, authenticity) of the flows exchanged between these administration tools and FAST Appliance.

2. **FAST Appliance** (refer to Figure 1)

   This element includes:

   - services: authentication, management, audit, key exchange (IKE). The scope of the evaluation includes these services.
   - a Key Generation Center (refer to Figure 3) which is not part of the evaluation.
   - the operating system kernel: IP Stack, IPSEC Stack, FAST Engine, IP Packet filter, Transport Layer filters, Applicative layer filters. The scope of the evaluation includes these modules.

Only the software part of the TOE is evaluated.

The Key Generation Center provided by the TOE and enabling the TOE to generate its own cryptographic keys is not included in the scope of the evaluation. This is justified by the fact that the PP [PP_CIP] from which the VPN service of the TOE is inspired mentions that the Key Generation Center is out of the TOE.

2.3 Services provided by the TOE

2.3.1 Services provided by the TOE

2.3.1.1 Firewall: application of the filtering policy

The firewall of the TOE enables filtering IP flows between two IP networks according to the security policy defined by the TOE security administrator.

The firewall of the TOE enables to authorize or deny IP packets according to their characteristics (source port, destination port, source IP address, destination IP address, protocol, application, etc.) and according to the filtering policy defined by the security administrator.

2.3.1.2 VPN component: application of the VPN security policy

The VPN component of the TOE enables to protect the authenticity, the confidentiality and the integrity of flows exchanged between two private networks by using the IPSEC protocol. The VPN component:

- Protects the confidentiality of applicative data: by encrypting applicative data encapsulated in IP flows, the VPN component prevents data from being divulgated when they flow through a public network (for example Internet) not secure.
- Protects the authenticity of applicative data: by signing applicative data encapsulated in IP flows, the VPN component enables to detect any modification made to them.
- Protects the confidentiality of network topologic data: by encrypting topologic data of IP packets, the VPN component prevents internal IP addresses (source and destination) of devices from private networks to be divulgated.
- Protects the authenticity of network topologic data: by signing topologic data of IP packets, the VPN component enables to detect any modification made to them.
- Allows partitioning flows by partitioning a private network in several sub-networks. Flow partitioning enables to apply different VPN security policies for each sub-network.

2.3.2 Management services provided by the TOE

2.3.2.1 Administration accounts management

This service enables the TOE security officers to manage the TOE administration accounts.

2.3.2.2 Flows audit and logging

This service enables:

- to save all IP flows passing through the firewall and the VPN component in logs.
- the security administrator to define conditions of flow recording in these logs (accepted flow, denied flow, source IP address, destination IP address, integrity error, etc.).
- to generate alarms whose configuration is defined by the security administrator.
- the TOE security administrators, the security supervisors and the auditors to check the logs.

2.3.2.3 Definition of the security policies

This service enables the security administrator to define the firewall filtering policy as well as the VPN policy of the VPN component. The configuration of security policies (firewall and VPN component) is only accessible to the TOE security administrators.

2.3.2.4 Administration operations audit and logging

This service enables to save all the administration operations performed by the TOE administrators in logs. It enables also the security administrators, the security supervisors and the auditors to check the logs.

2.3.2.5 Monitoring

This service enables the system and network administrator and supervisor to manage the availability status of the TOE. It also enables the system and network administrator to configure the TOE network parameters. This service is performed from a monitoring workstation from which the Arkoon Monitoring software enables to monitor the TOE.

2.3.2.6 Cryptographic keys management

This service enables the TOE security administrator to manage cryptographic keys used to authenticate users and to protect the confidentiality and authenticity of VPN flows. This service enables to:

- protect the access to cryptographic keys: the security administrator only can access the TOE cryptographic keys.
- manage the life-cycle of the cryptographic keys: the cryptographic keys used in the TOE shall be renewed regularly to guarantee a good level of security of the TOE.
- upload cryptographic keys: the security administrator uploads safely the cryptographic keys required by the TOE.
- delete safely cryptographic keys: the security administrator can delete safely the cryptographic keys of the TOE.

Note: Arkoon FAST has its own Key Generation Center enabling to generate cryptographic keys used by the TOE to authenticate users and protect flows passing through the VPN component (confidentiality and authenticity). The Key Generation Center is out of the scope of the evaluation. This is justified by the fact that the PP [PP_CIP] from which the VPN service of the TOE is inspired mentions that the Key Generation Center is out of the TOE.

2.3.2.7 Reinitializing

This service enables the security administrator to delete safely all sensitive data in the TOE in case of a context change (new assignment, maintenance, etc.): security policy (firewall and VPN), cryptographic keys, user authentication data, etc.

3. SECURITY ENVIRONMENT OF THE TOE

This chapter describes the security aspects of the environment in which the TOE shall be used.

3.1 Sensitive assets

The description of each asset provides the types of protection required for each one (Protection part).

The assets of the information system are protected by the TOE providing that the firewall and VPN security policies require the application of one or several protection types. When the protection type (Protection part) is followed by « (opt.) » meaning optional, it means the protection shall be provided by the TOE but it is not systematically applied by the TOE.

Assets relating to the firewall of the TOE only are identified by the prefix D.FW.
Assets relating to the VPN service of the TOE only are identified by the prefix D.VPN.

3.1.1 Assets protected by the TOE

Firewall

D.FW.DONNEES_RESEAU_PRIVE

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

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

VPN component

D.VPN.DONNEES_APPLICATIVES

Applicative data are data which flow through a private network to another via VPN components. They are included in the IP packets payload routed to the VPN components and received and sent by these components. These data can be stored temporarily in the VPN components to be processed (i.e. applying security services) before being sent to the private or public network.

Protection: confidentiality (opt.) and authenticity (opt.).

D.VPN.INFO_TOPOLOGIE

Private networks topologic data (source and destination IP addresses) are included in IP packets headers.

Protection: confidentiality (opt.) and authenticity (opt.).

3.1.2 TOE sensitive assets

D.LOGICIELS

TOE softwares enabling the enforcement of all TOE services.

Protection: integrity.

Firewall

D.FW.POLITIQUE_FILTRAGE

Filtering policies and contexts of connection define how the firewall shall process IP packets (implicit filtering and security services). This includes the audit policy of user flows.

Protection: authenticity when policies (and their contexts) flow from where the administrator remotely defines them to the firewall, integrity of the policies (and contexts) stored by the firewall, coherency between the policy defined (and its context) and the policy applied, confidentiality.

D.FW.AUDIT_FLUX

Data generated by the audit policy in order to track flows processed by the firewall.

Protection: integrity.

D.FW.PARAM_CONFIG

Configuration parameters of the firewall include among others:

- IP addresses internal to protected networks and routing tables (network configuration);
- authentication and integrity data;
- access rights;
- the audit policy of the administration operations.

Protection: confidentiality and integrity.

D.FW.AUDIT_ADMIN

Data generated by the audit policy in order to track administration operations performed on the firewall.

Protection: integrity.

D.FW.ALARMES

Security alarms generated by the TOE to prevent a possible security violation of the firewall.

Protection: integrity.

VPN component

D.VPN.POLITIQUE_VPN

VPN security policies define processing functions (implicit filtering and security services) to be performed on data received and sent by every IP encryptor. This asset also includes the security contexts which are linked with security policies. Every security context includes all security parameters necessary to the enforcement of its associated VPN security policy. These parameters are defined by the security administrator.

Protection: integrity of the policies (and their contexts) stored in VPN components, confidentiality.

D.VPN.PARAM_CONFIG

Configuration parameters of the VPN component include among others: IP addresses internal to private networks and routing matrices (network configuration), authentication data and access rights.

Protection: confidentiality and integrity.

D.VPN.CLES_CRYPTO

This asset includes all cryptographic keys (symmetric or asymmetric) necessary for the operation of the TOE such as:

- session keys.
- keys used by security services enforced by VPN security policies.

Protection: confidentiality (for secret and private keys) and integrity (for all keys).

D.VPN.AUDIT_FLUX

Data generated by the audit policy in order to track activities which occurred on VPN links.

Protection: integrity.

D.VPN.AUDIT_ADMIN

Data generated by the audit policy in order to track administration operations performed on the VPN component.

Protection: integrity.

Application note: the D.AUDIT asset identified in the [PP_CIP] protection profile of the VPN component has been divided into two assets D.VPN.AUDIT_FLUX and D.VPN.AUDIT_ADMIN.

D.VPN.ALARMES

Security alarms generated by the TOE to prevent a possible security violation of the VPN component.

Protection: integrity.•

3.2 Roles

In its operating environment, the TOE involves directly or indirectly the roles described below. These roles are « logic » and they are distributed to different people or not according to the security policy defined by the organization which implements the TOE.

Security officer

He/she configures roles and accesses to administration tools and functions. He/she manages authentication processes to access administration tools.

Security administrator

Local or remote administrator of the TOE. He/she defines the filtering policy applied by the firewall. He/she defines the VPN security policy and security contexts applied by the VPN component. He/she generates and distributes keys in the VPN component. He/she defines audit events to be tracked as well as security alarms to be generated. He/she analyzes, manages and deletes generated security alarms.

Auditor

He/she analyzes and manages audit events related to activities on IP flows passing through the firewall and the VPN component as well as administration operations.

Network and system administrator

Administrator responsible for the system information on which the TOE is. He/she is responsible for maintaining the operating condition of the TOE (software and hardware maintenance).

He/she configures the TOE network parameters and system parameters linked to operating network contexts to consider: he/she defines the global network topology but he/she defines neither the filtering policy to be applied by the firewall nor VPN security policies. He/she supervises also the TOE status.

Network and system supervisor

He/she checks the system status and network events.

Security supervisor

He/she monitors security events and checks/deletes security alerts.

Role all permissions

This role is used in organizations where only one person is in charge of the FAST360 appliance. He has all the permissions.

Protected network user

Protected network user connected to another network through the firewall. This user is able to send/receive information to/from another network using applications through its network firewall.

Private network user

Private network user connected to another private network through a VPN component. This user is able to send/receive information to/from anonther private network using applications through its network VPN component.

A private network user is also a protected network user, but the contrary is not always true. A protected network user uses the network protected by the TOE firewall, and a private network user uses the protected network (i.e. protected by the TOE firewall) and the TOE VPN service.

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

3.3 Hypothesis

Hypothesis relating to the firewall of the TOE only are identified by the prefix A.FW.
Hypothesis relating to the VPN service of the TOE only are identified by the prefix A.VPN.

A.ADMIN

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

A.LOCAL

Equipments containing the TOE services (firewall, VPN and administration equipments) and supports containing the sensitive assets of the TOE (paper, floppy disks, backup, etc.) shall be in a secure room, accessible only by administrators.

However, equipments do not need to be in a secure room if they do not contain sensitive assets: in cases of change in the context of use of the firewall or the VPN component for instance.

A.INITIALISATION_LOCAL

Equipments containing the TOE services (firewall, VPN and administration equipments) are initialized in a secure room accessible only by administrators. The initialization is performed from an administration station directly connected to the equipments.

A.AUTHENTIFICATION_ADMIN_DISTANT

The TOE environment enables to authenticate the administrator for the appliance remote accesses.

Firewall

A.FW.AUDIT

The auditor shall regularly consult the audit events generated by the firewall and he/she handles the audits to avoid data loss.

A.FW.ALARMES

The security administrator shall handle the alarms generated and sent by the firewall.

A.FW.MAITRISE_CONFIGURATION

The administrator shall control or regenerate the hardware and software configuration (services and assets) of the firewall according to a reference state.

VPN component

A.VPN.AUDIT

The auditor shall regularly consult the audit events generated by the VPN component and he/she handles the audits to avoid data loss.

A.VPN.ALARMES

The security administrator shall handle the alarms generated and sent by the VPN component.

A.VPN.MAITRISE_CONFIGURATION

The administrator shall control or regenerate the VPN component hardware and software configuration (services and assets) according to a reference state.

A.VPN.CRYPTO_EXT

The cryptographic keys generated outside and injected into the TOE shall have been generated according to the recommandations specified in the [CRYPTO] and [GC] ANSSI reference documents for the standard resistance level.

3.4 Threats

3.4.1 Profile of the attackers

Threats can come from:

- a malfunction of the TOE or of its environment (workstation, network, etc.).
- people who can access the network on which the TOE is connected and may be devious and steal administration rights.

Threatening agents are:

- internal attackers: any authorized user of the protected network
- external attackers: any user external to the protected network

Administrators are not considered as attackers (hypothesis A.ADMIN).

3.4.2 Level of knowledge of the attackers

Attackers are considered to be physical persons with a basic attack capacity that is to say devious people with computer skills of an advanced user.

3.4.3 Threats not taken into consideration

The threats to take into account are only threats which alter the security of the TOE and not the services provided by the TOE because all the environment elements concerning the services provided by the TOE are considered as security policies of the organization. For this reason, physical damages, natural events, main services loss, disruptions due to radiation, equipment robbery, denial of service are not threats to take into account.

Threats relating to the firewall of the TOE only are identified by the prefix T.FW.
Threats relating to the VPN service of the TOE only are identified by the prefix T.VPN.

3.4.4 Threats taken into consideration

3.4.4.1 Threats to the security policies (TSP) of the TOE

Firewall

T.FW.MODIFICATION_POL_FILTRAGE

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

Threatened asset: D.FW.POLITIQUE_FILTRAGE

T.FW.DIVULGATION_POL_FILTRAGE

An attacker steals the filtering policy and/or the contexts of connection of the firewall.

Threatened asset: D.FW.POLITIQUE_FILTRAGE

VPN component

T.VPN.MODIFICATION_POL_VPN

An attacker illegally modifies VPN security policies and their contexts.

Threatened asset: D.VPN.POLITIQUES_VPN.

T.VPN.DIVULGATION_POL_VPN

An attacker steals VPN security policies and their contexts.

Threatened asset: D.VPN.POLITIQUES_VPN.

T.VPN.USURPATION_ID

An external attacker steals the identity of a VPN component on a private network to steal applicative or network topologic data or send fake data.

Threatened asset: D.VPN.DONNEES_APPLICATIVES, D.VPN.INFO_TOPOLOGIE.

3.4.4.2 Threats to the configuration of the TOE

Firewall

T.FW.MODIFICATION_PARAM

An attacker illegally modifies the firewall configuration parameters.

Threatened asset: D.FW.PARAM_CONFIG

T.FW.DIVULGATION_PARAM

An attacker illegally accesses the firewall configuration parameters.

Threatened asset: D.FW.PARAM_CONFIG

VPN component

T.VPN.MODIFICATION_PARAM

An attacker illegally modifies the VPN component configuration parameters.

Threatened asset: D.VPN.PARAM_CONFIG.

T.VPN.DIVULGATION_PARAM

An attacker steals the VPN component configuration parameters.

Threatened asset: D.VPN.PARAM_CONFIG

3.4.4.3 Threats to the cryptographic keys

VPN component

T.VPN.MODIFICATION_CLES

An attacker illegally modifies cryptographic keys by using the keys injection service for example.

Threatened asset: D.VPN.CLES_CRYPTO.

T.VPN.DIVULGATION_CLES

An attacker illegally retrieves cryptographic keys.

Threatened asset: D.VPN.CLES_CRYPTO (only secret and private keys).

3.4.4.4 Threats to flow logs

Firewall

T.FW.MODIFICATION_AUDIT_FLUX

An attacker illegally modifies or deletes flow audit logs.

Threatened asset: D.FW.AUDIT_FLUX

VPN component

T.VPN.MODIFICATION_AUDIT_FLUX

An attacker illegally modifies or deletes audit logs on VPN links activities.

Threatened asset: D.VPN.AUDIT_FLUX

3.4.4.5 Threats to administration logs

Firewall

T.FW.MODIFICATION_AUDIT_ADMIN

An attacker illegally modifies or deletes administration audit logs.

Threatened asset: D.FW.AUDIT_ADMIN

VPN component

T.VPN.MODIFICATION_AUDIT_ADMIN

An attacker illegally modifies or deletes VPN component administration audit logs

Threatened asset: D.VPN.AUDIT_ADMIN

Application note : the threat T.MODIFICATION_AUDIT identified in the VPN component [PP_CIP] protection profile has been divided into two threats T.VPN.MODIFICATION_AUDIT_FLUX and T.VPN.MODIFICATION_AUDIT_ADMIN.

3.4.4.6 Threats to alarms

Firewall

T.FW.MODIFICATION_ALARMES

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

Threatened asset: D.FW.ALARMES

VPN component

T.VPN.MODIFICATION_ALARMES

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

Threatened asset: D.VPN.ALARMES.

3.4.4.7 Threats to the administration

T.USURPATION_ADMIN

An attacker usurps the identity of an administrator and performs administration operations on the TOE.

Threatened asset: all the assets.

3.4.4.8 Threats to the change of the context of use of the TOE

Firewall

T.FW.CHANGEMENT_CONTEXTE

By accessing directly the TOE, an attacker or an administrator of a new protected network has been informed of the firewall sensitive assets during a change of the context of use of the firewall (assignment of the firewall to a new network, maintenance, etc.).

Threatened asset: D.FW.DONNEES_RESEAU_PRIVE, D.FW.POLITIQUE_FILTRAGE, D.FW.AUDIT_FLUX, D.FW.PARAM_CONFIG, D.FW.AUDIT_ADMIN, D.FW.ALARMES.

VPN component

T.VPN.CHANGEMENT_CONTEXTE

By accessing directly the TOE, an attacker or an administrator of a new encryption network has been informed of the VPN component sensitive assets (keys, VPN security policies, etc.) during a change of the context of use (assignment of the VPN component to a new network, maintenance, etc.).

Threatened asset: D.VPN.POLITIQUES_VPN, D.VPN.PARAM_CONFIG, D.VPN.CLES_CRYPTO, D.VPN.AUDIT_FLUX, D.VPN.AUDIT_ADMIN and D.VPN.ALARMES.

3.4.4.9 Threat to the working condition of the services of the TOE

T. DYSFONCTIONNEMENT

An attacker makes the TOE out of order which makes the services unavailable and the status not secure.

Threatened asset: all the *assets*.

3.5 Organisational security policies

The organisational security policies described in this section concern only expected TOE functions and concern therefore services provided by the TOE in the information system.

OSP.QUALIF

The TOE is evaluated according to the Common Criteria [CC] and the EAL3 package of assurance requirements enhanced with the ALC_FLR.3, AVA_VLA.2 components to get a standard qualification [QS].

OSP.CRYPTO

For the standard resistance level, the management of keys (generation, destruction, use and distribution), of cryptography functions used in the TOE and of authentication mechanisms shall comply with [CRYPTO], [GC] and [AUTH] cryptographic reference documents of the ANSSI.

Application note : This organisational security policy, extracted from the [PP_FWIP] and [PP_CIP] protection profiles has been enhanced to take into account the two new ANSSI reference documents about the management of keys used in standard level cryptographic mechanisms [GC] and about the management of authentication mechanisms [AUTH].

OSP.GESTION_ROLES

The TOE shall enable to define different roles of security officer, security administrator, security supervisor, auditor and system and network administrator, system and network supervisor. It also enables to provide logs for the actions performed by each role.

Firewall

OSP.FW.SERVICE

The TOE shall apply the filtering policy defined by the security administrator according to the security policy of the information system.

In contextual mode, the TOE shall be able to set up and apply filtering rules based on the characteristics of the processed flows (for example: source, destination, applicative protocol).

OSP.FW.VISUALISATION_POL

The TOE shall display the current filtering rules.

Application note: the OSP.FILTRAGE organization security policy identified in the [PP_FWIP] protection profile has been divided into two organization security policies: OSP.FW.SERVICE and OSP.FW.VISUALISATION_POL.

OSP.FW.AUDIT_FLUX

The TOE shall track the flows it processes in order to:

- record at least the events generated when a flow is rejected;
- enable the administrator to arrange the recorded events in chronological order;
- enable the administrator to associate an event to a person;

allow reading logs and selecting the recorded events to guarantee the filtering policy is relevant and instancing is good.

VPN component

OSP.VPN.SERVICE

The TOE shall apply the VPN security policies defined by the security administrator. It shall also provide all the security services required to apply the protections specified in these policies:

- protection of the confidentiality of applicative data,
- protection of the authenticity of applicative data,
- protection of the confidentiality of network topologic data,
- protection of the authenticity of network topologic data.

In addition, the TOE shall allow isolating IP flows to make sub-networks (of private networks) communicate and apply a security policy on each communication link between IP sub-networks.

OSP.VPN.VISUALISATION_POL

The TOE shall enable the security administrators to individually visualize the VPN security policies and their security contexts present on the VPN component.

OSP.VPN.SUPERVISION

The TOE shall enable the system and network administrator to check the working status of the VPN component.

4. SECURITY OBJECTIVES

4.1 Security objectives for the TOE

4.1.1 Security objectives on services provided by the TOE

OT.QUALIF

The TOE level of evaluation shall be EAL3 enhanced with the ALC_FLR.3, AVA_VLA.2 components as described in the standard qualification process [QS].

OT.GESTION_ROLES

The TOE shall allow defining the different roles described in §**Erreur ! Source du renvoi introuvable.** and associating the roles to users in a safe manner.

Firewall

OT.FW.APPLICATION_POL_FILTRAGE

The TOE shall apply the filtering policy specified by the administrator and the filtering rules set up by the TOE (contextual mode). This policy can apply to user flows and administration flows.

OT.FW.COHERENCE_POL

In the case of a remote administration, the TOE shall guarantee the coherency between the definition of filtering policies and policies applied on the firewall.

VPN component

OT.VPN.APPLICATION_POL

The TOE shall apply the VPN security policies specified in the VPN components.

OT.VPN.CONFIDENTIALITE_APPLI

The TOE shall provide mechanisms to protect the confidentiality of applicative data which flow between two VPN components.

OT.VPN.AUTHENTICITE_APPLI

The TOE shall provide mechanisms to protect the authenticity of applicative data which flow between two VPN components.

OT.VPN.CONFIDENTIALITE_TOPO

The TOE shall provide mechanisms to protect the confidentiality of private network topologic data included in the IP packets which flow between two VPN components.

OT.VPN.AUTHENTICITE_TOPO

The TOE shall provide mechanisms to protect the authenticity of private network topologic data included in the IP packets which flow between two VPN components.

OT.VPN. CLOISONNEMENT_FLUX

The TOE shall provide the capability to partition IP networks interconnected together thanks to VPN components, by enabling the creation of a new extended IP network, stacked up to the initial IP network made up of IP sub-networks. The TOE shall also provide the capability to enforce a security policy upon every communication link between IP sub-networks.

4.1.2 Security objectives to protect TOE sensitive assets

4.1.2.1 TOE security policies (TSP)

Firewall

OT_FW.PROTECTION_POL_FILTRAGE

The TOE shall supervise the local access (viewing, modification) to the filtering rules and to the connection contexts on the firewall.

OT.FW .VISUALISATION_POL

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

VPN component

OT.VPN.DEFINITION_POL

The TOE shall enable only the security administrator to define the VPN security policies and their security contexts.

OT.VPN.PROTECTION_POL

The TOE shall supervise the access (viewing, modification) to VPN security policies and to their security contexts. Security administrators only have this access.

OT.VPN.VISUALISATION_POL

The TOE shall enable security administrators to individually visualize VPN security policies and their security contexts present on the VPN component.

4.1.2.2 Cryptography and cryptographic keys management

OT.CRYPTO

The TOE shall implement cryptography features and manage (generate, destroy, renew) cryptographic keys according to the [CRYPTO], [GC] and [AUTH] ANSSI cryptography reference documents for the standard resistance level.

Note: There are two types of cryptographic keys in the TOE as described in the D.VPN.CRYPTO sensitive *asset* (session cryptographic keys and static cryptographic keys defined by the VPN security policies). Static cryptographic keys are either generated by the Key Generation Center (out of the scope of the TOE), or generated by the environment and injected in the TOE. The generation/renewal of static cryptographic keys is out of the scope of the TOE then.

VPN component

OT.VPN.ACCES_CLES

The TOE shall protect the access to cryptographic keys.

OT.VPN.INJECTION_CLES

The TOE shall protect the confidentiality of keys (only secret and private keys) and their integrity when injecting them in the VPN components.

4.1.2.3 Configuration

Firewall

OT.FW.PROTECTION_PARAM

The TOE shall supervise the local access on the firewall (viewing, modification) to configuration parameters, access rights, authentication data and elements allowing managing the integrity of administration flows.

VPN component

OT.VPN.PROTECTION_PARAM

The TOE shall protect the confidentiality and integrity of the configuration parameters which can be accessed only by a system and network administrator (for network configuration parameters) and by a security administrator (for access rights and authentication data).

4.1.2.4 Administration

OT.PROTECTION_FLUX_ADMIN

The TOE shall guarantee the authenticity and confidentiality of remote administration flows. The protection of the confidentiality is not always applied if data passing through the flow are not confidential. TOE shall also protect flows against replay attacks.

OT.AUTHENTIFICATION_ADMIN

The TOE shall provide identification and local authentication mechanisms for the different administrators.

4.1.2.5 Recycling

Firewall

OT.FW.CHANGEMENT_CONTEXTE

The TOE shall provide a functionality allowing making the firewall sensitive *assets*unavailable before a change in the context of use: new assignement, maintenance, etc.

VPN component

OT.VPN.CHANGEMENT_CONTEXTE

The TOE shall provide a functionality allowing making the VPN component sensitive *assets*unavailable before a change in the context of use: new assignement, maintenance, etc.

4.1.2.6 Supervision

Firewall

OT.FW.SUPERVISION

The TOE shall enable the system and network administrator and the system and network supervisor to check the working status of the firewall.

OT.FW.IMPACT_SUPERVISION

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

VPN component

OT.VPN.SUPERVISION

The TOE shall enable the system and network administrator and the system and network supervisor to check the working status of the VPN component.

OT.VPN.IMPACT_SUPERVISION

The TOE shall guarantee that the VPN component supervision service does not endanger its sensitive assets.

4.1.2.7 Flows audit

Firewall

OT.FW .AUDIT_FLUX

The TOE shall track the flows it processes in order to:

- record at least the events generated when a flow is rejected;
- enable the administrator to arrange the recorded events in chronological order;
- enable the administrator to associate an event to a person;
- allow reading logs and selecting the recorded events to guarantee the filtering policy is relevant and instancing is good.

OT.FW.PROTECTION_AUDIT_FLUX

The TOE shall supervise the local access on the firewall (viewing, modification) to recorded flow logs and shall enable an auditor to detect the loss of flow log events (using a counter for example).

VPN component

OT.VPN.AUDIT_FLUX

The TOE shall track all the operations performed by the VPN components concerning security and the communications on VPN links. In addition, only an auditor shall be allowed to check what have been tracked.

OT.VPN.PROTECTION_AUDIT_FLUX

The TOE shall guarantee the integrity of log events (operations performed by the VPN component, operations concerning VPN links) it records and shall enable an auditor to detect the loss of log events (using a counter for example).

4.1.2.8 Administration operations audit

Firewall

OT.FW.AUDIT_ADMIN

TOE shall generate logs of operations performed by the firewall administrators. The TOE shall display these logs. Logs generation shall allow associating the recorded administration events to persons.

OT.FW.PROTECTION_AUDIT_ADMIN

The TOE shall supervise the local access on the firewall (viewing, modification) to recorded administration logs and shall enable an auditor to detect the loss of administration log events (using a counter for example).

VPN component

OT.VPN.AUDIT_ADMIN

The TOE shall track all the operations performed by an administrator on VPN components. In addition, only an auditor shall be allowed to check what have been tracked.

OT.VPN.PROTECTION_AUDIT_ADMIN

The TOE shall guarantee the integrity of recorded audit events (operations performed by an administrator on the VPN component) and shall enable an auditor to detect the loss of audit events (using a counter for example).

4.1.3 Alarms

Firewall

OT.FW.ALARMES

The TOE shall generate security alarms if the sensitive assets of the TOE are attacked.

OT.FW.PROTECTION_ALARMES

The TOE shall supervise the local access on the firewall (viewing, modification) to security alarms (set up for local or remote security administrators) and shall enable a security administrator or supervisor to detect the loss of security alarms (using a counter for example).

VPN component

OT.VPN.ALARMES

The TOE shall generate security alarms if the sensitive assets of the TOE are attacked.

OT.VPN.PROTECTION_ALARMES

The TOE shall guarantee the integrity of security alarms (set up for security administrators) it generates and shall enable a security administrator or supervisor to detect the loss of security alarms (using a counter for example).

4.2 Security objectives for the environment of the TOE

4.2.1 TOE designing

OE.CRYPTO

[CRYPTO], [GC] and [AUTH] ANSSI cryptography reference documents shall be followed when designing and operating the TOE for key management (generation, destruction, use and distribution) and the cryptography features used in the TOE for the standard resistance level.

4.2.2 Security objectives for the operation of the TOE

4.2.2.1 Hardware environment

OE.PROTECTION_LOCAL

Equipments containing the TOE services (firewall, VPN and administration equipments) and supports containing the sensitive assets of the TOE (paper, floppy disks, backup, etc.) shall be in a secure room, accessible only by administrators.

However, equipments do not need to be in a secure room if they do not contain sensitive assets: in cases of change in the context of use of the firewall or the VPN component for instance.

OE.INITIALISATION_LOCAL

Equipments containing the TOE services (firewall, VPN and administration equipments) shall be initialized in the secure room of the appliance which is only accessible by administrators. Initialization shall be performed from an administration workstation directly connected to the equipments.

4.2.2.2 Cryptographic keys management

VPN component

OE.VPN.CRYPTO_EXT

The cryptographic keys generated outside and injected into the TOE shall have been generated according to the recommandations specified in the [CRYPTO] ANSSI reference document for the standard resistance level.

In addition, these keys shall be managed according to the recommandations of the [GC] ANSSI for the standard resistance level.

4.2.2.3 TOE management

OE.ADMIN

Administrators have adequate resources to complete their tasks, are trained to carry out the operations which they are responsible for and follow manuals and administration procedures.

Administrators can be trusted..

OE.AUTHENTIFICATION_ADMIN_DISTANT

The TOE environment shall allow authenticating the TOE administrator for the administration equipments remote access.

4.2.2.4 Logs and alarms management

Firewall

OE.FW.ANALYSE_AUDIT

The auditor shall regularly analyze audit logs recorded by the TOE and make decisions accordingly. The memory storing audit logs is managed in such a way that administrators cannot lose logs.

In addition, audit logs shall be backed up and archived in case they would be deleted by accident or intentionally.

OE.FW.TRAITE_ALARMES

The security administrator shall analyze and manage security alarms generated and displayed by the TOE.

VPN component

OE.VPN.ANALYSE_AUDIT

The auditor shall regularly analyze the audit logs recorded by the TOE and make decisions accordingly. The memory storing audit logs is managed in such a way that admninistrators cannot lose logs.

OE.VPN.TRAITE_ALARMES

The security administrator shall manage security alarms generated by the TOE.

4.2.2.5 Control of the TOE

Firewall

OE.FW.INTEGRITE

The administrator has adequate resources to control or regenerate in a safe state the firewall hardware and software configuration according to a reference state.

VPN component

OE.VPN.INTEGRITE

The administrator has adequate resources to control or regenerate in a safe state the VPN component hardware and software configuration according to a reference state.

Application note: This security objective for the environment of the TOE, extracted from the [PP_CIP] protection profile has been enhanced: it requires now the TOE to be able to regenerate the configuration in a safe state.

5. SECURITY REQUIREMENTS

5.1 Functional requirements for the TOE

5.1.1 Summary

Requirements	Titles
Class FAU: 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_STG.1	Protected audit trail storage
Class FCS: Cryptographic support	
FCS_COP.1	Cryptographic operation
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
Class FDP: User data protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple secure attributes
FDP_ITC.1	Import of user data without security attributes
FDP_RIP.1	Subset residual information protection
Class FIA: Identification and authentication	
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Class FPT: Protection of the TSF	
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency
Class FMT: Security management	

	FMT_MSA.1	**Management of security attributes**
	FMT_MSA.3	**Static attribute initialisation**
	FMT_SMF.1	**Specification of Management Functions**
	FMT_SMR.1	**Security roles**
	FMT_MTD.1	**Management of TSF data**
Class FTA: TOE access		
	FTA_TSE.1	**TOE session establishment**

All functional security requirements for the TOE are extracted from the part 2 of Common Criteria [CC].

5.1.2 Detail of the functional requirements for the TOE

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Global refinement:

The expected reliability of time stamps relies on the fact that only the administrator of the TOE is allowed to modify them. Time stamps shall be reliable between two updates performed by the administrator.

Remote administration protection

FPT_ITT.1-Administration_distante Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1-Administration_distante The TSF shall protect TSF data from [selection: disclosure (when data are confidential) and modification] when it is transmitted between separate parts of the TOE.

FPT_ITT.3-Administration_distante TSF data integrity monitoring

FPT_ITT.3.1-Administration_distante The TSF shall be able to detect [selection: modification of data, substitution of data, re-ordering of data, deletion of data] for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2-Administration_distante Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: stop the current connection].

FIA_UAU.2-Station_administration_distante User authentication before any action

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1

FIA_UAU.2.1-Station_administration_distante The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Global refinement:

This requirement concerns the authentication for the remote administration of the TOE. This requirement concerns the authentication of the administration station regarding the TOE. The authentication can be reinforced within the TOE with an authentication of the administrator directly in the TOE. For reference, the authentication of the remote administrator on the remote administration station is part of the TOE environment.

Roles management

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: security officer, security administrator, system and network administrator, auditor, system and network supervisor, security supervisor].

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

FIA_UID.2-Administrateurs User identification before any action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies.

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

Global refinement:

Here users are the administrators. Do not confuse with the ability of some firewall to link filtering to an identification/authentication of networks users.

The identification of administrators can be local or included in the remote administration flow.

FIA_UAU.2-Administrateurs_local User authentication before any action

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1

FIA_UAU.2.1-Administrateurs_local The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Global refinement:

This requirement concerns the authentication of the administrators for the local administration of the TOE. For the remote administration, the authentication of the administrator on the administration station is not included in the scope of the TOE and is then covered by an objective on the environment. For the requirements about remote administration, refer to functional security requirements for the TOE technical environment.

FMT_MTD.1-Param_security_administrator Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1, FMT_SMF.1

FMT_MTD.1.1-Param_security_administrator The TSF shall restrict the ability to [selection: modify] the [assignment: identification and authentication data and access rights] to [assignment: security officer].

FMT_MTD.1-Param_auditor Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1, FMT_SMF.1

FMT_MTD.1.1-Param_auditor The TSF shall restrict the ability to [selection: query] the [assignment: identification and authentication data and access rights] to [auditor].

5.1.2.1 Functional security requirements for the firewall

Filtering policy application

FDP_IFC.2/FW-Enforcement_policy Complete information flow control

Hierarchical to: FDP_IFC.1

Dependencies: FDP_IFF.1

FDP_IFC.2.1/FW-Enforcement_policy The TSF shall enforce the [assignment: filtering policy (and rules relative to connection contexts in contextual mode)] on [assignment:

- users IP flows using TCP, UDP, ICMP network protocols,
- users IP flows using HTTP, FTP, DNS and SMTP applicative protocols,
- administration flows]

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

FDP_IFC.2.2/FW-Enforcement_policy 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/FW-Enforcement_policy Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1, FMT_MSA.3

FDP_IFF.1.1/FW-Enforcement_policy The TSF shall enforce the [assignment: filtering policy (and rules relative to connection contexts in contextual mode)] based on the following types of subject and information security attributes: [assignment:

- source and destination IP addresses of IP packets,
- TCP, ICMP and UDP network protocols of IP packets,
- source and destination services of IP packets,
- applicative commands of HTTP, FTP, DNS and SMTP applicative protocols of IP packets,
- source and destination communication ports of IP packets].

FDP_IFF.1.2/FW-Enforcement_policy The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment:

a. Users of the protected network can send IP flows from the protected network to the external network through the TOE if:
   - the attributes of the IP packet processed match the criteria defined in the filtering policy and/or filtering rules relative to the connection context in contextual mode,
   - the source address of the IP packet translates to an internal address,
   - the destination address of the IP packet is translated to an external address.

b. Users of the external network can send IP flows from the external network to the protected network through the TOE if:
   - the attributes of the IP packet processed match the criteria defined in the filtering policy and/or filtering rules relative to the connection context in contextual mode,
   - the source address of the IP packet translates to an external address,
   - the destination address of the IP packet is translated to an internal address].

FDP_IFF.1.3/FW-Enforcement_policy The TSF shall enforce the [assignment: none].

FDP_IFF.1.4/FW-Enforcement_policy The TSF shall provide the following [assignment: none].

FDP_IFF.1.5/FW-Enforcement_policy The TSF shall explicitly authorise an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6/FW-Enforcement_policy The TSF shall explicitly deny an information flow based on the following rules: [assignment:

a. Reject packets reaching the TOE external interface and of which the source address corresponds to an address on the protected network.

b. Reject packets reaching the TOE internal interface and of which the source address corresponds to an address on the external network.

c. Reject packets reaching the TOE internal or external interface and of which the source address corresponds to an external address on a broadcast network.

d. Reject packets in which users (of the protected network or of the external network) specify the route of the packets to reach the destination address.

e. Reject the packets reaching the TOE internal or external interface and of which source and destination addresses are the same.

f. For network protocols supported by the TOE (IP, TCP, UDP and ICMP), the TOE shall reject malformed packets.

g. Reject TCP packets which do not contain a connection sequence number unexpected by the TOE.

h. The TOE shall reject packets when the number of concurrent active connections reaches or exceeds the number of concurrent active connections defined by the security administrator.

i. For applicative protocols supported by the TOE (DNS, HTTP, SMTP and FTP), the TOE shall reject all applicative commands non identified in the following table:

HTTP							
OPTIONS	GET	HEAD	POST	PUT	DELETE	TRACE	CONNECT
SMTP							
HELO	MAIL	RCPT	DATA	RSET	SEND	SOML	SAML
VRFY	EXPN	NOOP	HELP	QUIT	AUTH	EHLO	ETRN
STARTTLS							
FTP							
USER	PASS	ACCT	CWD	CDUP	SMNT	QUIT	REIN
PORT	PASV	TYPE	STRU	MODE	RETR	STOR	STOU
APPE	ALLO	REST	RNFR	RNTO	ABOR	DELE	RMD
MKD	PWD	LIST	NLST	SITE	SYST	STAT	HELP
NOOP	MKD	XRMD	XPWD	XCUP	MDTM	SIZE	FEAT
MLST	MLSD	OPTS					
DNS							
NS	CNAME	SOA	WKS	PTR	HINFO	MINFO	MX
TXT	AAAA	AXFR	IN				

j. For HTTP, FTP, SMTP and DNS protocols, the TOE shall reject all applicative flows which do not respect the specifications of these protocols (RFC for example).

k. For HTTP, FTP, SMTP and DNS protocols, the TOE shall reject flows containing applicative commands from the table above and which are not authorized by the security administrator.

l. For the HTTP applicative protocol; the TOE shall reject flows which break HTTP applicative options configured by the security administrator:
   - URL maximum size
   - Forbidden keywords in URLs
   - Forbidden client HTTP header
   - Client HTTP header maximum size
   - Forbidden server HTTP header
   - Server HTTP header maximum size

m. For the FTP protocol, the TOE shall reject flows which break FTP applicative options configured by the security administrator:
   - Authorized users
   - Command lines maximum size

n. For the SMTP protocol, the TOE shall reject flows which break SMTP applicative options configured by the security administrator:
    - Command lines maximum size

o. For the DNS protocol, the TOE shall reject flows which break DNS applicative options configured by the security administrator:
    - Authorized DNS types
    - Authorized DNS classes

FMT_SMF.1/FW-Visualisation_politique_filtrage Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/FW-Visualisation_politique_filtrage The TSF shall be capable of performing the following security management functions: [assignment: viewing of the filtering policy and of connection contexts present on the firewall].

FPT_TDC.1/FW-Administration_distante Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1/FW-Administration_distante The TSF shall provide the capability to consistently interpret [assignment: the filtering policy of the TOE firewall] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/FW-Administration_distante The TSF shall use [assignment: none] when interpreting the TSF data from another trusted IT product.

Filtering policy protection

FDP_ACC.1/FW-Filtering_policy Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1

FDP_ACC.1.1/FW-Filtering_policy The TSF shall enforce the [assignment: access policies to filtering rules] on [assignment:

- subjects: administrators;
- objects: filtering policy rules;
- operations: read, insert, modify, delete].

FDP_ACF.1/FW-Filtering_policy Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1/FW-Filtering_policy The TSF shall enforce the [assignment: access policies to filtering rules] to objects based on the following: [assignment:

- subjects: administrators based on their role;
- objects: filtering policy rules].

FDP_ACF.1.2/FW-Filtering_policy The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- only the security administrator is allowed to insert, modify and delete (totally or partially) filtering rules;
- only the security administrator and the auditor are allowed to read filtering rules and connection contexts].

FDP_ACF.1.3/FW-Filtering_policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: none].

FDP_ACF.1.4/FW-Filtering_policy The TSF shall explicitly deny access of subjects to objects based on the [assignment: none].

Flow audit data generation

FAU_GEN.1/FW-Audit_flux Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1

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

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

b) All auditable events for the minimal or basic level of audit defined in appendix 1 with the associated audit level;

c) At least events generated when a flow is rejected.

FAU_GEN.1.2/FW-Audit_flux 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:
   - a unique digital ID for every flow audit event of the firewall, incremented by one unit for every record of a new flow audit event of the firewall].

Global refinement:

The recorded audit data shall enable administrators in particular to be sure the filtering policy is reliable and instancing within the firewall is good.

FAU_GEN.2/FW-Audit_flux User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1, FIA_UID.1

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

Non-editorial refinement:

The ‘identity of the user’ is the IP address of the flows issuers.

FIA_UID.2/FW-Flux User identification before any action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies.

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

Global refinement:

Here ‘users’ are issuers and recipients of flows processed by the firewall and who are identified by their IP addresses.

FAU_SAR.1/FW-Audit_flux Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit

FAU_SAR.1.1/FW-Audit_flux The TSF shall provide [assignment: security administrators, auditors] with the capability to read [assignment: audit data of flows processed by the firewall] from the audit records.

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

FAU_SAR.3/FW-Audit_flux Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1

FAU_SAR.3.1/FW-Audit_flux The TSF shall provide the ability to perform [selection: sorting, searches] of audit data based on [assignment:

- source IP addresses of packets,
- destination IP addresses of packets,
- a range of source IP addresses,
- a range of destination IP addresses,
- packets applications (HTTP, FTP, DNS and SMTP),
- processing date and time of packets].

Flows audit data protection

FAU_STG.1/FW-Traces_audit_flux Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

FAU_STG.1.1/FW-Traces_audit_flux The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2/FW-Traces_audit_flux The TSF shall be able to [selection: prevent] unauthorised modifications to the stored audit records in the audit trail.

Administration operations audit data generation

FAU_GEN.1/FW-Audit_admin Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1

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

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

b) All auditable events for the minimal or basic level of audit defined in appendix 1 with the associated audit level; and

c) [assignment: none]

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

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

d) b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment:
   - a unique digital ID for every administration audit event of the firewall, incremented by one unit for every record of a new administration audit event of the firewall].

FAU_GEN.2/FW-Audit_admin User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1, FIA_UID.1

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

FAU_SAR.1/FW-Audit_admin Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

FAU_SAR.1.1/FW-Audit_admin The TSF shall provide [assignment: security administrators, auditors] with the capability to read [assignment: audit data of firewall administration events] from the audit records.

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

FAU_SAR.3/FW-Audit_admin Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1

FAU_SAR.3.1/FW-Audit_admin The TSF shall provide the ability to perform [selection: sorting, searches] of audit data based on [assignment:

- the type of administration operation,
- the identity of the administrator,
- the date and time at which the administration operation has been performed.]

Administration operations audit data protection

FAU_STG.1/FW-Traces_audit_admin Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

FAU_STG.1.1/FW-Traces_audit_admin The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2/FW-Traces_audit_admin The TSF shall be able to [selection: prevent] unauthorised modifications to the stored audit records in the audit trail.

Alarms

FAU_SAA.1/FW-Alarmes Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

FAU_SAA.1.1/FW-Alarmes 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/FW-Alarmes The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment:
   - violation of the security policy of the TOE firewall,
   - saturation of logs of the TOE firewall,
   - TOE firewall integrity loss,
   - system saturation (hard disk, quarantine, etc.),
   - denial of service of the TOE firewall,
   - incorrect packets reception by the TOE firewall]

   known to indicate a potential security violation;

b) [assignment: none].

FAU_ARP.1/FW-Alarmes Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1

FAU_ARP.1.1-Alarmes The TSF shall take [assignment:

- forwarding an alarm to the security administrator.
- stop all flows passing through the TOE firewall, except TOE firewall administration flows when logs of the firewall are saturated] upon detection of a potential security violation.

Configuration

FMT_SMF.1/FW-Configuration Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/VPN-Configuration The TSF shall be capable of performing the following security management functions: [assignment:

- TOE parameters configuration:
  - administrators roles,
  - administrators identification and authentication data,
  - access rights
  - system date and time
- TOE system and network parameters configuration ;
- filtering policy configuration].

FMT_MTD.1/FW-Network_param Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1, FMT_SMF.1

FMT_MTD.1.1/FW-Network_param The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear] the [assignment: system and network configuration parameters, system date and time] to [assignment: system and network administrators].

Monitoring

FMT_SMF.1/FW-Supervision Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/FW-Supervision The TSF shall be capable of performing the following security management functions: [assignment:

- viewing of the VPN component system and network parameters,
- of the VPN component system and network parameters,
- firewall status supervision].

FPT_ITC.1/FW-Supervision Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Global refinement:

Data exported out of the control of the TOE are data strictly necessary to the monitoring, and are transmitted to a monitoring equipment. If these data include confidential information, they need to be protected.

Recycling

FDP_RIP.1/FW-Recyclage_TOE Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1/FW-Recyclage_TOE The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: deallocation of the resource from] the following objects: [assignment: all firewall sensitive assets:

- firewall filtering policies,
- configuration parameters,
- audit data of the flows processed by the firewall,
- firewall alarms,
- audit data of administration operations performed on the firewall].

FDP_ACC.1/FW-Recyclage_TOE Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1

FDP_ACC.1.1Recyclage_TOE The TSF shall enforce the [assignment: access policy to sensitive assets] on [assignment:

- subjects: administrators;
- objects: all sensitive assets of the firewall: filtering policy, configuration parameters, audit data of flows processed by the firewall, audit data of administration operations performed on the firewall;
- operations: clear].

FDP_ACF.1/FW-Recyclage_TOE Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1/FW-Recyclage_TOE The TSF shall enforce the [assignment: access policy to sensitive assets] to objects based on the following: [assignment:

- subjects: administrators based on their role;
- objects: all sensitive assets of the firewall: filtering policy, configuration parameters, audit data of flows processed by the firewall, audit data of administration operations performed on the firewall].

FDP_ACF.1.2/FW-Recyclage_TOE The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: Only the security officer is allowed to clear (totally or partially) sensitive assets (filtering policy, configuration parameters, audit data of flows processed by the firewall, audit data of administration operations performed on the firewall)].

FDP_ACF.1.3/FW-Recyclage_TOE The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: none].

FDP_ACF.1.4/FW-Recyclage_TOE The TSF shall explicitly deny access of subjects to objects based on the [assignment: none].

5.1.2.2 Functional security requirements for the VPN component

VPN security policy application

FDP_IFC.1/VPN-Enforcement_policy Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1

FDP_IFC.1.1/VPN-Enforcement_policy The TSF shall enforce the [assignment: the VPN protection policy] on [assignment:

- Information: applicative and topologic data included in IP packets.
- Subject: the VPN component.
- Operations: all operations performed by the VPN component transforming applicative and topologic data in flows. It concerns the following operations:
  - Sending an IP packet to the external network
  - Sending an IP packet to the private network
  - Receiving a packet from the external network
  - Receiving a packet from the internal network].

FDP_IFF.1/VPN-Enforcement_policy Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1, FMT_MSA.3

FDP_IFF.1.1/VPN-Enforcement_policy The TSF shall enforce the [assignment: the VPN protection policy] based on the following types of subject and information security attributes: [assignment:

- AT.policy_defined: attribute indicating if a VPN security policy has been defined for a given VPN link].

FDP_IFF.1.2/VPN-Enforcement_policy The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment:

- sending IP packets to the external network is permitted only if security protections defined in the associated VPN protection policy are applied to IP packets applicative and topologic data before sending them to the external network.
- sending IP packets to the internal network is permitted only if security protections defined in the associated VPN protection policy are applied to IP packets applicative and topologic data before sending them to the internal network.
- receiving IP packets from the external network is permitted.
- receiving IP packets from the private internal network is permitted].

FDP_IFF.1.3/VPN-Enforcement_policy The TSF shall enforce the [assignment: none].

FDP_IFF.1.4/VPN-Enforcement_policy The TSF shall provide the following [assignment: none].

FDP_IFF.1.5/VPN-Enforcement_policy The TSF shall explicitly authorise an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6/VPN-Enforcement_policy The TSF shall explicitly deny an information flow based on the following rules: [assignment

- when no VPN protection policy has been defined for a given VPN link (attribute AT.policy_defined with the value « VPN protection policy not defined »), the TSF shall reject IP packets. They are not transmitted then.
- when a VPN protection policy indicates that sending IP packets to an address is not permitted, the TSF shall not transmit IP packets.
- when an error is detected during the operation of the TOE, or as a result of the check of security protections, sending IP packets is not permitted].

FDP_ITC.1/VPN-Enforcement_policy Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3

FDP_ITC.1.1/VPN-Enforcement_policy The TSF shall enforce the [assignment: the VPN protection policy] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2/VPN-Enforcement_policy The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3/VPN-Enforcement_policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: none].

Global refinement:

User data mentioned in these requirements are IP packets of internal network users, including applicative and topologic data.

FDP_ETC.1/VPN-Enforcement_policy Export of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 or FDP_IFC.1]

FDP_ETC.1.1/VPN-Enforcement_policy The TSF shall enforce the [assignment: the VPN protection policy] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2/VPN-Enforcement_policy The TSF shall export the user data without the user data's associated security attributes.

Global refinement:

User data mentioned in these requirements are IP packets of internal network users, including applicative and topologic data.

FCS_COP.1/VPN-Enforcement_policy Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2

FCS_COP.1.1/VPN-Enforcement_policy The TSF shall perform [assignment: encryption, decryption, authentication] in accordance with a specified cryptographic algorithm [assignment: RSA, SHA256, AES] and cryptographic key sizes [assignment: 128 bits (AES), 256 bits (AES), 2048 bits (RSA)] that meet the following: [assignment : [AES], [RSA], [SHA256], and cryptographic referential of ANSSI ([CRYPTO])].

Global refinement:

RSA (2048 bits), AES (128 and 256 bits) and SHA-256 cryptographic algorithms are implemented in the framework of the IKE protocol. AES (128 and 256 bits) and SHA-256 cryptographic algorithms are implemented in the framework of the IPSEC protocol.

VPN security policy protection

FDP_ACC.1/VPN-VPN_policy Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1

FDP_ACC.1.1/VPN-VPN_policy The TSF shall enforce the [assignment: VPN protection policy] on [assignment:

- objects: VPN protection policies and the associated security contexts.
- subjects: TOE security administration functions enabling to define and display the VPN protection policies and the associated contexts.
- operations: define and display the VPN protection policies and the associated contexts.].

FDP_ACF.1/VPN-VPN_policy Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1/VPN-VPN_policy The TSF shall enforce the [assignment: the VPN protection policy] to objects based on the following: [assignment:

- AT.policy_defined : AT.policy_defined : attribute indicating if a VPN security policy has been defined for a given VPN link].

FDP_ACF.1.2/VPN-VPN_policy The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- only a security administrator and no other role is allowed to define VPN protection policies and the associated security contexts.
- only a security administrator and no other role is allowed to display VPN protection policies and the associated security contexts].

FDP_ACF.1.3/VPN-VPN_policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: none].

FDP_ACF.1.4/VPN-VPN_policy The TSF shall explicitly deny access of subjects to objects based on the [assignment: none].

FDP_ITC.1/VPN-VPN_policy Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3

FDP_ITC.1.1/VPN-VPN_policy The TSF shall enforce the [assignment: the VPN protection policy] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2/VPN-VPN_policy The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3/VPN-VPN_policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: none].

Global refinement:

User data mentioned in these requirements correspond to VPN component security policies.

FMT_MSA.3/VPN-VPN_policy Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1, FMT_SMR.1

FMT_MSA.3.1/VPN-VPN_policy The TSF shall enforce the [assignment: the VPN protection policy] to provide [selection: restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/VPN-VPN_policy The TSF shall allow the [assignment: none] to specify alternative initial values to override the default values when an object or information is created.

Global refinement:

The security attribute involved in these requirements is the AT.policy_defined attribute which indicates for each VPN communication link if a VPN security policy and its security context are defined. The initial value of the AT.policy_defined attribute is: « VPN security policy not defined ». This value is changed by the TOE security administrator when he defines the security policy and context of a VPN communication link. The value of this attribute becomes then: « VPN security policy defined ».

FMT_MSA.1/VPN-VPN_policy Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1

FMT_MSA.1.1/VPN-VPN_policy The TSF shall enforce the [assignment: the VPN protection policy] to restrict the ability to [selection: modify] the security attributes [assignment: AT.policy_defined] to [assignment: security administrator].

FMT_SMF.1/VPN-VPN_policy Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/VPN-VPN_policy The TSF shall be capable of performing the following security management functions: [assignment:

- TOE parameters configuration:
    - administrators roles,
    - administrators identification and authentication data,
    - access rights,
    - system date and time
- system and network parameters configuration;
- VPN security policy configuration (VPN component revocation, attribution of cryptographic keys to VPN links, distribution of the VPN component certificate to other VPN components, etc.)].

Flows audit data generation

FAU_GEN.1/VPN-Audit_flux Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1

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

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

b) All auditable events for the minimal or basic level of audit defined in appendix 1 with the associated audit level ; and

c) [assignment : none]

FAU_GEN.1.2/VPN-Audit_flux 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

d) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment:
   - a unique digital ID for each flow audit event of the VPN component, incremented by one unit for each record of a new flow audit event of the VPN component].

Global refinement:

Audit events mentioned in these requirements correspond to events relative to the communication between VPN components.

FAU_SAR.1/VPN-Audit_flux Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

FAU_SAR.1.1/VPN-Audit_flux The TSF shall provide [assignment: auditors] with the capability to read [assignment: audit data of flows processed by the VPN component] from the audit records.

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

FAU_SAR.3/VPN-Audit_flux Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1

FAU_SAR.3.1/VPN-Audit_flux The TSF shall provide the ability to perform [selection: searches, sorting, ordering] of audit data based on [assignment:

- source and destination IP address of encrypted flows,
- date and time of the processing of packets].

Flows audit data protection

FAU_STG.1/VPN-Traces_audit_flux Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

FAU_STG.1.1/VPN-Traces_audit_flux The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2/VPN-Traces_audit_flux The TSF shall be able to [selection: prevent] unauthorised modifications to the stored audit records in the audit trail.

Administration operations audit data generation

FAU_GEN.1/VPN-Audit_admin **Audit data generation**

Hierarchical to: No other components.

Dependencies: FPT_STM.1

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

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

b) All auditable events for the minimal or basic level of audit defined in appendix 1 with the associated audit level; and

c) [assignment: none].

FAU_GEN.1.2/VPN-Audit_admin 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:
   - a unique digital ID for each administration audit event of the VPN component, incremented by one unit for each record of a new administration audit event of the VPN component].

Global refinement:

Audit events mentioned in these requirements correspond to events relative to TOE administration operations.

FAU_SAR.1/VPN-Audit_admin Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

FAU_SAR.1.1/VPN-Audit_admin The TSF shall provide [assignment: authorised users] with the capability to read [assignment: administration operations audit data] from the audit records.

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

FAU_SAR.3/VPN-Audit_admin Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1

FAU_SAR.3.1/VPN-Audit_admin The TSF shall provide the ability to perform [selection: searches, sorting, ordering] of audit data based on [assignment:

- the type of administration operation,
- the administrator identity,
- the date and time at which the administration operation has been performed.]

Protection of administration operations audit data

FAU_STG.1/VPN-Traces_audit_admin Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

FAU_STG.1.1/VPN-Traces_audit_admin The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2/VPN-Traces_audit_admin The TSF shall be able to [selection: prevent] unauthorised modifications to the stored audit records in the audit trail.

Alarms

FAU_SAA.1/VPN-Alarmes Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

FAU_SAA.1.1/VPN-Alarmes 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/VPN-Alarmes The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment:
   - violation of the TOE VPN component security policy,
   -
   - integrity loss of the TOE VPN component,
   - system saturation (hard disk, quarantine, etc.),
   - denial of service of the TOE VPN component,
   - failure of the authentication of a private network user (use of a certificate revoked or not complete, incorrect shared secret, incorrect key)
   - encrypted data which do not correspond to the security context of the VPN link]

   known to indicate a potential security violation;

b) overflow of the audit trail capacity

c) [assignment: none].

FAU_ARP.1/VPN-Alarmes Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1

FAU_ARP.1.1/VPN-Alarmes The TSF shall take [assignment:

- a security alarm is forwarded to the security administrator,
- [assignment: none]]

upon detection of a potential security violation.

Configuration

FMT_MTD.1/VPN-Network_param Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1, FMT_SMF.1

FMT_MTD.1.1/VPN-Network_param The TSF shall restrict the ability to [selection: query and modify] the [assignment: system and network configuration parameters] to [assignment: system and network administrator].

Monitoring

FMT_SMF.1/VPN-Config_supervision Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/VPN-Config_supervision The TSF shall be capable of performing the following security management functions: [assignment:

- viewing of system and network parameters of the VPN component,
- modification of system and network parameters of the VPN component,
- monitoring of the VPN component status].

Recycling

FDP_RIP.1/VPN Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1/VPN The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: deallocation of the resource from] the following objects: [assignment: all sensitive assets of the VPN component:

- VPN protection policies,
- configuration parameters,
- cryptographic keys,
- audit data of flows processed by the VPN component,
- VPN component alarms,
- audit data of administration operations performed by the VPN component].

Cryptographic key management

FDP_ITC.1/VPN-Key_policy Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3

FDP_ITC.1.1/VPN-Key_policy The TSF shall enforce the [assignment: politique de gestion des clés cryptographiques] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2/VPN-Key_policy The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3/VPN-Key_policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: none].

Global refinement:

User data mentioned in these requirements correspond to cryptographic keys which are injected in the TOE VPN component.

FDP_IFC.1/VPN-Key_policy Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1

FDP_IFC.1.1/Key_policy The TSF shall enforce the [assignment: cryptographic key management policy] on [assignment:

- Information: VPN component cryptographic keys value
- Subjects: security administrators
- Operations: injecting cryptographic keys in the VPN component and exporting VPN component cryptographic keys].

FDP_IFF.1/VPN-Key_policy Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1, FMT_MSA.3

FDP_IFF.1.1/VPN-Key_policy The TSF shall enforce the [assignment: cryptographic key management policy] based on the following types of subject and information security attributes: [assignment:

- AT.key_type attribute: indicates if a cryptographic key is public, private or secret.
- [assignment: none].

FDP_IFF.1.2/VPN-Key_policy The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: local injection of cryptographic keys is authorized only if it is performed by a security administrator authenticated beforehand].

FDP_IFF.1.3/VPN-Key_policy The TSF shall enforce the [assignment: injection of private and secret static cryptographic keys in the VPN component protecting their integrity and confidentiality].

FDP_IFF.1.4/VPN-Key_policy The TSF shall provide the following [assignment: none].

FDP_IFF.1.5/VPN-Key_policy The TSF shall explicitly authorise an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6/VPN-Key_policy The TSF shall explicitly deny an information flow based on the following rules: [assignment: the export of uncoded private or secret keys out of the VPN component is forbidden].

FMT_MSA.3/VPN-Key_policy Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1, FMT_SMR.1

FMT_MSA.3.1/VPN-Key_policy The TSF shall enforce the [assignment: cryptographic key management policy] to provide [selection: [assignment: the cryptographic key type (private, secret, public, appropriate)]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/VPN-Key_policy The TSF shall allow the [assignment: none] to specify alternative initial values to override the default values when an object or information is created.

FTA_TSE.1/VPN-Key_policy TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1/VPN-Key_policy The TSF shall be able to deny session establishment based on [assignment: the lifetime of session cryptographic keys].

FCS_CKM.1/VPN-Key_policy Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or FDP_ITC2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2

FCS_CKM.1.1/Key_policy The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: AES] and specified cryptographic key sizes [assignment: 128 bits, 256 bits] that meet the following: [assignment: [AES] [CRYPTO], [GC], [AUTH]].

FCS_CKM.4/VPN-Key_policy Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or FDP_ITC2 or FCS_CKM.1], FMT_MSA.2

FCS_CKM.4.1/VPN-Key_policy The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method by overwriting keys 7 times with random patterns] that meets the following: [assignment: none].

5.1.3 Minimal resistance level of security funcions

The required minimal level of resistance for the TOE security functions (SOF-Claim) [1] is: **high** (**SOF-high**).

5.2 Assurance requirements for the TOE

The aimed level is **EAL3 enhanced** with AVA_VLA.2 and ALC_FLR.3 components.

Requirements	Titles
Class ACM: Configuration Management	
ACM_CAP.3	**Configuration items**
ACM_SCP.1	**TOE CM coverage**
Class ADO: Delivery and Operation	
ADO_DEL.1	**Delivery procedures**
ADO_IGS.1	**Installation, generation, and start-up procedures**
Class ADV: Development	
ADV_FSP.1	**Informal functional specification**
ADV_HLD.2	**Security enforcing high-level design**
ADV_RCR.1	**Informal correspondence demonstration**
Class AGD: Guidance Documents	
AGD_ADM.1	**Administrator guidance**
AGD_USR.1	**User guidance**
Class ALC: Life Cycle Support	
ALC_DVS.1	**Identification of security measures**
ALC_FLR.3	**Systematic flaw remediation**
Class ATE: Tests	
ATE_COV.2	**Evidence of coverage**
ATE_DPT.1	**Testing: high-level design**
ATE_FUN.1	**Functional testing**
ATE_IND.2	**Independent testing - sample**
Class AVA: Vulnerability Assessment	
AVA_MSU.1	**Examination of guidance**
AVA_SOF.1	**Strength of TOE security function evaluation**
AVA_VLA.2	**Independent vulnerability analysis**

[1] Intrinsic resistance level of a function against attacks.This level is different from the TOE global resistance level (level defined by the AVA_VLA component) which takes into account attacks affecting TOE functions or making them ineffective.

All assurance requirements for the TOE are extracted from Part 3 of Common Criteria [CC].

Dependencies of the AVA_VLA.2 (ADV_IMP.1 and ADV_LLD.1) assurance requirement are handled by cryptographic expert work carried out by the CESTI. This work is described in [QS].

5.3 Requirements for the technical environment of the TOE

All functional security requirements for the technical environment of the TOE are extracted from Part 2 of Common Criteria [CC].

FIA_UAU.2-Administration_distante User authentication before any action

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1

FIA_UAU.2.1-Administration_distante The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Global refinement:

It deals with the remote authentication of the administrator on the remote administration station.

6. TOE SPECIFICATIONS SUMMARY

6.1 Security functions

F.RELIABLE_TIME

SOF-claim : No SOF claim

This function provides reliable and unique time stamps to the TOE. Only an authenticated security administrator or system and network administrator is allowed to change the TOE system time.

Rational: F.RELIABLE_TIME covers time delivery security requirement FPT_STM.1.

F.AUDIT

SOF-claim : No SOF claim

The audit function provides security functions relative to TOE events logging. It manages the identification, recording and storage of TOE events. There are three types of recorded events: flows audit data, administration audit data and security alarms. Flows audit data provide information about packets processed by the firewall and the VPN component of the TOE (flows stopped or rejected because of the TOE security policy). Administration audit data provide information about operations performed by administrators on the TOE. Security alarms indicate a serious problem which could weaken the security of the TOE.

FAST Monitoring Console software is installed on a remote administration station and provides to authorized and authenticated administrators a graphical environment enabling them to consult audit logs and to detect all events relative to the security of the TOE. Alerts provide a severity level, a time stamp and an explanatory description enabling administrators to act accordingly. Flows audit data provide details relative to packets which have been recorded and are time stamped. Administration audit data provide the identity of the administrator, the description of the operation performed and are time stamped. The graphical interface of FAST Monitoring enables to sort out each event type according to criteria defined by the TOE administrators.

The TOE audit function provides an interface enabling TOE administrators to export these data outside the TOE, which flushes the disk space dedicated to logs. Only authenticated administrators are allowed to access event logs.

Rational: F.AUDIT covers all security requirements generating logging events:

- *Flow audit data generation:* *FAU_GEN.1/FW-Audit_flux, FAU_GEN.2/FW-Audit_flux, FAU_SAR.1/FW-Audit_flux, FAU_SAR.3/FW-Audit_flux, FAU_GEN.1/VPN-Audit_flux, FAU_SAR.1/VPN-Audit_flux, FAU_SAR.3/VPN-Audit_flux*
- *Flows audit data protection :* *FAU_STG.1/FW-Traces_audit_flux, FAU_STG.1/VPN-Traces_audit_flux*
- *Administration operations audit data generation:* *FAU_GEN.1/FW-Audit_admin, FAU_GEN.2/FW-Audit_admin, FAU_SAR.1/FW-Audit_admin, FAU_SAR.3/FW-Audit_admin FAU_GEN.1/VPN-Audit_admin, FAU_SAR.1/VPN-Audit_admin, FAU_SAR.3/VPN-Audit_admin*
- *Administration operations audit data protection:* *FAU_STG.1/FW-Traces_audit_admin, FAU_STG.1/VPN-Traces_audit_admin*
- *Alarms :* *FAU_SAA.1/FW-Alarmes, FAU_ARP.1/FW-Alarmes FAU_SAA.1/VPN-Alarmes, FAU_ARP.1/VPN-Alarmes*

F.USER_DATA_PROTECTION_FW

SOF-claim : No SOF claim

User protection function provides TOE security functions relative to the firewall. This function guarantees the protection of users of the protected network by filtering flows exchanged between the protected network and the external network (unsafe), according to a firewall security policy (also known as filtering policy) defined by the administrator.

The TOE performs a first check (IP address, port, etc.) to check the consistency of the IP packet with regard to the filtering policy defined by the security administrator. After this first check, the IP packet is either rejected or accepted. If the packet is accepted, a second check (applicative layer) is performed to check the consistency of the packet with regard to the applicative filtering policy of the TOE. The TOE is able to perform a filtering on HTTP, FTP, SMTP, DNS protocols. For each of these supported protocols, the TOE checks the syntactic consistency of packets with regard to the RFCs of these protocols. The TOE also checks applicative commands used in packets. As a result, a TOE security administrator is able to allow only some commands for a given applicative protocol among HTTP, FTP, SMTP, DNS.

Rational: F.USER_DATA_PROTECTION_FW covers security requirements ensuring:

-	*filtering policy application:*	*FDP_IFC.2/FW-Enforcement_policy,* *FDP_IFF.1/FW-Enforcement_policy,*
-	*filtering policy administration:*	*FPT_TDC.1/FW-Administration_distante*
-	*identification of issuers and recipients of flows: FIA_UID.2/FW-Flux.*	

F.USER_DATA_PROTECTION_VPN

SOF-claim : high

Private network user protection function provides TOE security functions relative to the VPN component. This function guarantees the protection of private network users by ensuring the confidentiality, integrity and authenticity of flows emitted between a user of the private network and another user of another private network, and which pass through an external network (unsafe).

The TOE supports the following cryptographic algorithms: AES and RSA.

Rational: F.USER_DATA_PROTECTION_VPN covers security requirements ensuring:

-	VPN security policy application	FDP_IFC.1/VPN-Enforcement_policy FDP_IFF.1/VPN-Enforcement_policy FDP_ITC.1/VPN-Enforcement_policy FDP_ETC.1/VPN-Enforcement_policy FCS_COP.1/VPN-Enforcement_policy
-	VPN security policy protection:	FDP_ACF.1/VPN-VPN_policy FDP_ITC.1/VPN-VPN_policy
-	Cryptographic key management:	FDP_IFC.1/VPN-Key_policy FDP_IFF.1/VPN-Key_policy FTA_TSE.1/VPN-Key_policy FCS_CKM.1/VPN-Key_policy

F.ROLES

SOF-claim : No SOF claim

The role management function enables to manage the different roles inside the TOE: security officer, security administrator, system and network administrator and auditor. The four administrator roles provide different privileges and thus different administration functions. Authenticated security officers only are allowed to configure and assign roles.

Rational: F.ROLES manages roles (FMT_SMR.1) and controls access to:

- *filtering policy:*	*FDP_ACC.1/FW-Filtering_policy,*
- *VPN policy:*	*FDP_ACC.1/VPN-VPN_policy,*
- *Recycling:*	*(FDP_ACC.1/FW-Recyclage_TOE.*

F.ADMINISTRATION

SOF-claim : No SOF claim

The administration function enables TOE administrators to access locally or remotely (from an administration station) the TOE administration functions. The administration function enables:

Security officers: to manage (create, modify, delete) accounts of TOE administrators,

Security administrators: to manage (create, modify, delete) rules implemented in filtering policies of the TOE firewall, to manage (create, modify, delete) VPN security policies of the TOE VPN component, to manage (create, modify, delete) accounts for users of the TOE VPN service, to check audit logs and alarms of the TOE, to clear sensitive assets of the TOE in a safe manner,

Auditors: to check and manage audit events and security alarms relative to IP flows passing through the TOE firewall or VPN component and to administration operations,

System and network administrators: to configure the TOE network parameters and to monitor the status of the TOE.

Arkoon Manager and Arkoon Monitoring softwares are installed on administration stations and provide a graphical interface to administrators, enabling them to perform administration operations according to their rights.

Rational: F.ADMINISTRATION ensures:

- *Access control to:*	
- *filtering policy:*	*FDP_ACF.1/FW-Filtering_policy,*
- *network parameters:*	*FMT_MTD.1/FW-Network_param,*
- *administrators parameters:*	*FMT_MTD.1-Param_security_administrator,*
- *auditors parameters:*	*FMT_MTD.1-Param_auditor.*
- *Specification of Policy and TOE configuration:*	*FMT_SMF.1/FW-Configuration* *FMT_SMF.1/FW-Visualisation_politique_filtrage* *FMT_MTD.1/VPN-Network_param* *FMT_MSA.3/VPN-VPN_policy* *FMT_MSA.1/VPN-VPN_policy* *FMT_SMF.1/VPN-VPN_policy*
- *Monitoring*	*FMT_SMF.1/FW-Supervision* *FMT_SMF.1/VPN-Config_supervision*
- *Cryptographic key management*	*FDP_ITC.1/VPN-Key_policy* *FMT_MSA.3/VPN-Key_policy*

F.REINIT

SOF-claim : high

The reset function of the TOE enables security administrators to permanently delete TOE sensitive assets (filtering policies, VPN policies, private keys, authentication information, etc.). The safe way to delete sensitive data is to overwrite data 7 times with random patterns: each cluster on the hard disk referencing sensitive data to delete is completed by random values. The action must be repeated six times.

Rational: F.REINIT covers:

-	*Access control to recycling:*	*FDP_ACF.1/FW-Recyclage_TOE*
-	*Destruction of keys and sensitive data :*	*FDP_RIP.1/FW-Recyclage_TOE* *FDP_RIP.1/VPN* *FCS_CKM.4/VPN-Key_policy*

F.LOCAL_ADMIN_IDENTIFICATION_AUTHENTICATION

SOF-claim : high

The local authentication function enables TOE administrators to authenticate locally on the TOE. An administrator is imperatively authenticated before accessing administration functions.

Rational: F.LOCAL_ADMIN_IDENTIFICATION_AUTHENTICATION covers identification (FIA_UID.2-Administrateurs) and authentication (FIA_UAU.2-Administrateurs_local) of local administrators.

F.REMOTE_STATION_AUTHENTICATION

SOF-claim : high

A thick administration client and a certificate (and a private key) are installed on TOE administration stations for every administrator. Administrators authenticate to the TOE administration service using the private key/public key couple installed on the administration station. Both keys enable a mutual authentication between the administrator and the TOE on the one hand and on the other hand the protection (confidentiality, integrity and authenticity) of flows exchanged between the TOE and the administration station.

Rational: F.REMOTE_STATION_AUTHENTICATION covers FIA_UAU.2-Station_administration_distante.

F.REMOTE_ADMIN_PROTECTION

SOF-claim : high

The protection function of the TOE remote administration enables to protect the confidentiality, integrity and authenticity of the flows exchanged between the TOE and administrators when remotely administering the TOE from a remote administration station.

Rational: F.REMOTE_ADMIN_PROTECTION protects data transmitted between the TOE and the administration workstation (FPT_ITT.1-Administration_distante and FPT_ITT.3-Administration_distante).

6.2 Assurance measures

The developer has implemented the following security assurance measures.

CONFIGURATION MANAGEMENT

The developer uses a configuration management system which ensures the integrity of the TOE and its documentation during development steps.

Rational: CONFIGURATION MANAGEMENT covers assurance requirements ACM_CAP.3 and ACM_SCP.1.

DELIVERY AND OPERATION

Safe delivery and installation procedures are available.

Rational: DELIVERY AND OPERATION covers assurance requirements ADO_DEL.1 and ADO_IGS.1.

DESIGN DOCUMENTS

The developer has a technical documentation describing the design of the TOE with different technical levels (functional specifications, high-level design, low-level design).

Rational: DESIGN DOCUMENTS covers assurance requirements ADV_FSP.1, ADV_HLD.2 and ADV_RCR.1.

GUIDES

User and administration guides are available.

Rational: GUIDES covers assurance requirements AGD_ADM.1 and AGD_USR.1.

LIFE-CYCLE SUPPORT

The development of the TOE is performed in a secured environment.

A technical support is responsible for the corrective and evolutive maintenance of the product.

Rational: LIFE-CYCLE SUPPORT covers assurance requirements ALC_DVS.1 and ALC_FLR.3.

FUNCTIONAL TESTS

Intensive functional tests are performed for all the versions of the TOE.

Rational: FUNCTIONAL TESTS covers assurance requirements ATE_COV.2, ATE_DPT.1, ATE_FUN.1 and ATE_IND.2.

VULNERABILITIES ASSESSMENT

All vulnerabilities known by the developer for this type of product have been taken into account when developing the product.

Rational: VULNERABILITIES ASSESSMENT covers assurance requirements AVA_MSU.1, AVA_SOF.1 and AVA_VLA.2.

7. PROTECTION PROFILE CONFORMITY

This security target complies with the protection profile [PP_FWIP].

With regard to the protection profile [PP_CIP], the following elements have been modified:

In the VPN component protection profile [PP_CIP], the security administrator configures roles and accesses to administration tools and functions and also manages keys and authentication means to access administration tools. In the firewall protection profile [PP_FWIP], the security officer is responsible for these operations (this role does not exist in [PP_CIP]).

In this target, the ability to deal with role management for the VPN component, access to VPN component administration tools and functions and VPN component cryptographic keys is transferred to the security officer.

8. RATIONALES

8.1 Rationale for security objectives

Table 1: Threats, hypothesis and organisational security policies coverage

Security objectives	A.ADMIN	A.INITIALISATION_LOCAL	A.LOCAL	A.AUTHENTIFICATION_ADMIN_DISTANT	A.FW.AUDIT	A.FW.ALARMES	A.FW.MAITRISE_CONFIGURATION	A.VPN.AUDIT	A.VPN.ALARMES	A.VPN.MAITRISE_CONFIGURATION	A.VPN.CRYPTO_EXT	T.USURPATION_ADMIN	T.DYSFONCTIONNEMENT	T.FW.MODIFICATION_POL_FILTRAGE	T.FW.DIVULGATION_POL_FILTRAGE	T.FW.MODIFICATION_PARAM	T.FW.DIVULGATION_PARAM	T.FW.MODIFICATION_AUDIT_FLUX	T.FW.MODIFICATION_AUDIT_ADMIN	T.FW.MODIFICATION_ALARMES	T.FW.CHANGEMENT_CONTEXTE	T.VPN.MODIFICATION_POL_VPN	T.VPN.DIVULGATION_POL_VPN	T.VPN.USURPATION_ID	T.VPN.MODIFICATION_PARAM	T.VPN.DIVULGATION_PARAM	T.VPN.MODIFICATION_CLES	T.VPN.DIVULGATION_CLES	T.VPN.MODIFICATION_AUDIT_FLUX	T.VPN.MODIFICATION_AUDIT_ADMIN	T.VPN.MODIFICATION_ALARMES	T.VPN.CHANGEMENT_CONTEXTE	OSP.QUALIF	OSP.CRYPTO	OSP.GESTION_ROLES	OSP.FW.SERVICE	OSP.FW.VISUALISATION_POL	OSP.FW.AUDIT_FLUX	OSP.VPN.SERVICE	OSP.VPN.VISUALISATION_POL	OSP.VPN.SUPERVISION
	Hypothesis											**Threats**																					**OSP**								
OT.QUALIF																																	X								
OT.GESTION_ROLES																																			X						
OT.PROTECTION_FLUX_ADMIN												X		X	X	X	X	X	X	X		X	X		X	X	X	X	X	X	X										
OT.AUTHENTIFICATION_ADMIN												X		X	X	X	X	X	X	X		X	X		X	X	X	X	X	X	X				X						
OT.FW .APPLICATION_POL_FILTRAGE														X	X	X	X	X	X	X		X	X		X	X	X	X	X	X	X					X					
OT.FW .COHERENCE_POL																																				X					
OT.FW.PROTECTION_POL_FILTRAGE														X	X																										
OT.FW .VISUALISATION_POL																																					X				
OT.FW.PROTECTION_PARAM																X	X																								
OT.FW.CHANGEMENT_CONTEXTE																	X				X																				
OT.FW.SUPERVISION													X																												
OT.FW.IMPACT_SUPERVISION													X	X	X	X	X	X	X	X																					
OT.FW .AUDIT_FLUX														X	X	X	X																					X			
OT.FW.PROTECTION_AUDIT_FLUX																		X																							
OT.FW.AUDIT_ADMIN												X		X	X	X	X	X	X	X															X						
OT.FW.PROTECTION_AUDIT_ADMIN																			X																						
OT.FW.ALARMES												X		X	X	X	X	X	X																						
OT.FW.PROTECTION_ALARMES																				X																					
OT.VPN.APPLICATION_POL																																							X		
OT.VPN.CONFIDENTIALITE_APPLI																								X															X		
OT.VPN.AUTHENTICITE_APPLI																								X															X		
OT.VPN.CONFIDENTIALITE_TOPO																								X															X		
OT.VPN.AUTHENTICITE_TOPO																								X															X		

Security objectives	A.ADMIN	A.INITIALISATION_LOCAL	A.LOCAL	A.AUTHENTIFICATION_ADMIN_DISTANT	A.FW.AUDIT	A.FW.ALARMES	A.FW.MAITRISE_CONFIGURATION	A.VPN.AUDIT	A.VPN.ALARMES	A.VPN.MAITRISE_CONFIGURATION	A.VPN.CRYPTO_EXT	T.USURPATION_ADMIN	T.DYSFONCTIONNEMENT	T.FW.MODIFICATION_POL_FILTRAGE	T.FW.DIVULGATION_POL_FILTRAGE	T.FW.MODIFICATION_PARAM	T.FW.DIVULGATION_PARAM	T.FW.MODIFICATION_AUDIT_FLUX	T.FW.MODIFICATION_AUDIT_ADMIN	T.FW.MODIFICATION_ALARMES	T.FW.CHANGEMENT_CONTEXTE	T.VPN.MODIFICATION_POL_VPN	T.VPN.DIVULGATION_POL_VPN	T.VPN.USURPATION_ID	T.VPN.MODIFICATION_PARAM	T.VPN.DIVULGATION_PARAM	T.VPN.MODIFICATION_CLES	T.VPN.DIVULGATION_CLES	T.VPN.MODIFICATION_AUDIT_FLUX	T.VPN.MODIFICATION_AUDIT_ADMIN	T.VPN.MODIFICATION_ALARMES	T.VPN.CHANGEMENT_CONTEXTE	OSP.QUALIF	OSP.CRYPTO	OSP.GESTION_ROLES	OSP.FW.SERVICE	OSP.FW.VISUALISATION_POL	OSP.FW.AUDIT_FLUX	OSP.VPN.SERVICE	OSP.VPN.VISUALISATION_POL	OSP.VPN.SUPERVISION
OT.VPN. CLOISONNEMENT_FLUX																																							X		
OT.VPN.DEFINITION_POL																						X	X				X	X													
OT.VPN.PROTECTION_POL																						X	X																		
OT.VPN.VISUALISATION_POL																																								X	
OT.CRYPTO																								X				X						X							
OT.VPN.ACCES_CLES																											X	X													
OT.VPN. INJECTION_CLES																											X	X													
OT.VPN.PROTECTION_PARAM																									X	X															
OT.VPN.CHANGEMENT_CONTEXTE																																X									
OT.VPN.SUPERVISION													X																												X
OT.VPN.IMPACT_SUPERVISION													X									X	X		X	X	X	X	X	X	X										
OT.VPN.AUDIT_FLUX																						X			X	X													X		
OT.VPN.PROTECTION_AUDIT_FLUX																													X												
OT.VPN.AUDIT_ADMIN												X										X	X	X	X	X	X	X	X	X	X				X						
OT.VPN.PROTECTION_AUDIT_ADMIN																														X											
OT.VPN.ALARMES												X										X	X	X	X	X	X	X	X	X									X		
OT.VPN.PROTECTION_ALARMES																															X										
OE.ADMIN	X													X	X	X	X	X	X	X		X	X		X	X	X		X	X	X										
OE.PROTECTION_LOCAL			X											X	X	X	X	X	X	X		X	X		X	X	X		X	X	X	X									
OE.AUTHENT_ADMIN_DISTANT				X								X		X	X	X	X	X	X	X		X	X		X	X	X		X	X	X				X						
OE.CRYPTO																																		X							
OE.FW.ANALYSE_AUDIT					x													X	X																						
OE.FW.TRAITE_ALARMES						X								X	X	X	X	X	X	X																					
OE.FW.INTEGRITE							X						X	X		X	X																			X			X		
OE.VPN.ANALYSE_AUDIT								X																					X	X											
OE.VPN.TRAITE_ALARMES									X													X	X	X	X	X			X	X	X										
OE.VPN.INTEGRITE										X			X									X			X																
OE.VPN.CRYPTO_EXT											x													x			x	x						x							
OE.INITIALISATION_LOCAL		x																																							

8.1.1 Hypothesis

A.ADMIN

This hypothesis results in the OE.ADMIN security objective which requires administrators to be non hostile and trained to carry out their tasks.

A.LOCAL

This hypothesis results in the OE.PROTECTION_LOCAL security objective which requires the TOE equipments and the supports containing the sensitive assets of the TOE to be in a secure room.

A.INITIALISATION_LOCAL

This hypothesis results in the OE.INITIALISATION_LOCAL security objective which requires the TOE equipments to be initialized in the secure room of the appliance which is accessible only by administrators. The initialization shall be performed from an administration station directly connected to equipments.

A.AUTHENTIFICATION_ADMIN_DISTANT

This hypothesis results in the OE.AUTHENTIFICATION_ADMIN_DISTANT security objective which requires the TOE environment to enable the authentication of administrators for the TOE remote accesses.

Firewall

A.FW.AUDIT

This hypothesis results in the OE.FW.ANALYSE_AUDIT security objective which requires the auditor to check regularly audit logs generated by the firewall and to manage logs in order to avoid data loss.

A.FW.ALARMES

This hypothesis results in the OE.FW.TRAITE_ALARMES security objective which requires the security administrator to handle the alarms generated and forwarded by the firewall.

A.FW.MAITRISE_CONFIGURATION

This hypothesis results in the OE.FW.INTEGRITE security objective which enables the administrator to control or regenerate the hardware and software configuration (services and assets) of the firewall according to a reference state.

VPN component

A.VPN.AUDIT

This hypothesis results in the OE.VPN.ANALYSE_AUDIT security objective which requires the auditor to check regularly audit logs generated by the VPN component and to manage logs in order to avoid data loss.

A.VPN.ALARMES

This hypothesis results in the OE. VPN.TRAITE_ALARMES security objective which requires the security administrator to handle the alarms generated and sent by the VPN component.

A.VPN.MAITRISE_CONFIGURATION

This hypothesis results in the OE.VPN.INTEGRITE security objective which enables the administrator to control or regenerate the hardware and software configuration (services and assets) of the VPN component according to a reference state.

A.VPN.CRYPTO_EXT

This hypothesis results in the OE.VPN.CRYPTO_EXT security objective which requires cryptographic keys, generated outside and injected into the TOE, to be generated according to the recommandations specified in the [CRYPTO] and [GC] ANSSI reference documents for the standard resistance level.

8.1.2 Threats

8.1.2.1 Coverage of threats to the security policies (TSP) of the TOE

Firewall

T.FW.MODIFICATION_POL_FILTRAGE

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- enable filtering flows (OT.FW.APPLICATION_POL_FILTRAGE).
- provide access control to the firewall filtering policy (OT.FW.PROTECTION_POL_FILTRAGE).
- provide a monitoring service of the firewall which does not affect sensitive assets because it does not modify or disclose them (OT.FW.IMPACT_SUPERVISION).
- protect remote administration flows (OT.PROTECTION_FLUX_ADMIN) and authenticate locally the TOE administrator (OT.AUTHENTIFICATION_ADMIN). The TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).

To detect the threat ; the TOE shall:

- generate firewall audit logs and alarms (OT.FW.AUDIT_ADMIN, OT.FW.AUDIT_FLUX and OT.FW.ALARMES). The security administrator shall analyze and handle them (OE.FW.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- be able to get back to a previous validated status (OE.FW.INTEGRITE).

T.FW.DIVULGATION_POL_FILTRAGE

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- enable filtering firewall administration flows (OT.FW.APPLICATION_POL_FILTRAGE).
- provide access control to the firewall filtering policy (OT.FW.PROTECTION_POL_FILTRAGE).
- provide a monitoring service of the firewall which do not affect sensitive assets because it does not modify or disclose them (OT.FW.IMPACT_SUPERVISION).
- protect remote administration flows (OT.PROTECTION_FLUX_ADMIN) and authenticate locally the TOE administrator (OT.AUTHENTIFICATION_ADMIN). The TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).

To detect the threat; the TOE shall:

- generate firewall audit logs and alarms (OT.FW.AUDIT_ADMIN, OT.FW.AUDIT_FLUX and OT.FW.ALARMES). The security administrator shall analyze and handle them (OE.FW.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- no action

VPN component

T.VPN.MODIFICATION_POL_VPN

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL)
- be used by trusted administrators (OE.ADMIN)

To be protected, the TOE shall:

- provide access control to the VPN component flow protection policy (OT.VPN.PROTECTION_POL and OT.VPN.DEFINITION_POL).
- provide a monitoring service of the VPN component which do not affect sensitive assets because it does not modify or disclose them (OT.VPN.IMPACT_SUPERVISION).
- protect remote administration flows (OT.PROTECTION_FLUX_ADMIN) and authenticate locally the TOE administrator (OT.AUTHENTIFICATION_ADMIN). The TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- enable filtering the VPN component administration flows (OT.FW.APPLICATION_POL_FILTRAGE).

To detect the threat; the TOE shall:

- generate VPN component audit logs and alarms (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES) The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- be able to get back to a previous validated status (OE.VPN.INTEGRITE)

T.VPN.DIVULGATION_POL_VPN

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL)
- be used by trusted administrators (OE.ADMIN)

To be protected, the TOE shall:

- provide access control to the VPN component flow protection policy (OT.VPN.PROTECTION_POL and OT.VPN.DEFINITION_POL).
- provide a monitoring service of the VPN component which do not affect sensitive assets because it does not modify or disclose them (OT.VPN.IMPACT_SUPERVISION).
- protect remote administration flows (OT.PROTECTION_FLUX_ADMIN) de la TOE and authenticate locally the TOE administrator (OT.AUTHENTIFICATION_ADMIN). The TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- enable filtering the VPN component administration flows (OT.FW.APPLICATION_POL_FILTRAGE).

To detect the threat; the TOE shall:

- generate VPN component audit logs and alarms (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES) The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- no action

T.VPN.USURPATION_ID

To prevent the threat, the TOE shall:

- no action

To be protected, the TOE shall:

- provide security services protecting the authenticity and confidentiality of applicative and topologic data of the private network (OT.VPN.AUTHENTICITE_APPLI, OT.VPN.CONFIDENTIALITE_APPLI, OT.VPN.AUTHENTICITE_TOPO, OT.VPN.CONFIDENTIALITE_TOPO).
- generate reliable cryptographic keys for security services mentioned above and use the IKE protocol to set up a VPN link (OT.CRYPTO).
- use reliable cryptographic keys, generated outside the TOE, for security services mentioned above (OE.VPN.CRYPTO_EXT).

To detect the threat; the TOE shall:

- generate VPN component audit logs and alarms (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- no action

8.1.2.2 Coverage of threats to the configuration of the TOE

Firewall

T.FW.MODIFICATION_PARAM

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- enable filtering the firewall administration flows (OT.FW.APPLICATION_POL_FILTRAGE).
- provide access control to the firewall sensitive assets (OT.FW.PROTECTION_PARAM).
- provide a monitoring service of the firewall which do not affect sensitive assets because it does not modify or disclose them (OT.FW.IMPACT_SUPERVISION).
- protect remote administration flows (OT.PROTECTION_FLUX_ADMIN) and authenticate locally the TOE administrator (OT.AUTHENTIFICATION_ADMIN). The TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).

To detect the threat, the TOE shall:

- generate firewall audit logs and alarms (OT.FW.AUDIT_ADMIN, OT.FW.AUDIT_FLUX and OT.FW.ALARMES). The security administrator shall analyze and handle them (OE.FW.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- be able to get back to a previous validated status (OE.FW.INTEGRITE).

T.FW.DIVULGATION_PARAM

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).
- be recycled when the context changes (OT.FW.CHANGEMENT_CONTEXTE)

To be protected, the TOE shall:

- enable filtering the firewall administration flows (OT.FW.APPLICATION_POL_FILTRAGE).
- provide access control to the firewall sensitive assets (OT.FW.PROTECTION_PARAM).
- provide a monitoring service of the firewall which do not affect sensitive assets because it does not modify or disclose them (OT.FW.IMPACT_SUPERVISION).

- protect remote administration flows (OT.PROTECTION_FLUX_ADMIN) and authenticate locally the TOE administrator (OT.AUTHENTIFICATION_ADMIN). The TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).

To detect the threat, the TOE shall:

- generate firewall audit logs and alarms (OT.FW.AUDIT_ADMIN, OT.FW.AUDIT_FLUX and OT.FW.ALARMES). The security administrator shall analyze and handle them (OE.FW.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- no action

VPN component

T.VPN.MODIFICATION_PARAM

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- provide access control to the VPN component sensitive assets (OT.VPN.PROTECTION_PARAM).
- provide a monitoring service of the VPN component which do not affect sensitive assets because it does not modify or disclose them (OT.VPN.IMPACT_SUPERVISION).
- protect remote administration flows (OT.PROTECTION_FLUX_ADMIN) and authenticate locally the TOE administrator (OT.AUTHENTIFICATION_ADMIN). The TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- enable filtering the VPN component administration flows (OT.FW.APPLICATION_POL_FILTRAGE).

To detect the threat, the TOE shall:
- generate VPN component audit logs and alarms (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- be able to get back to a previous validated status (OE.VPN.INTEGRITE).

T.VPN.DIVULGATION_PARAM

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).
- be recycled when the context changes (OT.VPN.CHANGEMENT_CONTEXTE)

To be protected, the TOE shall:

- provide access control to the VPN component sensitive assets (OT.VPN.PROTECTION_PARAM).
- provide a monitoring service of the VPN component which do not affect sensitive assets because it does not modify or disclose them (OT.VPN.IMPACT_SUPERVISION).
- protect remote administration flows (OT.PROTECTION_FLUX_ADMIN) and authenticate locally the TOE administrator (OT.AUTHENTIFICATION_ADMIN). The TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- enable filtering the VPN component administration flows(OT.FW.APPLICATION_POL_FILTRAGE).

To detect the threat, the TOE shall:

- generate VPN component audit logs and alarms (OT.VPN.AUDIT_ADMIN, OT.VPN.AUDIT_FLUX and OT.VPN.ALARMES). The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- no action

8.1.2.3 Coverage of threats to cryptographic keys

VPN component

T.VPN.MODIFICATION_CLES

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- guarantee the integrity and confidentiality of cryptographic keys when they are injected in the TOE (OT.VPN.INJECTION_CLES)
- guarantee that only authenticated local administrators can access cryptographic keys (OT.AUTHENTIFICATION_ADMIN). The TOE shall protect remote administration flows (OT.PROTECTION_FLUX_ADMIN), and the TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT)
- protect the access to cryptographic keys (OT.VPN.ACCES_CLES).
- provide a monitoring service of the VPN component which do not affect the integrity of cryptographic keys because it does not modify or disclose them (OT.VPN.IMPACT_SUPERVISION).
- enable filtering the VPN component administration flows (OT.FW.APPLICATION_POL_FILTRAGE).
- use reliable cryptographic keys, generated outside the TOE (OE.VPN.CRYPTO_EXT).

To detect the threat, the TOE shall:

- generate VPN component audit logs and alarms (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- be able to allow the security administrator to modify the VPN security policy for a VPN link (OT.VPN.DEFINITION_POL), by injecting new static keys for the VPN link (OT.VPN.INJECTION_CLES) for example.

T.VPN.DIVULGATION_CLES

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).
- use cryptographic keys regularly renewed (OT.CRYPTO)

To be protected, the TOE shall:

- guarantee the integrity and confidentiality of cryptographic keys when they are injected in the TOE (OT.VPN.INJECTION_CLES)
- guarantee that only authenticated local administrators can access cryptographic keys (OT.AUTHENTIFICATION_ADMIN). The TOE shall protect remote administration flows (OT.PROTECTION_FLUX_ADMIN), and the TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT)
- protect the access to cryptographic keys (OT.VPN.ACCES_CLES).
- provide a monitoring service of the VPN component which do not affect the integrity of cryptographic keys because it does not modify or disclose them (OT.VPN.IMPACT_SUPERVISION).
- enable filtering the VPN component administration flows (OT.FW.APPLICATION_POL_FILTRAGE).
- use reliable cryptographic keys, generated outside the TOE (OE.VPN.CRYPTO_EXT).

To detect the threat, the TOE shall:

- generate VPN component audit logs and alarms (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).

To limit the impact of the threat, the TOE shall:

- be able to allow the security administrator to modify the VPN security policy for a VPN link (OT.VPN.DEFINITION_POL), by injecting new static keys for the VPN link (OT.VPN.INJECTION_CLES) for example.

8.1.2.4 Coverage of threats to flow audit logs

Firewall

T.FW.MODIFICATION_AUDIT_FLUX

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- enable filtering firewall administration flows (OT.FW.APPLICATION_POL_FILTRAGE).
- provide access control to audit logs of flows processed by the firewall (OT.FW.PROTECTION_AUDIT_FLUX).
- provide a monitoring service of the firewall which do not affect sensitive assets because it does not modify or disclose them (OT.FW.IMPACT_SUPERVISION).
- guarantee that only authenticated local administrators can access audit logs of the firewall flows (OT.AUTHENTIFICATION_ADMIN). The TOE shall protect remote administration flows (OT.PROTECTION_FLUX_ADMIN), and the TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).

To detect the threat, the TOE shall:

- enable to detect the loss of the firewall audit logs (OT.FW.PROTECTION_AUDIT_FLUX).

To limit the impact of the threat, the TOE shall:

- generate VPN component audit logs and alarms (OT.FW.AUDIT_ADMIN, OT.FW.ALARMES). The security administrator shall analyze and handle them (OE.FW.TRAITE_ALARMES).
- rely on measures of audit log backup and storage (OE.FW.ANALYSE_AUDIT).

VPN component

T.VPN.MODIFICATION_AUDIT_FLUX

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- provide an access control to audit logs of flows processed by the VPN component (OT.VPN.PROTECTION_AUDIT_FLUX).
- provide a monitoring service of the VPN component which do not affect sensitive assets because it does not modify or disclose them (OT.VPN.IMPACT_SUPERVISION).
- guarantee that only authenticated local administrators can access audit logs of the VPN component flows (OT.AUTHENTIFICATION_ADMIN). The TOE shall protect remote administration flows (OT.PROTECTION_FLUX_ADMIN), and the TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).

- enable filtering the VPN component administration flows (OT.FW.APPLICATION_POL_FILTRAGE).

To detect the threat, the TOE shall:

- enable to detect the loss of the VPN component audit logs (OT.VPN.PROTECTION_AUDIT_FLUX).

To limit the impact of the threat, the TOE shall:

- generate VPN component audit logs and alarms (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).
- rely on measures of audit log backup and storage (OE.VPN.ANALYSE_AUDIT).

8.1.2.5 Coverage of threats to administration audit logs

Firewall

T.FW.MODIFICATION_AUDIT_ADMIN

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- enable filtering the firewall administration flows (OT.FW.APPLICATION_POL_FILTRAGE).
- provide an access control to audit logs of flows processed by the firewall (OT.FW.PROTECTION_AUDIT_ADMIN).
- provide a monitoring service of the firewall which do not affect sensitive assets because it does not modify or disclose them (OT.FW.IMPACT_SUPERVISION).
- guarantee that only authenticated local administrators can access cryptographic keys (OT.AUTHENTIFICATION_ADMIN). The TOE shall protect remote administration flows (OT.PROTECTION_FLUX_ADMIN), and the TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).

To detect the threat, the TOE shall:

- enable to detect the loss of the firewall audit logs (OT.FW.PROTECTION_AUDIT_ADMIN).

To limit the impact of the threat, the TOE shall:

- generate firewall audit logs and alarms (OT.FW.AUDIT_ADMIN, OT.FW.ALARMES). The security administrator shall analyze and handle them (OE.FW.TRAITE_ALARMES).
- rely on measures of audit log backup and storage (OE.FW.ANALYSE_AUDIT).

VPN component

T.VPN.MODIFICATION_AUDIT_ADMIN

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- provide an access control to audit logs of flows processed by the VPN component (OT.VPN.PROTECTION_AUDIT_ADMIN).
- provide a monitoring service of the VPN component which do not affect the sensitive assets because it does not modify or disclose them (OT.FW.IMPACT_SUPERVISION).
- guarantee that only authenticated local administrators can access cryptographic keys (OT.AUTHENTIFICATION_ADMIN). TOE shall protect remote administration flows (OT.PROTECTION_FLUX_ADMIN), and the TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- enable filtering the VPN component administration flows (OT.FW.APPLICATION_POL_FILTRAGE).

To detect the threat, the TOE shall:

- enable to detect the loss of the VPN component audit logs (OT.VPN.PROTECTION_AUDIT_ADMIN).

To limit the impact of the threat, the TOE shall:

- generate VPN component audit logs and alarms (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).
- rely on measures of audit log backup and storage (OE.VPN.ANALYSE_AUDIT).

8.1.2.6 Coverage of threats to alarms

Firewall

T.FW.MODIFICATION_ALARMES

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- enable filtering the firewall administration flows (OT.FW.APPLICATION_POL_FILTRAGE).
- provide a monitoring service of the firewall which do not affect sensitive assets because it does not modify or disclose them (OT.FW.IMPACT_SUPERVISION).

- guarantee that only authenticated local administrators can access cryptographic keys (OT.AUTHENTIFICATION_ADMIN). The TOE shall protect remote administration flows (OT.PROTECTION_FLUX_ADMIN), and the TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).

To detect the threat, the TOE shall:

- enable to detect the loss of the firewall alarms (OT.FW.PROTECTION_ALARMES).

To limit the impact of the threat, the TOE shall:

- generate firewall audit logs (OT.FW.AUDIT_ADMIN).The security administrator shall analyze and handle them (OE.FW.TRAITE_ALARMES).

VPN component

T.VPN.MODIFICATION_ALARMES

To prevent the threat, the TOE shall:

- be deployed in a secure room (OE.PROTECTION_LOCAL).
- be used by trusted administrators (OE.ADMIN).

To be protected, the TOE shall:

- provide an access control to audit logs of flows processed by the VPN component (OT.VPN.PROTECTION_ALARMES).
- provide a monitoring service of the VPN component which do not affect the sensitive assets because it does not modify or disclose them (OT.FW.IMPACT_SUPERVISION).
- guarantee that only authenticated local administrators can access cryptographic keys (OT.AUTHENTIFICATION_ADMIN). The TOE shall protect remote administration flows (OT.PROTECTION_FLUX_ADMIN), and the TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- enable filtering the VPN component administration flows (OT.FW.APPLICATION_POL_FILTRAGE).

To detect the threat, the TOE shall:

- enable to detect the loss of the VPN component audit logs (OT.VPN.PROTECTION_ALARMES).

To limit the impact of the threat, the TOE shall:

- generate VPN component audit logs (OT.VPN.AUDIT_ADMIN).. The security administrator shall analyze and handle them (OE.VPN.TRAITE_ALARMES).

8.1.2.7 Coverage of threats to the administration

T.USURPATION_ADMIN

To prevent the threat, the TOE shall:

- no action

To be protected, the TOE shall:

- require the local or remote authentication (OT.AUTHENTIFICATION_ADMIN or OE.AUTHENTIFICATION_ADMIN_DISTANT) of administrators before doing any administration operation.
- protect remote administration flows (OT.PROTECTION_FLUX_ADMIN).

To detect the threat:

- OT.FW.AUDIT_ADMIN and OT.FW.ALARMES guarantee that operations (viewing, modification) performed on the firewall sensitive assets are tracked and that security alarms are generated to indicate failures of the TOE. They enable to detect and handle errors or attacks after analyzing audit events and security alarms.
- OT.VPN.AUDIT_ADMIN and OT.VPN.ALARMES guarantee that operations (viewing, modification) performed on the VPN component sensitive assets are tracked and that security alarms are generated to indicate failures of the TOE. They enable to detect and handle errors or attacks after analyzing audit events and security alarms.

To limit the impact of the threat, the TOE shall:

- no action

8.1.2.8 Coverage of threats to the change of the context of use of the TOE

Firewall

T.FW.CHANGEMENT_CONTEXTE

To prevent the threat, the TOE shall:

- provide a functionality which makes the firewall sensitive assets unavailable before a change of the context of use: new assignement, maintenance, etc. (OT.FW.CHANGEMENT_CONTEXTE).

To be protected, the TOE shall:

- no action

To detect the threat, the TOE shall:

- no action

To limit the impact of the threat, the TOE shall:

- no action

VPN component

T.VPN.CHANGEMENT_CONTEXTE

To prevent the threat, the TOE shall:

- provide a functionality which makes the VPN component sensitive assets unavailable before a change of the context of use: new assignement, maintenance, etc. (OT.VPN.CHANGEMENT_CONTEXTE).

To be protected, the TOE shall:

- no action

To detect the threat, the TOE shall:

- no action

To limit the impact of the threat, the TOE shall:

- no action

T.DYSFONCTIONNEMENT

To prevent the threat, the TOE shall:

- no action

To be protected, the TOE shall:

- no action

To detect the threat, the TOE shall:

- provide a monitoring service of the TOE (OT.FW.SUPERVISION and OT.VPN.SUPERVISION) but without disclosing its sensitive assets (OT.FW.IMPACT_SUPERVISION and OT.VPN.IMPACT_SUPERVISION).

To limit the impact of the threat, the TOE shall:

- be able to get back to a previous validated status (OE.FW.INTEGRITE and OE.VPN.INTEGRITE).

8.1.3 Organisational security policies

OSP.QUALIF

To implement the policy, the TOE:

- relies on the ANSSI standard qualification process (OT.QUALIF).

To guarantee the enforcement of the policy, the TOE:

- no action

To control the enforcement of the policy, the TOE:

- no action

OSP.CRYPTO

To implement the policy, the TOE:

- implements cryptographic functions and manages (generate, destroy, renew) cryptographic keys according to ANSSI [CRYPTO] and [GC] cryptographic reference documents for the standard resistance level (OT.CRYPTO).
- uses cryptographic keys (generated outside), generated and managed according to the recommendations of ANSSI [CRYPTO] and [GC] cryptographic reference documents for the standard resistance level (OE.VPN.CRYPTO_EXT).
- relies on ANSSI cryptographic reference documents (OE.CRYPTO)

To guarantee the enforcement of the policy, the TOE:

- no action

To control the enforcement of the policy, the TOE:

- no action

OSP.GESTION_ROLES

To implement the policy, the TOE:

- defines roles for the TOE administrators. Each role has specific access rights (OT.GESTION_ROLES).
- authenticates locally the TOE administrator (OT.AUTHENTIFICATION_ADMIN). The TOE environment shall enable to authenticate the TOE administrator in order to access remote administration equipments (OE.AUTHENTIFICATION_ADMIN_DISTANT).

To guarantee the enforcement of the policy, the TOE:

- no action

To control the enforcement of the policy, the TOE:

- records operations performed by the administrators on the TOE (OT.VPN.AUDIT_ADMIN and OT.FW.AUDIT_ADMIN)

Firewall

OSP.FW.SERVICE

To implement the policy, the TOE:

- applies the firewall filtering policy defined by the security administrator (OT.FW.APPLICATION_POL_FILTRAGE).

To guarantee the enforcement of the policy, the TOE:

- guarantees the consistency between the definition of filtering policies and policies applied to the firewall (OT.FW .COHERENCE_POL).
- guarantees the integrity of the code of softwares applying filtering policies can be verified (OE.FW.INTEGRITE).

To control the enforcement of the policy, the TOE:

- enables the TOE security administrator to see the firewall filtering policy (OT.FW .VISUALISATION_POL).

OSP.FW.VISUALISATION_POL

To implement the policy, the TOE:

- enables to see the current filtering rules on the firewall (OT.FW.VISUALISATION_POL).

To guarantee the enforcement of the policy, the TOE:

- no action

To control the enforcement of the policy, the TOE:

- no action

OSP.FW.AUDIT_FLUX

To implement the policy, the TOE:

- tracks flows processed by the firewall in audit logs enabling administrators to see them, to organize them, etc. (OT.FW.AUDIT_FLUX).

To guarantee the enforcement of the policy, the TOE:

- no action

To control the enforcement of the policy, the TOE:

- no action

VPN component

OSP.VPN.SERVICE

To implement the policy, the TOE:

- applies a flow protection policy (OT.VPN.APPLICATION_POL) protecting the confidentiality and authenticity of applicative data (OT.VPN.CONFIDENTIALITE_APPLI, OT.VPN.AUTHENTICITE_APPLI) and topologic data (OT.VPN.CONFIDENTIALITE_TOPO, OT.VPN.AUTHENTICITE_TOPO).
- guarantees the partitioning of flows (OT.VPN.CLOISONNEMENT_FLUX).

To guarantee the enforcement of the policy, the TOE:

- guarantees the integrity of the code of softwares applying VPN security policies can be verified (OE.VPN.INTEGRITE).

To control the enforcement of the policy, the TOE:

- guarantees operations on VPN links are tracked and security alarms are generated to indicate any failure (OT.VPN.AUDIT_FLUX, OT.VPN.ALARMES). The environment of the TOE guarantees alarms are handled by security administrators (OE.VPN.TRAITE_ALARMES).

OSP.VPN.VISUALISATION_POL

To implement the policy, the TOE:

- enables to see each VPN security policy, enabling an administrator to verify he correctly defined each VPN security policy (OT.VPN.VISUALISATION_POL).

To guarantee the enforcement of the policy, the TOE:

- no action

To control the enforcement of the policy, the TOE:

- no action

OSP.VPN.SUPERVISION

To implement the policy, the TOE:

- enables the system and network administrator to check the VPN component operational status (OT.VPN.SUPERVISION).

To guarantee the enforcement of the policy, the TOE:

- no action

To control the enforcement of the policy, the TOE:

- no action

8.2 Rationale for security requirements

8.2.1 Security objectives for the TOE firewall

Table 2: Coverage of objectives for the TOE firewall

Security objectives for the TOE firewall	FPT_STM.1	FPT_ITT.1-Administration_distante	FPT_ITT.3-Administration_distante	FIA_UAU.2-Station_administration_distante	FMT_SMR.1	FIA_UID.2-Administrateurs	FIA_UAU.2-Administrateurs_local	FDP_IFC.2/FW-Enforcement_policy	FDP_IFF.1/FW-Enforcement_policy	Visualisation_politique_filtrage	FPT_TDC.1/FW-Administration_distante	FDP_ACC.1/FW-Filtering_policy	FDP_ACF.1/FW-Filtering_policy	FAU_GEN.1/FW-Audit_flux	FAU_GEN.2/FW-Audit_flux	FIA_UID.2/FW-Flux	FAU_SAR.1/FW-Audit_flux	FAU_SAR.3/FW-Audit_flux	FAU_STG.1/FW-Traces_audit_flux	FAU_GEN.1/FW-Audit_admin	FAU_GEN.2/FW-Audit_admin	FAU_SAR.1/FW-Audit_admin	FAU_SAR.3/FW-Audit_admin	FAU_STG.1/FW-Traces_audit_admin	FAU_SAA.1/FW-Alarmes	FAU_ARP.1/FW-Alarmes	FMT_SMF.1/FW-Configuration	FMT_MTD.1/FW-Network_param	FMT_MTD.1-Param_security_administrator	FMT_MTD.1-Param_auditor	FMT_SMF.1/FW-Supervision	FPT_ITC.1/FW-Supervision	FDP_RIP.1/FW-Recyclage_TOE	FDP_ACC.1/FW-Recyclage_TOE	FDP_ACF.1/FW-Recyclage_TOE
OT.FW .APPLICATION_POL_FILTRAGE								X	X																										
OT.FW .COHERENCE_POL											X																								
OT.FW.PROTECTION_POL_FILTRAGE												X	X																						
OT.FW .VISUALISATION_POL										X																									
OT.FW.PROTECTION_PARAM																											X	X	X	X					
OT.FW.CHANGEMENT_CONTEXTE																																	X	X	X
OT.FW.SUPERVISION																															X				
OT.FW.IMPACT_SUPERVISION																																X			
OT.FW .AUDIT_FLUX	X													X	X	X	X	X																	
OT.FW.PROTECTION_AUDIT_FLUX																			X																
OT.FW.AUDIT_ADMIN	X					X														X	X	X	X												
OT.FW.PROTECTION_AUDIT_ADMIN																								X											
OT.FW.ALARMES																									X	X									
OT.FW.PROTECTION_ALARMES																			X					X											

8.2.2 Security objectives for the TOE VPN component

Table 3: Coverage of the security objectives for the TOE VPN component

Security objectives for the TOE VPN component	FPT_STM.1	FPT_ITT.1-Administration_distante	FPT_ITT.3-Administration_distante	FIA_UAU.2-Station_administration_distante	FMT_SMR.1	FIA_UID.2-Administrateurs	FIA_UAU.2-Administrateurs_local	FDP_IFC.1/VPN-Enforcement_policy	FDP_IFF.1/VPN-Enforcement_policy	FDP_ITC.1/VPN-Enforcement_policy	FDP_ETC.1/VPN-Enforcement_policy	FCS_COP.1/VPN-Enforcement_policy	FDP_ACC.1/VPN-VPN_policy	FDP_ACF.1/VPN-VPN_policy	FDP_ITC.1/VPN-VPN_policy	FMT_MSA.3/VPN-VPN_policy	FMT_MSA.1/VPN-VPN_policy	FMT_SMF.1/VPN-VPN_policy	FAU_GEN.1/VPN-Audit_flux	FAU_SAR.1/VPN-Audit_flux	FAU_SAR.3/VPN-Audit_flux	FAU_STG.1/VPN-Traces_audit_flux	FAU_GEN.1/VPN-Audit_admin	FAU_SAR.1/VPN-Audit_admin	FAU_SAR.3/VPN-Audit_admin	FAU_STG.1/VPN-Traces_audit_admin	FAU_SAA.1/VPN-Alarmes	FAU_ARP.1/VPN-Alarmes	FMT_MTD.1/VPN-Network_param	FMT_MTD.1/Param _security_administrator	FMT_SMF.1/VPN-Config_supervision	FDP_RIP.1/VPN	FDP_ITC.1/VPN-Key_policy	FDP_IFC.1/VPN-Key_policy	FDP_IFF.1/VPN-Key_policy	FMT_MSA.3/VPN-Key_policy	FTA_TSE.1/VPN-Key_policy	FCS_CKM.4/VPN-Key_policy	FCS_CKM.1/ VPN-Key_policy
OT.VPN.APPLICATION_POL								X	X	X	X	X																											
OT.VPN.CONFIDENTIALITE_APPLI												X																											
OT.VPN.AUTHENTICITE_APPLI												X																											
OT.VPN.CONFIDENTIALITE_TOPO												X																											
OT.VPN.AUTHENTICITE_TOPO												X																											
OT.VPN. CLOISONNEMENT_FLUX								X	X		X																												
OT.VPN.DEFINITION_POL													X	X	X	X	X	X																					
OT.VPN.PROTECTION_POL													X	X		X	X	X																					
OT.VPN.VISUALISATION_POL													X	X																									
OT.CRYPTO												X																									X		x
OT.VPN.ACCES_CLES																																		X	X	X			
OT.VPN. INJECTION_CLES																																	X	X	X	X			
OT.VPN.PROTECTION_PARAM																													X	X	X								
OT.VPN.CHANGEMENT_CONTEXTE																																X						X	
OT.VPN.SUPERVISION																															X								
OT.VPN.IMPACT_SUPERVISION								X	X				X	X															X	X				X	X				
OT.VPN.AUDIT_FLUX	X																		X	X	X																		
OT.VPN.PROTECTION_AUDIT_FLUX																			X			X	X																
OT.VPN.AUDIT_ADMIN	X																						X	X	X														
OT.VPN.PROTECTION_AUDIT_ADMIN																			X				X			X													
OT.VPN.ALARMES																											X	X											
OT.VPN.PROTECTION_ALARMES																			X			X	X			X													

8.2.3 Security objectives for the TOE administration

Table 4: Coverage of the security objectives for the TOE administration

Security objectives for the TOE administration	FPT_STM.1	FPT_ITT.1-Administration_distante	FPT_ITT.3-Administration_distante	FIA_UAU.2-Station_administration_distante	FMT_SMR.1	FIA_UID.2-Administrateurs	FIA_UAU.2-Administrateurs_local
OT.GESTION_ROLES				X	X	X	X
OT.PROTECTION_FLUX_ADMIN		X	X				
OT.AUTHENTIFICATION_ADMIN					X	X	X

8.2.4 Security objectives for the TOE technical environment

Table 5: Coverage of the security objectives for the TOE technical environment

Security objectives for the TOE technical environment	FIA_UAU.2-Administration_distante
OE.AUTHENTIFICATION_ADMIN_DISTANT	X

8.2.5 Rationale for the coverage of the functional security requirements for the TOE

8.2.5.1 TOE administration

OT.GESTION_ROLES

The objective results in the requirement FMT_SMR.1 which requires that the TOE manages the different roles (administrators). To manage these roles, administrators have to be identified (FIA_UID.2-Administrateurs). The local authentication of administrators is covered by FIA_UAU.2-Administrateurs_local; the authentication for the remote administration is covered by FIA_UAU.2-Station_administration_distante.

OT.PROTECTION_FLUX_ADMIN

This objective results in the requirements FPT_ITT.1-Administration_distante and FPT_ITT.3-Administration_distante about the protection of data transmitted between the firewall and the remote administration station.

OT.AUTHENTIFICATION_ADMIN

This objective is covered by FIA_UID.2-Administrateurs and FIA_UAU.2-Administrateurs_local which require the identification and authentication of users before doing any local administration operation. Furthermore, this objective is covered by FMT_SMR.1 which requires the TOE to maintain the different roles.

8.2.5.2 TOE firewall

OT.FW.APPLICATION_POL_FILTRAGE

This objective results in the requirement FDP_IFF.1/FW-Enforcement_policy which enables to define the minimal rules which shall be respected by the filtering policy and the requirement FDP_IFC.2/FW-Enforcement_policy which requires the TOE to apply this filtering policy.

OT.FW.COHERENCE_POL

This objective results in FPT_TDC.1/FW-Administration_distante to guarantee the consistency between the filtering policy defined on the remote administration station and the firewall.

OT.FW.PROTECTION_POL_FILTRAGE

This objective results in the access rules to the filtering policy (FDP_ACC.1/FW-Filtering_policy and FDP_ACF.1/FW-Filtering_policy).

OT.FW.VISUALISATION_POL

This objective results in the requirement FMT_SMF.1/FW-Visualisation_politique_filtrage which requires the possibility to display the filtering rules and the connection contexts.

OT.FW.PROTECTION_PARAM

This objective results in the following protection requirements:

- for network configuration parameters: FMT_MTD.1/FW-Network_param;
- for access rights and authentication data: FMT_MTD.1-Param_security_administrator for security administrators and FMT_MTD.1-Param_auditor for auditors;

The configuration functionality of these parameters is covered by FMT_SMF.1/FW-Configuration.

OT.FW.CHANGEMENT_CONTEXTE

This objective results in the following requirements:

- FDP_RIP.1/FW-Recyclage_TOE which requires the TOE to provide the capability to make unavailable contents of resources corresponding to TOE sensitive assets;
- FDP_ACC.1/FW-Recyclage_TOE and FDP_ACF.1/FW-Recyclage_TOE which require access rules to the operation of deletion of the sensitive assets.

OT.FW.SUPERVISION

This objective results in the requirement FMT_SMF.1/FW-Supervision which requires a service to indicate the status of the firewall.

OT.FW.IMPACT_SUPERVISION

This objective results in the requirement FPT_ITC.1/FW-Supervision which requires protecting data exported out of the control of the firewall if they include confidential data.

OT.FW.AUDIT_FLUX

This objective results in FAU_GEN.1/FW-Audit_flux for the generation of event logs on flows processed by the firewall and on FAU_GEN.2/FW-Audit_flux to be able to know who emitted the flows. In order to apply this requirement, flows have to be identified (FIA_UID.2/FW-Flux). The dates of audited events are recorded, for this reason the TOE shall have a reliable clock (FPT_STM.1). The possibility to consult audit logs of the flows processed by the firewall relies on FAU_SAR.1/FW-Audit_flux and FAU_SAR.3/FW-Audit_flux.

OT.FW.PROTECTION_AUDIT_FLUX

This objective results in FAU_STG.1/FW-Traces_audit_flux which requires the protection of the integrity of the records of log events.

OT.FW.AUDIT_ADMIN

This objective results in FAU_GEN.1/FW-Audit_admin for the generation of event logs on the firewall administration events and on FAU_GEN.2/FW-Audit_admin to be able to attribute events to administrators. Administrators have to be identified (FIA_UID.2-Administrateurs). The dates of audited events are recorded, for this reason the TOE shall have a reliable clock (FPT_STM.1). The possibility to consult audit logs of the administration events on the firewall relies on FAU_SAR.1/FW-Audit_admin and FAU_SAR.3/FW-Audit_admin.

OT.FW.PROTECTION_AUDIT_ADMIN

This objective results in FAU_STG.1/FW-Traces_audit_admin which protects the integrity of the records of administration events.

OT.FW.ALARMES

This objective results in FAU_ARP.1/FW-Alarmes which requires raising a security alarm when a potential security violation is detected and on FAU_SAA.1/FW-Alarmes which indicates the rules used to detect these potential violations.

OT.FW.PROTECTION_ALARMES

This objective results in FAU_STG.1/FW-Traces_audit_admin and FAU_STG.1/FW-Traces_audit_flux which protects the integrity of the records of events.

8.2.5.3 TOE VPN component

OT.VPN.APPLICATION_POL

This objective is covered by the VPN application policy (FDP_IFC.1/VPN-Enforcement_policy, FDP_IFF.1/VPN-Enforcement_policy, FDP_ITC.1/VPN-Enforcement_policy and FDP_ETC.1/VPN-Enforcement_policy), because it controls flows of IP packets by applying to them security services provided by the cryptographic operations of FCS_COP.1/VPN-Enforcement_policy.

OT.VPN.CONFIDENTIALITE_APPLI

This objective is covered by FCS_COP.1/VPN-Enforcement_policy which provides cryptographic operations to protect data confidentiality.

OT.VPN.AUTHENTICITE_APPLI

This objective is covered by FCS_COP.1/VPN-Enforcement_policy which provides cryptographic operations to protect data authenticity.

OT.VPN.CONFIDENTIALITE_TOPO

This objective is covered by FCS_COP.1/VPN-Enforcement_policy which provides cryptographic operations to protect data confidentiality.

OT.VPN.AUTHENTICITE_TOPO

This objective is covered by FCS_COP.1/VPN-Enforcement_policy which provides cryptographic operations to protect data authenticity.

OT.VPN. CLOISONNEMENT_FLUX

This objective is covered by the VPN application policy (FDP_IFC.1/VPN-Enforcement_policy, FDP_IFF.1/VPN-Enforcement_policy and FDP_ETC.1/VPN-Enforcement_policy), because it controls the sending of IP packets on the appropriate sub-networks of the private network.

OT.VPN.DEFINITION_POL

This objective is covered by the protection policy of VPN security policies (FDP_ACC.1/VPN-VPN_policy, FDP_ACF.1/VPN-VPN_policy, FDP_ITC.1/VPN-VPN_policy, FMT_MSA.3/VPN-VPN_policy, FMT_MSA.1/VPN-VPN_policy and FMT_SMF.1/VPN-VPN_policy) which controls the access to the definition of VPN security policies.

OT.VPN.PROTECTION_POL

This objective is covered by the protection policy of VPN security policies which controls the access to these policies and their contexts: FDP_ACC.1/VPN-VPN_policy, FDP_ACF.1/VPN-VPN_policy, FMT_MSA.3/VPN-VPN_policy, FMT_MSA.1/VPN-VPN_policy et FMT_SMF.1/VPN-VPN_policy.

OT.VPN.VISUALISATION_POL

This objective is covered by the protection policy of VPN security policies (FDP_ACC.1/VPN-VPN_policy and FDP_ACF.1/VPN-VPN_policy) by controlling the access to the display of VPN security policies and to their contexts.

OT.CRYPTO

This objective is covered by requirements concerning cryptographic keys and cryptographic operations:

- cryptographic operations: FCS_COP.1/VPN-Enforcement_policy,
- keys renewal: FTA_TSE.1/VPN-Key_policy.
- generation of session cryptographic keys: FCS_CKM.1/ VPN-Key_policy

OT.VPN.ACCES_CLES

This objective is covered by the key policy (FDP_IFC.1/VPN-Key_policy, FDP_IFF.1/VPN-Key_policy and FMT_MSA.3/VPN-Key_policy) which controls keys flows.

OT.VPN. INJECTION_CLES

This objective is covered by the key policy (FDP_IFC.1/VPN-Key_policy, FDP_IFF.1/VPN-Key_policy and FMT_MSA.3/VPN-Key_policy) which controls keys flows including keys injection (FDP_ITC.1/VPN-Key_policy).

OT.VPN.PROTECTION_PARAM

This objective is covered by FMT_MTD.1/VPN-Network_param (for network configuration parameters), FMT_MTD.1/Param_security_administrator (for access rights and authentication data) and FMT_SMF.1/VPN-Config_supervision because these requirements guarantee the confidentiality and integrity of configuration parameters by restricting the access to the operations performed on these parameters.

OT.VPN.CHANGEMENT_CONTEXTE

This objective is covered by FDP_RIP.1/VPN, because this requirement guarantees the TOE provides the capability to make unavailable contents of resources corresponding to TOE sensitive assets. In addition, this objective is covered by FCS_CKM.4/VPN-Key_policy, because this requirement requires the TOE to be able to destroy its cryptographic keys.

OT.VPN.SUPERVISION

This objective is covered by FMT_SMF.1/VPN-Config_supervision, because this requirement requires a function of monitoring of the status of VPN components.

OT.VPN.IMPACT_SUPERVISION

This objective is covered by all the policies of access controls and information flows about the sensitive assets of the TOE by restricting the access to operations performed on these assets: FDP_ACC.1/VPN-VPN_policy, FDP_ACF.1/VPN-VPN_policy, FDP_IFC.1/VPN-Key_policy, FDP_IFF.1/VPN-Key_policy, FDP_IFC.1/VPN-Enforcement_policy and FDP_IFF.1/VPN-Enforcement_policy. In addition, for the same reasons this objective is covered by all the requirements about the management of the TSF data: FMT_MTD.1/VPN-Network_param and FMT_MTD.1/Param_security_administrator.

OT.VPN.AUDIT_FLUX

This objective is covered by FAU_GEN.1/VPN-Audit_flux which guarantees the generation of audit events for the VPN communication links and by FPT_STM.1 which guarantees the date associated to each audit event is reliable. In addition, this objective is also covered by FAU_SAR.1/VPN-Audit_flux and FAU_SAR.3/VPN-Audit_flux which provide the ability to view audit events.

OT.VPN.PROTECTION_AUDIT_FLUX

This objective is covered by FAU_STG.1/VPN-Traces_audit_flux which protects the integrity of the records of audit events. In addition, FAU_GEN.1/VPN-Audit_flux and FAU_GEN.1/VPN-Audit_admin enable to detect the loss of audit events.

OT.VPN.AUDIT_ADMIN

This objective is covered by FAU_GEN.1/VPN-Audit_admin which guarantees the generation of audit events about the administration operations and by FPT_STM.1 which guarantees the date associated to each audit event is reliable. In addition, this objective is also covered by FAU_SAR.1/VPN-Audit_admin and FAU_SAR.3/VPN-Audit_admin which provide the ability to view audit events.

OT.VPN.PROTECTION_AUDIT_ADMIN

This objective is covered by FAU_STG.1/VPN-Traces_audit_admin which protects the integrity of the records of audit events. In addition, FAU_GEN.1/VPN-Audit_flux and FAU_GEN.1/VPN-Audit_admin enable to detect the loss of audit events.

OT.VPN.ALARMES

This objective is covered by FAU_ARP.1/VPN-Alarmes which requires raising a security alarm when a potential security violation is detected and by FAU_SAA.1/VPN-Alarmes which indicates the rules used to detect these potential violations.

OT.VPN.PROTECTION_ALARMES

This objective is covered by FAU_STG.1/VPN-Traces_audit_admin and FAU_STG.1/VPN-Traces_audit_flux which protect the integrity of the records of security alarms. In addition, FAU_GEN.1/VPN-Audit_flux and FAU_GEN.1/VPN-Audit_admin enable to detect the loss of security alarms.

8.2.6 Rationale for the coverage of the functional security requirements for the technical environment of the TOE

OE.AUTHENTIFICATION_ADMIN_DISTANT

The objective directly results in the requirement of authentication of the administrators on the remote administration station: FIA_UAU.2-Administration_distante.

8.2.7 Dependencies fulfillment

Table 6: Dependencies of functional security requirements for the TOE

Requirements	CC dependencies	ST dependencies	Fulfillment
Class FAU : Security Audit			
FAU_ARP.1/FW-Alarmes	FAU_SAA.1	FAU_SAA.1/FW-Alarmes	ok
FAU_ARP.1/VPN-Alarmes	FAU_SAA.1	FAU_SAA.1/VPN-Alarmes	ok
FAU_GEN.1/FW-Audit_flux	FPT_STM.1	FPT_STM.1	ok
FAU_GEN.1/FW-Audit_admin	FPT_STM.1	FPT_STM.1	ok
FAU_GEN.1/VPN-Audit_flux	FPT_STM.1	FPT_STM.1	ok
FAU_GEN.1/VPN-Audit_admin	FPT_STM.1	FPT_STM.1	ok
FAU_GEN.2/FW-Audit_flux	FAU_GEN.1	FAU_GEN.1/FW-Audit_flux	ok
	FIA_UID.1	FIA_UID.2/FW-Flux	ok
FAU_GEN.2/FW-Audit_admin	FAU_GEN.1	FAU_GEN.1/FW-Audit_admin	ok
	FIA_UID.1	FIA_UID.2-Administrateurs	ok
FAU_SAA.1/VPN-Alarmes	FAU_GEN.1	FAU_GEN.1/VPN-Audit_flux	ok
		FAU_GEN.1/VPN-Audit_admin	ok
FAU_SAA.1/FW-Alarmes	FAU_GEN.1	FAU_GEN.1/FW-Audit_flux	ok
		FAU_GEN.1/FW-Audit_admin	ok
FAU_SAR.1/FW-Audit_flux	FAU_GEN.1	FAU_GEN.1/FW-Audit_flux	ok
FAU_SAR.1/VPN-Audit_flux	FAU_GEN.1	FAU_GEN.1/VPN-Audit_flux	ok
FAU_SAR.1/FW-Audit_admin	FAU_GEN.1	FAU_GEN.1/FW-Audit_admin	ok
FAU_SAR.1/VPN-Audit_admin	FAU_GEN.1	FAU_GEN.1/FW-Audit_admin	ok
FAU_SAR.3/FW-Audit_flux	FAU_SAR.1	FAU_SAR.1/FW-Audit_flux	ok
FAU_SAR.3/FW-Audit_admin	FAU_SAR.1	FAU_SAR.1/FW-Audit_admin	ok
FAU_SAR.3/VPN-Audit_admin	FAU_SAR.1	FAU_SAR.1/VPN-Audit_admin	ok
FAU_SAR.3/VPN-Audit_flux	FAU_SAR.1	FAU_SAR.1/VPN-Audit_flux	ok
FAU_STG.1/FW-Traces_audit_flux	FAU_GEN.1	FAU_GEN.1/FW-Audit_flux	ok
FAU_STG.1/VPN-Traces_audit_flux	FAU_GEN.1	FAU_GEN.1/VPN-Audit_flux	ok
FAU_STG.1/VPN-Traces_audit_admin	FAU_GEN.1	FAU_GEN.1/VPN-Audit_admin	ok
FAU_STG.1/FW-Traces_audit_admin	FAU_GEN.1	FAU_GEN.1/FW-Audit_admin	ok
Class FCS : Cryptographic Support			
FCS_CKM.1/ VPN-Key_policy	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/VPN-Key_policy	ok
	FCS_CKM.4	FCS_CKM.4/VPN-Key_policy	ok
	FMT_MSA.2	NOT OK	NOT OK
FCS_CKM.4/VPN-Key_policy	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/VPN-Key_policy	ok
	FMT_MSA.2	NOT OK	NOT OK
FCS_COP.1/VPN-Enforcement_policy	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/VPN-Key_policy	ok
	FCS_CKM.4	FCS_CKM.4/VPN-Key_policy	ok

	FMT_MSA.2	NOT OK	NOT OK
Class FDP : User Data Protection			
FDP_ACC.1/FW-Filtering_policy	FDP_ACF.1	FDP_ACF.1/FW-Filtering_policy	ok
FDP_ACC.1/FW-Recyclage_TOE	FDP_ACF.1	FDP_ACF.1/FW-Recyclage_TOE	ok
FDP_ACC.1/VPN-VPN_policy	FDP_ACF.1	FDP_ACF.1/VPN-VPN_policy	ok
FDP_ACF.1/FW-Filtering_policy	FDP_ACC.1	FDP_ACC.1/FW-Filtering_policy	ok
	FMT_MSA.3	NOT OK	NOT OK
FDP_ACF.1/FW-Recyclage_TOE	FDP_ACC.1	FDP_ACC.1/FW-Recyclage_TOE	ok
	FMT_MSA.3	NOT OK	NOT OK
FDP_ACF.1/VPN-VPN_policy	FDP_ACC.1	FDP_ACC.1/VPN-VPN_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-VPN_policy	ok
FDP_ETC.1/VPN-Enforcement_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/VPN-Enforcement_policy	ok
FDP_IFC.1/VPN-Enforcement_policy	FDP_IFF.1	FDP_IFF.1/VPN-Enforcement_policy	ok
FDP_IFC.1/VPN-Key_policy	FDP_IFF.1	FDP_IFF.1/VPN-Key_policy	ok
FDP_IFC.2/FW-Enforcement_policy	FDP_IFF.1	FDP_IFF.1/FW-Enforcement_policy	ok
FDP_IFF.1/FW-Enforcement_policy	FDP_IFC.1	FDP_IFC.2/FW-Enforcement_policy	ok
	FMT_MSA.3	NOT OK	NOT OK
FDP_IFF.1/VPN-Enforcement_policy	FDP_IFC.1	FDP_IFC.1/VPN-Enforcement_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-VPN_policy	ok
FDP_IFF.1/VPN-Key_policy	FDP_IFC.1	FDP_IFC.1/VPN-Key_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-Key_policy	ok
FDP_ITC.1/VPN-Enforcement_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/VPN-Enforcement_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-VPN_policy	ok
FDP_ITC.1/VPN-VPN_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/VPN-Enforcement_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-VPN_policy	ok
FDP_ITC.1/VPN-Key_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/VPN-Key_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-Key_policy	ok
FDP_RIP.1/FW-Recyclage_TOE	-	-	ok
FDP_RIP.1/VPN	-	-	ok
Class FIA : Identification and Authentication			
FIA_UAU.2-Station_administration_distante	FIA_UID.1	FIA_UID.2/FW-Flux	ok
FIA_UAU.2-Administrateurs_local	FIA_UID.1	FIA_UAU.2-Administrateurs_local	ok
FIA_UID.2-Administrateurs	-	-	ok
FIA_UID.2/FW-Flux	-	-	ok
Class FMT : Security Management			
FMT_MSA.1/VPN-VPN_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/VPN-VPN_policy	ok
	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/VPN-VPN_policy	ok
FMT_MSA.3/VPN-Key_policy	FMT_MSA.1	NOT OK	NOT OK

	FMT_SMR.1	FMT_SMR.1	ok
FMT_MSA.3/VPN-VPN_policy	FMT_MSA.1	FMT_MSA.1/VPN-VPN_policy	ok
	FMT_SMR.1	FMT_SMR.1	ok
FMT_MTD.1/FW-Network_param	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/FW-Configuration	ok
FMT_MTD.1-Param_security_administrator	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/FW-Configuration	ok
FMT_MTD.1-Param_auditor	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/FW-Configuration	ok
FMT_MTD.1/VPN-Network_param	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/VPN-Config_supervision	ok
FMT_SMF.1/FW-Supervision	-	-	ok
FMT_SMF.1/VPN-Config_supervision	-	-	ok
FMT_SMF.1/VPN-VPN_policy	-	-	ok
FMT_SMF.1/FW-Visualisation_politique_filtrage	-	-	ok
FMT_SMF.1/FW-Configuration	-	-	ok
FMT_SMR.1	FIA_UID.1		ok
Class FPT : Protection of the TSF			
FPT_ITC.1/FW-Supervision	-	-	ok
FPT_ITT.1-Administration_distante	-	-	ok
FPT_ITT.3-Administration_distante	FPT_ITT.1	FPT_ITT.1-Administration_distante	ok
FPT_STM.1	-	-	ok
FPT_TDC.1/FW-Administration_distante	-	-	ok
Class FTA : TOE Access			
FTA_TSE.1/VPN-Key_policy	-	-	ok

8.2.8 Rationale for unsatisfied dependencies

The dependency of FMT_MSA.3 from FDP_ACF.1/FW-Filtering_policy is not satisfied. This dependency is not satisfied in the [PP_FWIP] protection profile for the following reason: the protection profile does not require the TOE to predefine default values of security attributes for the access control to the filtering policy.

The dependency of FMT_MSA.3 from FDP_ACF.1/FW-Recyclage_TOE is not satisfied. This dependency is not satisfied in the [PP_FWIP] protection profile for the following reason: the protection profile does not require the TOE to predefine default values of security attributes for the access control to sensitive assets.

The dependency of FMT_MSA.3 from FDP_IFF.1/FW-Enforcement_policy is not satisfied. This dependency is not satisfied in the [PP_FWIP] protection profile for the following reason: the protection profile does not require restrictive values for the attributes on which the filtering policy relies. However, it could be possible a product does it.

The dependency of FMT_MSA.2 from FCS_COP.1/VPN-Enforcement_policy is not satisfied. This dependency is not satisfied in the [PP_ CIP] protection profile for the following reason: as there is no security attribute used in cryptographic functions to apply the VPN security policies, this dependency cannot be satisfied.

The dependency of FMT_MSA.1 from FMT_MSA.3/VPN-Key_policy is not satisfied. This dependency is not satisfied in the [PP_ CIP] protection profile for the following reason: the AT.key_type security attribute only has the viewing operation and it is provided only to the TSF. As this operation is not provided to a given role, this dependency is not satisfied.

The dependency of FMT_MSA.2 from FCS_CKM.4/VPN-Key_policy is not satisfied. This dependency is not satisfied in the [PP_ CIP] protection profile for the following reason: as there is no security attribute used to destroy cryptographic keys concerned by this requirement, this dependency is not satisfied. The dependency of FMT_MSA.2 from FCS_CKM.1/VPN-Key_policy is not satisfied for the same reasons.

8.3 Rationale for the specifications

8.3.1 Coverage of functional requirements

Table 7: Coverage of security functional requirements for the TOE

TOE functions	Security functional requirements for the TOE									
	F.RELIABLE_TIME	F.AUDIT	F.USER_DATA_PROTECTION_FW	F.USER_DATA_PROTECTION_VPN	F.ROLES	F.ADMINISTRATION	F.REINIT	F.LOCAL_ADMIN_IDENTIFICATION_AUTHENTICATION	F.REMOTE_STATION_AUTHENTICATION	F.REMOTE_ADMIN_PROTECTION
FPT_STM.1	X									
FPT_ITT.1-Administration_distante										X
FPT_ITT.3-Administration_distante										x
FIA_UAU.2-Station_administration_distante									X	
FMT_SMR.1					X					
FIA_UID.2-Administrateurs								X		
FIA_UAU.2-Administrateurs_local								X		
FDP_IFC.2/FW-Enforcement_policy			X							
FDP_IFF.1/FW-Enforcement_policy			X							
FMT_SMF.1/FW-Visualisation_politique_filtrage						X				
FPT_TDC.1/FW-Administration_distante			X							
FDP_ACC.1/FW-Filtering_policy					X					
FDP_ACF.1/FW-Filtering_policy						X				
FAU_GEN.1/FW-Audit_flux		X								
FAU_GEN.2/FW-Audit_flux		X								
FIA_UID.2/FW-Flux			X							

FAU_SAR.1/FW-Audit_flux		X								
FAU_SAR.3/FW-Audit_flux		X								
FAU_STG.1/FW-Traces_audit_flux		X								
FAU_GEN.1/FW-Audit_admin		X								
FAU_GEN.2/FW-Audit_admin		X								
FAU_SAR.1/FW-Audit_admin		X								
FAU_SAR.3/FW-Audit_admin		X								
FAU_STG.1/FW-Traces_audit_admin		X								
FAU_SAA.1/FW-Alarmes		X								
FAU_ARP.1/FW-Alarmes		X								
FMT_SMF.1/FW-Configuration						X				
FMT_MTD.1/FW-Network_param						X				
FMT_MTD.1-Param_security_administrator						X				
FMT_MTD.1-Param_auditor						X				
FMT_SMF.1/FW-Supervision						X				
FPT_ITC.1/FW-Supervision										X
FDP_RIP.1/FW-Recyclage_TOE							X			
FDP_ACC.1/FW-Recyclage_TOE					X					
FDP_ACF.1/FW-Recyclage_TOE							X			
FDP_IFC.1/VPN-Enforcement_policy				X						
FDP_IFF.1/VPN-Enforcement_policy				X						
FDP_ITC.1/VPN-Enforcement_policy				X						
FDP_ETC.1/VPN-Enforcement_policy				X						
FCS_COP.1/VPN-Enforcement_policy				X						
FDP_ACC.1/VPN-VPN_policy					X					
FDP_ACF.1/VPN-VPN_policy				X						
FDP_ITC.1/VPN-VPN_policy				X						
FMT_MSA.3/VPN-VPN_policy						X				
FMT_MSA.1/VPN-VPN_policy						X				
FMT_SMF.1/VPN-VPN_policy						X				
FAU_GEN.1/VPN-Audit_flux		X								
FAU_SAR.1/VPN-Audit_flux		X								
FAU_SAR.3/VPN-Audit_flux		X								
FAU_STG.1/VPN-Traces_audit_flux		X								
FAU_GEN.1/VPN-Audit_admin		X								
FAU_SAR.1/VPN-Audit_admin		X								
FAU_SAR.3/VPN-Audit_admin		X								
FAU_STG.1/VPN-Traces_audit_admin		X								
FAU_SAA.1/VPN-Alarmes		X								
FAU_ARP.1/VPN-Alarmes		X								
FMT_MTD.1/VPN-Network_param						X				
FMT_SMF.1/VPN-Config_supervision						X				
FDP_RIP.1/VPN							X			
FDP_ITC.1/VPN-Key_policy						X				
FDP_IFC.1/VPN-Key_policy				X						
FDP_IFF.1/VPN-Key_policy				X						
FMT_MSA.3/VPN-Key_policy						X				
FTA_TSE.1/VPN-Key_policy				X						
FCS_CKM.4/VPN-Key_policy							X			
FCS_CKM.1/VPN-Key_policy				X						

9. APPENDIX

9.1 Appendix 1: Minimal audit logs and associated level

Security functional requirement	CC recommendation part 2	Level adopted
FAU_ARP.1/FW-Alarmes	a) Minimal: Actions taken due to imminent security violations.	Minimal
FAU_ARP.1/VPNarmes	a) Minimal: Actions taken due to imminent Security violations.	Minimal
FAU_GEN.1/FW-Audit_flux	N/A	N/A
FAU_GEN.1/FW-Audit_admin	N/A	N/A
FAU_GEN.1/VPN-Audit_flux	N/A	N/A
FAU_GEN.1/VPN-Audit_admin	N/A	N/A
FAU_GEN.2/FW-Audit_flux	N/A	N/A
FAU_GEN.2/FW-Audit_admin	N/A	N/A
FAU_SAA.1/VPN-Alarmes	a) Minimal: Enabling and disabling of any of the analysis mechanisms; b) Minimal: Automated Responses performed by the tool.	Minimal
FAU_SAA.1/FW-Alarmes	a) Minimal: Enabling and disabling of any of the analysis mechanisms; b) Minimal: Automated Responses performed by the tool.	Minimal
FAU_SAR.1/FW-Audit_flux	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.1/VPN-Audit_flux	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.1/FW-Audit_admin	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.1/VPN-Audit_admin	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.3**/FW**-Audit_flux	a) Detailed: the parameters used for the viewing.	-
FAU_SAR.3/FW-Audit_admin	a) Detailed: the parameters used for the viewing.	-
FAU_SAR.3/VPN-Audit_admin	a) Detailed: the parameters used for the viewing.	-
FAU_SAR.3**/VPN**-Audit_flux	a) Detailed: the parameters used for the viewing.	-
FAU_STG.1/FW-Traces_audit_flux	N/A	N/A
FAU_STG.1/VPN-Traces_audit_flux	N/A	N/A
FAU_STG.1/FW-Traces_audit_admin	N/A	N/A
FAU_STG.1/VPN-Traces_audit_admin	N/A	N/A
FCS_CKM.4/VPN-Key_policy	a) Minimal: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	Basic
FCS_COP.1/VPN-Enforcement_policy	a) Minimal: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of	Basic

	operation, subject attributes and object attributes.	
FDP_ACC.1/FW-Filtering_policy	N/A	N/A
FDP_ACC.1/FW-Recyclage_TOE	N/A	N/A
FDP_ACC.1VPN-VPN_policy	N/A	N/A
FDP_ACF.1/FW-Filtering_policy	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by The SFP. c) Detailed: The specific security attributes used in making an access check.	Basic
FDP_ACF.1/FW-Recyclage_TOE	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Basic
FDP_ACF.1/VPN-VPN_policy	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Basic
FDP_ETC.1/VPN-Enforcement_policy	a) Minimal: Successful export of information. b) Basic: All attempts to export information.	Minimal
FDP_IFC.1/VPN-Enforcement_policy	N/A	N/A
FDP_IFC.1/VPN-Key_policy	N/A	N/A
FDP_IFC.2/FW-Enforcement_policy	N/A	N/A
FDP_IFF.1/FW-Enforcement_policy	a) Minimal: Decisions to permit requested information flows. b) Basic: All decisions on requests for information flow. c) Detailed: The specific security attributes used in making an information flow enforcement decision. d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	Basic
FDP_IFF.1/VPN-Enforcement_policy	a) Minimal: Decisions to permit requested information flows. b) Basic: All decisions on requests for information flow. c) Detailed: The specific security attributes used in making an information flow enforcement decision.	Basic

	d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	
FDP_IFF.1/VPN-Key_policy	a) Minimal: Decisions to permit requested information flows. b) Basic: All decisions on requests for information flow. c) Detailed: The specific security attributes used in making an information flow enforcement decision. d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	Basic
FPT_ITC.1/VPN-Enforcement_policy	N/A	N/A
FPT_ITC.1/VPN-VPN_policy	N/A	N/A
FPT_ITC.1/VPN-Key_policy	N/A	N/A
FDP_RIP.1/FW-Recyclage_TOE	N/A	N/A
FDP_RIP.1/VPN	N/A	N/A
FIA_UAU.2-Station_administration_distante	a) Minimal:Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	Basic
FIA_UAU.2-Administrateurs_local	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	Basic
FIA_UID.2-Administrateurs	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Basic
FIA_UID.2/FW-Flux	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Basic
FMT_MSA.1/VPN-VPN_policy	a) Basic: All modifications of the values of security attributes.	Basic
FMT_MSA.3/VPN-Key_policy	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.	Basic
FMT_MSA.3/VPN-VPN_policy	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.	Basic
FMT_MTD.1/FW-Network_param	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1-Param_security_administrator	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1-Param_auditor	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1/VPN-Network_param	a) Basic: All modifications to the values of TSF data.	Basic

FMT_SMF.1/FW-Supervision	a) Minimal: Use of the Management functions.	Minimal
FMT_SMF.1/**VPN**-Config_supervision	a) Minimal: Use of the management functions.	Minimal
FMT_SMF.1/**VPN**-VPN_policy	a) Minimal: Use of the management functions.	Minimal
FMT_SMF.1/**FW**-Visualisation_politique_filtrage	a) Minimal: Use of the management functions.	Minimal
FMT_SMF.1/FW-Configuration	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	Minimal
FMT_SMR.1	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	Minimal
FPT_ITC.1/FW-Supervision	N/A	N/A
FPT_ITT.1-Administration_distante	N/A	N/A
FPT_ITT.3-Administration_distante	a) Minimal: the detection of modification of TSF data; b) Basic: the action taken following detection of an integrity error.	Basic
FPT_STM.1	a) Minimal: changes to the time; b) Detailed: providing a timestamp.	Minimal
FPT_TDC.1/FW-Administration_distante	a) Minimal: Successful use of TSF data consistency mechanisms. b) Basic: Use of the TSF data consistency mechanisms. Identification of which TSF data have been interpreted. d) Basic: Detection of modified TSF data.	Basic
FTA_TSE/VPN-Keypolicy	a) Minimal: Denial of a session establishment due to the session establishment mechanism. b) Basic: All attempts at establishment of a user session. c) Detailed: Capture of the value of the selected access parameters (e.g. location of access, time of access).	Basic