Direction centrale de la sécurité des systèmes d'information

IP Encryptor Protection Profile - CC3.1

Creation date	July 2008
Reference	PP-CIP-3.1
Version	1.9

Courtesy Translation

Courtesy translation of the protection profile registered and certified by the French Certification Body under the reference DCSSI-PP-2008/08.

Table of contents

List of figures

List of tables

1. Protection Profile introduction

1.1. Protection Profile identification

Title:	Protection Profile, IP encryptor.
Author:	Trusted Labs S.A.S.
Version:	1.9, July 2008
Sponsor:	DCSSI
CC version:	3.1 revision 2

1.2. Protection Profile introduction

This protection profile specifies security requirements for a virtual private network gateway (VPN).

These VPN gateways are placed in the inputs/outputs of private networks, considered to be secure, to establish communication links between some of these private networks by using a public network (as Internet), considered to be not secure. These communication links between several VPN gateways, so called VPN links, must be secured so that the data which flow through private networks can be protected from all public network users.

This protection profile concentrates only to define security requirements on VPN gateways, which enable communications between private networks, and does not define security requirements on the VPN client part which enables the establishment of secure communications between mobile equipments (PC, laptop) or between mobile equipments and private networks.

A security target claiming conformance to this PP is allowed to introduce additional functionalities not taken into account by this PP: firewall, authentication server, antivirus gateway... Additional functionalities and their implementation do not have to question the requirements of the current PP. When writing a security target claiming conformance to this protection profile, these functionalities are perfectly possible to express and, if needed, the target can make reference to any protection profile covering them (such as [PP-FIR]).

Later in this document, the expression « VPN gateway » is refered to as « IP encryptor ».

This protection profile defines requirements for the minimal configuration of an IP encryptor which includes the local administration of the IP encryptor. Three other configurations can be taken into account from the two following options: the remote administration of IP encryptors in addition to the local administration and the dynamic negotiation of a part of the contexts of security policies enforced by IP encryptors. As the Common Criteria methodology does not provide the capability to evaluate a profile with options, it was therefore chosen to evaluate the minimal configuration and to define, in application notes, specific elements (threats, assumptions, OSP, objectives and requirements) for each option. These application notes will also contain the rationale of associations between these elements only for the maximal configuration (remote administration and dynamic negotiation) in order to preserve the work realized in a previous version of the protection profile.

A security target claiming conformance to this PP and including one or two options defined in application notes shall take into account elements and rationales of these application notes.

1.3. VPN technologies introduction

This section introduces various standards used in VPN technologies. This section is only introduced for an informative purpose. Security services described in this profile were partially established on the basis of those offered by these standards, but this profile does not claim compliance to any of these.

1.3.1. IPsec

IPsec (IP security) is a set of standards implementing mechanisms to secure IP (IPv4 and IPv6) by offering authentication, integrity and confidentiality services ([RFC2401]).

IPsec offers these services by the means of two protocols for data exchange security:

- AH (Authentication Header) provides the authentication of the origin and the on-the-fly integrity of the IP packets. It can also provide an optional protection against replay attacks ([RFC2402]).
- ESP (Encapsulating Security Payload) provides confidentiality, protection against replay attacks and an optional authentication of the origin and the on-the-fly integrity of a part of IP packets, which part does not contain the IP header ([RFC2406]).

These two protocols can be combined and used in one out of the two following data exchange modes:

- Transport mode: the IP packet is sent by adding specific parts to AH and/or ESP.
- Tunnel mode: the IP packet is encapsulated in a new IP packet containing specific parts of AH and/or ESP.

IPsec uses the concept of security association (SA) covered by AH and ESP. A security association provides the capability to define characteristics of a unidirectional connection: IP destination address, security protocol (AH or ESP), security parameters index (SPI), used cryptographic algorithms, used keys, expiration date and hour, etc. This association is used to enforce a security policy during the processing of IP packets flowing through the connection.

IPsec also offers protocols for cryptographic keys and security associations management:

- IKE (Internet Key Exchange): [RFC2409]. The security associations' management is covered by ISAKMP ([RFC2408]), while the keys exchange is covered by Oakley ([RFC2412]) and SKEME ([SKEME]) protocols.

1.4. Acronyms

CC	*Common Criteria*
KGEF	*Key Generation and Escrow Facility*
EAL	*Evaluation Assurance Level*
IP	*Internet Protocol*
IT	*Information Technology*
OSP	*Organisational Security Policy*
PP	*Protection Profile*
SF	*Security Function*
SFP	*Security Function Policy*
SOF	*Strength Of Function*
ST	*Security Target*
TOE	*Target Of Evaluation*
TSF	*TOE Security Function*
VPN	*Virtual Private Network*

1.5. References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006. CCMB-2007-09-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007. CCMB-2007-09-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007. CCMB-2007-09-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007. CCMB-2007-09-004.

[CRYPTO] Cryptographic mechanisms – Rules and recommendations about the choice and parameters sizes of cryptographic mecanisms with standard robustness level. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications

[CRYPTO_GESTION] Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications

[AUTH] Authentification : Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications

[PB-INT] Problématique d'interconnexion des réseaux IP. Version 1.8, mai 2003. Premier Ministre, Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information, Sous-direction scientifique et technique, Laboratoire Technologies de l'Information.

[PP-CIP] Profil de protection Chiffreur IP – CC - version 2.2

[PP-FIR] Profil de Protection Pare-feu IP. Version 3.0f, Juin 2008.

[QUA-STD] Processus de qualification d'un produit de sécurité – niveau standard. Version 1.1, N°549/SGDN/DCSSI/SDR, 18/03/08, DCSSI.

[RFC2401] Security Architecture for the Internet Protocol. RFC 2401. November 1998. S. Kent, R. Atkinson. http://www.ietf.org/rfc/rfc2401.

[RFC2402] IP Authentication Header (AH). RFC 2402. November 1998. S. Kent, R. Atkinson. http://www.ietf.org/rfc/rfc2402.

[RFC2406] IP Encapsulating Security Payload (ESP). RFC 2406. November 1998. S. Kent, R. Atkinson. http://www.ietf.org/rfc/rfc2406.

[RFC2408] Internet Security Association and Key Management Protocol (ISAKMP). RFC 2408. November 1998. D. Maughan, M. Schertler, M. Schneider, J. Turner. http://www.ietf.org/rfc/rfc2408.

[RFC2409] The Internet Key Exchange (IKE). RFC 2409. November 1998. D. Harkins, D. Carrel. http://www.ietf.org/rfc/rfc2409.

[RFC2412] The OAKLEY Key Determiniation Protocol. RFC 2412. November 1998. H. Orman. http://www.ietf.org/rfc/rfc2412.

[SKEME] SKEME: A Versatile Secure Key Exchange Mechanism for Internet. IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security. Krawczyk, H.

2. TOE description

2.1. TOE features

The TOE main feature is to supply to the information system secured communication links between several private networks. The following services are offered to protect and partition dataflows (IP packets flowing through IP encryptors):

- VPN security policies enforcement:
    - confidentiality protection of applicative data,
    - authenticity protection of applicative data,
    - confidentiality protection of private networks topologic data,
    - authenticity protection of private networks topologic data,
- IP flows partitionning.

Furthermore, for its correct operation, the TOE requires the following services:

- VPN security policies management:
    - VPN security policies definition,
    - access protection to the VPN security policies.
- Cryptographic keys management:
    - access protection to the cryptographic keys,
    - cryptographic keys injection,
    - proper use of cryptographic keys.
- Audit and supervision:
    - audit/logging of the activities on VPN links,
    - audit/logging of administration operations,
    - security alarms generation,
    - TOE supervision.
- Administration operations protection: local authentication of administrators.
- Acces protection to the configuration parameters.

2.1.1. Services supplied by the TOE

VPN security policies enforcement

VPN security policies specify the security rules which determine the processing to apply to data. These latters represent:

- Data which result from information system applications and which are conveyed by the network. They are called applicative data.
- Data added by the network mechanisms which notably permit the IP packets routing. They are called topologic data.

These data flow between every pair of IP encryptors.

IP encryptors apply functions of implicit filtering, because if no VPN security policy is defined on a given VPN link, incoming or outgoing packets are rejected (default filtering rule).

The security services which can be applied by a VPN security policy are:

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

These policies are kept at the level of every IP encryptor concerned to be applied locally.

Confidentiality protection of applicative data

Ensuring confidentiality of the applicative data provides the capability to prevent the disclosure of these data when they flow through a non secure public network. For that purpose, these data can be ciphered before going through the public network and deciphered in the entry of the private network recipient.

The encryption/decryption algorithm and used keys characteristics are defined in the security context associated to the VPN security policy defined on a given communication link.

Authenticity protection of applicative data

To ensure the applicative data authenticity, it is necessary to ensure at the same moment the on-the-fly integrity of these data as well as the authentication of the origin of these. Ensuring the data integrity provides the capability to detect that they were not modified accidentally or voluntarily during their transmission of an IP encryptor to another one. Ensuring the data authenticity ensures that the data origin is correct.

The algorithm to generate authenticity informations and verify them as well as used keys characteristics are defined in the security context associated to the VPN security policy defined on a given communication link.

Confidentiality protection of topologic data

Ensuring the topologic data confidentiality of private networks provides the capability to prevent the disclosure of the internal IP addresses (source and destination) of equipments being on private networks.

As for applicative data, encryption/decryption algorithms are used and defined in security contexts.

Authenticity protection of topologic data

Ensuring the topologic data authenticity of private networks provides the capability to detect any modification of the internal IP addresses (source and destination) of equipments being on private networks.

As for applicative data, algorithms to generate authenticity informations or to verify them are used and defined in security contexts.

IP flows partitionning

Every private network can be divided into several IP subnetworks to permit to partition IP flows inside a private network. The IP flows partitionning service enables to enforce different VPN security policies following the subnetworks which communicate. This service also provides the capability to filter incoming IP packets and send them on the appropriate subnetwork.

2.1.2. Required services for the correct operation of the TOE

2.1.2.1. VPN security policies management

VPN security policies definition

VPN security policies are defined for every authorized VPN communication link. This communication link is established between two IP subnetworks. It can exist a policy by communication direction. Only the security administrator is authorized to define these policies. He specifies the rule of implicit filtering for the sending or the reception of data: acceptance, reject or security services enforcement. In the last case, he also specifies the security service(s) to be applied to the data sent or received as well as the security context which is associated to this policy. The security context contains among others used cryptographic algorithms, keys sizes and the association with keys to be used.

Access protection to the VPN security policies

This service provides the capability to control different access types (modification, viewing) in VPN security policies and their security contexts according to the role of the authenticated person.

2.1.2.2. Cryptographic keys management

Access protection to the cryptographic keys

This service provides the capability to prevent secret and private keys to be exported in an unauthorized way outside the TOE. It also enables ascertaining that a given key is useful (accessible) only by services which need it.

Cryptographic keys injection

This service provides the capability to inject cryptographic keys in a secure way, generated outside the TOE, in IP encryptors or administration equipments. During the distribution, this service protects keys in integrity and/or in confidentiality according to the type of keys.

Proper use of cryptographic keys

This service provides the capability to correctly manage cryptographic keys life cycle: bypass, regular renewal, destruction.

2.1.2.3. Audit and supervision

Audit/logging of the activities on VPN links

This service provides the capability to log all operations made by IP encryptors concerning the communication on VPN links, as for example the establishment of the sessions and their lock. It also provides the capability to define the events to record and their consultation.

Audit/logging of administration operations

This service provides the capability to log all operations made by the administrator on IP encryptors concerning the administration of this cipher unit, as for example modifications of VPN security policies. It also provides the capability to define the events to record and their consultation.

Security alarms generation

This service provides the capability to generate security alarms to indicate any major operational failure of IP encryptors, as for example an integrity loss on keys. It also permits a security administrator to define alarms to be generated and their broadcast mode and to review these alarms.

TOE supervision

This service permits a system and network administrator to control the availability state of each IP encryptor (operation state, levels of resources use...).

2.1.2.4. Administration operations protection

IP encryptors are administered locally: it is an administration which is directly made on the machine containing the services of the IP encryptor.

Local authentication of administrators

This service provides the capability to authenticate all administrators who perform local administration operations in an IP encryptor.

2.1.2.5. Access protection to the configuration parameters

This service protects (of network attack) the configuration parameters of IP encryptors in confidentiality and integrity. These parameters include the network configuration parameters (topologic data on private networks), authentication data and access rights.

2.1.3. Roles

The operation of the TOE in its operational environment manipulates directly or indirectly the roles described below.

Security administrator

IP encryptor administrator. He generates and distributes keys in IP encryptors. He defines VPN security policies and their security contexts that every cipher unit is going to apply.

He defines audit events to keep as well as security alarms to generate. Furthermore, he analyzes, processes and deletes generated security alarms.

He configures roles and accesses to tools and administration functions. He manages keys and authentication means to access administration tools or IP encryptors.

Auditor

His role is to analyze audit events concerning activities on VPN links and administration operations.

System and network administrator

Administrator responsible for the information system on which the IP encryptor is. He is responsible for the preservation in operational condition of the TOE (software and hardware maintenance included).

He configures network parameters of cipher units and system parameters which are bound in the operational network contexts to be taken into account: he defines the global network topology, but does not define VPN security policies.

His role also is to control the IP encryptors state.

Private network user

User of a private network connected to another private network by an IP encryptor. This user can, through applications, send/receive informations towards/to another private network via the IP encryptor of his network.

During the document, the administrator role includes following roles: security administrator, auditor and system and network administrator.

2.2. TOE architecture

This section introduces the TOE architecture under two different aspects: physical aspect and functional aspect.

2.2.1. Physical architecture

The Figure 1 introduces an example of physical architecture of a virtual private network on which the TOE will be evaluated.

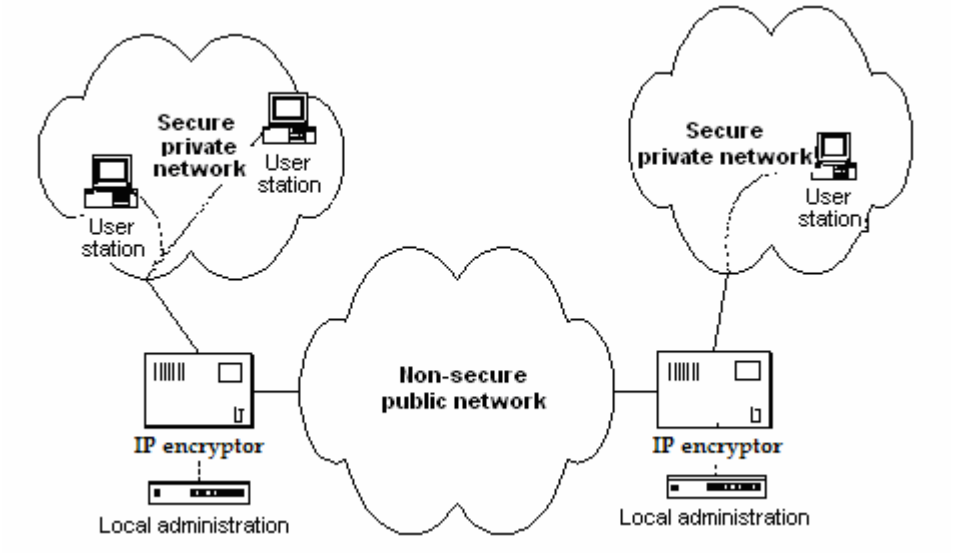

Figure 1 Example of possible VPN architecture

On the Figure 1, IP encryptors are directly connected to the public network and to the private networks, but they can be inserted inside a global structure of IP internetworking (cf. [PB-INT]).

As illustrate in the Figure 1, every IP encryptor presents three logical external interfaces: an interface towards the private network, an interface towards the public network and an administration interface. The example of the figure contains two IP encryptors, minimal number required to the establishment of a VPN link between two private networks, but it could contains as well a superior number.

2.2.2. Functional architecture

The figures of this section show elements which constitute the TOE at the functional level. These elements appear grayed out in figures. Furthermore, the assets appear italicized.

These figures are given on illustrative purpose and form an abstracted view from the functional architecture of the TOE. The disposition of services stated in these figures may therefore not correspond to a given implementation.

Figure 2 introduces the functionalities which concern the VPN security policies management and their security contexts. All services are part of the TOE.

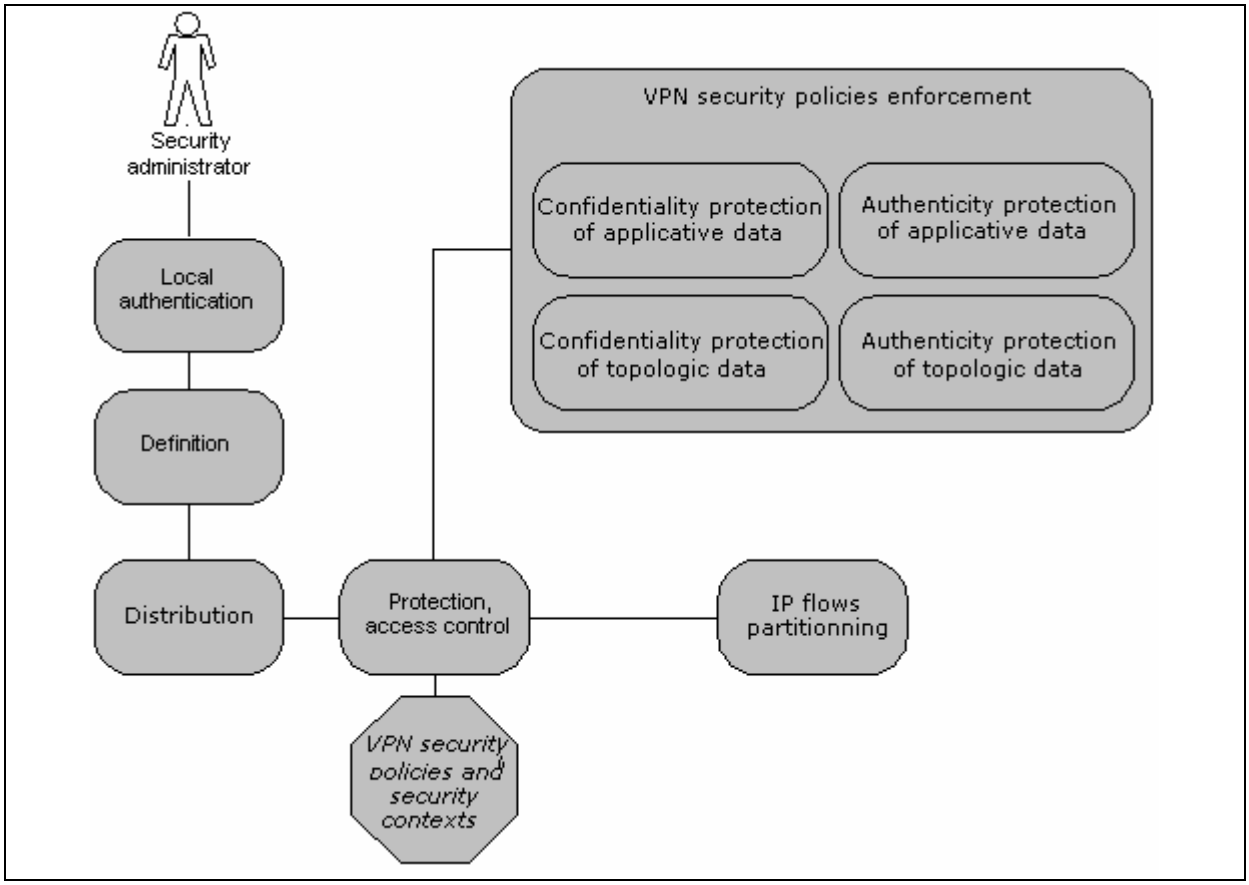

Figure 2 VPN security policies management

This figure (Figure 3) does not introduce all services of the TOE performing read access to configuration parameters, because they are many. These services are among others local authentication services, VPN security policies enforcement and all services which make use of the access rights and the internal IP addresses for their own need.

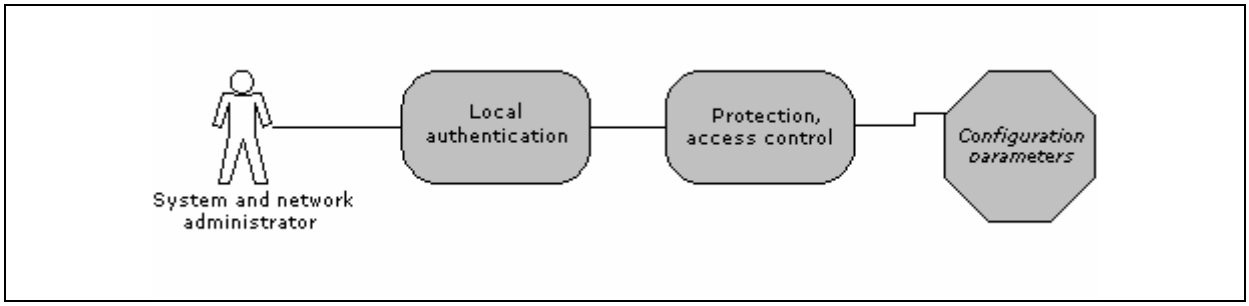

Figure 3 IP encryptors configuration

At the keys management level, the keys generation performed by the KGEF does not belong to the TOE (Figure 4).

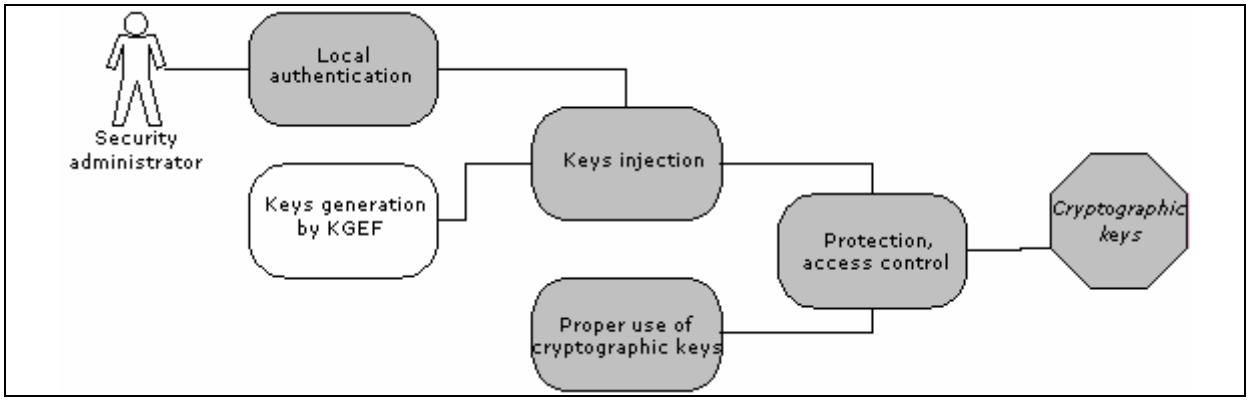

Figure 4 Cryptographic keys management

At the audit level, all services are part of the TOE (Figure 5).

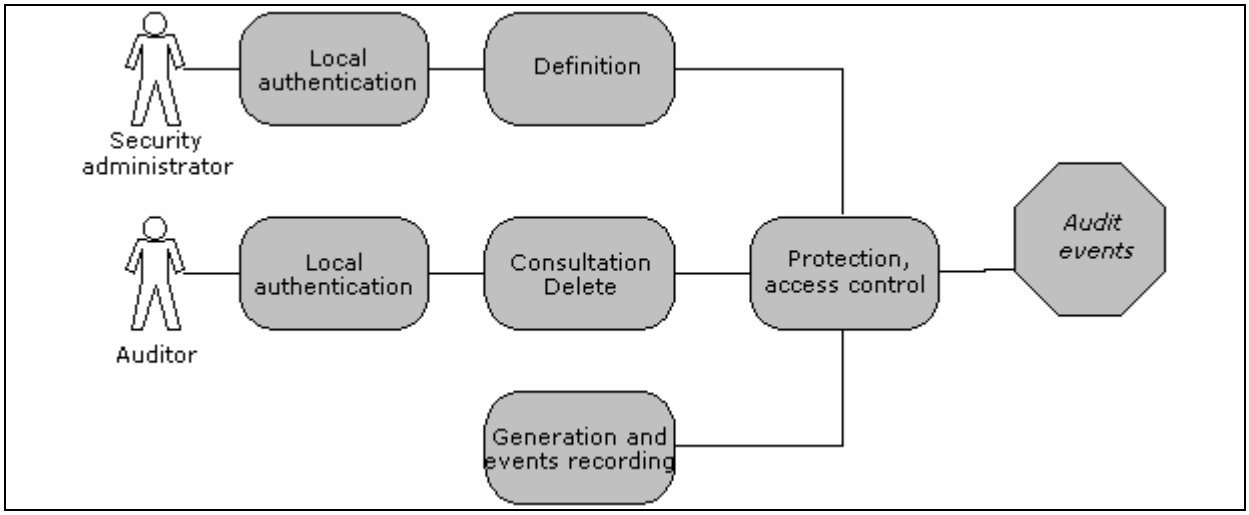

Figure 5 Audit management

At the security alarms level, the alarms processing does not belong to the TOE (Figure 6).

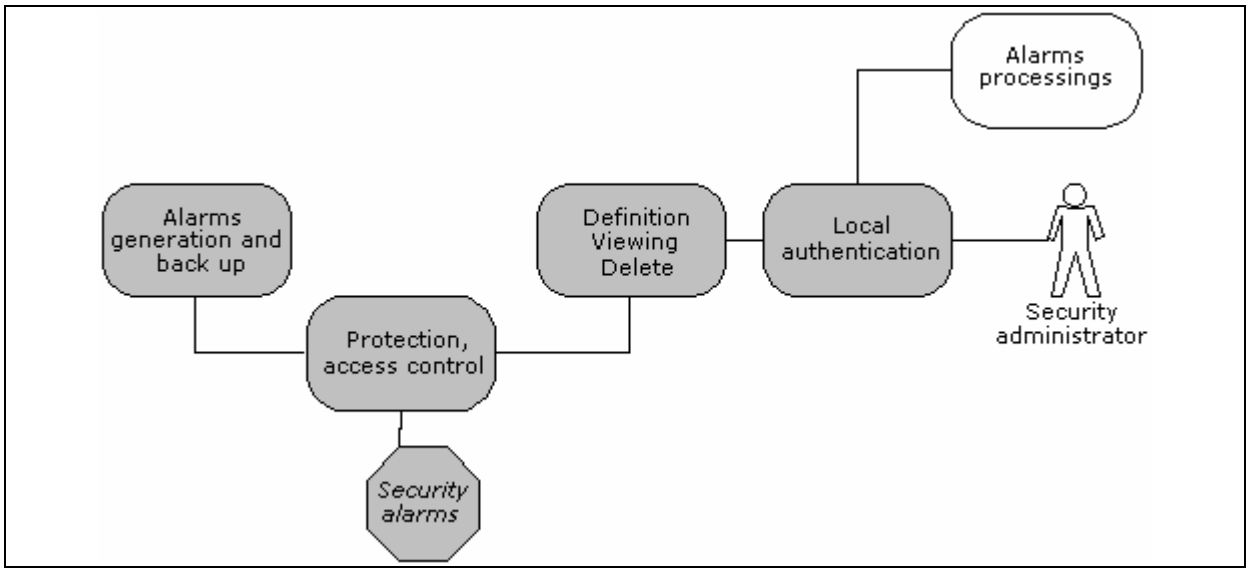

Figure 6 Security alarms management

Supervision is part of the TOE (Figure 7).

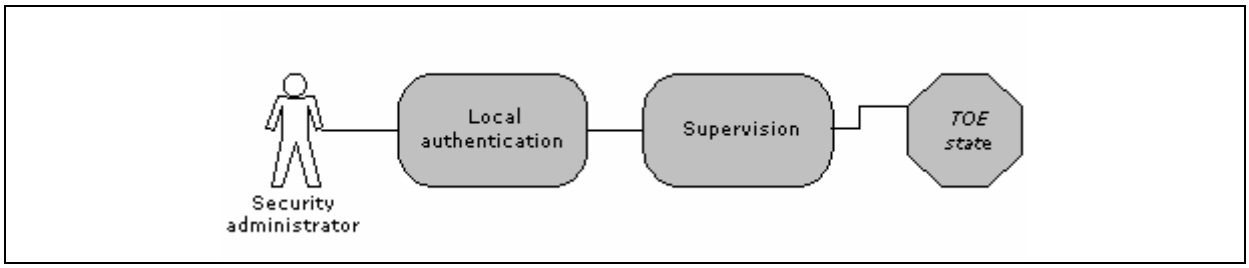

Figure 7 TOE supervision

3. Conformance claims

This chapter contains the following sections:

3.1. CC conformance claim

This protection profile is conformant with Common Criteria version 3.1.

This PP was written according to CC version 3.1:

- CC Part 1 [CC1]
- CC Part 2 [CC2]
- CC Part 3 [CC3]
- CC evaluation methodology [CEM]

3.2. Package conformance claim

This PP is conformant with the assurance requirements package for the standard level qualification defined in [QUA-STD].

3.3. PP conformance claim

This PP declares no conformance with other PP.

3.4. Conformance claim to the PP

The compliance retained in this PP for Security Targets and Protection Profiles which claim conformance to it is the **demonstrable** compliance according to the definition of CC Part 1 [CC1].

4. Security problem definition

4.1. Assets

The description of every asset supplies protection types required for each of them (part *Protection*).

4.1.1. Assets protected by the TOE (User data)

Information system assets are protected by the TOE under the condition that VPN security policies require the enforcement of one or several protection types. As illustration, data which flow between two IP encryptors will be protected in confidentiality only if the VPN security policy defined for this VPN link requires confidentiality protection.

When the protection type (part *Protection*) is followed by "(opt.)" for optional, it means that this protection must be provided by the TOE, but what it is not systematically enforced by the TOE.

D.APPLICATIVE_DATA

Applicative data are data which flow through a private network to another through IP encryptors. They are contained in the IP packets payload routed up to the cipher units and received and sent by these cipher units. These data can be temporarily stored in IP encryptors to be able to process them (i.e., enforce security services) before sending them on the private or public network.

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

D.TOPOLOGIC_INFO

Information pertaining to private networks topology (source and destination IP adresses) are contained within IP packets headers.

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

4.1.2. TOE sensitive assets (TSF data)

D.VPN_POLICIES

VPN security policies define processings functions (implicit filtering and security services) to be performed on data received and sent by every IP encryptor.

This asset also contains the security contexts which are linked with security policies. Every security context contains all security parameters necessary to the enforcement of its associated VPN security policy. These parameters are defined by the security administrator.

Protection:

- o integrity of the policies (and their contexts) stored in IP encryptors,
- o confidentiality.

D.CONFIG_PARAM

Configuration parameters of IP encryptors include among others:

- o private networks internal IP addresses and routing matrices (network configuration),
- o authentication data and
- o access rights.

Protection: confidentiality and integrity.

D.CRYPTO_KEYS

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

- o session keys,
- o keys used by security services enforced by VPN security policies,
- o keys to protect VPN security policies during their storage,
- o keys to protect the injection of cryptographic keys in IP encryptors.

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

D.AUDIT

Data generated by the audit policy to provide the capability to log administration operations performed as well as activities which took place on VPN links.

Protection: integrity.

D.ALARMS

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

Protection: integrity.

D.SOFTWARES

TOE softwares items which permit enforcement of all TOE services.

Protection: integrity.

D.TIME_BASE

Reliable time base of the TOE.

Protection: integrity.

4.2. Threats

Standard level qualification policy, within the context of French IT security regulations ("*politique de qualification au niveau standard*"), applies to consumer market products ensuring the protection of sensitive but not defence-classified information. Consequently, some threats will not be taken into account thereafter in this PP such as for example, equipment items theft (which must be detected by organizational measures) or denial of service.

Threats present in this section are only threats which compromise the security of the TOE and not the security of the services provided by the TOE, because all elements of the environment concerning services provided by the TOE are considered to be organisational security policies.

Administrators are not considered to be attackers (assumption A.ADMIN).

4.2.1. Threats concerning VPN security policies and their contexts

T.POL_MODIFICATION

An attacker illicitly modifies VPN security policies and their security contexts.

Threatened asset: D.VPN_POLICIES.

T.POL_DISCLOSURE

An attacker illicitly retrieves VPN security policies and their security contexts.

Threatened asset: D.VPN_POLICIES.

4.2.2. Threats concerning the configuration

T.PARAM_MODIFICATION

An attacker illicitly modifies configuration parameters.

Threatened asset: D.CONFIG_PARAM.

T.PARAM_DISCLOSURE

An attacker retrieves configuration parameters in an unauthorized way.

Threatened asset: D.CONFIG_PARAM.

4.2.3. Threats concerning the keys management

T.KEYS_MODIFICATION

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

Threatened asset: D.CRYPTO_KEYS.

T.KEYS_DISCLOSURE

An attacker illicitly retrieves cryptographic keys.

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

4.2.4. Threats concerning the audit

T.AUDIT_MODIFICATION

An attacker modifies or deletes illicitly audit events recordings.

Threatened asset: D.AUDIT.

T.ALARM_MODIFICATION

An attacker modifies or deletes illicitly security alarms while they are forward by the TOE to the security administrator.

Threatened asset: D.ALARMS.

T.TIME_BASE

An attacker disturbs or tampers with the TOE time base with the aim of falsifying audit data.

Threatened asset: D.TIME_BASE.

4.2.5. Threats concerning the administration

T.ADMIN_USURPATION

An attacker usurps the administrator identity and performs administration operations on IP encryptors.

Threatened assets: D.VPN_POLICIES, D.CRYPTO_KEYS, D.AUDIT, D.CONFIG_PARAM.

T.UNAVAILABLE_ASSETS

An attacker acquires knowledge, by direct access to the TOE, of sensitive assets of an IP encryptor (keys, VPN security policies...) during a change of operational context (assignment of the IP encryptor in a new network, maintenance...).

Threatened assets: D.VPN_POLICIES, D.CONFIG_PARAM, D.CRYPTO_KEYS, D.AUDIT and D.ALARMS.

4.3. Organisational security policies (OSP)

Organisational security policies present in this section concern only expected TOE functions and concern therefore services provided by the TOE in the information system.

OSP.PROVIDED_SERVICES

The TOE shall enforce VPN security policies defined by the security administrator.

It also shall provide all required security services to apply protections specified in these policies:

- o confidentiality protection of applicative data,
- o authenticity protection of applicative data,
- o confidentiality protection of topologic data and
- o authenticity protection of topologic data.

Furthermore, the TOE shall provide the capability to separate IP flows to make communicate subnetworks (of private networks) and enforce a security policy to every communication link between IP subnetworks.

OSP.CRYPTO

The DCSSI cryptographic referential ([CRYPTO]) must be followed for the keys management (generation, destruction, use and distribution) and cryptographic functions used in the TOE, for the standard resistance level.

OSP.POL_VIEW

The TOE shall enable the security administrators to individually view VPN security policies and their security contexts upon each IP encryptor.

OSP.SUPERVISION

The TOE shall enable the system and network administrator to review the operational status of each IP encryptor.

4.4. Assumptions

4.4.1. Assumptions on the intended usage of the TOE

A.AUDIT

It is assumed that the auditor regulary reviewed audit events generated by the TOE. It is also assumed that the memory units storing audit events are managed so that the auditor does not lose events.

A.ALARM

It is assumed that the security administrator analyzes and processes security alarms generated and forwarded by the TOE.

4.4.2. Assumptions on the TOE operational environment

A.ADMIN

Administrators are not hostile and competent persons with necessary resources for the implementation of their tasks. They are trained to perform the operations for which they are responsible and they follow manuals and administration procedures.

A.PREMISE

Equipments items containing TOE services (IP encryptors and administration equipments), as well as any storage units containing TOE sensitive assets (paper, floppy disks...) shall be stored in secure premises where access is restricted to the administrators. However, equipments items containing TOE services are allowed to not be put in secure premises if they do not contain sensitive assets: for example in the cases of change of IP encryptor operational context.

A.CONFIGURATION_CONTROL

The administrator has got means to control the hardware and software configuration of the TOE (including services and assets) with respect to baseline state, or to restore it in a secure state.

Application note

This assumption especially concerns the asset D.SOFTWARES.

A.CRYPTO

The cryptographic keys, generated outside, which are injected in the TOE must have been generated by following the recommendations specified in DCSSI cryptographic referentials [CRYPTO] and [CRYPTO_GESTION] for the standard resistance level.

5. Security objectives

5.1. Security objectives for the TOE

5.1.1. Security objectives on services provided by the TOE

O.POL_ENFORCEMENT

The TOE shall enforce VPN security policies specified in IP encryptors.

O.APPLI_CONFIDENTIALITY

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

O.APPLI_AUTHENTICITY

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

O.TOPO_CONFIDENTIALITY

The TOE shall provide mechanisms to protect the confidentiality of information on the private networks topology contained in the IP packets which flow between two IP encryptors.

O.TOPO_AUTHENTICITY

The TOE shall provide mechanisms to protect the authenticity of information on the private networks topology contained in the IP packets which flow between two IP encryptors.

O.FLOW_PARTITIONING

The TOE shall provide the capability to partition IP networks interconnected together thanks to IP encryptors, by permiting creation of a new extended IP network, stacked up to the initial IP network make up of IP subnetworks. The TOE shall also provide the capability to enforce a security policy upon every communication link between IP subnetworks.

5.1.2. Security objectives to protect TOE sensitive assets

5.1.2.1. VPN security policies management

O.POL_DEFINITION

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

O.POL_PROTECTION

The TOE shall control the access (viewing, modification) of the VPN security policies and their security contexts which is authorized only to security administrators.

O.POL_VIEW

The TOE shall enable the security administrators alone to individually view VPN security policies and their security contexts upon each IP encryptor.

5.1.2.2. Cryptographic keys management

O.CRYPTO

The TOE shall implement cryptographic functions and manage (generate, destroy, renew) cryptographic keys in accordance with cryptographic referentials defined by the DCSSI ([CRYPTO] and [CRYPTO_GESTION]) for the standard resistance level.

O.KEYS_ACCESS

The TOE shall protect access to cryptographic keys.

O.KEYS_INJECTION

The TOE shall protect the confidentiality (only for secret and private keys) and integrity of keys during their injection on IP encryptors.

5.1.2.3. Configuration and supervision

O.PARAM_PROTECTION

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

O.SUPERVISION

The TOE shall enable the system and network administrator to review the operational status of each IP encryptor.

O.SUPERVISION_IMPACT

The TOE shall ensure that the supervision service does not put in danger its sensitive assets.

5.1.2.4. Audit and alarm

O.VPN_AUDIT

The TOE shall record all security-relevant operations performed by IP encryptors and concerning the communications on VPN links. Furthermore, it shall enable only an auditor to review what was logged.

O.ADMIN_AUDIT

The TOE shall record all operations performed by an administrator on IP encryptors. Furthermore, it shall enable only an auditor to review what was logged.

O.AUDIT_PROTECTION

The TOE shall ensure the integrity of recorded audit events and shall enable an auditor to detect loss of audit events (by using a counter for example).

O.ALARMS

The TOE shall generate security alarms in case of compromise to TOE sensitive assets.

O.ALARM_PROTECTION

The TOE shall ensure the integrity of security alarms (destined to security administrators) which it generates and shall enable a security administrator to detect loss of security alarms (by using a counter for example).

O.TIME_BASE

The TOE provides a time base upon which the audit records are based and ensures its reliability.

5.1.2.5. Local administration

O.ADMIN_AUTHENTICATION

The TOE shall provide the identification mechanisms and local authentication mechanisms of different administrators in conformance with the DCSSI referential [AUTH].

O.UNAVAILABLE_ASSETS

The TOE shall provide a functionality which permits to make the IP encryptor sensitive assets unavailable before a change of operational context: new assignment, maintenance...

5.2. Security objectives for the operational environment

5.2.1. Administrators

OE.ADMIN

The administrators shall be trained to the tasks which they have to perform on the TOE.

5.2.2. Cryptography

OE.CRYPTO

The cryptographic keys, generated outside, which are injected within the TOE shall be generated in accordance with the recommendations specified in DCSSI cryptographic referentials [CRYPTO] and [CRYPTO_GESTION] for the standard resistance level.

5.2.3. Audit and alarm

OE.AUDIT_ANALYSIS

The auditor shall regularly analyze audit events recorded by the TOE and react accordingly. Furthermore, the management of the memory units storing audit events must be made so that the auditor does not lose events.

OE.ALARM_PROCESS

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

5.2.4. Hardware and software

OE.PREMISE_PROTECTION

The TOE physical environment, including equipments items upon which the TOE is running, shall protect the TOE. These equipments items, as well as the supports containing all or any of the TOE sensitive assets shall be in secure premises where access is controlled and restricted to administrators.

However, equipments items containing TOE services are allowed to not be put in secure premises if they do not contain sensitive assets: for example in the cases of change of IP encryptor operational context.

OE.TOE_INTEGRITY

The TOE environment shall provide the capability to check the integrity of the TOE hardware and software configuration.

6. Security requirements

6.1. Security functional requirements

In requirements, following both terms are used to indicate a refinement:

- Editorial refinement (term defined in [CC1]): refinement where a small change is made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar. This change is not allowed to modify the meaning of the requirement in any way,
- Non-editorial refinement: refinement allowing to make a requirement more precise or to limit the scope of its acceptable implementations.

6.1.1. VPN security policies enforcement

FDP_IFC.1/Enforcement_policy Subset information flow control

FDP_IFC.1.1/Enforcement_policy The TSF shall enforce the **VPN enforcement policy** on

- **Information: applicative and topologic data contained in IP packets.**
- **Subject: IP encryptor using a given VPN link**
- **Operations: sending and receiving operations that cause applicative and topologic data to flow through the IP encryptors to and from private and public networks defined as follows:**
  - **OP.sending_public: IP packet sending to a public network,**
  - **OP.sending_private: IP packet sending to a private (sub)network,**
  - **OP.receipt_public: IP packet receipt from a public network,**
  - **OP.receipt_private: IP packet receipt from a private (sub)network**.

Non-editorial refinement:

The VPN enforcement policy is the security policy that enforces the VPN security policies on the IP packets that flow through the IP encryptor.

FDP_IFF.1/Enforcement_policy Simple security attributes

FDP_IFF.1.1/Enforcement_policy The TSF shall enforce the **VPN enforcement policy** based on the following types of subject and information security attributes:

- **Security attribute of the VPN link used by the subject IP encryptor: "AT.policy", which may hold one of the following values**
  - **"defined" if a VPN policy is associated with the VPN link used by the IP encryptor**
  - **"undefined" if no VPN policy is associated with the VPN link used by the IP encryptor**
- **[assignment: other security attributes]**.

Non-editorial refinement:

The ST author can specify other security attributes on which other rules of the VPN enforcement policy might be based.

FDP_IFF.1.2/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:

- **OP.sending_public is authorized if the security protections defined in the related VPN security policy are applied to the applicative and topologic data of IP packets before sending the IP packets to the public network.**
- **OP.sending_private is authorized if the communication with the destination subnetwork is authorized and if the security protections defined in the related VPN security policy are verified on the applicative and topologic data of IP packets before sending the IP packets to the private network.**
- **OP.receipt_public and OP.receipt_private are authorized**.

Non-editorial refinement:

The related VPN security policy can be retrieved thanks to the source and destination addresses contained in IP packets.

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

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

FDP_IFF.1.5/Enforcement_policy The TSF shall explicitly deny an information flow based on the following rules:

- **When no VPN security policy has been explicitly defined for the given VPN communication link (AT.policy is "undefined"), the default screening rule applies. This latter rule shall reject the IP packets, that is no sending is performed.**
- **When the given VPN security policy specifies that sending IP packets to the destination address (specific to a subnetwork) is forbidden, no sending is performed.**
- **When an error occurs during the application or verification of security protections, no sending of IP packets is authorized**.

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

FDP_ITC.1.1/Enforcement_policy The TSF shall enforce the **VPN enforcement policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/Enforcement_policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: additional importation control rules]**.

Non-editorial refinement:

The user data of those requirements are the IP packets, which comprise applicative and topologic data.

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

FDP_ETC.1.1/Enforcement_policy The TSF shall enforce the **VPN enforcement policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

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

Non-editorial refinement:

The user data of those requirements are the IP packets, which comprise applicative and topologic data.

FCS_COP.1/Enforcement_policy Cryptographic operation

FCS_COP.1.1/Enforcement_policy The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **DCSSI cryptographic referentials ([CRYPTO] and [CRYPTO_GESTION])**.

Non-editorial refinement:

The ST author shall specify all the cryptographic operations used to enforce the VPN security policies concerning the confidentiality and authenticity security properties.

6.1.2. VPN security policies protection

FDP_ACC.1/VPN_policy Subset access control

FDP_ACC.1.1/VPN_policy The TSF shall enforce the **VPN protection policy** on

- **Objects: VPN links and VPN security policies, where VPN security policies include VPN security contexts**
- **Subjects: IP encryptor administration component**
- **Operations:**
  - **OP.VPN_SP_definition: allows to define the VPN security policy applicable to a given VPN link**
  - **OP.VPN_SP_display: allows to display the VPN security policy of a given VPN link**.

FDP_ACF.1/VPN_policy Security attribute based access control

FDP_ACF.1.1/VPN_policy The TSF shall enforce the **VPN protection policy** to objects based on the following:

- **Security attribute of the VPN link: "AT.policy", which may hold one of the following values**
  - **"defined" if a VPN policy is associated with the VPN link**
  - **"undefined" if no VPN policy is associated with the VPN link**.

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

- **The IP encryptor administration component is allowed to define the VPN security policy of a given VPN link by means of OP.VPN_SP_definition on behalf of an authenticated security administrator. Upon completion of the operation, the attribute AT.policy of the VPN link holds the value "defined".**
- **The IP encryptor administration component is allowed to display the VPN security policy of a given VPN link by means of OP.VPN_SP_display on behalf of an authenticated security administrator**.

FDP_ACF.1.3/VPN_policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/VPN_policy The TSF shall explicitly deny access of subjects to objects based on the

- **The operation OP.VPN_SP_definition is denied to any user that has not been authenticated as a security administrator.**
- **The operation OP.VPN_SP_display is denied to any user that has not been authenticated as a security administrator.**.

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

FDP_ITC.1.1/VPN_policy The TSF shall enforce the **VPN protection policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/VPN_policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: additional importation control rules]**.

Non-editorial refinement:

The user data of those requirements are the VPN security policies.

FMT_MSA.3/VPN_policy Static attribute initialisation

FMT_MSA.3.1/VPN_policy The TSF shall enforce the **VPN protection policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/VPN_policy The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

Non-editorial refinement:

The security attribute concerned by these requirements is the attribute AT.policy that indicates for each VPN communication link if a VPN security policy and its context are defined. Its initial value is "undefined". This value is changed by the security administrator when he defines the VPN security policy and its context ("defined").

FMT_MSA.1/VPN_policy Management of security attributes

FMT_MSA.1.1/VPN_policy The TSF shall enforce the **VPN protection policy** to restrict the ability to **modify** the security attributes **AT.policy of a VPN link** to **the security administrator**.

FMT_SMF.1/VPN_policy Specification of Management Functions

FMT_SMF.1.1/VPN_policy The TSF shall be capable of performing the following management functions: **modification of the VPN link attribute AT.policy**.

6.1.3. Keys management policy

FDP_IFC.1/Key_policy Subset information flow control

FDP_IFC.1.1/Key_policy The TSF shall enforce the **key management policy** on

- **Information: cryptographic keys**
- **Subjects: IP encryptor key management component**
- **Operations:**
  - **OP.local_key_injection: allows to import within the TOE cryptographic keys generated outside the TOE**
  - **OP.key_export: allows to export TOE public keys**.

FDP_IFF.1/Key_policy Simple security attributes

FDP_IFF.1.1/Key_policy The TSF shall enforce the **key management policy** based on the following types of subject and information security attributes:

- **Security attribute of cryptographic keys: "AT.key_type", which may hold one of the following three values:**
  - **"public" applies to the public part of asymmetric cryptographic keys**
  - **"private" applies to the private part of asymmetric cryptographic keys**
  - **"secret" applies to symmetric cryptographic keys**
- **[assignment: other security attributes]**.

FDP_IFF.1.2/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:

- **The IP encryptor key management component is allowed to perform local injection of keys by means of the operation OP.local_key_injection on behalf of an authenticated local security administrator. Upon completion of the operation, the attribute AT.key_type of the injected key holds the value corresponding to the kind of key injected**.

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

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

FDP_IFF.1.5/Key_policy The TSF shall explicitly deny an information flow based on the following rules:

- **The local injection (OP.local_key_inject) of keys is denied to any user that has not been authenticated as a local security administrator**
- **The export (OP.key_export) of keys with AT.key_type equal to "private" or "secret" is denied to any user**.

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

FDP_ITC.1.1/Key_policy The TSF shall enforce the **key management policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/Key_policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: additional importation control rules]**.

Non-editorial refinement:

"User data" stands for cryptographic keys imported in the TOE.

Application note

Additional rules of import do not have to put in failure the requirements of integrity (FDP_UIT.1/Key_policy) and confidentiality (FDP_UCT.1/Key_policy).

FDP_UCT.1/Key_policy Basic data exchange confidentiality

FDP_UCT.1.1/Key_policy The TSF shall enforce the **key management policy** to be able to **receive** user data in a manner protected from unauthorised disclosure.

Non-editorial refinement:

"User data" stands for private or secret cryptographic keys injected in the TOE.

Application note

FDP_UCT.1/Key_policy requires the confidentiality of cryptographic keys injected in the TOE. The choice is left to the ST writer to specify the type of trusted channel (FTP_ITC.1) or trusted path (FTP_TRP.1) the TOE shall enforce.

FDP_UIT.1/Key_policy Data exchange integrity

FDP_UIT.1.1/Key_policy The TSF shall enforce the **key management policy** to be able to **receive** user data in a manner protected from **modification, deletion, insertion and replay** errors.

FDP_UIT.1.2/Key_policy The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

Non-editorial refinement:

"User data" stands for public, private and secret cryptographic keys injected in the TOE.

Application note

FDP_UIT.1/Key_policy requires the integrity of cryptographic keys injected in the TOE. The choice is left to the ST writer to specify the type of trusted channel (FTP_ITC.1) or trusted path (FTP_TRP.1) the TOE shall enforce.

FMT_MSA.3/Key_policy Static attribute initialisation

FMT_MSA.3.1/Key_policy The TSF shall enforce the **key management policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Key_policy The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

FCS_CKM.4/Key_policy Cryptographic key destruction

FCS_CKM.4.1/Key_policy The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **DCSSI cryptographic referentials ([CRYPTO] and [CRYPTO_GESTION])**.

FCS_CKM.3/Key_policy Cryptographic key access

FCS_CKM.3.1/Key_policy The TSF shall perform **[assignment: type of cryptographic key access]** in accordance with a specified cryptographic key access method **[assignment: cryptographic key access method]** that meets the following: **[assignment: list of standards]**.

Non-editorial refinement:

"Key access" stands for "Key renewal". The requirement reads as follows:

The TSF shall perform **key renewal** in accordance with a specified cryptographic key renewal method **[assignment: cryptographic key renewal method]** that meets the following: **DCSSI cryptographic referentials ([CRYPTO] and [CRYPTO_GESTION])**.

6.1.4. Configuration and supervision

FMT_MTD.1/Network_param Management of TSF data

FMT_MTD.1.1/Network_param The TSF shall restrict the ability to **query and modify** the **network configuration parameters** to **system and network administrators**.

FMT_MTD.1/Param Management of TSF data

FMT_MTD.1.1/Param The TSF shall restrict the ability to **modify** the **access rights and the authentication data** to **security administrators**.

FMT_SMF.1/Config_supervision Specification of Management Functions

FMT_SMF.1.1/Config_supervision The TSF shall be capable of performing the following management functions:

- **request and modification of network configuration parameters,**
- **modification of access rights and authentication data,**
- **supervision of the state of IP encryptors**.

6.1.5. TSF and TSF data protection

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **all the sensitive data (VPN security policies and their contexts, cryptographic keys, configuration parameters, audit events and security alarms)**.

6.1.6. Audit and alarms

FAU_GEN.1/VPN Audit data generation

FAU_GEN.1.1/VPN 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 **basic** level of audit; and

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

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **information that make possible to detect a loss of an audit record (like a counter), [assignment: other audit relevant information]**.

Non-editorial refinement:

The subject identity corresponds to the identity of the IP packets' recipient and sender (respectively destination IP address and source IP address).

The audit events considered in those requirements focus on the VPN communication links between IP encryptors.

FAU_GEN.1/Administration Audit data generation

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

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

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

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

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

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

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

Non-editorial refinement:

The audit events considered in those requirements are related to the administration operations.

FAU_SAR.1 Audit review

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

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

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **[assignment: methods of selection and/or ordering]** of audit data based on **[assignment: criteria with logical relations]**.

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

FAU_ARP.1/Alarm Security alarms

FAU_ARP.1.1/Alarm The TSF shall take **the following actions:**

- **a security alarm is raised to the security administrator,**
- **[assignment: list of the other least disruptive actions]** upon detection of a potential security violation.

Non-editorial refinement:

The ST author can specify other least disruptive actions by completing the assignment.

FAU_SAA.1/Alarm Potential violation analysis

FAU_SAA.1.1/Alarm The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

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

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

b) **overflow of the audit trail capacity,**

c) [assignment: any other rules].

FPT_STM.1 Reliable time stamps

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

Non-editorial refinement:

TSF provides reliable time stamps for its own use.

6.1.7. Roles and authentication

FMT_SMR.1 Security roles

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

- **security administrator,**
- **system and network administrator,**
- **auditor**.

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

Application note

The same person can be associated to several roles. In the case of the IP encryptor, the same person could be at the same moment the security administrator and the system and network administrator for example.

FIA_UID.2 User identification before any action

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

FIA_UAU.2 User authentication before any action

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

Non-editorial refinement:

The authentication mechanism shall be conformant with the DCSSI referential [AUTH].

6.2. Security assurance requirements

The security assurance requirements level is EAL3 augmented by ALC_FLR.3 and AVA_VAN.3.

7. Rationales

7.1. Security objectives / security problem

7.1.1. Threats

7.1.1.1. Threats concerning VPN security policies and their contexts

T.POL_MODIFICATION

This threat is countered by O.POL_DEFINITION, O.POL_PROTECTION and O.ADMIN_AUTHENTICATION which enforce that VPN security policies and their contexts can only be modified by security administrators authenticated as such.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.
- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.
- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.POL_DISCLOSURE

This threat is countered by O.POL_DEFINITION, O.POL_PROTECTION O.ADMIN_AUTHENTICATION and O.POL_VIEW which enforce that VPN security policies and their contexts can only be consulted/viewed by security administrators authenticated as such.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.
- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.
- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

7.1.1.2. Threats concerning the configuration

T.PARAM_MODIFICATION

O.PARAM_PROTECTION counters this threat by protecting the integrity of configuration parameters. This objective and O.ADMIN_AUTHENTICATION enable to ensure that only system and network administrators and security administrators authenticated as such can access these parameters.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.
- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.
- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.PARAM_DISCLOSURE

The objective O.PARAM_PROTECTION counters this threat by protecting the confidentiality of configuration parameters. The objectives O.SUPERVISION and O.ADMIN_AUTHENTICATION enable ascertaining that only system and network administrators and security administrators authenticated as such can access these parameters.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.
- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.
- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

7.1.1.3. Threats concerning the keys management

T.KEYS_MODIFICATION

This threat is countered by O.KEYS_INJECTION during the keys injection in cipher units, because this objective ensures the integrity protection of keys during their injection. Furthermore, the objectives O.KEYS_INJECTION and O.ADMIN_AUTHENTICATION ensure that only security administrators authenticated as such can inject keys. This threat is also countered by O.KEYS_ACCESS which protects the logical access to keys.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.
- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.
- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.KEYS_DISCLOSURE

This threat is countered by O.KEYS_INJECTION during the keys injection in cipher units, because this objective ensures the confidentiality protection of keys during their injection. Furthermore, the objectives O.KEYS_INJECTION and O.ADMIN_AUTHENTICATION ensure that only security administrators authenticated as such can inject keys. This threat is also countered by O.KEYS_ACCESS which protects the logical access to keys. Finally, this threat is countered by O.CRYPTO which ensures a regular keys renewal and therefore makes more difficult the use of revealed keys.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.
- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.
- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

7.1.1.4. Threats concerning the audit

T.AUDIT_MODIFICATION

This threat is countered by O.AUDIT_PROTECTION and O.ADMIN_AUTHENTICATION which enforce that audit events recordings can be deleted only by auditors authenticated as such.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.
- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.
- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.ALARM_MODIFICATION

This threat is countered by O.ALARM_PROTECTION and O.ADMIN_AUTHENTICATION which enforce that security alarms are only accessible to a security administrator and that they are protected in integrity.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.
- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.TIME_BASE

This threat is covered by the objective O.TIME_BASE which ensures the time base reliability.

7.1.1.5. Threats concerning the administration

T.ADMIN_USURPATION

This threat is countered by O.ADMIN_AUTHENTICATION, because this objective enforces the authentication of different administrators before performing any administration operation.

The following objectives also contribute to the threat coverage:

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

T.UNAVAILABLE_ASSETS

This threat is covered by O.UNAVAILABLE_ASSETS, because it enforces that the TOE provides a functionality which permits to do the TOE sensitive assets unavailable during a change of operational context. Furthermore, this threat is covered by OE.PREMISE_PROTECTION, because it enforces that TOE equipments items are placed in a secure premise when they contain sensitive assets.

7.1.2. Organisational security policies (OSP)

OSP.PROVIDED_SERVICES

This OSP is covered by O.APPLI_CONFIDENTIALITY, O.APPLI_AUTHENTICITY, O.TOPO_CONFIDENTIALITY and O.TOPO_AUTHENTICITY which enforce that the TOE provides security services. It is also covered by O.POL_ENFORCEMENT and O.FLOW_PARTITIONING which enforce that these security services are enforced and provide the capability to partition IP flows.

O.VPN_AUDIT and O.ALARMS cover this OSP, because they ensure that operations concerning VPN links are logged and that security alarms are generated to indicate operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

This OSP is covered by OE.TOE_INTEGRITY, because it ensures that the integrity of the software code which enforce VPN security policies can be checked.

OSP.CRYPTO

This OSP is covered by O.CRYPTO and OE.CRYPTO.

OSP.POL_VIEW

This OSP is covered by O.POL_VIEW, because it provides the viewing of VPN security policies on an individual basis, that permits a security administrator to visually check that he defined correctly every VPN security policy.

OSP.SUPERVISION

This OSP is covered by O.SUPERVISION.

7.1.3. Assumptions

7.1.3.1. Assumptions on the intended usage of the TOE

A.AUDIT

This assumption is upheld by OE.AUDIT_ANALYSIS.

A.ALARM

This assumption is upheld by OE.ALARM_PROCESS.

7.1.3.2. Assumptions on the TOE operational environment

A.ADMIN

This assumption is upheld by OE.ADMIN which enforces the training of administrators on their tasks.

A.PREMISE

This assumption is upheld by OE.PREMISE_PROTECTION, because it enforces that TOE equipments items as well as the supports containing TOE sensitive assets are in a secure premises.

A.CONFIGURATION_CONTROL

This assumption is upheld by OE.TOE_INTEGRITY.

A.CRYPTO

This assumption is upheld by OE.CRYPTO.

7.1.4. Coverage between problem definition and security objectives

Threats	Security objectives	Rationale
T.POL_MODIFICATION	O.POL_DEFINITION, O.SUPERVISION_IMPACT, O.POL_PROTECTION, O.ADMIN_AUTHENTICATION, O.ADMIN_AUDIT, O.ALARMS, OE.TOE_INTEGRITY	Section 7.1.1
T.POL_DISCLOSURE	O.POL_DEFINITION, O.SUPERVISION_IMPACT, O.POL_PROTECTION, O.ADMIN_AUTHENTICATION, O.ADMIN_AUDIT, O.ALARMS, OE.TOE_INTEGRITY, O.POL_VIEW	Section 7.1.1
T.PARAM_MODIFICATION	O.PARAM_PROTECTION, O.SUPERVISION_IMPACT, O.ADMIN_AUTHENTICATION, O.ADMIN_AUDIT, O.ALARMS, OE.TOE_INTEGRITY	Section 7.1.1
T.PARAM_DISCLOSURE	O.PARAM_PROTECTION, O.SUPERVISION_IMPACT, O.ADMIN_AUTHENTICATION, O.ADMIN_AUDIT, O.ALARMS, OE.TOE_INTEGRITY, O.SUPERVISION	Section 7.1.1
T.KEYS_MODIFICATION	O.KEYS_ACCESS, O.KEYS_INJECTION, O.SUPERVISION_IMPACT, O.ADMIN_AUTHENTICATION, O.ADMIN_AUDIT, O.ALARMS, OE.TOE_INTEGRITY	Section 7.1.1
T.KEYS_DISCLOSURE	O.KEYS_INJECTION, O.KEYS_ACCESS, O.SUPERVISION_IMPACT, O.ADMIN_AUTHENTICATION, O.ADMIN_AUDIT, O.ALARMS, OE.TOE_INTEGRITY, O.CRYPTO	Section 7.1.1
T.AUDIT_MODIFICATION	O.SUPERVISION_IMPACT, O.AUDIT_PROTECTION, O.ADMIN_AUTHENTICATION, OE.TOE_INTEGRITY, O.ADMIN_AUDIT, O.ALARMS	Section 7.1.1
T.ALARM_MODIFICATION	O.SUPERVISION_IMPACT, O.ALARM_PROTECTION, O.ADMIN_AUTHENTICATION, OE.TOE_INTEGRITY, O.ADMIN_AUDIT, O.ALARMS	Section 7.1.1
T.TIME_BASE	O.TIME_BASE	Section 7.1.1

Threats	Security objectives	Rationale
T.ADMIN_USURPATION	O.ADMIN_AUTHENTICATION, O.ADMIN_AUDIT, O.ALARMS	Section 7.1.1
T.UNAVAILABLE_ASSETS	O.UNAVAILABLE_ASSETS, OE.PREMISE_PROTECTION	Section 7.1.1

Table 1 Mapping threats to security objectives

Security objectives	Threats
O.POL_ENFORCEMENT	
O.APPLI_CONFIDENTIALITY	
O.APPLI_AUTHENTICITY	
O.TOPO_CONFIDENTIALITY	
O.TOPO_AUTHENTICITY	
O.FLOW_PARTITIONING	
O.POL_DEFINITION	T.POL_MODIFICATION, T.POL_DISCLOSURE
O.POL_PROTECTION	T.POL_MODIFICATION, T.POL_DISCLOSURE
O.POL_VIEW	T.POL_DISCLOSURE
O.CRYPTO	T.KEYS_DISCLOSURE
O.KEYS_ACCESS	T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE
O.KEYS_INJECTION	T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE
O.PARAM_PROTECTION	T.PARAM_MODIFICATION, T.PARAM_DISCLOSURE
O.SUPERVISION	T.PARAM_DISCLOSURE
O.SUPERVISION_IMPACT	T.POL_MODIFICATION, T.POL_DISCLOSURE, T.PARAM_MODIFICATION, T.PARAM_DISCLOSURE, T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE, T.AUDIT_MODIFICATION, T.ALARM_MODIFICATION
O.VPN_AUDIT	
O.ADMIN_AUDIT	T.POL_MODIFICATION, T.POL_DISCLOSURE, T.PARAM_MODIFICATION, T.PARAM_DISCLOSURE, T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE, T.AUDIT_MODIFICATION, T.ALARM_MODIFICATION, T.ADMIN_USURPATION
O.AUDIT_PROTECTION	T.AUDIT_MODIFICATION

Security objectives	Threats
O.ALARMS	T.POL_MODIFICATION, T.POL_DISCLOSURE, T.PARAM_MODIFICATION, T.PARAM_DISCLOSURE, T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE, T.AUDIT_MODIFICATION, T.ALARM_MODIFICATION, T.ADMIN_USURPATION
O.ALARM_PROTECTION	T.ALARM_MODIFICATION
O.TIME_BASE	T.TIME_BASE
O.ADMIN_AUTHENTICATION	T.POL_MODIFICATION, T.POL_DISCLOSURE, T.PARAM_MODIFICATION, T.PARAM_DISCLOSURE, T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE, T.AUDIT_MODIFICATION, T.ALARM_MODIFICATION, T.ADMIN_USURPATION
O.UNAVAILABLE_ASSETS	T.UNAVAILABLE_ASSETS
OE.ADMIN	
OE.CRYPTO	
OE.AUDIT_ANALYSIS	
OE.ALARM_PROCESS	
OE.PREMISE_PROTECTION	T.UNAVAILABLE_ASSETS
OE.TOE_INTEGRITY	T.POL_MODIFICATION, T.POL_DISCLOSURE, T.PARAM_MODIFICATION, T.PARAM_DISCLOSURE, T.KEYS_MODIFICATION, T.KEYS_DISCLOSURE, T.AUDIT_MODIFICATION, T.ALARM_MODIFICATION

Table 2 Mapping security objectives to threats

Organisational security policies (OSP)	Security objectives	Rationale
OSP.PROVIDED_SERVICES	O.POL_ENFORCEMENT, O.APPLI_CONFIDENTIALITY, O.APPLI_AUTHENTICITY, O.TOPO_CONFIDENTIALITY, O.TOPO_AUTHENTICITY, O.FLOW_PARTITIONING, O.VPN_AUDIT, OE.TOE_INTEGRITY, O.ALARMS	Section 7.1.2
OSP.CRYPTO	O.CRYPTO, OE.CRYPTO	Section 7.1.2
OSP.POL_VIEW	O.POL_VIEW	Section 7.1.2
OSP.SUPERVISION	O.SUPERVISION	Section 7.1.2

Table 3 Mapping organisational security policies to security objectives

Security objectives	Organisational security policies (OSP)
O.POL_ENFORCEMENT	OSP.PROVIDED_SERVICES
O.APPLI_CONFIDENTIALITY	OSP.PROVIDED_SERVICES
O.APPLI_AUTHENTICITY	OSP.PROVIDED_SERVICES
O.TOPO_CONFIDENTIALITY	OSP.PROVIDED_SERVICES
O.TOPO_AUTHENTICITY	OSP.PROVIDED_SERVICES
O.FLOW_PARTITIONING	OSP.PROVIDED_SERVICES
O.POL_DEFINITION	
O.POL_PROTECTION	
O.POL_VIEW	OSP.POL_VIEW
O.CRYPTO	OSP.CRYPTO
O.KEYS_ACCESS	
O.KEYS_INJECTION	
O.PARAM_PROTECTION	
O.SUPERVISION	OSP.SUPERVISION
O.SUPERVISION_IMPACT	
O.VPN_AUDIT	OSP.PROVIDED_SERVICES
O.ADMIN_AUDIT	
O.AUDIT_PROTECTION	
O.ALARMS	OSP.PROVIDED_SERVICES
O.ALARM_PROTECTION	
O.TIME_BASE	
O.ADMIN_AUTHENTICATION	
O.UNAVAILABLE_ASSETS	
OE.ADMIN	
OE.CRYPTO	OSP.CRYPTO
OE.AUDIT_ANALYSIS	
OE.ALARM_PROCESS	
OE.PREMISE_PROTECTION	
OE.TOE_INTEGRITY	OSP.PROVIDED_SERVICES

Table 4 Mapping security objectives to organisational security policies

Assumptions	Security objectives for the operational environment	Rationale
A.AUDIT	OE.AUDIT_ANALYSIS	Section 7.1.3
A.ALARM	OE.ALARM_PROCESS	Section 7.1.3
A.ADMIN	OE.ADMIN	Section 7.1.3
A.PREMISE	OE.PREMISE_PROTECTION	Section 7.1.3
A.CONFIGURATION_CONTROL	OE.TOE_INTEGRITY	Section 7.1.3
A.CRYPTO	OE.CRYPTO	Section 7.1.3

Table 5 Mapping assumptions to security objectives for the operational environment

Security objectives for the operational environment	Assumptions
OE.ADMIN	A.ADMIN
OE.CRYPTO	A.CRYPTO
OE.AUDIT_ANALYSIS	A.AUDIT
OE.ALARM_PROCESS	A.ALARM
OE.PREMISE_PROTECTION	A.PREMISE
OE.TOE_INTEGRITY	A.CONFIGURATION_CONTROL

Table 6 Mapping security objectives for the operational environment to assumptions

7.2. Security requirements / security objectives

7.2.1. Objectives

7.2.1.1. Security objectives for the TOE

7.2.1.1.1. Security objectives on services provided by the TOE

O.POL_ENFORCEMENT

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

O.APPLI_CONFIDENTIALITY

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

O.APPLI_AUTHENTICITY

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

O.TOPO_CONFIDENTIALITY

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

O.TOPO_AUTHENTICITY

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

O.FLOW_PARTITIONING

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

7.2.1.1.2. Security objectives to protect TOE sensitive assets

7.2.1.1.2.1 VPN security policies management

O.POL_DEFINITION

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

O.POL_PROTECTION

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

O.POL_VIEW

This objective is covered by the protection policy of VPN security policies (FDP_ACC.1/VPN_policy and FDP_ACF.1/VPN_policy) by controling access to the action allowing review of VPN security policies and of their contexts.

7.2.1.1.2.2 Cryptographic keys management

O.CRYPTO

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

- cryptographic operations: FCS_COP.1/Enforcement_policy,
- keys renewal: FCS_CKM.3/Key_policy,
- keys destruction: FCS_CKM.4/Key_policy.

O.KEYS_ACCESS

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

O.KEYS_INJECTION

This objective is covered by the keys policy (FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FDP_ITC.1/Key_policy and FMT_MSA.3/Key_policy) which controls keys flows of keys injection. In addition, FDP_UCT.1/Key_policy and FDP_UIT.1/Key_policy ensure the integrity of all keys and the confidentiality of private and secret keys during their transmission.

7.2.1.1.2.3 Configuration and supervision

O.PARAM_PROTECTION

This objective is covered by FMT_MTD.1/Network_param (for network configuration parameters), FMT_MTD.1/Param (for access rights and authentication data), and FMT_SMF.1/Config_supervision, because these requirements ensure the confidentiality and integrity protection of configuration parameters by restricting access to operations which manipulate these parameters.

O.SUPERVISION

This objective is covered by FMT_SMF.1/Config_supervision, because this requirement requires a supervision function of the IP encryptors state.

O.SUPERVISION_IMPACT

This objective is covered by all access controls policies and information flow policies concerning TOE sensitive assets by restricting access to operations handling these assets: FDP_ACC.1/VPN_policy, FDP_ACF.1/VPN_policy, FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FDP_IFC.1/Enforcement_policy and FDP_IFF.1/Enforcement_policy. Furthermore, for the same reasons this objective is covered by all requirements concerning the TSF data management: FMT_MTD.1/Network_param and FMT_MTD.1/Param.

7.2.1.1.2.4 Audit and alarm

O.VPN_AUDIT

This objective is covered by FAU_GEN.1/VPN which ensures the generation of audit events for VPN communication links. Furthermore, this objective is also covered by FAU_SAR.1 and FAU_SAR.3 which provide the capability to review audit events.

O.ADMIN_AUDIT

This objective is covered by FAU_GEN.1/Administration which ensures the generation of audit events concerning administration operations. Furthermore, this objective is also covered by FAU_SAR.1 and FAU_SAR.3 which provide the capability to review audit events.

O.AUDIT_PROTECTION

This objective is covered by FAU_STG.1 which protects audit events recordings integrity. Furthermore, FAU_GEN.1/VPN and FAU_GEN.1/Administration provide the capability to detect the loss of audit events.

O.ALARMS

This objective is covered by FAU_ARP.1/Alarm which requires to raise a security alarm when a potential security violation is detected and by FAU_SAA.1/Alarm which indicates rules used to detect these potential violations.

O.ALARM_PROTECTION

This objective is covered by FAU_STG.1 which protects security alarms recordings integrity. Furthermore, FAU_GEN.1/VPN and FAU_GEN.1/Administration provide the capability to detect the loss of security alarms.

O.TIME_BASE

This objective is directly covered by the requirement FPT_STM.1.

7.2.1.1.2.5 Local administration

O.ADMIN_AUTHENTICATION

This objective is covered by FIA_UID.2 and FIA_UAU.2 which requires users identification and authentication before performing any local administration operation. Furthermore, this objective is covered by FMT_SMR.1 which requires for the preservation of different roles by the TOE.

O.UNAVAILABLE_ASSETS

This objective is covered by FDP_RIP.1, because this requirement ensures that the TOE provides the capability to make unavailable contents of resources corresponding to TOE sensitive assets. Furthermore, this objective is covered by FCS_CKM.4/Key_policy, because this requirement imposes that the TOE can destroy its cryptographic keys.

7.2.2. Coverage between objectives and security requirements

Security objectives	Functional requirements for the TOE	Rationale
O.POL_ENFORCEMENT	FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy, FDP_ITC.1/Enforcement_policy, FDP_ETC.1/Enforcement_policy, FCS_COP.1/Enforcement_policy	Section 7.2.1
O.APPLI_CONFIDENTIALITY	FCS_COP.1/Enforcement_policy	Section 7.2.1
O.APPLI_AUTHENTICITY	FCS_COP.1/Enforcement_policy	Section 7.2.1
O.TOPO_CONFIDENTIALITY	FCS_COP.1/Enforcement_policy	Section 7.2.1
O.TOPO_AUTHENTICITY	FCS_COP.1/Enforcement_policy	Section 7.2.1
O.FLOW_PARTITIONING	FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy, FDP_ETC.1/Enforcement_policy	Section 7.2.1
O.POL_DEFINITION	FDP_ACC.1/VPN_policy, FDP_ACF.1/VPN_policy, FMT_MSA.3/VPN_policy, FMT_MSA.1/VPN_policy, FMT_SMF.1/VPN_policy, FDP_ITC.1/VPN_policy	Section 7.2.1
O.POL_PROTECTION	FDP_ACC.1/VPN_policy, FDP_ACF.1/VPN_policy, FMT_MSA.3/VPN_policy, FMT_MSA.1/VPN_policy, FMT_SMF.1/VPN_policy	Section 7.2.1
O.POL_VIEW	FDP_ACC.1/VPN_policy, FDP_ACF.1/VPN_policy	Section 7.2.1
O.CRYPTO	FCS_COP.1/Enforcement_policy, FCS_CKM.4/Key_policy, FCS_CKM.3/Key_policy	Section 7.2.1
O.KEYS_ACCESS	FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FMT_MSA.3/Key_policy	Section 7.2.1
O.KEYS_INJECTION	FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FMT_MSA.3/Key_policy, FDP_UCT.1/Key_policy, FDP_UIT.1/Key_policy, FDP_ITC.1/Key_policy	Section 7.2.1
O.PARAM_PROTECTION	FMT_MTD.1/Network_param, FMT_MTD.1/Param, FMT_SMF.1/Config_supervision	Section 7.2.1
O.SUPERVISION	FMT_SMF.1/Config_supervision	Section 7.2.1

Security objectives	Functional requirements for the TOE	Rationale
O.SUPERVISION_IMPACT	FDP_ACC.1/VPN_policy, FDP_ACF.1/VPN_policy, FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FMT_MTD.1/Network_param, FMT_MTD.1/Param, FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy	Section 7.2.1
O.VPN_AUDIT	FAU_GEN.1/VPN, FAU_SAR.1, FAU_SAR.3	Section 7.2.1
O.ADMIN_AUDIT	FAU_GEN.1/Administration, FAU_SAR.1, FAU_SAR.3	Section 7.2.1
O.AUDIT_PROTECTION	FAU_STG.1, FAU_GEN.1/VPN, FAU_GEN.1/Administration	Section 7.2.1
O.ALARMS	FAU_ARP.1/Alarm, FAU_SAA.1/Alarm	Section 7.2.1
O.ALARM_PROTECTION	FAU_STG.1, FAU_GEN.1/VPN, FAU_GEN.1/Administration	Section 7.2.1
O.TIME_BASE	FPT_STM.1	Section 7.2.1
O.ADMIN_AUTHENTICATION	FMT_SMR.1, FIA_UID.2, FIA_UAU.2	Section 7.2.1
O.UNAVAILABLE_ASSETS	FDP_RIP.1, FCS_CKM.4/Key_policy	Section 7.2.1

Table 7 Mapping security objectives for the TOE to functional requirements

Functional requirements for the TOE	Security objectives
FDP_IFC.1/Enforcement_policy	O.POL_ENFORCEMENT, O.FLOW_PARTITIONING, O.SUPERVISION_IMPACT
FDP_IFF.1/Enforcement_policy	O.POL_ENFORCEMENT, O.FLOW_PARTITIONING, O.SUPERVISION_IMPACT
FDP_ITC.1/Enforcement_policy	O.POL_ENFORCEMENT
FDP_ETC.1/Enforcement_policy	O.POL_ENFORCEMENT, O.FLOW_PARTITIONING
FCS_COP.1/Enforcement_policy	O.POL_ENFORCEMENT, O.APPLI_CONFIDENTIALITY, O.APPLI_AUTHENTICITY, O.TOPO_CONFIDENTIALITY, O.TOPO_AUTHENTICITY, O.CRYPTO
FDP_ACC.1/VPN_policy	O.POL_DEFINITION, O.POL_PROTECTION, O.POL_VIEW, O.SUPERVISION_IMPACT
FDP_ACF.1/VPN_policy	O.POL_DEFINITION, O.POL_PROTECTION, O.POL_VIEW, O.SUPERVISION_IMPACT
FDP_ITC.1/VPN_policy	O.POL_DEFINITION
FMT_MSA.3/VPN_policy	O.POL_DEFINITION, O.POL_PROTECTION
FMT_MSA.1/VPN_policy	O.POL_DEFINITION, O.POL_PROTECTION
FMT_SMF.1/VPN_policy	O.POL_DEFINITION, O.POL_PROTECTION
FDP_IFC.1/Key_policy	O.KEYS_ACCESS, O.KEYS_INJECTION, O.SUPERVISION_IMPACT
FDP_IFF.1/Key_policy	O.KEYS_ACCESS, O.KEYS_INJECTION, O.SUPERVISION_IMPACT
FDP_ITC.1/Key_policy	O.KEYS_INJECTION
FDP_UCT.1/Key_policy	O.KEYS_INJECTION
FDP_UIT.1/Key_policy	O.KEYS_INJECTION
FMT_MSA.3/Key_policy	O.KEYS_ACCESS, O.KEYS_INJECTION
FCS_CKM.4/Key_policy	O.UNAVAILABLE_ASSETS, O.CRYPTO
FCS_CKM.3/Key_policy	O.CRYPTO
FMT_MTD.1/Network_param	O.PARAM_PROTECTION, O.SUPERVISION_IMPACT

Functional requirements for the TOE	Security objectives
FMT_MTD.1/Param	O.PARAM_PROTECTION, O.SUPERVISION_IMPACT
FMT_SMF.1/Config_supervision	O.PARAM_PROTECTION, O.SUPERVISION
FDP_RIP.1	O.UNAVAILABLE_ASSETS
FAU_GEN.1/VPN	O.VPN_AUDIT, O.AUDIT_PROTECTION, O.ALARM_PROTECTION
FAU_GEN.1/Administration	O.ADMIN_AUDIT, O.AUDIT_PROTECTION, O.ALARM_PROTECTION
FAU_SAR.1	O.VPN_AUDIT, O.ADMIN_AUDIT
FAU_SAR.3	O.VPN_AUDIT, O.ADMIN_AUDIT
FAU_STG.1	O.AUDIT_PROTECTION, O.ALARM_PROTECTION
FAU_ARP.1/Alarm	O.ALARMS
FAU_SAA.1/Alarm	O.ALARMS
FPT_STM.1	O.TIME_BASE
FMT_SMR.1	O.ADMIN_AUTHENTICATION
FIA_UID.2	O.ADMIN_AUTHENTICATION
FIA_UAU.2	O.ADMIN_AUTHENTICATION

Table 8 Mapping functional requirements to security objectives for the TOE

7.3. Dependencies

7.3.1. Security functional requirements dependencies

Requirements	CC dependencies	Satisfied dependencies
FDP_IFC.1/Enforcement_policy	(FDP_IFF.1)	FDP_IFF.1/Enforcement_policy
FDP_IFF.1/Enforcement_policy	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ITC.1/Enforcement_policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ETC.1/Enforcement_policy	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/Enforcement_policy
FCS_COP.1/Enforcement_policy	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/Key_policy, FDP_ITC.1/Key_policy
FDP_ACC.1/VPN_policy	(FDP_ACF.1)	FDP_ACF.1/VPN_policy
FDP_ACF.1/VPN_policy	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/VPN_policy, FMT_MSA.3/VPN_policy
FDP_ITC.1/VPN_policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/VPN_policy, FMT_MSA.3/VPN_policy
FMT_MSA.3/VPN_policy	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/VPN_policy, FMT_SMR.1
FMT_MSA.1/VPN_policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/VPN_policy, FMT_SMF.1/VPN_policy, FMT_SMR.1
FMT_SMF.1/VPN_policy	No dependency	
FDP_IFC.1/Key_policy	(FDP_IFF.1)	FDP_IFF.1/Key_policy
FDP_IFF.1/Key_policy	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Key_policy, FMT_MSA.3/Key_policy
FDP_ITC.1/Key_policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Key_policy, FMT_MSA.3/Key_policy
FDP_UCT.1/Key_policy	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/Key_policy
FDP_UIT.1/Key_policy	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/Key_policy

Requirements	CC dependencies	Satisfied dependencies
FMT_MSA.3/Key_policy	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1
FCS_CKM.4/Key_policy	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1/Key_policy
FCS_CKM.3/Key_policy	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/Key_policy, FDP_ITC.1/Key_policy
FMT_MTD.1/Network_param	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1
FMT_MTD.1/Param	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1
FMT_SMF.1/Config_supervision	No dependency	
FDP_RIP.1	No dependency	
FAU_GEN.1/VPN	(FPT_STM.1)	FPT_STM.1
FAU_GEN.1/Administration	(FPT_STM.1)	FPT_STM.1
FAU_SAR.1	(FAU_GEN.1)	FAU_GEN.1/VPN, FAU_GEN.1/Administration
FAU_SAR.3	(FAU_SAR.1)	FAU_SAR.1
FAU_STG.1	(FAU_GEN.1)	FAU_GEN.1/VPN, FAU_GEN.1/Administration
FAU_ARP.1/Alarm	(FAU_SAA.1)	FAU_SAA.1/Alarm
FAU_SAA.1/Alarm	(FAU_GEN.1)	FAU_GEN.1/VPN, FAU_GEN.1/Administration
FPT_STM.1	No dependency	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	No dependency	
FIA_UAU.2	(FIA_UID.1)	FIA_UID.2

Table 9 Functional requirements dependencies

7.3.1.1. Rationale for unsatisfied dependencies

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/Key_policy is not satisfied. FDP_UCT.1/Key_policy requires confidentiality of cryptographic keys imported in the TOE. This Protection Profile lets the developper select the type of trusted channel (FTP_ITC.1 or FTP_TRP.1) which the TOE shall implement.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/Key_policy is not satisfied. FDP_UCT.1/Key_policy requires integrity of cryptographic keys imported in the

TOE. This Protection Profile lets the developper select the type of trusted channel (FTP_ITC.1 or FTP_TRP.1) which the TOE shall implement.

The dependency FMT_MSA.1 of FMT_MSA.3/Key_policy is not satisfied. The security attribute AT.key_type has only the reviewing operation which is only provided for TSF. As this operation is not provided for a given role, this dependency is not satisfied.

7.3.2. Security assurance requirements dependencies

Requirements	CC dependencies	Satisfied dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.3, ADV_TDS.2
ADV_FSP.3	(ADV_TDS.1)	ADV_TDS.2
ADV_TDS.2	(ADV_FSP.3)	ADV_FSP.3
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.3
AGD_PRE.1	No dependency	
ALC_CMC.3	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	No dependency	
ALC_DEL.1	No dependency	
ALC_FLR.3	No dependency	
ALC_DVS.1	No dependency	
ALC_LCD.1	No dependency	
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependency	
ASE_INT.1	No dependency	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependency	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.3, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.3, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1

Requirements	CC dependencies	Satisfied dependencies
AVA_VAN.3	(ADV_ARC.1) and (ADV_FSP.2) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.3, AGD_OPE.1, AGD_PRE.1

Table 10 Assurance requirements dependencies

7.3.2.1. Rationale for unsatisfied dependencies

The dependency ADV_IMP.1 of AVA_VAN.3 is not satisfied. This dependency is not necessary in conformance with the EAL required for the standard qualification [QUA-STD].

The dependency ADV_TDS.3 of AVA_VAN.3 is not satisfied. This dependency is not necessary in conformance with the EAL required for the standard qualification [QUA-STD].

7.4. Rationale for the EAL

The assurance level of this PP is EAL3 +, because it is required by the standard qualification process [QUA-STD].

7.5. Rationale for the EAL augmentations

7.5.1. ALC_FLR.3 Systematic flaw remediation

Augmentation required by the standard qualification process [QUA-STD].

7.5.2. AVA_VAN.3 Focused vulnerability analysis

Augmentation required by the standard qualification process [QUA-STD].

A Application notes

As explained in the introduction of this protection profile, these application notes define elements (threats, assumptions, OSP, objectives and requirements) specific to each of the two options. Elements which are defined in these notes must either be added to the profile, or replace elements already existing for the minimal configuration. In this latter case, element identifiers which are used in these notes are those used for the minimal configuration.

The first section concerns elements for remote administration option, the second for dynamic negotiation option. Finally, the third section introduces rationale for the maximal configuration covering both options.

A.1 Option « remote administration »

A.1.1 TOE description

IP encryptors can be also remotely administered: it is an administration which is performed through a LAN or WAN network.

VPN security policies distribution

After VPN security policies have been defined, they are distributed to concerned IP encryptors with their security contexts. The consistency between the policy defined by the security administrator through the use of a tool and the one existing inside the concerned IP encryptor must be ensured so that the protection of data circulating on VPN links is indeed the one expected and defined by the security administrator. This policy definition tool shall ensure the reliability of the translation between the language used by the security administrator to define the policy (by using the tool) and the language used in IP encryptors to enforce these policies.

A secure channel must be used to distribute VPN security policies and their security contexts in order to protect their authenticity and confidentiality.

Remote administration flows protection

This service provides the capability to protect the authenticity of dataflows exchanged between IP encryptors and administration equipments to perform remote administration operations. This service also provides the capability to protect the confidentiality of administration flows. This protection concerns security administration flows (VPN security policies and keys) and system and network administration flows (configuration parameters). On the other hand, this service does not apply this protection to supervision flows. This service is divided into two parts which are both included in the TOE: one on IP encryptors and the other one on administration equipments.

Protection against administration flows replay

This service protects against replay of remote administration operations sequences flowing through links between IP encryptors and administration equipments.

A.1.2 Security environment

A.1.2.1 Threats

T.POL_CONSISTENCY

An attacker modifies the VPN security policy enforced at the IP subnetwork level, which is therefore different from the one defined by the security administrator for this subnetwork.

Threatened asset: D.VPN_POLICIES.

T.ADMIN_REPLAY

An attacker captures a packets sequence within an administration flow, corresponding to a complete sequence to perform an administration operation, and replays it in order to gain a certain benefit.

Threatened assets: all assets.

A.1.3 Security objectives

A.1.3.1 Security objectives for the TOE

O.POL_CONSISTENCY

The TOE shall ensure the consistency between VPN security policies definitions (and their contexts) and policies enforced on each IP encryptor during the remote administration.

O.POL_DISTRIBUTION

The TOE shall protect the confidentiality and authenticity of VPN security policies and their security contexts which flow through equipment items containing the software which provide the capability to define them and IP encryptors.

O.ADMIN_REPLAY_PROTECTION

The TOE shall prevent the replay of any previously sent sequence of administration data.

O.ADMIN_FLOWS_PROTECTION

The TOE shall ensure the authenticity and confidentiality of remote administration flows. Confidentiality protection is not systematically enforced if data transfered through the flow are not confidential such as public keys.

A.1.3.2 Security objectives for the environment

OE.ADMIN_AUTHENTICATION

The TOE environment shall provide identification and remote authentication mechanisms for different administrators. It shall also ensure that remote administration services access is allowed under the condition of a preliminary authentication on the administration station.

A.1.4 Security functional requirements for the TOE

FPT_TRC.1/VPN_policy Internal TSF consistency

FPT_TRC.1.1/VPN_policy The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2/VPN_policy When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for **[assignment: list of SFs dependent on TSF data replication consistency]**.

Non-editorial refinement:

The TSF data concerned are the VPN security policies and their contexts.

FDP_ACC.1/VPN_policy Subset access control

FDP_ACC.1.1/VPN_policy The TSF shall enforce the **VPN protection policy** on

- **Objects: VPN links and VPN security policies, where VPN security policies include VPN security contexts**
- **Subjects: IP encryptor administration component**
- **Operations:**
  - **OP.VPN_SP_definition: allows to define the VPN security policy applicable to a given VPN link**
  - **OP.VPN_SP_display: allows to display the VPN security policy of a given VPN link.**
  - **OP.VPN_SP_distribution: allows to distribute the VPN security policy of a given VPN link**

FDP_ACF.1/VPN_policy Security attribute based access control

FDP_ACF.1.1/VPN_policy The TSF shall enforce the **VPN protection policy** to objects based on the following:

- **Security attribute of the VPN link: "AT.policy", which may hold one of the following values**
  - **"defined" if a VPN policy is associated with the VPN link**
  - **"undefined" if no VPN policy is associated with the VPN link**.

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

- **The IP encryptor administration component is allowed to define the VPN security policy of a given VPN link by means of OP.VPN_SP_definition on behalf of an authenticated security administrator. Upon completion of**

the operation, the attribute AT.policy of the VPN link holds the value "defined".

- **The IP encryptor administration component is allowed to display the VPN security policy of a given VPN link by means of OP.VPN_SP_display on behalf of an authenticated security administrator**.
- **The IP encryptor administrator component is allowed to distribute the VPN security policy of a given VPN link by means of OP.VPN_SP_distribute on behalf of an authenticated remote security administrator provided the VPN security policies and security contexts are protected from modification and disclosure during the distribution**.

FDP_ACF.1.3/VPN_policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/VPN_policy The TSF shall explicitly deny access of subjects to objects based on the

- **The operation OP.VPN_SP_definition is denied to any user that has not been authenticated as a security administrator.**
- **The operation OP.VPN_SP_display is denied to any user that has not been authenticated as a security administrator.**
- **The operation OP.VPN_SP_distribute is denied to any user that has not been authenticated as a remote security administrator or if the distribution channel does not ensure integrity and confidentiality.**

FDP_IFC.1/Key_policy Subset information flow control

FDP_IFC.1.1/Key_policy The TSF shall enforce the **key management policy** on

- **Information: cryptographic keys**
- **Subjects: IP encryptor key management component**
- **Operations:**
  - **OP.local_key_injection: allows to import within the TOE cryptographic keys generated outside the TOE**
  - **OP.key_export: allows to export TOE public keys.**
  - **OP.remote_key_injection: allows to import within the TOE cryptographic keys generated outside the TOE remotely.**

FDP_IFF.1/Key_policy Simple security attributes

FDP_IFF.1.1/Key_policy The TSF shall enforce the **key management policy** based on the following types of subject and information security attributes:

- **Security attribute of cryptographic keys: "AT.key_type", which may hold one of the following three values:**
  - **"public" applies to the public part of asymmetric cryptographic keys**
  - **"private" applies to the private part of asymmetric cryptographic keys**
  - **"secret" applies to symmetric cryptographic keys**
- **[assignment: other security attributes]**.

FDP_IFF.1.2/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:

- **The IP encryptor key management component is allowed to perform local injection of keys by means of the operation OP.local_key_injection on behalf of an authenticated local security administrator. Upon completion of the operation, the attribute AT.key_type of the injected key holds the value corresponding to the kind of key injected.**
- **The IP encryptor key management component is allowed to perform remote key injection by means of the operation OP.remote_key_injection on behalf of an authenticated remote security administrator provided the imported keys are protected from modification and the private and secret imported keys are protected from disclosure during the injection.**

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

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

FDP_IFF.1.5/Key_policy The TSF shall explicitly deny an information flow based on the following rules:

- **The injection (OP.key_inject) of keys is denied to any user that has not been authenticated as a security administrator**
- **The export (OP.key_export) of keys with AT.key_type equal to "private" or "secret" is denied to any user**.

FPT_ITT.1/Administration Basic internal TSF data transfer protection

FPT_ITT.1.1/Administration [Editorial refined] The TSF shall protect TSF data from **disclosure (when data are confidential) and modification** when it is transmitted between separate parts of the TOE.

Non-editorial refinement:

All remote administration operations must be protected including operations on:

- o VPN security policies and their contexts (one possible for each subnetwork),
- o cryptographic keys,
- o configuration parameters,
- o audit events and security alarms.

FPT_ITT.3/Administration TSF data integrity monitoring

FPT_ITT.3.1/Administration The TSF shall be able to detect **[selection : modification of data, substitution of data, re-ordering of data, deletion of data, [assignment : other integrity errors]]** for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2/Administration Upon detection of a data integrity error, the TSF shall take the following actions : **[assignment: specify the action to be taken]**.

FDP_IFC.1/Config_audit Subset information flow control

FDP_IFC.1.1/Config_audit The TSF shall enforce the **configuration and audit policy** on

- o **Information: configuration parameters, audit events and security alarms.**
- o **Operations: all remote operations that cause this information to flow.**
- o **Subjects: subjects of administration software that consults or modifies this information**.

FDP_IFF.1/Config_audit Simple security attributes

FDP_IFF.1.1/Config_audit The TSF shall enforce the **configuration and audit policy** based on the following types of subject and information security attributes: **none**.

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

- o **Remote administration operations on configuration parameters are authorized if this information is protected from modification and disclosure when flowing between the administration equipment and the IP encryptor.**

- **Remote administration operations on audit events and security alarms are authorized if this information is protected from modification when flowing between the administration equipment and the IP encryptor**.

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

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

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

FPT_RPL.1 Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities:

- **sequences of administration data exchanged between an IP encryptor and an administration equipment**.

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

A.2 Option « dynamic negotiation »

A.2.1 TOE description

VPN security policies definition

When a negotiation phase is performed between two IP encryptors, a part of security policies and security contexts can be defined during this phase by taking into account constraints defined previously. These global security constraints are defined by the security administrator and can include several strategies classified by preference order according to their force or their attacks resistance. IP encryptors can begin a negotiation phase to agree on a specific VPN security policy to be enforced by respecting global constraints and preference orders defined by the security administrator, so as to select dynamically the strongest policy common to both IP encryptors that must establish a VPN link.

This service shall permit every IP encryptor to authenticate itself with another IP encryptor (and reciprocally) in order to negotiate the security context (algorithms to be used for encryption, algorithm for the sealing, keys length, validity period...) before establishing licit VPN links. This service is useful for IP encryptors which are brought to generate on-the-fly keys (during every VPN links establishment).

Cryptographic keys generation

This service permits IP encryptors to generate keys at the end of the mutual authentication and the negotiation phase during VPN links establishment. These generated keys will then be used to enforce security services of VPN security policies.

A.2.2 Security environment

There is no environment element which is specific for this option.

A.2.3 Security objectives

A.2.3.1 Security objectives for the TOE

O.POL_DEFINITION

The TOE shall enable only the security administrator to define VPN security policies and their security contexts. The TOE shall also provide the capability to ascertain that a negotiation of a part of policy and context between two IP encryptors leads to the choice of a policy and a context which are in conformance with the security administrator strategy selected.

O.MUTUAL_AUTHENTICATION

The TOE shall provide a mutual authentication mechanism for IP encryptors which communicate together and so provide the capability to negotiate dynamically VPN security policies and their contexts.

A.2.4 Security functional requirements for the TOE

FDP_ACC.1/VPN_policy Subset access control

FDP_ACC.1.1/VPN_policy The TSF shall enforce the **VPN protection policy** on

- **Objects: VPN links and VPN security policies, where VPN security policies include VPN security contexts and, potentially, constraints for dynamic negotiation**
- **Subjects: IP encryptor administration and dynamic negotiation components**
- **Operations:**
  - **OP.VPN_SP_definition: allows to completely or partially define the VPN security policy applicable to a given VPN link**
  - **OP.VPN_SP_dyn_neg: allows to dynamically complete the VPN security policy applicable to a given VPN link**
  - **OP.VPN_SP_display: allows to display the VPN security policy of a given VPN link**.

FDP_ACF.1/VPN_policy Security attribute based access control

FDP_ACF.1.1/VPN_policy The TSF shall enforce the **VPN protection policy** to objects based on the following:

- **Security attribute of the VPN link: "AT.policy", which may hold one of the following values**
  - **"defined" if a VPN policy is associated with the VPN link**
  - **"constrained" if a partial VPN policy and constraints for a dynamic negotiation are associated with the VPN link**
  - **"undefined" if no VPN policy is associated with the VPN link**.

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

- **The IP encryptor administration component is allowed to completely or partially define the VPN security policy of a given VPN link by means of OP.VPN_SP_definition on behalf of an authenticated security administrator. Upon completion of the operation, the attribute AT.policy of the VPN link holds the value "defined" if the VPN policy is complete and “constrained” if the VPN policy contains constraints for dynamic negotiation.**
- **The IP encryptor dynamic negotiation component is allowed to complete the VPN security policy of a VPN link with the attribute AT.policy equal to "constrained" by means of OP.VPN_SP_dyn_neg on behalf of an authenticated provided the definition fulfils the constrains.**
- **The IP encryptor administration component is allowed to display the VPN security policy of a given VPN link by means of OP.VPN_SP_display on behalf of an authenticated security administrator**.

FDP_ACF.1.3/VPN_policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/VPN_policy The TSF shall explicitly deny access of subjects to objects based on the

- **The operation OP.VPN_SP_definition is denied to any user that has not been authenticated as a security administrator.**
- **The operation OP.VPN_SP_dyn_neg is denied to any user that has not been authenticated as an IP encryptor.**
- **The operation OP.VPN_SP_display is denied to any user that has not been authenticated as a security administrator.**

FMT_MSA.3/VPN_policy Static attribute initialisation

FMT_MSA.3.1/VPN_policy The TSF shall enforce the **VPN protection policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/VPN_policy The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

Non-editorial refinement:

The security attribute concerned by these requirements is the attribute AT.policy that indicates for each VPN communication link if a VPN security policy and its context are defined. Its initial value is "undefined". This value is changed by the security administrator when he defines the VPN security policy and its context ("defined") or when he specifies constraints on the VPN security policy and its context ("constrained").

FCS_COP.1/Mutual_auth Cryptographic operation

FCS_COP.1.1/Mutual_auth The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **cryptographic referentials of DCSSI ([CRYPTO] and [AUTH])**.

Non-editorial refinement:

The ST author shall complete the operations of this requirement to specify all the cryptographic operations necessary to provide the mutual authentication mechanism between two IP encryptors.

FIA_UAU.4/Mutual_auth Single-use authentication mechanisms

FIA_UAU.4.1/Mutual_auth The TSF shall prevent reuse of authentication data related to **mutual authentication of IP encryptors**.

FDP_IFF.1/Key_policy Simple security attributes

FDP_IFF.1.1/Key_policy The TSF shall enforce the **key management policy** based on the following types of subject and information security attributes:

- **Security attribute of cryptographic keys: "AT.key_type", which may hold one of the following three values:**
  - **"public" applies to the public part of asymmetric cryptographic keys**
  - **"private" applies to the private part of asymmetric cryptographic keys**
  - **"secret" applies to symmetric cryptographic keys**
- **[assignment: other security attributes]**.

FDP_IFF.1.2/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:

- **The IP encryptor key management component is allowed to perform local injection of keys by means of the operation OP.local_key_injection on behalf of an authenticated local security administrator. Upon completion of the operation, the attribute AT.key_type of the injected key holds the value corresponding to the kind of key injected.**
- **The IP encryptor key management component is allowed to perform remote key injection by means of the operation OP.remote_key_injection on behalf of an authenticated remote security administrator provided the imported keys are protected from modification and the private and secret imported keys are protected from disclosure during the injection.**

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

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

FDP_IFF.1.5/Key_policy The TSF shall explicitly deny an information flow based on the following rules:

- **The injection (OP.key_inject) of keys is denied to any user that has not been authenticated as a security administrator**
- **The export (OP.key_export) of keys with AT.key_type equal to "private" or "secret" is denied to any user unless the keys are protected (encrypted) according to a negociation protocol before being exported**.

FCS_CKM.1/Key_policy Cryptographic key generation

FCS_CKM.1.1/Key_policy The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **cryptographic referential of DCSSI ([CRYPTO])**.

Non-editorial refinement:

These keys can be generated by the TOE or imported from the outside.

A.3 Rationale of the maximal configuration

A.3.1 Rationale for security objectives

A.3.1.1 Threats

T.POL_MODIFICATION

This threat is countered by O.POL_DEFINITION, O.POL_PROTECTION, O.ADMIN_AUTHENTICATION and OE.ADMIN_AUTHENTICATION which enforce that VPN security policies and their contexts can only be modified by security administrators authenticated as such. Furthermore, this threat is also countered by O.ADMIN_FLOWS_PROTECTION and O.POL_DISTRIBUTION which provide the capability to protect the authenticity of policies flows and their contexts during their distribution to IP encryptors.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.POL_DISCLOSURE

This threat is countered by O.POL_DEFINITION, O.POL_PROTECTION, O.ADMIN_AUTHENTICATION and OE.ADMIN_AUTHENTICATION which enforce that VPN security policies and their contexts can only be viewed by security administrators authenticated as such. Furthermore, this threat is also countered by O.ADMIN_FLOWS_PROTECTION and O.POL_DISTRIBUTION which enforce the confidentiality protection of policies flows and their contexts during their distribution to IP encryptors.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.POL_CONSISTENCY

This threat is countered by O.POL_CONSISTENCY which ensures the consistency between VPN security policies defined by the security administrator and those enforced in IP encryptors.

The following objectives also contribute to the threat coverage:

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY, because it ensures that the integrity of the software code which define and enforce VPN security policies can be checked.

T.PARAM_MODIFICATION

O.PARAM_PROTECTION counters this threat by protecting the integrity of configuration parameters. This objective with O.ADMIN_AUTHENTICATION and OE.ADMIN_AUTHENTICATION enable ascertaining that only system and network administrators and security administrators, authenticated as such, can access these parameters. Furthermore, O.ADMIN_FLOWS_PROTECTION ensures the integrity of these parameters when these are remote defined.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.PARAM_DISCLOSURE

O.PARAM_PROTECTION counters this threat by protecting the confidentiality of configuration parameters. This objective with O.ADMIN_AUTHENTICATION and OE.ADMIN_AUTHENTICATION enable ascertaining that only system and network administrators and security administrators, authenticated as such, can access these parameters. Furthermore, O.ADMIN_FLOWS_PROTECTION ensures the integrity of these parameters when these are remote defined.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.KEYS_MODIFICATION

This threat is countered by O.KEYS_INJECTION and O.ADMIN_FLOWS_PROTECTION during keys injection in cipher units, because these objectives ensure the integrity protection of keys during their injection. Moreover the objectives O.KEYS_INJECTION, O.ADMIN_AUTHENTICATION and OE.ADMIN_AUTHENTICATION ensure that only security administrators authenticated as such can inject keys. This threat is also countered by O.KEYS_ACCESS which protects the keys logical access.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.KEYS_DISCLOSURE

This threat is countered by O.KEYS_INJECTION and O.ADMIN_FLOWS_PROTECTION during keys injection in cipher units, because these objectives ensure the confidentiality protection of keys during their injection. Furthermore, the objectives O.KEYS_INJECTION, O.ADMIN_AUTHENTICATION and OE.ADMIN_AUTHENTICATION ensure that only security administrators authenticated as such can inject keys. This threat is also countered by O.KEYS_ACCESS which protects the keys logical access. Finally, this threat is countered by O.CRYPTO which ensures a regular keys renewal and therefore makes more difficult the use of revealed keys.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.AUDIT_MODIFICATION

This threat is countered by O.AUDIT_PROTECTION, O.ADMIN_AUTHENTICATION and OE.ADMIN_AUTHENTICATION which enforce that audit events recordings can be deleted only by auditors authenticated as such. Furthermore, this threat is also countered by O.ADMIN_FLOWS_PROTECTION which provides the capability to protect the integrity of audit events flows necessary for the viewing of these (remote) by the auditors.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.ALARM_MODIFICATION

This threat is countered by O.ALARM_PROTECTION, O.ADMIN_AUTHENTICATION and OE.ADMIN_AUTHENTICATION which enforce that security alarms can be deleted only by security administrators authenticated as such. Furthermore, this threat is also countered by O.ADMIN_FLOWS_PROTECTION which provides the capability to protect the integrity of security alarms flows during their issuance to security administrators.

The following objectives also contribute to the threat coverage:

- O.SUPERVISION_IMPACT ensures that the TOE supervision service does not question sensitive assets security.

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY ensures the integrity check of the TOE hardware and software configuration.

T.TIME_BASE

This threat is covered by the objective O.TIME_BASE which ensures the time base reliability.

T.ADMIN_USURPATION

This threat is countered by O.ADMIN_AUTHENTICATION and OE.ADMIN_AUTHENTICATION, because these objectives enforce the authentication (local or remote) of different administrators before performing any administration operation.

The following objectives also contribute to the threat coverage:

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the capability to detect and process errors or attacks after an analyse of audit events and security alarms.

T.ADMIN_REPLAY

This threat is countered by O.ADMIN_REPLAY_PROTECTION, because it prevents the administration operations replay.

The following objectives also contribute to the threat coverage:

- O.ADMIN_AUDIT and O.ALARMS ensure that operations (viewing, modification) performed on TOE sensitive assets as well as the TOE services uses are logged and that security alarms are generated to indicate TOE operational failures. They so provide the

capability to detect and process errors or attacks after an analyse of audit events and security alarms.

- OE.TOE_INTEGRITY, because it ensures that the integrity of the software code which prevents this replay can be checked.

T.UNAVAILABLE_ASSETS

This threat is covered by O.UNAVAILABLE_ASSETS, because it enforces that the TOE provides a functionality which allows to make TOE sensitive assets unavailable during a change of operational context. Furthermore, this threat is covered by OE.PREMISE_PROTECTION, because it enforces that TOE equipments items are stored within secure premise when they contain sensitive assets.

A.3.2 Rationale for security functional requirements

A.3.2.1 Security objectives for the TOE

O.MUTUAL_AUTHENTICATION

This objective is covered by FCS_COP.1/Mutual_auth, because this requirement provides all cryptographic operations required for mutual authentication mechanism. Furthermore, this objective is covered by FIA_UAU.4/Mutual_auth which prevents the re-use of authentication data during mutual authentication.

O.POL_DISTRIBUTION

This objective is covered by the protection policy of VPN security policies (FDP_ACC.1/VPN_policy and FDP_ACF.1/VPN_policy) which controls access to the operation of VPN security policies distribution. It is also covered by FPT_ITT.1/Administration and FPT_ITT.3/Administration which ensure a confidentiality and integrity protection of VPN security policies flows during this remote distribution.

O.POL_CONSISTENCY

This objective is covered by FPT_TRC.1/VPN_policy which ensures a correct interpretation and consequently a correct enforcement of VPN security policies defined.

O.CRYPTO

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

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

O.KEYS_INJECTION

This objective is covered by the keys policy (FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy and FMT_MSA.3/Key_policy) which monitors keys flows including keys injection (FDP_ITC.1/Key_policy). Furthermore, this objective is covered by FDP_ITT.1/Administration and FDP_ITT.3/Administration which ensure a confidentiality and integrity protection of keys flows during a remote injection.

O.PARAM_PROTECTION

This objective is covered by FMT_MTD.1/Network_param (for network configuration parameters), FMT_MTD.1/Param (for access rights and authentication data) and FMT_SMF.1/Config_supervision, because these requirements ensure the confidentiality and integrity protection of configuration parameters by restricting access to operations which manipulate these parameters. Furthermore, this objective is covered by the configuration and audit policy (FDP_IFC.1/Config_audit and FDP_IFF.1/Config_audit) which protects the integrity and the confidentiality of configuration parameters during their viewing or remote modification.

O.AUDIT_PROTECTION

This objective is covered by FAU_STG.1 which protects the integrity of audit events recordings. It is also covered by the configuration and audit policy (FDP_IFC.1/Config_audit and FDP_IFF.1/Config_audit) which protects the integrity of audit events during their viewing or remote deletion. Furthermore, FAU_GEN.1/VPN and FAU_GEN.1/Administration provide the capability to detect the loss of audit events.

O.ALARM_PROTECTION

This objective is covered by FAU_STG.1 which protects the integrity of security alarms recordings. It is also covered by the configuration and audit policy (FDP_IFC.1/Config_audit and FDP_IFF.1/Config_audit) which protects the integrity of security alarms during their viewing or remote deletion. Furthermore, FAU_GEN.1/VPN and FAU_GEN.1/Administration provide the capability to detect the loss of security alarms.

O.ADMIN_REPLAY_PROTECTION

This objective is covered by FPT_RPL.1 which imposes the replay detection of administration data sequences as well as actions to be performed in case of detection.

O.ADMIN_FLOWS_PROTECTION

This objective is covered by FPT_ITT.1/Administration and FPT_ITT.3/Administration which ensures (if applicable) confidentiality and integrity of data which transit through administration flows.

A.3.3 Dependencies

A.3.3.1 Security functional requirements dependencies

Remark:

This dependencies matrix summarizes all SFR whether optional or not.

Requirements	CC dependencies	Satisfied dependencies
FDP_IFC.1/Enforcement_policy	(FDP_IFF.1)	FDP_IFF.1/Enforcement_policy
FDP_IFF.1/Enforcement_policy	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ITC.1/Enforcement_policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ETC.1/Enforcement_policy	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/Enforcement_policy
FCS_COP.1/Enforcement_policy	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1/Key_policy, FCS_CKM.4/Key_policy
FPT_TRC.1/VPN_policy	(FPT_ITT.1)	FPT_ITT.1/Administration
FDP_ACC.1/VPN_policy	(FDP_ACF.1)	FDP_ACF.1/VPN_policy
FDP_ACF.1/VPN_policy	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/VPN_policy, FMT_MSA.3/VPN_policy
FDP_ITC.1/VPN_policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/VPN_policy, FMT_MSA.3/VPN_policy
FMT_MSA.3/VPN_policy	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/VPN_policy, FMT_SMR.1
FMT_MSA.1/VPN_policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/VPN_policy, FMT_SMF.1/VPN_policy, FMT_SMR.1
FMT_SMF.1/VPN_policy	No dependency	
FCS_COP.1/mutual_auth	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1/Key_policy, FCS_CKM.4/Key_policy
FIA_UAU.4/Mutual_auth	No dependency	
FDP_ITC.1/Key_policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Key_policy, FMT_MSA.3/Key_policy
FDP_IFC.1/Key_policy	(FDP_IFF.1)	FDP_IFF.1/Key_policy

Requirements	CC dependencies	Satisfied dependencies
FDP_IFF.1/Key_policy	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Key_policy, FMT_MSA.3/Key_policy
FDP_UCT.1/Key_policy	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/Key_policy
FDP_UIT.1/Key_policy	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/Key_policy
FMT_MSA.3/Key_policy	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1
FCS_CKM.1/Key_policy	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/Enforcement_policy, FCS_COP.1/mutual_auth, FCS_CKM.4/Key_policy
FCS_CKM.4/Key_policy	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1/Key_policy
FCS_CKM.3/Key_policy	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/Key_policy, FDP_ITC.1/Key_policy
FMT_MTD.1/Network_param	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1
FMT_MTD.1/Param	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1
FMT_SMF.1/Config_supervision	No dependency	
FPT_ITT.1/Administration	No dependency	
FPT_ITT.3/Administration	(FPT_ITT.1)	FPT_ITT.1/Administration
FDP_IFC.1/Config_audit	(FDP_IFF.1)	FDP_IFF.1/Config_audit
FDP_IFF.1/Config_audit	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Config_audit
FPT_RPL.1	No dependency	
FDP_RIP.1	No dependency	
FAU_GEN.1/VPN	(FPT_STM.1)	FPT_STM.1
FAU_GEN.1/Administration	(FPT_STM.1)	FPT_STM.1
FAU_SAR.1	(FAU_GEN.1)	FAU_GEN.1/VPN, FAU_GEN.1/Administration
FAU_SAR.3	(FAU_SAR.1)	FAU_SAR.1

Requirements	CC dependencies	Satisfied dependencies
FAU_STG.1	(FAU_GEN.1)	FAU_GEN.1/VPN, FAU_GEN.1/Administration
FAU_ARP.1/Alarm	(FAU_SAA.1)	FAU_SAA.1/Alarm
FAU_SAA.1/Alarm	(FAU_GEN.1)	FAU_GEN.1/VPN, FAU_GEN.1/Administration
FPT_STM.1	No dependency	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	No dependency	
FIA_UAU.2	(FIA_UID.1)	FIA_UID.2

Table 11 Functional requirements dependencies

A.3.3.2 Rationale for unsatisfied dependencies

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/Key_policy is not satisfied. FDP_UCT.1/Key_policy requires confidentiality of cryptographic keys imported within the TOE. This Protection Profile lets the developper select the type of trusted channel (FTP_ITC.1 or FTP_TRP.1) which the TOE shall implement.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/Key_policy is not satisfied. FDP_UCT.1/Key_policy requires integrity of cryptographic keys imported within the TOE. This Protection Profile lets the developper select the type of trusted channel (FTP_ITC.1 or FTP_TRP.1) which the TOE shall implement.

The dependency FMT_MSA.1 of FMT_MSA.3/Key_policy is not satisfied. The security attribute AT.key_type has only the reviewing operation which is only provided to TSF. As this operation is not provided for a given role, this dependency is not satisfied.

The dependency FMT_MSA.3 of FDP_IFF.1/Config_audit is not satisfied. As there is no security attribute used in this information flow control policy, this dependency is not satisfied.

B Glossary

This appendix gives the definition of main terms used in this document. For the definition of Common Criteria terminology, refer to [CC1], §4.

Administrator	User authorized to manage whole or part of the TOE. He can possess particular privileges which provide the capability to modify TOE security policy.
Authentication	Security measure which checks the declared identity.
Mutual authentication	Security measure which permits for each entities pair to authenticate the other entity of the pair.
Session key	Key with short validity period randomly generated and used to ensure the confidentiality, the authenticity and the integrity of data.
Security context	Security parameters negotiated between two IP encryptors which permit to know which security characteristics must be used to enforce the given VPN security policy. These parameters include cryptographic algorithms, keys sizes...
Operational environment	TOE environment during its phase of use.
Gateway	Device which provides the capability to interconnect two networks presenting different structures.
VPN security policy	Unidirectional security policy defined between two given IP encryptors. This policy specifies security services to be enforced on informations which flow through the cipher unit towards the other cipher unit.
Private network	Internal network of an entity (as a company or a service) which must be protected from flows coming from the outside but not from its own flows. It is a network considered to be secure.
Public network	Network accessible to any entity and any person which cannot be considered to be secure.

Index