Direction centrale de la sécurité des systèmes d'information

Profil de protection Chiffreur IP - CC3.1

Date d'émission	**:** Juillet 2008
Référence	**:** PP-CIP-3.1
Version	**:** 1.9

Profil de protection enregistré et certifié par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) sous la référence DCSSI-PP-2008/08.

Table des matières

Table des figures

Table of tableaux

1. Introduction au profil de protection

1.1. Identification du profil de protection

Titre :	Profil de protection, Chiffreur IP.
Auteur :	Trusted Labs S.A.S.
Version :	1.9, Juillet 2008
Sponsor :	DCSSI
Version des CC :	3.1 revision 2

1.2. Présentation du profil de protection

Ce profil de protection spécifie les exigences de sécurité pour une passerelle (ou « gateway ») d'un réseau privé virtuel (VPN).

Ces passerelles VPN sont placées aux entrées/sorties de réseaux privés, considérés comme sûrs, pour établir des liens de communication entre plusieurs de ces réseaux privés en utilisant un réseau public (comme Internet), considéré comme non sûr. Ces liens de communication entre plusieurs passerelles VPN, aussi appelé liens VPN, doivent être sécurisés pour que les données qui transitent entre les réseaux privés puissent être protégées de tous les utilisateurs du réseau public.

Ce profil de protection se concentre seulement à définir des exigences de sécurité sur les passerelles VPN, qui permettent de faire communiquer des réseaux privés, et ne définit pas d'exigences de sécurité sur la partie VPN clients qui permet d'établir des communications sécurisées entre équipements nomades (PC, portables) ou entre des équipements nomades et des réseaux privés.

Une cible de sécurité se réclamant conforme au PP peut présenter des fonctionnalités supplémentaires non prises en compte par ce PP : pare-feu (ou « firewall »), serveur d'authentification, passerelle anti-virus, … Les fonctionnalités additionnelles et leur implémentation ne doivent pas remettre en cause les exigences du présent PP. Lors de la rédaction d'une cible de sécurité se réclamant conforme à ce profil de protection, ces fonctionnalités sont parfaitement exprimables et, le cas échéant, la cible pourra faire référence à tout autre profil de protection les couvrant (tel que [PP-FIR]).

Dans la suite du document, l'expression « passerelle VPN » est désignée par « chiffreur IP ».

Ce profil de protection définit les exigences sur la configuration minimale d'un chiffreur IP qui comprend l'administration locale du chiffreur IP. Trois autres configurations peuvent être envisagées à partir des deux options suivantes : l'administration à distance des chiffreurs IP en plus de l'administration locale et la négociation dynamique d'une partie des contextes des politiques de sécurité appliquées par les chiffreurs IP. La méthodologie Critères Communs ne permettant pas l'évaluation d'un profil avec options, il a donc été choisi d'évaluer la configuration minimale et de définir les éléments (menaces, hypothèses, OSP, objectifs et

exigences) spécifiques à chaque option en notes d'application. Ces notes d'application contiendront aussi l'argumentaire d'associations entre ces éléments uniquement pour la configuration maximale (administration à distance et négociation dynamique) afin de conserver le travail réalisé dans une version précédente du profil de protection.

Une cible de sécurité se réclamant conforme au PP et incluant une ou deux options définies dans les notes d'application doit prendre en compte les éléments et argumentaires de ces notes d'application.

1.3. Présentation des technologies VPN

Cette section présente les différents standards utilisés dans les technologies VPN. Cette section est présentée uniquement dans un but informatif. Les services de sécurité décrits dans ce profil ont été établis en partie en se basant sur ceux offerts par ces standards, mais ce profil ne réclame en aucun cas la conformité à ceux-ci.

1.3.1. IPsec

IPsec (IP security) est un ensemble de standards qui mettent en oeuvre des mécanismes pour sécuriser IP (IPv4 et IPv6) en offrant des services d'authentification, d'intégrité et de confidentialité ([RFC2401]).

IPsec offre ces services au moyen de deux protocoles pour la sécurité des échanges :

- AH (Authentication Header) fournit l'authentification de l'origine et l'intégrité en continu des paquets IP. Il peut aussi fournir en option la protection contre le rejeu ([RFC2402]).
- ESP (Encapsulating Security Payload) fournit la confidentialité, la protection contre le rejeu et en option l'authentification de l'origine et l'intégrité en continu d'une partie des paquets IP, partie qui ne contient pas l'en-tête IP ([RFC2406]).

Ces deux protocoles peuvent être combinés et peuvent être utilisés dans l'un des deux modes d'échanges suivants :

- Mode transport : le paquet IP est envoyé en ajoutant des parties spécifiques à AH et/ou ESP.
- Mode tunnel : le paquet IP est encapsulé dans un nouveau paquet IP contenant les parties spécifiques à AH et/ou ESP.

IPsec utilise le concept d'association de sécurité (SA) qui est supporté par AH et ESP. Une association de sécurité permet de définir les caractéristiques d'une connexion unidirectionnelle : adresse de destination IP, protocole de sécurité (AH ou ESP), index des paramètres de sécurité (SPI), algorithmes cryptographiques utilisés, clés utilisées, date et heure d'expiration, etc. Cette association est utilisée pour appliquer une politique de sécurité lors du traitement des paquets IP passant sur la connexion.

IPsec offre aussi des protocoles pour la gestion des clés cryptographiques et des associations de sécurité :

- IKE (Internet Key Exchange) : [RFC2409]. La partie gestion des associations de sécurité est supportée par ISAKMP ([RFC2408]), alors que la partie échange des clés est supportée par les protocoles Oakley ([RFC2412]) et SKEME ([SKEME]).

1.4. Acronymes

CC	(*Common Criteria*) Critères Communs
CEC	Centre d'Elaboration des Clés
EAL	(*Evaluation Assurance Level*) Niveau d'assurance de l'évaluation
IP	(*Internet Protocol*) Protocole Internet
IT	(*Information Technology*) Technologie de l'information
OSP	(*Organisational Security Policy*) Politique de sécurité organisationnelle
PP	(*Protection Profile*) Profil de protection
SF	(*Security Function*) Fonction de sécurité
SFP	(*Security Function Policy*) Politique des fonctions de sécurité
SOF	(*Strength Of Function*) Résistance des fonctions
ST	(*Security Target*) Cible de sécurité
TI	Technologie de l'Information
TOE	(*Target Of Evaluation*) Cible d'évaluation
TSF	(*TOE Security Function*) Fonctions de sécurité de la TOE
VPN	(*Virtual Private Network*) Réseau privé virtuel

1.5. Références

[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] Mécanismes de cryptographie : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard. 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.

[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.

[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. Description de la TOE

2.1. Fonctionnalités de la TOE

La fonctionnalité principale de la TOE est de fournir au système d'information des liens de communication sécurisés entre plusieurs réseaux privés en offrant les services suivants pour protéger et cloisonner les flux de données (paquets IP transitant entre les chiffreurs IP) :

- Application des politiques de sécurité VPN :
    - Protection en confidentialité des données applicatives,
    - Protection en authenticité des données applicatives,
    - Protection en confidentialité des données topologiques des réseaux privés,
    - Protection en authenticité des données topologiques des réseaux privés,
- Cloisonnement des flux IP.

De plus, pour son bon fonctionnement, la TOE requiert les services suivants :

- Gestion des politiques de sécurité VPN :
    - Définition des politiques de sécurité VPN.
    - Protection de l'accès aux politiques de sécurité VPN.
- Gestion des clés cryptographiques :
    - Protection de l'accès aux clés cryptographiques.
    - Injection des clés cryptographiques.
    - Bonne consommation des clés cryptographiques.
- Audit et supervision :
    - Audit/journalisation des activités sur les liens VPN.
    - Audit/journalisation des opérations d'administration.
    - Génération d'alarmes de sécurité.
    - Supervision de la TOE.
- Protection des opérations d'administration : Authentification locale des administrateurs.
- Protection de l'accès aux paramètres de configuration.

2.1.1. Services fournis par la TOE

Application des politiques de sécurité VPN

Les politiques de sécurité VPN spécifient les règles de sécurité qui déterminent le traitement à appliquer aux données. Ces dernières représentent :

- Les données qui proviennent des applications du système d'information et qui sont véhiculées par le réseau. On parle alors de données applicatives.
- Les données ajoutées par les mécanismes réseaux qui permettent notamment le routage des paquets IP. On parle alors de données topologiques.

Ces données transitent entre chaque paire de chiffreurs IP.

Les chiffreurs IP appliquent des fonctions de filtrage implicite, car si aucune politique de sécurité VPN n'est définie sur un lien VPN donné, les paquets entrants ou sortants sont rejetés (règle de filtrage par défaut).

Les services de sécurité qui peuvent être appliqués par une politique de sécurité VPN sont :

- la protection en confidentialité des données applicatives,
- la protection en authenticité des données applicatives,
- la protection en confidentialité des données topologiques,
- la protection en authenticité des données topologiques.

Ces politiques sont conservées au niveau de chaque chiffreur IP concerné pour être appliquées localement.

Protection en confidentialité des données applicatives

Assurer la confidentialité des données applicatives permet d'empêcher la divulgation de ces données lorsqu'elles transitent sur un réseau public non sûr. Pour cela, ces données peuvent être chiffrées avant de passer sur le réseau public et déchiffrées à l'entrée du réseau privé destinataire.

L'algorithme de chiffrement/déchiffrement et les caractéristiques des clés utilisées sont définis dans le contexte de sécurité associé à la politique de sécurité VPN définie sur un lien de communication donné.

Protection en authenticité des données applicatives

Pour assurer l'authenticité des données applicatives, il faut assurer à la fois l'intégrité en continu de ces données ainsi que l'authentification de l'origine de celles-ci. Assurer l'intégrité des données permet de détecter qu'elles n'ont pas été modifiées accidentellement ou volontairement lors de leur transmission d'un chiffreur IP à un autre. Assurer l'authenticité des données permet de s'assurer que l'origine des données est celle attendue.

L'algorithme pour générer les informations d'authenticité et les vérifier ainsi que les caractéristiques des clés utilisées sont définis dans le contexte de sécurité associé à la politique de sécurité VPN définie sur un lien de communication donné.

Protection en confidentialité des données topologiques

Assurer la confidentialité des données topologiques des réseaux privés permet d'empêcher la divulgation des adresses IP internes (source et destination) des équipements se trouvant sur les réseaux privés.

Comme pour les données applicatives, des algorithmes de chiffrement/déchiffrement sont utilisés et définis dans les contextes de sécurité.

Protection en authenticité des données topologiques

Assurer l'authenticité des données topologiques des réseaux privés permet de détecter toute modification des adresses IP internes (source et destination) des équipements se trouvant sur les réseaux privés.

Comme pour les données applicatives, des algorithmes pour générer les informations d'authenticité ou pour les vérifier sont utilisés et définis dans les contextes de sécurité.

Cloisonnement des flux IP

Chaque réseau privé peut être divisé en plusieurs sous-réseaux IP pour permettre de cloisonner des flux IP à l'intérieur même d'un réseau privé. Le service de cloisonnement des flux IP permet d'appliquer des politiques de sécurité VPN différentes suivant les sous-réseaux qui communiquent. Ce service permet aussi de filtrer les paquets IP entrants et de les envoyer sur le sous-réseau approprié.

2.1.2. Services nécessaires au bon fonctionnement de la TOE

2.1.2.1. Gestion des politiques de sécurité VPN

Définition des politiques de sécurité VPN

Les politiques de sécurité VPN sont définies pour chaque lien de communication VPN autorisé. Ce lien de communication est établi entre deux sous-réseaux IP. Il peut exister une politique par sens de communication. Seul l'administrateur de sécurité est autorisé à définir ces politiques. Il spécifie la règle de filtrage implicite pour l'envoi ou la réception de données : acceptation, rejet ou application de services de sécurité. Dans le dernier cas, il spécifie aussi le(s) service(s) de sécurité à appliquer aux données envoyées ou reçues ainsi que le contexte de sécurité qui est associé à cette politique. Le contexte de sécurité contient entre autres les algorithmes cryptographiques utilisés, les tailles de clés et l'association avec les clés à utiliser.

Protection de l'accès aux politiques de sécurité VPN

Ce service permet de contrôler les différents types d'accès (modification, consultation) aux politiques de sécurité VPN et à leurs contextes de sécurité suivant le rôle de la personne authentifiée.

2.1.2.2. Gestion des clés cryptographiques

Protection de l'accès aux clés cryptographiques

Ce service permet d'empêcher les clés secrètes et privées d'être exportées de manière non autorisée à l'extérieur de la TOE. Il permet aussi d'assurer qu'une clé donnée est utilisable (accessible) seulement par les services qui en ont besoin.

Injection des clés cryptographiques

Ce service permet d'injecter de façon sûre les clés cryptographiques, générées à l'extérieur de la TOE, dans les chiffreurs IP ou les équipements d'administration. Lors de la distribution, ce service protège les clés en intégrité et/ou en confidentialité en fonction du type de clés.

Bonne consommation des clés cryptographiques

Ce service permet de gérer correctement le cycle de vie des clés cryptographiques : dérivation, renouvellement régulier, destruction.

2.1.2.3. Audit et supervision

Audit / journalisation des activités sur les liens VPN

Ce service permet de tracer toutes les opérations effectuées par les chiffreurs IP concernant la communication sur les liens VPN, comme par exemple l'établissement des sessions et leur fermeture. Il permet aussi la définition des événements à tracer et leur consultation.

Audit / journalisation des opérations d'administration

Ce service permet de tracer toutes les opérations effectuées par l'administrateur sur les chiffreurs IP concernant l'administration de ce chiffreur, comme par exemple les modifications des politiques de sécurité VPN. Il permet aussi la définition des événements à tracer et leur consultation.

Génération d'alarmes de sécurité

Ce service permet de générer des alarmes de sécurité pour signaler tout dysfonctionnement majeur des chiffreurs IP, comme par exemple une perte d'intégrité sur des clés. Il permet aussi à un administrateur de sécurité de définir les alarmes à générer et leur mode de diffusion et de consulter ces alarmes.

Supervision de la TOE

Ce service permet à un administrateur système et réseau de contrôler l'état de disponibilité de chaque chiffreur IP (état de fonctionnement, niveaux d'utilisation des ressources, ...).

2.1.2.4. Protection des opérations d'administration

Les chiffreurs IP sont administrés localement : c'est une administration qui se fait directement sur la machine contenant les services du chiffreur IP.

Authentification locale des administrateurs

Ce service permet d'authentifier tous les administrateurs qui effectuent des opérations d'administration locale à un chiffreur IP.

2.1.2.5. Protection de l'accès aux paramètres de configuration

Ce service protège (d'une attaque par réseau) les paramètres de configuration des chiffreurs IP en confidentialité et en intégrité. Ces paramètres comprennent entre autres les paramètres de configuration réseau (données topologiques sur les réseaux privés), les données d'authentification et les droits d'accès.

2.1.3. Rôles

Le fonctionnement de la TOE dans son environnement opérationnel manipule directement ou indirectement les rôles décrits ci-dessous.

Administrateur de sécurité

Administrateur des chiffreurs IP. Il génère et distribue les clés dans les chiffreurs IP. Il définit les politiques de sécurité VPN et leurs contextes de sécurité que va appliquer chaque chiffreur. Il définit les événements d'audit à tracer ainsi que les alarmes de sécurité à générer. De plus, il analyse, traite et supprime les alarmes de sécurité générées.

Il configure les rôles et les accès aux outils et fonctions d'administration. Il gère les clés et les moyens d'authentification pour accéder aux outils d'administration ou aux chiffreurs IP.

Auditeur

Son rôle est d'analyser les événements d'audit concernant les activités sur les liens VPN et les opérations d'administration.

Administrateur système et réseau

Administrateur responsable du système d'information sur lequel se trouve le chiffreur IP. Il est responsable du maintien en condition opérationnelle de la TOE (maintenance logicielle et matérielle comprises).

Il configure les paramètres réseaux des chiffreurs et les paramètres systèmes qui sont liés aux contextes réseaux opérationnels à prendre en compte : il définit la topologie réseau globale, mais ne définit pas les politiques de sécurité VPN.

Son rôle est aussi de contrôler l'état des chiffreurs IP.

Utilisateur du réseau privé

Utilisateur d'un réseau privé connecté à un autre réseau privé par un chiffreur IP. Cet utilisateur peut, par l'intermédiaire d'applications, envoyer/recevoir des informations vers/d'un autre réseau privé via le chiffreur IP de son réseau.

Dans la suite du document, le rôle administrateur regroupe les rôles suivants : administrateur de sécurité, auditeur et administrateur système et réseau.

2.2. Architecture de la TOE

Cette section présente l'architecture de la TOE sous deux aspects différents : aspect physique et aspect fonctionnel.

2.2.1. Architecture physique

La Figure 1 présente un exemple d'architecture physique d'un réseau privé virtuel sur lequel la TOE sera évaluée.

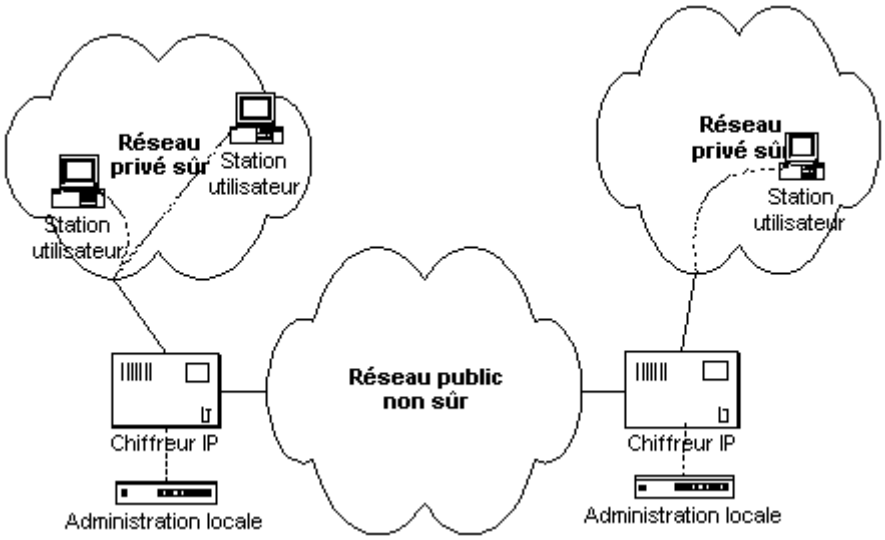

Figure 1 Exemple d'architecture possible d'un VPN

Sur la Figure 1, les chiffreurs IP sont directement connectés au réseau public et aux réseaux privés, mais ils peuvent être insérés à l'intérieur d'une structure globale d'interconnexion de réseaux IP (cf. [PB-INT]).

Comme l'illustre la Figure 1, chaque chiffreur IP présente trois interfaces externes logiques : une interface vers le réseau privé, une interface vers le réseau public et une interface d'administration. L'exemple de la figure contient deux chiffreurs IP, nombre minimum nécessaire à l'établissement d'un lien VPN entre deux réseaux privés, mais il pourrait tout aussi bien en contenir un nombre supérieur.

2.2.2. Architecture fonctionnelle

Les figures de cette section montrent les éléments qui constituent la TOE au niveau fonctionnel. Ces éléments apparaissent en grisé dans les figures. De plus, les biens apparaissent en italique.

Ces schémas sont donnés à titre illustratif et forment une vue abstraite de l'architecture fonctionnelle de la TOE. L'ordonnancement des services présentés dans ces schémas ne correspond donc pas forcément à celui d'une implémentation donnée.

La Figure 2 présente les fonctionnalités qui concernent la gestion des politiques de sécurité VPN et de leurs contextes de sécurité. Tous les services font partie de la TOE.

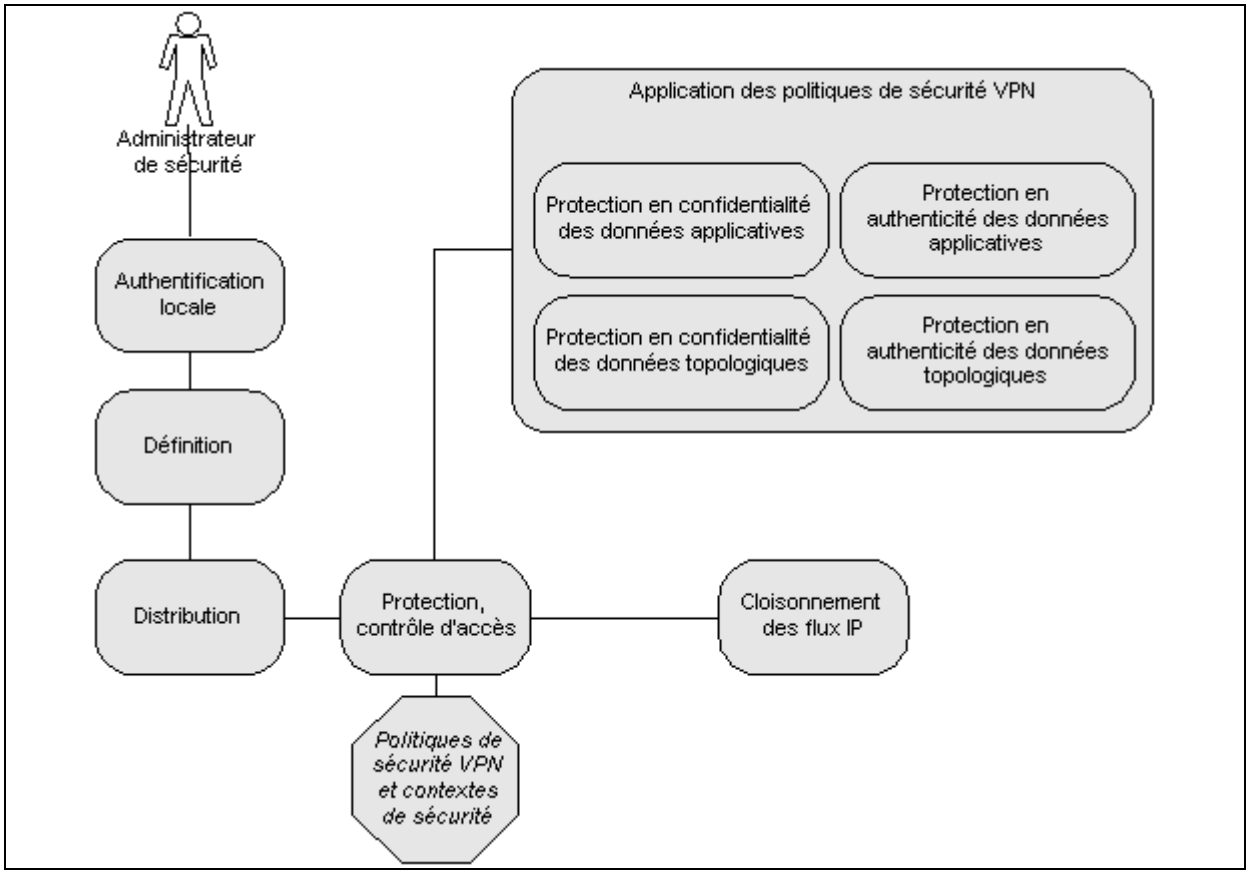

Figure 2 Gestion des politiques de sécurité VPN

Ce schéma (Figure 3) ne présente pas tous les services de la TOE accédant en lecture aux paramètres de configuration, car ils sont nombreux. Ces services sont entre autres les services d'authentification locale, l'application des politiques de sécurité VPN et tous les services qui consultent les droits d'accès et les adresses IP internes pour leur propre besoin.

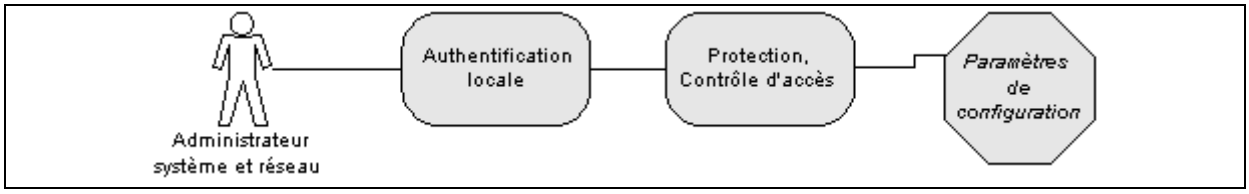

Figure 3 Configuration des chiffreurs IP

Au niveau de la gestion des clés, la génération des clés faite par le CEC ne font pas partie de la TOE (Figure 4).

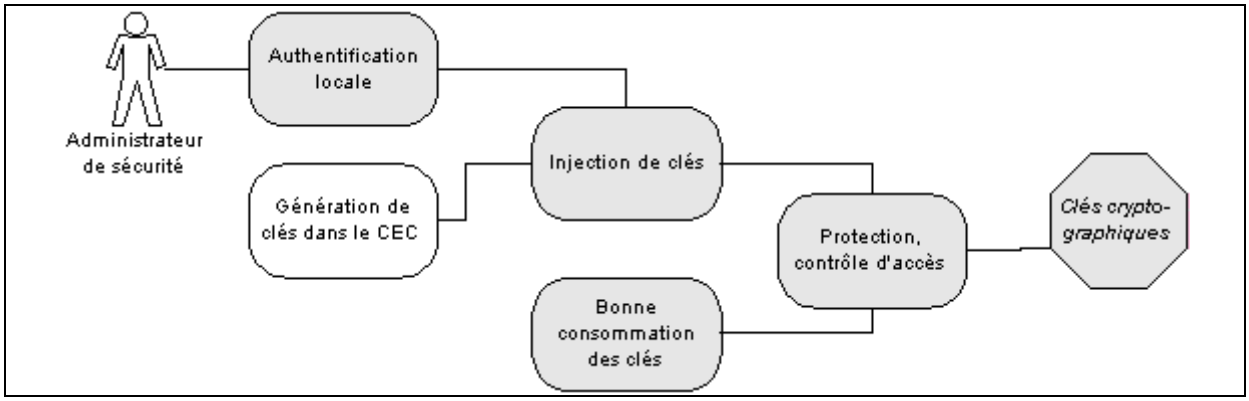

Figure 4 Gestion des clés cryptographiques

Au niveau de l'audit, tous les services font partie de la TOE (Figure 5).

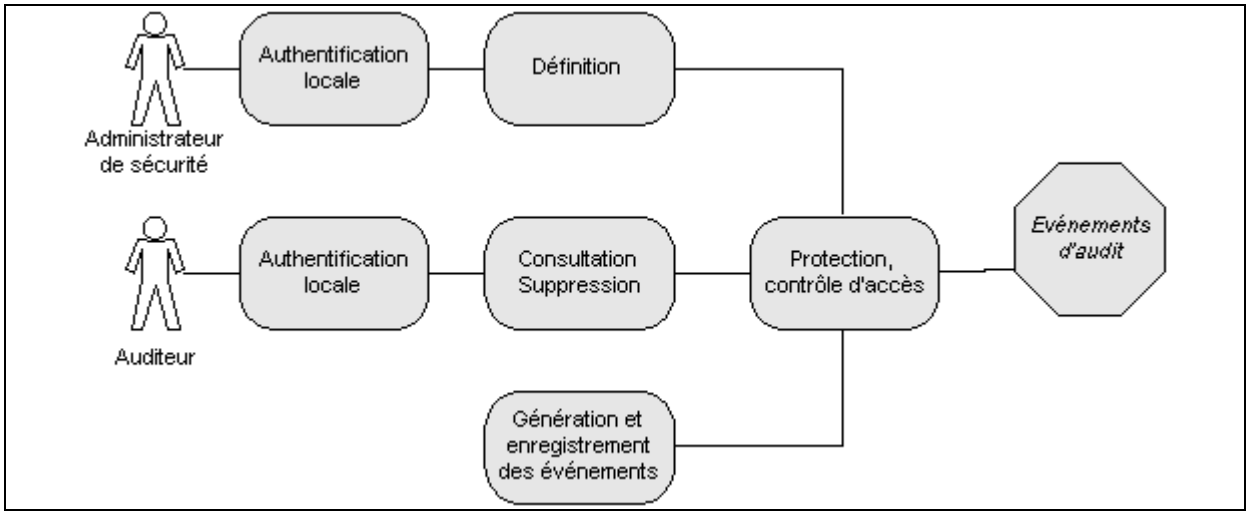

Figure 5 Gestion de l'audit

Au niveau des alarmes de sécurité, le traitement des alarmes ne fait pas partie de la TOE (Figure 6).

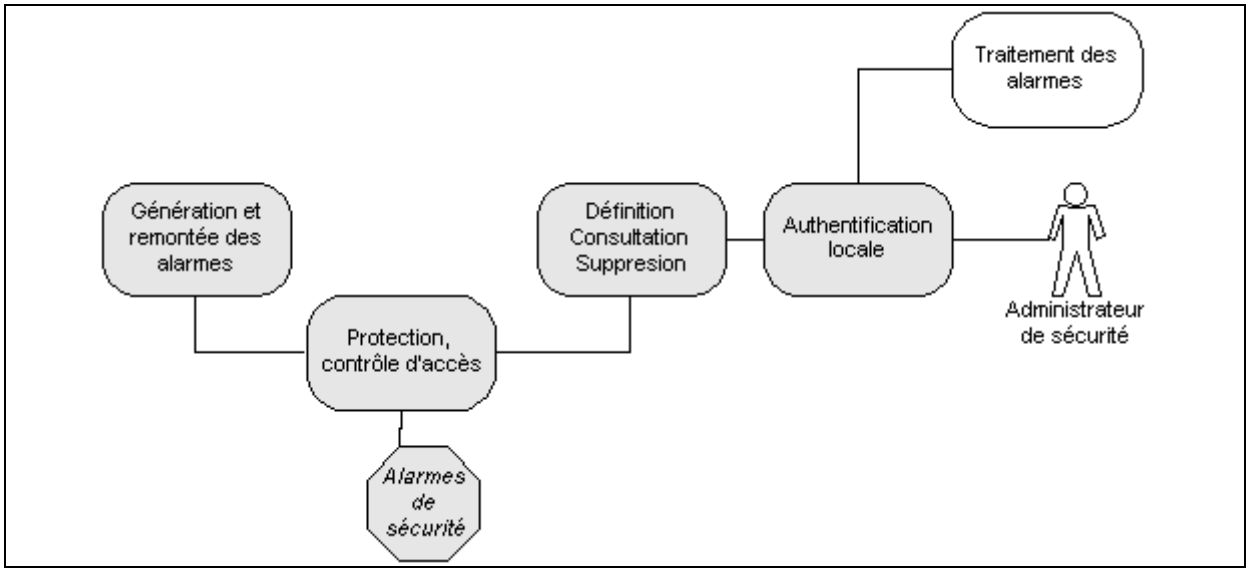

Figure 6 Gestion des alarmes de sécurité

La supervision fait partie de la TOE (Figure 7).

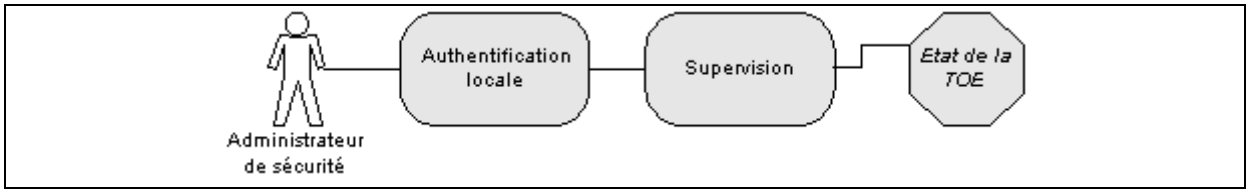

Figure 7 Supervision de la TOE

3. Déclarations de conformité

Ce chapitre contient les sections suivantes :

3.1. Déclaration de Conformité aux CC

Ce profil de protection est conforme aux Critères Communs version 3.1.

Ce PP a été écrit conformément aux CC version 3.1 :

- CC Partie 1 [CC1]
- CC Partie 2 [CC2]
- CC Partie 3 [CC3]
- Méthodologie d'évaluation des CC [CEM]

3.2. Déclaration de conformité à un Paquet

Ce PP est conforme au paquet d'exigences d'assurance pour la qualification de niveau standard défini dans [QUA-STD].

3.3. Déclaration de conformité du PP

Ce PP ne déclare de conformité à aucun autre PP.

3.4. Déclaration de conformité au PP

La conformité retenue dans ce PP pour les Cibles de Sécurité et Profils de Protection qui s'y déclarent conformes est la conformité **démontrable** selon la définition dans la Partie 1 des CC [CC1].

4. Définition du problème de sécurité

4.1. Biens

La description de chaque bien fournit les types de protection requis pour chacun d'eux (partie *Protection*).

4.1.1. Biens protégés par la TOE

Les biens du système d'information sont protégés par la TOE sous la condition que les politiques de sécurité VPN demandent l'application d'un ou plusieurs types de protection. A titre d'illustration, les données qui transitent entre deux chiffreurs IP seront protégées en confidentialité seulement si la politique de sécurité VPN définie pour ce lien VPN exige la protection en confidentialité.

Lorsque le type de protection (partie *Protection*) est suivi de "(opt.)" pour optionnel, cela signifie que cette protection doit être fournie par la TOE, mais qu'elle n'est pas systématiquement appliquée par la TOE.

D.DONNEES_APPLICATIVES

Les données applicatives sont les données qui transitent d'un réseau privé à un autre par l'intermédiaire des chiffreurs IP. Elles sont contenues dans la charge utile des paquets IP routés jusqu'aux chiffreurs et reçus et envoyés par ces chiffreurs. Ces données peuvent être stockées temporairement dans les chiffreurs IP pour pouvoir les traiter (i.e., appliquer les services de sécurité) avant de les envoyer sur le réseau privé ou public.

Protection: confidentialité (opt.) et authenticité (opt.).

D.INFO_TOPOLOGIE

Les informations de topologie des réseaux privés (adresses IP source et destination) se trouvent dans les en-têtes de paquets IP.

Protection: confidentialité (opt.) et authenticité (opt.).

4.1.2. Biens sensibles de la TOE

D.POLITIQUES_VPN

Les politiques de sécurité VPN définissent les traitements (filtrage implicite et services de sécurité) à effectuer sur les données reçues et envoyées par chaque chiffreur IP.

Ce bien comporte aussi les contextes de sécurité qui sont rattachés aux politiques de sécurité. Chaque contexte de sécurité contient tous les paramètres de sécurité nécessaires à l'application de la politique de sécurité VPN à laquelle il est associé. Ces paramètres sont définis par l'administrateur de sécurité.

Protection:

- o intégrité des politiques (et de leur contextes) stockées sur les chiffreurs IP,
- o confidentialité.

D.PARAM_CONFIG

Les paramètres de configuration des chiffreurs IP comprennent entre autres:

- o les adresses IP internes aux réseaux privés et les tables de routage (configuration réseau),
- o les données d'authentification et
- o les droits d'accès.

Protection: confidentialité et intégrité.

D.CLES_CRYPTO

Ce bien représente toutes les clés cryptographiques (symétriques ou asymétriques) nécessaires à la TOE pour fonctionner telles que:

- o Les clés de session.
- o Les clés utilisées par les services de sécurité appliqués par les politiques de sécurité VPN.
- o Les clés pour protéger les politiques de sécurité VPN lors de leur stockage.
- o Les clés pour protéger l'injection de clés cryptographiques dans les chiffreurs IP.

Protection: confidentialité (pour les clés secrètes et privées) et intégrité (pour toutes les clés).

D.AUDIT

Données générées par la politique d'audit pour permettre de tracer les opérations d'administration effectuées ainsi que les activités qui ont eu lieu sur les liens VPN.

Protection: intégrité.

D.ALARMES

Alarmes de sécurité générées par la TOE pour prévenir une possible violation de sécurité.

Protection: intégrité.

D.LOGICIELS

Logiciels de la TOE qui permettent de mettre en oeuvre tous les services de la TOE.

Protection: intégrité.

D.BASE_TEMPS

Base de temps fiable de la TOE.

Protection: intégrité.

4.2. Menaces

La politique de qualification au niveau standard s'applique à des produits grand public assurant la protection d'informations sensibles non classifiées de défense. Par conséquent, un certain nombre de menaces ne seront pas prises en compte dans la suite du PP comme par exemple, le vol de l'équipement (qui doit être détecté par des mesures organisationnelles) ou le déni de service.

Les menaces présentes dans cette section sont uniquement des menaces qui portent atteinte à la sécurité de la TOE et pas aux services rendus par la TOE, car tous les éléments de

l'environnement concernant les services rendus par la TOE sont considérés comme des politiques de sécurité organisationnelle.

Les administrateurs ne sont pas considérés comme des attaquants (hypothèse A.ADMIN).

4.2.1. Menaces portant sur les politiques de sécurité VPN et leurs contextes

T.MODIFICATION_POL

Un attaquant modifie illégalement des politiques de sécurité VPN et leurs contextes de sécurité.

Bien menacé: D.POLITIQUES_VPN.

T.DIVULGATION_POL

Un attaquant récupère illégalement des politiques de sécurité VPN et leurs contextes de sécurité.

Bien menacé: D.POLITIQUES_VPN.

4.2.2. Menaces portant sur la configuration

T.MODIFICATION_PARAM

Un attaquant modifie illégalement des paramètres de configuration.

Bien menacé: D.PARAM_CONFIG.

T.DIVULGATION_PARAM

Un attaquant récupère de manière non autorisée des paramètres de configuration.

Bien menacé: D.PARAM_CONFIG.

4.2.3. Menaces portant sur la gestion des clés

T.MODIFICATION_CLES

Un attaquant modifie illégalement des clés cryptographiques, par exemple en utilisant le service d'injection des clés.

Bien menacé: D.CLES_CRYPTO.

T.DIVULGATION_CLES

Un attaquant récupère illégalement des clés cryptographiques.

Bien menacé: D.CLES_CRYPTO (seulement les clés secrètes et privées).

4.2.4. Menaces portant sur l'audit

T.MODIFICATION_AUDIT

Un attaquant modifie ou supprime illégalement des enregistrements d'événements d'audit.

Bien menacé: D.AUDIT.

T.MODIFICATION_ALARME

Un attaquant modifie ou supprime illégalement les alarmes de sécurité lorsqu'elles sont remontées par la TOE à l'administrateur de sécurité.

Bien menacé: D.ALARMES.

T.BASE_TEMPS

Un attaquant perturbe ou altère la base de temps de la TOE dans le but de falsifier les données d'audit.

Bien menacé: D.BASE_TEMPS.

4.2.5. Menaces portant sur l'administration

T.USURPATION_ADMIN

Un attaquant usurpe l'identité d'un administrateur et effectue des opérations d'administration sur les chiffreurs IP.

Biens menacés: D.POLITIQUES_VPN, D.CLES_CRYPTO, D.AUDIT, D.PARAM_CONFIG.

T.BIENS_INDISPONIBLES

Un attaquant prend connaissance, par accès direct à la TOE, des biens sensibles d'un chiffreur IP (clés, politiques de sécurité VPN,...) lors d'un changement de contexte d'utilisation (affectation du chiffreur IP à un nouveau réseau, maintenance,...).

Biens menacés: D.POLITIQUES_VPN, D.PARAM_CONFIG, D.CLES_CRYPTO, D.AUDIT et D.ALARMES.

4.3. Politiques de sécurité organisationnelles (OSP)

Les politiques de sécurité organisationnelle présentes dans cette section portent uniquement sur les fonctions attendues de la TOE et concernent donc que les services rendus par la TOE au système d'information.

OSP.SERVICES_RENDUS

La TOE doit appliquer les politiques de sécurité VPN définies par l'administrateur de sécurité.

Elle doit aussi fournir tous les services de sécurité nécessaires pour appliquer les protections spécifiées dans ces politiques:

- protection en confidentialité des données applicatives,
- protection en authenticité des données applicatives,
- protection en confidentialité des données topologiques et
- protection en authenticité des données topologiques.

De plus, la TOE doit permettre de cloisonner des flux IP pour faire communiquer des sous-réseaux (de réseaux privés) et appliquer une politique de sécurité sur chaque lien de communication entre sous-réseaux IP.

OSP.CRYPTO

Le référentiel de cryptographie de la DCSSI ([CRYPTO]) doit être suivi pour la gestion des clés (génération, destruction, consommation et distribution) et les fonctions de cryptographie utilisées dans la TOE, pour le niveau de résistance standard.

OSP.VISUALISATION_POL

La TOE doit permettre aux administrateurs de sécurité de visualiser unitairement les politiques de sécurité VPN et leurs contextes de sécurité présents sur chaque chiffreur IP.

OSP.SUPERVISION

La TOE doit permettre à l'administrateur système et réseau de consulter l'état opérationnel de chaque chiffreur IP.

4.4. Hypothèses

4.4.1. Hypothèses sur l'usage attendu de la TOE

A.AUDIT

Il est supposé que l'auditeur consulte régulièrement les événements d'audit générés par la TOE. Il est aussi supposé que la mémoire stockant les événements d'audit soit gérée de telle sorte que l'auditeur ne perde pas d'événements.

A.ALARME

Il est supposé que l'administrateur de sécurité analyse et traite les alarmes de sécurité générées et remontées par la TOE.

4.4.2. Hypothèses sur l'environnement d'utilisation de la TOE

A.ADMIN

Les administrateurs sont des personnes non hostiles et compétentes qui disposent des moyens nécessaires à la réalisation de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.

A.LOCAL

Les équipements contenant les services de la TOE (chiffreurs IP et équipements d'administration), ainsi que tous supports contenant les biens sensibles de la TOE (papier, disquettes,...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs. Cependant, les équipements contenant les services de la TOE peuvent ne pas se trouver dans des locaux sécurisés s'ils ne contiennent pas de biens sensibles: par exemple dans les cas de changement de contexte d'utilisation d'un chiffreur IP.

A.MAITRISE_CONFIGURATION

L'administrateur dispose des moyens de contrôler la configuration matérielle et logicielle de la TOE (services et biens compris) par rapport à un état de référence, ou de la régénérer dans un état sûr.

Note d'application

Cette hypothèse concerne en particulier le bien D.LOGICIELS.

A.CRYPTO

Les clés cryptographiques, générées à l'extérieur, qui sont injectées dans la TOE doivent avoir été générées en suivant les recommandations spécifiées dans les référentiels cryptographiques de la DCSSI [CRYPTO] et [CRYPTO_GESTION] pour le niveau de résistance standard.

5. Objectifs de sécurité

5.1. Objectifs de sécurité pour la TOE

5.1.1. Objectifs de sécurité sur les services rendus par la TOE

O.APPLICATION_POL

La TOE doit appliquer les politiques de sécurité VPN spécifiées dans les chiffreurs IP.

O.CONFIDENTIALITE_APPLI

La TOE doit fournir des mécanismes pour protéger en confidentialité les données applicatives qui transitent entre deux chiffreurs IP.

O.AUTHENTICITE_APPLI

La TOE doit fournir des mécanismes pour protéger en authenticité les données applicatives qui transitent entre deux chiffreurs IP.

O.CONFIDENTIALITE_TOPO

La TOE doit fournir des mécanismes pour protéger en confidentialité les informations sur la topologie des réseaux privés contenues dans les paquets IP qui transitent entre deux chiffreurs IP.

O.AUTHENTICITE_TOPO

La TOE doit fournir des mécanismes pour protéger en authenticité les informations sur la topologie des réseaux privés contenues dans les paquets IP qui transitent entre deux chiffreurs IP.

O.CLOISONNEMENT_FLUX

La TOE doit permettre de cloisonner les réseaux IP interconnectés ensembles grâce aux chiffreurs IP, en permettant de créer un nouveau réseau IP étendu, superposé au réseau IP initial constitué de sous-réseaux IP. La TOE doit aussi permettre d'appliquer une politique de sécurité sur chaque lien de communication entre sous-réseaux IP.

5.1.2. Objectifs de sécurité pour protéger les biens sensibles de la TOE

5.1.2.1. Gestion des politiques de sécurité VPN

O.DEFINITION_POL

La TOE doit permettre seulement à l'administrateur de sécurité de définir les politiques de sécurité VPN et leurs contextes de sécurité.

O.PROTECTION_POL

La TOE doit contrôler l'accès (consultation, modification) aux politiques de sécurité VPN et à leurs contextes de sécurité qui est autorisé seulement aux administrateurs de sécurité.

O.VISUALISATION_POL

La TOE doit permettre aux seuls administrateurs de sécurité de visualiser unitairement les politiques de sécurité VPN et leurs contextes de sécurité présents sur chaque chiffreur IP.

5.1.2.2. Gestion des clés cryptographiques

O.CRYPTO

La TOE doit implémenter les fonctions de cryptographie et gérer (générer, détruire, renouveler) les clés cryptographiques en accord avec les référentiels de cryptographie définis par la DCSSI ([CRYPTO] et [CRYPTO_GESTION]) pour le niveau de résistance standard.

O.ACCES_CLES

La TOE doit protéger l'accès aux clés cryptographiques.

O.INJECTION_CLES

La TOE doit protéger les clés en confidentialité (seulement pour les clés secrètes et privées) et en intégrité lors de leur injection sur les chiffreurs IP.

5.1.2.3. Configuration et supervision

O.PROTECTION_PARAM

La TOE doit protéger en confidentialité et intégrité les paramètres de configuration qui ne peuvent être accédés que par un administrateur système et réseau pour les paramètres de configuration réseaux et par un administrateur de sécurité pour les droits d'accès et les données d'authentification.

O.SUPERVISION

La TOE doit permettre à l'administrateur système et réseau de consulter l'état opérationnel de chaque chiffreur IP.

O.IMPACT_SUPERVISION

La TOE doit garantir que le service de supervision ne met pas en péril ses biens sensibles.

5.1.2.4. Audit et alarme

O.AUDIT_VPN

La TOE doit tracer toutes les opérations effectuées par les chiffreurs IP relevant de la sécurité et concernant les communications sur les liens VPN. De plus, elle doit permettre seulement à un auditeur de consulter ce qui a été tracé.

O.AUDIT_ADMIN

La TOE doit tracer toutes les opérations effectuées par un administrateur sur les chiffreurs IP. De plus, elle doit permettre seulement à un auditeur de consulter ce qui a été tracé.

O.PROTECTION_AUDIT

La TOE doit garantir l'intégrité des événements d'audit qu'elle enregistre et doit permettre à un auditeur de détecter la perte d'événements d'audit (en utilisant un compteur par exemple).

O.ALARMES

La TOE doit générer des alarmes de sécurité en cas d'atteinte aux biens sensibles de la TOE.

O.PROTECTION_ALARME

La TOE doit garantir l'intégrité des alarmes de sécurité (à destination des administrateurs de sécurité) qu'elle génère et doit permettre à un administrateur de sécurité de détecter la perte d'alarmes de sécurité (en utilisant un compteur par exemple).

O.BASE_TEMPS

La TOE fournit une base de temps sur laquelle reposent les enregistrements d'audit et garantit sa fiabilité.

5.1.2.5. Administration locale

O.AUTHENTIFICATION_ADMIN

La TOE doit fournir des mécanismes d'identification et d'authentification locale des différents administrateurs conformes au référentiel DCSSI [AUTH].

O.BIENS_INDISPONIBLES

La TOE doit fournir une fonctionnalité qui permet de rendre indisponibles les biens sensibles d'un chiffreur IP préalablement à un changement de contexte d'utilisation: nouvelle affectation, maintenance,...

5.2. Objectifs de sécurité pour l'environnement opérationnel

5.2.1. Administrateurs

OE.ADMIN

Les administrateurs doivent être formés aux tâches qu'ils ont à réaliser sur la TOE.

5.2.2. Cryptographie

OE.CRYPTO

Les clés cryptographiques, générées à l'extérieur, qui sont injectées dans la TOE doivent avoir été générées en suivant les recommandations spécifiées dans les référentiels cryptographiques de la DCSSI [CRYPTO] et [CRYPTO_GESTION] pour le niveau de résistance standard.

5.2.3. Audit et alarme

OE.ANALYSE_AUDIT

L'auditeur doit régulièrement analyser les événements d'audit enregistrés par la TOE et agir en conséquence. De plus, la gestion de la mémoire stockant les événements d'audit doit être faite de telle sorte que l'auditeur ne perde pas d'événements.

OE.TRAITE_ALARME

L'administrateur de sécurité doit traiter les alarmes de sécurité générées par la TOE.

5.2.4. Matériels et logiciels

OE.PROTECTION_LOCAL

L'environnement physique de la TOE, comprenant les équipements sur lesquels la TOE se trouvent, doit protéger la TOE. Ces équipements, ainsi que les supports contenant tout ou partie des biens sensibles de la TOE doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

Cependant, les équipements contenant les services de la TOE peuvent ne pas se trouver dans des locaux sécurisés s'ils ne contiennent pas de biens sensibles: par exemple dans les cas de changement de contexte d'utilisation d'un chiffreur IP.

OE.INTEGRITE_TOE

L'environnement de la TOE doit permettre de vérifier l'intégrité de la configuration matérielle et logicielle de la TOE.

6. Exigences de sécurité

6.1. Exigences de sécurité fonctionnelles

Dans les exigences, qui sont écrites en anglais, l'expression "chiffreur IP" a été traduite par "IP encrypter". Les autres traductions sont évidentes.

Dans les exigences, les trois termes suivants sont utilisés pour désigner un raffinement:

- Raffinement éditorial (terme défini dans [CC1]): raffinement dans lequel une modification mineure est faite sur un élément d'exigence, telle que la reformulation d'une phrase pour des raisons de respect de la grammaire anglaise. En aucun cas, cette modification ne doit changer la signification de l'exigence,
- Raffinement non éditorial: raffinement qui permet d'ajouter des précisions ou de limiter l'ensemble des implémentations acceptables pour un élément d'exigence.

6.1.1. Application des politiques de sécurité VPN

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 encrypter using a given VPN link**
- **Operations: sending and receiving operations that cause applicative and topologic data to flow through the IP encrypters 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**.

Raffinement non éditorial:

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

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 encrypter: "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 encrypter**

- **"undefined" if no VPN policy is associated with the VPN link used by the IP encrypter**

- **[assignment: other security attributes]**.

Raffinement non éditorial:

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**.

Raffinement non éditorial:

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]**.

Raffinement non éditorial :

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

Raffinement non éditorial :

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])**.

Raffinement non éditorial:

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. Protection des politiques de sécurité VPN

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 encrypter 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 encrypter 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 encrypter 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]**.

Raffinement non éditorial :

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.

Raffinement non éditorial :

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. Politique de gestion des clés

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 encrypter 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 encrypter 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]**.

Raffinement non éditorial :

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

Note d'application

Les règles d'importation additionnelles ne doivent pas mettre en échec les exigences d'intégrité (FDP_UIT.1/Key_policy) et de confidentialité (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.

Raffinement non éditorial:

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

Note d'application

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.

Raffinement non éditorial :

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

Note d'application

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]**.

Raffinement non éditorial:

"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 et 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 encrypters**.

6.1.5. Protection des TSF et des TSF data

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 et alarmes

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]**.

Raffinement non éditorial :

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 encrypters.

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]**.

Raffinement non éditorial :

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.

Raffinement non éditorial:

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.

Raffinement non éditorial :

TSF provides reliable time stamps for its own use.

6.1.7. Rôles et authentification

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.

Note d'application

Une même personne peut être associée à plusieurs rôles. Dans le cas du chiffreur IP, une même personne pourrait être à la fois l'administrateur de sécurité et l'administrateur système et réseau par exemple.

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.

Raffinement non éditorial:

Le mécanisme d'authentification doit être conforme au référentiel [AUTH] de la DCSSI.

6.2. Exigences de sécurité d'assurance

Le niveau des exigences d'assurance de sécurité est EAL3 augmenté de ALC_FLR.3 et AVA_VAN.3.

7. Argumentaires

7.1. Objectifs de sécurité / problème de sécurité

7.1.1. Menaces

7.1.1.1. Menaces portant sur les politiques de sécurité VPN et leurs contextes

T.MODIFICATION_POL Cette menace est contrée par O.DEFINITION_POL, O.PROTECTION_POL et O.AUTHENTIFICATION_ADMIN qui imposent que les politiques de sécurité VPN et leurs contextes ne peuvent être modifiés que par des administrateurs de sécurité authentifiés comme tels.

Les objectifs suivants contribuent aussi à la couverture de la menace:

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.
- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.
- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.DIVULGATION_POL Cette menace est contrée par O.DEFINITION_POL, O.PROTECTION_POL O.AUTHENTIFICATION_ADMIN et O.VISUALISATION_POL qui imposent que les politiques de sécurité VPN et leurs contextes ne peuvent être consultés/visualisées que par des administrateurs de sécurité authentifiés comme tels.

Les objectifs suivants contribuent aussi à la couverture de la menace:

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.
- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.
- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

7.1.1.2. Menaces portant sur la configuration

T.MODIFICATION_PARAM O.PROTECTION_PARAM contre cette menace en protégeant en intégrité les paramètres de configuration. Cet objectif plus O.AUTHENTIFICATION_ADMIN permettent de garantir que seuls les administrateurs

système et réseau et les administrateurs de sécurité authentifiés comme tels peuvent accéder à ces paramètres.

Les objectifs suivants contribuent aussi à la couverture de la menace:

- o O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.
- o O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.
- o OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.DIVULGATION_PARAM L'objectif O.PROTECTION_PARAM contre cette menace en protégeant en confidentialité les paramètres de configuration. Les objectifs O.SUPERVISION et O.AUTHENTIFICATION_ADMIN permettent de garantir que seuls les administrateurs système et réseau et les administrateurs de sécurité authentifiés comme tels peuvent accéder à ces paramètres.

Les objectifs suivants contribuent aussi à la couverture de la menace:

- o O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.
- o O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.
- o OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

7.1.1.3. Menaces portant sur la gestion des clés

T.MODIFICATION_CLES Cette menace est contrée par O.INJECTION_CLES lors de l'injection des clés dans les chiffreurs, car cet objectif garantit la protection en intégrité des clés lors de leur injection. De plus, les objectifs O.INJECTION_CLES et O.AUTHENTIFICATION_ADMIN garantissent que seuls les administrateurs de sécurité authentifiés comme tels peuvent injecter des clés. Cette menace est aussi contrée par O.ACCES_CLES qui protège l'accès logique aux clés.

Les objectifs suivants contribuent aussi à la couverture de la menace:

- o O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.
- o O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- o OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.DIVULGATION_CLES Cette menace est contrée par O.INJECTION_CLES lors de l'injection des clés dans les chiffreurs, car cet objectif garantit la protection en confidentialité des clés lors de leur injection. De plus, les objectifs O.INJECTION_CLES et O.AUTHENTIFICATION_ADMIN garantissent que seuls les administrateurs de sécurité authentifiés comme tels peuvent injecter des clés. Cette menace est aussi contrée par O.ACCES_CLES qui protège l'accès logique aux clés. Enfin, cette menace est contrée par O.CRYPTO qui garantit un renouvellement régulier des clés et donc rend plus difficile l'utilisation de clés divulguées.

Les objectifs suivants contribuent aussi à la couverture de la menace:

- o O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.
- o O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.
- o OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

7.1.1.4. Menaces portant sur l'audit

T.MODIFICATION_AUDIT Cette menace est contrée par O.PROTECTION_AUDIT et O.AUTHENTIFICATION_ADMIN qui imposent que les enregistrements d'événements d'audit ne peuvent être supprimés que par des auditeurs authentifiés comme tels.

Les objectifs suivants contribuent aussi à la couverture de la menace:

- o O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.
- o O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.
- o OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.MODIFICATION_ALARME Cette menace est contrée par O.PROTECTION_ALARME et O.AUTHENTIFICATION_ADMIN qui imposent que les alarmes de sécurité ne sont accessibles qu'à un administrateur de sécurité et qu'elles sont protégées en intégrité.

Les objectifs suivants contribuent aussi à la couverture de la menace:

- o O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.
- o O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations

des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.BASE_TEMPS Cette menace est couverte par l'objectif O.BASE_TEMPS qui garantit la fiabilité de la base de temps.

7.1.1.5. Menaces portant sur l'administration

T.USURPATION_ADMIN Cette menace est contrée par O.AUTHENTIFICATION_ADMIN, car cet objectif impose l'authentification des différents administrateurs avant d'effectuer toute opération d'administration.

Les objectifs suivants contribuent aussi à la couverture de la menace:

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

T.BIENS_INDISPONIBLES Cette menace est couverte par O.BIENS_INDISPONIBLES, car il impose que la TOE fournisse une fonctionnalité qui permette de rendre les biens sensibles de la TOE indisponibles lors d'un changement de contexte d'utilisation. De plus, cette menace est couverte par OE.PROTECTION_LOCAL, car il impose que les équipements de la TOE doivent se trouver dans un local sécurisé lorsqu'ils contiennent des biens sensibles.

7.1.2. Politiques de sécurité organisationnelles (OSP)

OSP.SERVICES_RENDUS Cette OSP est couverte par O.CONFIDENTIALITE_APPLI, O.AUTHENTICITE_APPLI, O.CONFIDENTIALITE_TOPO et O.AUTHENTICITE_TOPO qui imposent que la TOE fournisse les services de sécurité. Elle est aussi couverte par O.APPLICATION_POL et O.CLOISONNEMENT_FLUX qui imposent que ces services de sécurité sont appliqués et permettent de cloisonner les flux IP.

O.AUDIT_VPN et O.ALARMES couvrent cette OSP, car ils assurent que les opérations concernant les liens VPN sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

Cette OSP est couverte par OE.INTEGRITE_TOE, car il garantit que l'intégrité du code des logiciels qui appliquent les politiques de sécurité VPN peut être vérifiée.

OSP.CRYPTO Cette OSP est couverte par O.CRYPTO et OE.CRYPTO.

OSP.VISUALISATION_POL Cette OSP est couverte par O.VISUALISATION_POL, car il fournit la visualisation unitaire des politiques de sécurité VPN, ce qui permet à un

administrateur de sécurité de vérifier visuellement qu'il a définit correctement chaque politique de sécurité VPN.

OSP.SUPERVISION Cette OSP est couverte par O.SUPERVISION.

7.1.3. Hypothèses

7.1.3.1. Hypothèses sur l'usage attendu de la TOE

A.AUDIT Cette hypothèse est supportée par OE.ANALYSE_AUDIT.

A.ALARME Cette hypothèse est supportée par OE.TRAITE_ALARME.

7.1.3.2. Hypothèses sur l'environnement d'utilisation de la TOE

A.ADMIN Cette hypothèse est supportée par OE.ADMIN qui impose la formation des administrateurs à leurs tâches.

A.LOCAL Cette hypothèse est supportée par OE.PROTECTION_LOCAL, car il impose que les équipements de la TOE ainsi que les supports contenant les biens sensibles de la TOE se trouvent dans un lieu sécurisé.

A.MAITRISE_CONFIGURATION Cette hypothèse est supportée par OE.INTEGRITE_TOE.

A.CRYPTO Cette hypothèse est supportée par OE.CRYPTO.

7.1.4. Tables de couverture entre définition du problème et objectifs de sécurité

Menaces	Objectifs de sécurité	Argumentaire
T.MODIFICATION_POL	O.DEFINITION_POL, O.IMPACT_SUPERVISION, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN, O.AUDIT_ADMIN, O.ALARMES, OE.INTEGRITE_TOE	Section 7.1.1
T.DIVULGATION_POL	O.DEFINITION_POL, O.IMPACT_SUPERVISION, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN, O.AUDIT_ADMIN, O.ALARMES, OE.INTEGRITE_TOE, O.VISUALISATION_POL	Section 7.1.1
T.MODIFICATION_PARAM	O.PROTECTION_PARAM, O.IMPACT_SUPERVISION, O.AUTHENTIFICATION_ADMIN, O.AUDIT_ADMIN, O.ALARMES, OE.INTEGRITE_TOE	Section 7.1.1

Menaces	Objectifs de sécurité	Argumentaire
T.DIVULGATION_PARAM	O.PROTECTION_PARAM, O.IMPACT_SUPERVISION, O.AUTHENTIFICATION_ADMIN, O.AUDIT_ADMIN, O.ALARMES, OE.INTEGRITE_TOE, O.SUPERVISION	Section 7.1.1
T.MODIFICATION_CLES	O.ACCES_CLES, O.INJECTION_CLES, O.IMPACT_SUPERVISION, O.AUTHENTIFICATION_ADMIN, O.AUDIT_ADMIN, O.ALARMES, OE.INTEGRITE_TOE	Section 7.1.1
T.DIVULGATION_CLES	O.INJECTION_CLES, O.ACCES_CLES, O.IMPACT_SUPERVISION, O.AUTHENTIFICATION_ADMIN, O.AUDIT_ADMIN, O.ALARMES, OE.INTEGRITE_TOE, O.CRYPTO	Section 7.1.1
T.MODIFICATION_AUDIT	O.IMPACT_SUPERVISION, O.PROTECTION_AUDIT, O.AUTHENTIFICATION_ADMIN, OE.INTEGRITE_TOE, O.AUDIT_ADMIN, O.ALARMES	Section 7.1.1
T.MODIFICATION_ALARME	O.IMPACT_SUPERVISION, O.PROTECTION_ALARME, O.AUTHENTIFICATION_ADMIN, OE.INTEGRITE_TOE, O.AUDIT_ADMIN, O.ALARMES	Section 7.1.1
T.BASE_TEMPS	O.BASE_TEMPS	Section 7.1.1
T.USURPATION_ADMIN	O.AUTHENTIFICATION_ADMIN, O.AUDIT_ADMIN, O.ALARMES	Section 7.1.1
T.BIENS_INDISPONIBLES	O.BIENS_INDISPONIBLES, OE.PROTECTION_LOCAL	Section 7.1.1

Tableau 1 Association menaces vers objectifs de sécurité

Objectifs de sécurité	Menaces
O.APPLICATION_POL	
O.CONFIDENTIALITE_APPLI	
O.AUTHENTICITE_APPLI	
O.CONFIDENTIALITE_TOPO	
O.AUTHENTICITE_TOPO	
O.CLOISONNEMENT_FLUX	
O.DEFINITION_POL	T.MODIFICATION_POL, T.DIVULGATION_POL
O.PROTECTION_POL	T.MODIFICATION_POL, T.DIVULGATION_POL
O.VISUALISATION_POL	T.DIVULGATION_POL
O.CRYPTO	T.DIVULGATION_CLES
O.ACCES_CLES	T.MODIFICATION_CLES, T.DIVULGATION_CLES
O.INJECTION_CLES	T.MODIFICATION_CLES, T.DIVULGATION_CLES
O.PROTECTION_PARAM	T.MODIFICATION_PARAM, T.DIVULGATION_PARAM
O.SUPERVISION	T.DIVULGATION_PARAM
O.IMPACT_SUPERVISION	T.MODIFICATION_POL, T.DIVULGATION_POL, T.MODIFICATION_PARAM, T.DIVULGATION_PARAM, T.MODIFICATION_CLES, T.DIVULGATION_CLES, T.MODIFICATION_AUDIT, T.MODIFICATION_ALARME
O.AUDIT_VPN	
O.AUDIT_ADMIN	T.MODIFICATION_POL, T.DIVULGATION_POL, T.MODIFICATION_PARAM, T.DIVULGATION_PARAM, T.MODIFICATION_CLES, T.DIVULGATION_CLES, T.MODIFICATION_AUDIT, T.MODIFICATION_ALARME, T.USURPATION_ADMIN
O.PROTECTION_AUDIT	T.MODIFICATION_AUDIT

Objectifs de sécurité	Menaces
O.ALARMES	T.MODIFICATION_POL, T.DIVULGATION_POL, T.MODIFICATION_PARAM, T.DIVULGATION_PARAM, T.MODIFICATION_CLES, T.DIVULGATION_CLES, T.MODIFICATION_AUDIT, T.MODIFICATION_ALARME, T.USURPATION_ADMIN
O.PROTECTION_ALARME	T.MODIFICATION_ALARME
O.BASE_TEMPS	T.BASE_TEMPS
O.AUTHENTIFICATION_ADMIN	T.MODIFICATION_POL, T.DIVULGATION_POL, T.MODIFICATION_PARAM, T.DIVULGATION_PARAM, T.MODIFICATION_CLES, T.DIVULGATION_CLES, T.MODIFICATION_AUDIT, T.MODIFICATION_ALARME, T.USURPATION_ADMIN
O.BIENS_INDISPONIBLES	T.BIENS_INDISPONIBLES
OE.ADMIN	
OE.CRYPTO	
OE.ANALYSE_AUDIT	
OE.TRAITE_ALARME	
OE.PROTECTION_LOCAL	T.BIENS_INDISPONIBLES
OE.INTEGRITE_TOE	T.MODIFICATION_POL, T.DIVULGATION_POL, T.MODIFICATION_PARAM, T.DIVULGATION_PARAM, T.MODIFICATION_CLES, T.DIVULGATION_CLES, T.MODIFICATION_AUDIT, T.MODIFICATION_ALARME

Tableau 2 Association objectifs de sécurité vers menaces

Politiques de sécurité organisationnelles (OSP)	Objectifs de sécurité	Argumentaire
OSP.SERVICES_RENDUS	O.APPLICATION_POL, O.CONFIDENTIALITE_APPLI, O.AUTHENTICITE_APPLI, O.CONFIDENTIALITE_TOPO, O.AUTHENTICITE_TOPO, O.CLOISONNEMENT_FLUX, O.AUDIT_VPN, OE.INTEGRITE_TOE, O.ALARMES	Section 7.1.2
OSP.CRYPTO	O.CRYPTO, OE.CRYPTO	Section 7.1.2
OSP.VISUALISATION_POL	O.VISUALISATION_POL	Section 7.1.2
OSP.SUPERVISION	O.SUPERVISION	Section 7.1.2

Tableau 3 Association politiques de sécurité organisationnelles vers objectifs de sécurité

Objectifs de sécurité	Politiques de sécurité organisationnelles (OSP)
O.APPLICATION_POL	OSP.SERVICES_RENDUS
O.CONFIDENTIALITE_APPLI	OSP.SERVICES_RENDUS
O.AUTHENTICITE_APPLI	OSP.SERVICES_RENDUS
O.CONFIDENTIALITE_TOPO	OSP.SERVICES_RENDUS
O.AUTHENTICITE_TOPO	OSP.SERVICES_RENDUS
O.CLOISONNEMENT_FLUX	OSP.SERVICES_RENDUS
O.DEFINITION_POL	
O.PROTECTION_POL	
O.VISUALISATION_POL	OSP.VISUALISATION_POL
O.CRYPTO	OSP.CRYPTO
O.ACCES_CLES	
O.INJECTION_CLES	
O.PROTECTION_PARAM	
O.SUPERVISION	OSP.SUPERVISION
O.IMPACT_SUPERVISION	
O.AUDIT_VPN	OSP.SERVICES_RENDUS
O.AUDIT_ADMIN	
O.PROTECTION_AUDIT	
O.ALARMES	OSP.SERVICES_RENDUS
O.PROTECTION_ALARME	
O.BASE_TEMPS	
O.AUTHENTIFICATION_ADMIN	
O.BIENS_INDISPONIBLES	
OE.ADMIN	
OE.CRYPTO	OSP.CRYPTO
OE.ANALYSE_AUDIT	
OE.TRAITE_ALARME	
OE.PROTECTION_LOCAL	
OE.INTEGRITE_TOE	OSP.SERVICES_RENDUS

Tableau 4 Association objectifs de sécurité vers politiques de sécurité organisationnelles

Hypothèses	Objectifs de sécurité pour l'environnement opérationnel	Argumentaire
A.AUDIT	OE.ANALYSE_AUDIT	Section 7.1.3
A.ALARME	OE.TRAITE_ALARME	Section 7.1.3
A.ADMIN	OE.ADMIN	Section 7.1.3
A.LOCAL	OE.PROTECTION_LOCAL	Section 7.1.3
A.MAITRISE_CONFIGURATION	OE.INTEGRITE_TOE	Section 7.1.3
A.CRYPTO	OE.CRYPTO	Section 7.1.3

Tableau 5 Association hypothèses vers objectifs de sécurité pour l'environnement opérationnel

Objectifs de sécurité pour l'environnement opérationnel	Hypothèses
OE.ADMIN	A.ADMIN
OE.CRYPTO	A.CRYPTO
OE.ANALYSE_AUDIT	A.AUDIT
OE.TRAITE_ALARME	A.ALARME
OE.PROTECTION_LOCAL	A.LOCAL
OE.INTEGRITE_TOE	A.MAITRISE_CONFIGURATION

Tableau 6 Association objectifs de sécurité pour l'environnement opérationnel vers hypothèses

7.2. Exigences de sécurité / objectifs de sécurité

7.2.1. Objectifs

7.2.1.1. Objectifs de sécurité pour la TOE

7.2.1.1.1. Objectifs de sécurité sur les services rendus par la TOE

O.APPLICATION_POL Cet objectif est couvert par la politique d'application VPN (FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy, FDP_ITC.1/Enforcement_policy et FDP_ETC.1/Enforcement_policy), car elle contrôle les flux de paquets IP en leur appliquant des services de sécurité fournit par les opérations cryptographiques de FCS_COP.1/Enforcement_policy.

O.CONFIDENTIALITE_APPLI Cet objectif est couvert par FCS_COP.1/Enforcement_policy qui fournit les opérations cryptographiques pour protéger des données en confidentialité.

O.AUTHENTICITE_APPLI Cet objectif est couvert par FCS_COP.1/Enforcement_policy qui fournit les opérations cryptographiques pour protéger des données en authenticité.

O.CONFIDENTIALITE_TOPO Cet objectif est couvert par FCS_COP.1/Enforcement_policy qui fournit les opérations cryptographiques pour protéger des données en confidentialité.

O.AUTHENTICITE_TOPO Cet objectif est couvert par FCS_COP.1/Enforcement_policy qui fournit les opérations cryptographiques pour protéger des données en authenticité.

O.CLOISONNEMENT_FLUX Cet objectif est couvert par la politique d'application VPN (FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy et FDP_ETC.1/Enforcement_policy), car elle contrôle l'envoi des paquets IP sur les sous-réseaux appropriés du réseau privé.

7.2.1.1.2. Objectifs de sécurité pour protéger les biens sensibles de la TOE

7.2.1.1.2.1 Gestion des politiques de sécurité VPN

O.DEFINITION_POL Cet objectif est couvert par la politique de protection des politiques de sécurité VPN (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 et FMT_SMF.1/VPN_policy) qui contrôle l'accès à la définition des politiques de sécurité VPN.

O.PROTECTION_POL Cet objectif est couvert par la politique de protection des politiques de sécurité VPN qui contrôle les accès à ces politiques et leurs contextes: FDP_ACC.1/VPN_policy, FDP_ACF.1/VPN_policy, FMT_MSA.3/VPN_policy, FMT_MSA.1/VPN_policy et FMT_SMF.1/VPN_policy.

O.VISUALISATION_POL Cet objectif est couvert par la politique de protection des politiques de sécurité VPN (FDP_ACC.1/VPN_policy et FDP_ACF.1/VPN_policy) en

contrôlant l'accès à l'opération de visualisation des politiques de sécurité VPN et de leurs contextes.

7.2.1.1.2.2 Gestion des clés cryptographiques

O.CRYPTO Cet objectif est couvert par les exigences concernant les clés cryptographiques et les opérations cryptographiques:

- opérations cryptographiques: FCS_COP.1/Enforcement_policy,
- renouvellement des clés: FCS_CKM.3/Key_policy
- destruction des clés: FCS_CKM.4/Key_policy.

O.ACCES_CLES Cet objectif est couvert par la politique des clés (FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy et FMT_MSA.3/Key_policy) qui contrôle les flux de clés.

O.INJECTION_CLES Cet objectif est couvert par la politique des clés (FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FDP_ITC.1/Key_policy et FMT_MSA.3/Key_policy) qui contrôle les flux de clés d'injection de clés. Par ailleurs, FDP_UCT.1/Key_policy et FDP_UIT.1/Key_policy garantissent l'intégrité de toutes les clés et la confidentialité de clés privées et secrètes pendant leur transmission.

7.2.1.1.2.3 Configuration et supervision

O.PROTECTION_PARAM Cet objectif est couvert par FMT_MTD.1/Network_param (pour les paramètres de configuration réseau), FMT_MTD.1/Param (pour les droits d'accès et les données d'authentification), et FMT_SMF.1/Config_supervision, car ces exigences assurent la protection des paramètres de configuration en confidentialité et intégrité en restreignant l'accès aux opérations qui manipulent ces paramètres.

O.SUPERVISION Cet objectif est couvert par FMT_SMF.1/Config_supervision, car cette exigence demande une fonction de supervision de l'état des chiffreurs IP.

O.IMPACT_SUPERVISION Cet objectif est couvert par toutes les politiques de contrôles d'accès et de flux d'information concernant les biens sensibles de la TOE en restreignant l'accès aux opérations manipulant ces biens: 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 et FDP_IFF.1/Enforcement_policy. De plus, pour les mêmes raisons cet objectif est couvert par toutes les exigences portant sur la gestion des données de la TSF: FMT_MTD.1/Network_param et FMT_MTD.1/Param.

7.2.1.1.2.4 Audit et alarme

O.AUDIT_VPN Cet objectif est couvert par FAU_GEN.1/VPN qui assure la génération d'événement d'audit pour les liens de communication VPN. De plus, cet objectif est aussi couvert par FAU_SAR.1 et FAU_SAR.3 qui fournissent la consultation des événements d'audit.

O.AUDIT_ADMIN Cet objectif est couvert par FAU_GEN.1/Administration qui assure la génération d'événement d'audit concernant les opérations d'administration. De plus, cet

objectif est aussi couvert par FAU_SAR.1 et FAU_SAR.3 qui fournissent la consultation des événements d'audit.

O.PROTECTION_AUDIT Cet objectif est couvert par FAU_STG.1 qui protège en intégrité les enregistrements d'événements d'audit. De plus, FAU_GEN.1/VPN et FAU_GEN.1/Administration permettent de détecter si des événements d'audit ont été perdus.

O.ALARMES Cet objectif est couvert par FAU_ARP.1/Alarm qui exige de lever une alarme de sécurité quand une violation potentielle de sécurité est détectée et par FAU_SAA.1/Alarm qui indique les règles utilisées pour détecter ces violations potentielles.

O.PROTECTION_ALARME Cet objectif est couvert par FAU_STG.1 qui protège en intégrité les enregistrements d'alarmes de sécurité. De plus, FAU_GEN.1/VPN et FAU_GEN.1/Administration permettent de détecter si des alarmes de sécurité ont été perdues.

O.BASE_TEMPS Cet objectif est directement couvert par l'exigence FPT_STM.1.

7.2.1.1.2.5 Administration locale

O.AUTHENTIFICATION_ADMIN Cet objectif est couvert par FIA_UID.2 et FIA_UAU.2 qui exige l'identification et l'authentification des utilisateurs avant d'effectuer toute opération d'administration locale. De plus, cet objectif est couvert par FMT_SMR.1 qui demande le maintien des différents rôles par la TOE.

O.BIENS_INDISPONIBLES Cet objectif est couvert par FDP_RIP.1, car cette exigence assure que la TOE permet de rendre indisponible le contenu des ressources qui correspondent aux biens sensibles de la TOE. De plus, cet objectif est couvert par FCS_CKM.4/Key_policy, car cette exigence impose que la TOE puisse détruire ses clés cryptographiques.

7.2.2. Tables de couverture entre objectifs et exigences de sécurité

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.APPLICATION_POL	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.CONFIDENTIALITE_APPLI	FCS_COP.1/Enforcement_policy	Section 7.2.1
O.AUTHENTICITE_APPLI	FCS_COP.1/Enforcement_policy	Section 7.2.1
O.CONFIDENTIALITE_TOPO	FCS_COP.1/Enforcement_policy	Section 7.2.1
O.AUTHENTICITE_TOPO	FCS_COP.1/Enforcement_policy	Section 7.2.1
O.CLOISONNEMENT_FLUX	FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy, FDP_ETC.1/Enforcement_policy	Section 7.2.1

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.DEFINITION_POL	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.PROTECTION_POL	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.VISUALISATION_POL	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.ACCES_CLES	FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FMT_MSA.3/Key_policy	Section 7.2.1
O.INJECTION_CLES	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.PROTECTION_PARAM	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
O.IMPACT_SUPERVISION	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.AUDIT_VPN	FAU_GEN.1/VPN, FAU_SAR.1, FAU_SAR.3	Section 7.2.1
O.AUDIT_ADMIN	FAU_GEN.1/Administration, FAU_SAR.1, FAU_SAR.3	Section 7.2.1
O.PROTECTION_AUDIT	FAU_STG.1, FAU_GEN.1/VPN, FAU_GEN.1/Administration	Section 7.2.1
O.ALARMES	FAU_ARP.1/Alarm, FAU_SAA.1/Alarm	Section 7.2.1

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.PROTECTION_ALARME	FAU_STG.1, FAU_GEN.1/VPN, FAU_GEN.1/Administration	Section 7.2.1
O.BASE_TEMPS	FPT_STM.1	Section 7.2.1
O.AUTHENTIFICATION_ADMIN	FMT_SMR.1, FIA_UID.2, FIA_UAU.2	Section 7.2.1
O.BIENS_INDISPONIBLES	FDP_RIP.1, FCS_CKM.4/Key_policy	Section 7.2.1

Tableau 7 Association objectifs de sécurité de la TOE vers les exigences fonctionnelles

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_IFC.1/Enforcement_policy	O.APPLICATION_POL, O.CLOISONNEMENT_FLUX, O.IMPACT_SUPERVISION
FDP_IFF.1/Enforcement_policy	O.APPLICATION_POL, O.CLOISONNEMENT_FLUX, O.IMPACT_SUPERVISION
FDP_ITC.1/Enforcement_policy	O.APPLICATION_POL
FDP_ETC.1/Enforcement_policy	O.APPLICATION_POL, O.CLOISONNEMENT_FLUX
FCS_COP.1/Enforcement_policy	O.APPLICATION_POL, O.CONFIDENTIALITE_APPLI, O.AUTHENTICITE_APPLI, O.CONFIDENTIALITE_TOPO, O.AUTHENTICITE_TOPO, O.CRYPTO
FDP_ACC.1/VPN_policy	O.DEFINITION_POL, O.PROTECTION_POL, O.VISUALISATION_POL, O.IMPACT_SUPERVISION
FDP_ACF.1/VPN_policy	O.DEFINITION_POL, O.PROTECTION_POL, O.VISUALISATION_POL, O.IMPACT_SUPERVISION
FDP_ITC.1/VPN_policy	O.DEFINITION_POL
FMT_MSA.3/VPN_policy	O.DEFINITION_POL, O.PROTECTION_POL
FMT_MSA.1/VPN_policy	O.DEFINITION_POL, O.PROTECTION_POL
FMT_SMF.1/VPN_policy	O.DEFINITION_POL, O.PROTECTION_POL
FDP_IFC.1/Key_policy	O.ACCES_CLES, O.INJECTION_CLES, O.IMPACT_SUPERVISION
FDP_IFF.1/Key_policy	O.ACCES_CLES, O.INJECTION_CLES, O.IMPACT_SUPERVISION
FDP_ITC.1/Key_policy	O.INJECTION_CLES
FDP_UCT.1/Key_policy	O.INJECTION_CLES
FDP_UIT.1/Key_policy	O.INJECTION_CLES
FMT_MSA.3/Key_policy	O.ACCES_CLES, O.INJECTION_CLES
FCS_CKM.4/Key_policy	O.BIENS_INDISPONIBLES, O.CRYPTO
FCS_CKM.3/Key_policy	O.CRYPTO

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FMT_MTD.1/Network_param	O.PROTECTION_PARAM, O.IMPACT_SUPERVISION
FMT_MTD.1/Param	O.PROTECTION_PARAM, O.IMPACT_SUPERVISION
FMT_SMF.1/Config_supervision	O.PROTECTION_PARAM, O.SUPERVISION
FDP_RIP.1	O.BIENS_INDISPONIBLES
FAU_GEN.1/VPN	O.AUDIT_VPN, O.PROTECTION_AUDIT, O.PROTECTION_ALARME
FAU_GEN.1/Administration	O.AUDIT_ADMIN, O.PROTECTION_AUDIT, O.PROTECTION_ALARME
FAU_SAR.1	O.AUDIT_VPN, O.AUDIT_ADMIN
FAU_SAR.3	O.AUDIT_VPN, O.AUDIT_ADMIN
FAU_STG.1	O.PROTECTION_AUDIT, O.PROTECTION_ALARME
FAU_ARP.1/Alarm	O.ALARMES
FAU_SAA.1/Alarm	O.ALARMES
FPT_STM.1	O.BASE_TEMPS
FMT_SMR.1	O.AUTHENTIFICATION_ADMIN
FIA_UID.2	O.AUTHENTIFICATION_ADMIN
FIA_UAU.2	O.AUTHENTIFICATION_ADMIN

Tableau 8 Association exigences fonctionnelles vers objectifs de sécurité de la TOE

7.3. Dépendances

7.3.1. Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_IFC.1/Enforcement_policy	(FDP_IFF.1)	FDP_IFF.1/Enforcement_policy
FDP_IFF.1/Enforcement_policy	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ITC.1/Enforcement_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ETC.1/Enforcement_policy	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Enforcement_policy
FCS_COP.1/Enforcement_policy	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (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) et (FMT_MSA.3)	FDP_ACC.1/VPN_policy, FMT_MSA.3/VPN_policy
FDP_ITC.1/VPN_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_ACC.1/VPN_policy, FMT_MSA.3/VPN_policy
FMT_MSA.3/VPN_policy	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/VPN_policy, FMT_SMR.1
FMT_MSA.1/VPN_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1/VPN_policy, FMT_SMF.1/VPN_policy, FMT_SMR.1
FMT_SMF.1/VPN_policy	Pas de dépendance	
FDP_IFC.1/Key_policy	(FDP_IFF.1)	FDP_IFF.1/Key_policy
FDP_IFF.1/Key_policy	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Key_policy, FMT_MSA.3/Key_policy
FDP_ITC.1/Key_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Key_policy, FMT_MSA.3/Key_policy
FDP_UCT.1/Key_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Key_policy

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_UIT.1/Key_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Key_policy
FMT_MSA.3/Key_policy	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1
FCS_CKM.4/Key_policy	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)	FDP_ITC.1/Key_policy
FCS_CKM.3/Key_policy	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FCS_CKM.4/Key_policy, FDP_ITC.1/Key_policy
FMT_MTD.1/Network_param	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1
FMT_MTD.1/Param	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1
FMT_SMF.1/Config_supervision	Pas de dépendance	
FDP_RIP.1	Pas de dépendance	
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	Pas de dépendance	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	Pas de dépendance	
FIA_UAU.2	(FIA_UID.1)	FIA_UID.2

Tableau 9 Dépendances des exigences fonctionnelles

7.3.1.1. Argumentaire pour les dépendances non satisfaites

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_UCT.1/Key_policy n'est pas supportée. FDP_UCT.1/Key_policy requiert la confidentialité des clés cryptographiques importées dans la TOE. Ce Profil de Protection laisse au développeur le choix du type de canal de confiance (FTP_ITC.1 ou FTP_TRP.1) que la TOE doit implémenter.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_UIT.1/Key_policy n'est pas supportée. FDP_UCT.1/Key_policy requiert l'intégrité des clés cryptographiques importées dans la TOE. Ce Profil de Protection laisse au développeur le choix du type de canal de confiance (FTP_ITC.1 ou FTP_TRP.1) que la TOE doit implémenter.

La dépendance FMT_MSA.1 de FMT_MSA.3/Key_policy n'est pas supportée. L'attribut de sécurité AT.key_type ne possède que l'opération de consultation qui est fournie seulement aux TSF. Comme cette opération n'est pas fournie à un rôle donné, cette dépendance n'est pas satisfaite.

7.3.2. Dépendances des exigences de sécurité d'assurance

Exigences	Dépendances CC	Dépendances Satisfaites
ADV_ARC.1	(ADV_FSP.1) et (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	Pas de dépendance	
ALC_CMC.3	(ALC_CMS.1) et (ALC_DVS.1) et (ALC_LCD.1)	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	Pas de dépendance	
ALC_DEL.1	Pas de dépendance	
ALC_FLR.3	Pas de dépendance	
ALC_DVS.1	Pas de dépendance	
ALC_LCD.1	Pas de dépendance	
ASE_CCL.1	(ASE_ECD.1) et (ASE_INT.1) et (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	Pas de dépendance	
ASE_INT.1	Pas de dépendance	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) et (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	Pas de dépendance	
ASE_TSS.1	(ADV_FSP.1) et (ASE_INT.1) et (ASE_REQ.1)	ADV_FSP.3, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) et (ATE_FUN.1)	ADV_FSP.3, ATE_FUN.1

Exigences	Dépendances CC	Dépendances Satisfaites
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) et (AGD_OPE.1) et (AGD_PRE.1) et (ATE_COV.1) et (ATE_FUN.1)	ADV_FSP.3, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) et (ADV_TDS.2) et (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) et (ADV_FSP.2) et (ADV_IMP.1) et (ADV_TDS.3) et (AGD_OPE.1) et (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.3, AGD_OPE.1, AGD_PRE.1

Tableau 10 Dépendances des exigences d'assurance

7.3.2.1. Argumentaire pour les dépendances non satisfaites

La dépendance ADV_IMP.1 de AVA_VAN.3 n'est pas supportée. Cette dépendance n'est pas nécessaire conformément à l'EAL requis pour la qualification standard [QUA-STD].

La dépendance ADV_TDS.3 de AVA_VAN.3 n'est pas supportée. Cette dépendance n'est pas nécessaire conformément à l'EAL requis pour la qualification standard [QUA-STD].

7.4. Argumentaire pour l'EAL

Le niveau d'assurance de ce PP est EAL3+, car il est requis par le processus de qualification standard [QUA-STD].

7.5. Argumentaire pour les augmentations à l'EAL

7.5.1. ALC_FLR.3 Systematic flaw remediation

Augmentation requise par le processus de qualification standard [QUA-STD].

7.5.2. AVA_VAN.3 Focused vulnerability analysis

Augmentation requise par le processus de qualification standard [QUA-STD].

8. Notice

Ce document a été généré avec TL SET version 2.2.8 (for CC3). Pour plus d'informations sur l'outil d'édition sécuritaire de Trusted Labs consultez le site internet www.trusted-labs.com.

A Notes d'application

Comme expliqué dans l'introduction de ce profil de protection, ces notes d'application définissent les éléments (menaces, hypothèses, OSP, objectifs et exigences) spécifiques à chacune des deux options. Les éléments qui sont définis dans ces notes doivent soit être ajoutés au profil, soit remplacer des éléments déjà existant pour la configuration minimale. Dans ce dernier cas, les identifiants des éléments utilisés dans ces notes sont ceux utilisés pour la configuration minimale.

La première section concerne les éléments pour l'option d'administration à distance, la deuxième pour l'option de négociation dynamique. Enfin, la troisième section présente l'argumentaire de la configuration maximale supportant les deux options à la fois.

A.1 Option « Administration à distance »

A.1.1 Description de la TOE

Les chiffreurs IP peuvent aussi être administrés à distance : c'est une administration qui s'effectue au travers d'un réseau LAN ou WAN.

Distribution des politiques de sécurité VPN

Une fois les politiques de sécurité VPN définies, elles sont distribuées aux chiffreurs IP concernés avec leurs contextes de sécurité. La cohérence entre la politique définie par l'administrateur de sécurité en utilisant un outil et celle se trouvant dans le chiffreur IP concerné doit être assurée afin que la protection des données circulant sur les liens VPN soit bien celle attendue et définie par l'administrateur de sécurité. Cet outil de définition de politique doit garantir la fiabilité de la traduction entre le langage utilisé par l'administrateur de sécurité pour définir la politique (en utilisant l'outil) et le langage utilisé dans les chiffreurs IP pour appliquer ces politiques.

Un canal sécurisé doit être utilisé pour distribuer les politiques de sécurité VPN et leurs contextes de sécurité afin de les protéger en authenticité et confidentialité.

Protection des flux d'administration à distance

Ce service permet de protéger en authenticité les flux de données échangées entre les chiffreurs IP et les équipements d'administration pour effectuer des opérations d'administration à distance. Ce service permet aussi de protéger en confidentialité les flux d'administration. Cette protection concerne les flux d'administration de sécurité (politiques de sécurité VPN et clés) et les flux d'administration système et réseau (paramètres de configuration). En revanche, ce service n'applique pas cette protection aux flux de supervision. Ce service est divisé en deux parties qui sont toutes les deux incluses dans la TOE : l'une sur les chiffreurs IP et l'autre sur les équipements d'administration.

Protection contre le rejeu des flux d'administration

Ce service protège contre le rejeu de séquences d'opérations d'administration à distance passant sur les liens entre les chiffreurs IP et les équipements d'administration.

A.1.2 Environnement de sécurité

A.1.2.1 Menaces

T.COHERENCE_POL

Un attaquant modifie la politique de sécurité VPN appliquée au niveau d'un sous-réseau IP, qui est donc différente de celle définie par l'administrateur de sécurité pour ce sous-réseau.

Bien menacé: D.POLITIQUES_VPN.

T.REJEU_ADMIN

Un attaquant capture une séquence de paquets passant à travers des flux d'administration, correspondant à une séquence complète pour effectuer une opération d'administration, et la rejoue pour en retirer un certain bénéfice.

Biens menacés: tous les biens.

A.1.3 Objectifs de sécurité

A.1.3.1 Objectifs de sécurité pour la TOE

O.COHERENCE_POL

La TOE doit garantir la cohérence des définitions des politiques de sécurité VPN (et de leurs contextes) avec les politiques appliquées sur chaque chiffreur IP lors de l'administration à distance.

O.DISTRIBUTION_POL

La TOE doit protéger en confidentialité et en authenticité les politiques de sécurité VPN et leurs contextes de sécurité qui transitent entre l'équipement contenant le logiciel permettant de les définir et les chiffreurs IP.

O.PROTECTION_REJEU_ADMIN

La TOE doit empêcher le rejeu d'une séquence d'envoi de données d'administration.

O.PROTECTION_FLUX_ADMIN

La TOE doit garantir l'authenticité et la confidentialité des flux d'administration à distance. La protection en confidentialité n'est pas systématiquement appliquée si les données passant dans le flux ne sont pas confidentielles telles que les clés publiques.

A.1.3.2 Objectifs de sécurité pour l'environnement

OE.AUTHENTIFICATION_ADMIN

L'environnement de la TOE doit fournir des mécanismes d'identification et d'authentification à distance des différents administrateurs. Il doit aussi s'assurer que l'accès aux services de téléadministration est conditionné par une authentification préalable sur la station d'administration.

A.1.4 Exigences de sécurité fonctionnelles pour la 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]**.

Raffinement non éditorial :

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 encypter 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 encrypter 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 encrypter 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 encrypter 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 encrypter 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 encrypter 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 encrypter 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 [Raffiné éditorialement] The TSF shall protect TSF data from **disclosure (when data are confidential) and modification** when it is transmitted between separate parts of the TOE.

Raffinement non éditorial:

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 encrypter.**

- **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 encrypter**.

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 encrypter and an administration equipment**.

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

A.2 Option « Négociation dynamique »

A.2.1 Description de la TOE

Définition des politiques de sécurité VPN

Lorsqu'une phase de négociation est effectuée entre deux chiffreurs IP, une partie des politiques de sécurité et des contextes de sécurité peut être définie lors de cette phase en tenant compte de contraintes définies auparavant. Ces contraintes de sécurité globales sont définies par l'administrateur de sécurité et peuvent comprendre plusieurs stratégies classées par ordre de préférence selon leur force ou leur résistance à des attaques. Les chiffreurs IP peuvent entamer une négociation pour se mettre d'accord sur une politique de sécurité VPN spécifique à appliquer en respectant les contraintes globales et les ordres de préférence définis par l'administrateur de sécurité, de manière à choisir dynamiquement la politique la plus forte commune aux deux chiffreurs IP devant établir un lien VPN.

Ce service doit permettre à chaque chiffreur IP de s'authentifier auprès d'un autre chiffreur IP (et réciproquement) afin de négocier le contexte de sécurité (algorithmes à utiliser pour le chiffrement, algorithme pour le scellement, longueur des clés, durée de vie, ...) avant d'établir des liens VPN légitimes. Ce service est utile pour les chiffreurs IP qui sont amenés à générer des clés à la volée (lors de chaque établissement de liens VPN).

Génération des clés cryptographiques

Ce service permet aux chiffreurs IP de générer des clés à l'issue de la phase d'authentification mutuelle et de négociation lors de l'établissement de liens VPN. Ces clés générées seront ensuite utilisées pour appliquer les services de sécurité des politiques de sécurité VPN.

A.2.2 Environnement de sécurité

Il n'y a pas d'élément de l'environnement spécifique à cette option.

A.2.3 Objectifs de sécurité

A.2.3.1 Objectifs de sécurité pour la TOE

O.DEFINITION_POL

La TOE doit permettre seulement à l'administrateur de sécurité de définir les politiques de sécurité VPN et leurs contextes de sécurité. La TOE doit aussi permettre de s'assurer qu'une négociation d'une partie de politique et de contexte entre deux chiffreurs IP conduit au choix d'une politique et d'un contexte conformes à la stratégie décidée par l'administrateur de sécurité.

O.AUTHENTIFICATION_MUTUELLE

La TOE doit fournir un mécanisme d'authentification mutuelle pour les chiffreurs IP qui communiquent entre eux et ainsi permettre de négocier dynamiquement les politiques de sécurité VPN et leurs contextes.

A.2.4 Exigences de sécurité fonctionnelles pour la 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 encypter 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 encrypter 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 encrypter 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 encrypter 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 encrypter.**
- **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.

Raffinement non éditorial :

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])**.

Raffinement non éditorial:

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 encrypters.

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 encrypters**.

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 encrypter 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 encrypter 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])**.

Raffinement non éditorial:

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

A.3 Argumentaire de la configuration maximale

A.3.1 Argumentaire pour les objectifs de sécurité

A.3.1.1 Menaces

T.MODIFICATION_POL Cette menace est contrée par O.DEFINITION_POL, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN et OE.AUTHENTIFICATION_ADMIN qui imposent que les politiques de sécurité VPN et leurs contextes ne peuvent être modifiés que par des administrateurs de sécurité authentifiés comme tels. De plus, cette menace est aussi contrée par O.PROTECTION_FLUX_ADMIN et O.DISTRIBUTION_POL qui permettent la protection en authenticité des flux de politiques et de leurs contextes lors de leur distribution aux chiffreurs IP.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.DIVULGATION_POL Cette menace est contrée par O.DEFINITION_POL, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN et OE.AUTHENTIFICATION_ADMIN qui imposent que les politiques de sécurité VPN et leurs contextes ne peuvent être consultés que par des administrateurs de sécurité authentifiés comme tels. De plus, cette menace est aussi contrée par O.PROTECTION_FLUX_ADMIN et O.DISTRIBUTION_POL qui imposent la protection en confidentialité des flux de politiques et de leurs contextes lors de leur distribution aux chiffreurs IP.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.COHERENCE_POL Cette menace est contrée par O.COHERENCE_POL qui garantit la cohérence entre les politiques de sécurité VPN définies par l'administrateur de sécurité et celles appliquées dans les chiffreurs IP.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE, car il garantit que l'intégrité du code des logiciels qui définissent et appliquent les politiques de sécurité VPN peut être vérifiée.

T.MODIFICATION_PARAM O.PROTECTION_PARAM contre cette menace en protégeant en intégrité les paramètres de configuration. Cet objectif plus O.AUTHENTIFICATION_ADMIN et OE.AUTHENTIFICATION_ADMIN permettent de garantir que seuls les administrateurs système et réseau et les administrateurs de sécurité authentifiés comme tels peuvent accéder à ces paramètres. De plus, O.PROTECTION_FLUX_ADMIN garantit l'intégrité de ces paramètres lorsque ceux-ci sont définis à distance.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.DIVULGATION_PARAM O.PROTECTION_PARAM contre cette menace en protégeant en confidentialité les paramètres de configuration. Cet objectif plus O.AUTHENTIFICATION_ADMIN et OE.AUTHENTIFICATION_ADMIN permettent de garantir que seuls les administrateurs système et réseau et les administrateurs de sécurité authentifiés comme tels peuvent accéder à ces paramètres. De plus, O.PROTECTION_FLUX_ADMIN garantit l'intégrité de ces paramètres lorsque ceux-ci sont définis à distance.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.MODIFICATION_CLES Cette menace est contrée par O.INJECTION_CLES et O.PROTECTION_FLUX_ADMIN lors de l'injection des clés dans les chiffreurs, car ces objectifs garantissent la protection en intégrité des clés lors de leur injection. De plus les objectifs O.INJECTION_CLES, O.AUTHENTIFICATION_ADMIN et OE.AUTHENTIFICATION_ADMIN garantissent que seuls les administrateurs de sécurité

authentifiés comme tels peuvent injecter des clés. Cette menace est aussi contrée par O.ACCES_CLES qui protège l'accès logique aux clés.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.DIVULGATION_CLES Cette menace est contrée par O.INJECTION_CLES et O.PROTECTION_FLUX_ADMIN lors de l'injection des clés dans les chiffreurs, car ces objectifs garantissent la protection en confidentialité des clés lors de leur injection. De plus, les objectifs O.INJECTION_CLES, O.AUTHENTIFICATION_ADMIN et OE.AUTHENTIFICATION_ADMIN garantissent que seuls les administrateurs de sécurité authentifiés comme tels peuvent injecter des clés. Cette menace est aussi contrée par O.ACCES_CLES qui protège l'accès logique aux clés. Enfin, cette menace est contrée par O.CRYPTO qui garantit un renouvellement régulier des clés et donc rend plus difficile l'utilisation de clés divulguées.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.MODIFICATION_AUDIT Cette menace est contrée par O.PROTECTION_AUDIT, O.AUTHENTIFICATION_ADMIN et OE.AUTHENTIFICATION_ADMIN qui imposent que les enregistrements d'événements d'audit ne peuvent être supprimés que par des auditeurs authentifiés comme tels. De plus, cette menace est aussi contrée par O.PROTECTION_FLUX_ADMIN qui permet la protection en intégrité des flux d'événements d'audit nécessaire à la consultation de ceux-ci (à distance) par les auditeurs.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.MODIFICATION_ALARME Cette menace est contrée par O.PROTECTION_ALARME, O.AUTHENTIFICATION_ADMIN et OE.AUTHENTIFICATION_ADMIN qui imposent que les alarmes de sécurité ne peuvent être supprimées que par des administrateurs de sécurité authentifiés comme tels. De plus, cette menace est aussi contrée par O.PROTECTION_FLUX_ADMIN qui permet la protection en intégrité des flux d'alarmes de sécurité lors de leur remontée aux administrateurs de sécurité.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.BASE_TEMPS Cette menace est couverte par l'objectif O.BASE_TEMPS qui garantit la fiabilité de la base de temps.

T.USURPATION_ADMIN Cette menace est contrée par O.AUTHENTIFICATION_ADMIN et OE.AUTHENTIFICATION_ADMIN, car ces objectifs imposent l'authentification (locale ou à distance) des différents administrateurs avant d'effectuer toute opération d'administration.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

T.REJEU_ADMIN Cette menace est contrée par O.PROTECTION_REJEU_ADMIN, car il empêche le rejeu d'opérations d'administration.

Les objectifs suivants contribuent aussi à la couverture de la menace :

- O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

- OE.INTEGRITE_TOE, car il garantit que l'intégrité du code des logiciels qui empêche ce rejeu peut être vérifiée.

T.BIENS_INDISPONIBLES Cette menace est couverte par O.BIENS_INDISPONIBLES, car il impose que la TOE fournisse une fonctionnalité qui permette de rendre les biens sensibles de la TOE indisponibles lors d'un changement de contexte d'utilisation. De plus, cette menace est couverte par OE.PROTECTION_LOCAL, car il impose que les équipements de la TOE doivent se trouver dans un local sécurisé lorsqu'ils contiennent des biens sensibles.

A.3.2 Argumentaire pour les exigences de sécurité fonctionnelles

A.3.2.1 Objectifs de sécurité pour la TOE

O.AUTHENTIFICATION_MUTUELLE Cet objectif est couvert par FCS_COP.1/Mutual_auth, car cette exigence fournit toutes les opérations cryptographiques nécessaires pour le mécanisme d'authentification mutuelle. De plus, cet objectif est couvert par FIA_UAU.4/Mutual_auth qui empêche la réutilisation des données d'authentification lors de l'authentification mutuelle.

O.DISTRIBUTION_POL Cet objectif est couvert par la politique de protection des politiques de sécurité VPN (FDP_ACC.1/VPN_policy et FDP_ACF.1/VPN_policy) qui contrôle l'accès à l'opération de distribution des politiques de sécurité VPN. Il est aussi couvert par FPT_ITT.1/Administration et FPT_ITT.3/Administration qui assure une protection en confidentialité et intégrité des flux de politiques de sécurité VPN lors de cette distribution à distance.

O.COHERENCE_POL Cet objectif est couvert par FPT_TRC.1/VPN_policy qui assure une interprétation correcte et par conséquent une application correcte des politiques de sécurité VPN définies.

O.CRYPTO Cet objectif est couvert par les exigences concernant les clés cryptographiques et les opérations cryptographiques:

- opérations cryptographiques: FCS_COP.1/Mutual_auth, FCS_COP.1/Enforcement_policy,
- génération de clés: FCS_CKM.1/Key_policy,
- renouvellement des clés: FTA_TSE.1/Key_policy.

O.INJECTION_CLES Cet objectif est couvert par la politique des clés (FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy et FMT_MSA.3/Key_policy) qui contrôle les flux de clés dont l'injection de clés (FDP_ITC.1/Key_policy). De plus, cet objectif est couvert par FDP_ITT.1/Administration et FDP_ITT.3/Administration qui assure une protection en confidentialité et intégrité des flux de clés lors d'une injection à distance.

O.PROTECTION_PARAM Cet objectif est couvert par FMT_MTD.1/Network_param (pour les paramètres de configuration réseau), FMT_MTD.1/Param (pour les droits d'accès et les données d'authentification) et FMT_SMF.1/Config_supervision, car ces exigences assurent la protection des paramètres de configuration en confidentialité et intégrité en restreignant l'accès aux opérations qui manipulent ces paramètres. De plus, cet objectif est couvert par la politique de configuration et d'audit (FDP_IFC.1/Config_audit et FDP_IFF.1/Config_audit) qui protège en intégrité et en confidentialité les paramètres de configuration lors de leur consultation ou modification à distance.

O.PROTECTION_AUDIT Cet objectif est couvert par FAU_STG.1 qui protège en intégrité les enregistrements d'événements d'audit. Il est aussi couvert par la politique de configuration et d'audit (FDP_IFC.1/Config_audit et FDP_IFF.1/Config_audit) qui protège en intégrité les événements d'audit lors de leur consultation ou suppression à distance. De plus, FAU_GEN.1/VPN et FAU_GEN.1/Administration permettent de détecter si des événements d'audit ont été perdus.

O.PROTECTION_ALARME Cet objectif est couvert par FAU_STG.1 qui protège en intégrité les enregistrements d'alarmes de sécurité. Il est aussi couvert par la politique de configuration et d'audit (FDP_IFC.1/Config_audit et FDP_IFF.1/Config_audit) qui protège en intégrité les alarmes de sécurité lors de leur consultation ou suppression à distance. De plus, FAU_GEN.1/VPN et FAU_GEN.1/Administration permettent de détecter si des alarmes de sécurité ont été perdus.

O.PROTECTION_REJEU_ADMIN Cet objectif est couvert par FPT_RPL.1 qui impose la détection du rejeu de séquences de données d'administration ainsi que les actions à réaliser dans en cas de détection.

O.PROTECTION_FLUX_ADMIN Cet objectif est couvert par FPT_ITT.1/Administration et FPT_ITT.3/Administration qui assure la confidentialité (si nécessaire) et l'intégrité des données qui passent dans les flux d'administration.

A.3.3 Dépendances

A.3.3.1 Dépendances des exigences de sécurité fonctionnelles

Remarque :

Cette table des dépendances reprend l'ensemble des SFR qu'elles soient ou non optionnelles.

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_IFC.1/Enforcement_policy	(FDP_IFF.1)	FDP_IFF.1/Enforcement_policy
FDP_IFF.1/Enforcement_policy	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ITC.1/Enforcement_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ETC.1/Enforcement_policy	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Enforcement_policy
FCS_COP.1/Enforcement_policy	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (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) et (FMT_MSA.3)	FDP_ACC.1/VPN_policy, FMT_MSA.3/VPN_policy
FDP_ITC.1/VPN_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_ACC.1/VPN_policy, FMT_MSA.3/VPN_policy
FMT_MSA.3/VPN_policy	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/VPN_policy, FMT_SMR.1

Exigences	Dépendances CC	Dépendances Satisfaites
FMT_MSA.1/VPN_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1/VPN_policy, FMT_SMF.1/VPN_policy, FMT_SMR.1
FMT_SMF.1/VPN_policy	Pas de dépendance	
FCS_COP.1/mutual_auth	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.1/Key_policy, FCS_CKM.4/Key_policy
FIA_UAU.4/Mutual_auth	Pas de dépendance	
FDP_ITC.1/Key_policy	(FDP_ACC.1 ou FDP_IFC.1) et (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
FDP_IFF.1/Key_policy	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Key_policy, FMT_MSA.3/Key_policy
FDP_UCT.1/Key_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Key_policy
FDP_UIT.1/Key_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Key_policy
FMT_MSA.3/Key_policy	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1
FCS_CKM.1/Key_policy	(FCS_CKM.2 ou FCS_COP.1) et (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 ou FDP_ITC.1 ou FDP_ITC.2)	FDP_ITC.1/Key_policy
FCS_CKM.3/Key_policy	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FCS_CKM.4/Key_policy, FDP_ITC.1/Key_policy
FMT_MTD.1/Network_param	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1
FMT_MTD.1/Param	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1

Exigences	Dépendances CC	Dépendances Satisfaites
FMT_SMF.1/Config_supervision	Pas de dépendance	
FPT_ITT.1/Administration	Pas de dépendance	
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) et (FMT_MSA.3)	FDP_IFC.1/Config_audit
FPT_RPL.1	Pas de dépendance	
FDP_RIP.1	Pas de dépendance	
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	Pas de dépendance	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	Pas de dépendance	
FIA_UAU.2	(FIA_UID.1)	FIA_UID.2

Tableau 11 Tableau 12 Dépendances des exigences fonctionnelles

A.3.3.2 Argumentaire pour les dépendances non satisfaites

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_UCT.1/Key_policy n'est pas supportée. FDP_UCT.1/Key_policy requiert la confidentialité des clés cryptographiques importées dans la TOE. Ce Profil de Protection laisse au développeur le choix du type de canal de confiance (FTP_ITC.1 ou FTP_TRP.1) que la TOE doit implémenter.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_UIT.1/Key_policy n'est pas supportée. FDP_UCT.1/Key_policy requiert l'intégrité des clés cryptographiques

importées dans la TOE. Ce Profil de Protection laisse au développeur le choix du type de canal de confiance (FTP_ITC.1 ou FTP_TRP.1) que la TOE doit implémenter.

La dépendance FMT_MSA.1 de FMT_MSA.3/Key_policy n'est pas supportée. L'attribut de sécurité AT.key_type ne possède que l'opération de consultation qui est fournie seulement aux TSF. Comme cette opération n'est pas fournie à un rôle donné, cette dépendance n'est pas satisfaite.

La dépendance FMT_MSA.3 de FDP_IFF.1/Config_audit n'est pas supportée. Comme il n'y a pas d'attribut de sécurité utilisé dans cette politique de contrôle de flux d'information, cette dépendance n'est pas satisfaite.

B Glossaire

Cette annexe donne la définition des principaux termes utilisés dans ce document. Pour la définition des termes Critères Communs se référer à [CC1], §4.

Administrateur	Utilisateur autorisé à gérer tout ou une partie de la TOE. Il peut posséder des privilèges particuliers qui permettent de modifier la politique de sécurité de la TOE.
Authentification	Mesure de sécurité qui vérifie l'identité déclarée.
Authentification mutuelle	Mesure de sécurité qui permet pour chaque paire d'entités d'authentifier l'autre entité de la paire.
Clé de session	Clé à durée de vie courte générée aléatoirement et utilisée pour assurer la confidentialité, l'authenticité et l'intégrité de données.
Contexte de sécurité	Paramètres de sécurité négociés entre deux chiffreurs IP qui permettent de savoir quelles caractéristiques de sécurité doivent être utilisées pour appliquer la politique de sécurité VPN donnée. Ces paramètres comprennent entre autres les algorithmes cryptographiques, les tailles de clés, ...
Environnement opérationnel	Environnement de la TOE lors de sa phase d'utilisation.
Gateway	Dispositif qui permet d'interconnecter deux réseaux présentant des structures différentes.
Passerelle	Voir Gateway.
Politique de sécurité VPN	Politique de sécurité unidirectionnelle définie entre deux chiffreurs IP donnés. Cette politique spécifie les services de sécurité à appliquer sur les informations qui transitent du chiffreur vers l'autre chiffreur.
Réseau privé	Réseau interne à une entité (comme une entreprise ou un service) qui doit être protégé des flux arrivant de l'extérieur mais pas de ces propres flux. C'est un réseau considéré comme sûr.
Réseau public	Réseau accessible à toute entité et toute personne qui ne peut être considéré comme sûr.

Index