ARKOON FAST360/5.0

Cible de sécurité Critères Communs
Niveau EAL3+

Reference : ST_ARKOON_FAST360_50
Version 2.6
Date : 14/09/2011

ARKOON Network Security
1, place Verrazzano - 69009 Lyon
France

Suivi des modifications

Date	Version	Modifications
0.1	15 janvier 2007	Création du document
0.2	14 mars 2007	Draft soumis à la DCSSI
0.3	02 avril 2007	Version soumise à la DCSSI
0.4	16 mai 2007	Prise en compte des remarques de la DCSSI
0.5	26 novembre 2007	FIA_UAU.2-Station_administration_distante : authentification mutuelle entre les administrateurs et la TOE et ajout des algorithmes cryptographiques dans FCS_COP.1/VPN-Enforcement_policy
0.51	04 décembre 2007	Corrections orthographiques
0.52	06 décembre 2007	Ajout de FCS_CKM.1/VPN-Key_policy pour la génération des clés cryptographiques de sessions.
0.53	11 février 2008	Prise en compte des remarques de la DCSSI
1.0	21 février 2008	Prise en compte des remarques de la DCSSI
1.1	20 Mars 2008	Ajout de la version de la ST concernée
2.0	29 juillet 2009	Prise en compte des remarques du CESTI
2.1	15 Juin 2010	Ajout des 3 rôles supplémentaires gérés par le produit
2.2	02 Sept 2010	Précision de la version mineure du produit
2.3	07 Sept 2010	Mise à jour des objectifs sur l'environnement
2.4	13 Juillet 2011	Mises à jour mineures suite retours Oppida
2.5	22 Juillet 2011	Ajout Reference QS
2.6	14 Septembre 2011	Prise en comptes des remarques de l'ANSSI

Table des matières

Index des figures

Index des tableaux

Références

Référence	Document
[AUTH]	Authentification : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard – version 0.13, ref. N° 729/SGDN/DCSSI/SDS/AsTeC, 12 avril 2007.
[AES]	NIST, FIPS PUB 197, Advanced Encryption Standard (AES), November 2001.
[CC]	Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, ref. ISO/IEC 15408-1:2005(E) - Part 2: Security functional requirements, ref. ISO/IEC 15408-2:2005(E) - Part 3: Security assurance requirements, ref. ISO/IEC 15408-3:2005(E)
[CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, Version 1.10 du 19 décembre 2006. DCSSI, 2741/SGDN/DCSSI/SDS/LCR.
[GC]	Gestion des clés cryptographiques, Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard – version 1.0, ref. N° 724/SGDN/DCSSI/SDS/AsTec, SGDN/DCSSI/SDS/AsTeC, 13 mars 2006.
[PP_CIP]	Profil de protection Chiffreur IP, version 1.5 du 3 février 2005.
[PP_FWIP]	Profil de protection Firewall d'interconnexion IP, version 2.2, 10 mars 2006.
[QS]	Processus de qualification d'un produit de sécurité - niveau standard - version 1.2
[RSA]	RSA Laboratories. PKCS #1 v2.1: RSA Encryption Standard. June 2000.
[SHA256]	FIPS 180-2, Secure Hash Standard (SHS), August 2002

Glossaire

Glossaire issu des Critères Communs [CC] :

Terme	*Définition*
OSP	Organisational Security Policy: Politique de sécurité de l'environnement dans lequel s'insère le produit ou le système à évaluer et qui peut avoir un impact sur ses fonctions de sécurité.
SOF	Strength Of Function: Niveau de résistance intrinsèque d'une fonction face à des attaques. Ce niveau ne doit pas être confondu avec le niveau de résistance global de la TOE (niveau défini par le composant AVA_VLA) qui prend en compte des attaques altérant ou rendant inopérantes des fonctions de la TOE.
ST	Security Target : le présent document
TOE	Target Of Evaluation: il s'agit du produit ou du système dont la présente cible de sécurité constitue le cahier des charges de l'évaluation.
TSF	TOE Security Functions: Sous-ensemble du produit ou du système à évaluer qui participe à la réalisation des exigences fonctionnelles de sécurité.

Glossaire de la TOE :

Terme	*Définition*
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.
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, …
Politique de filtrage	Politique de sécurité définie pour la gestion des flux au niveau d'une interconnexion. Cette poltique est appliquée par le pare-feu de la TOE. Le terme *politique de sécurité du pare-feu* est également utilisé.
Politique de sécurité	Politique de sécurité de la TOE, composée des politiques de filtrage du pare-feu de la TOE et des politiques de sécurité VPN du chiffreur IP de la TOE.
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 externe	Réseau accessible à toute entité et toute personne qui ne peut être

	considéré comme sûr. Le terme *réseau public* est également utilisé.
Réseau interne	Réseau interne à une entité (comme une entreprise ou un service) qui doit être protégé des flux arrivant de l'extérieur, et dont on doit maîtriser les flux sortants. C'est un réseau considéré comme sûr. Le terme *réseau protégé* est également utilisé. Le pare-feu de la TOE est l'interface entre un réseau interne et un réseau externe.
Réseau privé	Réseau interne à une entité (comme une entreprise ou un service) dont les communications avec d'autres réseaux privés via un réseau public doivent être protégées en confidentialité, en intégrité et en authenticité. Le service de chiffrement IP de la TOE permet de protéger les communications entre deux réseaux privés.

Acronymes

Les acronymes suivants, issus des Critères Communs **[CC]**, sont utilisés dans la présente cible de sécurité :

Acronyme	*Anglais*	*Français*
CC	Common Criteria	Critères Communs
EAL	Evaluation Assurance Level	Niveau d'assurance de l'évaluation
IT	Information Technology	Technologie de l'information
OSP	Organisational Security Policy	Politique de sécurité de l'organisation
PP	Protection Profile	Profil de protection
SF	Security Function	Fonction de sécurité
SFR	Security Functional Requirement	Exigence de sécurité fonctionnelle
SFP	Security Function Policy	Politique de la fonction de sécurité
SOF	Strength Of Function	Résistance des fonctions
ST	Security Target	Cible de sécurité
TOE	Target Of Evaluation	Cible de l'évaluation
TSP	TOE Security Policy	Politique de sécurité de la cible d'évaluation
TSF	TOE Security Functions	Fonctions de sécurité de la TOE

Les acronymes suivants, non issus des Critères Communs, sont utilisés dans la présente cible de sécurité :

Acronyme	*Définition*
CEC	Centre d'Elaboration des clés
DMZ	Demilitarized Zone
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IKE	Internet Key Exchange

IP	Internet Protocol
IPSEC	IP Security Protocol
LAN	Local Area Network
NAT	Network Address Translation
OS	Operating System
PC	Personal Computer
SMTP	Simple Mail Transfer Protocol

Conventions utilisées

La liste ci-après fournit les racines utilisées pour les différents éléments identifiés dans la présente cible de sécurité.

Racine	***Eléments désignés***
D.FW.	Biens sensibles de la TOE relatifs au service pare-feu de la TOE
D.VPN.	Biens sensibles de la TOE relatifs au service VPN de la TOE
A.FW.	Hypothèses relatives au service pare-feu de la TOE
A.VPN	Hypothèses relatives au service VPN de la TOE
T.FW.	Menaces relatives au service pare-feu de la TOE
T.VPN.	Menaces relatives au service VPN de la TOE
OSP.FW	Politiques de sécurité de l'organisation relatives au service pare-feu de la TOE
OSP.VPN	Politiques de sécurité de l'organisation relatives au service VPN de la TOE

1 Introduction

1.1 Identification du document

Titre	Cible de sécurité Arkoon FAST360
Référence	ST_ARKOON_FAST360_50
Version	2.6
Auteur(s)	Arkoon, Oppida
Date	14 Septembre 2011
Produit	Arkoon FAST360 5.0/22
Identification CC	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (ISO 15408)
Niveau d'assurance	Evaluation Assurance Level 3 (EAL3) augmenté des composants ALC_FLR.3 et AVA_VLA.2
Résistance des fonctions (SOF)	SOF-high

Le présent document constitue la cible de sécurité du produit Arkoon FAST360 5.0/22.

Ce document précise les exigences de sécurité en termes fonctionnels et en termes de tâches d'évaluation qui doivent être satisfaites par le produit évalué (la cible de l'évaluation, ci-après la « TOE »).
La cible de sécurité indique également comment le produit évalué répond à ces exigences.

1.2 Organisation du document

Le **Chapitre 1** constitue l'introduction du document.
Le **Chapitre 2** décrit dans un langage naturel les services fournis par le produit évalué (la TOE) ainsi que son architecture.
Le **Chapitre 3** précise les conditions prévues d'exploitation du produit évalué ; en particulier les services de sécurité offerts par le produit et les menaces auxquelles le produit aura à faire face.
Le **Chapitre 4** indique les objectifs de sécurité à atteindre par le produit et par son environnement d'exploitation notamment pour offrir les services de sécurité requis et contrer les menaces identifiées.
Le **Chapitre 5** détaille les exigences de sécurité à satisfaire pour atteindre ces objectifs de sécurité : exigences fonctionnelles et exigences d'assurance.
Le **Chapitre 6** indique les fonctionnalités présentes dans le produit évalué pour répondre aux exigences fonctionnelles et les mesures mises en places pour répondre aux exigences d'assurance.
Le **Chapitre 7** indique si le produit évalué se veut également conforme aux exigences spécifiées dans un profil de protection (PP).
Le **Chapitre 8** regroupe tous les argumentaires permettant de s'assurer notamment de la couverture complète des menaces par les objectifs de sécurité et les exigences de sécurité ou de la couverture des exigences fonctionnelles par les fonctionnalités du produit.

1.3 Conformité aux Critères communs

Le présent document est conforme aux exigences de la norme ISO/IEC 15408: 2005 (Critères communs version 2.3) [CC].

2 Description de la TOE

2.1 Présentation générale

Les appliances UTM Arkoon FAST360 sont conçues pour protéger un réseau informatique contre le plus large spectre de menaces.

Basées sur la technologie brevetée FAST (Fast Applicative Shield Technology), les appliances FAST360 réunissent les fonctions de pare-feu, de serveur VPN/IPSEC, de détection et de prévention d'intrusions en temps réel, d'antivirus, d'antispyware, serveur d'authentification…

Les appliances UTM Arkoon FAST360 sont disponibles en plusieurs gammes (notamment NPA – Network Processor Appliance) permettant ainsi de répondre aux besoins de performance de chacun.

Fournis nativement avec tout équipement de sécurité réseau ARKOON, les outils d'administration Arkoon Management Tools permettent l'administration (Arkoon Manager) et la supervision (Arkoon Monitoring) de la politique de sécurité réseau de façon centralisée.

Ils permettent de configurer et de superviser un ensemble d'appliances UTM Arkoon FAST360 à partir d'une seule console d'administration. Ils sont adaptés à des configurations multisites importantes, notamment grâce à des fonctionnalités complémentaires telle que l'architecture "maître/esclave" permettant de télédistribuer les configurations et d'automatiser les process de mise à jour.

2.1.1 Pare-feu FAST

Grâce à leur technologie FAST, les appliances UTM FAST360 permettent à la fois un contrôle "temps réel" au niveau applicatif (niveaux 5 à 7) et un contrôle "Stateful" (niveaux 3 et 4) des flux internet sans compromettre les performances du réseau.

Le service de filtrage des appliances FAST bloque les attaques en contrôlant la conformité aux RFC de plus de 20 protocoles les plus utilisés (HTTP, SMTP, FTP, POP3, IMAP4, NNTP, DNS, RTSP, H323, Netbios, SSL,…), en applicant des règles permettant de détecter l'utilisation anormale de ces protocoles et en limitant certaines commandes ou paramètres des protocoles, à potentiel intrusif.

Le pare-feu FAST est doté d'une technologie de décodage applicatif permettant l'analyse les paquets circulant sur le réseau. Cette technologie décode le protocole applicatif utilisé, vérifie la conformité de la communication par rapport à la norme du protocole applicatif (RFC) et dissocie dans cette même communication les différents éléments du protocole applicatif (commandes, paramètres, données, etc...).
Elle est proactive face aux attaques inconnues car elle permet de détecter et de bloquer les attaques qui violent les protocoles applicatifs, ainsi que celles qui ne sont pas conformes aux règles d'utilisation de ces protocoles, définies par l'administrateur sécurité (règle d'usage)

La technologie FAST combine un très haut de niveau de sécurité avec des performances exceptionnelles qui permet de gérer des débits supérieurs à 4 Gbits/s, 2 millions de connexions simultanées et plus de 40000 nouvelles connexions par seconde.

2.1.2 VPN FAST

Les appliances UTM FAST360 intègrent un serveur VPN/IPSEC supportant les applications de communication "Lan to Lan" et "Host to Lan" ou la protection des réseaux WiFi avec des niveaux de performance très élevés (jusqu'à 500 Mbits/s en AES et 25000 tunnels simultanés).

Basé sur la norme IPSec qui lui garantit l'interopérabilité avec les solutions du marché, le module VPN supporte notamment les algorithmes de chiffrement 3DES, AES 128/192/256 et Blowfish. Grâce à sa fonctionnalité NAT-Traversal, il est compatible avec les systèmes de translation d'adresses. Il supporte les systèmes d'authentification forte (clé USB, carte à puce, biométrie, ...) et s'appuie sur les méthodes d'authentification par clé partagée et certificat X509. Ces certificats peuvent être générés soit par l'Autorité de Certification proposée par ARKOON en standard sur les appliances, soit par une PKI externe.

2.2 Architecture

Seule la partie logicielle de la TOE, et non le matériel, est soumise à l'évaluation Critères Communs.

2.2.1 Architecture du système

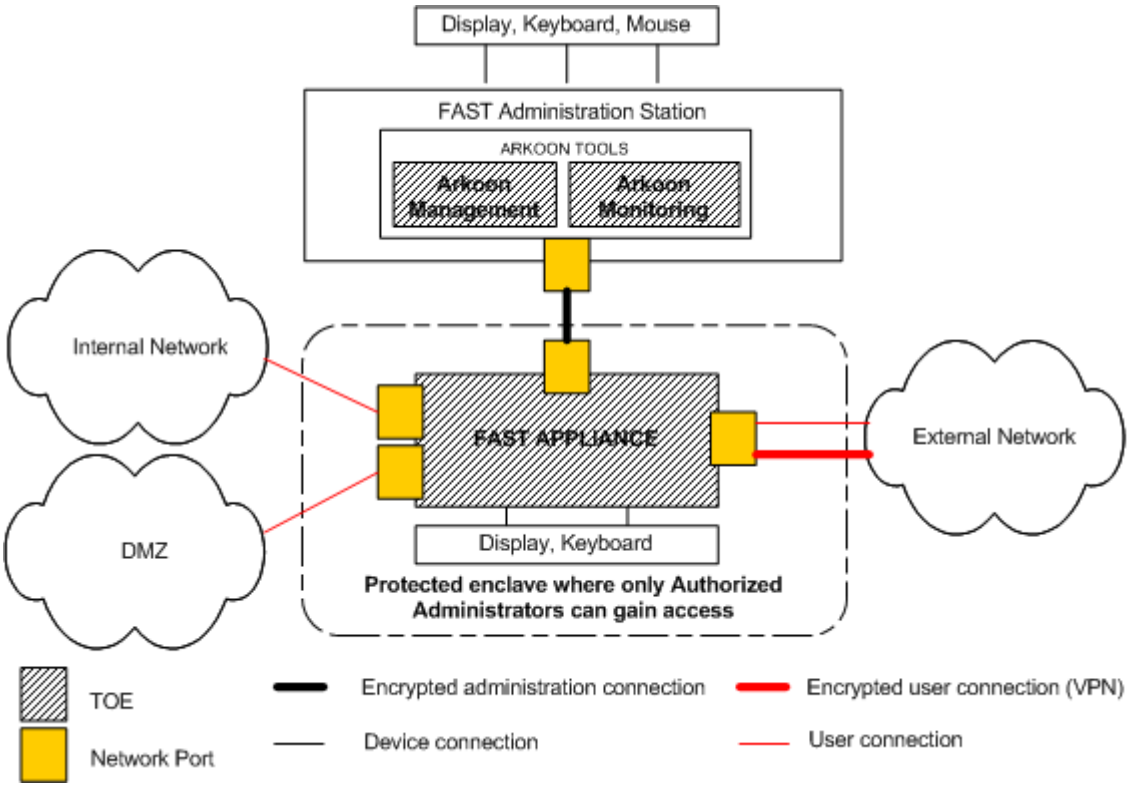

Figure 1 : Interfaces de la TOE

La TOE est dotée de quatre interfaces réseau :

1. une interface administration : cette interface relie la TOE à sa station d'administration via un réseau d'administration, et permet donc l'administration à distance de la TOE.
2. une interface réseau externe : cette interface relie la TOE au réseau externe, considéré comme non sûr (Internet par exemple).
3. une interface réseau interne : cette interface relie la TOE au réseau interne, c'est-à-dire le réseau protégé par la TOE.
4. une interface réseau DMZ : relie la TOE à un réseau DMZ, c'est-à-dire un réseau sur lequel seuls les machines devant être visibles depuis le réseau externe sont présentes.

La TOE peut être administrée à distance via une station d'administration sur laquelle les outils Arkoon (Arkoon Tools) sont installés (Arkoon Management et Arkoon Monitoring). Les outils Arkoon permettent aux administrateurs de s'authentifier auprès de la TOE, et les opérations d'administration sont protégées en confidentialité, intégrité et authenticité par la TOE.
Les opérations d'administration de la TOE ne sont réalisées que depuis l'interface réseau d'administration de la TOE, et en aucun cas les flux d'administration ne transitent par une autre interface réseau de la TOE (externe, interne ou DMZ).

La TOE offre également un service d'administration locale minimale, via un écran et un clavier branchés directement sur l'appliance, permettant aux administrateurs d'effectuer leurs opérations.

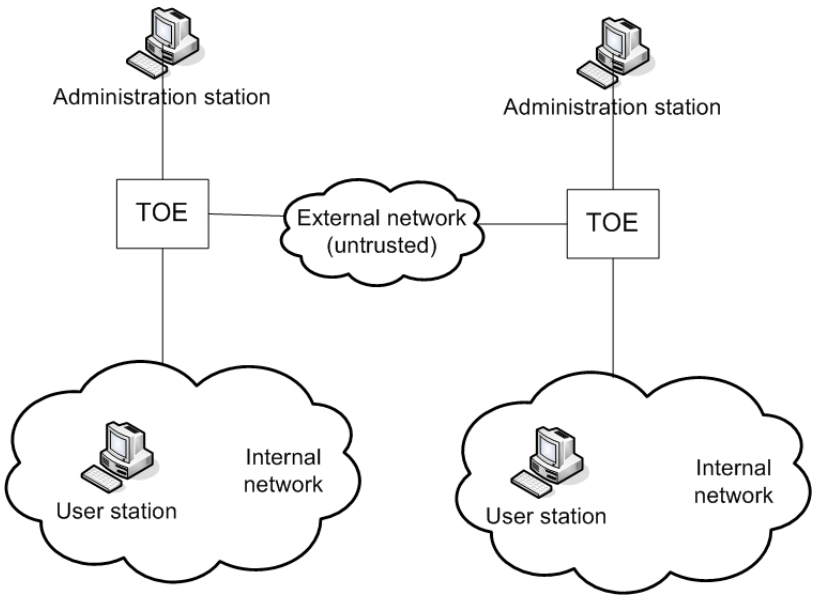

Figure 2 : Architecture d'évaluation de la TOE

Comme le montre la figure ci-dessus, la configuration dans laquelle la TOE sera évaluée est la suivante : deux TOE reliées via un réseau externe (non sûr) via leur interface externe. Chaque TOE disposera de sa propre station d'administration (reliée à l'interface administration de la TOE) sur laquelle les outils Arkoon Management et Arkoon Monitoring sont installés.

Figure 3 : Architecture interne de la TOE

La TOE est constituée des éléments suivants :

FAST Management Console : Logiciel installé sur la station d'administration distante permettant aux administrateurs de sécurité de la TOE de s'authentifier et de réaliser des opérations d'administration sur la TOE.

FAST Monitoring Console : Logiciel installé sur la station d'administration distante permettant aux administrateurs système et réseau de configurer les paramètres réseau de la TOE et de superviser l'état de la TOE.

Service d'authentification : Ce service permet d'authentifier les stations d'administrations distantes et les administrateurs de la TOE (locaux et distants).

Service d'administration : Ce service offre des fonctionnalités d'administration de la TOE différentes en fonction des rôles de chacun des administrateurs. La TOE distingue sept rôles différents pour les administrateurs : responsable de sécurité, administrateur de sécurité, auditeur

et administrateur système et réseau, superviseur système et réseau, superviseur sécurité et rôle « Toutes Autorisations »

Service d'audit : Ce service permet d'enregistrer dans des journaux les évènements relatifs à la TOE : opérations d'administration, flux traités par le pare-feu de la TOE, flux traités par le chiffreur IP de la TOE, …

Centre d'Elaboration des Clés (CEC) : il permet à la TOE de générer elle-même ses propres clés cryptographiques (ce composant est hors périmètre de l'évaluation (voir 2.2.2).

Service d'échange de clés (IKE): Afin de créer les clés cryptographiques symétriques utilisés par la pile IPSec, le service d'échange de clé établit une connexion sécurisée entre deux machines communiquant à travers un réseau hostile. Implémentant, la norme Internet Key Exchange (IKE), ce service interopère avec tous les services d'échange de clés IKE du marché.

Operating System Kernel : Le kernel, partie fondamentale du système d'exploitation, gère l'ensemble des ressources matérielles et logicielles et permet à l'ensemble des composants de communiquer entre eux.

IP Stack: La pile IP est le module en charge de l'acheminement des paquets IP en appliquant les règles de routage.

IPSEC Stack : Ce module permet de garantir l'authenticité, la confidentialité et la protection contre le rejeu des données d'une communication IP entre deux machines. Il reçoit des clés cryptographiques symétriques négociées par le service d'échange de clé IKE, les stocke pendant leur durée de vie, et les utilise pour appliquer la politique de chiffrement sur les flux. Ce module implémente la norme IPSec, il peut intéropérer avec tous les autres produits IPSec du marché.

FAST Engine : Ce mécanisme est le cœur de la technologie FAST360 et met en œuvre les règles qui acceptent ou refusent l'établissement d'une nouvelle connexion. En appliquant les règles de filtrage et soumettant pour validation, les flux aux modules spécialisés par protocole, il fournit un ensemble de services comme par exemple le suivi des sessions, la limitation du nombre de connexions établies ou en attentes.

IP Packet filter : L'IP Packet filter est le module FAST en charge du filtrage IP. Il fournit des mécanismes spécifiques IP tels que la limitation du nombre de connexions, la translation d'adresses (NAT) et la gestion des options IP.

Transport Layer filters : Ces filtres sont les modules FAST en charge du filtrage des protocoles de niveau transport : TCP et UDP. Ils assurent que les paquets reçus respectent les contraintes définies par les normes de ces protocoles. Par exemple, un mécanisme contrôle le séquencement des paquets TCP.

Applicative layer filters : Ces modules sont activés par configuration de la politique de filtrage. Ils permettent d'analyser la conformité d'un flux à un protocole applicatif (HTTP, FTP, SMTP, DNS) et de le filtrer sur la base de la politique applicative paramétrée par l'administrateur de sécurité.

2.2.2 Limites du périmètre de l'évaluation

Les éléments constituant la TOE sont :
1. FAST Administration Station (c.f. Figure 1)
Cet élément se compose de deux logiciels : FAST Management Console et FAST Monitoring Console. Seuls leurs modules permettant l'authentification et la protection (confidentialité, intégrité, authenticité) des flux échangés entre ces outils d'administration et FAST Appliance sont inclus dans le périmètre de l'évaluation.

2 - FAST Appliance (c.f. Figure 1)
Cet élément comprend :

- des services : authentification, administration, audit, échange de clés (IKE). Cesservices sont inclus dans le périmètre de l'évaluation.
- un Centre d'Elaboration des Clés (« Key Generation Center » sur la figure 3) qui ne fait pas partie de l'évaluation
- le noyau du système d'exploitation : IP Stack, IPSEC Stack, FAST Engine, IP Packet filter, Transport Layer filters, Applicative layer filters. Ces modules sont inclusdans le périmètre de l'évaluation.

Seule la partie logicielle est évaluée dans le cadre de la TOE.

Le Centre d'Elaboration des Clés offert par la TOE et permettant à la TOE de générer elle-même ses propres clés cryptographiques ne fait pas partie du périmètre de l'évaluation. La non-inclusion du CEC dans le périmètre de l'évaluation est justifiée par le fait que le PP [PP_CIP] duquel le service VPN de la TOE s'inspire mentionne que le CEC est hors TOE.

2.3 Services fournis par la TOE

2.3.1 Services fournis par la TOE

2.3.1.1 Pare-feu : application de la politique de filtrage

Le pare-feu de la TOE permet d'assurer le filtrage des flux IP entre deux réseaux IP conformément à une politique de sécurité définie par l'administrateur de sécurité de la TOE.

Le pare-feu de la TOE permet donc d'autoriser ou de rejeter les paquets IP en fonction de leurs caractéristiques (port source, port destination, adresse IP source, adresse IP destination, protocole, application…) conformément à la politique de filtrage définie par l'administrateur de sécurité.

2.3.1.2 Chiffreur IP : application de la politique de sécurité VPN

Le chiffreur IP de la TOE permet d'assurer la protection en authenticité, en confidentialité et en intégrité des flux échangés entre deux réseaux privés en utilisant le protocole IPSEC. Le chiffreur IP permet d'assurer :

- Protection en confidentialité des données applicatives : en chiffrant les données applicatives encapsulées dans les flux IP, le chiffreur IP empêche la divulgation de

ces dernières lorsqu'elle transitent sur un réseau public non sûr (Internet par exemple).
- Protection en authenticité des données applicatives : en signant les données applicatives encapsulées dans les flux IP, le chiffreur IP permet de détecter toute modification de ces dernières.
- Protection en confidentialité des données topologiques : en chiffrant les données topologiques des paquets IP, le chiffreur IP empêche la divulgation des adresses IP internes (source et destination) des équipements se trouvant dans le réseaux privés.
- Protection en authenticité des données topologiques : en signant les données topologiques des paquets IP, le chiffreur permet de détecter toute modification de ces dernières.
- Cloisonnement des flux : en cloisonnant un réseau privé en plusieurs sous-réseaux. Le cloisonnement des flux permet d'appliquer des politiques de sécurité VPN différentes selon chaque sous-réseau.

2.3.2 Services d'administration fournis par la TOE

La figure ci-dessous représente un diagramme d'utilisation UML montrant les principaux services offerts par la TOE aux administrateurs.

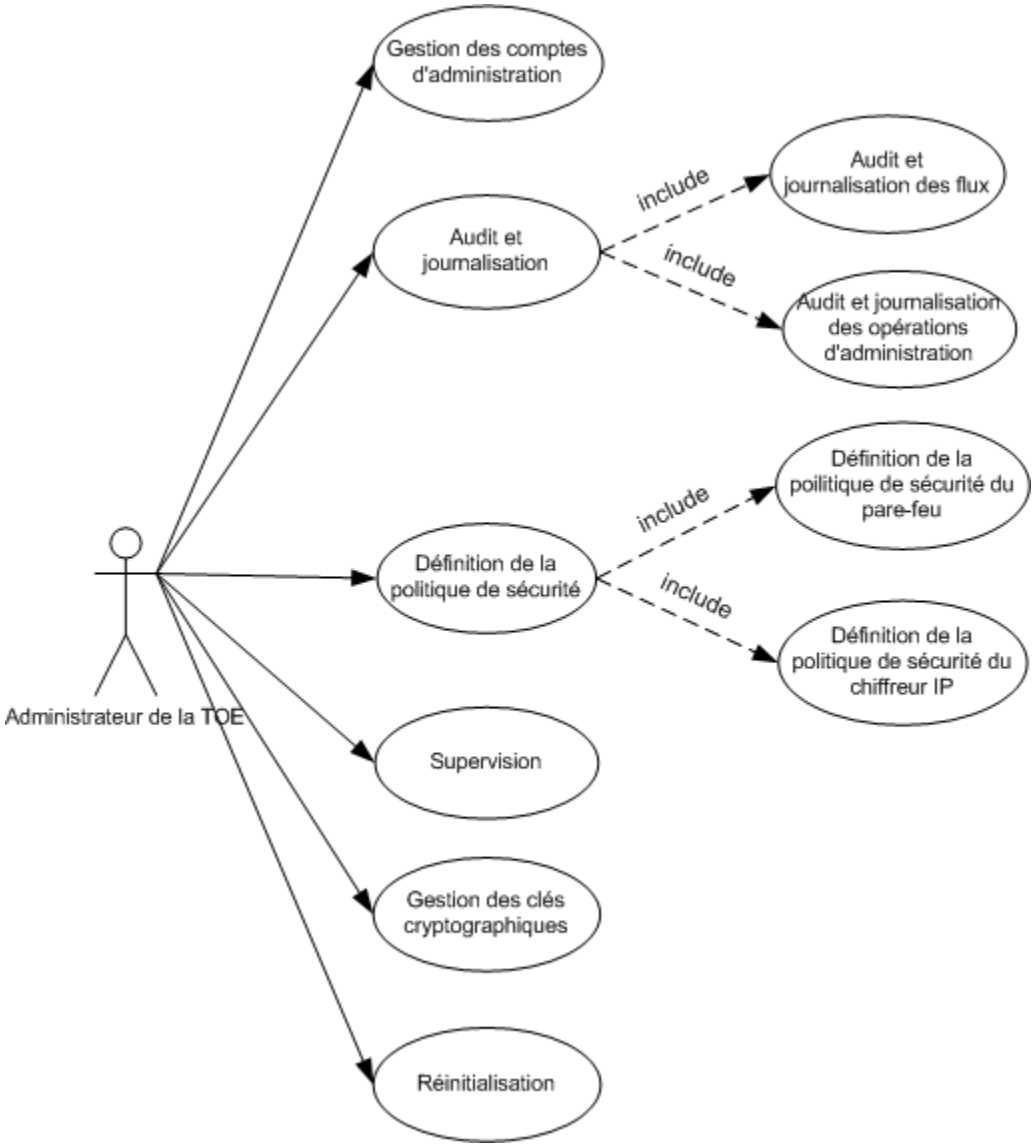

Figure 4 : Services d'administration offerts par la TOE aux administrateurs

2.3.2.1 Gestion des comptes d'administration

Ce service permet aux responsables de sécurité de la TOE de gérer les comptes des administrateurs de la TOE.

2.3.2.2 Audit et journalisation des flux

Ce service permet d'enregistrer dans des journaux d'audit tous les flux IP transitant par le pare-feu et le chiffreur IP. Il permet également à l'administrateur de sécurité de définir les conditions d'enregistrement d'un flux dans ces journaux (flux accepté, flux rejeté, adresse IP source, adresse IP destination, erreur d'intégrité, …). Ce service permet également de générer des alarmes dont les caractéristiques sont définies par l'administrateur de sécurité. Ce service

permet également aux administrateurs de sécurité, aux superviseurs de sécurité et aux auditeurs de la TOE de consulter les journaux.

2.3.2.3 Définition des politiques de sécurité

Ce service permet à l'administrateur de sécurité de définir la politique de filtrage du pare-feu de la TOE, ainsi que la politique VPN du chiffreur IP. La définition des politiques de sécurité (pare-feu et chiffreur IP) n'est accessible qu'aux administrateurs de sécurité de la TOE.

2.3.2.4 Audit et journalisation des opérations d'administration

Ce service permet d'enregistrer dans des journaux d'audit toutes les opérations d'administrations effectuées par les administrateurs sur la TOE. Ce service permet également aux administrateurs de sécurité, aux superviseurs de sécurité et aux auditeurs de la TOE de consulter les journaux.

2.3.2.5 Supervision

Ce service permet à l'administrateur système et réseau et au superviseur système et réseau de contrôler l'état de disponibilité de la TOE. Il permet également à l'administrateur système et réseau de configurer les paramètres réseau de la TOE. Ce service est réalisé depuis un poste, également appelé station de supervision, sur lequel le logiciel Arkoon Monitoring permet la supervision de la TOE.

2.3.2.6 Gestion des clés cryptographiques

Ce service permet à l'administrateur de sécurité de la TOE de gérer les clés cryptographiques nécessaires à l'authentification des administrateurs et à la protection en confidentialité et en authenticité des flux VPN. Ce service permet de :

- Protéger l'accès aux clés cryptographiques : seul l'administrateur de sécurité peut accéder aux clés cryptographiques de la TOE.
- Gérer le cycle de vie des clés cryptographiques : les clés cryptographiques utilisées dans la TOE doivent être renouvelées régulièrement pour assurer un bon niveau de sécurité de la TOE.
- Injecter des clés cryptographiques : l'administrateur de sécurité injecte, de manière sécurisée, les clés cryptographiques nécessaires à la TOE.
- Supprimer, en toute sécurité, des clés cryptographiques : l'administrateur de sécurité peut supprimer de manière sécurisée les clés cryptographiques de la TOE.

Remarque : Arkoon FAST dispose d'un Centre d'Elaboration des Clés (CEC) permettant de générer les clés cryptographiques pouvant être utilisées par la TOE pour l'authentification des administrateurs et la protection (confidentialité et authenticité) des flux transitant par le chiffreur IP. Le CEC n'est pas inclus dans le périmètre de l'évaluation. La non inclusion du CEC dans le périmètre de l'évaluation est justifiée par le fait que le PP [PP_CIP] sur lequel le service VPN de la TOE s'inspire mentionne que le CEC est hors TOE.

2.3.2.7 Réinitialisation

Ce service permet à l'administrateur de sécurité, lors d'un changement de contexte de la TOE (nouvelle affectation, maintenance, …), d'effacer de manière sécurisé toutes les données sensibles de la TOE : politiques de sécurité (pare-feu et VPN), clés cryptographiques, données d'authentification des administrateurs, …

3 Environnement de sécurité de la TOE

Ce chapitre précise les aspects de sécurité de l'environnement dans lequel il est prévu d'utiliser la TOE.

3.1 Biens sensibles

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

Les biens du système d'information sont protégés par la TOE sous la condition que les politiques de sécurités Pare-feu et VPN demandent l'application d'un ou plusieurs types de protection. 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.

Les biens relatifs uniquement au service pare-feu de la TOE sont identifiés par la racine D.FW. Les biens relatifs uniquement au service VPN de la TOE sont identifiés par la racine D.VPN.

3.1.1 Biens protégés par la TOE

Pare-feu

D.FW.DONNEES_RESEAU_PRIVE

La TOE contribue à protéger des biens utilisateurs de type informations et services du réseau protégé, par le filtrage des flux susceptibles d'accéder ou de modifier ces biens. *Protection :* confidentialité (opt.), intégrité (opt.) ou disponibilité (opt.)

Chiffreur IP

D.VPN.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.).

3.1.2 Biens sensibles de la TOE

D.LOGICIELS

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

Protection : intégrité.

Pare-feu

D.FW.POLITIQUE_FILTRAGE

Les politiques de filtrage et les contextes de connexion définissent les traitements (filtrage implicite et services de sécurité) à effectuer sur les paquets IP traités par le firewall. Cela inclut la politique d'audit des flux utilisateurs.

Protection: authenticité lorsque les politiques (et leurs contextes) transitent de l'endroit où l'administrateur les définit à distance vers le firewall, intégrité des politiques (et des contextes) stockées sur le firewall, cohérence entre la politique définie (et son contexte) et celle appliquée, confidentialité.

D.FW.AUDIT_FLUX

Données générées par la politique d'audit pour permettre de retracer les flux traités par le pare-feu.

Protection : intégrité.

D.FW.PARAM_CONFIG

Les paramètres de configuration du pare-feu comprennent entre autres:

- les adresses IP internes aux réseaux protégés et les tables de routage (configuration réseau);
- les données d'authentification et d'intégrité;
- les droits d'accès ;
- la politique d'audit des opérations d'administration.

Protection : confidentialité et intégrité.

D.FW.AUDIT_ADMIN

Données générées par la politique d'audit pour permettre de retracer les opérations d'administration effectuées sur le pare-feu.

Protection : intégrité.

D.FW.ALARMES

Alarmes de sécurité générées par la TOE pour prévenir une possible violation de sécurité du pare-feu.

Protection : intégrité.

Chiffreur IP

D.VPN.POLITIQUE_VPN

Les politiques de sécurité VPN définissent les traitements (filtrage implicite et services de sécurité) à effectuer sur les données reçues et envoyées par le 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 : intégrité des politiques (et de leur contextes) stockées sur les chiffreurs IP, confidentialité.

D.VPN.PARAM_CONFIG

Les paramètres de configuration du chiffreur IP comprennent entre autres: les adresses IP internes aux réseaux privés et les tables de routage (configuration réseau), les données d'authentification et les droits d'accès.

Protection : confidentialité et intégrité.

D.VPN.CLES_CRYPTO

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

- les clés de session.
- les clés utilisées par les services de sécurité appliqués par les politiques de sécurité VPN.

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

D.VPN.AUDIT_FLUX

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

Protection : intégrité.

D.VPN.AUDIT_ADMIN

Données générées par la politique d'audit pour permettre de tracer les opérations d'administration effectuées sur le chiffreur IP.

Protection : intégrité.

Note d'application : le bien D.AUDIT identifié dans le profil de protection du chiffreur IP [PP_CIP] a été scindée en deux biens D.VPN.AUDIT_FLUX et D.VPN.AUDIT_ADMIN.

D.VPN.ALARMES

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

Protection : intégrité.

3.2 Acteurs

Le fonctionnement de la TOE dans son environnement opérationnel manipule directement ou indirectement les rôles décrits ci-dessous. Il s'agit de rôles « logiques » dont l'attribution à des personnes distinctes ou non relève de la politique de sécurité de l'organisation qui met en oeuvre la TOE.

Agent / Officier / Responsable de sécurité

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

Administrateur de sécurité

Administrateur (local ou distant) de la TOE. Il définit la politique de filtrage que va appliquer le pare-feu. Il définit la politique de sécurité VPN ainsi que les contextes de sécurité que va appliquer le chiffreur IP. Il génère et distribue les clés dans le chiffreur IP. 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.

Auditeur

Son rôle est d'analyser et de gérer les événements d'audit concernant les activités sur les flux IP transitant par le pare-feu et le chiffreur ainsi que les opérations d'administration.

Administrateur système et réseau

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

Il configure les paramètres réseaux de la TOE et les paramètres systèmes qui sont liés aux contextes réseaux opérationnels à prendre en compte : il définit la topologie réseau globale mais ne définit ni la politique de filtrage applicable par le pare-feu, ni les politiques de sécurité VPN. Son rôle est aussi de contrôler l'état de la TOE.

Superviseur système et réseau

Ce rôle est attribué à une personne qui vérifie l'état du système et les événements de réseau.

Superviseur sécurité

Ce rôle est attribué à la personne qui suit les événements de sécurité et vérifie/supprime les alertes de sécurité.

Rôle toutes autorisations

Ce rôle sera utilisé dans les organisations au sein desquelles une seule personne est responsable de l'appliance FAST360. Il bénéficie alors de l'ensemble des autorisations.

Utilisateur du réseau protégé

Utilisateur d'un réseau protégé connecté à un autre réseau à travers le pare-feu. Cet utilisateur peut, par l'intermédiaire d'applications, envoyer/recevoir des informations vers/d'un autre réseau via le firewall de son réseau.

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.

Un utilisateur de réseau privé est également un utilisateur de réseau protégé, mais la réciproque n'est pas forcément vraie. Ainsi un utilisateur du réseau protégé est un utilisateur du réseau protégé par le service pare-feu de la TOE, et un utilisateur du réseau privé est un utilisateur du réseau protégé (c'est-à-dire protégé par le service pare-feu de la TOE) et qui utilise le service VPN de la TOE.

Dans la suite du document, on parlera de Responsable de sécurité pour définir Agent / Officier / Responsable de sécurité.

Dans la suite du document, à moins de distinction spécifiquement exprimée, le rôle administrateur regroupe les rôles suivants : responsable de sécurité, administrateur de sécurité, superviseur de sécurité, auditeur et administrateur système et réseau, superviseur système et réseau.

3.3 Hypothèses

Les hypothèses relatives uniquement au service Pare-feu de la TOE sont identifiées par la racine A.FW. Les hypothèses relatives uniquement au service VPN de la TOE sont identifiées par la racine A.VPN.

A.ADMIN

Les administrateurs sont des personnes non hostiles. Elles disposent des moyens nécessaires à la réalisation de leurs tâches, sont formées 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 (pare-feu, VPN et équipements d'administration), ainsi que tous supports contenant les biens sensibles de la TOE (papier, disquettes, sauvegardes,...) se trouvent dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

Cependant, les équipements 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 du pare-feu ou du chiffreur IP.

A.INITIALISATION_LOCAL

Les équipements contenant les services de la TOE (pare-feu, VPN et équipements d'administration) sont initialisés dans le local protégé de l'appliance dont l'accès est contrôlé

et restreint aux administrateurs. Cette initialisation est effectuée depuis une station d'administration directement connectée sur les équipements.

A.AUTHENTIFICATION_ADMIN_DISTANT

L'environnement de la TOE permet d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants.

Pare-feu

A.FW.AUDIT

Il est supposé que l'auditeur consulte régulièrement les événements d'audit générés par le pare-feu. La mémoire stockant les événements d'audit est gérée de telle sorte que les administrateurs ne perdent pas d'événements.

A.FW.ALARMES

Il est supposé que l'administrateur de sécurité analyse et traite les alarmes de sécurité générées et remontées par le pare-feu.

A.FW.MAITRISE_CONFIGURATION

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

Chiffreur IP

A.VPN.AUDIT

Il est supposé que l'auditeur consulte régulièrement les événements d'audit générés par le chiffreur IP. 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.VPN.ALARMES

Il est supposé que l'administrateur de sécurité analyse et traite les alarmes de sécurité générées et remontées par le chiffreur IP.

A.VPN.MAITRISE_CONFIGURATION

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

A.VPN.CRYPTO_EXT

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 de cryptographie de la DCSSI [CRYPTO] et [GC] pour le niveau de résistance standard.

3.4 Menaces

3.4.1 Profil des attaquants

Les menaces peuvent avoir pour origine :
- Un dysfonctionnement de la TOE ou de l'environnement de la TOE (poste, réseau…)
- Des personnes disposant d'un accès au réseau sur lequel est connecté la TOE, qui peuvent agir de manière malveillante, usurper des droits d'administration.

Les différents agents menaçant sont :
- les attaquants internes : tout utilisateur autorisé du réseau protégé
- les attaquant externes : tout personne extérieur au réseau protégé

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

3.4.2 Niveau des attaquants

On considère que les attaquants sont des personnes physiques disposant d'un potentiel d'attaque de niveau élémentaire ce qui correspond à des personnes malintentionnées disposant des compétences informatiques d'un utilisateur averti.

3.4.3 Menaces non retenues

Les menaces retenues 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 de l'organisation. A ce titre, les sinistres physiques, les événements naturels, les pertes de services essentiels, les perturbations dues au rayonnement, le de vol de matériel, le déni de service ne sont pas des menaces retenues.

Les menaces relatives uniquement au service Pare-feu de la TOE sont identifiées par la racine T.FW. Les menaces relatives uniquement au service VPN de la TOE sont identifiées par la racine T.VPN.

3.4.4 Menace retenues

3.4.4.1 Menaces portant sur les politiques de sécurité de la TOE (TSP)

Pare-feu

T.FW.MODIFICATION_POL_FILTRAGE

Un attaquant modifie illégalement la politique de filtrage et/ou les contextes de connexion du pare-feu.

Bien menacé : D.FW.POLITIQUE_FILTRAGE

T.FW.DIVULGATION_POL_FILTRAGE

Un attaquant récupère illégalement la politique de filtrage et/ou les contextes de connexion du pare-feu.

Bien menacé : D.FW.POLITIQUE_FILTRAGE

Chiffreur IP

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

Bien menacé : D.VPN.POLITIQUES_VPN.

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

Bien menacé : D.VPN.POLITIQUES_VPN.

T.VPN.USURPATION_ID
Un attaquant externe usurpe l'identité d'un chiffreur IP existant sur un réseau privé pour récupérer des données applicatives ou topologiques ou envoyer des données falsifiées.

Biens menacés : D.VPN.DONNEES_APPLICATIVES, D.VPN.INFO_TOPOLOGIE.

3.4.4.2 Menaces portant sur la configuration de la TOE

Pare-feu

T.FW.MODIFICATION_PARAM
Un attaquant modifie illégalement les paramètres de configuration du pare-feu.

Bien menacé : D.FW.PARAM_CONFIG

T.FW.DIVULGATION_PARAM
Un attaquant accède illégalement aux paramètres de configuration du pare-feu.

Bien menacé : D.FW.PARAM_CONFIG

Chiffreur IP

T.VPN.MODIFICATION_PARAM
Un attaquant modifie illégalement des paramètres de configuration du chiffreur IP.

Bien menacé : D.VPN.PARAM_CONFIG.

T.VPN.DIVULGATION_PARAM

Un attaquant récupère de manière non autorisée des paramètres de configuration du chiffreur IP.

Bien menacé : D.VPN.PARAM_CONFIG

3.4.4.3 Menaces portant sur les clés cryptographiques

Chiffreur IP

T.VPN.MODIFICATION_CLES

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

Bien menacé : D.VPN.CLES_CRYPTO.

T.VPN.DIVULGATION_CLES

Un attaquant récupère illégalement des clés cryptographiques.

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

3.4.4.4 Menaces portant sur les traces d'audit des flux

Pare-feu

T.FW.MODIFICATION_AUDIT_FLUX

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

Bien menacé : D.FW.AUDIT_FLUX

Chiffreur IP

T.VPN.MODIFICATION_AUDIT_FLUX

Un attaquant modifie ou supprime illégalement des enregistrements d'événements d'audit des activités sur les liens VPN.

Bien menacé : D.VPN.AUDIT_FLUX

3.4.4.5 Menaces portant sur les traces d'audit d'administration

Pare-feu

T.FW.MODIFICATION_AUDIT_ADMIN

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

Bien menacé : D.FW.AUDIT_ADMIN

Chiffreur IP

T.VPN.MODIFICATION_AUDIT_ADMIN
Un attaquant modifie ou supprime illégalement des enregistrements d'événements d'audit d'administration du chiffreur IP.

Bien menacé : D.VPN.AUDIT_ADMIN

Note d'application : La menace T.MODIFICATION_AUDIT identifiée dans le profil de protection du chiffreur IP [PP_CIP] a été scindée en deux menaces T.VPN.MODIFICATION_AUDIT_FLUX et T.VPN.MODIFICATION_AUDIT_ADMINISTRATION.

3.4.4.6 Menaces portant sur les alarmes

Pare-feu

T.FW.MODIFICATION_ALARMES
Un attaquant modifie ou supprime illégalement des alarmes lorsqu'elles sont remontées par la TOE à l'administrateur de sécurité.

Bien menacé : D.FW.ALARMES

Chiffreur IP

T.VPN.MODIFICATION_ALARMES
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.VPN.ALARMES.

3.4.4.7 Menaces portant sur l'administration

T.USURPATION_ADMIN
Un attaquant usurpe l'identité d'un administrateur et effectue des opérations d'administration sur la TOE.

Biens menacés : tous les biens.

3.4.4.8 Menaces portant sur le changement de contexte d'utilisation de la TOE

Pare-feu

T.FW.CHANGEMENT_CONTEXTE

Un attaquant ou un administrateur d'un nouveau réseau protégé, prend connaissance, par accès direct à la TOE, des biens sensibles du pare-feu lors d'un changement de contexte d'utilisation du pare-feu (affectation du pare-feu à un nouveau réseau, maintenance,...).

Biens menacés : D.FW.DONNEES_RESEAU_PRIVE, D.FW.POLITIQUE_FILTRAGE, D.FW.AUDIT_FLUX, D.FW.PARAM_CONFIG, D.FW.AUDIT_ADMIN, D.FW.ALARMES.

Chiffreur IP

T.VPN.CHANGEMENT_CONTEXTE

Un attaquant ou un administrateur d'un nouveau réseau de chiffrement 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.VPN.POLITIQUES_VPN, D.VPN.PARAM_CONFIG, D.VPN.CLES_CRYPTO, D.VPN.AUDIT et D.VPN.ALARMES.

3.4.4.9 Menace sur le fonctionnel des services de la TOE

T. DYSFONCTIONNEMENT

Un attaquant met la TOE dans un état de dysfonctionnement qui contribue à rendre les services offerts par la TOE indisponibles ou la met dans un état non sûr.

Biens menacés : tous les biens.

3.5 Politiques de sécurité de l'organisation

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

OSP.QUALIF

La TOE est évaluée selon les Critères Communs [CC] selon le paquet d'assurance EAL3 augmenté des composants ALC_FLR.3, AVA_VLA.2 pour obtenir une qualification standard [QS].

OSP.CRYPTO

Les référentiels de cryptographie de la DCSSI [CRYPTO], [GC] et [AUTH] doivent être suivis pour la gestion des clés (génération, destruction, consommation et distribution), des fonctions de cryptographie utilisées dans la TOE et des mécanismes d'authentification pour le niveau de résistance standard.

Note d'application : Cette politique de sécurité de l'organisation, issue des profils de protection [PP_FWIP] et [PP_CIP] a été enrichie pour prendre en compte les deux nouveaux référentiels émis par la DCSSI concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau standard [GC], et la gestion des mécanismes d'authentification [AUTH].

OSP.GESTION_ROLES

La TOE doit permettre de définir différents rôles de responsable de sécurité, administrateur de sécurité, superviseur de sécurité, auditeur et administrateur système et réseau, superviseur système et réseau. Elle permet également de fournir les traces d'audits des actions réalisées par ces rôles.

Pare-feu

OSP.FW.SERVICE

La TOE doit appliquer la politique de filtrage définie par l'administrateur de sécurité, sur la base de la politique de sécurité du système d'information.

Dans le mode contextuel, la TOE doit pouvoir établir et appliquer à son niveau des règles de filtrage basées sur les caractéristiques des flux traités (par exemple: origine, destinataire, protocole applicatif).

OSP.FW.VISUALISATION_POL

La TOE doit permettre de visualiser les règles de filtrage courantes.

Note d'application : la politique de sécurité de l'organisation OSP.FILTRAGE identifiée dans le profil de protection [PP_FWIP] a été scindée en deux politiques de sécurité de l'organisation : OSP.FW.SERVICE et OSP.FW.VISUALISATION_POL.

OSP.FW.AUDIT_FLUX

La TOE doit tracer les flux qu'elle traite de manière :

- à enregistrer au minimum les événements générés lors du rejet d'un flux;
- à permettre à l'administrateur d'ordonner chronologiquement les événements enregistrés;
- à permettre à l'administrateur d'attribuer un événement à un acteur;
- à permettre la visualisation des journaux d'audit et la sélection des événements enregistrés afin de s'assurer de la pertinence de la politique de filtrage et de sa bonne instanciation au niveau du firewall.

Chiffreur IP

OSP.VPN.SERVICE

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
- 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.VPN.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 le chiffreur IP.

OSP.VPN.SUPERVISION

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

4 Objectifs de sécurité

4.1 Objectifs de sécurité pour la TOE

4.1.1 Objectifs sur les services de sécurité rendus par la TOE

OT.QUALIF
Le niveau d'évaluation de la TOE doit être EAL3 augmenté des composants ALC_FLR.3, AVA_VLA.2 tel que décrit dans le processus de qualification « standard ». [QS]

OT.GESTION_ROLES
La TOE doit permettre de définir les différents rôles définis au §3.2 et associer de manière sûre les rôles aux utilisateurs.

Pare-feu

OT.FW.APPLICATION_POL_FILTRAGE
La TOE doit appliquer la politique de filtrage spécifiée par l'administrateur et les règles de filtrage établies par la TOE (mode contextuel). Cette politique peut concerner à la fois les flux utilisateurs et les flux d'administration.

OT.FW.COHERENCE_POL
Dans le cas d'une administration à distance, la TOE doit garantir la cohérence entre la définition des politiques de filtrage et les politiques appliquées sur le firewall.

4.1.1.1 Chiffreur IP

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

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

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

OT.VPN.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.

OT.VPN.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.

OT.VPN. 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.

4.1.2 Objectifs pour protéger les biens sensibles de la TOE

4.1.2.1 Politiques de sécurité de la TOE (TSP)

Pare-feu

OT_FW.PROTECTION_POL_FILTRAGE

La TOE doit contrôler l'accès local (consultation, modification) aux règles de filtrage et aux contextes de connexion sur le firewall.

OT.FW .VISUALISATION_POL

La TOE doit permettre aux administrateurs de sécurité de visualiser unitairement la politique de filtrage et les contextes de connexion présents sur le firewall.

Chiffreur IP

OT.VPN.DEFINITION_POL

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

OT.VPN.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.

OT.VPN.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 le chiffreur IP.

4.1.2.2 Cryptographie et gestion des clés cryptographiques

OT.CRYPTO

La TOE doit implémenter les fonctions de cryptographie et gérer (générer, détruire, renouveler) les clés cryptographiques en accord avec le référentiel de cryptographie défini par la DCSSI dans les documents [CRYPTO], [GC] et [AUTH] pour le niveau de résistance standard.

Raffinement : Les clés cryptographiques au sein de la TOE sont de deux types comme l'indique la description du bien sensible de la TOE D.VPN.CRYPTO (les clés cryptographiques de sessions, et les clés cryptographiques statiques définies au sein des politiques de sécurité pour les liens VPN). Les clés cryptographiques statiques sont soit générées par le CEC (hors du périmètre de la TOE), soit générées par l'environnement et injectées dans la TOE. La génération/renouvellement des clés cryptographiques statiques est donc hors du périmètre de la TOE.

Chiffreur IP

OT.VPN.ACCES_CLES

La TOE doit protéger l'accès aux clés cryptographiques.

OT.VPN.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.

4.1.2.3 Configuration

Pare-feu

OT.FW.PROTECTION_PARAM

La TOE doit contrôler l'accès local sur le firewall (consultation, modification) aux paramètres de configuration, aux droits d'accès, aux données d'authentification et aux éléments permettant de gérer l'intégrité des flux d'administration.

Chiffreur IP

OT.VPN.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.

4.1.2.4 Administration

OT.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. La TOE doit également protéger les flux contre le rejeu.

OT.AUTHENTIFICATION_ADMIN
La TOE doit fournir des mécanismes d'identification et d'authentification locale des différents administrateurs.

4.1.2.5 Recyclage

Pare-feu

OT.FW.CHANGEMENT_CONTEXTE
La TOE doit fournir une fonctionnalité qui permet de rendre indisponibles les biens sensibles du pare-feu préalablement à un changement de contexte d'utilisation: nouvelle affectation, maintenance,...

Chiffreur IP

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

4.1.2.6 Supervision

Pare-feu

OT.FW.SUPERVISION
La TOE doit permettre à l'administrateur système et réseau et au superviseur système et réseau de consulter l'état opérationnel du pare-feu.

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

Chiffreur IP

OT.VPN.SUPERVISION
La TOE doit permettre à l'administrateur système et réseau et au superviseur système et réseau de consulter l'état opérationnel du chiffreur IP.

OT.VPN.IMPACT_SUPERVISION
La TOE doit garantir que le service de supervision du chiffreur IP ne met pas en péril ses biens sensibles.

4.1.2.7 Audit des flux

Pare-feu

OT.FW .AUDIT_FLUX

La TOE doit tracer les flux qu'elle traite de manière :

- à enregistrer au minimum les événements générés lors du rejet d'un flux;
- à permettre à l'administrateur d'ordonner chronologiquement les événements enregistrés;
- à permettre à l'administrateur d'attribuer un événement à un acteur;
- à permettre la visualisation des journaux d'audit et la sélection des événements enregistrés afin de s'assurer de la pertinence de la politique de filtrage et de sa bonne instanciation au niveau du firewall.

OT.FW.PROTECTION_AUDIT_FLUX

La TOE doit contrôler l'accès local sur le firewall (consultation, modification) aux traces d'audit des flux qu'elle enregistre et doit permettre à un auditeur de détecter la perte d'événements d'audit des flux (en utilisant un compteur par exemple).

Chiffreur IP

OT.VPN.AUDIT_FLUX

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.

OT.VPN.PROTECTION_AUDIT_FLUX

La TOE doit garantir l'intégrité des événements d'audit (opérations effectuées par le chiffreur, opérations concernant les liens VPN) qu'elle enregistre et doit permettre à un auditeur de détecter la perte d'événements d'audit (en utilisant un compteur par exemple).

4.1.2.8 Audit des opérations d'administration

Pare-feu

OT.FW.AUDIT_ADMIN

La TOE doit générer des traces d'audit des opérations effectuées par les administrateurs du firewall. La TOE doit permettre la visualisation de ces traces d'audit. La génération des traces doit permettre l'imputabilité des événements d'administration enregistrés.

OT.FW.PROTECTION_AUDIT_ADMIN

La TOE doit contrôler l'accès local sur le firewall (consultation, modification) aux traces d'audit d'administration qu'elle enregistre et doit permettre à un auditeur de détecter la perte d'événements d'audit d'administration (en utilisant un compteur par exemple).

Chiffreur IP

OT.VPN.AUDIT_ADMIN

La TOE doit aussi 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.

OT.VPN.PROTECTION_AUDIT_ADMIN
La TOE doit garantir l'intégrité des événements d'audit (opérations effectuées par un administrateur sur le chiffreur IP) qu'elle enregistre et doit permettre à un auditeur de détecter la perte d'événements d'audit (en utilisant un compteur par exemple).

4.1.2.9 Alarmes

Pare-feu

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

OT.FW.PROTECTION_ALARMES
La TOE doit contrôler l'accès local sur le firewall (consultation, modification) aux alarmes de sécurité (à destination des administrateurs de sécurité locaux ou à distance) qu'elle génère et doit permettre à un administrateur de sécurité ou un superviseur de sécurité de détecter la perte d'alarmes de sécurité (en utilisant un compteur par exemple).

Chiffreur IP

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

OT.VPN.PROTECTION_ALARMES
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 ou superviseur de sécurité de détecter la perte d'alarmes de sécurité (en utilisant un compteur par exemple).

4.2 Objectifs de sécurité pour l'environnement de la TOE

4.2.1 Conception de la TOE

OE.CRYPTO
Les référentiels de cryptographie de la DCSSI [CRYPTO], [GC] et [AUTH] doivent être suivis lors de la conception et l'exploitation de la TOE 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.

4.2.2 Objectifs de sécurité sur l'exploitation de la TOE

4.2.2.1 Environnement physique

OE.PROTECTION_LOCAL

Les équipements contenant les services de la TOE (pare-feu, VPN et équipements d'administration), ainsi que tous supports contenant les biens sensibles de la TOE (papier, disquettes, sauvegardes,...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

Cependant, les équipements 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 firewall ou du chiffreur IP.

OE.INITIALISATION_LOCAL

Les équipements contenant les services de la TOE (pare-feu, VPN et équipements d'administration) doivent être initalisés dans le local protégé de l'appliance dont l'accès est contrôlé et restreint aux administrateurs. Cette initialisation doit être effectuée depuis une station d'administration directement connectée sur les équipements.

4.2.2.2 Gestion des clés cryptographiques

Chiffreur IP

OE.VPN.CRYPTO_EXT

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

De plus, ces clés doivent être gérées conformément aux recommandations de la DCSSI [GC] pour le niveau de résistance standard.

4.2.2.3 Administration de la TOE

OE.ADMIN

Les administrateurs disposent des moyens nécessaires à la réalisation de leurs tâches, sont formées pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.

Les administrateurs doivent être de confiance.

OE.AUTHENTIFICATION_ADMIN_DISTANT

L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants.

4.2.2.4 Gestion des traces d'audit et des alarmes

Pare-feu

OE.FW.ANALYSE_AUDIT

L'auditeur doit régulièrement analyser les événements d'audit enregistrés par la TOE et agir en conséquence. La mémoire stockant les événements d'audit est gérée de telle sorte que les administrateurs ne perdent pas d'événements.

En outre, les audits doivent faire l'objet de sauvegarde et d'archivage afin que l'impact de leur suppression accidentelle ou volontaire soit limité.

OE.FW.TRAITE_ALARMES

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

Chiffreur IP

OE.VPN.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.VPN.TRAITE_ALARMES

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

4.2.2.5 Contrôle de la TOE

Pare-feu

OE.FW.INTEGRITE

L'administrateur dispose des moyens de contrôler la configuration matérielle et logicielle du pare-feu par rapport à un état de référence, ou de la régénérer dans un état sûr.

Chiffreur IP

OE.VPN.INTEGRITE

L'administrateur dispose des moyens de contrôler la configuration matérielle et logicielle du chiffreur IP par rapport à un état de référence, ou de la régénérer dans un état sûr.

Note d'application : Cet objectif de sécurité sur l'environnement de la TOE issu du Profil de Protection [PP_CIP] a été enrichi : il impose désormais la capacité de régénération de la TOE dans un état sûr.

5 Exigences de sécurité

5.1 Exigences fonctionnelles pour la TOE

5.1.1 Résumé

Exigences		Intitulés
Classe FAU : Security Audit		
	FAU_ARP.1	**Security alarms**
	FAU_GEN.1	**Audit data generation**
	FAU_GEN.2	**User identity association**
	FAU_SAA.1	**Potential violation analysis**
	FAU_SAR.1	**Audit review**
	FAU_SAR.3	**Selectable audit review**
	FAU_STG.1	**Protected audit trail storage**
Classe FCS : Cryptographic support		
	FCS_COP.1	**Cryptographic operation**
	FCS_CKM.1	**Cryptographic key generation**
	FCS_CKM.4	**Cryptographic key destruction**
Classe FDP : User data protection		
	FDP_ACC.1	**Subset access control**
	FDP_ACF.1	**Security attribute based access control**
	FDP_IFC.1	**Subset information flow control**
	FDP_IFC.2	**Complete information flow control**
	FDP_IFF.1	**Simple secure attributes**
	FDP_ITC.1	**Import of user data without security attributes**
	FDP_RIP.1	**Subset residual information protection**
Classe FIA : Identification and authentication		
	FIA_UAU.2	**User authentication before any action**
	FIA_UID.2	**User identification before any action**
Classe FPT : Protection of the TSF		
	FPT_ITC.1	**Inter-TSF confidentiality during transmission**
	FPT_ITT.1	**Basic internal TSF data transfer protection**
	FPT_STM.1	**Reliable time stamps**
	FPT_TDC.1	**Inter-TSF basic TSF data consistency**
Classe FMT : Security management		
	FMT_MSA.1	**Management of security attributes**
	FMT_MSA.3	**Static attribute initialisation**
	FMT_SMF.1	**Specification of Management Functions**
	FMT_SMR.1	**Security roles**
	FMT_MTD.1	**Management of TSF data**
Classe FTA : TOE access		
	FTA_TSE.1	**TOE session establishment**

Toutes les exigences de sécurité fonctionnelles pour la TOE sont extraites de la partie 2 des Critères Communs [CC].

5.1.2 Détail des exigences fonctionnelles pour la TOE

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Raffinement global:

La fiabilité attendue de la base de temps est que seul l'administrateur de la TOE a le droit de la modifier ; la base de temps devant être fiable entre deux mises à jour par l'administrateur.

Protection de l'administration distante

FPT_ITT.1-Administration_distante Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_ITT.3-Administration_distante TSF data integrity monitoring

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

FPT_ITT.3.2-Administration_distante Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: stopper la connexion en cours].

FIA_UAU.2-Station_administration_distante User authentication before any action

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1

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

Raffinement global:

Cette exigence est relative à l'authentification pour l'administration distante de la TOE. Cette exigence concerne l'authentification de la station d'administration vis-à-vis de la TOE. Cette authentification peut être renforcée au niveau de la TOE par une authentification de l'administrateur directement auprès de la TOE. Pour mémoire, l'authentification de l'administrateur distant vis-à-vis de la station d'administration distante relève de l'environnement de la TOE.

Gestion des rôles

FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1

FMT_SMR.1.1 The TSF shall maintain the roles [assignment : responsable de sécurité, administrateur de sécurité, administrateur système et réseaux, auditeur, superviseur système et réseau, superviseur sécurité].

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

FIA_UID.2-Administrateurs User identification before any action

Hierarchical to: FIA_UID.1
Dependencies: No dependencies.

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

Raffinement global:

Les « user » correspondent ici aux administrateurs; à ne pas confondre avec la possibilité de certains firewall de coupler le filtrage avec une identification/authentification des utilisateurs des réseaux.
L'identification des administrateurs peut être locale ou issue du flux d'administration distante.

FIA_UAU.2-Administrateurs_local User authentication before any action

Hierarchical to: FIA_UAU.1
Dependencies: FIA_UID.1

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

Raffinement global:

Cette exigence est relative à l'authentification des administrateurs pour l'administration locale de la TOE. Pour l'administration distante, l'authentification de l'administrateur sur la station d'administration n'est pas incluse dans le périmètre de la TOE et est donc couverte par un

objectif sur l'environnement. Concernant les exigences sur l'administration distante, se référer aux exigences de sécurité fonctionnelles pour l'environnement technique de la TOE.

FMT_MTD.1-Param_security_administrator Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1, FMT_SMF.1

FMT_MTD.1.1-Param_security_administrator The TSF shall restrict the ability to [selection: modify] the [assignment: données d'identification et d'authentification et droits d'accès] to [assignment: responsable de sécurité].

FMT_MTD.1-Param_auditor Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1, FMT_SMF.1

FMT_MTD.1.1-Param_auditor The TSF shall restrict the ability to [selection: query] the [assignment: données d'identification et d'authentification et droits d'accès] to [auditeur].

5.1.2.1 Exigences de sécurité fonctionnelles pour le pare-feu

Application de la politique de filtrage

FDP_IFC.2/FW-Enforcement_policy Complete information flow control

Hierarchical to: FDP_IFC.1
Dependencies: FDP_IFF.1

FDP_IFC.2.1/FW-Enforcement_policy The TSF shall enforce the [assignment: politique de filtrage (et les règles liées aux contextes de connexion en mode contextuel)] on [assignment:

- les flux IP utilisateurs utilisant les protocols réseaux TCP, UDP, ICMP,
- les flux IP utilisateurs utilisant les protocoles applicatifs sur HTTP, FTP, DNS et SMTP,
- les flux d'administration]

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

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

FDP_IFF.1/FW**-Enforcement_policy Simple security attributes**

Hierarchical to: No other components.
Dependencies: FDP_IFC.1, FMT_MSA.3

FDP_IFF.1.1/FW-Enforcement_policy The TSF shall enforce the [assignment: politique de filtrage (et les règles liées aux contextes de connexion en mode contextuel)] based on the following types of subject and information security attributes: [assignment:

- les adresses IP source et destination des paquets IP,
- les protocoles réseau TCP, ICMP, et UDP des paquets IP,
- les services sources et destination des paquets IP,
- les commandes applicatives des protocoles applicatifs HTTP, FTP, DNS et SMTP des paquets IP
- les ports de communication source et destination des paquets IP].

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

a. Les utilisateurs du réseau protégé peuvent transmettre des flux IP du réseau protégé vers le réseau externe, à travers la TOE si :
   - les attributs du paquet IP traité respectent les critères définis dans la politique de filtrage et/ou les règles de filtrage liées au contexte de connexion en mode contextuel
   - l'adresse source du paquet IP translate vers une adresse interne,
   - l'adresse destination du paquet IP translatée vers une adresse externe.
b. Les utilisateurs du réseau externe peuvent transmettre des flux IP du réseau externe vers le réseau protégé, à travers la TOE si :
   - les attributs du paquet IP traité respectent les critères définis dans la politique de filtrage et/ou les règles de filtrage liées au contexte de connexion en mode contextuel
   - l'adresse source du paquet IP translate vers une adresse externe,
   - l'adresse destination du paquet IP translatée vers une adresse interne].

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

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

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

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

a. Rejeter les paquets arrivant sur l'interface externe de la TOE et dont l'adresse source correspond à une adresse du réseau protégé.
b. Rejeter les paquets arrivants sur l'interface interne de la TOE et dont l'adresse source correspond à une adresse du réseau externe
c. Rejeter les paquets arrivants sur l'adresse interne ou externe de la TOE et dont l'adresse source correspond à une adresse externe sur un réseau broadcast.
d. Rejeter les paquets dans lesquels les utilisateurs (utilisateurs du réseau protégés ou utilisateurs du réseau externe) spécifient la route des paquets pour atteindre l'adresse destination.
e. Rejeter les paquets arrivant sur l'interface interne ou externe de la TOE et dont les adresses source et destination sont identiques.
f. Pour les protocoles réseau supporés par la TOE (IP, TCP, UDP and ICMP), la TOE doit rejeter les paquets malformés.
g. Rejeter les paquets TCP qui ne contiennent pas un numéro séquence de connexion non attendu par la TOE.
h. La TOE doit rejeter les paquets lorsque le nombre de connexions actives concurrentes atteint ou dépasse le nombre de connexions actives concurrentes défini par l'administrateur de sécurité.

i. Pour les protocoles d'application supportés par la TOE (DNS, HTTP, SMTP and FTP), la TOE doit rejeter toutes les commandes applicatives non identifiées dans le tableau ci-dessous :

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

j. Pour les protocoles HTTP, FTP, SMTP et DNS la TOE doit rejecter tous flux applicatifs qui ne respectent pas les specifications de ces protocoles (RFC par exemple).
k. Pour les protocoles HTTP, FTP, SMTP et DNS, la TOE doit rejeter les flux contenant des commandes applicatives issues du tableau ci-dessus, et qui ne sont pas autorisées par l'administrateur de sécurité.
l. Pour le protocole applicatif HTTP, la TOE doit rejeter les flux qui violent les options applicatives HTTP configurées par l'administrateur de sécurité :
   - Taille maximale d'une URL
   - Mots clés interdits dans une URL
   - Entête HTTP cliente interdite
   - Taille maximale de l'entête client http
   - Entête HTTP serveur interdite
   - Taille maximale de l'entête serveur HTTP
m. Pour le protocole FTP, la TOE doit rejeter les flux qui violent les options applicatives FTP configurées par l'administrateur de sécurité :
   - Les utilisateurs autorisés
   - La taille maximale des lignes de commande
n. Pour le protocole SMTP, la TOE doit rejeter les flux qui violent les options applicatives SMTP configurées par l'administrateur de sécurité :
   - La taille maximale des lignes de commande
o. Pour le protocole DNS, la TOE doit rejeter les flux applicatifs qui violent les options applicatives DNS configurées par l'administrateur de sécurité :
   - Les types DNS autorisés
   - Les classes DNS autorisées
   -

FMT_SMF.1/FW**-Visualisation_politique_filtrage Specification of management functions**

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1/FW-Visualisation_politique_filtrage The TSF shall be capable of performing the following security management functions: [assignment: visualisation de la politique de filtrage et des contextes de connexion présents sur le firewall].

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

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TDC.1.1/FW-Administration_distante The TSF shall provide the capability to consistently interpret [assignment: la politique de filtrage du pare-feu de la TOE] when shared between the TSF and another trusted IT product.

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

Protection de la politique de filtrage

FDP_ACC.1/FW**-Filtering_policy Subset access control**

Hierarchical to: No other components.
Dependencies: FDP_ACF.1

FDP_ACC.1.1/FW-Filtering_policy The TSF shall enforce the [assignment: d'accès aux règles de filtrage] on [assignment:

- sujets: les administrateurs;
- objets: les règles de la politique de filtrage;
- opérations: lire, insérer, modifier, supprimer].

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

Hierarchical to: No other components.
Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1/FW-Filtering_policy The TSF shall enforce the [assignment: politique d'accès aux règles de filtrage] to objects based on the following: [assignment:

- sujets: les administrateurs sur la base de leur rôle;
- objets: les règles de la politique de filtrage].

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

- l'insertion, la modification et la suppression (complète ou partielle) des règles de filtrage n'est autorisée qu'au rôle administrateur de sécurité;
- la lecture des règles de filtrage et des contextes de connexion n'est autorisée qu'aux rôles administrateur de sécurité et auditeur].

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

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

Génération des traces d'audit des flux

FAU_GEN.1/FW**-Audit_flux Audit data generation**

Hierarchical to: No other components.
Dependencies: FPT_STM.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the minimal or basic level of audit définis dans l'annexe 1 avec le niveau d'audit associé ; and
c) au minimum les événements générés lors du rejet d'un flux

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment:
- un indentifiant numérique unique pour chaque évènement d'audit de flux du pare-feu, incrémenté d'une unité à chaque enregistrement d'un nouvel évènement d'audit de flux du pare-feu].

Raffinement global:

Les traces enregistrées doivent permettre notamment aux administrateurs de s'assurer de la pertinence de la politique de filtrage et de sa bonne instanciation au niveau du pare-feu.

FAU_GEN.2/FW**-Audit_flux User identity association**

Hierarchical to: No other components.
Dependencies: FAU_GEN.1, FIA_UID.1

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

Raffinement non éditorial:

On entend par 'identité des utilisateurs' l'adresse IP des émetteurs des flux.

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

Hierarchical to: FIA_UID.1
Dependencies: No dependencies.

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

Raffinement global:

On entend ici 'utilisateur' par les émétteurs et les destinataires des flux traités par le pare-feu identifiés par leurs adresses IP.

FAU_SAR.1/FW**-Audit_flux Audit review**

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit

FAU_SAR.1.1/FW-Audit_flux The TSF shall provide [assignment: les administrateurs de sécurité, les auditeurs] with the capability to read [assignment: les traces d'audit des flux traités par le firewall] from the audit records.

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

FAU_SAR.3/FW**-Audit_flux Selectable audit review**

Hierarchical to: No other components.
Dependencies: FAU_SAR.1

FAU_SAR.3.1/FW-Audit_flux The TSF shall provide the ability to perform [selection: sorting, searches] of audit data based on [assignment:
- les adresses IP source des paquets,
- les adresses IP destination des paquets,
- une plage d'adresses IP source,
- une plage d'adresses IP destination,
- les applications des paquets (HTTP, FTP, DNS et SMTP)
- la date et l'heure du traitrement des paquets].

Protection des traces d'audit des flux

FAU_STG.1/FW**-Traces_audit_flux Protected audit trail storage**

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

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

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

Génération des traces d'audit des opérations d'administration

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

Hierarchical to: No other components.
Dependencies: FPT_STM.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the minimal or basic level of audit définis dans l'annexe 1 avec le niveau d'audit associé; and
c) [assignment: none]

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment:

- un indentifiant numérique unique pour chaque évènement d'audit d'administration du pare-feu, incrémenté d'une unité à chaque enregistrement d'un nouvel évènement d'audit d'administration du pare-feu.]

FAU_GEN.2/FW**-Audit_admin User identity association**

Hierarchical to: No other components.
Dependencies: FAU_GEN.1, FIA_UID.1

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

FAU_SAR.1/FW**-Audit_admin Audit review**

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

FAU_SAR.1.1/FW-Audit_admin The TSF shall provide [assignment: les administrateurs de sécurité, les auditeurs] with the capability to read [assignment: les traces d'audit des évènements d'administration du firewall] from the audit records.

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

FAU_SAR.3/FW**-Audit_admin Selectable audit review**

Hierarchical to: No other components.
Dependencies: FAU_SAR.1

FAU_SAR.3.1/FW-Audit_admin The TSF shall provide the ability to perform [selection: sorting, searches] of audit data based on [assignment:
- Le type d'opération d'administration,
- L'identité de l'administrateur,
- La date et l'heure à laquelle l'opération d'administration a été effectuée.]

Protection des traces d'audit des opérations d'administration

FAU_STG.1/FW**-Traces_audit_admin Protected audit trail storage**

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

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

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

Alarmes

FAU_SAA.1/FW**-Alarmes Potential violation analysis**

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

FAU_SAA.1.1/FW-Alarmes The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

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

a) Accumulation or combination of [assignment:
- Violation de la politique de sécurité du pare-feu de la TOE,
- Saturation des journaux du pare-feu de la TOE,
- Perte d'intégrité du pare-feu de la TOE,
- Saturation système (disque dur, quarantaine, …)
- Déni de service du pare-feu de la TOE,
- Réception de paquets erronés par le pare-feu de la TOE]

known to indicate a potential security violation;

b) [assignment: aucun].

FAU_ARP.1/FW**-Alarmes Security alarms**

Hierarchical to: No other components.
Dependencies: FAU_SAA.1

FAU_ARP.1.1-Alarmes The TSF shall take [assignment:
- déclencher la remontée d'une alarme à l'administrateur de sécurité

- bloquer tous les flux transitant par le pare-feu de la TOE, sauf les flux d'administration du pare-feu de la TOE, lorsque les journaux du pare-feu sont saturés] upon detection of a potential security violation.

Configuration

FMT_SMF.1/FW**-Configuration Specification of management functions**

Hierarchical to: No other components.
Dependencies: No dependencies.

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

- configuration des paramètres de la TOE :
  - des rôles des administrateurs,
  - données d'identification et d'authentification des administrateurs,
  - droits d'accès
  - date et heure du système
- configuration des paramètres système et réseau de la TOE ;
- configuration de la politique de filtrage].

FMT_MTD.1/FW**-Network_param Management of TSF data**

Hierarchical to: No other components.
Dependencies: FMT_SMR.1, FMT_SMF.1

FMT_MTD.1.1/FW-Network_param The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear] the [assignment: les paramètres de configuration réseau et système, la date et l'heure du système] to [assignment: administrateurs système et réseau].

Supervision

FMT_SMF.1/FW**-Supervision Specification of management functions**

Hierarchical to: No other components.
Dependencies: No dependencies.

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

- visualisation des paramètres systèmes et réseau du chiffreur IP,
- modification des paramètres systèmes et réseau du chiffreur IP,
- supervision de l'état du pare-feu].

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

Hierarchical to: No other components.
Dependencies: No dependencies.

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

Raffinement global:

Les données exportées hors du contrôle de la TOE sont les données strictement nécessaires à la supervision, transmises à un équipement de supervision. Il faut s'assurer que ces données ne contiennent pas d'informations confidentielles ou sinon, les protéger.

Recyclage

FDP_RIP.1/FW**-Recyclage_TOE Subset residual information protection**

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_RIP.1.1/FW-Recyclage_TOE The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: deallocation of the resource from] the following objects: [assignment: tous les biens sensibles du pare-feu:

- Politiques de filtrage du pare-feu,
- Paramètres de configuration,
- Traces d'audit des flux traités par le pare-feu,
- Alarmes du pare-feu,
- Traces d'audit des opérations d'administration éffectuées sur le pare-feu].

FDP_ACC.1/FW**-Recyclage_TOE Subset access control**

Hierarchical to: No other components.
Dependencies: FDP_ACF.1

FDP_ACC.1.1Recyclage_TOE The TSF shall enforce the [assignment: politique d'accès aux biens sensibles] on [assignment:

- sujets: les administrateurs;
- objets: tous les biens sensibles du pare-feu : politiques de filtrage, paramètres de configuration, traces d'audit des flux traités par le pare-feu, traces d'audit des opérations d'administration éffectuées sur le pare-feu;
- opérations: effacer].

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

Hierarchical to: No other components.
Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1/FW-Recyclage_TOE The TSF shall enforce the [assignment: politique d'accès aux biens sensibles] to objects based on the following: [assignment:

- sujets: les administrateurs sur la base de leur rôle;
- objets: tous les biens sensibles du pare-feu : politiques de filtrage, paramètres de configuration, traces d'audit des flux traités par le pare-feu, traces d'audit des opérations d'administration éffectuées sur le pare-feu].

FDP_ACF.1.2/FW-Recyclage_TOE The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: L'effacement (complet ou partiel) des biens sensibles (politiques de filtrage, parameters de configuration, traces d'audit des flux traités par le pare-feu, traces d'audit des operations d'administration éffectuées sur le pare-feu) n'est autorisé qu'au rôle de responsable de sécurité].

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

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

5.1.2.2 Exigences de sécurité fonctionnelles pour le chiffreur IP

Application de la politique de sécurité VPN

FDP_IFC.1/VPN-Enforcement_policy Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1

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

- Information: données applicatives et toplogiques continues dans les paquets IP.
- Subject: le chiffreur IP.
- Operations: toutes les operations effectuées par le chiffreur IP transformant les données applicatives et topologiques en flux. Cela concerne les operations suivantes :
  - Envoi d'un paquet IP vers le réseau externe
  - Envoi d'un paquet IP vers le réseau privé
  - Réception d'un paquet provenant du réseau externe
  - Réception d'un paquet provenant du réseau interne].

FDP_IFF.1/VPN-Enforcement_policy Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1, FMT_MSA.3

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

- AT.policy_defined : attribut indiquant si une politique de sécurité VPN a été définie pour un lien VPN donné].

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

- L'envoi de paquets IP vers le réseau externe n'est autorisé que si les protections de sécurité définies dans la poltique de protection VPN associée sont appliquées aux données applicatives et topologiques des paquets IP avant l'envoi vers le réseau externe.
- L'envoi de paquets IP vers le réseau interne n'est autorisé que si les protections de sécurité définies dans la politique de protection VPN associée sont appliquées aux données applicatives et topologiques avant l'envoi vers le réseau privé interne.
- La reception de paquets IP en provenance du réseau externe est autorisée.
- La reception de paquets IP en provenance d'un réseau privé interne est autorisée].

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

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

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

FDP_IFF.1.6/VPN-Enforcement_policy The TSF shall explicitly deny an information flow based on the following rules: [assignment
- Lorsqu'aucune politique de protection VPN n'a été définie pour un lien VPN donné (attribut AT.policy_defined ayant pour valeur « Politique de protection VPN non définie »), la TSF doit rejeter les paquets IP, les paquets IP ne sont donc pas transmis.
- Lorsqu'une politique de protection VPN indique que l'envoi de paquets IP à destination d'une adresse est interdit, la TSF ne doit pas transmettre les paquets IP.
- Lorsqu'une erreur est détectée durant l'exploitation de la TOE, ou suite à la verification des protections de sécurité, tous les envois de paquets IP sont interdits].

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

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3

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

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

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

Raffinement global:

Les données utilisateurs (user data) mentionnées dans ces exigences sont les paquets IP des utilisateurs du réseau interne, comprenant les données applicatives et topologiques.

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

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 or FDP_IFC.1]

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

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

Raffinement global:

Les données utilisateurs (user data) mentionnées dans ces exigences sont les paquets IP des utilisateurs du réseau interne, comprenant les données applicatives et topologiques.

FCS_COP.1/VPN-Enforcement_policy Cryptographic operation

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2

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

Raffinement global:

Les algorithmes cryptographiques RSA (2048 bits), AES (128 et 256 bits) et SHA256 sont mis en œuvre dans le cadre du protocole IKE.
Les algorithmes cryptographiques AES (128 et 256 bits) et SHA256 bits sont eux mis en œuvre dans le cadre du protocole IPSEC.

Protection de la politique de sécurité VPN

FDP_ACC.1/VPN-VPN_policy **Subset access control**

Hierarchical to: No other components.
Dependencies: FDP_ACF.1

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

- Objects: les politiques de protection VPN et leurs contexts de sécurité associés.
- Subjects: fonctions d'administration de sécurité de la TOE permettant de definer et d'afficher les politiques de protection VPN et leurs contexts associés.
- Operations: definer et d'afficher les politiques de protection VPN et leurs contexts de sécurité associés.].

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

Hierarchical to: No other components.
Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1/VPN-VPN_policy The TSF shall enforce the [assignment: la politique de protection VPN] to objects based on the following: [assignment:
- AT.policy_defined : AT.policy_defined : attribut indiquant si une politique de sécurité VPN a été définie pour un lien VPN donné].

FDP_ACF.1.2/VPN-VPN_policy The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:
- La definition des politiques de protection VPN et leurs contextes de sécurité associés n'est autorisée qu'à un administrateur de sécurité et aucun autre rôle.
- L'affichage des politiques de protection VPN et leurs contextes de sécurité associés n'est autorisée qu'à un administrateur de sécurité et aucun autre rôle].

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

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

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

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3

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

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

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

Raffinement global:

Les données utilisateurs (user data) mentionnées dans ces exigences correspondent aux politiques de sécurité du chiffreur IP.

FMT_MSA.3/VPN-VPN_policy Static attribute initialisation

Hierarchical to: No other components.
Dependencies: FMT_MSA.1, FMT_SMR.1

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

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

Raffinement global:

L'attribut de sécurité (security attribute) concerné par ces exigences est l'attribut AT.policy_defined qui indique pour chaque lien de communication VPN si une politique de sécurité VPN et son contexte de sécurité sont defines. La valeur initiale de l'attribut AT.policy_defined est : « Politique de sécurité VPN non définie ». Cette valeur est changée par l'administrateur de sécurité de la TOE lorsqu'il définit pour un lien de communication VPN, la politique de sécurité et le contexte de sécurité de ce lien. La valeur de cet attribut devient alors : « Politique de sécurité VPN définie ».

FMT_MSA.1/VPN-VPN_policy Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1

FMT_MSA.1.1/VPN-VPN_policy The TSF shall enforce the [assignment: la politique de protection VPN] to restrict the ability to [selection: modify] the security attributes [assignment: AT.policy_defined] to [assignment: administrateur de sécurité].

FMT_SMF.1/VPN-VPN_policy Specification of management functions

Hierarchical to: No other components.
Dependencies: No dependencies.

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

- configuration des paramètres de la TOE :
  - des rôles des administrateurs,
  - données d'identification et d'authentification des administrateurs,
  - droits d'accès
  - date et heure du système
- configuration des paramètres système et réseau ;
- configuration de la politique de sécurité VPN (révocation d'un chiffreur IP, attribution des clés cryptographiques aux liens VPN, diffusion du certificat d'un chiffreur IP vers les autres chiffreur IP, …)].

Génération des traces d'audit des flux

FAU_GEN.1/VPN-Audit_flux Audit data generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the minimal or basic level of audit définis dans l'annexe 1 avec le niveau d'audit associé ; and
c) [assignment : none]

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

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

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

- un indentifiant numérique unique pour chaque évènement d'audit de flux du chiffreur IP, incrémenté d'une unité à chaque enregistrement d'un nouvel évènement d'audit de flux du chiffreur IP].

Raffinement global:

Les évènements d'audit (audit events) mentionnés dans ces exigences correspondent aux évènements liés à la communication entre des chiffreurs IP.

FAU_SAR.1/VPN-Audit_flux Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

FAU_SAR.1.1/VPN-Audit_flux The TSF shall provide [assignment: auditeurs] with the capability to read [assignment: les traces d'audit des flux traits par le chiffreur IP] from the audit records.

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

FAU_SAR.3/VPN-Audit_flux Selectable audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1

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

- L'adresse IP source et destination des flux chiffrés,
- la date et l'heure du traitrement des paquets].

Protection des traces d'audit de flux

FAU_STG.1/VPN-Traces_audit_flux Protected audit trail storage

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

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

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

Génération des traces d'audit des opérations d'administration

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

Hierarchical to: No other components.
Dependencies: FPT_STM.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the minimal or basic level of audit définis dans l'annexe 1 avec le niveau d'audit associé ; and
c) [assignment: none].

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment:

- un indentifiant numérique unique pour chaque évènement d'audit d'administration du chiffreur IP, incrémenté d'une unité à chaque enregistrement d'un nouvel évènement d'audit d'administration du chiffreur IP].

Raffinement global:

Les évènements d'audit (audit events) mentionnés dans ces exigences correspondent aux évènements liés aux opérations d'administration de la TOE.

FAU_SAR.1/VPN-Audit_admin Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

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

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

FAU_SAR.3/VPN-Audit_admin Selectable audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1

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

- Le type d'opération d'administration,
- L'identité de l'administrateur,
- La date et l'heure à laquelle l'opération d'administration a été effectuée.]

Protection des traces d'audit des opérations d'administration

FAU_STG.1/VPN-Traces_audit_admin Protected audit trail storage

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

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

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

Alarmes

FAU_SAA.1/VPN-Alarmes Potential violation analysis

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

FAU_SAA.1.1/VPN-Alarmes The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

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

a) Accumulation or combination of [assignment:
- Violation de la politique de sécurité du chiffreur IP de la TOE,
- Saturation des journaux du chiffreur IP de la TOE,
- Perte d'intégrité du chiffreur IP de la TOE,
- Saturation système (disque dur, quarantaine, …)
- Déni de service du chiffreur IP de la TOE,
- Echec d'authentification d'un utilisateur du réseau privé (utilisation d'un certificat révoqué ou non intègre, secret partagé erroné, clé proposée non valable
- Données chiffrées ne correspondant pas au contexte de sécurité du lien VPN]

known to indicate a potential security violation;
b) [assignment: aucun].

FAU_ARP.1/VPN-Alarmes **Security alarms**

Hierarchical to: No other components.
Dependencies: FAU_SAA.1

FAU_ARP.1.1/VPN-Alarmes The TSF shall take [assignment:
- Une alarme de sécurité est transmise à l'administrateur de sécurité,
- [assignment: aucun]]

upon detection of a potential security violation.

Configuration

FMT_MTD.1/VPN-Network_param Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1, FMT_SMF.1

FMT_MTD.1.1/VPN-Network_param The TSF shall restrict the ability to [selection: query and modify] the [assignment: paramètres de configuration système et réseau] to [assignment: administrateur système et réseaux].

Supervision

FMT_SMF.1/VPN-Config_supervision **Specification of management functions**

Hierarchical to: No other components.
Dependencies: No dependencies.

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

- visualisation des paramètres systèmes et réseau du chiffreur IP,
- modification des paramètres systèmes et réseau du chiffreur IP,
- supervision de l'état du chiffreur IP].

Recyclage

FDP_RIP.1/VPN Subset residual information protection

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_RIP.1.1/VPN The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: deallocation of the resource from] the following objects: [assignment: tous les biens sensibles du chiffreur IP :

- Politiques de protection VPN,
- Paramètres de configuration,
- Clés cryptographiques,
- Traces d'audit des flux traités par le chiffreur IP,
- Alarmes du chiffreur IP,
- Traces d'audit des opérations d'administration éffectuées sur le chiffreur IP].

Gestion des clés cryptographiques

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

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3

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

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

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

Raffinement global:

Les données utilisateurs (user data) mentionnées dans ces exigences correspondent aux clés cryptographiques qui sont injectées dans le chiffreur IP de la TOE.

FDP_IFC.1/VPN-Key_policy Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1

FDP_IFC.1.1/Key_policy The TSF shall enforce the [assignment: la politique de gestion des clés cryptographiques] on [assignment:

- Information: valeur des clés cryptographiques du chiffreur IP
- Subjects: les administrateurs de sécurité
- Operations: l'injection des clés cryptographiques dans le chiffreur IP, et l'export des clés cryptographiques du chiffreur IP hors de ce dernier].

FDP_IFF.1/VPN-Key_policy Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1, FMT_MSA.3

FDP_IFF.1.1/VPN-Key_policy The TSF shall enforce the [assignment: la politique de gestions des clés cryptographiques] based on the following types of subject and information security attributes: [assignment:

- AT.key_type attribute : indique si une clé cryptographique est publique, privée ou secrete.
- [assignment: none].

FDP_IFF.1.2/VPN-Key_policy The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: l'injection locale des clés cryptographiques n'est autorisée que si elle est realise par un administrateur de sécurité préalablement authentifié].

FDP_IFF.1.3/VPN-Key_policy The TSF shall enforce the [assignment: injection des clés cryptographiques statiques privées et secrètes dans le chiffreur IP en les protégeant en intégrité et en confidentialité].

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

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

FDP_IFF.1.6/VPN-Key_policy The TSF shall explicitly deny an information flow based on the following rules: [assignment: l'export en clair, hors du chiffreur IP, de clés privées ou secretes est interdit].

FMT_MSA.3/VPN-Key_policy Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1, FMT_SMR.1

FMT_MSA.3.1/VPN-Key_policy The TSF shall enforce the [assignment: la politique de gestion des clés cryptographiques] to provide [selection: [assignment: le type de clé cryptographiques (privée, secrete, publique, approprié] default values for security attributes that are used to enforce the SFP.

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

FTA_TSE.1/VPN-Key_policy TOE session establishment

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_TSE.1.1/VPN-Key_policy The TSF shall be able to deny session establishment based on [assignment: la durée de vie des clés cryptographiques de session].

FCS_CKM.1/VPN-Key_policy Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2

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

FCS_CKM.4/VPN-Key_policy Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC2 or FCS_CKM.1], FMT_MSA.2

FCS_CKM.4.1/VPN-Key_policy The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: méthode de destruction des clés cryptographiques par réécriture de motifs aléatoires 7 passes] that meets the following: [assignment: none].

5.1.3 Niveau minimal de résistance des fonctions de sécurité

Le niveau minimal exigé de résistance des fonctions de sécurité de la TOE (SOF-Claim) [1] est : **élevé** (**SOF-high**).

5.2 Exigences d'assurance pour la TOE

Le niveau visé est **EAL3 augmenté** des composants AVA_VLA.2 et ALC_FLR.3.

[1] Niveau de résistance intrinsèque d'une fonction face à des attaques. Ce niveau ne doit pas être confondu avec le niveau de résistance global de la TOE (niveau défini par le composant AVA_VLA) qui prend en compte des attaques altérant ou rendant inopérantes des fonctions de la TOE.

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

Toutes les exigences d'assurance pour la TOE sont extraites de la partie 3 des Critères communs [CC].

Les dépendances de l'exigence d'assurance AVA_VLA.2 (ADV_IMP.1 et ADV_LLD.1) sont couvertes par les travaux d'expertise cryptographique réalisés par le CESTI. Ces travaux sont décrits dans [QS].

5.3 Exigences pour l'environnement technique de la TOE

Toutes les exigences de sécurité fonctionnelles pour l'environnement technique de la TOE sont issues de la Partie 2 des Critères Communs [CC].

FIA_UAU.2-Administration_distante User authentication before any action

Hierarchical to: FIA_UAU.1
Dependencies: FIA_UID.1

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

Raffinement global:

Il s'agit ici de l'authentification distante de l'administrateur sur la station d'administration distante.

6 Résumé des spécifications de la TOE

6.1 Fonctions de sécurité

F.RELIABLE_TIME

SOF-claim : No SOF claim

Cette fonction fournit à la TOE une base de temps fiable et unique. La modification de l'heure système de la TOE ne peut-être effectuée que par un administrateur de sécurité ou un administrateur système et réseau authentifié.

F.AUDIT

SOF-claim : No SOF claim

La fonction d'audit implémente les functions de sécurité relatives à la journalisation des évènements de la TOE. Elle gère l'identification, l'enregistrement, et le stockage des évènements de la TOE. Les évènements enregistrés sont de trois types : les traces d'audit de flux, les traces d'administration et les alarmes de sécurité. Les traces d'audit de flux fournissent des informations sur les paquets traités par le pare-feu et le chiffreur IP de la TOE (flux bloqué ou rejeté à cause de la politique de sécurité de la TOE). Les traces d'audit d'administration fournissent des informations sur les opérations d'administrateurs effectués sur la TOE. Les alarmes de sécurité indiquent un problème sévère pouvant mettre en cause la sécurité de la TOE.

Le logiciel FAST Monitoring Console, installé sur une station d'administration distante offre aux administrateurs autorisés et authentifiés un environnement graphique leur permettant de consulter les journaux d'audit et de détecter ainsi tous les évènements relatifs à la sécurité de la TOE. Les alertes possèdent un niveau de sévèrité, sont horodatées, et accompagnées d'une description explicative permettant aux administrateurs d'agir en conséquence. Les traces d'audit de flux possèdent les détails relatifs aux paquets ayant entrainé les enregistrements, et sont horodatés. Les traces d'audit d'administration possèdent l'identité de l'administrateur, la description de l'opération effectuée, et sont horodatées. L'interface graphique de FAST Monitoring permet de trier chacun des types d'évènement selon les critères définis par les administrateurs de la TOE.

La focntion d'audit de la TOE offre une interface permettant aux administrateurs de la TOE d'exporter ces données hors de la TOE, purgeant ainsi l'espace disque dédié aux journaux. L'accès aux journaux d'évènement n'est accessible qu'aux administrateurs authentifiés.

F.USER_DATA_PROTECTION_FW

SOF-claim : No SOF claim

La fonction de protection des utilisateurs implémente les fonctions de sécurité de la TOE relative au pare-feu. Cette fonction assure la protection des utilisateurs du réseau protégé

en effectuant un filtrage des flux échangés entre le réseau protégé et le réseau externe (non sûr), conformément à un politique de sécurité du pare-feu (également appelée politique de filtrage) définie par l'administrateur.

La TOE effectue d'abrord une permière vérification (adresse IP, port, …) pour vérifier la cohérence du paquet IP par rapport à la politique de filtrage définie par l'administrateur de sécurité. A la suite de cette première vérification, le paquet IP peut être soit rejeté, soit accepté. Si le paquet accepté, une seconde vérification (couche applicative) est ensuite réalisée pour vérifier la cohérence du paquet par rapport à la politique de filtrage applicative de la TOE. La TOE est capable d'effectuer un filtrage sur les protocoles HTTP, FTP, SMTP, DNS. Pour chacun de ces protocoles supprotés, la TOE vérifie la cohérence syntaxique des paquets par rapport aux RFCs de ces protocoles. La TOE effectue également un contrôle sur les commandes applicatives utilisées dans les paquets. Ainsi, un administrateur de sécurité de la TOE peut n'autoriser que certaines commandes pour un protocole applicatif donné parmi HTTP, FTP, SMTP, DNS.

F.USER_DATA_PROTECTION_VPN

SOF-claim : high

La fonction de protection des utilisateurs des réseaux privés implémente les fonctions de sécurité de la TOE relative au chiffreur IP. Cette fonction assure la protection des utilisateurs du réseau privé en assurant la confidentialité, l'intégrité et l'authenticité des flux émis entre un utilisateur du réseau privé et un autre utilisateur d'un autre réseau privé, et qui transitent par un réseau externe (non sûr).

La TOE supporte les algorithmes cryptographiques suivants : AES et RSA.

F.ROLES

SOF-claim : No SOF claim

La fonction de gestion des rôles permet de gérer les différents rôles des administrateurs au sein de la TOE : responsable de sécurité, administrateur de sécurité, administrateur système et réseau et auditeur. Les quatres rôles administrateurs offrent des privilèges différents et donc fonctions d'administrations différentes. La configuration des rôles, et l'attribution d'un rôle sont des opérations qui ne sont accessibles qu'aux responsables de sécurité authentifiés.

F.ADMINISTRATION

SOF-claim : No SOF claim

La fonction d'administration permet aux administrateurs de la TOE d'accéder localement ou à distance (depuis une station d'administration) aux fonctions d'administration de la TOE. La fonction d'administration permet :

- Aux responsables de sécurité : de gérer (créer, modifier, supprimer) les comptes des différents administrateurs de la TOE,

- Aux administrateurs de sécurité : de gérer (créer, modifier, supprimer) les règles implémentées dans les politiques de filtrage du pare-feu de la TOE, de gérer (créer, modifier, supprimer) les politiques de sécurité VPN du chiffreur IP de la TOE, de gérer (créer, modifier, supprimer) les comptes des utilisateurs du service VPN de la TOE, de consulter les journaux d'audit et alarmes de la TOE, d'effacer de manière sécurisée les biens sensibles de la TOE.
- Aux auditeurs : consulter et gérer les évènements d'audit et les alarmes de sécurité relatifs aux flux IP transitant par le pare-feu de la TOE ou le chiffreur IP de la TOE et aux opérations d'administrations.
- Aux administrateurs système et réseau : de configurer les paramètres réseau de la TOE et de superviser l'état de la TOE.

Les logiciels Arkoon Manager et Arkoon Monitoring, installés sur les stations d'administration permettent offrent une interface graphique aux administrateurs leur permettant de réaliser des opérations d'administration en accors avec leurs privilèges.

F.REINIT

SOF-claim : high

La fonction de réinitialisation de la TOE permet aux administrateurs de sécurité de la TOE d'effacer définitivement les biens sensibles de la TOE (politiques de filtrage, politique VPN, clés privées, informations d'authentification, …). Le mécanisme de sécurité pour effacer une donnée sensible est une surcharge aléatoire 7 passes : chaque cluster du disque dur référençant la donnée sensible à effacer est comblé par des valeurs aléatoires. L'étape est ensuite répétée six fois.

F.LOCAL_ADMIN_IDENTIFICATION_AUTHENTICATION

SOF-claim : high

La fonction d'authentification locale permet aux administrateurs de la TOE de s'authentifier en local sur la TOE. Un administrateur est impérativement authentifié avant tout accès aux fonctions d'administration.

F.REMOTE_STATION_AUTHENTICATION

SOF-claim : high

Sur les stations d'administration de la TOE sont installés un client lourd d'administration et un certificat (et une clé privée) propre à chaque administrateur. Les administrateurs de la TOE s'authentifient au service d'administration de la TOE en utilisant leur couple clé privée/clé publique installé sur la station d'administration. La bi-clé des administrateurs permet d'une part une authentification mutuelle entre l'administrateur et la TOE, et d'autre part de protéger (en confidentialité/intégrité/authenticité) les flux échangés entre la TOE et la station d'administration.

F.REMOTE_ADMIN_PROTECTION

SOF-claim : high

La fonction de protection de l'administration distante de la TOE permet de protéger en confidentialité, en intégrité et en authenticité les flux échangés entre la TOE et les administrateurs lors de l'administration distante de la TOE depuis une station d'administration distante.

6.2 Mesures d'assurance

Le développeur a mis en place les mesures suivantes d'assurance de sécurité.

GESTION DE CONFIGURATION

Le développeur utilise un système de gestion de configuration qui permet d'assurer l'intégrité de la TOE et de sa documentation lors des phases de développement.

LIVRAISON ET EXPLOITATION

Des procédures de livraison sûre et d'installation de la TOE sont disponibles.

DOCUMENTS DE CONCEPTION

Le développeur dispose d'une documentation technique décrivant la conception de la TOE à plusieurs niveau de raffinement (spécifications fonctionnelles, conception de haut-niveau, conception de bas-niveau).

GUIDES

La documentation d'utilisation et d'administration de la TOE est disponible.

SUPPORT AU CYCLE DE VIE

Le développement de la TOE est réalisé dans un environnement sécurisé.

Il existe un support technique assurant la maintenance corrective et évolutive du produit.

TESTS FONCTIONNELS

Des tests fonctionnels intensifs sont réalisés pour toutes les versions de la TOE.

ANALYSE DE VULNERABILITES

Toutes les vulnérabilités connues par le développeur pour ce type de produit ont été prises en compte lors du développement du produit.

7 Conformité à un profil de protection

La présente cible de sécurité est conforme au profil de protection [PP_FWIP].

Cette cible ne peut prétendre une conformité par rapport au profil de protection [PP_CIP], puisque [PP_CIP] est conforme à la version 2.2 des Critères Communs, alors que ce document réclame une conformité à la version 2.3 des Critères Communs. Cependant, la totalité des hypothèses, menaces, politiques de sécurité de l'organisation, objectifs de sécurité pour la TOE, objectifs de sécurité pour l'environnement de la TOE et exigences de sécurité fonctionnelles définies par [PP_CIP] sont intégrées dans la présente cible.

Par rapport au profil de protection [PP_CIP], les éléments suivants ont été modifiés :

Dans le profil de protection du chiffreur IP [PP_CIP], l'administrateur de sécurité configure les rôles et les accès aux outils et fonctions d'administration, il gère également les clés et les moyens d'authentification pour accéder aux outils d'administration. Dans le profil de protection du pare-feu [PP_FWIP], c'est le responsable de sécurité (rôle n'existant pas dans [PP_CIP]) qui effectue ces opérations.

Dans la présente cible, les compétences de gestion des rôles pour le chiffreur IP, des accès aux outils et fonctions d'administration du chiffreur IP, et des clés cryptographiques du chiffreur IP sont transférées au responsable de sécurité.

8 Argumentaires

8.1 Argumentaires des objectifs de sécurité

Tableau 1 : Couverture menaces, hypothèses et politiques de sécurité organisationelles

	Hypothèses										Menaces																				OSP								
Objectifs de sécurité	A.ADMIN	A.INITIALISATION_LOCAL	A.LOCAL	A.AUTHENTIFICATION_ADMIN_DISTANT	A.FW.AUDIT	A.FW.ALARMES	A.FW.MAITRISE_CONFIGURATION	A.VPN.AUDIT	A.VPN.ALARMES	A.VPN.MAITRISE_CONFIGURATION	A.VPN.CRYPTO_EXT	T.USURPATION_ADMIN	T.DYSFONCTIONNEMENT	T.FW.MODIFICATION_POL_FILTRAGE	T.FW.DIVULGATION_POL_FILTRAGE	T.FW.MODIFICATION_PARAM	T.FW.DIVULGATION_PARAM	T.FW.MODIFICATION_AUDIT_FLUX	T.FW.MODIFICATION_AUDIT_ADMIN	T.FW.MODIFICATION_ALARMES	T.FW.CHANGEMENT_CONTEXTE	T.VPN.MODIFICATION_POL_VPN	T.VPN.DIVULGATION_POL_VPN	T.VPN.USURPATION_ID	T.VPN.MODIFICATION_PARAM	T.VPN.DIVULGATION_PARAM	T.VPN.MODIFICATION_CLES	T.VPN.DIVULGATION_CLES	T.VPN.MODIFICATION_AUDIT_FLUX	T.VPN.MODIFICATION_AUDIT_ADMIN	T.VPN.MODIFICATION_ALARMES	T.VPN.CHANGEMENT_CONTEXTE	OSP.QUALIF	OSP.CRYPTO	OSP.GESTION_ROLES	OSP.FW.SERVICE	OSP.FW.VISUALISATION_POL	OSP.FW.AUDIT_FLUX	OSP.VPN.SERVICE	OSP.VPN.VISUALISATION_POL	OSP.VPN.SUPERVISION
OT.QUALIF																																		X								
OT.GESTION_ROLES																																				X						
OT.PROTECTION_FLUX_ADMIN												X		X	X	X	X	X	X	X		X	X		X	X	X	X	X	X	X				X						
OT.AUTHENTIFICATION_ADMIN												X		X	X	X	X	X	X	X		X	X		X	X	X	X	X	X	X				X						
OT.FW .APPLICATION_POL_FILTRAGE														X	X	X	X	X	X	X		X	X		X	X	X	X	X	X	X					X					
OT.FW .COHERENCE_POL																																					X					
OT.FW.PROTECTION_POL_FILTRAGE														X	X																											
OT.FW .VISUALISATION_POL																																						X				
OT.FW.PROTECTION_PARAM																X	X																									
OT.FW.CHANGEMENT_CONTEXTE																	X					X																				
OT.FW.SUPERVISION													X																													
OT.FW.IMPACT_SUPERVISION													X	X	X	X	X	X	X	X																						
OT.FW .AUDIT_FLUX														X	X	X	X																						X			
OT.FW.PROTECTION_AUDIT_FLUX																		X																								
OT.FW.AUDIT_ADMIN												X		X	X	X	X	X	X	X																X						
OT.FW.PROTECTION_AUDIT_ADMIN																				X																						
OT.FW.ALARMES												X		X	X	X	X	X	X																						
OT.FW.PROTECTION_ALARMES																					X																					
OT.VPN.APPLICATION_POL																																									X		
OT.VPN.CONFIDENTIALITE_APPLI																									X																X		

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

	Hypothèses											Menaces																					OSP								
Objectifs de sécurité	A.ADMIN	A.INITIALISATION_LOCAL	A.LOCAL	A.AUTHENTIFICATION_ADMIN_DISTANT	A.FW.AUDIT	A.FW.ALARMES	A.FW.MAITRISE_CONFIGURATION	A.VPN.AUDIT	A.VPN.ALARMES	A.VPN.MAITRISE_CONFIGURATION	A.VPN.CRYPTO_EXT	T.USURPATION_ADMIN	T.DYSFONCTIONNEMENT	T.FW.MODIFICATION_POL_FILTRAGE	T.FW.DIVULGATION_POL_FILTRAGE	T.FW.MODIFICATION_PARAM	T.FW.DIVULGATION_PARAM	T.FW.MODIFICATION_AUDIT_FLUX	T.FW.MODIFICATION_AUDIT_ADMIN	T.FW.MODIFICATION_ALARMES	T.FW.CHANGEMENT_CONTEXTE	T.VPN.MODIFICATION_POL_VPN	T.VPN.DIVULGATION_POL_VPN	T.VPN.USURPATION_ID	T.VPN.MODIFICATION_PARAM	T.VPN.DIVULGATION_PARAM	T.VPN.MODIFICATION_CLES	T.VPN.DIVULGATION_CLES	T.VPN.MODIFICATION_AUDIT_FLUX	T.VPN.MODIFICATION_AUDIT_ADMIN	T.VPN.MODIFICATION_ALARMES	T.VPN.CHANGEMENT_CONTEXTE	OSP.CRYPTO	OSP.GESTION_ROLES	OSP.FW.SERVICE	OSP.FW.VISUALISATION_POL	OSP.FW.AUDIT_FLUX	OSP.VPN.SERVICE	OSP.VPN.VISUALISATION_POL	OSP.VPN.SUPERVISION	OSP.CRYPTO
OE.FW.INTEGRITE							X						X	X		X	X																							
OE.VPN.ANALYSE_AUDIT								X																						X	X				X			X			
OE.VPN.TRAITE_ALARMES									X														X	X	X	X	X			X	X	X								
OE.VPN.INTEGRITE										X			X										X			X														
OE.VPN.CRYPTO_EXT											X														X			X	X					X						
OE.INITIALISATION_LOCAL		X																																					

8.1.1 Hypothèses

A.ADMIN

Cette hypothèse se traduit par l'objectif de sécurité OE.ADMIN qui impose que les administrateurs soient non hostiles et formés à leurs tâches.

A.LOCAL

Cette hypothèse se traduit par l'objectif de sécurité OE.PROTECTION_LOCAL qui impose que les équipements de la TOE ainsi que les supports contenant les biens sensibles de la TOE doivent se trouver dans un lieu sécurisé.

A.INITIALISATION_LOCAL

Cette hypothèse se traduit par l'objectif de sécurité OE.INITIALISATION_LOCAL qui impose que les équipements de la TOE doivent être initialisés dans le local protégé de l'appliance dont l'accès est contrôlé et restreint aux administrateurs. Cette initialisation doit être effectuée depuis une station d'administration directement connectée sur les équiements.

A.AUTHENTIFICATION_ADMIN_DISTANT

Cette hypothèse se traduit par l'objectif de sécurité OE.AUTHENTIFICATION_ADMIN_DISTANT qui impose que l'environnement de la TOE doit permettre d'authentifier les administrateurs pour les accès distants à la TOE.

Pare-feu

A.FW.AUDIT

Cette hypothèse se traduit par l'objectif de sécurité OE.FW.ANALYSE_AUDIT qui impose une consultation régulière des évènements d'audit générés par le pare-feu par l'auditeur et une gestion des audits évitant la perte de tout enregistrement.

A.FW.ALARMES

Cette hypothèse se traduit par l'objectif de sécurité OE.FW.TRAITE_ALARMES qui impose un traitement des alarmes générées et remontées par le pare-feu par l'administrateur de sécurité.

A.FW.MAITRISE_CONFIGURATION

Cette hypothèse se traduit par l'objectif de sécurité OE.FW.INTEGRITE qui donne à l'administrateur les moyens de contrôler la configuration matérielle et logicielle du pare-feu (services et biens) par rapport à un état de référence, ou de la régénérer.

Chiffreur IP

A.VPN.AUDIT

Cette hypothèse est supportée par OE.VPN.ANALYSE_AUDIT qui impose une consultation régulière des évènements d'audit générés par le chiffreur IP par l'auditeur et une gestion des audits évitant la perte de tout enregistrement.

A.VPN.ALARMES

Cette hypothèse est supportée par OE.VPN.TRAITE_ALARMES qui impose un traitement des alarmes générées et remontées par le chiffreur par l'administrateur de sécurité.

A.VPN.MAITRISE_CONFIGURATION

Cette hypothèse est supportée par OE.VPN.INTEGRITE qui donne à l'administrateur les moyens de contrôler la configuration matérielle et logicielle du chiffreur (services et biens) par rapport à un état de référence, ou de la régénérer.

A.VPN.CRYPTO_EXT

Cette hypothèse est supportée par OE.VPN.CRYPTO_EXT impose que les clés cryptographiques, générées à l'extérieur de la TOE, et qui sont injectées dans la TOE doivent avoir été générées en suivant les recommandations spécifiées dans les référentiels de cryptographie de la DCSSI [CRYPTO] et [GC] pour le niveau de résistance standard.

8.1.2 Menaces

8.1.2.1 Couverture des menaces portant sur les politiques de sécurité de la TOE (TSP)

Pare-feu

T.FW.MODIFICATION_POL_FILTRAGE

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- permettre de filtrer les flux (OT.FW.APPLICATION_POL_FILTRAGE).
- offrir un contrôle d'accès à la politique de filtrage du pare-feu (OT.FW.PROTECTION_POL_FILTRAGE).
- offrir un service de supervision du pare-feu qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.FW.IMPACT_SUPERVISION).
- protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN) et authentifier localement l'administrateur de la TOE (OT.AUTHENTIFICATION_ADMIN). L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du pare-feu (OT.FW.AUDIT_ADMIN, OT.FW.AUDIT_FLUX et OT.FW.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.FW.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- pouvoir être remise dans un état précédemment validé (OE.FW.INTEGRITE).

T.FW.DIVULGATION_POL_FILTRAGE

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- permettre de filtrer les flux d'administration du pare-feu (OT.FW.APPLICATION_POL_FILTRAGE).
- offrir un contrôle d'accès à la politique de filtrage du pare-feu (OT.FW.PROTECTION_POL_FILTRAGE).
- offrir un service de supervision du pare-feu qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en les divulguant pas (OT.FW.IMPACT_SUPERVISION).
- protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN) et authentifier localement l'administrateur de la TOE (OT.AUTHENTIFICATION_ADMIN). L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du pare-feu (OT.FW.AUDIT_ADMIN, OT.FW.AUDIT_FLUX et OT.FW.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.FW.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- aucune action

Chiffreur IP

T.VPN.MODIFICATION_POL_VPN

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL)
- être utilisée par des administrateurs de confiance (OE.ADMIN)

Pour se protéger, la TOE doit :

- offrir un contrôle d'accès à la politique de protection des flux du chiffreur IP (OT.VPN.PROTECTION_POL et OT.VPN.DEFINITION_POL).
- offrir un service de supervision du chiffreur IP qui ne remet pas en cause ses biens sensibles car il ne les modifie pas et ne divulgue pas (OT.VPN.IMPACT_SUPERVISION).
- protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN) et authentifier localement l'administrateur de la TOE (OT.AUTHENTIFICATION_ADMIN). L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- permettre de filtrer les flux d'administration du chiffreur IP (OT.FW.APPLICATION_POL_FILTRAGE).

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES) L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- pouvoir être remise dans un état précédemment validé (OE.VPN.INTEGRITE)

T.VPN.DIVULGATION_POL_VPN

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL)
- être utilisée par des administrateurs de confiance (OE.ADMIN)

Pour se protéger, la TOE doit :

- offrir un contrôle d'accès à la politique de protection des flux du chiffreur IP (OT.VPN.PROTECTION_POL et OT.VPN.DEFINITION_POL).
- offrir un service de supervision du chiffreur IP qui ne remet pas en cause ses biens sensibles car il ne les modifie pas et ne divulgue pas (OT.VPN.IMPACT_SUPERVISION).
- protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN) et authentifier localement l'administrateur de la TOE (OT.AUTHENTIFICATION_ADMIN). L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- permettre de filtrer les flux d'administration du chiffreur IP (OT.FW.APPLICATION_POL_FILTRAGE).

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES) L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- aucune action

T.VPN.USURPATION_ID

Pour prévenir la menace, la TOE doit :

- aucune action

Pour se protéger, la TOE doit :

- offrir des services de sécurité permettant de protéger l'authenticité et la confidentialité des données applicatives et topologiques du réseau privé (OT.VPN.AUTHENTICITE_APPLI, OT.VPN.CONFIDENTIALITE_APPLI, OT.VPN.AUTHENTICITE_TOPO, OT.VPN.CONFIDENTIALITE_TOPO).
- générer de des clés cryptographiques de bonne qualité pour les services de sécurité cités plus haut et utiliser le protocole IKE lors de l'établissement d'un lien VPN (OT.CRYPTO).
- Utiliser des clés cryptographiques, générées à l'extérieur de la TOE, de bonne qualité, pour les services de sécurité cités plus haut (OE.VPN.CRYPTO_EXT).

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- aucune action

8.1.2.2 Couverture des menaces portant sur la configuration de la TOE

Pare-feu

T.FW.MODIFICATION_PARAM

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- permettre de filtrer les flux d'administration du pare-feu (OT.FW.APPLICATION_POL_FILTRAGE).
- offrir un contrôle d'accès aux biens sensibles du pare-feu (OT.FW.PROTECTION_PARAM).
- offrir un service de supervision du pare-feu qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.FW.IMPACT_SUPERVISION).
- protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN) et authentifier localement l'administrateur de la TOE (OT.AUTHENTIFICATION_ADMIN). L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du pare-feu (OT.FW.AUDIT_ADMIN, OT.FW.AUDIT_FLUX et OT.FW.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.FW.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- pouvoir être remise dans un état précédemment validé (OE.FW.INTEGRITE).

T.FW.DIVULGATION_PARAM

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).
- être recyclée lors d'un changement de contexte (OT.FW.CHANGEMENT_CONTEXTE)

Pour se protéger, la TOE doit :

- permettre de filtrer les flux d'administration du pare-feu (OT.FW.APPLICATION_POL_FILTRAGE).

- offrir un contrôle d'accès aux biens sensibles du pare-feu (OT.FW.PROTECTION_PARAM).
- offrir un service de supervision du pare-feu qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.FW.IMPACT_SUPERVISION).
- protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN) et authentifier localement l'administrateur de la TOE (OT.AUTHENTIFICATION_ADMIN). L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du pare-feu (OT.FW.AUDIT_ADMIN, OT.FW.AUDIT_FLUX et OT.FW.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.FW.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- aucune action

Chiffreur IP

T.VPN.MODIFICATION_PARAM

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- offrir un contrôle d'accès aux biens sensibles du chiffreur IP (OT.VPN.PROTECTION_PARAM).
- offrir un service de supervision du chiffreur IP qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.VPN.IMPACT_SUPERVISION).
- protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN) et authentifier localement l'administrateur de la TOE (OT.AUTHENTIFICATION_ADMIN). L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- permettre de filtrer les flux d'administration du chiffreur IP (OT.FW.APPLICATION_POL_FILTRAGE).

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- pouvoir être remise dans un état précédemment validé (OE.VPN.INTEGRITE).

T.VPN.DIVULGATION_PARAM

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).

- être utilisée par des administrateurs de confiance (OE.ADMIN).
- être recyclée lors d'un changement de contexte (OT.VPN.CHANGEMENT_CONTEXTE)

Pour se protéger, la TOE doit :

- offrir un contrôle d'accès aux biens sensibles du chiffreur IP (OT.VPN.PROTECTION_PARAM).
- offrir un service de supervision du chiffreur IP qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.VPN.IMPACT_SUPERVISION).
- protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN) et authentifier localement l'administrateur de la TOE (OT.AUTHENTIFICATION_ADMIN). L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- permettre de filtrer les flux d'administration du chiffreur IP (OT.FW.APPLICATION_POL_FILTRAGE).

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.VPN.AUDIT_ADMIN, OT.VPN.AUDIT_FLUX et OT.VPN.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- aucune action

8.1.2.3 Couverture des menaces portant sur les clés cryptographiques

Chiffreur IP

T.VPN.MODIFICATION_CLES

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- garantir l'intégrité et la confidentialité des clés cryptographiques lors de leur injection dans la TOE (OT.VPN.INJECTION_CLES)
- garantir que seuls les administrateurs locaux authentifiés ont accès aux clés cryptographiques (OT.AUTHENTIFICATION_ADMIN). La TOE doit protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN), et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)
- Protéger l'accès aux clés cryptographiques (OT.VPN.ACCES_CLES).
- offrir un service de supervision du chiffreur IP qui ne remet pas en cause l'intégrité des clés cryptographiques en ne les modifiant pas et en ne les divulguant pas (OT.VPN.IMPACT_SUPERVISION).

- permettre de filtrer les flux d'administration du chiffreur IP (OT.FW.APPLICATION_POL_FILTRAGE).
- Utiliser des clés cryptographiques, générées à l'extérieur de la TOE, de bonne qualité (OE.VPN.CRYPTO_EXT).

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- pouvoir offrir à l'administrateur de sécurité de modifier la politique de sécurité VPN pour un lien VPN (OT.VPN.DEFINITION_POL), en injectant de nouvelles clés statique pour le lien VPN (OT.VPN.INJECTION_CLES) par exemple.

T.VPN.DIVULGATION_CLES

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).
- utiliser des clés cryptographiques renouvelées régulièrement (OT.CRYPTO)

Pour se protéger, la TOE doit :

- garantir l'intégrité et la confidentialité des clés cryptographiques lors de leur injection dans la TOE (OT.VPN.INJECTION_CLES)
- garantir que seuls les administrateurs locaux authentifiés ont accès aux clés cryptographiques (OT.AUTHENTIFICATION_ADMIN). La TOE doit protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN), et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)
- Protéger l'accès aux clés cryptographiques (OT.VPN.ACCES_CLES).
- offrir un service de supervision du chiffreur IP qui ne remet pas en cause l'intégrité des clés cryptographiques en ne les modifiant pas et en ne les divulguant pas (OT.VPN.IMPACT_SUPERVISION).
- permettre de filtrer les flux d'administration du chiffreur IP (OT.FW.APPLICATION_POL_FILTRAGE).
- Utiliser des clés cryptographiques, générées à l'extérieur de la TOE, de bonne qualité (OE.VPN.CRYPTO_EXT).

Pour détecter l'occurrence de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- pouvoir offrir à l'administrateur de sécurité de modifier la politique de sécurité VPN pour un lien VPN (OT.VPN.DEFINITION_POL), en injectant de nouvelles clés statique pour le lien VPN (OT.VPN.INJECTION_CLES) par exemple.

8.1.2.4 Couverture des menaces portant sur les traces d'audit des flux

Pare-feu

T.FW.MODIFICATION_AUDIT_FLUX

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- permettre de filtrer les flux d'administration du pare-feu (OT.FW.APPLICATION_POL_FILTRAGE).
- offrir un contrôle d'accès aux journaux d'audit des flux traités par le pare-feu (OT.FW.PROTECTION_AUDIT_FLUX).
- offrir un service de supervision du pare-feu qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.FW.IMPACT_SUPERVISION).
- garantir que seuls les administrateurs locaux authentifiés ont accès aux traces d'audit des flux du pare-feu (OT.AUTHENTIFICATION_ADMIN). La TOE doit protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN), et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurrence de la menace, la TOE doit :

- permettre de détecter la perte de traces d'audits du pare-feu (OT.FW.PROTECTION_AUDIT_FLUX).

Pour limiter l'impact de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.FW.AUDIT_ADMIN, OT.FW.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.FW.TRAITE_ALARMES).
- s'appuyer sur des mesures de sauvegarde et d'archivage des traces d'audit (OE.FW.ANALYSE_AUDIT).

Chiffreur IP

T.VPN.MODIFICATION_AUDIT_FLUX

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- offrir un contrôle d'accès aux journaux d'audit des flux traités par le chiffreur IP (OT.VPN.PROTECTION_AUDIT_FLUX).
- offrir un service de supervision du chiffreur IP qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.VPN.IMPACT_SUPERVISION).
- garantir que seuls les administrateurs locaux authentifiés ont accès aux traces des flux du chiffreur IP (OT.AUTHENTIFICATION_ADMIN). La TOE doit

protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN), et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- permettre de filtrer les flux d'administration du chiffreur IP (OT.FW.APPLICATION_POL_FILTRAGE).

Pour détecter l'occurrence de la menace, la TOE doit :

- permettre de détecter la perte de traces d'audits du chiffreur IP (OT.VPN.PROTECTION_AUDIT_FLUX).

Pour limiter l'impact de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).
- s'appuyer sur des mesures de sauvegarde et d'archivage des traces d'audit (OE.VPN.ANALYSE_AUDIT).

8.1.2.5 Couverture des menaces portant sur les traces d'audit d'administration

Pare-feu

T.FW.MODIFICATION_AUDIT_ADMIN

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- permettre de filtrer les flux d'administration du pare-feu (OT.FW.APPLICATION_POL_FILTRAGE).
- offrir un contrôle d'accès aux journaux d'audit des flux traités par le pare-feu (OT.FW.PROTECTION_AUDIT_ADMIN).
- offrir un service de supervision du pare-feu qui ne remet pas en cause ses biens sensibles en les modifiant pas et en ne les divulguant pas (OT.FW.IMPACT_SUPERVISION).
- garantir que seuls les administrateurs locaux authentifiés ont accès aux clés cryptographiques (OT.AUTHENTIFICATION_ADMIN). La TOE doit protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN), et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurrence de la menace, la TOE doit :

- permettre de détecter la perte de traces d'audits du pare-feu (OT.FW.PROTECTION_AUDIT_ADMIN).

Pour limiter l'impact de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du pare-feu (OT.FW.AUDIT_ADMIN, OT.FW.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.FW.TRAITE_ALARMES).

- s'appuyer sur des mesures de sauvegarde et d'archivage des traces d'audit (OE.FW.ANALYSE_AUDIT).

Chiffreur IP

T.VPN.MODIFICATION_AUDIT_ADMIN

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- offrir un contrôle d'accès aux journaux d'audit des flux traités par le chiffreur IP (OT.VPN.PROTECTION_AUDIT_ADMIN).
- offrir un service de supervision du chiffreur IP qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.FW.IMPACT_SUPERVISION).
- garantir que seuls les administrateurs locaux authentifiés ont accès aux clés cryptographiques (OT.AUTHENTIFICATION_ADMIN). La TOE doit protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN), et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- permettre de filtrer les flux d'administration du chiffreur IP (OT.FW.APPLICATION_POL_FILTRAGE).

Pour détecter l'occurrence de la menace, la TOE doit :

- permettre de détecter la perte de traces d'audits du chiffreur IP (OT.VPN.PROTECTION_AUDIT_ADMIN).

Pour limiter l'impact de la menace, la TOE doit :

- générer des traces d'audit et des alarmes du chiffreur IP (OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).
- s'appuyer sur des mesures de sauvegarde et d'archivage des traces d'audit (OE.VPN.ANALYSE_AUDIT).

8.1.2.6 Couverture des menaces portant sur les alarmes

Pare-feu

T.FW.MODIFICATION_ALARMES

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- permettre de filtrer les flux d'administration du pare-feu (OT.FW.APPLICATION_POL_FILTRAGE).

- offrir un service de supervision du pare-feu qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.FW.IMPACT_SUPERVISION).
- garantir que seuls les administrateurs locaux authentifiés ont accès aux clés cryptographiques (OT.AUTHENTIFICATION_ADMIN). La TOE doit protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN), et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurrence de la menace, la TOE doit :

- permettre de détecter la perte d'alarmes du pare-feu (OT.FW.PROTECTION_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- générer des traces d'audit du pare-feu (OT.FW.AUDIT_ADMIN).. L'administrateur de sécurité doit les analyser et les traiter (OE.FW.TRAITE_ALARMES).

Chiffreur IP

T.VPN.MODIFICATION_ALARMES

Pour prévenir la menace, la TOE doit :

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL).
- être utilisée par des administrateurs de confiance (OE.ADMIN).

Pour se protéger, la TOE doit :

- offrir un contrôle d'accès aux journaux d'audit des flux traités par le chiffreur IP (OT.VPN.PROTECTION_ALARMES).
- offrir un service de supervision du chiffreur IP qui ne remet pas en cause ses biens sensibles en ne les modifiant pas et en ne les divulguant pas (OT.FW.IMPACT_SUPERVISION).
- garantir que seuls les administrateurs locaux authentifiés ont accès aux clés cryptographiques (OT.AUTHENTIFICATION_ADMIN). La TOE doit protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN), et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT).
- permettre de filtrer les flux d'administration du chiffreur IP (OT.FW.APPLICATION_POL_FILTRAGE).

Pour détecter l'occurrence de la menace, la TOE doit :

- permettre de détecter la perte de traces d'audits du chiffreur IP (OT.VPN.PROTECTION_ALARMES).

Pour limiter l'impact de la menace, la TOE doit :

- générer des traces d'audit du chiffreur IP (OT.VPN.AUDIT_ADMIN).. L'administrateur de sécurité doit les analyser et les traiter (OE.VPN.TRAITE_ALARMES).

8.1.2.7 Couverture des menaces portant sur l'administration

T.USURPATION_ADMIN

Pour prévenir la menace, la TOE doit :

- aucune action

Pour se protéger, la TOE doit :

- imposer l'authentification locale (OT.AUTHENTIFICATION_ADMIN) ou à distance (OE.AUTHENTIFICATION_ADMIN_DISTANT) des différents administrateurs avant d'effectuer toute opération d'administration.
- protéger les flux d'administration distante (OT.PROTECTION_FLUX_ADMIN).

Pour détecter l'occurrence de la menace, la TOE doit :

- OT.FW.AUDIT_ADMIN et OT.FW.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles du pare-feu sont tracées et que les 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 évènements d'audit et des alarmes de sécurité.
- OT.VPN.AUDIT_ADMIN, OT.VPN.ALARMES, assurent que les opérations (consultation, modification) effectuées sur les biens sensibles du chiffreur IP sont tracées et que les 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 évènements d'audit et des alarmes de sécurité.

Pour limiter l'impact de la menace, la TOE doit :

- aucune action

8.1.2.8 Couverture des menaces portant sur les changement de contexte de la TOE

Pare-feu

T.FW.CHANGEMENT_CONTEXTE

Pour prévenir la menace, la TOE doit :

- fournir une fonctionnalité qui permet de rendre indisponibles les biens sensibles du pare-feu préalablement à un changement de contexte d'utilisation : nouvelle affectation, maintenance, … (OT.FW.CHANGEMENT_CONTEXTE).

Pour se protéger, la TOE doit :

- aucune action

Pour détecter l'occurrence de la menace, la TOE doit :

- aucune action

Pour limiter l'impact de la menace, la TOE doit :

- aucune action

Chiffreur IP

T.VPN.CHANGEMENT_CONTEXTE
Pour prévenir la menace, la TOE doit :

- fournir une fonctionnalité qui permet de rendre indisponibles les biens sensibles du chiffreur IP préalablement à un changement de contexte d'utilisation : nouvelle affectation, maintenance, … (OT.VPN.CHANGEMENT_CONTEXTE).

Pour se protéger, la TOE doit :

- aucune action

Pour détecter l'occurrence de la menace, la TOE doit :

- aucune action

Pour limiter l'impact de la menace, la TOE doit :

- aucune action

T.DYSFONCTIONNEMENT
Pour prévenir la menace, la TOE doit :

- aucune action

Pour se protéger, la TOE doit :

- aucune action

Pour détecter l'occurrence de la menace, la TOE doit :

- offrir un service de supervision de la TOE (OT.FW.SUPERVISION et OT.VPN.SUPERVISION) tout en ne dévoilant pas ses éléments sensibles (OT.FW.IMPACT_SUPERVISION et OT.VPN.IMPACT_SUPERVISION)

Pour limiter l'impact de la menace, la TOE doit :

- pouvoir être remise dans un état précédemment validé (OE.FW.INTEGRITE et OE.VPN.INTEGRITE).

8.1.3 Politiques de sécurité de l'organisation

OSP.QUALIF
Pour mettre en œuvre la politique, la TOE :

- s'appuie sur le processus de qualification standard de la DCSSI (OT.QUALIF)

Pour garantir la mise en œuvre de la politique, la TOE :

- aucune action

Pour contrôler la mise en œuvre de la politique, la TOE :

- aucune action

OSP.CRYPTO
Pour mettre en œuvre la politique, la TOE :

- implémente les fonctions de cryptographie et gérer (générer, détruire, renouveler) les clés cryptographiques en accord avec le référentiel de cryptographie défini par la DCSSI dans les documents [CRYPTO] et [GC] pour le niveau de résistance standard (OT.CRYPTO)

- utilise des clés cryptographiques (générées à l'extérieur), générées et gérées en suivant les recommandations spécifiées dans les référentiels de cryptographie de la DCSSI [CRYPTO] et [GC] pour le niveau de résistance standard (OE.VPN.CRYPTO_EXT)
- s'appuie sur les référentiels de cryptographie de la DCSSI (OE.CRYPTO)

Pour garantir la mise en œuvre de la politique, la TOE :

- aucune action

Pour contrôler la mise en œuvre de la politique, la TOE :

- aucune action

OSP.GESTION_ROLES

Pour mettre en œuvre la politique, la TOE :

- définit des rôles aux administrateurs de la TOE, chaque rôle disposant de droits d'accès spécifiques (OT.GESTION_ROLES).
- authentifier localement l'administrateur de la TOE (OT.AUTHENTIFICATION_ADMIN). L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT).

Pour garantir la mise en œuvre de la politique, la TOE :

- aucune action

Pour contrôler la mise en œuvre de la politique, la TOE :

- enregistre les opérations effectuées par les administrateurs sur la TOE (OT.VPN.AUDIT_ADMIN et OT.FW.AUDIT_ADMIN)

Pare-feu

OSP.FW.SERVICE

Pour mettre en œuvre la politique, la TOE :

- applique la politique de filtrage du pare-feu définie par l'administrateur de sécurité (OT.FW.APPLICATION_POL_FILTRAGE).

Pour garantir la mise en œuvre de la politique, la TOE :

- garantit la cohérence entre la définition des politiques de filtrage et les politiques appliquées sur le pare-feu (OT.FW .COHERENCE_POL)
- garantit que l'intégrité du code des logiciels qui appliquent les politiques de filtrage peut être vérifiée (OE.FW.INTEGRITE)

Pour contrôler la mise en œuvre de la politique, la TOE doit :

- permet à l'administrateur de sécurité de la TOE de visualiser la politique de filtrage du pare-feu (OT.FW .VISUALISATION_POL)

OSP.FW.VISUALISATION_POL

Pour mettre en œuvre la politique, la TOE :

- permet de visualiser les règles de filtrage courantes sur le pare-feu (OT.FW.VISUALISATION_POL)

Pour garantir la mise en œuvre de la politique, la TOE :

- aucune action

Pour contrôler la mise en œuvre de la politique, la TOE :

- aucune action

OSP.FW.AUDIT_FLUX

Pour mettre en œuvre la politique, la TOE :

- trace les flux traités par le pare-feu dans des journaux d'audit permettant aux administrateurs de les visualiser, de les ordonner, … (OT.FW.AUDIT_FLUX)

Pour garantir la mise en œuvre de la politique, la TOE :

- aucune action

Pour contrôler la mise en œuvre de la politique, la TOE :

- aucune action

Chiffreur IP

OSP.VPN.SERVICE

Pour mettre en œuvre la politique, la TOE :

- applique une politique de protection des flux (OT.VPN.APPLICATION_POL) en protégeant en confidentialité et en authenticité les données applicatives (OT.VPN.CONFIDENTIALITE_APPLI, OT.VPN.AUTHENTICITE_APPLI) et topologiques (OT.VPN.CONFIDENTIALITE_TOPO, OT.VPN.AUTHENTICITE_TOPO).
- assure le cloisonnement des flux (OT.VPN.CLOISONNEMENT_FLUX)

Pour garantir la mise en œuvre de la politique, la TOE :

- garantit que l'intégrité du code des logiciels qui appliquent les politiques de sécurité VPN peut être vérifiée (OE.VPN.INTEGRITE)

Pour contrôler la mise en œuvre de la politique, la TOE :

- assure que les opérations concernant les liens VPN sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements (OT.VPN.AUDIT_FLUX, OT.VPN.ALARMES). L'environnement de la TOE assure que les alarmes émises sont traitées par les administrateurs de sécurité (OE.VPN.TRAITE_ALARMES).

OSP.VPN.VISUALISATION_POL

Pour mettre en œuvre la politique, la TOE :

- permet la visualisation unitaire des politiques de sécurité VPN, ce qui permet à un administrateur de vérifier visuellement qu'il a définit correctement chaque politique de sécurité VPN (OT.VPN.VISUALISATION_POL).

Pour garantir la mise en œuvre de la politique, la TOE :

- aucune action

Pour contrôler la mise en œuvre de la politique, la TOE :

- aucune action

OSP.VPN.SUPERVISION

Pour mettre en œuvre la politique, la TOE :

- permet à l'administrateur système et réseau de consulter l'état opérationnel du chiffreur IP (OT.VPN.SUPERVISION).

Pour garantir la mise en œuvre de la politique, la TOE :

- aucune action

Pour contrôler la mise en œuvre de la politique, la TOE :

- aucune action

8.2 Argumentaire des exigences de sécurité

8.2.1 Objectifs de sécurité pour le pare-feu de la TOE

Tableau 2 : Couverture des objectifs sur le pare-feu de la TOE

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

8.2.2 Objectifs de sécurité pour le chiffreur IP de la TOE

Tableau 3 : Couverture des objectifs de sécurité sur le chiffreur IP de la TOE

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

8.2.3 Objectifs de sécurité pour l'administration de la TOE

Tableau 4 : Couverture des objectifs de sécurité sur l'administration de la TOE

Objectifs de sécurité pour l'administration de la TOE	FPT_STM.1	FPT_ITT.1-Administration_distante	FPT_ITT.3-Administration_distante	FIA_UAU.2-Station_administration_distante	FMT_SMR.1	FIA_UID.2-Administrateurs	FIA_UAU.2-Administrateurs_local
OT.GESTION_ROLES				X	X	X	X
OT.PROTECTION_FLUX_ADMIN		X	X				
OT.AUTHENTIFICATION_ADMIN					X	X	X

8.2.4 Objectifs de sécurité pour l'environnement technique de la TOE

Tableau 5 : Couverture des objectifs de sécurité pour l'environnement TI de la TOE

Objectifs de sécurité pour l'environnement TI de la TOE	FIA_UAU.2-Administration_distante
OE.AUTHENTIFICATION_ADMIN_DISTANT	X

8.2.5 Argumentaire de la couverture des exigences de sécurité fonctionnelles pour la TOE

8.2.5.1 Administration de la TOE

OT.GESTION_ROLES

L'objectif se traduit par l'exigence FMT_SMR.1 qui demande à ce que la TOE gère les différents rôles (administrateurs). Pour pourvoir gérer ces rôles, les administrateurs doivent impérativement être identifiés (FIA_UID.2-Administrateurs). L'authentification locale des administrateurs est couverte par FIA_UAU.2-Administrateurs_local;

l'authentification pour l'administration distante relève de FIA_UAU.2-Station_administration_distante.

OT.PROTECTION_FLUX_ADMIN

Cet objectif est traduit par les exigences FPT_ITT.1-Administration_distante et FPT_ITT.3-Administration_distante sur la protection des données transmises entre le firewall et la station d'administration distante.

OT.AUTHENTIFICATION_ADMIN

Cet objectif est couvert par FIA_UID.2-Administrateurs et FIA_UAU.2-Administrateurs_local 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.

8.2.5.2 Pare-feu de la TOE

OT.FW.APPLICATION_POL_FILTRAGE

Cet objectif se traduit par les exigences FDP_IFF.1/FW-Enforcement_policy qui permet de définir les règles minimales que doit respecter la politique de filtrage et FDP_IFC.2/FW-Enforcement_policy qui demande à ce que la TOE applique cette politique de filtrage.

OT.FW.COHERENCE_POL

Cet objectif se traduit par FPT_TDC.1/FW-Administration_distante pour assurer la cohérence entre la politique de filtrage définie sur la station d'administration distante et le firewall.

OT.FW.PROTECTION_POL_FILTRAGE

Cet objectif se traduit par les règles d'accès à la politique de filtrage (FDP_ACC.1/FW-Filtering_policy et FDP_ACF.1/FW-Filtering_policy).

OT.FW.VISUALISATION_POL

Cet objectif se traduit par l'exigence FMT_SMF.1/FW-Visualisation_politique_filtrage qui nécessite la possibilité de visualiser les règles de filtrage et les contextes de connexion.

OT.FW.PROTECTION_PARAM

Cet objectif est traduit par les exigences de protection suivantes:

- pour les paramètres de configuration réseau: FMT_MTD.1/FW-Network_param;
- pour les droits d'accès et les données d'authentification: FMT_MTD.1-Param_security_administrator pour les administrateurs de sécurité et FMT_MTD.1-Param_auditor pour les auditeurs;

La fonctionnalité de configuration de ces paramètres est quant à elle couverte par FMT_SMF.1/FW-Configuration.

OT.FW.CHANGEMENT_CONTEXTE

Cet objectif est traduit par les exigences suivantes :

- FDP_RIP.1/FW-Recyclage_TOE qui exige que la TOE permette de rendre indisponible le contenu des ressources correspondant aux biens sensibles de la TOE ;
- FDP_ACC.1/FW-Recyclage_TOE et FDP_ACF.1/FW-Recyclage_TOE qui exigent des règles d'accès à l'opération d'effacement des biens sensibles.

OT.FW.SUPERVISION

Cet objectif est traduit par l'exigence FMT_SMF.1/FW-Supervision qui exige la fourniture d'un service indiquant l'état du firewall.

OT.FW.IMPACT_SUPERVISION

Cet objectif est traduit par l'exigence FPT_ITC.1/FW-Supervision qui exige de protéger les données exportées hors du contrôle du firewall si elles contiennent des informations confidentielles.

OT.FW.AUDIT_FLUX

Cet objectif est traduit par FAU_GEN.1/FW-Audit_flux pour la génération des traces d'évènements sur les flux traités par le firewall, FAU_GEN.2/FW-Audit_flux pour pouvoir imputer les événements à des émetteurs de ces flux. Pour réaliser ce dernier, les flux doivent être impérativement identifiés (FIA_UID.2/FW-Flux). Les dates des événements audités étant enregistrées, la TOE doit de plus disposer d'une horloge fiable (FPT_STM.1). La possibilité de consultation de ces traces d'audit des flux traités par le firewall est traduite par FAU_SAR.1/FW-Audit_flux et FAU_SAR.3/FW-Audit_flux

OT.FW.PROTECTION_AUDIT_FLUX

Cet objectif se traduit par FAU_STG.1/FW-Traces_audit_flux qui exige la protection en intégrité des enregistrements d'événements d'audit.

OT.FW.AUDIT_ADMIN

Cet objectif est traduit par FAU_GEN.1/FW-Audit_admin pour la génération des traces d'évènements sur les évènements d'administration du firewall, FAU_GEN.2/FW-Audit_admin pour pouvoir imputer les événements aux administrateurs. Les administrateurs doivent être impérativement identifiés (FIA_UID.2-Administrateurs). Les dates des événements audités étant enregistrées, la TOE doit de plus disposer d'une horloge fiable (FPT_STM.1). La possibilité de consultation de ces traces d'audit des évenements d'administration du firewall est traduite par FAU_SAR.1/FW-Audit_admin et FAU_SAR.3/FW-Audit_admin.

OT.FW.PROTECTION_AUDIT_ADMIN

Cet objectif se traduit par FAU_STG.1/FW-Traces_audit_admin qui protège en intégrité les enregistrements d'événements d'administration.

OT.FW.ALARMES

Cet objectif se traduit par FAU_ARP.1/FW-Alarmes qui exige de lever une alarme de sécurité quand une violation potentielle de la sécurité est détectée et par FAU_SAA.1/FW-Alarmes qui indique les règles utilisées pour détecter ces violations potentielles.

OT.FW.PROTECTION_ALARMES

Cet objectif se traduit par FAU_STG.1/FW-Traces_audit_admin et FAU_STG.1/FW-Traces_audit_flux qui protègent en intégrité les enregistrements d'événements.

8.2.5.3 Chiffreur IP de la TOE

OT.VPN.APPLICATION_POL
Cet objectif est couvert par la politique d'application VPN (FDP_IFC.1/VPN-Enforcement_policy, FDP_IFF.1/VPN-Enforcement_policy , FDP_ITC.1/VPN-Enforcement_policy et FDP_ETC.1/VPN-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/VPN-Enforcement_policy.

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

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

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

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

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

OT.VPN.DEFINITION_POL
Cet objectif est couvert par la politique de protection des politiques de sécurité VPN (FDP_ACC.1/VPN-VPN_policy, FDP_ACF.1/VPN-VPN_policy, FDP_ITC.1/VPN-VPN_policy, FMT_MSA.3/VPN-VPN_policy, FMT_MSA.1/VPN-VPN_policy et FMT_SMF.1/VPN-VPN_policy) qui contrôle l'accès à la définition des politiques de sécurité VPN.

OT.VPN.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-VPN_policy, FDP_ACF.1/VPN-VPN_policy, FMT_MSA.3/VPN-VPN_policy, FMT_MSA.1/VPN-VPN_policy et FMT_SMF.1/VPN-VPN_policy.

OT.VPN.VISUALISATION_POL

Cet objectif est couvert par la politique de protection des politiques de sécurité VPN (FDP_ACC.1/VPN-VPN_policy et FDP_ACF.1/VPN-VPN_policy) en contrôlant l'accès à l'opération de visualisation des politiques de sécurité VPN et de leurs contextes.

OT.CRYPTO

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

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

OT.VPN.ACCES_CLES

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

OT.VPN. INJECTION_CLES

Cet objectif est couvert par la politique des clés (FDP_IFC.1/VPN-Key_policy, FDP_IFF.1/VPN-Key_policy et FMT_MSA.3/VPN-Key_policy) qui contrôle les flux de clés dont l'injection de clés (FDP_ITC.1/VPN-Key_policy).

OT.VPN.PROTECTION_PARAM

Cet objectif est couvert par FMT_MTD.1/VPN-Network_param (pour les paramètres de configuration réseau), FMT_MTD.1/Param_security_administrator (pour les droits d'accès et les données d'authentification), et FMT_SMF.1/VPN-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.

OT.VPN.CHANGEMENT_CONTEXTE

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

OT.VPN.SUPERVISION

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

OT.VPN.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-VPN_policy, FDP_ACF.1/VPN-VPN_policy, FDP_IFC.1/VPN-Key_policy, FDP_IFF.1/VPN-Key_policy, FDP_IFC.1/VPN-Enforcement_policy et FDP_IFF.1/VPN-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/VPN-Network_param et FMT_MTD.1/Param_security_administrator.

OT.VPN.AUDIT_FLUX

Cet objectif est couvert par FAU_GEN.1/VPN-Audit_flux qui assure la génération d'événement d'audit pour les liens de communication VPN et par FPT_STM.1 qui assure que la date associée à chaque événement d'audit est fiable. De plus, cet objectif est aussi couvert par FAU_SAR.1/VPN-Audit_flux et FAU_SAR.3/VPN-Audit_flux qui fournissent la consultation des événements d'audit.

OT.VPN.PROTECTION_AUDIT_FLUX

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

OT.VPN.AUDIT_ADMIN

Cet objectif est couvert par FAU_GEN.1/VPN-Audit_admin qui assure la génération d'événement d'audit concernant les opérations d'administration et par FPT_STM.1 qui assure que la date associée à chaque événement d'audit est fiable. De plus, cet objectif est aussi couvert par FAU_SAR.1/VPN-Audit_admin et FAU_SAR.3/VPN-Audit_admin qui fournissent la consultation des événements d'audit.

OT.VPN.PROTECTION_AUDIT_ADMIN

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

OT.VPN.ALARMES

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

OT.VPN.PROTECTION_ALARMES

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

8.2.6 Argumentaire de la couverture des exigences de sécurité fonctionnelles pour l'environnement technique de la TOE

OE.AUTHENTIFICATION_ADMIN_DISTANT

L'objectif est traduit directement par l'exigence d'authentification des administrateurs sur la station d'administration distante: FIA_UAU.2-Administration_distante.

8.2.7 Satisfaction de dépendances

Tableau 6 : Dépendances des exigences de sécurité fonctionelles de sécurité pour la TOE

Exigences	Dépendances CC	Dépendances ST	Réalisation
Classe FAU : Security Audit			
FAU_ARP.1/FW-Alarmes	FAU_SAA.1	FAU_SAA.1/FW-Alarmes	ok
FAU_ARP.1/VPN-Alarmes	FAU_SAA.1	FAU_SAA.1/VPN-Alarmes	ok
FAU_GEN.1/FW-Audit_flux	FPT_STM.1	FPT_STM.1	ok
FAU_GEN.1/FW-Audit_admin	FPT_STM.1	FPT_STM.1	ok
FAU_GEN.1/VPN-Audit_flux	FPT_STM.1	FPT_STM.1	ok
FAU_GEN.1/VPN-Audit_admin	FPT_STM.1	FPT_STM.1	ok
FAU_GEN.2/FW-Audit_flux	FAU_GEN.1	FAU_GEN.1/FW-Audit_flux	ok
	FIA_UID.1	FIA_UID.2/FW-Flux	ok
FAU_GEN.2/FW-Audit_admin	FAU_GEN.1	FAU_GEN.1/FW-Audit_admin	ok
	FIA_UID.1	FIA_UID.2-Administrateurs	ok
FAU_SAA.1/VPN-Alarmes	FAU_GEN.1	FAU_GEN.1/VPN-Audit_flux	ok
		FAU_GEN.1/VPN-Audit_admin	ok
FAU_SAA.1/FW-Alarmes	FAU_GEN.1	FAU_GEN.1/FW-Audit_flux	ok
		FAU_GEN.1/FW-Audit_admin	ok
FAU_SAR.1/FW-Audit_flux	FAU_GEN.1	FAU_GEN.1/FW-Audit_flux	ok
FAU_SAR.1/VPN-Audit_flux	FAU_GEN.1	FAU_GEN.1/VPN-Audit_flux	ok
FAU_SAR.1/FW-Audit_admin	FAU_GEN.1	FAU_GEN.1/FW-Audit_admin	ok
FAU_SAR.1/VPN-Audit_admin	FAU_GEN.1	FAU_GEN.1/FW-Audit_admin	ok
FAU_SAR.3/FW-Audit_flux	FAU_SAR.1	FAU_SAR.1/FW-Audit_flux	ok

FAU_SAR.3/FW-Audit_admin	FAU_SAR.1	FAU_SAR.1/FW-Audit_admin	ok
FAU_SAR.3/VPN-Audit_admin	FAU_SAR.1	FAU_SAR.1/VPN-Audit_admin	ok
FAU_SAR.3/VPN-Audit_flux	FAU_SAR.1	FAU_SAR.1/VPN-Audit_flux	ok
FAU_STG.1/FW-Traces_audit_flux	FAU_GEN.1	FAU_GEN.1/FW-Audit_flux	ok
FAU_STG.1/VPN-Traces_audit_flux	FAU_GEN.1	FAU_GEN.1/VPN-Audit_flux	ok
FAU_STG.1/VPN-Traces_audit_admin	FAU_GEN.1	FAU_GEN.1/VPN-Audit_admin	ok
FAU_STG.1/FW-Traces_audit_admin	FAU_GEN.1	FAU_GEN.1/FW-Audit_admin	ok
Classe FCS : Cryptographic Support			
FCS_CKM.1/ VPN-Key_policy	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/VPN-Key_policy	Ok
	FCS_CKM.4	FCS_CKM.4/VPN-Key_policy	Ok
	FMT_MSA.2	NON REALISE	NON REALISE
FCS_CKM.4/VPN-Key_policy	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/VPN-Key_policy	ok
	FMT_MSA.2	NON REALISE	NON REALISE
FCS_COP.1/VPN-Enforcement_policy	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1/VPN-Key_policy	ok
	FCS_CKM.4	FCS_CKM.4/VPN-Key_policy	ok
	FMT_MSA.2	NON REALISE	NON REALISE
Classe FDP : User Data Protection			
FDP_ACC.1/FW-Filtering_policy	FDP_ACF.1	FDP_ACF.1/FW-Filtering_policy	ok
FDP_ACC.1/FW-Recyclage_TOE	FDP_ACF.1	FDP_ACF.1/FW-Recyclage_TOE	ok
FDP_ACC.1/VPN-VPN_policy	FDP_ACF.1	FDP_ACF.1/VPN-	ok

		VPN_policy	
FDP_ACF.1/FW-Filtering_policy	FDP_ACC.1	FDP_ACC.1/FW-Filtering_policy	ok
	FMT_MSA.3	NON REALISE	NON REALISE
FDP_ACF.1/FW-Recyclage_TOE	FDP_ACC.1	FDP_ACC.1/FW-Recyclage_TOE	ok
	FMT_MSA.3	NON REALISE	NON REALISE
FDP_ACF.1/VPN-VPN_policy	FDP_ACC.1	FDP_ACC.1/VPN-VPN_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-VPN_policy	ok
FDP_ETC.1/VPN-Enforcement_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/VPN-Enforcement_policy	ok
FDP_IFC.1/VPN-Enforcement_policy	FDP_IFF.1	FDP_IFF.1/VPN-Enforcement_policy	ok
FDP_IFC.1/VPN-Key_policy	FDP_IFF.1	FDP_IFF.1/VPN-Key_policy	ok
FDP_IFC.2/FW-Enforcement_policy	FDP_IFF.1	FDP_IFF.1/FW-Enforcement_policy	ok
FDP_IFF.1/FW-Enforcement_policy	FDP_IFC.1	FDP_IFC.2/FW-Enforcement_policy	ok
	FMT_MSA.3	NON REALISE	NON REALISE
FDP_IFF.1/VPN-Enforcement_policy	FDP_IFC.1	FDP_IFC.1/VPN-Enforcement_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-VPN_policy	ok
FDP_IFF.1/VPN-Key_policy	FDP_IFC.1	FDP_IFC.1/VPN-Key_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-Key_policy	ok
FDP_ITC.1/VPN-Enforcement_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/VPN-Enforcement_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-VPN_policy	ok
FDP_ITC.1/VPN-VPN_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/VPN-Enforcement_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-	ok

		VPN_policy	
FDP_ITC.1/VPN-Key_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/VPN-Key_policy	ok
	FMT_MSA.3	FMT_MSA.3/VPN-Key_policy	ok
FDP_RIP.1/FW-Recyclage_TOE	-	-	ok
FDP_RIP.1/VPN	-	-	ok
Classe FIA : Identification and Authentication			
FIA_UAU.2-Station_administration_distante	FIA_UID.1	FIA_UID.2/FW-Flux	ok
FIA_UAU.2-Administrateurs_local	FIA_UID.1	FIA_UAU.2-Administrateurs_local	ok
FIA_UID.2-Administrateurs	-	-	ok
FIA_UID.2/FW-Flux	-	-	ok
Classe FMT : Security Management			
FMT_MSA.1/VPN-VPN_policy	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/VPN-VPN_policy	ok
	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/VPN-VPN_policy	ok
FMT_MSA.3/VPN-Key_policy	FMT_MSA.1	NON REALISE	NON REALISE
	FMT_SMR.1	FMT_SMR.1	ok
FMT_MSA.3/VPN-VPN_policy	FMT_MSA.1	FMT_MSA.1/VPN-VPN_policy	ok
	FMT_SMR.1	FMT_SMR.1	ok
FMT_MTD.1/FW-Network_param	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/FW-Configuration	ok
FMT_MTD.1-Param_security_administrator	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/FW-Configuration	ok
FMT_MTD.1-Param_auditor	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/FW-Configuration	ok
FMT_MTD.1/VPN-Network_param	FMT_SMR.1	FMT_SMR.1	ok
	FMT_SMF.1	FMT_SMF.1/VPN-	ok

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

8.2.7.1 Argumentaire des dépendances non satisfaites

La dépendance FMT_MSA.3 de FDP_ACF.1/FW-Filtering_policy n'est pas réalisée. Cette dépendance n'est pas réalisée dans le Profil de Protection [PP_FWIP] avec l'argumentaire suivant : Le profil de protection n'impose pas que la TOE prédéfinisse des valeurs par défaut des attributs de sécurité pour le contrôle d'accès à la politique de filtrage.

La dépendance de FMT_MSA.3 de FDP_ACF.1/FW-Recyclage_TOE n'est pas réalisée. Cette dépendance n'est pas réalisée dans le Profil de Protection [PP_FWIP] avec l'argumentaire suivant : Le profil de protection n'impose pas que la TOE prédéfinisse des valeurs par défaut des attributs de sécurité pour le contrôle d'accès aux biens sensibles.

La dépendance de FMT_MSA.3 de FDP_IFF.1/FW-Enforcement_policy n'est pas réalisée. Cette dépendance n'est pas réalisée dans le Profil de Protection [PP_FWIP] avec l'argumentaire suivant : Dans le cadre de ce profil de protection, il n'est pas imposé de valeurs restrictives pour les attributs sur lesquels s'appuie la politique de filtrage. Il n'est pas en revanche exclu qu'un produit le fasse.

La dépendance de FMT_MSA.2 de FCS_COP.1/VPN-Enforcement_policy n'est pas réalisée. Cette dépendance n'est pas réalisée dans le Profil de Protection [PP_CIP] avec l'argumentaire suivant : Comme il n'y a pas d'attribut de sécurité utilisé dans les opérations

cryptographiques qui permettent d'appliquer les politiques de sécurité VPN, cette dépendance n'est pas satisfaite.

La dépendance de FMT_MSA.1 FMT_MSA.3/VPN-Key_policy n'est pas réalisée. Cette dépendance n'est pas réalisée dans le Profil de Protection [PP_CIP] avec l'argumentaire suivant : 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 de FMT_MSA.2 de FCS_CKM.4/VPN-Key_policy n'est pas réalisée. Cette dépendance n'est pas réalisée dans le Profil de Protection [PP_CIP] avec l'argumentaire suivant : Comme il n'y a pas d'attribut de sécurité utilisé pour détruire les clés cryptographiques concernées par cette exigence, cette dépendance n'est pas satisfaite. La non réalisation de la dépendance de FMT_MSA.2 de FCS_CKM.1/VPN-Key_policy n'est pas réalisée pour les mêmes raisons.

8.3 Argumentaire des spécifications

8.3.1 Couverture des exigences fonctionnelles

Tableau 7 : Couverture des exigences fonctionnelles de sécurité pour la TOE

Fonctions de la TOE	Exigences de sécurité fonctionnelles pour la TOE									
	F.RELIABLE_TIME	F.AUDIT	F.USER_DATA_PROTECTION_FW	F.USER_DATA_PROTECTION_VPN	F.ROLES	F.ADMINISTRATION	F.REINIT	F.LOCAL_ADMIN_IDENTIFICATION_AUTHENTICATION	F.REMOTE_STATION_AUTHENTICATION	F.REMOTE_ADMIN_PROTECTION
FPT_STM.1	X									
FPT_ITT.1-Administration_distante										X
FPT_ITT.3-Administration_distante										X
FIA_UAU.2-Station_administration_distante									X	
FMT_SMR.1					X					
FIA_UID.2-Administrateurs								X		
FIA_UAU.2-Administrateurs_local								X		
FDP_IFC.2/FW-Enforcement_policy			X							
FDP_IFF.1/FW-Enforcement_policy			X							
FMT_SMF.1/FW-Visualisation_politique_filtrage						X				
FPT_TDC.1/FW-Administration_distante			X							

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

FTA_TSE.1/VPN-Key_policy				X						
FCS_CKM.4/VPN-Key_policy							X			
FCS_CKM.1/VPN-Key_policy				X						

9 Annexes

9.1 Annexe 1 : Traces d'audits minimales et niveau associé

Exigence de sécurité fonctionnelle	Préconisation CC partie 2	Niveau retenu
FAU_ARP.1/FW-Alarmes	a) Minimal: Actions taken due to imminent security violations.	Minimal
FAU_ARP.1/VPNarmes	a) Minimal: Actions taken due to imminent Security violations.	Minimal
FAU_GEN.1/FW-Audit_flux	N/A	N/A
FAU_GEN.1/FW-Audit_admin	N/A	N/A
FAU_GEN.1/VPN-Audit_flux	N/A	N/A
FAU_GEN.1/VPN-Audit_admin	N/A	N/A
FAU_GEN.2/FW-Audit_flux	N/A	N/A
FAU_GEN.2/FW-Audit_admin	N/A	N/A
FAU_SAA.1/VPN-Alarmes	a) Minimal: Enabling and disabling of any of the analysis mechanisms; b) Minimal: Automated Responses performed by the tool.	Minimal
FAU_SAA.1/FW-Alarmes	a) Minimal: Enabling and disabling of any of the analysis mechanisms; b) Minimal: Automated Responses performed by the tool.	Minimal
FAU_SAR.1/FW-Audit_flux	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.1/VPN-Audit_flux	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.1/FW-Audit_admin	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.1/VPN-Audit_admin	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.3**/**FW-Audit_flux	a) Detailed: the parameters used for the viewing.	-
FAU_SAR.3/FW-Audit_admin	a) Detailed: the parameters used for the viewing.	-
FAU_SAR.3/VPN-Audit_admin	a) Detailed: the parameters used for the	-

	viewing.	
FAU_SAR.3/VPN-Audit_flux	a) Detailed: the parameters used for the viewing.	-
FAU_STG.1/FW-Traces_audit_flux	N/A	N/A
FAU_STG.1/VPN-Traces_audit_flux	N/A	N/A
FAU_STG.1/FW-Traces_audit_admin	N/A	N/A
FAU_STG.1/VPN-Traces_audit_admin	N/A	N/A
FCS_CKM.4/VPN-Key_policy	a) Minimal: Success and failure of the activity. b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	Basic
FCS_COP.1/VPN-Enforcement_policy	a) Minimal: Success and failure, and the type of cryptographic operation. b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	Basic
FDP_ACC.1/FW-Filtering_policy	N/A	N/A
FDP_ACC.1/FW-Recyclage_TOE	N/A	N/A
FDP_ACC.1VPN-VPN_policy	N/A	N/A
FDP_ACF.1/FW-Filtering_policy	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by The SFP. c) Detailed: The specific security attributes used in making an access check.	Basic
FDP_ACF.1/FW-Recyclage_TOE	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Basic
FDP_ACF.1/VPN-VPN_policy	a) Minimal: Successful requests to perform an	Basic

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

	permit requested information flows. b) Basic: All decisions on requests for information flow. c) Detailed: The specific security attributes used in making an information flow enforcement decision. d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	
FPT_ITC.1/VPN-Enforcement_policy	N/A	N/A
FPT_ITC.1/VPN-VPN_policy	N/A	N/A
FPT_ITC.1/VPN-Key_policy	N/A	N/A
FDP_RIP.1/FW-Recyclage_TOE	N/A	N/A
FDP_RIP.1/VPN	N/A	N/A
FIA_UAU.2-Station_administration_distante	a) Minimal:Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	Basic
FIA_UAU.2-Administrateurs_local	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	Basic
FIA_UID.2-Administrateurs	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Basic
FIA_UID.2/FW-Flux	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification	Basic

	mechanism, including the user identity provided.	
FMT_MSA.1/VPN-VPN_policy	a) Basic: All modifications of the values of security attributes.	Basic
FMT_MSA.3/VPN-Key_policy	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.	Basic
FMT_MSA.3/VPN-VPN_policy	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.	Basic
FMT_MTD.1/FW-Network_param	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1-Param_security_administrator	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1-Param_auditor	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1/VPN-Network_param	a) Basic: All modifications to the values of TSF data.	Basic
FMT_SMF.1/FW-Supervision	a) Minimal: Use of the Management functions.	Minimal
FMT_SMF.1**/**VPN-Config_supervision	a) Minimal: Use of the management functions.	Minimal
FMT_SMF.1**/**VPN-VPN_policy	a) Minimal: Use of the management functions.	Minimal
FMT_SMF.1**/**FW-Visualisation_politique_filtrage	a) Minimal: Use of the management functions.	Minimal
FMT_SMF.1/FW-Configuration	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	Minimal
FMT_SMR.1	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	Minimal
FPT_ITC.1/FW-Supervision	N/A	N/A
FPT_ITT.1-Administration_distante	N/A	N/A

FPT_ITT.3-Administration_distante	a) Minimal: the detection of modification of TSF data; b) Basic: the action taken following detection of an integrity error.	Basic
FPT_STM.1	a) Minimal: changes to the time; b) Detailed: providing a timestamp.	Minimal
FPT_TDC.1/FW-Administration_distante	a) Minimal: Successful use of TSF data consistency mechanisms. b) Basic: Use of the TSF data consistency mechanisms. Identification of which TSF data have been interpreted. d) Basic: Detection of modified TSF data.	Basic
FTA_TSE/VPN-Keypolicy	a) Minimal: Denial of a session establishment due to the session establishment mechanism. b) Basic: All attempts at establishment of a user session. c) Detailed: Capture of the value of the selected access parameters (e.g. location of access, time of access).	Basic