TheGreenBow VPN Client

Cible de Sécurité
Evaluation Critères Communs
TheGreenBow VPN Certified 2013

WebSite :	http://www.thegreenbow.com
Contact :	support@thegreenbow.com

Table des matières

TABLE DES FIGURES

TABLE DES TABLEAUX

REFERENCES DOCUMENTAIRES

Référence	Titre
[AUTH]	Authentification : Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard. ANSSI
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIMB-2009-07-001 Version 3.1 Release 3, July 2009.
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-2009-07-002 Version 3.1 Release 3, July 2009.
[CC-3]	Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIMB-2009-07-003 Version 3.1 Release 3, July 2009.
[CRYPTO]	RGS V1.0, Annexe B1. Mécanismes de cryptographie : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques
[CRYPTO-G]	RGS V1.0, Annexe B2. Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques
[PP-VPNC]	PP Application VPN cliente, PP-VPNC-CCv3.1 Version 1.3, juin 2008
[QUA-STD]	Processus de qualification d'un produit de sécurité – niveau standard Version 1.1, 18 mars 2008. N°549/SGDN/DCSSI/SDR

ABREVIATIONS

Abréviation	Description
CC	Critères Communs
CDS	Cible De Sécurité (en anglais : ST pour Security Target)
ESP	Encapsulating Security Payload (sécurisation des données échangées)
IKE	Internet Key Exchange (négociation de connexion IPSec)
IP	Internet Protocol
IPSec	Internet Protocol Security
PP	Protection Profile : Profil de Protection (sans autre mention, il s'agira du [PP-VPNC])
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target (i-e : CDS Cible De Sécurité en français)
TI	Technologies de l'Information
TSF	TOE Security Functionality
TOE	Target Of Evaluation : Cible à évaluer
TSF	TOE Security Functionality
VPN	Virtual Private Network : Réseau privé virtuel

1 Introduction (ASE_INT.1)

1.1 Référence de la CDS

1 Le tableau suivant définit complètement la présente Cible De Sécurité (CDS).

Titre	Cible de Sécurité CC / Application VPN cliente : TheGreenBow VPN Client
Référence	CDS-TGB-CC
Version	V1.5
Émetteur	THEGREENBOW
Évaluateur	OPPIDA
Certificateur	ANSSI (FRANCE)

Tableau 1 : Références de la CDS

2 Cette CDS décrit :

- un produit TI à évaluer selon la méthodologie des Critères Communs (TOE) : le type de produit, son utilisation et son environnement d'utilisation, les limites de son périmètre dans le cadre de l'évaluation ;
- les biens à protéger et les menaces que la TOE doit craindre durant son utilisation ;
- les politiques de sécurité organisationnelles et les hypothèses ;
- les objectifs de sécurité pour la TOE et les objectifs de sécurité pour son environnement ;
- les exigences fonctionnelles de sécurité pour la TOE et son environnement TI ;
- les exigences d'assurance de sécurité pour la TOE ;
- les fonctions de sécurité mises en œuvre par la TOE ;
- Les justifications argumentées.

1.2 Référence de la TOE

3 Le tableau suivant définit complètement la cible à évaluer (TOE) couverte par la présente CDS.

Nom de la TOE	Application VPN cliente : TheGreenBow VPN client
Type de produit	Logiciel de communication sécurisée
Référence de la TOE	TheGreenBow VPN Client
Version de la TOE	TheGreenBow VPN Certified 2013, version 5.22.005
Émetteur	THEGREENBOW

Tableau 2 : Références de la TOE

1.3 Type de TOE

4 Le type de TOE considéré est une application logicielle conçue pour des machines nomades ou fixes tournant sur toute plateforme Windows (XP 32bit, 7 32/64bit), afin de servir de client VPN IPSec. La plateforme utilisée pour les tests d'évaluation est décrite en annexe de la présente cible de sécurité.

1.4 Utilisation de la TOE

5 TheGreenBow VPN Client est un logiciel client VPN IPSec conçu pour tout poste de travail sous Windows, nomade ou fixe. Il permet d'établir une connexion et d'assurer la communication avec le système d'information de l'entreprise, de façon sécurisée.

6 TheGreenBow VPN Client est interopérable et compatible avec toutes les passerelles VPN IPSec du marché. Il permet aussi d'établir des tunnels VPN en mode point-à-point entre deux machines équipées du logiciel. TheGreenBow VPN Client implémente les protocoles IPSec et IKE standards.

7 TheGreenBow VPN Client est configurable et permet d'établir des associations de sécurité sur la base de mécanismes d'authentification variés : clé partagée, X-Auth, utilisation de certificats X509, PKCS12 ou PEM pouvant être stockés sur carte à puce, sur token, dans un fichier ou dans le magasin des certificats Windows. Le paramétrage de l'application permet également d'activer le filtrage des flux non IPSec et non IKE au travers d'une fonction de Firewall IP qui ne fait pas partie de la présente CDS.

1.5 Limites de la TOE

8 Dans le cadre de la présente CDS, les protocoles mis en œuvre par la TOE et reconnus conformes pour la qualification standard sont :

- le protocole IKEv1, configuré en mode « main », avec les algorithmes AES-128/192/256, HMAC-SHA2, DH Groupe 14;
- le protocole ESP en mode « tunnel », configuré en mode « Encrypt Then Mac », avec les algorithmes AES-128/192/256 et HMAC-SHA2, avec l'option PFS.

9 Les politiques de sécurité VPN mises en œuvre par la TOE opèrent des clés cryptographiques générées à l'intérieur de la TOE et d'autres qui sont importées, générées à l'extérieur de la TOE. Les clés cryptographiques et les éléments de sécurité générés à l'extérieur de la TOE ne doivent pas être sauvegardés dans la politique de sécurité (fichier de configuration).

10 La TOE génère des événements d'audit sur la machine hôte, mais ne fournit aucune fonction d'exploitation de ces événements d'audit.

1.6 Intégration de la TOE dans son environnement

11 La TOE se situe dans le contexte d'un système (Cf. Figure 1) composé de machines hôtes hébergeant l'application TheGreenBow VPN Client, en interface :

- avec le chiffreur IP du serveur d'accès distant ;

12 La TOE ne comporte pas d'interface d'administration distante (type télégestion) pour la mise à jour des politiques VPN.

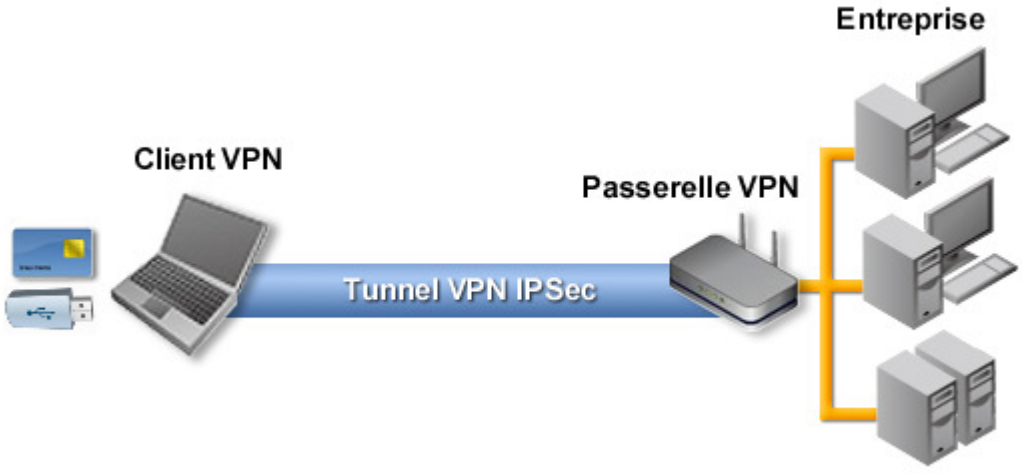


Figure 1 : Environnement d'exploitation de la TOE

13 Afin de s'intégrer et de communiquer avec les différentes entités du système, la TOE dispose de politiques de sécurité VPN et de différents types de clés cryptographiques, en particulier :

- celles permettant la communication sécurisée avec un chiffreur IP (clés utilisées par les services de sécurité et clés de session) ;
- celles permettant la protection de la TOE et de ses fichiers de configuration.

14 Deux phases peuvent être distinguées pour l'intégration de la TOE dans son environnement. D'une part une phase d'initialisation qui consiste à injecter les informations nécessaires à son bon fonctionnement et d'autre part une phase opérationnelle où la TOE est réellement utilisée.

1.6.1 Phase d'initialisation

15 Le logiciel TheGreenBow VPN Client est fourni dans un installeur packagé (setup) qui peut être exécuté par lancement direct, par ligne de commande et/ou de façon silencieuse.

16 Ce package intègre la prise en compte de nombreuses options telles que l'importation de configuration VPN, la définition du mode de démarrage du logiciel (Gina, manuel, automatique) et d'ouverture des tunnels (manuel ou automatique sur détection de trafic), la protection par mot de passe de l'accès à l'interface principale ou plus généralement l'apparence du logiciel sur la station cible.

17 Le déploiement du logiciel est facilité par le fait que la configuration VPN est stockée dans un fichier unique qui peut être joint à l'installeur et ainsi pris en compte automatiquement au cours l'installation.

1.6.2 Phase opérationnelle

18 Le logiciel TheGreenBow VPN Client fonctionne dans les environnements Windows XP 32bit, 7 32/64bit.

19 TheGreenBow VPN Client s'adresse principalement à des utilisateurs nomades ou à des utilisateurs qui travaillent de leur domicile, à distance. Dans le premier cas, le matériel informatique peut être l'objet d'un vol, dans le second, il peut être l'objet de dégradation matérielle ou logicielle.

20 TheGreenBow VPN Client permet d'assurer la sécurité des connexions au réseau privé de l'entreprise, à la fois en terme de confidentialité via le chiffrement des connexions IPSec, ainsi qu'en terme d'authentification via les mécanismes IKE et la possibilité d'utiliser des moyens d'authentification forte tels que les tokens et autres supports de certificats.

21 Le mode nomade qui permet de stocker une configuration protégée par mot de passe sur une clé USB, complète les fonctions de sécurité offertes par le produit.

2 Déclaration de conformité (ASE_CCL.1)

2.1 Déclaration de conformité aux CC

22 Cette CDS est strictement conforme aux CC version V3.1 Révision 3 finale, partie 2 et partie 3.

23 Toutes les exigences fonctionnelles de sécurité (SFR) utilisées dans cette CDS sont strictement issues de la partie 2 des CC version 3.1 Révision 3 finale (référence [CC-2]).

24 Toutes les exigences d'assurance utilisées dans cette CDS sont strictement issues de la partie 3 des CC version 3.1 Révision 3 finale (référence [CC-3]).

2.2 Déclaration de conformité à un Paquet

25 Les exigences d'assurances correspondent à celles requises pour un processus de qualification d'un produit de sécurité au niveau standard (Cf. [QUA-STD]), c'est-à-dire celles du paquet EAL3 du catalogue de référence [CC-3] augmentées des exigences d'assurances ALC_FLR.3 et AVA_VAN.3 (EAL3+).

2.3 Déclaration de conformité au PP 'Application VPN cliente'

26 Cette CDS a une conformité démontrable (Cf. [CC-1]) au profil de protection [PP-VPNC], ci après désigné par « le PP ».

2.4 Justification de conformité au PP

27 Le type de TOE décrit au §1.3 de la présente cible est le même que celui décrit au §1.3.1 du PP, à savoir une « application VPN présente sur un poste client ».

28 Le contexte de sécurité décrit dans la CDS est conforme à celui qui est décrit dans le PP, en ce sens que les seules différences entre la CDS et le PP sont dues à des conditions plus restrictives dans la CDS. En particulier, la TOE ne permet pas de fonction de Télé-administration centralisée telle que décrite dans le PP. Les menaces, PSO, hypothèses et objectifs de sécurité portant sur cette fonction sont donc sans objet et non repris dans la présente CDS.

29 Les différences entre les contextes de sécurité de la CDS et du PP sont les suivantes :

- Les biens décrits au §3.1 de la CDS et la protection requise pour ces biens sont identiques à ceux du §3.1 du PP, seul le bien D.LOGICIEL sur lequel le PP ne définit aucune menace, étant supprimé.
- Les rôles décrits au §3.2 de la CDS sont identiques à ceux du §3.2 du PP, le rôle utilisateur étant précisé.
- Les menaces décrites au §3.3 de la CDS sont identiques à celles du §3.3 du PP. à l'exception de T.REJEU qui concerne explicitement l'administration à distance, non supportée par la TOE.
- Les Politiques de Sécurité Organisationnelles décrites au §3.4 de la CDS sont identiques à celles du §3.4 du PP.
- Les hypothèses décrites au §3.5 de la CDS sont identiques à celles du §3.5 du PP, à l'exception de A.EQUIPEMENT_TELEADMINISTRATION qui concerne l'administration à distance, non supportée par la TOE.
- L'hypothèse A.COMPOSANT_AUTHENTIFIANT est également supprimée, du fait que le composant authentifiant fait partie de la CDS, comme proposé dans le PP. Elle se trouve remplacée par les objectifs pour la TOE : O.AUTHENTIFICATION_ADMINISTRATEUR et O.AUTHENTIFICATION_UTILISATEUR.
- Les objectifs de sécurité pour la TOE décrits au §4.1 sont identiques à ceux du PP. Seules les politiques du PP concernant l'administration à distance des politiques ne sont pas reprises, puisque la TOE ne comporte pas cette fonction.
- Les objectifs de sécurité pour l'environnement de la TOE décrits au §4.2 de la CDS sont identiques à ceux décrits au §4.2 du PP, à l'exception de l'objectif OE.EQUIPEMENT_TELEADMINISTRATION qui est sans objet du fait que la TOE ne comporte pas cette fonction d'administration à distance.
- L'objectif sur l'environnement opérationnel OE.COMPOSANT_AUTHENTIFIANT est supprimé, du fait que les fonctions d'authentification sont assurées par la TOE elle-même : il se trouve couvert par les objectifs pour la TOE : O.AUTHENTIFICATION_ADMINISTRATEUR et O.AUTHENTIFICATION_UTILISATEUR.

3 Définition du problème de sécurité (ASE_SPD.1)

3.1 Biens

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

3.1.1 Biens protégés par la TOE

31 D.DONNEES_APPLICATIVES

Les données applicatives sont les données provenant et à destination des applications du système d'information de la machine nomade et qui sont véhiculées par le réseau. Elles transitent entre la machine qui héberge la TOE et un chiffreur IP. Ces informations sont contenues dans la charge utile des paquets IP échangés entre l'application VPN cliente et le chiffreur IP et peuvent être stockées temporairement dans la machine par l'application VPN cliente pour pouvoir les traiter (i.e. appliquer les services de sécurité) avant de les envoyer sur le réseau non sûr.

Protection : confidentialité et authenticité et intégrité

32 D.DONNEES_TOPOLOGIQUES

Les informations de topologie du réseau privé (adresses IP source et destination) sont échangées chiffrées (au cours de la phase2 du protocole IKE).

Protection : confidentialité et authenticité et intégrité.

3.1.2 Biens sensibles de la TOE

33 D.POLITIQUES_VPN

Les politiques de sécurité VPN définissent les traitements (filtrage implicite et services de sécurité) à effectuer sur les données échangées entre l'application VPN cliente et un 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.

Protection : confidentialité et authenticité et intégrité

34 D.CLES_CRYPTO

Ce bien représente toutes les clés cryptographiques (symétriques ou asymétriques) nécessaires à l'application VPN cliente pour fonctionner telles que :

- les clés de session ;
- les clés utilisées par les services de sécurité appliqués par les politiques de sécurité VPN ;
- les clés pour protéger les politiques de sécurité VPN lors de leur stockage ;
- les clés pour protéger l'import de clés cryptographiques et de politiques de sécurité VPN dans l'application VPN cliente ;
- les clés pour protéger l'export de politiques de sécurité VPN hors de la machine hébergeant la TOE.

Protection : confidentialité (pour les clés secrètes et la partie privée des clés asymétriques), authenticité et intégrité

35

3.2 Rôles

36 Le fonctionnement de l'application VPN cliente dans son environnement opérationnel manipule directement ou indirectement les rôles décrits ci-dessous :

37 UTILISATEUR

C'est l'usager de la machine hébergeant la TOE et utilisant l'application VPN cliente pour accéder au réseau privé de l'organisation. Cet utilisateur peut envoyer/recevoir des informations vers/de ce réseau privé à travers un lien VPN établi entre l'application VPN cliente et le chiffreur IP.

38 ADMINISTRATEUR SYSTÈME ET RÉSEAU

C'est l'administrateur responsable de la machine hébergeant la TOE. Il configure les paramètres de la machine (comme les comptes utilisateurs), les paramètres réseaux de l'application VPN cliente et les paramètres systèmes qui sont liés aux contextes réseaux opérationnels, mais ne définit pas les politiques de sécurité VPN.

39 ADMINISTRATEUR SÉCURITÉ

C'est l'administrateur responsable de la gestion des éléments de sécurité de la TOE. Il génère et distribue les clés dans l'application VPN cliente et importe les politiques de sécurité VPN et leurs contextes de sécurité que va appliquer l'application VPN cliente.

40 **N.B.**: Dans la suite du document, le rôle administrateur regroupe les rôles administrateur de sécurité et administrateur système et réseau.

3.3 Menaces

41 Les agents menaçants sont les attaquants externes. Ce sont des personnes projetant de se connecter à un réseau privé :

- pour réaliser des opérations auxquelles elles ne sont pas autorisées ou
- pour récupérer des informations auxquelles elles ne sont pas autorisées à accéder.

42 Les administrateurs (hypothèse A.ADMIN) et les utilisateurs (hypothèse A.UTILISATEUR) de la TOE ne sont pas considérés comme des attaquants.

3.3.1 Menaces portant sur les communications

43 T.USURPATION_ADMIN

Un attaquant usurpe l'identité d'un administrateur et l'utilise pour effectuer des opérations d'administration sur l'application VPN cliente.

Biens menacés : D.POLITIQUES_VPN, D.CLES_CRYPTO

44 T.USURPATION_UTILISATEUR

Un attaquant usurpe l'identité d'un utilisateur et l'utilise pour accéder illégalement aux services rendus par le client VPN ou pour réaliser des opérations sur la TOE pour lesquelles l'utilisateur est autorisé.

Biens menacés : D.DONNEES_APPLICATIVES, D.DONNEES_TOPOLOGIQUES, D.CLES_CRYPTO

3.3.2 Menaces portant sur la gestion des clés cryptographiques

45 T.MODIFICATION_CLES

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

Biens menacés : D.CLES_CRYPTO

46 T.DIVULGATION_CLES

Un attaquant récupère illégalement des clés cryptographiques.

Biens menacés : D.CLES_CRYPTO

3.3.3 Menaces portant sur les politiques de sécurité VPN et leur contexte

47 T.MODIFICATION_POL

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

Biens menacés : D.POLITIQUES_VPN

48 T.DIVULGATION_POL

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

Biens menacés : D.POLITIQUES_VPN

3.4 Politiques de sécurité organisationnelles (OSP)

3.4.1 Services rendus

49 OSP.SERVICES_RENDUS

L'application VPN cliente doit appliquer les politiques de sécurité VPN définies pour les utilisateurs et les liens VPN logiques (établis physiquement entre l'application VPN cliente et un chiffreur IP), sur les données transitant sur ces liens.
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 intégrité des données applicatives ;
- protection en confidentialité des données topologiques ;
- protection en intégrité des données topologiques.

Biens protégés : D.DONNEES_APPLICATIVES, D.DONNEES_TOPOLOGIQUES

3.4.2 Autres services

50 OSP.CRYPTO

Les référentiels de cryptographie de l'ANSSI ([CRYPTO] et [CRYPTO_G]) définis pour le niveau de résistance standard doivent être suivis pour la gestion des clés (renouvellement) et les fonctions cryptographiques utilisées dans l'application VPN cliente.
Les fonctions cryptographiques concernées par cet objectif incluent la génération des clés cryptographiques (D.CRYPTO) elles-mêmes, pour celles qui sont générées par la TOE, comme les clés de session ou les clés protégeant les fichiers de configuration.

Biens protégés : tout bien sensible utilisant la cryptographie pour sa protection

51 OSP.EXPORT_POL

L'application VPN cliente doit permettre d'exporter les politiques de sécurité VPN et leur contexte de sécurité, stockées dans la machine hébergeant la TOE, vers un administrateur pour consultation.

Biens protégés : D.POLITIQUES_VPN

3.5 Hypothèses

3.5.1 Interactions avec la TOE

52 A.ADMIN

Les administrateurs sont des personnes non hostiles et compétentes qui disposent des moyens nécessaires à la réalisation de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration. Ces personnes sont considérés de confiance, et comme n'ayant pas intérêt à dégrader la sécurité des tunnels. Elles sont censées administrer correctement la TOE.

53 A.UTILISATEUR

L'utilisateur de l'application VPN cliente est une personne non hostile et formée à l'utilisation de l'application VPN cliente. En particulier, elle ne doit pas divulguer les données lui permettant de s'authentifier auprès du système de chiffrement. Cette personne est considérée de confiance, et comme n'ayant pas intérêt à dégrader la sécurité du tunnel. Elle est censée utiliser correctement la TOE.

54 A.CHIFFREUR_IP

Le chiffreur IP avec lequel l'application VPN cliente communique est supposé tracer les activités qui ont eu lieu sur le lien VPN. Il est par ailleurs supposé activer des alarmes de sécurité permettant de remonter vers un administrateur de sécurité toute violation des politiques de sécurité VPN sur le lien considéré.

3.5.2 Machine hôte

55 A.MACHINE

Il est supposé que la machine sur laquelle est installée et exécutée l'application VPN cliente est saine et correctement administrée. En particulier, elle dispose d'un anti-virus dont la base de données est régulièrement mise à jour et est protégée par un pare-feu.
Il est par ailleurs supposé que la machine hôte hébergeant l'application VPN cliente continue d'assurer la protection des données ayant été récupérées au travers de liens VPN.
Enfin, il est supposé que la machine hôte garantit l'intégrité du logiciel permettant de mettre en œuvre tous les services de l'application VPN cliente.

56 A.DROITS_UTILISATEUR

Il est supposé que l'utilisateur de la machine hébergeant l'application VPN cliente ne possède pas les droits d'installation, de configuration, de mise à jour et de désinstallation de l'application VPN cliente.

57 A.CONFIGURATION

Il est supposé que la configuration de la machine hébergeant l'application VPN cliente garantit la protection des impacts que peuvent avoir les communications en clair de la machine via différentes interfaces physiques ou logiques (consultation de sites Internet par exemple) sur les communications sur les liens VPN.

58 A.COMM

Il est supposé que l'environnement de la TOE permet de maîtriser les communications vers et depuis l'extérieur de la machine qui ne transitent pas par la TOE.

59 A.EXPORT_CLES

Il est supposé que l'export, par l'utilisateur, des clés cryptographiques secrètes ou privées importées ou générées dans la TOE hors de la machine sur laquelle la TOE est installée, est rendu impossible par la configuration de la machine.

60 A.MULTI-UTILISATEURS

Il est supposé que la gestion des identifications/authentifications des différents utilisateurs d'une machine multi-utilisateurs est prise en compte par l'environnement de la TOE.

3.5.3 Réinitialisation

61 A.REINITIALISATION

Il est supposé que l'environnement permet de réinitialiser l'application VPN cliente dans un état sûr.

3.5.4 Cryptographie

62 A.ACCES

Il est supposé que l'accès aux différents composants du système de chiffrement est restreint grâce à une gestion de clé cryptographiques (secret partagé, infrastructure à clé publique,...) associée à une politique de sécurité VPN.

4 Objectifs de sécurité (ASE_OBJ.2)

4.1 Objectifs de sécurité pour la TOE

4.1.1 Objectifs de sécurité pour les services rendus par la TOE

63 O.APPLICATION_POL

La TOE doit appliquer aux données transitant sur les liens VPN les politiques de sécurité VPN présentes dans l'application VPN cliente et associées à l'utilisateur authentifié.
Ces politiques de sécurité peuvent inclure en particulier la confidentialité, l'authenticité et l'intégrité des données échangées.

64 O.CONFIDENTIALITE_APPLI

La TOE doit fournir des mécanismes pour protéger en confidentialité les données applicatives qui transitent entre la machine hébergeant l'application VPN cliente et un chiffreur IP.

65 O.AUTHENTICITE_APPLI

La TOE doit fournir des mécanismes pour protéger en intégrité et en authenticité les données applicatives qui transitent entre la machine hébergeant l'application VPN cliente et un chiffreur IP.

66 O.CONFIDENTIALITE_TOPO

La TOE doit fournir des mécanismes pour protéger en confidentialité les données topologiques qui transitent entre la machine hébergeant l'application VPN cliente et un chiffreur IP.

67 O.AUTHENTICITE_TOPO

La TOE doit fournir des mécanismes pour protéger en intégrité et en authenticité les données topologiques qui transitent entre la machine hébergeant l'application VPN cliente et un chiffreur IP.

4.1.2 Objectifs de sécurité pour protéger les biens sensibles de la TOE

4.1.2.1 Authentification

68 O.AUTHENTIFICATION_ADMIN

La TOE doit vérifier que l'administrateur a été authentifié par un composant du système de chiffrement avant de pouvoir réaliser des opérations d'administration sur la TOE. Le mécanisme d'authentification utilisé doit être conforme aux recommandations du référentiel de l'ANSSI [AUTH] pour le niveau de robustesse standard.

69 O.AUTHENTIFICATION_UTILISATEUR

La TOE doit vérifier que l'utilisateur a été authentifié par un composant du système de chiffrement avant de pouvoir accéder aux services rendus par la TOE et aux opérations autorisées aux utilisateurs. Le mécanisme d'authentification utilisé doit être conforme aux recommandations du référentiel de l'ANSSI [AUTH] pour le niveau de robustesse standard.
Cette authentification peut être vérifiée, selon les paramètres indiqués dans la configuration, par :

- l'application VPN cliente elle-même,
- le chiffreur IP distant qui établira un lien VPN avec la machine hébergeant la TOE,
- le module cryptographique de l'utilisateur (clé USB ou carte à puce).

4.1.2.2 Gestion des clés cryptographiques

70 O.IMPORT_CLES

La TOE doit permettre uniquement à l'utilisateur et à l'administrateur d'importer des clés cryptographiques dans la TOE.

71 O.PROTECTION_CLES

La TOE doit protéger en confidentialité les clés secrètes et la partie privée des clés asymétriques. La TOE doit protéger en intégrité toutes les clés lors de leur import dans l'application VPN cliente. La protection en intégrité devra consister en la détection de la perte d'intégrité et l'annulation de l'opération d'import.
L'intégrité des clés doit aussi être assurée lors de leur stockage dans la machine hébergeant l'application VPN cliente ; en cas de détection de perte d'intégrité de la clé, la TOE devra annuler l'établissement de tout lien VPN.
Cet objectif est complété par O.IMPORT_CLES qui restreint la possibilité d'importation des clés cryptographiques dans la TOE à l'utilisateur et l'administrateur.

4.1.2.3 Gestion des politiques de sécurité VPN

72 O.IMPORT_POL

La TOE doit permettre uniquement aux administrateurs d'importer les politiques de sécurité VPN et leurs contextes de sécurité.

73 O.PROTECTION_POL

La TOE doit fournir des mécanismes pour protéger les politiques de sécurité VPN en confidentialité et en intégrité lors de leur import et de leur export. Lors de l'import, la protection en intégrité devra consister en la détection de la perte d'intégrité et l'annulation de l'opération. Lors de l'export, elle consistera à rendre possible la détection de toute perte d'intégrité. L'intégrité des politiques de sécurité VPN doit aussi être assurée lors de leur stockage; en cas de détection de perte d'intégrité de la politique de sécurité VPN, la TOE devra annuler l'établissement de tout lien VPN.
Par ailleurs, la TOE doit permettre d'exporter les politiques de sécurité VPN vers un administrateur.

4.1.2.4 Administration à distance

74 La TOE ne comporte pas d'interface d'administration à distance : les politiques correspondantes du Profil de Protection sont donc sans objet.

4.1.2.5 Gestion de la cryptographie

75 O.CRYPTO

La TOE doit implémenter les fonctions cryptographiques et gérer (renouveler) les clés cryptographiques en accord avec les référentiels de cryptographie définis par l'ANSSI ([CRYPTO] et [CRYPTO_G]) pour le niveau de résistance standard.

4.2 Objectifs de sécurité pour l'environnement opérationnel

4.2.1 Interactions avec la TOE

76 OE.ADMIN

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

77 OE.UTILISATEUR

L'utilisateur est formé à l'utilisation de la TOE et sensibilisé à la sécurité, en particulier sur les risques liés à la divulgation des informations qu'il détient et qui lui permettent de s'authentifier auprès du système de chiffrement.

78 OE.CHIFFREUR_IP

Le chiffreur IP avec lequel l'application VPN cliente communique doit permettre de tracer les activités qui ont eu lieu sur le lien VPN. Il devra par ailleurs activer des alarmes de sécurité permettant de remonter vers un administrateur de sécurité toute violation des politiques de sécurité VPN sur le lien considéré.

4.2.2 Machine hôte

79 OE.MACHINE

La machine hôte sur laquelle est exécutée l'application VPN cliente doit être saine, protégée et configurée de manière à garantir sa sécurité et celle des données qu'elle héberge. En particulier, elle assure l'intégrité de l'application VPN cliente qu'elle héberge. A ce titre, plusieurs recommandations de configuration de la machine sont indiquées dans le guide utilisateur (chapitre 19.2.2) et doivent être respectées.

80 OE.DROITS_UTILISATEURS

Seuls les administrateurs peuvent réaliser les tâches d'administration relatives à l'application VPN cliente (installation, configuration, mise à jour et désinstallation).

81 OE.CONFIGURATION

La configuration de la machine hébergeant l'application VPN cliente doit protéger les communications sur les liens VPN des impacts pouvant résulter de communications en clair de la machine via différents canaux physiques ou logiques.

82 OE.COMM

L'environnement de la TOE doit permettre de maîtriser les communications vers et depuis l'extérieur de la machine hôte qui ne transitent pas par la TOE.

83 OE.EXPORT_CLES

La configuration de la machine hôte hébergeant l'application VPN cliente doit rendre impossible à l'utilisateur l'export hors de la machine des clés cryptographiques secrètes ou privées importées ou générées dans la TOE.

84 OE.MULTI-UTILISATEURS

La gestion des identifications/authentifications des différents utilisateurs d'une machine multi-utilisateurs doit être prise en compte par l'environnement de la TOE.

4.2.3 Réinitialisation

85 OE.REINITIALISATION

L'environnement doit permettre de réinitialiser la TOE dans un état sûr.

4.2.4 Cryptographie

86 OE.CRYPTO

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

87 OE.ACCES

L'accès aux différents composants du système de chiffrement doit être restreint grâce à une gestion de clés cryptographiques (secret partagé, infrastructure à clé publique,...) associée à une politique de sécurité VPN.

5 Exigences de sécurité (ASE_REQ.2)

5.1 Exigences de sécurité fonctionnelles (SFR)

88 Les opérations d'assignation, de sélection et de raffinement sont identifiées par du texte en gras.

89 Les itérations sont identifiées par un caractère séparateur "/". Par exemple : FDP_ETC.1/EXPORT.

5.1.1 Définition des éléments du modèle de sécurité sous-jacent

90 L'instanciation des exigences fonctionnelles de sécurité repose sur les sujets, objets, opérations, attributs et utilisateurs définis ci-après.

5.1.1.1 Sujets

91 S.user_manager

Ce sujet est en charge de la communication avec les utilisateurs de la TOE (U.user) et les administrateurs (U.administrator). Il gère en particulier l'authentification ainsi que l'import et l'export des biens sensibles de la TOE.

92 S.communication_manager

Ce sujet est en charge de la communication avec le chiffreur IP (U.IP_encrypter) ; pour cela il applique la politique de sécurité VPN associée à un lien VPN logique donné.

5.1.1.2 Objets

93 **N.B.**: les objets sont stockés dans la TOE afin d'être traités ou de participer à son fonctionnement. Ils sont encapsulés dans des informations lors de leur communication avec l'extérieur de la TOE.

94 OB.keys

Cet objet correspond au bien sensible D.CLES_CRYPTO ; il s'agit des clés cryptographiques générées hors de la TOE / par la TOE et utilisées par la TOE.

95 OB.vpn_policies

Cet objet correspond au bien sensible D.POLITIQUES_VPN, il s'agit des politiques de sécurité VPN et leurs contextes de sécurité utilisés par la TOE.

96 OB.data

Cet objet correspond aux biens sensibles D.DONNEES_APPLICATIVES et D.DONNEES_TOPOLOGIQUES ; il s'agit des informations applicatives et topologiques contenues dans les paquets IP échangés entre la TOE et le chiffreur IP, via le canal VPN.

5.1.1.3 Opérations

97 Import

Cette opération permet d'importer une donnée dans la TOE. Elle est utilisée pour l'import des clés cryptographiques et des politiques de sécurité VPN stockées dans la TOE, ainsi que pour l'import de données applicatives et topologiques.

98 Export

Cette opération permet d'exporter une donnée hors de la TOE. Elle s'applique aux politiques de sécurité VPN stockées dans la TOE ainsi qu'aux données applicatives et topologiques.

99 Use

Cette opération permet l'utilisation d'une donnée par une autre opération que l'import ou l'export. Elle s'applique aux clés cryptographiques pour réaliser les opérations cryptographiques.

100 Application

Cette opération permet d'appliquer une protection à une donnée. Elle s'applique aux données (applicatives et topologiques) afin de leur appliquer les protections en authenticité et/ou confidentialité et/ou intégrité (i.e. la politique de sécurité associée), pour le transfert vers le chiffreur IP, via le canal VPN.

101 Authentification

Cette opération permet d'authentifier les utilisateurs de la TOE (U.user) et les administrateurs (U.administrator). Elle est utilisée en préalable aux autres fonctions.

5.1.1.4 Attributs

102 AT.user_type

Cet attribut spécifie le type d'utilisateur lié au sujet S.user_manager ; ce type doit être choisi dans l'ensemble {null, user, administrator}. Il s'agit d'un attribut du sujet S.user_manager.

103 AT.user_id

Cet attribut est associé à un sujet S.user_manager et fournit un identifiant de l'utilisateur lié au sujet S.user_manager. Il est égal à "null" pour préciser qu'aucun utilisateur n'est authentifié ou à "user identifier" sinon (l'ensemble des valeurs n'est donc pas fini). Il s'agit d'un attribut du sujet S.user_manager.

104 AT.user_name

Cet attribut est associé à l'objet OB.vpn_policies et spécifie à quel utilisateur cet objet (donc cette politique de sécurité VPN) est associé. La valeur de cet attribut est l'identificateur d'un utilisateur (Cf. la description de l'attribut AT.user_id). Il s'agit d'un attribut de l'objet OB.vpn_policies.

105 AT.VPN_link_id

Cet attribut correspond à l'identifiant d'un lien VPN logique établit entre la TOE et un sous réseau du réseau privé, via un chiffreur IP. La valeur de cet attribut est l'identificateur d'un lien logique (l'ensemble des valeurs n'est donc pas fini). Il s'agit d'un attribut du sujet OB.vpn_policies.

106 AT.data_confidentiality

Cet attribut est associé à un objet OB.vpn_policies et spécifie si cet objet (donc cette politique de sécurité VPN) impose l'application de la propriété de confidentialité sur les données transmises au chiffreur IP. Cet attribut peut prendre les valeurs "true" ou "false". Il s'agit d'un attribut de l'objet OB.vpn_policies.

107 AT.data_authenticity

Cet attribut est associé à un objet OB.vpn_policies et spécifie si cet objet (donc cette politique de sécurité VPN) impose l'application de la propriété d'authenticité (intégrité et authentification d'origine) sur les données transmises au chiffreur IP. Cet attribut peut prendre les valeurs "true" ou "false". Il s'agit d'un attribut de l'objet OB.vpn_policies.

5.1.1.5 Utilisateurs

108 U.administrator

Cet utilisateur représente l'administrateur de l'application VPN cliente tel que spécifié au paragraphe 3.2. Il devra être lié au sujet S.user_manager.

109 U.user

Cet utilisateur représente l'utilisateur de l'application VPN cliente tel que spécifié au paragraphe 3.2. Il devra être lié au sujet S.user_manager.

110 U.IP_encrypter

Cet utilisateur représente le chiffreur IP avec lequel l'application VPN cliente communique via un lien VPN. Il devra être lié au sujet S.communication_manager.

5.1.2 Provided service

5.1.2.1 VPN communication link management

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

111 FDP_ETC.1.1/EXPORT The TSF shall enforce the **data access policy** when exporting user data, controlled under the SFP, outside of the TOE.

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

113 Note complémentaire : Les "user data" sont les données applicatives et topologiques (OB.data) contenues dans les paquets IP fournis au sujet (S.communication_manager) qui gère les communications VPN échangées entre la TOE et un chiffreur IP (U.IP_encrypter).

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

114 FDP_ITC.1.1/IMPORT The TSF shall enforce the **data access policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

116 FDP_ITC.1.3/IMPORT The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **Vérification de l'intégrité des données importées**.

117 Note complémentaire : Les "user data" sont les données applicatives et topologiques (OB.data) contenues dans les paquets IP fournis au sujet (S.communication_manager) qui gère les communications VPN échangées entre la TOE et un chiffreur IP (U.IP_encrypter).

5.1.2.2 Data access protection

FDP_IFC.1/DATA Subset information flow control

118 FDP_IFC.1.1/DATA The TSF shall enforce the **data access policy** on subjects, objects and operations identified by this following table:

Subjects	**S.user_manager, S.communication_manager**
Objects	**OB.data, OB.vpn_policies**
Operations	**application, import, export**

FDP_IFF.1/DATA Simple security attributes

119 FDP_IFF.1.1/DATA The TSF shall enforce the **data access policy** based on the following types of subject and information security attributes:

Type	Element	Relevant security attributes(s)
Subjects	**S.user_manager, S.communication_manager**	**AT.user_type, AT.VPN_link_id**
Objects	**OB.data, OB.vpn_policies**	**AT.data_authenticity, AT.data_confidentiality**

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

- **Rule 1**: the subject S.communication_manager is allowed to perform application of OB.vpn_policies on OB.data ;
- **Rule 2**: the subject S.communication_manager is allowed to import OB.data provided the S.user_manager is a "user" (i.e. the value of the attribute S.user_manager.user_type is equal to "user") ;

- **Rule 3**: the subject S.communication_manager is allowed to export OB.data provided the S.user_manager is a "user" (i.e. the value of the attribute S.user_manager.user_type is equal to "user") and the keys and the VPN security policy are integer.

121 FDP_IFF.1.3/DATA The TSF shall enforce the **VPN security policy of the VPN link on the applicative and topologic data (OB.data) contained in IP packets before exporting/importing the IP packets to/from the user, by application of the following rules:**

- **Rule 4**: the authenticity security protection (i.e. integrity and authentication of origin) must be applied to OB.data if the following conditions hold:
  - OB.vpn_policies requires authenticity (i.e. OB.vpn_policies.data_authenticity is equal to "True") and
  - the user linked to S.user_manager is allowed to use the OB.vpn_policies (i.e. OB.vpn_policies.user_name is equal to S.user_manager.user_id) and
  - OB.vpn_policies is associated to the VPN link established with U.IP_encrypter (i.e. OB.vpn_policies.VPN_link_id corresponds to the identifier of the VPN link established with U.IP_encrypter) ;
- **Rule 5**: the confidentiality security protection must be applied to OB.data if the following conditions hold:
  - OB.vpn_policies requires confidentiality (i.e. OB.vpn_policies.data_confidentiality is equal to "True") and
  - the user linked to S.user_manager is allowed to use the OB.vpn_policies (i.e. OB.vpn_policies.user_name is equal to S.user_manager.user_id) and
  - OB.vpn_policies is associated to the VPN link established with U.IP_encrypter (i.e. OB.vpn_policies.VPN_link_id corresponds to the identifier of the VPN link established with U.IP_encrypter).

122 FDP_IFF.1.4/DATA The TSF shall explicitly authorise an information flow based on the following rules: none.

123 FDP_IFF.1.5/DATA The TSF shall explicitly deny an information flow based on the following rules: none.

5.1.2.3 Data authenticity

FDP_UIT.1/DATA Data exchange integrity

124 FDP_UIT.1.1/DATA The TSF shall enforce the **data access policy** to be able to **transmit and receive** user data in a manner protected from **modification, deletion and replay** errors.

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

126 Note complémentaire : les "user data" sont les données applicatives et topologiques (OB.data) contenues dans les paquets IP fourni au sujet (S.communication_manager) qui gère les communications VPN échangées entre la TOE et un chiffreur IP (U.IP_encrypter).

Note d'application : L'application effective ou pas de cette propriété est spécifiée dans l'exigence fonctionnelle FDP_IFF.1/DATA.

FCO_NRO.1/DATA Selective proof of origin

127 FCO_NRO.1.1/DATA The TSF shall be able to generate evidence of origin for transmitted **applicative and topologic data** at the request of **no third parties**.

128 FCO_NRO.1.2/DATA The TSF shall be able to relate **no attributes** of the originator of the information, and **no information fields** of the information to which the evidence applies.

129 FCO_NRO.1.3/DATA The TSF shall provide a capability to verify the evidence of origin of information **to no third parties**.

130 Note complémentaire : Les "applicative and topologic data" sont les données applicatives et topologiques (OB.data) contenues dans les paquets IP fourni au sujet (S.communication_manager) qui gère les communications VPN échangées entre la TOE et un chiffreur IP (U.IP_encrypter).

Note d'application : L'application effective ou pas de cette propriété est spécifiée dans l'exigence fonctionnelle FDP_IFF.1/DATA.

5.1.2.4 Data confidentiality

FDP_UCT.1/DATA Basic data exchange confidentiality

131 FDP_UCT.1.1/DATA The TSF shall enforce the **data access policy** to be able to **transmit and receive** user data in a manner protected from unauthorised disclosure.

Note complémentaire : Les "user data" sont les données applicatives et topologiques (OB.data) contenues dans les paquets IP fourni au sujet (S.communication_manager) qui gère les communications VPN échangées entre la TOE et un chiffreur IP (U.IP_encrypter).
Note d'application : L'application effective ou pas de cette propriété est spécifiée dans l'exigence fonctionnelle FDP_IFF.1/DATA.

5.1.3 Authentication

132 L'authentification, réalisée par un tiers, peut être vérifiée par l'un des composants suivants du système :

- l'application VPN cliente elle-même,
- le chiffreur IP distant qui établira un tunnel VPN avec la machine hébergeant la TOE,
- le module cryptographique de l'utilisateur (clé USB ou carte à puce).

5.1.3.1 User authentication

FIA_UID.2/USER User identification before any action

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

Notes complémentaires :

- Le "user" considéré dans cette exigence est l'utilisateur U.user ;
- L'identification n'est pas effectuée par la TOE mais la TOE vérifie que cette identification a été effectuée.

FIA_UAU.2/USER User authentication before any action

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

Notes complémentaires :

- Le "user" considéré dans cette exigence est l'utilisateur U.user ;
- L'authentification n'est pas effectuée par la TOE mais la TOE vérifie que cette authentification a été effectuée ;
- Le mécanisme d'authentification doit respecter les exigences de [AUTH].

FIA_USB.1/USER User-subject binding

135 FIA_USB.1.1/USER The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- **AT.user_id ;**
- **AT.user_type.**

136 FIA_USB.1.2/USER The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- **the security attribute AT.user_id corresponding to the identifier of the user shall be set to the user identifier ;**
- **the security attribute AT.user_type shall be set to "user".**

137 FIA_USB.1.3/USER The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **no rules for user attributes changes.**

Notes complémentaires :

- Le "user" considéré dans cette exigence est l'utilisateur U.user ;
- Le "subject" considéré dans cette exigence est le sujet S.user_manager.

5.1.3.2 Administrator authentication

FIA_UID.2/ADMIN User identification before any action

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

Note complémentaire : le "user" considéré dans cette exigence est l'utilisateur U.administrator.

FIA_UAU.2/ADMIN User authentication before any action

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

Notes complémentaires :

- Le "user" considéré dans cette exigence est l'utilisateur U.administrator ;
- L'authentification doit être effectuée par la TOE ;
- Le mécanisme d'authentification doit respecter les exigences de [AUTH].

FIA_USB.1/ADMIN User-subject binding

140 FIA_USB.1.1/ADMIN The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- **AT.user_type.**

141 FIA_USB.1.2/ADMIN The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- **the security attribute AT.user_type shall be set to "administrator".**

142 FIA_USB.1.3/ADMIN The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **No change of attributes**.

Notes complémentaires :

- Le "user" considéré dans cette exigence est l'utilisateur U.administrator ;
- Le "subject" considéré dans cette exigence est le sujet S.user_manager.

5.1.4 Security attributes management

FMT_MSA.3 Static attribute initialisation

143 FMT_MSA.3.1 The TSF shall enforce the **data access policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

144 FMT_MSA.3.2 The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

Notes complémentaires : La TSF doit assigner la valeur "null" aux attributs de sécurité AT.user_type et AT.user_id chaque fois qu'un sujet S.user_manager is created.

FMT_MSA.1/MODIFY Management of security attributes

145 FMT_MSA.1.1/MODIFY The TSF shall enforce the **data access policy** to restrict the ability to **modify** the security attributes **AT.user_type and AT.user_id values** to **the user bound to S.user_manager**.

FMT_MSA.1/QUERY Management of security attributes

146 FMT_MSA.1.1/QUERY: The TSF shall enforce the **data access policy** to restrict the ability **to query** the security attributes **AT.user_type and AT.user_id of S.user_manager, and AT.user_name and AT.vpn_link_id of OB.vpn_policies**, to **S.communication_manager, which is bound to the IP encrypter and manages transmission**.

5.1.5 Cryptographic key management

5.1.5.1 Key policy

FDP_IFC.1/KEY_IMPORT Subset information flow control

147 FDP_IFC.1.1/KEY_IMPORT: The TSF shall enforce the **key management policy** on subjects, objects and operations identified by this following table:

Subjects	**S.user_manager, S.communication_manager**
Objects	**OB.keys**
Operations	**import, use**

FDP_IFF.1/KEY_IMPORT Simple security attributes

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

Type	Element	Relevant security attributes(s)
Subjects	**S.user_manager, S.communication_manager**	**AT.user_type**
Objects	**OB.keys**	

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

- **Rule 1**: the subject S.user_manager is allowed to import keys in OB.keys provided it has been authenticated either as "user" or as "administrator" (i.e. S.user_manager.user_type is equal to "user" or to "administrator");
- **Rule 2**: the subject S.communication_manager is allowed to use OB.keys.

150 FDP_IFF.1.3/KEY_IMPORT: The TSF shall enforce **no additional information flow control SFP rules**.

151 FDP_IFF.1.4/KEY_IMPORT: The TSF shall explicitly authorise an information flow based on the following rules: **none**.

152 FDP_IFF.1.5/KEY_IMPORT: The TSF shall explicitly deny an information flow based on the following rules: **none**.

Note d'application : Les utilisateurs U.user et U.administrator doivent être authentifiés auprès de la TOE.

5.1.5.2 Cryptographic key import

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

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

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

155 FDP_ITC.1.3/KEY_IMPORT: The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **On detection of an anomaly, in particular an integrity problem, the TSF shall discard the data and/or the security attributes**.

Note complémentaire : Les "user data" sont les valeurs des clés secrètes et de la partie privée des clés asymétriques fournies au sujet (S.user_manager) qui gère les communications avec les utilisateurs.

FDP_UCT.1/KEY_IMPORT Basic data exchange confidentiality

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

157 Note complémentaire : Les "user data" sont les valeurs des clés secrètes et de la partie privée des clés asymétriques fournies au sujet (S.user_manager) qui gère les communications avec les utilisateurs.

FDP_UIT.1/KEY_IMPORT Data exchange integrity

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

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

Note complémentaire : Les "user data" sont les valeurs des clés secrètes et de la partie privée des clés asymétriques fournies au sujet (S.user_manager) qui gère les communications avec les utilisateurs.

5.1.6 VPN security policies management

5.1.6.1 VPN security policies import/export

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

160 FDP_ETC.1.1/VPN_POL The TSF shall enforce the **VPN protection policy** when exporting user data, controlled under the SFP, outside of the TOE.

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

Note complémentaire : Les "user data" sont les politiques de sécurité VPN (OB.vpn_policies).

FDP_ITC.2/VPN_POL Import of user data with security attributes

162 FDP_ITC.2.1/VPN_POL The TSF shall enforce the **VPN protection policy** when importing user data, controlled under the SFP, from outside of the TOE.

163 FDP_ITC.2.2/VPN_POL The TSF shall use the security attributes associated with the imported user data.

164 FDP_ITC.2.3/VPN_POL The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

165 FDP_ITC.2.4/VPN_POL The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

166 FDP_ITC.2.5/VPN_POL The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **the data shall be imported with the security attribute AT.user_name which corresponds to the identifier of the user who will use this VPN security policy and AT.VPN_link_id which corresponds to the identifier of a link;**
- **on detection of an anomaly, in particular an integrity problem, the TSF shall discard the data and/or the security attributes.**

Note complémentaire : Les "user data" sont les politiques de sécurité VPN (OB.vpn_policies).

5.1.6.2 VPN security policies properties

FDP_UCT.1/VPN_POL Basic data exchange confidentiality

167 FDP_UCT.1.1/VPN_POL The TSF shall enforce the **VPN protection policy** to be able to **transmit and receive** user data in a manner protected from unauthorised disclosure.

168 Note complémentaire : Les "user data" sont les politiques de sécurité VPN (OB.vpn_policies).

FDP_UIT.1/VPN_POL Data exchange integrity

169 FDP_UIT.1.1/VPN_POL The TSF shall enforce the **VPN protection policy** to be able to **transmit and receive** user data in a manner protected from **modification, deletion and replay** errors.

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

Note complémentaire : Les "user data" sont les politiques de sécurité VPN (OB.vpn_policies).

5.1.6.3 Divers

FDP_IFC.1/VPN_POL Subset information flow control

171 FDP_IFC.1.1/VPN_POL The TSF shall enforce the **VPN protection policy** on subjects, objects and operations identified by this following table:

Subjects	**S.user_manager, S.communication_manager**
Objects	**OB.vpn_policies**
Operations	**application, import, export**

FDP_IFF.1/VPN_POL Simple security attributes

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

Type	Element	Relevant security attributes(s)
Subjects	**S.user_manager, S.communication_manager**	**AT.user_type, AT.VPN_link_id**
Objects	**OB.vpn_policies**	

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

- **Rule 1**: the subject S.user_manager is allowed to import a VPN security policy in OB.vpn_policies provided it has been authenticated as "administrator" (i.e. S.user_manager.user_type is equal to "administrator");
- **Rule 2**: the subject S.user_manager is allowed to export a VPN security policy from OB.vpn_policies provided it has been authenticated as "administrator" (i.e. S.user_manager.user_type is equal to "administrator");
- **Rule 3**: the subject S.communication_manager is allowed to perform application of OB.vpn_policies.

174 FDP_IFF.1.3/VPN_POL The TSF shall enforce the:

- **no user can trigger the export of a VPN security policy, but the user U.administrator**

175 FDP_IFF.1.4/VPN_POL The TSF shall explicitly authorise an information flow based on the following rules: **none**.

176 FDP_IFF.1.5/VPN_POL The TSF shall explicitly deny an information flow based on the following rules: **none**.

5.1.7 Cryptography

177 La génération de clés cryptographiques ne fait pas partie de la définition du problème de sécurité du [PP-VPNC]. Cette fonction est toutefois intégrée dans la présente CDS conforme à celui-ci.

FCS_CKM.1 Cryptographic key generation

178 FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with the cryptographic key generation algorithm **OpenSSL random with post-treatment**, and specified cryptographic key sizes of 128, 192 and 256 bits that meet the following: **cryptographic referential ([CRYPTO] and [CRYPTO_G])**.

FCS_CKM.3 Cryptographic key access

179 FCS_CKM.3.1 The TSF shall perform key renegotiation in accordance with cryptographic key renewal that meets the following: **cryptographic referential ([CRYPTO] and [CRYPTO_G])**.

180 Note complémentaire : Lorsqu'une clé a dépassé sa durée de validité, une autre clé doit être utilisée pour les communications via le tunnel VPN. La liste des standards doit être conforme aux recommandations des référentiels de l'ANSSI [CRYPTO] et [CRYPTO-G].

FCS_COP.1 Cryptographic operation
FCS_COP.1/AES

181 FCS_COP.1.1/AES The TSF shall perform **encryption and decryption** in accordance with the **AES** cryptographic algorithm and cryptographic key sizes **of 128, 192 and 256 bits** that meet the following: **ANSSI cryptographic referential ([CRYPTO] and [CRYPTO_G])**.

FCS_COP.1/RSA

182 FCS_COP.1.1/RSA The TSF shall perform **encryption and decryption** in accordance with the **RSA** cryptographic algorithm and cryptographic key sizes of **2048 bits minimum** that meet the following: **ANSSI cryptographic referential ([CRYPTO] and [CRYPTO_G])**.

FCS_COP.1/SHA-2

183 FCS_COP.1.1/SHA-2 The TSF shall perform **hash** in accordance with the **SHA-2** cryptographic algorithm and cryptographic key sizes **of 256 bits (taille du condensat)** that meet the following: **ANSSI cryptographic referential ([CRYPTO] and [CRYPTO_G])**.

5.2 Exigences de sécurité d'assurance (SAR)

184 Le niveau d'assurance de l'évaluation de cette CDS est EAL3 augmenté des composants ALC_FLR.3 et AVA_VAN.3 conformément au processus de qualification de niveau standard défini dans [QUA-STD].

185 Le tableau ci-après présente la liste des exigences de sécurité d'assurance requises par le niveau d'assurance de l'évaluation de cette CDS.

RÉFÉRENCE	TITRE
ADV_ARC.1	Security architecture description
ADV_FSP.3	Functional specification with complete summary
ADV_TDS.2	Architectural design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.3	Authorisation controls
ALC_CMS.3	Implementation representation CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_FLR.3	Systematic flaw remediation
ALC_LCD.1	Developer defined life-cycle model
ASE_INT.1	ST introduction
ASE_CCL.1	Conformance claims
ASE_SPD.1	Security problem definition
ASE_OBJ.2	Security objectives
ASE_ECD.1	Extended components definition
ASE_REQ.2	Derived security requirements
ASE_TSS.1	TOE summary specification
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.3	Focused vulnerability analysis

Tableau 3 : Liste des exigences de sécurité d'assurance requises

6 Spécifications sommaires de la TOE (ASE_TSS.1)

6.1 Fonctions de Sécurité

6.1.1 Fonctions Générales

186 F_APPLICATION_POLITIQUE

TheGreenBow VPN client applique aux données transitant sur les liens VPN les politiques de sécurité associées à l'utilisateur authentifié.

187 F_CONFIDENTIALITE_APPLI

TheGreenBow VPN client fournit des mécanismes cryptographiques pour protéger en confidentialité les données applicatives qui transitent entre l'équipement sur lequel il est installé et un chiffreur IP.

188 F_INTEGRITE_APPLI

TheGreenBow VPN client fournit des mécanismes cryptographiques pour protéger en intégrité et en authenticité les données applicatives qui transitent entre l'équipement sur lequel il est installé et un chiffreur IP.

189 F_CONFIDENTIALITE_TOPO

TheGreenBow VPN client fournit des mécanismes cryptographiques pour protéger en confidentialité les données topologiques qui transitent entre l'équipement sur lequel il est installé et un chiffreur IP.

190 F_INTEGRITE_TOPO

TheGreenBow VPN client fournit des mécanismes cryptographiques pour protéger en intégrité et en authenticité les données topologiques qui transitent entre l'équipement sur lequel il est installé et un chiffreur IP.

191 F_AUTHENTIFICATION_ADMIN

TheGreenBow VPN client vérifie que l'administrateur a été authentifié avant de pouvoir réaliser des opérations d'administration.

192 F_AUTHENTIFICATION_UTILISATEUR

TheGreenBow VPN client vérifie que l'utilisateur a été authentifié avant de pouvoir accéder aux services rendus par le produit et aux opérations autorisées aux utilisateurs, en l'occurrence monter un tunnel et utiliser les fonctions de chiffrement / déchiffrement.

6.1.2 Gestion des clés cryptographiques

193 F_IMPORT_CLES

TheGreenBow VPN client permet uniquement à l'utilisateur et l'administrateur d'importer des clés cryptographiques pour la mise en œuvre du VPN. Avec des certificats sur token ou dans le certificate store windows, pas d'import de clefs mais appel à une API de signature pour la phase1 par le module IKE. Pour la phase 2 , les clefs de session sont échangées avec la gateway via le protocole IKE en mode protégé. Les clefs sont ensuite transmises aux drivers. Ces clefs de session restent dans la mémoire des modules IKE et drivers.

194 F_PROTECTION_CLES

TheGreenBow VPN client protège les clés secrètes et privées en confidentialité et toutes les clés en intégrité lors de leur import dans l'application VPN cliente.
TheGreenBow VPN client vérifie l'utilisation des clés, y compris la validité des clés utilisées.
Avec des certificats sur token ou dans le certificate store windows, pas d'import de clefs mais appel à une API de signature pour la phase1 par le module IKE. Pour la phase 2 , les clefs de session sont échangées avec la gateway via le protocole IKE en mode protégé. Les clefs sont ensuite transmises aux drivers. Ces clefs de session restent dans la mémoire des modules IKE et drivers.

6.1.3 Gestion des politiques de sécurité VPN

195 F_IMPORT_POL

TheGreenBow VPN client permet uniquement aux administrateurs d'importer les politiques de sécurité VPN et leurs contextes de sécurité.

196 F_PROTECTION_POL

TheGreenBow VPN Client fournit des mécanismes cryptographiques pour protéger les politiques de sécurité VPN en intégrité et confidentialité lors de leur import et de leur export.

6.1.4 Fonctions Cryptographiques

197 F_GENERATION_CLE

TheGreenBow VPN client permet de générer des clés symétriques de chiffrement.
Un algorithme est disponible pour la version certifiée : DH14

198 F_CHIFFREMENT_SYM

TheGreenBow VPN client permet de chiffrer et déchiffrer un flux de données.
Un algorithme est disponible pour la version certifiée : AES

199 F_CHIFFREMENT_ASYM

TheGreenBow VPN client permet de chiffrer et déchiffrer un flux de données.
Un algorithme est disponible : RSA

200 F_SCELLEMENT

TheGreenBow VPN client permet de sceller (hash) un flux de données.
Un algorithme est disponible pour la version certifiée : SHA-2

6.2 Composants logiciels

201 Le logiciel TheGreenBow VPN Client est un programme exécutable sur Windows.

Il est composé de plusieurs modules interconnectés : exécutables, dll (Dynamic Link Library), drivers, service.

6.2.1 Service (TgbStarter)

202 TgbStarter.exe est un programme exécuté en tant que service Windows. Il a pour rôles :

- De vérifier le bon état de marche des autres modules (watchdog), et le cas échéant, de les lancer.
- De répartir les messages échangés entre les modules (p.ex. entre l'interface et IKE)
- D'être le point d'entrée pour tous les accès au fichier de configuration VPN (ce qui permet de s'affranchir des problèmes de droits d'accès au fichier, et d'autoriser ainsi le fonctionnement de l'IHM en mode "utilisateur").

6.2.2 IKE (TgbIKE)

203 TgbIKE.exe est un programme lancé par TgbStarter.exe.

Il gère l'intégralité des protocoles IKE/ISAKMP (ouverture et fermeture d'un tunnel).
Pour ce faire, il s'interface avec différents modules :

- Pour récupérer les éléments de sécurité nécessaires à l'ouverture du tunnel (VpnCfg.dll principalement),
- Pour recevoir les ordres d'ouverture et de fermeture des tunnels, et transmettre les informations pendant l'ouverture d'un tunnel (VpnConf)
- Pour transmettre les informations des tunnels au module chargé d'assurer le tunnel (Drivers)

6.2.3 Drivers

204 Les Drivers sont les modules – dépendants du Système d'Exploitation – qui assurent la réalisation et le maintien du tunnel, une fois celui-ci ouvert (via le protocole IKE/Isakmp assuré par IKE).

6.2.4 IHM (VpnConf)

205 L'IHM (Interface Homme Machine) est un programme lancé depuis le bureau Windows, ou automatiquement après le logon Windows. Il permet de :

- Paramétrer le Fichier de Configuration VPN
- Visualiser graphiquement l'état des tunnels
- Configurer des paramètres qui ne sont pas dans le fichier de configuration mais en registry.
- Lancer les commandes d'ouverture / fermeture des tunnels
- Gérer une éventuelle ligne de commande
- Il assure aussi le processus d'activation du logiciel

6.2.5 Config (VpnCfg)

206 La Dll VpnCfg.dll est utilisée pour tous les accès au fichier de configuration VPN, qu'il se trouve sur le disque dur ou sur clé USB, que ce soit pour des opérations de lecture, écriture, importation ou exportation. La Dll VpnCfg.dll est aussi utilisée pour tous les accès aux medias de type token, smartcard, etc… pour l'exploitation des certificats requis pour l'établissement du tunnel.

6.2.6 Libeay

207 La Dll tgblibeay32.dll est la librairie cryptographique utilisée par la plupart des composants du logiciel. Elle constitue la ressource cryptographique de tous les composants du logiciel, hormis les drivers.

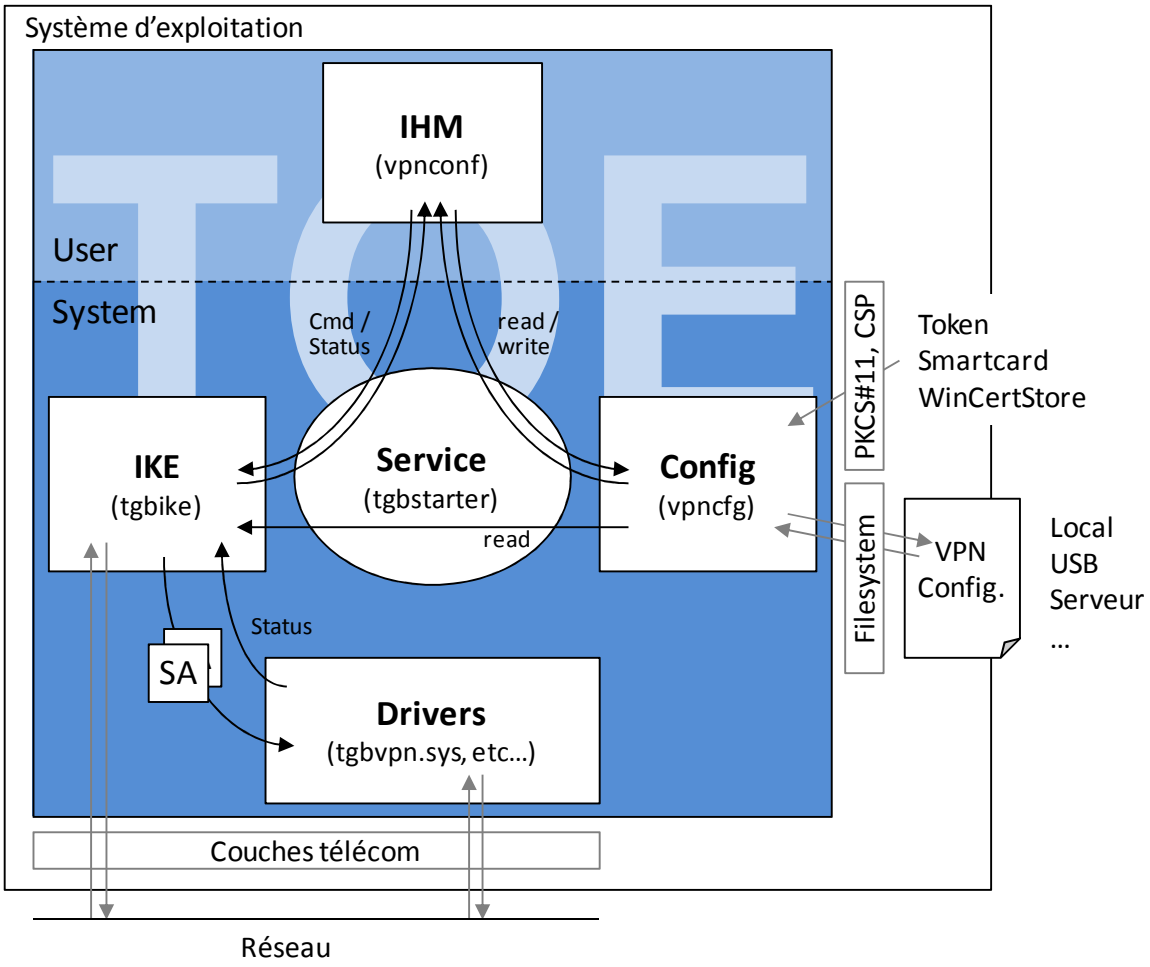
6.2.7 Autres composants

208 Les 2 Dlls complémentaires "comlib.dll" et "tgbconfigmode.dll" concernent respectivement :

1/ Comlib.dll : Communications entre les drivers et le module IKE
2/ tgbconfigmode.dll : Mise à jour de la pile TCP/IP avec les informations reçues de la passerelle VPN via le protocole "Config Mode".

6.3 Communications entre composants

209 Les communications entre les différents composants du logiciel se représentent ainsi :


Système d'exploitation
IHM
(vpnconf)
User
System
TOE
Cmd /
Status
read /
write
IKE
(tgbike)
Service
(tgbstarter)
read
Config
(vpncfg)
PKCS#11, CSP
Token
Smartcard
WinCertStore
Filesystem
VPN
Config.
Local
USB
Serveur
...
Status
SA
Drivers
(tgbvpn.sys, etc...)
Couches télécom
Réseau

7 Argumentaire

7.1 Couverture du problème de sécurité par les objectifs de sécurité

7.1.1 Couverture des menaces

7.1.1.1 Menaces portant sur les communications

210 MENACE : **T.USURPATION_ADMIN**

Pour prévenir la menace :

- la TOE doit imposer l'authentification de l'administrateur au système de chiffrement et vérifier cette authentification, avant d'effectuer toute opération d'administration (O.AUTHENTIFICATION_ADMIN) ;
- l'accès aux différents composants du système de chiffrement doit être restreint grâce à une gestion de clés cryptographiques associée à une politique de sécurité VPN (OE.ACCES) ;

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

- aucune action.

212 Pour réagir à la menace, la TOE doit :

- aucune action.

213 MENACE : **T.USURPATION_UTILISATEUR**

Pour prévenir la menace :

- la TOE doit imposer l'authentification de l'utilisateur au système de chiffrement et vérifier cette authentification, avant d'accéder aux services rendus par la TOE ou d'effectuer toute opération d'administration autorisée aux utilisateurs (O.AUTHENTIFICATION_UTILISATEUR) ;
- l'accès aux différents composants du système de chiffrement doit être restreint grâce à une gestion de clés cryptographiques associée à une politique de sécurité VPN (OE.ACCES) ;

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

- aucune action.

215 Pour réagir à la menace, la TOE doit :

- aucune action.

7.1.1.2 Menaces portant sur la gestion des clés cryptographiques

216 MENACE : **T.MODIFICATION_CLES**

Pour prévenir la menace :

- la TOE doit garantir la protection des clés cryptographiques en intégrité lors de leur stockage (O.PROTECTION_CLES) ;
- la TOE doit authentifier les utilisateurs et administrateurs, afin de pouvoir déterminer leurs droits d'accès (O.AUTHENTIFICATION_UTILISATEUR et O.AUTHENTIFICATION_ADMIN) ;
- la TOE n'autorise que les utilisateurs et administrateurs authentifiés à importer des clés cryptographiques dans la TOE (O.IMPORT_CLES) ;

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

- détecter la perte d'intégrité des clés cryptographiques lors de leur import en local (O.PROTECTION_CLES) ;

218 Pour réagir à la menace, la TOE doit :

- annuler toute opération d'import local de clés cryptographiques dont la perte d'intégrité serait détectée (O.PROTECTION_CLES) ;

219 MENACE : **T.DIVULGATION_CLES**

Pour prévenir la menace :

- la TOE doit garantir la protection en confidentialité des clés lors de leur import en local (O.PROTECTION_CLES) ;
- la TOE doit authentifier les utilisateurs et administrateurs, afin de pouvoir déterminer leurs droits d'accès (O.AUTHENTIFICATION_UTILISATEUR et O.AUTHENTIFICATION_ADMIN) ;
- la TOE doit n'autoriser que les utilisateurs et administrateurs authentifiés à importer des clés cryptographiques dans la TOE (O.IMPORT_CLES) ;
- la TOE doit se prémunir contre l'export des clés hors de la TOE (OE.EXPORT_CLES) ;
- la TOE doit permettre de renouveler régulièrement les clés cryptographiques afin de rendre plus difficile l'utilisation de clés divulguées (O.CRYPTO).

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

- aucune action.

221 Pour réagir à la menace, la TOE doit :

- permettre de se réinitialiser dans un état sûr (OE.REINITIALISATION).

7.1.1.3 Menaces portant sur les politiques de sécurité VPN et leur contexte

222 MENACE : **T.MODIFICATION_POL**

Pour prévenir la menace :

- la TOE doit garantir la protection en intégrité des politiques VPN lors de leur stockage (O.PROTECTION_POL) ;
- la TOE doit authentifier les administrateurs, afin de pouvoir déterminer leurs droits d'accès (O.AUTHENTIFICATION_ADMIN) ;
- la TOE doit autoriser uniquement les administrateurs authentifiés à importer des politiques de sécurité dans la TOE (O.IMPORT_POL) ;

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

- détecter la perte d'intégrité des politiques VPN lors de leur import en local (O.PROTECTION_POL) ;
- rendre possible la détection de toute perte d'intégrité des politiques VPN lors de leur export en local (O.PROTECTION_POL) ;

224 Pour réagir à la menace, la TOE doit :

- annuler toute opération d'import local de politiques VPN dont la perte d'intégrité serait détectée (O.PROTECTION_POL) ;
- permettre de se réinitialiser dans un état sûr (OE.REINITIALISATION).

225 MENACE : **T.DIVULGATION_POL**

Pour prévenir la menace :

- la TOE doit garantir la protection en confidentialité des politiques VPN lors de leur import et leur export en local (O.PROTECTION_POL) ;
- la TOE doit authentifier les administrateurs, afin de pouvoir déterminer leurs droits d'accès (O.AUTHENTIFICATION_ADMIN) ;
- la TOE doit n'autoriser que les administrateurs authentifiés à importer des politiques de sécurité dans la TOE (O.IMPORT_POL) ;

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

- aucune action.

227 Pour réagir à la menace, la TOE doit :

- aucune action.

7.1.2 Couverture des politiques de sécurité organisationnelles (OSP)

7.1.3 Services rendus

228 OSP : **OSP.SERVICES_RENDUS**

Cette OSP est traduite par O.CONFIDENTIALITE_APPLI, O.AUTHENTICITE_APPLI, O.CONFIDENTIALITE_TOPO et O.AUTHENTICITE_TOPO qui imposent que la TOE fournisse les services correspondant de sécurité. Elle est aussi couverte par O.APPLICATION_POL qui impose que ces services de sécurité soient appliqués sur les données transitant sur les liens VPN.

229 De plus, OE.ACCES assure que des clés cryptographiques ont été distribuées (grâce à une gestion de clés) afin de réaliser l'authentification d'origine, requise si la politique de sécurité stipule la protection en authenticité des données transmises sur le lien VPN.

230 Par ailleurs, O.AUTHENTIFICATION_UTILISATEUR assure qu'une politique associée à l'utilisateur (que l'on aura donc authentifié) sera utilisée sur le lien VPN établit. La connaissance de l'identifiant du lien VPN logique est assurée par la configuration de la machine qui ne peut être accédée et modifiée que par un administrateur (OE.DROITS_UTILISATEURS).

231 Enfin, OE.CHIFFREUR_IP participe à cette OSP, car il assure que les opérations concernant le lien VPN sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements. Il permet ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

232

7.1.3.1 Autres services

233 OSP : **OSP.CRYPTO**

Cette OSP est supportée par les objectifs O.CRYPTO (pour la cryptographie utilisée par la TOE) et OE.CRYPTO (pour la cryptographie utilisée par l'environnement de la TOE).

234 OSP : **OSP.EXPORT_POL**

Cette OSP est supportée par O.PROTECTION_POL qui assure que les politiques de sécurité VPN peuvent être exportées vers un administrateur.

7.1.4 Couverture des hypothèses

7.1.4.1 Interactions avec la TOE

235 ASSUMPTION : **A.ADMIN**

Cette hypothèse est supportée par OE.ADMIN qui impose la formation des administrateurs aux tâches qui leur incombent.

236 ASSUMPTION : **A.UTILISATEUR**

Cette hypothèse est supportée par OE.UTILISATEUR qui impose la formation à l'usage de la TOE et la sensibilisation des utilisateurs aux problématiques de sécurité liées à l'utilisation d'un VPN.

237 ASSUMPTION : **A.CHIFFREUR_IP**

Cette hypothèse est entièrement supportée par OE.CHIFFREUR_IP qui impose que le chiffreur IP trace l'activité des liens VPN sur lesquels il communique et remonte toutes les violations des politiques de sécurité VPN vers un administrateur de sécurité afin que celui-ci puisse analyser et traiter les erreurs ou attaques le cas échéant.

7.1.4.2 Machine hôte

238 ASSUMPTION : **A.MACHINE**

Cette hypothèse est entièrement supportée par OE.MACHINE qui assure que la machine hôte est saine, protégée et configurée de manière à garantir sa sécurité et celle des données qu'elle héberge.
De plus cet objectif sur l'environnement assure l'intégrité du logiciel.

239 ASSUMPTION : **A.DROITS_UTILISATEUR**

Cette hypothèse est entièrement supportée par OE.DROITS_UTILISATEURS qui assure que seuls les administrateurs peuvent réaliser les tâches d'administration système.

240 ASSUMPTION : **A.CONFIGURATION**

Cette hypothèse est supportée par OE.CONFIGURATION qui protège des impacts que peuvent avoir les canaux de communication non gérés par la TOE sur les communications sur les liens VPN et par OE.COMM qui garantit que l'environnement peut maîtriser les communications vers et depuis la machine hôte qui ne transitent pas par la TOE.

241 ASSUMPTION : **A.COMM**

Cette hypothèse est supportée par OE.COMM qui assure que toute communication ne passant pas par la TOE peut être maîtrisée par l'environnement de la TOE.

242 ASSUMPTION : **A.EXPORT_CLES**

Cette hypothèse est supportée par OE.EXPORT_CLES qui assure que l'utilisateur ne peut exporter les clés cryptographiques (secrètes et privées) qui sont importées ou générées dans la TOE.

243 ASSUMPTION : **A.MULTI-UTILISATEURS**

Cette hypothèse est entièrement supportée par l'objectif OE.MULTI-UTILISATEURS qui assure que la gestion des identifications/authentifications des différents utilisateurs d'une machine multi-utilisateurs est prise en compte par l'environnement de la TOE.

7.1.4.3 Réinitialisation

244 ASSUMPTION : **A.REINITIALISATION**

Cette hypothèse est entièrement supportée par OE.REINITIALISATION qui assure que la TOE pourra être remise dans un état sûr.

7.1.4.4 Cryptographie

245 ASSUMPTION : **A.ACCES**

Cette hypothèse est entièrement supportée par OE.ACCES qui restreint l'accès aux différents composants du système de chiffrement grâce à une gestion de clés cryptographiques associée à une politique de sécurité VPN.

7.1.5 Tables de couverture

246 Le tableau ci-dessous trace l'association des menaces vers les objectifs de sécurité.

MENACES	OBJECTIFS DE SÉCURITÉ	ARGUMENTAIRE
T.USURPATION_ADMIN	O.AUTHENTIFICATION_ADMIN OE.ACCES	Cf. § 210
T.USURPATION_UTILISATEUR	O.AUTHENTIFICATION_UTILISATEUR OE.ACCES	Cf. § 213

MENACES	OBJECTIFS DE SÉCURITÉ	ARGUMENTAIRE
T.MODIFICATION_CLES	O.PROTECTION_CLES O.AUTHENTIFICATION_UTILISATEUR O.AUTHENTIFICATION_ADMIN O.IMPORT_CLES	Cf. § 216
T.DIVULGATION_CLES	O.PROTECTION_CLES O.AUTHENTIFICATION_UTILISATEUR O.AUTHENTIFICATION_ADMIN O.CRYPTO, O.IMPORT_CLES OE.EXPORT_CLES OE.REINITIALISATION	Cf. § 219
T.MODIFICATION_POL	O.IMPORT_POL O.PROTECTION_POL O.AUTHENTIFICATION_ADMIN OE.REINITIALISATION	Cf. § 222
T.DIVULGATION_POL	O.PROTECTION_POL O.AUTHENTIFICATION_ADMIN O.IMPORT_POL	Cf. § 225

Tableau 4 : Association MENACES vers OBJECTIFS DE SÉCURITÉ

247 Le tableau ci-dessous trace l'association des objectifs de sécurité vers les menaces.

OBJECTIFS DE SÉCURITÉ	MENACES
O.APPLICATION_POL	
O.CONFIDENTIALITE_APPLI	
O.AUTHENTICITE_APPLI	
O.CONFIDENTIALITE_TOPO	
O.AUTHENTICITE_TOPO	
O.AUTHENTIFICATION_ADMIN	T.USURPATION_ADMIN T.MODIFICATION_CLES T.DIVULGATION_CLES T.MODIFICATION_POL T.DIVULGATION_POL
O.AUTHENTIFICATION_UTILISATEUR	T.USURPATION_UTILISATEUR T.MODIFICATION_CLES T.DIVULGATION_CLES
O.IMPORT_CLES	T.MODIFICATION_CLES T.DIVULGATION_CLES
O.PROTECTION_CLES	T.MODIFICATION_CLES T.DIVULGATION_CLES
O.IMPORT_POL	T.MODIFICATION_POL T.DIVULGATION_POL
O.PROTECTION_POL	T.MODIFICATION_POL T.DIVULGATION_POL
O.CRYPTO	T.DIVULGATION_CLES
OE.ADMIN	
OE.UTILISATEUR	
OE.CHIFFREUR_IP	
OE.MACHINE	

OBJECTIFS DE SÉCURITÉ	MENACES
OE.DROITS_UTILISATEURS	
OE.CONFIGURATION	
OE.COMM	
OE.EXPORT_CLES	T.DIVULGATION_CLES
OE.MULTI-UTILISATEURS	
OE.REINITIALISATION	T.DIVULGATION_CLES T.MODIFICATION_POL
OE.CRYPTO	
OE.ACCES	T.USURPATION_ADMIN T.USURPATION_UTILISATEUR

Tableau 5 : Association OBJECTIFS DE SÉCURITÉ vers MENACES

248 Le tableau ci-dessous trace l'association des OSP vers les objectifs de sécurité.

OSP	OBJECTIFS DE SÉCURITÉ	ARGUMENTAIRE
OSP.SERVICES_RENDUS	O.AUTHENTICITE_APPLI O.CONFIDENTIALITE_TOPO O.AUTHENTICITE_TOPO OE.CHIFFREUR_IP O.CONFIDENTIALITE_APPLI O.APPLICATION_POL O.AUTHENTIFICATION_UTILISATEUR OE.DROITS_UTILISATEURS OE.ACCES	Cf. § 228
OSP.CRYPTO	O.CRYPTO OE.CRYPTO	Cf. § 233
OSP.EXPORT_POL	O.PROTECTION_POL	Cf. § 234

Tableau 6 : Association OSP vers OBJECTIFS DE SÉCURITÉ

249 Le tableau ci-dessous trace l'association des objectifs de sécurité vers les OSP.

OBJECTIFS DE SÉCURITÉ	OSP
O.APPLICATION_POL	OSP.SERVICES_RENDUS
O.CONFIDENTIALITE_APPLI	OSP.SERVICES_RENDUS
O.AUTHENTICITE_APPLI	OSP.SERVICES_RENDUS
O.CONFIDENTIALITE_TOPO	OSP.SERVICES_RENDUS
O.AUTHENTICITE_TOPO	OSP.SERVICES_RENDUS
O.AUTHENTIFICATION_ADMIN	
O.AUTHENTIFICATION_UTILISATEUR	OSP.SERVICES_RENDUS
O.IMPORT_CLES	
O.PROTECTION_CLES	
O.IMPORT_POL	
O.PROTECTION_POL	OSP.EXPORT_POL
O.CRYPTO	OSP.CRYPTO
OE.ADMIN	
OE.UTILISATEUR	

OBJECTIFS DE SÉCURITÉ	OSP
OE.CHIFFREUR_IP	OSP.SERVICES_RENDUS
OE.MACHINE	
OE.DROITS_UTILISATEURS	OSP.SERVICES_RENDUS
OE.CONFIGURATION	
OE.COMM	
OE.EXPORT_CLES	
OE.MULTI-UTILISATEURS	
OE.REINITIALISATION	
OE.CRYPTO	OSP.CRYPTO
OE.ACCES	OSP.SERVICES_RENDUS

Tableau 7 : Association OBJECTIFS DE SÉCURITÉ vers OSP

250 Le tableau ci-dessous trace l'association des hypothèses vers les objectifs de sécurité pour l'environnement opérationnel.

HYPOTHÈSES	OBJECTIFS DE SÉCURITÉ (OE.)	ARGUMENTAIRE
A.ADMIN	OE.ADMIN	Cf. § 235
A.UTILISATEUR	OE.UTILISATEUR	Cf. § 236
A.CHIFFREUR_IP	OE.CHIFFREUR_IP	Cf. § 237
A.MACHINE	OE.MACHINE	Cf. § 238
A.DROITS_UTILISATEUR	OE.DROITS_UTILISATEURS	Cf. § 239
A.CONFIGURATION	OE.CONFIGURATION OE.COMM	Cf. § 240
A.COMM	OE.COMM	Cf. § 241
A.EXPORT_CLES	OE.EXPORT_CLES	Cf. § 242
A.MULTI-UTILISATEURS	OE.MULTI-UTILISATEURS	Cf. § 243
A.REINITIALISATION	OE.REINITIALISATION	Cf. § 244
A.ACCES	OE.ACCES	Cf. § 245

Tableau 8 : Association HYPOTHÈSES vers OBJECTIFS DE SÉCURITÉ (OE.)

251 Le tableau ci-dessous trace l'association des objectifs de sécurité pour l'environnement opérationnel vers les hypothèses.

OBJECTIFS DE SÉCURITÉ (OE.)	HYPOTHÈSES
OE.ADMIN	A.ADMIN
OE.UTILISATEUR	A.UTILISATEUR
OE.CHIFFREUR_IP	A.CHIFFREUR_IP
OE.MACHINE	A.MACHINE
OE.DROITS_UTILISATEURS	A.DROITS_UTILISATEURS
OE.CONFIGURATION	A.CONFIGURATION
OE.COMM	A.CONFIGURATION A.COMM
OE.EXPORT_CLES	A.EXPORT_CLES
OE.MULTI-UTILISATEURS	A.MULTI-UTILISATEURS
OE.REINITIALISATION	A.REINITIALISATION

OBJECTIFS DE SÉCURITÉ (OE.)	HYPOTHÈSES
OE.CRYPTO	
OE.ACCES	A.ACCES

Tableau 9 : Association OBJECTIFS DE SÉCURITÉ (OE.) vers HYPOTHÈSES

7.2 Couverture des objectifs de sécurité par les exigences de sécurité

7.2.1 Argumentation

252 **O.APPLICATION_POL**

Cet objectif se traduit par :

- FDP_ETC.1/EXPORT qui assure que les politiques VPN doivent être appliquées sur les données applicatives et topologiques exportées hors de la TOE,
- FDP_ITC.1/IMPORT qui assure que les politiques VPN doivent être appliquées sur les données applicatives et topologiques importées dans la TOE,
- FDP_IFC.1/DATA qui définit la politique de contrôle de flux des trames échangées entre un utilisateur, la TOE et un chiffreur IP,
- FDP_IFF.1/DATA qui
  - spécifie la politique de sécurité VPN à appliquer et autorise l'application de la protection en confidentialité,
  - spécifie la politique de sécurité VPN à appliquer et autorise l'application de la protection en authenticité (i.e. intégrité et authentification d'origine),
  - autorise l'accès aux données (topologiques applicatives) pour application des protections spécifiées dans les politiques de sécurité VPN utilisée et l'envoi sur le lien VPN,
- FDP_IFC.1/KEY_IMPORT qui définit la politique de contrôle de flux des keys,
- FDP_IFF.1/KEY_IMPORT qui assure l'accès aux clés afin d'assurer les protections spécifiées dans les politiques de sécurité VPN,
- FMT_MSA.1/QUERY, FMT_MSA.1/MODIFY, FDP_IFC.1/VPN_POL et FDP_IFF.1/VPN_POL qui assure l'accès aux politiques VPN et à leurs attributs afin qu'elles soient appliquées,
- FDP_ITC.2/VPN_POL qui assure que les politiques de sécurité VPN stockées dans la TOE sont associées à un nom d'utilisateur et un lien VPN,
- FIA_USB.1/USER qui permet de déterminer qu'un utilisateur s'est authentifié comme tel auprès de la TSF et que l'identifiant de cet utilisateur authentifié est connu,
- FMT_MSA.1/QUERY qui autorise l'accès à l'identifiant de l'utilisateur,
- FMT_MSA.3 qui assure que les attributs AT.user_type et AT.user_id sont initialisés par défaut à une valeur restrictive afin de se prémunir contre toute tentative d'outrepassement des mécanismes de sécurité de la TOE.

253 **O.CONFIDENTIALITE_APPLI**

Cet objectif se traduit par :

- FDP_UCT.1/DATA qui assure la confidentialité des données applicatives transitant entre la TOE et le chiffreur IP.

254 **O.AUTHENTICITE_APPLI**

Cet objectif se traduit par :

- FDP_UIT.1/DATA qui assure l'intégrité des données applicatives transitant entre le chiffreur IP et la TOE,
- FCO_NRO.1/DATA qui assure l'authentification d'origine des données applicatives transitant entre la TOE et le chiffreur IP.

255 **O.CONFIDENTIALITE_TOPO**

Cet objectif se traduit par :

- FDP_UCT.1/DATA qui assure la confidentialité des données topologiques transitant entre la TOE et le chiffreur IP.

256 **O.AUTHENTICITE_TOPO**

Cet objectif se traduit par :

- FDP_UIT.1/DATA qui assure l'intégrité des données topologiques transitant entre le chiffreur IP et TOE,
- FCO_NRO.1/DATA qui assure l'authentification d'origine des données topologiques transitant entre la TOE et le chiffreur IP.

257 **O.AUTHENTIFICATION_ADMIN**

Cet objectif se traduit par :

- FIA_UAU.2/ADMIN pour assurer l'authentification de l'administrateur par un composant du système de chiffrement et la vérification de cette authentification avant de permettre la liaison au sujet S.user_manager qui effectue (en particulier) les commandes d'administration (i.e. import et export des biens sensibles de la TOE) (FDP_IFC.1/KEY_IMPORT, FDP_IFF.1/KEY_IMPORT, FDP_IFC.1/VPN_POL et FDP_IFF.1/VPN_POL). Pour être reconnu comme authentifié auprès de la TOE, l'administrateur devra se lier au sujet S.user_manager afin de poser l'attribut AT.user_type à "administrator" (FIA_USB.1/ADMIN). Cet attribut est initialisé par défaut à une valeur restrictive pour se prémunir contre toute tentative d'outrepassement des mécanismes de sécurité de la TOE (FMT_MSA.3), il est modifiable (FMT_MSA.1/MODIFY) et consultable (FMT_MSA.1/QUERY),
- FIA_UID.2/ADMIN, sa dépendance, pour assurer l'identification de l'administrateur qui tente de se lier au sujet cité ci-dessus.

258 **O.AUTHENTIFICATION_UTILISATEUR**

Cet objectif se traduit par :

- FIA_UAU.2/USER pour assurer l'authentification de l'utilisateur par un composant du système de chiffrement et la vérification de cette authentification avant que :
  - l'utilisateur puisse se lier à S.user_manager qui effectue (en particulier) les commandes d'import et d'export des biens sensibles de la TOE (FDP_IFC.1/KEY_IMPORT, FDP_IFF.1/KEY_IMPORT, FDP_IFC.1/DATA, FDP_IFF.1/DATA),
  - la TOE autorise l'établissement de liens VPN (FMT_MSA.1/QUERY permet d'accéder au type d'utilisateur). En effet, l'utilisateur devra se lier au sujet S.user_manager afin de poser l'attribut AT.user_type à "User" (FIA_USB.1/USER) et l'identifiant de l'utilisateur AT.user_id, tous deux modifiables (FMT_MSA.1/MODIFY). Par ailleurs, FMT_MSA.3 assure que AT.user_type et AT.user_id sont initialisés par défaut à une valeur restrictive afin de se prémunir contre toute tentative d'outrepassement des mécanismes de sécurité de la TOE. L'établissement du lien VPN sera alors autorisé (FDP_ETC.1/EXPORT et FDP_ITC.1/IMPORT),
- FIA_UID.2/USER, sa dépendance, pour assurer l'identification de l'utilisateur qui tente de se lier au sujet cité ci-dessus.

259 **O.IMPORT_CLÉS**

Cet objectif se traduit par :

- FDP_ITC.1/KEY_IMPORT qui assure que la politique de sécurité d'import des clés est bien appliquée lors de leur import dans la TOE,
- FDP_IFC.1/KEY_IMPORT qui définit la politique de contrôle de flux pour l'importation de clés dans la TOE,
- FDP_IFF.1/KEY_IMPORT pour :
  - assurer que l'importation de clés dans la TOE n'est possible que par un administrateur ou un utilisateur authentifié comme tel auprès de la TSF (FMT_MSA.1/QUERY et FMT_MSA.1/MODIFY spécifient la gestion de l'attribut user_type qui permet de déterminer s'il s'agit d'un administrateur ou pas),
  - exprimer que seul le sujet S.user_manager peut importer des clés,
- FIA_USB.1/ADMIN qui permet de déterminer qu'un administrateur s'est authentifié comme tel auprès de la TSF,
- FIA_USB.1/USER qui permet de déterminer qu'un utilisateur s'est authentifié comme tel auprès de la TSF,

- FMT_MSA.3 qui assure que l'attribut AT.user_type est initialisé par défaut à une valeur restrictive afin de se prémunir contre toute tentative d'outrepassement des mécanismes de sécurité de la TOE.

260 **O.PROTECTION_CLÉS**

Cet objectif se traduit par :

- FDP_UCT.1/KEY_IMPORT qui assure la confidentialité des clés cryptographiques importées dans la TOE (donc en particulier, lorsqu'elles sont importées localement),
- FDP_UIT.1/KEY_IMPORT qui protège les clés secrètes et de la partie privée des clés asymétriques lors des communications avec les utilisateurs,
- FDP_ITC.1/KEY_IMPORT qui assure la détection de toute perte d'intégrité des clés cryptographiques importées dans la TOE (donc en particulier, lorsqu'elles sont importées localement). Elle assure aussi l'annulation de l'import en cas d'anomalie,
- FDP_IFC.1/DATA et FDP_IFF.1/DATA qui assure que l'intégrité des clés est vérifiée lors de leur utilisation (i.e. leur utilisation pour l'application des propriétés de sécurité aux données envoyées sur le lien VPN); ceci assure ainsi que le stockage les a protégé en intégrité.

261 Par ailleurs, cet objectif est complété par O.IMPORT_CLES qui restreint la possibilité d'importation des clés cryptographiques dans la TOE à l'utilisateur et l'administrateur.

262 **O.IMPORT_POL**

Cet objectif se traduit par :

- FDP_ITC.2/VPN_POL qui assure que la politique de sécurité d'import des politiques VPN est bien appliquée lors de leur import dans la TOE,
- FDP_IFC.1/VPN_POL qui définit la politique de contrôle de flux des trames échangées entre la TOE et un administrateur ou un utilisateur afin de paramétrer les politiques de sécurité utilisées par la TOE,
- FDP_IFF.1/VPN_POL pour :
  - assurer que l'import de politiques de sécurité VPN dans la TOE n'est possible que par un administrateur authentifié comme tel auprès de la TSF (FMT_MSA.1/QUERY permet de déterminer s'il s'agit d'un administrateur),
  - exprimer que seul le sujet S.user_manager peut importer des politiques de sécurité VPN,
- FIA_USB.1/ADMIN qui permet de déterminer qu'un administrateur s'est authentifié comme tel auprès de la TSF,
- FMT_MSA.3 qui assure que l'attribut AT.user_type est initialisé par défaut à une valeur restrictive afin de se prémunir contre toute tentative d'outrepassement des mécanismes de sécurité de la TOE.

263 **O.PROTECTION_POL**

Cet objectif se traduit par :

- FDP_UCT.1/VPN_POL qui assure la confidentialité des politiques de sécurité VPN importées et exportées dans la TOE (donc en particulier, lorsqu'elles sont importées localement),
- FDP_UIT.1/VPN_POL qui assure la détection de toute perte d'intégrité des politiques de sécurité VPN importées et exportées dans la TOE (donc en particulier, lorsqu'elles sont importées localement),
- FDP_IFF.1/DATA qui assure que l'intégrité des politiques de sécurité VPN est vérifiée lors de leur utilisation (i.e. leur application à des données, pour envoi sur le lien VPN); ceci assure ainsi que le stockage les a protégé en intégrité. En réponse, si une perte d'intégrité est détectée, le lien VPN ne pourra pas s'établir,
- FIA_USB.1/ADMIN qui permet de déterminer qu'un administrateur s'est authentifié comme tel auprès de la TSF,
- FMT_MSA.3 qui assure que l'attribut AT.user_type est initialisé par défaut à une valeur restrictive afin de se prémunir contre toute tentative d'outrepassement des mécanismes de sécurité de la TOE,
- FDP_ETC.1/VPN_POL qui assure que l'export n'est autorisé que vers un administrateur authentifié comme tel auprès de la TSF (FMT_MSA.1/QUERY permet de déterminer si l'utilisateur est un administrateur),
- FDP_IFF.1/VPN_POL pour :
  - exprimer que seul le sujet S.user_manager peut exporter des politiques de sécurité VPN,

- exprimer que l'import de politiques de sécurité VPN est soumis à un contrôle d'accès; participant ainsi à la protection en intégrité des politiques de sécurité VPN lors de leur stockage.

264 **O.CRYPTO**

Cet objectif se traduit par :

- FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/SHA-2, qui assurent l'utilisation de fonctions cryptographiques conformes au référentiel cryptographique de l'ANSSI,
- FCS_CKM.1 et FCS_CKM.3 qui assurent que la TOE met en œuvre des mécanismes imposant le renouvellement des clés cryptographiques.

7.2.2 Tables de couverture

265 Le tableau ci-dessous trace l'association des objectifs de sécurité pour la TOE (O.) vers les exigences fonctionnelles de sécurité.

OBJECTIFS DE SÉCURITÉ (O.)	EXIGENCES FONCTIONNELLES	ARGUMENTAIRE
O.APPLICATION_POL	FDP_IFF.1/DATA FMT_MSA.3 FIA_USB.1/USER FDP_ITC.2/VPN_POL FMT_MSA.1/QUERY FDP_IFF.1/KEY_IMPORT FDP_IFF.1/VPN_POL FDP_ETC.1/EXPORT FDP_ITC.1/IMPORT FDP_IFC.1/DATA FDP_IFC.1/VPN_POL FMT_MSA.1/MODIFY FDP_IFC.1/KEY_IMPORT	Cf. § 252
O.CONFIDENTIALITE_APPLI	FDP_UCT.1/DATA	Cf. § 253
O.AUTHENTICITE_APPLI	FDP_UIT.1/DATA FCO_NRO.1/DATA	Cf. § 254
O.CONFIDENTIALITE_TOPO	FDP_UCT.1/DATA	Cf. § 255
O.AUTHENTICITE_TOPO	FDP_UIT.1/DATA FCO_NRO.1/DATA	Cf. § 256
O.AUTHENTIFICATION_ADMIN	FIA_UID.2/ADMIN FIA_UAU.2/ADMIN FDP_IFC.1/KEY_IMPORT FDP_IFC.1/VPN_POL FIA_USB.1/ADMIN FMT_MSA.1/MODIFY FMT_MSA.3 FDP_IFF.1/KEY_IMPORT FMT_MSA.1/QUERY FDP_IFF.1/VPN_POL	Cf. § 257

OBJECTIFS DE SÉCURITÉ (O.)	EXIGENCES FONCTIONNELLES	ARGUMENTAIRE
O.AUTHENTIFICATION_UTILISATEUR	FIA_UID.2/USER FIA_UAU.2/USER FMT_MSA.3 FIA_USB.1/USER FDP_ETC.1/EXPORT FDP_ITC.1/IMPORT FMT_MSA.1/MODIFY FMT_MSA.1/QUERY FDP_IFC.1/DATA FDP_IFF.1/DATA FDP_IFC.1/KEY_IMPORT FDP_IFF.1/KEY_IMPORT	Cf. § 258
O.IMPORT_CLES	FDP_IFF.1/KEY_IMPORT FIA_USB.1/USER FIA_USB.1/ADMIN FMT_MSA.3 FDP_ITC.1/KEY_IMPORT FDP_IFC.1/KEY_IMPORT FMT_MSA.1/QUERY FMT_MSA.1/MODIFY	Cf. § 259
O.PROTECTION_CLES	FDP_UCT.1/KEY_IMPORT FDP_UIT.1/KEY_IMPORT FDP_IFF.1/DATA FDP_IFC.1/DATA FDP_ITC.1/KEY_IMPORT	Cf. § 260
O.IMPORT_POL	FMT_MSA.3 FIA_USB.1/ADMIN FDP_IFF.1/VPN_POL FDP_ITC.2/VPN_POL FDP_IFC.1/VPN_POL FMT_MSA.1/QUERY	Cf. § 262
O.PROTECTION_POL	FDP_UCT.1/VPN_POL FDP_UIT.1/VPN_POL FIA_USB.1/ADMIN FMT_MSA.3 FDP_IFF.1/DATA FDP_IFF.1/VPN_POL FDP_ETC.1/VPN_POL FMT_MSA.1/QUERY	Cf. § 263
O.CRYPTO	FCS_COP.1/AES FCS_COP.1/RSA FCS_COP.1/SHA-2 FCS_CKM.1 FCS_CKM.3	Cf. § 264

Tableau 10 : Association OBJECTIFS DE SÉCURITÉ (O.) vers EXIGENCES FONCTIONNELLES

266 Le tableau ci-dessous trace l'association des exigences fonctionnelles de sécurité vers les objectifs de sécurité pour la TOE (O.).

EXIGENCES FONCTIONNELLES	OBJECTIFS DE SÉCURITÉ (O.)

EXIGENCES FONCTIONNELLES	OBJECTIFS DE SÉCURITÉ (O.)
FDP_ETC.1/EXPORT	O.APPLICATION_POL O.AUTHENTIFICATION_UTILISATEUR
FDP_ITC.1/IMPORT	O.APPLICATION_POL O.AUTHENTIFICATION_UTILISATEUR
FDP_IFC.1/DATA	O.APPLICATION_POL O.PROTECTION_CLES O.AUTHENTIFICATION_UTILISATEUR
FDP_IFF.1/DATA	O.APPLICATION_POL O.PROTECTION_CLES O.PROTECTION_POL O.AUTHENTIFICATION_UTILISATEUR
FDP_UIT.1/DATA	O.AUTHENTICITE_APPLI O.AUTHENTICITE_TOPO
FCO_NRO.1/DATA	O.AUTHENTICITE_APPLI O.AUTHENTICITE_TOPO
FDP_UCT.1/DATA	O.CONFIDENTIALITE_APPLI O.CONFIDENTIALITE_TOPO
FIA_UID.2/USER	O.AUTHENTIFICATION_UTILISATEUR
FIA_UAU.2/USER	O.AUTHENTIFICATION_UTILISATEUR
FIA_USB.1/USER	O.APPLICATION_POL O.AUTHENTIFICATION_UTILISATEUR O.IMPORT_CLES
FIA_UID.2/ADMIN	O.AUTHENTIFICATION_ADMIN
FIA_UAU.2/ADMIN	O.AUTHENTIFICATION_ADMIN
FIA_USB.1/ADMIN	O.AUTHENTIFICATION_ADMIN O.IMPORT_CLES O.IMPORT_POL O.PROTECTION_POL
FMT_MSA.3	O.APPLICATION_POL O.AUTHENTIFICATION_ADMIN O.AUTHENTIFICATION_UTILISATEUR O.IMPORT_CLES O.IMPORT_POL O.PROTECTION_POL
FMT_MSA.1/MODIFY	O.APPLICATION_POL O.AUTHENTIFICATION_ADMIN O.AUTHENTIFICATION_UTILISATEUR O.IMPORT_CLES
FMT_MSA.1/QUERY	O.APPLICATION_POL O.AUTHENTIFICATION_ADMIN O.AUTHENTIFICATION_UTILISATEUR O.IMPORT_CLES O.IMPORT_POL O.PROTECTION_POL
FDP_IFC.1/KEY_IMPORT	O.APPLICATION_POL O.AUTHENTIFICATION_ADMIN O.IMPORT_CLES O.AUTHENTIFICATION_UTILISATEUR

EXIGENCES FONCTIONNELLES	OBJECTIFS DE SÉCURITÉ (O.)
FDP_IFF.1/KEY_IMPORT	O.APPLICATION_POL O.AUTHENTIFICATION_ADMIN O.IMPORT_CLES O.AUTHENTIFICATION_UTILISATEUR
FDP_ITC.1/KEY_IMPORT	O.IMPORT_CLES O.PROTECTION_CLES
FDP_UCT.1/KEY_IMPORT	O.PROTECTION_CLES
FDP_UIT.1/KEY_IMPORT	O.PROTECTION_CLES
FDP_ETC.1/VPN_POL	O.PROTECTION_POL
FDP_ITC.2/VPN_POL	O.APPLICATION_POL O.IMPORT_POL
FDP_UCT.1/VPN_POL	O.PROTECTION_POL
FDP_UIT.1/VPN_POL	O.PROTECTION_POL
FDP_IFC.1/VPN_POL	O.APPLICATION_POL O.AUTHENTIFICATION_ADMIN O.IMPORT_POL
FDP_IFF.1/VPN_POL	O.APPLICATION_POL O.AUTHENTIFICATION_ADMIN O.IMPORT_POL O.PROTECTION_POL
FCS_COP.1/AES	O.CRYPTO
FCS_COP.1/RSA	O.CRYPTO
FCS_COP.1/SHA-2	O.CRYPTO
FCS_CKM.1	O.CRYPTO
FCS_CKM.3	O.CRYPTO

Tableau 11 : Association EXIGENCES FONCTIONNELLES vers OBJECTIFS DE SÉCURITÉ (O.)

7.3 Couverture des exigences de sécurité par les spécifications

7.3.1 Argumentation

267 Les fonctions de sécurité décrites au § 6.1 correspondent par construction aux objectifs de sécurité, de sorte que la couverture des exigences sécurité par les spécifications fonctionnelles est établie par la couverture des objectifs de sécurité par les exigences fonctionnelles montrée au § 7.2 précédent.

7.3.2 Tables de Couverture

268 Le tableau ci-après montre la correspondance entre les fonctions de sécurité et les objectifs de sécurité :

Objectifs	Fonctions
O.APPLICATION_POL	F_APPLICATION_POLITIQUE
O.CONFIDENTIALITE_APPLI	F_CONFIDENTIALITE_APPLI
O.AUTHENTICITE_APPLI	F_INTEGRITE_APPLI
O.CONFIDENTIALITE_TOPO	F_CONFIDENTIALITE_TOPO
O.AUTHENTICITE_TOPO	F_INTEGRITE_TOPO
O.AUTHENTIFICATION_ADMIN	F_AUTHENTIFICATION_ADMIN
O.AUTHENTIFICATION_UTILISATEUR	F_AUTHENTIFICATION_UTILISATEUR
O.IMPORT_CLES	F_IMPORT_CLES
O.PROTECTION_CLES	F_PROTECTION_CLES
O.IMPORT_POL	F_IMPORT_POL
O.PROTECTION_POL	F_PROTECTION_POL
O.CRYPTO	F_GENERATION_CLE
O.CRYPTO	F_CHIFFREMENT_SYM
O.CRYPTO	F_CHIFFREMENT_ASYM
O.CRYPTO	F_SCELLEMENT

Tableau 12 : Association FONCTIONS de SECURITE vers OBJECTIFS DE SÉCURITÉ (O.)

269 Le tableau ci-après montre la couverture des exigences fonctionnelles par les spécifications de sécurité :

Exigences	Fonctions
FDP_ETC.1/EXPORT	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR
FDP_ITC.1/IMPORT	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR
FDP_IFC.1/DATA	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR F_PROTECTION_CLES
FDP_IFF.1/DATA	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR F_PROTECTION_CLES F_PROTECTION_POL
FDP_UIT.1DATA	F_INTEGRITE_APPLI F_INTEGRITE_TOPO F_PROTECTION_REJEU
FCO_NRO.1/DATA	F_INTEGRITE_APPLI F_INTEGRITE_TOPO
FDP_UCT.1/DATA	F_CONFIDENTIALITE_APPLI F_CONFIDENTIALITE_TOPO
FIA_UID.2/USER	F_AUTHENTIFICATION_UTILISATEUR
FIA_UAU.2/USER	F_AUTHENTIFICATION_UTILISATEUR
FIA_USB.1/USER	F_AUTHENTIFICATION_UTILISATEUR F_APPLICATION_POLITIQUE
FIA_UID.2/ADMIN	F_AUTHENTIFICATION_ADMIN

FIA_UAU.2/ADMIN	F_AUTHENTIFICATION_ADMIN
FIA_USB.1/ADMIN	F_AUTHENTIFICATION_ADMIN F_IMPORT_CLES F_IMPORT_POL F_PROTECTION_POL
FMT_MSA.3	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_ADMIN F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES F_IMPORT_POL F_PROTECTION_POL
FMT_MSA.1/MODIFY	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_ADMIN F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES
FMT_MSA.1/QUERY	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_ADMIN F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES F_IMPORT_POL F_PROTECTION_POL
FDP_IFC.1/KEY_IMPORT	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_ADMIN F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES
FDP_IFF.1/KEY_IMPORT	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_ADMIN F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES
FDP_ITC.1/KEY_IMPORT	F_IMPORT_CLES F_PROTECTION_CLES
FDP_UTC.1/KEY_IMPORT	F_PROTECTION_CLES F_PROTECTION_FLUX_ADMIN
FDP_UIT.1/KEY_IMPORT	F_PROTECTION_CLES F_PROTECTION_FLUX_ADMIN
FDP_ETC.1/VPN_POL	F_PROTECTION_POL
FDP_ITC.2/VPN_POL	F_APPLICATION_POLITIQUE F_IMPORT_POL
FDP_UCT.1/VPN_POL	F_PROTECTION_POL F_PROTECTION_FLUX_ADMIN
FDP_UIT.1/VPN_POL	F_PROTECTION_POL F_PROTECTION_REJEU F_PROTECTION_FLUX_ADMIN
FDP_IFC.1/VPN_POL	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_ADMIN
FDP_IFF.1/VPN_POL	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_ADMIN F_IMPORT_POL F_PROTECTION_POL
FCS_CKM.1	F_GENERATION_CLE

FCS_CKM.3	F_GENERATION_CLE
FCS_COP.1/AES	F_CHIFFREMENT_SYM
FCS_COP.1/RSA	F_CHIFFREMENT_ASYM
FCS_COP.1/SHA-2	F_SCELLEMENT

Tableau 13 : Association FONCTIONS de SECURITE vers EXIGENCES FONCTIONNELLES

7.4 Dépendances

7.4.1 Dépendances des exigences de sécurité fonctionnelles

270 Le tableau ci-dessous présente les dépendances des exigences de sécurité fonctionnelles qui sont satisfaites.

EXIGENCES	DÉPENDANCES CC	DÉPENDANCES SATISFAITES
FMT_MSA.3	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/MODIFY
FMT_MSA.1/MODIFY	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/DATA
FMT_MSA.1/QUERY	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_IFC.1/DATA
FDP_IFC.1/VPN_POL	(FDP_IFF.1)	FDP_IFF.1/VPN_POL
FDP_IFF.1/VPN_POL	(FDP_IFC.1) et (FMT_MSA.3)	FMT_MSA.3 FDP_IFC.1/VPN_POL
FCS_COP.1	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)	FDP_ITC.1/KEY_IMPORT
FCS_CKM.1	(FCS_CKM.2 ou FCS_COP.1) et (FCS_CKM.4)	FCS_COP.1
FCS_CKM.3	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.1/KEY_IMPORT
FDP_ETC.1/EXPORT	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/DATA
FDP_ITC.1/IMPORT	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FMT_MSA.3 FDP_IFC.1/DATA
FDP_IFC.1/DATA	(FDP_IFF.1)	FDP_IFF.1/DATA
FDP_IFF.1/DATA	(FDP_IFC.1) et (FMT_MSA.3)	FMT_MSA.3 FDP_IFC.1/DATA
FDP_UIT.1/DATA	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/VPN_POL
FCO_NRO.1/DATA	(FIA_UID.1)	
FDP_UCT.1/DATA	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/VPN_POL
FIA_UID.2/USER	Pas de dépendance	
FIA_UAU.2/USER	(FIA_UID.1)	FIA_UID.2/USER
FIA_USB.1/USER	(FIA_ATD.1)	
FIA_UID.2/ADMIN	Pas de dépendance	
FIA_UAU.2/ADMIN	(FIA_UID.1)	FIA_UID.2/ADMIN
FIA_USB.1/ADMIN	(FIA_ATD.1)	
FDP_IFC.1/KEY_IMPORT	(FDP_IFF.1)	FDP_IFF.1/KEY_IMPORT
FDP_IFF.1/KEY_IMPORT	(FDP_IFC.1) et (FMT_MSA.3)	FMT_MSA.3 FDP_IFC.1/KEY_IMPORT

EXIGENCES	DÉPENDANCES CC	DÉPENDANCES SATISFAITES
FDP_ITC.1/KEY_IMPORT	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/KEY_IMPORT
FDP_UCT.1/KEY_IMPORT	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/KEY_IMPORT
FDP_UIT.1/KEY_IMPORT	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/KEY_IMPORT
FDP_ETC.1/VPN_POL	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/VPN_POL
FDP_ITC.2/VPN_POL	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/VPN_POL
FDP_UCT.1/VPN_POL	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/VPN_POL
FDP_UIT.1/VPN_POL	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/VPN_POL

Tableau 14 : Dépendances satisfaites des exigences de sécurité fonctionnelles

271 L'argumentaire des dépendances des exigences de sécurité fonctionnelles qui ne sont pas supportées est le suivant :

- **La dépendance FMT_SMR.1 de FMT_MSA.3 n'est pas supportée**. Les rôles sont définis par la valeur de l'attribut AT.user_type du sujet S.user_manager.
- **La dépendance FMT_SMR.1 de FMT_MSA.1/MODIFY n'est pas supportée.** Les rôles sont définis par la valeur de l'attribut AT.user_type du sujet S.user_manager.
- **La dépendance FMT_SMF.1 de FMT_MSA.1/MODIFY n'est pas supportée.** Dans le modèle, il n'y a pas de fonction spécifique de management des attributs.
- **La dépendance FMT_SMR.1 de FMT_MSA.1/QUERY n'est pas supportée.** Les rôles sont définis par la valeur de l'attribut AT.user_type du sujet S.user_manager.
- **La dépendance FMT_SMF.1 de FMT_MSA.1/QUERY n'est pas supportée.** Dans le modèle, il n'y a pas de fonction spécifique de management des attributs.
- **La dépendance FCS_CKM.4 de FCS_COP.1 n'est pas supportée.** Cette dépendance n'est pas applicable puisque la destruction des clés n'entre pas dans le périmètre de la TOE.
- **La dépendance FCS_CKM.4 de FCS_CKM.1 n'est pas supportée.** Cette dépendance n'est pas applicable puisque la destruction des clés n'entre pas dans le périmètre de la TOE.
- **La dépendance FCS_CKM.4 de FCS_CKM.3 n'est pas supportée.** Cette dépendance n'est pas applicable puisque la destruction des clés n'entre pas dans le périmètre de la TOE.
- **La dépendance FTP_ITC.1 ou FTP_TRP.1 de FDP_UIT.1/DATA n'est pas supportée.** Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.
- **La dépendance FIA_UID.1 de FCO_NRO.1/DATA n'est pas supportée.** Cette dépendance n'est pas requise car l'authentification d'origine des trames émises et reçues par la TOE est indépendante de l'identification des utilisateurs ("user" et "administrator").
  Par ailleurs l'utilisation de la TOE n'est pas subordonnée à l'identification de la TOE et du chiffreur.
- **La dépendance FTP_ITC.1 ou FTP_TRP.1 de FDP_UCT.1/DATA n'est pas supportée.** Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.
- **La dépendance FIA_ATD.1 de FIA_USB.1/USER n'est pas supportée.** Cette dépendance n'est pas requise puisque les attributs de sécurité associés aux utilisateurs sont maintenus par le sujet S.user_manager.
- **La dépendance FIA_ATD.1 de FIA_USB.1/ADMIN n'est pas supportée.** Cette dépendance n'est pas requise puisque les attributs de sécurité associés aux utilisateurs sont maintenus par le sujet S.user_manager.

- **La dépendance FMT_MSA.3 de FDP_ITC.1/KEY_IMPORT n'est pas supportée.** Cette dépendance n'est pas applicable puisque OB.keys n'utilise pas d'attributs.
- **La dépendance FTP_ITC.1 ou FTP_TRP.1 de FDP_UCT.1/KEY_IMPORT n'est pas supportée.** Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.
- **La dépendance FTP_ITC.1 ou FTP_TRP.1 de FDP_UIT.1/KEY_IMPORT n'est pas supportée.** Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.
- **La dépendance FPT_TDC.1 de FDP_ITC.2/VPN_POL n'est pas supportée.** Cette dépendance n'est pas applicable car l'administrateur qui importe les politiques de sécurité est de confiance et formate celles-ci de manière à être interprétées correctement par la TOE.
- **La dépendance FTP_ITC.1 ou FTP_TRP.1 de FDP_ITC.2/VPN_POL n'est pas supportée.** Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.
- **La dépendance FTP_ITC.1 ou FTP_TRP.1 de FDP_UCT.1/VPN_POL n'est pas supportée.** Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.
- **La dépendance FTP_ITC.1 ou FTP_TRP.1 de FDP_UIT.1/VPN_POL n'est pas supportée.** Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées

7.4.2 Dépendances des exigences de sécurité d'assurance

272 Le tableau ci-dessous présente les dépendances des exigences d'assurance qui sont satisfaites.

EXIGENCES	DÉPENDANCES CC	DÉPENDANCES SATISFAITES
ADV_ARC.1	(ADV_FSP.1) et (ADV_TDS.1)	ADV_FSP.3 ADV_TDS.2
ADV_FSP.3	(ADV_TDS.1)	ADV_TDS.2
ADV_TDS.2	(ADV_FSP.3)	ADV_FSP.3
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.3
AGD_PRE.1	Pas de dépendance	
ALC_CMC.3	(ALC_CMS.1) et (ALC_DVS.1) et (ALC_LCD.1)	ALC_CMS.3 ALC_DVS.1 ALC_LCD.1
ALC_CMS.3	Pas de dépendance	
ALC_DEL.1	Pas de dépendance	
ALC_DVS.1	Pas de dépendance	
ALC_FLR.3	Pas de dépendance	
ALC_LCD.1	Pas de dépendance	
ASE_CCL.1	(ASE_ECD.1) et (ASE_INT.1) et (ASE_REQ.1)	ASE_ECD.1 ASE_INT.1 ASE_REQ.2
ASE_ECD.1	Pas de dépendance	
ASE_INT.1	Pas de dépendance	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) et (ASE_OBJ.2)	ASE_ECD.1 ASE_OBJ.2
ASE_SPD.1	Pas de dépendance	

EXIGENCES	DÉPENDANCES CC	DÉPENDANCES SATISFAITES
ASE_TSS.1	(ADV_FSP.1) et (ASE_INT.1) et (ASE_REQ.1)	ADV_FSP.3 ASE_INT.1 ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) et (ATE_FUN.1)	ADV_FSP.3 ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) et (ADV_TDS.2) et (ATE_FUN.1)	ADV_ARC.1 ADV_TDS.2 ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) et (AGD_OPE.1) et (AGD_PRE.1) et (ATE_COV.1) et (ATE_FUN.1)	ADV_FSP.3 AGD_OPE.1 AGD_PRE.1 ATE_COV.2 ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) et (ADV_FSP.4) et (ADV_IMP.1) et (ADV_TDS.3) et (AGD_OPE.1) et (AGD_PRE.1) et (ATE_DPT.1)	ADV_ARC.1 ADV_FSP.3 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1 (ADV_TDS.2)

Tableau 15 : Dépendances satisfaites des exigences de sécurité d'assurance

273 L'argumentaire des dépendances des exigences de sécurité d'assurance qui ne sont pas supportées est le suivant :

- **La dépendance ADV_IMP.1 de AVA_VAN.3 n'est pas supportée.** Cette dépendance n'est pas nécessaire conformément à l'EAL requis pour la qualification standard [QUA-STD].
- **La dépendance ADV_TDS.3 de AVA_VAN.3 n'est pas supportée.** Cette dépendance n'est pas nécessaire conformément à l'EAL requis pour la qualification standard [QUA-STD]. Le composant ADV_TDS.2 est retenu.
- **La dépendance ADV_FSP.4 de AVA_VAN.3 n'est pas supportée.** Cette dépendance n'est pas nécessaire conformément à l'EAL requis pour la qualification standard [QUA-STD].

7.5 Argumentaire pour l'EAL

274 Le niveau d'assurance de l'évaluation de ce profil de protection est EAL3 augmenté de ALC_FLR.3 et AVA_VAN.3 conformément au processus de qualification de niveau standard défini dans [QUA-STD].

7.6 Argumentaire pour les augmentations à l'EAL

7.6.1 AVA_VAN.3 'Focused vulnerability analysis'

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

7.6.2 ALC_FLR.3 'Systematic flaw remediation'

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

7.7 Annexe – Plateforme évaluée

La plate forme de test TheGrrenBow est réalisée en machines virtuelles.
Elle se compose d'une partie cliente, d'une gateway Strongswan, d'un hôte distant et éventuellement d'un routeur entre la partie client et la gateway. Pour les tests qui le nécessitent, le token feitian epass 2003 et son middleware sont installés sur le poste client.

Plateforme Tests à réaliser sans NAT-T :
Description partie cliente :
OS : Windows XP 32 bits, Windows 7 32/64 Bits
Configuration réseau : Une interface ethernet configurée en mode bridgé qui sert à monter les tunnels
Le client VPN a qualifier est installé sur cette machine virtuelle.

Descritpion Gateway Strongswan :
OS : debian 7 (Wheezy) 64 Bits
Strongswan : Linux strongswan U5.0.4/K3.2.0.4-amd64
Configuration réseau : 2 interfaces ethernet
eth0 == bridgée
eth1 == wmnet6 (Host Only)
Interface utilisée pour monter les tunnels : eth0

Description Hôte distant :
OS : Windows XP 32 bits, Windows 7 32/64 Bits
Configuration réseau : Une interface ethernet configurée en mode Host Only sur WMNet6.
Particularitée : doit répondre aux pongs et permettre le transfert de fichier

Plateforme Tests à réaliser avec NAT-T :
Description partie cliente :
OS : Windows XP 32 bits, Windows 7 32/64 Bits
Configuration réseau : Une interface ethernet configurée en mode bridgé qui sert à monter les tunnels
Le client VPN a qualifier est installé sur cette machine virtuelle.
Particularité : mettre la route par défaut vers l'adresse du routeur debian

Description routeur :
OS : Debian 7 (Wheezy) 64 bits
Configuration réseau : 2 interfaces ethernet
eth0 == bridgée
eth1 == wmnet1 (Host Only)

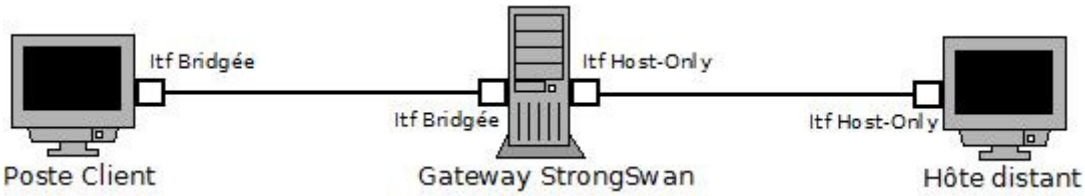
Descritpion Gateway Strongswan :
OS : debian 7 (Wheezy) 64 Bits
Strongswan : Linux strongswan U5.0.4/K3.2.0.4-amd64
Configuration réseau : 2 interfaces ethernet
eth0 == wmnet1 (Host Only)
eth1 == wmnet6 (Host Only)
Interface utilisée pour monter les tunnels : eth0

Description Hôte distant :
OS : Windows XP 32 bits, Windows 7 32/64 Bits
Configuration réseau : Une interface ethernet configurée en mode Host Only sur WMNet6.

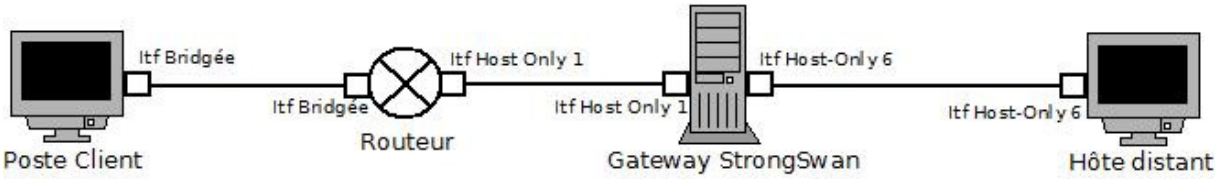
Particularité : doit répondre aux pings et permettre le transfert de fichier

Schémas d'architecture :

Sans NAT-T :



Avec NAT-T :



--- FIN DU DOCUMENT ---