THEGREENBOW

Référence doc : tgbvlx_CDS_CC
Version doc : 3.5 – 05/02//2021
Version VPN : TheGreenBow VPN linux Certified

TheGreenBow
VPN Linux Certified

Cible de Sécurité
Evaluation Critères Communs

Historique

Date	Version	Description	Auteur
18/01/2017	0.1	Création	JC
19/02/2017	0.2	Version de travail interne	JC
24/04/2017	0.3	Version de travail inerne	JC
09/05/2017	0.4	Corrections diverses suite à échanges Sponsor et ANSSI	JC
31/10/2017	0.5	- Précisions sur le périmètre de la cible - Suppression d'une cible (TOE4) envisagée à la version précédente - Ajout menace T.INTERCEPTION - Précision et correction sur gestion de clés	JC
28/02/12018	0.6	Version de travail interne	JC
16/03/2018	0.7	Version de travail interne	JC
19/03/2018	0.8	- Correction références documentaires - Correction OS cibles - Précision algorithmes cryptographiques et gestion des clés - Précisions fonctionnelles, précision sur le logiciel et sa protection - précision sur mécanismes anti-rejeu	JC
13/06/2018	0.9	- précision sur couche IPsec/ESP et non-adhérence au matériel	JC
22/11/2018	1.0	Corrections suite au RTI_ASE v1.0 [OUT.001] et suite à retour ANSSI/CCN (version présentée à la RE0) - précision sur périmètre CDS inclut drivers - précision sur rôle administrateur, mode d'administration - précisions et corrections sur la gestion de configuration - précision sur CDS vs PP - précision sur gestion des clés - correction sur fonction intégrité du logiciel	JC/LF/OM
08/08/2019	1.1	- Corrections suite au RTI_ASE v1.1 [OUT.003] - Corrections points cryptographiques suite à rédaction fourniture crypto - Ajout de l'historique du document	JC
09/08/2019	1.2	- Corrections diverses, échange OPPIDA	JC
17/09/2019	1.3	- Précision sur périmètre de la TOE, précision sur contrôle d'intégrité, mise jour versions documents	JC
07/10/2019	1.4	Modification du numéro de version de la TOE	JC
21/10/2019	1.5	Correction version document et modification version TOE 1.4.0	JC
07/11/2019	1.6	Correction version document et modification version TOE 1.4.1	JC
15/11/2019	1.7	Correction version document	JC
02/12/2019	1.8	Correction version document (livraison TOE 1.4.2)	JC
04/12/2019	1.9	Correction version document	JC
20/12/2019	2.0	Correction suite à revue ANSSI 15	JC
13/01/2020	2.1	Correction version document	JC
16/01/2020	2.2	Correction version document	JC
14/04/2020	3.0	Nouvelle version pour ré-évaluation TOE 1.5.0	JC
02/07/2020	3.1	Précision sur hypothèse A_CLES_PRIVEES	JC
21/08/2020	3.2	Correction suite à remarques ANSSI	MM
13/10/2020	3.3	Ajout ECDSA	JC
02/11/2020	3.4	Correction RSASSA-PKCS1-v1_5	MM
05/02/2021	3.5	Correction F_CHIFFREMENT_ASYM	JC

Table des matières

TABLE DES FIGURES

TABLE DES TABLEAUX

RÉFÉRENCES 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 April 2017 - Version 3.1, Revision 5 - CCMB-2017-04-001
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017 - Version 3.1, Revision 5 - CCMB-2017-04-002
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017 - Version 3.1, Revision 5 - CCMB-2017-04-003
[RGS_B1]	RGS V2.0, Annexe B1. Mécanismes de cryptographie : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques V2.03
[RGS_B2]	RGS V2.0, Annexe B2. Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques V2.0
[RGS_B3]	RGS V2.0, Annexe B3. Règles et recommandations concernant les mécanismes d'authentification (1)
[ANSSI_IPSEC]	Recommandations de sécurité relatives à IPsec (Réf. DAT-NT-003/ANSSI/SDE version 1.1, 3 août 2015)
[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
[CDS_VLX_2020]	Cible de Sécurité du Client VPN Linux Certified (Client VPN Linux 1.4.2)
[GUIDE_DGAMI]	2005/102317 / CELAR/SSI/SSY/EA / 51703616/NC V2. Recommandations pour la sécurisation des distributions GNU/Linux Redhat et Mandrake
[ANSSI_LINUX1]	Recommandations de configuration d'un système GNU/Linux DAT-NT-28/ANSSI/SDE/NP, 12 janvier 2016
[ANSSI_LINUX2]	Recommandations de sécurité relatives à un système GNU/Linux Réf. DAT-NT-002/ANSSI/SDE/NP, 27 juillet 2012
[SPEC_CRYPTO]	Spécifications cryptographiques TheGreenBow VPN Linux Certified

ABRÉVIATIONS

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 / Evaluation Critères Communs / TheGreenBow VPN Certified
Référence	tgbvlx_CDS-CC
Version	V3.5
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 les cibles à évaluer (TOE) couvertes par la présente CDS.

4

Nom de la TOE	Application VPN cliente : TheGreenBow VPN Linux
Type de produit	Logiciel de communication sécurisée
Référence de la TOE	TheGreenBow VPN Linux ELinOS
Version de la TOE	TheGreenBow VPN Linux Certified, version 1.5.0
Émetteur	THEGREENBOW

Nom de la TOE	Application VPN cliente : TheGreenBow VPN Linux
Type de produit	Logiciel de communication sécurisée
Référence de la TOE	TheGreenBow VPN Linux Red Hat
Version de la TOE	TheGreenBow VPN Linux Certified, version 1.5.0
Émetteur	THEGREENBOW

Tableau 2 : Références des TOEs

1.3 Type de TOE

5 Le type de TOE considéré est une application logicielle apportant la fonction de Client VPN à des machines embarquées, fixes ou itinérantes s'exécutant sur toute plateforme Linux ElinOS 6.1 64 bits, RedHat Enterprise Linux 7 64 bits.

6 Le driver IPsec du noyau Linux sur lequel est installé le logiciel est inclus dans le périmètre de la TOE.

7 Les plateformes utilisées pour les tests d'évaluation sont décrites en annexe de la présente CDS.

1.4 Utilisation de la TOE

8 Dans le cadre de la présente CDS, TheGreenBow VPN Linux est un logiciel VPN IPsec IKEv2 conçu et utilisé pour assurer la sécurité des communications entre un équipement mobile ou nomade et une station fixe d'une part, entre deux équipements mobiles d'autre part.

Le logiciel TheGreenBow VPN Linux est ainsi mis en œuvre de deux façons :
1/ VPN Client en environnement embarqué
2/ VPN Client sur poste nomade, fonctionnant en mode serveur VPN
Les différents cas d'usage sont illustrés et détaillés au chapitre 1.6 Fig.1 ci-dessous.
A noter que le logiciel TheGreenBow VPN Linux permet l'ouverture simultanée de plusieurs tunnels VPN.

9 Le logiciel TheGreenBow VPN Linux s'appuie sur un logiciel opensource VPN Strongswan et implémente en standard les protocoles IKEv1, IKEv2. Toutefois, dans le cadre de la présente CDS, seul le protocole IKEv2 est mis en œuvre, conformément à R8 de [ANSSI_IPSEC].

10 En standard, le logiciel TheGreenBow VPN Linux permet d'établir des associations de sécurité sur la base de mécanismes d'authentification variés : clé partagée, EAP, utilisation de certificats aux formats X509, PKCS12 ou PEM. Dans le cadre de la présente CDS, seule l'authentification par certificat est considérée dans la TOE, conformément à [RGS_B2]. A noter que le mode EAP est exclu du logiciel.

11 Le logiciel TheGreenBow VPN Linux est fourni sous la forme d'un package, contenant les binaires issus du code source, de l'environnement de développement et des options de compilations maîtrisés par TheGreenBow à l'exception du composant IPsec issu du noyau Linux.

1.5 Limites de la TOE

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

- IKEv2 avec les algorithmes :
  - AES CBC 128/192/256 avec PRF et HMAC SHA2 256/384/512
  - AES CTR 128/192/256 avec PRF et HMAC SHA2 256/384/512
  - AES GCM 128/192/256 avec ICV16
  - DH groupes 14, 15, 16, 17, 18, 19, 20, 21
  - PFS avec les groupes DH14, 15, 16, 17, 18, 19, 20, 21
- ESP en mode "tunnel" configuré en mode "encrypt then Mac" avec les algorithmes :
  - AES CBC 128/192/256 avec HMAC SHA2 256/384/512
  - AES CTR 128/192/256 avec HMAC SHA2 256/384/512
  - AES GCM 128/192/256 avec ICV16
  - PFS avec les groupes DH14, 15, 16, 17, 18, 19, 20, 21

13 Les politiques de sécurité VPN mises en œuvre par la TOE opèrent des clés cryptographiques générées à l'intérieur de la TOE (typiquement les clés de chiffrement des tunnels VPN) et d'autres qui sont utilisées, générées à l'extérieur de la TOE (typiquement les clés privées issues des certificats utilisateurs).

14 La TOE génère des événements d'audit sur la machine hôte, mais ne fournit aucune fonction d'exploitation de ces événements d'audit. Les événements d'audit générés par la TOE sur la machine hôte ne contiennent pas d'éléments sensibles.

15 Le logiciel TheGreenBow VPN Linux propose un grand nombre de possibilités de configuration et d'options. Toutefois, sur l'ensemble de ces possibilités,

- certaines ne font pas partie de la TOE,
- certaines sont configurées ou forcées par défaut dans le logiciel, tel qu'il est livré en standard,
- et enfin, certaines font l'objet de recommandations de sécurité dans les guides utilisateur et administrateur.

16 Le tableau ci-dessous identifie les fonctions principales de l'application TheGreenBow VPN Linux et précise le périmètre de la présente CDS :

Fonctions	CDS	Commentaire
Protocoles		
IKEv1 / IPsec	Hors CDS	Ce mode n'est pas recommandé en "mode certifié"
IKEv2 / IPsec	Dans CDS	Dans le cadre de cette cible, la couche IPsec (protocole ESP) est celle du noyau Linux sur lequel la TOE est installée.
SSL / TLS	Hors CDS	La TOE n'implémente pas cette fonction
Gestion de configuration VPN		
Protection de l'accès à la politique de sécurité VPN	Hors CDS	La TOE n'implémente pas cette fonction
Import de la politique de sécurité VPN	Dans CDS	La fonction d'import est réduite à la lecture par la TOE de la politique de sécurité VPN. La TOE n'implémente pas de fonction d'import de configuration pour l'administrateur ou l'utilisateur.
Export de la politique de sécurité VPN	Hors CDS	La TOE n'implémente pas cette fonction
Gestion centralisée des politiques de sécurité VPN, téléadministration	Hors CDS	La TOE n'implémente pas cette fonction
Mécanismes d'authentification		
Clé partagée (PSK)	Hors CDS	Ce mode n'est pas recommandé en "mode certifié".
EAP	Hors CDS	La TOE n'implémente pas cette fonction
X509	Dans CDS	En "mode certifié" il est recommandé d'utiliser RSA avec une clé d'une longueur supérieure ou égale à 2048 bits (schéma RSASSA-PKCS1-v1_5) ou ECDSA
Authentification du certificat passerelle	Dans CDS	
Algorithmes		
Algorithmes cryptographiques	Dans CDS	Tous les algorithmes cryptographiques sont disponibles dans la TOE. toutefois 1/ la TOE est livrée avec une configuration en mode certifié 2/ un ensemble de recommandations sont faites dans les guides utilisateur et administrateur
Réseau		
Mode CP (Configuration Payload) (fourniture d'informations topologiques par le serveur VPN)	Dans CDS	Ce mode est configurable dans la TOE. toutefois 1/ la TOE est livrée avec ce mode positionné par défaut 2/ ce mode est recommandé dans les guides utilisateur et administrateur
Contrôle des flux non chiffrés	Hors CDS	Le contrôle du flux lorsque le tunnel n'est pas monté, ou - a fortiori - lorsque le logiciel ne fonctionne pas, n'est pas réalisé par le logiciel VPN mais via les règles/contraintes du système qui l'héberge (avec des règles de filtrage IP par exemple, du type "ne laisser passer que les ports 500 et 4500"). Cette configuration du système est de la responsabilité de l'administrateur du système.
Fonctions diverses		
Génération de logs	Dans CDS	
Mode "VPN Point à point"	Dans CDS	Ce mode est aussi identifié par le mode "serveur" pour la TOE

1.6 Intégration de la TOE dans son environnement

17 La présente Cible porte sur deux TOEs : TheGreenBow VPN Linux ELinOS et TheGreenBow VPN Linux Red Hat.

18 Ces deux TOEs sont des applications Client VPN Linux qui permettent d'établir un tunnel VPN IPsec avec Chiffreur IP ou entre elles (Cf. Figure 1). Dans le cas ou le tunnel IPsec est créé entre les deux TOEs, l'une des deux TOE est initiatrice de la connexion VPN, l'autre se comporte en mode serveur VPN.

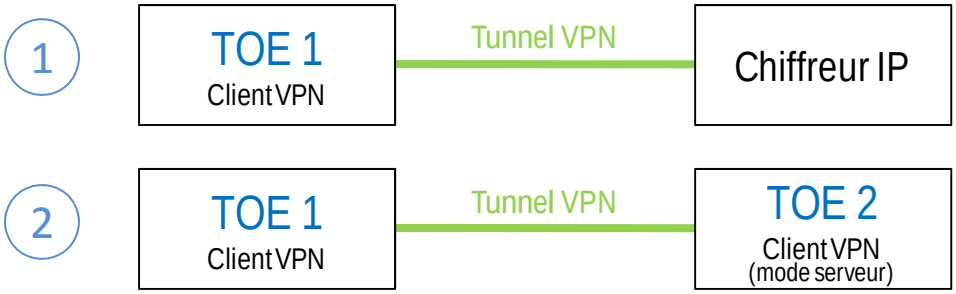


Figure 1 : Environnement d'exploitation de la TOE

19 La TOE objet de cette cible n'est pas utilisée par un utilisateur humain mais par un processus exécuté sur la machine hôte de la TOE. Ce processus a en charge le lancement de la TOE et le déclenchement de l'ouverture du tunnel. Ce rôle Utilisateur est décrit au chapitre 3.2 "Rôles".

20 Deux phases sont 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 effectivement utilisée.

1.6.1 Phase d'initialisation

21 Le logiciel TheGreenBow VPN Linux est fourni dans un installeur packagé qui peut être exécuté par lancement direct ou par ligne de commande.

22 Le package d'installation est fourni pour installer le logiciel en mode certifié, c'est-à-dire que l'ensemble des paramètres configurant le logiciel en mode certifié sont préconfigurés dans ce package. Les éléments de sécurité quant à eux (clés privées, certificats, autres clés) ne font pas partie de l'installeur. Leur configuration reste du ressort de l'administrateur de sécurité (Cf chapitre 3.3).

23 Le package d'installation est fourni signé de façon à permettre à l'Administrateur de vérifier son intégrité avant installation.

1.6.2 Phase opérationnelle

24 Le logiciel TheGreenBow VPN Linux fonctionne dans les environnements Linux ElinOS 6.1 64 bits, RedHat Enterprise Linux 7 64 bits. Les OS sont sécurisés.

25 Le logiciel TheGreenBow VPN Linux permet d'assurer la sécurité des connexions, à la fois en terme de confidentialité via le chiffrement des connexions IPsec et d'intégrité via les mécanismes de hashage IPsec, et en terme d'authentification via les mécanismes IKE et la possibilité d'utiliser des moyens d'authentification forte.

1.6.3 Mode d'administration

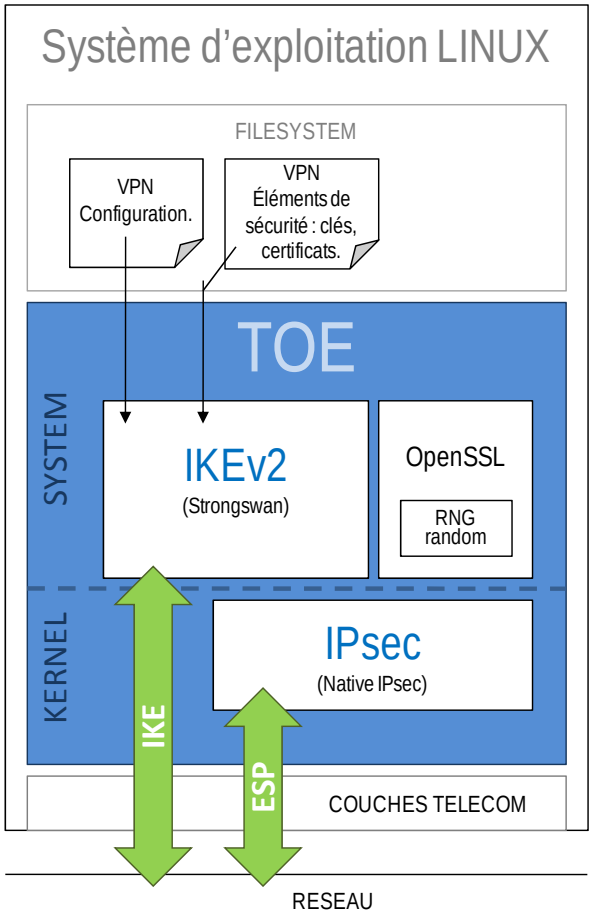
26 Le logiciel TheGreenBow VPN Linux n'implémente pas d'administration à distance (télé-administration), donc la TOE ne comporte pas d'interface d'administration distante (type télégestion) pour la mise à jour des politiques VPN

27 Par ailleurs, la gestion de la configuration est opérée par l'Administrateur, et consiste dans le dépôt des fichiers de configuration VPN et des éléments de sécurité dans le file system de l'OS qui héberge le logiciel TheGreenBow VPN Linux.

1.7 Périmètre de la TOE

1.7.1 Contenu de la TOE et périmètre de la Cible

28 La TOE est un système composé d'un moteur IKE assurant le service IKE V2 en s'appuyant sur la librairie OpenSSL, et d'une couche IPsec assurant le service ESP.



29 Le composant IKE et la librairie OpenSSL sont fournis par TheGreenBow. Le composant IPsec de la TOE est fourni par le noyau Linux sur lequel est installée la TOE (ce sont les drivers IPsec du noyau Linux). Ainsi, le package d'installation du logiciel TheGreenBow VPN Linux contient les composants IKE et OpenSSL, mais ne contient pas les drivers IPsec.

30 Comme la TOE intègre les drivers IPsec du noyau Linux sur lequel elle est installée, et comme cette Cible de Sécurité concerne deux distributions Linux, cette Cible s'applique donc à 2 TOEs :

1/ La TOE "TheGreenBow VPN Linux ELinOS" intégrant les drivers IPsec du noyau Linux ELinOS

2/ La TOE "TheGreenBow VPN Linux Red Hat" intégrant les drivers IPsec du noyau Linux Red Hat.

1.7.2 Eléments hors périmètre de la Cible

31 Les éléments suivants ne font pas partie de la Cible de Sécurité :

- Infrastructure réseau entre l'équipement hébergeant la TOE et l'autre extrémité de la connexion VPN,
- Chiffreur IP (Gateway VPN)
- Infrastructure de gestion de clés (IGC)
- Équipements de stockage amovible de certificats (tokens, lecteurs de carte à puce, carte à puce)

Note 1 : L'adhérence de la TOE au système concernant la gestion des aléas (en particulier la gestion des seeds) est détaillée dans le document de cotation cryptographique.

Note 2 : La TOE n'a pas d'adhérence avec le matériel sur lequel elle est installée. En particulier, le démon IKEv2 n'utilise pas d'élément matériel (par exemple de type TPM).

2 Déclaration de conformité (ASE_CCL.1)

2.1 Déclaration de conformité aux CC

32 Cette CDS est strictement conforme aux CC version V3.1 Révision 5 finale, partie 2 et partie 3.

33 Toutes les exigences fonctionnelles de sécurité (SFR) utilisées dans cette CDS sont strictement issues de la partie 2 des CC version 3.1 Révision 5 finale (référence [CC-2]).

34 Toutes les exigences d'assurance utilisées dans cette CDS sont strictement issues de la partie 3 des CC version 3.1 Révision 5 finale (référence [CC-3]).

2.2 Déclaration de conformité à un Paquet

35 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'

36 Cette CDS est basée sur le profil de protection [PP-VPNC], ci-après désigné par « le PP », mais n'en réclame pas une conformité démontrable ou stricte.

2.4 Différence entre le PP et cette Cible

37 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 ».

38 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 :

39 Multi-utilisateur

L'utilisation de la machine hébergeant la TOE par plusieurs utilisateurs simultanément n'est pas un cas d'usage identifié. Cette utilisation n'est pas recommandée en mode certifié. Ce mode ne fait donc pas partie de la présente cible. L'objectif OE-MULTI-UTILISATEUR est sans objet.

Note : cette fonction est sans rapport avec la capacité de la TOE d'établir plusieurs tunnels simultanément (éventuellement pour un même utilisateur).

40 Intégrité et authenticité de la TOE

L'Administrateur qui installe la TOE peut en vérifier l'intégrité et l'authenticité.

41 Anti-rejeu

la TOE implémente des mécanismes d'anti-rejeu s'appliquant aux données applicatives transportées dans le tunnel VPN. Dans le PP, la menace T.REJEU porte sur les données de télé-administration. Dans cette cible, elle porte sur les données applicatives.

42 Menaces de type "interception"

Les menaces sur les communications de type "interceptions" (MITM, écoute passive, etc.) sont identifiées par la menace T.INTERCEPTION ajoutée par rapport au PP.

43 Contrôle des accès non-chiffrés

Le contrôle des accès non-chiffrés n'est pas du ressort de la TOE

Le contrôle du flux lorsque le tunnel n'est pas monté, ou - a fortiori - lorsque le logiciel ne fonctionne pas, n'est pas réalisé par le logiciel VPN mais via les règles/contraintes du système qui l'héberge (avec des règles de filtrage IP par exemple, du type "ne laisser passer que les ports 500 et 4500"). Cette configuration du système est de la responsabilité de l'administrateur du système.

44 Import des clés cryptographiques

Plusieurs clés sont gérées par la TOE.

1/ Clés privées : les clés privées utilisées par la TOE sont importées depuis un fichier extérieur à la TOE.

2/ Preshared Key (PSK) : l'usage de PSK est non recommandé en mode certifié.

3/ Clés de session : les clés de session sont générées par la TOE, et ne sont donc pas importées.

Dans le cadre de cette CDS, l'opération d'import des clés ne concerne donc que les clés privées. Elle est réduite à la lecture par la TOE des clés privées (issues des certificats) stockées dans les fichiers ad hoc.
Le stockage des clés (session, clé privée) est effectué en mémoire système pendant le temps de leur utilisation. En cas de détection de perte d'intégrité des clés de session, la TOE annule le trafic du lien VPN.

45 Protection des données topologiques

Les données topologiques sont considérées comme un bien sensible. La protection de ces données est donc réintroduite dans le périmètre de cette cible.

Note complémentaire : La protection des données topologiques est assurée par la mise en œuvre du Mode CP IKEv2 (équivalent du Mode Config IKEv1), qui permet de les échanger chiffrées.

46 Import, export de la politique de sécurité

Dans le cadre de cette cible, la TOE n'offre pas de fonction de gestion de configuration VPN : import, export, vérification d'intégrité ou chiffrement (confidentialité). La gestion de la politique de sécurité VPN (configuration VPN et éléments de sécurité) est du ressort de l'administrateur qui assure le dépôt des fichiers de configuration dans le système de façon à ce qu'ils soient exploités correctement par la TOE.

Dans le cadre de cette cible, l'import d'une politique de sécurité VPN est donc réduit à la lecture de la configuration VPN par la TOE elle-même, et la protection de la politique de sécurité VPN en intégrité et en confidentialité n'est pas du ressort de la TOE.

47 Précision sur Utilisateur et Machine

Les différents cas d'usage considérés par cette cible identifient entre autres l'utilisation de la TOE par une machine (mode embarqué). Les hypothèses A.UTILISATEUR et A.MACHINE sont précisées dans ce sens.

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

Sujet	Chapitre et différence
Multi-utilisateur	Ajout de remarques complémentaires aux chapitres 3.5.2 A.MULTI-UTILISATEURS, 4.2.2 OE.MULTI-UTILISATEURS, , 7.1.3.2 A.MULTI-UTILISATEURS
Protection contre le rejeu	§ 3.1.1 : Ajout de la protection anti-rejeu sur D.DONNEES_APPLICATIVES § 3.3.1 : Modification des biens menacés par T.REJEU : D_DONNEES_APPLICATIVES § 4.1.1 : Introduction de l'objectif O.PROTECTION_REJEU § 7.1.1.1 : T.REJEU : Modification des biens menacés (de "opération de téléadministration" en "trames IKE"). § 7.1.4 Table de couverture : ajout de T.REJEU
Protection contre les interceptions	§ 3.3.1 : Ajout de la menace T.INTERCEPTION § 7.1.1 : Ajout de la menace T.INTERCEPTION couverte par O.CONFIDENTIALITE_APPLI et O.AUTHENTICITE_APPLI

Intégrité du logiciel	§ 3.1.1 : Précision sur le bien protégé D.LOGICIEL § 4.2.2 OE.MACHINE : Ajout de la note complémentaire sur l'intégrité du logiciel § 4.2.2 OE.LOGICIEL ajouté (objectif de sécurité sur intégrité du logiciel)
Import et export des clés cryptographiques	§ 3.5.2 : Précision sur l'hypothèse "Machine hôte" A.EXPORT_CLES. § 4.1.2.2 : O.IMPORT_CLES et O.PROTECTION_CLES : précisions sur la gestion des clés. § 5.1.1.3 : Suppression des "clés cryptographiques" de l'opération Import, qui ne s'y applique pas dans le cadre de cette CDS. § 6.1.2 : Précision sur les limites des fonctions F_IMPORT_CLES et F_PROTECTION_CLES
Utilisateur et machine	§ 3.2 Rôles + § 3.5.1 A.UTILISATEUR et A.MACHINE

49 Autres différences entre le PP et la présente CDS :

- Les rôles décrits au §3.2 de la CDS sont identiques à ceux du §3.2 du PP, le rôle utilisateur étant précisé.
- L'hypothèse A.COMPOSANT_AUTHENTIFIANT est 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_ADMIN et O.AUTHENTIFICATION_UTILISATEUR.
- 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_ADMIN et O.AUTHENTIFICATION_UTILISATEUR.

3 Définition du problème de sécurité (ASE_SPD.1)

Convention typographique : dans ce chapitre les caractères en bleu identifient le texte directement issu du [PP]. Les caractères en noir identifient les modifications ou compléments apportés par le développeur.

3.1 Biens

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

51 Dans la suite du document, la notion de "mode certifié" définit une utilisation de la TOE qui prend en compte toutes les recommandations de mise en œuvre et d'utilisation du logiciel décrits dans la présente cible ainsi que dans les guides d'utilisation et d'administration de la TOE (choix des algorithmes, etc.).

3.1.1 Biens protégés par la TOE

52 D.DONNEES_APPLICATIVES

Les données applicatives sont les données provenant et à destination des applications du système d'information de l'équipement nomade et qui sont véhiculées par le réseau. Elles transitent entre deux équipements hébergeant la TOE, ou entre l'équipement qui héberge la TOE et un chiffreur IP. Ces informations sont contenues dans la charge utile des paquets IP échangés et peuvent être stockées temporairement dans la TOE 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 et anti-rejeu

53 D.DONNEES_TOPOLOGIQUES

Les informations de topologie du réseau privé (adresses IP source et destination) sont échangées chiffrées (au cours de l'échange Child SA du protocole IKEv2).

Protection : confidentialité et authenticité et intégrité et anti-rejeu.

54 D.LOGICIEL

Logiciel de la TOE qui permet de mettre en œuvre tous les services de la TOE.
La TOE est livrée signée. Elle offre ainsi la possibilité de vérifier son intégrité et son authenticité avant installation.
A noter : La TOE n'implémente pas en propre, de vérification de son intégrité ou de l'authenticité de ses composants. Dans cette cible, cette fonction est considérée comme étant du ressort de l'environnement de la TOE.

Protection : intégrité et authenticité

3.1.2 Biens sensibles de la TOE

55 D.POLITIQUES_VPN

Les politiques de sécurité VPN définissent les traitements (filtrage implicite et services de sécurité) à effectuer sur les données échangées entre les TOES ou entre la TOE 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 : aucune

56 D.CLES_CRYPTO

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

- des clés de session ;
- des clés utilisées par les services de sécurité appliqués par les politiques de sécurité VPN ;
- des clés privées issues des certificats utilisateurs

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

3.2 Rôles

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

58 UTILISATEUR

Dans le cadre de la présente CDS, deux types d'utilisateurs sont à distinguer :

- L'utilisateur de l'équipement de type "Terminal" hébergeant la TOE. Cet utilisateur a pour rôle d'autoriser l'ouverture du tunnel VPN en passant le Terminal en mode réception numérique, c'est-à-dire en démarrant la TOE en mode serveur. Cet utilisateur peut recevoir des informations à travers le lien VPN établit entre la TOE hébergée par le Terminal et la TOE embarquée dans l'équipement mobile décrit ci-dessous.
- L'applicatif embarqué dans l'équipement mobile hébergeant la TOE. Cet applicatif déclenche l'ouverture du tunnel VPN, réalisée par la TOE, configurée en mode client. Cet applicatif peut transmettre des informations à travers le lien VPN établi entre la TOE embarquée et le chiffreur IP, ou la TOE hébergée par l'équipement de type "Terminal" cité ci-dessus.

59 ADMINISTRATEUR SYSTÈME ET RÉSEAU

C'est l'administrateur responsable de la machine hébergeant la TOE. Il configure les paramètres de la machine, 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.

60 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 configure les politiques de sécurité VPN et leurs contextes de sécurité utilisés par l'application VPN cliente. ~~De plus, il gère (génération, diffusion, ...) les clés et les moyens d'authentification pour accéder à l'application VPN cliente.~~

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

3.3 Menaces

62 Les agents menaçants sont les attaquants externes : toute personne projetant de se connecter à un réseau privé et de réaliser des opérations pour lequel elle n'est pas autorisée ou tentant de récupérer des informations qui ne lui sont pas destinées.

63 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

64 T.REJEU

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

Biens menacés: D.DONNEES_APPLICATIVES

65 T.INTERCEPTION
un attaquant passif écoute sur le réseau, un attaquant en MITM modifie des paquets arbitrairement.

Biens menacés: D.DONNEES_APPLICATIVES

66 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

67 T.LOGICIEL
Un attaquant modifie la TOE avant son installation sur le système hôte, pour accéder illégalement aux services rendus par le client VPN.

Biens menacés : D.LOGICIEL

3.3.2 Menaces portant sur la gestion des clés cryptographiques

68 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

69 T.DIVULGATION_CLES
Un attaquant récupère illégalement des clés cryptographiques.

Biens menacés : D.CLES_CRYPTO

3.4 Politiques de sécurité organisationnelles (OSP)

3.4.1 Services rendus

70 OSP.SERVICES_RENDUS
La TOE doit appliquer les politiques de sécurité VPN définies pour les utilisateurs et les liens VPN logiques (établis physiquement entre deux TOE ou entre la TOE 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.
- protection contre le rejeu
- génération de logs

Biens protégés : D.DONNEES_APPLICATIVES, D.DONNEES_TOPOLOGIQUES

3.4.2 Autres services

71 OSP.CRYPTO

Les référentiels de cryptographie de l'ANSSI ([RGS_B1] et [RGS_B2]) définis pour le niveau de résistance standard doivent être suivis pour la gestion des clés (renouvellement) et les fonctions cryptographiques utilisées dans la TOE.
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.

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

3.5 Hypothèses

3.5.1 Interactions avec la TOE

72 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.

73 A.UTILISATEUR

L'utilisateur de la TOE embarquée dans l'équipement mobile est une application. Il n'y a pas d'objectif sur cet utilisateur.
L'utilisateur de l'application VPN cliente hébergée sur un équipement de type Terminal est une personne non hostile et formée à l'utilisation de la TOE. 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.

74 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

75 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.~~ Dans le cadre de cette CDS, la configuration des machines hébergeant la TOE s'appuie sur les recommandations des guides [GUIDE_DGAMI] , [ANSSI_LINUX1] , [ANSSI_LINUX2]. La machine hôte fait en outre l'objet d'un maintien en condition de sécurité (à jour des patches de sécurité).
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 la TOE.

76 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.
Note : L'utilisateur est soit l'utilisateur de la machine "Terminal" hébergeant la TOE, soit l'application embarquée dans l'équipement mobile hébergeant la TOE

77 A.CONFIGURATION

Il est supposé que la configuration de la machine hébergeant l'application VPN cliente garantit que les communications en clair de la machine via différentes interfaces physiques ou logiques (consultation de sites Internet par exemple) n'ont pas d'impact sur les communications sur les liens VPN.

78 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.

79 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.

Précision :
Plusieurs clés sont gérées par la TOE.

1/ Clés privées
Les clés privées utilisées par la TOE sont importées depuis un fichier extérieur à la TOE. L'export de ces clés consiste en une attaque de type "dump" de la mémoire système.

2/ Preshared Key (PSK)
L'usage de PSK est non recommandé en mode certifié. L'export de PSK n'est donc pas considéré dans cette hypothèse.

3/ Clés de session
Les clés de session sont générées par la TOE. L'export de ces clés consiste en une attaque de type "dump" de la mémoire système.

Conclusion : aucun export ne peut être initié par un utilisateur.

80 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

81 A.REINITIALISATION

Il est supposé que l'environnement permet de réinitialiser la TOE dans un état sûr.
Cette réinitialisation dans un état sûr peut être faite de manière organisationnelle ou technique. Elle comprend l'importation de politiques de sécurité de référence dans la TOE, lorsque celles-ci sont compromises ou supposées compromises, et la vérification de l'intégrité des biens sensibles de la TOE.

3.5.4 Cryptographie

82 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.

Note d'application
Cela fait donc l'hypothèse que des clés secrètes ou privées doivent être distribuées et importées dans la TOE que l'on souhaite intégrer au système de chiffrement. Ces clés doivent alors pouvoir être utilisées pour prouver l'appartenance de la TOE au système de chiffrement.

83 A.CLES_PRIVEES

Les bi-clés et certificats utilisés pour monter les tunnels sont générés par une autorité de confiance externe à la TOE. Ils doivent respecter un ensemble de recommandations décrites dans [RGS_B2] parmi lesquelles : la durée de vie du certificat doit être inférieure à 5 ans et l'algorithme de signature du certificat doit être d'une qualité suffisante. La vérification de ces caractéristiques n'est pas du ressort de la TOE, mais du ressort de la gestion de l'IGC.
Les bi-clés, et en particulier les clés privées, sont stockées de manière sécurisée par l'environnement.
De même, la gestion des CRLs associées aux certificats utilisés pour monter les tunnels n'est pas du ressort de la TOE mais du ressort de la gestion de l'IGC.

4 Objectifs de sécurité (ASE_OBJ.2)

Convention typographique : dans ce chapitre les caractères en bleu identifient le texte directement issu du [PP]. Les caractères en noir identifient les modifications ou compléments apportés par le développeur.

4.1 Objectifs de sécurité pour la TOE

4.1.1 Objectifs de sécurité pour les services rendus par la TOE

84 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.

85 O.CONFIDENTIALITE_APPLI

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

86 O.AUTHENTICITE_APPLI

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

87 O.CONFIDENTIALITE_TOPO

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

88 O.AUTHENTICITE_TOPO

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

89 O.PROTECTION_REJEU

La TOE doit fournir des mécanismes pour protéger les données applicatives contre les opérations de rejeu.

90 O.LOG

La TOE doit générer et maintenir un enregistrement des événements de sécurité en rapport avec son fonctionnement.

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

4.1.2.1 Authentification

91 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.

L'authentification de l'utilisateur ou de l'administrateur peut être vérifiée en pratique par l'un des composants du système de chiffrement suivant :

- 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 (token ou carte à puce).

4.1.2.2 Gestion des clés cryptographiques

92 O.IMPORT_CLES

~~La TOE doit permettre uniquement à l'utilisateur et à l'administrateur d'importer des clés cryptographiques dans la TOE.~~
Comme décrit au § 44 "Import des clés cryptographiques" du chapitre 2.4, la fonction d'import des clés cryptographiques se réduit, dans le cadre de cette Cible, à la lecture par la TOE des clés privées dans les fichiers dans lesquels elles sont stockées. La TOE est donc la seule à importer ces clés.

93 O.PROTECTION_CLES

La TOE doit protéger les clés secrètes et privées en confidentialité et toutes les clés en intégrité 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 ; 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.~~ la TOE elle-même.
Note complémentaire : Dans le cadre de cette CDS, l'opération d'import des clés est réduite à la lecture par la TOE des clés privées stockées dans les fichiers ad hoc.
Le stockage des clés (session, clé privée) est effectué en mémoire système pendant le temps de leur utilisation. En cas de détection de perte d'intégrité des clés de session, la TOE annule le trafic du lien VPN.

4.1.2.3 Administration à distance

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

4.1.2.4 Gestion de la cryptographie

95 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 ([RGS_B1] et [RGS_B2]) pour le niveau de résistance standard.

4.2 Objectifs de sécurité pour l'environnement opérationnel

4.2.1 Interactions avec la TOE

96 OE.ADMIN

Les administrateurs doivent être de confiance et formés aux tâches qu'ils ont à réaliser sur la TOE.
En particulier, dans le cadre de cette cible, c'est l'administrateur qui a en charge la mise à disposition des politiques de sécurité VPN pour la TOE, et à ce titre qui a la responsabilité du contrôle de leur intégrité.

97 OE.UTILISATEUR

Concernant la TOE embarquée sur l'équipement mobile, l'utilisateur est un processus, sur lequel le seul objectif de sécurité, assuré par le système, est une protection en intégrité.
Concernant la TOE hébergée sur l'équipement "Terminal", 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.

98 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

99 OE.MACHINE

La machine hôte sur laquelle est exécutée la TOE 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 la TOE qu'elle héberge.
Note complémentaire : Dans le cadre de cette cible, les machines hébergeant les TOE sont configurées conformément aux guides [GUIDE_DGAMI], [ANSSI_LINUX1], [ANSSI_LINUX2].
Note complémentaire : Dans le cadre de cette cible, le contrôle d'intégrité des composants de la TOE (au démarrage ou périodiquement en cours de fonctionnement) est du ressort de l'environnement de la TOE.

100 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).

101 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.

102 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.

103 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.
Note complémentaire : Dans le cadre de cette CDS, la TOE n'implémente pas de fonction "légitime" d'export de clés. L'objectif de sécurité sur l'export de clés concerne donc la protection contre un accès illégitime aux clés (pour les exporter hors de la TOE ou pour les corrompre), ainsi que décrit au chapitre 3.5.2. "A.EXPORT_CLES".

104 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.

105 OE.LOGICIEL

La TOE est fournie sous forme d'un package signé, qui permet à l'Administrateur d'en vérifier l'intégrité.

4.2.3 Réinitialisation

106 OE.REINITIALISATION

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

4.2.4 Cryptographie

107 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 [RGS_B1] et [RGS_B2] pour le niveau de résistance standard. La gestion des CRLs est effectuée à l'extérieur de la TOE.

108 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)

Convention typographique : dans ce chapitre les caractères en bleu identifient le texte directement issu du [PP]. Les caractères en noir identifient les modifications ou compléments apportés par le développeur.

5.1 Exigences de sécurité fonctionnelles (SFR)

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

110 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

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

5.1.1.1 Sujets

112 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.

113 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

114 Remarque : 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.

115 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.

116 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.

117 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

118 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.

119 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.

120 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 nécessaires.

121 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 ou entre TOE, via le canal VPN.

122 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

123 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.

124 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 peut être égal à "null" (pour préciser qu'aucun utilisateur n'est authentifié) ou "user identifier (tout autre valeur différente de "null" associée à l'utilisateur authentifié; l'ensemble des valeurs n'est donc pas fini). Il s'agit d'un attribut du sujet S.user_manager.

125 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.

126 AT.VPN_link_id

Cet attribut correspond à l'identifiant d'un lien VPN logique établi 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.

127 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.

128 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

129 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.

130 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.

131 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

132 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.

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

134 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

135 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.

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

137 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.**

138 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

139 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

140 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

141 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.

142 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).

  - Note complémentaire : L'authentification et le contrôle d'intégrité assurés par le protocole ESP ne sont pas désactivables dans la politique de sécurité. La protection en confidentialité assurée par le protocole ESP peut être désactivée via le paramètre ESP=NULL.

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

144 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

145 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.

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

147 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. En particulier, la fonction d'anti-rejeu n'est pas débrayable.

FCO_NRO.1/DATA Selective proof of origin

148 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.

149 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.

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

151 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 deux TOE et 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

152 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

153 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 (token ou carte à puce).

5.1.3.1 User authentication

FIA_UID.2/USER User identification before any action

154 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

155 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

156 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.

157 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".

158 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.

5.1.4 Security attributes management

FMT_MSA.3 Static attribute initialisation

159 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.

160 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

161 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

162 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

163 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

164 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	

165 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.

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

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

168 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

169 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.

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

171 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

172 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.

173 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

174 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.

175 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 Cryptography

176 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

177 FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specific 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 ([RGS_B1] and [RGS_B2]).

FCS_CKM.3 Cryptographic key access

178 FCS_CKM.3.1 The TSF shall perform key renegotiation in accordance with cryptographic key renewal that meets the following: cryptographic referential ([RGS_B1] and [RGS_B2]).

179 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 [RGS_B1] et [RGS_B2].

FCS_COP.1 Cryptographic operation

FCS_COP.1/AES

180 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 ([RGS_B1] and [RGS_B2]).

FCS_COP.1/RSA

181 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 ([RGS_B1] and [RGS_B2]).

FCS_COP.1/ECDSA

182 FCS_COP.1.1/ECDSA The TSF shall perform signature in accordance with the ECDSA cryptographic algorithm and cryptographic key sizes of 256,384 et 521 bits that meet the following: ANSSI cryptographic referential ([RGS_B1] and [RGS_B2]).

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 384 bits or 512 bits (taille du condensat) that meet the following: ANSSI cryptographic referential ([RGS_B1] and [RGS_B2]).

5.1.7 Logs (FAU)

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the minimum level of audit; and
c) événements journalisés au titre de l'ouverture, de la fermeture d'un tunnel et du renouvellement de clés

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity (if applicable). And the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, l'identifiant de l'utilisateur

FAU_GEN.2 User identity association

FAU_GEN.2.1

186 **FAU_GEN.2.1** For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2 Exigences de sécurité d'assurance (SAR)

187 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].

188 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

189 F_APPLICATION_POLITIQUE

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

190 F_CONFIDENTIALITE_APPLI

Le logiciel TheGreenBow VPN Linux 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. Cette fonction met en œuvre le protocole ESP.

191 F_INTEGRITE_APPLI

Le logiciel TheGreenBow VPN Linux 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. Cette fonction met en œuvre le protocole ESP.

192 F_CONFIDENTIALITE_TOPO

Le logiciel TheGreenBow VPN Linux 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. Cette fonction met en œuvre le protocole IKEv2.

193 F_INTEGRITE_TOPO

Le logiciel TheGreenBow VPN Linux 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. Cette fonction met en œuvre le protocole IKEv2.

194 F_PROTECTION_REJEU

TheGreenBow VPN Linux fournit des mécanismes empêchant le rejeu des trames IKE et ESP.

195 F_AUTHENTIFICATION_UTILISATEUR

Le logiciel TheGreenBow VPN Linux 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.
Note : Dans le cadre de cette cible, les deux types d'utilisateurs seront à distinguer : l'utilisateur "embarqué" (une application) et l'utilisateur du terminal (une personne).
Dans les deux cas, l'authentification est basée sur l'utilisation de certificats.

196 F_LOG

Le logiciel TheGreenBow VPN Linux permet la génération de log (enregistrement des événements de sécurité survenant sur la TOE).

6.1.2 Gestion des clés cryptographiques

197 F_IMPORT_CLES

Dans le cadre de cette CDS, la fonction d'import de clés par le logiciel TheGreenBow VPN Linux se réduit à la lecture des clés privées dans les fichiers dans lesquels elles sont stockées.

198 F_PROTECTION_CLES

Le logiciel TheGreenBow VPN Linux, en mode certifié, assure la protection en confidentialité et en intégrité des clés de sessions (échangées avec la gateway en mode protégé via IKE) et des clés privées (importée par la TOE par lecture dans les fichiers ad hoc) dans la mesure où les clés sont stockées en mémoire système (confidentialité) et dans la mesure où si elles sont corrompues (intégrité), le tunnel VPN se ferme ou ne s'ouvre pas.

6.1.3 Fonctions Cryptographiques

199 F_GENERATION_CLE

Le logiciel TheGreenBow VPN Linux permet de générer des clés symétriques de chiffrement.
Les algorithmes disponibles et recommandés pour la version certifiée sont : DH groupe 14, 15, 16, 17, 18, 19, 20, 21 et PRF SHA2 256/384/512.
Le générateur d'aléa utilisé pour la génération des clés de session est RAND_Bytes de la librairie OpenSSL, version 1.1.1f

200 F_CHIFFREMENT_SYM

Le logiciel TheGreenBow VPN Linux permet de chiffrer et déchiffrer un flux de données.
Les algorithmes disponibles et recommandés pour la version certifiée sont :

- AES CBC 128/192/256
- AES CTR 128/192/256
- AES GCM 128/192/256

La mise en œuvre de ces algorithmes est détaillée dans la Spécification Cryptographique de la TOE [SPEC_CRYPTO].

201 F_CHIFFREMENT_ASYM

Le logiciel TheGreenBow VPN Linux permet de générer et vérifier une signature.
Note : Bien que cette fonction soit nommée F_CHIFFREMENT_ASYM, elle traite de signature.
Les algorithmes disponibles et recommandés pour la version certifiée sont : RSA et ECDSA
La mise en œuvre de ces algorithmes est détaillée dans la Spécification Cryptographique de la TOE [SPEC_CRYPTO].

202 F_SCELLEMENT

Le logiciel TheGreenBow VPN Linux permet de sceller (hash) un flux de données.
Les algorithmes disponibles pour la version certifiée sont : HMAC SHA2 256/384/512.

6.2 Composants logiciels

203 Le logiciel TheGreenBow VPN Linux est un programme exécutable sur Linux.

Il est composé de plusieurs modules interconnectés : exécutables, drivers, service.

6.2.1 Module IKE Strongswan

204 Le module IKE est constitué du logiciel Strongswan qui fonctionne en service.

Il gère l'intégralité du protocole IKEv2 (ouverture et fermeture d'un tunnel).
Pour ce faire :

- Il récupère du système de fichiers les éléments de sécurité nécessaires à l'ouverture du tunnel
- Il reçoit les ordres d'ouverture et de fermeture de la part de l'utilisateur
- Il transmet les informations des tunnels au module chargé d'assurer le tunnel (Drivers)

6.2.2 Drivers

205 Les Drivers de la TOE sont les modules qui assurent l'encapsulation ESP. Ils assurent les fonctions de sécurité (anti-rejeu, ESP, etc.) nécessaires à la réalisation et au maintien du tunnel, une fois celui-ci négocié (la négociation a lieu via le

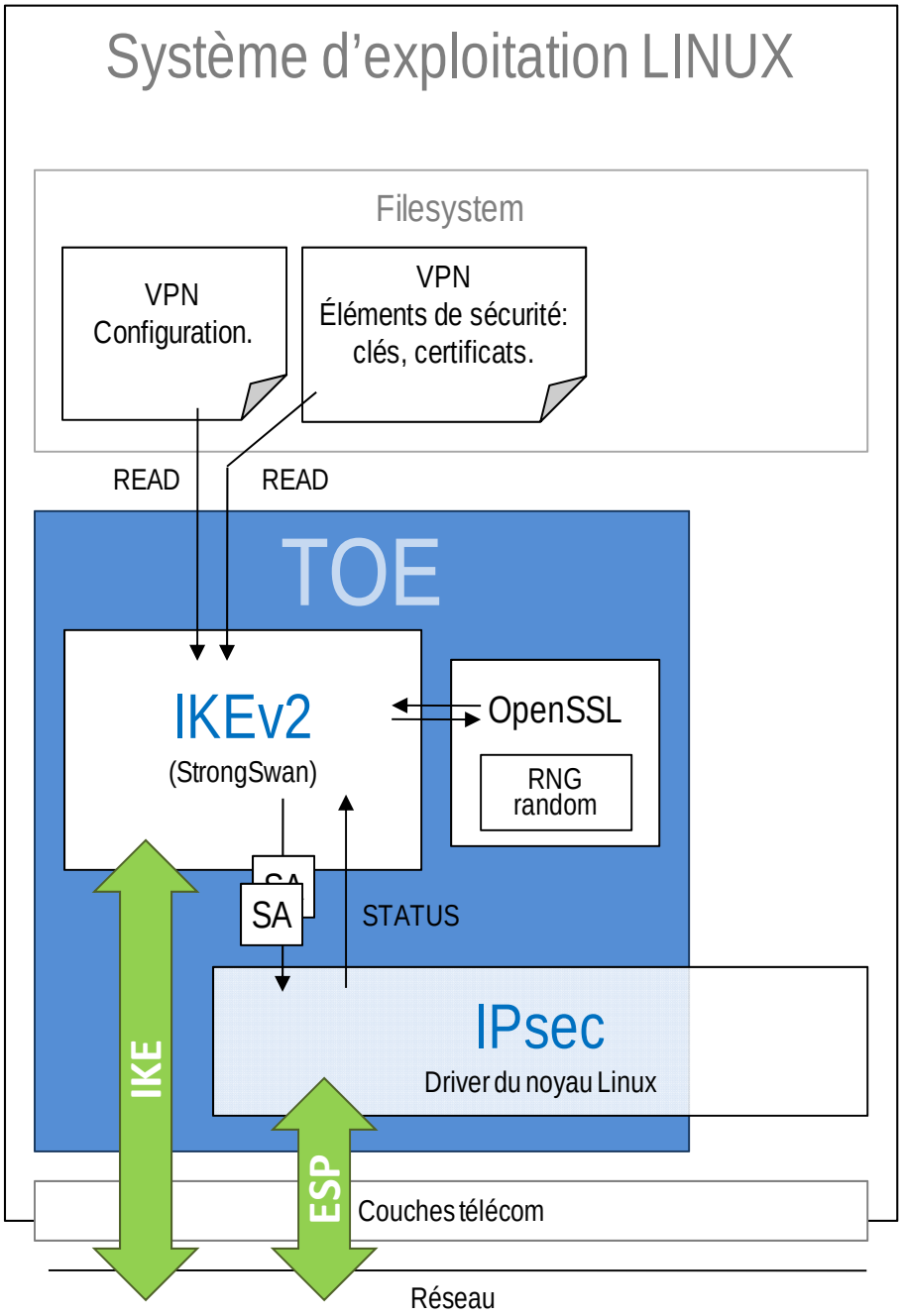
protocole IKEv2 assuré par le module IKE). Le driver IPsec de la TOE est le driver IPsec du noyau Linux sur lequel est installé le logiciel TheGreenBow VPN Linux.

6.2.3 Librairie OpenSSL

206 La librairie OpenSSL est la librairie cryptographique utilisée par les composants du logiciel. Elle constitue la ressource cryptographique de tous les composants du logiciel, hormis les drivers.

6.3 Communication entre les composants

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



- OpenSSL : Librairie indépendante compilée par TheGreenBow et livrée dans le package de l'application

- RNG random : Module de génération des aléas compilé par TheGreenBow et livré dans le package de l'application
- Drivers (Native IPsec) : Fonctions IPsec du noyau Linux.
- VPN Configuration : Politique de sécurité VPN

7 Argumentaire

Convention typographique : dans ce chapitre les caractères en bleu identifient le texte directement issu du [PP]. Les caractères en noir identifient les modifications ou compléments apportés par le développeur.

7.1 Objectifs de sécurité / problème de sécurité

7.1.1 Couverture des menaces

7.1.1.1 Menaces portant sur les communications

208 T.REJEU

Pour prévenir la menace :

- aucune action.

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

- détecter le rejeu de trames ESP ou IKE (O.PROTECTION_REJEU)
- journaliser un événement (O.LOG)

210 Pour réagir à la menace, la TOE doit :

- annuler le rejeu des trames ESP ou IKE (O.PROTECTION_REJEU).

211 T.INTERCEPTION

Pour prévenir la menace :

- la TOE doit garantir la protection en confidentialité et en authenticité les données applicatives (O.CONFIDENTIALITE_APPLI et O.AUTHENTICITE_APPLI).

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

- aucune action

213 Pour réagir à la menace, la TOE doit :

- aucune action

214 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) ;
- ~~le composant authentifiant doit être certifié au niveau standard (OE.COMPOSANT_AUTHENTIFIANT)~~

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

- ~~aucune action.~~
- journaliser un événement (O.LOG)

216 Pour réagir à la menace, la TOE doit :

- aucune action.

217 T.LOGICIEL

Pour prévenir la menace :

- la TOE est livrée dans un package signé qui permet à l'Administrateur de vérifier son intégrité (OE.LOGICIEL).

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

- aucune action

219 Pour réagir à la menace, la TOE doit :

- aucune action

7.1.1.2 Menaces portant sur la gestion des clés cryptographiques

Note : Les clés concernées dans ce paragraphe sont les clés de session uniquement. Comme vu au chapitre 4.1.2.2, la gestion des clés secrètes et privées (import, stockage, export) ne fait pas partie de cette Cible.

220 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) ;

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

- détecter la perte d'intégrité des clés cryptographiques lors de leur utilisation (O.PROTECTION_CLES) ;
- journaliser un événement (O.LOG)

222 Pour réagir à la menace, la TOE doit :

- annuler toute opération d'ouverture ou de maintien de tunnel avec des clés cryptographiques dont la perte d'intégrité serait détectée (O.PROTECTION_CLES) ;

223 T.DIVULGATION_CLES

Pour prévenir la menace :

- la TOE doit garantir la protection en confidentialité des clés lors de leur utilisation (O.PROTECTION_CLES) ;
- la TOE doit permettre de renouveler régulièrement les clés cryptographiques afin de rendre plus difficile l'utilisation de clés divulguées (O.CRYPTO).

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

- aucune action.

225 Pour réagir à la menace, la TOE doit :

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

7.1.2 Couverture des politiques de sécurité organisationnelles (OSP)

7.1.2.1 Services rendus

226 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.

227 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.

228 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).

229 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.

230 Enfin, O.LOG permet de générer et enregistrer les événements de sécurité de la TOE.

7.1.2.2 Autres services

231 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).

7.1.3 Hypothèses

7.1.3.1 Interactions avec la TOE

232 A.ADMIN

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

233 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.

234 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.

7.1.3.2 Machine hôte

235 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.
Note complémentaire : dans le cadre de cette cible, le contrôle d'intégrité des composants de la TOE, au démarrage et en cours de fonctionnement, est assuré par l'environnement de la TOE.

236 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.

237 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.

238 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.

239 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.

240 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.
Note complémentaire : Cette hypothèse est non applicable dans le cadre de cette cible.

7.1.3.3 Réinitialisation

241 A.REINITIALISATION

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

7.1.3.4 Cryptographie

242 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.

243 A.CLES_PRIVEES

Cette hypothèse est entièrement supportée par l'objectif OE.CRYPTO qui assure que les clés privées utilisées par la TOE sont sûres, générées avec des moyens de confiance, et stockées de manière sécurisées par l'environnement de la TOE.

7.1.4 Tables de couverture

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

MENACES	OBJECTIFS DE SÉCURITÉ	ARGUMENTAIRE
T.REJEU	O.PROTECTION_REJEU O.LOG	Cf. § 208
T.INTERCEPTION	O.CONFIDENTIALITE_APPLI O.AUTHENTICITE_APPLI	Cf. § 211
T.USURPATION_UTILISATEUR	O.AUTHENTIFICATION_UTILISATEUR OE.ACCES O.LOG	Cf. § 214
T.LOGICIEL	OE.LOGICIEL	Cf. § 67
T.MODIFICATION_CLES	O.PROTECTION_CLES O.LOG	Cf. § 220
T.DIVULGATION_CLES	O.PROTECTION_CLES O.CRYPTO OE.REINITIALISATION	Cf. § 223

Tableau 4 : Association MENACES vers OBJECTIFS DE SÉCURITÉ

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

OBJECTIFS DE SÉCURITÉ	MENACES
O.APPLICATION_POL	
O.CONFIDENTIALITE_APPLI	T.INTERCEPTION
O.AUTHENTICITE_APPLI	T.INTERCEPTION
O.CONFIDENTIALITE_TOPO	
O.AUTHENTICITE_TOPO	
O.AUTHENTIFICATION_UTILISATEUR	T.USURPATION_UTILISATEUR
O.PROTECTION_CLES	T.MODIFICATION_CLES T.DIVULGATION_CLES
O.PROTECTION_REJEU	T.REJEU

OBJECTIFS DE SÉCURITÉ	MENACES
O.CRYPTO	T.DIVULGATION_CLES
O.LOG	T.REJEU T.USURPATION_UTILISATEUR T.MODIFICATION_CLES
OE.LOGICIEL	T.LOGICIEL
OE.ADMIN	
OE.UTILISATEUR	
OE.CHIFFREUR_IP	
OE.MACHINE	
OE.DROITS_UTILISATEURS	
OE.CONFIGURATION	
OE.COMM	
OE.EXPORT_CLES	
OE.MULTI-UTILISATEURS	
OE.REINITIALISATION	T.DIVULGATION_CLES
OE.CRYPTO	
OE.ACCES	T.USURPATION_UTILISATEUR

Tableau 5 : Association OBJECTIFS DE SÉCURITÉ vers MENACES

246 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 O.LOG	Cf. § 226
OSP.CRYPTO	O.CRYPTO OE.CRYPTO	Cf. § 231

Tableau 6 : Association OSP vers OBJECTIFS DE SÉCURITÉ

247 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_UTILISATEUR	OSP.SERVICES_RENDUS
O.IMPORT_CLES	
O.PROTECTION_CLES	
O.PROTECTION_REJEU	
O.CRYPTO	OSP.CRYPTO

OBJECTIFS DE SÉCURITÉ	OSP
OE.LOGICIEL	
OE.ADMIN	
OE.UTILISATEUR	
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
O.LOG	OSP.SERVICES_RENDUS

Tableau 7 : Association OBJECTIFS DE SÉCURITÉ vers OSP

248 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. § 232
A.UTILISATEUR	OE.UTILISATEUR	Cf. § 233
A.CHIFFREUR_IP	OE.CHIFFREUR_IP	Cf. § 234
A.MACHINE	OE.MACHINE	Cf. § 235
A.DROITS_UTILISATEUR	OE.DROITS_UTILISATEURS	Cf. § 236
A.CONFIGURATION	OE.CONFIGURATION OE.COMM	Cf. § 237
A.COMM	OE.COMM	Cf. § 238
A.EXPORT_CLES	OE.EXPORT_CLES	Cf. § 239
A.MULTI-UTILISATEURS	OE.MULTI-UTILISATEURS	Cf. § 240
A.REINITIALISATION	OE.REINITIALISATION	Cf. § 241
A.ACCES	OE.ACCES	Cf. § 242
A.CLES_PRIVEES	OE.CRYPTO	Cf. § 243

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

249 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

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

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

7.2 Exigences de sécurité / objectifs de sécurité

7.2.1 Argumentation

250 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 qui assure l'accès aux politiques VPN et à leurs attributs afin qu'elles soient appliquées,
- 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.

251 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.

252 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.

253 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.

254 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.

255 O.PROTECTION_REJEU

Cet objectif se traduit par :

- FDP_UIT.1/DATA qui assure l'unicité des données applicatives transitant entre le chiffreur IP et TOE,

256 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.

257 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.

258 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.

259 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.

260 O.CRYPTO

Cet objectif se traduit par :

- FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/ECDSA, 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.

261 O.LOG

Cet objectif se traduit par :

- FAU_GEN.1 qui assure que la TOE met en œuvre des mécanismes de génération de logs.
- FAU_GEN.2 qui assure que la TOE assure la correspondance entre un utilisateur et un événement enregistré.

7.2.2 Tables de couverture

262 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 FMT_MSA.1/QUERY FDP_IFF.1/KEY_IMPORT FDP_ETC.1/EXPORT FDP_ITC.1/IMPORT FDP_IFC.1/DATA FMT_MSA.1/MODIFY FDP_IFC.1/KEY_IMPORT	Cf. § 250
O.CONFIDENTIALITE_APPLI	FDP_UCT.1/DATA	Cf. § 251
O.AUTHENTICITE_APPLI	FDP_UIT.1/DATA FCO_NRO.1/DATA	Cf. § 252
O.CONFIDENTIALITE_TOPO	FDP_UCT.1/DATA	Cf. § 253
O.AUTHENTICITE_TOPO	FDP_UIT.1/DATA FCO_NRO.1/DATA	Cf. § 254
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. § 256
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. § 257

OBJECTIFS DE SÉCURITÉ (O.)	EXIGENCES FONCTIONNELLES	ARGUMENTAIRE
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. § 258
O.CRYPTO	FCS_COP.1/AES FCS_COP.1/RSA FCS_COP.1/ECDSA FCS_COP.1/SHA-2 FCS_CKM.1 FCS_CKM.3	Cf. § 260
O.PROTECTION_REJEU	FDP_UIT.1/DATA	Cf. § 255
O.LOG	FAU_GEN.1 FAU_GEN.2	Cf. § 261

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

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

264

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.AUTHENTIFICATION_UTILISATEUR
FDP_UIT.1/DATA	O.AUTHENTICITE_APPLI O.AUTHENTICITE_TOPO O.PROTECTION_REJEU
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
FMT_MSA.3	O.APPLICATION_POL O.AUTHENTIFICATION_UTILISATEUR O.IMPORT_CLES
FMT_MSA.1/MODIFY	O.APPLICATION_POL O.AUTHENTIFICATION_UTILISATEUR O.IMPORT_CLES

EXIGENCES FONCTIONNELLES	OBJECTIFS DE SÉCURITÉ (O.)
FMT_MSA.1/QUERY	O.APPLICATION_POL O.AUTHENTIFICATION_UTILISATEUR O.IMPORT_CLES
FDP_IFC.1/KEY_IMPORT	O.APPLICATION_POL O.IMPORT_CLES O.AUTHENTIFICATION_UTILISATEUR
FDP_IFF.1/KEY_IMPORT	O.APPLICATION_POL 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
FCS_COP.1/AES	O.CRYPTO
FCS_COP.1/RSA	O.CRYPTO
FCS_COP.1/ECDSA	O.CRYPTO
FCS_COP.1/SHA-2	O.CRYPTO
FCS_CKM.1	O.CRYPTO
FCS_CKM.3	O.CRYPTO
FAU_GEN.1	O.LOG
FAU_GEN.2	O.LOG

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

7.3 Couverture des exigences de sécurité par les spécifications

7.3.1 Argumentation

265 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

266 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.PROTECTION_REJEU	F_PROTECTION_REJEU
O.AUTHENTIFICATION_UTILISATEUR	F_AUTHENTIFICATION_UTILISATEUR
O.IMPORT_CLES	F_IMPORT_CLES
O.PROTECTION_CLES	F_PROTECTION_CLES
O.CRYPTO	F_GENERATION_CLE
O.CRYPTO	F_CHIFFREMENT_SYM

O.CRYPTO	F_CHIFFREMENT_ASYM
O.CRYPTO	F_SCELLEMENT
O.LOG	F_LOG

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

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

Exigences	Fonctions	Mécanismes de sécurité
FDP_ETC.1/EXPORT	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR	Caractérisation des flux de données applicatives à protéger, ouverture d'une SA sur détection de trafic, synchronisation des politiques de sécurité VPN, gestion des états du logiciel TheGreenBow VPN Linux
FDP_ITC.1/IMPORT	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR	Synchronisation des politiques de sécurité VPN, caractérisation des flux de données applicatives à protéger, intégrité, authentification et non répudiation des paquets ESP
FDP_IFC.1/DATA	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR F_PROTECTION_CLES	Caractérisation des flux de données applicatives à protéger, synchronisation des politiques de sécurité VPN, authentification IKE, confidentialité des échanges IKE, intégrité des échanges IKE
FDP_IFF.1/DATA	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR F_PROTECTION_CLES	Intégrité, Authentification et non répudiation des paquets ESP, confidentialité des données applicatives et topologiques, synchronisation des politiques de sécurité VPN, Authentification de l'utilisateur, caractérisation des flux de données applicatives à protéger, intégrité des échanges IKE, confidentialité des échanges IKE, gestion des états du logiciel TheGreenBow VPN Linux (RFC7296)
FDP_UIT.1/DATA	F_INTEGRITE_APPLI F_INTEGRITE_TOPO F_PROTECTION_REJEU	Intégrité, Authentification et non répudiation des paquets ESP, unicité des paquets IKE, (mécanisme anti-rejeu)
FCO_NRO.1/DATA	F_INTEGRITE_APPLI F_INTEGRITE_TOPO	Intégrité, authentification et non répudiation des paquets ESP
FDP_UCT.1/DATA	F_CONFIDENTIALITE_APPLI F_CONFIDENTIALITE_TOPO	Ouverture d'une SA sur détection de trafic, caractérisation des flux de données applicatives à protéger, confidentialité des données applicatives et topologiques (RFC7296)
FIA_UID.2/USER	F_AUTHENTIFICATION_UTILISATEUR	Authentification de l'utilisateur
FIA_UAU.2/USER	F_AUTHENTIFICATION_UTILISATEUR	Authentification de l'utilisateur
FIA_USB.1/USER	F_AUTHENTIFICATION_UTILISATEUR F_APPLICATION_POLITIQUE	Synchronisation des politiques de sécurité VPN, authentification de l'utilisateur
FMT_MSA.3	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES	Synchronisation des politiques de sécurité VPN

FMT_MSA.1/MODIFY	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES	Authentification de l'utilisateur, Authentification IKE, confidentialité des échanges IKE, intégrité des échanges IKE
FMT_MSA.1/QUERY	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES F_IMPORT_POL	Authentification de l'utilisateur, synchronisation des politiques de sécurité VPN, authentification IKE, confidentialité des échanges IKE, intégrité des échanges IKE
FDP_IFC.1/KEY_IMPORT	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES	Synchronisation des politiques de sécurité VPN, caractérisation des flux de données applicatives à protéger, intégrité des échanges IKE, authentification IKE (RFC7296)
FDP_IFF.1/KEY_IMPORT	F_APPLICATION_POLITIQUE F_AUTHENTIFICATION_UTILISATEUR F_IMPORT_CLES	Caractérisation des flux de données applicatives à protéger, synchronisation des politiques de sécurité VPN, intégrité des échanges IKE, authentification de l'utilisateur
FDP_ITC.1/KEY_IMPORT	F_IMPORT_CLES F_PROTECTION_CLES	Synchronisation des politiques de sécurité VPN, intégrité des échanges IKE, authentification IKE (RFC7296), authentification de l'utilisateur
FDP_UTC.1/KEY_IMPORT	F_PROTECTION_CLES	synchronisation des politiques de sécurité VPN Confidentialité des échanges IKE (RFC7296)
FDP_UIT.1/KEY_IMPORT	F_PROTECTION_CLES	Chiffrement des politiques de sécurité VPN, synchronisation des politiques de sécurité VPN Intégrité des échanges IKE
FCS_CKM.1	F_GENERATION_CLE	Mécanisme inhérent au protocole IKE
FCS_CKM.3	F_GENERATION_CLE	Mécanisme inhérent au protocole IKE
FCS_COP.1/AES	F_CHIFFREMENT_SYM	Confidentialité des échanges IKE, confidentialité des données applicatives et topologiques. Implémentation standard du chiffrement AES, disponible en versions 128, 192 et 256 bit.
FCS_COP.1/RSA	F_CHIFFREMENT_ASYM	Authentification IKE, implémentation standard de l'algorithme RSA, avec support de clés jusqu'à 8192 bit
FCS_COP.1/ECDSA	F_CHIFFREMENT_ASYM	Authentification IKE, implémentation standard de l'algorithme ECDSA avec support de clé de 256, 384 et 521 bits
FCS_COP.1/SHA-2	F_SCELLEMENT	Authentification IKE, intégrité, authentification et non répudiation des paquets ESP, implémentation standard de SHA-2, disponible jusqu'à 512 bit
FAU_GEN.1 FAU_GEN.2	F_LOG	Génération de logs

Tableau 13 : Association FONCTIONS de SECURITE vers EXIGENCES FONCTIONNELLES

7.4 Dépendances

7.4.1 Dépendances des exigences de sécurité fonctionnelles

268 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
FCS_COP.1/AES	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.1/KEY_IMPORT
FCS_COP.1/RSA	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.1/KEY_IMPORT
FCS_COP.1/ECDSA	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.1/KEY_IMPORT
FCS_COP.1/SHA-2	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)	FDP_ITC.1/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
FCO_NRO.1/DATA	(FIA_UID.1)	FIA_UID.2
FDP_UCT.1/DATA	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1
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)	
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
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
FAU_GEN.1	FPT_STM.1	
FAU_GEN.2	FAU_GEN.1 et FIA_UID.1	FAU_GEN.1 FIA_UID.2/USER

Tableau 14 : Dépendances satisfaites des exigences de sécurité fonctionnelles

269 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/SHA-2 n'est pas supportée. La dépendance avec FCS_CKM.4 n'est pas satisfaite car la fonction de hachage ne nécessite pas de clé cryptographique.
- La dépendance FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2 de FCS_COP.1 n'est pas supportée. La dépendance avec FCS_CKM.1, FDP_ITC.1 ou FDP_ITC.2 n'est pas satisfaite car la fonction de hachage ne nécessite ni la génération ni l'import de clé dans 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 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 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 FAU_GEN.1 avec FPT_STM.1 n'est pas supportée dans la mesure où la base de temps est fournie par le système d'exploitation.

7.4.2 Dépendances des exigences de sécurité d'assurance

270 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	
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

271 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]. Le composant ADV_FSP.3 est retenu.

7.5 Argumentaire pour l'EAL

272 Le niveau d'assurance 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'

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

7.6.2 ALC_FLR.3 'Systematic flaw remediation'

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

7.7 Annexe – Plateformes évaluées

Les plateformes évaluées sur lesquelles s'exécute la TOE sont :

- Linux ElinOS 6.1 64 bits,
- RedHat Enterprise Linux 7 64 bits

La gateway VPN en extrémité VPN est :
OS : debian 8
Strongswan : Linux strongswan U5.2.1/K3.16.8-4-amd64
Configuration réseau : 2 interfaces ethernet
eth0 == bridgée
eth1 == wmnet6 (Host Only)
Interface utilisée pour monter les tunnels : eth0

--- FIN DU DOCUMENT ---