Direction centrale de la sécurité des systèmes d'information

PP Application VPN cliente

Date de Création	:	Juin 2008
Référence	:	PP-VPNC-CCv3.1
Version	:	1.3

Profil de protection enregistré et certifié par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) sous la référence DCSSI-PP-2008/03.

Table des matières

Liste des figures

Liste des tables

1 Introduction

1.1 Identification du profil de protection

Titre :	Profil de protection, Application VPN cliente
Auteurs :	Trusted Labs S.A.S.
Version :	1.3, Juin 2008
Commanditaire :	DCSSI
Version des CC :	3.1 revision 2

Remarque:

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

1.2 Contexte

Ce PP est réalisé sous l'égide de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI). L'objectif est de fournir un cadre administratif à la certification d'applications VPN clientes pour les besoins des secteurs public et privé en vue de leur qualification.

1.3 Présentation générale de la cible d'évaluation

1.3.1 Type de TOE

L'objectif visé par le présent profil de protection est de définir les exigences de sécurité associées à une application VPN présente sur un poste client. Il complète ainsi le profil « Chiffreur IP »[1] ([PPnc0502]) qui spécifie les exigences sécuritaires d'une passerelle VPN.

Les technologies « VPN » (Réseaux Privés Virtuels) permettent de protéger les flux de données échangées entre deux équipements réseaux interconnectés à travers un réseau public non sûr (comme Internet), ou bien de protéger les flux échangés entre un équipement terminal mobile et un équipement réseau distant à travers un réseau non sûr (cas du VPN nomade). Elles assurent l'obtention d'une sécurité des échanges réseaux équivalente à celle fournie par une liaison point à point, physiquement et logiquement dédiée.

[1] Ce PP est disponible en CC3.1 revision 2 sous la référence PP-CIP-CCv3.1

Le type de TOE considéré est un client de type IPsec, mais les développeurs de produits implémentant un client VPN SSL pourront s'inspirer au besoin du présent PP pour la rédaction de la cible de sécurité de leur produit.

1.3.2 Utilisation de la TOE

L'application VPN cliente permet d'établir un lien de communication entre un équipement nomade ne disposant pas nécessairement d'une adresse prédictible (de type ordinateur portable connecté via un fournisseur d'accès ou via un réseau d'entreprises) et une passerelle VPN placée à l'entrée du réseau privé d'une organisation. Ce lien de communication peut potentiellement utiliser un réseau public non sûr, comme Internet, et des moyens d'accès extrêmement variés (tel que Wi-Fi), exposant ainsi le lien de communication à de nombreuses menaces qui imposent sa sécurisation.

Par ailleurs, la TOE peut être utilisée de deux manières. Un utilisateur peut soit interagir directement avec l'application VPN cliente pour établir un lien VPN, soit, cela est fait via une application qui sert d'intermédiaire entre l'utilisateur et la TOE (en particulier c'est alors l'application intermédiaire qui active la TOE). Dans ce dernier cas, l'utilisateur et l'application intermédiaire seront assimilés à un même utilisateur.

1.3.3 Limite logiques de la TOE

La fonction principale de l'application VPN cliente est d'assurer la sécurité des données transitant entre un équipement nomade et la passerelle d'un réseau privé (également désignée sous le terme chiffreur IP) en établissant des liens VPN. Pour cela, des politiques de sécurité VPN sont définies. Elles incluent l'ensemble des paramètres de la connexion sécurisée (algorithmes de chiffrement et d'authentification, tailles de clés, ...)[2], ainsi que les services de sécurité pouvant être appliqués (confidentialité et/ou authenticité).

Différentes clés cryptographiques sont nécessaires pour l'application des services de sécurité garantissant la confidentialité et l'authenticité des données applicatives transmises. En outre, des clés sont également nécessaires afin d'assurer la confidentialité et/ou l'authenticité des flux d'administration à distance. Deux approches peuvent être suivies pour la gestion de ces clés par la TOE :

- Importation de clés cryptographiques générées à l'extérieur de la TOE,
- Génération des clés cryptographiques dans la TOE.

Dans ce profil, les clés cryptographiques sont générées à l'extérieur de la TOE et importées dans la TOE, l'auteur d'une cible de sécurité pourra ajouter la génération des clés dans la TOE, tout en restant conforme à ce profil.

L'authentification de l'utilisateur ou de l'administrateur est réalisée par un composant appartenant au même système de chiffrement que la TOE (comme spécifié au paragraphe 1.3.4.2). Celui-ci peut être des types suivants :

- Un module de l'application VPN cliente (inclue dans le périmètre de la TOE d'une cible de sécurité conforme à ce PP),
- le chiffreur IP distant qui établira un tunnel VPN avec la machine hébergeant la TOE,
- un équipement de téléadministration centralisé,
- le module cryptographique de l'utilisateur (clé USB ou carte à puce).

La TOE ne gère pas d'évènements d'audit sur la machine hôte compte tenu :

- de la difficulté d'exploitation de l'audit dans la gestion de machines nomades, et

[2] Les clés elles-même sont gérées indépendamment des politiques de sécurité.

- de l'administration de la TOE considérée comme principalement réalisée au moyen d'un équipement de téléadministration centralisé.

1.3.4 Intégration de la TOE dans son environnement

La TOE se situe dans le contexte d'un système de chiffrement composé de machine hôtes hébergeant l'application VPN cliente, de chiffreurs IP et d'équipements d'administration (ou de télégestion) pouvant héberger des services de mise à jour des politiques de sécurité VPN.

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

- celles permettant la communication sécurisée avec un chiffreur IP (clés utilisées par les services de sécurité et clés de session),
- celles permettant la communication sécurisée à distance avec un administrateur (ce rôle peut-être joué par un équipement de téléadministration centralisé), afin de renouveler les politiques de sécurité VPN et importer de nouvelles clés.

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

1.3.4.1 Phase d'initialisation

Lorsque la définition des politiques de sécurité VPN est réalisée de manière centralisée sur un équipement de télé-administration de manière à pouvoir distribuer automatiquement ces politiques à l'ensemble des machines hébergeant l'application VPN cliente, l'installation de l'application VPN doit comporter une phase de pré-configuration. Cette phase, réalisée par un administrateur, est nécessaire au chargement ultérieur des politiques au travers d'un canal d'administration sécurisé.

Néanmoins, la définition (*i.e.* le chargement) des politiques de sécurité VPN permettant de rendre l'application VPN cliente opérationnelle peut par ailleurs être également réalisée :

- au sein de l'application VPN cliente lors de son installation (grâce, par un exemple, à l'utilisation d'un « master »),
- manuellement par l'administrateur une fois l'application installée.

1.3.4.2 Phase opérationnelle

En phase opérationnelle, la TOE permet l'importation locale ou à distance via un équipement de télégestion par un administrateur authentifié de nouvelles politiques VPN et clés cryptographiques, utilisées par les services de sécurité et pour l'application des politiques de sécurité VPN.

L'utilisation de l'application VPN cliente doit être contrôlée afin d'éviter toute connexion frauduleuse. Dans cette optique une authentification devra être assurée par un tiers de confiance, faisant partie de système de chiffrement[3], et vérifiée par la TOE. Cela permettra à un utilisateur d'établir un lien VPN en appliquant la politique de sécurité liée à cet utilisateur.

[3] La TOE faisant partie du système de chiffrement, l'auteur d'une ST conforme à ce profil pourra assimiler la TOE à ce tiers de confiance.

Pour un administrateur, cela permettra de réaliser des opérations d'administration sur la TOE.

L'administration de l'application VPN cliente en phase opérationnelle peut par ailleurs se faire à distance de manière centralisée[4] (via un serveur qui regroupe les politiques VPN) et automatique, afin de pouvoir mettre à jour un ensemble de machines de manière souple et rapide sans avoir à toutes les rapatrier vers un administrateur de sécurité. Cependant, dans ce cas, des clés permettant de protéger les flux d'administration de sécurité lors de mises à jour doivent être injectées en phase d'initialisation ou distribuées de manière organisationnelle ; ces mises à jour concernent en premier lieu les politiques de sécurité VPN à appliquer sur chaque lien de communication (politiques associées à un utilisateur, une machine et un lien VPN) et leur contexte de sécurité.

1.3.5 Utilisation du profil de protection

Dans le cadre de ce PP, les données envoyées et reçues via un lien de communication VPN sont supposées sensibles mais non classifiées de défense (couvrant les besoins de diffusion restreinte par exemple).

Certaines propriétés de sécurité relatives aux biens sont qualifiées « d'optionnelles » dans le présent profil de protection. Cette mention indique que des mécanismes garantissant ces propriétés devront être implémentés dans la TOE mais que leur application ou leur utilisation ne doit pas être considérée comme systématique.

Les exigences introduites dans ce profil de protection définissent les règles minimales auxquelles une cible de sécurité pour une application VPN cliente doit se conformer ; elles ne sont aucunement limitatives. Ainsi, il est possible d'ajouter d'autres fonctionnalités (telles que, par exemple, certaines traduites sous forme d'hypothèses dans le présent PP) ou de se référer également à un autre profil de protection. Cependant, toute modification au profil est restreinte par les règles associées à la conformité précisée au paragraphe 2.4. Cette dernière stipule en particulier que pour une cible conforme à ce PP, les objectifs techniques sur l'environnement opérationnel pourront être transférés en objectifs sur la TOE (et, de la même manière, les hypothèses transférées en menaces ou politiques de sécurité organisationnelles). Une telle démarche vise à diminuer la dépendance sécuritaire de la TOE à son d'environnement. Dans ce cadre, des indications en notes d'application sont données dans ce PP afin d'indiquer au rédacteur de cibles de sécurité les objectifs sur l'environnement opérationnel qui pourrait être transférés en objectifs sur la TOE.

Les exigences fonctionnelles assurant les objectifs associés à l'import et l'export de biens sensibles dans et hors de la TOE, ne différencient pas l'administration locale de l'administration distante ; les exigences de sécurité étant identiques. Cependant, l'auteur d'une cible de sécurité conforme à ce profil pourra envisager de différencier les deux cas pour accroître les exigences de sécurité de l'un des deux modes d'administration.

Dans le cadre d'une administration distante en particulier, la cible de sécurité devra faire apparaître que la TOE doit permettre d'authentifier la machine distante à partir de laquelle l'administrateur exécute ses opérations d'administration, et d'assurer un canal sûr en intégrité et confidentialité avec cette machine. Les mécanismes associés seront inclus dans la TOE.

Note d'application :

La fusion des deux modes d'administration locale et à distance, n'impose pas un mécanisme unique pour leur implémentation dans le produit.

[4] L'équipement de téléadministration centralisé joue alors le rôle d'administrateur.

2 Déclaration de conformité

Ce chapitre contient les sections suivantes :

2.1 Déclaration de conformité aux CC

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

Ce PP a été écrit conformément aux CC version 3.1 :

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

2.2 Déclaration de conformité à un Paquet

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

2.3 Déclaration de conformité du PP

Ce PP ne déclare de conformité à aucun autre PP.

2.4 Déclaration de conformité au PP

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

3 Définition du problème de sécurité

3.1 Biens

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

La mention "(opt.)" pour "optionnel", stipule que le produit devra supporter des mécanismes permettant d'assurer cette protection, mais que son application ne doit pas être considérée comme systématique.

3.1.1 Biens protégés par la TOE

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 l'équipement qui héberge la TOE et un chiffreur IP. Ces informations sont contenues dans la charge utile des paquets IP échangés entre la TOE et le chiffreur IP 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 (opt.) et authenticité (opt.).

D.DONNEES_TOPOLOGIQUES

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

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

3.1.2 Biens sensibles de la TOE

D.POLITIQUES_VPN

Les politiques de sécurité VPN définissent les traitements (filtrage implicite et services de sécurité) à effectuer sur les données échangées 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: authenticité et confidentialité.

D.CLES_CRYPTO

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

- o des clés de session,
- o des clés utilisées par les services de sécurité appliqués par les politiques de sécurité VPN,
- o des clés pour protéger les politiques de sécurité VPN lors de leur stockage,

- o des clés pour protéger l'import de clés cryptographiques et de politiques de sécurité VPN dans la TOE,
- o des clés pour protéger l'export de politiques de sécurité VPN hors de la TOE,

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

D.LOGICIEL

Logiciel de la TOE qui permet de mettre en oeuvre tous les services de la TOE.

Protection: intégrité.

3.2 Rôles

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

Utilisateur

Utilisateur de la machine accédant au réseau privé de l'organisation au travers d'un chiffreur IP. Cet utilisateur peut envoyer/recevoir des informations vers/de ce réseau privé à travers un lien VPN établi entre l'application VPN cliente et le chiffreur IP.

Note d'application

L'utilisateur peut éventuellement être une application ou un processus exécuté sur la machine hôte considérée.

Administrateur système et réseau

Administrateur responsable de la machine. Il configure les paramètres de la machine (les comptes utilisateurs par exemple), mais ne définit pas les politiques de sécurité VPN.

Il configure les paramètres réseaux de l'application VPN cliente et les paramètres systèmes qui sont liés aux contextes réseaux opérationnels.

Administrateur de sécurité

Il génère et distribue les clés dans l'application VPN cliente et importe les politiques de sécurité VPN et leurs contextes de sécurité que va appliquer l'application VPN cliente.

Il peut définir et mettre à jour les politiques de sécurité VPN au niveau d'un équipement de téléadministration centralisé présent sur le réseau privé de l'organisation de manière à ce que ces politiques puissent être « télé-distribuées » par chaque machine hébergeant l'application VPN cliente en phase opérationnelle.

De plus, il gère (génération, diffusion,...) les clés et les moyens d'authentification pour accéder à l'application VPN cliente.

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

3.3 Menaces

La politique de qualification au niveau standard s'applique à des produits grand public assurant la protection d'informations sensibles non classifiées de défense.

Les agents menaçants sont:

- les attaquants externes: toute personne projetant de se connecter à un réseau privé et de réaliser des opérations pour lequel il n'est pas autorisé ou tentant de récupérer des informations qui ne lui sont pas destinée.

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

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.POLITIQUES_VPN, D.CLES_CRYPTO

Note d'application

Un chemin d'attaque correspondant à cette menace pourrait être:

Un administrateur importe dans la TOE via une commande d'administration « C », une politique de sécurité autorisant la communication en clair des données applicatives (pas de confidentialité) vers une machine « M ». Un attaquant capture « C ». Peu après la machine « M » doit recevoir des données confidentielles. L'administrateur remplace ainsi la politique de sécurité de manière à assurer la confidentialité des données applicatives. L'attaquant rejoue la commande « C ». La communication vers la machine « M » se fera ainsi en clair, mais l'attaquant est le seul à le savoir alors. L'utilisateur envoie de ce fait ses données confidentielles en clair sur le lien VPN. L'attaquant les intercepte.

T.USURPATION_ADMIN

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

Biens menacés: D.POLITIQUES_VPN, D.CLES_CRYPTO

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 réaliser des opérations sur la TOE pour lesquels l'utilisateur est autorisé.

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

3.3.2 Menaces portant sur la gestion des clés cryptographiques

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

T.DIVULGATION_CLES

Un attaquant récupère illégalement des clés cryptographiques.

Biens menacés: D.CLES_CRYPTO

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

T.MODIFICATION_POL

Un attaquant modifie illégalement les politiques de sécurité VPN et leurs contextes de sécurité. Cette modification peut par exemple résulter de la modification de commandes d'import envoyées par l'administrateur.

Biens menacés: D.POLITIQUES_VPN

T.DIVULGATION_POL

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

Biens menacés: D.POLITIQUES_VPN

3.4 Politiques de sécurité organisationnelles (OSP)

3.4.1 Services rendus

OSP.SERVICES_RENDUS

La TOE doit appliquer les politiques de sécurité VPN définies pour les utilisateurs et les liens VPN logiques (établis physiquement 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 authenticité des données applicatives,
- protection en confidentialité des données topologiques,
- protection en authenticité des données topologiques.

Biens protégés: D.DONNEES_APPLICATIVES, D.DONNEES_TOPOLOGIQUES

3.4.2 Autres services

OSP.CRYPTO

Les référentiels de cryptographie de la DCSSI ([CRYPTO] et [CRYPTO_GESTION]) définis pour le niveau de résistance standard doit être suivi pour la gestion des clés (renouvellement) et les fonctions cryptographiques utilisées dans la TOE.

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

Note d'application

L'auteur d'une ST se réclamant conforme à ce PP pourra considérer l'ajout de la génération de clés cryptographiques dans la TOE.

OSP.EXPORT_POL

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

Biens protégé: D.POLITIQUES_VPN

3.5 Hypothèses

3.5.1 Interactions avec la TOE

A.ADMIN

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

A.UTILISATEUR

L'utilisateur de l'application VPN cliente 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.

A.EQUIPEMENT_TELEADMINISTRATION

Il est supposé que l'équipement de téléadministration centralisé permettant de distribuer les politiques de sécurité VPN est hébergé sur une machine sûre qui doit être placée dans des locaux sécurisés dont l'accès est restreint aux seuls administrateurs. Sa disponibilité est par ailleurs assurée et son bon fonctionnement régulièrement contrôlé.

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.

A.COMPOSANT_AUTHENTIFIANT

Il est supposé que le composant du système de chiffrement réalisant l'authentification de l'utilisateur et de l'administrateur est évalué conformément au processus de qualification de niveau standard défini par la DCSSI dans [QUA-STD].

Note d'application

Ce composant pourra éventuellement être intégré dans le périmètre de la TOE lors de l'écriture d'une cible de sécurité conforme à ce PP. Dans ce cas, l'évaluation selon le processus de qualification de niveau standard sera de fait requise.

3.5.2 Machine hôte

A.MACHINE

Il est supposé que la machine sur laquelle est installée et exécutée l'application VPN cliente est saine et correctement administrée. En particulier, elle dispose d'un anti-virus dont la base de données est régulièrement mise à jour et est protégée par un pare-feu.

Il est par ailleurs supposé que la machine hôte hébergeant l'application VPN cliente continue d'assurer la protection des données ayant été récupérées au travers de liens VPN.

Enfin, il est supposé que la machine hôte garantit l'intégrité du logiciel permettant de mettre en oeuvre tous les services de la TOE.

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.

A.CONFIGURATION

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

Note d'application

Les interfaces physiques et logiques mentionnées dans cet objectif sont celles de la machine.

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.

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.

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

A.REINITIALISATION

Il est supposé que l'environnement permet de réinitialiser la TOE dans un état sûr.

Note d'application

Cette réinitialisation dans un état sûr pourra être faite de manière organisationnelle ou technique. Par exemple, elle peut comprendre 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

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.

4 Objectifs de sécurité

4.1 Objectifs de sécurité pour la TOE

4.1.1 Objectifs de sécurité pour les services rendus par la TOE

O.APPLICATION_POL

La TOE doit appliquer les politiques de sécurité VPN présentes dans l'application VPN cliente et associées à l'utilisateur authentifié, aux données transitant sur les liens VPN.

Note d'application

Ces politiques de sécurité peuvent inclure en particulier la confidentialité et l'authenticité des données échangées.

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.

O.AUTHENTICITE_APPLI

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

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.

O.AUTHENTICITE_TOPO

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

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

4.1.2.1 Authentification

O.AUTHENTIFICATION_ADMIN

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

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 méchanisme d'authentification utilisé doit être conforme aux recommendations du référentiel de la DCSSI [AUTH] pour le niveau de robustesse standard.

Note d'application:

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,
- l'équipement de téléadministration centralisé,
- le module cryptographique de l'utilisateur (clé USB ou carte à puce).

4.1.2.2 Gestion des clés cryptographiques

O.IMPORT_CLES

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

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.

Note d'application

Cet objectif ne concerne pas l'administration à distance (c.f. O.PROTECTION_FLUX_ADMIN).

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.

4.1.2.3 Gestion des politiques de sécurité VPN

O.IMPORT_POL

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

O.PROTECTION_POL

La TOE doit fournir des mécanismes pour protéger les politiques de sécurité VPN en intégrité et confidentialité lors de leur import et de leur export. Lors de l'import, la protection en intégrité devra consister en la détection de la perte d'intégrité et l'annulation de l'opération. Lors de l'export, elle consistera à rendre possible la détection de toute perte d'intégrité.

L'intégrité des politiques de sécurité VPN doit aussi être assurée lors de leur stockage; en cas de détection de perte d'intégrité de la politique de sécurité VPN, la TOE devra annuler l'établissement de tout lien VPN.

Par ailleurs, la TOE doit permettre d'exporter les politiques de sécurité VPN vers un administrateur.

Note d'application

Cet objectif ne concerne pas l'administration à distance (c.f. O.PROTECTION_FLUX_ADMIN).

4.1.2.4 Administration à distance

O.PROTECTION_REJEU

La TOE doit détecter le rejeu de séquences d'envoi de données d'administration à distance. A la détection de cette attaque, la TOE doit répondre par l'annulation de l'opération.

O.PROTECTION_FLUX_ADMIN

La TOE doit garantir l'intégrité et la confidentialité des flux d'administration. La protection en confidentialité n'est pas systématiquement appliquée si les données passant dans le flux ne sont pas confidentielles. Pour un flux entrant, la protection en intégrité devra consister en la détection de la perte d'intégrité et l'annulation de l'opération. Pour un flux sortant, elle consistera à rendre possible la détection de toute perte d'intégrité.

4.1.2.5 Gestion de la cryptographie

O.CRYPTO

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

Note d'application

L'auteur d'une cible de sécurité se réclamant conforme à ce PP pourra considérer l'ajout de la génération de clés cryptographiques dans la TOE.

4.2 Objectifs de sécurité pour l'environnement opérationnel

4.2.1 Interactions avec la TOE

OE.ADMIN

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

OE.UTILISATEUR

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

OE.EQUIPEMENT_TELEADMINISTRATION

L'équipement de téléadministration centralisé doit se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs. Sa disponibilité devra par ailleurs être assurée et son bon fonctionnement régulièrement contrôlé.

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.

OE.COMPOSANT_AUTHENTIFIANT

Le composant du système de chiffrement réalisant l'authentification de l'utilisateur et de l'administrateur de sécurité doit être qualifiés (au moins) au niveau standard tel que défini par la DCSSI dans [QUA-STD].

Note d'application

Cet objectif sur l'environnement opérationnel pourra être passé en objectif sur la TOE dans une cible de sécurité, afin que la TOE assure seule les fonctions d'authentification; dans ce cas, le composant authentifiant fera partie du périmètre de la TOE.

4.2.2 Machine hôte

OE.MACHINE

La machine hôte sur laquelle est exécutée l'application VPN cliente doit être saine, protégée et configurée de manière à garantir sa sécurité et celle des données qu'elle héberge. En particulier, elle assure l'intégrité de l'application VPN cliente qu'elle héberge.

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).

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.

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.

OE.EXPORT_CLES

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

OE.MULTI-UTILISATEURS

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

4.2.3 Réinitialisation

OE.REINITIALISATION

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

4.2.4 Cryptographie

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

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

5.1 Exigences de sécurité fonctionnelles

5.1.1 Définition des éléments du modèle de sécurité sous-jacent

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

5.1.1.1 Sujets

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 bien sensibles de la TOE.

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

Remarque: les objets sont stockés sur 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.

OB.keys

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

Note d'application:

L'auteur d'une ST conforme à ce profil pourra introduire la génération des clés cryptographique dans la TOE.

OB.vpn_policies

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

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

import

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

export

Cette opération permet d'exporter une donnée hors de la TOE. Elle s'applique dans le PP aux politiques de sécurité VPN stockées dans la TOE ainsi que l'export de données applicative et topologique.

use

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

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 confidentialité et/ou authenticité (i.e., la politique de sécurité associée), pour le transfert vers le chiffreur IP, via le canal VPN.

5.1.1.4 Attributs

AT.user_type

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

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.

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 (c.f. description de l'attribut AT.user_id). Il s'agit d'un attribut de l'objet OB.vpn_policies.

AT.VPN_link_id

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

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.

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

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.

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.

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.

U.encrypter_system_component

Cet utilisateur représente un composant système de chiffrement dans lequel s'insère l'application VPN cliente. Il est chargé de l'authentification des utilisateurs et des administrateurs communiquant avec la TOE.

Note d'application: ce composant peut-être par exemple:

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

Note d'application générale à ce paragraphe:

Les applications émettant et recevant les données OB.data (auxquels sont appliquées les politiques VPN) ne sont pas considérées comme des "utilisateurs" au sens Critères Communs. En effet, l'import et l'export d'informations vers celles-ci ne nécessitent pas dans ce PP de protections particulières, de ce fait le traitement de ces fonctions n'entre pas dans le cadre de la sécurité.

Cependant, le rédacteur d'une cible conforme à ce PP pourra introduire cet utilisateur dans les exigences si des menaces particulières sont envisagées lors du transfert d'information entre la TOE et les applications.

5.1.2 Provided service

5.1.2.1 VPN communication link management

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

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

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

Raffinement non-éditorial:

Les user data sont les données applicatives et topologiques contenues dans les paquets IP échangés entre la TOE et un chiffreur IP.

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

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.

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

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

Raffinement non-éditorial:

Les user data sont les données applicatives et topologiques contenues dans les paquets IP échangés entre la TOE et un chiffreur IP.

5.1.2.2 Data access protection

FDP_IFC.1/DATA Subset information flow control

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

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**

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**.

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:**

- **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"),**
  - **the user linked to S.user_manager is allowed to use the OB.vpn_policies (ie. 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"),**
  - **the user linked to S.user_manager is allowed to use the OB.vpn_policies (ie. 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)**.

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

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

5.1.2.3 Data authenticity

FDP_UIT.1/DATA Data exchange integrity

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 **replay, deletion and modification** errors.

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

Raffinement non éditorial:

User data are applicative data and topologic data (OB.data) contained in IP packets provided to the subject that manages VPN communications (S.communication_manager).

In this requirement the TSF communicates with the user U.IP_encrypter.

Note d'application

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

FCO_NRO.1/DATA Selective proof of origin

FCO_NRO.1.1/DATA The TSF shall be able to generate evidence of origin for transmitted **applicative and topologic data (OB.data)** at the request of the **[assignment: list of third parties]**.

FCO_NRO.1.2/DATA The TSF shall be able to relate the **[assignment: list of attributes]** of the originator of the information, and the **[assignment: list of information fields]** of the information to which the evidence applies.

FCO_NRO.1.3/DATA The TSF shall provide a capability to verify the evidence of origin of information to **[assignment: list of third parties]** given **[assignment: limitations on the evidence of origin]**.

Note d'application

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

Les données applicatives et topologiques mentionnées dans l'exigence transitent entre la TOE et un chiffreur IP.

5.1.2.4 Data confidentiality

FDP_UCT.1/DATA Basic data exchange confidentiality

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.

Raffinement non éditorial:

User data are applicative data and topologic data (OB.data) contained in IP packets provided by the subject that manages VPN communications (S.communication_manager).

In this requirement the TSF communicates with the user 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

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

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

5.1.3.1 User authentication

FIA_UID.2/USER User identification before any action

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.

Raffinement non éditorial:

The user considered in this requirement is U.user.

The identification must be performed by a component of the encryption system (U.encrypter_system_component).

FIA_UAU.2/USER User authentication before any action

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.

Raffinement non-éditorial:

The user considered in this requirement is U.user.

The authentication must be performed by a component of the encryption system (U.encrypter_system_component).

The authentication mechanism must meet [AUTH] requirements.

FIA_USB.1/USER User-subject binding

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**.

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 "**.

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: **[assignment: rules for the changing of attributes]**.

Raffinement non éditorial:

The user considered in this requirement is U.user.

The subject considered in this requirement is S.user_manager.

5.1.3.2 Administrator authentication

FIA_UID.2/ADMIN User identification before any action

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

Raffinement non éditorial:

The user considered in this requirement is U.administrator.

FIA_UAU.2/ADMIN User authentication before any action

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

Raffinement non-éditorial:

The user considered in this requirement is U.administrator.

The authentication must be performed by a component of the encryption system (U.encrypter_system_component).

The authentication mechanism must meet [AUTH] requirements.

FIA_USB.1/ADMIN User-subject binding

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

- **AT.user_type**.

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

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

FIA_USB.1.3/ADMIN The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: rules for the changing of attributes]**.

Raffinement non-éditorial:

The user considered in this requirement is U.administator.

The subject considered in this requirement is S.user_manager.

5.1.4 Security attributes management

FMT_MSA.3 Static attribute initialisation

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.

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

Raffinement non éditorial:

The TSF shall assign the value "null" to the security attributes AT.user_type and AT.user_id whenever a subject S.user_manager is created.

FMT_MSA.1/MODIFY Management of security attributes

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

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

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

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

FDP_IFF.1/KEY_IMPORT Simple security attributes

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**	

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**.

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

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

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

Note d'application

Les utilistateurs U.user et U.adminstrator doivent être authentifés auprès de la TOE.

5.1.5.2 Cryptographic key import

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

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.

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

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 security attributes**.

FDP_UCT.1/KEY_IMPORT Basic data exchange confidentiality

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.

Raffinement non éditorial:

User data are the values of secret and private cryptographic keys provided to the subject that manages the communication with the users (S.user_manager).

FDP_UIT.1/KEY_IMPORT Data exchange integrity

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 **replay, deletion and modification** errors.

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

Raffinement non éditorial:

User data are the values of secret and private cryptographic keys provided to the subject that manages the communication with the users (S.user_manager).

5.1.6 VPN security policies management

5.1.6.1 VPN security policies import/export

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

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

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

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

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

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

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

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

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

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

5.1.6.2 VPN security policies properties

FDP_UCT.1/VPN_POL Basic data exchange confidentiality

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

FDP_UIT.1/VPN_POL Data exchange integrity

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

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

5.1.6.3 Divers

FDP_IFC.1/VPN_POL Subset information flow control

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

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

FDP_IFF.1/VPN_POL Simple security attributes

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

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

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

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

- **Rule 3: the subject S.communication_manager is allowed to perform application of OB.vpn_policies**.

FDP_IFF.1.3/VPN_POL The TSF shall enforce the

- **any user can trigger the export of a VPN security policy,**
- **[assignment: additional information flow control SFP rules]**.

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

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

5.1.7 Cryptography

La génération de clés cryptographiques ne fait pas partie de la définition du problème de sécurité de ce PP mais peut être considérée dans une ST se réclamant conforme à celui-ci. Le rédacteur de la cible pourra utiliser l'exigence FCS_CKM.1 avec **[CRYPTO]** comme standard cryptographique et introduire les exigences fonctionnelles nécessaires pour couvrir les dépendances de FCS_CKM.1, à savoir: (FCS_CKM.2 ou FCS_COP.1) et (FCS_CKM.4).

FCS_COP.1 Cryptographic operation

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

FCS_CKM.3 Cryptographic key access

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

Raffinement non éditorial:

When the lifetime of a key is over, another key must be used for communication on VPN links. The list of standards shall meet [CRYPTO] and [CRYPTO_GESTION] requirements.

5.2 Exigences de sécurité d'assurance

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

6 Argumentaires

6.1 Objectifs de sécurité / problème de sécurité

6.1.1 Menaces

6.1.1.1 Menaces portant sur les communications

T.REJEU Pour prévenir la menace:

- aucune action.

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

- détecter le rejeu d'opérations d'administration (O.PROTECTION_REJEU).

Pour réagir à la menace, la TOE doit:

- annuler l'opération d'administration victime de rejeu (O.PROTECTION_REJEU).

T.USURPATION_ADMIN Pour prévenir la menace:

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

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

- aucune action.

Pour réagir à la menace, la TOE doit:

- aucune action.

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).

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

- aucune action.

Pour réagir à la menace, la TOE doit:

- aucune action.

6.1.1.2 Menaces portant sur la gestion des clés cryptographiques

T.MODIFICATION_CLES Pour prévenir la menace:

- o la TOE doit garantir la protection des clés cryptographiques en intégrité lors de leur stockage (O.PROTECTION_CLES),
- o la TOE doit authentifier les utilisateurs et administrateurs, afin de pouvoir déterminer leurs droits d'accès (O.AUTHENTIFICATION_UTILISATEUR et O.AUTHENTIFICATION_ADMIN).
- o la TOE n'autorise que les utilisateurs et administrateurs authentifiés à importer des clés cryptographiques dans la TOE (O.IMPORT_CLES),
- o le composant authentifiant doit être certifié au niveau standard (OE.COMPOSANT_AUTHENTIFIANT),

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

- o détecter la perte d'intégrité des clés cryptographiques lors de leur import en local (O.PROTECTION_CLES),
- o détecter la perte d'intégrité des clés cryptographiques lors de leur import à distance (O.PROTECTION_FLUX_ADMIN),

Pour réagir à la menace, la TOE doit:

- o annuler toute opération d'import local de clés cryptographiques dont la perte d'intégrité serait détectée (O.PROTECTION_CLES),
- o annuler toute opération d'import à distance de clés cryptographiques dont la perte d'intégrité serait détectée (O.PROTECTION_FLUX_ADMIN).

T.DIVULGATION_CLES Pour prévenir la menace:

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

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

- o aucune action

Pour réagir à la menace, la TOE doit:

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

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

T.MODIFICATION_POL Pour prévenir la menace:

- o la TOE doit garantir la protection en intégrité des politiques VPN lors de leur stockage (O.PROTECTION_POL),
- o la TOE doit authentifier les administrateurs, afin de pouvoir déterminer leurs droits d'accès (O.AUTHENTIFICATION_ADMIN).
- o la TOE doit autoriser uniquement les administrateurs authentifiés à importer des politiques de sécurité dans la TOE (O.IMPORT_POL),
- o le composant authentifiant doit être certifié au niveau standard (OE.COMPOSANT_AUTHENTIFIANT).

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

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

Pour réagir à la menace, la TOE doit:

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

T.DIVULGATION_POL Pour prévenir la menace:

- o la TOE doit garantir la protection en confidentialité des politiques VPN lors de leur import et leur export en local (O.PROTECTION_POL),
- o la TOE doit garantir la protection en confidentialité des politiques VPN lors de leur import et leur export à distance (O.PROTECTION_FLUX_ADMIN),
- o la TOE doit authentifier administrateurs, afin de pouvoir déterminer leurs droits d'accès (O.AUTHENTIFICATION_ADMIN).
- o la TOE doit n'autoriser que les administrateurs authentifiés à importer des politiques de sécurité dans la TOE (O.IMPORT_POL),
- o le composant authentifiant doit être certifié au niveau standard (OE.COMPOSANT_AUTHENTIFIANT).

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

- o aucune action

Pour réagir à la menace, la TOE doit:

- o aucune action

6.1.2 Politiques de sécurité organisationnelles (OSP)

6.1.2.1 Services rendus

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.

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.

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).

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

6.1.2.2 Autres services

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).

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

6.1.3 Hypothèses

6.1.3.1 Interactions avec la TOE

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

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.

A.EQUIPEMENT_TELEADMINISTRATION Cette hypothèse est entièrement supportée par OE.EQUIPEMENT_TELEADMINISTRATION qui assure la disponibilité de l'équipement de téléadministration centralisé ainsi que l'accès restreint et sécurisé à celui-ci.

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.

A.COMPOSANT_AUTHENTIFIANT Cette hypothèse est entièrement supportée par OE.COMPOSANT_AUTHENTIFIANT qui assure la qualification de l'équipement du système de chiffrement permettant l'authentification au niveau standard défini par la DCSSI dans [QUA-STD].

6.1.3.2 Machine hôte

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.

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

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.

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

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.

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.

6.1.3.3 Réinitialisation

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

6.1.3.4 Cryptographie

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.

6.1.4 Tables de couverture entre définition du problème et objectifs de sécurité

Menaces	Objectifs de sécurité	Argumentaire
T.REJEU	O.PROTECTION_REJEU	Section 6.1.1
T.USURPATION_ADMIN	O.AUTHENTIFICATION_ADMIN, OE.COMPOSANT_AUTHENTIFIANT, OE.ACCES	Section 6.1.1
T.USURPATION_UTILISATEUR	O.AUTHENTIFICATION_UTILISATEUR, OE.COMPOSANT_AUTHENTIFIANT, OE.ACCES	Section 6.1.1

Menaces	Objectifs de sécurité	Argumentaire
T.MODIFICATION_CLES	O.PROTECTION_CLES, O.AUTHENTIFICATION_UTILISATEUR, OE.COMPOSANT_AUTHENTIFIANT, O.AUTHENTIFICATION_ADMIN, O.IMPORT_CLES, O.PROTECTION_FLUX_ADMIN	Section 6.1.1
T.DIVULGATION_CLES	O.PROTECTION_CLES, OE.COMPOSANT_AUTHENTIFIANT, O.AUTHENTIFICATION_UTILISATEUR, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, O.CRYPTO, O.IMPORT_CLES, OE.EXPORT_CLES, OE.REINITIALISATION	Section 6.1.1
T.MODIFICATION_POL	O.IMPORT_POL, OE.COMPOSANT_AUTHENTIFIANT, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, OE.REINITIALISATION	Section 6.1.1
T.DIVULGATION_POL	OE.COMPOSANT_AUTHENTIFIANT, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, O.IMPORT_POL	Section 6.1.1

Tableau 1 Association menaces vers objectifs de sécurité

Objectifs de sécurité	Menaces
O.APPLICATION_POL	
O.CONFIDENTIALITE_APPLI	
O.AUTHENTICITE_APPLI	
O.CONFIDENTIALITE_TOPO	
O.AUTHENTICITE_TOPO	
O.AUTHENTIFICATION_ADMIN	T.USURPATION_ADMIN, T.MODIFICATION_CLES, T.DIVULGATION_CLES, T.MODIFICATION_POL, T.DIVULGATION_POL
O.AUTHENTIFICATION_UTILISATEUR	T.USURPATION_UTILISATEUR , T.MODIFICATION_CLES, T.DIVULGATION_CLES
O.IMPORT_CLES	T.MODIFICATION_CLES, T.DIVULGATION_CLES
O.PROTECTION_CLES	T.MODIFICATION_CLES, T.DIVULGATION_CLES
O.IMPORT_POL	T.MODIFICATION_POL, T.DIVULGATION_POL
O.PROTECTION_POL	T.MODIFICATION_POL, T.DIVULGATION_POL
O.PROTECTION_REJEU	T.REJEU
O.PROTECTION_FLUX_ADMIN	T.MODIFICATION_CLES, T.DIVULGATION_CLES, T.MODIFICATION_POL, T.DIVULGATION_POL
O.CRYPTO	T.DIVULGATION_CLES
OE.ADMIN	
OE.UTILISATEUR	
OE.EQUIPEMENT_TELEADMINISTRATION	
OE.CHIFFREUR_IP	
OE.COMPOSANT_AUTHENTIFIANT	T.USURPATION_ADMIN, T.USURPATION_UTILISATEUR , T.MODIFICATION_CLES, T.DIVULGATION_CLES, T.MODIFICATION_POL, T.DIVULGATION_POL
OE.MACHINE	
OE.DROITS_UTILISATEURS	
OE.CONFIGURATION	

Objectifs de sécurité	Menaces
OE.COMM	
OE.EXPORT_CLES	T.DIVULGATION_CLES
OE.MULTI-UTILISATEURS	
OE.REINITIALISATION	T.DIVULGATION_CLES, T.MODIFICATION_POL
OE.CRYPTO	
OE.ACCES	T.USURPATION_ADMIN, T.USURPATION_UTILISATEUR

Tableau 2 Association objectifs de sécurité vers menaces

Politiques de sécurité organisationnelles (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	Section 6.1.2
OSP.CRYPTO	O.CRYPTO, OE.CRYPTO	Section 6.1.2
OSP.EXPORT_POL	O.PROTECTION_POL	Section 6.1.2

Tableau 3 Association politiques de sécurité organisationnelles vers objectifs de sécurité

Objectifs de sécurité	Politiques de sécurité organisationnelles (OSP)
O.APPLICATION_POL	OSP.SERVICES_RENDUS
O.CONFIDENTIALITE_APPLI	OSP.SERVICES_RENDUS
O.AUTHENTICITE_APPLI	OSP.SERVICES_RENDUS
O.CONFIDENTIALITE_TOPO	OSP.SERVICES_RENDUS
O.AUTHENTICITE_TOPO	OSP.SERVICES_RENDUS
O.AUTHENTIFICATION_ADMIN	
O.AUTHENTIFICATION_UTILISATEUR	OSP.SERVICES_RENDUS
O.IMPORT_CLES	
O.PROTECTION_CLES	
O.IMPORT_POL	
O.PROTECTION_POL	OSP.EXPORT_POL
O.PROTECTION_REJEU	
O.PROTECTION_FLUX_ADMIN	
O.CRYPTO	OSP.CRYPTO
OE.ADMIN	
OE.UTILISATEUR	
OE.EQUIPEMENT_TELEADMINISTRATION	
OE.CHIFFREUR_IP	OSP.SERVICES_RENDUS
OE.COMPOSANT_AUTHENTIFIANT	
OE.MACHINE	
OE.DROITS_UTILISATEURS	OSP.SERVICES_RENDUS
OE.CONFIGURATION	
OE.COMM	
OE.EXPORT_CLES	
OE.MULTI-UTILISATEURS	
OE.REINITIALISATION	
OE.CRYPTO	OSP.CRYPTO
OE.ACCES	OSP.SERVICES_RENDUS

Tableau 4 Association objectifs de sécurité vers politiques de sécurité organisationnelles

Hypothèses	Objectifs de sécurité pour l'environnement opérationnel	Argumentaire
A.ADMIN	OE.ADMIN	Section 6.1.3
A.UTILISATEUR	OE.UTILISATEUR	Section 6.1.3
A.EQUIPEMENT_TELEADMINISTRATION	OE.EQUIPEMENT_TELEADMINISTRATION	Section 6.1.3
A.CHIFFREUR_IP	OE.CHIFFREUR_IP	Section 6.1.3
A.COMPOSANT_AUTHENTIFIANT	OE.COMPOSANT_AUTHENTIFIANT	Section 6.1.3
A.MACHINE	OE.MACHINE	Section 6.1.3
A.DROITS_UTILISATEUR	OE.DROITS_UTILISATEURS	Section 6.1.3
A.CONFIGURATION	OE.CONFIGURATION, OE.COMM	Section 6.1.3
A.COMM	OE.COMM	Section 6.1.3
A.EXPORT_CLES	OE.EXPORT_CLES	Section 6.1.3
A.MULTI-UTILISATEURS	OE.MULTI-UTILISATEURS	Section 6.1.3
A.REINITIALISATION	OE.REINITIALISATION	Section 6.1.3
A.ACCES	OE.ACCES	Section 6.1.3

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

Objectifs de sécurité pour l'environnement opérationnel	Hypothèses
OE.ADMIN	A.ADMIN
OE.UTILISATEUR	A.UTILISATEUR
OE.EQUIPEMENT_TELEADMINISTRATION	A.EQUIPEMENT_TELEADMINISTRATION
OE.CHIFFREUR_IP	A.CHIFFREUR_IP
OE.COMPOSANT_AUTHENTIFIANT	A.COMPOSANT_AUTHENTIFIANT
OE.MACHINE	A.MACHINE
OE.DROITS_UTILISATEURS	A.DROITS_UTILISATEUR
OE.CONFIGURATION	A.CONFIGURATION
OE.COMM	A.CONFIGURATION, A.COMM
OE.EXPORT_CLES	A.EXPORT_CLES
OE.MULTI-UTILISATEURS	A.MULTI-UTILISATEURS
OE.REINITIALISATION	A.REINITIALISATION
OE.CRYPTO	
OE.ACCES	A.ACCES

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

6.2 Exigences de sécurité / objectifs de sécurité

6.2.1 Objectifs

6.2.1.1 Objectifs de sécurité pour la TOE

Objectifs de sécurité pour les services rendus par la TOE

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,

o FDP_IFC.1/KEY_IMPORT qui définit la politique de contrôle de flux des keys,

o FDP_IFF.1/KEY_IMPORT qui assure l'accès aux clés afin d'assurer les protections spécifiées dans les politiques de sécurité VPN,

o FMT_MSA.1/QUERY, FMT_MSA.1/MODIFY, FDP_IFC.1/VPN_POL et FDP_IFF.1/VPN_POL qui assure l'accès aux politiques VPN et à leurs attributs afin qu'elles soient appliquées,

o FDP_ITC.2/VPN_POL qui assure que les politiques de sécurité VPN stockées dans la TOE sont associées à un nom d'utilisateur et un lien VPN,

o 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

o FMT_MSA.1/QUERY qui autorise l'accès à l'identifiant de l'utilisateur,

o 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.

O.CONFIDENTIALITE_APPLI Cet objectif se traduit par:

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

O.AUTHENTICITE_APPLI Cet objectif se traduit par:

o FDP_UIT.1/DATA qui assure l'intégrité des données applicatives transitant entre le chiffreur IP et la TOE.

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

O.CONFIDENTIALITE_TOPO Cet objectif se traduit par:

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

O.AUTHENTICITE_TOPO Cet objectif se traduit par:

o FDP_UIT.1/DATA qui assure l'intégrité des données topologiques transitant entre le chiffreur IP et TOE.

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

Objectifs de sécurité pour protéger les biens sensibles de la TOE

Authentification

O.AUTHENTIFICATION_ADMIN L'objectif se traduit par:

o FIA_UAU.2/ADMIN pour assurer l'authentification de l'administrateur par un composant du système de chiffrement et la vérification de cette authentification avant de permettre la liaison au sujet S.user_manager qui effectue (en particulier)

les commandes d'administration (i.e. import et export des biens sensibles de la TOE) (FDP_IFC.1/KEY_IMPORT, FDP_IFF.1/KEY_IMPORT, FDP_IFC.1/VPN_POL et FDP_IFF.1/VPN_POL). Pour être reconnu comme authentifié auprès de la TOE, l'administrateur devra se lier au sujet S.user_manager afin de poser l'attribut AT.user_type à *"administrator"* (FIA_USB.1/ADMIN). Cet attribut est initialisé par défaut à une valeur restrictive pour se prémunir contre toute tentative d'outrepassement des mécanismes de sécurité de la TOE (FMT_MSA.3), il est modifiable (FMT_MSA.1/MODIFY) et consultable (FMT_MSA.1/QUERY).

- sa dépendance FIA_UID.2/ADMIN pour assurer l'identification de l'administrateur qui tente de se lier au sujet cité ci-dessus.

O.AUTHENTIFICATION_UTILISATEUR L'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),
  - avant que la TOE autorise l'établissement de liens VPN (FMT_MSA.1/QUERY permet d'acceder 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),
- sa dépendance FIA_UID.2/USER pour assurer l'identification de l'utilisateur qui tente de se lier au sujet cité ci-dessus.

Gestion des clés cryptographiques

O.IMPORT_CLES 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 a'git 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

O.PROTECTION_CLES 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_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.

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.

Gestion des politiques de sécurité VPN

O.IMPORT_POL Cet objectif se traduit par:

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

O.PROTECTION_POL Cet objectif se traduit par:

- FDP_UCT.1/VPN_POL qui assure la confidentialité des politiques de sécurité VPN importées et exportées dans la TOE (donc en particulier, lorsqu'elles sont importées localement),
- FDP_UIT.1/VPN_POL qui assure la détection de toute perte d'intégrité des politiques de sécurité VPN importées et exportées dans la TOE (donc en particulier, lorsqu'elles sont importées localement),
- FDP_IFF.1/DATA qui assure que l'intégrité des politiques de sécurité VPN est vérifiée lors de leur utilisation (i.e. leur application à des données, pour envoi sur

le lien VPN); ceci assure ainsi que le stockage les a protégé en intégrité. En réponse, si une perte d'intégrité est détectée, le lien VPN ne pourra pas s'établir.

- FIA_USB.1/ADMIN qui permet de déterminer qu'un administrateur s'est authentifié comme tel auprès de la TSF,
- FMT_MSA.3 qui assure que l'attribut AT.user_type est initialisé par défaut à une valeur restrictive afin de se prémunir contre toute tentative d'outrepassement des mécanismes de sécurité de la TOE,
- FDP_ETC.1/VPN_POL qui assure que l'export n'est autorisé que vers un administrateur authentifié comme tel auprès de la TSF (FMT_MSA.1/QUERY permet de déterminer si l'utilisateur est un administrateur),
- FDP_IFF.1/VPN_POL pour
  - exprimer que seul le sujet S.user_manager peut exporter des politiques de sécurité VPN,
  - exprimer que l'import de politiques de sécurité VPN est soumis à un contrôle d'accès; participant ainsi à la protection en intégrité des politiques de sécurité VPN lors de leur stockage.

Administration à distance

O.PROTECTION_REJEU Cet objectif se traduit par les exigences suivantes, qui assurent que le rejeu d'opération d'administration est détecté et l'opération annulée:

- lors de l'import et de l'export de politiques de sécurité VPN dans la TOE (FDP_UIT.1/VPN_POL),
- lors de l'import de clés cryptographiques dans la TOE (FDP_UIT.1/KEY_IMPORT).

O.PROTECTION_FLUX_ADMIN Cet objectif se traduit par:

- FDP_UCT.1/VPN_POL qui assure la confidentialité des politiques de sécurité VPN importées et exportées dans la TOE (donc en particulier, contenues dans les flux d'administration transmis vers la TOE),
- FDP_UIT.1/VPN_POL qui assure la détection de toute perte d'intégrité des politiques de sécurité VPN importées dans la TOE (donc en particulier, contenues dans les flux d'administration transmis vers la TOE). Elle assure aussi l'annulation de l'import en cas d'anomalie,
- FDP_UCT.1/KEY_IMPORT qui assure la confidentialité des clés cryptographiques importées dans la TOE (donc en particulier, contenues dans les flux d'administration transmis vers la TOE),
- FDP_UIT.1/KEY_IMPORT qui assure la détection de toute perte d'intégrité des clés cryptographiques importées dans la TOE (donc en particulier, contenues dans les flux d'administration transmis vers la TOE).

Gestion de la cryptographie

O.CRYPTO Cet objectif se traduit par:

- FCS_COP.1 qui assure l'utilisation de fonctions cryptographiques conformes au référentiel cryptographique de la DCSSI,
- FCS_CKM.3 qui assure que la TOE met en oeuvre des mécanismes imposant le renouvellement des clés cryptographiques.

6.2.2 Tables de couverture entre objectifs et exigences de sécurité

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.APPLICATION_POL	FDP_IFF.1/DATA, FMT_MSA.3, FIA_USB.1/USER, FDP_ITC.2/VPN_POL, FMT_MSA.1/QUERY, FDP_IFF.1/KEY_IMPORT, FDP_IFF.1/VPN_POL, FDP_ETC.1/EXPORT, FDP_ITC.1/IMPORT, FDP_IFC.1/DATA, FDP_IFC.1/VPN_POL, FMT_MSA.1/MODIFY, FDP_IFC.1/KEY_IMPORT	Section 6.2.1
O.CONFIDENTIALITE_APPLI	FDP_UCT.1/DATA	Section 6.2.1
O.AUTHENTICITE_APPLI	FDP_UIT.1/DATA, FCO_NRO.1/DATA	Section 6.2.1
O.CONFIDENTIALITE_TOPO	FDP_UCT.1/DATA	Section 6.2.1
O.AUTHENTICITE_TOPO	FDP_UIT.1/DATA, FCO_NRO.1/DATA	Section 6.2.1
O.AUTHENTIFICATION_ADMIN	FIA_UID.2/ADMIN, FIA_UAU.2/ADMIN, FDP_IFC.1/KEY_IMPORT, FDP_IFC.1/VPN_POL, FIA_USB.1/ADMIN, FMT_MSA.1/MODIFY, FMT_MSA.3, FDP_IFF.1/KEY_IMPORT, FMT_MSA.1/QUERY, FDP_IFF.1/VPN_POL	Section 6.2.1
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	Section 6.2.1

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
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	Section 6.2.1
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	Section 6.2.1
O.IMPORT_POL	FMT_MSA.3, FIA_USB.1/ADMIN, FDP_IFF.1/VPN_POL, FDP_ITC.2/VPN_POL, FDP_IFC.1/VPN_POL, FMT_MSA.1/QUERY	Section 6.2.1
O.PROTECTION_POL	FDP_UCT.1/VPN_POL, FDP_UIT.1/VPN_POL, FIA_USB.1/ADMIN, FMT_MSA.3, FDP_IFF.1/DATA, FDP_IFF.1/VPN_POL, FDP_ETC.1/VPN_POL, FMT_MSA.1/QUERY	Section 6.2.1
O.PROTECTION_REJEU	FDP_UIT.1/KEY_IMPORT, FDP_UIT.1/VPN_POL	Section 6.2.1
O.PROTECTION_FLUX_ADMIN	FDP_UCT.1/KEY_IMPORT, FDP_UIT.1/KEY_IMPORT, FDP_UCT.1/VPN_POL, FDP_UIT.1/VPN_POL	Section 6.2.1
O.CRYPTO	FCS_COP.1, FCS_CKM.3	Section 6.2.1

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

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_ETC.1/EXPORT	O.APPLICATION_POL, O.AUTHENTIFICATION_UTILISATEUR
FDP_ITC.1/IMPORT	O.APPLICATION_POL, O.AUTHENTIFICATION_UTILISATEUR
FDP_IFC.1/DATA	O.APPLICATION_POL, O.PROTECTION_CLES, O.AUTHENTIFICATION_UTILISATEUR
FDP_IFF.1/DATA	O.APPLICATION_POL, O.PROTECTION_CLES, O.PROTECTION_POL, O.AUTHENTIFICATION_UTILISATEUR
FDP_UIT.1/DATA	O.AUTHENTICITE_APPLI, O.AUTHENTICITE_TOPO
FCO_NRO.1/DATA	O.AUTHENTICITE_APPLI, O.AUTHENTICITE_TOPO
FDP_UCT.1/DATA	O.CONFIDENTIALITE_APPLI, O.CONFIDENTIALITE_TOPO
FIA_UID.2/USER	O.AUTHENTIFICATION_UTILISATEUR
FIA_UAU.2/USER	O.AUTHENTIFICATION_UTILISATEUR
FIA_USB.1/USER	O.APPLICATION_POL, O.AUTHENTIFICATION_UTILISATEUR, O.IMPORT_CLES
FIA_UID.2/ADMIN	O.AUTHENTIFICATION_ADMIN
FIA_UAU.2/ADMIN	O.AUTHENTIFICATION_ADMIN
FIA_USB.1/ADMIN	O.AUTHENTIFICATION_ADMIN, O.IMPORT_CLES, O.IMPORT_POL, O.PROTECTION_POL
FMT_MSA.3	O.APPLICATION_POL, O.AUTHENTIFICATION_ADMIN, O.AUTHENTIFICATION_UTILISATEUR, O.IMPORT_CLES, O.IMPORT_POL, O.PROTECTION_POL
FMT_MSA.1/MODIFY	O.APPLICATION_POL, O.AUTHENTIFICATION_ADMIN, O.AUTHENTIFICATION_UTILISATEUR, O.IMPORT_CLES
FMT_MSA.1/QUERY	O.APPLICATION_POL, O.AUTHENTIFICATION_ADMIN, O.AUTHENTIFICATION_UTILISATEUR, O.IMPORT_CLES, O.IMPORT_POL, O.PROTECTION_POL

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_IFC.1/KEY_IMPORT	O.APPLICATION_POL, O.AUTHENTIFICATION_ADMIN, O.IMPORT_CLES, O.AUTHENTIFICATION_UTILISATEUR
FDP_IFF.1/KEY_IMPORT	O.APPLICATION_POL, O.AUTHENTIFICATION_ADMIN, O.IMPORT_CLES, O.AUTHENTIFICATION_UTILISATEUR
FDP_ITC.1/KEY_IMPORT	O.IMPORT_CLES, O.PROTECTION_CLES
FDP_UCT.1/KEY_IMPORT	O.PROTECTION_CLES, O.PROTECTION_FLUX_ADMIN
FDP_UIT.1/KEY_IMPORT	O.PROTECTION_CLES, O.PROTECTION_REJEU, O.PROTECTION_FLUX_ADMIN
FDP_ETC.1/VPN_POL	O.PROTECTION_POL
FDP_ITC.2/VPN_POL	O.APPLICATION_POL, O.IMPORT_POL
FDP_UCT.1/VPN_POL	O.PROTECTION_POL, O.PROTECTION_FLUX_ADMIN
FDP_UIT.1/VPN_POL	O.PROTECTION_POL, O.PROTECTION_REJEU, O.PROTECTION_FLUX_ADMIN
FDP_IFC.1/VPN_POL	O.APPLICATION_POL, O.AUTHENTIFICATION_ADMIN, O.IMPORT_POL
FDP_IFF.1/VPN_POL	O.APPLICATION_POL, O.AUTHENTIFICATION_ADMIN, O.IMPORT_POL, O.PROTECTION_POL
FCS_COP.1	O.CRYPTO
FCS_CKM.3	O.CRYPTO

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

6.3 Dépendances

6.3.1 Dépendances des exigences de sécurité fonctionnelles

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

Exigences	Dépendances CC	Dépendances Satisfaites
FDP_UIT.1/KEY_IMPORT	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/KEY_IMPORT
FDP_ETC.1/VPN_POL	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/VPN_POL
FDP_ITC.2/VPN_POL	(FDP_ACC.1 ou FDP_IFC.1) et (FPT_TDC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/VPN_POL
FDP_UCT.1/VPN_POL	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/VPN_POL
FDP_UIT.1/VPN_POL	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/VPN_POL

Tableau 9 Dépendances des exigences fonctionnelles

6.3.1.1 Argumentaire pour les dépendances non satisfaites

La dépendance FMT_SMR.1 de FMT_MSA.3 n'est pas supportée. Les rôles sont definis 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 definis 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. Il n'y a pas de fonction de management des attributs specifique dans le modèle.

La dépendance FMT_SMR.1 de FMT_MSA.1/QUERY n'est pas supportée. Les rôles sont definis 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. Il n'y a pas de fonction de management des attributs specifique dans le modèle.

La dépendance FCS_CKM.4 de FCS_COP.1 n'est pas supportée. Cette dépendance n'est pas applicable puisque la destruction des clés n'entre pas dans le périmètre de la TOE.

La dépendance FCS_CKM.4 de FCS_CKM.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 or FTP_TRP.1 de FDP_UIT.1/DATA n'est pas supportée. Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.

La dépendance FIA_UID.1 de FCO_NRO.1/DATA n'est pas supportée. Cette dépendance n'est pas requise car l'authentification d'origine des trames émises et reçues par la TOE est indépendante de l'identification des utilisateurs ("user" et "administrator").

Par ailleurs l'utilisation de la TOE n'est pas subordonnée à l'identification de la TOE et du chiffreur.

La dépendance FTP_ITC.1 or 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 atributs de sécurité associés aux utilisateurs sont maintenus par le sujet S.user_manager.

La dépendance FIA_ATD.1 de FIA_USB.1/ADMIN n'est pas supportée. Cette dépendance n'est pas requise puisque les atributs 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 or 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 or FTP_TRP.1 de FDP_UIT.1/KEY_IMPORT n'est pas supportée. Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.

La dépendance FPT_TDC.1 de FDP_ITC.2/VPN_POL n'est pas supportée. Cette dépendance n'est pas applicable car l'administrateur qui importe les politiques de sécurité est de confiance et formate celles-ci de manière à être interprétées correctement par la TOE.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_ITC.2/VPN_POL n'est pas supportée. Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_UCT.1/VPN_POL n'est pas supportée. Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.

La dépendance FTP_ITC.1 or FTP_TRP.1 de FDP_UIT.1/VPN_POL n'est pas supportée. Cette dépendance n'est pas requise puisque la TOE n'utilise pas de canal ou de chemin sécurisé mais communique via des trames sécurisées.

6.3.2 Dépendances des exigences de sécurité d'assurance

Exigences	Dépendances CC	Dépendances Satisfaites
ADV_ARC.1	(ADV_FSP.1) et (ADV_TDS.1)	ADV_FSP.3, ADV_TDS.2

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

Tableau 10 Dépendances des exigences d'assurance

6.3.2.1 Argumentaire pour les dépendances non satisfaites

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

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

6.4 Argumentaire pour l'EAL

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

6.5 Argumentaire pour les augmentations à l'EAL

6.5.1 AVA_VAN.3 Focused vulnerability analysis

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

6.5.2 ALC_FLR.3 Systematic flaw remediation

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

7 Notice

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

Annexe A Complément de description de la TOE et de son environnement

A.1 Présentation des technologies VPN

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

A.1.1 IPsec

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

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

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

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

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

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

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

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

A.2 Positionnement physique de la TOE dans son environnement

Cette section a pour objectif de décrire, uniquement pour illustration, différents scénarios d'utilisation possibles décrivant le mode de fonctionnement du VPN nomade. Par souci de simplification, d'autres équipements réseaux rendant des services complémentaires au VPN (notamment, les routeurs, les concentrateurs Ethernet, les pare-feux, les différentes zones contrôlées par les pare-feux) qui peuvent être présents chez les utilisateurs ne sont pas présentés. Les aspects techniques liés à la haute disponibilité et au partage de charges pouvant également exister ne sont pas abordés.

L'application VPN cliente est installée sur une machine nomade qui possède une adresse IP dynamique ou statique délivrée par un fournisseur d'accès ou obtenue dans le réseau privé d'une organisation sur lequel est connecté le PC nomade. Compte tenu de la mobilité du poste nomade, l'adresse IP de celui-ci, quelle soit affectée dynamiquement ou statiquement, ne constitue pas un paramètre prédictible pouvant être utilisé pour identifier le PC nomade. Le chiffreur IP possède quant à lui une adresse IP publique prédictible. Le client VPN établit un lien VPN entre l'équipement nomade et le chiffreur IP pour pouvoir accéder au réseau privé de l'organisation. Dans certaines implémentations, la machine cliente peut alors se voir attribuer par le chiffreur IP une adresse IP privée (fixe ou prise dans un ensemble d'adresses) indépendamment de l'adresse publique non prédictible, permettant aux flux arrivant de ce nomade d'être confinés et cloisonnés dans des zones ou à des applications situées dans le réseau privé. L'utilisateur de la machine peut alors utiliser le réseau privé de manière transparente depuis l'extérieur de l'organisation.

Les données transitant entre la machine nomade et le réseau privé traversent ici des réseaux non sûrs et la machine peut être connectée à Internet par de nombreuses technologies d'accès, dans différents lieux et auprès de différents opérateurs :

- connexion depuis le domicile personnel en utilisant une connexion ADSL;
- connexion depuis un lieu public (hôtel, café, train, ...) en utilisant une technologie d'accès Wi-Fi ;
- connexion depuis le réseau local d'une entreprise ou d'une organisation partenaire.

A.2.1 Système de chiffrement sans équipement d'administration centralisé

Dans l'environnement illustré sur la figure 1, l'application VPN cliente fonctionne dans le contexte d'un système de chiffrement qui n'inclut pas de station d'administration « centralisée » (ni localisée sur le chiffreur IP qui termine les liens VPN des nomades, ni localisée à part sur une autre partie du réseau).

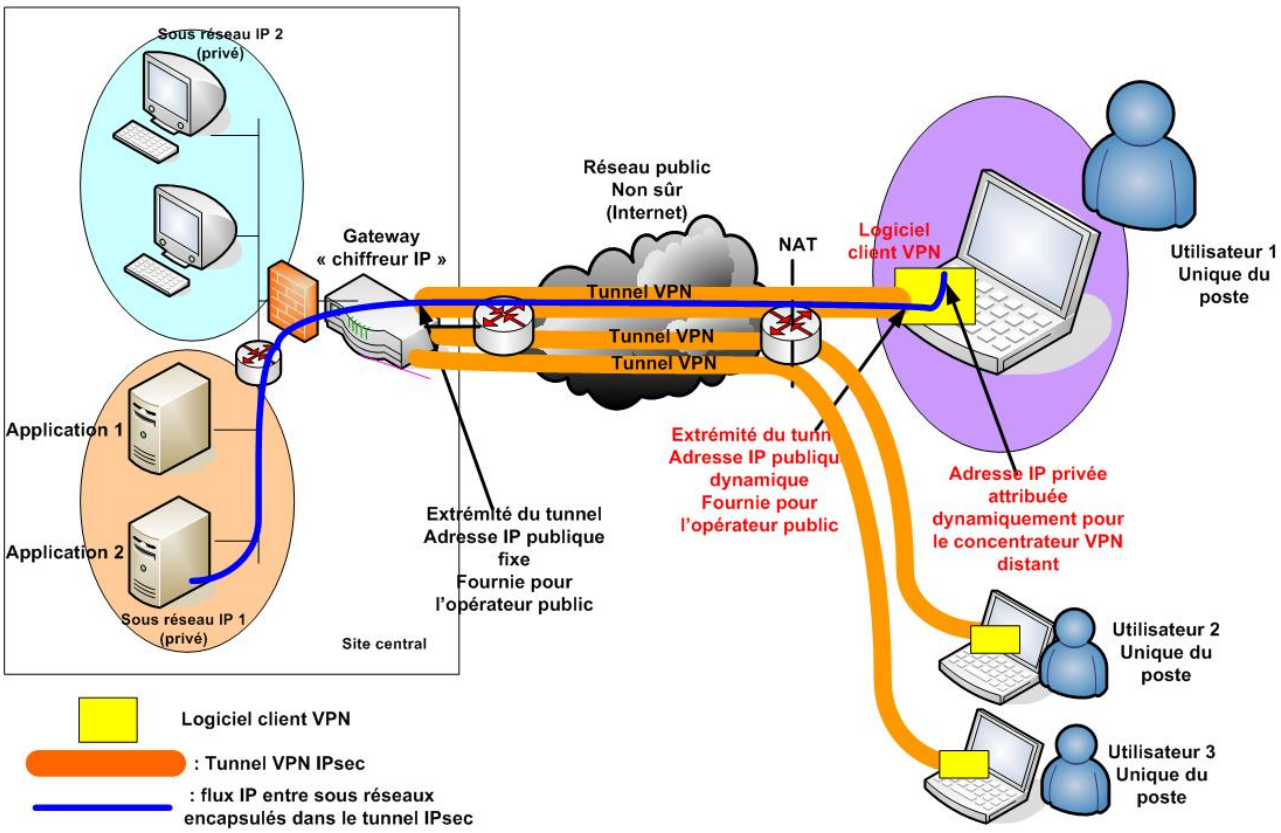

Figure 1. Fonctionnement sans équipement de téléadministration centralisée.

L'application VPN cliente ainsi que le chiffreur IP qui reçoit les connexions VPN des utilisateurs appliquent les politiques de sécurité VPN définies sur chaque extrémité. Ces politiques précisent par exemple, sur notre schéma, que les applications VPN clientes peuvent échanger des flux avec tous les équipements ou applications IP présents dans le sous-réseau IP 1 du site central de l'organisme (vers les applications 1 et 2).

Par contre, dans notre exemple, les applications VPN clientes ne peuvent pas émettre des flux vers les équipements ou applications situés dans le sous-réseau IP 2 du site central de ce même organisme.

A.2.2 Système de chiffrement avec équipement d'administration centralisé spécifique

Dans l'environnement illustré sur la figure 2, l'application VPN cliente fonctionne dans le contexte d'un système de chiffrement qui inclut une station d'administration « centralisée » localisée sur un brin réseau spécifique.

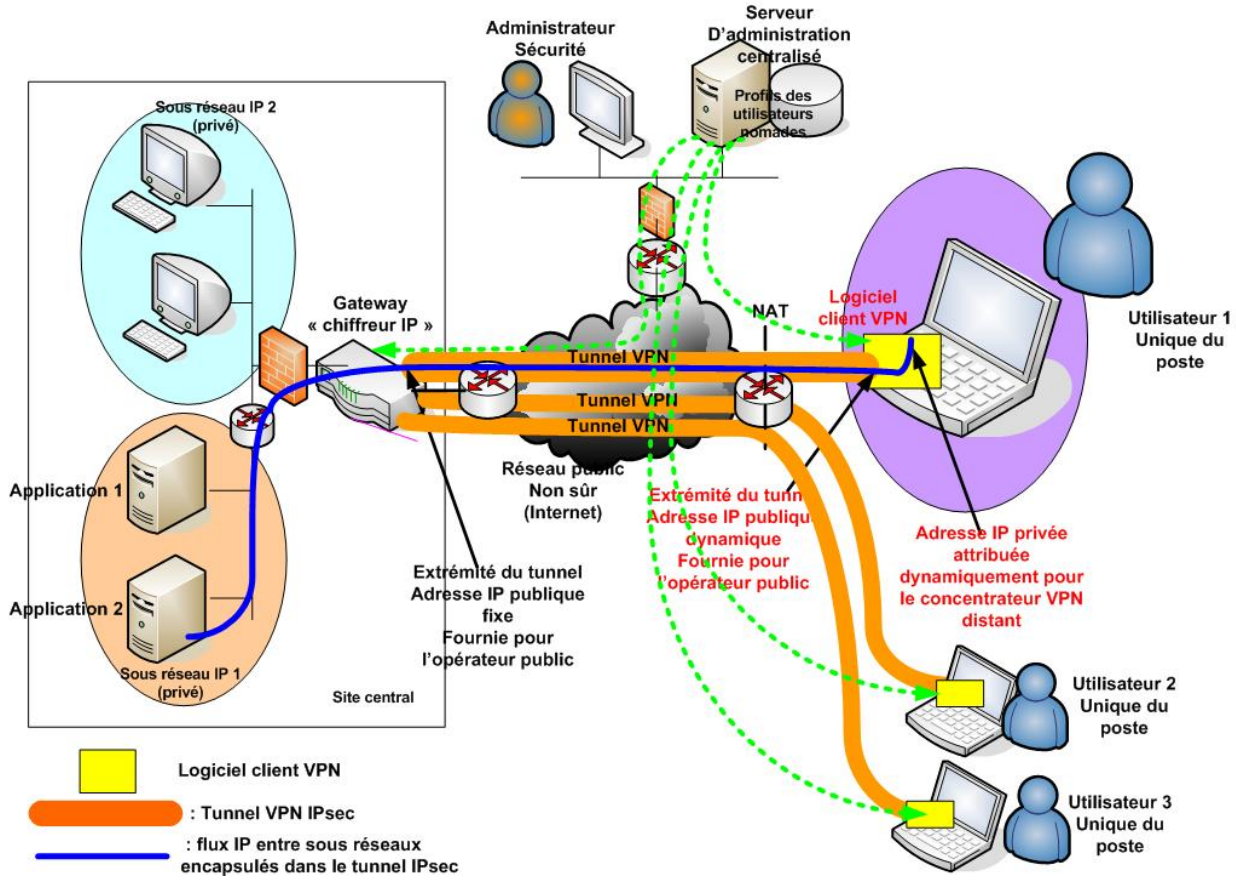

Figure 2. Fonctionnement avec équipement de téléadministration centralisée spécifique.

Les flux en vert sur le schéma correspondent aux flux d'administration. Dans ce cas d'utilisation, les applications VPN clientes viennent chercher leur politique de sécurité VPN sur la station d'administration (téléadministration) centralisée (la station d'administration importe les configurations vers les clients VPN, mais ce sont les clients VPN qui prennent l'initiative de la connexion vers la station d'administration car les adresses IP des clients VPN ne sont pas fixes).

A.2.3 Système de chiffrement avec administration centralisé sur un chiffreur IP

Dans l'environnement illustré sur la figure 3, l'application VPN cliente fonctionne dans le contexte d'un système de chiffrement qui inclut une station d'administration « centralisée » localisée sur le chiffreur IP qui termine les liens VPN avec les applications VPN clientes.

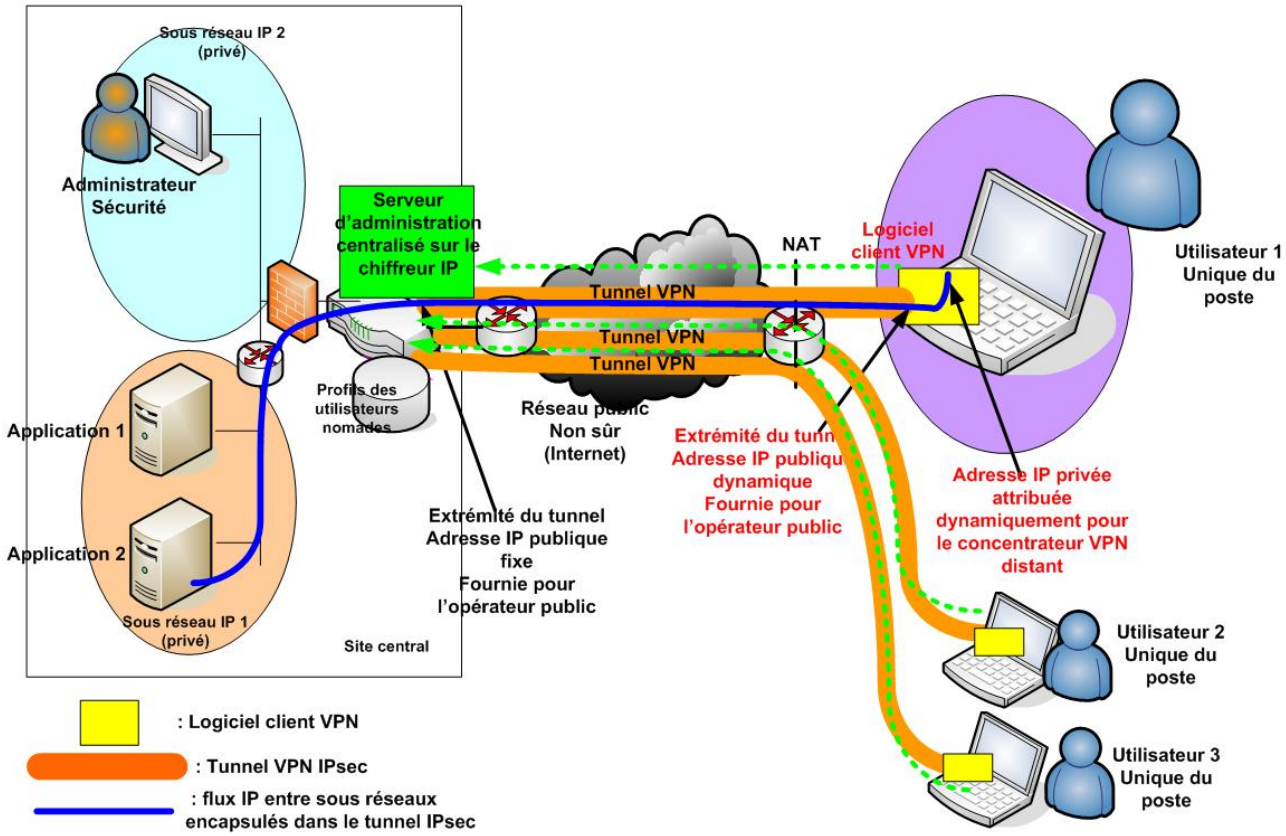

Figure 3. Fonctionnement avec équipement de téléadministration centralisée sur un chiffreur IP.

Les flux en vert sur le schéma correspondent aux flux d'administration. Dans ce cas d'utilisation, les applications VPN clientes viennent chercher leur politique de sécurité VPN sur le chiffreur IP (dans le module de gestion centralisée qui gère les configurations utilisateurs). Dans ce mode de fonctionnement, les flux d'administration ne passent pas par les tunnels VPN qui ne sont pas encore établis à ce stade (ces flux d'administration peuvent utiliser, par exemple, des connexions SSL afin de les sécuriser).

A.2.4 Système de chiffrement avec machine hôte partagée

Dans l'environnement illustré sur la figure 4, la machine multi-utilisateurs hébergeant l'application VPN cliente se connecte à une application précise ou à toutes les applications situées dans un sous réseau précis situé dans l'entreprise avec une station d'administration centralisée sur le chiffreur IP.

Ce cas d'utilisation, plus rare, est représentatif d'une organisation qui met à disposition de ses utilisateurs nomades un ensemble de machines qui ne sont pas affectées à des utilisateurs spécifiques. Chaque utilisateur nomade dispose néanmoins d'un compte et d'un profil VPN qui lui est propre.

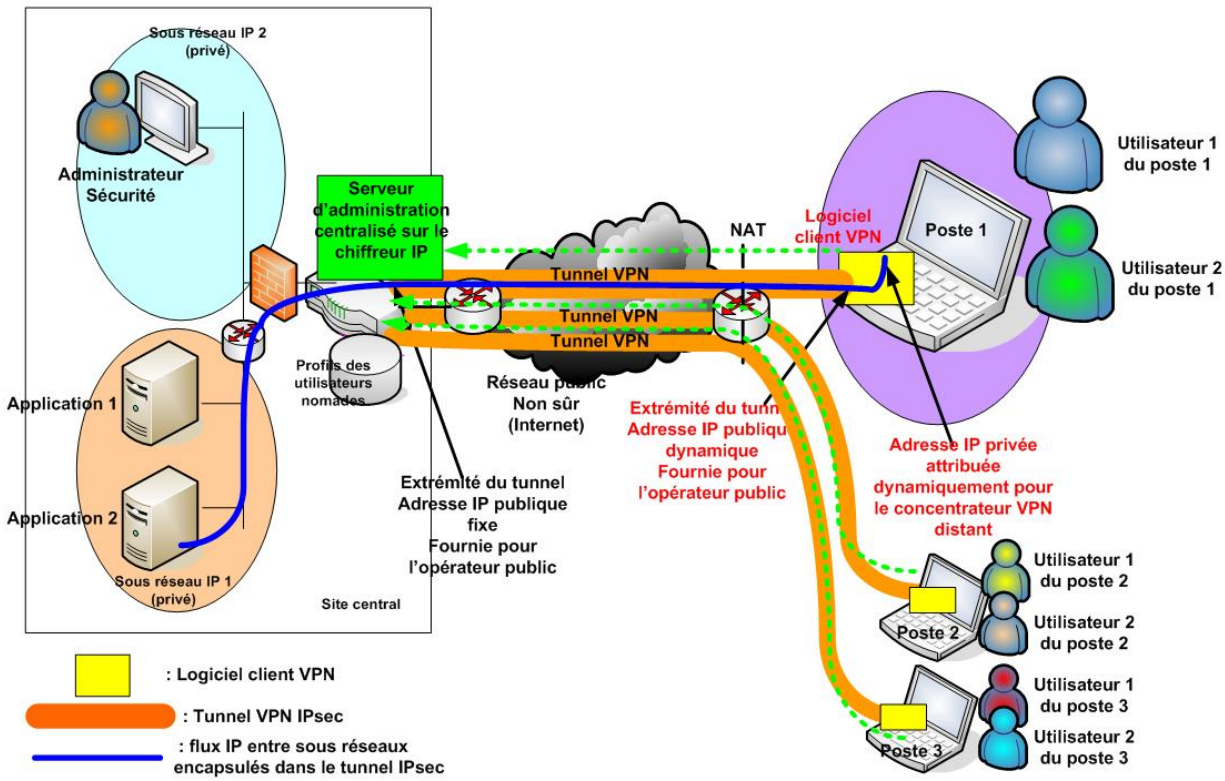

Figure 4. Fonctionnement avec machine hôte partagée.

Dans ce contexte, chaque utilisateur s'authentifie sur le module d'administration centralisé et récupère ainsi automatiquement sa politique de sécurité VPN, qui lui est propre. Dans ce modèle, la politique de sécurité VPN de chaque utilisateur n'est pas stockée sur le poste nomade, mais sur le module d'administration centralisé sur le chiffreur.

A.3 Fonctionnalités de la TOE

La fonctionnalité principale de la TOE est de fournir au système d'information un lien de communication sécurisé avec un chiffreur IP en offrant les services suivants pour protéger le flux de données applicatives (paquets IP transitant entre la machine hébergeant l'application VPN cliente et un chiffreur IP en frontal d'une organisation) :

- Application des politiques de sécurité VPN
- Protection en confidentialité des données applicatives.
- Protection en authenticité des données applicatives.
- Protection en confidentialité des informations topologiques.
- Protection en authenticité des informations topologiques.

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

- Authentification :
  - Vérification de l'authentification au système de chiffrement.
- Gestion des politiques de sécurité VPN :
  - Import des politiques de sécurité VPN.

- Export des politiques de sécurité VPN.
- Protection de l'accès aux politiques de sécurité VPN.

- Gestion des clés cryptographiques :
  - Import des clés cryptographiques.
  - Protection de l'accès aux clés cryptographiques.
  - Bonne consommation des clés cryptographiques.
- Administration:
  - Protection des flux d'administration à distance.

A.3.1 Services fournis par la TOE

Application des politiques de sécurité VPN

Les politiques de sécurité VPN spécifient les règles de sécurité qui déterminent le traitement à appliquer aux données. Ces dernières représentent les données qui proviennent des applications du système d'information et qui sont véhiculées par le réseau. On parle alors de données applicatives qui transitent entre la TOE et un chiffreur IP

L'application VPN cliente applique des fonctions de filtrage implicite. Ainsi si aucune politique de sécurité VPN n'est définie sur un lien VPN donné, les paquets entrants ou sortants sont rejetés (règle de filtrage par défaut).

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

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

Ces politiques sont conservées au niveau de la TOE et du chiffreur IP concerné pour être appliquées localement.

Protection en confidentialité des données applicatives

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

L'algorithme de chiffrement/déchiffrement et les caractéristiques des clés utilisées sont définis dans le contexte de sécurité associé à la politique de sécurité VPN appliquée.

Protection en authenticité des données applicatives

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

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

Protection en confidentialité des informations topologiques

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

L'algorithme de chiffrement/déchiffrement et les caractéristiques des clés utilisées sont définis dans le contexte de sécurité associé à la politique de sécurité VPN appliquée.

Protection en authenticité des informations topologiques

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

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

A.3.2 Services nécessaires au bon fonctionnement de la TOE

A.3.2.1 Authentification

Vérification de l'authentification au système de chiffrement

Ce service permet de vérifier que l'utilisateur et l'administrateur se sont bien authentifiés vis-à-vis du système de chiffrement avant de pouvoir utiliser l'application VPN cliente.

A.3.2.2 Gestion des politiques de sécurité VPN

Importation des politiques de sécurité VPN

Ce service permet d'assurer l'importation de façon sûre des politiques de sécurité VPN dans la TOE en garantissant leur authenticité et leur confidentialité. Générées à l'extérieur de la TOE, elles sont importées de deux manières :

- En local :

L'administrateur se connecte directement et physiquement à la TOE. Cette méthode est généralement retenue en phase d'initialisation afin de distribuer les politiques de sécurité initiales et leur contexte. En phase opérationnelle, elle permet à l'administrateur de sécurité d'opérer directement sur la TOE.

- À distance :

Les politiques sont importées via un flux de données entre la TOE et l'administrateur ; il est protégé en authenticité et en confidentialité. Cette téléadministration permet

d'importer de nouvelles politiques de sécurité avec leur contexte au niveau d'un parc de machines, et n'est généralement utilisée qu'en phase opérationnelle.

Export des politiques de sécurité VPN

Ce service permet d'exporter les politiques de sécurité VPN vers un administrateur distant authentifié en garantissant leur authenticité. Il permet à un administrateur distant de consulter les politiques de sécurité VPN appliquées et d'ainsi faciliter la résolution de problèmes rencontrés en phase opérationnelle.

Protection de l'accès aux politiques de sécurité VPN

Ce service permet d'empêcher les politiques de sécurité VPN d'être exportées de manière non autorisée à l'extérieur de la TOE. Il permet aussi d'assurer qu'une politique de sécurité donnée est utilisable (accessible) seulement par les services qui en ont besoin, et uniquement après authentification préalable de l'utilisateur.

Les politiques de sécurité VPN sont ainsi soumises à un contrôle d'accès dépendant de l'authentification de l'utilisateur de la machine.

A.3.2.3 Gestion des clés cryptographiques

Protection de l'accès aux clés cryptographiques

Ce service permet d'empêcher les clés secrètes et privées d'être exportées de manière non autorisée à l'extérieur de la TOE. Il permet aussi d'assurer qu'une clé donnée est utilisable (accessible) seulement par les services qui en ont besoin, et uniquement après authentification préalable de l'utilisateur (les clés sont déverrouillées sous condition de vérification des données d'authentification fournies par l'utilisateur).

Import des clés cryptographiques

Ce service permet d'importer de façon sûre les clés cryptographiques, générées à l'extérieur de la TOE, dans la machine hôte :

- En local par un administrateur de sécurité :

L'administrateur se connecte alors directement à la TOE. Cette méthode est généralement retenue en phase d'initialisation afin de distribuer les clés cryptographiques initiales. En phase opérationnelle, elle permet à l'administrateur de sécurité d'opérer directement sur la TOE.

- À distance, avec un utilisateur ou via un mécanisme de téléadministration:

Les clés cryptographiques sont importées via un flux de données entre la TOE et un administrateur ou un équipement de téléadministration.

- En local par l'utilisateur :

Lorsque les clés sont présentes sur un support externe (carte à puce ou clé USB par exemple), cette méthode permet directement à l'utilisateur d'importer des clés dans l'application VPN cliente en phase opérationnelle.

Lors de l'import, ce service protège les clés en intégrité et/ou en confidentialité en fonction du type de clés.

Bonne consommation des clés cryptographiques

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

A.3.2.4 Administration

Protection des flux d'administration à distance

Ce service permet de protéger en authenticité et en confidentialité, les flux d'administration à distance pour le renouvellement des clés ou des politiques de sécurité VPN et de leur contexte de sécurité. Ce service permet ainsi d'assurer la protection de données sensibles de la TOE, en n'autorisant leur accès uniquement à des services de confiance, habilités à procéder à ces opérations.

Ce service protège également contre le rejeu de séquences d'opérations d'administration à distance passant sur les liens entre l'application VPN cliente et le service de mise à jour présent sur le réseau privé de l'organisation.

A.4 Fonctionnalités complémentaires possibles pour l'application VPN cliente

Cette annexe présente des fonctionnalités complémentaires qui pourront être proposées par les industriels en réponses à des besoins spécifiques des usagers.

Audit local

L'enregistrement de données d'audit local sur la machine hôte par la TOE n'a pas été retenu dans la problématique de sécurité considérée. Cet audit permettrait de tracer les éventuels évènements qui ne pourraient être audités au niveau des chiffreurs IP ou de l'équipement de téléadministration centralisé.

Protection en confidentialité des politiques de sécurité VPN

Ce service permettrait de garantir, en plus de l'intégrité, la confidentialité des politiques de sécurité VPN lors de leur stockage sur la machine hôte hébergeant la TOE.

Annexe B Définitions et acronymes

B.1 Définitions

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

Terme	Définition
Administrateur	Utilisateur autorisé à gérer tout ou une partie de la TOE. Il peut posséder des privilèges particuliers qui permettent de modifier les politiques de sécurité et les clés cryptographiques de la TOE.
Authenticité	Propriété de sécurité assurant l'intégrité et l'authentification de l'origine des données considérées.
Authentification	Mesure de sécurité qui vérifie l'identité déclarée.
Chiffreur IP	Dispositif placé en amont d'un réseau privé et destiné à chiffrer les communications échangées entre des équipements de ce réseau et des équipements externes en garantissant la protection en confidentialité et/ou authenticité des données (via l'utilisation d'un canal VPN).
Clé de session	Clé à durée de vie courte générée aléatoirement et utilisée pour assurer la confidentialité, l'authenticité et l'intégrité de données.
Contexte de sécurité	Paramètres de sécurité qui permettent de savoir quelles caractéristiques de sécurité doivent être utilisées pour appliquer la politique de sécurité VPN donnée. Ces paramètres comprennent entre autres les algorithmes cryptographiques, les tailles de clés, …
Environnement opérationnel	Environnement de la TOE lors de sa phase d'utilisation.
Equipement de téléadministration centralisé	Equipement automatique jouant le rôle de l'administrateur et chargé de l'administration à distance de la TOE.
Optionnel	Dans le cadre de ce profil de protection, « optionnel » signifie que le service ou la propriété de sécurité considérés doivent être implantés dans TOE, mais que leur application ou leur utilisation n'est pas obligatoire.

Terme	Définition
Politique de sécurité VPN	Politique de sécurité permettant de spécifier les services de sécurité (confidentialité et/ou authenticité) à appliquer sur les informations qui transitent entre l'application VPN cliente et un chiffreur IP.
Raffinement éditorial	Raffinement dans lequel une modification mineure est faite sur un élément d'exigence, telle que la reformulation d'une phrase pour des raisons de respect de la grammaire anglaise. En aucun cas, cette modification ne doit changer la signification de l'exigence.
Raffinement non éditorial	raffinement qui permet d'ajouter des précisions ou de limiter l'ensemble des implémentations acceptables pour un élément d'exigence.
Réseau privé	Réseau interne à une entité (comme une entreprise ou un service) qui doit être protégé des flux arrivant de l'extérieur mais pas de ces propres flux. C'est un réseau considéré comme sûr.
Réseau public	Réseau accessible à toute entité et toute personne qui ne peut être considéré comme sûr.
Système de chiffrement	Ensemble d'équipements partageant une même infrastructure de gestion des clés et pouvant concourir en particulier à l'établissement de communications chiffrées entre ses différents membres.

B.2 Acronymes

CC (*Common Criteria*) Critères Communs

EAL (*Evaluation Assurance Level*) Niveau d'assurance de l'évaluation

IP (*Internet Protocol*) Protocole Internet

IT (*Information Technology*) Technologie de l'information

OSP (*Organisational Security Policy*) Politique de sécurité organisationnelle

PP (*Protection Profile*) Profil de protection

SPD (*Security Problem Definition*) Définition du problème de sécurité

SSL (*Secure Sockets Layer*)

ST (*Security Target*) Cible de sécurité

TOE (*Target Of Evaluation*) Cible d'évaluation

VPN (*Virtual Private Network*) Réseau privé virtuel

Annexe C Traduction des termes anglais

Administrator	Administrateur
Applicative data	Données applicatives
Authenticity	Authenticité
Communication link	Lien de communication
Communication manager	Gestionnaire de communication
Confidentiality	Confidentialité
Cryptographic key(s)	Clé(s) cryptographique
Encryption system	Système de chiffrement
Enforcement manager	Gestionnaire d'application (de protection)
Identifier	Identifiant
Integrity	Intégrité
IP encrypter	Chiffreur IP
IP packets	Paquets IP
Object	Objet
Operation	Opération
Remote administration equipment	Equipement de téléadministration
Replay	Rejeu
Secret and private keys	Clés secrètes et privées
Security alarm	Alarme de sécurité
Security attribute	Attribut de sécurité
Security VPN policy/policies	Politique(s) de sécurité VPN
Subject	Sujet
Topologic data	Données topologiques
User	Utilisateur
User manager	Gestionnaire d'utilisateur

Annexe D Références

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

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

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

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

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

[CRYPTO_GESTION] Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard. DCSSI.

[AUTH] Authentification : Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard. DCSSI.

[QUA-STD] Processus de qualification d'un produit de sécurité – niveau standard. Version 1.1, 18 mars 2008. N°549/SGDN/DCSSI/SDR.

[PP-VPNC] Profil de Protection « Application VPN cliente », version cc3.0, ref. « pp0602 »

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

[PP-FIR] Profil de Protection, Firewall d'interconnexion de réseaux IP. Version 1.07, mars 2004. AQL. http://meleze.arkoon.net/pps.html.

[PPnc0502] Profil de Protection, Chiffreur IP. Version 1.5, février 2005. DCSSI. http://www.ssi.gouv.fr/site_documents/pp/ppnc0502.pdf.

[PRIS] Politique de Référencement Intersectorielle de Sécurité (PRIS), Préambule, version 2.0, juin 2002, OID 1.2.250.1.137.2.2.1.2.1.1

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

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

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

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

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

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

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

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

Index