IGOR

Titre: **M>Tunnel 2.5 – Cible de sécurité**

Issue Number: **1.16**

Date : 4 novembre 2002

Auteur: Didier BONNEROT

Document Référence: **100-400-2002001**

CVS_TAG: **C1_Doc_____**

Sommaire:

Ce document définit la cible de sécurité pour M>Tunnel 2.5 dans le cadre de l'évaluation et de la certification selon les Critères Communs.

Visa:

Visa: **Date:** **Signature**:	**Visa:** **Date:** **Signature:**

CONTENTS

0. SUIVI du DOCUMENT

0.1 Historique

Version 1.0	Création
Version 1.1	Intégration des exigences de sécurité
Version 1.2	Prise en compte des remarques de la DCSSI
Version 1.3	Prise en compte des remarques d'AQL
Version 1.4	Prise en compte des nouvelles remarques d'AQL et de la DCSSI
Version 1.5	Prise en compte des nouvelles remarques de la DCSSI
Version 1.6	Prise en compte de la limitation des exigences d'assurance
Version 1.7	Prise en compte de la fiche de commentaires FdC01 émise par le Cesti
Version 1.8	Prise en compte de la remarque 22 de FdC01
Version 1.9	Prise en compte des remarques de la DCSSI
Version 1.10	Prise en compte de remarques internes
Version 1.11	Prise en compte de remarques internes, et de Fiche FdC03
Version 1.12	Modifications suite au changement de protocole d'authentification
Version 1.13	Modification FPT_ITT.1
Version 1.14	Suppression algorithme DES
Version 1.15	Suppression IA_4

0.2 Abbréviations

Ce chapitre présente quelques abréviations qui sont aussi décrites dans le [DocPlan].

AH	Authentication Header
ESP	Encapsulating Security Payload
BSD	Berkeley Software Distributions.
BSDI	Berkeley Software Design, Inc.
CA	Certification Authority
CC	Common Criteria
CM	Configuration Management
CRL	Certificate Revocation List
DNS	Domain Name Server.

FTP	File Transfer Protocol.
HTML	HyperText Markup Language - the formatting language used to construct web pages.
HTTP	HyperText Transfer Protocol.
IA	Identification and Authentification.
ICMP	Internet Control Message Protocol
IP	Internet Protocol.
MATRAnet	MATRAnet company.
MIME	Multipurpose Internet Mail Extensions.
NAT	Network Address Translation
PC	Personal Computer.
PP	Protection Profile
SFP	Security Function Policy
SMTP	Simple Mail Transfer Protocol.
ST	Security Target.
TCP	Transmission Control Protocol - TCP/IP's connection-oriented transport layer communications protocol.
TOE	Target of Evaluation - the CC term for the system or product being evaluated.
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
URL	Uniform Resource Locator, e.g. http://www.org.com/index.htm.

0.3 Terminologie

Ce chapitre présente quelques termes utilisés dans ce document.

Administrateurs	Personnes autorisées à accéder à la station d'administration et aux M>Tunnel Gateway pour faire la gestion de la politique de chiffrement
Attaquant	Une personne malintentionnée cherchant à perturber le fonctionnement du VPN ou à récupérer des informations sensibles.

Authentification	Mécanisme permettant de s'assurer que les deux extrémités d'un tunnel appartiennent à la même autorité de certification et qu'elles sont autorisées à créer un tunnel entre elles
Certificats	La clé publique d'un utilisateur signée par la clé privée de l'autorité de certification
Clé de session	Clé aléatoire servant soit pour faire du chiffrement de paquet soit pour signer celui-ci
CRL	Liste des certificats qui ne sont pas autorisés
Interne	Se situant sur le réseau protégé par le VPN M>Tunnel
Externe	Se situant sur un réseau non protégé par le VPN M>Tunnel
Personne	Personne n'étant pas forcément équipé d'un M>Tunnel Client
Politique de chiffrement	La définition des algorithmes de chiffrement et d'authentification qu'il est nécessaire d'appliquer entre les deux extrémités d'un tunnel
Identifiant	Certificat et clé privée d'un composant de la TOE
Utilisateur	Personne dont le poste de travail est équipé d'un M>Tunnel Client et dont l'identifiant est stocké sur un support externe
Station d'administration	L'application permettant de gérer la politique de chiffrement
Tunnel	Une liaison point à point sécurisée

0.4 Documents applicables et de références

Ce chapitre présente les autres documents référencés dans la présente cible de sécurité. En outre, tous les documents utilisés au titre de l'évaluation sont listés dans [PlanDoc], où le dernier numéro de version de chacun est mentionné.

[PlanDoc] *M>Tunnel 2.5 – Plan de Documentation,* MATRAnet, Référence 400-xxx.

[TCP/IP] *TCP/IP Illustrated Volume 1 - The Protocols*. W. Richard Stevens. Addison-Wesley. ISBN: 0-201-63346-9.

1. INTRODUCTION de la CIBLE de SECURITE

1.1 Identification de la Cible de Sécurité

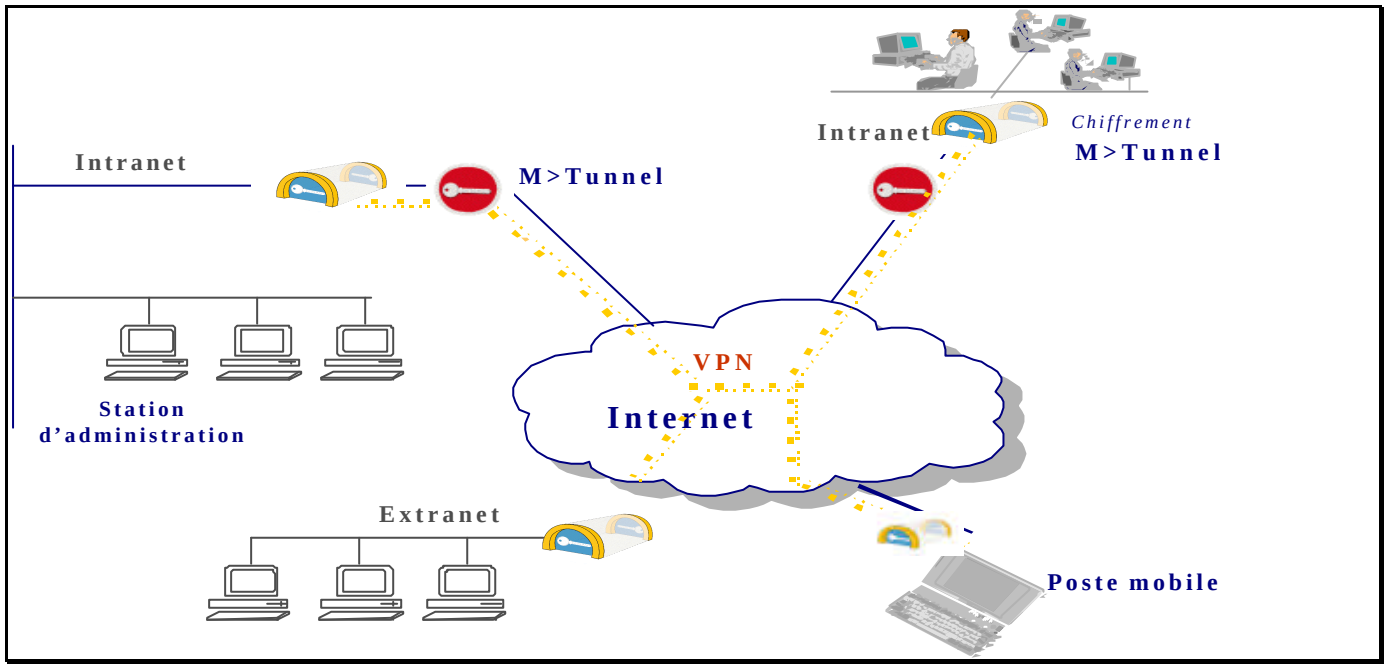
Ce document constitue la cible de sécurité de M>Tunnel, un VPN (Virtual Private Network). La version prise en compte est 2.5 :

- Nom de la ST : **M>Tunnel 2.5 – Cible de sécurité**
- Version : **1.16**
- Identifiant de la TOE : **M>Tunnel**
- Version : **2.5**
- Référence Critères Commun : **Version 2.1 d'Août 1999**

1.2 Principe général du fonctionnement du VPN M>Tunnel

1.2.1 Les réseaux privés virtuels

Un réseau privé virtuel (VPN) est un ensemble de nœuds sur un réseau public tel qu'Internet qui communiquent entre eux en utilisant le chiffrement. Ainsi leurs messages ne risquent pas d'être interceptés et déchiffrés par des utilisateurs non autorisés de la même façon que s'ils circulaient sur des réseaux privés.



Quand on protége un réseau à l'aide d'un firewall, toutes les machines derrière le firewall sont à priori protégées contre les tentatives d'intrusion, mais les échanges de données (mail, transfert de fichiers ...) vers les autres sites de la société, ou vers les sites des partenaires, circulent non-chiffrés sur l'Internet. A moins de créer son propre réseau de télécommunications, les informations confidentielles peuvent être interceptées ou corrompues. Pour tirer avantage de la performance et des faibles coûts d' Internet tout en assurant la confidentialité des échanges, les données peuvent être chiffrées en créant des canaux pour connecter des sites séparés par Internet. Cette connexion chiffrée entre ces sites constitue un réseau privé virtuel, virtuel car il utilise une infrastructure partagée et privé car la sécurité y est équivalente à celle d'un réseau conventionnel. L'architecture des VPN peut être très variée selon les besoins de chaque société. Il peut connecter divers sites d'un Intranet, ou des sites partenaires sur un extranet. Il peut également relier une Gateway M>Tunnel et un ordinateur portable sur lequel tourne un M>Tunnel Client. Parce que les communications n'ont pas le même degré de confidentialité, il est intéressant de chiffrer uniquement certains flux (par exemple il peut s'avérer utile de ne pas chiffrer les consultations d'un site Web public), ou de les chiffrer avec différents algorithmes suivant le type de flux.

1.2.2 Le chiffrement asymétrique

Avec le chiffrement asymétrique, on utilise deux clefs pour chiffrer et déchiffrer un message : une clef privée, tenue secrète, qui ne doit, par conséquent, jamais être communiquée, et une clef publique diffusée largement sans restriction (la connaissance de la clé publique ne permet pas de calculer la clé privée associée). Un message chiffré avec une clef ne peut être déchiffré que par l'autre clef associée. Ainsi si Alan veut envoyer un message à Susan, il chiffrera le message avec la clef publique de Susan. Susan est la seule personne à pouvoir déchiffrer ce message à l'aide de sa clef privée. Même Alan qui pourtant a chiffré le message, n'est plus en mesure de le faire. Ce système assure la confidentialité des échanges. Pour assurer l'identité des correspondants, Alan signe le message avec sa clef privée. Susan va le contrôler avec la clef publique d'Alan. Susan sera alors certaine que c'est bien Alan qui échange des données avec elle. Ce système assure l'authentification des données.

Les systèmes de chiffrement asymétrique sont coûteux en terme de ressources ; ils sont donc utilisés en association avec des systèmes symétriques (tels que le DES ou AES) et servent seulement à échanger des informations d'authentification (voir § 1.2.4 L'authentification des correspondants et la négociation des clef) ainsi que les clefs de chiffrement des systèmes symétriques (voir § 1.2.3 Le chiffrement symétrique). Ceci assure à la fois une meilleure sécurité et une meilleure performance.

1.2.3 Le chiffrement symétrique

Le système de chiffrement symétrique utilise une clef unique pour le chiffrement et le déchiffrement. Une clef unique est partagée par deux parties qui doivent la tenir secrète. L'expéditeur de la communication chiffre le message avec celle-ci ; le destinataire doit le déchiffrer avec cette même clef. M>Tunnel utilise le chiffrement symétrique pour chiffrer les données des messages, ce qui est un procédé plus rapide qu'en utilisant un algorithme asymétrique. M>Tunnel utilise les algorithmes de chiffrement suivants qui sont utilisés par le service de sécurité ESP (Encapsulating Security Payload):

- Le DES, avec des clefs de 56 bits, en mode chaîné (CBC),
- Le triple DES, avec des clefs de 168 bits, en mode chaîné (CBC),
- L'AES, avec des clefs de 128 bits ou 192 bits,

Pour renforcer le niveau de sécurité M>Tunnel renégocie fréquemment les clefs de session pour compliquer les efforts importants déployés pour "craquer" une clef. Le 3-DES utilise trois clefs DES distinctes pour faire un chiffrement en 3 étapes de DES. La longueur de clef le rend quasiment incassable. Les paquets sont chiffrés 3 fois. L'AES est le dernier algorithme de chiffrement standardisé, conçu pour résister, bien mieux que le DES, aux attaques par cryptanalyse différentielle.

1.2.4 L'authentification des correspondants et la négociation des clefs

M>Tunnel utilise le chiffrement asymétrique pour authentifier les extrémités du tunnel. Cette authentification de l'identité de chaque extrémité est réalisé à l'aide de certificats numérique (à ne pas confondre avec l'authentification au niveau du paquet avec AH ou ESP). Après que les deux extrémités aient vérifié avec certitude l'identité de l'autre partie, une clef secrète (qu'on peut appeler une clef de session) est négociée et sera utilisée pour chiffrer les données. Les clefs de session sont négociées automatiquement entre les extrémités du tunnel, de façon fréquente pour garantir une sécurité forte.

1.2.5 Définition d'un tunnel

Un tunnel se définit entre deux extrémités et à l'aide des informations suivantes :

- Les sous-réseau protégés par les deux extrémités et qui doivent être reliés par ce tunnel,
- Le type de flux IP concernés par ce tunnel (TCP, UDP, les ports, …).

1.2.6 Infrastructure de clé publique (PKI)

L'infrastructure de clé publique (PKI) est un système d'autorités de certifications qui peut créer, gérer, stocker, distribuer et révoquer des certificats numériques basés sur un chiffrement asymétrique. Les principales fonctions sont :

- Enregistrer les utilisateurs et délivrer leurs certificats à clef publique.
- Révoquer les certificats quand c'est nécessaire.
- Archiver les données pour valider les certificats ultérieurement.

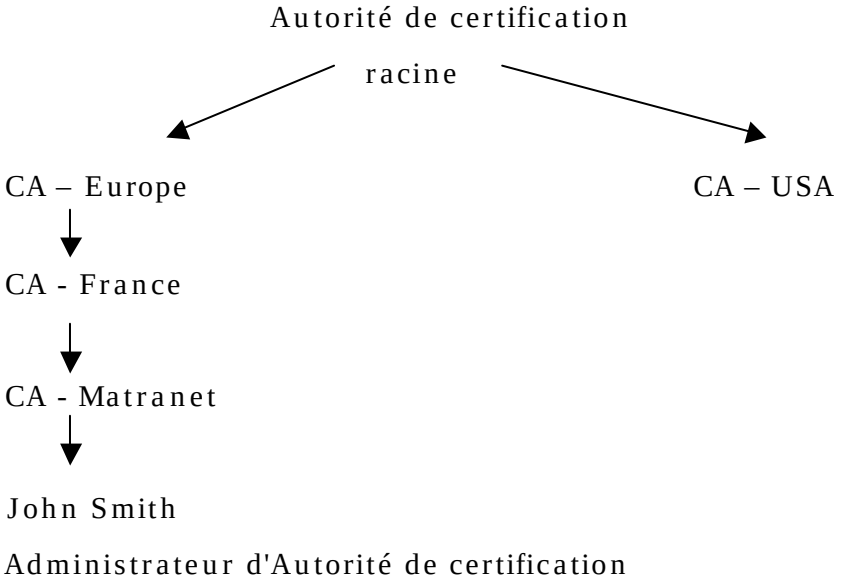
Pour créer et gérer les certificats numériques, on peut soit utiliser le générateur de certificats IPsec, solution logiciel fournie avec M>Tunnel, soit obtenir des certificats d'une tierce partie.

Architecture

L'infrastructure à clef publique est constituée des composants suivants :

- Des Autorités de certification (CA) dirigées par des administrateurs d'Autorité de certification. Les autorités ce certification sont responsables de la publication des certificats qu'ils signent numériquement ainsi que de la révocation des certificats dont la sécurité a été compromise.
- Les entités finales ou end entity (EE). Il s'agit d'une personne ou machine pour qui le certificat est publié. Une EE utilise un certificat pour s'authentifier lui-même, chiffrer des données et diffuser sa clef publique.

Le schéma ci-dessous montre une simple architecture à clef publique :



L'Autorité de certification racine est celle qui se situe en haut de la chaîne. Elle signe son propre certificat en qui la confiance doit être totale. Le certificat de chaque CA intérieur est signé par le CA qui se trouve au-dessus dans la hiérarchie. Dans le diagramme ci-dessus, le certificat de MATRAnet CA est signé par l'Autorité de certification France.

Les certificats

Un certificat est un message spécial contenant la clef publique et des renseignements pour l'authentification basique d'un utilisateur. Il est signé avec la clef privée d'une Autorité de certification, ce qui prouve sa véracité. Les certificats sont conformes au standard X509. Ils sont publiés par une Autorité de certification.

Structure d'un certificat

Tous les certificats contiennent un nombre de champs standards concernant l' "émetteur" et le "destinataire" de ce certificat. Il est essentiel de remplir avec soin les champs suivants lors de l'émission de la génération du certificat pour pouvoir ensuite configurer correctement M>Tunnel. En effet, M>Tunnel utilise des groupes d'accès qui sont déterminés par les champs dans les certificats des utilisateurs. Les certificats sont valides pour une période définie indiquée par les champs Début et Fin.

C	Pays
ST	Département
L	Ville
O	Organisation ou Société
OU	Unité d'organisation ou Service
CN	Pour un utilisateur : nom et prénom Pour une passerelle : Fully Qualified Name

Les autorités de certification

Un certificat est identifié par son numéro de série et par son Autorité de certification. Ces certificats sont échangés entre deux composants de M>Tunnel, entourent la clef publique des tunnels chacune leur tour et sont signés avec la clef privée de l'Autorité de certification. Quand le destinataire reçoit le certificat, il vérifie sa signature avec la clef publique de l'Autorité de certification.

Liste de révocation des certificats (CRL)

Les certificats sont valides pendant une période définie indiquée dans le certificat. Parfois pour des raisons de sécurité, on peut avoir besoin de révoquer un certificat avant sa date d'expiration. Un des motifs les plus courants serait que le certificat ne soit plus valide suite au départ d'un des employés de la société ou bien parce qu'il a été compromis. Si la clef privée correspondant à la clef publique contenue dans le certificat, la demande de révocation doit être faite à l'Autorité de certification. Quand un certificat est révoqué, son numéro de série est ajouté à la liste de révocation des certificats (CRL), liste qui est publiée régulièrement par le CA. Le certificat est alors rejeté par le Tunnel.

Chemin de certification

Les certificats des Autorités de certification des utilisateurs M>Tunnel sont importés lors de la configuration. Les certificats sont de deux types : root (racine) et signing (de signature). Les certificats root sont auto-signés par l'Autorité de certification. Cette Autorité de certification peut par la suite signer des certificats pour des "sous" Autorités de certification ; les certificats de ces sous-autorités de certification sont appelés certificats "signing" et servent à signer soit les certificats des utilisateurs soit les certificats «signing » qui lui sont associés. Durant la vérification des certificats numériques—qui est effectuée avant que les Gateways et les clients ne téléchargent les informations et durant la négociation des clefs de session entre les points du tunnel, c'est à dire lors de l'authentification—le certificat de l'utilisateur est en premier validé, puis c'est le tour du certificat du CA de l'utilisateur ainsi que celui du certificat du CA du CA de l'utilisateur. Le processus continue jusqu'à ce que l'Autorité de certification root soit atteinte. Le chemin de validation du certificat est le chemin à partir du certificat de l'utilisateur jusqu'au CA racine. Si dans ce chemin au moins un certificat n'est pas valide—par exemple, le certificat a expiré ou il appartient à un CRL—alors la vérification échoue.

1.2.7 Internet Protocol Security

Internet Protocol Security (IPsec) est le standard de sécurité pour sécuriser l'Internet Protocol (IP). IPsec utilise le chiffrement pour protéger le trafic au niveau du paquet. Chiffrer au niveau des paquets plutôt qu'au niveau de l'application permet à IPsec de pouvoir être implémenté de façon transparente dans l'infrastructure réseau sans affecter les machines individuelles ou les PCs. IPsec fournit deux solutions de sécurité : Authentication Header (AH) qui permet essentiellement l'authentification de l'émetteur et protège l'intégrité des données, et Encapsulating Security Payload (ESP), qui supporte à la fois l'authentification de l'émetteur et le chiffrement des données. Les informations spécifiques associées avec chacun de ces services sont insérées dans le paquet dans un en-tête qui suit l'en-tête IP. M>Tunnel supporte à la fois AH et ESP. Les services d'authentification supportés par AH et ESP concernent l'authentification au niveau du paquet. Cette authentification vérifie l'origine des paquets et l'intégrité des données (par exemple que les données dans le paquet n'aient pas été altérées depuis leur envoi). L'authentification au niveau du paquet est totalement différente de celle utilisée pour connaître l'identité des correspondants, cette dernière utilisant des certificats numériques. AH et ESP peuvent être implémentés soit en mode transport soit en mode tunnel. En mode transport, la protection s'applique aux paquets de la couche supérieure - qui sont traités au-dessus d'IP, alors qu'en mode tunnel elle s'applique aux paquets IP. En mode transport les deux extrémités doivent être des machines ; avec le mode tunnel chaque extrémité peut être soit une machine soit une gateway.

1.2.7.1 Authentification Header (AH)

AH est un protocole Internet IPsec créé pour fournir l'intégrité des données et l'authentification d'origine pour les paquets IP, et (optionnelement) pour fournir une protection contre le rejeu. Les algorithmes utilisés sont HMAC-SHA1et HMAC-MD5. M>Tunnel supporte les options suivantes du protocole AH :

- Authentification (intégrité des données et origine)
- Protection contre le rejeu

Les paquets qui échouent à l'authentification sont rejetés et ne sont pas délivrés aux couches supérieures. AH est très efficace pour éviter que le service ne soit refusé quand un pirate essaye de bloquer la communication d'un hôte ou d'une passerelle en l'inondant de paquets corrompus. L'authentification AH et l'authentification ESP sont implémentés après le chiffrement bien qu'avec AH l'en-tête du paquet IP est signé tandis qu'avec ESP, ce sont les données qui sont signées. Cela signifie que les paquets qui échouent au niveau de l'authentification seront rejetés plus vite s'ils sont authentifiés avec AH plutôt que ESP. Toutefois, on peut utiliser à la fois les deux authentifications si on le désire.

Quand on active l'option anti-rejeu, M>Tunnel rejette le paquet s'il est identique à l'un des derniers paquets reçus. L'anti-rejeu protège contre les pirates qui réussissent à récupérer un paquet sur Internet puis à l'aide de ce même

paquet ils bombardent sans cesse une des extrémités du tunnel afin de la faire céder. L'en-tête AH est toujours derrière l'en-tête IP dans le paquets IP. Il existe deux façons d'utiliser AH : mode transport et mode tunnel.

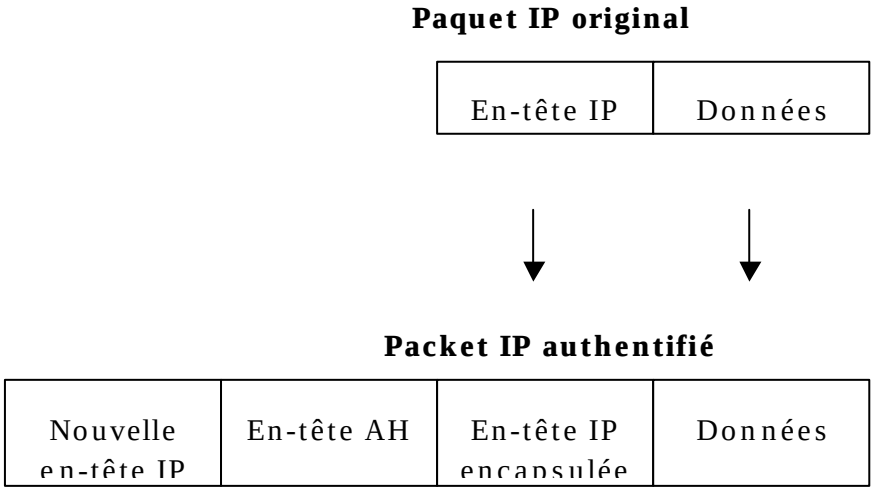
Mode transport

Le mode transport signifie que le paquet original n'est pas encapsulé dans un nouveau paquet. Les adresses IP source et destination demeurent inchangées. Par conséquent, on peut seulement utiliser AH en mode transport entre les machines qui ont une adresse publique IP ; on ne peut pas utiliser AH en mode transport quand l'une des extrémités est un M>Tunnel Gateway qui route les paquets des réseaux internes. Dans ce mode, l'en-tête AH est placée après l'en-tête IP, mais avant le protocole.

|IP header|AH|Data

Mode Tunnel

En mode tunnel, le paquet IP est encapsulé dans un nouveau paquet IP. En mode tunnel, l'en-tête du paquet "d'origine" transporte les adresses finales source et destination, pendant que le "nouveau" paquet peut contenir des adresses IP distinctes, telles que les adresses des passerelles de sécurité. De cette façon deux passerelles de sécurité peuvent créer un tunnel AH qui authentifiera tout le trafic entre les réseaux auxquels ils sont connectés. Ce mode est utilisé par des M>Tunnel Gateways et entre des M>Tunnel Gateways et des Clients. Le paquet AH en mode Tunnel a le format suivant :



1.2.7.2 Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) est un protocole Internet IPsec qui fournit des services tels que l'intégrité, l'authentification et le chiffrement des datagrammes IP. Il peut être utilisé seul ou en association avec l'En-tête d'Authentification. M>Tunnel supporte les options suivantes du protocole ESP :

- Chiffrement (algorithmes DES, 3 DES et AES)
- Authentification (intégrité des données et origine)
- Protection contre le rejeu

Quand on active l'option anti-rejeu, M>Tunnel rejette le paquet s'il est identique à l'un des derniers paquets reçus. L'anti-rejeu protège contre les pirates qui réussissent à récupérer un paquet sur Internet puis à l'aide de ce même paquet ils bombardent sans cesse une des extrémités du tunnel afin de la faire céder. Comme avec AH, ESP peut être utilisé en mode transport ou tunnel.

Mode transport

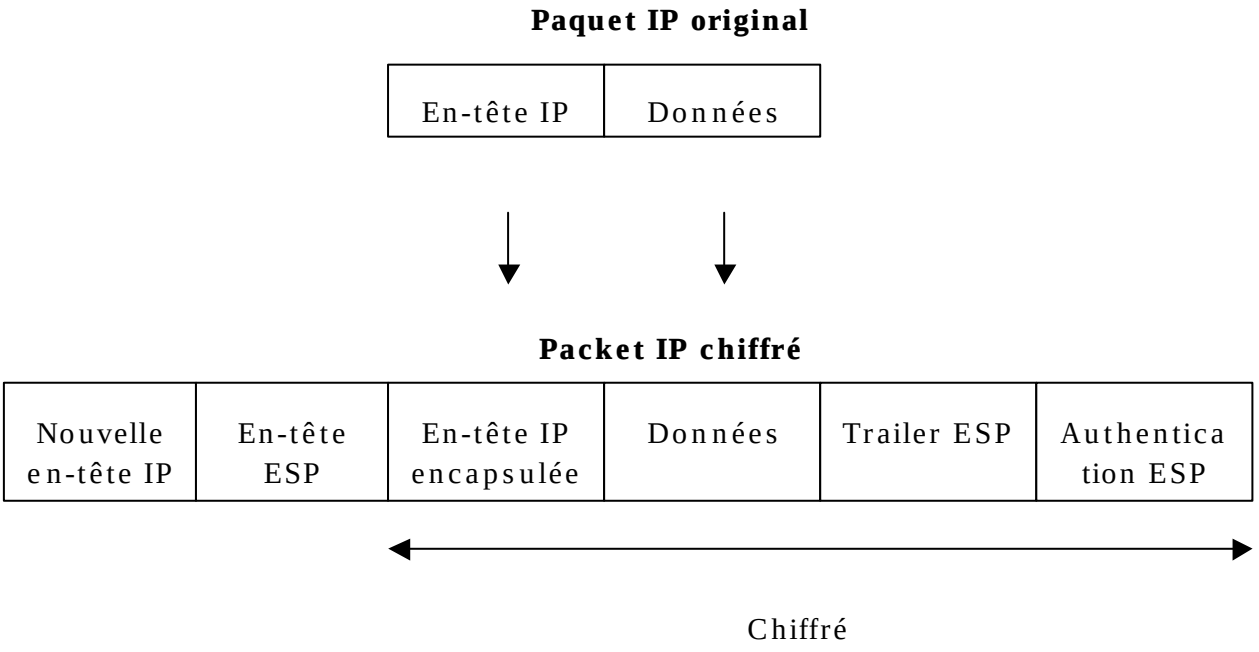
Le mode transport signifie que le paquet original n'est pas encapsulé dans un nouveau paquet. Les adresses IP source et destination demeurent inchangées. Par conséquent on peut utiliser ESP en mode transport entre les machines qui ont une adresse publique IP ; on ne peut pas utiliser AH en mode transport quand l'une des extrémités est un M>Tunnel Gateway qui route les paquets des réseaux internes. En mode transport le paquet apparaît sous cette forme :

| IP header | ESP header | Data | ESP trailer | ESP authentication |

Ce mode ne fournit pas d'authentification ou de chiffrement de l'en-tête du paquet IP.

Mode tunnel

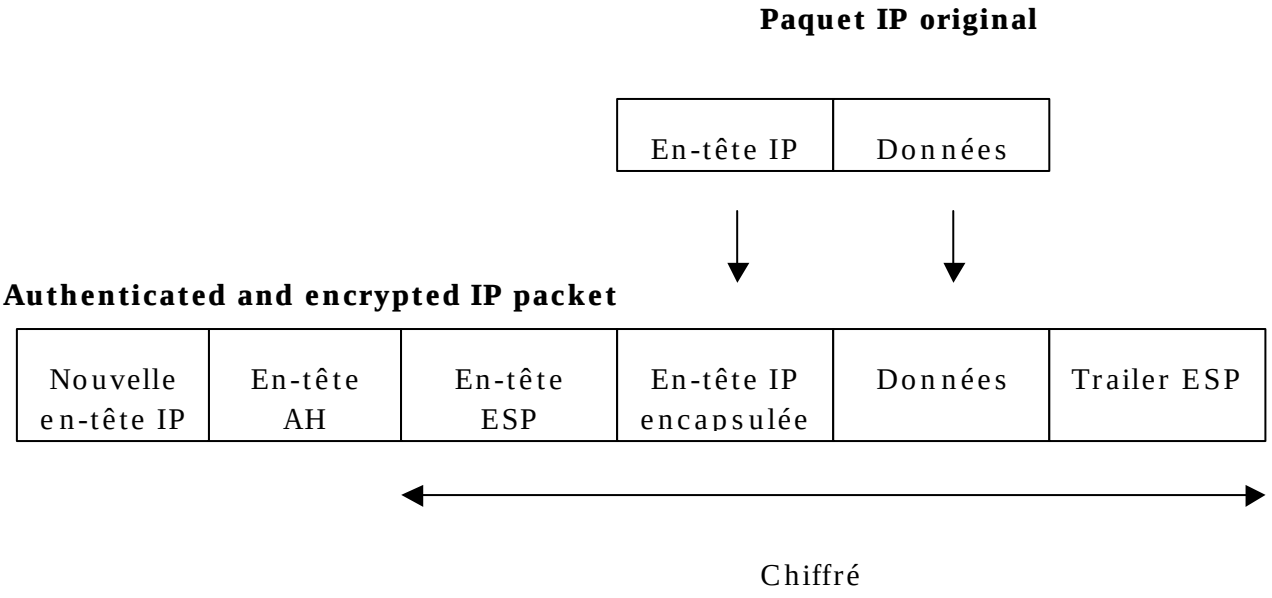
En mode tunnel, le paquet IP est encapsulé dans un nouveau paquet IP. En mode tunnel, l'en-tête du paquet "d'origine" transporte les adresses finales source et destination, pendant que le "nouveau" paquet peut contenir des adresses IP distinctes, telles que les adresses des passerelles de sécurité. De cette façon deux passerelles de sécurité peuvent créer un tunnel ESP qui authentifiera tout le trafic entre les réseaux auxquels ils sont connectés. Ce mode est utilisé par des M>Tunnel Gateways et entre des M>Tunnel Gateways et des Clients. En mode transport, les paquets se présentent comme ci-dessous :



Le mode Tunnel est utilisé quand l'un des points terminaux est une gateway. Comme avec AH les deux adresses en-tête IP dans le paquet n'ont pas à être identiques. Puisque le paquet est encapsulé de cette façon, ce mode assure une parfaite protection des datagrammes IP et permet d'utiliser des adresses privées non-routables.

AH et ESP combinés

On peut combiner l'utilisation à la fois de AH et ESP. La différence principale entre les services d'authentification fournies par ESP et AH est une extension de la couverture ; ESP ne protège pas les champs de l'en-tête IP. Si on utilise les services d'authentification à la fois de ESP et AH, l'algorithme utilisé sera le même. Le format d'un paquet avec les options AH et ESP à la fois sélectionnées (en mode tunnel) se présentent comme ci-dessous :



1.2.7.3 Compatibilité IKE

M>Tunnel n'est pas compatible avec le standard IKE sauf pour le mode manual-keying. Ce mode particulier, non pris en compte dans la TOE, consiste à

- utiliser des clés de session pré-définies qui sont intégrées, dans les composants M>Tunnel, lors de son initialisation,
- supprimer la phase d'authentification des correspondants et de négociation des clés

1.3 Niveau d'évaluation

La cible d'évaluation doit être conforme avec les parties 2 et 3 des Critères Communs version 2.1 pour le niveau EAL2 augmenté de ADV_HLD.2, ADV_LLD.1 et AVA_VLA.2

Note : Le composant d'assurance ADV_LLD.1 s'applique aux sous-systèmes de la TOE réalisant les fonctions cryptographiques.

2. DESCRIPTION de la TOE

2.1 Fonctionnalités de la TOE

La TOE, qui a pour but d'assurer la fonction VPN pour les flux IP (et uniquement ces flux là), se décompose en cinq composants :

- M>Tunnel Master
- M>Tunnel Gateway
- M>Tunnel Client
- Les politiques M>Tunnel
- L'administration M>Tunnel

Les flux, autres que les flux IP, ne sont pas traités par la TOE et ne sont donc pas, à priori, bloqués par cette dernière. Dans le cas de l'équipement M>Tunnel Gateway, il est conseillé de le paramétrer de façon à bloquer ce type de flux.

2.1.1 Le M>Tunnel Master

Le Master est le point de configuration central du réseau privé virtuel. Sur un M>Tunnel Master, on définit les informations sur la configuration et les groupes d'accès.

Point de configuration des informations du déploiement

Sur le Master sont configurées les informations suivantes :

- Certificats des Autorités de certification
- Liste de révocation des certificats (CRL)
- Liste des M>Tunnel Gateways dans l'organisation VPN

Ces informations sont alors téléchargées par les Gateways et les Clients du VPN. Quand une gateway ou un client télécharge ces informations à partir du Master, ce dernier vérifie tout d'abord lors de l'authentification :

- le chemin de validation
- la liste de révocation des certificats émise par l'Autorité de certification
- la période de validité du certificat du client ou de la gateway

C'est seulement une fois que ces vérifications auront été effectuées que les informations sur la configuration seront téléchargées du moment que le M>Tunnel Client ou les M>Tunnel Gateways appartiennent au groupe d'accès requis. Le M>Tunnel Master doit être situé sur un réseau qui est accessible à partir de tout endroit sur l'Internet ou l'Intranet de façon à permettre aux M>Tunnel Clients et aux M>Tunnel Gateways de télécharger les informations dont ils ont besoin. La phase d'authentification, préalable à tout envoi d'informations par le M>Tunnel Master, garantit la sécurité du système. De plus, cette communication est protégée en confidentialité et en intégrité.

Les groupes d'accès

Les groupes d'accès sur le M>Tunnel Master déterminent les personnes qui ont le droit de télécharger des informations spécifiques. Quand une Gateway ou un Client se connecte au M>Tunnel Master pour télécharger la liste des Gateways M>Tunnel avec lesquelles il a le droit de communiquer, les champs du certificat sont filtrés pour établir la liste des Gateways. Un groupe d'accès établit les Gateways M>Tunnel avec lesquelles un M>Tunnel Client ou une M>Tunnel Gateway a le droit de créer un tunnel. Par exemple; on peut avoir une M>Tunnel Gateway 'Fuschia" qui est utilisée par les employés du département Ventes et une autre M>Tunnel Gateway "Gypsophile" qui est utilisée par une M>Tunnel Gateway d'une organisation séparée. Sur le M>Tunnel Master, on a besoin d'associer un groupe d'accès avec "Fuschia" qui limite l'accès pour les employés du département Ventes et d'associer un autre groupe d'accès avec "Gypsophile" qui limite l'accès pour le M>Tunnel Gateway de l'autre organisation.

Le fichier de configuration

Sur le M>Tunnel Master, on a aussi besoin de créer un fichier de configuration qui est utilisé quand on installe une M>Tunnel Gateway ou un M>Tunnel Client. Ce fichier de configuration contient :

- L'adresse IP de l'interface réseau du M>Tunnel Master auquel les M>Tunnel Gateways et les Clients sont connectés

- La liste des certificats de l'Autorité de certification (CAs) et leur date de validité.
- La liste des listes de révocation des certificats (CRLs) et leur date de validité .
- L'adresse IP des M>Tunnel Gateways avec lesquelles la M>Tunnel Gateway ou le M>Tunnel Client peut communiquer.
- Paramètres de configuration pour la M>Tunnel Gateway ou Client.

On peut appliquer un groupe d'accès au fichier de configuration afin qu'il contienne uniquement la liste des Gateways utilisées.

Condition d'activation

Le logiciel M>Tunnel Master est activé dès la mise sous tension du matériel

2.1.2 Les M>Tunnel Gateways

Les M>Tunnel Gateways sont les extrémités du tunnel pour les réseaux auxquels ils sont connectés. Dans la configuration d'une organisation VPN, les M>Tunnel Gateways :

- Téléchargent les informations de configuration à partir du M>Tunnel Master.
- Créent des politiques de tunnel.

Téléchargement des informations sur la configuration

Les M>Tunnel Gateways téléchargent un sous-ensemble d'informations sur la configuration à partir du Master :

- Le chemin de validation de la certification
- Les listes de révocation des certificats (CRLs)
- La liste des M>Tunnel Gateways avec lesquelles la M>Tunnel Gateway a le droit de se connecter

Elles vérifient que les informations sur la configuration sont mises à jour régulièrement en comparant le numéro de série de leur configuration avec le numéro de série de la configuration sur le M>Tunnel Master.

En cas de non connexion réussie avec le M>Tunnel Master, le M>Tunnel Gateway utilise les informations issues de sa précédente connexion avec ce dernier.

Configuration de la politique M>Tunnel

Les politiques M>Tunnel sont configurées sur les Gateways par les administrateurs locaux. Les M>Tunnel Clients téléchargent leurs politiques à partir des M>Tunnel Gateways spécifiées dans leur fichier de configuration. Il existe cinq types de politiques M>Tunnel :

- Gateway vers Gateway (standard IPsec)
- Gateway vers client (standard IPsec)
- Les politiques de filtrage
- Gateway vers Gateway (standard MATRAnet)
- Gateway vers client (standard MATRAnet)

Pour des raisons de compatibilité ascendante, MATRAnet continue à maintenir le protocole (appelé standard MATRAnet) qu'elle avait mis au point. Ce dernier est très proche du standard IPSEC et diffère principalement de ce dernier par le numéro de protocole.

Condition d'activation

Le logiciel M>Tunnel Gateway est activé dés la mise sous tension du matériel.

Le logiciel M>Tunnel Gateway peut être installé sur le même poste que le M>Tunnel Master.

L'enclenchement d'un tunnel se fait par l'une ou l'autre des extrémités dés que cette dernière est prête. Entre deux M>Tunnel Gateway, chacune va essayer d'établir un tunnel et c'est la dernière, qui sera mise sous tension, qui parviendra à initialiser le tunnel.

2.1.3 Les M>Tunnel Clients

Les M>Tunnel Clients téléchargent les informations à la fois à partir du M>Tunnel Master et des M>Tunnel Gateways :

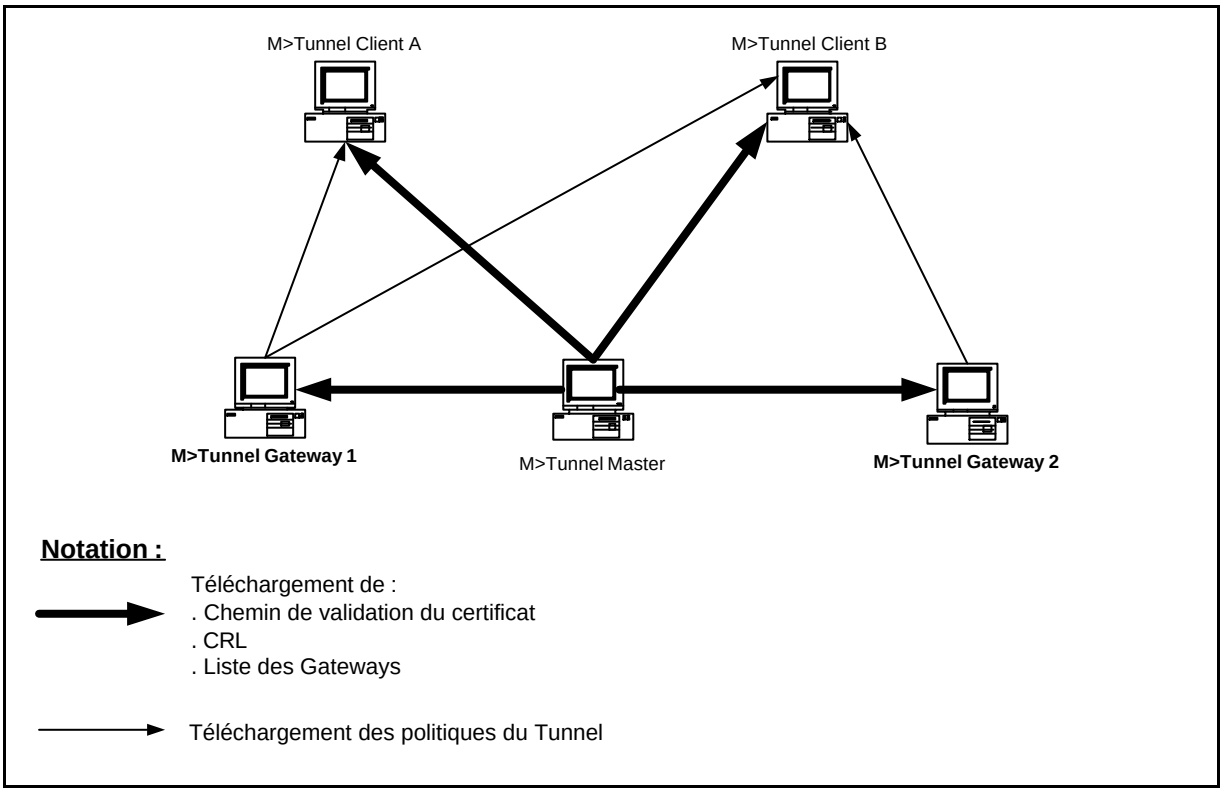
- A partir du M>Tunnel Master, ils téléchargent les informations sur l'Autorité de certification, la liste des M>Tunnels Gateways et la liste de révocation des certificats qui sont en cohérence avec le groupe d'accès de l'utilisateur.
- A partir des M>Tunnel Gateways, ils téléchargent les politiques M>Tunnel.

Les M>Tunnel Clients vérifient que les informations sur la configuration sont mises à jour régulièrement ou chaque fois que le M>Tunnel Client est redémarré en comparant le numéro de série de leur configuration avec ceux sur le M>Tunnel Master et les M>Tunnel Gateways correspondants.

En cas de non connexion réussie avec le M>Tunnel Master, le M>Tunnel Client utilise les informations issues de sa précédente connexion avec ce dernier.

Exemple de téléchargement de configuration

Un exemple simplifié de la façon de télécharger les informations est présenté ci-dessous. Les deux M>Tunnel Gateways téléchargent les informations sur la certification (le chemin de validation du certificat et la liste de révocation du certificat). Les deux M>Tunnel Clients téléchargent, à partir du M>Tunnel Master, les informations sur l'autorité de certification et la liste des M>Tunnel Gateways, qui leur sont autorisées selon le groupe d'accès de chaque utilisateur. Chaque M>Tunnel Client télécharge alors les politiques M>Tunnel à partir des M>Tunnel Gateways, selon la liste de ces dernières qu'il a préalablement téléchargée à partir du M>Tunnel Master. Dans l'exemple ci-dessous, le M>Tunnel Client A télécharge seulement les politiques à partir du M>Tunnel Gateway 1 pendant que le M>Tunnel B télécharge les politiques à partir des M>Tunnel Gateway 1 et 2.



Condition d'activation

Le logiciel M>Tunnel Client peut être activé soit dès la mise sous tension du matériel du poste de travail soit par une action manuel de l'utilisateur mais il ne devient réellement effectif qu'après avoir permis l'accès au support d'identifiant de l'utilisateur.

L'enclenchement d'un tunnel se fait par l'une ou l'autre des extrémités dés que cette dernière est prête. Entre un M>Tunnel Client et un M>Tunnel Gateway, l'enclenchement se fait toujours à l'initiative de l'utilisateur.

2.1.4 Les politiques M>Tunnel

Une politique M>Tunnel est négociée entre deux M>Tunnel Gateways ou entre une M>Tunnel Gateway et un M>Tunnel Client. Il existe cinq types de politiques du tunnel :

- Gateway vers Gateway (standard IPsec)
- Gateway vers client (standard IPsec)

- Les politiques de filtrage
- Gateway vers Gateway (standard MATRAnet)
- Gateway vers Client (standard MATRAnet)

Une politique entre deux Gateways est parfois dite politique "statique", car les adresses IP des deux extrémités sont connues. Une politique entre une Gateway et un Client est dite politique "dynamique" car l'adresse IP de l'extrémité du M>Tunnel Client n'est pas connue d'avance (dans le cas d'ordinateurs portables se connectant à Internet au moyen d'un ISP par exemple).

Translation d'adresse

Une politique M>Tunnel peut changer les adresses source pour d'autres adresses. Cette opération est nécessaire si on veut créer une politique M>Tunnel qui chiffre les données entre deux réseaux qui ont les mêmes adresses réseau. Dans le cas d'une société qui a un réseau 10.1* et qui veut créer un canal de chiffrement avec une autre société qui possède aussi un réseau 10.1* , les paquets ne peuvent pas être routés. Dans ce cas on peut utiliser une translation d'adresse pour changer l'adresses source des ordinateurs pour les nouvelles adresses spécifiées. La politique correspondante pour l'autre M>Tunnel Gateway doit spécifier les adresses translatées comme étant les adresses destination. M>Tunnel utilise une adresse de translation statique ; une adresse source donnée est toujours fournie avec la même adresse translatée. Le nombre des adresses des deux sous-réseaux doit donc être identique. Pour créer un réseau de chiffrement entre deux sociétés ayant des adresses internes identiques, on peut utiliser les règles suivantes de translation d'adresse (NAT) : une sur la première M>Tunnel Gateway qui remplace les adresses source 10.1.* avec 30.1* et une deuxième sur l'autre M>Tunnel Gateway qui remplace les adresses source 10.1* par les adresses source 20.1*.

Politiques de Gateway vers Gateway

Comme son nom l'indique, une politique de Gateway vers Gateway crée un tunnel avec une Gateway à chaque extrémité. Ce type de politique permet d'ouvrir un Tunnel permanent entre deux sous-réseaux ou deux entités qui sont dites sûres. Les adresses IP des Gateways sont fixées, et ainsi ce type de politique est parfois appelée "statique". Les politiques pour une gateway sont configurées sur la M>Tunnel Gateway elle-même. Les politiques de Gateway vers Gateway ne sont pas téléchargées par les autres M>Tunnel Gateway donc il faut les configurer de chaque côté. On peut créer un groupe d'accès pour une politique de gateway à gateway qui vérifie que le certificat de l'autre gateway est conforme au groupe d'accès. Deux types de politiques de Gateway vers Gateway peuvent être configurées : standard IPsec et standard MATRAnet. Les politiques standard IPsec sont compatibles avec RFC2401, et utilisent le numéro de protocole 50 pour ESP ou 51 pour AH dans l'en-tête du paquet (si ESP et AH sont à la fois appliqués, c'est le numéro du dernier service appliqué qui apparaît).

Politiques de Gateway vers Client

Une politique de Gateway vers Client crée un tunnel entre une Gateway et un ordinateur avec une adresse inconnue. Parce que l'adresse IP de l'extrémité de la destination n'a pas besoin d'être connue, on parle parfois de politique "dynamique". Les politiques de Client vers Gateway sont configurées sur les Gateways et téléchargées par les Clients à partir des Gateways. Il n'y a donc aucune configuration à effectuer côté Client. On peut attribuer un groupe d'accès à la politique de Client vers Gateway pour limiter les accès. Ce groupe permet d'accepter ou de refuser l'accès des utilisateurs à la politique, en filtrant le contenu des certificats. De plus, quand la politique est négociée entre le M>Tunnel Client et la M>Tunnel Gateway, la Gateway vérifie le certificat du client pour s'assurer que celui-ci est dans le groupe d'accès requis. Si on sélectionne l'option de filtrage associée avec les politiques de Gateway vers Client, tout le trafic qui traite la politique sera bloqué à moins qu'un tunnel soit établi. Les politiques de Gateway à Client peuvent utiliser soit une connexion Ethernet (LAN), soit un modem de connexion (WAN). Dans le cas d'un Client qui télécharge plusieurs politiques à partir de différentes Gateways, les politiques sont triées selon l'ordre établi dans la liste des Gateways qui est téléchargée à partir du M>Tunnel Master. Par conséquent, dans le cas où un Tunnel Client aurait deux politiques incompatibles, ce serait la première politique qui serait utilisée. Deux types de politiques de Gateway vers Client peuvent être configurées : standard IPsec et standard MATRAnet. Les politiques standard IPsec sont compatibles avec RFC2401, et utilisent le numéro de protocole 50, pour ESP ou 51 pour AH dans l 'en-tête du paquet (si ESP et AH sont à la fois appliqués, c'est le numéro du dernier service implémenté qui apparaît). Les politiques standard IPsec rendent possible la création de tunnels vers d'autres sociétés à l'aide d'un logiciel de chiffrement. Les politiques standards MATRAnet utilisent le numéro 181 dans l'en-tête du paquet et sont compatibles avec M>Tunnel 2.0 et les versions antérieures.

Politique de filtrage

Une politique de filtrage filtre les données sur la M>Tunnel Gateway elle-même et traite les paquets de deux façons différentes :

- Soit elle les rejette.

- Soit elle les autorise.

Une politique de filtrage peut s'appliquer au trafic entrant et/ou sortant à partir de la M>Tunnel Gateway. Une politique de filtrage qui rejette les paquets spécifiés est utile pour les administrateurs avec une version autonome de M>Tunnel (sans firewall) qui peut facilement créer des règles de filtrage de paquets. Une politique de filtrage qui contourne le tunnel est utile pour le traitement des paquets qui ne contiennent aucune information confidentielle. On peut l'illustrer à l'aide de l'exemple suivant : Si on veut tout chiffrer entre deux réseaux exceptées les communications HTTP, qui représentent un gros débit de données, mais qui demeurent malgré tout peu importantes en matière de sécurité, on peut créer une règle de politique de filtrage qui contourne le tunnel pour tous les paquets qui ont pour origine un port spécifique, dans ce cas le port numéro 80 pour les paquets HTTP, puis une politique standard de Gateway à Gateway qui chiffre toutes les autres données entre les réseaux spécifiques. Les politiques de filtrage, qui peuvent servir à ne laisser passer que les flux IP correspondants à des communications autorisées avec les Gateways, ne sont pas téléchargées par les machines Client.

Exemples de configuration de politique

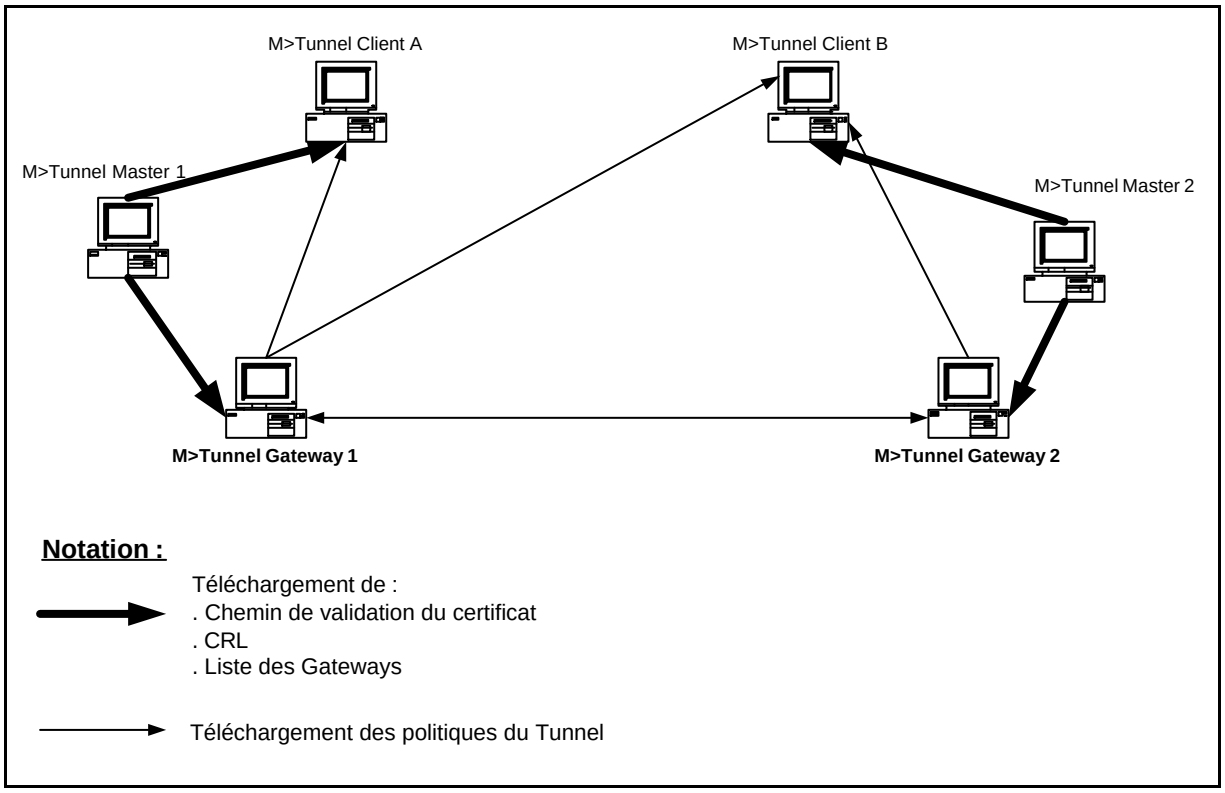
Le diagramme ci-dessous montre un VPN entre deux entités ou filiales qui sont associées et deux utilisateurs nomades qui possèdent des portables et ayant besoin de se connecter aux deux réseaux à la fois. Il existe cinq politiques de tunnel :

- une politique de Gateway vers Gateway entre Gateway 1 et Gateway 2
- une politique de Gateway vers Gateway entre Gateway 2 et Gateway 1

trois politiques de gateway vers client entre :

- Client tunnel B et Gateway 2
- Client tunnel B et Gateway 1
- Client tunnel A et Gateway 1

Les Gateways et les Clients téléchargent les informations sur les certificats et la liste des Gateways à partir de leur M>Tunnel Master respectif. Chaque administrateur local de chaque Gateway détermine la politique du tunnel. Chaque Client peut alors télécharger les politiques des Gateways auxquelles il peut accéder conformément à la liste qu'il a reçue. Dans le schéma ci-dessus, les deux M>Tunnel Masters doivent connaître chaque Autorité de certification, afin que le M>Tunnel Client B puisse télécharger les politiques du Tunnel à partir des deux M>Tunnel Gateways.



2.1.5 L'administration M>Tunnel

La gestion des équipements M>Tunnel Master et M>Tunnel Gateway ainsi que l'administration de la politique de chiffrement se font à l'aide d'un logiciel d'administration. La communication entre la station d'administration et chaque M>Tunnel (Master ou Gateway) se fait de façon sécurisée sur un port particulier. Cette sécurisation est faite en installant un logiciel M>Tunnel Client sur la station qui héberge le logiciel d'administration et en imposant une politique de chiffrement et de filtrage de haut niveau de sécurité (Confidentialité :Triple-DES, Intégrité : Hmac-MD5, Filtrage : interdiction de tous les flux à l'exception de ceux d'administration). Le logiciel d'administration, qui est une application écrite en JAVA, est installée sur un PC muni de l'OS Windows 2000.

2.2 Composition de la cible d'évaluation

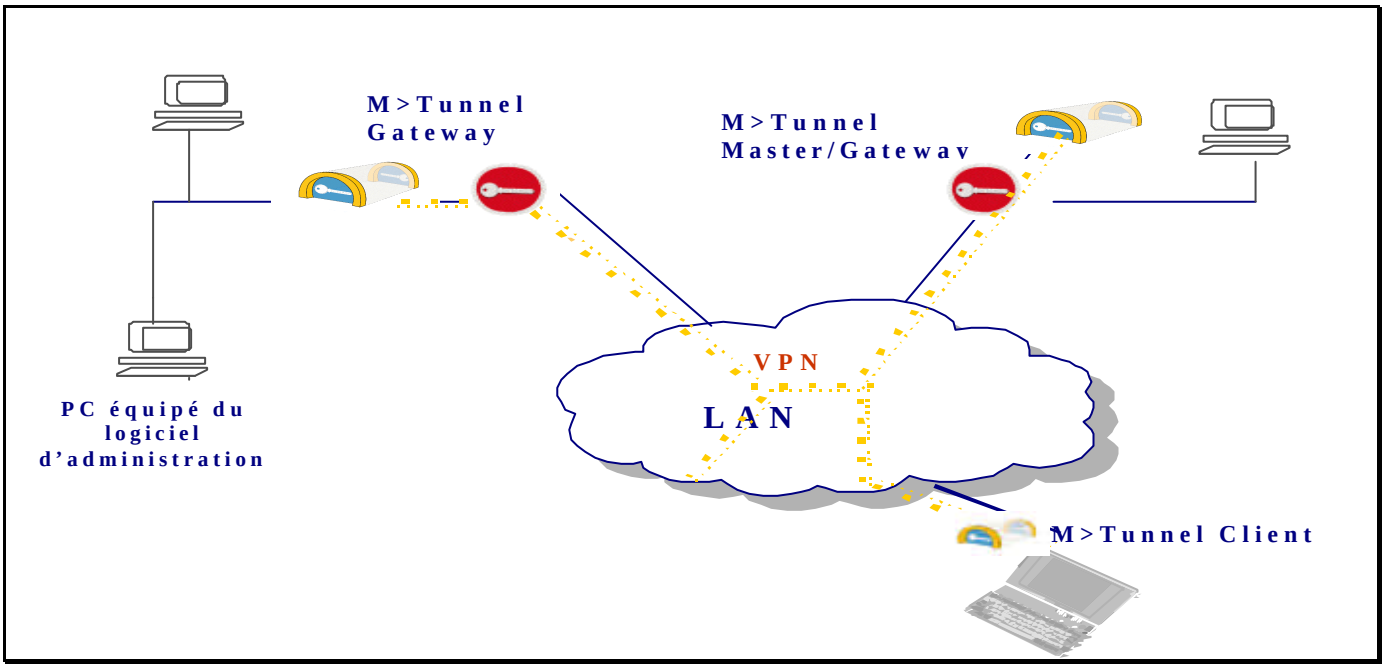
La cible d'évaluation est composée des éléments suivants :

- 1 M>Tunnel Master installé sur le même PC qu'un M>Tunnel Gateway
- 2 M>Tunnel Gateway installés chacun sur un PC équipé de l'Operating System BSDi 4.3 de WindRiver expurgé des services non utilisés (cet OS est fourni par MATRAnet et fait partie de la TOE)
- 1 M>Tunnel Client installé sur un poste nomade équipé d'un Windows 2000 et d'un lecteur de carte à puce Gemplus ; la fonctionnalité est enclenchée dés la mise sous tension du poste de travail
- le logiciel d'administration, couplé avec un M>Tunnel Client, installés sur un PC équipé d'un Windows 2000 et d'un lecteur de carte à puce Gemplus

La configuration de la TOE doit respecter les règles suivantes :

- les algorithmes de chiffrement utilisés sont Triple-DES ou AES.
- Le seuil de renégociation des clés est inférieur à 150000 paquets.
- Il faut toujours travailler en ESP authentifié.
- Le délai maximum de re-négociation des clés est de 30 minutes.

Le schéma ci-dessous donne un exemple de topologie pour la TOE :



La gestion des certificats ne fait pas partie de la TOE ; seul le téléchargement de la CRL via le logiciel d'administration est pris en compte.

La carte à puce, le lecteur et le driver associés (jusqu'à l'interface PKCS#11) ne font pas partie de la TOE car on doit pouvoir utiliser n'importe quel support de certificat à condition que ce dernier ait été certifié et qu'il possède une interface PKCS#11 (le seul protocole de chargement des certificats supporté par M>Tunnel est PKCS#11).

L'authentification local de l'utilisateur ainsi que les mécanismes d'accès aux informations stockées sur son PC ne font pas partie de la TOE.

La TOE intègre un ensemble de ressources ayant pour but de protéger (en intégrité et/ou en confidentialité) les informations externes et le transfert des informations internes suivantes (biens) :

- Informations internes :
    - Politique de chiffrement : informations définissant les algorithmes de chiffrements (confidentialité) et de signature (intégrité), les flux sur lesquels ces algorithmes doivent s'appliquer
    - Politique de filtrage : informations définissant les flux qui sont autorisés à traverser la TOE et ceux qui doivent être bloqués ainsi que les changements d'adresse à appliquer (NAT)
    - CA : liste des authorités de certification
    - CRL : liste des certificats révoqués
    - Configuration : informations définies sur le M>Tunnel Master permettant aux M>Tunnels Clients de connaître les M>Tunnels Gateway avec lesquels il peut établir un VPN
    - Fichiers d'évènements : fichiers contenant l'ensemble des messages fournis par un composant de la TOE
    - Clés de session : clés servant au chiffrement ou à l'authentification des paquets IP
    - Identifiant : le certificat et la clé privée d'un composant de la TOE (M>Tunnel Master, M>Tunnel Gateway ou M>Tunnel Client)
- Ressources internes :
    - Authentification : mécanisme permettant l'authentification mutuelle entre les deux extrémités d'un tunnel
    - Négociation des clés de session : mécanisme permettant l'échange de clés de session entre les deux extrémités d'un tunnel
    - Confidentialité et intégrité des paquets : mécanisme permettant le chiffrement (algorithmes 3 DES, AES) et l'intégrité des paquets IP
    - Daemon d'administration : mécanisme de dialogue entre le M>Tunnel Master ou Gateway et le logiciel d'administration
- Informations externes (données utilisateur) :
    - Informations transitant sur un tunnel : tout paquet IP arrivant à une extrémité du tunnel et à destination d'une machine située derrière l'autre extrémité du tunnel

3. ENVIRONNEMENT de SECURITE

3.1 Hypothèses d'utilisation

SU1 Les M>Tunnel Master et Gateway ainsi que le logiciel d'administration sont physiquement protégés de façon à ce que seuls les administrateurs aient accès physiquement à ces machines.

SU2 Les fonctions de sécurité incluses dans la TOE pouvant être compromises par les administrateurs, ces derniers sont des gens de confiance et ont été formés.

SU3 Le logiciel d'administration est utilisée conformément à sa documentation « Guide de l'administrateur ».

SU4 Sur les postes de travail intégrant les logiciels M>Tunnel Master, M>Tunnel Gateway ou celui d'administration, les administrateurs modifient périodiquement les mots de passe d'accès en prenant comme contrainte qu'ils doivent être aléatoires et d'une longueur supérieure à 7 caractères alphanumériques.

SU5 Les administrateurs analysent périodiquement les fichiers d'évènements afin de s'assurer qu'aucune attaque n'a eu lieu et vérifient le bon fonctionnement de l'enregistrement des évènements (Typiquement, ils s'assurent qu'il y a de la place disque suffisante).

SU6 La TOE est administrée, par un seul administrateur autorisé à la fois, à l'aide du logiciel d'administration (ceci a pour but d'éviter un conflit d'accès à la politique de chiffrement ou de filtrage qui peut entraîner une non prise en compte de modifications de ces politiques)

SU7 Le M>Tunnel Master doit être connecté à un réseau accessible par tous les M>Tunnel Client et les M>Tunnel Gateways.

SU8 Chaque utilisateur doit recevoir, de façon sécurisé, son certificat et sa clé privée associée, stockés sur un support indépendant. Les sauvegardes des clés privées des utilisateurs, si elles existent, doivent être sécurisées.

SU9 L'utilisateur n'est pas administrateur de son poste de travail (cette hypothèse a pour but d'empêcher les erreurs de manipulation, ou l'éventuelle malhonnêteté de l'utilisateur) .

SU10 Le logiciel d'administration est installé sur un poste disposant d'un M>Tunnel Client, et les M>Tunnel Master sont installés sur un poste équipé d'un M>Tunnel Gateway.

SU11 La politique de chiffrement doit être définie en un seul point même si elle s'applique dans un environnement distribué où les informations traversent un réseau non sûr.

3.2 Menaces

Les menaces prises en compte peuvent l'être soit par la TOE elle-même soit par l'environnement opérationnel mis en œuvre autour de cette dernière.

3.2.1 Menaces prises en compte par la TOE

T1 Un utilisateur autorisé peut, par erreur, modifier les politiques de chiffrement et de filtrage concernant le M>Tunnel Client.

T2 Un attaquant (externe ou interne) peut modifier les politiques de chiffrement et de filtrage afin d'avoir accès, en clair, lors de leur transfert sur le réseau, à des informations qui auraient du transiter chiffrées.

T3 Un attaquant peut bloquer le fonction du VPN en empêchant la communication (daemon d'administration) entre le logiciel d'administration et les M>Tunnel Master ou Gateway, ou en modifiant les informations transitant entre ces différents composants (Politique de chiffrement, Politique de filtrage, CRL, Configuration).

T4 Une personne non autorisée peut accéder ou modifier les fichiers d'évènements stockés sur les M>Tunnels Gateway et Master de la TOE.

T5 La TOE n'est plus en mesure de remplir les fichiers d'évènements.

T6 Un attaquant peut capturer les clés de session servant au chiffrement des paquets IP.

T7 Un utilisateur, autre que celui à l'initiative de la mise en œuvre du tunnel, peut récupérer, les clés de session de ce tunnel et déchiffrer ainsi les paquets IP transitant sur ce dernier.

T8 Un utilisateur peut , par des erreurs de manipulations du M>Tunnel Client, entraîner le blocage ou la destruction d'un M>Tunnel Gateway.

T9 Un attaquant , muni d'un logiciel M>Tunnel Client , ou un utilisateur sans sa carte à puce, peut se connecter à un M>Tunnel Master puis à un M>Tunnel Gateway et ainsi établir un tunnel afin d'avoir accès aux informations protégées par la politique de filtrage.

T10 Un attaquant peut modifier l'intégrité des paquets IP circulant sur le réseau sans que les utilisateurs de ces informations s'en aperçoivent.

T11 Un utilisateur, suite à une erreur de manipulation, empêche la mise en œuvre du M>Tunnel Client sur son poste de travail et envoie, sans le savoir, des données non chiffrées.

T12 Lors d'un dysfonctionnement (ou d'un déni de service) du M>Tunnel Master, les utilisateurs ne peuvent plus accéder aux différents M>Tunnel Gateway dont ils connaissent les caractéristiques. Ces caractéristiques n'ayant pas changé depuis le début du dysfonctionnement (ou déni de service) du M>Tunnel Master.

T13 Un attaquant peut effectuer une attaque en confidentialité et/ou en intégrité sans connaissance préalable des secrets.

T14 La sécurité de la TOE peut être réduite suite à des non cohérences dans les règles de sécurité définies par l'administrateur à l'aide du logiciel d'administration.

3.2.2 Menaces liées à l'environnement opérationnel

TE1 La sécurité de la TOE peut être réduite suite à des erreurs ou omissions des règles de sécurité par le logiciel d'administration.

TE2 La TOE est installée de façon non sûre.

3.3 Politique de sécurité organisationnelle

P1 La PKI doit fournir des identifiants uniques pour chaque utilisateur et chaque équipement de la TOE.

P2 La politique de chiffrement doit garantir que les informations sensibles, contenues dans des paquets IP, circulant sur des réseaux non sûr doivent être chiffrées et authentifiées.

P3 La politique de filtrage doit garantir que seuls les flux autorisés peuvent traverser les équipements M>Tunnel Gateway.

P4 L'administrateur doit tenir à jour la CRL à partir des informations fournies par la PKI.

4. OBJECTIFS DE SECURITE

Les objectifs à satisfaire peuvent l'être soit par la TOE elle-même soit par l'environnement opérationnel mis en œuvre autour de cette dernière.

4.1 Objectifs de sécurité pour la TOE

O1 La TOE doit s'assurer, lors de la phase de mise en œuvre d'un tunnel, que l'utilisateur, possède un identifiant autorisé et qu'aucune phase de re-jeu n'est en cours.

O2 La TOE doit appliquer la politique de chiffrement et de filtrage définie par l'administrateur.

O3 La TOE doit fournir les moyens permettant d'enregistrer les événements de sécurité tels que :

- **les tentatives d'intrusion,**
- **les authentifications de chaque utilisateur.**

O4 La TOE doit s'assurer que seuls les administrateurs autorisés ont le droit, grâce au logiciel d'administration, de se connecter sur la station d'administration et/ou sur les M>Tunnel Master et Gateway afin de changer les politiques de chiffrement, de filtrage, la CRL et la configuration et d'avoir accès aux messages de sécurité.

O5 La TOE doit se protéger contre les modifications ou désactivations, non intentionnelles, des mécanismes de sécurité et des modifications non intentionnelles des informations propres à la TOE.

O6 La TOE doit fournir, à l'administrateur, lors de la mise en œuvre d'une politique de chiffrement et/ou de filtrage, une vérification de cohérence.

O7 La TOE doit pouvoir rejeter tout paquet IP signé qui a subi des modifications durant son transfert sur le réseau.

O8 La TOE doit pouvoir chiffrer les paquets IP transitant sur le réseau.

O9 La TOE doit protéger le transfert des clés de session.

O10 La TOE doit empêcher un utilisateur d'un tunnel d'accéder aux informations transitant sur un autre tunnel.

O11 La TOE doit être capable de renouveler, automatiquement et de façon sûr, les clés de session selon des critères paramétrables (durée, quantité d'information traitées).

O12 M>Tunnel Gateway et M>Tunnel Master doivent pouvoir fonctionner même s'il n'y a plus de liaison avec la station d'administration.

O13 La TOE doit être capable de gérer les cas d'erreurs de manipulation lors de la mise en œuvre d'un tunnel ou lors de la négociation des clés de session.

O14 Toutes les informations liées à la politique de chiffrement ou de filtrage ainsi que la configuration et transitant sur un réseau non sûr doivent être sécurisées. De plus, ces informations doivent être stockées sur le poste de l'utilisateur et utilisées en cas de rupture de la communication avec le M>Tunnel Master.

4.2 Objectifs de sécurité pour l'environnement

OE1 Le responsable de la TOE doit s'assurer que la TOE a été correctement installée selon les indications fournies dans le guide d'installation (en particulier les services fournis de base avec l'Operating System et n'étant pas requis ont été inhibés).

OE2 Le responsable de la TOE doit s'assurer que les M>Tunnel Gateway et la station d'administration se situent dans un lieu où seules les personnes autorisées peuvent accéder.

OE3 Le responsable de la TOE doit s'assurer que les administrateurs sont des personnes de confiance.

OE4 Tous les administrateurs doivent avoir été formés sur le produit M>Tunnel et leur niveau doit avoir été reconnu par le formateur.

OE5 Les administrateurs doivent s'assurer que la politique par défaut qui est appliquée est le chiffrement et l'authentification des paquets IP.

OE6 Le M>Tunnel Master doit être placé sur le réseau de façon à ce que les M>Tunnel Client et les M>Tunnel Gateways puissent se connecter à lui.

OE7 Les certificats et les clés privées des utilisateurs doivent être stockées sur un support indépendant et fourni, de façon sécurisée, à ces derniers. Les clés privées ne doivent pas pouvoir être extraites de ce support.

OE8 Tous les postes de travail équipés de M>Tunnel Client doivent être administrés par des administrateurs autorisés.

OE9 Le poste où est installée la station d'administration doit être équipé d'un M>Tunnel Client et ceux où sont installés les M>Tunnel Master doivent être équipés de M>Tunnel Gateway.

5. Exigences de sécurité

5.1 Exigences de sécurité fonctionnelles

Les exigences de sécurité à prendre en compte sont les suivantes :

Classe	Composants
Audit de sécurité	FAU_GEN Génération des données de l'audit de sécurité
	FAU_SAR Revue de l'audit de sécurité
	FAU_STG Enregistrement d'évènements de l'audit de sécurité
Support Cryptographique	FCS_CKM Gestion des clés cryptographiques
	FCS_COP Opération cryptographique
Protection des données utilisateur	FDP_ACC Politique de contrôle d'accès
	FDP_ACF Fonctions de contrôle d'accès
	FDP_IFC Politique de contrôle de flux d'informations
	FDP_IFF Fonctions de contrôle de flux d'informations
	FDP_ITT Transfert interne à la TOE
	FDP_UCT Protection de la confidentialité des données de l'utilisateur lors d'un transfert inter-TSF
	FDP_UIT Protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF
Identification et Authentification	FIA_AFL Défaillance de l'authentification
	FIA_ATD Définition des attributs d'un utilisateur
	FIA_UAU Authentification d'un utilisateur
	FIA_UID Identification d'un utilisateur
Gestion de la sécurité	FMT_MSA Gestion des attributs de sécurité
	FMT_MTD Gestion des données de la TSF
	FMT_SMR Rôle pour la gestion de la sécurité
Protection des fonctions de sécurité de la TOE	FPT_ITT Transfert des données de la TSF à l'intérieur de la TOE
	FPT_RPL Détection de rejeu
	FPT_RVM Passage obligatoire par un moniteur de référence
	FPT_STM Horodatage

5.1.1 Définition des SFP

Users access control SFP : politique définissant les différents droits d'accès des utilisateurs de M>Tunnel Client aux informations circulant sur le réseau (appartenance à une autorité de certification, la non révocation, l'appartenance à un groupe d'accès).

Administrators access control SFP : politique définissant les différents droits d'accès des administrateurs aux informations issues des équipements M>Tunnel (M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client et logiciel d'administration)

information flow control SFP : politique de chiffrement et de filtrage, stockée sur l'équipement M>Tunnel Gateway ou M>Tunnel Client, concernant les paquets IP transitant entre deux extrémités d'un tunnel

5.1.2 Audit de sécurité

5.1.2.1 FAU_GEN Génération des données de l'audit de sécurité

FAU_GEN.1 Génération de données d'audit

- Hiérarchiquement supérieur à : aucun autre composant.
- **FAU_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:
  - Start-up and shutdown of the audit functions;
  - All auditable events for the [*detailed*] level of audit; and
  - [
    - *result of authentication step,*
    - *result of key negotiation step,*
    - *result of key renegotiation step,*
    - *refused packets and the reason of it (no ciphering policy, packet integrity problem)*
    - *no coherent ciphering policy between 2 M>Tunnel Gateway,*
    - *software integrity problem*].
- **FAU_GEN.1.2** The TSF shall record within each audit record at least the following information:
  - Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
  - For each audit event type, based on the auditable event definitions of the functional components included in the ST, [
    - *user identity,*
    - *source and destination IP addresses,*
    - *different states of authentication step,*
    - *different states of key negotiation step,*
    - *different states of key renegotiation step*]
- Dépendances : FPT_STM.1 Horodatage fiable
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client, station d'administration

FAU_GEN.2 Lien avec l'identité de l'utilisateur

- Hiérarchiquement supérieur à : aucun autre composant.
- **FAU_GEN.2.1** The TSF shall be able to associate each auditable event with the identity of the user that caused the event.
- Dépendances :
  - FAU_GEN.1 Génération de données d'audit
  - FIA_UID.1 Timing de l'identification
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client, station d'administration

5.1.2.2 FAU_SAR Revue de l'audit de sécurité

FAU_SAR.1 Revue d'audit

Le présent composant fournit aux utilisateurs autorisés la possibilité d'obtenir et d'interpréter les informations. Dans le cas où il s'agit d'utilisateurs humains (de personnes), ces informations doivent être présentées sous une forme compréhensible. Dans le cas où il s'agit d'entités TI externes, les information doivent être présentées sans ambiguïté sous un format électronique.

- Hiérarchiquement supérieur à : aucun autre composant.
- **FAU_SAR.1.1** The TSF shall provide [*identified administrators*] with the capability to read [*all audit information*] from the audit records.
- **FAU_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
- Dépendances : FAU_GEN.1 Génération de données d'audit
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client, station d'administration

FAU_SAR.2 Revue d'audit restreinte

- Hiérarchiquement supérieur à : aucun autre composant.
- **FAU_SAR.2.1** The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
- Dépendances : FAU_SAR.1 Revue d'audit
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, station d'administration

FAU_SAR.3 Revue d'audit sélective

- Hierarchical to: No other components.
- **FAU_SAR.3.1** The TSF shall provide the ability to perform [*searches and sorting*] of audit data based on [
  - *presence or absence of keywords,*
  - *ranges of dates*].
- Dépendances : FAU_SAR.1 Revue d'audit
- Composants de la TOE concernés : station d'administration

5.1.2.3 FAU_STG Enregistrement d'évènements de l'audit de sécurité

FAU_STG.2 Garanties de disponibilité des données d'audit

- Hiérarchiquement supérieur à : FAU_STG.1
- **FAU_STG.2.1** The TSF shall protect the stored audit records from unauthorised deletion.
- **FAU_STG.2.2** The TSF shall be able to [*prevent*] modifications to the audit records.
- **FAU_STG.2.3** The TSF shall ensure that [*all*] audit records will be maintained when the following conditions occur: [
  - *audit storage exhaustion*].
- Dépendances : FAU_GEN.1 Génération de données d'audit
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client, station d'administration

FAU_STG.4 Prévention des pertes de données d'audit

- Hiérarchiquement supérieur à : FAU_STG.3
- **FAU_STG.4.1** The TSF shall [*ignore auditable events*] and [*write a specific message into the audit database*] if the audit trail is full.
- Dépendances : FAU_GEN.1 Génération de données d'audit
- Composants de la TOE concernés : M>Tunnel Gateway, station d'administration

5.1.3 Support Cryptographique

5.1.3.1 FCS_CKM Gestion des clés cryptographiques

FCS_CKM.1 Génération de clés cryptographiques

- Hiérarchiquement supérieur à : aucun autre composant.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*pseudo-random number generation*] and specified cryptographic key sizes [*56,128 et 168*] that meet the following: [*Ipsec specification for key generation*].

- Dépendances :
  - FCS_COP.1 Opération cryptographique
- Composants de la TOE concernés : M>Tunnel Gateway, M>Tunnel Client

FCS_CKM.2 Distribution de clés cryptographiques

- Hiérarchiquement supérieur à : aucun autre composant.
- **FCS_CKM.2.1** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [*key negotiation protocol with RSA algorithm*] that meets the following: [*Nothing*].
- Dépendances :
  - FCS_CKM.1 Génération de clés cryptographiques
  - FCS_COP.1 Opération cryptographique
- Composants de la TOE concernés : M>Tunnel Gateway, M>Tunnel Client

5.1.3.2 FCS_COP Opération cryptographique

FCS_COP.1 Opération cryptographique

- Hiérarchiquement supérieur à : aucun autre composant.
- **FCS_COP.1.1-1** The TSF shall perform [
  - *session key generation]*

  in accordance with a specified cryptographic algorithm [
  - *specific algorithm*]

  and cryptographic key sizes [
  - *168*
  - *128, 192*]

that meet the following: [nothing].

- **FCS_COP.1.1-2** The TSF shall perform [
  - *ciphering and deciphering of data]*

  in accordance with a specified cryptographic algorithm [
  - *Triple DES*
  - *AES*]

  and cryptographic key sizes [*respectively :*
  - *168*
  - *128, 192*]

  that meet the following: [
  - *Ipsec specifications*].
- **FCS_COP.1.1-3** The TSF shall perform [
  - *ciphering and deciphering of session keys]*

  in accordance with a specified cryptographic algorithm [
  - *RSA]*

  and cryptographic key sizes [
  - *1024]*

  that meet the following: [Nothing].
- **FCS_COP.1.1-4** The TSF shall perform [
  - *integrity verification]*

  in accordance with a specified cryptographic algorithm [
  - *Hmac-MD5 (integrity verification)*
  - *Hmac-SHA1 (integrity verification)*]

  and cryptographic key sizes [*respectively :*
  - *128 bits*
  - *160 bits*]

  that meet the following: [
  - *Ipsec specifications*].
- **FCS_COP.1.1-5** The TSF shall perform [
  - *user authentication (except for M>Tunnel Client)*]

  in accordance with a specified cryptographic algorithm [
  - *RSA]*

  and cryptographic key sizes [
  - *1024]*

  that meet the following: [*Nothing*].
- Dépendances :
  - FCS_CKM.1 Génération de clés cryptographiques (pour « session key generation » qui utilise un algorithme propriétaire)
  - FCS_CKM.2 Distribution des clés cryptographiques (pour « *ciphering and deciphering of session keys")*
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client

5.1.4 Protection des données utilisateur

5.1.4.1 FDP_ACC Politique de contrôle d'accès

FDP_ACC.2 Contrôle d'accès complet

- Hiérarchiquement supérieur à : FDP_ACC.1
- **FDP_ACC.2.1-1**The TSF shall enforce the [*users access control SFP*] on [
  - Subjects : *users*,
  - Objects : *data protection crossing the network*]

  and all operations among subjects and objects covered by the SFP.
- **FDP_ACC.2.1-2** The TSF shall enforce the [*administrators access control SFP*] on [
  - Subjects : *administrators*,
  - Objects : *ciphering and filtering policy*]

  and all operations among subjects and objects covered by the SFP.
- **FDP_ACC.2.2** The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.
- Dépendances : FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client, station d'administration

5.1.4.2 FDP_ACF Fonctions de contrôle d'accès

FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité

- Hiérarchiquement supérieur à : aucun autre composant.
- **FDP_ACF.1.1-1** The TSF shall enforce the [users *access control SF*P] to objects based on [
    - *X509v3 Certificats (O, OU, CN)*].
- **FDP_ACF.1.2-1** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
    - *Certification Authority verification*].
- **FDP_ACF.1.3-1** The TSF shall explicitly access of subjects to objects based on the following additional rules: [*nothing*].
- **FDP_ACF.1.4-1** The TSF shall explicitly deny access of subjects to objects based on the [*CRL (Certificates Revocation List)*].
- **FDP_ACF.1.1-2** The TSF shall enforce the [administrators *access control SF*P] to objects based on [
    - *Role assigned to Login*].
- **FDP_ACF.1.2-2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
    - *authorise an administrator*].
- **FDP_ACF.1.3-2** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*nothing*].
- **FDP_ACF.1.4-2** The TSF shall explicitly deny access of subjects to objects based on the [nothing].
- Dépendances :
    - FDP_ACC.1 Contrôle d'accès partiel
    - FCS_CKM.2 Distribution des clés cryptographiques (pour « *user authentication")*
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client, station d'administration

5.1.4.3 FDP_IFC Politique de contrôle de flux d'informations

FDP_IFC.2 Contrôle de flux d'informations complet

- Hiérarchiquement supérieur à : FDP_IFC.1
- **FDP_IFC.2.1** The TSF shall enforce the [*information flow control SF*P] on [
    - Subject : *protected information*
    - Object : *IP packets*
    - Operation : *to send information from an point of a tunnel to the other*]

  and all operations that cause that information to flow to and from subjects covered by the SFP.
- **FDP_IFC.2.2** The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.
- Dépendances : FDP_IFF.1 Attributs de sécurité simples
- Composants de la TOE concernés : M>Tunnel Gateway, M>Tunnel Client

5.1.4.4 FDP_IFF Fonctions de contrôle de flux d'informations

FDP_IFF.1 Attributs de sécurité simples

- Hiérarchiquement supérieur à : aucun autre composant.
- **FDP_IFF.1.1** The TSF shall enforce the [*information flow control SF*P] based on the following types of subject and information security attributes: [6 minimum as :
    - *source IP address,*
    - *destination IP address,*
    - *protocol,*
    - *source port,*
    - *destination port,*
    - *X509v3 Certificat*].
- **FDP_IFF.1.2** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [
    - *If there is a rule dedicated to this flow defined into ciphering and filtering policy*].
- **FDP_IFF.1.3** The TSF shall enforce the [*Nothing*].
- **FDP_IFF.1.4** The TSF shall provide the following [processing
    - *ciphering of IP packets,*
    - *NAT*].
- **FDP_IFF.1.5** The TSF shall explicitly authorize an information flow based on the following rules: [no further *rules*].
- **FDP_IFF.1.6** The TSF shall explicitly deny an information flow based on the following rules: [
    - *when there is no rules dedicated to this flow defined into ciphering and filtering policy, or*
    - *when there is no VPN tunnel,*
    - *when there is a integrity error*]
- Dépendances :

    - FDP_IFC.1 Contrôle de flux d'informations partiel
    - FCS_COP.1 Operation cryptographique (pour « *ciphering and deciphering of data and integrity verification")*
- Composants de la TOE concernés : M>Tunnel Gateway, M>Tunnel Client

5.1.4.5 FDP_ITT Transfert interne à la TOE

FDP_ITT.1 Protection élémentaire d'un transfert interne

- Hiérarchiquement supérieur à : aucun autre composant.
- **FDP_ITT.1.1** The TSF shall enforce the [*information flow control SFP*] to prevent the [*disclosure and modification*] of user data when it is transmitted between physically-separated parts of the TOE.
- Dépendances : FDP_IFC.1 Contrôle de flux d'informations partiel
- Composants de la TOE concernés : M>Tunnel Gateway, M>Tunnel Client

5.1.4.6 FDP_UCT Protection de la confidentialité des données de l'utilisateur lors d'un transfert inter-TSF

FDP_UCT.1 Confidentialité élémentaire lors d'un échange de données

- Hiérarchiquement supérieur à : aucun autre composant.
- **FDP_UCT.1.1** The TSF shall enforce the [*information flow control SFP*] to be able to [*transmit or receiv*e] objects in a manner protected from unauthorised disclosure.
- Dépendances :
    - FDP_IFC.1 Contrôle de flux d'informations partiel
- Composants de la TOE concernés : M>Tunnel Gateway, M>Tunnel Client

5.1.4.7 FDP_UIT Protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF

FDP_UIT.1 Intégrité lors d'un échange de données

- Hiérarchiquement supérieur à : aucun autre composant.
- **FDP_UIT.1.1** The TSF shall enforce the [*information flow control SFP*] to be able to [*transmit or receiv*e] user data in a manner protected from [*modification, insertion, replay*] errors.
- **FDP_UIT.1.2** The TSF shall be able to determine on receipt of user data, whether [*modificatio*n*, insertion, repla*y] has occurred.
- Dépendances :
    - FDP_IFC.1 Contrôle de flux d'informations partiel
- Composants de la TOE concernés : M>Tunnel Gateway, M>Tunnel Client

5.1.5 Identification et Authentification

5.1.5.1 FIA_AFL Défaillance de l'authentification

FIA_AFL.1 Gestion d'une défaillance de l'authentification

- Hiérarchiquement supérieur à : aucun autre composant.
- **FIA_AFL.1.1** The TSF shall detect when [*n*] unsuccessful authentication attempts occur related to [*administrator authentication*].
- **FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [*close login windows during 2*(n-1) seconds and definitively after 4 unsuccessful following authentication*].
- Dépendances : FIA_UAU.1 Timing de l'authentification
- Composants de la TOE concernés : station d'administration

5.1.5.2 FIA_ATD Définition des attributs d'un utilisateur

FIA_ATD.1 Définition des attributs d'un utilisateur

- Hiérarchiquement supérieur à : aucun autre composant.
- **FIA_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users: [
    - *X509v3 Certificate,*
    - *User private key*].
- Dépendances : pas de dépendances.
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client

5.1.5.3 FIA_UAU Authentification d'un utilisateur

FIA_UAU.2 Authentification d'un utilisateur préalablement à toute action

- Hiérarchiquement supérieur à : FIA_UAU.1
- **FIA_UAU.2.1** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

- Dépendances : FIA_UID.1 Timing de l'identification
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client

FIA_UAU.3 Authentification infalsifiable

- Hiérarchiquement supérieur à : aucun autre composant.
- **FIA_UAU.3.1** The TSF shall [*detect and prevent*] use of authentication data that has been forged by any user of the TSF.
- **FIA_UAU.3.2** The TSF shall [*detect and prevent*] use of authentication data that has been copied from any other user of the TSF.
- Dépendances : pas de dépendances.
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client

FIA_UAU.6 Réauthentification

- Hiérarchiquement supérieur à : aucun autre composant.
- **FIA_UAU.6.1** The TSF shall re-authenticate the user under the conditions [
    - *whenever a session key renegotiation occurs*]
- Dépendances : pas de dépendances.
- Composants de la TOE concernés : M>Tunnel Gateway, M>Tunnel Client

5.1.5.4 FIA_UID Identification d'un utilisateur

FIA_UID.2 Identification d'un utilisateur préalablement à toute action

- Hiérarchiquement supérieur à : FIA_UID.1
- **FIA_UID.2.1** The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
- Dépendances : pas de dépendances.
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client, station d'administration

5.1.6 Gestion de la sécurité

5.1.6.1 FMT_MSA Gestion des attributs de sécurité

FMT_MSA.1 Gestion des attributs de sécurité

- Hiérarchiquement supérieur à : aucun autre composant.
- **FMT_MSA.1.1** The TSF shall enforce the [administrators *access control SFP*] to restrict the ability to [*change_default, query, modify (only with allowed values) or delete*] the security attributes [
    - *ciphering and filtering policy,*
    - *CRL update,*
    - *Configuration information,*
    - *access authorization of M>Tunnel Gateway and software administration*]

  to [*identified administrators*].
- Dépendances :
    - FDP_ACC.1 Contrôle d'accès partiel
    - FMT_SMR.1 Rôles de sécurité
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client

5.1.6.2 FMT_MTD Gestion des données de la TSF

FMT_MTD.1 Gestion des données de la TSF

- Hiérarchiquement supérieur à : aucun autre composant.
- **FMT_MTD.1.1** The TSF shall restrict the ability to [*modify*] the [
    - *configuration information,*
    - *ciphering and filtering policy between Administration Software and all M>Tunnel Gateways,*
    - *CRL updates,*
    - *session key exchange policy (parameters about key negotiation : time, number of packets or number of octets between two negotiations*]

  to [*identified administrators*].
- Dépendances : FMT_SMR.1 Rôles de sécurité
- Composants de la TOE concernés : station d'administration

5.1.6.3 FMT_SMR Rôle pour la gestion de la sécurité

FMT_SMR.1 Rôles de sécurité

- Hiérarchiquement supérieur à : aucun autre composant.
- **FMT_SMR.1.1** The TSF shall maintain the roles [*administrators and users*].
- **FMT_SMR.1.2** The TSF shall be able to associate users with roles.
- Dépendances : FIA_UID.1 Timing de l'identification
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client

5.1.7 Protection des fonctions de sécurité de la TOE

5.1.7.1 FPT_ITT Transfert des données de la TSF à l'intérieur de la TOE

FPT_ITT.1 Protection élémentaire du transfert de données à l'intérieur de la TSF

- Hiérarchiquement supérieur à : aucun autre composant.
- **FPT_ITT.1.1** The TSF shall protect TSF data from [disclosure] when it is transmitted between separate parts of the TOE.
- Dépendances : pas de dépendances.
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client, station d'administration

FPT_ITT.3 Contrôle de l'intégrité des données de la TSF

- Hiérarchiquement supérieur à : aucun autre composant.
- **FPT_ITT.3.1** The TSF shall be able to detect [*modification of data*] for TSF data transmitted between separate parts of the TOE.
- **FPT_ITT.3.2** Upon detection of a data integrity error, the TSF shall take the following actions: [
    - *To write dedicated message into audit records*].
- Dépendances : FPT_ITT.1 Protection élémentaire du transfert de données à l'intérieur de la TSF
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client

5.1.7.2 FPT_RPL Détection de rejeu

FPT_RPL.1 Détection de rejeu

- Hiérarchiquement supérieur à : aucun autre composant.
- **FPT_RPL.1.1** The TSF shall detect replay for the following entities: [
    - *During negotiation step between M>Tunnel Gateway and M>Tunnel Client,*
    - *During negotiation step between two M>Tunnel Gateway,*
    - *During negotiation step between M>Tunnel Master and M>Tunnel Client,*
    - *During negotiation step between M>Tunnel Master and M>Tunnel Gateway].*
- **FPT_RPL.1.2** The TSF shall perform [*to declare negotiation failed*] when replay is detected.
- Dépendances : pas de dépendances.
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client

5.1.7.3 FPT_RVM Passage obligatoire par un moniteur de référence

FPT_RVM.1 Capacité de la TSP à ne pas être court-circuitée

- Hiérarchiquement supérieur à : aucun autre composant.
- **FPT_RVM.1.1** The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
- Dépendances : pas de dépendances.
- Composants de la TOE concernés : M>Tunnel Gateway, M>Tunnel Client

5.1.7.4 FPT_STM Horodatage

FPT_STM.1 Horodatage fiable

- Hiérarchiquement supérieur à : aucun autre composant.
- **FPT_STM.1.1** The TSF shall be able to provide reliable time stamps for its own use.
- Dépendances : pas de dépendances.
- Composants de la TOE concernés : M>Tunnel Master, M>Tunnel Gateway, M>Tunnel Client, station d'administration

5.1.8 Niveau de résistance des exigences de sécurité

Le niveau de résistance des exigences de sécurités spécifiques sont les suivants :

- FCS_COP.1 : la résistance de cette fonction sera démontrée pour les algorithmes cryptographique et les mécanismes de génération d'aléas à l'aide du « dossier de test des algorithmes cryptographiques » et du dossier de test de la génération des nombres aléatoires. Le niveau visé est SOF-high.
- FIA_UAU.2 : la résistance de cette fonction sera démontrée si le temps nécessaire pour deviner l'identifiant de l'utilisateur est supérieur au temps défini par les critères communs. Le niveau visé est SOF-high.
- FIA_UAU.3 : la résistance de cette fonction sera démontrée si le temps nécessaire pour deviner l'identifiant de l'utilisateur est supérieur au temps défini par les critères communs. Le niveau visé est SOF-high.

5.2 Exigences de sécurité fonctionnelles liées à l'environnement

Les exigences spécifiques de sécurité à prendre en compte, liées à l'utilisation, par le M>Tunnel Client, d'un support indépendant muni d'un processeur cryptographique, sont les suivantes :

Classe	Composants
Support Cryptographique	FCS_COP Opération cryptographique

5.2.1 Support Cryptographique

5.2.1.1 FCS_COP Opération cryptographique

FCS_COP.1 Opération cryptographique

- Hiérarchiquement supérieur à : aucun autre composant.
- **FCS_COP.1.1** The TSF shall perform [
  - *session key generation,*
  - *user authentication*]

  in accordance with a specified cryptographic algorithm [
  - *RSA (user authentication)]*

  and cryptographic key sizes [*respectively :*
  - *1024*]

  that meet the following: [
  - *Ipsec specifications*].
- Dépendances :
  - FCS_CKM.1 Génération de clés cryptographiques (uniquement pour « session key generation »)
- Composants de la TOE concernés : M>Tunnel Client

5.3 Exigences de sécurité d'assurance

Les exigences à prendre en compte pour EAL2 augmenté de ADV_HLD.2, ADV_LLD.1 et AVA_VLA.2 sont les suivantes :

Classe d'assurance	Composants d'assurance
Gestion de configuration	ACM_CAP.2 Éléments de configuration
Livraison et exploitation	ADO_DEL.1 Procédures de livraison
	ADO_IGS.1 Procédures d'installation, de génération et de démarrage
Développement	ADV_FSP.1 Spécifications fonctionnelles informelles
	ADV_HLD.2 Conception de haut niveau – identification des sous-sytèmes dédiés à la sécurité
	ADV_LLD.1 Conception de bas niveau descriptive
	ADV_RCR.1 Démonstration de correspondance informelle
Guides	AGD_ADM.1 Guide de l'administrateur
	AGD_USR.1 Guide de l'utilisateur
Tests	ATE_COV.1 Éléments de preuve de la couverture
	ATE_FUN.1 Tests fonctionnels
	ATE_IND.2 Tests indépendants – par échantillonnage
Estimation des vulnérabilité	AVA_SOF.1 Évaluation de la résistance des fonctions de sécurité de la TOE
	AVA_VLA.2 Analyse de vulnérabilités indépendante

5.3.1 Gestion de configuration (ACM)

5.3.1.1 ACM_CAP.2 Éléments de configuration

Objectifs :

Une référence unique est exigée pour garantir qu'il n'y a pas d'ambiguïté sur l'exemplaire de la TOE qui fait l'objet de l'évaluation. L'identification de la TOE par ses références garantit que les utilisateurs de la TOE peuvent être à même de savoir quel exemplaire de la TOE ils utilisent. L'identification unique des éléments de configuration conduit à une

perception plus claire de la composition de la TOE, ce qui, à son tour, aide à déterminer les éléments qui font l'objet des exigences d'évaluation pour la TOE.

Tâches du développeur :

- **ACM_CAP.2.1D** Le développeur doit fournir une référence pour la TOE.
- **ACM_CAP.2.2D** Le développeur doit utiliser un système de CM.
- **ACM_CAP.2.3D** Le développeur doit fournir une documentation de CM.

Contenu et présentation des éléments de preuve :

- **ACM_CAP.2.1C** La référence de la TOE doit être unique pour chaque version de la TOE.
- **ACM_CAP.2.2C** La TOE doit être identifiée par sa référence.
- **ACM_CAP.2.3C** La documentation de CM doit inclure une liste de configuration.
- **ACM_CAP.2.4C** La liste de configuration doit décrire les éléments de configuration qui constituent la TOE.
- **ACM_CAP.2.5C** La documentation CM doit décrire la méthode utilisée pour identifier de façon unique les éléments de configuration.
- **ACM_CAP.2.6C** Le système de CM doit identifier de façon unique tous les éléments de configuration.

Tâches de l'évaluateur :

- **ACM_CAP.2.1^{E}** L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

5.3.2 Livraison et exploitation (ADO)

5.3.2.1 ADO_DEL.1 Procédures de livraison

Objectifs :

Les exigences pour la livraison demandent un contrôle du système ainsi que des réseaux et procédures de distribution qui procurent l'assurance que le destinataire reçoit la TOE que l'expéditeur a voulu envoyer, sans aucune modification. Pour que la livraison soit valide, ce qui est reçu doit correspondre précisément à l'exemplaire original de la TOE, évitant ainsi toute altération de la version reçue ou toute substitution par une version falsifiée.

Tâches du développeur :

- **ADO_DEL.1.1D** Le développeur doit documenter les procédures de livraison à l'utilisateur de la TOE ou de parties de celle-ci.
- **ADO_DEL.1.2D** Le développeur doit utiliser les procédures de livraison.

Contenu et présentation des éléments de preuve :

- **ADO_DEL.1.1C** La documentation de livraison doit décrire toutes les procédures qui sont nécessaires pour maintenir la sécurité lors de la distribution de versions de la TOE vers le site d'un utilisateur.

Tâches de l'évaluateur :

- **ADO_DEL.1.1^{E}** L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences pour le contenu et la présentation des éléments de preuve.

5.3.2.2 ADO_IGS.1 Procédures d'installation, de génération et de démarrage

Objectifs :

Les procédures d'installation, de génération et de démarrage sont utiles pour garantir que la TOE a été installée, générée et démarrée d'une façon sûre, comme prévu par le développeur. Les exigences relatives à l'installation, la génération et le démarrage font appel à une transition sûre entre la représentation de l'implémentation de la TOE sous contrôle de configuration et son exploitation initiale dans l'environnement de l'utilisateur.

Tâches du développeur :

- **ADO_IGS.1.1D** Le développeur doit documenter les procédures nécessaires à une installation, une génération et un démarrage sûrs de la TOE.

Contenu et présentation des éléments de preuve :

- **ADO_IGS.1.1C** La documentation doit décrire les étapes nécessaires à une installation, une génération et un démarrage sûrs de la TOE.

Tâches de l'évaluateur :

- **ADO_IGS.1.1^{E}** L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences pour le contenu et la présentation des éléments de preuve.
- **ADO_IGS.1.2^{E}** L'évaluateur doit déterminer que les procédures d'installation, de génération et de démarrage conduisent à une configuration sûre.

5.3.3 Développement (ADV)

5.3.3.1 ADV_FSP.1 Spécifications fonctionnelles

Objectifs :

Les spécifications fonctionnelles représentent une description de haut niveau de l'interface visible par l'utilisateur et du comportement de la TSF. Il s'agit d'une instantiation des exigences de sécurité fonctionnelles de la TOE. Les spécifications fonctionnelles doivent montrer que toutes les exigences de sécurité fonctionnelles sont traitées.

Tâches du développeur :

- **ADV_FSP.1.1D** Le développeur doit fournir des spécifications fonctionnelles.

Contenu et présentation des éléments de preuve :

- **ADV_FSP.1.1C** Les spécifications fonctionnelles doivent décrire la TSF et ses interfaces externes dans un style informel.
- **ADV_FSP.1.2C** Les spécifications fonctionnelles doivent avoir une cohérence interne.
- **ADV_FSP.1.3C** Les spécifications fonctionnelles doivent décrire le but et le mode d'emploi de toutes les interfaces externes de la TSF, en fournissant lorsque cela est approprié les détails sur les effets, les exceptions et les messages d'erreur.
- **ADV_FSP.1.4C** Les spécifications fonctionnelles doivent représenter complètement la TSF.

Tâches de l'évaluateur :

- **ADV_FSP.1.1**^{E} L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.
- **ADV_FSP.1.2**^{E} L'évaluateur doit déterminer que les spécifications fonctionnelles constituent une instantiation correcte et complète des exigences fonctionnelles de sécurité de la TOE.

5.3.3.2 ADV_HLD.2 Conception de haut niveau – identification des sous-sytèmes dédiés à la sécurité

Objectifs :

La conception de haut niveau d'une TOE apporte une description de la TSF en termes d'éléments structurels principaux (i.e. sous-systèmes) et relie ces éléments aux fonctions qu'ils remplissent. Les exigences relatives à la conception de haut niveau sont censées apporter l'assurance que la TOE fournit une architecture appropriée pour implémenter les exigences de sécurité fonctionnelles de la TOE.

La conception de haut niveau est un raffinement des spécifications fonctionnelles en sous-systèmes. Pour chaque sous-système de la TSF, la conception de haut niveau décrit sa finalité et sa fonction, et identifie les fonctions de sécurité contenues dans le sous-système. Les relations mutuelles entre tous les sous-systèmes sont également définies dans la conception de haut niveau. Ces relations mutuelles seront représentées comme interfaces externes pour les flux de données, flux de contrôle, etc., lorsque cela est approprié.

Tâches du développeur :

- **ADV_HLD.2.1D** Le développeur doit fournir la conception de haut niveau de la TSF.

Contenu et présentation des éléments de preuve :

- **ADV_HLD.2.1C** La présentation de la conception de haut niveau doit être en style informel.
- **ADV_HLD.2.2C** La conception de haut niveau doit avoir une cohérence interne.
- **ADV_HLD.2.3C** La conception de haut niveau doit décrire la structure de la TSF en termes de sous-systèmes.
- **ADV_HLD.2.4C** La conception de haut niveau doit décrire les fonctionnalités de sécurité fournies par chaque sous-système de la TSF.
- **ADV_HLD.2.5C** La conception de haut niveau doit identifier tout matériel, micro-programme ou logiciel sous-jacent exigé par la TSF, et présenter les fonctions fournies par le mécanisme de protection de soutien implémenté dans ce matériel, micro-programme ou logiciel.
- **ADV_HLD.2.6**C La conception de haut niveau doit identifier toutes les interfaces des sous-systèmes de la TSF.
- **ADV_HLD.2.7C** La conception de haut niveau doit identifier les interfaces des sous-systèmes de la TSF qui sont visibles de l'extérieur.
- **ADV_HLD.2.8C** La conception de haut niveau doit décrire le but et le mode d'emploi de toutes les interfaces des sous-systèmes de la TSF, en fournissant, lorsque cela est approprié, les détails sur les effets, les exceptions et les messages d'erreur.
- **ADV_HLD.2.9C** La conception de haut niveau doit décrire la séparation de la TOE entre les sous-systèmes dédiés à la mise en oeuvre de la TSP et les autres sous-systèmes.

Tâches de l'évaluateur :

- **ADV_HLD.2.1**^{E} L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.
- **ADV_HLD.2.2**^{E} L'évaluateur doit déterminer que la conception de haut niveau est une instantiation correcte et complète des exigences fonctionnelles de sécurité de la TOE.

5.3.3.3 ADV_LLD.1 Conception de bas niveau descriptive

Objectifs :

La conception de bas niveau d'une TOE fournit une description du fonctionnement interne de la TSF sous forme de modules, ainsi que de leurs relations et de leurs dépendances mutuelles. La conception de bas niveau procure l'assurance que les sous-systèmes de la TSF ont été raffinés de façon correcte et efficace. Pour chaque module de la TSF, la conception de bas niveau décrit son but, sa fonction, ses interfaces, ses dépendances et l'implémentation de toutes les fonctions dédiées à la mise en oeuvre de la TSP.

Tâches du développeur :

- **ADV_LLD.1.1D** Le développeur doit fournir la conception de bas niveau de la TSF.

Contenu et présentation des éléments de preuve :

- **ADV_LLD.1.1C** La présentation de la conception de bas niveau doit être en style informel.
- **ADV_LLD.1.2C** La conception de bas niveau doit avoir une cohérence interne.
- **ADV_LLD.1.3C** La conception de bas niveau doit décrire la TSF en termes de modules.
- **ADV_LLD.1.4C** La conception de bas niveau doit décrire le but de chaque module.
- **ADV_LLD.1.5C** La conception de bas niveau doit définir les relations mutuelles entre les modules en termes de fonctionnalités de sécurité fournies et de dépendances vis-à-vis des autres modules.
- **ADV_LLD.1.6C** La conception de bas niveau doit décrire comment chaque fonction dédiée à la mise en oeuvre de la TSP est fournie.
- **ADV_LLD.1.7C** La conception de bas niveau doit identifier toutes les interfaces des modules de la TSF.
- **ADV_LLD.1.8C** La conception de bas niveau doit identifier les interfaces des modules de la TSF qui sont visibles de l'extérieur.
- **ADV_LLD.1.9C** La conception de bas niveau doit décrire le but et le mode d'utilisation de toutes les interfaces des modules de la TSF, en fournissant, lorsque cela est approprié, les détails sur les effets, les exceptions et les messages d'erreur.
- **ADV_LLD.1.10C** La conception de bas niveau doit décrire la séparation de la TOE en modules dédiés à la mise en oeuvre de la TSP et en autres modules.

Tâches de l'évaluateur :

- **ADV_LLD.1.1^{E}** L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.
- **ADV_LLD.1.2^{E}** L'évaluateur doit déterminer que la conception de bas niveau est une instantiation correcte et complète des exigences fonctionnelles de sécurité de la TOE.

Raffinement :

Le composant d'assurance ADV_LLD.1 ne s'applique qu'aux sous-systèmes de la TOE réalisant les exigences fonctionnelles de la classe FCS.

5.3.3.4 ADV_RCR.1 Correspondance des représentations

Objectifs :

La correspondance entre les différentes représentations de la TSF (i.e. spécifications globales de la TOE, spécifications fonctionnelles, conception de haut niveau, conception de bas niveau, représentation de l'implémentation) concerne l'instantiation correcte et complète des exigences jusqu'au niveau le moins abstrait de représentation de la TSF fourni. Ce résultat est obtenu grâce au raffinement par étapes et par les résultats cumulés des déterminations de correspondance entre les représentations de niveaux d'abstraction adjacents.

Tâches du développeur :

- **ADV_RCR.1.1D** Le développeur doit fournir une analyse de correspondance entre toutes les paires de représentations de la TSF adjacentes fournies.

Contenu et présentation des éléments de preuve :

- **ADV_RCR.1.1C** Pour chaque paire de représentations de la TSF adjacentes fournies, l'analyse doit démontrer que toutes les fonctionnalités de sécurité pertinentes de la représentation de la TSF la plus abstraite sont correctement et complètement raffinées dans la représentation de la TSF la moins abstraite.

Tâches de l'évaluateur :

- **ADV_RCR.1.1^{E}** L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

5.3.4 Guides (AGD)

5.3.4.1 AGD_ADM.1 Guide de l'administrateur

Objectifs :

Le guide de l'administrateur est l'ensemble des documents prévus pour être utilisés par les personnes chargées d'effectuer de façon correcte la configuration, la maintenance et l'administration de la TOE, afin d'obtenir une sécurité maximum. L'exploitation sûre de la TOE dépendant du fonctionnement correct de la TSF, les personnes chargées d'exécuter les opérations précédentes sont considérées comme étant de confiance par la TSF. Le guide de l'administrateur est prévu pour aider les administrateurs à comprendre les fonctions de sécurité fournies par la TOE, incluant à la fois les fonctions qui obligent l'administrateur à effectuer des tâches critiques pour la sécurité et les fonctions qui fournissent des informations critiques pour la sécurité.

Tâches du développeur :

- **AGD_ADM.1.1D** Le développeur doit fournir un guide de l'administrateur à l'attention du personnel chargé de l'administration du système.

Contenu et présentation des éléments de preuve :

- **AGD_ADM.1.1C** Le guide de l'administrateur doit décrire les fonctions et les interfaces d'administration à la disposition de l'administrateur de la TOE.

- **AGD_ADM.1.2C** Le guide de l'administrateur doit décrire comment administrer la TOE d'une façon sûre.
- **AGD_ADM.1.3C** Le guide de l'administrateur doit contenir des avertissements concernant les fonctions et les privilèges qui devraient être contrôlés dans un environnement d'exploitation sûr.
- **AGD_ADM.1.4C** Le guide de l'administrateur doit décrire toutes les hypothèses relatives au comportement de l'utilisateur, qui ont un rapport avec l'exploitation sûre de la TOE.
- **AGD_ADM.1.5C** Le guide de l'administrateur doit décrire tous les paramètres de sécurité qui sont sous le contrôle de l'administrateur, en indiquant les valeurs sûres quand cela est approprié.
- **AGD_ADM.1.6C** Le guide de l'administrateur doit décrire chaque type d'événement touchant à la sécurité, relatif aux fonctions d'administration qui doivent être réalisées, y compris le changement des caractéristiques de sécurité d'entités qui sont sous le contrôle de la TSF.
- **AGD_ADM.1.7C** Le guide de l'administrateur doit être cohérent avec tous les autres documents fournis pour l'évaluation.
- **AGD_ADM.1.8C** Le guide de l'administrateur doit décrire toutes les exigences de sécurité pour l'environnement TI, qui concernent l'administrateur.

Tâches de l'évaluateur :

- **AGD_ADM.1.1^{E}** L'évaluateur doit confirmer que les informations foumies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

5.3.4.2 AGD_USR.1 Guide de l'utilisateur

Objectifs :

Le guide de l'utilisateur fait référence à des éléments prévus pour être utilisés par des utilisateurs humains de la TOE ne remplissant pas de fonctions d'administration et par d'autres utilisateurs (e.g. des programmeurs) qui utilisent les interfaces externes de la TOE. Le guide de l'utilisateur décrit les fonctions de sécurité fournies par la TSF et offre des instructions et des directives, comprenant des avertissements, pour l'utilisation sûre de la TSF.
Le guide de l'utilisateur donne une base pour former des hypothèses quant à l'utilisation de la TOE et une mesure de la confiance dans le fait que des utilisateurs, des fournisseurs d'applications et d'autres entités faisant appel aux interfaces externes de la TOE, comprendront ce qu'est l'exploitation sûre de la TOE et l'utiliseront comme cela est prévu.

Tâches du développeur :

- **AGD_USR.1.1D** Le développeur doit fournir un guide de l'utilisateur.

Contenu et présentation des éléments de preuve :

- **AGD_USR.1.1C** Le guide de l'utilisateur doit décrire les fonctions et les interfaces disponibles aux utilisateurs ne remplissant pas des fonctions d'administrateurs de la TOE.
- **AGD_USR.1.2C** Le guide de l'utilisateur doit décrire l'utilisation des fonctions de sécurité fournies par la TOE accessibles aux utilisateurs.
- **AGD_USR.1.3C** Le guide de l'utilisateur doit contenir des avertissements concernant les fonctions et les privilèges accessibles aux utilisateurs qui devraient être contrôlés dans un environnement d'exploitation sûr.
- **AGD_USR.1.4C** Le guide de l'utilisateur doit présenter clairement toutes les responsabilités qui incombent à l'utilisateur dont l'exercice est nécessaire pour une exploitation sûre de la TOE, y compris celles liées aux hypothèses relatives au comportement de l'utilisateur figurant dans l'énoncé de l'environnement de sécurité de la TOE.
- **AGD_USR.1.5C** Le guide de l'utilisateur doit être cohérent avec toute autre documentation fournie pour l'évaluation.
- **AGD_USR.1.6C** Le guide de l'utilisateur doit décrire toutes les exigences de sécurité pour l'environnement TI, qui concernent l'utilisateur.

Tâches de l'évaluateur :

- **AGD_USR.1.1^{E}** L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

5.3.5 Tests (ATE)

5.3.5.1 ATE_COV.1 Éléments de preuve de la couverture

Objectifs :

Dans ce composant, l'objectif est d'établir que la TSF a été testée par rapport à ses spécifications fonctionnelles. Cela doit être accompli au moyen d'un examen des éléments de preuve de correspondance du développeur.

Tâches du développeur :

- **ATE_COV.1.1D** Le développeur doit fournir les éléments de preuve de la couverture des tests.

Contenu et présentation des éléments de preuve :

- **ATE_COV.1.1C** Les éléments de preuve de la couverture des tests doivent montrer la correspondance entre les tests identifiés dans la documentation de test et la TSF, telle qu'elle est décrite dans les spécifications fonctionnelles.

Tâches de l'évaluateur :

- **ATE_COV.1.1^{E}** L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

5.3.5.2 ATE_FUN.1 Tests fonctionnels

Objectifs :

L'objectif pour le développeur est de démontrer que toutes les fonctions de sécurité fonctionnent conformément à leurs spécifications. Le développeur doit exécuter les tests et fournir la documentation de test.

Tâches du développeur :

- **ATE_FUN.1.1D** Le développeur doit tester la TSF et documenter les résultats.
- **ATE_FUN.1.2D** Le développeur doit fournir la documentation de test.

Contenu et présentation des éléments de preuve :

- **ATE_FUN.1.1C** La documentation de test doit être constituée par les plans de test, les descriptions de procédures de test, les résultats de tests attendus et les résultats de tests réellement obtenus.
- **ATE_FUN.1.2C** Les plans de test doivent identifier les fonctions de sécurité à tester et décrire le but des tests à exécuter.
- **ATE_FUN.1.3C** Les descriptions des procédures de test doivent identifier les tests à exécuter et décrire les scenarii de test de chaque fonction de sécurité. Ces scénario doivent inclure tous les ordonnancements relatifs aux résultats des autres tests.
- **ATE_FUN.1.4C** Les résultats de tests attendus doivent montrer les résultats prévus à la suite d'une exécution réussie des tests.
- **ATE_FUN.1.5C** Les résultats de tests provenant de l'exécution des tests par le développeur doivent démontrer que chaque fonction de sécurité testée s'est comportée conformément à ses spécifications.

Tâches de l'évaluateur :

- **ATE_FUN.1.1^{E}** L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

5.3.5.3 ATE_IND.2 Tests indépendants – par échantillonnage

Objectifs :

L'objectif est de démontrer que les fonctions de sécurité fonctionnent conformément à leurs spécifications. Les tests de l'évaluateur comprennent la sélection et la réexécution d'un échantillon des tests du développeur.

Tâches du développeur :

- **ATE_IND.2.1D** Le développeur doit fournir la TOE afin d'exécuter les tests.

Contenu et présentation des éléments de preuve :

- **ATE_IND.2.1C** La TOE doit se prêter à l'exécution de tests.
- **ATE_IND.2.2C** Le développeur doit fournir un ensemble de ressources équivalent à celui qui a été utilisé pour les tests fonctionnels de la TSF qu'il a effectués.

Tâches de l'évaluateur :

- **ATE_IND.2.1^{E}** L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.
- **ATE_IND.2.2^{E}** L'évaluateur doit tester un sous-ensemble de la TSF quand cela est approprié pour confirmer que la TOE fonctionne conformément à ses spécifications.
- **ATE_IND.2.3^{E}** L'évaluateur doit exécuter un échantillon de tests choisi dans la documentation de test afin de contrôler les résultats des tests du développeur.

5.3.6 Estimation des vulnérabilités (AVA)

5.3.6.1 AVA_SOF.1 Résistance des fonctions de sécurité de la TOE

Objectifs :

Même si une fonction de sécurité de la TOE ne peut pas être court-circuitée, désactivée ou altérée, il est encore possible de la mettre en échec parce qu'une vulnérabilité s'est introduite dans le concept de ses mécanismes de sécurité sous-jacents. Pour ces fonctions, une qualification de leur comportement de sécurité peut être faite en utilisant les résultats d'une analyse quantitative ou statistique du comportement de sécurité de tels mécanismes et de l'effort requis pour les mettre en échec. Cette qualification se fait sous la forme d'une annonce de la résistance des fonctions de sécurité de la TOE.

Tâches du développeur :

- **AVA_SOF.1.1D** Le développeur doit effectuer une analyse de la résistance des fonctions de sécurité de la TOE pour chaque mécanisme identifié dans la ST comme faisant l'objet d'une annonce de résistance des fonctions de sécurité de la TOE.

Contenu et présentation des éléments de preuve :

- **AVA_SOF.1.1C** Pour chaque mécanisme faisant l'objet d'une annonce de résistance des fonctions de sécurité de la TOE, l'analyse de la résistance des fonctions de sécurité de la TOE doit montrer qu'elle atteint ou dépasse le niveau de résistance minimum défini dans le PP ou la ST.

- **AVA_SOF.1.2C** Pour chaque mécanisme faisant l'objet d'une annonce spécifique de résistance des fonctions de sécurité de la TOE, l'analyse de la résistance des fonctions de sécurité de la TOE doit montrer qu'elle atteint ou dépasse la métrique spécifique de la résistance des fonctions définie dans le PP ou la ST.

Tâches de l'évaluateur :

- **AVA_SOF.1.1**[E] L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.
- **AVA_SOF.1.2**[E] L'évaluateur doit confirmer que les annonces de la résistance sont correctes.

5.3.6.2 AVA_VLA.2 Analyse de vulnérabilités indépendante

Objectifs :

Une analyse de vulnérabilités est effectuée par le développeur pour vérifier la présence de vulnérabilités de sécurité et pour confirmer qu'elles ne peuvent pas être exploitées dans l'environnement prévu pour la TOE.
L'évaluateur effectue des tests de pénétration indépendants, en s'appuyant sur une analyse de vulnérabilités indépendante, afin de déterminer si la TOE est résistante aux attaques de pénétration effectuées par des attaquants ayant un potentiel d'attaque élémentaire.

Tâches du développeur :

- **AVA_VLA.2.1D** Le développeur doit effectuer et documenter une analyse des fournitures de la TOE pour rechercher les **moyens** par lesquels un utilisateur peut violer la TSP.
- **AVA_VLA.2.2D** Le développeur doit documenter les caractéristiques des vulnérabilités identifiées.

Contenu et présentation des éléments de preuve :

- **AVA_VLA.2.1C** La documentation doit montrer, pour toutes les vulnérabilités identifiées, que la vulnérabilité ne peut pas être exploitée dans l'environnement prévu pour la TOE.
- **AVA_VLA.2.2C** La documentation doit justifier que la TOE, compte tenu des vulnérabilités identifiées, est résistante aux attaques de pénétration évidentes.

Tâches de l'évaluateur :

- **AVA_VLA.2.1**[E] L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.
- **AVA_VLA.2.2**[E] L'évaluateur doit effectuer des tests de pénétration, en s'appuyant sur l'analyse de vulnérabilités du développeur, pour garantir que les vulnérabilités identifiées ont été prises en compte.
- **AVA_VLA.2.3**[E] L'évaluateur doit effectuer une analyse de vulnérabilités indépendante.
- **AVA_VLA.2.4**[E] L'évaluateur doit effectuer des tests de pénétration indépendants, basés sur une analyse de vulnérabilités indépendante, afin de déterminer le caractère exploitable des vulnérabilités supplémentaires identifiées dans l'environnement prévu.
- **AVA_VLA.2.5**[E] L'évaluateur doit déterminer si la TOE est résistante aux attaques de pénétration effectuées par un attaquant ayant un potentiel d'attaque élémentaire.

5.3.7 Etude des dépendances et de la complémentarité des exigences d'assurances

Toutes les dépendances, entre les exigences de sécurité retenues pour la TOE, définies par les « Critères Communs » ont été respectées à l'exception de celles correspondant aux exigences suivantes :

- ADV_LLD.1 : Cette dépendance est, normalement, prévue par l'exigence d'assurance AVA_VLA.2 qui traite de l'analyse de la vulnérabilité. Il a été choisi d'ajouter AVA_VLA.2 à la certification pour augmenter l'analyse de vulnérabilité pour la partie cryptographique. Par conséquent, elle ne nécessite pas ADV_LLD.1 sur l'ensemble des fonctions mais uniquement pour les fonctions cryptographiques.

- ADV_IMP.1 : Cette dépendance est, normalement, prévue par l'exigence d'assurance AVA_VLA.2 qui traite de l'analyse de la vulnérabilité. Il a été choisi d'ajouter AVA_VLA.2 à la certification pour augmenter l'analyse de vulnérabilité pour la partie cryptographique mais en se limitant à la conception détaillée de ces fonctions. Par conséquent, elle ne nécessite pas ADV_IMP.1.

6. Spécifications globales de la TOE

6.1 Fonctions de sécurité

6.1.1 Introduction

L'objet de ce paragraphe est de présenter les fonctions de sécurité (SEF) qui sont intégrées dans la TOE. Les différentes familles de fonctions sont :

- Audit (**AU**) :*Cette famille regroupe toutes les fonctions liées à l'audit.*
- Cryptographie (**CR**) :*Cette famille regroupe toutes les fonctions liées aux clés de session.*
- Protection et filtrage (**PR**) :*Cette famille regroupe toutes les fonctions liées à la protection des données des utilisateurs.*
- Identification et Authentification (**IA**) :*Cette famille regroupe toutes les fonctions liées à l'identification et à l'authentification des utilisateurs et des administrateurs.*
- Gestion de la sécurité (**GS**) :*Cette famille regroupe toutes les fonctions liées à la gestion des politiques de sécurité.*

6.1.2 Audit

6.1.2.1 AU_1

Les fonctions de sécurité doivent générer des messages d'audit, lisibles et interprétables par les administrateurs, au moins pour les évènements suivants :

- Pour l'ensemble des équipements de la TOE :
  - erreur de fonctionnement
  - tentative d'attaque
- Pour les équipements M>Tunnel Gateway et M>Tunnel Clients de la TOE :
  - rejet d'un paquet
  - renégociation des clés
- Pour l'équipement M>Tunnel Client de la TOE :
  - authentification d'un utilisateur
- Pour les équipements M>Tunnel Master et logiciel d'administration de la TOE :
  - Changement de configuration
  - Changement de CRL
- Pour les équipements M>Tunnel Gateway et logiciel d'administration de la TOE :
  - Changement de politique de chiffrement ou de filtrage

6.1.2.2 AU_2

Le fichier de log doit contenir au moins les informations suivantes pour les évènements définis en AU-1 :

- type d'évènement
- date et heure de l'événement (les évènements doivent datés avec précision)
- l'adresse IP source (si applicable)
- l'adresse IP destination (si applicable)
- réussite ou échec de l'évènement
- l'identifiant de l'utilisateur (si applicable)

6.1.2.3 AU_3

Les M>Tunnel Gateway, Master et le logiciel d'administration, doivent être capable de gérer les fichiers d'évènements :

- les protéger face à une destruction ou une modification non autorisée (seuls les administrateurs ont le droit de modifier ou détruire ces fichiers)
- ne pas les endommager quand il n'y a plus de place sur le disque
- N'autoriser leur lecture que par les administrateurs (seuls eux peuvent se connecter à ces équipements)
- Effectuer un filtrage à la lecture des messages d'audit

6.1.3 Cryptographie

6.1.3.1 CR_1

Une des deux extrémités d'un tunnel (M>Tunnel Gateway ou M>Tunnel Client) doit être capable de générer de façon sécurisée et indépendante une clé de session dont la taille dépend de l'algorithme choisi.

6.1.3.2 CR_2

Une des deux extrémités d'un tunnel (M>Tunnel Master, M>Tunnel Gateway ou M>Tunnel Client) doit être capable d'enclencher une phase de négociation de clé de session avec l'autre extrémité. Les principales étapes de cette phase de négociation sont :

- génération d'une clé de session
- envoi de la clé et d'aléas, qui ont servi lors de la phase d'authentification, chiffrés par la clé publique de l'extrémité émettrice
- vérification des aléas par l'extrémité réceptrice et stockage de la clé
- renvoi des aléas, qui ont servi lors de la phase d'authentification, chiffrés par la clé publique de l'extrémité émettrice
- vérification des aléas par l'extrémité réceptrice

Si la connexion est coupée lors de la phase de négociation, cette dernière est abandonnée et est considérée comme échouée.

6.1.3.3 CR_3

Une des deux extrémités (M>Tunnel Gateway ou M>Tunnel Client) d'un tunnel doit être capable d'enclencher une phase de renégociation de clé de session avec l'autre dès qu'un des critères suivants a été atteint :

- la clé n'a pas été changée depuis x secondes
- depuis le dernier changement de clé, n paquets ont été émis
- depuis le dernier changement de clé, p octets ont été émis

Les paramètres (x, n, p) doivent être programmables par la station d'administration.

Lors de cette phase, une authentification est effectuée (présence de l'identifiant de l'utilisateur sur sa carte à puce)

Si cette phase de renégociation des clés échoue, le tunnel doit être automatiquement coupé.

6.1.3.4 CR_4

Une fois que la clé de session a été initialisée ou modifiée, chaque extrémité du tunnel (M>Tunnel Gateway ou M>Tunnel Client) doit l'appliquer pour l'intégrité, le chiffrement et le déchiffrement des paquets.

6.1.3.5 CR_5

Les algorithmes cryptographiques suivants peuvent être configurés :

- clé de session :
  - Triple DES
  - AES
  - rien
- authentification des utilisateurs :
  - RSA 1024
- authentification des paquets :

- Hmac-MD5
- Hmac-SHA1
- rien

- chiffrement des paquets :
  - celui choisi pour la clé de session
  - rien

6.1.4 Protection et filtrage

6.1.4.1 PR_1

Tout paquet émis, par un M>Tunnel Gateway ou par un M>Tunnel Client, doit appliquer les politiques de chiffrement et de filtrage le concernant :

- Application d'une politique, rejet ou émission sans modification
- mode tunnel ou mode transport
- authentification ou non (intégrité, rejeu)
- chiffrement ou non (confidentialité)
- translation d'adresse source (NAT)

Un paquet IP est caractérisé par les informations suivantes :
- Adresse IP source,
- Adresse IP destination,
- Protocole,
- Port Source,
- Port Destination
- Certificat X509v3

6.1.4.2 PR_2

Tout paquet reçu, par un M>Tunnel Gateway ou par un M>Tunnel Client, doit appliquer les politiques de chiffrement et de filtrage le concernant :

- Application d'une politique, rejet ou réception sans modification
- mode tunnel ou mode transport
- authentification ou non (intégrité, rejeu)
- chiffrement ou non (confidentialité)
- translation d'adresse destination (NAT)

Un paquet IP est caractérisé par les informations suivantes :
- Adresse IP source,
- Adresse IP destination,
- Protocole,
- Port Source,
- Port Destination
- Certificat X509v3

6.1.4.3 PR_3

Quand le tunnel n'est pas démarré, aucun paquet IP ne peut sortir des équipements M>Tunnel Client et M>Tunnel Gateway.

6.1.4.4 PR_4

Dès la mise sous tension de la station d'administration, le M>Tunnel Client associé crée des tunnels permanents entre elle et toutes les M>Tunnel Gateway.

6.1.4.5 PR_5

Les fichiers de politique de chiffrement, de filtrage , CRL et de configuration doivent être stockés et utilisées, sur les équipements.

6.1.5 Identification et Authentification

6.1.5.1 **IA_1**

Chaque extrémité de tunnel (M>Tunnel Master, M>Tunnel Gateway ou M>Tunnel Client) doit posséder un identifiant contenant les informations suivantes :

- Un certificat X509.
- La clé privée RSA 1024 associée.

Lors de l'installation du logiciel M>Tunnel, le certificat de l'autorité de certification est fourni.

6.1.5.2 **IA_2**

Une des deux extrémités d'un tunnel (M>Tunnel Gateway ou M>Tunnel Client) doit être capable d'enclencher une phase d'authentification avec l'autre extrémité (M>Tunnel Master, M>Tunnel Gateway ou M>Tunnel Client) afin de s'assurer de l'appartenance des extrémités à la même autorité de certification.

Si la connexion est coupée lors de la phase d'authentification, cette dernière est abandonnée et est considérée comme échouée

6.1.5.3 **IA_3**

Seule l'introduction, dans le M>Tunnel Client, d'un support contenant l'identifiant de l'utilisateur et la mise en œuvre des mécanismes permettant d'y accéder entraîne la mise en œuvre du ou des tunnels de ce dernier.

6.1.5.4 **IA_5**

Un administrateur qui se connecte sur la station d'administration doit fournir un login et un mot de passe. Une erreur lors de la phase d'authentification doit déconnecter automatiquement l'administrateur. Après n erreurs consécutives, l'écran de login est verrouillé pendant 2*n secondes et si n devient supérieur à 4, le login est définitivement bloqué (il devra être débloqué par action sur la gateway).

6.1.5.5 **IA_6**

Pour qu'une authentification soit considérée comme valable, il faut que cette phase se soit déroulée sans problème et que ni le certificat de l'utilisateur du M>Tunnel Client ni le certificat des M>Tunnel Gateway (en cas de tunnels entre 2 de ces équipements) n'appartienne à la CRL

6.1.6 **Gestion de la sécurité**

6.1.6.1 **GS_1**

La mise en œuvre d'un tunnel (soit entre 2 M>Tunnel Gateway ou entre un M>Tunnel Gateway et un M>Tunnel Client) doit se faire selon le procédé suivant :

- cas d'un tunnel entre 2 M>Tunnel Gateway :
    - Authentification entre les deux M>Tunnel Gateway
    - Vérification de la cohérence des politiques de chiffrement stockées sur les 2 M>Tunnels Gateway
- cas d'un tunnel initialisé par un M>Tunnel Client :
    - Authentification du M>Tunnel Client vis à vis d'un M>Tunnel Master
    - Téléchargement sécurisé automatique de la liste des M>Tunnel Gateway avec lequel le M>Tunnel Client doit établir un tunnel
    - avec chacun de ces M>Tunnel Gateway :
        - Authentification du M>Tunnel Client vis à vis de ce M>Tunnel Gateway
        - Téléchargement sécurisé automatique de la politique de chiffrement du client
        - Négociation des clés de session

6.1.6.2 **GS_2**

L'initialisation de chaque M>Tunnel Gateway et du M>Tunnel Master se fait par l'administrateur en se connectant sur chaque équipement.

6.1.6.3 **GS_3**

La mise à jour de la CRL se fait, pour le M>Tunnel Master, par action de l'administrateur à partir du logiciel d'administration

6.1.6.4 **GS_4**

Les politiques de chiffrement et de filtrage, la configuration et les paramètres d'échange de clé doivent être définies à l'aide du logiciel d'administration, envoyées à l'ensemble des M>Tunnel Master et Gateway et stockées sur les équipements. Le logiciel d'administration doit vérifier la cohérence des informations qui ont été fournies par l'administrateur.

6.1.7 Niveau de résistance des fonctions de sécurité

Le niveau de résistance des fonctions de sécurités spécifiques sont les suivants :

- CR5 : la résistance de cette fonction sera démontrée pour les algorithmes cryptographiques et les mécanismes de génération d'aléas à l'aide du « dossier de test des algorithmes cryptographiques » et du dossier de test de la génération des nombres aléatoires. Le niveau visé est « SOF-high ».
- IA2 : la résistance de cette fonction sera démontrée si le temps nécessaire pour deviner l'identifiant de l'utilisateur est supérieur au temps défini par les critères communs. Le niveau visé est « SOF-high ».

6.2 Mesures d'assurance

Les mesures d'assurance correspondante aux classes d'assurance sont celles exprimées au paragraphe 5.3 dans les rubriques « Contenu et présentation des éléments de preuve ». Ce paragraphe identifie :

- La gestion de configuration
- Les procédures de livraison et d'installation,
- Le développement du produit,
- La documentation,
- Cycle de vie,
- Les tests,
- L'analyse de vulnérabilité

mis en œuvre pour satisfaire les exigences liées au niveau d'évaluation souhaité (voir § 1.3)

6.2.1 Configuration Management

La gestion de configuration permet d'avoir un identifiant unique pour chaque release de la TOE. Une release est une liste de composants Software identifiés par un numéro de version. Le document suivant décrit les procédures de gestion de configuration :

- M>Tunnel : Procédures de développement

Les exigences de sécurité satisfaites sont : ACM_CAP.2

6.2.2 Procédures de livraison et d'installation

Le document de livraison explique les procédures à suivre pour assurer de façon sécurisée la livraison du produit. Le guide d'installation présente les procédure à suivre pour installer de façon sur les différents composant de la TOE. Les documents suivants décrivent les procédures de livraison et d'installation :

- Procédure de livraison
- Guide administrateur

Les exigences de sécurité satisfaites sont : ADO_IGS.1 et ADO_DEL.1

6.2.3 Développement

Les documents permettant d'assurer un niveau de qualité compatible avec les exigences liées au niveau d'évaluation choisie sont les suivants :

- M>Tunnel : Spécifications fonctionnelles
- M>Tunnel : Conception générale de M>Tunnel 2.5
- M>Tunnel : Conception détaillée (partie cryptographique)

Les exigences de sécurité satisfaites sont : ADV_FSP.1, ADV_HLD.2, ADV_LLD.1, et ADV_RCR.1

6.2.4 Documentation

La documentation, fournie lors de la livraison du produit, intègre à la fois l'installation et la configuration de ce dernier. Ces documents mettent en garde l'administrateur des erreurs ou omissions à éviter qui risquent de mettre en péril la sécurité de la TOE . Les documents sont les suivants :

- M>Tunnel Guide de l'administration système,
- M>Tunnel Guide de l'administrateur,
- M>Tunnel Client Guide de l'utilisateur

Les exigences de sécurité satisfaites sont : AGD_USR.1 et AGD_ADM.1

6.2.5 Test

Le document suivant décrit les tests réalisés sur la TOE pour mettre en évidence la conformité par rapport aux spécifications et la robustesse de cette dernière :

- M>Tunnel : Plan de test

Les exigences de sécurité satisfaites sont : ATE_FUN.1, ATE_COV.1 et ATE_IND.2

6.2.6 Analyse de Vulnerabilité

Le document suivant fournit l'analyse des failles de sécurité qui pourraient être utilisées par un attaquant :

- Analyse de vulnérabilité de M>Tunnel

Le document suivant démontre le niveau de résistance des mécanismes d'authentification (utilisateurs et administrateurs) et de générations d'aléas

- Niveau de résistance des fonctions de sécurité

Les exigences de sécurité satisfaites sont : AVA_SOF.1 et AVA_VLA.2

7. Conformité à un profil de protection

La cible de sécurité ne fait référence à aucun profil de protection

7.1 Référence du profil de protection

Sans Objet

7.2 Raffinement du profil de protection

Sans Objet

7.3 Complément au profil de protection

Sans Objet

8. Argumentaire

Cette section fournit les matrices de cohérence qui démontrent que :

- Les objectifs de sécurité fournissent les contre mesures pour faire face à toutes les menaces identifiées
- Les exigences de sécurité permettent de couvrir tous les objectifs de sécurité
- Les fonctions de sécurité permettent de couvrir toutes les exigences de sécurité

8.1 Argumentaire pour les objectifs de sécurité

Cette section démontre que les objectifs de sécurité contrent toutes les menaces identifiées.

Le tableau ci-dessous montre que chaque menace est prise en compte par au moins un objectif de sécurité et que chaque objectif de sécurité est corrélé avec au moins une menace.

	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10	O11	O12	O13	O14	OE1	OE2	OE3	OE4	OE5	OE6	OE7	OE8	OE9
T1				X	X																		
T2	X	X														X							
T3			X									X		X									
T4				X																			
T5			X															X					
T6									X														
T7	X																						
T8			X										X										
T9	X									X													
T10							X																
T11		X																	X				
T12														X									
T13							X	X			X												
T14						X																	
TE1																		X					
TE2															X		X	X					
SU1																X							
SU2																	X	X					
SU3																		X					
SU4																		X					
SU5																		X					
SU6															X			X					
SU7																				X			
SU8																					X		
SU9																						X	
SU10																							X
SU11																		X					
P1																		X					

	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10	O11	O12	O13	O14	OE1	OE2	OE3	OE4	OE5	OE6	OE7	OE8	OE9
P2		X					X	X										X					
P3																		X					
P4																		X					

8.1.1 Les hypothèses d'utilisation

SU1 Les M>Tunnel Master et Gateway ainsi que le logiciel d'administration sont physiquement protégés de façon à ce que seuls les administrateurs aient accès physiquement à ces machines

Il est nécessaire que la station de travail et les M>Tunnel Gateway soient dans des lieux protégées (OE2).

SU2 Les fonctions de sécurité incluses dans la TOE pouvant être compromises par les administrateurs, ces derniers sont des gens de confiance et ont été formés.

Les deux conditions décrites ci-dessus sont prises en compte par OE3 et OE4

SU3 Le logiciel d'administration est utilisée conformément à sa documentation « Guide de l'administrateur »

Pour réduire tous risques d'erreurs ou d'omissions lors de l'élaboration de la politique de chiffrement, il est nécessaire que les administrateurs soient formés et respecte les préconisations écrites par le fournisseur. Ceci est précisé dans OE4.

SU4 Sur les postes de travail intégrant les logiciels M>Tunnel Master, M>Tunnel Gateway ou celui d'administration, les administrateurs modifient périodiquement les mots de passe d'accès en prenant comme contrainte qu'ils doivent être aléatoires et d'une longueur supérieure à 7 caractères alphanumériques

Pour réduire les risques de compromission des équipements, il est nécessaire que les administrateurs soient formés (OE4)

SU5 Les administrateurs analysent périodiquement les fichiers d'évènements afin de s'assurer qu'aucune attaque n'a eu lieu et vérifient le bon fonctionnement de l'enregistrement des évènements (Typiquement, ils s'assurent qu'il y a de la place disque suffisante)

Cette recommandation fait partie de la formation des administrateurs (OE4).

SU6 la TOE est administrée, par un seul administrateur à la fois, à l'aide d'un seul logiciel d'administration

Cette recommandation a pour but d'éviter que plusieurs personnes manipulent la politique de chiffrement en même temps. Cela fait partie de la formation des administrateurs (OE4). L'unicité de la station d'administration autorisée doit être vérifié par le responsable de la TOE (OE1)

SU7 le M>Tunnel Master doit être connecté à un réseau accessible par tous les M>Tunnel Client

OE6 répond à cette exigence en imposant que le M>Tunnel Master soit accessible par tous les M>Tunnel Clients

SU8 Chaque utilisateur doit recevoir, de façon sécurisé, son certificat et sa clé privée associée, stockés sur une carte à puce. Les sauvegardes des clés privées des utilisateurs, si elles existent, doivent être sécurisées.

OE7 répond à cette exigence en imposant que les clés privées et les certificats des utilisateurs soient stockés sur un support indépendant (carte à puce)

SU9 L'utilisateur n'est pas administrateur de son poste de travail.

OE8 répond à cette exigence en imposant que tous les postes de travail équipés de M>Tunnel Client soient administrés par des administrateurs autorisés

SU10 le logiciel d'administration est installé sur un poste disposant d'un M>Tunnel Client, et les M>Tunnel Master sont installés sur un poste équipé d'un M>Tunnel Gateway.

OE9 répond à cette exigence en imposant d'équiper le poste de la station d'administration d'un M>Tunnel Client et les postes M>Tunnel Master de M>Tunnel Gateway.

SU11 La politique de chiffrement doit être définie en un seul point même si elle s'applique dans un environnement distribué où les informations traversent un réseau non sûr.

Lors de la formation des administrateurs, ceci a été expliqué (OE4) afin d'éviter des conflits lors de la définition de la politique de chiffrement.

8.1.2 Les menaces prises en compte par la TOE

Ce paragraphe explique les relations qui existent entre les menaces et les objectifs de sécurité chargés de les contrer.

T1 Un utilisateur autorisé peut, par erreur, modifier les politiques de chiffrement et de filtrage concernant le M>Tunnel Client.

Les politiques de chiffrement et de filtrage du M>Tunnel Client sont contenues soit sur le poste de travail soit sur la gateway. O5 empêche l'utilisateur de modifier non intentionnellement le logiciel M>Tunnel Client et les politiques de filtrage et de chiffrement installés sur son poste et O4 ne permet la modification de la politique de chiffrement que par les administrateurs.

T2 Un attaquant (externe ou interne) peut modifier les politiques de chiffrement et de filtrage afin d'avoir accès, en clair, lors de leur transfert sur le réseau, à des informations qui auraient du transiter chiffrées.

Pour avoir accès à des applications non autorisées protégées par un tunnel, il faut soit avoir accès physiquement à la machine (OE2 ne le permet pas) soit d'avoir accès via le réseau. Dans ce deuxième cas, il faut soit enclencher un tunnel mais O1 ne le permet que pour les utilisateurs autorisés soit contourner la politique de chiffrement ce qui est contraire à O2.

T3 Un attaquant empêche la communication (daemon d'administration) entre le logiciel d'administration et les M>Tunnel Master ou Gateway ou modifie les informations transitant entre ces différents composants (Politique de chiffrement, Politique de filtrage, CRL, Configuration)

Si un attaquant arrive à couper la liaison entre la station d'administration et les M>Tunnel Gateway, cela ne met pas en péril la sécurité car le système peut fonctionner en mode autonome comme le stipule O12. O14 empêche un attaquant de modifier la politique de chiffrement, de filtrage ainsi que la configuration. De plus grâce à O3, cet incident sera inscrit dans le fichier d'évènement.

T4 Une personne non autorisée peut accéder ou modifier les fichiers d'évènements stockés sur les M>Tunnels Gateway et Master de la TOE

Pour accéder ou modifier les fichiers d'évènements, il faut pouvoir se connecter sur la station d'administration ou sur les M>Tunnels Gateway. Ceci n'est autorisé que pour les administrateurs comme le précise O4.

T5 La TOE n'est plus en mesure de remplir les fichiers d'évènements.

O3 oblige l'administrateur de vérifier que le système d'enregistrement des évènements fonctionne correctement. Ceci est facilement réalisable car les administrateurs ont été formés comme l'impose OE4 et qu'ils doivent analyser périodiquement les fichiers d'évènements (SU5).

T6 Un attaquant peut capturer les clés de session servant au chiffrement des paquets IP

Pour empêcher la capture et l'exploitation des clés de chiffrement qui transitent sur le réseau, O9 impose que ces dernières soient chiffrées.

T7 Un utilisateur, autre que celui à l'initiative de la mise en œuvre du tunnel, peut récupérer, les clés de session de ce tunnel et déchiffrer ainsi les paquets IP transitant sur ce dernier

Pour empêcher à un utilisateur de participer à une négociation en cours, il est nécessaire d'avoir un système d'anti rejeu (O1)et que le transfert des clés de session soient protégées en confidentialité et en intégrité (O9).

T8 Un utilisateur peut , par des erreurs de manipulations du M>Tunnel Client, entraîner le blocage ou la destruction d'un M>Tunnel Gateway.

O13 impose la gestion des cas d'erreur de manipulation lors des phases d'authentification et de négociation des clés afin d'empêcher un M>Tunnel Gateway de rester bloquer en attente des messages provenant de l'autre extrémité du tunnel. De plus, toutes ces actions sont stockées dans le fichiers d'évènements comme l'impose O3.

T9 Un attaquant , muni d'un logiciel M>Tunnel Client , ou un utilisateur sans sa carte à puce, peut se connecter à un M>Tunnel Master puis à un M>Tunnel Gateway et ainsi établir un tunnel afin d'avoir accès aux informations protégées par la politique de filtrage

Pour avoir accès à des données sensibles protégées par un tunnel, il faut enclencher un tunnel mais O1 ne le permet que pour les utilisateurs autorisés et de ce dernier on ne doit pas pouvoir récupérer des informations transitant sur un autre tunnel. Ceci est pris en compte par O10

T10 Un attaquant peut modifier l'intégrité des paquets IP circulant sur le réseau sans que les utilisateurs de ces informations s'en aperçoivent

O7 empêche toute modification des données transitant sur le réseau car il oblige une vérification d'intégrité pour tous les paquets IP signés.

T11 Un utilisateur, suite à une erreur de manipulation, empêche la mise en œuvre du M>Tunnel Client sur son poste de travail et envoie, sans le savoir, des données non chiffrées

O2 empêche que par erreur de manipulation des données chiffrées puissant transiter sur le réseau en clair. Pour plus de sécurité, OE5 demande à l'administrateur de mettre comme politique par défaut le chiffrement des paquets IP.

T12 Lors d'un dysfonctionnement (ou d'un déni de service) du M>Tunnel Master, les utilisateurs ne peuvent plus accéder aux différents M>Tunnel Gateway dont ils connaissent les caractéristiques. Ces caractéristiques n'ayant pas changé depuis le début du dysfonctionnement (ou déni de service) du M>Tunnel Master.

Comme O14 impose de stocker et d'utiliser les politiques de chiffrement et de filtrage sur les postes client et Gateway, cela permet au M>Tunnel Client de mettre en œuvre ses tunnels même si la connexion au M>Tunnel Master est impossible

T13 un attaquant peut effectuer une attaque en confidentialité et/ou en intégrité sans connaissance préalable des secrets

O8 empêche toute accès aux données transitant sur le réseau et O7 empêche toute modification de ces dernières car il oblige une vérification d'intégrité pour tous les paquets IP. Par ailleurs, O11 tient compte du problème de l'usure des clés.

T14 La sécurité de la TOE peut être réduite suite à des non cohérence dans les règles de sécurité définies par l'administrateur à l'aide du logiciel d'administration

L'objectif O6 prend en compte cette menace en intégrant, dans la station d'administration, des mécanismes de vérification de cohérence de la politique de chiffrement et de filtrage.

8.1.3 Les menaces liées à l'environnement opérationnel

TE1 La sécurité de la TOE peut être réduite suite à des erreurs ou omissions des règles de sécurité par le logiciel d'administration

Pour réduire tous risques d'erreurs ou d'omissions lors de l'élaboration de la politique de chiffrement, il est nécessaire que les administrateurs soient formés et reconnus compétent par le fournisseur de M>Tunnel. Ceci est précisé dans OE4.

TE2 La TOE est installée de façon non sûre

Pour éviter que la TOE soit installée n'importe comment, il faut que :

- *Le responsable de la TOE vérifie son installation avant de la mettre en service (OE1)*
- *Les administrateurs soient correctement formés (OE4)*
- *Le responsable ait confiance dans les administrateurs (OE3)*

8.1.4 Politique de sécurité

P1 La PKI doit fournir des identifiants uniques pour chaque utilisateur et chaque équipement de la TOE

Lors de la formation des administrateurs, ceci a été expliqué (OE4)

P2 La politique de chiffrement doit garantir que les informations sensibles, contenues dans des paquets IP, circulant sur des réseaux non sûr doivent être chiffrées et authentifiées

Les objectifs O2,O7 et O8 prennent en compte cette exigence de la politique de chiffrement car :

- *O2 précise que ce sont les administrateurs qui définissent la politique de chiffrement*
- *O7 garantit l'intégrité des données*
- *O8 garantit le chiffrement des données*

De plus, OE4 permet d'assurer que les administrateurs sont compétents pour définir la politique.

P3 La politique de filtrage doit garantir que seuls les flux autorisés peuvent traverser les équipements M>Tunnel Gateway

Lors de la formation des administrateurs, ceci a été expliqué (OE4)

P4 L'administrateur doit mettre à jour régulièrement la CRL

Lors de la formation des administrateurs, ceci a été expliqué (OE4)

8.2 Argumentaire pour les exigences de sécurité

8.2.1 Matrice de cohérence Exigences de sécurité-objectifs

Cette section démontre que les exigences de sécurité couvrent l'ensemble des objectifs.

Le tableau ci-dessous montre que chaque objectif est pris en compte par au moins une exigence de sécurité et que chaque exigence de sécurité est corrélée avec au moins un objectif.

	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10	O11	O12	O13	O14
FAU_GEN			**1,2**											
FAU_SAR			**1,2,3**											
FAU_STG			**2,4**											
FCS_CKM									**1,2**	**1,2**	**1,2**			
FCS_COP							**1**	**1**	**1**					
FDP_ACC	**2**	**2**		**2**										
FDP_ACF	**1**													
FDP_IFC		**2**												
FDP_IFF		**1**					**1**	**1**						
FDP_ITT		**1**												**1**
FDP_UCT								**1**				**1**		**1**
FDP_UIT							**1**					**1**		**1**
FIA_AFL				**1**										
FIA_ATD	**1**													
FIA_UAU	**2,3**									**3**	**6**			
FIA_UID	**2**													
FMT_MSA				**1**		**1**								
FMT_MTD				**1**					**1**					
FMT_SMR	**1**			**1**										
FPT_ITT					**3**									**1**
FPT_RPL	**1**													
FPT_RVM					**1**							**1**	**1**	
FPT_STM			**1**											

O1 La TOE doit s'assurer, lors de la phase de mise en œuvre d'un tunnel, que l'utilisateur, possède un identifiant autorisé et qu'aucune phase de re-jeu n'est en cours

Cet objectif est couvert par l'ensemble des exigences de sécurité suivantes :

- Chaque utilisateur a un identifiant et un rôle défini (FIA_ATD.1, FMT_SMR.1)
- Il est nécessaire de définir un mécanisme d'authentification (FIA_UAU.2, FIA_UAU.3)
- Il est nécessaire de définir les conditions d'enclenchement de l'authentification (FIA_UID.2, FDP_ACC.2)
- Il est nécessaire de définir les conditions d'interdiction de l'authentification (FDP_ACF.1)
- Il est nécessaire d'avoir une exigence de sécurité liée à la détection du rejeu (FPT_RPL.1)

O2 La TOE doit appliquer la politique de chiffrement et de filtrage définie par l'administrateur

Cet objectif est couvert par les exigences de sécurité de protection des données de l'utilisateur :

- Chaque information émise ou reçue doit respecter la politique de chiffrement (FDP_IFC.2, FDP_IFF.1, FDP_ITT.1)
- La politique est définie par l'administrateur (FDP_ACC.2)

O3 La TOE doit fournir les moyens permettant d'enregistrer les événements de sécurité tels que :

- **les tentatives d'intrusion,**
- **les authentifications de chaque utilisateur.**

Cet objectif est couvert par les exigences de sécurité d'audit :

- Définition des messages et les informations associés (FAU_GEN.1, FAU_GEN.2)
- Définition des actions qui peuvent être entreprises sur les fichiers d'audit (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)
- Définition des conditions de stockage de ces fichiers (FAU_STG.2, FAU_STG.4)

De plus, il est nécessaire de pouvoir dater avec précision l'ensemble de ces informations (FPT_STM.1)

O4 la TOE doit s'assurer que seuls les administrateurs autorisés ont le droit, grâce au logiciel d'administration, de se connecter sur la station d'administration et/ou sur les M>Tunnel Master et Gateway afin de changer les politiques de chiffrement, de filtrage, la CRL et la configuration et d'avoir accès aux messages de sécurité

Cet objectif est couvert par les exigences de sécurité suivantes :

- Le rôle d'administrateur doit être défini (FMT_SMR.1)
- Il est nécessaire de définir les conditions d'authentification des administrateurs (FDP_ACC.2, FIA_AFL.1)
- L'administrateur doit définir les conditions d'accès aux équipements et aux politiques de chiffrement, de filtrage (FMT_MSA.1, FMT_MTD.1)

O5 La TOE doit se protéger contre les modifications ou désactivations, non intentionnelles, des mécanismes de sécurité et des modifications non intentionnelles des informations propres à la TOE .

Cet objectif est couvert par les exigences suivantes :

- Une protection afin d'éviter de court-circuiter les mécanismes de sécurité (FPT_RVM.1)
- Une protection des mécanismes de sécurité à l'aide d'une vérification automatique de l'intégrité des informations lorsqu'elles transitent entre les différents éléments de la TOE (FPT_ITT.3),

O6 La TOE doit fournir, à l'administrateur, lors de la mise en œuvre d'une politique de chiffrement et/ou de filtrage, une vérification de cohérence.

Cet objectif est couvert par l'exigence de gestion de la sécurité (FMT_MSA.1) qui impose une vérification de la cohérence des attributs de sécurité.

O7 La TOE doit pouvoir rejeter tout paquet IP signé qui a subi des modifications durant son transfert sur le réseau.

Cet objectif est couvert par l'ensemble des exigences de sécurité suivantes :

- Chaque information émise ou reçue doit respecter la politique de chiffrement (FDP_IFF.1)
- Il est nécessaire d'avoir une protection de l'intégrité des données transitant sur le réseau (FDP_UIT.1)
- Selon la politique de chiffrement, il y a un choix des algorithmes de cryptographie qui est fait (FCS_COP.1)

O8 La TOE doit pouvoir chiffrer les paquets IP transitant sur le réseau.

Cet objectif est couvert par l'ensemble des exigences de sécurité suivantes :

- Chaque information émise ou reçue doit respecter la politique de chiffrement (FDP_IFF.1)
- Il est nécessaire d'avoir une protection de confidentialité des données transitant sur le réseau (FDP_UCT.1)
- Selon la politique de chiffrement, il y a un choix des algorithmes de cryptographie qui est fait (FCS_COP.1)

O9 La TOE doit protéger le transfert des clés de session

Cet objectif est pris en compte par les exigences de sécurité suivantes :

- Il est nécessaire d'avoir des mécanismes de gestion (création, distribution) des clés de session (FCS_CKM.1, FCS_CKM.2)
- Ces mécanismes utilisent des algorithmes de cryptographie (FCS_COP.1)
- Il faut aussi définir la politique de chiffrement concernant l'envoi des clés de session (FMT_MTD.1)

O10 La TOE doit empêcher un utilisateur d'un tunnel d'accéder aux informations transitant sur un autre tunnel

Cet objectif est pris en compte par les exigences de sécurité suivantes :

- Il est nécessaire d'avoir des mécanismes de gestion (création, distribution) des clés de session (FCS_CKM.1, FCS_CKM.2)
- Il est nécessaire d'authentifier l'utilisateur pour échanger les clés de session de ses tunnels (FIA_UAU.3)

O11 La TOE doit être capable de renouveler automatiquement et de façon sur les clés de chiffrement selon des critères paramétrables (durée, débit)

Cet objectif est pris en compte par les exigences de sécurité suivantes :

- Il est nécessaire d'avoir des mécanismes de gestion (création, distribution) des clés de session (FCS_CKM.1, FCS_CKM.2)
- Il est nécessaire de ré authentifier régulièrement l'utilisateur pour changer les clés de session de ces tunnels (FIA_UAU.6)

O12 M>Tunnel Gateway et M>Tunnel Master doivent pouvoir fonctionner même s'il n'y a plus de liaison avec la station d'administration.

Cet objectif est pris en compte en imposant l'application des fonctions de sécurité (FPT_RVM.1) qui demande l'application de la politique de sécurité stockée sur les équipements (FDP_UCT.1, FDP_UIT.1)

O13 La TOE doit être capable de gérer les cas d'erreurs de manipulation lors de la mise en œuvre d'un tunnel ou lors de la négociation des clés de session.
Cet objectif est pris en compte en garantissant que les fonctions qui mettent en oeuvre la politique de chiffrement sont appelées et s'exécutent dans tous les cas (FTP_RVM.1)

O14 Toutes les informations liées à la politique de chiffrement ou de filtrage ainsi que la configuration et transitant sur un réseau non sûr doivent être sécurisées. De plus, ces informations doivent être stockées sur le poste de l'utilisateur.

Cet objectif est couvert par exigences de sécurité de protection des données de l'utilisateur :

- Il est nécessaire d'avoir une protection de confidentialité des données transitant sur le réseau (FDP_UCT.1)

- Il est nécessaire d'avoir une protection de l'intégrité des données transitant sur le réseau (FDP_UIT.1)
- Il est nécessaire d'avoir une protection des données lors de leur transfert sur le réseau et entre deux éléments de la TOE (FPT_ITT.1, FDP_ITT.1)

8.2.2 Etude des dépendances et de la complémentarité des exigences de sécurité

Toutes les dépendances, entre les exigences de sécurité retenues pour la TOE, définies par les « Critères Communs » ont été respectées à l'exception de celles correspondant aux exigences suivantes :

- FMT_MSA.2 : Cette dépendance est, normalement, prévue par les exigences de sécurité FCS_CKM.1, FCS_CKM.2, FCS_COP.1 qui traitent de la génération et la distribution des clés de session ainsi que des algorithmes de cryptographie. Pour toutes ces exigences, il n'y a pas de prise en compte de valeur sure car on utilise uniquement des valeurs générées par des algorithmes pseudo-aléatoires (même pour l'initialisation). C'est la raison pour laquelle l'exigence de sécurité FMT_MSA.2 n'a pas été retenue,
- FCS_CKM.4 : cette dépendance est, normalement, prévue par les exigences de sécurité FCS_CKM.1, FCS_CKM.2, FCS_COP.1 qui traitent de la génération et la distribution des clés de session ainsi que des algorithmes de cryptographie. La destruction des clés de session ne peut se faire immédiatement car il faut être sur d'avoir reçu tous les paquets chiffrés avec cette clé avant de la détruire (ceci dépend du temps de transit à travers le réseau). C'est pourquoi, le système garde en mémoire en permanence trois clés (la précédente, la courante et la suivante) et uniquement trois clés,
- FTP_ITC.1 : cette dépendance est, normalement, prévue par les exigences de sécurité FDP_UCT.1, FDP_UIT.1 qui traitent de la protection des données échangées. Ces exigences s'appliquant aussi aux données internes échangées entre les différents équipements de la TOE et la TOE n'ayant qu'une seule TSF, il n'est pas utile d'avoir cette exigence,
- FTP_TRP.1 : cette dépendance est, normalement, prévue par les exigences de sécurité FDP_UCT.1, FDP_UIT.1 qui traitent de la protection des données échangées. Ces exigences s'appliquant aussi aux données des utilisateurs échangées entre les différents équipements de la TOE, il n'est pas utile d'avoir une exigence qui traite spécifiquement des mécanismes de sécurité des utilisateurs,
- FMT_MSA.3 : cette dépendance est, normalement, prévue par les exigences de sécurité FDP_ACF.1 qui n'a pas besoin de données d'initialisation et FDP_IFF.1 dont l'initialisation est laissée à la charge de l'administrateur (cette initialisation est décrite dans la documentation livrée avec la TOE),

L'ensemble des exigences de sécurité définies dans la cible de sécurité de M>Tunnel forment un soutien mutuel et de non contradiction pour les raisons suivantes :

- Le choix des exigences de sécurité et d'assurance a été fait en prenant en compte les hypothèses, les objectifs, les menaces concernant la TOE et son environnement et le niveau de certification visé. Cette cible de sécurité fournit les preuves que les objectifs de sécurité contre les menaces de la TOE et que les hypothèses et les objectifs contre les menaces liées à l'environnement de la TOE,
- Toutes les dépendances des exigences de sécurité ont été justifiées,
- Le niveau des exigences de sécurité a été justifié et est en adéquation avec le niveau de la certification visé.

8.2.3 Etude du niveau d'évaluation demandé

Après analyse de l'utilisation potentielle de la TOE dans certains environnements, EAL 2 augmenté de ADV_HLD.2, ADV_LLD.1, ALC_TAT.1 et AVA_VLA.2 a été choisi car il impose :

- la réalisation de tests indépendants faits par l'évaluateur afin de montrer la cohérence entre les spécifications fonctionnelles et la TOE (ceci permet de garantir à l'utilisateur que le produit possède les fonctionnalités attendues),
- une analyse de vulnérabilité indépendante démontrant la résistance à la pénétration d'attaquants possédant un potentiel d'attaque élémentaire (ceci permet de garantir à l'utilisateur que le produit a la capacité à résister à un certains nombre d'attaques),
- une évaluation des mécanismes de sécurité (authentifications et algorithmes de cryptographie) de la TOE (ceci permet de garantir à l'utilisateur la robustesse des mécanismes de sécurité),
- une maîtrise des procédés de réalisation des logiciels à l'aide d'une conception de haut niveau, d'une conception détaillée (bas niveau) afin de vérifier l'absence de trous de sécurité (ou back doors) et une maîtrise des outils de développement utilisés (ceci permet de garantir à l'utilisateur que le produit a été correctement conçu et réalisé).

Le niveau de résistance des exigences de sécurités spécifiques a été choisi à élevé afin de répondre aux exigences de la DCSSI en matière de cryptographique liées à l'utilisation de la TOE. Ce niveau se justifie par le fait qu'il existe

trois cas d'usurpation de l'authentification et que chaque cas nécessite un temps supérieur à la spécification requise. Les trois cas sont les suivants :

- création d'une bi-clé afin de permettre la mise en œuvre d'un certificat : dans ce cas, il faut trouver la clé privée de l'autorité,
- détermination de la clé privée d'un utilisateur,
- faire une phase de rejeu : du à la création d'aléa de chaque extrémité, il est nécessaire de connaître la clé privée d'un des utilisateurs.

Dans tous les cas, il faut découvrir une clé privée à partir d'une clé publique. Ces clés correspondent à un algorithme de RSA 1024 bits. RSA s'appuyant sur une factorisation de nombres premiers, ceci revient à forger une clé d'entropie 90 bits. Pour forger une clé privée, l'algorithme le plus performant le fait en 3 milliard de MIPS ans. Ce temps est très nettement supérieur à l'exigence.

8.3 Argumentaires pour les spécifications globales de la TOE

Cette section démontre que les fonctions de sécurité couvrent l'ensemble des exigences de sécurité.

Le tableau ci-dessous montre que chaque fonction de sécurité est pris en compte par au moins une exigence de sécurité et que chaque exigence de sécurité est corrélée avec au moins une fonction de sécurité.

	AU_1	AU_2	AU_3	CR_1	CR_2	CR_3	CR_4	CR_5	PR_1	PR_2	PR_3	PR_4	PR_5
FAU_GEN	**1,2**	**1,2**											
FAU_SAR	**1**		**2,3**										
FAU_STG			**2,4**										
FCS_CKM				**1**	**1,2**	**2**	**2**						
FCS_COP								**1**					
FDP_ACC													
FDP_ACF													
FDP_IFC									**2**	**2**			
FDP_IFF									**1**	**1**	**1**		
FDP_ITT									**1**	**1**			
FDP_UCT									**1**	**1**		**1**	
FDP_UIT									**1**	**1**		**1**	
FIA_AFL													
FIA_ATD													
FIA_UAU						**6**							
FIA_UID											**2**		
FMT_MSA													
FMT_MTD													
FMT_SMR													
FPT_ITT									**1**	**1**		**1**	
FPT_RPL					**1**								
FPT_RVM											**1**		**1**
FPT_STM		**1**											

IA_1	IA_2	IA_3	IA_5	IA_6	GS_1	GS_2	GS_3	GS_4

	IA_1	IA_2	IA_3	IA_5	IA_6	GS_1	GS_2	GS_3	GS_4
FAU_GEN									
FAU_SAR				1,2,3					
FAU_STG				2,4					
FCS_CKM						2			
FCS_COP									
FDP_ACC	2			2					
FDP_ACF	1	1		1	1	1			
FDP_IFC									
FDP_IFF									
FDP_ITT									
FDP_UCT									
FDP_UIT									
FIA_AFL				1					
FIA_ATD	1								
FIA_UAU	2	2,3	2,3		2,3				
FIA_UID		2	2			2			
FMT_MSA				1			1	1	1
FMT_MTD							1	1	1
FMT_SMR	1			1			1	1	
FPT_ITT						1			
FPT_RPL									
FPT_RVM									
FPT_STM									

FAU_GEN.1 Génération de données d'audit

- Cette exigence est prise en compte par les fonctions d'audit AU_1 et AU_2 qui assurent l'enregistrement des fichiers d'évènements ainsi que la définition des informations contenues dans ces fichiers

FAU_GEN.2 Lien avec l'identité de l'utilisateur

- Cette exigence est prise en compte par les fonctions d'audit AU_1 et AU_2 qui assurent l'horodatage des événement et la traçabilité vis à vis de l'origine de ces derniers

FAU_SAR.1 Revue d'audit

- Cette exigence est prise en compte par la fonction d'audit AU_1 qui assure la lisibilité des fichiers d'évènements et par la fonction d'identification IA_5 qui assure l'accès de ces fichiers aux administrateurs

FAU_SAR.2 Revue d'audit restreinte

- Cette exigence est prise en compte par la fonction d'audit AU_3 qui assure la lisibilité des fichiers d'évènements et par la fonction d'identification IA_5 qui restreint l'accès de ces fichiers aux administrateurs

FAU_SAR.3 Revue d'audit sélective

- Cette exigence est prise en compte par la fonction d'audit AU_3 qui assure le filtrage des données dans les fichiers d'évènements et par la fonction d'identification IA_5 qui restreint l'accès de ces fichiers aux administrateurs

FAU_STG.2 Garanties de disponibilité des données d'audit

- Cette exigence est prise en compte par la fonction d'audit AU_3 qui assure la protection des fichiers d'évènements même en cas de dépassement de la capacité de stockage et par la fonction d'identification IA_5 qui assure l'accès de ces fichiers aux administrateurs

FAU_STG.4 Prévention des pertes de données d'audit

- Cette exigence est prise en compte par la fonction d'audit AU_3 qui assure la protection des fichiers d'évènements même en cas de dépassement de la capacité de stockage et par la fonction d'identification IA_5 qui assure l'accès de ces fichiers aux administrateurs

FCS_CKM.1 Génération de clés cryptographiques

- Cette exigence est prise en compte par les fonctions de cryptographie CR_1 et CR_2 qui assurent la génération des clés de session à l'issue de la phase d'authentification

FCS_CKM.2 Distribution de clés cryptographiques

- Cette exigence est prise en compte par les fonctions de cryptographie CR_2, CR_3 et CR_4, qui mettent en œuvre le procédé de négociation, d'échange et d'application des clés de session, et par la fonction de gestion de sécurité GS_1 qui définit l'ordre des opérations lors de la phase de mise en œuvre d'un tunnel

FCS_COP.1 Opération cryptographique

- Cette exigence est prise en compte par la fonction de cryptographie CR_5 qui prend en compte l'ensemble des algorithmes cryptographiques

FDP_ACC.2 Contrôle d'accès complet

- Pour les utilisateurs, cette exigence est prise en compte par la fonction d'identification IA_1 qui assure l'identification de l'utilisateur.
- Pour les administrateurs, cette exigence est prise en compte par la fonction IA_5 qui assure l'identification des administrateurs.

FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité

- Pour les utilisateurs, cette exigence est prise en compte par la fonction de gestion de sécurité GS_1, qui impose la mise en œuvre de l'authentification, et par les fonctions d'identification IA_1, IA_2 et IA_6, qui assurent l'identification de l'utilisateur, son appartenance à l'autorité de certification et sa non révocation.
- Pour les administrateurs, cette exigence est prise en compte par la fonction IA_5 qui assure l'identification des administrateurs.

FDP_IFC.2 Contrôle de flux d'informations complet

- Cette exigence est prise en compte par les fonctions de protection et filtrage PR_1 et PR_2 qui assurent l'application des politiques de chiffrement et de filtrage à toute information transitant à travers un équipement M>Tunnel.

FDP_IFF.1 Attributs de sécurité simples

- Cette exigence est prise en compte par les fonctions de protection et filtrage PR_1 et PR_2, qui assurent l'application des politiques de chiffrement et de filtrage à paquet IP transitant à travers un équipement M>Tunnel, et PR_3 qui impose que tout paquet n'étant pas associé à une politique de chiffrement et de filtrage doit être rejeté.

FDP_ITT.1 Protection élémentaire d'un transfert interne

- Cette exigence est prise en compte par les fonctions de protection et filtrage PR_1 et PR_2, associés aux utilisateurs de M>Tunnel Client, qui assurent l'application des politiques de chiffrement et de filtrage à toute information transitant à travers un équipement M>Tunnel.

FDP_UCT.1 Confidentialité élémentaire lors d'un échange de données

- Cette exigence est prise en compte par les fonctions de protection et filtrage PR_1 et PR_2 qui assurent l'application des politiques de chiffrement et de filtrage à toute information transitant à travers un équipement M>Tunnel.

- Pour les informations issues du logiciel d'administration, la fonction de protection PR_4 répond à l'exigence de confidentialité

FDP_UIT.1 Intégrité lors d'un échange de données

- Cette exigence est prise en compte par les fonctions de protection et filtrage PR_1 et PR_2 qui assurent l'application des politiques de chiffrement et de filtrage à toute information transitant à travers un équipement M>Tunnel.
- Pour les informations issues du logiciel d'administration, la fonction de protection PR_4 répond à l'exigence d'intégrité.

FIA_AFL.1 Gestion d'une défaillance de l'authentification

- Pour les administrateurs, cette exigence est prise en compte par la fonction d'identification IA_5 qui assure l'identification des administrateurs et le rejet de ce dernier en cas de 4 tentatives infructueuses

FIA_ATD.1 Définition des attributs d'un utilisateur

- Cette exigence est prise en compte par la fonction d'identification IA_1 qui définit l'identifiant d'un utilisateur

FIA_UAU.2 Authentification d'un utilisateur préalablement à toute action

- Cette exigence est prise en compte par les fonctions d'identification IA_1, IA_2, IA_3 et IA_6 qui assurent l'authentification sure d'un utilisateur à l'aide d'un certificat.

FIA_UAU.3 Authentification infalsifiable

- Cette exigence est prise en compte par les fonctions d'identification IA_2, IA_3 et IA_6 qui assurent l'anti-rejeu au niveau de l'authentification d'un utilisateur.

FIA_UAU.6 Réauthentification

- Cette exigence est prise en compte par la fonction CR_3 qui assure une réauthentification périodique de l'utilisateur.

FIA_UID.2 Identification d'un utilisateur préalablement à toute action

- Cette exigence est prise en compte par les fonctions IA_2, IA_3, qui assurent l'obligation de l'utilisation de l'identifiant de l'utilisateur pendant la phase de négociation, par PR_3, qui impose la présence d'un tunnel avant tout transfert de paquets IP et par GS_1, qui impose l'authentification lors de la mise en œuvre d'un tunnel.

FMT_MSA.1 Gestion des attributs de sécurité

- Cette exigence est prise en compte par les fonctions de gestion GS_2, GS_3 et GS_4, qui assurent que seul le logiciel d'administration peut gérer les politiques de chiffrement et de filtrage, la CRL et la configuration sur les équipements M>Tunnel Master, Gateway, et IA_5, qui ne permet qu'aux administrateurs, d'avoir accès à ce logiciel d'administration. De plus, GS_4 qui impose au logiciel d'administration de vérifier la cohérence des informations fournies par l'administrateur

FMT_MTD.1 Gestion des données de la TSF

- Cette exigence est prise en compte par les fonctions de gestion GS_2, GS_3 et GS_4 qui assurent que seul l'administrateur peut modifier les politiques de chiffrement et de filtrage et la configuration sur les équipements M>Tunnel Master, Gateway

FMT_SMR.1 Rôles de sécurité

- Cette exigence est prise en compte par les fonctions d'identification IA_1 et IA_5, qui définissent les identifiants utilisateur de M>Tunnel Client et administrateurs des équipement M>Tunnel, et par les fonctions de gestion de sécurité GS_1 et GS_2, qui définissent le rôle de l'administrateur

FPT_ITT.1 Protection élémentaire du transfert de données à l'intérieur de la TSF

- Cette exigence est prise en compte par les fonctions de protection PR_1, PR_2_ et PR_4 qui assurent que les données échangées entre la station d'administration et les M>Tunnel Master et Gateway sont sécurisées.
- Cette exigence est prise en compte par la fonction de gestion GS_1 qui assure que les données de configuration de M>Tunnel Client échangées entre ce dernier et les M>Tunnel Master et Gateway sont sécurisées.

FPT_ITT.3 Contrôle de l'intégrité des données de la TSF

- Cette exigence est prise en compte par la fonction de protection PR_2 qui assure l'intégrité du et la confidentialité des informations transitant entre les différents éléments de la TOE.

FPT_RPL.1 Détection de rejeu

- Cette exigence est prise en compte par la fonction de cryptographie CR_2 qui assure le non rejeu de la phase d'authentification et de négociation des clés

FPT_RVM.1 Capacité de la TSP à ne pas être court-circuitée

- Cette exigence est prise en compte par les fonctions de protection PR_3 et PR_5 qui assure le non transfert des paquets IP tant que les tunnels ne sont pas mis en œuvre même en cas d'indisponibilité du M>Tunnel Master
- Cette exigence est prise en compte par la fonction de protection PR_5 qui impose l'utilisation des politiques de chiffrement et de filtrage stockées sur l'équipement quand ce dernier ne peut les remettre à jour

FPT_STM.1 Horodatage fiable

- Cette exigence est prise en compte par la fonction d'audit AU_2 qui assure que les évènements doivent être datés avec précision

Le raisonnement sur le niveau de résistance des fonctions de sécurités spécifiques est le même que celui sur le niveau de résistance des exigences de sécurité associées.

Les fonctions de sécurité définies dans la cible de sécurité de M>Tunnel forment un ensemble homogène permettant de répondre aux exigences de sécurité pour les raisons suivantes :

- Le choix des fonctions de sécurité a été fait en prenant en compte les exigences de sécurité concernant la TOE et son environnement et le niveau de certification visé. Cette cible de sécurité fournit les preuves que les fonctions de sécurité remplissent les exigences de sécurité,
- Chaque exigence de sécurité est couverte par au moins une fonction de sécurité,
- Chaque fonction de sécurité est couverte par au moins une exigences de sécurité,
- Le niveau des fonctions de sécurité a été justifié et est en adéquation avec le niveau de la certification visé.