TRUSTWAY

Trustway IP Protect

Cible de sécurité

Référence	TW/IPP/IP Protect_Cible de sécurité - Light/PU
Nom du Document	Trustway_IP Protect _Cible de sécurité_FR
Version	1.22 - Light

Table des matières

Chapitre 1. Introduction

1.1 Présentation du document

L'objectif de ce document est de décrire la cible de sécurité des chiffreurs Trustway IP Protect dans un fonctionnement défini par le référentiel IPsec DR - Profil de Protection « Chiffreur IP ».

Les produits de la famille Trustway offrent une gamme personnalisée de chiffreurs "plug and play" ciblés sur des besoins de sécurité spécifiques.

Les produits de l'offre Trustway IP Protect fournissent une plateforme pour la création d'infrastructures de réseau de confiance.

1.2 Documents de référence

1. **Common Criteria for Information Technology Security Evaluation, Part 1**: Introduction and General Model; Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

2. **Common Criteria for Information Technology Security Evaluation, Part 2**: Security Functional Components; Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

3. **Common Criteria for Information Technology Security Evaluation, Part 3**: Security Assurance Components; Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

4. **Common Methodology for Information Technology Security Evaluation, Evaluation Methodology**. Version 3.1, Revision 5, April 2017. CCMB-2017-04-004

5. **Algorithmes Cryptographiques** : Guide de sélection d'algorithmes cryptographiques. https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf

6. **Recommandations de sécurité relatives aux mots de passe** : Réf DAT-NT-001/ANSSI/SDE/NP

7. **Problématique d'interconnexion des réseaux IP**. Version 1.9, mars 2004. Premier Ministre, Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information, Sous-direction scientifique et technique, Laboratoire Technologies de l'Information

8. **Profil de Protection « Chiffreur IP »**, réf PP-CIP-3.1, version 1.9 (https://www.ssi.gouv.fr/entreprise/certification_cc/pp-chiffreur-ip-ref-pp-cip-3-1-version-1-9)

9. **ANSSI : Note Crypto Référentiel IPsec DR Profil de Protection « Chiffreur IP »** (version du 16 mars 2021)

10. Référentiel général de sécurité. **Processus de qualification d'un produit – niveau standard** – Référence QUAL-PROD-PROCESS/1.0 du 12 janvier 2017.

11. **Security Architecture for the Internet Protocol**. RFC 4301. December 2005. http://www.ietf.org/rfc/rfc4301

12. **IP Encapsulating Security Payload (ESP)**. RFC 4303. December 2005. http://www.ietf.org/rfc/rfc4303

13. **The Internet Key Exchange Version 2 (IKEv2)**. RFC 7296. October 2014. http://www.ietf.org/rfc/rfc2409

14. **ANSSI – Référentiel IPsec DR** – Version ipsec-dr-ddea6592db-2019-11-05

1.3 Glossaire

Acronyme	Définition
AES	Advanced Encryption Standard
Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la partie 3 à un EAL ou à un paquet d'assurance
Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement
CAP	Carte à Puce
CC	Critères Communs
CIK	Crypto Ignition Key
Cible d'évaluation	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée
EAL	Niveau d'assurance d'évaluation : Paquet composé de composants d'assurance tirés de la partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC
EC	Equipement de Chiffrements
ECDSA	Elliptic Curve Digital Signature Algorithm
ESN	Extended Sequence Number
ESP	Encapsulating Security Payload
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis
HMAC	Keyed-Hash Message Authentication Code
HSM	Hardware Security Module. Equipement effectuant des opérations cryptographiques.
IP	Internet Protocol
IT	Technologie de l'Information
Objectif de sécurité	Une expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses
OCSP	(Online Certificate Status Protocol) Protocole permettant de valider un certificat en ligne auprès d'un répondeur OCSP
OSP	(Organisational Security Policy) Politique de sécurité organisationnelle

Acronyme	Définition
PP	Profil de Protection : Ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs
PRF	Pseudo Random Function
SA	Security Association
SF	(Security Function) Fonction de sécurité
SP	Security Policy
SFP	(Security Function Policy) Politique des fonctions de sécurité
SHA	Secure Hash Algorithm
SO	Security Officer
ST	Security Target
TDM	Trustway Domain Manager
TOE	Target of Evaluation
TPM	Trusted Platform Module. Composant de confiance utilisé par le chiffreur pour le stockage sécurisé de clés et le génération d'aléa.
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding

Table 1-1. Glossaire

Chapitre 2. Introduction de la cible de sécurité

2.1 Identification de la cible de sécurité

Titre : **Trustway IP Protect - Cible de Sécurité**

Version de la cible : **1.22 Light**

Référence : TW/IPP/IP Protect_Cible de sécurité/PU

Version de la TOE : **6.01.17**

Nom commercial de la TOE : **Trustway IP Protect**

2.2 Interopérabilité avec les anciens chiffreurs de la gamme Trustway

Afin de pouvoir réaliser la migration des réseaux de chiffreurs Trustway vers le mode IPsec DR, les chiffreurs IP Protect sont interopérables avec les TCRX et TVPN3 en utilisant des mécanismes non IPsec DR.

Une fois que tous les chiffreurs ont été remplacés par des IP Protect, une option TDM « Full IPsec DR » permet d'interdire tous les modes incompatibles avec le référentiel (**ANSSI : Note Crypto Référentiel IPsec DR Profil de Protection « Chiffreur IP »)**.

Seul le mode « Full IPSec DR » est pris en compte dans cette cible de sécurité ainsi que le mécanisme d'inhibition des fonctions d'interopérabilité.

2.3 Vue d'ensemble de la cible de sécurité

L'offre de chiffreurs IP Protect repose sur plusieurs éléments (voir Figure 1).

Les chiffreurs IP Protect représentent les points de liaison entre les réseaux sécurisés et les réseaux ouverts, effectuant le filtrage et appliquant la politique de sécurité.

Le TDM (Trustway Domain Manager) est un outil de configuration et de supervision nécessaire à la définition et l'application des politiques de sécurité sur les différents équipements de chiffrement Trustway utilisant un protocole propriétaire sécurisé. Le TDM détermine également les règles, vérifie l'état du réseau virtuel et permet la mise à jour à distance des équipements de chiffrement Trustway IP Protect. Le TDM permet notamment de configurer un mode « Full IPsec DR » qui interdit tous les modes incompatibles avec le référentiel ANSSI (**ANSSI : Note Crypto Référentiel IPsec DR Profil de Protection « Chiffreur IP »)**.

Le SPC (Station de Personnalisation Client) est nécessaire pour la personnalisation client des équipements de chiffrement Trustway. Le SPC est utilisé pour injecter des secrets spécifiques à un équipement en particulier et à un utilisateur particulier. L'équipement reçoit alors une personnalisation cryptographique et peut désormais être introduit dans le réseau du client.

L'offre des équipements de chiffrement Trustway inclut également des options :

- La communication sécurisée avec des stations de travail contenues dans un groupe de client VPN de type GVPNC ;
- La communication avec des équipements non gérés par le TDM, permettant notamment la mise en œuvre de mécanismes cryptographiques conformes aux exigences IPSec DR ANSSI et non utilisés pour la communication entre chiffreurs IP Protect (Cf **ANSSI : Note Crypto Référentiel IPsec DR Profil de Protection « Chiffreur IP »**) :
    - Authentification IKE par ECDSA sur BrainpoolP256r1 ;
    - Chiffrement IKE AES-CTR 256bits;
    - Diffie-Hellman DH28(BrainpoolP256r1) ;
    - Chiffrement ESP AES-CTR 256bits.

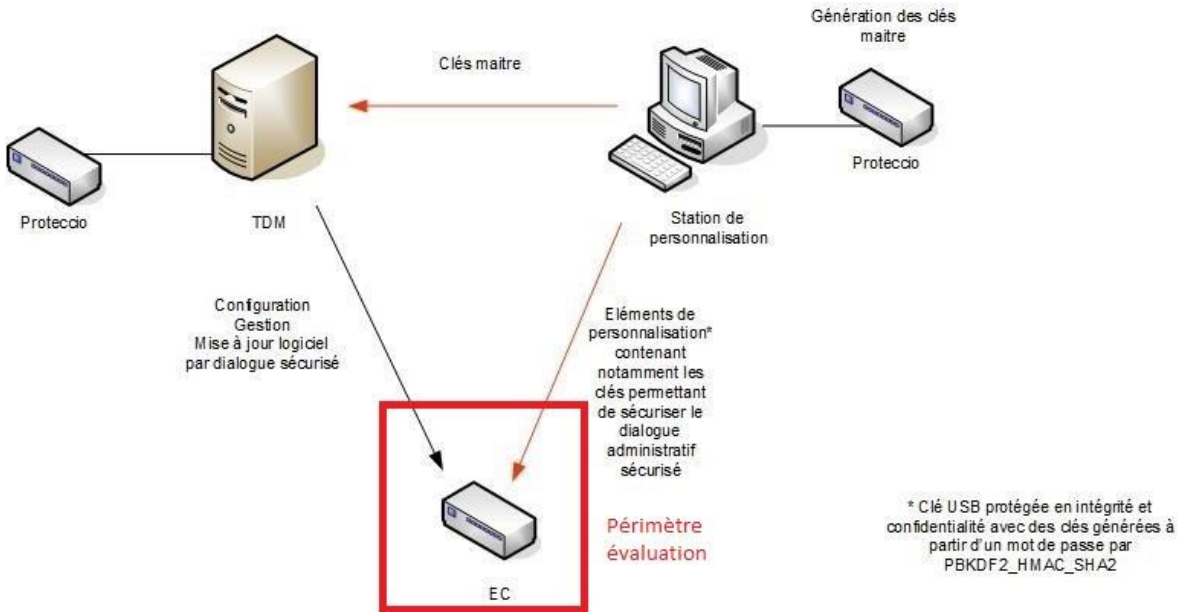


Figure 1 - Offre Trustway IP Protect : Infrastructure de Gestion

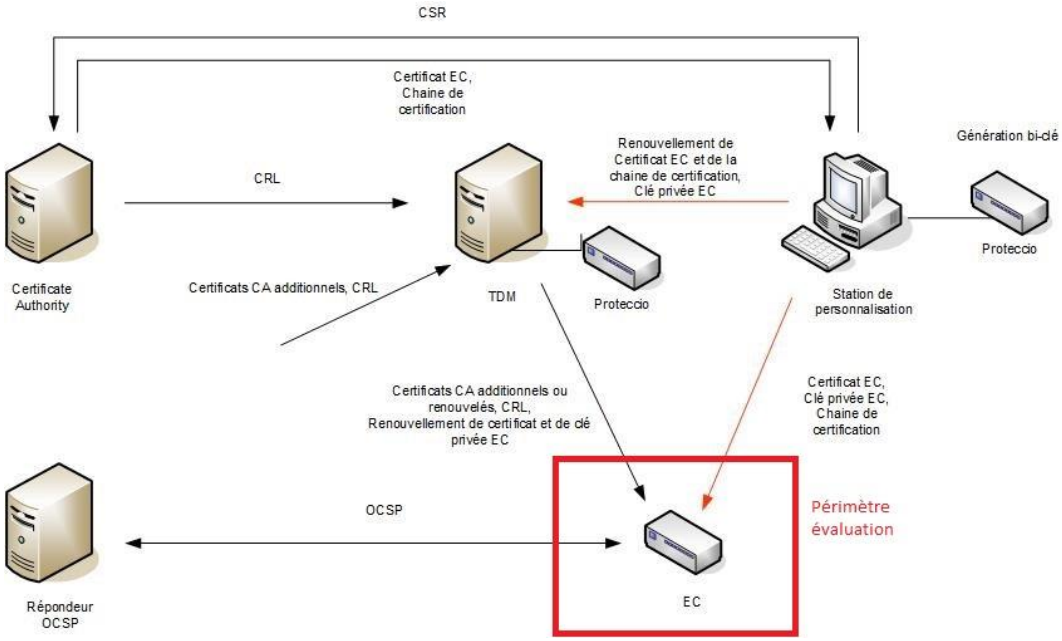


Figure 2 - Offre Trustway IP Protect : PKI

La flèche en rouge entre la station de personnalisation et le chiffreur (EC) représente l'opération de personnalisation du chiffreur qui est réalisée avec une clé USB protégée cryptographiquement créée sur la station de personnalisation et injectée sur le chiffreur.

Les SPC, TDM et stations nomades GVPNC ne sont pas inclus dans la TOE.

Les opérations cryptographiques du noyau Linux sont considérées de confiance et ne font pas partie du périmètre d'évaluation.

La TOE est composée (voir Figure 3) :

- du système d'exploitation des équipements de chiffrement Trustway IP Protect à l'exclusion du noyau Linux,
- du protocole sécurisé d'échange de données avec la station de configuration à distance (TDM).

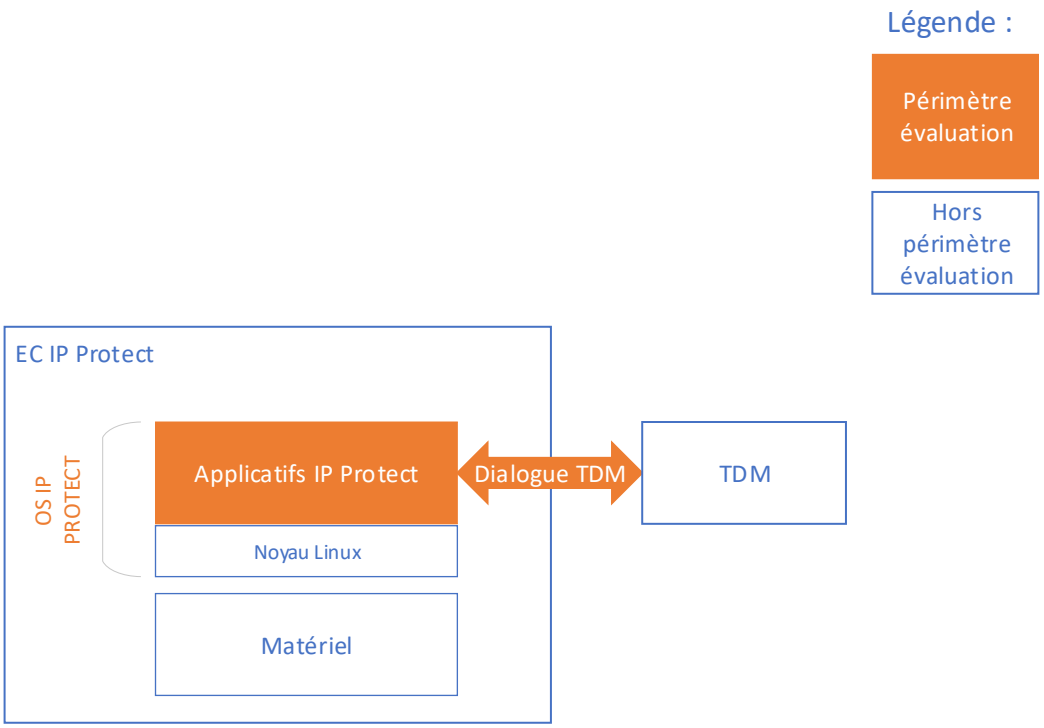


Figure 3 - Périmètre de l'évaluation

2.4 Conformité aux Critères Communs

La cible de sécurité est conforme aux Critères Communs v3.1 :

- CC Partie 1 [1] ;
- CC Partie 2 [2] (conformité stricte) ;
- CC Partie 3 [3] (conformité stricte) ;
- Méthodologie d'évaluation des CC [4].

Le niveau d'assurance pour cette cible de sécurité est EAL4, augmentée avec :

- ALC_FLR.3 (Systematic Flaw Remediation).

Cette augmentation est requise par le processus de qualification standard [10].

2.5 Conformité à un Profil de Protection

La cible de sécurité est basée sur le PP "chiffreur IP [8]" sans revendiquer une conformité.

2.6 Conformité à la qualification de niveau standard

Cette cible de sécurité est conforme au processus de qualification de niveau standard défini par l'ANSSI dans [9]. Elle est donc conforme au référentiel associé édité par l'ANSSI :

- Algorithmes de cryptographie [5].

Guides d'exploitation de la TOE

Titre	Version
86F223ET – Manuel d'installation des chiffreurs Trustway	31
86F227ET - Manuel de dépannage des chiffreurs Trustway	24
86F226ET - Manuel d'installation et d'utilisation TDM	44

Chapitre 3.Description de la TOE

L'offre de chiffreurs IP Protect se décline sous forme des modèles suivants:

Chiffreur 4 ports connectique 1Gbits/s (IE5L-4, IE20L-4, IE50L-4, IE100L-4):

Chiffreur 4 ports connectique 1Gbits/s (IE50-4, IE100-4, IE300-4):

Chiffreur 8 ports connectique 1Gbits/s (IE50-8, IE100-8, IE300-8):

Chiffreur 8 ports 1Gbits/s (IE900-8) ou 16 ports connectique 1G/10Gbits/s (IE1800-16):

3.1 Périmètre physique de la TOE

La cible d'évaluation décrite dans cette cible de sécurité comprend :

- Le service de sécurisation des paquets IP utilisateur ;
- Le service de démarrage sécurisé ;
- Le service de cryptographie et de protection des données sensibles ;
- Le service de télégestion du chiffreur (comprenant le protocole propriétaire d'échange de données sécurisé entre le TDM et le chiffreur) ;
- Le service d'envoi de traps SNMP et Syslog protégés par un tunnel ESP;
- Le service de négociation de clés IKE incluant OCSP pour la vérification de l'état de révocation d'un certificat en ligne ;
- Le service de communication IP.

Le système d'exploitation Linux 5.4.199 qui héberge ces fonctionnalités est hors TOE.

La version logicielle d'un chiffreur est monolithique et contient tous les composants logiciels intégrés. Il n'est pas possible de mettre à jour un composant logiciel indépendamment des autres.

3.1.1 Plateforme d'évaluation

La plateforme d'évaluation inclura :

- Une station TDM/SPC hébergeant l'application TDM et l'application SPC avec sa Proteccio ;
- Trois IP Protect, un par modèle disponible.

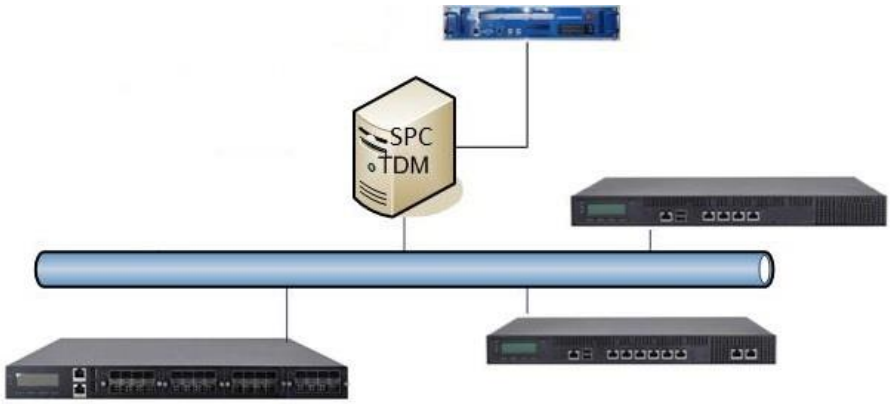


Figure 4 - Plateforme d'évaluation

La station TDM/SPC accueille l'application TDM et l'application SPC.

La Proteccio est le HSM des applications TDM et SPC (dans deux espaces cryptographiques distincts) utilisée pour leurs opérations cryptographiques.

Le HSM Proteccio en version 3.01.02 (V162/X163) possède une Qualification Renforcée.

3.2 Fonctionnalités de la TOE

La fonctionnalité principale de la TOE est de fournir au système d'information des liens de communication sécurisés entre plusieurs réseaux privés en offrant les services suivants pour protéger et cloisonner les flux de données (paquets IP transitant entre les chiffreurs IP) :

- Application des politiques de sécurité VPN :
  - Protection en confidentialité des données applicatives ;
  - Protection en authenticité des données applicatives ;
  - Protection anti-rejeu des données applicatives ;
  - Protection en confidentialité des données topologiques des réseaux privés ;
  - Protection en authenticité des données topologiques des réseaux privés,
- Cloisonnement des flux IP.

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

- Gestion des politiques de sécurité VPN:

  - Définition des politiques de sécurité VPN (assurée par le TDM hors TOE);
  - Protection de l'accès aux politiques de sécurité VPN.
- Gestion des clés cryptographiques :
  - Protection de l'accès aux clés cryptographiques ;
  - Injection des clés cryptographiques.
- Audit et supervision :
  - Audit/journalisation des opérations d'administration (assuré par le TDM hors TOE);
  - Génération d'alarmes de sécurité ;
  - Supervision de la TOE (émission d'événements vers des stations de supervision hors TOE).

3.2.1 Services fournis par la TOE

Application des politiques de sécurité VPN

Les politiques de sécurité VPN spécifient les règles de sécurité qui déterminent le traitement à appliquer aux données. Ces dernières représentent :

- Les données qui proviennent des applications du système d'information et qui sont véhiculées par le réseau. On parle alors de données applicatives ;
- Les données ajoutées par les mécanismes réseaux qui permettent notamment le routage des paquets IP. On parle alors de données topologiques.

Ces données transitent entre chaque paire de chiffreurs IP.

Les chiffreurs IP Protect appliquent des fonctions de filtrage implicite, car si aucune politique de sécurité VPN n'est définie sur un lien VPN donné, les paquets entrants ou sortants sont rejetés.

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

- La protection en confidentialité des données applicatives ;
- La protection en authenticité des données applicatives ;
- Protection anti-rejeu des données applicatives ;
- La protection en confidentialité des données topologiques ;
- La protection en authenticité des données topologiques.

Ces politiques sont conservées au niveau de chaque chiffreur IP concerné pour être appliquées localement.

Protection en confidentialité des données applicatives

Assurer la confidentialité des données applicatives permet d'empêcher la divulgation de ces données lorsqu'elles transitent sur un réseau public non sûr. Pour cela, ces données sont chiffrées avant de passer sur le réseau public et déchiffrées à l'entrée du réseau privé destinataire.

L'algorithme de chiffrement/déchiffrement et les caractéristiques des clés utilisées sont définis dans le contexte de sécurité associé à la politique de sécurité VPN définie sur un lien de communication donné.

Protection en authenticité des données applicatives

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

L'algorithme pour générer les informations d'authenticité et les vérifier ainsi que les caractéristiques des clés utilisées sont définies dans le contexte de sécurité associé à la politique de sécurité VPN définie sur un lien de communication donné.

Protection en anti-rejeu des données applicatives

La protection anti-rejeu de ESP est mise en œuvre conformément au référentiel IPsec-DR.

Protection en confidentialité des données topologiques

Assurer la confidentialité des données topologiques des réseaux privés permet d'empêcher la divulgation des adresses IP internes (source et destination) des équipements se trouvant sur les réseaux privés.

Comme pour les données applicatives, des algorithmes de chiffrement/déchiffrement sont utilisés et définis dans les contextes de sécurité.

Protection en authenticité des données topologiques

Assurer l'authenticité des données topologiques des réseaux privés permet de détecter toute modification des adresses IP internes (source et destination) des équipements se trouvant sur les réseaux privés.

Comme pour les données applicatives, des algorithmes pour générer les informations d'authenticité ou pour les vérifier sont utilisés et définis dans les contextes de sécurité.

Cloisonnement des flux IP

Chaque réseau privé peut être divisé en plusieurs sous-réseaux IP pour permettre de cloisonner des flux IP à l'intérieur même d'un réseau privé. Le service de cloisonnement des flux IP permet d'appliquer des politiques de sécurité VPN différentes suivant les sous-réseaux qui communiquent. Ce service permet aussi de filtrer les paquets IP entrants et de les envoyer sur le sous-réseau approprié.

3.2.2 Services nécessaires au bon fonctionnement de la TOE

3.2.2.1 Gestion des politiques de sécurité VPN

Définition des politiques de sécurité VPN (station TDM hors TOE)

Les politiques de sécurité VPN sont définies pour chaque lien de communication VPN autorisé. Ce lien de communication est établi entre deux sous-réseaux IP. Seul l'administrateur de sécurité TDM est autorisé à définir ces politiques. Il spécifie la règle de filtrage implicite pour l'envoi ou la réception de données : rejet ou application de services de sécurité. Dans le dernier cas, il spécifie aussi le(s) service(s) de sécurité à appliquer aux données envoyées ou reçues ainsi que le contexte de sécurité qui est associé à cette politique. Le contexte de sécurité contient entre autres les algorithmes cryptographiques utilisés, les tailles de clés et l'association avec les clés à utiliser.

Lorsqu'une phase de négociation est effectuée entre deux chiffreurs IP, une partie des politiques de sécurité et des contextes de sécurité peut être définie lors de cette phase en tenant compte de contraintes définies auparavant. Ces contraintes de sécurité globales sont définies par l'administrateur de sécurité et peuvent comprendre plusieurs stratégies classées par ordre de préférence selon leur force ou leur résistance à des attaques. Les chiffreurs IP peuvent entamer une négociation pour se mettre d'accord sur une politique de sécurité VPN spécifique à appliquer en respectant les contraintes globales et les ordres de préférence définis par l'administrateur de sécurité, de manière à choisir dynamiquement la politique la plus forte commune aux deux chiffreurs IP devant établir un lien VPN.

Ce service doit permettre à chaque chiffreur IP de s'authentifier auprès d'un autre chiffreur IP (et réciproquement) afin de négocier le contexte de sécurité (algorithmes à utiliser pour le chiffrement, algorithme pour le scellement, longueur des clés, ...) avant d'établir des liens VPN légitimes. Ce service est utile pour les chiffreurs IP qui sont amenés à générer des clés à la volée (lors de chaque établissement de liens VPN).

Protection de l'accès aux politiques de sécurité VPN

Ce service permet de contrôler les différents types d'accès (modification, consultation) aux politiques de sécurité VPN et à leurs contextes de sécurité suivant le rôle de la personne authentifiée.

3.2.2.2 Gestion des clés cryptographiques

Protection de l'accès aux clés cryptographiques

Ce service permet d'empêcher les clés secrètes et privées d'être exportées de manière non autorisée à l'extérieur de la TOE. Il permet aussi d'assurer qu'une clé donnée est utilisable (accessible) seulement par les services qui en ont besoin.

Injection des clés cryptographiques

Ce service permet d'injecter de façon sûre les clés cryptographiques, générées à l'extérieur de la TOE, dans les chiffreurs IP ou les équipements d'administration. Lors de la distribution, ce service protège les clés en intégrité et/ou en confidentialité en fonction du type de clés.

Bonne consommation des clés cryptographiques

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

Génération des clés cryptographiques

Ce service permet aux chiffreurs IP de générer des clés à l'issue de la phase d'authentification mutuelle et de négociation lors de l'établissement de liens VPN. Ces clés générées seront ensuite utilisées pour appliquer les services de sécurité des politiques de sécurité VPN.

3.2.2.3 Audit et supervision

Audit/journalisation des activités sur les liens VPN

Ce service permet de tracer toutes les opérations effectuées par les chiffreurs IP concernant la communication sur les liens VPN, comme par exemple la comptabilité du nombre de paquets chiffrés ou déchiffrés et les erreurs lors de l'établissement ou de l'utilisation des VPN. Il permet aussi la définition des événements à tracer et leur consultation.

Audit/journalisation des opérations d'administration (station TDM hors TOE)

Ce service permet de tracer toutes les opérations effectuées par l'administrateur TDM sur les chiffreurs IP concernant l'administration de ce chiffreur, comme par exemple les modifications des politiques de sécurité VPN. Il permet aussi la définition des événements à tracer et leur consultation.

Génération d'alarmes de sécurité

Ce service permet de générer des alarmes de sécurité pour signaler tout dysfonctionnement majeur des chiffreurs IP, comme par exemple une perte d'intégrité sur des clés.

Supervision de la TOE

Ce service permet à un auditeur des événements du chiffreur de contrôler l'état de disponibilité de chaque chiffreur IP (état de fonctionnement, niveaux d'utilisation des ressources, ...).

3.2.2.4 Protection des opérations d'administration

Les chiffreurs IP sont administrés localement et à distance. L'administration locale se fait directement sur la machine contenant les services du chiffreur IP alors que l'administration distante s'effectue au travers d'un réseau LAN ou WAN par la station TDM hors TOE.

Authentification locale des administrateurs

Ce service permet d'authentifier tous les administrateurs qui effectuent des opérations d'administration locale à un chiffreur IP.

Il n'y a pas de configuration locale complète du chiffreur. La seule configuration locale concerne les informations minimales pour recevoir la configuration complète du TDM. Il y une authentification par mot de passe pour l'accès à la configuration minimale.

Distribution des politiques de sécurité VPN

Une fois les politiques de sécurité VPN définies sur le TDM, elles sont distribuées aux chiffreurs IP concernés avec leurs contextes de sécurité. La cohérence entre la politique définie par l'administrateur de sécurité TDM en utilisant l'application TDM et celle se trouvant dans le chiffreur IP concerné doit être assurée afin que la protection des données circulant sur les liens VPN soit bien celle attendue et définie par l'administrateur de sécurité. Cet outil de définition de politique doit garantir la fiabilité de la traduction entre le langage utilisé par l'administrateur de sécurité pour définir la politique (en utilisant l'outil) et le langage utilisé dans les chiffreurs IP pour appliquer ces politiques.

Un canal sécurisé est utilisé pour distribuer les politiques de sécurité VPN et leurs contextes de sécurité afin de les protéger en authenticité et confidentialité.

Protection des flux d'administration à distance

Ce service permet de protéger en authenticité les flux de données échangées entre les chiffreurs IP et les équipements d'administration pour effectuer des opérations d'administration à distance. Ce service permet aussi de protéger en confidentialité les flux d'administration. Cette protection concerne les flux d'administration de sécurité (politiques de sécurité VPN et clés) et les flux d'administration système et réseau (paramètres de configuration). En revanche, ce service n'applique pas cette protection aux flux de supervision

Protection contre le rejeu des flux d'administration

Ce service protège contre le rejeu de séquences d'opérations d'administration à distance passant sur les liens entre les chiffreurs IP et les équipements d'administration.

3.2.2.5 Protection de l'accès aux paramètres de configuration

Ce service protège (d'une attaque par réseau) les paramètres de configuration des chiffreurs IP en confidentialité et en intégrité. Ces paramètres comprennent entre autres les paramètres de configuration réseau (données topologiques sur les réseaux privés).

3.3 Architecture de la TOE

3.3.1 Périmètre logique de la TOE

La Figure 5 présente un exemple d'architecture physique d'un réseau privé virtuel sur lequel la TOE sera évaluée.

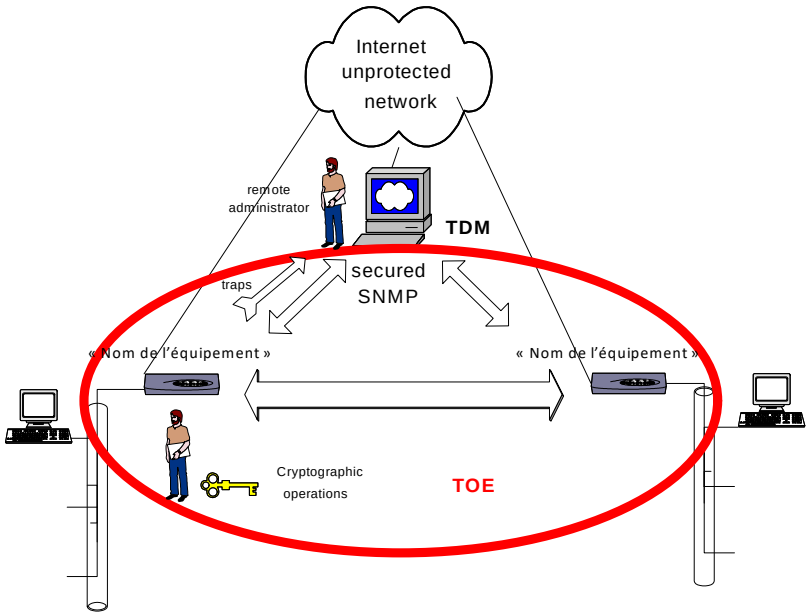


Figure 5 - Architecture physique et limites de la TOE

Sur la Figure 5, les chiffreurs IP sont directement connectés au réseau public et aux réseaux privés, mais ils peuvent être insérés à l'intérieur d'une structure globale d'interconnexion de réseaux IP.

Comme l'illustre la Figure 5, chaque chiffreur IP présente trois types d'interfaces externes logiques : Des interfaces vers le réseau privé, des interfaces vers le réseau public et une interface d'administration. L'exemple de la figure contient deux chiffreurs IP, nombre minimum nécessaire à l'établissement d'un lien VPN entre deux réseaux privés, mais le nombre n'est pas limité.

3.3.2 Rôles

Les rôles suivants sont définis dans la gestion du chiffreur :

- Administrateur ;
- Administrateur des paramètres réseau initiaux ;
- Administrateur de la personnalisation du chiffreur ;
- Auditeur.

3.3.2.1 Rôle Administrateur

Le rôle Administrateur a plusieurs fonctions :

- Gestion des politiques de sécurité du chiffreur (station TDM);
- Création des éléments de personnalisation du chiffreur (station SPC) ;
- Gestion des paramètres d'audit et de supervision du chiffreur (station TDM) ;
- Dépersonnalisation à distance du chiffreur (station TDM)

3.3.2.1.1 Gestion des politiques de sécurité du chiffreur

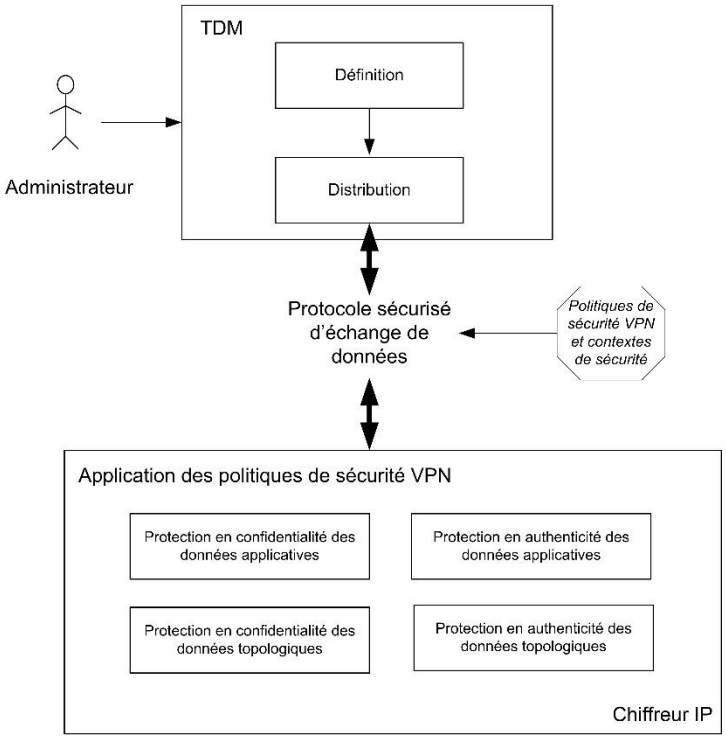


Figure 6 - Gestion des politiques de sécurité

Cette fonction nécessite une authentification sur la station TDM (donc hors TOE). Cette authentification est réalisée par mot de passe géré par le HSMv Proteccio associé au TDM.

Ce rôle a aussi la responsabilité de la mise à jour logicielle à distance des équipements de chiffrement.

3.3.2.1.2 Création des éléments de personnalisation du chiffreur

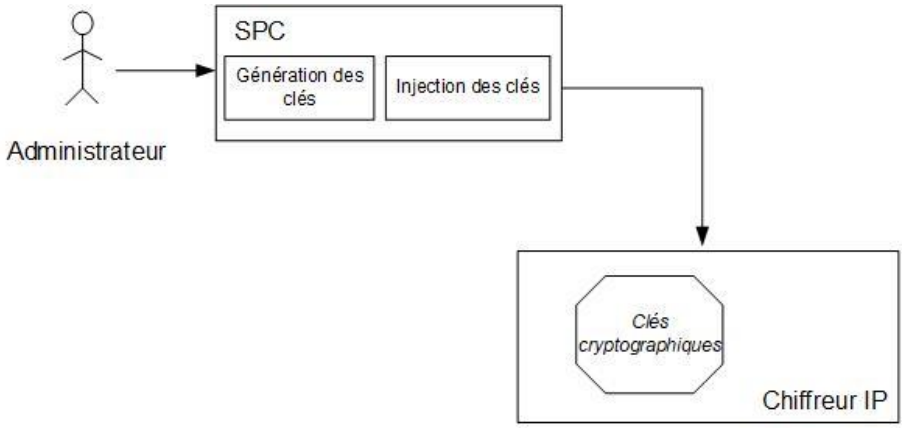


Figure 7 - Gestion des clés cryptographiques

Cette fonction nécessite une authentification sur la station SPC (donc hors TOE). Cette authentification est réalisée par mot de passe géré par le HSMv Proteccio associé au SPC.

3.3.2.1.3 Gestion des paramètres d'audit et de supervision du chiffreur

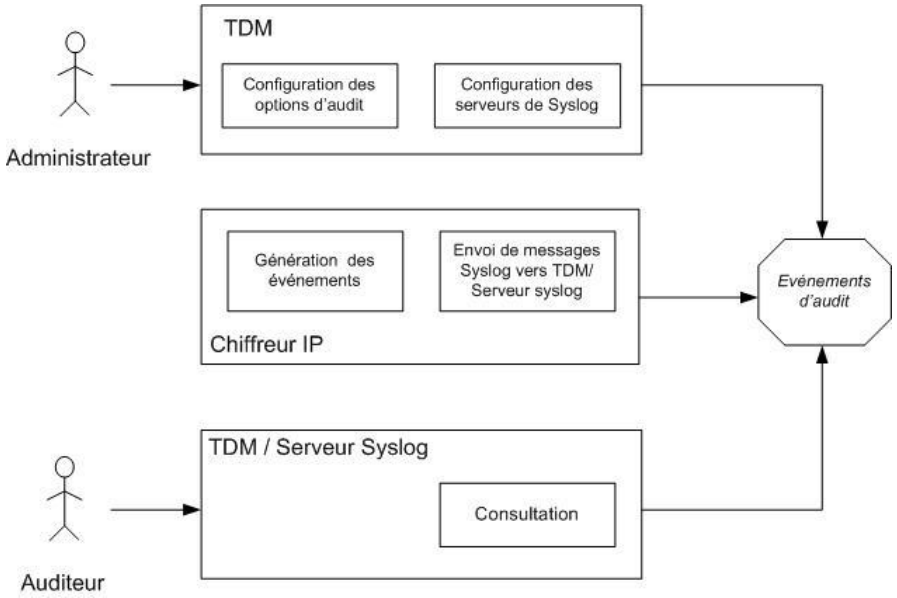


Figure 8 - Gestion de l'audit

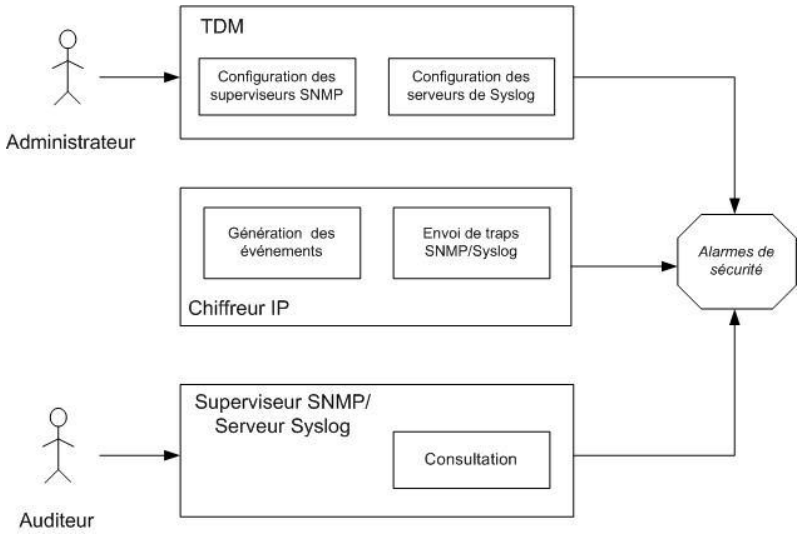


Figure 9 - Supervision de la TOE

Cette fonction nécessite une authentification sur la station TDM (donc hors TOE). Cette authentification est réalisée par mot de passe géré par le HSMv Proteccio associé au TDM.

3.3.2.1.4 Dépersonnalisation à distance du chiffreur

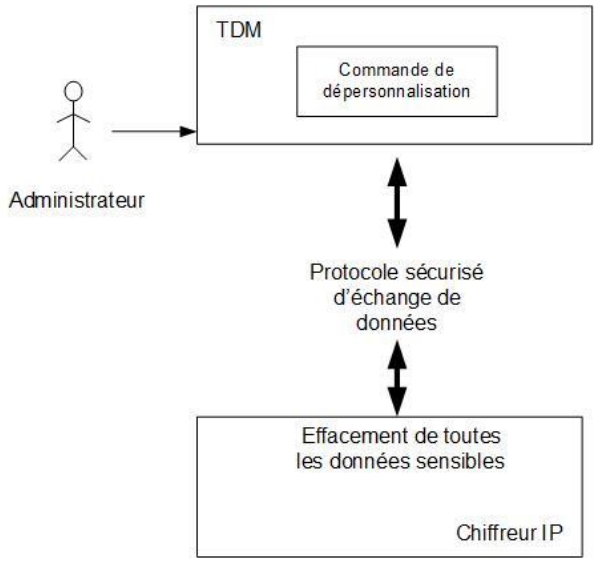


Figure 10 - Dépersonnalisation à distance de la TOE

Cette fonction nécessite une authentification sur la station TDM (donc hors TOE). Cette authentification est réalisée par mot de passe géré par le HSMv Proteccio associé au TDM.

3.3.2.2 Rôle Administrateur des paramètres réseau initiaux

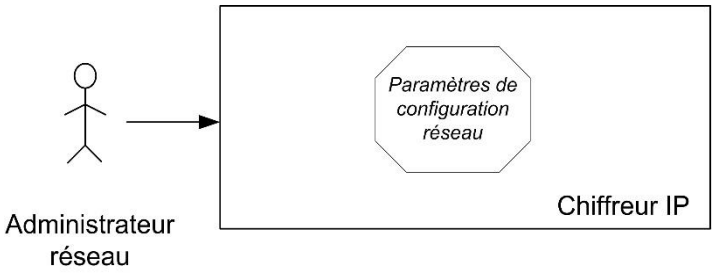


Figure 11 - Configuration réseau initiale des chiffreurs IP

Cette fonction est réalisée localement sur le chiffreur par l'application locale d'administration. L'accès à cette fonction est protégé par mot de passe.

3.3.2.3 Rôle Personnalisation du chiffreur

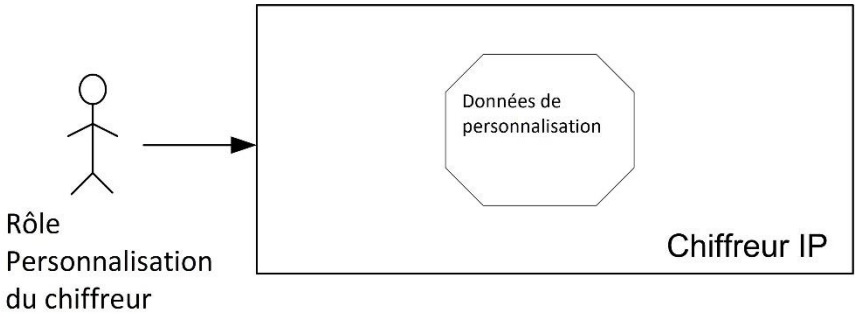


Figure 12 - Personnalisation du chiffreur

Cette opération est réalisée localement sur le chiffreur par l'application locale d'administration. Ce rôle nécessite la connaissance du mot de passe de protection des données de personnalisation.

3.3.2.4 Rôle Auditeur

3.3.2.4.1 Auditeur des événements du chiffreur

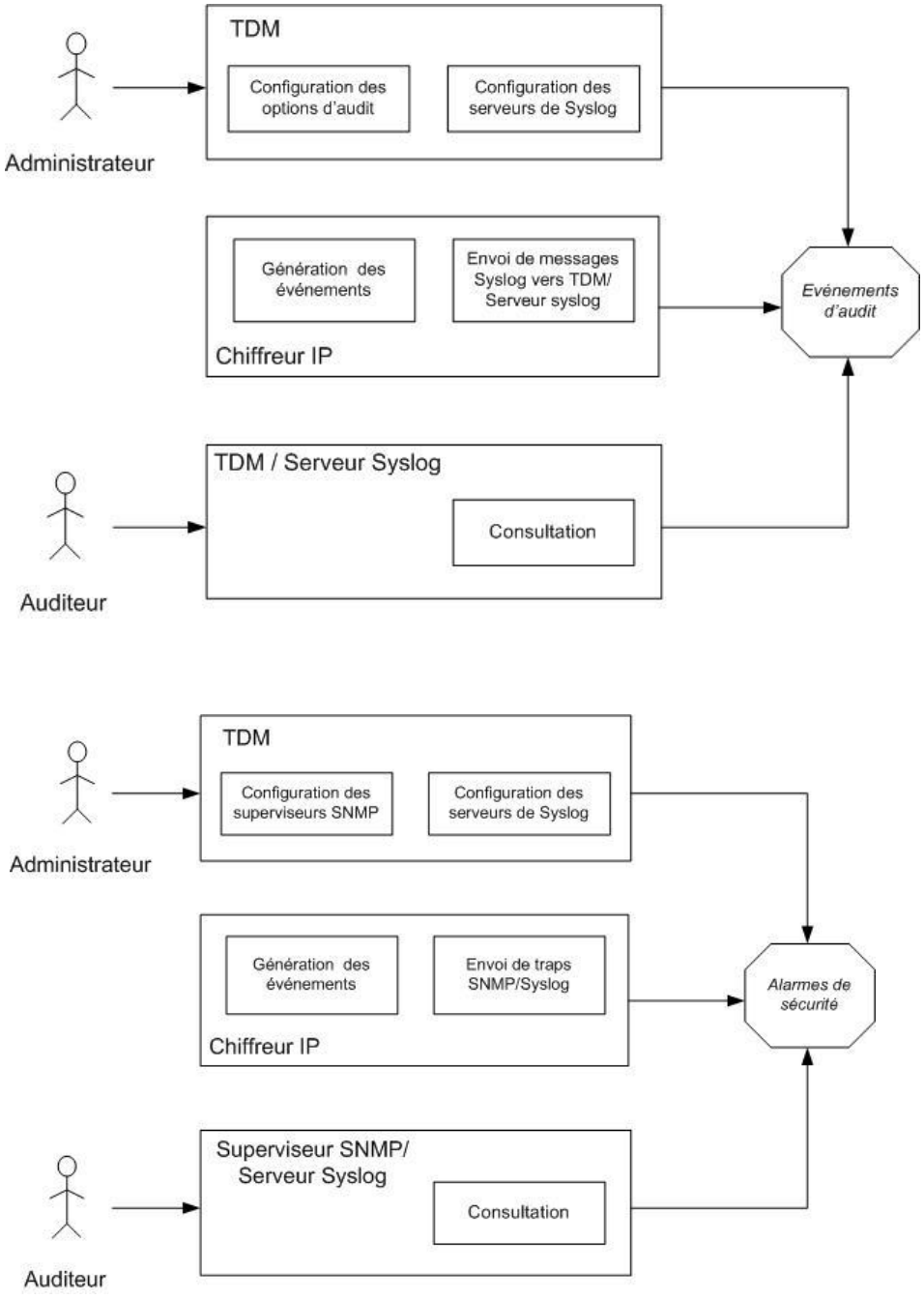


Figure 13 - Supervision de la TOE

Le superviseur SNMP et le serveur syslog ne sont pas fournis par Trustway. L'authentification de ce rôle n'est donc pas assurée par la TOE.

3.3.2.4.2 Auditeur des événements de l'application TDM

Figure 14 - Audit événements TDM

Cette fonction nécessite une authentification Windows sur la station TDM (donc hors TOE).

3.3.2.4.3 Auditeur des alarmes du chiffreur

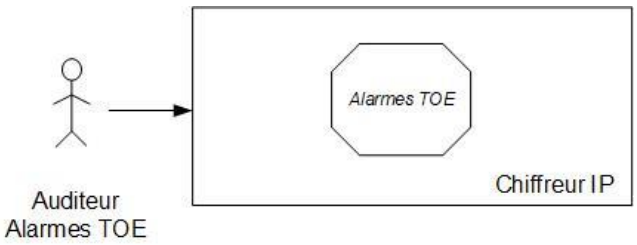


Figure 15 - Audit alarmes TOE

Cette fonction est réalisée localement sur le chiffreur par l'application locale d'administration. L'accès à cette fonction est protégé par mot de passe.

3.4 Cycle de vie

3.4.1 Personnalisation

Les clés maitre sont créées sur le SPC et injectées dans la Proteccio du TDM pour pouvoir être utilisées par l'application SPC ou TDM. Certaines clés issues des clés maitres sont positionnées dans la clé USB de personnalisation pour être injectées dans le chiffreur. La clé USB est protégée en confidentialité et intégrité (Cf §7.1.5).

La création de la clé USB de personnalisation est réalisée sous le rôle « Création des éléments de personnalisation du chiffreur » (Cf .3.3.2.1.2) et l'injection des secrets est réalisée sous la rôle « Personnalisation du chiffreur » (Cf 3.3.2.3).

Après cette phase de personnalisation, le matériel peut être introduit dans le réseau pour établir le dialogue avec le TDM qui partage les mêmes secrets issus des clés maitre utilisés pour distribuer les clés cryptographiques.

Dans la phase suivante, la configuration IP initiale est chargée dans l'équipement (via le port console locale par l'administrateur des paramètres réseau initiaux) et, après l'activation du CIK par le TDM, le matériel entre dans l'état attente d'enregistrement par le TDM. L'enregistrement est effectué sous le contrôle de l'administrateur du TDM et est destiné à injecter en toute sécurité les secrets partagés (clés de base) utilisés par le dialogue administratif sécurisé.

L'équipement IP Protect est alors prêt à recevoir en toute sécurité la politique de sécurité définie par l'administrateur sur le TDM et enfin communiquer conformément à cette politique.

3.4.2 Diffusion des versions logiciel

Le chiffreur est livré avec le logiciel installé par la production (lors de la production usine du chiffreur).

Les nouvelles versions du logiciel sont livrées au client sous forme d'un fichier .iso par le support niveau 2 :

- Par le service SOL (Software On Line) aux clients identifiés possédant un contrat de maintenance. Ce service est géré par le gestionnaire SOL qui fournit un identifiant et un mot de passe uniquement à ces clients
- Ponctuellement (et rarement en cas de problème administratif ou technique) par un accès à un serveur de téléchargement (Bull Upload Center) protégé par un jeton à usage unique envoyé par mail et utilisable dans un temps très court

Un BLL (Bulletin de Livraison Logiciel) est associé à chaque version logicielle qui décrit :

- Les corrections ;
- Les améliorations ;
- Les nouvelles fonctionnalités ;
- Les dépendances avec les autres logiciels du système (TDM, SPC, …).

La documentation utilisateur peut être téléchargée sur le service SOL ou est disponible sur le CDRom de l'application TDM.

La version logicielle d'un chiffreur est monolithique et contient tous les composants logiciels intégrés. Il n'est pas possible de mettre à jour un composant logiciel indépendamment des autres.

L'intégrité du logiciel est vérifiée lors de la mise à jour et à chaque démarrage du chiffreur.

3.5 Gestion de la sécurité

3.5.1 Topologie réseau

Le chiffreur IP Protect est orienté : il divise la topologie d'un réseau en un réseau fiable (sûr et / ou protégé) et un réseau peu fiable de la façon suivante (voir Figure 16~~Figure 15~~) :

- Interfaces A (Rouge/Clair): réseau fiable (trafic non sécurisé)
- Interfaces B (Noir/Chiffré): réseau non fiable (trafic sécurisé)

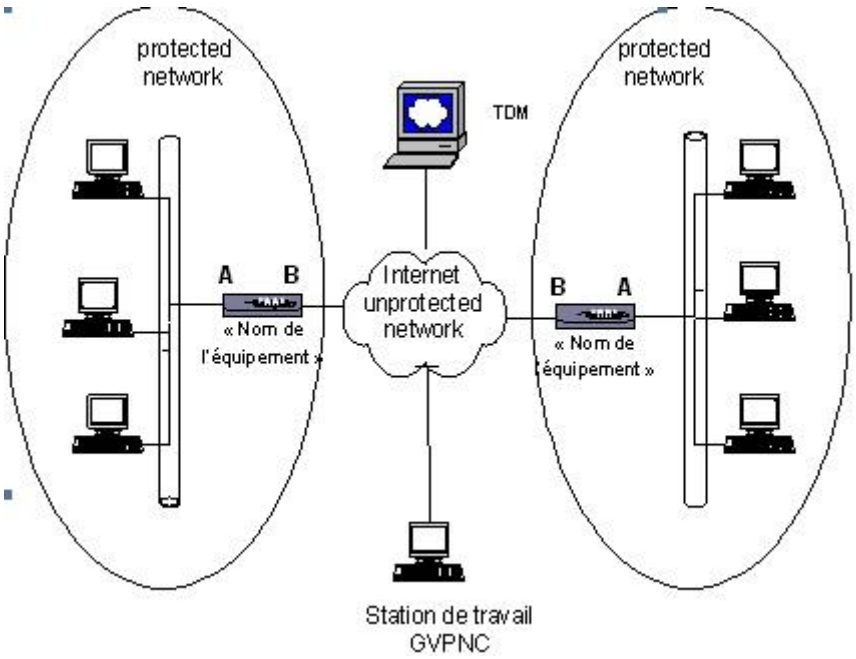


Figure 16 - Vue générale d'un réseau protégé par des chiffreurs IP Protect

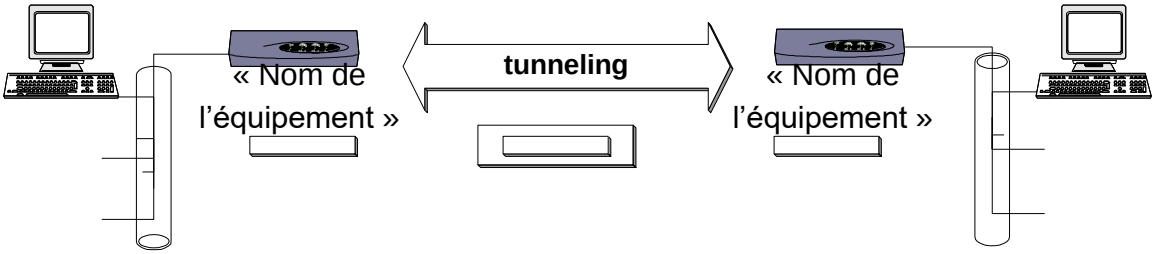
Le IP Protect communiquera en fonction de la politique de sécurité configurée par le TDM.

Les politiques de sécurité suivantes sont possibles:

Politique de sécurité	Description
drop	Données jetées
IPSec-Tunnel	IPSec tunnel (authentification et chiffrement)

Mode Drop : si, lorsqu'un paquet arrive il n'y a aucune règle qui s'applique (sur la source et la destination), alors le paquet est jeté.

Mode tunnel : tous les paquets sont encapsulés lorsque la politique de sécurité pour les correspondants est en mode IPSec Tunnel. Les paquets sont authentifiés et chiffrés.



3.5.2 Politique de sécurité

3.5.2.1 Communication entre IP Protect

La représentation administrative des politiques de sécurité est obtenue par la définition de domaines de sécurité sur le TDM (hors TOE).

Un domaine de sécurité est un espace virtuel qui regroupe un ensemble de systèmes autorisés à communiquer entre eux avec une politique de sécurité. Les systèmes sont des machines ou des sous-réseaux installés sur le réseau fiable (sur le côté d'un IP Protect où les données apparaissent en clair) c'est à dire sur une interface A.

La politique de sécurité associée aux flux syslog ou de supervision SNMP (interrogation de MIB2 ou réception de traps) est aussi définie dans des domaines de sécurité.

Pour la communication entre IP Protect, seuls les systèmes protégés par un IP Protect appartenant au même domaine de sécurité sont en mesure de communiquer entre eux. Ils communiquent dans le mode correspondant à la politique de sécurité du domaine concerné (seul le mode ESP Tunnel est autorisé en mode « Full IPsec DR »).

3.5.2.2 Communication avec des chiffreurs non gérés par le TDM

La politique de sécurité est définie de manière unitaire non graphique sur l'application TDM par le menu « Manage external devices configuration ».

3.5.3 Redondance

Plusieurs équipements IP Protect protégeant le même site peuvent être regroupés pour créer un équipement virtuel.

Un équipement unique, appelé le maître, est chargé de relayer le trafic. Les autres équipements restent en attente, prêts à intervenir. Lorsqu'un problème se produit qui rend le maître non opérationnel, les autres équipements choisissent un nouveau maître chargé de relayer le trafic. Le processus d'élection du nouveau maitre n'a pas d'effet sur les autres éléments du réseau.

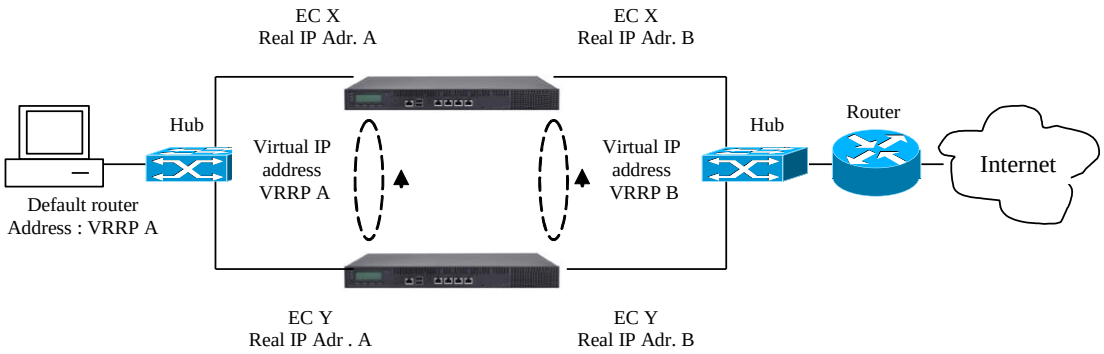


Figure 17 - Vue générale d'un réseau implémentant VRRP

Les équipements IP Protect appartenant à un groupe redondant mettent en œuvre un mécanisme conforme au protocole VRRP (RFC3768: **V**irtual **R**outer **R**edundancy **P**rotocol) sur chaque interface. Une adresse IP virtuelle VRRP est alors définie sur chaque interface de l'équipement : les autres équipements du réseau (routeurs, systèmes d'extrémité) sont configurés pour utiliser ces adresses virtuelles. En outre, les 2 instances VRRP d'un équipement redondant sont couplées pour basculer d'une manière cohérente l'adresse IP virtuelle de chaque interface. L'équipement maître est le matériel qui possède les deux adresses IP virtuelles à un moment donné.

Les stations d'administration Trustway (TDM) continuent à adresser chacun des équipements d'un groupe de redondance avec les adresses IP réelles.

3.5.4 Marquage QoS

Les équipements IP Protect permettent de copier le champ QoS de la trame initiale dans le champ QoS de la trame IPSec, ou de positionner ce champ indépendamment de la trame originale.

3.5.4.1 Champ DSCP

Les équipements IP Protect permettent de marquer les trames chiffrées en positionnant le champ DSCP [RFC 2474: définition du champ services différenciés (champ DS) dans les en-têtes IPv4 et IPv6].

Il est possible avec le TDM de positionner n'importe quelle valeur dans le champ DSCP de la trame émise IPSec. Grâce à cette fonctionnalité, le réseau va appliquer un traitement prioritaire spécifique basé sur la valeur de marquage.

Le marquage des trames peut être défini par :

- Adresses IP source et destination / masque d'adresse ;
- Port ;
- Protocole IP.

Ce marquage peut aussi servir à positionner les adresses noires pour différencier le flux par adresse IP sur le réseau noir.

3.5.5 Relais DHCP

Les équipements IP Protect proposent la fonctionnalité de relais DHCP. Les réseaux sur le côté clair sécurisé qui sont dynamiquement configurés avec DHCP peuvent utiliser le chiffreur en tant que relais DHCP. Cela implique qu'aucune requête ni réponse DHCP ne sont émises sur le réseau non sécurisé afin de ne pas révéler les adresses des équipements sur le côté sécurisé.

3.5.6 Tunnelisation (Tunneling) entre IP Protect

Le IP Protect implémente le protocole IPSec en mode ESP tunnel.

Ce mode est compatible (Cf Tableau des exigences supportées du référentiel IPSec DR de l'ANSSI) avec le document **Note Crypto Référentiel IPsec DR Profil de Protection « Chiffreur IP »** émis par l'ANSSI.

Les tunnels établis en ESP Tunnel entre les divers équipements (IP Protect ou station de travail GVPNC) mettent en œuvre un chiffrement en mode AES-GCM (clés de 256 bits et ICV de 16 octets) qui assure la sécurité et l'intégrité du flux de données. L'anti-rejeu sera réalisé uniquement en ESN (Extended Sequence Number).

Les contextes de sécurité (SA : Security Association) sont négociés par le protocole IKEv2 avec les algorithmes cryptographiques suivants :

- Confidentialité/Intégrité : AES-GCM (clés de 256 bits et ICV de 16 octets) ;
- PRF : PRF_HMAC_SHA2_256 ;
- Authentification : ECDSA sur secp256r1 avec SHA256 ;
- Diffie-Hellman DH19(secp256r1).

La validité du certificat envoyé par le chiffreur homologue est contrôlée par la chaine de certification et les CRL téléchargés à partir du TDM ou par le protocole OCSP.

3.5.7 Tunnelisation (Tunneling) avec des chiffreurs non gérés par le TDM

Le chiffreur IP Protect permet aussi la communication en mode ESP Tunnel avec des équipements non gérés par le TDM.

Cela permet notamment la mise en œuvre de mécanismes cryptographiques conformes aux exigences IPSec DR ANSSI (Cf **ANSSI : Note Crypto Référentiel IPsec DR Profil de Protection « Chiffreur IP »**) mais non utilisés pour la communication entre chiffreurs IP Protect :

- ESP
    - Chiffrement IKE AES-CTR 256bits ;
    - Intégrité HMAC_SHA2_256_128.

- IKE
    - Authentification IKE ECDSA BrainpoolP256r1 ;
    - Authentification IKE ECSDSA secp256r1 avec SHA256 ;
    - Authentification IKE ECSDSA BrainpoolP256r1 ;
    - Diffie-Hellman DH28(BrainpoolP256r1) ;
    - Chiffrement ESP AES-CTR 256bits ;
    - Intégrité HMAC_SHA2_256_128.

La validité du certificat envoyé par le chiffreur homologue est contrôlée par la chaine de certification et les CRL téléchargés à partir du TDM ou par le protocole OCSP.

3.5.8 Support du VLAN

Le Trustway IP Protect supporte la fonctionnalité de VLAN (Virtual LAN) uniquement sur ses interfaces A (rouges/claires).

Les VLAN permettent :

- D'améliorer la gestion du réseau ;
- D'optimiser la bande passante ;
- De séparer les flux ;
- De réduire la taille d'un domaine de broadcast.

3.5.9 Clés de session pour la sécurisation des données

Les clés sont négociées à chaque établissement de VPN. Les clés sont aussi renégociées à une fréquence très inférieure par rapport à la cryptopériode (8 heures pour les SA ESP et 24 heures pour les SA IKE pour les communications entre chiffreurs).

3.6 Evènements/Alarmes des IP Protect

3.6.1 Evénements du système IP Protect

3.6.1.1 Audit des flux

IP Protect émet des événements indiquant la cause des flux rejetés sous forme de traps SNMP ou de syslog.

Les événements sont protégés par un tunnel ESP lors de leur envoi vers les superviseurs SNMP ou les serveurs syslog.

Ces événements sont visualisables sur un superviseur SNMP ou un serveur syslog (hors TOE) par un auditeur (rôle Auditeur (Evenements_TOE)).

Un seuil et une période sont configurés par le TDM pour l'envoi de certains types d 'événements (l'événement démarrage du chiffreur est, par exemple, systématiquement envoyé).

Exemple d'événements générés :

Evénements	Signification
Démarrage du chiffreur	Démarrage IP Protect
Accès à la MIB interdit	Tentative d'accès à la MIB par un administrateur SNMP non autorisé
Trames en overflow AES	Trames détruites par saturation de la cryptographie.
Trames IP droppées	Trames détruites par la politique de sécurité
Erreur d'authentification IPSec	Trames détruites par erreur d'authentification IPSec.
Erreurs d'authentification dialogue administratif	Erreurs d'authentification entre le TDM et IP Protect .
Requêtes échouées dialogue administratif	Requêtes ayant échouée car tentative d'accès non autorisé ou timeout.
Erreurs d'intégrité dialogue administratif	Erreur de signature dans les trames échangées entre IP Protect et le TDM.

3.6.1.2 Audit d'administration

L'application TDM (hors TOE), trace les opérations d'administration dans un journal visualisable sur la station TDM.

La visualisation de ce journal est réalisable sous le rôle Auditeur (TDM).

3.6.1.3 Supervision SNMP des IP Protect

Le TDM offre la possibilité de déclarer des machines en tant que superviseurs de réseau pour un IP Protect, et de définir la politique de sécurité appliquée aux flux de supervision (le seul mode autorisé est ESP Tunnel). Ces superviseurs reçoivent les traps SNMP envoyés par le IP Protect et peuvent interroger les parties « system » et « interfaces » de la MIB2 de cet équipement.

3.6.2 Alarmes

IP Protect génère des alarmes en cas de problèmes sérieux relatifs à le sécurité ou l'opérabilité du chiffreur.

Le chiffreur effectue lui-même les opérations nécessaires à sa sécurité (redémarrage, ...).Ces alarmes sont consultables par l'application locale d'administration sous le rôle Auditeur (Alarmes_TOE).

Chapitre 4.Définition du problème de sécurité

4.1 Biens

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

4.1.1 Biens protégés par la TOE

Les biens du système d'information sont protégés par la TOE comme indiqué dans les politiques de sécurité VPN.

D.DONNEES_APPLICATIVES

Les données applicatives sont les données qui transitent d'un réseau privé à un autre par l'intermédiaire des chiffreurs IP. Elles sont contenues dans la charge utile des paquets IP routés jusqu'aux chiffreurs et reçus et envoyés par ces chiffreurs. Ces données peuvent être stockées temporairement dans les chiffreurs IP pour pouvoir les traiter (i.e., appliquer les services de sécurité) avant de les envoyer sur le réseau privé ou public.

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

D.INFO_TOPOLOGIE

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

Protection : confidentialité, intégrité et authenticité.

4.1.2 Biens sensibles de la TOE

D.POLITIQUES_VPN

Les politiques de sécurité VPN définissent les traitements (filtrage implicite et services de sécurité) à effectuer sur les données reçues et envoyées par chaque chiffreur IP.

Ce bien comporte aussi les contextes de sécurité qui sont rattachés aux politiques de sécurité. Chaque contexte de sécurité contient tous les paramètres de sécurité nécessaires à l'application de la politique de sécurité VPN à laquelle il est associé. Ces paramètres sont définis par l'administrateur de sécurité TDM.

Protection :

- Intégrité des politiques (et de leur contextes) stockées sur les chiffreurs IP Protect,
- Confidentialité.

D.PARAM_CONFIG

Les paramètres de configuration des chiffreurs IP comprennent entre autres:

- Les adresses IP internes aux réseaux privés et les tables de routage (configuration réseau).

Protection : confidentialité et intégrité.

D.CLES_CRYPTO

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

- Les clés de session.
- Les clés utilisées par les services de sécurité appliqués par les politiques de sécurité VPN.
- Les clés pour protéger les politiques de sécurité VPN lors de leur stockage.
- Les clés pour protéger l'injection de clés cryptographiques dans les chiffreurs IP.

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

D.AUDIT

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

Protection : intégrité.

D.ALARMES

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

Protection : intégrité.

D.LOGICIELS

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

Protection : intégrité.

D.BASE_TEMPS

Base de temps fiable de la TOE.

Protection : intégrité.

4.2 Menaces

La politique de qualification au niveau standard s'applique à des produits grand public assurant la protection d'informations sensibles non classifiées de défense. Par conséquent, un certain nombre de menaces ne seront pas prises en compte dans la suite comme par exemple, le vol de l'équipement (qui doit être détecté par des mesures organisationnelles) ou le déni de service.

Les menaces présentes dans cette section sont uniquement des menaces qui portent atteinte à la sécurité de la TOE et pas aux services rendus par la TOE, car tous les éléments de l'environnement concernant les services rendus par la TOE sont considérés comme des politiques de sécurité organisationnelle.

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

Dans la suite de ce chapitre, on entend par attaquant interne une personne malveillante ayant la capacité d'accéder aux composants matériels internes au chiffreur. Il s'agit donc d'un « utilisateur » (au sens où il est autorisé à accéder physiquement au chiffreur) malveillant avec des connaissances lui permettant de piéger les composants matériels internes de l'équipement.

Dans la suite de ce chapitre, on entend par attaquant externe une personne malveillante pouvant par modification de données externes à destination de l'équipement mettre œuvre les menaces. Il s'agit donc d'une personne ayant accès aux interfaces externes de l'équipement. Dans le cas d'une attaque par le réseau, l'accès direct au chiffreur par un attaquant n'est pas nécessaire. Une précision dans ce sens est donnée pour chaque attaque externe dans chaque menace.

4.2.1 Menaces portant sur les politiques de sécurité VPN et leurs contextes

T.MODIFICATION_POL

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

Attaquant interne à la TOE:

- modification des données sur le disque

Attaquant externe à la TOE:

- injection de données de personnalisation falsifiées (rôle administrateur donc non considéré comme attaquant)
- modification de la politique de sécurité sur le réseau lors de la configuration depuis le TDM (attaque réseau)
- hors TOE: usurpation du rôle Administrateur sur le TDM (rôle administrateur donc non considéré comme attaquant)

Bien menacé : D.POLITIQUES_VPN.

T.DIVULGATION_POL

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

Attaquant interne à la TOE:

- lecture des données sur le disque

Attaquant externe à la TOE:

- lecture des données de personnalisation (rôle administrateur donc non considéré comme attaquant)
- lecture de la politique de sécurité sur le réseau lors de la configuration depuis le TDM (attaque réseau)
- hors TOE: usurpation du rôle Administrateur sur le TDM (rôle administrateur donc non considéré comme attaquant)

Bien menacé : D.POLITIQUES_VPN.

T.COHERENCE_POL

Un attaquant modifie la politique de sécurité VPN appliquée au niveau d'un sous-réseau IP, qui est donc différente de celle définie par l'administrateur de sécurité pour ce sous-réseau.

Attaquant interne à la TOE:

- modification des données sur le disque

Attaquant externe à la TOE:

- injection de données de personnalisation falsifiées (rôle administrateur donc non considéré comme attaquant)
- modification de la politique de sécurité sur le réseau lors de la configuration depuis le TDM (attaque réseau)
- hors TOE: usurpation du rôle Administrateur sur le TDM (rôle administrateur donc non considéré comme attaquant)

Bien menacé : D.POLITIQUES_VPN.

4.2.2 Menaces portant sur la configuration

T.MODIFICATION_PARAM

Un attaquant modifie illégalement des paramètres de configuration.

Attaquant interne à la TOE:

- modification des données sur le disque

Attaquant externe à la TOE:

- injection de données de personnalisation falsifiées (rôle administrateur donc non considéré comme attaquant)
- modification des paramètres sur le réseau lors de la configuration depuis le TDM (attaque réseau)
- hors TOE: usurpation du rôle Administrateur sur le TDM (rôle administrateur donc non considéré comme attaquant)

Bien menacé : D.PARAM_CONFIG.

T.DIVULGATION_PARAM

Un attaquant récupère de manière non autorisée des paramètres de configuration.

Attaquant interne à la TOE:

- lecture des données sur le disque

Attaquant externe à la TOE:

- lecture des données de personnalisation (rôle administrateur donc non considéré comme attaquant)
- lecture des paramètres sur le réseau lors de la configuration depuis le TDM (attaque réseau)
- hors TOE: usurpation du rôle Administrateur sur le TDM (rôle administrateur donc non considéré comme attaquant)

Bien menacé : D.PARAM_CONFIG.

4.2.3 Menaces portant sur la gestion des clés

T.MODIFICATION_CLES

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

Attaquant interne à la TOE:

- modification des clés cryptographiques sur le disque ou dans le TPM

Attaquant externe à la TOE:

- injection de données (clés) de personnalisation falsifiées (rôle administrateur donc non considéré comme attaquant)

- modification des clés sur le réseau lors de la configuration depuis le TDM (attaque réseau)

Bien menacé : D.CLES_CRYPTO.

T.DIVULGATION_CLES

Un attaquant récupère illégalement des clés cryptographiques.

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

Attaquant interne à la TOE:

- lecture des clés cryptographiques sur le disque ou dans le TPM

Attaquant externe à la TOE:

- lecture de données (clés) de personnalisation (rôle administrateur donc non considéré comme attaquant)
- lecture des clés sur le réseau lors de la configuration depuis le TDM (attaque réseau)

4.2.4 Menaces portant sur l'audit

T.MODIFICATION_AUDIT

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

Attaquant externe à la TOE :

- Destruction sur le réseau des messages (Traps SNMP ou syslog) émis par la TOE et sécurisés par ESP Tunnel (attaque réseau)
- Hors TOE : usurpation du rôle Auditeur (Evenements_TOE) (nécessite l'accès au serveur syslog ou au superviseur SNMP).
- Hors TOE : usurpation du rôle Auditeur (TDM) (nécessite un accès Windows sur le TDM)

Bien menacé : D.AUDIT.

T.MODIFICATION_ALARME

Un attaquant modifie ou supprime illégalement les alarmes de sécurité lorsqu'elles sont remontées par la TOE à l'administrateur de sécurité.

Attaquant interne à la TOE :

- modification des alarmes sur le disque

Bien menacé : D.ALARMES.

T.BASE_TEMPS

Un attaquant perturbe ou altère la base de temps de la TOE dans le but de falsifier les données d'audit.

Attaquant interne à la TOE :

- modification de l'heure sur la TOE pendant son fonctionnement

Attaquant externe à la TOE :

- hors TOE : modification de l'heure sur le TDM (rôle administrateur donc non considéré comme attaquant)
- modification de l'heure envoyée par le TDM dans le flux sécurisé CIK (attaque réseau)

Bien menacé : D.BASE_TEMPS.

4.2.5 Menaces portant sur l'administration

T.USURPATION_ADMIN

Un attaquant usurpe l'identité d'un administrateur et effectue des opérations d'administration sur les chiffreurs IP.

Attaquant externe à la TOE :

- hors TOE (station TDM) : usurpation du rôle Administrateur TDM (protection par mot de passe Windows et mot de passe application TDM) (rôle administrateur donc non considéré comme attaquant)
- hors TOE (station SPC) : usurpation du rôle Administrateur SPC (protection par mot de passe Windows et mot de passe application SPC) (rôle administrateur donc non considéré comme attaquant)
- usurpation du rôle Administrateur local (protection par mot de passe) (rôle administrateur donc non considéré comme attaquant)

Biens menacés: D.POLITIQUES_VPN, D.CLES_CRYPTO, D.AUDIT, D.PARAM_CONFIG.

T.REJEU_ADMIN

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

Attaquant externe à la TOE:

- rejeu de la politique de sécurité ou des paramètres sur le réseau suite une capture lors de la configuration depuis le TDM (attaque réseau)

Biens menacés : D.POLITIQUES_VPN, D.CLES_CRYPTO, D.AUDIT, D.PARAM_CONFIG.

T.BIENS_INDISPONIBLES

Un attaquant prend connaissance, par accès direct à la TOE, des biens sensibles d'un chiffreur IP (clés, politiques de sécurité VPN,...) lors d'un changement de contexte d'utilisation (affectation du chiffreur IP à un nouveau réseau, maintenance,...).

Attaquant interne à la TOE:

- invalidation de la dépersonnalisation de l'équipement lors d'un changement de contexte d'utilisation

Biens menacés : D.POLITIQUES_VPN, D.PARAM_CONFIG, D.CLES_CRYPTO, D.AUDIT et D.ALARMES.

4.2.6 Menaces portant sur les données applicatives

T.DIVULGATION_DONNEES_APPLICATIVES

Un attaquant prend connaissance des données applicatives.

Attaquant externe à la TOE:

- Déchiffrement des paquets sécurisés par ESP Tunnel (attaque réseau)

Biens menacés: D.DONNEES_APPLICATIVES.

T.MODIFICATION_DONNEES_APPLICATIVES

Un attaquant modifie les données applicatives.

Attaquant externe à la TOE:

- Altération des paquets sécurisés par ESP Tunnel (attaque réseau)

Biens menacés: D.DONNEES_APPLICATIVES.

T.REJEU_DONNEES_APPLICATIVES

Un attaquant rejoue les données applicatives.

Attaquant externe à la TOE:

- Rejeu des paquets sécurisés par ESP Tunnel (attaque réseau)

Biens menacés: D.DONNEES_APPLICATIVES.

T.DIVULGATION_INFO_TOPOLOGIE

Un attaquant prend connaissance des informations de topologie des réseaux privés (adresses IP source et destination) qui se trouvent dans les en-têtes de paquets IP.

Attaquant externe à la TOE:

- Déchiffrement des paquets sécurisés par ESP Tunnel (attaque réseau)

Biens menacés: D.INFO_TOPOLOGIE.

T.MODIFICATION_INFO_TOPOLOGIE

Un attaquant modifie les informations de topologie des réseaux privés (adresses IP source et destination) qui se trouvent dans les en-têtes de paquets IP.

Attaquant externe à la TOE:

- Altération des paquets sécurisés par ESP Tunnel (attaque réseau)

Biens menacés: D.INFO_TOPOLOGIE.

4.2.7 Menaces portant sur les logiciels de la TOE

T.MODIFICATION_LOGICIELS

Un attaquant modifie le logiciel du chiffreur.

Attaquant interne à la TOE:

- Modification du logiciel sur le disque

Biens menacés: D.LOGICIELS.

4.3 Politiques de sécurité organisationnelles (OSP)

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

OSP.SERVICES_RENDUS

La TOE doit appliquer les politiques de sécurité VPN définies par l'administrateur de sécurité.

Elle doit aussi fournir tous les services de sécurité nécessaires pour appliquer les protections spécifiées dans ces politiques:

- Protection en confidentialité des données applicatives,
- Protection en authenticité des données applicatives,
- Protection anti-rejeu des données applicatives,
- Protection en confidentialité des données topologiques,
- Protection en authenticité des données topologiques.

De plus, la TOE doit permettre de cloisonner des flux IP pour faire communiquer des sous-réseaux (de réseaux privés) et appliquer une politique de sécurité sur chaque lien de communication entre sous-réseaux IP.

OSP.CRYPTO

Le référentiel de cryptographie de l'ANSSI ([5]) doit être suivi pour la gestion des clés (génération, destruction, consommation et distribution) et les fonctions de cryptographie utilisées dans la TOE, pour le niveau de résistance standard.

OSP.SUPERVISION

La TOE doit permettre à l'administrateur TDM (§ 3.3.2.1.1) ou à l'auditeur des événements du chiffreur (§ 3.3.2.4.1) de consulter l'état opérationnel de chaque chiffreur IP.

4.4 Hypothèses

4.4.1 Hypothèses sur l'usage attendu de la TOE

A.AUDIT

Il est supposé que l'auditeur consulte régulièrement les événements d'audit générés par la TOE. Les événements ne sont pas stockés localement et leur consultation est réalisée sur le serveur syslog. L'envoi de ces événements est protégé par un tunnel ESP et sont numérotés afin de détecter une perte d'événement.

A.ALARME

Il est supposé que l'auditeur des alarmes du chiffreur (Cf 3.3.2.4.3) analyse et traite les alarmes de sécurité générées et remontées par la TOE. Les actions liées à ces alarmes sont prises par le chiffreur lui-même et sont consultables par l'application locale. Une alarme sérieuse provoque un redémarrage de l'équipement avec émission d'un événement indiquant qu'une alarme s'est produite.

4.4.2 Hypothèses sur l'environnement d'utilisation de la TOE

A.ADMIN

Les administrateurs (Cf 3.3.2.1) sont des personnes non hostiles et compétentes qui disposent des moyens nécessaires à la réalisation de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration. Les mots de passe Windows de la session utilisateur permettant l'ouverture des applications TDM et SPC respectent les règles énoncées dans le document [6].

A.LOCAL

Les équipements contenant les services nécessaires à la TOE (chiffreurs IP (TOE) et équipements d'administration TDM et SPC (hors TOE), ainsi que tous supports contenant les biens sensibles de la TOE (papier, CDRom, clés USB de personnalisation créés par le SPC...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs (Cf 3.3.2.1). Cependant, les équipements contenant les services de la TOE peuvent ne pas se trouver dans des locaux sécurisés s'ils ne contiennent pas de biens sensibles: par exemple dans les cas de changement de contexte d'utilisation d'un chiffreur IP.

A.MAITRISE_CONFIGURATION

Les administrateurs (Cf 3.3.2.1) disposent des moyens de contrôler la configuration matérielle et logicielle de la TOE (services et biens compris) par rapport à un état de référence, ou de la régénérer dans un état sûr.

A.CRYPTO

Les clés cryptographiques, générées à l'extérieur, qui sont injectées dans la TOE doivent avoir été générées en suivant les recommandations spécifiées dans le référentiel cryptographique de l'ANSSI [5] pour le niveau de résistance standard.
Les opérations cryptographiques réalisées sur le TDM ou le TAM par l'intermédiaire de la ressource cryptographique Proteccio suivent les recommandations spécifiées dans le référentiel cryptographique de l'ANSSI [5] pour le niveau de résistance standard.

Chapitre 5.Objectifs de sécurité

5.1 Objectifs de sécurité pour la TOE

5.1.1 Objectifs de sécurité sur les services rendus par la TOE

O.APPLICATION_POL

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

O.CONFIDENTIALITE_APPLI

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

O.AUTHENTICITE_APPLI

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

O.REJEU_APPLI

La TOE doit fournir des mécanismes pour protéger du rejeu les données applicatives qui transitent entre deux chiffreurs IP.

O.CONFIDENTIALITE_TOPO

La TOE doit fournir des mécanismes pour protéger en confidentialité les informations sur la topologie des réseaux privés contenues dans les paquets IP qui transitent entre deux chiffreurs IP.

O.AUTHENTICITE_TOPO

La TOE doit fournir des mécanismes pour protéger en authenticité les informations sur la topologie des réseaux privés contenues dans les paquets IP qui transitent entre deux chiffreurs IP.

O.CLOISONNEMENT_FLUX

La TOE doit permettre de cloisonner les réseaux IP interconnectés ensembles grâce aux chiffreurs IP, en permettant de créer un nouveau réseau IP étendu, superposé au réseau IP initial constitué de sous-réseaux IP. La TOE doit aussi permettre d'appliquer une politique de sécurité sur chaque lien de communication entre sous-réseaux IP.

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

5.1.2.1 Gestion des politiques de sécurité VPN

O.DEFINITION_POL

La TOE doit permettre seulement à l'administrateur TDM (Cf 3.3.2.1.1) de définir les politiques de sécurité VPN et leurs contextes de sécurité. La TOE doit aussi permettre de s'assurer qu'une négociation d'une partie de politique et de contexte entre deux chiffreurs IP conduit au choix d'une politique et d'un contexte conformes à la stratégie décidée par l'administrateur de sécurité.

O.PROTECTION_POL

La TOE doit contrôler l'accès (consultation, modification) aux politiques de sécurité VPN et à leurs contextes de sécurité qui est autorisé seulement aux administrateurs TDM (Cf 3.3.2.1.1).

O.AUTHENTIFICATION_MUTUELLE

La TOE doit fournir un mécanisme d'authentification mutuelle pour les chiffreurs IP qui communiquent entre eux et ainsi permettre de négocier dynamiquement les politiques de sécurité VPN et leurs contextes.

5.1.2.2 Gestion des clés cryptographiques

O.CRYPTO

La TOE doit implémenter les fonctions de cryptographie et gérer (générer, détruire, renouveler) les clés cryptographiques en accord avec le référentiel de cryptographie défini par l'ANSSI ([5]) pour le niveau de résistance standard.

O.ACCES_CLES

La TOE doit protéger l'accès aux clés cryptographiques.

O.INJECTION_CLES

La TOE doit protéger les clés en confidentialité (seulement pour les clés secrètes et privées) et en intégrité lors de leur injection sur les chiffreurs IP lors de la personnalisation de l'équipement (Cf §3.4.1) et pour la gestion du dialogue administratif sécurisé.

5.1.2.3 Configuration et supervision

O.PROTECTION_PARAM

La TOE doit protéger en confidentialité et intégrité les paramètres de configuration qui ne peuvent être accédés que par les rôles suivants :

- Configuration réseau initiale : Administrateur des paramètres réseau initiaux (§ 3.3.2.2) ;
- Données de personnalisation : Création des éléments de personnalisation du chiffreur (station SPC) (§ 3.3.2.1.2) ;
- Paramètres d'audit et de supervision du chiffreur: Gestion des paramètres d'audit et de supervision du chiffreur (§3.3.2.1.3).

O.SUPERVISION

La TOE doit permettre à l'administrateur TDM (§ 3.3.2.1.1) ou à l'auditeur des événements du chiffreur (§ 3.3.2.4.1) de consulter l'état opérationnel de chaque chiffreur IP.

O.IMPACT_SUPERVISION

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

5.1.2.4 Audit et alarme

O.AUDIT_VPN

La TOE doit tracer toutes les opérations effectuées par les chiffreurs IP relevant de la sécurité et concernant les communications sur les liens VPN. De plus, elle doit permettre seulement à un auditeur de consulter ce qui a été tracé.

O.AUDIT_ADMIN

Toutes les opérations effectuées par un administrateur sur les chiffreurs IP doivent être tracées. De plus, elle doit permettre seulement à l'auditeur TDM (Cf 3.3.2.4.2) de consulter ce qui a été tracé.

O.PROTECTION_AUDIT

La TOE doit garantir l'intégrité des événements d'audit qu'elle enregistre et doit permettre à un auditeur de détecter la perte d'événements d'audit (utilisation d'un compteur).

O.ALARMES

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

O.PROTECTION_ALARME

La TOE doit garantir l'intégrité des alarmes de sécurité qu'elle génère.

O.BASE_TEMPS

La TOE fournit une base de temps sur laquelle reposent les enregistrements d'audit et garantit sa fiabilité.

5.1.2.5 Administration

O.AUTHENTIFICATION_ADMIN

L'environnement de la TOE doit fournir des mécanismes d'identification et d'authentification localement ou à distance des différents administrateurs. Il doit aussi s'assurer que l'accès aux services de télé-administration est conditionné par une authentification préalable sur la station d'administration.

Administration locale

La TOE fournit un service d'administration locale permettant de :

- Consulter les alarmes ;
- Réinitialiser la TOE ;
- Entrer les paramètres réseau initiaux ;
- Personnaliser l'équipement.

Administration à distance

L'administration à distance (assurant notamment la configuration de la politique de sécurité VPN de la TOE) est réalisée depuis la station TDM.

O.COHERENCE_POL

La TOE doit garantir la cohérence des définitions des politiques de sécurité VPN (et de leurs contextes) avec les politiques appliquées sur chaque chiffreur IP lors de l'administration à distance.

O.DISTRIBUTION_POL

La TOE doit protéger en confidentialité et en authenticité les politiques de sécurité VPN et leurs contextes de sécurité qui transitent entre l'équipement contenant le logiciel permettant de les définir et les chiffreurs IP.

O.PROTECTION_REJEU_ADMIN

La TOE doit empêcher le rejeu d'une séquence d'envoi de données d'administration.

O.PROTECTION_FLUX_ADMIN

La TOE doit garantir l'authenticité et la confidentialité des flux d'administration à distance. La protection en confidentialité n'est pas systématiquement appliquée si les données passant dans le flux ne sont pas confidentielles telles que les clés publiques.

5.1.2.6 Protection des biens

O.BIENS_INDISPONIBLES

La TOE doit fournir une fonctionnalité qui permet de rendre indisponibles les biens sensibles d'un chiffreur IP préalablement à un changement de contexte d'utilisation: nouvelle affectation, maintenance. Cette fonctionnalité s'appelle dépersonnalisation dans la terminologie IP Protect.

O.INTEGRITE_LOGICIELS

La TOE doit fournir des mécanismes pour garantir l'intégrité de son logiciel.

5.2 Objectifs de sécurité pour l'environnement opérationnel

5.2.1 Administrateurs

OE.ADMIN

Les administrateurs doivent être formés aux tâches qu'ils ont à réaliser sur la TOE (Cf 3.3.2) :

- Administrateur :
    - Gestion des politiques de sécurité du chiffreur (station TDM);
    - Création des éléments de personnalisation du chiffreur (station SPC) ;
    - Gestion des paramètres d'audit et de supervision du chiffreur (station TDM) ;
    - Dépersonnalisation à distance du chiffreur (station TDM)
- Administrateur des paramètres réseau initiaux ;
- Administrateur de la personnalisation du chiffreur.

5.2.2 Cryptographie

OE.CRYPTO

Les clés cryptographiques, générées à l'extérieur, qui sont injectées dans la TOE doivent avoir été générées en suivant les recommandations spécifiées dans le référentiel cryptographique de l'ANSSI [5] pour le niveau de résistance standard.

5.2.3 Audit et alarme

OE.ANALYSE_AUDIT

L'auditeur doit régulièrement analyser les événements d'audit enregistrés par la TOE et agir en conséquence. Les événements ne sont pas stockés localement et leur consultation est réalisée sur le serveur syslog. L'envoi de ces événements est protégé par un tunnel ESP et sont numérotés afin de déterminer une perte d'événement.

OE.TRAITE_ALARME

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

5.2.4 Matériels et logiciels

OE.PROTECTION_LOCAL

L'environnement physique de la TOE, comprenant les équipements sur lesquels la TOE se trouvent, doit protéger la TOE. Ces équipements, ainsi que les supports contenant tout ou partie des biens sensibles de la TOE doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

Cependant, les équipements contenant les services de la TOE peuvent ne pas se trouver dans des locaux sécurisés s'ils ne contiennent pas de biens sensibles: par exemple dans les cas de changement de contexte d'utilisation d'un chiffreur IP.

OE.INTEGRITE_TOE

L'environnement de la TOE doit permettre de vérifier l'intégrité de la configuration matérielle et logicielle de la TOE.

Chapitre 6.Exigences de sécurité

6.1 Exigences de sécurité fonctionnelles

Toutes les exigences fonctionnelles pour la TOE sont extraites de la partie 2 des critères communs.

Les raffinements (« refinements ») sont en caractères italiques.

Les textes extraits des critères communs sont en caractère normaux.

Les attributions (« assignements ») et les sélections (« selections ») sont identifiées par des crochets.

Les itérations sont identifiées par le signe « / » pour différencier les exigences comme par exemple FDP_IFC.1/Enforcement_policy.

Dans les exigences, qui sont écrites en anglais, l'expression "chiffreur IP" a été traduite par "IP encrypter". Les autres traductions sont évidentes.

Dans les exigences, les deux termes suivants sont utilisés pour désigner un raffinement:

- Raffinement éditorial (terme défini dans [CC1]): raffinement dans lequel une modification mineure est faite sur un élément d'exigence, telle que la reformulation d'une phrase pour des raisons de respect de la grammaire anglaise. En aucun cas, cette modification ne doit changer la signification de l'exigence,
- Raffinement non éditorial: raffinement qui permet d'ajouter des précisions ou de limiter l'ensemble des implémentations acceptables pour un élément d'exigence.

6.1.1 Application des politiques de sécurité VPN

6.1.1.1 FDP_IFC.1/Enforcement_policy Subset information flow control

FDP_IFC.1.1/Enforcement_policy The TSF shall enforce **the VPN enforcement policy** on

- **Information: applicative and topologic data contained in IP packets.**
- **Subject: IP encrypter using a given VPN link**
- **Operations: sending and receiving operations that cause applicative and topologic data to flow through the IP encrypters to and from private and public networks defined as follows:**
  - **OP.sending_public: IP packet sending to a public network,**
  - **OP.sending_private: IP packet sending to a private (sub)network,**
  - **OP.receipt_public: IP packet receipt from a public network,**
  - **OP.receipt_private: IP packet receipt from a private (sub)network.**

Raffinement non éditorial :

The VPN enforcement policy is the security policy that enforces (confidentiality, integrity and replay detection) the VPN security policies on the IP packets that flow through the IP encrypter.

6.1.1.2 FDP_IFF.1/Enforcement_policy Simple security attributes

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

- **Security attribute of the VPN link used by the subject IP encrypter: "AT.policy", which may hold one of the following values**
  - **"defined" if a VPN policy is associated with the VPN link used by the IP encrypter**
  - **"undefined" if no VPN policy is associated with the VPN link used by the IP encrypter**
- **[assignment:**
  - **address of source subject;**
  - **address of destination subject]**

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

- **OP.sending_public is authorized if the security protections defined in the related VPN security policy are applied to the applicative and topologic data of IP packets before sending the IP packets to the public network.**
- **OP.sending_private is authorized if the communication with the destination subnetwork is authorized and if the security protections defined in the related VPN security policy are verified on the applicative and topologic data of IP packets before sending the IP packets to the private network.**
- **OP.receipt_public and OP.receipt_private are authorized.**

Raffinement non éditorial :

The related VPN security policy can be retrieved thanks to the source and destination addresses contained in IP packets.

FDP_IFF.1.3/Enforcement_policy The TSF shall enforce **the [assignment: None]**.

FDP_IFF.1.4/Enforcement_policy The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: None]**.

FDP_IFF.1.5/Enforcement_policy The TSF shall explicitly deny an information flow based on the following rules:

- **When no VPN security policy has been explicitly defined for the given VPN communication link (AT.policy is "undefined"), the default screening rule applies. This latter rule shall reject the IP packets, that is no sending is performed.**

- **When the given VPN security policy specifies that sending IP packets to the destination address (specific to a subnetwork) is forbidden, no sending is performed.**
- **When an error occurs during the application or verification of security protections, no sending of IP packets is authorized.**

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

FDP_ITC.1.1/Enforcement_policy The TSF shall enforce the **VPN enforcement policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/Enforcement_policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: None].**

Raffinement non éditorial :

The user data of those requirements are the IP packets, which comprise applicative and topologic data.

6.1.1.4 FDP_ETC.1 Export of user data without security attributes

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

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

Raffinement non éditorial :

The user data of those requirements are the IP packets, which comprise applicative and topologic data.

6.1.1.5 FCS_COP.1/Enforcement_policy Cryptographic operation

FCS_COP.1.1/Enforcement_policy The TSF shall perform **[assignment: encryption, decryption, authentication]** in accordance with a specified cryptographic algorithm **[assignment: (Cf 3.5.7)]** and cryptographic key sizes **[assignment: 256 bits]** that meet the following: **ANSSI cryptographic referentials ([5]and [9])**.

6.1.1.6 FCS_COP.1/Mutual_auth Cryptographic operation

FCS_COP.1.1/Mutual_auth The TSF shall perform **[assignment: key exchange, HMAC]** in accordance with a specified cryptographic algorithm **[assignment: : Diffie-Hellman groupe 19 or group 28 along with a SHA256 hash]** and cryptographic key sizes **[assignment: 256 bits]** that meet the following: **cryptographic referentials of ANSSI ([5] ,and [9])**.

6.1.2 Protection des politiques de sécurité VPN

6.1.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **VPN protection policy** on

- **Objects: VPN links and VPN security policies, where VPN security policies include VPN security contexts**
- **Subjects: IP encrypter administration component**
- **Operations:**
  - **OP.VPN_SP_definition: allows to define the VPN security policy applicable to a given VPN link.**
  - **OP.VPN_SP_dyn_neg: allows to dynamically complete the VPN security policy applicable to a given VPN link.**
  - **OP.VPN_SP_display: allows to display the VPN security policy of a given VPN link.**
  - **OP.VPN_SP_distribute: allows to distribute the VPN security policy of a given VPN link.**

Raffinement non éditorial :

La configuration est réalisée sur l'application TDM (hors TOE) et est envoyée à la TOE par un dialogue administratif sécurisé.

La cohérence de la configuration est contrôlée sur la TOE (en particulier pour le paramètre « Full IPsec DR »).

6.1.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce **the VPN protection policy** to objects based on the following:

- **Security attribute of the VPN link: "AT.policy", which may hold one of the following values**
  - **"defined" if a VPN policy is associated with the VPN link.**
  - **"constrained" if a partial VPN policy and constraints for a dynamic negotiation are associated with the VPN link.**
  - **"undefined" if no VPN policy is associated with the VPN link.**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The IP encrypter administration component is allowed to define the VPN security policy of a given VPN link by means of OP.VPN_SP_definition on behalf of an authenticated security administrator. Upon completion of the operation, the attribute AT.policy of the VPN link holds the value "defined".**
- **The IP encrypter dynamic negotiation component is allowed to complete the VPN security policy of a VPN link with the attribute AT.policy equal to "constrained" by means of OP.VPN_SP_dyn_neg on behalf of an authenticated provided the definition fulfils the constrains.**
- **The IP encrypter administration component is allowed to display the VPN security policy of a given VPN link by means of OP.VPN_SP_display on behalf of an authenticated security administrator.**
- **The IP encrypter administrator component is allowed to distribute the VPN security policy of a given VPN link by means of OP.VPN_SP_distribute on behalf of an authenticated remote security administrator provided the VPN security policies and security contexts are protected from modification and disclosure during the distribution.**

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[assignment: None].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **The operation OP.VPN_SP_definition is denied to any user that has not been authenticated as a security administrator.**
- **The operation OP.VPN_SP_display is denied to any user that has not been authenticated as a security administrator.**
- **The operation OP.VPN_SP_distribute is denied to any user that has not been authenticated as a remote security administrator or if the distribution channel does not ensure integrity and confidentiality.**

Raffinement non éditorial :

La configuration est réalisée sur l'application TDM (hors TOE) et est envoyée à la TOE par un dialogue administratif sécurisé.

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

FDP_ITC.1.1/VPN_policy The TSF shall enforce the **VPN protection policy** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/VPN_policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: None].**

Raffinement non éditorial :

The user data of those requirements are the VPN security policies configured by the TDM application.

6.1.2.4 FMT_MSA.3/VPN_policy Static attribute initialisation

FMT_MSA.3.1/VPN_policy The TSF shall enforce the **VPN protection policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/VPN_policy The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

Raffinement non éditorial :

The security attribute concerned by these requirements is the attribute AT.policy that indicates for each VPN communication link if a VPN security policy and its context are defined. Its initial value is "undefined". This value is changed by the security administrator when he defines the VPN security policy and its context ("defined") or when he specifies constraints on the VPN security policy and its context ("constrained")

6.1.2.5 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **VPN protection policy** to restrict the ability to **modify** the security attributes **AT.policy of a VPN link** to **the security administrator.**

Raffinement non éditorial :

La configuration est réalisée sur l'application TDM (hors TOE) et est envoyée à la TOE par un dialogue administratif sécurisé.

6.1.2.6 FMT_SMF.1/VPN_policy Specification of Management Functions

FMT_SMF.1.1/VPN_policy The TSF shall be capable of performing the following management functions: **modification of the VPN link attribute AT.policy.**

Raffinement non éditorial :

La configuration est réalisée sur l'application TDM (hors TOE) et est envoyée à la TOE par un dialogue administratif sécurisé.

6.1.3 Politique de gestion des clés

6.1.3.1 FDP_IFC.1/Key_policy Subset information flow control

FDP_IFC.1.1/Key_policy The TSF shall enforce the **key management policy** on

- **Information: cryptographic keys**
- **Subjects: IP encrypter key management component**
- **Operations:**
    - **OP.local_key_injection: allows to import within the TOE cryptographic keys generated outside the TOE. This import is done at personalization time using an securized USB key;**

- **OP.remote_key_injection: allows to import within the TOE cryptographic keys generated outside the TOE remotely. This import is done from the TDM thru the Securized Administration flow.**

6.1.3.2 FDP_IFF.1/Key_policy Simple security attributes

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

- **Security attribute of cryptographic keys: "AT.key_type", which may hold one of the following three values:**
  - **"public" applies to the public part of asymmetric cryptographic keys**
  - **"private" applies to the private part of asymmetric cryptographic keys**
  - **"secret" applies to symmetric cryptographic keys**
- **[assignment: None].**

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

- **The IP encrypter key management component is allowed to perform local injection of keys by means of the operation OP.local_key_injection on behalf of an authenticated local security administrator (Personnalization Cf 3.3.2.3). Upon completion of the operation, the attribute AT.key_type of the injected key holds the value corresponding to the kind of key injected.**
- **The IP encrypter key management component is allowed to perform remote key injection by means of the operation OP.remote_key_injection on behalf of an authenticated remote security administrator (Configuration Cf 3.3.2.1.1) provided the imported keys are protected from modification and the private and secret imported keys are protected from disclosure during the injection.**

FDP_IFF.1.3/Key_policy The TSF shall enforce the **[assignment: None].**

FDP_IFF.1.4/Key_policy The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: None].**

FDP_IFF.1.5/Key_policy The TSF shall explicitly deny an information flow based on the following rules:

- **The injection (OP. key_inject) of keys is denied to any user that has not been authenticated as a security administrator (Personnalization Cf 3.3.2.3 or Configuration Cf 3.3.2.1.1)**

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

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

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

FDP_ITC.1.3/Key_policy The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: None].**

Raffinement non éditorial :

"User data" stands for cryptographic keys imported in the TOE.

Note d'application :

Les règles d'importation additionnelles ne doivent pas mettre en échec les exigences d'intégrité (FDP_UIT.1) et de confidentialité (FDP_UCT.1).

6.1.3.4 FDP_UCT.1 Basic data exchange confidentiality

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

Raffinement non éditorial :

"User data" stands for private or secret cryptographic keys injected in the TOE.

Note d'application :

FDP_UCT.1 requires the confidentiality of cryptographic keys injected in the TOE within a trusted path (**FTP_TRP.1**) for personalization key injection and within a trusted channel (**FTP_ITC.1**) for TDM key injection

6.1.3.5 FDP_UIT.1 Data exchange integrity

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

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

Raffinement non éditorial :

"User data" stands for public, private and secret cryptographic keys injected in the TOE.

Note d'application :

FDP_UIT.1 requires the integrity of cryptographic keys injected in the TOE within a trusted path (**FTP_TRP.1**) for personalization key injection and within a trusted channel (**FTP_ITC.1**) for TDM key injection.

6.1.3.6 FMT_MSA.3/Key_policy Static attribute initialisation

FMT_MSA.3.1/Key_policy The TSF shall enforce the **key management policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Key_policy The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

6.1.3.7 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **[assignment: the lifetime of session cryptographic keys]**.

Note d'application :

La date de validité du certificat est contrôlée lors de l'authentification mutuelle IKE.

6.1.3.8 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: AES and HMAC SHA256]** and specified cryptographic key sizes **[assignment: 256 bits]** that meet the following: **cryptographic referential of ANSSI ([5] and [9]).**

6.1.3.9 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: zeroisation method]** that meets the following: [Aucun]**.**

6.1.4 Configuration et supervision

6.1.4.1 FDP_IFC.1/Config_audit Subset information flow control

FDP_IFC.1.1/Config_audit The TSF shall enforce the **configuration and audit policy** on

- **Information: configuration parameters audit events and security alarms.**
- **Operations: all remote operations that cause this information to flow.**
- **Subjects: subjects of administration software that consults this information.**

6.1.4.2 FDP_IFF.1/Config_audit Simple security attributes

FDP_IFF.1.1/Config_audit The TSF shall enforce the **configuration and audit policy** based on the following types of subject and information security attributes: **none**.

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

- **Remote administration operations on configuration parameters are authorized if this information is protected from modification and disclosure when flowing between the administration equipment and the IP encrypter.**
- **Remote administration operations on audit events are authorized if this information is protected from modification when flowing between the administration equipment and the IP encrypter.**

FDP_IFF.1.3/Config_audit The TSF shall enforce the **[assignment: None]**.

FDP_IFF.1.4/Config_audit The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: None]**.

FDP_IFF.1.5/Config_audit The TSF shall explicitly deny an information flow based on the following rules: **[assignment: None]**.

6.1.4.3 FMT_MTD.1/Network_param Management of TSF data

FMT_MTD.1.1/Network_param The TSF shall restrict the ability to **query and modify** the **network configuration parameters** to **system and network administrators** (named Administrateur (Cf 3.3.2.1) for network parameters configured in TDM and Administrateur des paramètres réseau initiaux (Cf 3.3.2.2) for initial network parameters configured in the local application)**.**

6.1.4.4 FMT_MTD.1/Param Management of TSF data

FMT_MTD.1.1/Param The TSF shall restrict the ability to **modify** the **access rights and the authentication data** to **system and network administrators** (named Administrateur (Cf 3.3.2.1) for parameters configured in TDM and Administrateur des paramètres réseau initiaux (Cf 3.3.2.2) for parameters configured in the local application)**.**

6.1.4.5 FMT_SMF.1/Config_supervision Specification of Management Functions

FMT_SMF.1.1/Config_supervision The TSF shall be capable of performing the following management functions:

- **request and modification of network configuration parameters,**
- **modification of access rights and authentication data,**
- **supervision of the state of IP encrypters.**

6.1.5 Protection de l'administration

6.1.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from **disclosure (when data are confidential) and modification** when it is transmitted between separate parts of the TOE.

Raffinement non éditorial :

All remote administration operations must be protected including operations on:

- ***VPN security policies and their contexts (one possible for each subnetwork),***
- ***cryptographic keys,***
- ***configuration parameters,***
- ***audit events.***

The access to the local administration is protected (except for the depersonalization function) with a password.

6.1.5.2 FPT_ITT.3 TSF data integrity monitoring

This section is only significant for remote administration.

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

FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions: **[assignment: drop the frame and send an SNMP trap and a Syslog message]**.

6.1.6 Protection du flux d'administration

6.1.6.1 FPT_RPL.1 Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities:

- **sequences of administration data exchanged between an IP encrypter and an administration equipment.**

FPT_RPL.1.2 The TSF shall perform **[assignment: frame dropped]** when replay is detected.

6.1.7 Test de la TSF

6.1.7.1 FPT_TST.1 Tests de la TSF

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up to demonstrate the correct operation of the TSF

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [no parts of TSF data].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [no parts of TSF].

6.1.8 Protection des TSF et des TSF data

6.1.8.1 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **all the sensitive data (VPN security policies and their contexts, cryptographic keys, configuration parameters, audit events and security alarms).**

Note d'application :

Certaines données sont rendues inaccessibles par l'effacement des clés cryptographiques avec lesquelles les zones les contenant étaient chiffrées.

6.1.9 Audit et alarmes

6.1.9.1 FAU_GEN.1/VPN Audit data generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **basic** level of audit; and

c) **[assignment: at least the following events:**

- **TVPN Cold Start;**
- **IPSec authentication error].**

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **information that make possible to detect a loss of an audit record (like a counter), [assignment: information specified in column two of the following table].**

Raffinement non éditorial :

The subject identity corresponds to the identity of the IP packets' recipient and sender (respectively destination IP address and source IP address).

The audit events considered in those requirements focus on the VPN communication links between IP encrypters.

There is no local storage of audit data.

The audit data sent to the syslog server are protected by an ESP Tunnel as described in FDP_IFC.1.1/Enforcement_policy.

6.1.9.2 FAU_GEN.1/Administration Audit data generation

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

a) Start-up and shutdown of the audit functions;

All auditable events for the **detailed** level of audit; **FAU_GEN.1.2/Administration** The TSF shall record within each audit record at least the following information:

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

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

Raffinement non éditorial :

The audit events considered in those requirements are related to the administration operations.

6.1.9.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **auditors** (Cf 3.3.2.4) with the capability to read 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.

Note d'application:

Ne s'applique qu'à l'auditeur des événements du chiffreur (hors TOE) (Cf 3.3.2.4.1)

6.1.9.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply ordering or selection of audit data based on event type , date and time...

Note d'application:

Ne s'applique qu'à l'auditeur des événements du chiffreur (hors TOE) (Cf 3.3.2.4.1).

6.1.9.5 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

Raffinement non éditorial :

There is no local storage of audit data.

The audit data sent to the syslog server are protected by an ESP Tunnel as described in FDP_IFC.1.1/Enforcement_policy.A sequence number allows determining if at least one audit data has been destroyed.

6.1.9.6 FAU_ARP.1

FAU_ARP.1.1 The TSF shall take **the following actions:**

- **a security alarm is raised to the alarm administrator (named** Auditeur des alarmes du chiffreur (Cf 3.3.2.4.3)**),**
- **[assignment: generate an alarm which can be displayed by the local application**] upon detection of a potential security violation.

6.1.9.7 FAU_SAA.1/Alarm Potential violation analysis

FAU_SAA.1.1/Alarm The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

Raffinement non éditorial :

The alarms cannot be modified or destroyed by an external operation.

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

a) Reboot with a specific reboot code in case of security violation. This reboot code appears in the ColdStart syslog or SNMP Trap. The reason of the alarm can be displayed in the local application.

b) **[assignment: no other rules]**.

6.1.9.8 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Raffinement non éditorial :

TSF provides reliable time stamps for its own use.

6.1.10 Rôles et authentification

Certains rôles sont hors TOE (Cf 3.3.2).

6.1.10.1 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain several roles (Cf 3.3.2)

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

6.1.10.2 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified (Cf 3.3.2) before allowing any other TSF-mediated actions on behalf of that user.

Raffinement non éditorial :

Il n'y a qu"un seul utilisateur pour les rôles suivants :

- Rôle Administrateur des paramètres réseau initiaux (Cf 3.3.2.2) ;
- Auditeur des alarmes du chiffreur (Cf 3.3.2.4.3).

L'identification de l'utilisateur pour la personnalisation du chiffreur (Cf 3.3.2.3) est réalisée sur la station SPC (hors TOE) (Cf 3.3.2.1.2).

6.1.10.3 FIA_UAU.2 User authentication before any action

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.

Raffinement non éditorial :

A local user authentication by password is required.

6.1.10.4 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **mutual authentication of IP encrypters**.

6.1.11 Chemins et Canaux de confiance

6.1.11.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for security policy configuration.

Raffinement non éditorial :

The another trusted IT is the TDM station (Cf 3.3.2.1.1).

6.1.11.2 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, disclosure and confidentiality violation.

FTP_TRP.1.2 The TSF shall permit local users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for TSF personnalisation (Cf 3.4.1).

Raffinement non éditorial :

Cf 3.3.2.3 for local users définition.

6.2 Exigences de sécurité d'assurance

Le niveau des exigences d'assurance de sécurité est EAL4 augmenté de ALC_FLR.3.

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_FLR.3, ALC_LCD.1, ALC_TAT.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.3

6.3 Définition des éléments du modèle de sécurité

L'instanciation des exigences de sécurité fonctionnelles repose sur les sujets, opérations et objets décrits dans les chapitres suivants.

6.3.1 Sujets

S_encrypter_VPN

IP encrypter VPN Management component

S_encrypter_admin

IP encrypter remote administration component

S_encrypter_key

IP encrypter key management component

S_audit_event

Subjects of administration software that consults audit events

6.3.2 Opérations

OP.sending_public

IP packet sending to a public network

OP.sending_private

IP packet sending to a private (sub)network,

OP.receipt_public

IP packet receipt from a public network,

OP.receipt_private

IP packet receipt from a private (sub)network.

OP.VPN_SP

Allows to define the VPN security policy applicable to a given VPN link.

OP.VPN_SP_dyn_neg

Allows to dynamically complete the VPN security policy applicable to a given VPN link.

OP.VPN_SP_display

Allows to display the VPN security policy of a given VPN link.

OP.VPN_SP_distribute

Allows to distribute the VPN security policy of a given VPN link.

OP.local_key_injection

Allows to import within the TOE cryptographic keys generated outside the TOE.

OP.remote_key_injection

Allows to import within the TOE cryptographic keys generated outside the TOE remotely.

OPaudit_sending

All remote operations that cause this information (Audit) to flow.

6.3.3 Objets

OB.user_data

Applicative and topologic data contained in IP packets

OB.security_policies

VPN links and VPN security policies, where VPN security policies include VPN security contexts

OB.keys

Cryptographic keys

OB.audit events

Events sent by the TOE

Chapitre 7.Spécifications globales de la TOE

7.1 Fonctions de sécurité

7.1.1 SF.USER_DATA_PROTECTION

La fonction de protection des données de l'utilisateur du réseau privé garantit la protection des données des utilisateurs du réseau privé en assurant la confidentialité, l'intégrité et l'authenticité des flux émis entre un utilisateur du réseau privé et un autre utilisateur d'un autre réseau privé, et qui transitent par un réseau externe (non sécurisé).

La TOE supporte le protocole IPSec ESP de l'IETF (Internet Protocol Security Encapsulation Security Payload) en mode tunnel comme spécifié dans RFC4301.

Le chiffreur doit toujours être configuré en mode « Full IPsec DR » (l'option « Full IPsec DR » doit toujours être positionnée dans la politique de sécurité TDM).

La TOE prend en charge les algorithmes cryptographiques suivants :

Mode IPSec DR ANSSI entre IP Protect:

L'implémentation est compatible avec le document **Note Crypto Référentiel IPsec DR Profil de Protection « Chiffreur IP »** émis par l'ANSSI.

Les tunnels établis en ESP Tunnel entre les divers équipements (IP Protect et station de travail GVPNC) mettent en œuvre un chiffrement en mode AES-GCM (clés de 256 bits et ICV de 16 octets) qui assure la sécurité, l'intégrité et l'anti-rejeu du flux de données. L'anti-rejeu sera réalisé uniquement en ESN (Extended Sequence Number).

Les contextes de sécurité (SA : Security Association) sont négociés par le protocole IKEv2 avec les algorithmes cryptographiques suivants :

- Confidentialité : AES-GCM (clés de 256 bits et ICV de 16 octets) ;
- PRF : PRF_HMAC_SHA2_256 ;
- Authentification : ECDSA sur secp256r1 avec SHA256 ;
- Diffie-Hellman DH19(secp256r1).

Mode IPSec DR ANSSI avec des équipements non gérés par le TDM:

Le chiffreur IP Protect permet aussi la communication en mode ESP Tunnel avec des équipements non gérés par le TDM.

Cela permet notamment la mise en œuvre de mécanismes cryptographiques conformes aux exigences IPSec DR ANSSI (Cf **ANSSI : Note Crypto Référentiel IPsec DR Profil de Protection « Chiffreur IP »**) mais non utilisés pour la communication entre chiffreurs IP Protect :

- ESP

- Chiffrement IKE AES-CTR 256bits;
- Intégrité HMAC_SHA2_256_128.

- IKE
  - Authentification IKE ECDSA BrainpoolP256r1 ;
  - Authentification IKE ECSDSA secp256r1 avec SHA256 ;
  - Authentification IKE ECSDSA BrainpoolP256r1 ;
  - Diffie-Hellman DH28(BrainpoolP256r1) ;
  - Chiffrement ESP AES-CTR 256bits ;
  - Intégrité HMAC_SHA2_256_128.

Rationnel : SF.USER_DATA_PROTECTION couvre les exigences de sécurité assurant :

– Application des politiques de sécurité VPN :

FDP_IFC.1/Enforcement_policy
FDP_IFF.1/Enforcement_policy
FDP_ITC.1/Enforcement_policy
FDP_ETC.1
FCS_COP.1/Enforcement_policy

– Protection des politiques de sécurité VPN :

FDP_ACF.1
FDP_ITC.1/VPN_policy
FCS_COP.1/Mutual_auth
FIA_UAU.4

– Gestion des clés cryptographiques :

FDP_IFF.1/Key_policy
FTA_TSE.1
FCS_CKM.1

7.1.2 SF.ROLES

La fonction de gestion des rôles permet de gérer les différents rôles de la TOE . Ces rôles fournissent des privilèges différents et donc des fonctions d'administration différentes. Les rôles sont décrits dans le chapitre 3.3.2.

Rationnel : SF.ROLES gère les rôles (FMT_SMR.1) et contrôle l'accès à :

– Politiques de sécurité VPN :

FDP_ACC.1
FMT_SMR.1

7.1.3 SF.ADMINISTRATION

La fonction d'administration permet aux administrateurs de la TOE d'accéder à distance (à partir du TDM) aux fonctions d'administration de la TOE.

Cette fonction permet aussi d'accéder localement à quelques fonctions d'administration de la TOE.

Administration à distance à partir du TDM

Le TDM (Trustway Domain Manager) permet l'administration du Trustway IP Protect distant. Il est basé sur un système d'exploitation Windows Server 2019 durci, et équipé d'un HSM (Hardware Security Module) Proteccio développé par Bull, effectuant les opérations cryptographiques.

L'application de configuration TDM est chargée de la génération et l'envoi de la configuration des IP Protect sous le contrôle d'administrateur TDM.

La configuration des IP Protect se compose de:

- Règles de sécurité (domaines de sécurité et gestion des chiffreurs non gérés par le TDM);
- Configuration de la supervision du réseau;
- Configuration des répondeurs OCSP ;
- Configuration du réseau VPN (QoS, VRRP, etc) ;
- Gestion de l'envoi des événements d'audit ;
- Date et heure pour l'envoi différé des configurations ;
- Mode « Full IPSec DR » n'autorisant que les fonctionnalités définies dans le document **ANSSI : Note Crypto Référentiel IPsec DR Profil de Protection « Chiffreur IP »**. (seul mode autorisé dans le cadre de cette cible de sécurité).

Administration locale

L'administration locale permet de définir le paramètres réseau initiaux du chiffreur IP Protect. Les paramètres réseau initiaux sont les paramètres permettant au boîtier de communiquer avec le TDM lors de sa première mise en service dans le réseau. La configuration peut se faire sur le site de personnalisation ou sur le site opérationnel. Cette opération se fait via une application locale (protégée par mot de passe) au boîtier à laquelle on accède depuis une machine extérieure hébergeant un émulateur de terminal.

Les paramètres à initialiser sont :

- Adresse IP d'administration du boîtier/masque réseau associé ;
- Adresse IP du TDM ;
- Adresse IP du gateway d'accès au TDM ;
- Interface d'accès au TDM.

L'administration locale permet aussi :

- la personnalisation du chiffreur ;

- La consultation des alarmes ;
- La dépersonnalisation du chiffreur.

Rationnel : SF.ADMINISTRATION garantit :

– Contrôle d'accès à :

- Droits d'accès et données d'authentification :

FMT_MTD.1/Param

– Spécification des politiques et configuration de la TOE :

FMT_MTD.1/Network_param
FMT_MSA.3/VPN_policy
FMT_MSA.1
FMT_SMF.1/VPN_policy

– Surveillance :

FMT_SMF.1/Config_supervision

– Gestion des clés cryptographiques :

7.1.4 FDP_ITC.1/Key_policy FMT_MSA.3/Key_policySF.REINIT

La fonction de réinitialisation de la TOE permet à l'administrateur de supprimer définitivement les ressources sensibles de la TOE (politiques VPN, clés privées, informations d'authentification, etc.). Cette dépersonnalisation est suivie d'un redémarrage automatique de l'équipement.

Rationnel : SF.REINIT couvre :

– Destruction des clés et données sensibles :

FDP_RIP.1
FCS_CKM.4

7.1.5 SF.LOCAL_ADMIN_AUTHENTICATION

Il n'y a pas de configuration locale en dehors de la configuration réseau minimale.

La politique de sécurité est distribuée au travers du réseau par l'application TDM (Cf SF.REMOTE_ADMIN_AUTHENTICATION).

La personnalisation (injection des secrets initiaux) est réalisée par l'application locale avec une clé USB protégée en confidentialité et intégrité nécessitant un mot de passe pour pouvoir être vérifiée et déchiffrée.

Rationnel : SF. LOCAL_ADMIN_AUTHENTICATION couvre :

- L'identification (FIA_UID.2) et l'authentification (FIA_UAU.2) de l'administrateur local ;

- L'authentification du chemin de confiance (FTP_TRP.1)

7.1.6 SF.REMOTE_ADMIN_AUTHENTICATION

TDM communique avec la TOE par le biais d'un protocole sécurisé. Ce protocole est basé sur des secrets partagés implantés dans la TOE lors de la personnalisation permet une authentification mutuelle entre le TDM et la TOE.

Le secret partagé est spécifique à chaque TOE. Il est généré par le composant cryptographique utilisé par le SPC, et associé par le TDM à chaque équipement au cours de la phase d'enregistrement.

Rationnel : SF.REMOTE_ADMIN_AUTHENTICATION couvre l'identification (FIA_UID.2) et l'authentification (FIA_UAU.2) de l'administrateur distant.

7.1.7 SF.REMOTE_ADMIN_PROTECTION

La fonction de protection de l'administration à distance de la TOE permet de protéger la confidentialité, l'intégrité et l'authenticité des flux échangés entre la TOE et l'administrateur lors de l'administration à distance de la TOE à partir du TDM.

Le dialogue d'administration (y compris le plan d'adressage du réseau sécurisé et les politiques VPN) est protégé en intégrité par l'utilisation d'un dialogue administratif sécurisé.

Note : L'envoi de la politique de sécurité concernant la communication avec des équipements non gérés par le TDM s'appuie sur le dialogue administratif sécurisé mais utilise aussi le transfert de fichiers tftp. Les données transférées par tftp sont aussi protégées en confidentialité et en intégrité.

Rationnel : SF.REMOTE_ADMIN_PROTECTION protège les données transmises entre la TOE et le TDM :

- FPT_ITT.1 ;
- FPT_ITT.3 ;
- FTP_ITC.1.

7.1.8 SF.AUDIT

La fonction d'audit fournit des fonctions de sécurité relatives à la journalisation des événements de la TOE. Elle gère l'identification, l'enregistrement et le stockage des événements de la TOE.

Il existe trois types d'événements enregistrés : les données d'audit des flux, les données d'audit d'administration et les alarmes de sécurité. Les données d'audit des flux fournissent des informations sur les paquets traités par la TOE (flux rejetés en raison de la politique de sécurité de la TOE, d'une mauvaise intégrité ou d'un rejeu). Les données d'audit d'administration fournissent des informations sur les opérations effectuées par l'administrateur sur la TOE. Les alarmes de sécurité indiquent un problème sérieux qui pourrait affaiblir la sécurité de la TOE.

Les événements sont envoyés sécurisés par ESP Tunnel au serveur syslog. Un numéro de séquence permet de détecter les pertes d'événements.

Les journaux d'audit peuvent être visualisés sur le serveur syslog. Seuls les administrateurs authentifiés sur le serveur syslog sont autorisés à accéder aux journaux d'événements.

Les journaux d'audit du TDM sont stockés et peuvent être visualisés sur le TDM.

Les traps SNMP sont envoyés vers les superviseurs SNMP déclarés.

Les traps SNMP sont envoyés sécurisés par ESP Tunnel au superviseur SNMP.

Sur les superviseurs, il est nécessaire d'installer préalablement la MIB décrite par le fichier TW-public-MIB.txt contenu sur le CD d'installation du TDM pour pouvoir décoder les traps SNMP.

L'envoi de certains traps SNMP ou syslog est conditionné par des seuils configurés sur le TDM.

Les alarmes sont consultables localement par l'application locale d'administration IP Protect.

Rationnel : SF.AUDIT couvre toutes les exigences de sécurité générant des événements de journalisation :

- Génération des données d'audit des flux :

  FAU_GEN.1/VPN
  FAU_SAR.1
  FAU_SAR.3
  FPT_STM.1

- Protection des données d'audit des flux :

  FAU_STG.1

- Génération des données d'audit des opérations d'administration :

  FAU_GEN.1/Administration

- Protection des données d'audit des opérations d'administration :

  FAU_STG.1

- Alarmes :

FAU_ARP.1
FAU_SAA.1/Alarm

7.1.9 SF.SOFTWARE_INTEGRITY

La fonction de protection de l'intégrité du logiciel permet de garantir que le fonctionnement de la TOE est conforme aux spécifications.

Rationnel : SF.SOFTWARE_INTEGRITY couvre :

– Protection de l'intégrité du logiciel :

FPT_TST.1

7.2 Fonctions d'assurance de sécurité

Les fonctions d'assurance de sécurité suivantes ont été implémentées dans l'équipement.

7.2.1 DOCUMENTS DE CONCEPTION

Une documentation technique décrivant la conception de la TOE avec différents niveaux techniques (spécifications fonctionnelles, conception globale, conception détaillée) est disponible.

Rationnel : DOCUMENTS DE CONCEPTION couvre les exigences d'assurance ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3.

7.2.2 GUIDES

Les guides utilisateur et administrateur sont disponibles.

Rationnel : GUIDES couvre les exigences d'assurance AGD_OPE.1, AGD_PRE.1.

7.2.3 SUPPORT AU CYCLE DE VIE

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

Les développeurs utilisent un système de gestion de configuration qui garantit l'intégrité de la TOE et de sa documentation lors des différentes étapes du développement.

Des procédures de livraison et d'installation sécurisées sont disponibles.

Le développeur a mis en place des procédures de traitement des anomalies découvertes par les utilisateurs de la TOE, assurant leur prise en compte et leur correction.

Rationnel : SUPPORT AU CYCLE DE VIE couvre les exigences d'assurance ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_FLR.3, ALC_LCD.1, ALC_TAT.1.

7.2.4 TESTS FONCTIONNELS

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

Rationnel : TESTS FONCTIONNELS couvre les exigences d'assurance ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2.

7.2.5 EVALUATION DES VULNERABILITES

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

Rationnel : EVALUATION DES VULNERABILITES couvre les exigences d'assurance AVA_VAN.3.

Chapitre 8.Argumentaires

8.1 Objectifs de sécurité / problème de sécurité

8.1.1 Couverture des objectifs de sécurité

Politiques/Menaces/Hypothèses	Objectifs
Politiques	
OSP.SERVICES_RENDUS	O.APPLICATION_POL, O.CONFIDENTIALITE_APPLI, O.AUTHENTICITE_APPLI, O_REJEU_APPLI, O.CONFIDENTIALITE_TOPO, O.AUTHENTICITE_TOPO, O.CLOISONNEMENT_FLUX, O.AUDIT_VPN, O.ALARMES, OE.INTEGRITE_TOE, O.INTEGRITE_LOGICIELS
OSP.CRYPTO	O.CRYPTO, OE.CRYPTO
OSP.SUPERVISION	O.SUPERVISION
Menaces	
T.MODIFICATION_POL	O.DEFINITION_POL, O.IMPACT_SUPERVISION, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, O.DISTRIBUTION_POL, O.AUDIT_ADMIN, O.ALARMES, O.AUTHENTIFICATION_ADMIN, OE.INTEGRITE_TOE, O.INTEGRITE_LOGICIELS
T.DIVULGATION_POL	O.DEFINITION_POL, O.IMPACT_SUPERVISION, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, O.DISTRIBUTION_POL, O.AUDIT_ADMIN, O.ALARMES, O.AUTHENTIFICATION_ADMIN, OE.INTEGRITE_TOE, O.INTEGRITE_LOGICIELS
T.COHERENCE_POL	O.COHERENCE_POL, O.DISTRIBUTION_POL, O.AUDIT_ADMIN, O.ALARMES, OE.INTEGRITE_TOE, O.AUTHENTIFICATION_ADMIN, O.INTEGRITE_LOGICIELS
T.MODIFICATION_PARAM	O.PROTECTION_PARAM, O.IMPACT_SUPERVISION, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, O.AUDIT_ADMIN, O.ALARMES, O.AUTHENTIFICATION_ADMIN, OE.INTEGRITE_TOE, O.SUPERVISION, O.INTEGRITE_LOGICIELS
T.DIVULGATION_PARAM	O.PROTECTION_PARAM, O.IMPACT_SUPERVISION, O.SUPERVISION, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, O.AUDIT_ADMIN, O.ALARMES, OEAUTHENTIFICATION_ADMIN, OE.INTEGRITE_TOE, O.INTEGRITE_LOGICIELS
T.MODIFICATION_CLES	O.ACCES_CLES, O.INJECTION_CLES, O.IMPACT_SUPERVISION, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, O.AUDIT_ADMIN, O.ALARMES, O.AUTHENTIFICATION_ADMIN, OE.INTEGRITE_TOE, O.INTEGRITE_LOGICIELS
T.DIVULGATION_CLES	O.INJECTION_CLES, O.ACCES_CLES, O.IMPACT_SUPERVISION, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, O.CRYPTO, O.AUDIT_ADMIN, O.ALARMES, O.AUTHENTIFICATION_ADMIN, OE.INTEGRITE_TOE, O.INTEGRITE_LOGICIELS

T.MODIFICATION_AUDIT	O.IMPACT_SUPERVISION, O.PROTECTION_AUDIT, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_FLUX_ADMIN, O.AUDIT_ADMIN, O.ALARMES, O.AUTHENTIFICATION_ADMIN, OE.INTEGRITE_TOE ; O.AUDIT_VPN, O.INTEGRITE_LOGICIELS
T.MODIFICATION_ALARME	O.PROTECTION_ALARME, O.ALARMES, OE.INTEGRITE_TOE
T.BASE_TEMPS	O.BASE_TEMPS, OE.INTEGRITE_TOE, O.IMPACT_SUPERVISION
T.USURPATION_ADMIN	O.AUTHENTIFICATION_ADMIN, O.AUDIT_ADMIN, O.AUDIT_VPN, O.AUTHENTIFICATION_ADMIN
T.REJEU_ADMIN	O.PROTECTION_REJEU_ADMIN, O.AUDIT_ADMIN, O.AUDIT_VPN, OE.INTEGRITE_TOE, O.INTEGRITE_LOGICIELS
T.BIENS_INDISPONIBLES	O.BIENS_INDISPONIBLES, OE.PROTECTION_LOCAL, O.ALARMES
T.DIVULGATION_DONNEES_APPLICATIVES	O.CONFIDENTIALITE_APPLI
T.MODIFICATION_DONNEES_APPLICATIVES	O.AUTHENTICITE_APPLI
T.REJEU_DONNEES_APPLICATIVES	O.REJEU_APPLI
T.DIVULGATION_INFO_TOPOLOGIE	O.CONFIDENTIALITE_TOPO
T.MODIFICATION_INFO_TOPOLOGIE	O.AUTHENTICITE_TOPO
T.MODIFICATION_LOGICIELS	O.INTEGRITE_LOGICIELS, O_ALARMES, OE.INTEGRITE_TOE
Hypothèses	
A.AUDIT	OE.ANALYSE_AUDIT
A.ALARME	OE.TRAITE_ALARME
A.ADMIN	OE.ADMIN
A.LOCAL	OE.PROTECTION_LOCAL
A.MAITRISE_CONFIGURATION	OE.INTEGRITE_TOE
A.CRYPTO	OE.CRYPTO
A.CLOISONNEMENT_ADMIN_USER	O.PROTECTION_FLUX_ADMIN

Table 8-1. Correspondance Environnement de sécurité de la TOE / Objectifs de sécurité

8.1.2 Suffisance des Objectifs de sécurité

Dans ce chapitre nous allons établir la correspondance entre les objectifs de sécurité et les menaces, les hypothèses et les politiques de sécurité organisationnelles.

8.1.2.1 Menaces

8.1.2.1.1 Menaces portant sur les politiques de sécurité VPN et leurs contextes

T.MODIFICATION_POL

Cette menace est contrée par O.DEFINITION_POL, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN qui imposent que les politiques de sécurité VPN et leurs contextes ne peuvent être modifiés que par des administrateurs de sécurité authentifiés comme tels. De plus, cette menace est aussi contrée par O.PROTECTION_FLUX_ADMIN et O.DISTRIBUTION_POL qui permettent la protection en authenticité des flux de politiques et de leurs contextes lors de leur distribution aux chiffreurs IP. O.INTEGRITE_LOGICIELS permet la protection en intégrité des fonctions implémentant ces objectifs de sécurité.

Les objectifs suivants contribuent aussi à la couverture de la menace:

– O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

– O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

– OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

– O.INTEGRITE_LOGICIELS permet la protection en intégrité des fonctions implémentant ces objectifs de sécurité.

T.DIVULGATION_POL

Cette menace est contrée par O.DEFINITION_POL, O.PROTECTION_POL, O.AUTHENTIFICATION_ADMIN qui imposent que les politiques de sécurité VPN et leurs contextes ne peuvent être consultés/visualisées que par des administrateurs de sécurité authentifiés comme tels. De plus, cette menace est aussi contrée par O.PROTECTION_FLUX_ADMIN et O.DISTRIBUTION_POL qui imposent la protection en confidentialité des flux de politiques et de leurs contextes lors de leur distribution aux chiffreurs IP.

Les objectifs suivants contribuent aussi à la couverture de la menace:

– O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

– O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

– OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.COHERENCE_POL

Cette menace est contrée par O.COHERENCE_POL qui garantit la cohérence entre les politiques de sécurité VPN définies par l'administrateur de sécurité et celles appliquées dans les chiffreurs IP.

Les objectifs suivants contribuent aussi à la couverture de la menace :

– O.DISTRIBUTION_POL qui garantit l'intégrité de la politique de sécurité lors de son transfert entre le TDM et le chiffreur.

– O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

– OE.INTEGRITE_TOE, car il garantit que l'intégrité du code des logiciels qui définissent et appliquent les politiques de sécurité VPN peut être vérifiée.

– O.INTEGRITE_LOGICIELS permet la protection en intégrité des fonctions implémentant ces objectifs de sécurité.

8.1.2.1.2 Menaces portant sur la configuration

T.MODIFICATION_PARAM

L'objectif O.PROTECTION_PARAM contre cette menace en protégeant en intégrité les paramètres de configuration. Cet objectif plus O.AUTHENTIFICATION_ADMIN permettent de garantir que seuls les administrateurs système et réseau et les administrateurs de sécurité authentifiés comme tels peuvent accéder à ces paramètres. De plus, O.PROTECTION_FLUX_ADMIN garantit l'intégrité de ces paramètres lorsque ceux-ci sont définis à distance.

Les objectifs suivants contribuent aussi à la couverture de la menace:

– O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

– O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

– OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE

– O.INTEGRITE_LOGICIELS permet la protection en intégrité des fonctions implémentant ces objectifs de sécurité.

T.DIVULGATION_PARAM

L'objectif O.PROTECTION_PARAM contre cette menace en protégeant en confidentialité les paramètres de configuration. Les objectifs O.SUPERVISION, O.AUTHENTIFICATION_ADMIN permettent de garantir que seuls les administrateurs système et réseau et les administrateurs de sécurité authentifiés comme tels peuvent accéder à ces paramètres. De plus, O.PROTECTION_FLUX_ADMIN garantit l'intégrité de ces paramètres lorsque ceux-ci sont définis à distance.

Les objectifs suivants contribuent aussi à la couverture de la menace:

– O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

– O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

– OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

– O.INTEGRITE_LOGICIELS permet la protection en intégrité des fonctions implémentant ces objectifs de sécurité.

8.1.2.1.3 Menaces portant sur la gestion des clés

T.MODIFICATION_CLES

Cette menace est contrée par O.INJECTION_CLES et O.PROTECTION_FLUX_ADMIN lors de l'injection des clés dans les chiffreurs, car ces objectifs garantissent la protection en intégrité des clés lors de leur injection. De plus, les objectifs O.AUTHENTIFICATION_ADMIN garantissent que seuls les administrateurs de sécurité authentifiés comme tels peuvent injecter des clés. Cette menace est aussi contrée par O.ACCES_CLES qui protège l'accès logique aux clés.

Les objectifs suivants contribuent aussi à la couverture de la menace:

– O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

– O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

– OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

– O.INTEGRITE_LOGICIELS permet la protection en intégrité des fonctions implémentant ces objectifs de sécurité.

T.DIVULGATION_CLES

Cette menace est contrée par O.INJECTION_CLES et O.PROTECTION_FLUX_ADMIN lors de l'injection des clés dans les chiffreurs, car ces objectifs garantissent la protection en confidentialité des clés lors de leur injection. De plus, les objectifs O.AUTHENTIFICATION_ADMIN garantissent que seuls les administrateurs de sécurité authentifiés comme tels peuvent injecter des clés. Cette menace est aussi contrée par O.ACCES_CLES qui protège l'accès logique aux clés. Enfin, cette menace est contrée par O.CRYPTO qui garantit un renouvellement régulier des clés et donc rend plus difficile l'utilisation de clés divulguées.

Les objectifs suivants contribuent aussi à la couverture de la menace:

– O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

– O.AUDIT_ADMIN et O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

– OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

– O.INTEGRITE_LOGICIELS permet la protection en intégrité des fonctions implémentant ces objectifs de sécurité.

8.1.2.1.4 Menaces portant sur l'audit

T.MODIFICATION_AUDIT

Cette menace est contrée par O.PROTECTION_AUDIT, O.AUTHENTIFICATION_ADMIN qui imposent que les enregistrements d'événements d'audit ne peuvent être supprimés que par des auditeurs authentifiés comme tels. De plus, cette menace est aussi contrée par O.PROTECTION_FLUX_ADMIN qui permet la protection en intégrité des flux d'événements d'audit nécessaire à la consultation de ceux-ci (à distance) par les auditeurs.

Les objectifs suivants contribuent aussi à la couverture de la menace:

– O.IMPACT_SUPERVISION assure que le service de supervision de la TOE ne remet pas en cause la sécurité des biens sensibles.

– O.AUDIT_ADMIN et O.AUDIT_VPN assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

– OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.MODIFICATION_ALARME

Cette menace est contrée par O.PROTECTION_ALARME qui imposent que les alarmes de sécurité ne peuvent être supprimées que par des administrateurs de sécurité authentifiés comme tels.

Les objectifs suivants contribuent aussi à la couverture de la menace:

– O.ALARMES assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

– OE.INTEGRITE_TOE assure la vérification d'intégrité de la configuration matérielle et logicielle de la TOE.

T.BASE_TEMPS

Cette menace est couverte par l'objectif O.BASE_TEMPS qui garantit la fiabilité de la base de temps.

– OE.INTEGRITE_TOE assure la protection de la base de temps de la TOE.

8.1.2.1.1 Menaces portant sur l'administration

T.USURPATION_ADMIN

Cette menace est contrée par O.AUTHENTIFICATION_ADMIN, car ces objectifs imposent l'authentification (locale et/ou à distance) des différents administrateurs avant d'effectuer toute opération d'administration.

Les objectifs suivants contribuent aussi à la couverture de la menace:

– O.AUDIT_ADMIN et O.AUDIT_VPN assurent que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des événements sont générés pour signaler les tentatives d'usurpation. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit.

T.REJEU_ADMIN

Cette menace est contrée par O.PROTECTION_REJEU_ADMIN, car il empêche le rejeu d'opérations d'administration.

Les objectifs suivants contribuent aussi à la couverture de la menace :

– O.AUDIT_ADMIN et O.AUDIT_VPN assure que les opérations (consultation, modification) effectuées sur les biens sensibles de la TOE ainsi que les utilisations des services de la TOE sont tracées et que des événements sont générés pour signaler les dysfonctionnements de la TOE. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit.

– OE.INTEGRITE_TOE, car il garantit que l'intégrité du code des logiciels qui empêche ce rejeu peut être vérifiée.

– O.INTEGRITE_LOGICIELS permet la protection en intégrité des fonctions implémentant ces objectifs de sécurité.

T.BIENS_INDISPONIBLES

Cette menace est couverte par O.BIENS_INDISPONIBLES, car il impose que la TOE fournisse une fonctionnalité qui permette de rendre les biens sensibles de la TOE indisponibles lors d'un changement de contexte d'utilisation. De plus, cette menace est couverte par OE.PROTECTION_LOCAL, car il impose que les équipements de la TOE doivent se trouver dans un local sécurisé lorsqu'ils contiennent des biens sensibles.

T.MODIFICATION_LOGICIELS

Cette menace est couverte par O.INTEGRITE_LOGICIELS, car l'intégrité du logiciel est vérifiée à chaque démarrage de l'équipement. En cas de détection d'altération du logiciel, O_ALARMES signale l'altération du logiciel.

Cette menace est aussi couverte par OE.INTEGRITE_TOE qui permet la protection en intégrité des fonctions implémentant la vérification d'intégrité du logiciel.

8.1.2.2 Politiques de sécurité organisationnelles (OSP)

OSP.SERVICES_RENDUS

Cette OSP est couverte par O.CONFIDENTIALITE_APPLI, O.AUTHENTICITE_APPLI, O.REJEU_APPLI, O.CONFIDENTIALITE_TOPO et O.AUTHENTICITE_TOPO qui imposent que la TOE fournisse les services de sécurité. Elle est aussi couverte par O.APPLICATION_POL et O.CLOISONNEMENT_FLUX qui imposent que ces services de sécurité sont appliqués et permettent de cloisonner les flux IP.

O.AUDIT_VPN et O.ALARMES couvrent cette OSP, car ils assurent que les opérations concernant les liens VPN sont tracées et que des alarmes de sécurité sont générées pour signaler les dysfonctionnements. Ils permettent ainsi de détecter et de traiter des erreurs ou des attaques après analyse des événements d'audit et des alarmes de sécurité.

Cette OSP est couverte par OE.INTEGRITE_TOE, car il garantit que l'intégrité du code des logiciels qui appliquent les politiques de sécurité VPN peut être vérifiée.

OSP.CRYPTO

Cette OSP est couverte par O.CRYPTO et OE.CRYPTO.

OSP.SUPERVISION

Cette OSP est couverte par O.SUPERVISION.

8.1.2.3 Hypothèses

8.1.2.3.1 Hypothèses sur l'usage attendu de la TOE

A.AUDIT

Cette hypothèse est supportée par OE.ANALYSE_AUDIT.

A.ALARME

Cette hypothèse est supportée par OE.TRAITE_ALARME.

8.1.2.3.2 Hypothèses sur l'environnement d'utilisation de la TOE

A.ADMIN

Cette hypothèse est supportée par OE.ADMIN qui impose la formation des administrateurs à leurs tâches.

A.LOCAL

Cette hypothèse est supportée par OE.PROTECTION_LOCAL, car il impose que les équipements de la TOE ainsi que les supports contenant les biens sensibles de la TOE se trouvent dans un lieu sécurisé.

A.MAITRISE_CONFIGURATION

Cette hypothèse est supportée par OE.INTEGRITE_TOE.

A.CRYPTO

Cette hypothèse est supportée par OE.CRYPTO.

A.CLOISONNEMENT_ADMIN_USER

Cette hypothèse est supportée par O.PROTECTION_FLUX_ADMIN.

8.2 Exigences de sécurité / objectifs de sécurité

8.2.1 Couverture des exigences de sécurité

Objectifs	Exigences
Objectifs de Sécurité pour la TOE	
O.APPLICATION_POL	FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy, FDP_ITC.1/Enforcement_policy, FDP_ETC.1FCS_COP.1/Enforcement_policy
O.CONFIDENTIALITE_APPLI	FCS_COP.1/Enforcement_policy
O.AUTHENTICITE_APPLI	FCS_COP.1/Enforcement_policy
O.REJEU_APPLI	FCS_COP.1/Enforcement_policy
O.CONFIDENTIALITE_TOPO	FCS_COP.1/Enforcement_policy
O.AUTHENTICITE_TOPO	FCS_COP.1/Enforcement_policy
O.CLOISONNEMENT_FLUX	FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy, FDP_ETC.1
O.DEFINITION_POL	FDP_ACC.1, FDP_ACF.1, FDP_ITC.1/VPN_policy, FMT_MSA.3/VPN_policy, FMT_MSA.1, FMT_SMF.1/VPN_policy
O.PROTECTION_POL	FDP_ACC.1, FDP_ACF.1, FMT_MSA.3/VPN_policy, FMT_MSA.1, FMT_SMF.1/VPN_policy
O.AUTHENTIFICATION_MUTUELLE	FCS_COP.1/Mutual_auth, FIA_UAU.4
O.CRYPTO	FCS_COP.1/Enforcement_policy, FCS_COP.1/Mutual_auth, FCS_CKM.1, FCS_CKM.4, FTA_TSE.1
O.ACCES_CLES	FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FMT_MSA.3/Key_policy,, FCS_CKM.4
O.INJECTION_CLES	FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FMT_MSA.3/Key_policy, FDP_UCT.1, FDP_UIT.1, FDP_ITC.1/Key_policy, FDP_ITT.1/Administration, FDP_ITT.3/Administration, FAU_GEN.1.1/Administration, FTP_ITC.1, FTP_TRP.1
O.PROTECTION_PARAM	FMT_MTD.1/Network_param, FMT_MTD.1/Param, FMT_SMF.1/Config_supervision, FDP_IFC.1/Config_audit, FDP_IFF.1/Config_audit
O.SUPERVISION	FMT_SMF.1/Config_supervision
O.IMPACT_SUPERVISION	FDP_ACC.1, FDP_ACF.1, FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy, FMT_MTD.1/Network_param, FMT_MTD.1/Param
O.AUDIT_VPN	FAU_GEN.1/VPN, FAU_SAR.1, FAU_SAR.3
O.AUDIT_ADMIN	FAU_GEN.1/Administration, FAU_SAR.1, FAU_SAR.3
O.PROTECTION_AUDIT	FAU_STG.1, FDP_IFC.1/Config_audit, FDP_IFF.1/Config_audit, FAU_GEN.1/VPN, FAU_GEN.1/Administration
O.ALARMES	FAU_ARP.1, FAU_SAA.1/Alarm
O.PROTECTION_ALARME	FAU_SAA.1 ,
O.BASE_TEMPS	FPT_STM.1

Objectifs	Exigences
O.AUTHENTIFICATION_ADMIN	FMT_SMR.1, FIA_UID.2, FIA_UAU.2, FTP_TRP.1
O.COHERENCE_POL	FDP_ACC.1, FDP_ACF.1, FPT_ITT.1, FPT_ITT.3, FTP_ITC.1
O.DISTRIBUTION_POL	FDP_ACC.1, FDP_ACF.1, FPT_ITT.1, FPT_ITT.3, FTP_ITC.1
O.PROTECTION_REJEU_ADMIN	FPT_RPL.1, FTP_ITC.1
O.PROTECTION_FLUX_ADMIN	FPT_ITT.1, FPT_ITT.3, FTP_ITC.1
O.BIENS_INDISPONIBLES	FDP_RIP.1, FCS_CKM.4
O.INTEGRITE_LOGICIELS	FPT_TST.1, FAU_ARP.1

Table 8-2. Correspondance Objectifs de Sécurité / Exigences Fonctionnelles

8.2.2 Objectifs

8.2.2.1 Objectifs de sécurité pour la TOE

8.2.2.1.1 Objectifs de sécurité sur les services rendus par la TOE

O.APPLICATION_POL

Cet objectif est couvert par la politique d'application VPN (FDP_IFC.1/Enforcement_policy, FDP_IFF.1/Enforcement_policy, FDP_ITC.1/Enforcement_policy et FDP_ETC.1), car elle contrôle les flux de paquets IP en leur appliquant des services de sécurité fournit par les opérations cryptographiques de FCS_COP.1/Enforcement_policy.

O.CONFIDENTIALITE_APPLI

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

O.AUTHENTICITE_APPLI

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

O.REJEU_APPLI

Cet objectif est couvert par FCS_COP.1/Enforcement_policy qui fournit les opérations cryptographiques pour protéger des données du rejeu.

O.CONFIDENTIALITE_TOPO

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

O.AUTHENTICITE_TOPO

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

O.CLOISONNEMENT_FLUX

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

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

8.2.2.1.2.1 Gestion des politiques de sécurité VPN

O.DEFINITION_POL

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

O.PROTECTION_POL

Cet objectif est couvert par la politique de protection des politiques de sécurité VPN qui contrôle les accès à ces politiques et leurs contextes: FDP_ACC.1, FDP_ACF.1,FMT_MSA.3/VPN_policy, FMT_MSA.1 et FMT_SMF.1/VPN_policy.

O.AUTHENTIFICATION_MUTUELLE

Cet objectif est couvert par FCS_COP.1/Mutual_auth, car cette exigence fournit toutes les opérations cryptographiques nécessaires pour le mécanisme d'authentification mutuelle. De plus, cet objectif est couvert par FIA_UAU.4 qui empêche la réutilisation des données d'authentification lors de l'authentification mutuelle.

8.2.2.1.2.2 Gestion des clés cryptographiques

O.CRYPTO

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

- Opérations cryptographiques: FCS_COP.1/Enforcement_policy, FCS_COP.1/Mutual_auth,
- Génération de clés: FCS_CKM.1
- Gestion des durées de validité des certificats d'authentification IKE: FTA_TSE.1
- Destruction des clés: FCS_CKM.4.

O.ACCES_CLES

Cet objectif est couvert par la politique des clés (FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy et FMT_MSA.3/Key_policy) qui contrôle les flux de clés ainsi que par FCS_CKM.4 pour empêcher la lecture des clés en mémoire après leur destruction.

O.INJECTION_CLES

Cet objectif est couvert par la politique des clés (FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy et FMT_MSA.3/Key_policy) qui contrôle les flux de clés dont l'injection de clés (FDP_ITC.1/Key_policy). Par ailleurs, FDP_UCT.1 et FDP_UIT.1 garantissent l'intégrité de toutes les clés et la confidentialité de clés privées et secrètes pendant leur transmission. De plus, cet objectif est couvert par FDP_ITT.1/Administration et FDP_ITT.3/Administration qui assure une protection en confidentialité et intégrité des flux de clés lors d'une injection à distance. Une trace de cette opération est produite par FAU_GEN.1.1/Administration. De plus, cet objectif est couvert par FTP_TRP.1 qui demande la saisie d'un mot de passe pour la personnalisation client à partir d'une clé USB et par FTP_ITC.1 qui implémente un dialogue administratif sécurisé entre le TDM et la TOE.

8.2.2.1.2.3 Configuration et supervision

O.PROTECTION_PARAM

Cet objectif est couvert par FMT_MTD.1/Network_param (pour les paramètres de configuration réseau), FMT_MTD.1/Param (pour les droits d'accès et les données d'authentification) et FMT_SMF.1/Config_supervision, car ces exigences assurent la protection des paramètres de configuration en confidentialité et intégrité en restreignant l'accès aux opérations qui manipulent ces paramètres. De plus, cet objectif est couvert par la politique de configuration et d'audit (FDP_IFC.1/Config_audit et FDP_IFF.1/Config_audit) qui protège en intégrité et en confidentialité les paramètres de configuration lors de leur consultation ou modification à distance.

O.SUPERVISION

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

O.IMPACT_SUPERVISION

Cet objectif est couvert par toutes les politiques de contrôles d'accès et de flux d'information concernant les biens sensibles de la TOE en restreignant l'accès aux opérations manipulant ces biens: FDP_ACC.1, FDP_ACF.1FDP_IFC.1/Key_policy, FDP_IFF.1/Key_policy, FDP_IFC.1/Enforcement_policy et FDP_IFF.1/Enforcement_policy. De plus, pour les mêmes raisons cet objectif est couvert par toutes les exigences portant sur la gestion des données de la TSF: FMT_MTD.1/Network_param et FMT_MTD.1/Param.

8.2.2.1.2.4 Audit et alarme

O.AUDIT_VPN

Cet objectif est couvert par FAU_GEN.1/VPN qui assure la génération d'événement d'audit pour les liens de communication VPN. De plus, cet objectif est aussi couvert par FAU_SAR.1 et FAU_SAR.3 qui fournissent la consultation des événements d'audit.

O.AUDIT_ADMIN

Cet objectif est couvert par FAU_GEN.1/Administration qui assure la génération d'événement d'audit concernant les opérations d'administration. De plus, cet objectif est aussi couvert par FAU_SAR.1 et FAU_SAR.3 qui fournissent la consultation des événements d'audit.

O.PROTECTION_AUDIT

Cet objectif est couvert par FAU_STG.1 qui protège en intégrité les enregistrements d'événements d'audit. Il est aussi couvert par la politique de configuration et d'audit (FDP_IFC.1/Config_audit et FDP_IFF.1/Config_audit) qui protège en intégrité les événements d'audit lors de leur envoi vers un serveur syslog. De plus, FAU_GEN.1/VPN et FAU_GEN.1/Administration permettent de détecter si des événements d'audit ont été perdus.

O.ALARMES

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

O.PROTECTION_ALARME

Cet objectif est couvert par FAU_SAA.1qui protège en intégrité les enregistrements d'alarmes de sécurité.

O.BASE_TEMPS

Cet objectif est directement couvert par l'exigence FPT_STM.1.

8.2.2.1.2.5 Administration locale

O.AUTHENTIFICATION_ADMIN

Cet objectif est couvert par FIA_UID.2 et FIA_UAU.2 qui exige l'identification et l'authentification des utilisateurs avant d'effectuer toute opération d'administration locale ou distante. Cet objectif est couvert par FMT_SMR.1 qui demande le maintien des différents rôles par la TOE. De plus, cet objectif est couvert par FTP_TRP.1 qui demande la saisie d'un mot de passe pour la personnalisation client à partir d'une clé USB.

8.2.2.1.2.6 Administration à distance

O.COHERENCE_POL

Cet objectif est couvert par la politique de protection des politiques de sécurité VPN (FDP_ACC.1 et FDP_ACF.1) qui contrôle l'accès à l'opération de distribution des politiques de sécurité VPN. Il est aussi couvert par FPT_ITT.1 et FPT_ITT.3 qui assure une protection en confidentialité et intégrité des flux de politiques de sécurité VPN lors de cette distribution à distance. Il est aussi couvert par FTP_ITC.1 qui implémente un dialogue administratif sécurisé entre le TDM et la TOE.

O.DISTRIBUTION_POL

Cet objectif est couvert par la politique de protection des politiques de sécurité VPN (FDP_ACC.1 et FDP_ACF.1) qui contrôle l'accès à l'opération de distribution des politiques de sécurité VPN. Il est aussi couvert par FPT_ITT.1 et FPT_ITT.3 qui assure une protection en confidentialité et intégrité des flux de politiques de sécurité VPN lors de cette distribution à distance. Il est aussi couvert par FTP_ITC.1 qui implémente un dialogue administratif sécurisé entre le TDM et la TOE.

O.PROTECTION_REJEU_ADMIN

Cet objectif est couvert par FPT_RPL.1 qui impose la détection du rejeu de séquences de données d'administration ainsi que les actions à réaliser dans en cas de détection. Il est aussi couvert par FTP_ITC.1 qui implémente un dialogue administratif sécurisé entre le TDM et la TOE.

O.PROTECTION_FLUX_ADMIN

Cet objectif est couvert par FPT_ITT.1 et FPT_ITT.3 qui assure la confidentialité (si nécessaire) et l'intégrité des données qui passent dans les flux d'administration. Il est aussi couvert par FTP_ITC.1 qui implémente un dialogue administratif sécurisé entre le TDM et la TOE.

8.2.2.1.2.7 Protection des biens

O.BIENS_INDISPONIBLES

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

O.INTEGRITE_LOGICIELS

Cet objectif est couvert par FPT_TST.1 car l'intégrité du logiciel est vérifiée à chaque démarrage de l'équipement. De plus, en cas de détection d'altération du logiciel, FAU_ARP.1 signale l'altération du logiciel.

Exigences	Objectifs
Exigences fonctionnelles pour la TOE	
FDP_IFC.1/Enforcement_policy	O.APPLICATION_POL, O.CLOISONNEMENT_FLUX, O.IMPACT_SUPERVISION
FDP_IFF.1/Enforcement_policy	O.APPLICATION_POL, O.CLOISONNEMENT_FLUX, O.IMPACT_SUPERVISION
FDP_ITC.1/Enforcement_policy	O.APPLICATION_POL
FDP_ETC.1	O.APPLICATION_POL, O.CLOISONNEMENT_FLUX
FCS_COP.1/Enforcement_policy	O.APPLICATION_POL, O.CONFIDENTIALITE_APPLI, O.REJEU_APPLI, O.AUTHENTICITE_APPLI, O.CONFIDENTIALITE_TOPO, O.AUTHENTICITE_TOPO, O.CRYPTO
FDP_ACC.1	O.DEFINITION_POL, O.PROTECTION_POL, O.IMPACT_SUPERVISION, O.DISTRIBUTION_POL, O.COHERENCE_POL
FDP_ACF.1,	O.DEFINITION_POL, O.PROTECTION_POL, O.IMPACT_SUPERVISION, O.DISTRIBUTION_PO, O.COHERENCE_POL
FDP_ITC.1/VPN_policy	O.DEFINITION_POL
FMT_MSA.3/VPN_policy	O.DEFINITION_POL, O.PROTECTION_POL
FMT_MSA.1	O.DEFINITION_POL, O.PROTECTION_POL
FMT_SMF.1/VPN_policy	O.DEFINITION_POL, O.PROTECTION_POL
FCS_COP.1/Mutual_auth	O.AUTHENTIFICATION_MUTUELLE, O.CRYPTO
FIA_UAU.4	O.AUTHENTIFICATION_MUTUELLE
FDP_ITC.1/Key_policy	O.INJECTION_CLES
FDP_IFC.1/Key_policy	O.ACCES_CLES, O.INJECTION_CLES, O.IMPACT_SUPERVISION
FDP_IFF.1/Key_policy	O.ACCES_CLES, O.INJECTION_CLES, O.IMPACT_SUPERVISION
FDP_UCT.1	O.INJECTION_CLES
FDP_UIT.1	O.INJECTION_CLES
FMT_MSA.3/Key_policy	O.ACCES_CLES, O.INJECTION_CLES
FCS_CKM.1	O.CRYPTO
FTA_TSE.1	O.CRYPTO
FCS_CKM.4	O.CRYPTO, O.BIENS_INDISPONIBLES, O.ACCES_CLES
FMT_MTD.1/Network_param	O.PROTECTION_PARAM, O.IMPACT_SUPERVISION
FMT_MTD.1/Param	O.PROTECTION_PARAM, O.IMPACT_SUPERVISION

Exigences	Objectifs
FMT_SMF.1/Config_supervision	O.PROTECTION_PARAM, O.SUPERVISION
FPT_ITT.1	O.DISTRIBUTION_POL, O.COHERENCE_POL , O.PROTECTION_FLUX_ADMIN
FPT_ITT.3	O.DISTRIBUTION_POL, O.COHERENCE_POL , O.PROTECTION_FLUX_ADMIN
FDP_IFC.1/Config_audit	O.PROTECTION_PARAM, O.PROTECTION_AUDIT,
FDP_IFF.1/Config_audit	O.PROTECTION_PARAM, O.PROTECTION_AUDIT,
FPT_RPL.1	O.PROTECTION_REJEU_ADMIN
FPT_TST.1	O.INTEGRITE_LOGICIELS
FDP_RIP.1	O.BIENS_INDISPONIBLES
FAU_GEN.1/VPN	O.AUDIT_VPN, O.PROTECTION_AUDIT
FAU_GEN.1/Administration	O.AUDIT_ADMIN, O.PROTECTION_AUDIT, O.INJECTION_CLES
FAU_SAR.1	O.AUDIT_VPN, O.AUDIT_ADMIN
FAU_SAR.3	O.AUDIT_VPN, O.AUDIT_ADMIN
FAU_STG.1	O.PROTECTION_AUDIT, O.PROTECTION_ALARME
FAU_ARP.1	O.ALARMES
FAU_SAA.1/Alarm	O.ALARMES
FPT_STM.1	O.BASE_TEMPS
FMT_SMR.1	O.AUTHENTIFICATION_ADMIN
FIA_UID.2	O.AUTHENTIFICATION_ADMIN
FIA_UAU.2	O.AUTHENTIFICATION_ADMIN
FTP_TRP.1	O.AUTHENTIFICATION_ADMIN, O.INJECTION_CLES
FTP_ITC.1	O.INJECTION_CLES, O.DISTRIBUTION_POL, O.COHERENCE_POL, O.PROTECTION_REJEU_ADMIN, O.PROTECTION_FLUX_ADMIN

Table 8-3. Correspondance Exigences Fonctionnelles / Objectifs de Sécurité

8.3 Exigences de sécurité/Spécifications fonctionnelles

8.3.1 Couverture des fonctions de sécurité de la TOE

Exigences de sécurité	Fonctions de sécurité de la TOE
FDP_IFC.1/Enforcement_policy	SF.USER_DATA_PROTECTION
FDP_IFF.1/Enforcement_policy	SF.USER_DATA_PROTECTION
FDP_ITC.1/Enforcement_policy	SF.USER_DATA_PROTECTION
FDP_ETC.1	SF.USER_DATA_PROTECTION
FCS_COP.1/Enforcement_policy	SF.USER_DATA_PROTECTION
FDP_ACC.1	SF.ROLES
FDP_ACF.1,	SF.USER_DATA_PROTECTION
FDP_ITC.1/VPN_policy	SF.USER_DATA_PROTECTION
FMT_MSA.3/VPN_policy	SF.ADMINISTRATION
FMT_MSA.1	SF.ADMINISTRATION
FMT_SMF.1/VPN_policy	SF.ADMINISTRATION
FCS_COP.1/Mutual_auth	SF.USER_DATA_PROTECTION
FIA_UAU.4	SF.USER_DATA_PROTECTION
FDP_ITC.1/Key_policy	SF.ADMINISTRATION
FDP_IFC.1/Key_policy	SF.ADMINISTRATION
FDP_IFF.1/Key_policy	SF.USER_DATA_PROTECTION
FDP_UCT.1	SF.ADMINISTRATION
FDP_UIT.1	SF.ADMINISTRATION
FMT_MSA.3/Key_policy	SF.ADMINISTRATION
FCS_CKM.1	SF.USER_DATA_PROTECTION
FTA_TSE.1	SF.USER_DATA_PROTECTION
FCS_CKM.4	SF.REINIT
FMT_MTD.1/Network_param	SF.ADMINISTRATION
FMT_MTD.1/Param	SF.ADMINISTRATION
FMT_SMF.1/Config_supervision	SF.ADMINISTRATION
FPT_ITT.1	SF.REMOTE_ADMIN_PROTECTION
FPT_ITT.3	SF.REMOTE_ADMIN_PROTECTION
FDP_IFC.1/Config_audit	SF.AUTHENTICATION.ADMIN
FDP_IFF.1/Config_audit	SF.AUTHENTICATION.ADMIN
FPT_RPL.1	SF.REMOTE_ADMIN_PROTECTION
FPT_TST.1	SF.SOFTWARE_INTEGRITY
FDP_RIP.1	SF.REINIT

Exigences de sécurité	Fonctions de sécurité de la TOE
FAU_GEN.1/VPN	SF.AUDIT
FAU_GEN.1/Administration	SF.AUDIT
FAU_SAR.1	SF.AUDIT
FAU_SAR.3	SF.AUDIT
FAU_STG.1	SF.AUDIT
FAU_ARP.1	SF.AUDIT
FAU_SAA.1/Alarm	SF.AUDIT
FPT_STM.1	SF.AUDIT
FMT_SMR.1	SF.ROLES
FIA_UID.2	SF.LOCAL_ADMIN_AUTHENTICATION, SF.REMOTE_ADMIN_AUTHENTICATION
FIA_UAU.2	SF.LOCAL_ADMIN_AUTHENTICATION, SF.REMOTE_ADMIN_AUTHENTICATION
FTP_TRP.1	SF.LOCAL_ADMIN_AUTHENTICATION
FTP_ITC.1	SF.REMOTE_ADMIN_PROTECTION

Table 8-4. Correspondance Exigences de Sécurité – Fonctions de Sécurité de la TOE

8.4 Dépendances

8.4.1 Dépendances des exigences de sécurité fonctionnelles et d'assurance

Exigence	Dépendances exigées par les CC	Dépendances satisfaites
Exigences fonctionnelles pour la TOE		
FDP_IFC.1/Enforcement_policy	(FDP_IFF.1)	FDP_IFF.1/Enforcement_policy
FDP_IFF.1/Enforcement_policy	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ITC.1/Enforcement_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Enforcement_policy, FMT_MSA.3/VPN_policy
FDP_ETC.1	(FDP_ACC.1 ou FDP_IFC.1)	FDP_IFC.1/Enforcement_policy
FCS_COP.1/Enforcement_policy	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.1/Key_policy, FCS_CKM.4
FDP_ACC.1	(FDP_ACF.1)	FDP_ACF.1,
FDP_ACF.1	(FDP_ACC.1) et (FMT_MSA.3)	FDP_ACC.1, FMT_MSA.3/VPN_policy
FDP_ITC.1/VPN_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_ACC.1, FMT_MSA.3/VPN_policy
FMT_MSA.3/VPN_policy	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1. FMT_SMR.1
FMT_MSA.1.	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1, FMT_SMF.1/VPN_policy, FMT_SMR.1
FMT_SMF.1/VPN_policy	Pas de dépendance	
FCS_COP.1/Mutual_auth	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FDP_ITC.1/Key_policy, FCS_CKM.4
FIA_UAU.4	Pas de dépendance	
FDP_ITC.1/Key_policy	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Key_policy, FMT_MSA.3/Key_policy
FDP_IFC.1/Key_policy	(FDP_IFF.1)	FDP_IFF.1/Key_policy
FDP_IFF.1/Key_policy	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Key_policy, FMT_MSA.3/Key_policy
FDP_UCT.1	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Key_policy FTP_ITC.1 FTP_TRP.1
FDP_UIT.1	(FDP_ACC.1 ou FDP_IFC.1) et (FTP_ITC.1 ou FTP_TRP.1)	FDP_IFC.1/Key_policy FTP_ITC.1 FTP_TRP.1
FMT_MSA.3/Key_policy	(FMT_MSA.1) et (FMT_SMR.1)	FMT_SMR.1

Exigence	Dépendances exigées par les CC	Dépendances satisfaites
FCS_CKM.1	(FCS_CKM.2 ou FCS_COP.1) et (FCS_CKM.4)	FCS_COP.1/Enforcement_policy, FCS_COP.1/Mutual_auth, FCS_CKM.4
FTA_TSE.1	Pas de dépendance	
FCS_CKM.4	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)	FDP_ITC.1/Key_policy et FCS_CKM.1
FMT_MTD.1/Network_param	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1
FMT_MTD.1/Param	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1/Config_supervision, FMT_SMR.1
FMT_SMF.1/Config_supervision	Pas de dépendance	
FPT_ITT.1.	Pas de dépendance	
FPT_ITT.3	(FPT_ITT.1)	FPT_ITT.1
FDP_IFC.1/Config_audit	(FDP_IFF.1)	FDP_IFF.1/Config_audit
FDP_IFF.1/Config_audit	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.1/Config_audit
FPT_RPL.1	Pas de dépendance	
FPT_TST.1	Pas de dépendance	
FDP_RIP.1	Pas de dépendance	
FAU_GEN.1/VPN	(FPT_STM.1)	FPT_STM.1
FAU_GEN.1/Administration	(FPT_STM.1)	FPT_STM.1
FAU_SAR.1	(FAU_GEN.1)	FAU_GEN.1/VPN, FAU_GEN.1/Administration
FAU_SAR.3	(FAU_SAR.1)	FAU_SAR.1
FAU_STG.1	(FAU_GEN.1)	FAU_GEN.1/VPN, FAU_GEN.1/Administration
FAU_ARP.1	(FAU_SAA.1)	FAU_SAA.1/Alarm
FAU_SAA.1/Alarm	(FAU_GEN.1)	FAU_GEN.1/VPN, FAU_GEN.1/Administration
FPT_STM.1	Pas de dépendance	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	Pas de dépendance	
FIA_UAU.2	(FIA_UID.1)	FIA_UID.2
FTP_ITC.1	Pas de dépendance	
FTP_TRP.1	Pas de dépendance	
Exigences d'assurance		
ADV_ARC.1	(ADV_FSP.1) et (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) et (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4

Exigence	Dépendances exigées par les CC	Dépendances satisfaites
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	Pas de dépendance	
ALC_CMC.3	(ALC_CMS.1) et (ALC_DVS.1) et (ALC_LCD.1)	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	Pas de dépendance	
ALC_DEL.1	Pas de dépendance	
ALC_DVS.1	Pas de dépendance	
ALC_FLR.3	Pas de dépendance	
ALC_LCD.1	Pas de dépendance	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ATE_COV.2	(ADV_FSP.2) et (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) et (ADV_TDS.2) et (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) et (AGD_OPE.1) et (AGD_PRE.1) et (ATE_COV.1) et (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) et (ADV_FSP.4) et (ADV_IMP.1) et (ADV_TDS.3) et (AGD_OPE.1) et (AGD_PRE.1) et (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 8-5. Dépendances des exigences de sécurité fonctionnelles et d'assurance

8.4.2 Argumentaire pour les dépendances non satisfaites

La dépendance FMT_MSA.1 de FMT_MSA.3/Key_policy n'est pas supportée. L'attribut de sécurité AT.key_type ne possède que l'opération de consultation qui est fournie seulement aux TSF. Comme cette opération n'est pas fournie à un rôle donné, cette dépendance n'est pas satisfaite.

La dépendance FMT_MSA.3 de FDP_IFF.1/Config_audit n'est pas supportée. Comme il n'y a pas d'attribut de sécurité utilisé dans cette politique de contrôle de flux d'information, cette dépendance n'est pas satisfaite.

8.5 Besoins de sécurité

Le tableau suivant résume les protections associées à chaque bien :

- C : Confidentialité ;
- I : Intégrité ;

- A : Authenticité ;
- R : Anti-rejeu ;
- D : Disponibilité.

Description	C	I	A	R	D
Biens protégés par la TOE					
D.DONNEES_APPLICATIVES	X	X	X	X	
D.INFO_TOPOLOGIE	X	X	X		
Exigences d'assurance					
D.POLITIQUES_VPN	X	X			
D.PARAM_CONFIG	X	X			
D.CLES_CRYPTO	X	X			
D.AUDIT		X			
D.ALARMES		X			
D.LOGICIELS		X			
D.BASE_TEMPS		X			

Table 8-6. Besoins de sécurité

8.6 Argumentaire pour les augmentations à l'EAL

8.6.1 ALC_FLR.3 Systematic flaw remediation

Augmentation requise par le processus de qualification standard [9].

8.6.2 ALC_TAT.1 Well-defined development tools

Augmentation requise par le processus de qualification standard [9].

8.6.3 AVA_VAN.3 Focused vulnerability analysis

Augmentation requise par le processus de qualification standard [9].

8.6.4 ADV_IMP.1 Implementation representation of the TSF

Augmentation requise par le processus de qualification standard [9].

8.6.5 ADV_FSP.4 Complete functional specification

Augmentation requise par le processus de qualification standard [9].

8.6.6 ADV_TDS.3 Basic modular design

Augmentation requise par le processus de qualification standard [9].

Chapitre 9.Tableau des exigences supportées du référentiel IPSec DR de l'ANSSI

Matrice de conformité à la checklist du référentiel IPsecDR - Version BULL du 05/07/2021 relative à la version 6.01.17 de la TOE Document de référence : checklist-ipsec-dr.pdf reçue le 18/02/21				
N°	**Items Référentiel Ipsec DR**	**Conformité**	**Planning prévisionnel de mise en conformité**	**Commentaires**
1	Un élément de configuration (e.g. case à cocher, commande unique spécifique, etc) permet de mettre la ToE dans un état de configuration compatible de celui imposé par le référentiel (activation des fonctionnalités requises, désactivation des fonctionnalités interdites, désactivation des éléments crypto interdits, etc).	Conforme	NA	Case à cocher dans la configuration TDM. Si cette case est cochée, les menus non conformes à IPSec DR sont grisés. Cette information fait partie de la configuration TDM et est envoyée au chiffreur. Le positionnement de cette coche provoque une erreur si une option non IPSec DR est présente dans la configuration. Le chiffreur qui reçoit cette option refusera notamment les certificats RSA.
2	L'ensemble des valeurs par défaut des options de la ToE favorisent la sécurité, i.e. tout mécanisme augmentant la surface d'attaque ou réduisant la sécurité de la ToE est désactivé.	Conforme	NA	Toutes les fonctionnalités non nécessaires au chiffreur (en mode IPSec DR ou coexistence avec les anciens chiffreurs) sont absentes.
3	Le démon IKEv2 de la ToE implémente et négocie AES-GCM avec clé de 256 bits et ICV de 16 octets pour la protection des IKE_SA et des SA Ipsec	Conforme	NA	
4	Le démon IKEv2 et la pile IPsec de la ToE utilisent tous les deux des IV incrémentaux pour leurs implémentations d'AES_GCM	Conforme	NA	
5	Le démon IKEv2 de la ToE implémente et négocie AES-CTR avec clé de 256 bits et AUTH_HMAC_SHA2_256_128 pour la protection des IKE_SA et des SA Ipsec	Conforme	NA	La négociation entre deux chiffreurs Trustway IP Protect aboutira toujours à l'utilisation de l'AES GCM pour la protection des IKE SA et des SA Ipsec. Ce mode sera supporté pour interopérabilité avec des équipements tiers.

6	Le démon IKEv2 et la pile IPsec de la ToE utilisent tous les deux des IV incrémentaux pour leurs implémentations d'AES-CTR	Conforme	NA	
7	Aucune autre combinaison de mécanismes crypto que ceux listés ci-dessus n'est activée pour assurer la confidentialité et l'intégrité des données du démon IKEv2 et de la pile IPsec de la ToE.	Conforme	NA	
8	L'unique PRF négociée et utilisée dans le démon IKEv2 de la ToE est PRF_HMAC_SHA2_256.	Conforme	NA	
9	Le démon IKEv2 de la ToE implémente ECSDSA sur BrainpoolP256r1 avec SHA256 comme mécanisme d'authentification asymétrique (Auth Method 228, comme indiqué dans [NOTE-CRYPTO]).	Conforme	NA	Ce mode sera supporté pour interopérabilité avec des équipements tiers. Les chiffreurs Trustway IP Protect s'authentifieront entre eux en ECDSA sur secp256r1 avec SHA256.
10	Le démon IKEv2 de la ToE implémente ECSDSA sur secp256r1 avec SHA256 comme mécanisme d'authentification asymétrique (Auth Method 225, comme indiqué dans [NOTE-CRYPTO]).	Conforme	NA	Ce mode sera supporté pour interopérabilité avec des équipements tiers. Les chiffreurs Trustway IP Protect s'authentifieront entre eux en ECDSA sur secp256r1 avec SHA256.
11	L'implémentation ECSDSA du démon IKEv2 de la ToE inclut les vérifications complémentaires indiquées en section 3.3.3 de la note crypto du référentiel IPsec DR.	Conforme	NA	
12	Le démon IKEv2 de la ToE implémente ECDSA sur BrainpoolP256r1 avec SHA256 comme mécanisme d'authentification asymétrique (Auth Method 214, comme indiqué dans [NOTE-CRYPTO]).	Conforme	NA	
13	Le démon IKEv2 de la ToE implémente ECDSA sur secp256r1 avec SHA256 comme mécanisme d'authentification asymétrique (Auth Method 9, comme indiqué dans [NOTE-CRYPTO]).	Conforme	NA	
14	L'implémentation ECDSA du démon IKEv2 de la ToE inclut les vérifications complémentaires indiquées en section 3.4.3 de la note crypto du référentiel IPsec DR.	Conforme	NA	

15	Le démon IKEv2 de la ToE utilise PRF_HMAC_SHA2_256 comme mécanisme d'authentification symétrique (dans le cadre de l'Auth Method 2 et de la négociation de la PRF PRF_HMAC_SHA2_256).	Conforme	NA	Le mode PSK sera supporté pour interopérabilité avec des équipements tiers. Les chiffreurs Trustway IP Protect s'authentifieront entre eux en ECDSA sur secp256r1 avec SHA256.
16	Le démon IKEv2 de la ToE ne met en oeuvre aucun autre mécanisme d'authentification que les 5 listés ci-dessus.	Conforme	NA	
17	Le démon IKEv2 de la ToE négocie et impose le support de l'anti-rejeu via ESN en émission et réception.	Conforme	NA	
18	Le démon IKEv2 de la ToE implémente, négocie et impose le support des Childless SA défini dans [RFC6023].	Conforme	NA	
19	Le démon IKEv2 n'émet donc en particulier aucun payload SA ou TS lors de l'échange IKE_AUTH	Conforme	NA	
20	Le démon IKEv2 refuse tout échange IKE_AUTH contenant un payload SA ou TS	Conforme	NA	
21	Le démon IKEv2 de la ToE implémente et négocie secp256r1 comme groupe ECDH	Conforme	NA	
22	Le démon IKEv2 de la ToE implémente et négocie BrainpoolP256r1 comme groupe ECDH	Conforme	NA	Ce mode sera supporté pour interopérabilité avec des équipements tiers. Les chiffreurs Trustway IP Protect négocieront entre eux en ECDH sur secp256r1
23	Le démon IKEv2 de la ToE implémente et négocie les Diffie-Hellman Group Transform Ids 19 (256-bit random ECP group basé sur secp256r1) et 28 (brainpoolP256r1)	Conforme	NA	Ce mode sera supporté pour interopérabilité avec des équipements tiers. Les chiffreurs Trustway IP Protect négocieront entre eux en ECDH sur secp256r1
24	Le démon IKEv2 de la ToE ne négocie et n'utilise aucun autre Diffie-Hellman Group Transform IDs que ceux listés ci-dessus.	Conforme	NA	
25	Les payloads ID émis par le démon IKEv2 de la ToE n'incluent pas de données topologiques	Conforme	NA	Le certificat du chiffreur issu d'un CSR créé par la SPC ne contient pas d'ID de type adresses IPv4 ou IPv6.
26	Le démon IKEv2 de la ToE ne produit des payloads SA dont les proposal ne contiennent chacune qu'au plus une seule instance de chaque type de transform.	Conforme	NA	
27	Le démon IKEv2 ne propose pas et refuse le support d'Ipcomp	Conforme	NA	

28	Le démon IKEv2 ne permet que la mise en oeuvre de SA IPsec utilisant ESP en mode Tunnel (pas de mode transport, pas d'AH, etc).	Conforme	NA	
29	Lors d'une authentification asymétriques, le démon IKEv2 de la ToE vérifie la validité des certificats présentés par l'homologue (remontée à une racine de confiance locale, validité temporelle, validité du keyUsage, validation de l'identité, etc).	Conforme	NA	Vérification faite sur la chaine totale de certificat jusqu'au Root CA
30	Le démon IKEv2 de la ToE supporte et utilise la prise en compte de CRL comme mécanisme de révocation lors de l'utilisation de la validation de certificat.	Conforme	NA	
31	Le démon IKEv2 de la ToE supporte et utilise OCSP comme mécanisme de révocation lors de l'utilisation de la validation de certificat	Conforme	NA	
32	Les paquets IKEv2 et ESP reçus par la ToE avec une intégrité cryptographique invalide sont rejetés silencieusement par la ToE. Il en est de même des paquets rejoués.	Conforme	NA	
33	Le démon IKEv2 de la ToE émet et attend des payload KE (et NONCE) lors de chaque échange CREATE_CHILD_SA, i.e. chaque négociation de SA IPsec utilise un secret frais basé sur un échange ECDH utilisant l'un des deux groupes définis précédemment	Conforme	NA	
34	Lors des générations de points aléatoires sur une courbe par tirage d'une valeur secrète k dans]0,q[(q étant l'ordre de la courbe), la méthode de génération de k associé à un générateur d'aléa cryptographique conforme au RGS et est implémentée sous la forme de l'une des deux méthodes présentée en section 7.1 de [NOTE-CRYPTO].	Conforme	NA	Utilisation de la première méthode avec une taille de (3|q|/2)+1
35	Le démon IKEv2 de la ToE réalise les vérifications d'usage en terme de format et de valeur attendus sur les paramètres ECDH reçus dans les payloads KE, comme précisé en section 4.4 de [NOTE-CRYPTO].	Conforme	NA	
36	Les nonces produits par le démon IKEv2 ont une taille de 16 octets.	Conforme	NA	

37	Tout nonce reçu d'un homologue d'une taille inférieure à 16 octets résulte en un arrêt de l'échange.	Conforme	NA	
38	Chaque production d'un secret partagé via un échange de payload KE met en oeuvre une valeur secrète éphémère générée spécifiquement pour l'occasion et d'une manière sûre, et effacée de manière sûre après calcul du secret partagé. Ce dernier point est validé spécifiquement dans le binaire produit pour la ToE	Conforme	NA	
39	Le démon IKEv2 de la ToE utilise par défaut le mécanisme de COOKIE défini dans [RFC7296].	Conforme	NA	
40	Le démon IKEv2 n'utilise que le port 4500 UDP et met toujours en oeuvre les mécanismes de NAT-Traversal sans négociation	Conforme	NA	
41	Le démon IKEv2 de la ToE est développé de manière défensive et met en oeuvre des mécanismes de défense en profondeur	Conforme	NA	Utilisation en particulier de GRSec et mise en œuvre de RBAC
42	Les toolchains utilisés pour compiler la ToE sont à l'état de l'art et tirent partie de l'ensemble des mécanismes de durcissement disponibles. Les mécanismes de durcissement non activés sont listés et des justifications sérieuses sont apportées.	Conforme	NA	Fourniture de la liste des mécanismes de durcissement utilisés
43	L'ensemble des paquets ESP sont transportés encapsulés sur UDP port 4500	Conforme	NA	
44	La pile IPsec de la ToE implémente AES-GCM avec clé de 256 bits et ICV de 16 octets	Conforme	NA	
45	La pile IPsec de la ToE implémente AES-CTR avec clé de 256 bits et AUTH_HMAC_SHA2_256_128	Conforme	NA	Réservé à la communication avec d'autres types de chiffreurs.
46	La ToE implémente dans ses mécanismes d'auto-test les différents vecteurs de test fournis dans la note crypto [NOTE-CRYPTO]	Conforme	NA	

47	La ToE implémente les formats d'encodage de données fournis dans la note crypto [NOTE-CRYPTO]	Conforme	NA	Conformément à la [NOTE-CRYPTO] les formats d'encodage: - Du payload AUTH IKE - Du payload KE IKE - Du payload SA IKE sont respectés
48	Si la ToE met en oeuvre des coprocesseurs cryptographiques, celle-ci respecte [ANSSI-CC-CRY-P-01].	Conforme	NA	Le coprocesseur cryptographique DH8925 n'est utilisé que dans le mode de coexistence avec CRX et TVPN3 (non IPSec DR).
49	Le démon IKEv2 de la ToE supporte une window size de 1 non configurable, i.e. n'émet, ni n'accepte de notification SET_WINDOW_SIZE permettant de changer cette valeur. Toute notification SET_WINDOW_SIZE est ignorée	Conforme	NA	
50	La pile IPsec de la ToE ne produit pas pour une SA donnée de déséquencement de paquet avec une distance supérieure à 64, quelle que soit le la taille ou le débit considéré.	Conforme	NA	Utilisation d'un seul core par interface de réception et d'un seul core par interface d'émission. Allocation séquentielle des numéros de séquence.
51	La pile IPsec de la ToE supporte une fenêtre anti-rejeu d'au moins 1024 paquets par SA	Conforme	NA	
52	La pile IPsec de la ToE ne permet pas la désactivation des mécanismes d'anti-rejeu.	Conforme	NA	
53	La pile IPsec de la ToE implémente bien après déchiffrement une vérification des paquets contre la SP associée à la SA ayant permis le déchiffrement	Conforme	NA	
54	La ToE permet l'export des clés d'authentification symétrique (Auth Method 2) et asymétrique (Auth Method 9, 214, 225 et 228) dans un format documenté permettant la mise en place d'interopérabilité avec un autre équipement compatible du référentiel	Conforme	NA	Le PSK peut être récupéré sur le TDM. Le certificat du chiffreur peut être récupéré sur la SPC.
55	L'ensemble des composants logiciels de la ToE traitants des données extérieures sont programmés de manière défensive	Conforme	NA	
56	L'ensemble des composants logiciels de la ToE traitants des données extérieures sont compilés avec les différentes options de durcissement de la toolchain utilisée	Conforme	NA	

57	L’ensemble des composants logiciels de la ToE traitants des données extérieures sont compilés avec un niveau de warning élevé	Conforme	NA	
58	L’ensemble des composants logiciels de la ToE traitants des données extérieures compilent sans warning	Conforme	NA	
59	L’ensemble des composants logiciels de la ToE traitants des données extérieures sont compilés sans options de debug	Conforme	NA	
60	La toolchain utilisée pour la compilation des composants logiciels de la ToE est récente et à jour	Conforme	NA	
61	La ToE utilise les fonctionnalités de durcissement applicatifs fournis par l’OS support (e.g. ASLR, diminution de privilège, sandboxings, etc).	Conforme	NA	
62	La ToE fait un usage par défaut nul des mécanismes de bypass, garantissant ainsi par défaut l’absence de fuite de données claires vers l’extérieur	Conforme	NA	Lié à l'exigence 1