Firewalls NETASQ

Cible de sécurité - Suite logicielle IPS-Firewall Version 9.1

Évaluation selon un paquet EAL3 augmenté des Critères Communs V3.1

NETASQ

Secure Internet Connectivity

SUIVI DE DOCUMENT

Version	Auteur	Date	Modifications
1.0	Boris MARECHAL	01/07/2008	Intégration des commentaires de la DCSSI
1.1	Boris MARECHAL	11/09/2008	Intégration des commentaires préparation AQL
1.2	Ludovic FLAMENT	08/10/2008	Mise à jour des RFCs
1.3	Ludovic FLAMENT	31/10/2008	Intégration des commentaires du CESTI (JO-FdC01-ASE)
1.4	Ludovic FLAMENT	15/04/2009	Mise à jour du numéro de version de la libevent ajout remarques CESTI (JO-FdC03-ADV_FSP et JO-FdC10-ASE), mise à jour version TOE
1.5	Boris MARECHAL	24/01/2011	Mise à jour pour version 8.1.3
1.6	Boris MARECHAL	09/06/2011	Mise à jour suite aux remarques CESTI
1.7	Ludovic FLAMENT	20/02/2012	Mise à jour pour version 9.1
1.8	Ludovic FLAMENT	24/05/2012	Mise à jour suite remarque ANSSI
1.9	Ludovic FLAMENT	09/07/2012	Mise à jour suite remarques CESTI
1.10	Ludovic FLAMENT	12/11/2012	Ajout interfaces physiques, mise à jour FDP_IFF.1.Chiffrement.3
1.11	Ludovic FLAMENT	07/12/2012	Ajout Windows Seven, suppression FIA_UID.2
1.12	Ludovic FLAMENT	15/04/2013	Mise à jour suite remarque ANSSI
1.13	Boris MARECHAL	13/06/2014	Mise à jour pour version 9.1.0.5 (openssl 1.0.1h)

TABLE DES MATIÈRES

TABLE DES ILLUSTRATIONS

1 INTRODUCTION

Le but de cette section est de fournir des informations d'identification et de référence précises pour le présent document et pour le produit qui fait l'objet de l'évaluation, ainsi que les annonces appropriées de conformité aux Critères Communs et à d'autres référentiels applicables. Elle apporte également une vue d'ensemble des fonctionnalités du Firewall-VPN NETASQ.

1.1 Identification de la cible de sécurité

Titre :	Cible de sécurité - Suite logicielle IPS-Firewall Version 9.1
Référence de la ST :	NA_ASE_ciblesec_v91
Version de la ST :	1.13
Cible d'évaluation :	Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ
Version de la TOE :	9.1.0.5 (S, M, L, XL)
Paquet d'assurance sécurité :	EAL3 augmenté de ALC_CMS.4, ALC_CMC.4, ALC_FLR.3 et AVA_VAN.3.

1.2 Annonces de conformité

La version des Critères Communs applicable est la version 3.1 révision 3 de juillet 2009.

La fonctionnalité de sécurité de la cible d'évaluation est « Conforme à la partie 2 étendue des Critères Communs » avec l'introduction du composant FMT_MTD.BRS.

Les mesures d'assurance sécurité mises en œuvre sur la cible d'évaluation sont « Conformes à la partie 3 stricte des Critères Communs ».

Aucune annonce de conformité à un quelconque Profil de Protection ou à tout autre paquet d'exigences de sécurité, que celui sélectionné, n'est formulée.

Le paquet d'assurance sécurité sélectionné est une extension du paquet EAL3 augmenté des composants ALC_CMS.4, ALC_CMC.4, ALC_FLR.3 et AVA_VAN.3.

Ce paquet d'exigences d'assurance inclut toutes les exigences d'assurances demandées au titre de la qualification standard [QUALIF-STD].

1.3 Résumé des fonctionnalités du firewall-VPN NETASQ

Les firewall-VPN de la gamme NETASQ sont des boîtiers appliances fournissant les fonctionnalités de sécurité autorisant l'interconnexion entre un ou plusieurs réseaux de confiance (une ou plusieurs DMZ, etc.) et un réseau non maîtrisé, sans dégrader le niveau de sécurité du ou des réseaux de confiance.

Les fonctionnalités principales de la suite logicielle IPS-Firewall, qui équipe ces boîtiers, consistent en deux grands groupes :

- la fonctionnalité firewall regroupant : filtrage, détection d'attaques, gestion de la bande passante, gestion de la politique de sécurité, audit, imputabilité, authentification forte des administrateurs,

- la fonctionnalité VPN (Réseau Privé Virtuel : chiffrement et authentification) implémentant le protocole ESP en mode tunnel du standard IPSec, et sécurisant la transmission des données confidentielles entre sites distants, partenaires ou commerciaux nomades.

L'ASQ (Active Security Qualification) est une technologie de Prévention d'Intrusion en Temps Réel, intégrée dans tous les boîtiers appliances firewall-VPN de la gamme NETASQ. Basée sur une analyse multi-couches, l'ASQ détecte et empêche les attaques les plus élaborées sans diminuer les performances du boîtier firewall-VPN et réduit considérablement le nombre de faux positifs. Cette technologie est soutenue par des fonctionnalités d'alarme entièrement configurables.

Pour offrir les fonctionnalités d'authentification forte des administrateurs, la suite logicielle IPS-Firewall intègre une base d'utilisateurs et offre des services d'authentification auprès de celle-ci.

La suite logicielle IPS-Firewall comprend un package complet de fonctionnalités d'administration à distance, qui est constitué des outils NETASQ Web Manager, NETASQ Real-Time Monitor et NETASQ Event Reporter. Tous ces outils comportent une interface graphique intuitive et conviviale sous plate-forme Windows (Real-Time Monitor et Event Reporter) ou multi-plateforme (Web Manager), permettant une facilité d'installation et de configuration des boîtiers appliances firewall-VPN ainsi que des fonctionnalités de monitoring et de reporting simplifiées.

1.4 Documents applicables et de référence

1.4.1 Référentiel des Critères Communs

[CC-01] *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3 – Part 1: Introduction and general model*,
CCMB-2009-07-001, July 2009.

[CC-02] *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3 – Part 2: Security functional components*
CCMB-2009-07-002, July 2009.

[CC-03] *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3 – Part 3: Security assurance components*
CCMB-2009-07-003, July 2009.

[CEM-02] *Common Criteria - Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3 – Evaluation Methodology*
CCMB-2009-07-004, July 2009.

1.4.2 Référentiel de la Qualification Standard

[QUALIF-STD] *Référentiel Général de Sécurité, Processus de qualification d'un produit de sécurité – niveau standard – version* 1.2.

1.4.3 Schéma Français d'Évaluation et de Certification

[MQC] *Manuel Qualité du Centre de Certification, Version 1.0* Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI),
CCN-MQ.01, Janvier 2004.

1.4.4 RFC et autres standards supportés

[IP] P. Almquist, *Type of Service in the Internet Protocol Suite*, RFC 1349, July 1992.

[ICMP] Postel, J., *Internet Control Message Protocol - DARPA Internet Program Protocol Specification,* RFC 792, USC/Information Sciences Institute, September 1981.

[IGMP] Cain, B., Deering, S., Kouvelas, I., Fenner, B. and A. Thyagarajan, *Internet Group Management Protocol, Version 3*, RFC 3376, October 2002.

[UDP] Postel, J., *User Datagram Protocol*, STD 6, RFC 768, August 1980.

[TCP] Postel, J., *Transmission control protocol*, STD 7, RFC 793, September 1981.

[IPSec] Kent, S. and R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.

[ESP] Kent, S. and R. Atkinson, *IP Encapsulating Security Payload (ESP)*, RFC 2406, November 1998.

[ISKAMP] Maughan, D., Schertler, M., Schneider, M., and J. Turner, *Internet Security Association and Key Management Protocol (ISAKMP)*, RFC 2408, November 1998.

[IKE] Harkins, D., and D. Carrel, *The Internet Key Exchange (IKE)*, RFC 2409, November 1998.

[IKE-MODP] T. Kiniven, M. Kojo; *More Modular (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*, RFC 3526, May 2003.

[IKE-XAUTH] S. Beaulieu and R. Pereira, *Extended Authentication within IKE (XAUTH)*, draft-beaulieu-ike-xauth-02, October 2001

[IKE-MCFG] D. Dukes and R. Pereira, *The ISAKMP Configuration Method*, draft-dukes-ike-mode-cfg-02, September 2001

[ISAKMP-HAUTH]
M. Litvin, R. Shamir and T. Zegman, *A Hybrid Authentication Mode for IKE*, draft-ietf-ipsec-isakmp-hybrid-auth-05, August 2000

[FTP] Postel, J. and J. Reynolds, *File Transfer Protocol (FTP)*, STD 9, RFC 959, October 1985.

[FTP-security] Allman, M., Ostermann, S., *FTP Security Considerations*, RFC 2577, May 1999

[FTP-feature] Hethmon, P., Elz, R., *Feature negotiation mechanism for the File Transfer Protocol*, RFC 2389, August 1998

[FTP-IPV6] Allman, M., Ostermann, S. and C. Metz, *FTP Extensions for IPv6 and NATs*, RFC 2428, September 1998.

[HTTP] Fielding, R., Gettys, J., Mogul, J., Frysyk, H., Masinter, L., Leach, P. and T. Berners-Lee, *Hypertext Transfer Protocol -- HTTP/1.1*, RFC 2616, June 1999.

[WEBDAV] Goland, Y., Whitehead, E., Faizi, A., Carter, S. and D. Jensen, *HTTP Extensions for Distributed Authoring - WEBDAV*, RFC 2518, February 1999.

[WEBDAV-extensions]
Clemm, G., Amsden, J., Ellison, T., Kaler, C. and J. Whitehead, *Versioning Extensions to WebDAV (Web Distributed Authoring and Versioning)*, RFC 3253, March 2002.

[DNS-1] Mockapetris, P., *Domain names - Concepts and Facilities*, STD 13, RFC 1034, November 1987.

[DNS-2] Mockapetris, P., *Domain Names - Implementation and Specification*, STD 13, RFC 1035, November 1987.

[RIP-1] Hedrick, C., *Routing Information Protocol*, RFC 1058, Rutgers University, June 1988.

[RIP-2] Malkin, G., *RIP Version 2*, STD 56, RFC 2453, November 1998.

[DSCP] K. Nichols, Differentiated Services Field, RFC 2474, December 1998.

[MGCP] F. Andreasen and B. Foster, Media Gateway Control Protocol, RFC 3435, January 2003.

[SIP] *Session Initiation Protocol*, RFC 3261, June 2002.

[RTP] *RTP: A Transport Protocol for Real-Time Applications*, RFC 3550, Jully 2003.

[RTCP] *Real Time Control Protocol (RTCP) attribute in SDP*, RFC 3605, October 2003.

[TLS] T. Dierks and C. Allen, *The TLS Protocol Version 1.0*, RFC 2246, January 1999.

[TLS-AES] P. Chown, *Advanced Encryption Standard (AES) Ciphersuites Transport Layer Security (TLS)*, RFC 3268, June 2002.

[SRP] *The SRP Authentication and Key Exchange System*, RFC 2945, September 2000.

[Wu98] T. Wu, “The Secure Remote Password Protocol”, In *Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security*, San Diego, CA, pp. 97-111.

[DH] Rescorla, *Diffie-Hellman Key Agreement Method*, RFC 2631, June 1999.

[RSA] RSA Laboratories. *PKCS #1 v2.1: RSA Encryption Standard*. June 2000.

[AES] NIST, FIPS PUB 197, *Advanced Encryption Standard (AES)*, November 2001.

[DES] NIST, FIPS PUB 46-3, *Data Encryption Standard (DES)*, October 1999.

[Blowfish] B. Schneier, *Fast Software Encryption*, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag 1994, pp. 191-204.

[CAST] Adams, C., *The CAST-128 Encryption Algorithm*, RFC 2144, May 1997.

[HMAC] Krawczyk, H., Bellare, M. and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, RFC 2104, February 1997.

[MD5] Rivest, R., *The MD5 Message-Digest Algorithm*, RFC 1321, April 1992.

[SHA] NIST, FIPS 180-1, *Secure Hash Standard*, April 1993.

[SHA2] NIST, FIPS 180-2, *Secure Hash Standard*, February 2004.

[SMB2] MS-SMB2, *Server Message Block (SMB) Version 2 Protocol Specification*, December 30, 2010

[ITSEC] *Critères d’évaluation de la sécurité des systèmes informatiques*
Commission des Communautés Européennes, version 1.2, juin 1991.

1.5 Glossaire

TOE
Cible d'évaluation.

ST
Cible de sécurité.

TI
Technologie de l'information.

EAL
Niveau d'assurance de l'évaluation.

SFR
Exigence fonctionnelle de sécurité.

TSF
Fonction de sécurité de la TOE

CEMMéthodologie d'évaluation commune pour la sécurité des technologies de l'information.

CC
Critères communs pour l'évaluation de la sécurité.

Administrateur
Personnel habilité à effectuer certaines opérations d'administration de la sécurité et responsable de leur exécution correcte.

Auditeur
Administrateur habilité à effectuer des opérations d'audit de la sécurité et de gestion des traces d'audit, et responsable de leur exécution correcte.

Entité
Agent informatique ou utilisateur humain susceptible d'établir des flux d'information avec d'autres entités.

Boîtier appliance firewall-VPN
Équipement NETASQ placé à la frontière entre le réseau non maîtrisé et un ou plusieurs réseaux de confiance, dédié à la mise en œuvre de la politique de contrôle des flux d'information. C'est sur cet équipement que fonctionne le cœur des fonctions de sécurité de la suite logicielle IPS-Firewall.

Association de Sécurité IPSec (SA IPSec)
Connexion unidirectionnelle de niveau transport qui met en œuvre des services de sécurité sur les flux qu'elle transporte. Du point de vue d'une entité participant à un tunnel VPN, une SA IPSec peut être entrante ou sortante. Les SA sortantes servent à encapsuler et à protéger les datagrammes IP sortants, les SA entrantes servent à décapsuler et à contrôler les datagrammes IP entrants.

Extrémités du trafic / extrémités du tunnel
Dans le cas d'un tunnel VPN, les extrémités du trafic sont les entités formant les extrémités d'un flux transitant partiellement par le tunnel, par opposition aux extrémités du tunnel qui sont les équipements entre lesquels le tunnel est mis en œuvre. En ESP chiffré en mode tunnel, les adresses IP des extrémités du trafic sont protégées en confidentialité vis-à-vis d'attaquants capables d'écouter les flux sur les portions de réseau où le tunnel est mis en œuvre. Seules les adresses IP des extrémités du tunnel peuvent être lues par ces attaquants.

Correspondant VPN
Entité distante formant l'autre extrémité d'un tunnel VPN.

Entité locale / entité distante
Dans le cas d'un tunnel VPN, les entités locales sont les extrémités du trafic dont les flux parviennent au boîtier appliance firewall-VPN non encapsulés par ESP, et qui doivent l'être avant leur retransmission à l'autre extrémité du trafic via le correspondant VPN. Les entités distantes sont celles dont les flux parviennent au boîtier appliance firewall-VPN via le correspondant VPN et encapsulés par ESP.

Console locale
Terminal physiquement connecté sur un boîtier appliance firewall-VPN, servant à procéder à des opérations d'installation ou de maintenance du logiciel de ce boîtier.

Opérations d'administration de la sécurité
Opérations effectuées sur les boîtiers appliances firewall-VPN, confiées à la responsabilité d'un administrateur au titre de la politique de sécurité interne de l'organisation exploitant les réseaux de confiance. Ces opérations peuvent être dictées par la politique de sécurité interne (ex : revues d'audit) ou par la nécessité de maintenir la TOE dans des conditions d'exploitation nominales (ex : modification de la configuration de la fonction de contrôle des flux d'information, purge des journaux d'audit, arrêt/redémarrage du logiciel IPS-Firewall). Elles sont caractérisées par le fait d'avoir pour effet éventuel de modifier le comportement des fonctions de sécurité de la TOE.

Politique de filtrage
Ensemble de règles techniques décrivant quelles entités ont le droit d'établir des flux d'information avec quelles autres entités. Elle résulte de la concaténation des **règles implicites**, de la **politique de filtrage globale**, et de la **politique de filtrage locale**.

Politique de filtrage globale
Ensemble de règles techniques décrivant quelles entités ont le droit d'établir des flux d'information avec quelles autres entités. Cet ensemble est défini par un administrateur dans le but d'avoir une cohérence sur la **politique de filtrage** pour un ensemble de boîtiers appliance firewall-VPN.

Politique de filtrage locale
Ensemble de règles techniques décrivant quelles entités ont le droit d'établir des flux d'information avec quelles autres entités. Cet ensemble est défini par un administrateur dans le but d'ajuster la **politique de filtrage globale** en fonction des besoins spécifiques pour un boîtier appliance firewall-VPN.

Règle implicite
Ensemble de règles automatiquement générées par le boîtier appliance firewall-VPN afin d'assurer le bon fonctionnement des services configurés et démarrés par un administrateur.

Politique de chiffrement
Ensemble de règles techniques décrivant les traitements de chiffrement à appliquer à certains flux d'information dans le but de les protéger en confidentialité et en intégrité.

Politique de contrôle des flux d'information
Ensemble de règles techniques constitué de la politique de filtrage et de la politique de chiffrement.

Pseudo-connexion
1º) Ensemble de datagrammes UDP associés à un même échange applicatif.
2º) Ensemble de messages ICMP associés à un échange de type requête / réponse dans le cadre de l'utilisation de ce protocole (ex : 'echo request' / 'echo reply').

Réseau de confiance
Un réseau est dit de confiance si, du fait qu'il est sous le contrôle de l'exploitant de la TOE, la politique de sécurité interne n'implique pas qu'il faille se protéger des flux qui en proviennent, mais au contraire implique qu'il faille les protéger des flux qui y parviennent.

Réseau non maîtrisé
Un réseau est dit non maîtrisé s'il n'est pas sous le contrôle de l'exploitant de la TOE, ce qui implique qu'il faille se protéger des flux établis avec les équipements de ce réseau (par exemple Internet).

SRP
Secure Remote Password. Protocole d'authentification mutuelle basé un mot de passe réutilisable, sans divulgation de celui-ci.

Station d'administration à distance
Station de travail muni d'un logiciel NETASQ, connecté à un réseau de confiance ou non maîtrisé, dédiée aux opérations d'administration de la sécurité d'un ou plusieurs boîtiers appliance firewall-VPN à travers des sessions sécurisées d'administration de la sécurité.

Super-administrateur
Administrateur disposant de droits complets sur la configuration des boîtiers appliance firewall-VPN, seul habilité à s'y connecter à l'aide de la console locale, à définir les profils des autres administrateurs, et ne devant accomplir cette tâche qu'en dehors des phases d'exploitation (i.e. installation ou maintenance).

Utilisateur
Personne utilisant des ressources informatiques des réseaux de confiance protégées par la TOE à partir d'autres réseaux de confiance ou du réseau non maîtrisé.

Utilisateur IPSec
Correspondant VPN utilisant un client mobile avec une méthode d'authentification qui est HybridAuth+XAuth.

Tables de données
Ensemble des tables contenant des données (interfaces, ...) qui sont nécessaires au bon fonctionnement de la TOE. Ces tables sont automatiquement renseignées par le boîtier appliance firewall-VPN lors de son fonctionnement normal.

Paquet IP entrant
Paquet IP entrant devant être confronté à la **politique de filtrage.** Par conséquent il s'agit d'un paquet IP qui n'appartient pas à une connexion ou **pseudo-connexion** précédemment détectée et autorisée.

Base de connaissance
Ensemble, figé par version de la **TOE**, de points de contrôle permettant le bon fonctionnement de **la fonction de prévention des intrusions**.

Active Update
Service permettant une mise à jour automatique et régulière des bases de signatures des différents modules utilisant ses dernières pour optimiser leur efficacité. Il s'agit notamment des signatures IPS et NVM (Seismo), Antivirus, Antispam, Filtrage URL, ….

2 DESCRIPTION DE LA CIBLE D'ÉVALUATION

Le but de cette section est de présenter les notions qui vont être utilisées par la suite dans l'énoncé de la problématique de sécurité à laquelle répond la TOE, des objectifs de sécurité et des exigences de sécurité de la TOE. Elle sert aussi à préciser la portée et les limites de l'évaluation.

2.1 Caractéristiques de sécurité TI de la TOE

2.1.1 Généralités

La sécurisation de l'interconnexion entre des réseaux de confiance appartenant à une organisation et un **réseau non maîtrisé** nécessite la définition, par le responsable SSI de l'organisation, d'une **politique de sécurité interne**, récapitulant ou référençant les « lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les biens, en particulier les informations sensibles », au sein de l'organisation [ITSEC].

La politique de sécurité interne peut faire peser des exigences d'ordre technique sur le réseau et des contraintes sur les mesures physiques, relatives au personnel ou organisationnelles de son environnement d'exploitation. La **suite logicielle NETASQ IPS-Firewall** vise à répondre, dans le contexte de l'évaluation, aux exigences d'ordre technique de contrôle des flux d'information par des fonctionnalités de filtrage élaboré et des fonctionnalités chiffrement de type VPN (*virtual private network – réseau privé virtuel*).

2.1.2 Le contrôle des flux d'information

Cet ensemble d'exigences est la raison d'être d'un produit de type firewall-VPN. La politique de sécurité interne doit permettre de déduire :

- quelles **entités** (**utilisateurs** ou agents informatiques) ont le droit d'établir des flux d'information avec quelles autres entités, c'est ce qu'on appelle la **politique de filtrage**,
- parmi les flux d'information autorisés, lesquels nécessitent des protections en confidentialité ou en intégrité, et la nature de ces protections (protocoles et algorithmes de chiffrement), c'est ce qu'on appelle la **politique de chiffrement**.

Suivant les cas, les règles de cette **politique de chiffrement et de filtrage**, également appelée **politique de contrôle des flux d'information**, peuvent s'exprimer selon des critères plus ou moins sophistiqués : adresses IP source et destination, n° de protocole IP utilisé, port TCP/UDP source/destination.

La suite logicielle NETASQ IPS-Firewall fournit les **fonctionnalités de filtrage** suivantes :

- Filtrage des flux entre les équipements (*stateful inspection*), sur la base :
  - des caractéristiques au niveau IP et transport : n° de protocole IP, adresses IP source et destination, ports TCP/UDP source et destination.
- Imputabilité des flux aux entités les ayant suscités par la génération des données d'audit.

Les **fonctionnalités de chiffrement** sont celles offertes en standard par le protocole ESP en mode tunnel d'IPSec [ESP, IPSec], associé à ISAKMP [ISAKMP] et à IKE [IKE] pour la négociation des paramètres de sécurité et des clés de session :

- Confidentialité du contenu des flux ;

- Anonymat des équipements d'extrémité du trafic ;
- Intégrité du contenu des flux : intégrité des paquets, protection contre le rejeu, authentification de l'émetteur du paquet chiffré ;
- Authentification mutuelle des extrémités du tunnel (i.e. la portion du flux sur laquelle le chiffrement est appliqué).

L'interopérabilité du module VPN de la suite logicielle NETASQ IPS-Firewall permet de l'interconnecter à des systèmes de chiffrement IPSec hétérogènes.

Ces deux grands ensembles fonctionnels sont complétés par des **fonctionnalités de remontée d'alarmes** que l'administrateur peut définir à partir de l'ensemble des événements de sécurité que le firewall est susceptible de détecter (événements de filtrage, de chiffrement, événements remontés par le moteur ASQ (cf. §2.1.3), événements système bas niveau (arrêt/démarrage du firewall-VPN, erreurs hardware, etc.)).

2.1.3 La protection contre les attaques Internet

Le contrôle du trafic entre plusieurs réseaux de confiance et le réseau non maîtrisé permet de rejeter des tentatives évidentes d'établissement de flux illicites vis-à-vis de la politique de contrôle des flux d'information.

Néanmoins, à l'intérieur des limites d'une politique de contrôle des flux d'information adaptée au réseau et correctement implémentée au niveau du firewall-VPN, subsiste la possibilité pour des attaquants possédant un accès au réseau non maîtrisé :

- de contourner la politique de contrôle des flux d'information mise en œuvre par le firewall-VPN,
- et/ou d'« attaquer » les équipements des réseaux de confiance en se basant sur des détails et des erreurs de conception et d'implémentation des protocoles réseaux (IP, TCP, UDP, protocoles applicatifs).

Les effets de ce genre d'attaques peuvent être :

- une intrusion, c'est-à-dire un accès non autorisé à un service, ou aux fonctions du système d'exploitation d'un équipement ;
- le blocage ou le redémarrage d'un équipement, provoquant un déni de service ;
- la saturation des équipements réseau provoquant un déni de service ;
- la divulgation de la topologie et/ou des détails techniques des équipements du réseau de confiance dans le but d'obtenir des accès non autorisés supplémentaires à partir d'une première intrusion réussie.

Pour contrer ce risque, la suite logicielle NETASQ IPS-Firewall propose une **fonction de prévention des intrusions**, basée sur la **technologie ASQ**. Cette technologie inclut un moteur d'analyse dynamique aux niveaux IP, transport et applicatif avec optimisation des règles permettant l'application de la politique de contrôle des flux d'information de façon sûre et rapide. Elle permet :

- La détection d'attaques sans contexte de connexion, par exemple :
  - l'usurpation d'adresse IP (*IP spoofing*) par la corrélation de l'adresse IP source et de l'interface de réception des paquets,

- les paquets contrefaits comme ceux de type ‘xmas tree’ (toutes les options TCP sont mises) ou ‘land’ (l’adresse source et l’adresse destination sont identiques) qui visent à provoquer des défaillances sur les équipements cibles,
- les recouvrements de fragments dans le but de provoquer des défaillances sur les équipements cibles ou de contourner la politique de contrôle des flux d’information,
- les tentatives de débordement mémoire au niveau applicatif ;

- La détection des attaques avec contexte de connexion comme par exemple :
  - l’utilisation de numéros de séquence TCP incorrects ou hors fenêtre,
  - les attaques exhaustives (*brute force*) sur les mots de passe FTP ;
- La détection des attaques globales nécessitant de recouper les caractéristiques de nombreux flux d’information distincts comme par exemple :
  - la saturation des ressources des serveurs, par l’envoi d’un nombre abusif de demandes d’ouvertures de connexion TCP non acquittées (*SYN flooding*),
  - les tentatives de sondage de la topologie interne des réseaux de confiance avec les utilitaires nmap ou queso.

L’annexe B, §8 contient une liste exhaustive des attaques actuellement prises en compte par le moteur de filtrage ASQ.

2.1.4 Les risques d’utilisation impropre

La déclinaison d’une politique de contrôle des flux d’information au niveau de la configuration d’un firewall-VPN, ainsi que l’exploitation de ce type de produit (audits, réactions vis-à-vis des alarmes, etc.) est en général une tâche complexe, nécessitant des compétences spécifiques et présentant, en conséquence, des risques d’erreurs.

Ces risques rendent souhaitable une séparation des rôles administratifs afin de garantir que les seules personnes à même d’accomplir une activité d’exploitation donnée sont celles qui sont spécifiquement habilitées et formées pour le faire. À cet effet, la suite logicielle NETASQ IPS-Firewall fournit une **fonction de contrôle d’accès aux opérations d’administration de la sécurité** basée sur des droits permettant de constituer des profils administrateurs. La définition des profils est du ressort d’un administrateur spécial, le « super-administrateur », qui intervient exclusivement lors des phases d’installation et de maintenance et est le seul habilité à se connecter à la console locale.

Une **fonction de sauvegarde et de restitution des configurations** réduit le risque d’erreur en permettant de conserver des configurations types répondant à problématiques bien définies, et de revenir en arrière en cas d’erreur de manipulation.

La **qualité de la documentation** d’exploitation et la **facilité d’utilisation** des interfaces ont également un impact sur ce type de risque.

2.1.5 La protection de la TOE elle-même

Si on suppose que les fonctions de sécurité de la TOE sont efficaces pour implémenter la politique de sécurité réseau et contrer les attaques, et correctement configurées, la seule solution pour réussir une attaque c'est de modifier le comportement de la TOE :

- Soit en désactivant les fonctions de sécurité ou en modifiant leur configuration, par le biais d'une attaque locale ou distante exploitant d'éventuelles vulnérabilités permettant de contourner la fonction de contrôle d'accès aux opérations d'administration, sans nécessiter de droits particuliers ;
- Soit obtenant un accès administrateur légitime (par collusion avec un administrateur, en devinant son mot de passe, etc.).

Pour contrer ce risque, des mesures doivent être prises au niveau de la sécurité physique et logique des boîtiers appliances firewall-VPN et aussi des stations d'administration à distance (local à accès contrôlé, interdiction d'utiliser une console locale dans des conditions d'exploitation, etc.). La fonction de contrôle d'accès aux opérations d'administration évoquée au §2.1.4 est soutenue par des **mécanismes d'authentification forte des administrateurs basés : sur l'algorithme SRP ou sur une authentification mutuelle par certificat X.509 (TLS) ou sur une authentification de type identifiant / mot de passe (TLS)**. Par ailleurs l'administration à distance pouvant être effectuée à partir du réseau non maîtrisé, la suite logicielle NETASQ IPS-Firewall fournit une **fonction de protection des sessions d'administration en confidentialité et en intégrité** basée sur des opérations cryptographiques de chiffrement (AES 128 bits). Ces fonctions forment un ensemble distinct des fonctions de chiffrement IPSec et sont donc fournies dans tous les cas.

2.2 Limites physiques de la TOE

2.2.1 Équipements constituant la TOE

Une plate-forme sur laquelle la TOE s'exécute est constituée de deux types d'équipement :

- Des **boîtiers appliances firewall-VPN**, sur lesquels s'exécute **le logiciel NS-BSD (composant de la suite logicielle NETASQ IPS-Firewall)**. Ces boîtiers mettent en œuvre la fonction de filtrage et la fonction de chiffrement de la TOE, entre les différents sous-réseaux reliés à leurs interfaces,
- Des **stations d'administration à distance**, reliées au boîtier de façon sécurisée et sur lesquelles tourne les applications de la suite d'administration NETASQ (IHM) dédié à la gestion de la politique de filtrage et de chiffrement, le monitoring en temps réel, l'acquittement des alarmes et l'audit de la TOE par l'administrateur, et la gestion des comptes administrateurs.

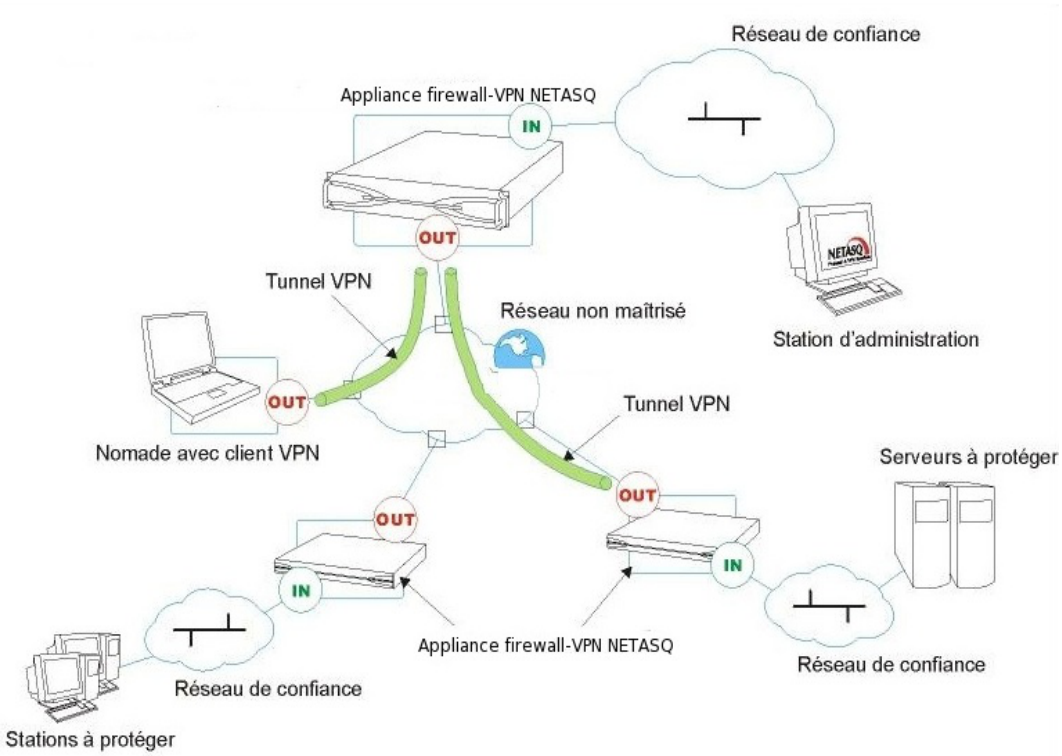


Illustration 1: Cas typique d'utilisation des composants de la TOE.

Dans l'exemple d'architecture réseau présenté ci-dessus, les boîtiers appliances firewall-VPN sont déployés à la frontière entre chaque réseau de confiance et le réseau non maîtrisé. Ils servent à protéger les stations et les serveurs présents sur les réseaux de confiance, en contrôlant tous les flux d'information qui transitent par cette frontière.

Ils mettent également en œuvre des tunnels VPN sur la portion du réseau non maîtrisé où ces flux sont véhiculés, aussi bien entre deux boîtiers qu'entre un boîtier et un poste nomade équipé d'un client VPN connecté sur le réseau non maîtrisé.

Les postes nomades ne font pas partie de la TOE, qu'ils soient équipés du client VPN fourni par NETASQ ou d'un autre logiciel.

Les stations d'administration à distance peuvent être connectées au réseau non maîtrisé ou à un réseau de confiance.

2.2.2 Interfaces physiques

Les interfaces physiques de la TOE sont constituées en fonction des modèles de :

- connecteurs RJ45 ;
- interface série RS-232 ;
- port VGA ;
- port mi-din PS2 ;
- port USB.

2.2.3 Caractéristiques minimales des plates-formes d'exploitation

Les boîtiers appliances firewall-VPN sont entièrement packagés par NETASQ. Ils sont développés autour du noyau FreeBSD 8.3, avec correctifs à jour, adapté et épuré par NETASQ.

Le logiciel **NS-BSD** (composant de la suite logicielle **IPS-Firewall)** utilise les composants « open-source » suivant avec leurs correctifs à jour dans les conditions d'évaluation :

- FreeBSD en version 8.3-p13
- Ipsec-tools en version 0.8.0
- OpenLDAP en version 2.4.31
- OpenSSL en version 1.0.1h
- Launchd en version 106.3
- Libevent en version 2.0.20

Il est à noter que seule la partie logicielle et non le matériel est soumise à l'évaluation.

Pour les stations d'administration à distance :

- NETASQ Web Manager :
  - CPU à 2Ghz minimum ;
  - 1 Go de RAM ;
  - Carte réseau Ethernet 100 ou 1000 Mbps ;
  - Microsoft Internet Explorer 7 ou plus *ou* Mozilla Firefox 3.6 ou plus.
- NETASQ Real-Time Monitor, NETASQ Event Reporter :
  - CPU à 2Ghz minimum ;
  - 2 Go de RAM ;
  - 500 Mo de disque dur ;
  - Carte réseau Ethernet 100 ou 1000 Mbps ;

- Microsoft Windows 2003 SP2 *ou* Microsoft Windows XP SP2 ou plus *ou* Microsoft Windows Seven.

2.3 Limites logiques de la TOE

Le périmètre de l'évaluation porte sur la suite logicielle IPS-Firewall dans sa version 9.1.0.5 qui est installée sur :

- les boîtiers appliances firewall-VPN de la gamme U30 à la gamme NG5000 (builds S, M, L, XL) pour le composant logiciel :
  - **NS-BSD** : logiciel **IPS-Firewall** pour boîtier appliance firewall-VPN incluant le noyau FreeBSD 8.3 avec correctifs à jour, adapté et épuré par NETASQ ;
- les stations d'administration à distance pour les composants logiciels :
  - **NETASQ Web Manager** : Interface graphique d'administration et de configuration des firewalls NETASQ ;
  - **NETASQ Real-Time Monitor** : Interface graphique de supervision et de monitoring d'un ou de plusieurs firewalls ;
  - **NETASQ Event Reporter** : Interface graphique d'analyse des traces et de reporting.

2.4 Architecture et interfaces de la TOE

Une TOE en exploitation est un produit réparti sur des boîtiers appliances firewall-VPN, et une ou plusieurs stations d'administration à distance. La figure ci-dessous schématise les interfaces existant entre ces composants ainsi qu'avec les autres entités TI hors TOE et les utilisateurs.

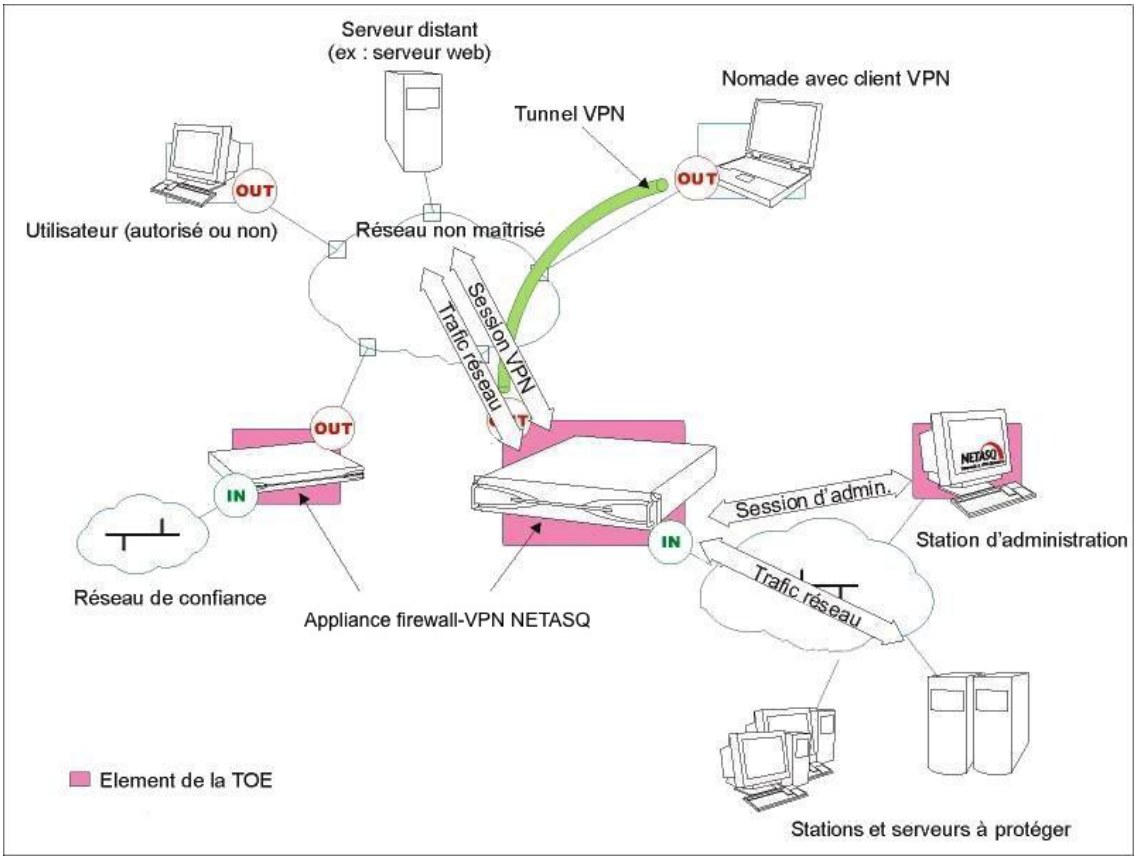


Illustration 2: Composants et interfaces de la TOE.

2.5 Configurations et modes d'utilisation soumis à l'évaluation

Le mode d'utilisation soumis à l'évaluation présente les caractéristiques suivantes :

- L'évaluation porte sur la suite logicielle IPS-Firewall qui équipe toutes les versions des boîtiers firewall-VPN, du U30 au NG-5000 ; Celle-ci se décline en 4 compilations distinctes (build S, M, L, XL) selon la position dans la gamme. Certains modèles (build S : U30, U70) ne dispose pas de journaux d'audit locaux conséquent et doivent émettre les événements par syslog.
- Les boîtiers appliances firewall-VPN doivent être stockés dans un local à accès sécurisé. Ces mesures, ainsi que les procédures organisationnelles de l'environnement d'exploitation, doivent garantir que les seuls accès physiques aux boîtiers appliances firewall-VPN se font sous la surveillance du super-administrateur ;
- La console locale n'est pas utilisée en exploitation. Seul le super-administrateur peut s'y connecter, et, par hypothèse, ce genre d'intervention ne se fait que lorsqu'une sortie du cadre de l'exploitation – pour procéder à une maintenance ou à une ré-installation – est décidée ;
- Les stations sur lesquelles s'exécutent la suite logicielle d'administration à distance sont sécurisées, dédiées à cette utilisation, et à jour de tous les correctifs concernant leur système d'exploitation et les logiciels applicatifs qui les équipent ;
- Tous les administrateurs sont soumis à une étape identification / authentification offerte par la TOE, et pouvant utiliser : le protocole SRP, une authentification identifiant / mot de passe dans un canal TLS ou une authentification mutuelle par certificat X.509 dans un canal TLS ;
- Le mode de distribution des certificats et des CRL est manuelle (importation).
- Le logiciel VPN client ne fait pas partie de l'évaluation ; du reste les utilisateurs peuvent utiliser le client IPSec de leur choix. Cependant, ces postes clients doivent être sécurisés avec un niveau de rigueur équivalent à celui des stations d'administration à distance ;
- En cas émission des événements d'audit via syslog, le serveur qui les réceptionne ne fait pas partie de l'évaluation.
- Le mode d'utilisation soumis à l'évaluation exclut le fait que la TOE s'appuie sur d'autres services tels que PKI, serveur DNS, DHCP, proxies. Les modules que NETASQ fournit en option pour la prise en charge de ces services sont désactivés par défaut et doivent le rester[1]. Il s'agit précisément :
  - des modules permettant la prise en charge des serveurs externes (ex : Kerberos, RADIUS...),
  - du module de routage dynamique,
  - de l'infrastructure à clés publiques (PKI) interne,
  - du module VPN SSL,
  - du cache DNS,
  - du moteur antivirus (ClamAV ou Kaspersky),
  - du module Active Update,

1 Les outils d'administration et de monitoring fournissent le moyen de vérifier, à tout moment lors de l'exploitation, que c'est bien le cas.

- des serveurs SSH, DHCP, MPD et SNMPD,
- du client DHCP et du démon NTP,
- du relai DHCP.

- Bien que supportée, la fonctionnalité de routage IPv6 est désactivée par défaut et doit le rester dans le cadre de l'évaluation.
- Les administrateurs et les utilisateurs IPSec sont gérés par une base LDAP interne au logiciel IPS-Firewall et qui fait partie de la TOE. Le mode d'utilisation soumis à l'évaluation exclut le fait que des clients LDAP externes au boîtier appliance firewall-VPN puissent se connecter à cette base ;
- Les journaux d'audit sont, selon les modèles, stockés localement ou émis par Syslog. Dans ce dernier cas, le chiffrement des messages Syslog n'est pas une fonction de sécurité soumise à l'évaluation.
- La technologie ASQ met en œuvre des analyses contextuelles au niveau applicatif, dans le but de vérifier la conformité aux RFC et de contrer les attaques au niveau applicatif. Les fonctions d'analyse applicative qui font l'objet de l'évaluation sont celles associées aux protocoles FTP, HTTP (incluant les extensions WEBDAV), SIP, SMTP et DNS ;
- La possibilité offerte par la politique de filtrage d'associer à chaque règle de filtrage une inspection applicative (proxies HTTP, SMTP, POP3, FTP) et une programmation horaire est hors du cadre de cette évaluation et ne devra pas être utilisé.
- La possibilité offerte par la politique de filtrage d'associer l'action « decrypt » (proxy SSL) à une règle de filtrage est hors du cadre de cette évaluation et ne devra pas être utilisé.
- Les fonctionnalités suivantes peuvent être utilisées, mais ne sont pas considérées comme des fonctions de sécurité :
  - la translation d'adresses (*network address translation* ou *NAT*) ;
  - le module Netasq Vulnerability Manager (*détection de vulnérabilités*) ;
  - le module Haute Disponibilité ;
  - la fonction de visualisation de rapports embarqués ;
  - l'utilisation des options « Mode Config » [IKE-MCFG] par les clients VPN pour la partie IPSec.

2.6 Plate-forme de test utilisée lors de l'évaluation

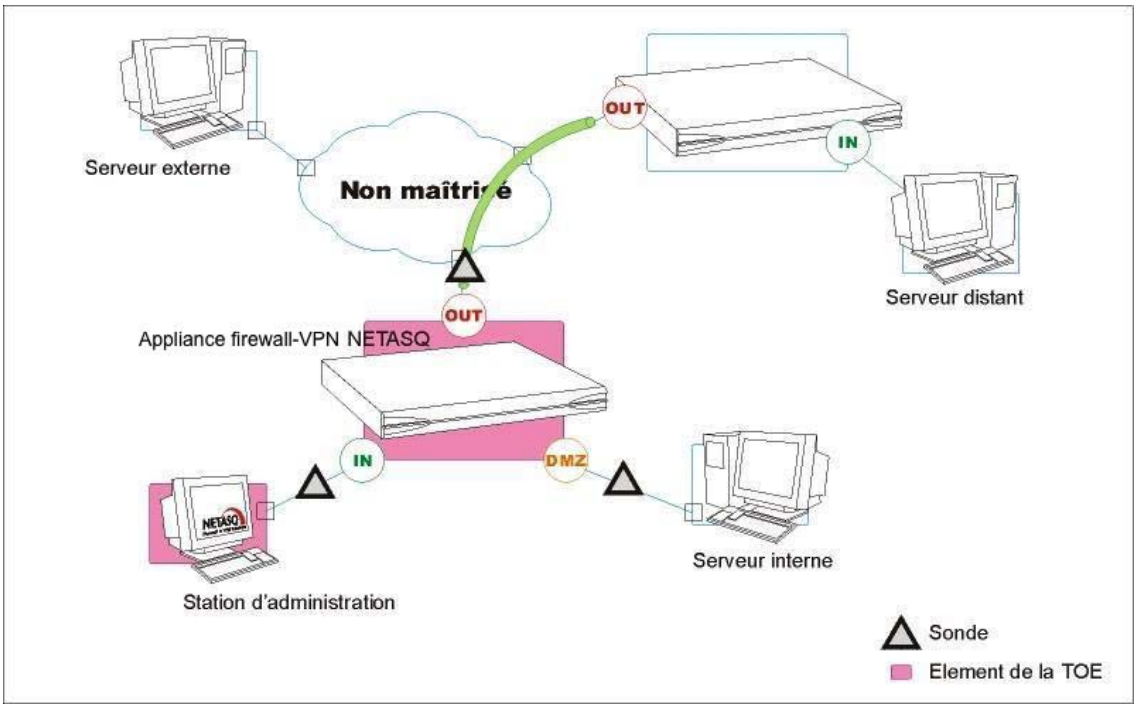


Illustration 3: Plate-forme de test utilisée lors de l'évaluation.

Les boîtiers appliances firewall-VPN sont un U250S et un NG1000.

Le système d'exploitation de la station d'administration à distance est Microsoft Windows Seven 32 bits édition Professionnelle à jour avec tous les correctifs publiés par Microsoft.

Le navigateur web utilisé pour le NETASQ Web Manager est Micorosoft Internet Explorer version 9 à jour avec tous les correctifs publiés par Microsoft.

Le logiciel du poste client nomade et des serveurs est constitué par des produits grand public représentatifs (ex : navigateurs, clients de messagerie, serveurs Web) et des applications développées spécifiquement aux fins des tests de conformité ou de pénétration (scripts, programmes d'attaque, etc.). Le poste client nomade est également équipé du logiciel client VPN NETASQ (non soumis à l'évaluation).

Des ordinateurs portables équipés de logiciels « sondes » servent à écouter les flux pour estimer la conformité du comportement du boîtier appliance firewall-VPN au niveau des interfaces réseau, ainsi qu'à mener des tests de pénétration en contrefaisant des paquets. Ils sont susceptibles d'être connectés en différents points du réseau.

3 ENVIRONNEMENT DE SÉCURITÉ DE LA CIBLE D'ÉVALUATION

Le but de cette section est de décrire le problème de sécurité auquel la TOE doit répondre sous la forme d'un jeu de menaces que la TOE doit contrer et des règles de la politique de sécurité que la TOE doit satisfaire. Cette spécification du cahier des charges sécuritaire du produit est faite moyennant des hypothèses portant sur les caractéristiques de sécurité de l'environnement dans lequel il est prévu d'utiliser la TOE ainsi que sur son mode d'utilisation attendu.

3.1 Convention de notation

Pour une meilleure compréhension des paragraphes suivants, nous explicitons ici les conventions de notation utilisées pour nommer les hypothèses, les menaces, les politiques et les objectifs :

- Les **H**ypothèses concernant l'environnement de sécurité de la TOE ont des noms commençant par les préfixes suivants :
  - **HH.** préfixe les **H**ypothèses relatives aux agents **H**umains,
  - **HP.** préfixe les **H**ypothèses relatives aux mesures **P**hysiques,
  - **HO.** préfixe les **H**ypothèses relatives aux mesures de sécurité **O**rganisationnelles,
  - **HTI.** préfixe les **H**ypothèses relatives à l'environnement de sécurité **TI.**
- Les **M**enaces sur l'environnement de sécurité de la TOE ou sur la sécurité de la TOE elle-même ont des noms commençant par le préfixe **M.**
- Les **P**olitiques de sécurité de l'organisation ont des noms commençant par le préfixe **P.**

3.2 Identification des biens sensibles

3.2.1 Biens protégés par la TOE

Le firewall-VPN NETASQ contribue à protéger les biens sensibles suivants, sous réserve d'une définition correcte et réalisable de la politique de contrôle des flux d'information à mettre en œuvre au niveau du système d'information dans sa globalité (cf. HO.BONNE_PCFI) :

- Les services applicatifs proposés par les serveurs des réseaux de confiance (en confidentialité, intégrité et disponibilité) ;
- Les logiciels s'exécutant sur les équipements des réseaux de confiance (serveurs, navigateurs, etc.), et la configuration de ces logiciels (intégrité et confidentialité) ;
- Le contenu des flux d'information transitant sur le réseau non maîtrisé, pour lesquels la mise en œuvre de VPN est envisageable (confidentialité et intégrité) ;
- Les informations de topologie du réseau (confidentialité), contre des tentatives de sondage basées sur une utilisation des protocoles Internet contraires aux bonnes pratiques.

3.2.2 Biens appartenant à la TOE

Dans le but de protéger ces biens sensibles externes, les différents composants de la suite logicielle NETASQ IPS-Firewall protègent également leurs propres paramètres de sécurité en confidentialité et en intégrité lors des échanges entre eux (sessions d'administration).

Par ailleurs, les biens sensibles de la TOE sont composés des données liées aux fonctions de sécurité de la TOE (TSF-Datas).

Les TSF-datas sont composées :

- des paramètres de configuration de la TOE,
- des politiques de contrôle de flux implémentée par la TOE,
- des contextes d'utilisation,
- des enregistrements d'événements de la TOE,
- des données d'authentification des administrateurs et des utilisateurs IPSec.

3.3 Menaces et règles de la politique de sécurité

L'énoncé des menaces et des règles de la politique de sécurité reprend le plan suivi pour la description des caractéristiques de sécurité TI de la TOE.

Les différents agents menaçants sont :

- attaquants internes : entités appartenant au réseau de confiance
- attaquants externes : entités n'appartenant pas au réseau de confiance

Les administrateurs ne sont pas considérés comme des attaquants.

3.3.1 Le contrôle des flux d'information

P.FILTRAGE

La TOE doit appliquer la politique de filtrage définie par l'administrateur. Cette politique s'exprime en termes de l'autorisation ou non d'établir des flux en fonction de ses caractéristiques au niveau IP (adresse source et destination, type de protocole IP) et transport (port source et destination TCP ou UDP),

P.VPN

La TOE doit appliquer la politique de chiffrement définie par l'administrateur. Cette politique s'exprime en termes :

1. de l'application de la fonction de chiffrement sur les flux en fonction de leurs caractéristiques au niveau IP (adresse source et destination, type de protocole IP),
2. des conditions de l'établissement des sessions IPSec (clé pré-partagée ou certificat, identité attendue du correspondant VPN),
3. des paramètres ESP utilisés (algorithmes d'authentification et de chiffrement des trames et longueur des clés associées).

P.AUDIT_ALARME

La TOE doit :

1. générer les événements de filtrage (incluant flux et rejets) et de chiffrement jugés sensibles par l'administrateur et pour les équipements capables d'enregistrer les événements, fournir les moyens de les imputer ultérieurement aux entités qui les ont suscités, à travers un audit ;
2. remonter des alarmes de sécurité pour les événements de filtrage, de chiffrement, liés à l'analyse contextuelle (cf. P.ANALYSE) ou à l'activité du logiciel des boîtiers appliances firewall-VPN, spécifiés comme tels par l'administrateur.

3.3.2 La protection contre les attaques Internet

P.ANALYSE

La TOE doit analyser les flux d'informations qui transitent par les boîtiers appliances firewall-VPN, détecter et éventuellement détruire sans les transmettre les types de flux suivants, potentiellement dangereux pour l'entité réceptrice :

1. ceux pouvant divulguer la topologie du réseau (ex : option route recording),
2. ceux valides au sens des protocoles Internet mais ne correspondant pas à certaines règles de bonnes pratiques (ex : ICMP redirect),
3. ceux pouvant provoquer des fautes logicielles sur les équipements destinataires,

4. ceux pouvant saturer les capacités de communication et de traitement des équipements destinataires.

M.IP_USURP

Une entité non-autorisée sur le réseau non maîtrisé contourne la politique de contrôle des flux d'informations en contrefaisant l'adresse IP source des paquets qu'il émet afin d'usurper l'identité d'une entité sur le réseau autorisé.

3.3.3 Les risques d'utilisation impropre

M.MAUVAIS_USAGE

Les fonctions de sécurité de la TOE ne se comportent pas en accord avec la politique de sécurité interne (cf. 2.1.1), du fait qu'un administrateur n'exerce pas correctement les responsabilités liées à son rôle, soit qu'il configure mal la TOE, soit qu'il l'exploite d'une manière non conforme à ses responsabilités ou au mode d'utilisation prévu. Cela permettrait à un attaquant d'exploiter une faille ou mauvaise configuration afin d'accéder aux biens protégés par la TOE, présents sur le réseau de confiance.

P.SAUVEGARDE_RESTAURATION

La TOE doit fournir des moyens de sauvegarder sa configuration, et de restaurer celle-ci ultérieurement, dans le but de faciliter la tâche de l'administrateur.

3.3.4 La protection de la TOE elle-même

M.ADMIN_ILLICITE

Une entité appartenant ou non au réseau de confiance parvient à effectuer des opérations d'administration illicites en mettant en défaut les politiques de contrôle de flux, les contextes d'utilisation, les données d'authentification des administrateurs ainsi que les paramètres de configuration de la TOE.

M.ADMIN_USURP

Une entité appartenant ou non au réseau de confiance parvient à établir une session d'administration sur un boîtier appliance firewall-VPN en usurpant l'identité d'un administrateur suite à des tentatives aléatoires répétées, ou par le biais d'analyses de séquences d'authentification interceptées. Les biens menacés concernent les données d'authentification des administrateurs.

M.SESSION_ADMIN_ILLICITE

Une entité appartenant ou non au réseau de confiance lit, modifie ou supprime le contenu d'une session d'administration établie entre un boîtier appliance firewall-VPN et une station d'administration à distance pour le compte d'un administrateur. Les biens menacés sont les politiques de contrôle de flux ainsi que les contextes d'utilisation.

Note : M.ADMIN_USURP et M.SESSION_ADMIN_ILLICITE sont des prérequis (non-exhaustifs) permettant de réaliser la menace M.ADMIN_ILLICITE.

M.PERTE_AUDIT

Une entité appartenant ou non au réseau de confiance empêche la génération d'événements de sécurité en épuisant la capacité de stockage ou d'émission par la TOE de ces événements, dans le but de masquer les actions illicites d'un attaquant.

3.4 Hypothèses

3.4.1 Hypothèses sur les mesures de sécurité physiques

HP.PROTECT_BOITIERS

Les boîtiers appliances firewall-VPN sont installés et stockés conformément à l'état de l'art concernant les dispositifs de sécurité sensibles : local à accès protégé, câbles blindés en paire torsadée, étiquetage des câbles, etc.

3.4.2 Hypothèses sur les mesures de sécurité organisationnelles

HO.SUPER_ADMIN

Un rôle administrateur particulier, le super-administrateur, présente les caractéristiques suivantes :

1. Il est le seul à être habilité à se connecter via la console locale sur les boîtiers appliances firewall-VPN, et ce uniquement lors de l'installation de la TOE ou pour des opérations de maintenance, en dehors de l'exploitation ;
2. Il est chargé de la définition des profils des autres administrateurs ;
3. Tous les accès dans les locaux où sont stockés les boîtiers appliances firewall-VPN se font sous sa surveillance, que l'accès soit motivé par des interventions sur les boîtiers ou sur d'autres équipements. Toutes les interventions sur les boîtiers appliances firewall-VPN se font sous sa responsabilité.

HO.MOT_PASSE

Les mots de passe des administrateurs et des utilisateurs IPSec doivent être choisis de façon à retarder toutes les attaques visant à les casser, via une politique de création et/ou de contrôle de ceux-ci (par ex : mélange alphanumérique, longueur minimum, ajout de caractères spéciaux, pas de mots des dictionnaires usuels, etc.).

Les administrateurs sont sensibilisés à ces bonnes pratiques de part leur fonction et il est de leur responsabilité de sensibiliser les utilisateurs IPSec.

HO.BONNE_PCFI

La politique de contrôle des flux d'informations à mettre en œuvre est définie, pour tous les équipements des réseaux de confiance à protéger, de manière :

1. complète : les cas d'utilisation standards des équipements ont tous été envisagés lors de la définition des règles et leurs limites autorisées ont été définies,
2. stricte : seuls les cas d'utilisation nécessaires des équipements sont autorisés,
3. correcte : les règles ne présentent pas de contradiction,
4. non-ambiguë : l'énoncé des règles fournit tous les éléments pertinents pour un paramétrage direct de la TOE par un administrateur compétent.

3.4.3 Hypothèses relatives aux agents humains

HH.PERSONNEL

Les administrateurs sont des personnes non hostiles et compétentes, disposant des moyens nécessaires à l'accomplissement de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité. Notamment, leur compétence et leur organisation implique que :

1. Différents administrateurs avec les mêmes droits ne mènent des actions d'administration qui se contredisent (ex : modifications incohérentes de la politique

de contrôle des flux d'information) ;

2. L'exploitation des journaux et le traitement des alarmes sont effectués dans les délais appropriés.

3.4.4 Hypothèses sur l'environnement de sécurité TI

HTI.COUPURE

Les boîtiers appliances firewall-VPN sont installés conformément à la politique d'interconnexion des réseaux en vigueur et sont les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle des flux d'information. Ils sont dimensionnés en fonction des capacités des équipements adjacents ou alors ces derniers réalisent des fonctions de limitation du nombre de paquets par seconde, positionnées légèrement en deçà des capacités maximales de traitement de chaque boîtier appliance firewall-VPN installé dans l'architecture réseau.

HTI.USAGE_STRICT

À part l'application des fonctions de sécurité, les boîtiers appliances firewall-VPN ne fournissent pas de service réseau autre que le routage et la translation d'adresse (ex : pas de DHCP, DNS, PKI, proxies applicatifs, etc.). Les boîtiers appliances firewall-VPN ne sont pas configurés pour retransmettre les flux IPX, Netbios, AppleTalk, PPPoE ou IPv6.

HTI.AUTONOME

La TOE ne dépend pas de services externes « en ligne » (DNS, DHCP, RADIUS, etc.) pour l'application de la politique de contrôle des flux d'information.

HTI.PROTECT_STATIONS

Les stations d'administration à distance sont sécurisées et maintenues à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées. Elles sont installées dans des locaux à accès protégé et sont exclusivement dédiées à l'administration de la TOE et au stockage des sauvegardes.

HTI.PROTECT_CORRESP_VPN

Les équipements réseau avec lesquels la TOE établit des tunnels VPN sont soumis à des contraintes de contrôle d'accès physique, de protection et de maîtrise de leur configuration équivalentes à celles des boîtiers appliances firewall-VPN de la TOE.

HTI.PROTECT_CLIENTS_VPN

Les postes sur lesquels s'exécutent les clients VPN des utilisateurs autorisés sont soumis à des contraintes de contrôle d'accès physique, de protection et de maîtrise de leur configuration équivalentes à celles des postes clients des réseaux de confiance. Ils sont sécurisés et maintenus à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées.

4 OBJECTIFS DE SÉCURITÉ

Le but de cette section est de fournir une présentation concise de la réponse prévue au problème de sécurité, sous la forme d'objectifs de sécurité. Les objectifs de sécurité sont normalement classés en objectifs de sécurité pour la TOE et en objectifs de sécurité pour l'environnement. L'argumentaire des objectifs de sécurité doit montrer que les objectifs de sécurité pour la TOE et pour l'environnement sont reliés aux menaces identifiées devant être contrées ou aux règles de la politique de sécurité et hypothèses devant être satisfaites par chacun d'entre eux.

4.1 Convention de notation

Pour une meilleure compréhension des paragraphes suivants, nous explicitons ici les conventions de notation utilisées pour les objectifs :

- Les **O**bjectifs de sécurité pour la TOE ont des noms commençant par le préfixe **O.**
- Les **O**bjectifs de sécurité pour l'**E**nvironnement de la TOE ont des noms commençant par le préfixe **OE.**

4.2 Généralités

La présentation des objectifs de sécurité pour la TOE reprend le plan suivi pour la description des caractéristiques de sécurité TI de la TOE et l'énoncé des menaces et des règles de la politique de sécurité.

L'argumentaire de chaque objectif de sécurité de la TOE est fourni immédiatement après l'énoncé de l'objectif, plutôt que dans une section à part. Un tableau récapitulatif est fourni à la fin de cette section.

Concernant les objectifs de sécurité O.PCAOA, O.PCAOA_I&A_ADMIN et O.RESIST_AUTH_ADMIN, il convient de noter que la politique de contrôle de l'accès aux opérations d'administration de la sécurité concourt en fait à la fois :

- à la prévention de l'utilisation impropre, en permettant d'implémenter une séparation des tâches d'administration adaptée à la responsabilité et à la compétence de chaque administrateur, dictées par les contraintes de l'organisation exploitant les réseaux de confiance,
- et à la protection de la TOE elle-même, puisqu'elle prévient les opérations d'administration illicites.

Ainsi, ces trois objectifs couvrent les problématiques abordées au §4.5 mais aussi §4.6.

L'ensemble des hypothèses énoncées dans la description de l'environnement de sécurité de la TOE doit être considérée comme constituant les objectifs de sécurité pour l'environnement. Lorsque les objectifs de sécurité pour l'environnement que constituent les hypothèses soutiennent spécifiquement des objectifs de sécurité de la TOE, ces hypothèses sont directement indiquées dans l'argumentaire des objectifs de sécurité de la TOE concernés. Lorsque les objectifs de sécurité pour l'environnement contrent directement des menaces, ou lorsque leur soutien est général, cela est présenté à la fin de cette section (§4.7).

4.3 Objectifs de contrôle des flux d'information

O.PCFI_FILTRAGE

La TOE doit fournir un contrôle des flux d'informations entre les réseaux qui lui sont connectés, en filtrant les flux en fonction de règles paramétrées par les administrateurs sur la base des caractéristiques suivantes :

L'interface de provenance du flux,

L'interface de destination du flux,

Machines aux extrémités du flux,

Type de protocole IP,

Pour ICMP : type de message,

Pour TCP et UDP : type de service,

Type de service DSCP.

Argumentaire : O.PCFI_FILTRAGE est principalement dédié à la satisfaction de la politique P.FILTRAGE.

O.PCFI_CONTEXTE_APPLICATIF

La TOE doit maintenir des contextes de suivi des sessions applicatives pour lesquelles des connexions « filles » sont nécessaires, et doit permettre de n'ouvrir les connexions filles liées à ces sessions que lorsque le contexte l'exige.

Note : Le cas le plus connu de « connexion fille » est celui des connexions de données FTP, dont les caractéristiques (port destination) ne peuvent être connues de manière prédéfinie et résultent du contenu de la session de commande.

Argumentaire : O.PCFI_CONTEXTE_APPLICATIF soutient O.PCFI_FILTRAGE pour couvrir la politique P.FILTRAGE. En effet, au cours d'une session applicative, les caractéristiques des connexions filles résultent du contenu de la session. En l'absence de suivi de ce contenu, la politique de filtrage devrait, dans le doute, autoriser toutes les variations possibles de ces caractéristiques pour que les protocoles applicatifs considérés puissent fonctionner. Cet objectif permet donc d'appliquer une politique de filtrage la plus restrictive possible.

O.PCFI_CHIFFREMENT

La TOE doit fournir des services de type VPN sur les flux échangés avec certains équipements distants afin d'assurer l'authentification mutuelle des extrémités, la confidentialité, et l'intégrité de ces flux.

Argumentaire : O.PCFI_CHIFFREMENT est principalement dédié à la satisfaction de la politique P.VPN.

Pour soutenir efficacement cet objectif, il est nécessaire d'empêcher les attaquants potentiels d'accéder aux clés de session VPN afin d'enfreindre l'objet de la politique P.VPN pour ce flux chiffré (le déchiffrer a posteriori, ou bien le modifier, le rejouer, ou y insérer des données). Cette protection est assurée :

- *du côté de la TOE, par HP.PROTECT_BOITIERS qui empêche un accès physique aux boîtiers,*
- *du côté des correspondants VPN par HTI.PROTECT_CORRESP_VPN et HTI.PROTECT_CLIENTS_VPN, selon que ces correspondants VPN sont des équipements réseau fixes ou des postes clients nomades.*

L'application d'une politique de chiffrement est le moyen le plus efficace de contrer l'usurpation d'adresse IP (M.IP_USURP), en imposant une authentification forte des entités aux extrémités du flux d'information. Cf. O.IPS_DETECTION_ATTAQUES pour les cas où la mise en place d'une politique de chiffrement n'est pas réalisable pour contrer cette menace.

O.JAA_PCFI[2]

La TOE doit :

journaliser les événements se rapportant à l'application de la politique de contrôle des flux d'information (filtrage et chiffrement),

permettre d'auditer les traces d'enregistrement de ces événements,

et remonter des alarmes à l'administrateur en cas de détection d'événements spécifiés comme critiques par ce dernier.

Argumentaire : O.JAA_PCFI est principalement dédié à la satisfaction de la politique P.AUDIT_ALARME. Il couvre l'aspect « enregistrement des événements de filtrage et de chiffrement jugés sensibles par l'administrateur » (P.AUDIT_ALARME.1).

2 'JAA' = journalisation, audit et alarmes.

4.4 Objectifs de protection contre les attaques Internet

O.IPS_DETECTION_ATTAQUES

La TOE doit être capable d'analyser les paquets associés aux flux d'information, ainsi que les requêtes / commandes / réponses applicatives incluses dans ces flux, afin de détecter et de rejeter des attaques sur les équipements des réseaux de confiance.

Argumentaire : O.IPS_DETECTION_ATTAQUES est principalement dédié à la satisfaction de la politique P.ANALYSE. La détection des attaques couvre notamment la corrélation entre l'adresse IP des paquets entrants et l'interface sur laquelle ils se présentent, ce qui permet de contrer les tentatives d'usurpation d'adresse IP (M.IP_USURP) menée avec des adresses non comprises dans la plage associée à l'interface de réception.

Note : Tous les flux autorisés à passer la TOE sont analysés même ceux qui sont à destination de celle-ci. Ce cas est particulier et n'est pas l'objectif de la formulation de O.IPS_DETECTION_ATTAQUES.

O.IPS_CONFORMITE_RFC

La TOE doit être capable d'analyser les paquets associés aux flux d'information, ainsi que les requêtes / commandes / réponses applicatives incluses dans ces flux afin de détecter et de rejeter les paquets et les flux applicatifs non conformes aux RFC.

Argumentaire : O.IPS_CONFORMITE_RFC est dédié à la satisfaction de la politique P.ANALYSE, particulièrement la prévention des infractions aux bonnes pratiques (P.ANALYSE.2).

O.JAA_IPS

La TOE doit :

journaliser les événements se rapportant à la détection des intrusions potentielles,

permettre d'auditer les traces d'enregistrement de ces événements,

et remonter des alarmes à l'administrateur en cas de détection d'événements spécifiés comme critiques par ce dernier.

Argumentaire : O.JAA_IPS est principalement dédié à la satisfaction de la politique P.AUDIT_ALARME. Il couvre les aspects de cette politique spécifiquement associés à la prise en compte des intrusions potentielles. Cet objectif soutient O.IPS_DETECTION_ATTAQUES et O.IPS_CONFORMITE_RFC en fournissant le moyen de contrôler a posteriori l'efficacité de la configuration de la fonction de prévention des intrusions, ainsi que de reconnaître d'éventuels faux positifs comme tels.

4.5 Objectifs de prévention de l'utilisation impropre

O.PCAOA

La TOE doit contrôler l'accès des administrateurs aux opérations d'administration de la sécurité en fonction de droits individuels associés à différentes tâches d'administration.

Argumentaire : O.PCAOA est dédié :

- *à la prévention de M.MAUVAIS_USAGE, puisqu'il permet d'implémenter une séparation des tâches adaptée à la responsabilité et à la compétence de chaque administrateur,*
- *à la prévention des opérations d'administration illicites (M.ADMIN_ILLICITE), puisqu'il permet de prévenir certaines opérations d'administration illicites (celles pour lesquelles un contrôle d'accès est techniquement réalisable, cf. O.JAA_PCAOA).*

O.PCAOA_I&A_ADMIN

La TOE doit exiger que les administrateurs soient identifiés et authentifiés avant de leur accorder l'accès à la fonction d'administration de la sécurité.

Argumentaire : O.PCAOA_I&A_ADMIN fournit les moyens de baser le contrôle d'accès spécifié par O.PCAOA et l'imputabilité spécifiée par O.JAA_PCAOA sur l'identité des administrateurs, afin de contrer M.MAUVAIS_USAGE et M.ADMIN_ILLICITE.

O.JAA_PCAOA

La TOE doit :

journaliser les événements se rapportant aux opérations d'administration de la sécurité effectuées par chaque administrateur autorisé,

permettre d'auditer et d'imputer les traces d'enregistrement de ces événements,

journaliser et remonter des alarmes à l'administrateur en cas de détection d'événements spécifiés comme critiques par ce dernier et notamment les tentatives d'ouverture de session d'administration non autorisées.

Argumentaire : Dans de nombreux contextes d'exploitation, il ne sera pas souhaitable ou techniquement possible d'empêcher les administrateurs d'effectuer certaines opérations d'administration de la sécurité, mais plutôt de les former et de les responsabiliser aux effets de ces opérations, tout en s'assurant a posteriori qu'ils les effectuent à bon escient. C'est en ce sens que O.JAA_PCAOA, avec le soutien de HH.PERSONNEL, complète O.PCAOA lorsque la prévention de M.MAUVAIS_USAGE et M.ADMIN_ILLICITE n'est pas réalisable par un contrôle d'accès technique aux opérations d'administration de la sécurité.

O.SAUVEGARDE_RESTAURATION

La TOE doit fournir des moyens de sauvegarder la configuration courante de ses fonctions de sécurité, et de restaurer celle-ci ultérieurement.

Argumentaire : O.SAUVEGARDE_RESTAURATION contribue à la prévention de l'utilisation impropre (M.MAUVAIS_USAGE) en permettant de conserver et de restaurer des configurations types validées par rapport à des problématiques de sécurité bien définies, et de revenir en arrière en cas d'erreur de manipulation. Cet objectif est dédié à la satisfaction de la politique P.SAUVEGARDE_RESTAURATION.

4.6 Objectifs de protection de la TOE

O.RESIST_AUTH_ADMIN

> La TOE doit fournir des mécanismes d'authentification qui empêchent que la réutilisation de données provenant de l'authentification d'administrateurs autorisés à se connecter à distance et/ou la contrefaçon de données d'authentification permette à un attaquant d'usurper l'identité d'un administrateur autorisé.

Argumentaire : O.RESIST_AUTH_ADMIN est dédié à la prévention de la menace M.ADMIN_USURP, qui est un pré requis possible pour la réalisation de M.ADMIN_ILLICITE.

O.PROTECT_JOURN

> La TOE capable de stocker localement les journaux, doit pouvoir mettre en œuvre des fonctions de rotation des fichiers de trace des événements de sécurité, d'arrêt de l'enregistrement de ces événements ou de blocage total des flux lorsqu'une saturation potentielle des fichiers survient.

Argumentaire : O.PROTECT_JOURN est dédié à la prévention de la menace M.PERTE_AUDIT. Il soutient les objectifs O.JAA_PCFI, O.JAA_IPS et O.JAA_PCAOA pour contrer les infractions à la politique P.AUDIT_ALARME et contrer les menaces M.MAUVAIS_USAGE et M.ADMIN_ILLICITE.

O.PROTECT_SESSIONS_ADMIN

> La TOE doit fournir des mécanismes permettant de protéger le contenu des sessions d'administration à distance contre les tentatives de visualisation, d'altération, de suppression par des attaquants.

Argumentaire : O.PROTECT_SESSIONS_ADMIN est dédié à la prévention de la menace M.SESSION_ADMIN_ILLICITE, qui est un pré requis possible pour la réalisation de M.ADMIN_ILLICITE.

4.7 Objectifs de sécurité pour l'environnement

OE.PROTECT_BOITIERS

Objectif permettant de s'assurer de la réalité de l'hypothèse HP.PROTECT_BOITIERS.

Argumentaire : Cet objectif de sécurité est dédié à la prévention de l'aspect physique de M.ADMIN_ILLICITE. Il élimine les possibilités d'effectuer des opérations d'administration de la sécurité illicites à partir d'un accès local aux boîtiers appliances firewall-VPN en l'absence du super-administrateur.

OE.SUPER_ADMIN

Objectif permettant de s'assurer de la réalité de l'hypothèse HO.SUPER_ADMIN.

Argumentaire :

1. *La centralisation, entre les mains du super-administrateur, de la capacité de procéder à l'installation ou à la maintenance des boîtiers firewall-VPN (HO.SUPER_ADMIN.1) a pour effet de garantir un fonctionnement correct des fonctions de sécurité de la TOE en général. HO.SUPER_ADMIN.1 soutient donc tous les objectifs de sécurité spécifiés pour la TOE pour contrer les menaces et satisfaire les règles de la politique de sécurité.*

2. La centralisation, entre les mains du super-administrateur, de la capacité d'implémenter la politique de séparation des tâches d'administration (HO.SUPER_ADMIN.2) a pour effet de garantir un fonctionnement correct des fonctions de sécurité dédiées à O.PCAOA et O.JAA_PCAOA. HO.SUPER_ADMIN.2 soutient donc ces objectifs de sécurité spécifiés pour la TOE pour contrer les menaces M.MAUVAIS_USAGE et M.ADMIN_ILLICITE.

3. Par ailleurs, le fait que toutes les interventions dans les locaux où sont stockés les boîtiers appliances firewall-VPN se fassent sous la surveillance et la responsabilité du super-administrateur (HO.SUPER_ADMIN.3) élimine les possibilités d'effectuer des opérations d'administration de la sécurité illicites à partir d'un accès local aux boîtiers appliances firewall-VPN en présence du super-administrateur. HO.SUPER_ADMIN.3 complète donc HP.PROTECT_BOITIERS pour contrer M.ADMIN_ILLICITE.

OE.MOT_PASSE

Objectif permettant de s'assurer de la réalité de l'hypothèse HO.MOT_PASSE.

Argumentaire : Cet objectif de sécurité soutient O.PCAOA_I&A_ADMIN pour contrer M.MAUVAIS_USAGE et M.ADMIN_ILLICITE en garantissant qu'on ne peut pas circonvenir à la fonction d'identification / authentification des administrateurs en obtenant le mot de passe d'un administrateur autorisé.

OE.BONNE_PCFI

Objectif permettant de s'assurer de la réalité de l'hypothèse HO.BONNE_PCFI.

Argumentaire : Cet objectif de sécurité est dédié à la prévention de M.MAUVAIS_USAGE.

OE.PERSONNEL

Objectif permettant de s'assurer de la réalité de l'hypothèse HH.PERSONNEL.

Argumentaire : Cet objectif de sécurité est dédié à la prévention de M.MAUVAIS_USAGE.

OE.COUPURE

Objectif permettant de s'assurer de la réalité de l'hypothèse HTI.COUPURE.

Argumentaire : Cet objectif de sécurité soutient tous les objectifs de sécurité spécifiés pour contrer les menaces et satisfaire les règles de la politique de sécurité associées au contrôle des flux d'information et à la protection contres les attaques Internet, puisqu'il permet d'éviter le contournement des fonctions de sécurité dédiées à ces objectifs en interdisant l'établissement de flux d'information soumis à la PCFI mais qui, du fait qu'ils ne passent par aucun des boîtiers appliances firewall-VPN, ne seraient pas soumis à ces fonctions de sécurité.

OE.USAGE_STRICT

Objectif permettant de s'assurer de la réalité de l'hypothèse HTI.USAGE_STRICT.

Argumentaire : Cet objectif de sécurité est dédié à la prévention de M.ADMIN_ILLICITE. Il élimine la possibilité d'effectuer des opérations d'administration de la sécurité illicites, ou de modifier le comportement des boîtiers appliances firewall-VPN de toute autre manière, à travers un accès détourné basé sur d'éventuelles vulnérabilités de logiciels non soumis à l'évaluation s'exécutant sur les boîtiers. L'interdiction des protocoles autres qu'IP (AppleTalk, IPX, etc.) permet d'empêcher le contournement de la politique de contrôle des flux d'information d'une manière similaire à OE.COUPURE.

OE.AUTONOME

Objectif permettant de s'assurer de la réalité de l'hypothèse HTI.AUTONOME.

Argumentaire : Cet objectif de sécurité élimine le risque de contournement des fonctions de sécurité à travers l'intrusion ou la substitution d'équipements externes dont dépendrait la TOE pour remplir ses fonctions. Il soutient donc tous les objectifs de sécurité spécifiés pour la TOE pour contrer les menaces et satisfaire les règles de la politique de sécurité.

OE.PROTECT_STATIONS

Objectif permettant de s'assurer de la réalité de l'hypothèse HTI.PROTECT_STATIONS.

Argumentaire : Cet objectif de sécurité est dédié à la prévention de M.ADMIN_ILLICITE.

OE.PROTECT_CORRESP_VPN

Objectif permettant de s'assurer de la réalité de l'hypothèse HTI.PROTECT_CORRESP_VPN.

Argumentaire : Cet objectif de sécurité soutient O.PCFI_CHIFFREMENT pour satisfaire P.VPN en garantissant que l'objet de la politique de chiffrement (la protection en confidentialité et en intégrité des flux d'information) ne peut être contourné à travers la récupération des clés de session sur les équipements distants.

OE.PROTECT_CLIENTS_VPN

Objectif permettant de s'assurer de la réalité de l'hypothèse HTI.PROTECT_CLIENTS_VPN.

Argumentaire : Cet objectif de sécurité soutient O.PCFI_CHIFFREMENT pour satisfaire P.VPN en garantissant que l'objet de la politique de chiffrement (la protection en confidentialité et en intégrité des flux d'information) ne peut être contourné à travers la récupération des clés de session sur les postes clients.

4.8 Argumentaire des objectifs de sécurité

La prévention des menaces et la satisfaction des règles de la politique de sécurité par les objectifs de sécurité est exprimée dans les rubriques « argumentaire » qui accompagnent l'énoncé de chaque objectif de sécurité. Le lien entre les objectifs de sécurité et les menaces ou les règles de la politique de sécurité est résumé ci-dessous.

		P.FILTRAGE	P.VPN	P.AUDIT_ALARME	P.ANALYSE	M.IP_USURP	M.MAUVAIS_USAGE	P.SAUVEGARDE_RESTAURATION	M.ADMIN_ILLICITE	M.ADMIN_USURP	M.SESSION_ADMIN_ILLICITE	M.PERTE_AUDIT
O.PCFI_FILTRAGE		X										
O.PCFI_CONTEXTE_APPLICATIF		S										
O.PCFI_CHIFFREMENT			X			X						
O.JAA_PCFI				X								
O.IPS_DETECTION_ATTAQUES					X	X						
O.IPS_CONFORMITE_RFC					X							
O.JAA_IPS				X	S	S						
O.PCAOA							X		X			
O.PCAOA_I&A_ADMIN							X		X			
O.JAA_PCAOA							X		X			
O.SAUVEGARDE_RESTAURATION							X	X				
O.RESIST_AUTH_ADMIN									X	X		
O.PROTECT_JOURN				S			S		S			X
O.PROTECT_SESSIONS_ADMIN									X		X	
OE.PROTECT_BOITIERS									X			
OE.SUPER_ADMIN	1	S	S	S	S	S	S	S	S	S	S	S
	2						S		S			
	3								S			
OE.MOT_PASSE							S		S			
OE.BONNE_PCFI							X					
OE.PERSONNEL							X					
OE.COUPURE		S	S	S	S	S						
OE.USAGE_STRICT		S	S	S	S	S			X			
OE.AUTONOME		S	S	S	S	S	S	S	S	S	S	S
OE.PROTECT_STATIONS									X			
OE.PROTECT_CORRESP_VPN			S									
OE.PROTECT_CLIENTS_VPN			S									

Légende :
X: l'objectif est dédié à la prévention de la menace / la satisfaction de la règle de la politique de sécurité.
S: l'objectif soutient d'autres objectifs pour prévenir les menaces / satisfaire les règles de la politique de sécurité.

4.9 Liens entre les hypothèses et les objectifs de sécurité pour l'environnement

Le tableau ci-dessous permet de faire le lien entre les hypothèses de sécurité pour l'environnement et les objectifs qui sont associés.

	HP.PROTECT_BOITIERS	HO.SUPER_ADMIN	HO.MOT_PASSE	HO.BONNE_PCFI	HH.PERSONNEL	HTI.COUPURE	HTI.USAGE_STRICT	HTI.AUTONOME	HTI.PROTECT_STATIONS	HTI.PROTECT_CORRESP_VPN	HTI.PROTECT_CLIENTS_VPN
OE.PROTECT_BOITIERS	X										
OE.SUPER_ADMIN		X									
OE.MOT_PASSE			X								
OE.BONNE_PCFI				X							
OE.PERSONNEL					X						
OE.COUPURE						X					
OE.USAGE_STRICT							X				
OE.AUTONOME								X			
OE.PROTECT_STATIONS									X		
OE.PROTECT_CORRESP_VPN										X	
OE.PROTECT_CLIENTS_VPN											X

Légende :
X: l'objectif est lié à l'hypothèse de sécurité pour l'environnement.

5 EXIGENCES DE SÉCURITÉ DES TI

Le but de cette section est de présenter les exigences de sécurité des TI, qui résultent du raffinement des objectifs de sécurité, ainsi qu'un argumentaire démontrant que ce raffinement a été correctement effectué.

Les exigences de sécurité des TI comprennent les exigences de sécurité pour la TOE et les exigences de sécurité pour l'environnement qui, si elles sont satisfaites, garantiront que la TOE peut satisfaire à ses objectifs de sécurité.

Les CC répartissent les exigences de sécurité en deux catégories : exigences fonctionnelles et exigences d'assurance. Les exigences fonctionnelles portent sur les fonctions de la TOE qui contribuent spécifiquement à la sécurité des TI et qui garantissent le comportement souhaité en terme de sécurité. Les exigences d'assurance portent sur les actions à effectuer par le développeur, les éléments de preuve à produire et les actions à effectuer par l'évaluateur.

5.1 Introduction

5.1.1 Généralités

Les exigences fonctionnelles de sécurité de la TOE ont été réparties dans les sous-ensembles fonctionnels suivants :

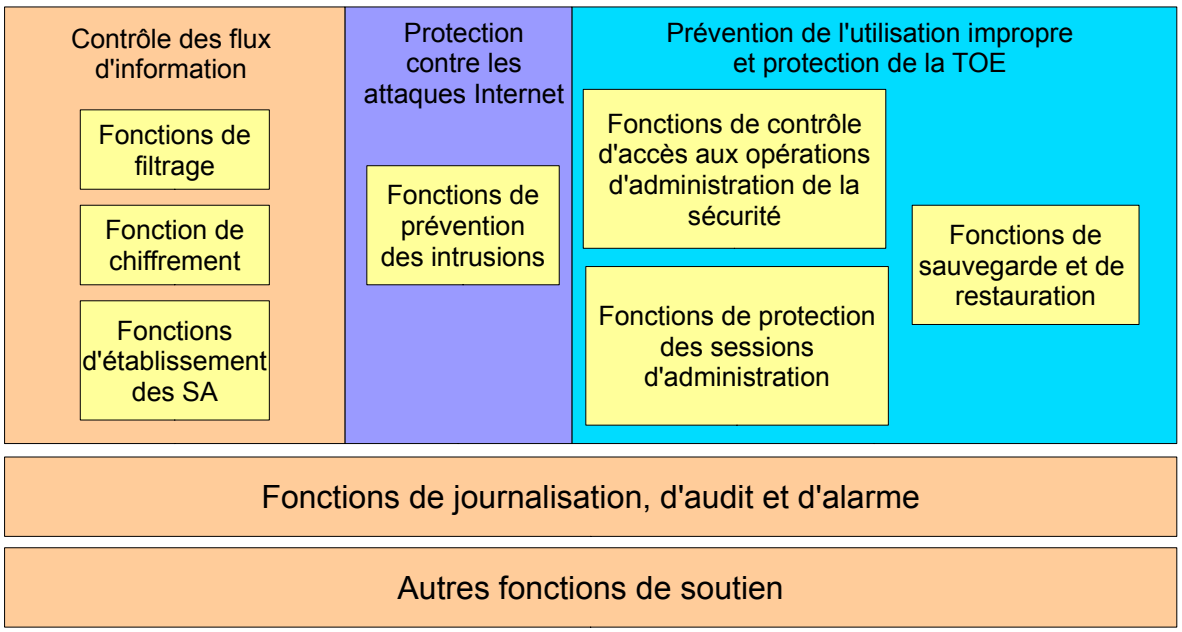


Illustration 4: Sous-ensembles fonctionnels de la TOE.

5.1.2 Conventions typographiques

Afin de présenter des exigences de sécurité faciles à lire et à utiliser, celles-ci ont été rédigées en français, en s'aidant de la traduction française des Critères Communs, et un effort a été accompli pour transposer les notions Critères Communs (comme « la TSF » ou « les sujets et les objets ») dans des termes correspondant au produit, par le jeu des opérations d'affectation, de sélection et de raffinement des Critères Communs. Les opérations n'ont pas été identifiées dans le texte des exigences de cette section, les libellés qui résultent de leur application sont seulement signalés en gras.

Or, seul l'énoncé en anglais extrait de [CC-02] et [CC-03] a une valeur normative et tient lieu de référence. De plus, les opérations effectuées doivent être précisément identifiées. L'annexe C, §9, a été spécialement rédigée à cet effet et constitue l'élément de preuve à prendre en compte comme énoncé des exigences de sécurité des TI.

Les exigences de sécurité explicitement énoncées ont également été spécifiées initialement en anglais puis traduites dans cette section. L'annexe D, §10, présente ces exigences de sécurité explicitement énoncées sous un format similaire à celui de [CC-02].

Format des étiquettes des exigences de sécurité :

- Les exigences d'assurance sécurité ont des étiquettes identiques à celles utilisées dans [CC-03] ;
- Les exigences fonctionnelles de sécurité ont des étiquettes au format suivant:

  F*CC_FFF.composant.<itération.>n*
  - F*CC* est le trigramme de la classe ;
  - *FFF* est le trigramme de la famille ;
  - *composant* est l'identifiant du composant : soit un numéro pour les composants extraits de [CC-02], soit un trigramme pour les exigences de sécurité explicitement énoncées;
  - *itération* est une étiquette permettant d'identifier les différentes itérations d'un même composant à l'intérieur de différents ensembles fonctionnels;
  - *n* est le numéro d'élément.

5.1.3 Présentation des données de sécurité

Attributs des paquets IP sur lesquels portent les règles de filtrage et de chiffrement

- L'interface de réception du paquet ;
- L'interface de destination du paquet ;
- L'adresse IP source et destination du paquet et, partant de là, la machine source et la machine destination du paquet ;
- Le numéro de protocole IP ;
- La valeur du champ DSCP ;
- L'index de sécurité ESP ;
- Le port source et destination TCP/UDP ou le type de message ICMP.

Notion de slot

Le comportement des fonctions de sécurité est décrit à l'aide de « *slots* », qui sont une représentation abstraite et interprétable par les administrateurs des fichiers de configuration du boîtier appliance firewall-VPN. Les slots décrivent des comportements de sécurité bien définis, pouvant être sauvegardés et réutilisés. Ils peuvent être activés à la demande.

Dans le cadre de l'évaluation, nous nous intéressons à deux types de slots : les slots de filtrage et les slots de chiffrement (aussi appelés « slots VPN »).

- Un slot de filtrage est une liste de règles de filtrage et de translation d'adresses. La politique de filtrage appliquée est la concaténation de deux slots de filtrage; le slot de filtrage global puis le slot de filtrage local. En fonctionnement, il y a toujours au moins un slot de filtrage local actif.
- Un slot de chiffrement est un ensemble de tunnels VPN.

Paramètres des règles de filtrage

- L'identifiant de la règle ;
- (critère) L'interface de réception des paquets IP couverts par la règle ;
- (critère) L'interface de destination des paquets IP couverts par la règle ;
- (critère) La ou les machines à l'origine des flux d'information couverts par la règle ;
- (critère) Le ou les protocoles IP, le champ DSCP, les services TCP/UDP ou les types de messages ICMP des flux d'information couverts par la règle ;
- (critère) La ou les machines destinataires des flux d'information couverts par la règle ;
- L'action : 'aucune', 'passer', 'bloquer', 'réinitialiser', 'déléguer' ;
- La génération d'un enregistrement d'audit et le niveau d'alarme éventuellement attribué ;
- La politique de qualité de service associée aux flux couverts par la règle ;
- Le taux maximum d'ouverture connexions / pseudo-connexions associé à la règle ;
- Le profil d'attaques internet associé aux connexions couvertes par la règle.

Paramètres d'une connexion / pseudo connexion

- (critère) L'adresse IP source, l'adresse IP destination ;
- (critère) Le type de protocole (TCP, UDP ou ICMP) ;
- (critère) Pour TCP et UDP : les ports source et destination ;
- (critère) Pour ICMP : les champs 'type' et 'code' du message ICMP ;
- Pour UDP et ICMP : l'âge de la pseudo connexion ;
- Pour TCP : l'état de la connexion, les fenêtres (dans le but de rejeter les paquets non conformes).

Caractéristiques des utilisateurs IPSec

- Le nom de login de l'utilisateur;
- Des renseignements sur l'utilisateur (nom, prénom, téléphone, mail, etc.) ;
- Le mot de passe de référence.

Droits des utilisateurs IPSec

- Le nom de login de l'utilisateur IPSec ;
- Le fait que l'utilisateur soit autorisé à s'authentifier (on peut révoquer un utilisateur sans supprimer son compte).

Paramètres des tunnels VPN

Un tunnel VPN consiste en un chemin de confiance (la SA ISAKMP) entre le boîtier appliance firewall-VPN et un correspondant VPN, ainsi qu'un ensemble de règles de chiffrement à appliquer aux flux d'information qui doivent passer par le tunnel. L'application de ces règles nécessite la négociation et l'établissement de contextes de sécurité qui sont les SA IPSec.

Les paramètres des tunnels VPN sont les suivants :

- L'interface locale sur laquelle le tunnel doit être mis en œuvre ;
- L'adresse IP de l'autre extrémité du tunnel (le correspondant VPN) ;
- Le mécanisme d'authentification mutuelle : clé pré-partagée (PSK) ou certificats (PKI) ou HybridAuth+XAuth ;
- En cas d'authentification par certificat ou HybridAuth+XAuth : le certificat X509 présenté par le boîtier appliance firewall-VPN ;
- En cas d'authentification par clé pré-partagée : l'adresse IP du boîtier appliance firewall-VPN ;
- Les règles de chiffrement associées au tunnel ;
- La paire de SA ISAKMP courantes associée au tunnel VPN.

Paramètres d'une SA ISAKMP

- Le correspondant VPN ;
- L'âge actuel de la SA ;
- Sa durée de vie ;
- L'algorithme d'authentification effectif, et sa clé ;
- L'algorithme de chiffrement effectif, et sa clé ;

Règle de chiffrement (entrée de SPD)

- (critère) La ou les machines locales couvertes par la règle ;
- (critère) La ou les machines distantes couvertes par la règle ;
- (critère) Le type de protocole couvert par la règle ;
- Les propositions acceptables lors de la négociation des SA :
  - Algorithmes d'authentification et tailles des clés ;
  - Algorithmes de chiffrement et tailles des clés ;
  - Durée de vie des SA.

- Les paires de SA IPSec courantes associées à la règle.

Paramètres d'une SA IPSec

- (critère) L'index de sécurité (*SPI – Security Parameter Index*) ;
- L'âge actuel de la SA ;
- Sa durée de vie ;
- Le caractère entrant ou sortant ;
- L'algorithme d'authentification effectif, et sa clé ;
- L'algorithme de chiffrement effectif, et sa clé.

Caractéristiques des correspondants VPN gérées par le boîtier appliance firewall-VPN

- Soit un certificat X509 ou une CA (avec la CRL associée) dans le cas de l'authentification par certificat ;
- Soit l'identifiant (adresse IP), associé à une clé pré-partagée ;
- Soit l'identifiant (login), associé au mot de passe de l'utilisateur.

Profil des attaques Internet

- Le libellé ;
- L'action associée : bloquer ou laisser passer le paquet (pas toujours configurable) ;
- Le niveau d'alarme désiré: ignorée, mineure ou majeure.

Profil des événements système

- Le libellé ;
- Le niveau d'alarme désiré: ignorée, mineure, majeure ou système.

Caractéristiques des administrateurs

- Le nom de login de l'administrateur ;
- Des renseignements sur l'administrateur (nom, prénom, téléphone, mail, etc.) ;
- Le fait que l'administrateur soit autorisé à s'authentifier (on peut révoquer un administrateur sans supprimer son compte) ;
- Le mécanisme d'authentification[3] ;
- Le mot de passe de référence.

Droits des administrateurs

- Le nom de login de l'administrateur ;

3 Obligatoirement SRP, identifiant / mot de passe (TLS) ou Certificat (TLS) dans le mode d'utilisation soumis à l'évaluation.

- Le groupe auquel l'administrateur appartient ;
- La liste des droits de l'administrateur.

Les administrateurs sont gérés dans la même base locale que les utilisateurs non administratifs, mais on leur attribue en plus un rôle administrateur explicite, ainsi qu'un profil construit à partir d'un droit de modification ('M') et de droits associés à différents domaines de gestion de la sécurité. Le détail des différents droit est fourni à l'annexe A, §7.

Les droits attribués aux administrateurs et utilisateurs IPSec sont gérés dans des fichiers distincts de la base locale des administrateur et des utilisateurs.

On utilise le terme 'auditeur' pour désigner les administrateurs chargés d'effectuer les audits et de gérer les traces d'audit. Ces auditeurs sont des administrateurs possédant le droit 'L'.

5.2 Exigences de sécurité pour la TOE

Cette section présente le raffinement des exigences fonctionnelles de la TOE. La description formelle de ces exigences figure au chapitre 9. L'exigence fonctionnelle étendue est décrite au chapitre 10. Pour assurer la traçabilité, on indique ici le titre des exigences fonctionnelles concernées entre crochets (ex : [FDP_IFC.2.1]).

5.2.1 Exigences de contrôle des flux d'information

Fonction de filtrage

FDP_IFC.2 – Filtrage complet des flux d'information

[FDP_IFC.2.1]

La fonction de filtrage doit appliquer la **politique de filtrage** aux **paquets IP entrants.**

[FDP_IFC.2.2]

La fonction de filtrage doit garantir que **tous les paquets IP entrants** sont couverts par **la politique de filtrage**.

Argumentaire : FDP_IFC.2 soutient FDP_IFF.1.Filtrage pour satisfaire O.PCFI_FILTRAGE, en définissant la politique de filtrage et en exigeant qu'elle s'applique à tous les paquets IP entrants.

FDP_IFF.1.Filtrage – Fonction de filtrage

[FDP_IFF.1.Filtrage.1]

La fonction de filtrage doit appliquer la **politique de filtrage** en fonction des types suivants d'attributs de sécurité **des paquets IP entrants :**

a. L'interface de réception,

b. L'interface de destination,

c. L'adresse IP source et destination du paquet et, partant de là, la machine source et la machine destination du paquet,

d. Le numéro de protocole IP,

e. La valeur du champ DSCP,

f. Si le protocole est TCP ou UDP : le port source et destination,

g. Si le protocole est ICMP : les champs 'type' et 'code' du message ,

[FDP_IFF.1.Filtrage.2]

La fonction de filtrage doit autoriser **un paquet IP entrant** si les règles suivantes s'appliquent :

a. Préalablement à l'application des règles de filtrage, le paquet est comparé à l'ensemble des connexions / pseudo-connexions actuellement établies et ayant été autorisées par les règles de filtrage ;

b. Si le paquet correspond à une de ces connexions / pseudo-connexions, il est autorisé à passer sans être soumis aux règles de filtrage ;

c. Sinon, le paquet est autorisé si l'action de la première règle de filtrage applicable est 'passer'.

[FDP_IFF.1.Filtrage.3]

La fonction de filtrage doit appliquer **les règles complémentaires suivantes :**

a. les règles de filtrage dont l'action est 'aucune' ont pour unique objet la génération d'enregistrements d'audit et ne rentrent pas en compte dans le filtrage des paquets.

b. les règles de filtrage dont l'action est 'déléguer' ont pour unique objet le saut de l'évaluation de la fin du slot de filtrage global pour reprendre au début du slot local et ne rentrent pas en compte dans le filtrage des paquets.

[FDP_IFF.1.Filtrage.4]

La fonction de filtrage doit autoriser explicitement **un paquet IP entrant** en fonction des règles suivantes :

a. Les sessions associées à des protocoles nécessitant des connexions filles sont suivies de manière à autoriser ces connexions filles conformément à l'état de la session principale ;

b. Des règles de filtrage implicites peuvent être générées par le firewall en liaison avec la configuration d'autres fonctions de sécurité. Ce sont les règles correspondant à :

i. l'administration à distance du firewall,

ii. l'établissement de VPN.

[FDP_IFF.1.Filtrage.5]

La fonction de filtrage doit interdire explicitement **un paquet IP entrant** en fonction des règles suivantes :

a. L'action de la première règle de filtrage applicable est 'bloquer' ou 'réinitialiser' ;

b. Aucune règle de filtrage n'a autorisé le paquet.

Argumentaire : FDP_IFF.1.Filtrage est dédié à la satisfaction de l'objectif O.PCFI_FILTRAGE. Le point FDP_IFF.1.Filtrage.4.a couvre également l'objectif O.PCFI_CONTEXTE_APPLICATIF.

Fonction de chiffrement

FDP_IFC.1 – Chiffrement des flux d'information

[FDP_IFC.1.1]

La fonction de chiffrement doit appliquer la **politique de chiffrement** aux **datagrammes ESP entrants et aux datagrammes IP sortants couverts par une règle de chiffrement**.

Argumentaire : FDP_IFC.1 soutient FDP_UCT.1, FDP_UIT.1 et FDP_IFF.1.Chiffrement pour satisfaire O.PCFI_CHIFFREMENT, en définissant la politique de chiffrement.

FDP_UCT.1 – Confidentialité du contenu des flux

[FDP_UCT.1.1]

La fonction de chiffrement doit appliquer la **politique de chiffrement** afin de pouvoir **transmettre et recevoir** des **datagrammes IP** d'une façon qui les protège d'une divulgation non autorisée.

Argumentaire : FDP_UCT.1 est dédié à la satisfaction de l'aspect « confidentialité » de l'objectif O.PCFI_CHIFFREMENT.

FDP_UIT.1 – Intégrité du contenu des flux

[FDP_UIT.1.1]

La fonction de chiffrement doit appliquer la **politique de chiffrement** afin de pouvoir **transmettre et recevoir** des **datagrammes IP** d'une façon qui les protège d'erreurs **de modification, d'insertion ou de rejeu**.

[FDP_UIT.1.2]

La fonction de chiffrement doit pouvoir déterminer lors de la réception **des datagrammes ESP entrants** si **une modification, une insertion ou un rejeu** a eu lieu.

Argumentaire : FDP_UIT.1 est dédié à la satisfaction de l'aspect « intégrité » de l'objectif O.PCFI_CHIFFREMENT.

FDP_IFF.1.Chiffrement – Fonction de chiffrement

[FDP_IFF.1.Chiffrement.1]

La fonction de chiffrement doit appliquer la **politique de chiffrement** en fonction des types suivants d'attributs de sécurité **des datagrammes ESP entrants et des datagrammes IP sortants couverts par une règle de chiffrement :**

Datagrammes ESP entrants :

a. L'index de sécurité (*SPI*),

Datagrammes IP sortants :

b. L'adresse IP source et destination du paquet et, partant de là, la machine source et la machine destination du paquet,

c. Le type de protocole IP.

[FDP_IFF.1.Chiffrement.2]

La fonction de chiffrement doit autoriser **un paquet ESP entrant** si les règles suivantes s'appliquent :

a. un datagramme ESP entrant est rattachable à une SA IPSec entrante active,

b. le paquet encapsulé dans le datagramme ESP correspond aux critères de la règle de chiffrement associée à la SA IPSec.

[FDP_IFF.1.Chiffrement.3]

La fonction de chiffrement doit appliquer **les règles complémentaires suivantes :**

a. utilise sur les datagrammes IP sortants, les algorithmes d'authentification et de chiffrement effectifs spécifiés par la SA IPSec sortante associée à la première règle de chiffrement applicable.

b. provoque une tentative de renégociation si un datagramme IP sortant est couvert par une règle de chiffrement sans SA IPSec sortante active et qu'une autre tentative n'est pas déjà en cours. Le datagramme est détruit.

[FDP_IFF.1.Chiffrement.4]

(sans objet).

[FDP_IFF.1.Chiffrement.5]

(sans objet).

Argumentaire : FDP_IFF.1.Chiffrement soutient FDP_UCT.1, FDP_UIT.1 et FTP_TRP.1.Corresp pour satisfaire O.PCFI_CHIFFREMENT :

en garantissant que la fonction de chiffrement est appliquée aux datagrammes IP sortants couverts par la politique de chiffrement,

en aiguillant les datagrammes ESP entrants vers les traitements de contrôle d'intégrité et de déchiffrement spécifiés par la SA IPSec entrant applicable,

en recourant à l'utilisation du chemin de confiance en cas de datagramme IP sortant couvert par une règle de chiffrement sans SA IPSec sortante applicable.

Fonction d'établissement des SA

FTP_TRP.1.Corresp – Chemin de confiance avec les correspondants VPN

[FTP_TRP.1.Corresp.1]
La fonction d'établissement des SA doit fournir un chemin de communication entre **le boîtier appliance firewall-VPN et les correspondants VPN** qui soit logiquement distinct des autres chemins de communication et qui garantisse l'identification de ses extrémités et la protection des données transférées contre une **modification ou une divulgation**.

[FTP_TRP.1.Corresp.2]
La fonction d'établissement des SA doit permettre **à le boîtier appliance firewall-VPN et aux correspondants VPN** d'initier une communication via le chemin de confiance. **L'établissement du chemin de confiance correspond à la phase 1 du protocole IKE.**

[FTP_TRP.1.Corresp.3]
La fonction d'établissement des SA doit exiger l'utilisation du chemin de confiance pour :

l'authentification mutuelle initiale des extrémités du tunnel (phase 1 du protocole IKE),

la négociation des SA IPSec (phase 2 du protocole IKE).

Argumentaire : FTP_TRP.1.Corresp est dédié à la satisfaction de l'aspect « authentification mutuelle des extrémités » de l'objectif O.PCFI_CHIFFREMENT.

FIA_UAU.5.Corresp – Multiples mécanismes d'authentification des correspondants VPN

[FIA_UAU.5.Corresp.1]
La fonction d'établissement des SA doit fournir **les mécanismes d'authentification suivants** pour contribuer à l'authentification **du correspondant VPN d'un tunnel donné, dans le cadre de l'authentification mutuelle initiale des extrémités de ce tunnel lors de la phase 1 IKE :**

certificats X509,

clé pré-partagée.

[FIA_UAU.5.Corresp.2]
La fonction d'établissement des SA doit authentifier l'identité annoncée de tout **correspondant VPN** selon **le mécanisme d'authentification spécifié pour le tunnel VPN**.

Argumentaire : FIA_UAU.5.Corresp soutient FTP_TRP.1.Corresp pour satisfaire l'objectif O.PCFI_CHIFFREMENT.

FPT_TDC.1 – Négociation des SA ISAKMP et IPSec

[FPT_TDC.1.1]

La fonction d'établissement des SA doit offrir la capacité **de négocier les paramètres des SA ISKAMP et IPSec lors de l'établissement des tunnels VPN entre le boîtier appliance firewall-VPN et les correspondants VPN**.

[FPT_TDC.1.2]

La fonction d'établissement des SA doit utiliser **les règles suivantes** pour **négocier les paramètres des SA ISAKMP ou IPSec avec les correspondants VPN :**

a. Si le boîtier appliance firewall-VPN est l'initiateur, proposer les paramètres de la SA ISAKMP ou IPSEC, et accepter les réponses aussi rigoureuses qu'une des propositions faites ;

b. Si le boîtier appliance firewall-VPN est le répondeur, n'accepter que les propositions aussi rigoureuses qu'une des propositions locales.

Argumentaire : FPT_TDC.1 soutient :

d'une part FTP_TRP.1 pour satisfaire les aspects « authentification mutuelle des extrémités » de l'objectif O.PCFI_CHIFFREMENT, en permettant de négocier les paramètres qui vont permettre l'authentification mutuelle,

d'autre part FDP_UCT.1 et FDP_UIT.1 pour satisfaire les aspects « confidentialité » et « intégrité » de l'objectif O.PCFI_CHIFFREMENT en permettant de négocier les paramètres des algorithmes de chiffrement et d'authentification.

Fonction de journalisation, d'audit et d'alarme

FAU_GEN.1 – Génération de données d'audit

[FAU_GEN.1.1]

La fonction de journalisation doit pouvoir générer un enregistrement d'audit des événements auditables suivants :

démarrage et arrêt de la **fonction de journalisation**,

et **les événements auditables énumérés dans le tableau au chapitre 5.2 (après FAU_GEN.1.2)**

[FAU_GEN.1.2]

La fonction de journalisation doit enregistrer au minimum les informations suivantes dans chaque enregistrement d'audit :

date et heure de l'événement,

type d'événement,

adresse IP source,

résultat (succès ou échec) de l'événement,

niveau d'alarme (si c'en est une),

pour chaque type d'événement d'audit, les informations d'audit complémentaires énoncées dans le tableau ci-dessous :

Composant	*Événements auditables*	*Informations d'audit*
FDP_IFF.1.Filtrage	Application d'une règle de filtrage pour laquelle la génération d'un enregistrement d'audit est spécifiée.	▪ Nom de l'interface de réception, ▪ Nom de l'interface de destination, ▪ Action appliquée, ▪ Identifiant de la règle, ▪ Type de protocole, ▪ Type ICMP, ▪ Port source, ▪ Adresse IP et port destination.
FTP_TRP.1.Corresp et FPT_TDC.1	Tentative d'établissement de SA ISAKMP et IPSec.	▪ Phase IKE (1 ou 2), ▪ Si échec : la raison de l'échec (si possible).
FAU_STG.3	Dépassement de la limite	
FAU_SAA.4	Détection d'attaque Internet potentielle	▪ Nom de l'interface de réception, ▪ Action appliquée, ▪ Libellé de l'attaque, ▪ Type de protocole, ▪ Type ICMP, ▪ Port source, ▪ Adresse IP et port destination.
FMT_SMR.1, FMT_MOF.1, FMT_MTD.1, FTP_TRP.1.Admin	Accomplissement d'une opération d'administration de la sécurité (dont tentative d'ouverture de session d'administration)	▪ Type de l'opération, ▪ Paramètres, ▪ Identifiant de session d'administration,

Argumentaire : FAU_GEN.1 est dédié à la satisfaction des aspects « journalisation » (point 1) des objectifs O.JAA_PCFI, O.JAA_IPS et O.JAA_PCAOA. Pour les événements associés à FDP_IFF.1.Filtrage et FAU_SAA.4, le résultat (succès ou échec) associé à l'événement correspond à l'action appliquée par le boîtier appliance firewall-VPN.

FAU_GEN.2 – Identification de l'utilisateur

[FAU_GEN.2.1]

Pour tout évènement d'audit résultant des actions des **administrateurs** identifiés, la **fonction de journalisation** doit pouvoir associer cet **événement auditable associé aux opérations d'administration de la sécurité** avec l'identité de **l'administrateur** qui a causé cet évènement.

Argumentaire : FAU_GEN.2 est dédié à la satisfaction des aspects « imputabilité » (point 2) de l'objectif O.JAA_PCAOA.

FAU_SAR.1 – Revue d'audit

[FAU_SAR.1.1]

La fonction d'audit doit offrir aux **auditeurs** la faculté de lire **toutes les informations d'audit** à partir des **fichiers de trace**.

[FAU_SAR.1.2]

La fonction d'audit doit présenter les **fichiers de trace** d'une façon permettant à **l'auditeur** de les interpréter.

Argumentaire : FAU_SAR.1 est dédié à la satisfaction des aspects « audit » (point 2) des objectifs O.JAA_PCFI, O.JAA_IPS et O.JAA_PCAOA.

FAU_STG.3 – Action en cas de perte possible de données d'audit

[FAU_STG.3.1]

La fonction de journalisation doit entreprendre **une action parmi les suivantes :**

a. Assurer la rotation des fichiers : les enregistrements d'audit les plus récents effacent les enregistrements d'audit les plus anciens,

b. Stopper l'écriture des fichiers : les enregistrements d'audit ne sont plus mémorisés,

c. Arrêter le Firewall : le boîtier appliance firewall-VPN ne s'arrête pas réellement mais il bloque l'ensemble des flux excepté les sessions d'administration du Web Manager depuis le réseau interne.

si un fichier de trace existant (exclus l'utilisation de Syslog) dépasse la taille de 5Mo.

Argumentaire : FAU_STG.3 est dédié à la satisfaction de l'objectif O.PROTECT_JOURN. Il ne s'applique pas à une TOE qui n'est pas capable d'enregistrer localement les événements.

FAU_ARP.1.Alarmes – Réponse automatique aux alarmes

[FAU_ARP.1.Alarmes.1]

La fonction d'alarme doit entreprendre **de transmettre l'alarme aux moniteurs temps-réel connectés** dès la **génération d'un enregistrement d'audit auquel est attribué un niveau d'alarme.**

Argumentaire : FAU_ARP.1.Alarmes est dédié à la satisfaction des aspects « remontée d'alarmes » (point 3) des objectifs O.JAA_PCFI, O.JAA_IPS et O.JAA_PCAOA. On notera que la dépendance avec FAU_GEN.1 est implicitement satisfaite puisqu'il agit sur des enregistrements d'audit.

5.2.2 Exigences de protection contre les attaques Internet

Fonction de prévention des intrusions

FAU_SAA.4 – Heuristiques des attaques complexes

[FAU_SAA.4.1]

La fonction de prévention des intrusions doit pouvoir maintenir une **base de connaissance**[4] des **types d'attaque suivants** qui peuvent indiquer une **attaque Internet potentielle** :

a. paquets IP dont l'adresse source est incohérente avec l'interface de réception,

b. paquets, datagrammes ou segments IP, ICMP, IGMP, TCP ou UDP non conformes aux RFC, ou utilisation abusive des possibilités offertes par ces protocoles,

c. commandes, requêtes ou réponses applicatives non conformes à la syntaxe générale des commandes / requêtes / réponses définie par les RFC, ou utilisation abusive des possibilités offertes par ces protocoles,

d. attaques basées sur des vulnérabilités connues des serveurs applicatifs,

4 La base de connaissance est un ensemble de contrôle figé par version de TOE

e. tentatives de récupération d'information concernant la configuration des serveurs applicatifs (*fingerprinting*, *port scanning*, etc.),

f. dépassement du taux d'ouverture de connexions associé à une règle de filtrage.

[FAU_SAA.4.2]

La fonction de prévention des intrusions doit pouvoir comparer **l'état des différents contextes associés à chaque paquet IP entrant et sortant aux types d'attaques présents dans la base de connaissance**.

[FAU_SAA.4.3]

La fonction de prévention des intrusions doit être capables d'indiquer une **attaque Internet potentielle** quand **l'état d'un ou plusieurs contextes associés à un paquet IP entrant** correspond à un **type d'attaque présent dans la base de connaissance**.

Argumentaire : FAU_SAA.4 est dédié à la satisfaction de l'objectif O.IPS_DETECTION_ATTAQUES ainsi que la mise en œuvre de la conformité aux RFC spécifiée par O.IPS_CONFORMITE_RFC (points FAU_SAA.4.1.b et FAU_SAA.4.1.c).

FAU_ARP.1.IPS – Réponse automatique aux attaques Internet potentielles

[FAU_ARP.1.IPS.1]

Dès la détection d'une **attaque Internet potentiellement véhiculée par un paquet IP entrant**, l**a fonction de prévention des intrusions** doit :

a. appliquer au paquet l'action associée au type de l'attaque,

b. si un niveau d'alarme est spécifié pour ce type d'attaque, générer un enregistrement d'audit de l'événement, en lui attribuant ce niveau d'alarme.

Argumentaire : FAU_ARP.1.IPS soutient FAU_SAA.4 pour la satisfaction de l'objectif O.IPS_DETECTION_ATTAQUES et pour la mise en œuvre de la conformité aux RFC spécifiée par O.IPS_CONFORMITE_RFC. De plus, FAU_ARP.1.IPS est spécifiquement dédié au point 3 de l'objectif O.JAA_IPS.

5.2.3 Exigences de prévention de l'utilisation impropre

Fonction de contrôle d'accès aux opérations d'administration de la sécurité

FMT_SMF.1 – Fonction d'administration de la sécurité

[FMT_SMF.1.1]

La fonction d'administration de la sécurité doit être capable de réaliser les fonctions d'administration de la sécurité suivantes :

a. La fonction de contrôle d'accès aux opérations d'administration de la sécurité ;

b. La fonction de protection des sessions d'administration

c. La fonction d'audit

d. La fonction de sauvegarde / restauration

Argumentaire : FMT_SMF.1 soutient FMT_MOF.1 et FMT_MTD.1 pour satisfaire à l'objectif de contrôle d'accès aux opérations d'administration spécifié par O.PCAOA. Il assure également la mise en oeuvre de FTP_ITT.1, FAU_SAR.1 et FMT_MTD.BRS

FMT_SMR.1 – Rôle d'administrateur de la sécurité

[FMT_SMR.1.1]

La fonction de contrôle d'accès aux opérations d'administration de la sécurité doit gérer les rôles **« administrateur » et « super administrateur ».**

[FMT_SMR.1.2]

La fonction de contrôle d'accès aux opérations d'administration de la sécurité doit être capables d'associer des rôles aux utilisateurs **en fonction des règles suivantes :**

a. Il n'y qu'un seul super-administrateur, distinct des autres administrateurs, et qui possède tous les droits ;

b. Les administrateurs sont ceux auxquels on a explicitement attribué ce rôle.

Argumentaire : FMT_SMR.1 soutient FMT_MOF.1 et FMT_MTD.1 pour satisfaire à l'objectif de contrôle d'accès aux opérations d'administration spécifié par O.PCAOA. FMT_SMR.1 soutient également FTP_TRP.1.Admin pour satisfaire l'objectif O.PCAOA_I&A_ADMIN.

FDP_ACC.2 – Contrôle d'accès complet aux opérations d'administration de la sécurité

[FDP_ACC.2.1]

La fonction de contrôle d'accès aux opérations d'administration de la sécurité doit appliquer la **politique de contrôle d'accès aux opérations d'administration de la sécurité** à toutes les opérations **d'administration de la sécurité effectuées par l'administrateur**.

[FDP_ACC.2.2]

La fonction de contrôle d'accès aux opérations d'administration de la sécurité doit garantir que toutes les opérations **d'administration de la sécurité effectuées par l'administrateur** sont couvertes par **la politique de contrôle d'accès aux opérations d'administration de la sécurité**.

Argumentaire : FDP_ACC.2 soutient FMT_MOF.1 et FMT_MTD.1 pour satisfaire à l'objectif de contrôle d'accès aux opérations d'administration spécifié par O.PCAOA, en garantissant que la politique de contrôle d'accès aux opérations d'administration est appliquée à toutes les opérations.

FMT_MOF.1 – Administration du comportement des fonctions de sécurité

[FMT_MOF.1.1]

La fonction de contrôle d'accès aux opérations d'administration de la sécurité doit restreindre la capacité d'**activer**, de **désactiver**, d'**effectuer** ou de **modifier les fonctions de sécurité du tableau ci-dessous** aux **administrateurs, en fonction des droits ci-dessous :**

Fonctions de sécurité	*Opérations / droits nécessaires*
Fonction de filtrage	Activer / désactiver : (F ou GF) +M
Fonction de chiffrement et d'établissement des SA	Activer / désactiver : V+M
Fonction de sauvegarde	Effectuer : Ma
Fonction de restauration	Effectuer : Ma+M

Argumentaire : FMT_MOF.1 est dédié à la satisfaction de l'objectif O.PCAOA. Ce composant couvre les tâches d'administration consistant à déclencher des fonctions de sécurité.

FMT_MTD.1 – Administration des données de sécurité

[FMT_MTD.1.1]

La fonction de contrôle d'accès aux opérations d'administration de la sécurité doit restreindre la capacité de **consulter**, de **modifier** ou d'**effacer** les **données de sécurité du tableau ci-dessous** aux **administrateurs, en fonction des droits ci-dessous :**

Données de sécurité	*Opérations / droits nécessaires*
Caractéristiques des utilisateurs IPSec et des administrateurs	Consulter : tous les administrateurs Modifier : U+M
Attribution du rôle administrateur et de droits administratifs à un utilisateur	Consulter : super-administrateur Modifier : A+M
Configuration des interfaces et des routes réseaux	Consulter : tous les administrateurs Modifier interfaces : N+M Modifier routes: R+M
Objets décrivant la topologie du réseau : machines, réseaux, protocoles et services prédéfinis	Consulter : tous les administrateurs Modifier : (O ou GO) +M
Slots de filtrage : contenu	Consulter : F Modifier : F+M
Slots de filtrage global: contenu	Consulter : GF Modifier : GF+M
Slots de chiffrement : contenu	Consulter : V Modifier : V+M
Fichiers de trace des événements de sécurité	Consulter (et auditer) : L Effacer : L+M
Données de monitoring	Consulter (et auditer) : L Modifier : L+MW
Paramètres de la journalisation et de la remontée d'alarmes dont les profils des événements système.	Consulter : tous les administrateurs Modifier : *+M
Paramètres de l'analyse dynamique, dont profils des attaques Internet	Consulter : As Modifier : As+M
Sauvegarde et restauration de configuration	Sauvegarde: Ma Restauration: Ma+M
Base de temps	Consulter : tous les administrateurs Modifier : Ma+M

Argumentaire : FMT_MTD.1 est dédié à la satisfaction de l'objectif O.PCAOA. Ce composant couvre les tâches d'administration consistant à modifier les données de sécurité.

Fonction de sauvegarde et de restauration

FMT_MTD.BRS – Sauvegarde et restauration des données de sécurité

[FMT_MTD.BRS.1]

La fonction de sauvegarde / restauration doit pouvoir sauvegarder **les données de sécurité** sur **le disque dur de la station d'administration.**

[FMT_MTD.BRS.2]

La fonction de sauvegarde / restauration doit permettre de restaurer des **données de sécurité** sauvées sur **le disque dur de la station d'administration**.

Argumentaire : FMT_MTD.BRS est dédié à la satisfaction de l'objectif O.SAUVEGARDE_RESTAURATION. Le recours à ce composant explicite a été nécessaire car les composants de [CC-02] ne permettent pas de spécifier la sauvegarde ou la restauration de données de sécurité.

5.2.4 Exigences de protection de la TOE

Fonction de protection des sessions d'administration

FPT_ITT.1 – Protection élémentaire du contenu des sessions d'administration

[FPT_ITT.1.1]

La fonction de protection des sessions d'administration doit protéger **le contenu des sessions d'administration** contre la **divulgation et la modification** quand elles sont transmises entre **la station d'administration et le boîtier appliance firewall-VPN**.

Argumentaire : FPT_ITT.1 est dédié à la satisfaction de l'objectif O.PROTECT_SESSIONS_ADMIN.

FTP_TRP.1.Admin – Chemin de confiance pour l'administration à distance

[FTP_TRP.1.Admin.1]

La fonction de protection des sessions d'administration doit fournir un chemin de communication entre **les administrateurs et le boîtier appliance firewall-VPN** qui soit logiquement distinct des autres chemins de communication et qui garantisse l'identification de ses extrémités et la protection des données transférées contre une **modification ou une divulgation**.

[FTP_TRP.1.Admin.2]

La fonction de protection des sessions d'administration doit permettre **aux administrateurs** d'initier une communication via le chemin de confiance.

[FTP_TRP.1.Admin.3]

La fonction de protection des sessions d'administration doit exiger l'utilisation du chemin de confiance pour :

a. l'authentification mutuelle initiale de l'administrateur et du boîtier appliance firewall-VPN,

b. les opérations d'administration à distance de la sécurité.

Argumentaire : FTP_TRP.1.Admin est dédié à la satisfaction de l'objectif O.PCAOA_I&A_ADMIN. Il soutient d'autre part FPT_ITT.1 pour satisfaire O.PROTECT_SESSIONS_ADMIN en fournissant les moyens de protéger les sessions d'administration.

FIA_UAU.5.Admin – Mécanisme d'authentification des administrateurs

[FIA_UAU.5.Admin.1]

La fonction de protection des sessions d'administration doit fournir **le mécanisme basé sur le protocole SRP ou le protocole TLS** pour contribuer à l'authentification de **l'administrateur**.

[FIA_UAU.5.Admin.2]

La fonction de protection des sessions d'administration doit authentifier l'identité annoncée de tout **administrateur** selon **le protocole SRP ou le protocole TLS (identifiant / mot de passe ou certificat X.509)**.

*Argumentaire : FIA_UAU.5.Admin soutient FTP_TRP.1.Admin pour satisfaire l'objectif O.PCAOA_I&A_ADMIN. La résistance des mécanismes associés aux protocoles SRP et TLS permet de satisfaire l'objectif O.RESIST_AUTH_ADMIN. Pour le protocole SRP, la protection contre le rejeu et la contrefaçon des données d'authentification est garantie par l'utilisation d'un défi / réponse basé sur des clés éphémères d'entropie supérieure à 2048 bits et générées d'une manière qui empêche les attaques par référence sur les secrets d'authentification de référence (valeur « **v** » de vérification du mot de passe, cf. [SRP]). Pour le protocole TLS, la protection contre le rejeu et la contrefaçon des données d'authentification est garantie par l'utilisation exclusive de la CipherSuite* ***TLS_DHE_RSA_WITH_AES_128_CBC_SHA*** (cf. [TLS-AES])

5.2.5 Autres exigences de sécurité de soutien

Autres fonctions de soutien

FCS_COP.1 – Fonction cryptographique

[FCS_COP.1.Elaboration_clés]

La fonction cryptographique doit effectuer **l'élaboration de clés** conformément à l'algorithme cryptographique **spécifié ci-dessous** et avec les tailles des clés cryptographiques **spécifiées ci-dessous**, en conformité avec **les standards énoncés ci-dessous**.

Algorithme	*Taille des clés*	*Réf. du standard*	*Exigences soutenues*
Diffie-Hellman	2048, 3072, 4096	[DH], [IKE], [IKE-MODP], [SRP]	FIA_UAU.5.Admin, FIA_UAU.5.Corresp.

[FCS_COP.1.Signature_Chiffrement]

La fonction cryptographique doit effectuer la **signature et le chiffrement/déchiffrement asymétrique** conformément à l'algorithme cryptographique **spécifié ci-dessous** et avec les tailles des clés cryptographiques **spécifiées ci-dessous**, en conformité avec **les standards énoncés ci-dessous**.

Algorithme	*Taille des clés*	*Réf. du standard*	*Exigences soutenues*
RSA	2048, 4096	[RSA]	FIA_UAU.5.Corresp (X509)

[FCS_COP.1.Hachage]

La fonction cryptographique doit effectuer le **hachage univoque** conformément aux algorithmes cryptographiques **spécifiés ci-dessous** et avec les tailles des clés cryptographiques **spécifiées ci-dessous**, en conformité avec **les standards énoncés ci-dessous**.

Algorithmes	*Taille des clés*	*Réf. du standard*	*Exigences soutenues*
HMAC-SHA1	160	[HMAC], [SHA1]	FTP_TRP.1.Corresp, FIA_UAU.5.Corresp, FDP_UIT.1
HMAC-SHA2	256, 384, 512	[HMAC], [SHA2]	FTP_TRP.1.Corresp, FIA_UAU.5.Corresp, FDP_UIT.1
SHA2	256, 384, 512	[SHA2]	FTP_TRP.1.Corresp, FIA_UAU.5.Corresp

[FCS_COP.1.Chiffrement_VPN]

La fonction cryptographique doit effectuer le **chiffrement/déchiffrement symétrique des paquets VPN** conformément aux algorithmes cryptographiques **spécifiés ci-dessous** et avec les tailles des clés cryptographiques **spécifiées ci-dessous**, en conformité avec **les standards énoncés ci-dessous**.

Algorithmes	*Taille des clés*	*Réf. du standard*	*Exigences soutenues*
AES	128, 192, 256	[AES]	FTP_TRP.1.Corresp, FDP_UCT.1
Triple DES	168	[DES]	
Blowfish	128 à 256	[Blowfish]	
CAST	128	[CAST]	

[FCS_COP.1.Chiffrement_sessions]

La fonction cryptographique doit effectuer le **chiffrement/déchiffrement symétrique des sessions d'administration** conformément à l'algorithme cryptographique **spécifié ci-dessous** et avec les tailles des clés cryptographiques **spécifiées ci-dessous**, en conformité avec **les standards énoncés ci-dessous**.

Algorithme	*Taille des clés*	*Réf. du standard*	*Exigences soutenues*
AES	128	[AES]	FPT_ITT.1

[FCS_COP.1.Intégrité_sessions]

La fonction cryptographique doit effectuer le **contrôle d'intégrité des sessions d'administration** conformément à l'algorithme cryptographique **spécifié ci-dessous** et avec les tailles des clés cryptographiques **spécifiées ci-dessous**, en conformité avec **les standards énoncés ci-dessous**.

Algorithme	*Taille des clés*	*Réf. du standard*	*Exigences soutenues*
HMAC-SHA1	160	[HMAC], [SHA1]	FPT_ITT.1

Argumentaire : FCS_COP.1 soutient toutes les exigences spécifiées dans la colonne de droite pour la satisfaction de leurs objectifs de sécurité respectifs.

FPT_STM.1 – Base de temps fiable

[FPT_STM.1.1]

L'horloge interne du boîtier appliance firewall-VPN doit être capable de fournir un horodatage fiable pour son propre usage.

Argumentaire : ce composant soutient FAU_GEN.1, pour la satisfaction des objectifs O.JAA_PCFI, O.JAA_IPS, O.JAA_PCAOA.

5.3 Exigences d'assurance sécurité pour la TOE

Cette section présente le paquet d'exigences d'assurance choisi. Le chapitre 9.2 présente les opérations sur ces exigences.

Le niveau d'assurance visé par la TOE est le niveau EAL3 augmenté des composants ALC_FLR.3, AVA_VAN.3, ALC_CMC.4 et ALC_CMS.4 associé à une expertise de l'implémentation de la cryptographie décrite dans [QUALIF-STD].

Le tableau ci-dessous détail la couverture des dépendances des exigences d'assurance.

Composants		Commentaires
ADV_ARC.1	Security architecture description	EAL3
ADV_FSP.3	Functional specification with complete summary	EAL3
ADV_TDS.2	Architectural design	EAL3
AGD_OPE.1	Operational user guidance	EAL3
AGD_PRE.1	Preparative procedures	EAL3
ALC_CMC.4	Production support, acceptance procedures and automation	+
ALC_CMS.4	Problem tracking CM coverage	+
ALC_DEL.1	Delivery procedures	EAL3
ALC_DVS.1	Identification of security measures	EAL3
ALC_FLR.3	Systematic flaw remediation	+
ALC_LCD.1	Developer defined life-cycle model	EAL3
ASE_CCL.1	Conformance claims	EAL3
ASE_ECD.1	Extended components definition	EAL3
ASE_INT.1	ST introduction	EAL3
ASE_OBJ.2	Security objectives	EAL3
ASE_REQ.2	Security requirements	EAL3
ASE_SPD.1	Security problem definition	EAL3
ASE_TSS.1	TOE summary specification	EAL3
ATE_COV.2	Analysis of coverage	EAL3
ATE_DPT.1	Testing: basic design	EAL3
ATE_FUN.1	Functional testing	EAL3
ATE_IND.2	Independent testing - sample	EAL3
AVA_VAN.3	Focused vulnerability analysis	+

5.4 Argumentaire des exigences de sécurité

5.4.1 Satisfaction des objectifs de sécurité

La satisfaction des objectifs de sécurité est exprimée dans les rubriques « argumentaires » qui accompagnent l'énoncé de chaque exigence de sécurité. Le lien entre les exigences et les objectifs de sécurité est résumé ci-dessous.

« S »: L'exigence soutient l'objectif, « X »: L'exigence réalise l'objectif

	O.PCFI_FILTRAGE	O.PCFI_CONTEXTE_APPLICATIF	O.PCFI_CHIFFREMENT	O.JAA_PCFI	O.IPS_DETECTION_ATTAQUES	O.IPS_CONFORMITE_RFC	O.JAA_IPS	O.PCAOA	O.PCAOA_I&A_ADMIN	O.JAA_PCAOA	O.SAUVEGARDE_RESTAURATION	O.RESIST_AUTH_ADMIN	O.PROTECT_JOURN	O.PROTECT_SESSIONS_ADMIN
FDP_IFC.2	S													
FDP_IFF.1.Filtrage	X	X												
FDP_IFC.1			S											
FDP_UCT.1			X											
FDP_UIT.1			X											
FDP_IFF.1.Chiffrement			S											
FTP_TRP.1.Corresp			X											
FIA_UAU.5.Corresp			S											
FPT_TDC.1			S											
FAU_GEN.1				X			X			X				
FAU_GEN.2										X				
FAU_SAR.1				X			X			X				
FAU_STG.3													X	
FAU_ARP.1.Alarmes				X			X			X				
FAU_SAA.4					X	X								
FAU_ARP.1.IPS					S	S	X							
FMT_SMF.1								S		S	S			S
FMT_SMR.1								S	S					
FDP_ACC.2								S						
FMT_MOF.1								X						
FMT_MTD.1								X						
FMT_MTD.BRS											X			
FPT_ITT.1														X
FTP_TRP.1.Admin									X					S
FIA_UAU.5.Admin									S			X		
FCS_COP.1.Elaboration_clés			X						X			S		S
FCS_COP.1.Signature_Chiffrement			X						X			X		S
FCS_COP.1.Hachage			X											
FCS_COP.1.Chiffrement_VPN			X											
FCS_COP.1.Chiffrement_sessions									X					X
FCS_COP.1.Intégrité_sessions									X			S		X

FPT_STM.1				S			S			S					

5.4.2 Soutien mutuel et non contradiction

Toutes les dépendances sont satisfaites ou bien leur non-satisfaction a été justifiée. Les exigences de sécurité forment donc un ensemble qui se soutient mutuellement et ne présente pas de contradiction.

5.4.3 Satisfaction des dépendances des SFRs

Le tableau ci-dessous résume les dépendances des composants d'exigences de sécurité et justifie en quoi elles sont satisfaites ou bien pourquoi elles ne le sont pas.

Composant	*Dépendances*	*Satisfaction*
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1.Filtrage
FDP_IFF.1.Filtrage	FDP_IFC.1	FDP_IFC.2
	FMT_MSA.3	Les attributs de sécurité des paquets IP sont déduits du contenu des en-têtes IP et transport. Dans ces conditions, la notion de « valeur restrictive des attributs » n'est pas claire et de toute manière ces attributs ne sont pas sous le contrôle de la TSF. La dépendance n'est donc pas applicable.
FPT_STM.1	Aucune	
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1.Chiffrement
FDP_UCT.1	FTP_ITC.1 | FTP_TRP.1	FTP_TRP.1.Corresp
	FDP_ACC.1 | FDP_IFC.1	FDP_IFC.1
FDP_UIT.1	FTP_ITC.1 | FTP_TRP.1	FTP_TRP.1.Corresp
	FDP_ACC.1 | FDP_IFC.1	FDP_IFC.1
FDP_IFF.1.Chiffrement	FDP_IFC.1	FDP_IFC.1
	FMT_MSA.3	Les attributs de sécurité des paquets IP sont déduits du contenu des en-têtes IP et transport. Dans ces conditions, la notion de « valeur restrictive des attributs » n'est pas claire et de toute manière ces attributs ne sont pas sous le contrôle de la TSF. La dépendance n'est donc pas applicable.
FTP_TRP.1.Corresp	Aucune	
FIA_UAU.5.Corresp	Aucune	
FPT_TDC.1	Aucune	
FAU_GEN.1	FPT_STM.1	Oui.
FAU_GEN.2	FAU_GEN.1	Oui.
	FIA_UID.1	Il n'est pas possible pour l'administrateur d'effectuer une quelconque opération d'administration sans être authentifié. La fonction d'authentification est donc la seule opération possible lors d'une connexion sur le serveur d'administration. La dépendance n'est donc pas applicable.
FAU_SAR.1	FAU_GEN.1	Oui.
FAU_STG.3	FAU_STG.1	La suppression ou la modification des journaux d'audit n'est réalisable qu'avec le compte « admin » et uniquement en console locale. Il n'y a de fonction d'administration pour effectuer ces opérations. La dépendance n'est donc pas applicable.
FAU_ARP.1.Alarmes	FAU_SAA.1	FAU_SAA.4
FAU_SAA.4	Aucune	
FAU_ARP.1.IPS	FAU_SAA.1	FAU_SAA.4
FMT_SMR.1	FIA_UID.1	Il n'est pas possible pour l'administrateur d'effectuer une quelconque opération d'administration sans être authentifié. La fonction d'authentification est donc la seule opération possible lors d'une connexion sur le serveur d'administration. La dépendance n'est donc pas applicable.
FDP_ACC.2	FDP_ACF.1	Tous les accès aux opérations d'administration sont contrôlés

Composant	*Dépendances*	*Satisfaction*
		par un ensemble de droits d'administration. Ces droits sont regroupés par catégorie fonctionnelle. Il n'est ainsi pas possible d'autoriser ou refuser l'accès à un élément particulier d'une catégorie fonctionnelle. La dépendance n'est donc pas applicable.
FMT_MOF.1	FMT_SMR.1	Oui
	FMT_SMF.1	Oui
FMT_MTD.1	FMT_SMR.1	Oui
	FMT_SMF.1	Oui
FMT_SMF.1	Aucune	
FMT_MTD.BRS	FMT_MTD.1	Oui
	FMT_SMF.1	Oui
FPT_ITT.1	Aucune	
FTP_TRP.1.Admin	Aucune	
FIA_UAU.5.Admin	Aucune	
FCS_COP.1.Elaboration_clés	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Non applicable : l'opération est une méthode de génération de clé.
	FCS_CKM.4	Non applicable : les clés ne sont pas accessibles physiquement ou logiquement aux attaquants. Il n'est donc pas nécessaire de les effacer d'une manière particulière.
FCS_COP.1.Signature_Chiffrement	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Non applicable car en dehors de la portée de la TOE. Les certificats sont téléchargés sur le boîtier appliance firewall-VPN par l'administrateur.
	FCS_CKM.4	Non applicable car en dehors de la portée de la TOE
FCS_COP.1.Hachage	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Satisfaite par FCS_COP.1.Elaborations_clés | FCS_COP.1.Signature_Chiffrement. Lorsqu'elles sont requises les clés sont générées ou échangées sans être accessibles physiquement ou logiquement aux attaquants
	FCS_CKM.4	Non applicable : les clés ne sont pas accessibles physiquement ou logiquement aux attaquants. Il n'est donc pas nécessaire de les effacer d'une manière particulière.
FCS_COP.1.Chiffrement_VPN	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Satisfaite par FCS_COP.1.Elaborations_clés | FCS_COP.1.Signature_Chiffrement. Lorsqu'elles sont requises les clés sont générées ou échangées sans être accessibles physiquement ou logiquement aux attaquants
	FCS_CKM.4	Non applicable : les clés ne sont pas accessibles physiquement ou logiquement aux attaquants. Il n'est donc pas nécessaire de les effacer d'une manière particulière.
FCS_COP.1.Chiffrement_sessions	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Satisfaite par FCS_COP.1.Elaborations_clés | FCS_COP.1.Signature_Chiffrement. Lorsqu'elles sont requises les clés sont générées ou échangées sans être accessibles physiquement ou logiquement aux attaquants
	FCS_CKM.4	Non applicable : les clés ne sont pas accessibles physiquement ou logiquement aux attaquants. Il n'est donc pas nécessaire de les effacer d'une manière particulière.
FCS_COP.1.Intégrité_sessions	FDP_ITC.1 | FDP_ITC.2 | FCS_CKM.1	Satisfaite par FCS_COP.1.Elaborations_clés | FCS_COP.1.Signature_Chiffrement. Lorsqu'elles sont requises les clés sont générées ou échangées sans être accessibles physiquement ou logiquement aux attaquants
	FCS_CKM.4	Non applicable : les clés ne sont pas accessibles physiquement ou logiquement aux attaquants. Il n'est donc pas nécessaire de les effacer d'une manière particulière.

5.4.4 Satisfaction des dépendances des SARs

Le niveau d'assurance de l'évaluation visé par cette cible de sécurité est une qualification standard augmenté des composants ALC_CMS.4 et ALC_CMC.4.

La dépendance de AVA_VAN.3 avec les composants ADV_FSP.4, ADV_IMP.1 et ADV_TDS.3 n'est pas satisfaite par construction du paquet d'assurance de la QS, or le présent paquet d'assurance a été construit pour couvrir au minimum tous les composants d'assurance de la QS, donc toutes les dépendances non satisfaites du paquet d'assurance de la QS sont reprises telles quelles.

Seules les éventuelles dépendances non satisfaites des augmentations réalisées par rapport au paquet d'assurance de la QS sont justifiées (Cf. CC part 3 V3.1r3 page 225 de 232)

- ALC_CMS.4 : Il n'y a pas de pas de dépendances.
- ALC_CMC.4 : Les dépendances sont satisfaites par les composants ALC_CMS.1, ALC_LCD.1 et ALC_DVS.1 inclus dans le paquet d'assurance de la QS.

6 SPÉCIFICATIONS ABRÉGÉES DE LA TOE

Le but de cette section est de fournir une définition de haut niveau des fonctions de sécurité des TI qui sont censées satisfaire aux exigences fonctionnelles de sécurité, et des mesures d'assurance sécurité prises pour satisfaire aux exigences d'assurance sécurité.

6.1 Fonctions de sécurité des TI

La présentation des fonctions de sécurité des TI reprend le plan suivi pour la description des exigences fonctionnelles de sécurité de la TOE.

6.1.1 Fonction de filtrage

La technologie ASQ inclut un moteur de filtrage dynamique des paquets (*stateful inspection*) avec optimisation des règles permettant l'application de la politique de filtrage de manière sûre et rapide. La mise en œuvre de la fonction de filtrage est basée sur la confrontation des attributs de chaque paquet IP reçu aux critères de chaque règle du slot de filtrage actif. Le filtrage porte sur tous les paquets sans exception. Les critères des règles de filtrage sont :

- L'interface de réception ou de destination des paquets IP couverts par la règle ;
- La ou les machines à l'origine des flux d'information couverts par la règle ;
- Le ou les protocoles IP, le champ DSCP, les services TCP/UDP ou les types de messages ICMP des flux d'information couverts par la règle ;
- La ou les machines destinataires des flux d'information couverts par la règle ;

Les attributs des paquets IP qui sont confrontés aux quatre premiers critères cités sont évidemment extraits des en-têtes Ethernet, IP, ICMP, UDP ou TCP des trames.

Chaque règle de filtrage peut spécifier une action de contrôle et une action de journalisation. Cette dernière est décrite au §6.1.4 Il y a cinq valeurs possibles pour l'action de contrôle :

'passer' : le paquet est accepté et n'est pas confronté aux règles suivantes ;

'bloquer' : le paquet est détruit sans que l'émetteur ne le sache et n'est pas confronté aux règles suivantes de la politique de filtrage ;

'réinitialiser' : le paquet est détruit et un signal TCP RST (cas TCP) ou ICMP unreachable (cas UDP) est envoyé à l'émetteur ;

'aucune' : le paquet est confronté aux règles suivantes (sert à spécifier une action de journalisation uniquement).

'déléguer: le paquet est confronté aux règles de filtrage du slot local (sert à sortir de l'évaluation de la politique de filtrage global pour permettre de déléguer un sous-ensemble de celle-ci à un administrateur local via la slot de filtrage local). Cette action n'est disponible que pour les régles du slot global.

Si aucune règle de filtrage n'est applicable au paquet, ou si les seules qui le sont ne spécifient 'aucune' action de contrôle, le paquet est détruit sans que l'émetteur ne le sache et n'est pas confronté aux règles suivantes de la politique de filtrage.

Il convient de noter qu'à proprement parler, pour un ensemble de paquets IP liés à un même échange au niveau transport (connexion TCP, pseudo-connexion UDP ou ICMP), le boîtier appliance firewall-VPN ne confronte que le paquet initial de l'échange aux règles du slot de filtrage courant. À la réception de tout paquet IP, préalablement à l'application des règles du slot de filtrage courant, le paquet est comparé aux connexions / pseudo-connexions actuellement établies. Si les attributs et les paramètres du paquet correspondent aux critères et à l'état d'une de ces connexions / pseudo-connexions, il est autorisé à passer sans être soumis aux règles de filtrage. Ce mécanisme permet notamment de gérer les échanges bidirectionnels (notamment les connexions TCP) sans avoir à définir une règle de filtrage dans les deux sens de traversée du firewall.

Des règles de filtrage implicites sont générées par le firewall en liaison avec la configuration d'autres fonctions de sécurité. Ce sont les règles correspondant à : l'administration à distance du firewall et l'établissement des VPN. Par ailleurs, des règles de filtrage dynamiques sont également générées pour les protocoles nécessitant des connexions filles.

La politique de filtrage est le résultat de concaténation des règles implicites, des règles de filtrage contenues dans la politique de filtrage globale (s'il y en a une) puis des règles de filtrage contenues dans la politique de filtrage locale.

A noter qu'à tout instant du fonctionnement du boîtier appliance firewall-VPN, il y a une politique de filtrage active.

Argumentaire : la fonction de filtrage satisfait FDP_IFC.2 et FDP_IFF.1.Filtrage.

6.1.2 Fonction de chiffrement

La fonction de chiffrement du boîtier appliance firewall-VPN implémente le protocole ESP d'IPSec [IPSec, ESP] pour fournir des services d'authentification et de chiffrement des datagrammes échangés avec un correspondant VPN (éventuellement un autre boîtier appliance firewall-VPN), possédant des fonctionnalités homologues.

Les algorithmes d'authentification supportés par le boîtier appliance firewall-VPN sont : HMAC-SHA1 (160 bits) et HMAC-SHA2 (256, 384, 512 bits).

Les algorithmes de chiffrement supportés par le boîtier appliance firewall-VPN sont : AES (128, 192 ou 256 bits), Triple-DES (168 bits), Blowfish (128 à 256 bits) et CAST (128 bits).

Le boîtier appliance firewall-VPN met en œuvre le protocole ESP en mode tunnel. Cela implique que la fonction de chiffrement peut ne pas être mise en œuvre sur le flux de bout en bout, mais uniquement sur une portion du réseau qui supporte le flux, physiquement délimitée par les correspondants VPN, typiquement le réseau non maîtrisé. Sur cette portion, les datagrammes IP à protéger sont intégralement chiffrés, signés et encapsulés dans des datagrammes ESP dont les adresses IP source et destination sont celles des correspondants VPN. Ainsi, les adresses IP des machines réelles d'extrémité du flux sont inaccessibles à des attaquants à l'écoute sur le réseau non maîtrisé. Les correspondants VPN sont appelés extrémités du tunnel, par opposition aux machines réelles d'extrémité du flux, situées « derrière » les correspondants VPN du point de vue du réseau non maîtrisé, et qu'on appelle les extrémités du trafic.

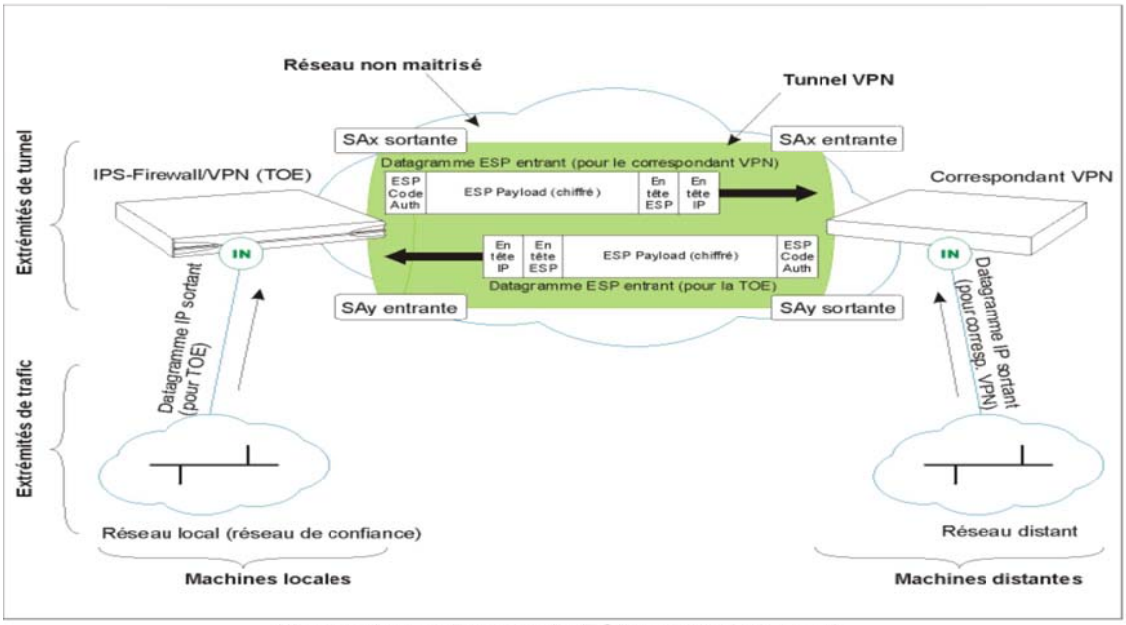


Illustration 5: Protocole ESP en mode tunnels.

Dans le cadre d'ESP, chaque datagramme échangé entre deux correspondants VPN donnés est rattaché à une connexion unidirectionnelle mettant en œuvre des services de sécurité, appelée Association de Sécurité (*Security Association* ou *SA*). Chaque datagramme ESP possède un index de sécurité (*Security Policy Identifier* ou *SPI*) qui identifie la SA IPSec à laquelle il est rattaché.

Une SA IPSec spécifie les algorithmes de chiffrement et d'authentification à appliquer sur les datagrammes qu'elle couvre, ainsi que les clés secrètes associées. Du point de vue d'un correspondant VPN, une SA IPSec peut être entrante ou sortante.

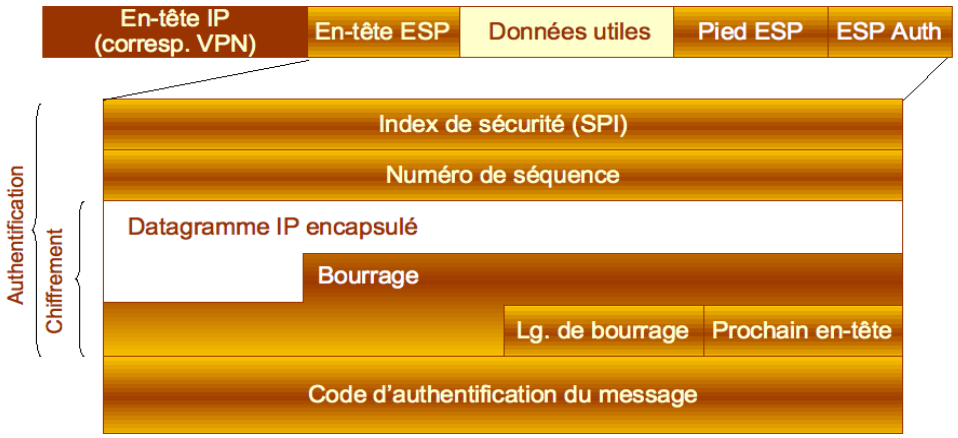


Illustration 6: Contenu d'un datagramme ESP.

Pour un échange bidirectionnel donné (par ex : une connexion TCP), les correspondants VPN établissent une paire de SA IPSec (une pour chaque direction), chaque SA IPSec étant sortante pour un correspondant et entrante pour l'autre. L'établissement des paires de SA IPSec fait l'objet d'un ensemble fonctionnel de sécurité spécifique (cf. IKE phase2 : établissement de SA IPSEC au §).

Une SA IPSec possède une durée de vie au-delà de laquelle elle expire et doit être re-négociée. Le correspondant VPN peut également provoquer la re-négociation de la SA IPSec en application d'autres critères (ex : volume de données échangées).

À un moment donné, le boîtier appliance firewall-VPN peut gérer une multitude de paires de SA IPSec. Il est relativement facile de trouver la SA IPSec entrante associée à un datagramme ESP entrant (grâce à l'index de sécurité), mais pour chaque datagramme IP sortant, la sélection de la SA IPSec sortante nécessite la confrontation des attributs du datagramme aux critères de chaque règle du slot de chiffrement actif. Les critères des règles de chiffrement[5] sont :

- La ou les machines à l'origine des flux d'information couverts par la règle ;
- Le ou les protocoles IP ;
- La ou les machines destinataires des flux d'information couverts par la règle.

À la différence de la fonction de chiffrement, si le datagramme IP sortant ne correspond à aucune règle, il continue son chemin dans la pile. Il est alors soumis en clair à la fonction de filtrage. Autre différence : à un moment donné, il peut n'y avoir aucun slot de chiffrement actif.

Chaque règle de chiffrement est normalement associée à une paire de SA IPSec. Si le datagramme IP sortant correspond à une règle de chiffrement possédant une SA IPSec sortante valide, les traitements de cette SA IPSec sont appliqués au datagramme. Sinon, la SA IPSec sortante est négociée (ou re-négociée). Si la négociation échoue, le paquet est détruit.

L'authenticité des datagrammes ESP entrants est contrôlée, puis ils sont déchiffrés. Une fois désencapsulés, on contrôle également que les attributs du paquet IP obtenu sont bien conformes aux critères de la règle de chiffrement associée à la SA IPSec.

Il convient de noter que l'on a parlé de « datagrammes » IP ou ESP dans toute cette section. En effet, en cas de fragmentation, les paquets IP sortants ou ESP entrants sont ré-assemblés avant l'application de la fonction de chiffrement.

Note d'application : les algorithmes DES (56 bits) et HMAC-MD5 (128 bits) sont également supportés mais sont exclus du mode d'utilisation soumis à l'évaluation. De même, les algorithmes CAST et Blowfish peuvent être paramétrés avec des tailles de clés inférieures à 128 bits, mais cela sort du mode d'utilisation soumis à l'évaluation.

Argumentaire : la fonction de chiffrement satisfait FDP_IFC.1, FDP_UCT.1, FDP_UIT.1 et FDP_IFF.1.Chiffrement.

L'utilisation des algorithmes HMAC-SHA1 et HMAC-SHA2 pour les services de confidentialité de la SA IPSec satisfait la partie de FCS_COP.1.Hachage qui soutient FDP_UIT.1.

L'utilisation des algorithmes AES, Triple DES, Blowfish et CAST pour les services de confidentialité de la SA IPSec satisfait la partie de FCS_COP.1.Chiffrement_VPN qui soutient FDP_UCT.1.

6.1.3 Fonction d'établissement des SA

IKE phase 2 : établissement de SA IPSec

L'établissement d'une SA IPSec entre deux correspondants VPN nécessite une phase de négociation des paramètres et d'établissement des clés afin d'assurer que les deux extrémités du tunnel appliquent la règle de chiffrement associée à la SA IPSec de manière cohérente. La négociation des SA IPSec est basée sur la phase 2 ('Quick Mode') du protocole IKE [IKE].

5 On peut dire que les règles de chiffrement correspondent aux *Security Policy Database entries* de la RFC 2401 [IPSec], à ceci près que la SPD, telle qu'elle est définie dans la RFC, couvre en toute rigueur les règles de chiffrement et de filtrage.

Les algorithmes d'authentification négociables sont le SHA1 (160 bits) et le SHA2 (256, 384 et 512 bits). L'algorithme de secret partagé négociable est Diffie-Hellman avec les groupes 14 – MODP 2048 bits, 15 – MODP 3072 bits, 16 – MODP 4096 bits [IKE-MODP]. Les algorithmes de chiffrement négociables sont l'AES (128, 192 ou 256 bits), le Triple DES (168 bits), Blowfish (128 à 256 bits) et CAST (128 bits).

En tant que répondeur, le boîtier appliance firewall-VPN sélectionne une réponse au moins aussi stricte que ses propositions locales.

Note d'application : d'autres stratégies peuvent être paramétrées par l'administrateur, mais elles sont exclues du mode d'utilisation soumis à l'évaluation.

Argumentaire : les messages de proposition-réponse satisfont à FPT_TDC.1 concernant les SA IPSec. La SA ISAKMP constitue un chemin de confiance (cf. IKE phase1 : établissement de SA ISAKMP et authentification mutuelle au §Fonction d'établissement des SA) dont l'utilisation, à travers la phase 2 d'IKE, pour la négociation des SA IPsec satisfait FTP_TRP.1.Corresp.3.b.

L'utilisation de l'algorithme Diffie-Hellman satisfait FCS_COP.1.Elaboration_clés concernant la partie de cette exigence qui soutient FIA_UAU.5.Corresp.

Les algorithmes SHA1 et SHA2 sont utilisés, conformément à la RFC 2409, pour générer les clés secrètes de la SA IPSec et les codes d'authentification, ce qui satisfait la partie de FCS_COP.1.Hachage qui soutient FTP_TRP.1.Corresp. Cet algorithme est également utilisé pour les services d'intégrité de la SA ISAKMP (cf. §Fonction d'établissement des SA), ce qui satisfait la partie de FCS_COP.1.Hachage qui soutient FTP_TRP.1.Corresp.1.

Les algorithmes AES, Triple DES, Blowfish et CAST sont utilisés pour les services de confidentialité de la SA ISAKMP (cf. §Fonction d'établissement des SA), ce qui satisfait la partie de FCS_COP.1.Chiffrement_VPN qui soutient FTP_TRP.1.Corresp.1.

IKE phase 1 : établissement de SA ISAKMP et authentification mutuelle

L'établissement d'une SA ISAKMP entre deux correspondants VPN nécessite une authentification mutuelle des correspondants VPN. Celle-ci est suivie d'une phase de négociation des paramètres et d'établissement des clés secrètes d'authentification, de chiffrement et de dérivation de la SA ISAKMP afin d'assurer que les deux extrémités du tunnel appliquent la règle de protection de la communication de manière cohérente.

L'extension Xauth du protocole « Mode Config » [IKE-MCFG] qui est décrite dans [IKE-XAUTH] permet une authentification du « client » IPSec après la phase 1. Les échanges Xauth sont par conséquent protégés par la SA ISAKMP qui a été établie. Le niveau de sécurité du mode XAuth repose donc essentiellement sur celui de la phase 1.

L'extension HybridAuth [ISAKMP-HAUTH] permet une authentification asymétrique des correspondants lors de la phase 1 IPSec. Il est ainsi possible d'avoir un correspondant qui prouve son identité via un certificat X.509, et un autre correspondant IPSec qui prouve son identité à l'aide d'un secret pré-partagé, voire qui ne la prouve pas du tout lors de la phase 1. L'intérêt principal de cette extension réside dans son utilisation en corrélation avec XAuth.

La négociation des SA ISAKMP peut être réalisée selon le mode « principal » telle que définie sur la phase 1 du protocole IKE [IKE].

L'authentification mutuelle peut être réalisée en utilisant soit :

- des clés pré-partagées ;
- des certificats X.509 telle que définie sur la phase 1 du protocole IKE [IKE] ;
- identifiant / mot de passe pour l'émetteur et certificat X.509 pour le correspondant tel que

défini dans la méthode HybridAuth+XAuth.

Le tableau ci-dessous précise la nature de l'identifiant et les protections appliquées à l'identité, en fonction du mode et de la méthode d'authentification :

Méthode *Mode*	*clé pré-partagée*	*certificat X509*	*HybridAuth+XAuth*
Principal	Identifiant : adresse IP Protection de l'identité : chiffrement de la SA ISAKMP.	Identifiant : certificat X509 Protection de l'identité : clé publique du vis-à-vis.	Identifiant : login de l'utilisateur Protection de l'identité : clé publique du vis-à-vis.

Note d'application : les algorithmes RSA et Diffie-Hellman avec des clés strictement inférieures à 2048 bits ainsi que la négociation de SA ISAKMP en mode « agressif » sont également supportés mais exclus du mode d'utilisation soumis à l'évaluation.

Argumentaire : le chemin de confiance spécifié par le composant FTP_TRP.1.Corresp est implémenté par la phase 1 d'IKE, ce qui satisfait l'élément FTP_TRP.1.Corresp.2. L'authentification mutuelle, qui garantit l'identification des extrémités (élément FTP_TRP.1.Corresp.1), est établie à la fin de la dernière passe de chaque mode. Les services assurant la confidentialité et l'intégrité (élément FTP_TRP.1.Corresp.1) sont effectifs à partir du cinquième message en mode principal. L'utilisation du chemin de confiance pour l'authentification mutuelle initiale des correspondants VPN satisfait FTP_TRP.1.Corresp.3.a.

Les deux mécanismes d'authentification sont ceux spécifiés par FIA_UAU.5.Corresp.

Les messages de proposition-réponse satisfont à FPT_TDC.1 concernant les SA ISAKMP.

L'utilisation de l'algorithme Diffie-Hellman satisfait FCS_COP.1.Elaboration_clés concernant la partie de cette exigence qui soutient FIA_UAU.5.Corresp.

En mode X509, l'utilisation de l'algorithme RSA satisfait FCS_COP.1.Signature_Chiffrement.

Les algorithmes SHA1 et SHA2 sont utilisés, conformément à la RFC 2409, pour générer les clés secrètes et les codes d'authentification, ce qui satisfait la partie de FCS_COP.1.Hachage qui soutient FIA_UAU.5.Corresp. Cet algorithme est également utilisé pour les services d'intégrité de la SA ISAKMP, ce qui satisfait la partie de FCS_COP.1.Hachage qui soutient FTP_TRP.1.Corresp.1.

Les algorithmes AES, Triple DES, Blowfish et CAST sont utilisés pour les services de confidentialité de la SA ISAKMP, ce qui satisfait la partie de FCS_COP.1.Chiffrement_VPN qui soutient FTP_TRP.1.Corresp.1.

6.1.4 Fonction de journalisation, d'audit et d'alarme

Fonction de journalisation

Le boîtier appliance firewall-VPN selon les modèles peut ou non stocker localement les événements d'audit, en particulier les modèles de la famille de build S (U30, U70) ne dispose que de la possibilité de les émettre via Syslog. Dans le cas où le stockage local est possible, le boîtier appliance firewall-VPN gère un certain nombre de fichiers de trace destinés à recueillir les événements détectés par la fonction de journalisation. Les fichiers concernés par les événements de sécurité sont :

Filtre : événements liés à l'application de la fonction de filtrage ;

VPN : événements liés à l'établissement des SA ;

Alarmes : événements liés à l'application de la fonction de prévention des intrusions ;

Histo Manager : événements liés à l'authentification des administrateurs et aux opérations d'administration de la sécurité ;

Système : arrêt/démarrage de la fonction de journalisation. Plus généralement : c'est dans ce journal que sont enregistrés les événements liés directement au système : arrêt/démarrage du boîtier appliance firewall-VPN, erreur système, etc. L'arrêt et démarrage de la fonction de journalisation correspondent à l'arrêt et au démarrage des « démons » qui génèrent les traces.

Tous les fichiers de trace partagent un espace global de stockage. L'administrateur possédant les droits '*+M' peut spécifier le pourcentage maximum que chacun des fichiers de trace peut occuper dans cet espace total. Lorsque le seuil maximum est atteint, le boîtier appliance firewall-VPN entreprend une action paramétrée, pour chaque fichier, parmi les trois suivantes :

Assurer la rotation des fichiers : les traces les plus récentes effacent les traces les plus anciennes,

Stopper l'écriture des fichiers : les traces ne sont plus mémorisées sur le Firewall,

Arrêter le Firewall : le Firewall ne s'arrête pas réellement mais il bloque l'ensemble des flux excepté les connexions du Web Manager depuis le réseau interne.

Argumentaire : la fonction de journalisation satisfait FAU_GEN.1 et FAU_GEN.2. La justification détaillée de la satisfaction de chaque exigence sur les informations d'audit enregistrées dans chaque type d'enregistrement sera apportée lors de l'évaluation. La limitation de la taille des fichiers de trace et les actions associées, satisfont à l'exigence FAU_STG.3 pour ces fichiers.

Fonction d'audit

La fonction d'audit du Firewall Reporter permet à l'auditeur d'afficher les événements stockés dans chacun des fichiers de trace en effectuant :

Des sélections selon des périodes prédéfinies par rapport à la date courante ('aujourd'hui', 'cette semaine', etc.) ou définies manuellement ;

Des tris (croissants/décroissants) sur la valeur de chacun des champs des événements de sécurité enregistrés ;

Des regroupements hiérarchiques en fonction de la valeur d'un ou plusieurs champs des événements de sécurité enregistrés.

Le Firewall Monitor permet également de visualiser les événements les plus récents.

Argumentaire : la fonction d'audit satisfait FMT_SMF.1.c, FAU_SAR.1.

Fonction d'alarme

La fonction d'alarme permet, suite à l'enregistrement d'un événement de sécurité possédant un niveau d'alarme, d'afficher l'alarme sur le Firewall Monitor.

Argumentaire : la fonction d'alarme satisfont FAU_ARP.1.Alarmes.

6.1.5 Fonction de prévention des intrusions

La technologie ASQ inclut un système de prévention des intrusions (*intrusion prevention system* ou *IPS*) permettant la détection des attaques :

sans contexte, c'est-à-dire n'utilisant qu'un paquet IP ;

avec contexte de connexion, c'est-à-dire impliquant d'analyser plusieurs paquets associés à une même connexion TCP / pseudo-connexion UDP ou ICMP ;

ou avec contexte global, c'est à dire nécessitant de recouper les contextes de plusieurs connexions TCP / pseudo-connexions UDP ou ICMP.

Une technologie à base de *plugins* permet d'effectuer des contrôles au niveau applicatif dans le but de mettre en œuvre la conformité aux RFC, le respect des bonnes pratiques et la prévention contre des attaques connues sur les serveurs applicatifs.

Le détail des attaques potentielles détectées est fourni à l'annexe B, §8 Pour chacune de ces attaques, l'administrateur possédant les droits 'As+M' peut définir si les paquets incriminés doivent être transmis ou détruits et s'il y a lieu de générer un événement de sécurité possédant un niveau d'alarme, automatiquement enregistré dans le fichier de trace 'Alarmes'.

Argumentaire : le système de prévention des intrusions satisfait aux exigences de FAU_SAA.4. L'annexe B, §8 rattache chaque attaque potentielle aux six types énoncés dans FAU_SAA.4.1. L'indication d'une attaque potentielle (FAU_SAA.4.3) peut se traduire par une action sur le paquet incriminé (ce qui satisfait FAU_ARP.IPS.1.a) et/ou la génération d'une alarme (ce qui satisfait FAU_ARP.IPS.1.b).

6.1.6 Fonction de contrôle d'accès aux opérations d'administration

Afin d'autoriser l'accès du boîtier appliance firewall-VPN à différentes personnes, le super-administrateur peut affecter des droits de modification ou de consultation de la configuration aux utilisateurs définis dans la base locale, ce qui en fait alors des administrateurs.

L'ensemble des droits d'administration figure à l'annexe A §7

Le droit particulier BASE (B) tient lieu de rôle administrateur explicite. Un utilisateur qui ne possède pas le droit 'B' n'est pas considéré comme un administrateur et ne peut pas ouvrir de session d'administration.

Le droit de modification MODIFY (M) complète tous les autres droits attribués à un administrateur pour lui permettre la consultation et la modification des données de sécurité.

Il existe un second droit de modification de données mais réservées au Monitoring (MW). Ce droit permet aux administrateurs via le moniteur temps réel d'effectuer des opérations sans pour autant interférer avec un administrateur possédant le droit M et connecté sur le boîtier appliance firewall-VPN au même instant.

Pour chaque opération élémentaire d'administration de la sécurité, les droits nécessaires sont définis de manière détaillée (les détails seront fournis lors de l'examen de la conception de haut niveau). Toutes les opérations d'administration de la sécurité effectuées par les administrateurs sont donc couvertes par la politique de contrôle d'accès que ces droits implémentent.

Le compte dont le login est 'admin' est toujours défini par défaut et n'est pas géré dans la base locale. On l'appelle le « super-administrateur ». Il possède tous les droits plus un droit spécial ADMIN (A), et il est le seul à pouvoir effectuer certaines opérations (créer un utilisateur et lui attribuer des droits administratifs, effectuer une restauration de la configuration, etc.)

Note d'application : On rappelle que dans le mode d'utilisation qui fait l'objet de l'évaluation, le super-administrateur n'est pas censé se connecter sur le boîtier appliance firewall-VPN lors des phases d'exploitation hormis la promotion d'un utilisateur en administrateur.

Argumentaire : le système de droits décrit ci-dessus satisfait aux exigences de FMT_SMF.1.a, FMT_MTD.1 et FMT_MOF.1. Le fait que toutes les opérations d'administration de la sécurité soient soumises aux contrôle d'accès satisfait FDP_ACC.2. La définition donnée ci-dessus des administrateurs et du super-administrateur satisfait FMT_SMR.1.1. L'association du compte 'admin' au super-administrateur satisfait FMT_SMR.1.2.a. La nécessité d'attribuer le droit 'B' explicitement aux administrateurs satisfait FMT_SMR.1.2.b.

6.1.7 Fonction de sauvegarde et de restauration

L'administrateur possédant le droit 'Ma' peut sauvegarder dans un fichier sur la station d'administration soit la configuration complète soit un sous-ensemble de celle-ci.

Les sous-ensembles peuvent par exemple être :

- La configuration réseau du boîtier appliance firewall-VPN (adresses du Firewall, routeurs,...) ;
- Les objets (machines, réseaux, services et chacun des groupes) ;
- Les règles de filtrage ;
- La base LDAP (base locale des utilisateurs).

La restauration de la configuration à partir d'un fichier de sauvegarde demande de disposer des droits de modification (M) en plus des droits de maintenance (Ma).

Le fichier de sauvegarde peut également être sécurisé par chiffrement. Dans ce cas la restauration de la sauvegarde nécessitera la restitution de la clé de chiffrement.

Argumentaire : la fonction de sauvegarde et de restauration satisfait FMT_SMF.1.d et FMT_MTD.BRS.

6.1.8 Fonction de protection des sessions d'administration

Chiffrement et authentification des sessions d'administration

Les sessions établies entre les outils de la suite d'administration (Web Manager, Real-Time Monitor, Event Reporter) et le boîtie appliance firewall-VPN sont chiffrées avec l'algorithme AES 128 bits. Leur contenu est donc protégé en confidentialité.

L'intégrité du contenu des sessions d'administration est contrôlé à l'aide de l'algorithme HMAC-SHA1, avec une longueur de clés de 160 bits.

Les clés d'authentification et de chiffrement des sessions d'administration à distance sont dérivées :

- soit de la clé de session établie suite à l'authentification SRP de l'administrateur (Real-Time Monitor et Event Reporter) ;
- soit de la clé de session établie durant l'établissement d'un canal TLS, que ce soit avec ou sans authentification mutuelle par certificat X.509 (Web Manager).

Argumentaire : le chiffrement en AES 128 bits des sessions d'administration satisfait FPT_ITT.1 et FCS_COP.1.Chiffrement_sessions. Le contrôlé d'intégrité par HMAC-SHA1 160 bits satisfait FPT_ITT.1 et FCS_COP.1.Intégrité_sessions. La nécessité pour l'administrateur de s'authentifier via le protocole SRP pour pouvoir dériver la clé de chiffrement de l'AES 128 bits de la clé de session SRP, ou de s'authentifier par identifiant / mot passe au travers du protocole TLS, ou de s'authentifier par certificat X.509 au travers du protocole TLS satisfait FMT_SMF.1.b, FTP_TRP.1.Admin.3.b.

Authentification des administrateurs et élaboration de la clé de chiffrement par le protocole SRP

Le protocole SRP [SRP] permet à un « client » (dans notre cas : les outils d'administration comme le Web Manager) et à un « serveur » (le boîtier appliance firewall-VPN) de s'authentifier mutuellement et de négocier une clé de session servant à protéger les échanges ultérieurs.

Lors de la création du profil de chaque administrateur, le boîtier appliance firewall-VPN génère une graine qui permet, combinée au mot de passe, de dériver une clé privée DH administrateur dont la clé publique DH correspondante est appelée valeur de vérification. La graine et la valeur de vérification sont stockées dans le profil de l'administrateur, la clé privée DH administrateur n'est pas conservée

par le boîtier appliance firewall-VPN. Notez que même si la valeur de vérification est une « clé publique » au sens Diffie-Hellman du terme, il est nécessaire que le boîtier appliance firewall-VPN la protège contre la divulgation, de plus celle-ci n'est jamais transmise à un tiers.

Note d'application : de plus amples détails sont fournis dans la RFC 2945 [SRP] et dans [Wu98].

Argumentaire : le chemin de confiance entre l'administrateur et le boîtier appliance firewall-VPN spécifié par FTP_TRP.1.Admin est implémenté par le protocole SRP, tel que spécifié par FIA_UAU.5.Admin. Dans ce protocole, l'initiative de l'authentification revient à l'administrateur, ce qui satisfait FTP_TRP.1.Admin.2. L'authentification mutuelle, qui garantit l'identification des extrémités (élément FTP_TRP.1.Admin.1), est établie à la fin de la dernière passe du protocole. L'utilisation du chemin de confiance pour l'authentification mutuelle initiale de l'administrateur et de le boîtier appliance firewall-VPN satisfait FTP_TRP.1.Admin.3.a et FMT_SMF.1.b

L'utilisation de l'algorithme Diffie-Hellman avec des clés éphémères d'entropie de 2048 bits satisfait FCS_COP.1.Elaboration_clés concernant la partie de cette exigence qui soutient FIA_UAU.5.Admin.

Authentification des administrateurs et élaboration de la clé de chiffrement par le protocole TLS

Le protocole TLS [TLS] permet à un « client » (dans notre cas : les outils d'administration comme le Web Manager) d'authentifier un « serveur » (le boîtier appliance firewall-VPN) et optionnellement de s'authentifier auprès de ce même serveur. Dans les deux cas, le protocole TLS permet également de négocier une clé de session servant à protéger les échanges ultérieurs.

Lors de la création du profil de chaque administrateur, il est possible de spécifier la méthode d'authentification qui sera utilisée (identifiant / mot de passe ou certificat X.509)

Note d'application : de plus amples détails sont fournis dans la RFC 2246 [TLS]. Dans le cadre de l'utilisation du protocole TLS par le Web Manager, l'établissement de la connexion est réalisé par le navigateur Web présent sur la station d'administration qui est hors évaluation. De même le protocole TLS lui-même est hors du cadre de cette évaluation.

Argumentaire : le chemin de confiance entre l'administrateur et le boîtier appliance firewall-VPN spécifié par FTP_TRP.1.Admin est implémenté par le protocole TLS, tel que spécifié par FIA_UAU.5.Admin. Dans ce protocole, l'initiative de l'authentification revient à l'administrateur, ce qui satisfait FTP_TRP.1.Admin.2. L'authentification mutuelle, qui garantit l'identification des extrémités (élément FTP_TRP.1.Admin.1), est établie lors dans le protocole TLS (cas d'utilisation de certificat X.509) ou à la suite de l'établissement de la connexion TLS (cas de l'identifiant / mot de passe). L'utilisation du chemin de confiance pour l'authentification mutuelle initiale de l'administrateur et de le boîtier appliance firewall-VPN satisfait FTP_TRP.1.Admin.3.a et FMT_SMF.1.b

L'utilisation de l'algorithme Diffie-Hellman avec des clés éphémères d'entropie de 2048 bits satisfait FCS_COP.1.Elaboration_clés concernant la partie de cette exigence qui soutient FIA_UAU.5.Admin.

6.1.9 Autres fonctions de soutien

La fonction cryptographique est présentée avec les sous-ensembles fonctionnels de sécurité qu'elle soutient, ainsi que la justification des différentes exigences élémentaires spécifiées par FCS_COP.1.

L'horloge interne du boîtier appliance firewall-VPN fournit une base de temps fiable (FPT_STM.1). Celle-ci est modifiable par le super-administrateur uniquement.

7 ANNEXE A – DROITS D'ADMINISTRATION

Cette section a pour objet l'énumération complète des droits d'administration sur le boîtier appliance firewall-VPN pouvant être attribués aux utilisateurs, tel que définie dans FMT_MOF.1.1 et FMT_MTD.1.1

Droits concernant des fonctions ou des données de sécurité:

- **ADMIN (A)** : super-administrateur (login « admin »)
- **BASE (B)** : administration minimum, tous les accès indispensables à l'administration.
- **LOG (L)** : accès aux fichiers de trace et à la fonction d'audit.
- **LOG_READ (LR)** : accès en lecture seule aux fichiers de trace et à la fonction d'audit.
- **FILTER (F)** : accès aux slots de filtrage.
- **FILTER_READ (FR)** : accès en lecture seule aux slots de filtrage.
- **GLOBALFILTER (GF)** : accès aux slots de filtrage de la configuration globale.
- **VPN (V)** : accès aux slots VPN, clés pré-partagées, certificat (boîtier appliance firewall-VPN).
- **VPN_READ (VR)** : accès en lecture seule aux slots VPN, clés pré-partagées, certificat (boîtier appliance firewall-VPN).
- **OBJECT (O)** : ajout et de suppression d'objets (de configuration du réseau).
- **GLOBALOBJECT (GO)** : ajout et suppression d'objets de la configuration globale.
- **USER (U)** : gestion des utilisateurs.
- **NETWORK (N)** : gestion de la configuration réseau (interfaces, bridges, dialups, VLANs, ...)
- **ROUTE (R)** : gestion du routage (route par défaut, routes statiques, réseaux de confiance)
- **ASQ (As)** : consultation de la configuration du moteur statefull ASQ
- **MAINTENANCE (Ma)** : accès aux opérations de maintenance
- **MODIFY (M)**: modification des données de sécurité incluant la configuration.
- **MON_WRITE (MW)** : modification de données réservées au Monitoring.
- **CONTENT_FILTERING (CF)** : définir les politiques de filtrage applicatives (url, smtp, antispam, antivirus, et ssl).

Autres droits ne concernant pas des fonctions ou des données de sécurité:

- **PKI** : gestion de la PKI interne (émission, révocation, …)
- **HA** : haute disponibilité (interne, interdit aux utilisateurs).
- **PVM** : gestion des vulnérabilités (consultation, modification)
- **REPORTING (R)** : accès aux rapports embarqués.
- **REPORTING_READ (RR)** : accès en lecture seule aux rapports embarqués.

8 ANNEXE B – ATTAQUES PRISES EN COMPTE PAR L'ASQ

Cette section a pour objet l'énumération complète des attaques prises en compte par le

moteur de filtrage ASQ et leur rattachement aux types d'attaques définies par l'exigence élémentaire FAU_SAA.4.1.

Niveau d'analyse	*Libellé de l'attaque*	*Id*	*Type d'attaque*
IP	Usurpation d'adresse de boucle	0	a
	Usurpation d'adresse IP	1	a
	Paquet broadcast	2	b
	Paquet multicast	3	b
	Adresse de classe expérimentale	4	b
	Mauvaise option IP	5	b
	Option IP inconnue	6	b
	Protocole IP non analysé	7	b
	Machine du réseau interne inconnue	8	b
	Débordement de fragment	9	b
	Recouvrement de fragment	10	b
	Adresse multicast avec TCP	18	b
	Attaque de type Land	21	b
	Routage par la source	23	b
	Détection de la politique de filtrage	26	e
	Possible scan de ports	27	e
	Fragment IP de taille nulle	33	b
	Petit fragment	57	b
	Sonde de port	63	e
	Usurpation d'adresse IP sur un bridge	70	a
	Adresse broadcast avec TCP	71	b
	Alarme de filtrage	72	-
	Utilisation de la plage d'adresse 'link local' (RFC 3330)	83	b
	Utilisation de l'adresse broadcast en source	89	b
	Attaque possible des ressources	91	b
	Protocole IP invalide	92	b
	Adresse dans la liste noire	93	-
	Adresse dans la liste blanche	94	-
	Paquet avec destination sur la même interface	95	-
	Somme de contrôle IP invalide	96	b
	Rejet pour qualité de service	101	-
	Analyse de fragment IP	102	-
	Usurpation d'adresse IP sur l'interface IPsec	108	a
	Connexion perdue	210	-
TCP	Option TCP invalide	14	b
	Option TCP inconnue	15	b
	Mauvais numéro de séquence TCP	16	b
	Somme de contrôle TCP invalide	17	b
	Attaque Xmas tree	20	b

Niveau d'analyse	*Libellé de l'attaque*	*Id*	*Type d'attaque*
	Sonde OS Nmap	24	e
	Sonde OS Queso	25	e
	Possible saturation TCP SYN	29	f
	Port 0 utilisé comme service	34	b
	Bug Windows sur les données OOB	35	d
	Attaque possible par MSS faible	36	b
	Option TCP au mauvais moment	58	b
	Evasion de données sur TCP	65	b
	Débordement de la file de donnée TCP	84	b
	Détection d'une connexion interactive	85	b
	Paquet TCP invalide par rapport à l'état	97	b
	Protocole TCP invalide	98	b
	Problème dans le suivi de données	99	-
	Détection de protocole non autorisé	110	-
	Données urgentes non autorisées dans du trafic TCP	162	c
	Désynchronisation du trafic TCP	211	b
	Pris en charge par le synproxy	212	-
	Etat de désynchronisation du trafic TCP	213	b
	Trafic Cisco WAN optimizer détecté	247	-
	Possible saturation requêtes TCP	253	f
UDP	Possible saturation UDP	29	f
	Bouclage de port UDP	31	b
	Port 0 utilisé comme service	34	b
	Somme de contrôle UDP invalide	73	b
	Problème dans le suivi de données	99	-
	Protocole UDP invalide	100	b
	Détection de protocole non autorisé	110	-
	Possible saturation requêtes UDP	253	f
ICMP	Type ICMP inconnu	11	b
	Réponse ICMP sans requête	12	b
	ICMP redirect	22	b
	Possible saturation ICMP	28	f
	Sonde OS XProbe	66	e
	Message ICMP invalide	67	b
	Demande ICMP 'timestamp'	68	b
	Demande ICMP 'mask'	69	b
	Somme de contrôle ICMP invalide	75	b
	Attaque possible par MTU faible	81	b
	Demande ICMP 'information'	103	b
	Autorisé par l'analyse ICMP	107	b
	Modification des données ECHO ICMP	109	b
	Protocole non analysé dans un message ICMP	112	b

Niveau d'analyse	*Libellé de l'attaque*	*Id*	*Type d'attaque*
IGMP	Type IGMP inconnu	19	c
	Demande IGMP pour une adresse non multicast	61	c
	Paquet IGMP invalide	62	c
	Somme de contrôle IGMP invalide	74	c
DNS	Récursion de label DNS	32	d
	DNS id spoofing	38	c
	DNS zone change	39	c
	DNS zone update	40	c
	Empoisonnement du cache DNS	60	d
	Mauvais pointeur	86	c
	Débordement possible avec une chaîne DNS	87	c
	Protocole DNS invalide	88	c
	Champ query DNS contradictoire	151	c
	Usurpation DNS ciblée	152	c
	Possible attaque 'DNS rebinding'	154	c
	Réponse DNS dupliquée	159	c
FTP	Attaque FTP bounce possible	37	d
	Tentative d'insertion de commande FTP PASV	41	c
	Commande FTP inconnue	42	c
	Débordement en FTP lors du login	43	d
	Débordement en FTP	44	d
	Attaque en force brute sur mot de passe FTP	45	c
	Exécution de commande via SITE EXEC	46	c
	FTP PASV DoS	59	c
	Protocole FTP invalide	76	c
	Commande PORT invalide	123	c
HTTP	Encodage en caractère %u invalide dans l'url	47	c
	Evasion utilisant l'encodage %u dans l'url	48	d
	Caractère d'échappement invalide dans l'URL	49	c
	Caractère NULL codé dans l'URL	50	d
	Caractère Pourcent codé dans l'URL	51	d
	Evasion utilisant l'encodage UTF-8	52	d
	Protocole HTTP invalide	53	c
	Débordement dans une URL	54	d
	Débordement dans le protocole HTTP	55	d
	Tunneling possible avec la méthode CONNECT	56	c
	Suite de slash dans l'URL	78	d
	Chemin avec auto-référence	79	c
	Chemin avec référence supérieure	80	c
	Encodage UTF-8 invalide dans URL	82	c
	Code malicieux possible dans l'entête HTTP	90	d
	Chemin avec référence supérieure en dehors du répertoire racine	124	d

Niveau d'analyse	*Libellé de l'attaque*	*Id*	*Type d'attaque*
	Site avec rebond par redirect	148	d
	Réponse 304 avec donnée	149	c
	Données additionnelles en fin de réponse	150	c
	Tentative de pollution de paramètres HTTP	160	d
	Caractère unicode de changement du sens de la lecture dans URL HTTP	161	d
	Trop d'entête HTTP dans la requête	232	c
	Réponse HTTP/1.1 inattendue pour ce User-Agent	242	c
	Décodage du champ HTML échoué, le code est invalide	243	c
	Récursion détectée dans le décodage du champ HTML	244	c
	Redirection HTTP vers fichier local	249	d
	Trop de ranges dans la requête HTTP	251	c
	Ranges mal formés dans la requête HTTP	252	c
SIP	Protocole SIP invalide	131	c
	Débordement dans le protocole SIP	132	c
	Code malicieux possible dans l'entête SIP	133	c
	Entête SIP nécessaire manquant	134	c
	Requête SIP usurpée	135	c
	Champ SDP nécessaire manquant dans le protocole SIP	136	c
	Valeur du champ SIP expires invalide	137	c
	Encodage UTF-8 invalide dans le protocole SIP	138	c
	Limite des opérations SIP dépassée	139	d
	Paramètre purpose manquant dans le protocole SIP	140	c
	Champ Via invalide dans le protocole SIP	141	c
	Paquet binaire dans le protocole SIP	142	c
	Valeur invalide dans l'entête SIP Max-Forward	153	c
	Entête SIP Max-Forwards manquante	248	c
SMTP	Protocole SMTP invalide	121	c
	Caractère invalide dans l'entête SMTP	122	c
	Débordement dans le protocole SMTP	217	c
	Paramètres invalides pour la commande SMTP BDAT	218	c
	Ligne de commande ou réponse SMTP vide	219	c
	Données base64 invalides dans une commande SMTP de type AUTH	220	c
	Commande SMTP DATA avec des paramètres	221	c
	Commande SMTP non supportée par le serveur	223	c
	Commande SMTP BDAT désactivée	224	-
	Commandes SMTP d'Exchange Server désactivées	225	-
	Commande SMTP EXPN utilisée	226	e
	Commande SMTP VRFY utilisée	227	e
	Commandes SMTP TURN, ATRN, ETRN désactivées	228	-
	Commande SMTP interdite trouvée	229	c
	Message SMTP avec trop d'octets d'entêtes	230	c
	Entête Subject SMTP contient des caractères non-ASCII	231	c

9 ANNEXE C – IDENTIFICATION DES OPÉRATIONS EFFECTUÉES SUR LES EXIGENCES DE SÉCURITÉ DES TI

Cette section a pour objet l'identification précise des opérations effectuées sur les exigences de sécurité des TI, requise par l'exigence ASE_REQ.2.3C. Elle doit être considérée comme « l'énoncé des exigences de sécurité des TI fourni en tant que partie de la ST », requis par l'exigence ASE_REQ.2.1D,

9.1 Introduction

En plus des quatre types d'opérations définies dans les Critères Communs (cf. [CC-01], § C.4, p. 77), deux types supplémentaires de modification du texte original des exigences de sécurité des TI ont été introduites :

Le raffinement systématique : il s'agit d'un raffinement effectué de manière homogène sur tous les éléments d'un composant ;

La mise en forme : il s'agit d'une transformation de la structure grammaticale d'un élément, de manière à le rendre plus facile à lire, ou à supprimer du texte inutile, mais qui ne change absolument pas le sens de l'élément. Cela correspond à la notion d'*editorial refinement* détaillée dans [CC-01], § C4.4, p. 80.

Les opérations ont été effectuées sur le texte anglais original des exigences de sécurité des TI, mais elles ont pour effet de remplacer ces termes anglais par des termes français, et/ou à ajouter des termes français à un patron original en anglais. Malgré leur difficulté d'emploi, ces exigences en « franglais » constituent en tout état de cause l'élément de preuve requis par l'élément ASE_REQ.2.1D, alors que les exigences énoncées au §5.2 du présent document ne sont qu'une reformulation du contenu de cette section, fournie dans le but de faciliter la compréhension de l'énoncé des exigences de sécurité des TI.

Dans l'identification des opérations, les raffinements qui consistent à substituer un terme à un autre, les affectations et les sélections sont identifiés par le symbole « := ». Les raffinements qui consistent à rajouter du texte sont identifiés par le symbole « + ». Les mises en forme sont identifiées par le symbole « → » pour les substitutions et « ⌫ » pour les suppressions.

Les itérations sont identifiables à l'aide des étiquettes, comme cela est expliqué au §5.1.2.

Les exigences de sécurité des TI sont présentées sous la forme suivante :

Pour chaque composant utilisé, les raffinements systématiques opérés sur les éléments de ce composant,

Pour chaque élément du composant :

Le texte anglais original de l'élément, tel qu'extrait de [CC-02] ou [CC-03],

La liste des opérations effectuées sur l'élément.

9.2 Exigences de sécurité pour la TOE

Cette section présente les exigences fonctionnelles de la TOE suivant une description formelle. Le lien avec le chapitre 5 est réalisé en conservant le même titre pour les exigences fonctionnelles concernées.

9.2.1 Exigences de contrôle des flux d'information

Fonction de filtrage

FDP_IFC.2 – Filtrage complet des flux d'information

Raffinement systématique	*The TSF* := la fonction de filtrage

FDP_IFC.2.1 *The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.*

Affectation	*information flow control SFP* := la politique de filtrage
Affectation	*list of subjects and information* := les équipements des réseaux interconnectés par le boîtier appliance firewall-VPN(*subjects*), les paquets IP (*information*)
Raffinement	*all operations that cause that information to flow to and from subjects covered by the SFP* := tous les transferts (*operations*) de paquets IP entre les équipements des réseaux interconnectés par le boîtier appliance firewall-VPN
Mise en forme	les équipements des réseaux interconnectés par le boîtier appliance firewall-VPN, les paquets IP et tous les transferts de paquets IP entre les équipements des réseaux interconnectés par le boîtier appliance firewall-VPN → les paquets IP entrants

FDP_IFC.2.2 *The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.*

Raffinement + mise en forme	*all operations that cause any information in the TOE to flow to and from any subject in the TOE* := tous les transferts de paquets les équipements des réseaux interconnectés par le boîtier appliance firewall-VPN → tous les paquets IP entrants
Raffinement	*an information flow control SFP* := la politique de filtrage

FDP_IFF.1.Filtrage – Fonction de filtrage

Raffinement systématique	*The TSF* := la fonction de filtrage
Raffinement systématique	*information flow between a controlled subject and controlled information via a controlled operation* := les paquets IP entrants

FDP_IFF.1.1 *The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and, for each, the security attributes].*

Affectation	*information flow control SFP* := la politique de filtrage
Raffinement + mise en forme	*subject and information* := équipements des réseaux interconnectés par le boîtier appliance firewall-VPN(*subjects*), les paquets IP (*information*) → les paquets IP entrants
Affectation	*list of subjects and information controlled under the indicated SFP, and, for each, the security attributes* :=

	a. L'interface de réception, b. L'interface de destination, c. L'adresse IP source et destination du paquet et, partant de là, la machine source et la machine destination du paquet, d. Le numéro de protocole IP, e. La valeur du champ DSCP, f. Si le protocole est TCP ou UDP : le port source et destination, g. Si le protocole est ICMP : les champs 'type' et 'code' du message.

FDP_IFF.1.2 *The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].*

Affectation	*for each operation, the security attribute-based relationship that must hold between subject and information security attributes* := a. Préalablement à l'application des règles de filtrage, le paquet est comparé à l'ensemble des connexions / pseudo-connexions actuellement établies et ayant été autorisées par les règles de filtrage ; b. Si le paquet correspond à une de ces connexions / pseudo-connexions, il est autorisé à passer sans être soumis aux règles de filtrage ; c. Sinon, le paquet est autorisé si l'action de la première règle de filtrage applicable est 'passer'.

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

Affectation	*additional information flow control SFP rules* := les règles complémentaires suivantes : a. Les règles de filtrage dont l'action est 'aucune' ont pour unique objet la génération d'enregistrements d'audit et ne rentrent pas en compte dans le filtrage des paquets. b. Les règles de filtrage dont l'action est 'déléguer' ont pour unique objet le saut de l'évaluation de la fin du slot de filtrage global pour reprendre au début du slot local et ne rentrent pas en compte dans le filtrage des paquets.

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

Affectation	*rules, based on security attributes, that explicitly authorise information flows* := a. Les sessions associées à des protocoles nécessitant des connexions filles sont suivies de manière à autoriser ces connexions filles conformément à l'état de la session principale ; b. Des règles de filtrage implicites peuvent être générées par le firewall en liaison avec la configuration d'autres fonctions de sécurité. Ce sont les règles correspondant à : i. l'administration à distance du firewall, ii. l'établissement de VPN.

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

Affectation	*rules, based on security attributes, that explicitly deny information flows* := a. L'action de la première règle de filtrage applicable est 'bloquer' ou 'réinitialiser' ;

	b. Aucune règle de filtrage n'a autorisé le paquet.

Fonction de chiffrement

FDP_IFC.1 – Chiffrement des flux d'information

Raffinement systématique	*The TSF* := la fonction de chiffrement

FDP_IFC.1.1 *The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].*

Affectation	*information flow control SFP* := la politique de chiffrement
Affectation + mise en forme	*list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP* := les correspondants VPN et les extrémités du trafic (côté TOE et côté correspondants VPN) (*subject*), les datagrammes ESP entrants et les datagrammes IP sortants couverts par une politique de chiffrement (*information*), les réceptions de datagrammes ESP entrants provenant des correspondants VPN et les émissions de datagrammes IP sortants couverts par une politique de chiffrement (*operations*) → les datagrammes ESP entrants et les datagrammes IP sortants couverts par une règle de chiffrement

FDP_UCT.1 – Confidentialité du contenu des flux

Raffinement systématique	*The TSF* := la fonction de chiffrement

FDP_UCT.1.1 *The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to be able to [selection: transmit, receive] user data in a manner protected from unauthorised disclosure.*

Affectation	*access control SFP(s) and/or information flow control SFP(s)* := la politique de chiffrement
Sélection	*transmit, receive* := *transmit and receive*
Raffinement	*user data* := des datagrammes IP

FDP_UIT.1 – Intégrité du contenu des flux

Raffinement systématique	*The TSF* := la fonction de chiffrement

FDP_UIT.1.1 *The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to be able to [selection: transmit, receive] user data in a manner protected from [selection: modification, deletion, insertion, replay] errors.*

Affectation	*access control SFP(s) and/or information flow control SFP(s)* := la politique de chiffrement
Sélection	*transmit, receive* := *transmit and receive*
Raffinement	*user data* := des datagrammes IP
Sélection	*modification, deletion, insertion, replay* := *modification, insertion, replay*

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

Raffinement	*user data* := les datagrammes ESP entrants
Sélection	*modification, deletion, insertion, replay* := *modification, insertion, replay*

FDP_IFF.1.Chiffrement – Fonction de chiffrement

Raffinement systématique	*The TSF* := la fonction de chiffrement

FDP_IFF.1.1 *The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].*

Affectation	*information flow control SFP* := la politique de chiffrement
Raffinement + mise en forme	*subject and information* := les correspondants VPN et les extrémités du trafic (côté TOE et côté correspondants VPN) (*subject*), les datagrammes ESP entrants et les datagrammes IP sortants couverts par une politique de chiffrement (*information*) → les datagrammes ESP entrants et les datagrammes IP sortants couverts par une règle de chiffrement
Affectation	*list of subjects and information controlled under the indicated SFP, and for each, the security attributes* := Datagrammes ESP entrants : a. L'index de sécurité (SPI), Datagrammes IP sortants : b. L'adresse IP source et destination du paquet et, partant de là, la machine source et la machine destination du paquet, c. Le type de protocole IP.

FDP_IFF.1.2 *The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].*

Raffinement	*information flow between a controlled subject and controlled information via a controlled operation* := paquet ESP entrant
Affectation	*for each operation, the security attribute-based relationship that must hold between subject and information security attributes* := a. un datagramme ESP entrant est rattachable à une SA IPSec entrante active, b. le paquet encapsulé dans le datagramme ESP correspond aux critères de la règle de chiffrement associée à la SA IPSec.

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

Affectation	*additional information flow control SFP rules* := les règles complémentaires suivantes : a. utilise sur les datagrammes IP sortants, les algorithmes d'authentification et de chiffrement effectifs spécifiés par la SA IPSec sortante associée à la première règle de chiffrement applicable. b. provoque une tentative de rénégociation si un datagramme IP sortant est couvert par une règle de chiffrement sans SA IPSec sortante active. Si la négociation échoue, le datagramme est détruit.

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

Affectation	*rules, based on security attributes, that explicitly authorise information flows* := aucune règle
Mise en forme	de l'élément

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

Affectation	*rules, based on security attributes, that explicitly deny information*

	flows := aucune règle
Mise en forme	de l'élément

Fonction d'établissement des SA

FTP_TRP.1.Corresp – Chemin de confiance avec les correspondants VPN

Raffinement systématique	*The TSF* := la fonction d'établissement des SA

FTP_TRP.1.1 *The TSF shall provide a communication path between itself and [selection: remote, 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 [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].*

Sélection	*remote, local* := *remote*
Raffinement	*Itself* := le boîtier appliance firewall-VPN
Raffinement	*remote users* := les correspondants VPN
Affectation	*other types of integrity or confidentiality violation* := none
Sélection	*modification, disclosure, none* := modification or disclosure

FTP_TRP.1.2 *The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path.*

Sélection	*the TSF, local users, remote users* := *the TSF and remote users*
Raffinement	*the TSF and remote users* := le boîtier appliance firewall-VPN et les correspondants VPN
Raffinement	*communication via the trusted path* := L'établissement du chemin de confiance correspond à la phase 1 du protocole IKE.

FTP_TRP.1.3 *The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].*

Sélection	*initial user authentication, [assignment: other services for which trusted path is required]* := *a. initial user authentication,* *b. [assignment: other services for which trusted path is required]*
Raffinement	*initial user authentication* := l'authentification mutuelle initiale des extrémités du tunnel (phase 1 du protocole IKE)
Affectation	*other services for which trusted path is required* := la négociation des SA IPSec (phase 2 du protocole IKE)

FIA_UAU.5.Corresp – Multiples mécanismes d'authentification des correspondants VPN

Raffinement systématique	*The TSF* := la fonction d'établissement des SA

FIA_UAU.5.1 *The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.*

Affectation	*list of multiple authentication mechanisms* := les mécanismes d'authentification suivants : certificats X509, clé pré-partagée
Raffinement	*user* := le correspondant VPN d'un tunnel donné, dans le cadre de l'authentification mutuelle initiale des extrémités de ce tunnel lors de la phase 1 IKE.

FIA_UAU.5.2 *The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].*

Affectation + mise en forme	*rules describing how the multiple authentication mechanisms provide authentication* := les règles du mécanisme d'authentification spécifié pour le tunnel VPN

	→ le mécanisme d'authentification spécifié pour le tunnel VPN
Raffinement	*user* := correspondant VPN

FPT_TDC.1 – Négociation des SA ISAKMP et IPSec

Raffinement systématique	*The TSF* := la fonction d'établissement des SA

FPT_TDC.1.1 *The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product.*

Affectation	*list of TSF data types* := les paramètres des SA ISKAMP et IPSec
Raffinement	*consistently interpret* les paramètres des SA ISKAMP et IPSec := négocier les paramètres des SA ISKAMP et IPSec
Raffinement	*when shared between the TSF and another trusted IT product* := lors de l'établissement des tunnels VPN entre l'appliance firewall-VPN et les correspondants VPN

FPT_TDC.1.2 *The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product.*

Affectation	*list of interpretation rules to be applied by the TSF* := les règles suivantes : a. Si l'appliance firewall-VPN est l'initiateur, proposer les paramètres de la SA ISAKMP ou IPSec, et accepter les réponses aussi rigoureuses qu'une des propositions faites ; b. Si l'appliance firewall-VPN est le répondeur, n'accepter que les propositions aussi rigoureuses qu'une des propositions locales.
Raffinement	*interpreting the TSF data from another trusted IT product* := négocier les paramètres des SA ISAKMP ou IPSec avec les correspondants VPN

Fonction de journalisation, d'audit et d'alarme

FAU_GEN.1 – Génération de données d'audit

Raffinement systématique	*The TSF* := la fonction de journalisation

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

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

b) All auditable events for the [selection: choose one of: minimum, basic, detailed, not specified] level of audit; and

c) [assignment: other specifically defined auditable events].

Sélection	*minimum, basic, detailed, not specified* := *not specified*
Mise en forme	de l'item b)
Affectation	*other specifically defined auditable events* := les événements auditables énumérés dans le tableau au chapitre 5.2 après FAU_GEN.1.2
Raffinement	*audit functions* := fonction de journalisation

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information]

Raffinement	*subject identity* := adresse IP source
Affectation	*other audit relevant information* := niveau d'alarme (si c'en est une), les

	informations d'audit complémentaires énoncées dans le tableau au chapitre 5.2
Mise en forme	"Factorisation" de « niveau d'alarme (si c'en est une) »

FAU_GEN.2 – Identification de l'utilisateur

Raffinement systématique	*The TSF* := la fonction de journalisation

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

Raffinement	*user* := administrateur
Raffinement	*auditable event* := événement auditable associé aux opérations d'administration de la sécurité

FAU_SAR.1 – Revue d'audit

Raffinement systématique	*The TSF* := la fonction d'audit

FAU_SAR.1.1 *The TSF shall provide [assignment: authorised users] with the capability to read [assignment: list of audit information] from the audit records.*

Affectation	*authorised users* := auditeurs
Affectation	*list of audit information* := toutes les informations d'audit
Raffinement	*audit records* := fichiers de trace

FAU_SAR.1.2 *The TSF shall provide the audit records in a manner suitable for the user to interpret the information.*

Raffinement	*audit records* := fichiers de trace
Raffinement	*user* := auditeur

FAU_STG.3 – Action en cas de perte possible de données d'audit

Raffinement systématique	*The TSF* := la fonction de journalisation

FAU_STG.3.1 *The TSF shall [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit].*

Affectation	*actions to be taken in case of possible audit storage failure* := une action parmi les suivantes : a. Assurer la rotation des fichiers : les enregistrements d'audit les plus récents effacent les enregistrements d'audit les plus anciens, b. Stopper l'écriture des fichiers : les enregistrements d'audit ne sont plus mémorisés, c. Arrêter le Firewall : l'appliance firewall-VPN ne s'arrête pas réellement mais il bloque l'ensemble des flux excepté les sessions d'administration du Web Manager depuis le réseau interne.
Raffinement	*audit trail* := un fichier de trace existant (exclus l'utilisation de Syslog)
Affectation	*pre-defined limit* := dépasse la taille de 5 Mo.

FAU_ARP.1.Alarmes – Réponse automatique aux alarmes

Raffinement systématique	*The TSF* := la fonction d'alarme

FAU_ARP.1.1 *The TSF shall take [assignment: list of actions] upon detection of a potential security violation.*

Affectation	*list of actions* := Transmettre l'alarme aux moniteurs temps-réel connectés
Raffinement	*detection of a potential security violation* := génération d'un enregistrement d'audit auquel est attribué un niveau d'alarme

9.2.2 Exigences de protection contre les attaques Internet

Fonction de prévention des intrusions

FAU_SAA.4 – Heuristiques des attaques complexes

Raffinement systématique	*The TSF* := la fonction de prévention des intrusions

FAU_SAA.4.1 *The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the enforcement of the SFRs.*

Raffinement	*internal representation* := base de connaissance
Mise en forme	*the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the enforcement of the SFRs.* *→ the following signature events and event sequences of known intrusion scenarios [assignment: list of system events or sequences of system events whose occurrence are representative of known penetration scenarios] that may indicate a potential violation of the enforcement of the SFRs.*
Affectation	*list of system events or sequences of system events whose occurrence are representative of known penetration scenarios* := les types d'attaque suivants : a. paquets IP dont l'adresse source est incohérente avec l'interface de réception, b. paquets, datagrammes ou segments IP, ICMP, IGMP, TCP ou UDP non conformes aux RFC, ou utilisation abusive des possibilités offertes par ces protocoles, c. commandes, requêtes ou réponses applicatives non conformes à la syntaxe générale des commandes / requêtes / réponses définie par les RFC, ou utilisation abusive des possibilités offertes par ces protocoles, d. attaques basées sur des vulnérabilités connues des serveurs applicatifs, e. tentatives de récupération d'information concernant la configuration des serveurs applicatifs (*fingerprinting*, *port scanning*, etc.), f. dépassement du taux d'ouverture de connexions associé à une règle de filtrage.
Raffinement	*potential violation of the enforcement of the SFRs* := attaque Internet potentielle

FAU_SAA.4.2 *The TSF shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of [assignment: information to be used to determine system activity].*

Raffinement	*signature events and event sequences* := types d'attaques présents dans la base de connaissance
Affectation	*information to be used to determine system activity* := les paquets IP entrants et sortants
Raffinement	*the record of system activity discernible from an examination of* les paquets IP entrants et sortants := l'état des différents contextes associés à chaque paquet IP entrant et sortant

FAU_SAA.4.3 *The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when system activity is found to match a signature event or event sequence that indicates a potential violation of the enforcement of the SFRs.*

Raffinement	*potential violation of the enforcement of the SFRs* := attaque Internet potentielle
Raffinement	*system activity* := l'état d'un ou plusieurs contextes associés à un paquet IP

	entrant
Raffinement	*signature event or event sequence that indicates a potential violation of the enforcement of the SFRs* := type d'attaque présent dans la base de connaissance

FAU_ARP.1.IPS – Réponse automatique aux attaques Internet potentielles

Raffinement systématique	*The TSF* := la fonction de prévention des intrusions

FAU_ARP.1.1 *The TSF shall take [assignment: list of actions] upon detection of a potential security violation.*

Affectation	*list of actions* := a. appliquer au paquet l'action associée au type de l'attaque, b. si un niveau d'alarme est spécifié pour ce type d'attaque, générer un enregistrement d'audit de l'événement, en lui attribuant ce niveau d'alarme.
Raffinement	*potential security violation* := attaque Internet potentiellement véhiculée par un paquet IP entrant

9.2.3 Exigences de prévention de l'utilisation impropre

Fonction de contrôle d'accès aux opérations d'administration de la sécurité

FMT_SMF.1 – Fonction d'administration de la sécurité

Raffinement systématique	*The TSF* := la fonction d'administration de la sécurité

FMT_SMF.1.1 *The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].*

Affectation	*list of management functions to be provided by the TSF* := a. La fonction de contrôle d'accès aux opérations d'administration de la sécurité ; b. La fonction de protection des sessions d'administration c. La fonction d'audit d. La fonction de sauvegarde / restauration

FMT_SMR.1 – Rôle d'administrateur de la sécurité

Raffinement systématique	*The TSF* := la fonction de contrôle d'accès aux opérations d'administration de la sécurité

FMT_SMR.1.1 *The TSF shall maintain the roles [assignment: the authorised identified roles].*

Affectation	*the authorised identified roles* := « administrateur » et « super administrateur »

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

Raffinement	+ en fonction des règles suivantes : a. Il n'y qu'un seul super-administrateur, distinct des autres administrateurs, et qui possède tous les droits ; b. Les administrateurs sont ceux auxquels on a explicitement attribué ce rôle.

FDP_ACC.2 – Contrôle d'accès complet aux opérations d'administration de la sécurité

Raffinement systématique	*The TSF* := la fonction de contrôle d'accès aux opérations d'administration de la sécurité

FDP_ACC.2.1 *The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.*

Affectation	*access control SFP* := la politique de contrôle d'accès aux opérations d'administration de la sécurité

Affectation	*list of subjects and objects* := les administrateurs (*subjects*), les données et les fonctions de sécurité (*objects*)
Raffinement	*all operations among subjects and objects covered by the SFP* := toutes les opérations d'administration de la sécurité
Mise en forme	les administrateurs, les données et les fonctions de sécurité et toutes les opérations d'administration de la sécurité → toutes les opérations d'administration de la sécurité effectuées par l'administrateur

FDP_ACC.2.2 *The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.*

Raffinement + mise en forme	*all operations between any subject controlled by the TSFand any object controlled by the TSF* := toutes les opérations d'administration de la sécurité entre les administrateurs et les données et les fonctions de sécurité → toutes les opérations d'administration de la sécurité effectuées par l'administrateur
Raffinement	*an access control SFP* := la politique de contrôle d'accès aux opérations d'administration de la sécurité

FMT_MOF.1 – Administration du comportement des fonctions de sécurité

Raffinement systématique	*The TSF* := la fonction de contrôle d'accès aux opérations d'administration de la sécurité

FMT_MOF.1.1 *The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorised identified roles].*

Sélection	*determine the behaviour of, disable, enable, modify the behaviour of* := *disable, enable, modify the behaviour of*
Raffinement	*modify the behaviour of* := effectuer, modifier
Affectation	*list of functions* := les fonctions de sécurité du tableau ci-dessous
Affectation	*the authorised identified roles* := les administrateurs
Raffinement	en fonction des droits ci-dessous

FMT_MTD.1 – Administration des données de sécurité

Raffinement systématique	*The TSF* := la fonction de contrôle d'accès aux opérations d'administration de la sécurité

FMT_MTD.1.1 *The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles].*

Sélection	*change_default, query, modify, delete, clear, [assignment: other operations]* := *query, modify, clear*
Affectation	*list of TSF data* := les données de sécurité du tableau ci-dessous
Affectation	*the authorised identified roles* := les administrateurs
Raffinement	+ en fonction des droits ci-dessous

Fonction de sauvegarde et de restauration

FMT_MTD.BRS – Sauvegarde et restauration des données de sécurité

Raffinement systématique	*The TSF* := la fonction de sauvegarde / restauration

FMT_MTD.BRS.1 *The TSF shall be able to back up [assignment: list of TSF data] into a storage device.*

Affectation	*list of TSF data* := les données de sécurité
Raffinement	*a storage device* := le disque sur de la station d'administration

FMT_MTD.BRS.2 The TSF shall allow restoration of TSF data backed up into a storage device.

Raffinement	*TSF data* := des données de sécurité
Raffinement	*a storage device* := le disque sur de la station d'administration

9.2.4 Exigences de protection de la TOE

Fonction de protection des sessions d'administration

FPT_ITT.1 – Protection élémentaire du contenu des sessions d'administration

Raffinement systématique	*The TSF* := la fonction de protection des sessions d'administration

FPT_ITT.1.1 The TSF shall protect TSF data from [selection: disclosure, modification] when it is transmitted between separate parts of the TOE.

Raffinement	*TSF data* := le contenu des sessions d'administration
Sélection	*disclosure, modification* := *disclosure, modification*
Raffinement	*separate parts of the TOE* := la station d'administration et le boîtier appliance firewall-VPN

FTP_TRP.1.Admin – Chemin de confiance pour l'administration à distance

Raffinement systématique	*The TSF* := la fonction de protection des sessions d'administration

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: remote, 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 [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].

Raffinement	*itself* := le boîtier appliance firewall-VPN
Sélection	*remote, local* := *remote*
Raffinement	*remote users* := les administrateurs
Affectation	*other types of integrity or confidentiality violation* := none
Sélection	*modification, disclosure, none* := modification or disclosure

FTP_TRP.1.2 The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path.

Sélection	*the TSF, local users, remote users* := *remote users*
Raffinement	*remote users* := les administrateurs

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].

Sélection	*initial user authentication, [assignment: other services for which trusted path is required]* := *initial user authentication, [assignment: other services for which trusted path is required]*
Raffinement	*initial user authentication* := l'authentification mutuelle initiale de l'administrateur et de le boîtier appliance firewall-VPN
Affectation	*other services for which trusted path is required* := les opérations d'administration à distance de la sécurité

FIA_UAU.5.Admin – Mécanisme d'authentification des administrateurs

Raffinement systématique	*The TSF* := la fonction de protection des sessions d'administration

FIA_UAU.5.1 The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.

Affectation	*list of multiple authentication mechanisms* := le mécanisme basé sur le protocole SRP ou le protocole TLS

Raffinement	*user* := administrateur

FIA_UAU.5.2 *The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].*

Raffinement	*user* := administrateur
Affectation + mise en forme	*rules describing how the multiple authentication mechanisms provide authentication* := les règles du protocole SRP ou les règles du protocole TLS (identifiant / mot de passe ou certificat X.509) →le protocole SRP ou le protocole TLS (identifiant / mot de passe ou certificat X.509)

9.2.5 Autres exigences de sécurité de soutien

Autres fonctions de soutien

FCS_COP.1 – Fonction cryptographique

Raffinement systématique	*The TSF* := la fonction cryptographique

FCS_COP.1.Elaboration_Clés *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Affectation	*list of cryptographic operations* := l'élaboration de clés
Affectation	*cryptographic algorithm* := l'algorithme cryptographique ⌫ spécifié ci-dessous
Affectation	*cryptographic key sizes* := les tailles des clés cryptographiques ⌫ spécifiées ci-dessous
Affectation	*list of standards* := les standards énoncés ci-dessous

FCS_COP.1.Signature_Chiffrement *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Affectation	*list of cryptographic operations* := la signature et le chiffrement/déchiffrement
Affectation	*cryptographic algorithm* := l'algorithme cryptographique ⌫ spécifié ci-dessous
Affectation	*cryptographic key sizes* := les tailles des clés cryptographiques ⌫ spécifiées ci-dessous
Affectation	*list of standards* := les standards énoncés ci-dessous

FCS_COP.1.Hachage *The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Affectation	*list of cryptographic operations* := le hachage univoque
Affectation	*cryptographic algorithm* := les algorithmes cryptographiques ⌫ spécifiés ci-dessous
Affectation	*cryptographic key sizes* := les tailles des clés cryptographiques ⌫ spécifiées ci-dessous
Affectation	*list of standards* := les standards énoncés ci-dessous

FCS_COP.1.Chiffrement_VPN	*The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Affectation	*list of cryptographic operations* := le chiffrement/déchiffrement symétrique des paquets VPN
Affectation	*cryptographic algorithm* := les algorithmes cryptographiques ⌫ spécifiés ci-dessous
Affectation	*cryptographic key sizes* := les tailles des clés cryptographiques ⌫ spécifiées ci-dessous
Affectation	*list of standards* := les standards énoncés ci-dessous

FCS_COP.1.Chiffrement_sessions	*The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Affectation	*list of cryptographic operations* := le chiffrement/déchiffrement symétrique des sessions d'administration
Affectation	*cryptographic algorithm* := l'algorithme cryptographique ⌫ spécifié ci-dessous
Affectation	*cryptographic key sizes* := les tailles des clés cryptographiques ⌫ spécifiées ci-dessous
Affectation	*list of standards* := les standards énoncés ci-dessous

FCS_COP.1.Intégrité_sessions	*The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].*

Affectation	*list of cryptographic operations* := le contrôle d'intégrité des sessions d'administration
Affectation	*cryptographic algorithm* := l'algorithme cryptographique ⌫ spécifié ci-dessous
Affectation	*cryptographic key sizes* := les tailles des clés cryptographiques ⌫ spécifiées ci-dessous
Affectation	*list of standards* := les standards énoncés ci-dessous

FPT_STM.1 – Base de temps fiable

Raffinement systématique	*The TSF* := l'horloge interne de le boîtier appliance firewall-VPN

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

10 ANNEXE D – EXIGENCE DE SÉCURITÉ EXPLICITEMENT ÉNONCÉE

Cette section a pour objet l'énoncé de l'exigence de sécurité explicitement énoncée dans le but de compléter celles existant dans la partie 2 et 3 des Critères Communs.

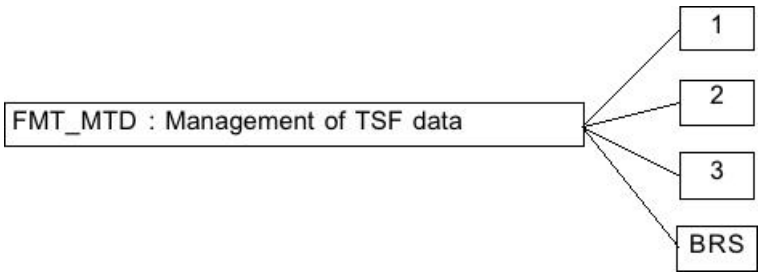
10.1 Introduction

L'exigence de sécurité explicitement énoncée dans la présente cible de sécurité est de nature fonctionnelle.

10.2 FMT_MTD - Management of TSF data

Component levelling

FMT_MTD.BRS



Backup and restoration of TSF data specifies the capacity to spare the configuration of the TSF, or part of it, into a separate storage device, and to restore it thereafter.

Management: FMT_MTD.BRS

a) Managing the group of roles that can perform backup.

b) Managing the group of roles that can perform restoration.

Audit: FMT_MTD.BRS

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Use of the backup functions.

b) Basic: Use of the restoration functions.

10.2.1 FMT_MTD.BRS – Backup and restoration of TSF data

Hierarchical to: no other component.

Dependencies: FMT_MTD.1 : Management of TSF data
FMT_SMF.1 : Specification of Management Functions

FMT_MTD.BRS.1 *The TSF shall be able to back up [assignment: list of TSF data] into a storage device.*

FMT_MTD.BRS.2 *The TSF shall allow restoration of TSF data backed up into a storage device.*

Application notes

Operations:

Assignment:

In FMT_MTD.BRS.1, the PP/ST author should specify the TSF data that can be backed up. In particular, it should be specified whether partial backup is possible.