



Firewalls NETASQ

Cible de sécurité

**Suite logicielle IPS-Firewall
Version 8.1**

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

NETASQ
Secure Internet Connectivity





SUIVI DE DOCUMENT

| Version | Auteur | Date | Modifications |
|---------|-----------------|------------|--|
| 1 | 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 | Boris MARECHAL | 10/05/2012 | Mise à jour suite aux remarques ANSSI |



TABLE DES MATIÈRES

| | |
|--|-----------|
| 1 INTRODUCTION | 6 |
| 1.1 Identification de la cible de sécurité | 6 |
| 1.2 Annonces de conformité | 6 |
| 1.3 Résumé des fonctionnalités du firewall-VPN NETASQ | 6 |
| 1.4 Documents applicables et de référence | 7 |
| 1.4.1 Référentiel des Critères Communs | 7 |
| 1.4.2 Schéma Français d'Évaluation et de Certification | 7 |
| 1.4.3 RFC et autres standards supportés | 7 |
| 1.5 Glossaire | 9 |
| 2 DESCRIPTION DE LA CIBLE D'ÉVALUATION | 12 |
| 2.1 Caractéristiques de sécurité TI de la TOE | 12 |
| 2.1.1 Généralités | 12 |
| 2.1.2 Le contrôle des flux d'information | 12 |
| 2.1.3 La protection contre les attaques Internet | 13 |
| 2.1.4 Les risques d'utilisation impropre | 14 |
| 2.1.5 La protection de la TOE elle-même | 15 |
| 2.2 Limites physiques de la TOE | 16 |
| 2.2.1 Équipements constituant la TOE | 16 |
| 2.2.2 Caractéristiques minimales des plates-formes d'exploitation | 17 |
| 2.3 Limites logiques de la TOE | 18 |
| 2.3.1 Composants logiciels | 18 |
| 2.3.2 Architecture et interfaces de la TOE | 19 |
| 2.3.3 Configurations et modes d'utilisation soumis à l'évaluation | 20 |
| 2.4 Plate-forme de test utilisée lors de l'évaluation | 22 |
| 3 ENVIRONNEMENT DE SÉCURITÉ DE LA CIBLE D'ÉVALUATION | 23 |
| 3.1 Convention de notation | 23 |
| 3.2 Identification des biens sensibles | 23 |
| 3.2.1 Biens protégés par la TOE | 23 |
| 3.2.2 Biens appartenant à la TOE | 23 |
| 3.3 Menaces et règles de la politique de sécurité | 25 |
| 3.3.1 Le contrôle des flux d'information | 25 |
| 3.3.2 La protection contre les attaques Internet | 25 |
| 3.3.3 Les risques d'utilisation impropre | 26 |
| 3.3.4 La protection de la TOE elle-même | 26 |
| 3.4 Hypothèses | 28 |
| 3.4.1 Hypothèses sur les mesures de sécurité physiques | 28 |
| 3.4.2 Hypothèses sur les mesures de sécurité organisationnelles | 28 |
| 3.4.3 Hypothèses relatives aux agents humains | 28 |
| 3.4.4 Hypothèses sur l'environnement de sécurité TI | 29 |
| 4 OBJECTIFS DE SÉCURITÉ | 29 |
| 4.1 Convention de notation | 30 |
| 4.2 Généralités | 30 |
| 4.3 Objectifs de contrôle des flux d'information | 31 |
| 4.4 Objectifs de protection contre les attaques Internet | 33 |
| 4.5 Objectifs de prévention de l'utilisation impropre | 34 |
| 4.6 Objectifs de protection de la TOE | 35 |
| 4.7 Objectifs de sécurité pour l'environnement | 36 |
| 4.8 Argumentaire des objectifs de sécurité | 37 |
| 4.9 Liens entre les hypothèses et les objectifs de sécurité pour l'environnement | 38 |
| 5 EXIGENCES DE SÉCURITÉ DES TI | 40 |
| 5.1 Introduction | 40 |
| 5.1.1 Généralités | 40 |



| | |
|--|------------|
| 5.1.2 Conventions typographiques..... | 41 |
| 5.1.3 Présentation des données de sécurité..... | 41 |
| 5.2 Exigences de sécurité pour la TOE..... | 45 |
| 5.2.1 Exigences de contrôle des flux d'information..... | 45 |
| 5.2.2 Exigences de protection contre les attaques Internet..... | 52 |
| 5.2.3 Exigences de prévention de l'utilisation impropre..... | 53 |
| 5.2.4 Exigences de protection de la TOE..... | 56 |
| 5.2.5 Autres exigences de sécurité de soutien..... | 57 |
| 5.3 Exigences d'assurance sécurité pour la TOE..... | 58 |
| 5.3.1 Mesures d'assurance sur la cible de sécurité (ASE)..... | 58 |
| 5.3.2 Autres mesures d'assurance sécurité..... | 59 |
| 5.4 Exigences de sécurité pour l'environnement TI..... | 60 |
| 5.5 Argumentaire des exigences de sécurité..... | 61 |
| 5.5.1 Satisfaction des objectifs de sécurité..... | 61 |
| 5.5.2 Soutien mutuel et non contradiction..... | 62 |
| 5.5.3 Satisfaction des dépendances des SFRs..... | 62 |
| 5.5.4 Satisfaction des dépendances des SARs..... | 63 |
| 6 SPÉCIFICATIONS ABRÉGÉES DE LA TOE..... | 64 |
| 6.1 Fonctions de sécurité des TI..... | 64 |
| 6.1.1 Fonction de filtrage..... | 64 |
| 6.1.2 Fonction d'identification / authentification..... | 65 |
| 6.1.3 Fonction de chiffrement..... | 66 |
| 6.1.4 Fonction d'établissement des SA..... | 68 |
| 6.1.5 Fonction de journalisation, d'audit et d'alarme..... | 70 |
| 6.1.6 Fonction de prévention des intrusions..... | 71 |
| 6.1.7 Fonction de contrôle d'accès aux opérations d'administration..... | 72 |
| 6.1.8 Fonction de sauvegarde et de restauration..... | 72 |
| 6.1.9 Fonction de protection des sessions d'administration..... | 73 |
| 6.1.10 Autres fonctions de soutien..... | 74 |
| 6.2 Mesures d'assurance sécurité..... | 75 |
| 6.2.1 Mesures de l'environnement de développement..... | 75 |
| 6.2.2 Documentation des fonctions de sécurité..... | 76 |
| 6.2.3 Test des fonctions de sécurité..... | 76 |
| 6.2.4 Documentation d'exploitation..... | 77 |
| 6.2.5 Estimation de la vulnérabilité..... | 77 |
| 6.3 Argumentaire des spécifications abrégées de la TOE..... | 78 |
| 6.3.1 Satisfaction des exigences fonctionnelles de sécurité..... | 78 |
| 6.3.2 Satisfaction des exigences d'assurance sécurité..... | 79 |
| 7 ANNEXE A – DROITS D'ADMINISTRATION..... | 80 |
| 8 ANNEXE B – ATTAQUES PRISES EN COMPTE PAR L'ASQ..... | 81 |
| 9 ANNEXE C – IDENTIFICATION DES OPÉRATIONS EFFECTUÉES SUR LES EXIGENCES DE SÉCURITÉ DES TI..... | 85 |
| 9.1 Introduction..... | 85 |
| 9.2 Exigences de sécurité pour la TOE..... | 86 |
| 9.2.1 Exigences de contrôle des flux d'information..... | 86 |
| 9.2.2 Exigences de protection contre les attaques Internet..... | 93 |
| 9.2.3 Exigences de prévention de l'utilisation impropre..... | 95 |
| 9.2.4 Exigences de protection de la TOE..... | 97 |
| 9.2.5 Autres exigences de sécurité de soutien..... | 98 |
| 10 ANNEXE D – EXIGENCE DE SÉCURITÉ EXPLICITEMENT ÉNONCÉE..... | 101 |
| 10.1 Introduction..... | 101 |
| 10.2 FMT_MTD - Management of TSF data..... | 101 |
| 10.2.1 FMT_MTD.BRS – Backup and restoration of TSF data..... | 101 |



TABLE DES ILLUSTRATIONS

| | |
|---|----|
| ILLUSTRATION 1: CAS TYPIQUE D'UTILISATION DES COMPOSANTS DE LA TOE..... | 16 |
| ILLUSTRATION 2: COMPOSANTS ET INTERFACES DE LA TOE..... | 19 |
| ILLUSTRATION 3: PLATE-FORME DE TEST UTILISÉE LORS DE L'ÉVALUATION..... | 22 |
| ILLUSTRATION 4: SOUS-ENSEMBLES FONCTIONNELS DE LA TOE..... | 40 |
| ILLUSTRATION 5: PROTOCOLE ESP EN MODE TUNNELS..... | 67 |
| ILLUSTRATION 6: CONTENU D'UN DATAGRAMME ESP..... | 67 |



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

| | |
|--------------------------------------|---|
| <u>Titre</u> : | Cible de sécurité - Suite logicielle IPS-Firewall Version 8.1 |
| <u>Référence de la ST</u> : | NA_ASE_ciblesec_v8 |
| <u>Version de la ST</u> : | 1.7 |
| <u>Cible d'évaluation</u> : | Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ |
| <u>Version de la TOE</u> : | 8.1.3 (S, M, L, XL) |
| <u>Paquet d'assurance sécurité</u> : | 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 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 « EAL3 augmented ».

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

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 utilisateurs,
- 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 IPS-Firewalls 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 utilisateurs, 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, appelé Administration Suite, constitué des outils Firewall Manager, Firewall Monitor et Firewall Reporter. Tous ces outils comportent une interface graphique intuitive et conviviale sous plateforme Windows, 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 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.

1.4.3 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.
- [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, July 2003.
- [RTCP] *Real Time Control Protocol (RTCP) attribute in SDP*, RFC 3605, October 2003.
- [SSL] T. Dierks and C. Allen, *The TLS Protocol Version 1.0*, RFC 2246, January 1999.
- [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.
- [QSTD] *Processus de qualification d'un produit de sécurité - niveau standard*, version 1.2.

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

CEM Méthodologie 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.



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 d'IPS-Firewalls.

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 IPS-Firewall.

Règle implicite

Ensemble de règles automatiquement générées par l'IPS-Firewall 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

1°) Ensemble de datagrammes UDP associés à un même échange applicatif.

2°) 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 appliances firewall-VPN à travers des sessions sécurisées d'administration de la sécurité.

Super-administrateur

Administrateur disposant de droits complets sur la configuration des boîtiers appliances 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.

Table des utilisateurs authentifiés

Ensemble des **utilisateurs** authentifiés à un instant donné sur l'IPS-Firewall.

Tables de données

Ensemble des tables contenant des données (utilisateurs, interfaces, ...) qui sont nécessaires au bon fonctionnement de la TOE. Ces tables sont automatiquement renseignées par l'IPS-Firewall 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.



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, heure de la journée et jour de la semaine, identité de l'utilisateur, authentification préalable, etc.

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,
 - de l'identité déclarée par les utilisateurs, suite à une étape d'identification/authentification ;
- Limitation du débit de certains flux ;
- Imputabilité des flux aux entités les ayant suscités ;



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.

Par ailleurs, un attaquant capable d'écouter les flux entre un utilisateur légitime du réseau non maîtrisé et un service du réseau de confiance, puis de contrefaire des paquets IP, peut tenter d'usurper l'identité de cet utilisateur :

- soit en jouant ses données d'authentification si celles-ci sont constantes (ex : mot de passe réutilisable),



- soit en tentant de les deviner (au hasard ou par prédiction sur la base d'analyses cryptographiques) si celles-ci comportent des éléments diversifiants.

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.

Les tentatives d'usurpation de l'identité des utilisateurs autorisés sont contrées par la fourniture par le boîtier appliance firewall-VPN de **mécanismes d'authentification forte des utilisateurs** comme le défi / réponse basé sur le protocole SRP.

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**. 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 IPS-Firewall NETASQ**. 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 le package NETASQ Administration suite (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.

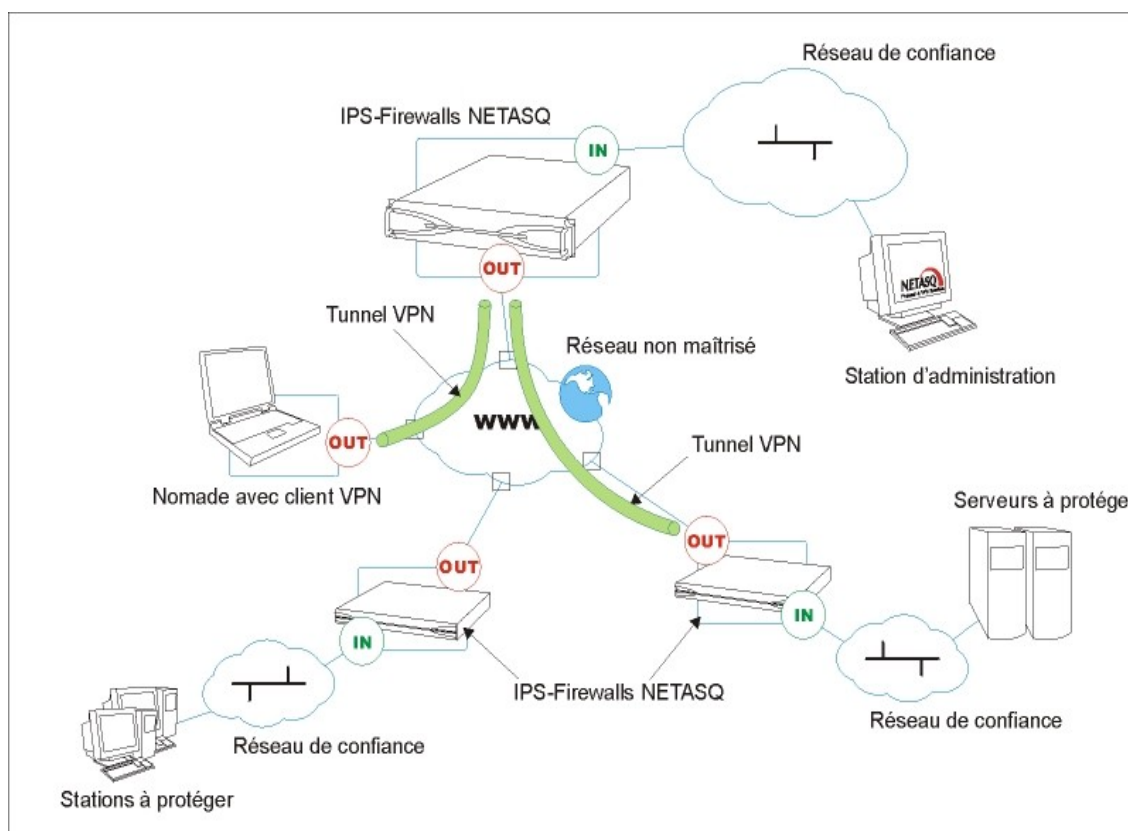


Illustration 1: Cas typique d'utilisation des composants de la TOE.

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 Caractéristiques minimales des plates-formes d'exploitation

Les boîtiers appliances firewall-VPN sont entièrement packagés par NETASQ. Ils sont développés autour du noyau FreeBSD 6.3, avec correctifs à jour, adapté et épuré par NETASQ.

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 :

- PC Pentium IV ou plus ;
- 512 Mo de RAM (1 Go conseillés) ;
- 200 Mo de disque dur ;
- Carte réseau Ethernet 10 ou 100 Mbps ;
- Windows Internet Explorer 6 ou plus ;
- Windows 2003 (SP2) ou XP (SP3).



2.3 Limites logiques de la TOE

2.3.1 Composants logiciels

Le logiciel à évaluer est constitué des composants suivants :

- Logiciel **IPS-Firewall** pour boîtier appliance firewall-VPN, aussi appelé **NS-BSD**, incluant le noyau FreeBSD 6.3 avec correctifs à jour, adapté et épuré par NETASQ,
- **NETASQ Unified 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.

Le logiciel **IPS-Firewall** (NS_BSD) dans les conditions d'évaluation utilise les composants « open-source » suivant avec leurs correctifs à jour:

- FreeBSD en version 6.3
- Ipssec-tools en version 0.7.3
- IPFilter en version 4.1.5
- OpenLDAP en version 2.3.43
- OpenSSL en version 1.0.0c
- Launchd en version 106.3
- Libevent en version 1.4.12

2.3.2 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.

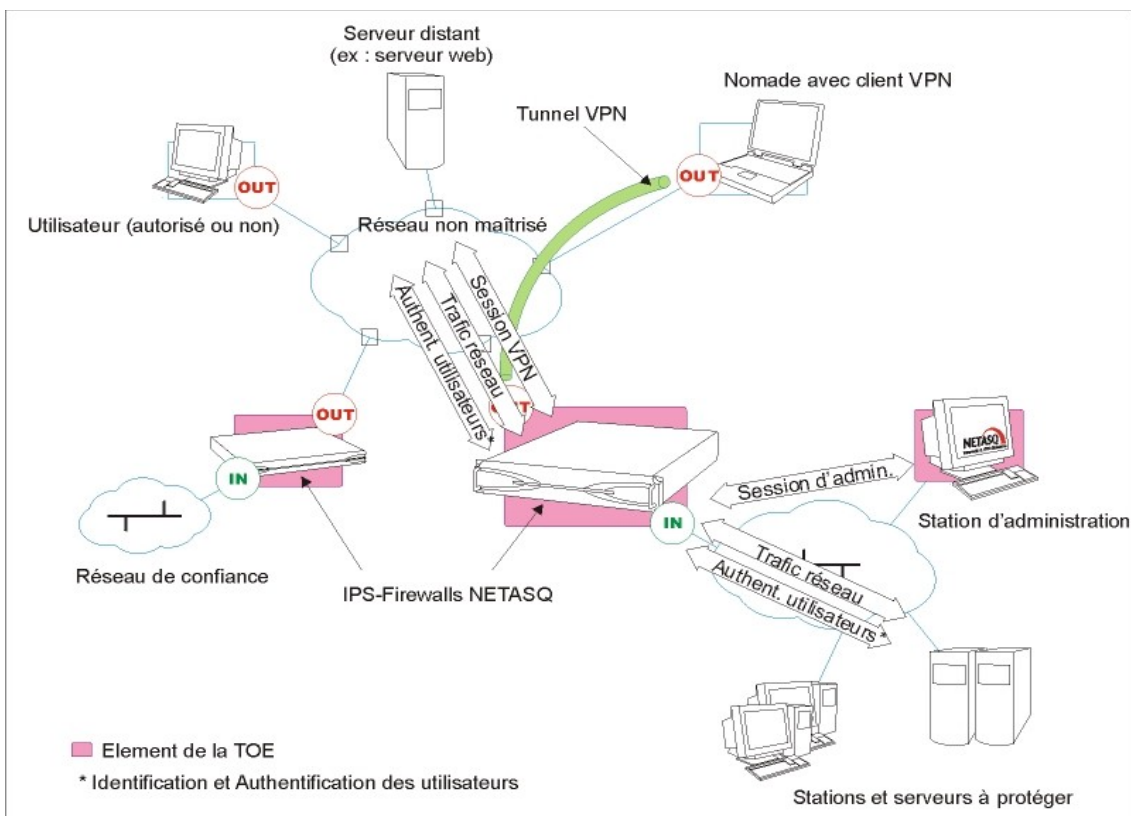


Illustration 2: Composants et interfaces de la TOE.



2.3.3 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 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 équiper ;
- Tous les administrateurs sont soumis à une étape identification / authentification utilisant le protocole SRP offert par la TOE ;
- Les méthodes d'authentification des utilisateurs sont également celles basées sur le protocole SRP offert par la TOE (Note: l'accès HTTPS est hors évaluation car n'apporte pas de niveau de sécurité supplémentaire vis-à-vis de SRP) ;
- La TOE est configurée de sorte que les utilisateurs ne puissent pas changer leurs mots de passe ;
- 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 rester¹. Il s'agit précisément :
 - des modules permettant la prise en charge des serveurs externes (ex : Kerberos, RADIUS...),
 - de l'infrastructure à clés publiques (PKI) interne,
 - du module VPN SSL,
 - des proxies HTTP, SMTP, POP3 et FTP,
 - du cache DNS,
 - du moteur antivirus (ClamAV ou Kaspersky),

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.



- du module Active Update,
 - des serveurs SSH, DHCP, MPD et SNMPD,
 - du client DHCP et du démon NTP,
 - de la programmation horaire des politiques de chiffrement et de filtrage ;
- Les utilisateurs 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, soit être stocké localement soit 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), SSL, SIP, MGCP, RTP, RTCP, RIP, DNS et SMB2 ;
 - L'utilisation de la translation d'adresses (*network address translation* ou *NAT*) est possible mais n'est pas considérée comme une fonction de sécurité.
 - L'utilisation du module Seismo (*détection de vulnérabilités*) est possible mais n'est pas considérée comme une fonction de sécurité.



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

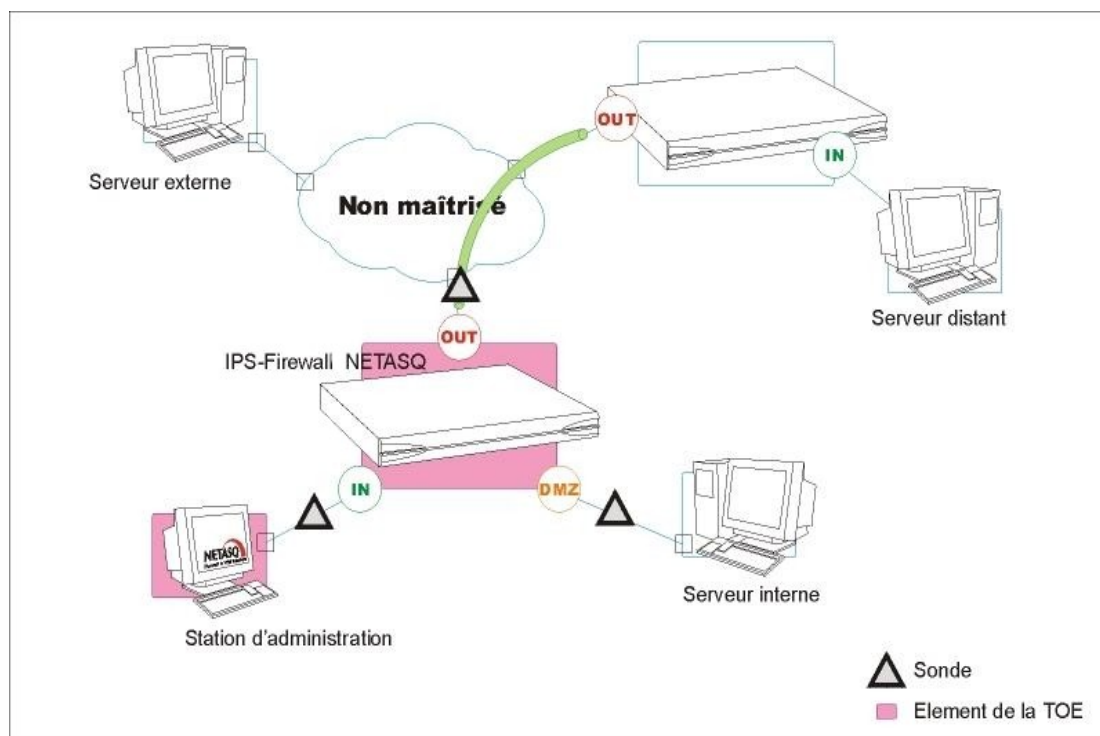


Illustration 3: Plate-forme de test utilisée lors de l'évaluation.

Les boîtiers appliances firewall-VPN sont un F200 et un U250.

Le système d'exploitation de la station d'administration à distance est Windows XP SP3.

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.



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 :

1. de ses caractéristiques au niveau IP (adresse source et destination, type de protocole IP) et transport (port source et destination TCP ou UDP),
2. de l'identité de l'utilisateur qui le suscite et de la réussite d'une étape d'authentification,

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.

M.UTIL_USURP

Une entité non-autorisée sur le réseau non maîtrisé parvient à accéder aux services réservés à un utilisateur soumis à une authentification obligatoire sur le réseau autorisé en usurpant son identité :

soit en rejouant une séquence d'authentification légitime basée sur des données réutilisables qu'elle a interceptée,

soit en devinant les données d'authentification de l'utilisateur suite à des tentatives aléatoires répétées, ou par le biais d'analyses de séquences d'authentification interceptées.

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 et des utilisateurs 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 utilisateurs et des administrateurs 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.).

Il est de la responsabilité des administrateurs de sensibiliser tous les utilisateurs à ces bonnes pratiques.

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 **Objectifs** de sécurité pour la TOE ont des noms commençant par le préfixe **O**.
- Les **Objectifs** de sécurité pour l'**Environnement** 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,
- 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,
- Éventuellement : identité de l'utilisateur associée à l'adresse IP source.

Argumentaire : O.PCFI_FILTRAGE est principalement dédié à la satisfaction de la politique P.FILTRAGE. Il couvre le filtrage en fonction des caractéristiques IP et transport (P.FILTRAGE.1) et de l'identité de l'utilisateur (P.FILTRAGE.2) spécifiée par cette politique.

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 les aspects « filtrage en fonction des caractéristiques IP et transport » (point 1) de 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_I&A_UTIL

La TOE doit permettre d'exiger que les utilisateurs soient identifiés et authentifiés avant de leur accorder l'accès à certains services qui leur sont autorisés.

Argumentaire : O.PCFI_I&A_UTIL est principalement dédié à la satisfaction de la politique P.FILTRAGE. Il couvre les exigences d'identification obligatoire et de réussite à l'étape d'authentification (P.FILTRAGE.2) de cette politique. Il est également dédié à la prévention de la menace M.UTIL_USURP. D'autre part, O.PCFI_I&A_UTIL rend difficiles les attaques utilisant l'IP spoofing (M.IP_USURP) car il permet d'imposer aux attaquants d'usurper l'identité d'un utilisateur et non celle d'un équipement, pour enfreindre la politique de contrôle des flux d'information, ce qui revient à réaliser la menace M.UTIL_USURP.

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 et O.PCFI_I&A_UTIL pour les cas où la mise en place d'une politique de chiffrement n'est pas réalisable pour contrer cette menace.

De même, dans le cas où l'établissement des sessions VPN permet de garantir l'identité des utilisateurs (par opposition à celle des équipements), cet objectif permet de contrer M.UTIL_USURP.

O.JAA_PCFI²

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.

O.RESIST_AUTH_UTIL

La TOE doit fournir des mécanismes d'authentification qui empêchent que la réutilisation de données provenant de l'authentification d'utilisateurs autorisés et/ou la contrefaçon de données d'authentification permette à un attaquant d'usurper l'identité d'un utilisateur autorisé.

Argumentaire : O.RESIST_AUTH_UTIL est dédié à la prévention de la menace M.UTIL_USURP. Dans le cas où l'exigence d'identification / authentification des utilisateurs est la stratégie sélectionnée pour contrer les attaques basées sur l'usurpation d'adresse IP, cet objectif soutient également O.PCFI_I&A_UTIL pour contrer M.IP_USURP.



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_ILLCITE.

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_ILLCITE.

O.PROTECT_SESSIONS_ADMIN

La TOE doit 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_ILLCITE, qui est un pré requis possible pour la réalisation de M.ADMIN_ILLCITE.



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_ILLCITE. 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 :

- *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.*
- *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_ILLCITE.*
- *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_ILLCITE.*

OE.MOT_PASSE

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

Argumentaire : Cet objectif de sécurité soutient O.PCFI_I&A_UTIL pour satisfaire P.FILTRAGE.2 en garantissant qu'on ne peut pas circonvenir à la fonction d'identification / authentification des utilisateurs en obtenant le mot de passe d'un utilisateur autorisé. De la même manière, cet objectif de sécurité soutient O.PCAOA_I&A_ADMIN pour contrer M.MAUVAIS_USAGE et M.ADMIN_ILLCITE.

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 contre 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_ILLCITE. 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_ILLCITE.

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.UTIL_USURP | M.MAUVAIS_USAGE | P.SAUVEGARDE_RESTAURATION | M.ADMIN_ILLICITE | M.ADMIN_USURP | M.SESSION_ADMIN_ILLICITE | M.PERTE_AUDIT |
|----------------------------|-------------------------|--------------------------|-------|----------------|-----------|------------|--------------|-----------------|---------------------------|------------------|---------------|--------------------------|---------------|
| | 1 : caractéristiques IP | 2 : identité utilisateur | | | | | | | | | | | |
| O.PCFI_FILTRAGE | X | X | | | | | | | | | | | |
| O.PCFI_CONTEXTE_APPLICATIF | S | | | | | | | | | | | | |
| O.PCFI_I&A_UTIL | | X | | | | X | X | | | | | | |
| O.PCFI_CHIFFREMENT | | | X | | | X | X | | | | | | |
| O.JAA_PCFI | | | | X | | | | | | | | | |
| O.IPS_DETECTION_ATTAQUES | | | | | X | X | | | | | | | |
| O.IPS_CONFORMITE_RFC | | | | | X | | | | | | | | |
| O.JAA_IPS | | | X | | S | S | | | | | | | |
| O.RESIST_AUTH_UTIL | | | | | | S | X | | | | | | |
| 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_BOITIERES | | | | | | | | | | X | | | |
| OE.SUPER_ADMIN | 1 | S | S | S | S | S | S | S | S | S | S | S | S |
| | 2 | | | | | | | S | | S | | | |
| | 3 | | | | | | | | | S | | | |
| OE.MOT_PASSE | | S | | | | | | S | | S | | | |
| OE.BONNE_PCFI | | | | | | | | X | | | | | |
| OE.PERSONNEL | | | | | | | | X | | | | | |
| OE.COUPURE | | S | S | S | S | S | S | | | | | | |
| OE.USAGE_STRICT | | S | S | S | S | S | S | | | X | | | |
| OE.AUTONOME | | S | 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 :

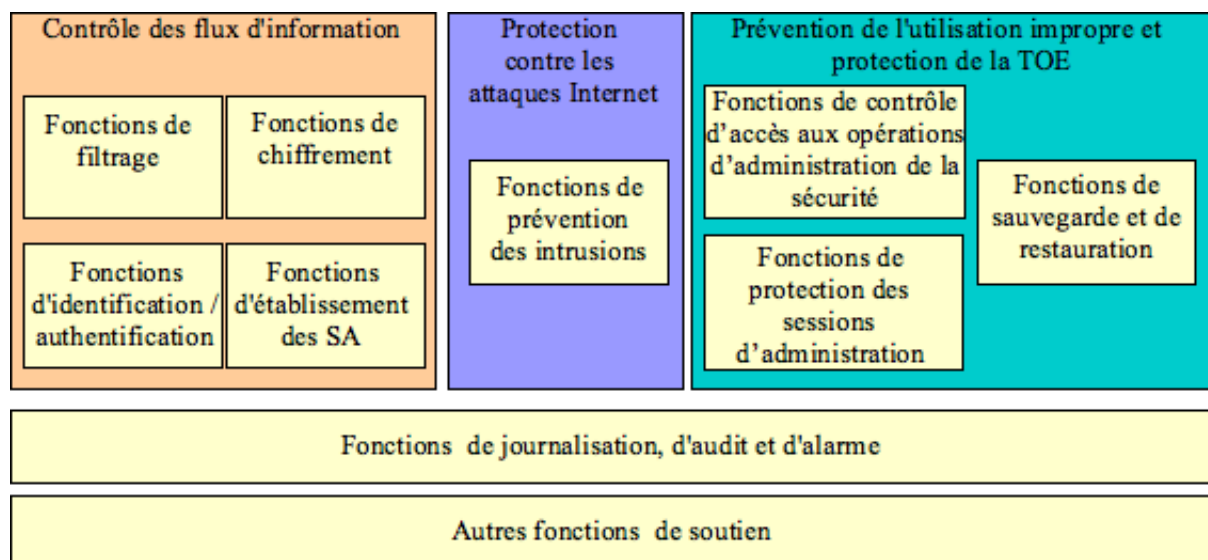


Illustration 4: Sous-ensembles fonctionnels de la TOE.



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:
FCC_FFF.composant.<itération.>n
 - *FCC* 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'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 ;
- Si l'utilisateur s'est préalablement identifié et authentifié, l'identité déclarée par l'utilisateur.

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 et servent également à construire les échéanciers de programmation horaire de la fonction de filtrage.

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. 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) 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;
- (critère) L'authentification des utilisateurs et éventuellement l'utilisateur ou le groupe d'utilisateurs autorisés 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

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



- Le fait que l'utilisateur soit autorisé à s'authentifier (on peut révoquer un utilisateur sans supprimer son compte);
- Le mécanisme d'authentification³ ;
- Le mot de passe de référence.

Table des utilisateurs authentifiés

- Le nom de login de l'utilisateur ;
- L'adresse IP de la machine depuis laquelle il s'est authentifié ;
- La durée restante avant que l'authentification n'expire.

Paramètres des tunnels VPN

Un tunnel VPN consiste en un chemin de confiance (la SA ISAKMP) entre l'IPS-Firewall 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);
- En cas d'authentification par certificat : le certificat X509 présenté par l'IPS-Firewall;
- En cas d'authentification par clé pré-partagée : l'adresse IP de l'IPS-Firewall;
- 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 ;

3 Obligatoirement SRP dans le mode d'utilisation soumis à l'évaluation.



- (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 l'IPS-Firewall

- 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.

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

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.

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'adresse IP source et destination du paquet et, partant de là, la machine source et la machine destination du paquet,**
- c. **Le numéro de protocole IP,**
- d. **La valeur du champ DSCP,**
- e. **Si le protocole est TCP ou UDP : le port source et destination,**
- f. **Si le protocole est ICMP : les champs 'type' et 'code' du message ,**
- g. **Si l'adresse IP source est associée à un utilisateur dans la table des utilisateurs authentifiés : l'identité de l'utilisateur.**

[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'authentification des utilisateurs,**
 - iii. **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.

Enfin, l'objectif O.PCFI_I&A_UTIL est satisfait en spécifiant, pour la ou les machines et les services sur lesquelles porte l'exigence d'identification / authentification, une règle 'passer' couvrant les utilisateurs authentifiés, suivie d'une règle 'bloquer' ou 'réinitialiser' de portée identique mais ne couvrant pas les utilisateurs authentifiés. Si l'utilisateur ne s'authentifie pas, c'est cette dernière règle qui s'appliquera, restreignant ainsi l'accès au service aux utilisateurs s'étant authentifiés et couverts par la première règle.

Fonction d'identification / authentification

FIA_UID.2 – Identification de l'utilisateur en vue de l'application de la politique de filtrage

[FIA_UID.2.1]

La fonction d'identification / authentification doit exiger que chaque utilisateur soit identifié avec succès avant de **pouvoir l'ajouter à la table des utilisateurs authentifiés.**

Argumentaire : FIA_UID.2 est dédié à la satisfaction de l'objectif O.PCFI_I&A_UTIL.



FIA_UAU.2 – Authentification de l'utilisateur en vue de l'application de la politique de filtrage

[FIA_UAU.2.1]

La fonction d'identification / authentification doit exiger que chaque utilisateur soit authentifié avec succès avant de **l'ajouter à la table des utilisateurs authentifiés**.

Argumentaire : FIA_UAU.2 est dédié à la satisfaction de l'objectif O.PCFI_I&A_UTIL.

FIA_UAU.5.Utilisateur – Mécanisme d'authentification des utilisateurs

[FIA_UAU.5.Utilisateur.1]

La fonction d'identification / authentification doit fournir **le mécanisme basé sur le protocole SRP** pour contribuer à l'authentification de l'utilisateur.

[FIA_UAU.5.Utilisateur.2]

La fonction d'identification / authentification doit authentifier l'identité annoncée de tout utilisateur selon **le protocole SRP**.

Argumentaire : FIA_UAU.5.Utilisateur soutient FIA_UID.2 et FIA_UAU.2 pour satisfaire l'objectif O.PCFI_I&A_UTIL. La résistance des mécanismes associés au protocole SRP permet de satisfaire l'objectif O.RESIST_AUTH_UTIL : 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 de vérification du mot de passe, cf. [SRP]).

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_UFF.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 négociation 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.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 et la fonction d'identification /d'authentification sont appliquées 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 l'**IPS-Firewall** 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 l'**IPS-Firewall** 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 ISAKMP et IPSec** lors de l'établissement des tunnels VPN entre l'**IPS-Firewall** 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 l'IPS-Firewall 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'IPS-Firewall 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 auditable suivants :

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

et les événements auditable 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, et identité de l'utilisateur (si elle est connue),

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. | <ul style="list-style-type: none">▪ Nom de l'interface de réception,▪ Action appliquée,▪ Identifiant de la règle,▪ Type de protocole,▪ Type ICMP,▪ Port source,▪ Adresse IP et port destination. |
| FIA_ UAU.2 | Tentative d'authentification. | <ul style="list-style-type: none">▪ Si échec : la raison de l'échec. |
| FTP_ TRP.1.Corresp et FPT_ TDC.1 | Tentative d'établissement de SA ISAKMP et IPSec. | <ul style="list-style-type: none">▪ 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 | <ul style="list-style-type: none">▪ 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) | <ul style="list-style-type: none">▪ 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 l'IPS-Firewall.

FAU_GEN.2 – Identification de l'utilisateur

[FAU_GEN.2.1]

Pour tout événement 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 événement.

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 : l’IPS-Firewall ne s’arrête pas réellement mais il bloque l’ensemble des flux excepté les sessions d’administration du Firewall Manager depuis le réseau interne.

si un fichier de trace dépasse le nombre d’éléments à journaliser suivant :

- a. build S : Pas de stockage local
- b. build M : 256
- c. build L : 512
- d. build XL : 1024

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 intrusionsFAU_SAA.4 – Heuristiques des attaques complexes

[FAU_SAA.4.1]

La fonction de prévention des intrusions doit pouvoir maintenir une base de connaissance⁴ 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,

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



- 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.

[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 capable 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**, la 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 :

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

La fonction de protection des sessions d'administration

La fonction d'audit



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 d'identification / authentification | Activer / désactiver : *+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** :

| <i>Données de sécurité</i> | <i>Opérations / droits nécessaires</i> |
|--|--|
| Caractéristiques des utilisateurs | Consulter : tous les administrateurs Modifier : U+M |
| Attribution du rôle administrateur et de droits administratifs à un utilisateur | Consulter : tous les administrateurs Modifier : uniquement par le super-administrateur. |
| 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 restaurationFMT_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** sauvees sur **le disque dur de la station d'administration**.

Argumentaire : FMT_MTD.BRS est dédié à la satisfaction de l'objectif O.SAUEGARDE_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 l'IPS-Firewall 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 :

l'authentification mutuelle initiale de l'administrateur et de l'IPS-Firewall,

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 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.

Argumentaire : FIA_UAU.5.Admin soutient FTP_TRP.1.Admin pour satisfaire l'objectif O.PCAOA_I&A_ADMIN. La résistance des mécanismes associés au protocole SRP permet de satisfaire l'objectif O.RESIST_AUTH_ADMIN : 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]).



5.2.5 Autres exigences de sécurité de soutien

Autres fonctions de soutien

FCS_COP.1 – Fonction cryptographique

[FCS_COP.1.1]

La fonction cryptographique doit effectuer les opérations cryptographiques du tableau ci-dessous 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**.

| Opération cryptographique | Algorithme | Taille des clés | Réf. du standard | Exigences soutenues |
|--|----------------|------------------|--------------------------------|--|
| Signature et élaboration de clés | Diffie-Hellman | 2048, 3072, 4096 | [DH], [IKE], [IKE-MODP], [SRP] | FIA_UAU.5.Utilisateur, FIA_UAU.5.Admin, FIA_UAU.5.Corresp. |
| Chiffrement / déchiffrement asymétrique | RSA | 2048, 4096 | [RSA] | FIA_UAU.5.Corresp (X509) |
| Hachage univoque | 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 |
| Chiffrement / déchiffrement symétrique des paquets VPN | AES | 128, 192, 256 | [AES] | FTP_TRP.1.Corresp, FDP_UCT.1 |
| | Triple DES | 168 | [DES] | |
| | Blowfish | 128 à 256 | [Blowfish] | |
| | CAST | 128 | [CAST] | |
| Chiffrement / déchiffrement symétrique des sessions d'administration | AES | 128 | [AES] | FPT_ITT.1 |
| Contrôle d'intégrité des sessions d'administration. | 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 de l'IPS-Firewall 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 9.2.5 présente les opérations sur ces exigences.

Ces exigences d'assurance sécurité ont été sélectionnées d'une part pour leur appartenance au paquet des exigences d'assurance de la qualification standard (EAL3 + ALC_FLR.3 et AVA_VAN.3) et d'autre part parce que le développeur est capable d'atteindre les exigences d'assurances ALC_CMC.4 et ALC_CMS.4 améliorant ainsi la maîtrise de la TOE dans le processus de développement.

5.3.1 Mesures d'assurance sur la cible de sécurité (ASE)

ASE_CCL.1 – Annonces de conformité

Cf. [CC-03], § 11.2, p. 66.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ASE_ECD.1 – Définition de composants étendus

Cf. [CC-03], § 11.5, p. 71.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ASE_INT.1 – Introduction de la cible de sécurité

Cf. [CC-03], § 11.1, p. 65.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ASE_OBJ.2 – Objectifs de sécurité

Cf. [CC-03], § 11.4, p. 69.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ASE_REQ.2 – Exigences de sécurité déduites

Cf. [CC-03], § 11.6, p. 72.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ASE_SPD.1 – Définition du problème de sécurité

Cf. [CC-03], § 11.3, p. 68.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ASE_TSS.1 – Spécifications abrégées de la TOE

Cf. [CC-03], § 11.7, p. 74.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.



5.3.2 Autres mesures d'assurance sécurité

ADV_ARC.1 – Description de l'architecture de sécurité

Cf. [CC-03], § 12.1, p. 85.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ADV_FSP.3 – Spécifications fonctionnelles avec résumé exhaustif

Cf. [CC-03], § 12.2, p. 91.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ADV_TDS.2 – Conception de haut niveau - identification des sous-systèmes dédiés à la sécurité

Cf. [CC-03], § 12.6, p. 110.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

AGD_OPE.1 – Guides opérationnels

Cf. [CC-03], § 13.1, p. 117-119.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

AGD_PRE.1 – Guides de préparation

Cf. [CC-03], § 13.2, p. 120-121.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ATE_COV.2 – Analyse de la couverture des tests

Cf. [CC-03], § 15.1, p. 153-154.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ATE_DPT.1 – Tests: conception simple

Cf. [CC-03], § 15.2, p. 156-157.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ATE_FUN.1 – Tests fonctionnels

Cf. [CC-03], § 15.3, p. 160-161.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ATE_IND.2 – Tests indépendants - échantillonnage

Cf. [CC-03], § 15.4, p. 165-166.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.



AVA_VAN.3 – Analyse de vulnérabilités

Cf. [CC-03], § 16.1, p. 169.

Argumentaire : ce composant est dédié à la satisfaction du package QS.

ALC_CMC.4 – Gestion de configuration avec procédures d'acceptation des modifications et de la génération de la TOE

Cf. [CC-03], § 14.1, p. 128-129.

Argumentaire : ce composant est dédié à la satisfaction d'une certification supérieure à la qualification standard (QS). Le développeur dispose d'un environnement permettant d'autres certifications au niveau EAL4+ comprenant le composant ALC_CMC.4 . Cela explique le choix de l'augmentation ALC_CMC.4.

ALC_CMS.4 – Gestion en configuration de la remontée d'erreurs

Cf. [CC-03], § 14.2, p. 135-136.

Argumentaire : ce composant est dédié à la satisfaction d'une certification supérieure à la qualification standard (QS). Le développeur dispose d'un environnement permettant d'autres certifications au niveau EAL4+ comprenant le composant ALC_CMS.4 . Cela explique le choix de l'augmentation ALC_CMS.4.

ALC_DEL.1 - Procédures de livraison

Cf. [CC-03], § 14.3, p. 138.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ALC_FLR.3 – Correction d'anomalies systématique

Cf. [CC-03], § 14.5, p. 143-144.

Argumentaire : ce composant est dédié à la satisfaction du package QS.

ALC_DVS.1 – Identification des mesures de sécurité

Cf. [CC-03], § 14.4, p. 139-140.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

ALC_LCD.1 – Modèle de cycle de vie défini par le développeur

Cf. [CC-03], § 14.6, p. 147.

Argumentaire : ce composant est dédié à la satisfaction du package EAL3.

5.4 Exigences de sécurité pour l'environnement TI

Aucune exigence de sécurité n'est spécifiée pour l'environnement TI.



5.5 Argumentaire des exigences de sécurité

5.5.1 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_I&A_UTIL | O.PCFI_CONTEXTE_APPLICATIF | O.PCFI_CHIFFREMENT | O.JAA_PCFI | O.IPS_DETECTION_ATTAKUES | O.IPS_CONFORMITE_RFC | O.JAA_IPS | O.RESIST_AUTH_UTIL | 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 | X | | | | | | | | | | | | | |
| FIA_UID.2 | | X | | | | | | | | | | | | | | |
| FIA_UAU.2 | | X | | | | | | | | | | | | | | |
| FIA_UAU.5.Utilisateur | | S | | | | | | 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 | | S | | S | | | | | S | | S | | | S | | S |
| FPT_STM.1 | | | | | S | | | S | | | | S | | | | |



5.5.2 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.

5.5.3 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. |
| FIA UID.2 | Aucune | |
| FIA UAU.2 | FIA UID.1 | FIA UID.2 |
| FIA UAU.5.Utilisateur | 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 | Satisfaite par FIA UID.2 |
| FAU SAR.1 | FAU GEN.1 | Oui. |
| FAU_STG.3 | FAU_STG.1 | Satisfaite par FMT_MTD.1 (fichiers de trace des événements de sécurité) |
| FAU_ARP.1.Alarmes | FAU_SAA.1 | .Non applicable: FAU_ARP.1.Alarmes traite déjà des violations de SFR. |
| FAU_SAA.4 | Aucune | |
| FAU_ARP.1.IPS | FAU_SAA.1 | FAU_SAA.4 |
| FMT_SMR.1 | FIA UID.1 | Satisfaite par FTP_TRP.1.Admin |
| | | FMT_MOF.1 |
| | | FMT_MTD.1 |
| FDP_ACC.2 | FDP_ACF.1 | Satisfaite par FMT_MOF.1 et FMT_MTD.1 |
| 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 | |



| Composant | Dépendances | Satisfaction |
|--|--------------------------------------|---|
| FTP TRP.1.Admin | Aucune | |
| FIA UAU.5.Admin | Aucune | |
| FCS_COP.1 Signature et élaboration de clé | FDP_ITC.1 FDP_ITC.2 FCS_CKM.1 | Non applicable : l'opération <u>est</u> 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 Chiffrement / déchiffrement asymétrique | 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 l'IPS-Firewall par l'administrateur. |
| | FCS_CKM.4 | Non applicable car en dehors de la portée de la TOE |
| FCS_COP.1 Hachage univoque | FDP_ITC.1 FDP_ITC.2 FCS_CKM.1 | Satisfaite par FCS_COP.1.a |
| | 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 / déchiffrement symétrique des paquets VPN | FDP_ITC.1 FDP_ITC.2 FCS_CKM.1 | Satisfaite par FCS_COP.1.a |
| | 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 / déchiffrement symétrique des sessions d'administration | FDP_ITC.1 FDP_ITC.2 FCS_CKM.1 | Satisfaite par FCS_COP.1.a |
| | 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 Contrôle d'intégrité des sessions d'administration. | FDP_ITC.1 FDP_ITC.2 FCS_CKM.1 | Satisfaite par FCS_COP.1.a |
| | 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. |
| FPT STM.1 | Aucune | |

5.5.4 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 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 ;
- L'utilisateur ou le groupe d'utilisateurs autorisés 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. En ce qui concerne l'utilisateur ou le groupe d'utilisateurs autorisés par la règle, à partir du moment où un utilisateur s'est identifié et authentifié avec succès à partir d'une machine donnée, l'IPS-Firewall note ce fait et attribue le nom de login de cet utilisateur à tous les paquets IP présentant l'adresse de cette machine comme adresse IP source (cf. fonction d'identification / authentification, §6.1.2). En conséquence, les règles qui spécifient l'authentification des utilisateurs, même sans préciser de contraintes sur les utilisateurs autorisés, ne peuvent s'appliquer qu'à des paquets IP émis d'une machine à partir de laquelle un utilisateur s'est préalablement authentifié.

Chaque règle de filtrage peut spécifier une action de contrôle et une action de journalisation. Cette dernière est décrite au §6.1.5 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 règles 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), l'IPS-Firewall 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, l'authentification des utilisateurs 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 d'identification / authentification

La fonction d'identification / authentification permet à l'utilisateur de déclarer son login (identification) et de vérifier que cet utilisateur est bien la personne qu'il prétend être, par la fourniture d'éléments qu'il est censé être le seul à pouvoir fournir (authentification). Une fois l'authentification réussie, le login de l'utilisateur est attribué, à travers la table des utilisateurs authentifiés, à la machine à partir de laquelle celui-ci s'est identifié et à tous les paquets IP qui en proviennent (cf. Authentification des administrateurs et élaboration de la clé de chiffrement par le protocole SRP au §), et ce pour une durée spécifiée par l'utilisateur. L'utilisateur peut également se retirer manuellement de la table des utilisateurs authentifiés avant cette échéance.

Le mode d'utilisation soumis à l'évaluation impose le recours au protocole SRP pour l'authentification des utilisateurs. Ce protocole sans divulgation de mot de passe est résistant aussi bien aux attaques d'écoute passive qu'aux attaques actives basées sur la modification ou l'insertion de paquets dans la séquence d'authentification. Il utilise un mot de passe réutilisable fourni par l'utilisateur, et conserve ses propriétés de résistance aux attaques même lorsque l'entropie du mot de passe est basse. Il fait l'objet de la RFC 2945 [SRP].

Concrètement, l'IPS-Firewall fournit, à travers des capacités de type 'serveur HTTP', des formulaires Web qui permettent de s'identifier, de s'authentifier en spécifiant la durée de la session, et de fermer la session manuellement. Il n'est pas nécessaire que la session HTTP persiste pour que la session reste active. Les étapes du protocole SRP sont effectuées par une applet Java téléchargée depuis l'IPS-Firewall sur le poste de l'utilisateur. Cette applet se sert du mot de passe fourni par l'utilisateur pour mener les étapes du protocole SRP.



Le protocole SRP est décrit plus en détail au §6.1.9 (remplacer 'administrateur' par 'utilisateur' et 'outil' par 'applet'). À la différence de la fonction de protection des sessions d'administration, l'utilisation du protocole SRP pour authentifier les utilisateurs ne sert pas à élaborer une clé de session dans le cadre d'un chemin de confiance.

Argumentaire : la fonction d'identification / authentification satisfait FIA_UID.2 et FIA_UAU.2.

L'utilisation du protocole SRP satisfait FIA_UAU.5.Utilisateur.

L'utilisation de l'algorithme Diffie-Hellman dans le cadre du protocole SRP satisfait FCS_COP.1.1.a concernant la partie de cette exigence qui soutient FIA_UAU.5.Utilisateur.

6.1.3 Fonction de chiffrement

La fonction de chiffrement de l'IPS-firewall 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 IPS-firewall), possédant des fonctionnalités homologues.

Les algorithmes d'authentification supportés par l'IPS-Firewall sont : HMAC-SHA1 (160 bits) et HMAC-SHA2 (256, 384, 512 bits).

Les algorithmes de chiffrement supportés par l'IPS-Firewall sont : AES (128, 192 ou 256 bits), Triple-DES (168 bits), Blowfish (128 à 256 bits) et CAST (128 bits).

L'IPS-firewall 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.

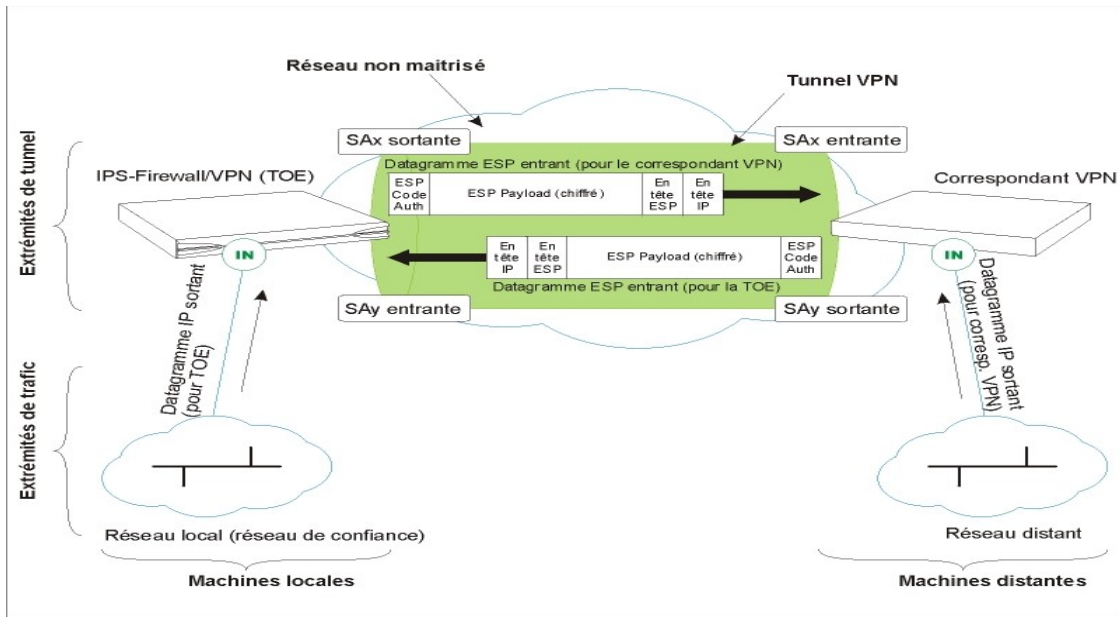


Illustration 5: Protocole ESP en mode tunnels.

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.

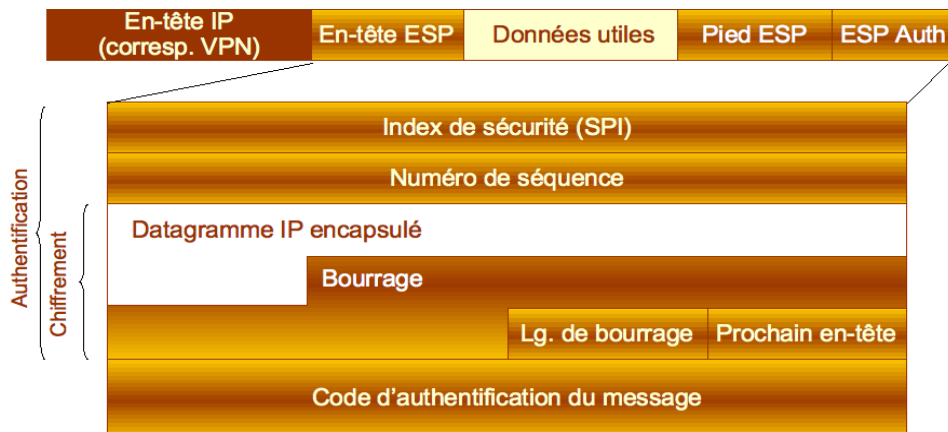


Illustration 6: Contenu d'un datagramme ESP.

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, l'IPS-Firewall 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 chiffrement⁵ 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_UFF.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.1.1.c 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.1.1.d qui soutient FDP_UCT.1.

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.



6.1.4 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].

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, l'IPS-Firewall 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 §) 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.1.1.a 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.1.1.c 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.1.1.c 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.1.1.d 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.

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 soit des certificats X509 telle que définie sur la phase 1 du protocole IKE [IKE].



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 |
|-----------------|---|--|
| 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. |

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.1.1.a concernant la partie de cette exigence qui soutient FIA_UAU.5.Corresp.

En mode X509, l'utilisation de l'algorithme RSA satisfait FCS_COP.1.1.b.

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.1.1.c 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.1.1.c 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.1.1.d qui soutient FTP_TRP.1.Corresp.1.

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

Fonction de journalisation

L'IPS-Firewall 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, L'IPS-Firewall 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 ;

Authentification : événements liés à l'authentification des utilisateurs ;

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 de l'IPS-Firewall, 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, l'IPS-Firewall 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 Firewall 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 satisfait FAU_ARP.1.Alarmes.

6.1.6 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).

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

Afin d'autoriser l'accès de l'IPS-Firewall 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 l'IPS-Firewall 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 : Rappel : dans le mode d'utilisation qui fait l'objet de l'évaluation, le super-administrateur n'est pas censé se connecter sur l'IPS-Firewall 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.



6.1.8 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 de l'IPS-Firewall (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.

6.1.9 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 NETASQ (Firewall Manager, Firewall Monitor, Firewall Reporter) et l'IPS-Firewall 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 de la clé de session établie suite à l'authentification SRP de l'administrateur.

Argumentaire : le chiffrement en AES 128 bits des sessions d'administration satisfait FPT_ITT.1 et FCS_COP.1.1.e. Le contrôle d'intégrité par HMAC-SHA1 160 bits satisfait FPT_ITT.1 et FCS_COP.1.1.f. 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 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 Firewall Manager) et à un « serveur » (l'IPS-Firewall) 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, l'IPS-Firewall 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 l'IPS-Firewall. Notez que même si la valeur de vérification est une « clé publique » au sens Diffie-Hellman du terme, il est nécessaire que l'IPS-Firewall 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 l'IPS-Firewall 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 l'IPS-Firewall 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.1.1.a concernant la partie de cette exigence qui soutient FIA_UAU.5.Admin.

6.1.10 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.



6.2 Mesures d'assurance sécurité

6.2.1 Mesures de l'environnement de développement

Méthodes et outils de gestion de configuration

Le système de gestion de configuration couvre la gestion et le contrôle du développement, de la production et de la maintenance de la suite logicielle IPS-Firewall. Son application permet d'affecter un identifiant unique à chaque version de la TOE et d'établir une liste des versions des composants qui constituent une version donnée.

Le commanditaire documente les procédures du système de gestion de configuration et fournit une liste de configuration pour chaque version de la TOE présentée.

L'évaluateur évalue la documentation et contrôle, sur les versions de la TOE qui lui sont livrées par le commanditaire, que le système de gestion de configuration est bien appliqué tel que décrit dans la documentation (pas d'audit de l'environnement de développement sous ce critère).

Argumentaire : ces procédures satisfont aux exigences ALC_CMC.4 et ALC_CMS.4

Sécurité de l'environnement de développement

Les mesures de sécurité appliquées pour le développement et la maintenance de la suite logicielle IPS-Firewall garantissent l'intégrité du code exécutable de la TOE et la confidentialité des documents de développement associés.

Le commanditaire documente les mesures de sécurité de l'environnement de développement en identifiant précisément le périmètre de cet environnement, et fournit des traces de l'application de ces mesures.

L'évaluateur évalue la documentation et procède à un audit de l'environnement afin de vérifier et d'apprécier l'application des mesures, et d'interviewer les personnels concernés sur leur connaissance des mesures.

Argumentaire : ces procédures satisfont à l'exigence ALC_DVS.1.

Procédures de livraison

Les procédures et mesures mises en place pour transférer la suite logicielle IPS-Firewall du développeur chez l'utilisateur final garantissent l'authenticité et l'intégrité de la TOE lors du transfert.

Le commanditaire documente les procédures de livraison.

L'évaluateur évalue la documentation et procède à un audit de l'environnement afin de vérifier et d'apprécier l'application des mesures, et d'interviewer les personnels concernés sur leur connaissance des mesures.

Argumentaire : ces procédures satisfont à l'exigence ALC_DEL.1.

Procédures de correction des anomalies

Des procédures de correction des anomalies sont mises en place au niveau du laboratoire et du service support pour assurer une gestion et un contrôle des anomalies de sécurité découvertes en interne ou soumises par les exploitants, ainsi que la distribution des correctifs associés, une fois les anomalies résolues.



Le commanditaire documente les procédures visant à la correction des anomalies, et fournit les documents donnant des lignes directrices aux exploitants pour lui soumettre les anomalies.

L'évaluateur évalue la documentation (pas d'audit de l'environnement de développement sous ce critère).

Argumentaire : ces procédures satisfont à l'exigence ALC_FLR.3.

Cycle de vie produit

Des procédures de cycle de vie produit sont mises en place au niveau du laboratoire, du support technique et du service de marketing produit pour assurer une maintenance et un suivi de l'évolution des produits tout au long de leur vie.

Le commanditaire documente les procédures définissant le cycle de vie de ses produits réalisés, en particulier la maintenance de ceux-ci.

L'évaluateur évalue la documentation (pas d'audit de l'environnement de développement sous ce critère).

Argumentaire : ces procédures satisfont à l'exigence ALC_LCD.1.

6.2.2 Documentation des fonctions de sécurité

Le commanditaire fournit les documents permettant d'assurer un niveau de qualité compatible avec les exigences liées au paquet d'assurance sécurité : spécifications fonctionnelles, conception de haut niveau et architecture de sécurité. Ces documents forment les niveaux successifs de représentation de la fonctionnalité de sécurité.

Des correspondances entre ces niveaux sont établies, en commençant par les fonctions de sécurité des TI spécifiées de manière abrégée dans ce document (§6.1).

L'évaluateur évalue la documentation, et vérifie que les exigences fonctionnelles de sécurité du §5.2 se reflètent bien dans les différents niveaux de représentation de la fonctionnalité de sécurité.

Argumentaire : ces mesures satisfont aux exigences ADV_ARC.1, ADV_FSP.3, ADV_TDS.2.

6.2.3 Test des fonctions de sécurité

Procédures de test du développeur

Le commanditaire fournit les documents produits à l'occasion des tests qu'il a effectués sur la TOE. Ces documents doivent décrire le plan et les procédures de tests suivies et montrer le degré de couverture des spécifications fonctionnelles par les tests. Ils doivent inclure les résultats effectifs des tests et démontrer que les fonctions de sécurité se comportent bien de la manière spécifiée dans les spécifications fonctionnelles.

Le commanditaire met également à disposition de l'évaluateur une TOE se prêtant au repassage des tests qu'il a effectués sur la TOE.

L'évaluateur évalue la documentation et repasse une partie des tests du développeur.

Argumentaire : ces procédures satisfont aux exigences ATE_COV.2, ATE_DPT.1, ATE_FUN.1 et à une partie d'ATE_IND.2 (repassage des tests).



Test indépendant par l'évaluateur

Le commanditaire met à disposition de l'évaluateur une TOE se prêtant à l'exécution de tests indépendants.

Sur la base des spécifications fonctionnelles et de la documentation de test, l'évaluateur conçoit des tests complémentaires des fonctions de sécurité, afin de valider des comportements de sécurité de la TOE que le commanditaire n'aurait pas testés.

Argumentaire : ces mesures satisfont à une partie de l'exigence ATE_IND.2 (test indépendant).

6.2.4 Documentation d'exploitation

Procédures d'installation et de démarrage

Ces procédures permettent l'installation et le démarrage de la TOE dans des conditions qui garantissent une exécution satisfaisante de ses fonctions de sécurité.

Afin de prévenir les risques d'utilisation impropre, la documentation d'installation et de démarrage doit spécifiquement identifier tous les modes d'exécution possibles de la TOE ainsi que leur impact sur la sécurité. Elle doit être claire, complète, cohérente, et accessible à l'auditoire visée. Elle doit enfin énumérer toutes les hypothèses relatives à l'environnement d'exploitation prévu et les exigences sur les mesures de sécurité (TI ou non-TI) qui doivent être présentes dans l'environnement.

Le commanditaire documente les procédures d'installation et de démarrage sûrs de la TOE.

L'évaluateur évalue la documentation, au besoin en ré-appliquant les procédures ou une partie d'entre elles.

Argumentaire : ces procédures satisfont à l'exigence AGD_PRE.1.

Documentation d'administration

La documentation d'exploitation à destination des administrateurs et des utilisateurs doit décrire le comportement des fonctions de sécurité et refléter les hypothèses sur l'environnement d'exploitation, dans une optique de configuration, de maintenance et de maintien en condition opérationnelle corrects des fonctions de sécurité. Elle doit également décrire les différents types d'événements relatifs à la sécurité susceptibles de survenir, et fournir des lignes directrices sur la manière de les prendre en compte.

Le commanditaire fournit la documentation d'administration.

L'évaluateur évalue la documentation d'administration.

Argumentaire : ces mesures satisfont à l'exigence AGD_OPE.1.

6.2.5 Estimation de la vulnérabilité

L'évaluateur rédige une analyse indépendante de vulnérabilités (à destination exclusive de l'organisme de certification). Il procède d'autre part à des tests de pénétration dans le but d'estimer les moyens nécessaires à la mise en œuvre des vulnérabilités (compétence technique, temps, expertise, etc.). Cette tâche s'appuie sur les résultats de toutes les tâches précédentes et sur des sources publiques pour identifier les faits techniques (vulnérabilités) susceptibles de causer la réalisation de menaces identifiées dans la présente cible de sécurité ou des infractions aux règles de politiques de sécurité organisationnelles de la présente cible de sécurité.

Argumentaire : ces mesures satisfont à l'exigence AVA_VAN.3.



6.3 Argumentaire des spécifications abrégées de la TOE

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

6.3.1 Satisfaction des exigences fonctionnelles de sécurité

| | | FDP_IFC.2 | FDP_IFF.1.Filtrage | FIA_UID.2 | FIA_UAU.2 | FIA_UAU.5.Utilisateur | FDP_IFC.1 | FDP_UCT.1 | FDP_UIT.1 | FDP_IFF.1.Chiffrement | FTP_TRP.1.Corresp | FIA_UAU.5.Corresp | FPT_TDC.1 | FAU_GEN.1 | FAU_GEN.2 | FAU_SAR.1 | FAU_STG.3 | FAU_ARP.1.Alarmes | FAU_SAA.4 | FAU_ARP.1.IPS | FMT_SMF.1 | FMT_SMR.1 | FDP_ACC.2 | FMT_MOF.1 | FMT_MTD.1 | FMT_MTD.BRS | FPT_ITT.1 | FTP_TRP.1.Admin | FIA_UAU.5.Admin | FCS_COP.1 | FPT_STM.1 |
|---|--|-----------|--------------------|-----------|-----------|-----------------------|-----------|-----------|-----------|-----------------------|-------------------|-------------------|-----------|-----------|-----------|-----------|-----------|-------------------|-----------|---------------|-----------|-----------|-----------|-----------|-----------|-------------|-----------|-----------------|-----------------|-----------|------------------|
| Fonction de filtrage | | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Fonction d'identification/ authentification | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | a |
| Fonction de chiffrement | | | | | | | X | X | X | X | | | | | | | | | | | | | | | | | | | | | c d |
| Établissement des SA | IKE phase 2: établist. de SA IPSec | | | | | | | | | | X | | X | | | | | | | | | | | | | | | | | | a c d |
| | IKE phase 1: établist. De SA ISAKMP et authent. mutuelle | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | a b c d |
| Fonction de journalisation | | | | | | | | | | | | | | X | X | | X | | | | | | | | | | | | | | |
| Fonction d'audit | | | | | | | | | | | | | | | | X | | | | | X | | | | | | | | | | |
| Fonction d'alarme | | | | | | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| Fonction de prévention des intrusions | | | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | | |
| Fonction de contrôle d'accès aux opé. d'admin. de la séc. | | | | | | | | | | | | | | | | | | | | | X | X | X | X | X | | | | | | |
| Fonction de sauvegarde et de restauration | | | | | | | | | | | | | | | | | | | | | X | | | | | X | | | | | |
| Protect. des sessions d'admin. | Chiffrement et authentification des sessions d'admin. | | | | | | | | | | | | | | | | | | | | X | | | | | X | X | | | | ef |
| | Auth. des admin. et élan. de la clé de chifft. | | | | | | | | | | | | | | | | | | | | X | | | | | | X | X | | | a |



7 ANNEXE A – DROITS D'ADMINISTRATION

Cette section a pour objet l'énumération complète des droits d'administration sur l'IPS-Firewall 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.
- **FILTER (F)** : accès 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 (VPN-Firewall)
- **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.
- **OTHER (*)** : gestion autre (actions diverses).
- **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.

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

- **URL** : accès aux slots du filtrage URL.
- **PKI** : gestion de la PKI interne (émission, révocation, ...)
- **HA** : haute disponibilité (interne, interdit aux utilisateurs).
- **PVM (SEISMO)** : gestion des vulnérabilités (consultation, modification)
- **GLOBALOTHER (G*)** : gestion autre (actions diverses) de la configuration globale



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.

| Catégorie | 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 |
| | Routage par la source | 23 | b |
| | Fragment IP de taille nulle | 33 | b |
| | Port 0 utilisé comme service | 34 | b |
| | Petit fragment | 57 | b |
| | Sonde de port | 63 | e |
| | Utilisation de l'adresse privée d'une interface | 64 | a |
| | Usurpation d'adresse IP sur un bridge | 70 | a |
| | Utilisation de la plage d'adresse 'link local' (RFC 3330) | 83 | b |
| | Utilisation de l'adresse broadcast en source | 89 | b |
| | Protocole IP invalide | 92 | b |
| | Somme de contrôle IP invalide | 96 | b |
| | Analyse de fragment IP | 102 | - |
| | Protocole GRE local | 104 | - |
| | Protocole IPSec ESP local | 105 | - |
| | Protocole IPSec AH local | 106 | - |
| | Usurpation d'adresse IP sur l'interface IPsec | 108 | a |
| Protocole OSPF local | 111 | - | |
| 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 |
| | Adresse multicast avec TCP | 18 | b |
| | Attaque Xmas tree | 20 | b |
| | Attaque possible par MSS faible | 36 | b |
| | Option TCP au mauvais moment | 58 | b |



| <i>Catégorie</i> | <i>Libellé de l'attaque</i> | <i>Id</i> | <i>Type d'attaque</i> |
|------------------|--|-----------|-----------------------|
| | Evasion de données sur TCP | 65 | b |
| | Adresse broadcast avec TCP | 71 | 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 |
| | Données urgentes non autorisées dans du trafic TCP | 162 | c |
| UDP | Bouclage de port UDP | 31 | b |
| | Somme de contrôle UDP invalide | 73 | b |
| | Protocole UDP invalide | 100 | b |
| ICMP | Type ICMP inconnu | 11 | b |
| | Réponse ICMP sans requête | 12 | b |
| | ICMP redirect | 22 | b |
| | 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 |
| IGMP | Type IGMP inconnu | 19 | b |
| | Demande IGMP pour une adresse non multicast | 61 | b |
| | Paquet IGMP invalide | 62 | b |
| | Somme de contrôle IGMP invalide | 74 | b |
| DOS | Attaque de type Land | 21 | b |
| | Possible saturation ICMP | 28 | f |
| | Possible saturation UDP | 29 | f |
| | Possible saturation TCP SYN | 30 | f |
| | Bug Windows sur les données OOB | 35 | d |
| | Attaque possible des ressources | 91 | b |
| Scan | Sonde OS Nmap | 24 | e |
| | Sonde OS Queso | 25 | e |
| | Détection de la politique de filtrage | 26 | e |
| | Possible scan de ports | 27 | e |
| | Sonde OS XProbe | 66 | e |
| 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 |



| <i>Catégorie</i> | <i>Libellé de l'attaque</i> | <i>Id</i> | <i>Type d'attaque</i> |
|------------------|---|-----------|-----------------------|
| | 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 |
| | 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 |
| MGCP | Erreur du protocole MGCP | 113 | c |
| | Réponse MGCP sans requête | 114 | c |
| | Débordement dans le protocole MGCP | 143 | c |
| | Code malicieux possible dans le paramètre MGCP | 144 | c |
| | Paramètre MGCP interdit | 145 | c |
| | Champ SDP nécessaire manquant dans le protocole MGCP | 146 | c |



| <i>Catégorie</i> | <i>Libellé de l'attaque</i> | <i>Id</i> | <i>Type d'attaque</i> |
|------------------|--|-----------|-----------------------|
| | Limite des opérations MGCP dépassée | 147 | c |
| RTCP | Protocole RTCP invalide | 128 | c |
| | Version RTCP invalide | 129 | c |
| | Type de paquet RTCP invalide | 130 | c |
| RTP | Protocole RTP invalide | 125 | c |
| | Version RTP invalide | 126 | c |
| | Type de donnée RTP invalide | 127 | 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 |
| SMTP | Protocole SMTP invalide | 121 | c |
| | Caractère invalide dans l'entête SMTP | 122 | c |
| SSL | Données non chiffrées détectées | 115 | d |
| | Niveau de chiffrement non autorisé | 116 | - |
| | Différence dans la version SSL | 117 | c |
| | Paquet SSL invalide | 118 | c |
| | SSL Record Layer invalide | 119 | c |
| SMB / SMB2 | Valeur invalide dans l'entête SMB PidHigh pour la commande NEGOTIATE | 155 | d |
| | Débordement dans le nom de fichier SMB2 Referral | 156 | d |
| | Protocole NBSS/SMB2 invalide | 157 | c |
| | Protocole NBSS/SMB invalide | 158 | c |
| Misc | Paquet RIP invalide | 13 | b |
| | Protocole eDonkey invalide | 77 | c |
| | Adresse dans la liste noire | 93 | - |
| | Adresse dans la liste blanche | 94 | - |
| | Paquet avec destination sur la même interface | 95 | - |
| | Problème dans le suivi de données | 99 | - |
| | Rejet pour qualité de service | 101 | - |
| | Détection de protocole non autorisé | 110 | - |
| | Protocole Skype détecté | 120 | - |



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 | <i>The TSF</i> := 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 | <i>information flow control SFP</i> := la politique de filtrage |
| Affectation | <i>list of subjects and information</i> := les équipements des réseaux interconnectés par l'IPS-Firewall(<i>subjects</i>), les paquets IP (<i>information</i>) |
| Raffinement | <i>all operations that cause that information to flow to and from subjects covered by the SFP</i> := tous les transferts (<i>operations</i>) de paquets IP entre les équipements des réseaux interconnectés par l'IPS-Firewall |
| Mise en forme | les équipements des réseaux interconnectés par l'IPS-Firewall, les paquets IP et tous les transferts de paquets IP entre les équipements des réseaux interconnectés par l'IPS-Firewall → 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 | <i>all operations that cause any information in the TOE to flow to and from any subject in the TOE</i> := tous les transferts de paquets les équipements des réseaux interconnectés par l'IPS-Firewall → tous les paquets IP entrants |
| Raffinement | <i>an information flow control SFP</i> := la politique de filtrage |

FDP_IFF.1.Filtrage – Fonction de filtrage

| | |
|--------------------------|---|
| Raffinement systématique | <i>The TSF</i> := la fonction de filtrage |
| Raffinement systématique | <i>information flow between a controlled subject and controlled information via a controlled operation</i> := 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 | <i>information flow control SFP</i> := la politique de filtrage |
| Raffinement + mise en forme | <i>subject and information</i> := équipements des réseaux interconnectés par l'IPS-Firewall(<i>subjects</i>), les paquets IP (<i>information</i>) → les paquets IP entrants |
| Affectation | <i>list of subjects and information controlled under the indicated SFP, and, for each, the security attributes</i> := a. L'interface de réception, b. L'adresse IP source et destination du paquet et, partant de là, la machine source et la machine destination du paquet, |



| | |
|--|--|
| | <p>c. Le numéro de protocole IP, d. La valeur du champ DSCP, e. Si le protocole est TCP ou UDP : le port source et destination, f. Si le protocole est ICMP : les champs 'type' et 'code' du message, g. Si l'adresse IP source est associée à un utilisateur dans la table des utilisateurs authentifiés : l'identité de l'utilisateur.</p> |
|--|--|

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 | <p><i>for each operation, the security attribute-based relationship that must hold between subject and information security attributes :=</i></p> <p>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'.</p> |
|-------------|--|

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

| | |
|-------------|---|
| Affectation | <p><i>additional information flow control SFP rules :=</i> les règles complémentaires suivantes :</p> <p>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.</p> |
|-------------|---|

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 | <p><i>rules, based on security attributes, that explicitly authorise information flows :=</i></p> <p>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 :</p> <p>i. l'administration à distance du firewall, ii. l'authentification des utilisateurs, iii. l'établissement de VPN.</p> |
|-------------|--|

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 | <p><i>rules, based on security attributes, that explicitly deny information flows :=</i></p> <p>a. L'action de la première règle de filtrage applicable est 'bloquer' ou 'réinitialiser' ; b. Aucune règle de filtrage n'a autorisé le paquet.</p> |
|-------------|--|



Fonction d'identification / authentification

FIA_UID.2 – Identification de l'utilisateur en vue de l'application de la politique de filtrage

| | |
|-----------------------------|--|
| Raffinement systématique | <i>The TSF := la fonction d'identification / authentification</i> |
| FIA_UID.2.1 | <i>The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.</i> |
| Raffinement + mise en forme | <i>before allowing any other TSF-mediated actions on behalf of that user := avant d'autoriser +à travers l'ajout dans la table des utilisateurs authentifiés suite à la réussite de l'authentification,+ toute autre action transitant par la TSF pour le compte de cet utilisateur. → avant de pouvoir l'ajouter à la table des utilisateurs authentifiés</i> |

FIA_UAU.2 – Authentification de l'utilisateur en vue de l'application de la politique de filtrage

| | |
|-----------------------------|---|
| Raffinement systématique | <i>The TSF := la fonction d'identification / authentification</i> |
| FIA_UAU.2.1 | <i>The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.</i> |
| Raffinement + mise en forme | <i>before allowing any other TSF-mediated actions on behalf of that user := avant d'autoriser +à travers l'ajout dans la table des utilisateurs authentifiés+ toute autre action transitant par la TSF pour le compte de cet utilisateur. → avant de l'ajouter à la table des utilisateurs authentifiés</i> |

FIA_UAU.5.Utilisateur – Mécanisme d'authentification des utilisateurs

| | |
|-----------------------------|---|
| Raffinement systématique | <i>The TSF := la fonction d'identification / authentification</i> |
| FIA_UAU.5.1 | <i>The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.</i> |
| Affectation | <i>list of multiple authentication mechanisms := le mécanisme basé sur le protocole SRP</i> |
| FIA_UAU.5.2 | <i>The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].</i> |
| Affectation + mise en forme | <i>rules describing how the multiple authentication mechanisms provide authentication := les règles définies par le protocole SRP → le protocole SRP</i> |

Fonction de chiffrement

FDP_IFC.1 – Chiffrement des flux d'information

| | |
|-----------------------------|--|
| Raffinement systématique | <i>The TSF := la fonction de chiffrement</i> |
| FDP_IFC.1.1 | <i>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].</i> |
| Affectation | <i>information flow control SFP := la politique de chiffrement</i> |
| Affectation + mise en forme | <i>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</i> |



| | |
|--|---|
| | des correspondants VPN et les émissions de datagrammes IP sortants couverts par une politique de chiffrement (<i>operations</i>) → 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 | <i>The TSF</i> := 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 | <i>access control SFP(s) and/or information flow control SFP(s)</i> := la politique de chiffrement |
| Sélection | <i>transmit, receive</i> := <i>transmit and receive</i> |
| Raffinement | <i>user data</i> := des datagrammes IP |

FDP_UIT.1 – Intégrité du contenu des flux

| | |
|--------------------------|--|
| Raffinement systématique | <i>The TSF</i> := 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 | <i>access control SFP(s) and/or information flow control SFP(s)</i> := la politique de chiffrement |
| Sélection | <i>transmit, receive</i> := <i>transmit and receive</i> |
| Raffinement | <i>user data</i> := des datagrammes IP |
| Sélection | <i>modification, deletion, insertion, replay</i> := <i>modification, insertion, replay</i> |

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 | <i>user data</i> := les datagrammes ESP entrants |
| Sélection | <i>modification, deletion, insertion, replay</i> := <i>modification, insertion, replay</i> |

FDP_IFF.1.Chiffrement – Fonction de chiffrement

| | |
|--------------------------|--|
| Raffinement systématique | <i>The TSF</i> := 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 | <i>information flow control SFP</i> := la politique de chiffrement |
| Raffinement + mise en forme | <i>subject and information</i> := les correspondants VPN et les extrémités du trafic (côté TOE et côté correspondants VPN) (<i>subject</i>), les datagrammes ESP entrants et les datagrammes IP sortants couverts par une politique de chiffrement (<i>information</i>) → les datagrammes ESP entrants et les datagrammes IP sortants couverts par une règle de chiffrement |
| Affectation | <i>list of subjects and information controlled under the indicated SFP, and for each, the security attributes</i> := 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 | <i>information flow between a controlled subject and controlled information via a controlled operation := paquet ESP entrant</i> |
| Affectation | <i>for each operation, the security attribute-based relationship that must hold between subject and information security attributes :=</i> 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 | <i>additional information flow control SFP rules := les règles complémentaires suivantes :</i> 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 négociation 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 | <i>rules, based on security attributes, that explicitly authorise information flows := aucune règle</i> |
| 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 | <i>rules, based on security attributes, that explicitly deny information flows := aucune règle</i> |
| Mise en forme | de l'élément |

Fonction d'établissement des SA

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

| | |
|--------------------------|--|
| Raffinement systématique | <i>The TSF := la fonction d'établissement des SA</i> |
|--------------------------|--|

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 | <i>remote, local := remote</i> |
| Raffinement | <i>Itself := l'IPS-firewall</i> |
| Raffinement | <i>remote users := les correspondants VPN</i> |
| Affectation | <i>other types of integrity or confidentiality violation := none</i> |



| | |
|-----------|---|
| Sélection | <i>modification, disclosure, none</i> := 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 | <i>the TSF, local users, remote users</i> := the TSF and remote users |
| Raffinement | <i>the TSF and remote users</i> := l'IPS-firewall et les correspondants VPN |
| Raffinement | <i>communication via the trusted path</i> := 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 | <i>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]</i> |
| Raffinement | <i>initial user authentication</i> := l'authentification mutuelle initiale des extrémités du tunnel (phase 1 du protocole IKE) |
| Affectation | <i>other services for which trusted path is required</i> := la négociation des SA IPSec (phase 2 du protocole IKE) |

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

| | |
|--------------------------|--|
| Raffinement systématique | <i>The TSF</i> := 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 | <i>list of multiple authentication mechanisms</i> := les mécanismes d'authentification suivants : certificats X509, clé pré-partagée |
| Raffinement | <i>user</i> := 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 | <i>rules describing how the multiple authentication mechanisms provide authentication</i> := les règles du mécanisme d'authentification spécifié pour le tunnel VPN → le mécanisme d'authentification spécifié pour le tunnel VPN |
| Raffinement | <i>user</i> := correspondant VPN |

FPT_TDC.1 – Négociation des SA ISAKMP et IPSec

| | |
|--------------------------|--|
| Raffinement systématique | <i>The TSF</i> := 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 | <i>list of TSF data types</i> := les paramètres des SA ISKAMP et IPSec |
| Raffinement | <i>consistently interpret</i> les paramètres des SA ISKAMP et IPSec := négocier les paramètres des SA ISKAMP et IPSec |
| Raffinement | <i>when shared between the TSF and another trusted IT product</i> := lors de l'établissement des tunnels VPN entre l'IPS-Firewall 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 | <i>list of interpretation rules to be applied by the TSF</i> := |
|-------------|---|



| | |
|-------------|---|
| | les règles suivantes : a. Si l'IPS-Firewall 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'IPS-Firewall est le répondeur, n'accepter que les propositions aussi rigoureuses qu'une des propositions locales. |
| Raffinement | <i>interpreting the TSF data from another trusted IT product</i> := 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 | <i>The TSF</i> := 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 | <i>minimum, basic, detailed, not specified</i> := not specified |
| Mise en forme | de l'item b) |
| Affectation | <i>other specifically defined auditable events</i> := les événements auditable énumérés dans le tableau au chapitre 5.2 après FAU_GEN.1.2 |
| Raffinement | <i>audit functions</i> := 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 | <i>subject identity</i> := adresse IP source, et identité de l'utilisateur (si elle est connue) |
| Affectation | <i>other audit relevant information</i> := 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 | <i>The TSF</i> := 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 | <i>user</i> := administrateur |
| Raffinement | <i>auditable event</i> := événement auditable associé aux opérations d'administration de la sécurité |

FAU_SAR.1 – Revue d'audit

| | |
|--------------------------|---------------------------------------|
| Raffinement systématique | <i>The TSF</i> := 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 | <i>authorised users</i> := auditeurs |
| Affectation | <i>list of audit information</i> := toutes les informations d'audit |
| Raffinement | <i>audit records</i> := 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 | <i>audit records</i> := fichiers de trace |
| Raffinement | <i>user</i> := auditeur |

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

| | |
|--------------------------|---|
| Raffinement systématique | <i>The TSF</i> := 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 | <i>actions to be taken in case of possible audit storage failure</i> := 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'IPS-Firewall ne s'arrête pas réellement mais il bloque l'ensemble des flux excepté les sessions d'administration du Firewall Manager depuis le réseau interne. |
| Raffinement | <i>audit trail</i> := un fichier de trace |
| Affectation | <i>pre-defined limit</i> := le nombre d'éléments à journaliser suivant : a. build S : Pas de stockage local b. build M : 256 c. build L : 512 d. build XL : 1024 |

FAU_ARP.1. Alarmes – Réponse automatique aux alarmes

| | |
|--------------------------|--|
| Raffinement systématique | <i>The TSF</i> := la fonction d'alarme |
|--------------------------|--|

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

| | |
|-------------|---|
| Affectation | <i>list of actions</i> := Transmettre l'alarme aux moniteurs temps-réel connectés |
| Raffinement | <i>detection of a potential security violation</i> := 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 | <i>The TSF</i> := 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 | <i>internal representation := base de connaissance</i> |
| Mise en forme | <i>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.</i> |
| Affectation | <i>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 (<i>fingerprinting, port scanning, etc.</i>), f. dépassement du taux d'ouverture de connexions associé à une règle de filtrage.</i> |
| Raffinement | <i>potential violation of the enforcement of the SFRs := attaque Internet potentielle</i> |

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 | <i>signature events and event sequences := types d'attaques présents dans la base de connaissance</i> |
| Affectation | <i>information to be used to determine system activity := les paquets IP entrants et sortants</i> |
| Raffinement | <i>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</i> |

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 | <i>potential violation of the enforcement of the SFRs := attaque Internet potentielle</i> |
| Raffinement | <i>system activity := l'état d'un ou plusieurs contextes associés à un paquet IP entrant</i> |
| Raffinement | <i>signature event or event sequence that indicates a potential violation of the enforcement of the SFRs := type d'attaque présent dans la base de</i> |



| | |
|--|--------------|
| | connaissance |
|--|--------------|

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

| | |
|--------------------------|--|
| Raffinement systématique | <i>The TSF := la fonction de prévention des intrusions</i> |
|--------------------------|--|

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

| | |
|-------------|--|
| Affectation | <i>list of actions :=</i> 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 | <i>potential security violation :=</i> 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 | <i>The TSF := la fonction d'administration de la sécurité</i> |
|--------------------------|---|

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 | <i>list of management functions to be provided by the TSF :=</i> La fonction de contrôle d'accès aux opérations d'administration de la sécurité ; La fonction de protection des sessions d'administration La fonction d'audit La fonction de sauvegarde / restauration |
|-------------|--|

FMT_SMR.1 – Rôle d'administrateur de la sécurité

| | |
|--------------------------|--|
| Raffinement systématique | <i>The TSF := la fonction de contrôle d'accès aux opérations d'administration de la sécurité</i> |
|--------------------------|--|

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

| | |
|-------------|--|
| Affectation | <i>the authorised identified roles :=</i> « 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 | <i>The TSF := la fonction de contrôle d'accès aux opérations d'administration de la sécurité</i> |
|--------------------------|--|

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 | <i>access control SFP := la politique de contrôle d'accès aux opérations</i> |
|-------------|--|



| | |
|---------------|---|
| | d'administration de la sécurité |
| Affectation | <i>list of subjects and objects</i> := les administrateurs (<i>subjects</i>), les données et les fonctions de sécurité (<i>objects</i>) |
| Raffinement | <i>all operations among subjects and objects covered by the SFP</i> := 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 | <i>all operations between any subject controlled by the TSF and any object controlled by the TSF</i> := 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 | <i>an access control SFP</i> := 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 | <i>The TSF</i> := 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 | <i>determine the behaviour of, disable, enable, modify the behaviour of</i> := <i>disable, enable, modify the behaviour of</i> |
| Raffinement | <i>modify the behaviour of</i> := effectuer, modifier |
| Affectation | <i>list of functions</i> := les fonctions de sécurité du tableau ci-dessous |
| Affectation | <i>the authorised identified roles</i> := les administrateurs |
| Raffinement | en fonction des droits ci-dessous |

FMT_MTD.1 – Administration des données de sécurité

| | |
|--------------------------|--|
| Raffinement systématique | <i>The TSF</i> := 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 | <i>change_default, query, modify, delete, clear, [assignment: other operations]</i> := <i>query, modify, clear</i> |
| Affectation | <i>list of TSF data</i> := les données de sécurité du tableau ci-dessous |
| Affectation | <i>the authorised identified roles</i> := 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 | <i>The TSF</i> := 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 | <i>list of TSF data := les données de sécurité</i> |
| Raffinement | <i>a storage device := le disque sur de la station d'administration</i> |

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

| | |
|-------------|---|
| Raffinement | <i>TSF data := des données de sécurité</i> |
| Raffinement | <i>a storage device := le disque sur de la station d'administration</i> |

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 | <i>The TSF := la fonction de protection des sessions d'administration</i> |
|--------------------------|---|

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

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

| | |
|--------------------------|---|
| Raffinement systématique | <i>The TSF := la fonction de protection des sessions d'administration</i> |
|--------------------------|---|

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 | <i>itself := l'IPS-firewall</i> |
| Sélection | <i>remote, local := remote</i> |
| Raffinement | <i>remote users := les administrateurs</i> |
| Affectation | <i>other types of integrity or confidentiality violation := none</i> |
| Sélection | <i>modification, disclosure, none := modification or disclosure</i> |

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

| | |
|-------------|---|
| Sélection | <i>the TSF, local users, remote users := remote users</i> |
| Raffinement | <i>remote users := les administrateurs</i> |

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 | <i>initial user authentication, [assignment: other services for which trusted path is required] := initial user authentication, [assignment: other services for which trusted path is required]</i> |
| Raffinement | <i>initial user authentication := l'authentification mutuelle initiale de l'administrateur et de l'IPS-Firewall</i> |
| Affectation | <i>other services for which trusted path is required := les opérations d'administration à distance de la sécurité</i> |

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

| | |
|--------------------------|---|
| Raffinement systématique | <i>The TSF := la fonction de protection des sessions d'administration</i> |
|--------------------------|---|



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

| | |
|-------------|---|
| Affectation | <i>list of multiple authentication mechanisms := le mécanisme basé sur le protocole SRP</i> |
| Raffinement | <i>user := administrateur</i> |

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 | <i>user := administrateur</i> |
| Affectation + mise en forme | <i>rules describing how the multiple authentication mechanisms provide authentication := les règles du protocole SRP →le protocole SRP</i> |

9.2.5 Autres exigences de sécurité de soutien

Autres fonctions de soutien

FCS_COP.1 – Fonction cryptographique

| | |
|--------------------------|---|
| Raffinement systématique | <i>The TSF := la fonction cryptographique</i> |
|--------------------------|---|

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

| | |
|-------------|---|
| Affectation | <i>list of cryptographic operations := les opérations cryptographiques du tableau ci-dessous</i> |
| Affectation | <i>cryptographic algorithm := les algorithmes cryptographiques □ spécifiés ci-dessous</i> |
| Affectation | <i>cryptographic key sizes := les tailles des clés cryptographiques □ spécifiées ci-dessous</i> |
| Affectation | <i>list of standards := les standards énoncés ci-dessous</i> |

FPT_STM.1 – Base de temps fiable

| | |
|--------------------------|---|
| Raffinement systématique | <i>The TSF := l'horloge interne de l'IPS-Firewall</i> |
|--------------------------|---|

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

Autres mesures d'assurance sécurité

ADV_ARC.1 – Description de l'architecture de sécurité

Pas d'opérations effectuées.

ADV_FSP.3 – Spécifications fonctionnelles avec résumé exhaustif

Pas d'opérations effectuées.

ADV_TDS.2 – Conception de haut niveau - identification des sous-systèmes dédiés à la sécurité

Pas d'opérations effectuées.



AGD_OPE.1 – Guides opérationnels

Pas d'opérations effectuées.

AGD_PRE.1 – Guides de préparation

Pas d'opérations effectuées.

ATE_COV.2 – Analyse de la couverture des tests

Pas d'opérations effectuées.

ATE_DPT.1 – Tests: conception simple

Pas d'opérations effectuées.

ATE_FUN.1 – Tests fonctionnels

Pas d'opérations effectuées.

ATE_IND.2 – Tests indépendants - échantillonnage

Pas d'opérations effectuées.

ALC_FLR.3 – Correction d'anomalies systématique

Pas d'opérations effectuées.

ALC_LCD.1 – Modèle de cycle de vie défini par le développeur

Pas d'opérations effectuées.

AVA_VAN.3 – Analyse de vulnérabilités

Pas d'opérations effectuées.

ALC_CMC.4 – Gestion de configuration avec procédures d'acceptation des modifications et de la génération de la TOE

Pas d'opérations effectuées.

ALC_CMS.4 – Gestion en configuration de la remontée d'erreurs

Pas d'opérations effectuées.

ALC_DEL.1 – Procédures de livraison

Pas d'opérations effectuées.

ALC_DVS.1 – Identification des mesures de sécurité

Pas d'opérations effectuées.

ASE_CCL.1 – Annonces de conformité

Pas d'opérations effectuées.



ASE_ECD.1 – Définition de composants étendus

Pas d'opérations effectuées.

ASE_INT.1 – Introduction de la cible

Pas d'opérations effectuées.

ASE_OBJ.2 – Objectifs de sécurité

Pas d'opérations effectuées.

ASE_REQ.2 – Exigences de sécurité déduites

Pas d'opérations effectuées.

ASE_SPD.1 – Définition du problème de sécurité

Pas d'opérations effectuées.

ASE_TSS.1 – spécifications abrégées de la TOE

Pas d'opérations effectuées.



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.

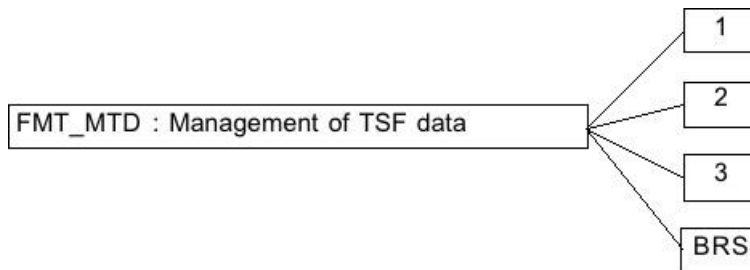
10.1 Introduction

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.