Firewalls NETASQ

Cible de sécurité fonction de filtrage de la suite logicielle IPS-Firewall Version 9.1

Évaluation selon un paquet EAL4 augmenté des Critères Communs V3.1

NETASQ

Secure Internet Connectivity

SUIVI DE DOCUMENT

Version	Auteur	Date	Modifications
0.1	Ludovic FLAMENT	22/08/2008	Version initiale du document
0.2	Ludovic FLAMENT	26/08/2008	Mise à jour suite relecture de Boris MARECHAL
1.0	Ludovic FLAMENT	11/09/2008	Commentaires suite à la préparation
1.1	Ludovic FLAMENT	13/10/2008	Intégration des commentaires du CESTI (SA-FdC01-ASE)
1.2	Ludovic FLAMENT	30/10/2008	Intégration des commentaires du CESTI (SA-FdC02-ASE)
1.3	Ludovic FLAMENT	27/03/2009	Intégration des commentaires du CESTI (SA-FdC12-ASE)
1.4	Ludovic FLAMENT	20/02/2012	Mise à jour version 9.1
1.5	Ludovic FLAMENT	22/02/2012	Correction AVA_VAN
1.6	Ludovic FLAMENT	24/05/2012	Mise à jour suite remarque ANSSI
1.7	Ludovic FLAMENT	09/07/2012	Mise à jour suite remarques CESTI
1.8	Boris MARECHAL	18/06/2014	Mise à jour version 9.1.0.5

TABLE DES MATIÈRES

TABLE DES ILLUSTRATIONS

1 INTRODUCTION

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

1.1 Identification de la cible de sécurité

Titre : Cible de sécurité fonction de filtrage de la suite logicielle IPS-Firewall Version 9.1

Référence de la ST : NA_ASE_ciblesec_filter_v91

Version de la ST : 1.8

Cible d'évaluation : Fonction de filtrage de la suite logicielle IPS-Firewall pour boîtiers appliances NETASQ

Version de la TOE : 9.1.0.5 (S, M, L, XL)

Paquet d'assurance sécurité : EAL4 augmenté de ALC_FLR.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 stricte des Critères Communs ».

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

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

Le paquet d'assurance sécurité sélectionné est une extension du paquet EAL4 augmenté du composant ALC_FLR.3.

1.3 Résumé des fonctionnalités du firewall-VPN NETASQ

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

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

- la fonctionnalité firewall regroupant : filtrage, détection d'attaques, gestion de la bande passante, gestion de la politique de sécurité, audit, imputabilité, authentification forte des administrateurs,
- la fonctionnalité VPN (Réseau Privé Virtuel : chiffrement et authentification) implémentant le protocole [ESP] en mode tunnel du standard IPSec, et sécurisant la transmission des données confidentielles entre sites distants, partenaires ou commerciaux nomades.

L'ASQ (Active Security Qualification) est une technologie de Prévention d'Intrusion en Temps Réel, intégrée dans tous les 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 administrateurs, la suite logicielle IPS-Firewall intègre une base d'utilisateurs et offre des services d'authentification auprès de celle-ci.

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

1.4 Documents applicables et de référence

1.4.1 Référentiel des Critères Communs

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

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

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

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

1.4.2 RFC et autres standards supportés

[DSCP] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, RFC 2474, December 1998.

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

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

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

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

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

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

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.

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 filtrage**. C'est sur cet équipement que fonctionne le cœur des fonctions de sécurité de la suite logicielle IPS-Firewall.

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 filtrage, purge des journaux d'audit, arrêt/redémarrage du logiciel IPS-Firewall). Elles sont caractérisées par le fait d'avoir pour effet éventuel de modifier le comportement des fonctions de sécurité de la TOE.

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

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

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

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

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

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

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

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**.

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

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

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.

2.1.2 Le contrôle des flux d'information

Cet ensemble d'exigences est la raison d'être d'un produit de type pare-feu. 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.**

Suivant les cas, les règles de cette **politique de filtrage** peuvent s'exprimer selon des critères plus ou moins sophistiqués : adresses IP source et destination, numéro 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, sur la base :
  - des caractéristiques au niveau IP et transport : n° de protocole IP, adresses IP source et destination, ports TCP/UDP source et destination.
- Imputabilité des flux aux entités les ayant suscités par la génération des données d'audit.

2.1.3 La protection contre la saturation des traces

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 filtrage**.

Les tentatives d'établissement de flux peuvent être tracées, afin de permettre un audit ultérieur. Il existe une protection contre la saturation d'écriture de ces traces, qui consiste à bloquer ces flux dès qu'il n'est plus possible de les tracer.

Il n'est donc pas possible qu'un trafic devant être tracé puisse passer la **fonction de filtrage** suite à une tentative de saturation des traces.

2.1.4 Les risques d'utilisation impropre

La déclinaison d'une **politique de filtrage** 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.

Le risque le plus important est la définition d'une mauvaise **politique de filtrage**. En effet, le fait que la **politique de filtrage** soit incorrectement déterminée peut engendrer des possibilités d'attaques. Ce risque est contré par le fait que l'**administrateur** définissant la **politique de filtrage** est considéré comme une personne compétente, non hostile et formée à cette tâche.

Le « **super-administrateur** », qui intervient exclusivement lors des phases d'installation et de maintenance est le seul habilité à se connecter à la **console locale**.

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 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 filtrage, sans nécessiter de droits particuliers ;

- Soit en 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 (local à accès contrôlé, interdiction d'utiliser une **console locale** dans des conditions d'exploitation, etc.).

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 **boîtiers appliances firewall-VPN** sur lesquels s'exécute **le logiciel IPS-Firewall NETASQ**. Ces boîtiers mettent en œuvre la fonction de filtrage (la TOE) entre les différents sous-réseaux reliés à leurs interfaces.

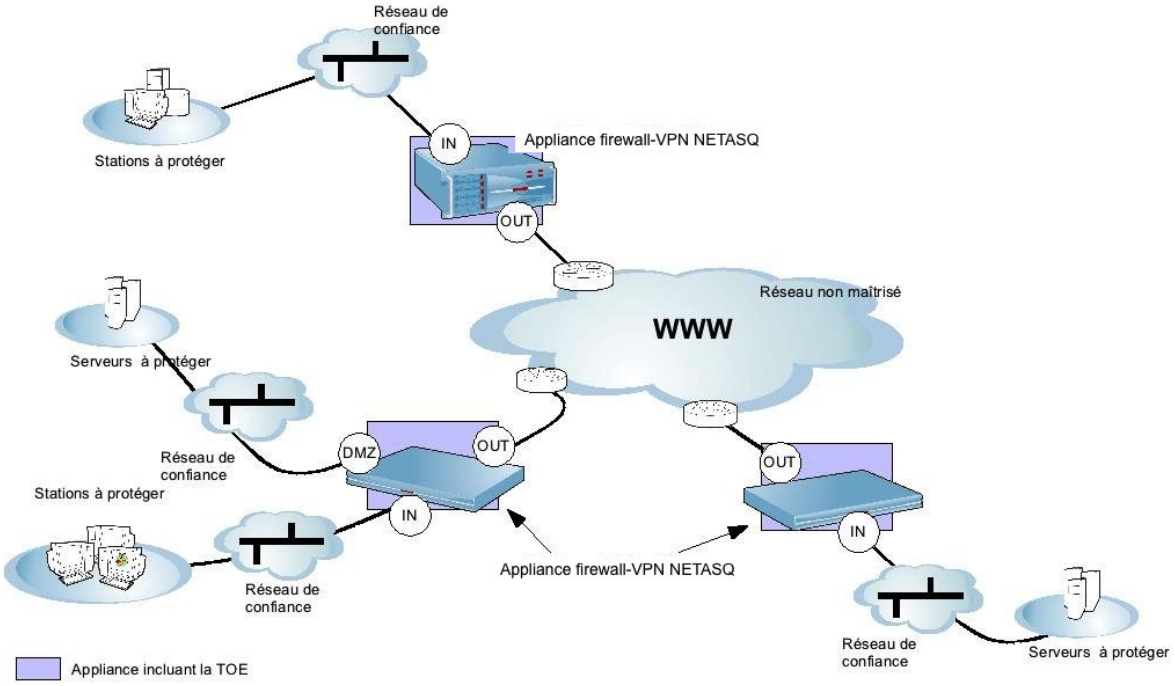

Illustration 1: Cas typique d'utilisation des composants de la TOE.

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.

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 8.3, 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.

2.3 Limites logiques de la TOE

Le périmètre de l'évaluation porte sur sur le composant Fonction de filtrage ***« Filter »*** inclus dans le module *ASQ* de la suite logicielle **IPS-Firewall** dans sa version 9.1.0.5 qui est installée sur les boîtiers appliances firewall-VPN de la gamme U30 à la gamme NG5000 (builds S, M, L, XL) pour le composant logiciel :

- **NS-BSD** : logiciel **IPS-Firewall** pour boîtier appliance firewall-VPN incluant le noyau FreeBSD 8.3 avec correctifs à jour, adapté et épuré par NETASQ

2.4 Architecture et interfaces de la TOE

Une TOE en exploitation est un élément logiciel inclus sur des boîtiers appliances firewall-VPN. La figure ci-dessous schématise la TOE dans son environnement.

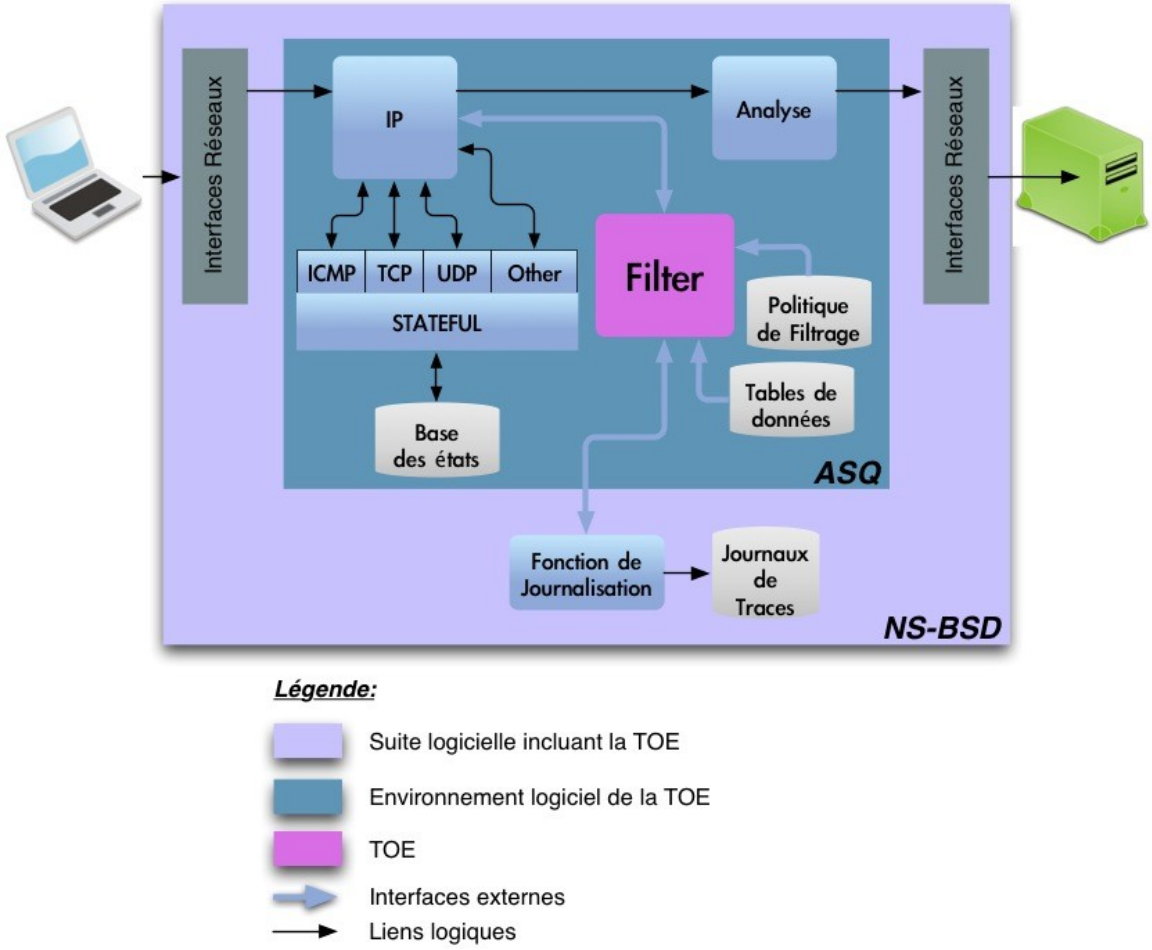

Illustration 2: Composants et interfaces de la TOE.

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

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

- L'évaluation porte sur la **fonction de filtrage** de la suite logicielle IPS-Firewall qui équipe toutes les versions des boîtiers firewall-VPN. La suite logicielle se décline en 4 compilations distinctes (build S, M, L, XL) selon la position dans la gamme.
- 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 **politique de filtrage** qui est utilisée par la **fonction de filtrage** est correctement configurée et installée. Ces actions sont effectuées par un **administrateur** formé, compétent et non hostile.
- Les **tables de données** (table des interfaces, des groupes d'IPs sources et des groupes d'IPs destinations) qui sont utilisées par la **fonction de filtrage** sont correctement initialisées et remplies par le boîtier applicance firewall-VPN.
- Les modules logiciels qui sont dans l'environnement de la **fonction de filtrage** et l'environnement lui-même sont correctement configurés et fonctionnels.
- 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.
- Le mode d'utilisation soumis à l'évaluation exclut le fait que la TOE s'appuie sur les services présents dans la suite logicielle IPS-Firewall version 9.1.0.5 ou pouvant être externe à celle-ci.

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

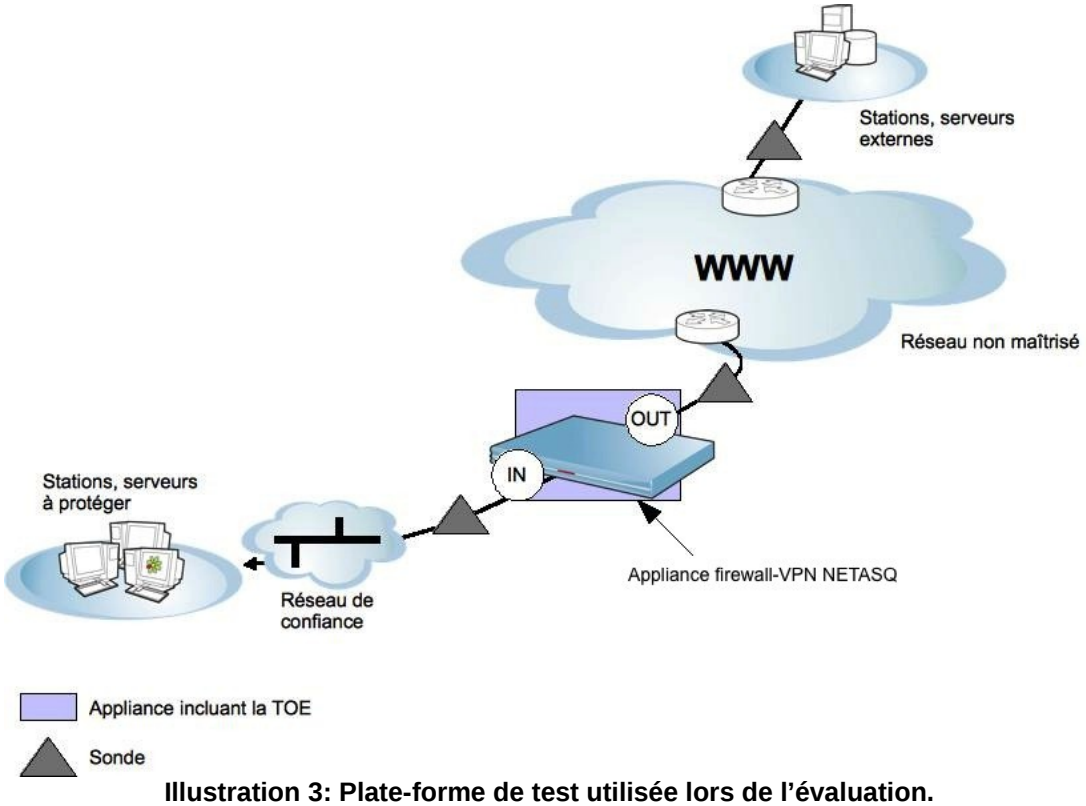

Illustration 3: Plate-forme de test utilisée lors de l'évaluation.

Le boîtier appliance firewall-VPN est un U250S ou un NG1000.

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. Ils sont susceptibles d'être connectés en différents points du réseau.

Ces ordinateurs portables serviront également à mener des tests de pénétration en contrefaisant des paquets.

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 et les politiques :

- 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 filtrage** à mettre en œuvre au niveau du système d'information dans sa globalité (cf. HO.BONNE_PF) :

- 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) ;
- Les informations de topologie du réseau (confidentialité), contre des tentatives de sondage.

3.2.2 Biens appartenant à la TOE

Dans le but de protéger ces biens sensibles externes, l'environnement logiciel qui est en interaction avec la TOE remplit correctement ses objectifs (exemple : confidentialité et intégrité de la configuration).

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 :

- de la **politique de filtrage** utilisée par la TOE,

- des tables de données.
- des données d'enregistrement d'évènements de sécurité.

3.3 Menaces et règles de la politique de sécurité

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

Les différents agents menaçants sont :

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

Les administrateurs ne sont pas considérés comme des attaquants.

3.3.1 Le contrôle des flux d'information

P.FILTRAGE

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

P.AUDIT

La TOE doit piloter l'enregistrement des événements de filtrage (incluant flux et rejets) jugés sensibles par l'**administrateur**.

3.3.2 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**.

3.3.3 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 mettant en défaut la politique de filtrage et les tables de données associées.

M.PERTE_AUDIT

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

3.4 Hypothèses

3.4.1 Hypothèse 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 Hypothèse sur les mesures de sécurité organisationnelles

HO.BONNE_PF

La **politique de filtrage** à mettre en œuvre est définie, pour tous les équipements des réseaux de confiance à protéger, de manière :

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,

stricte : seuls les cas d'utilisation nécessaires des équipements sont autorisés,

correcte : les règles ne présentent pas de contradiction,

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 Hypothèse relative 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 leur permet de constituer une **politique de filtrage** cohérente et conforme aux règles de l'état de l'art en la matière tel que défini au §3.3.2.

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 filtrage**. 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.INTEGRE

L'environnement logiciel qui est en interaction avec la TOE est considéré comme sûr et de confiance et ne peut être utilisé comme moyen de corruption de la TOE ou de sa configuration.

HTI.JOURNAL

La suite logicielle IPS-Firewall version 9.1.0.5 fournit à la TOE un service de journalisation sûr assurant la mise en forme, l'horodatage et l'enregistrement des données d'audit.

4 OBJECTIFS DE SÉCURITÉ

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

4.1 Convention de notation

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

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

4.2 Généralités

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

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

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 (§4.4).

4.3 Objectifs de contrôle des flux d'information

O.FILTRAGE

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

L'interface de provenance du flux,

L'interface de destination du flux,

Machines aux extrémités du flux,

Type de protocole IP,

Pour ICMP : type de message,

Pour TCP et UDP : type de service,

Type de service DSCP.

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

O.AUDIT

La TOE doit :

demander la génération des données d'audit relatives aux évènements se rapportant à l'application de la **politique de filtrage**, en vue du traitement de ces dernières par la fonction de journalisation qui va les mettre en forme, les horodater et les enregistrer.

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

O.PERTE_AUDIT

La TOE doit :

permettre d'interdire un trafic pour lequel une demande de génération de données d'audit est requise alors que cette dernière est impossible à réaliser.

Argumentaire : O.PERTE_AUDIT est principalement dédié à la prévention de la menace M.PERTE_AUDIT.

4.4 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 M.ADMIN_ILLICITE. Il élimine les possibilités d'effectuer des **opérations d'administration de la sécurité** illicites à partir d'un accès local aux boîtiers appliances firewall-VPN.*

OE.BONNE_PF

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

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 afin de satisfaire les règles de la politique de sécurité associées au contrôle des flux d'information 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 **politique de filtrage** mais qui, du fait qu'ils ne passent par aucun des boîtiers appliances firewall-VPN, ne seraient pas soumis à ces fonctions de sécurité.*

OE.USAGE_STRICT

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

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

OE.INTEGRE

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

Argumentaire : Cet objectif de sécurité soutient la mise en oeuvre des politiques P.FILTRAGE et P.AUDIT en assurant que les logiciels et autres services fonctionnant sur le produit, autour de la TOE, sont fiables et permettent à la TOE de s'exécuter correctement.

OE.JOURNAL

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

Argumentaire : Cet objectif de sécurité soutient la mise en oeuvre de la politique P.AUDIT en assurant la génération et l'enregistrement des données d'audit. Il participe également à contrer la menace M.PERTE_AUDIT en remontant à la TOE, sur chaque demande d'enregistrement de données d'audit, une erreur spécifique en cas de saturation des logs.

4.5 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.AUDIT	M.PERTE_AUDIT	M.ADMIN_ILLICITE	M.MAUVAIS_USAGE	HP.PROTECT_BOITIERS	HO.BONNE_PF	HH.PERSONNEL	HTI.COUPURE	HTI.USAGE_STRICT	HTI.INTEGRE	HTI.JOURNAL
O.FILTRAGE	X											
O.AUDIT		X										
O.PERTE_AUDIT			X									
OE.PROTECT_BOITIERS				X		X						
OE.BONNE_PF					X		X					
OE.PERSONNEL					X			X				
OE.COUPURE	S	S							X			
OE.USAGE_STRICT	S	S		X						X		
OE.INTEGRE	S	S									X	
OE.JOURNAL		S	S									X

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.

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 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 §7, 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.

Format des étiquettes des exigences de sécurité :

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

  F*CC_FFF.composant.n*

  - F*CC* est le trigramme de la classe ;
  - *FFF* est le trigramme de la famille ;
  - *composant* est l'identifiant du composant : soit un numéro pour les composants extraits de [CC-02], soit un trigramme pour les exigences de sécurité explicitement énoncées;
  - *n* est le numéro d'élément.

5.1.2 Présentation des données de sécurité

Attributs des paquets IP sur lesquels portent les règles de filtrage

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

Paramètres des règles de filtrage

- L'identifiant de la règle ;
- (critère) L'interface de réception des paquets IP couverts par la règle ;
- (critère) L'interface de destination des paquets IP couverts par la règle ;
- (critère) La ou les machines (nom, adresse IP, port) 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 (nom, adresse IP, port, nom associé au port) des flux d'information couverts par la règle ;
- L'action : 'aucune', 'passer', 'bloquer', 'réinitialiser', 'déléguer' ;
- La génération d'un enregistrement d'audit et le niveau d'alarme éventuellement attribué ;
- La politique de qualité de service associée aux flux couverts par la règle ;
- Le taux maximum d'ouverture connexions / **pseudo-connexions** associé à la règle ;
- Le profil d'attaques internet associé aux connexions couvertes par la règle.

Tables de données

Dans la description des tables de données qui suit, nous ne détaillerons que les informations, de ces différentes tables, qui sont essentielles au bon fonctionnement de la TOE.

Table des interfaces

- Identifiant unique de l'interface ;
- Nombre d'adresses IP valides sur l'interface ;
- Liste des adresses IP valides sur l'interface.

Table des groupes d'IPs sources

- Identifiant unique du groupe ;
- Nom du groupe ;
- Nombre d'adresses IP contenues dans le groupe ;
- Liste des adresses IP contenues dans le groupe.

Table des groupes d'IPs destinations

- Identifiant unique du groupe ;
- Nom du groupe ;
- Nombre d'adresses IP contenues dans le groupe ;
- Liste des adresses IP contenues dans le groupe.

Profil des enregistrements d'audit

- indique le groupe d'appartenance de la règle ayant déclenchée la trace ;
- identifiant de la règle ayant déclenché la trace ;
- nom interne de l'interface de la machine source ;
- nom de l'objet représentant l'interface de la machine source ;
- nom interne de l'interface de la machine de destination ;
- nom de l'objet représentant l'interface de la machine destination ;
- type de protocole réseau (tcp ou udp) ;
- nom du plugin associé, à défaut nom du service standard correspondant au port de destination ;
- adresse IP de la machine source ;
- nom de l'objet correspondant à l'adresse IP de la machine source ;
- numéro de port source du service ;
- nom de l'objet correspondant au port source ;
- adresse IP de la machine de destination ;
- nom de l'objet correspondant à l'adresse IP de la machine de destination ;
- numéro de port destination du service ;
- nom de l'objet correspondant au port de destination ;
- comportement associé à la règle de filtrage.

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 7. 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 pour satisfaire O.FILTRAGE, en définissant la **politique de filtrage** et en exigeant qu'elle s'applique à tous les **paquets IP entrants**.*

FDP_IFF.1 – Fonction de filtrage

[FDP_IFF.1.1]

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

a. L'interface de réception,

b. L'interface de destination,

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

d. Le numéro de protocole IP,

e. La valeur du champ DSCP,

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

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

[FDP_IFF.1.2]

La fonction de filtrage doit autoriser **un paquet IP entrant** si **l'action de la première règle de filtrage applicable est 'passer'.**

[FDP_IFF.1.3]

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 de la politique de filtrage globale pour reprendre au début de la politique de filtrage locale et ne rentrent pas en compte dans le filtrage des paquets.

[FDP_IFF.1.4]

La fonction de filtrage doit autoriser explicitement **un paquet IP entrant si il existe des règles de filtrage implicites associées à ce paquet IP entrant.**

[FDP_IFF.1.5]

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 est dédié à la satisfaction de l'objectif O.FILTRAGE.

Fonction de génération de données d'audit.

FAU_GEN.1 – Génération de données d'audit

[FAU_GEN.1.1]

La fonction de génération de données d'audit doit pouvoir demander l'enregistrement de l'évènement auditable suivant :

Application d'une règle de filtrage pour laquelle la génération d'un enregistrement d'audit est spécifiée.

[FAU_GEN.1.2]

La fonction de génération de données d'audit doit pouvoir demander l'enregistrement des informations suivantes dans chaque enregistrement d'audit :

a. adresse IP et port source,

b. adresse IP et port destination,

c. nom des interfaces source et destination,

d. identifiant du boîtier applicance firewall-VPN,

e. type de protocole et ICMP,

f. identifiant de la règle,

g. action appliquée

Argumentaire : FAU_GEN.1 est dédié à la satisfaction des aspects de génération de données d'audit de l'objectif O.AUDIT.

Raffinement : La TOE n'est concernée que par une partie de l'exigence, à savoir l'appel au service de journalisation de la suite logicielle, qui est lui-même hors TOE.

Raffinement FAU_GEN.1.1 : La fonction de journalisation, qui est hors TOE, enregistre son démarrage et son arrêt. En revanche, la fonction de génération de données d'audit n'a pas de notion de démarrage et d'arrêt proprement dit.

Raffinement FAU_GEN.1.2 : La fonction de journalisation, qui est hors TOE, dispose d'un mécanisme d'horodatage, qui est lui-même hors TOE.

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

[FAU_STG.3.1]

La fonction de filtrage doit **entreprendre de bloquer un paquet IP entrant devant être tracé d'après la politique de filtrage**, si la **quantité de traces** dépasse **le nombre d'éléments à journaliser suivant :**

a. build S : 100

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.PERTE_AUDIT.

5.3 Exigences d'assurance sécurité pour la TOE

Cette section présente le raffinement des exigences d'assurance de la TOE. La description formelle de ces exigences figure au chapitre 7.

Le niveau d'assurance visé par la TOE est le niveau EAL4 augmenté du composant ALC_FLR.3.

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

Composants		Commentaires
ADV_ARC.1	Security architecture description	EAL4
ADV_FSP.4	Formal functionnal specification	EAL4
ADV_IMP.1	Implementation representation of the TSF	EAL4
ADV_TDS.3	Basic modular design	EAL4
AGD_OPE.1	Operational user guidance	EAL4
AGD_PRE.1	Preparative procedures	EAL4
ALC_CMC.4	Production support, acceptance procedures and automation	EAL4
ALC_CMS.4	Problem tracking CM coverage	EAL4
ALC_DEL.1	Delivery procedures	EAL4
ALC_DVS.1	Identification of security measures	EAL4
ALC_FLR.3	Systematic flaw remediation	+
ALC_LCD.1	Developer defined life-cycle model	EAL4
ALC_TAT.1	Well-defined development tools	EAL4
ASE_CCL.1	Conformance claims	EAL4
ASE_ECD.1	Extended components definition	EAL4
ASE_INT.1	ST introduction	EAL4
ASE_OBJ.2	Security objectives	EAL4
ASE_REQ.2	Security requirements	EAL4
ASE_SPD.1	Security problem definition	EAL4
ASE_TSS.1	TOE summary specification	EAL4
ATE_COV.2	Analysis of coverage	EAL4
ATE_DPT.1	Testing: basic design	EAL4
ATE_FUN.1	Functional testing	EAL4
ATE_IND.2	Independent testing - sample	EAL4
AVA_VAN.3	Focused vulnerability analysis	EAL4

5.4 Argumentaire des exigences de sécurité

5.4.1 Satisfaction des objectifs de sécurité

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

	O.FILTRAGE	O.AUDIT	O.PERTE_AUDIT
FDP_IFC.2	S		
FDP_IFF.1	X		
FAU_GEN.1		X	
FAU_STG.3			X

X : l'exigence de sécurité réalise l'objectif
S : l'exigence de sécurité soutient l'objectif

5.4.2 Soutien mutuel et non contradiction

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

5.4.3 Satisfaction des dépendances des SFRs

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

Composant	*Dépendances*	*Satisfaction*
FDP_IFC.2	FDP_IFF.1	Oui
FDP_IFF.1	FDP_IFC.1	Oui via 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.
FAU_GEN.1	FPT_STM.1	Non applicable. L'exigence de FAU_GEN.1 relative à l'élaboration de l'enregistrement de log avec son horodatage est hors TOE.
FAU_STG.3	FAU_STG.1	Non applicable. L'exigence de FAU_STG.3 relative à la protection des enregistrements des logs est hors TOE.

5.4.4 Satisfaction des dépendances des SARs

Le niveau d'assurance de l'évaluation visé par cette cible de sécurité est EAL4+ (ou EAL4 augmenté) augmenté du composant ALC_FLR.3 qui ne possède pas de dépendance.

Les dépendances requises par les CC pour les composants d'assurance inclus dans le paquet EAL4 sont par ailleurs toutes respectées.

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 inclus 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 entrant** reçu aux critères de chaque règle de la **politique de filtrage**. Le filtrage porte sur tous les **paquets IP entrants**. Les critères des règles de filtrage sont :

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

Chaque règle de filtrage peut spécifier une action de contrôle et une action de génération de données d'audit. Cette dernière est décrite au §6.1.2.

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 génération de données d'audit uniquement).
- 'déléguer' : le paquet est confronté aux règles de filtrage de la **politique de filtrage locale** (permet de passer l'évaluation de la **politique de filtrage globale** afin de déléguer un sous-ensemble de celle-ci à un **administrateur** local via la **politique de filtrage locale**). Cette action n'est disponible que pour les règles de la **politique de filtrage globale**.

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

Il convient de noter qu'à proprement parler, pour un ensemble de paquets IP liés à un même échange au niveau transport (connexion TCP, **pseudo-connexion** UDP ou ICMP), le boîtier applicance firewall-VPN ne confronte que le paquet initial de l'échange aux règles de la **politique de filtrage**. À la réception de tout paquet IP, préalablement à l'application des règles de la **politique de filtrage**, 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.

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 les exigences FDP_IFC.2 et FDP_IFF.1

6.1.2 Fonction de génération de données d'audit

Le boîtier applicance firewall-VPN gère simultanément plusieurs fichiers de trace destinés à recueillir les événements détectés par la fonction de journalisation. Plus particulièrement, il existe un fichier dédié pour l'enregistrement des événements liés à l'application de la fonction de filtrage (fichier Filtre).

La fonction de génération de données d'audit (sous-ensemble de la TOE) effectue des demandes d'enregistrements de traces à la fonction de journalisation (qui est hors TOE) par l'intermédiaire d'une file de messages ayant une capacité fixe du nombre d'éléments à journaliser suivant les builds :

- build S : 100
- build M : 256
- build L : 512
- build XL : 1024

En cas de débordement de cette dernière, la fonction de filtrage bloque le trafic afin d'éviter toute perte de traces.

La fonction de génération de données d'audit adresse les informations suivantes à la fonction de journalisation :

- adresse IP et port source,
- adresse IP et port destination,
- nom des interfaces source et destination,
- identifiant du boîtier applicance firewall-VPN,
- type de protocole et ICMP,
- identifiant de la règle,
- action appliquée.

Argumentaire : la fonction de génération de données d'audit satisfait l'exigence FAU_GEN.1. La limitation de la taille de la file de messages, et les actions associées, satisfont à l'exigence FAU_STG.3.

7 ANNEXE – 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.2.3.C. Elle doit être considérée comme « l'énoncé des exigences de sécurité des TO fourni en tant que partie de la ST », requis par l'exigence ASE_REQ.2.1D,

7.1 Introduction

En plus des quatre types d'opérations définies dans les Critères Communs (cf. [CC-01], § C.2, 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'é*ditorial 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 §5.1.1.

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.

7.2 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.

7.2.1 Exigences de contrôle des flux d'information

Fonction de filtrage

FDP_IFC.2 – Filtrage complet des flux d'information

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

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

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

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

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

FDP_IFF.1 – Fonction de filtrage

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

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

Affectation	*information flow control SFP* := la **politique de filtrage**
Raffinement + mise en forme	*subject and information* := équipements des réseaux interconnectés par le boîtier applicance firewall-VPN(*subjects*), les paquets IP (*information*) → les paquets IP entrants

Affectation	*list of subjects and information controlled under the indicated SFP, and, for each, the security attributes* := a. L'interface de réception, b. L'interface de destination, c. L'adresse IP source et destination du paquet et, partant de là, la machine source et la machine destination du paquet, d. Le numéro de protocole IP, e. La valeur du champ DSCP, f. Si le protocole est TCP ou UDP : le port source et destination, g. Si le protocole est ICMP : les champs 'type' et 'code' du message.

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

Affectation	*for each operation, the security attribute-based relationship that must hold between subject and information security attributes* := le paquet est autorisé si l'action de la première règle de filtrage applicable est 'passer'.

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

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

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

Affectation	*rules, based on security attributes, that explicitly authorise information flows* := si il existe des règles de filtrage implicites associées à ce paquet IP entrant

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

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

Fonction de génération de données d'audit

FAU_GEN.1 – Génération de données d'audit

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

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

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

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

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

Sélection	*minimum*, *basic*, *detailed*, *not specified* := *not specified*
Mise en forme	de l'item b)
Affectation	*other specifically defined auditable events* := application d'une règle de filtrage pour laquelle la génération d'un enregistrement d'audit est spécifiée.

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

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

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

Raffinement	*subject identity* := adresse IP source, et identité de l'**utilisateur** (si elle est connue)
Affectation	*other audit relevant information* := les informations d'audit complémentaires suivantes : a. adresse IP et port source, b. adresse IP et port destination, c. nom des interfaces sources et destination, d. identifiant du boîtier applicance firewall-VPN, e. type de protocole et ICMP, f. identifiant de la règle, g. action appliquée.

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

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].*

Raffinement	*The TSF* := la fonction de filtrage
Raffinement	*audit trail* := la quantité de traces
Affectation	*actions to be taken in case of possible audit storage failure* := entreprendre de bloquer un **paquet IP entrant** devant être tracé d'après la **politique de filtrage**
Affectation	*pre-defined limit* := le nombre d'éléments à journaliser suivant : a. build S : 100 b. build M : 256 c. build L : 512 d. build XL : 1024