Direction centrale de la sécurité des systèmes d'information

Profil de protection - Firewall d'interconnexion IP

Version	:	Version 3.0f
Date	:	Juin 2008
Classification	:	Public
Référence	:	PP-FWIP

Profil de protection enregistré et certifié par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) sous la référence DCSSI-PP-2008/02.

Historique du document

Version	Date	État	Modifications
2.0	Juillet 2005	Document de référence pour le lancement de l'évaluation	
2.0a	Septembre 2005	Document de référence pour le lancement de l'évaluation après phase de relecture et prise en compte des remarques.	Voir document *PP-FWIP-2_0-Fiche-Commentaires-Réponses DCSSI-ARKOON.doc*
2.0b	Septembre 2005	Document de référence pour le lancement de l'évaluation.	« Données sensibles » deviennent « Biens sensibles » Prise en compte de l'administration distante et de l'intégrité des données échangées avec la TOE via FPT_TDC.
2.1	Octobre 2005	Document de référence pour le lancement de l'évaluation.	Mise à jour des niveaux d'audit.
2.2	Mars 2006	Document repris suite aux re-commandations du rapport d'évaluation MELEZE_APE_1.1	
3.0	Avril 2008	Document de référence pour la validation.	Portage du profil de protection « Firewall d'interconnexion IP » de la version 2.3 vers la version 3.1r2 des Critères Communs. Modification de la fonction d'administration distante à la demande de la DCSSI.
3.0a	Avril 2008	Document de référence pour le lancement de l'évaluation.	Prise en compte remarques de la DCSSI suite relecture de validation.
3.0b	Mai 2008	Document de référence pour l'évaluation.	Suppression OSP.EAL & O.EAL à la demande de la DCSSI
3.0c & 3.0d	Mai 2008	Document de référence pour l'évaluation.	Prise en compte des remarques formulées dans le RTE.
3.0e & 3.0f	Juin 2008	Document de référence pour l'évaluation	Prise en compte des remarques formulées dans la fiche de revue du rapport APE, émise par la DCSSI.

Table des matières

Table des figures

Table des tableaux

1 Introduction

1.1 Identification du profil de protection

Titre :	Profil de protection - Firewall d'interconnexion IP
Auteur :	FIDENS
Version :	Version 3.0f

1.2 Contexte

Ce PP est réalisé sous l'égide de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI).

L'objectif est de fournir un cadre administratif à la certification de firewall d'interconnexion IP pour les besoins des secteurs public et privé en vue de leur qualification.

Le portage de ce profil protection de la version 2.3 vers la version 3.1r2 des Critères Communs a été réalisé par la la société FIDENS. La version précédente de ce profil de protection a été rédigée par la société ARKOON.

1.3 Présentation générale de la cible d'évaluation

Nota : on trouvera une description détaillée de la TOE en Annexe A.

1.3.1 Type de la TOE

Ce profil de protection (PP) exprime les objectifs de sécurité ainsi que les exigences fonctionnelles et d'assurance pour une cible d'évaluation (TOE) correspondant à un firewall permettant d'assurer le filtrage des flux dans le cadre de l'interconnexion de réseaux IP.

Ce firewall est un équipement matériel ayant vocation à être mis en coupure entre un réseau IP à protéger et un autre réseau IP. Cet équipement peut être administré localement ou depuis un poste d'administration distant.

Note d'application

Si un client logiciel destiné à l'administration et à la supervision du firewall est livré avec ce firewall, ce client logiciel doit être inclus dans le périmètre de la TOE.

1.3.2 Utilisation de la TOE

Cette TOE est destinée à participer à la mise en œuvre de la politique de sécurité associée à l'interconnexion d'un réseau protégé avec un autre réseau. Elle vise à conserver à ce réseau protégé son niveau de sécurité d'avant interconnexion, et à le défendre contre des attaques en provenance de l'autre réseau par un contrôle des flux d'informations en provenance ou à destination de ce réseau.

Les fonctions principales de la TOE sont :

- L'application d'une politique de filtrage ;
- L'audit et la journalisation des flux et de l'application de la politique de filtrage.

La mise en œuvre de cette politique de filtrage s'appuie sur des règles de filtrage qui permettent d'assurer :

- Un filtrage non contextuel : l'action de filtrage (acceptation, blocage, rejet, avec journalisation ou non) est déterminée en fonction du contenu d'un paquet réseau.
- Un filtrage contextuel : sur la base d'un premier filtrage non contextuel, la TOE établit un contexte et des règles de filtrage adaptées, basées sur les caractéristiques du flux identifié (origine, destinataire, protocoles). La connaissance de ce contexte permet à la TOE d'une part de gagner en performance, et d'autre part d'augmenter la pertinence du filtrage et sa précision.

Les fonctionnalités de filtrage, contextuel ou non, offertes par la TOE s'appliquent uniquement aux flux portés par le protocole IP et prennent en compte les couches réseau et transport.

De plus, pour son bon fonctionnement, la TOE met en œuvre les services suivants :

- La gestion de la politique de filtrage :
  - Définition de la politique de filtrage ;
  - Contrôle d'accès aux règles de filtrage ;
- La protection des opérations d'administration et de supervision :
  - Authentification locale des administrateurs ;
  - Contribution à la protection des flux d'administration à distance ;
  - Protection des flux de supervision ;
- L'audit des opérations d'administration et de supervision :
  - Audit et journalisation des opérations d'administration ;
  - Génération d'alarmes de sécurité ;
  - Supervision de la TOE ;
- La protection de l'accès aux paramètres de configuration de la TOE (paramètres de configuration réseau, données d'authentification, droits d'accès).

1.3.3 Particularités et caractéristiques de sécurité de la TOE

Ce PP a été rédigé conformément aux attentes et aux préconisations du document [QUA-STD]. Ce document définit le niveau standard comme un premier niveau de robustesse correspondant à un produit permettant de résister à un attaquant doté d'un potentiel d'attaque élémentaire au sens des Critères Communs.

Une cible de sécurité se réclamant conforme au PP peut présenter des fonctionnalités supplémentaires non prises en compte par ce PP : chiffrement IP, serveur d'authentification, passerelle anti-virus, ... Les fonctionnalités additionnelles et leur implémentation ne doivent pas remettre en cause les exigences du présent PP. Lors de la rédaction d'une cible de sécurité se réclamant conforme à ce profil de protection, ces fonctionnalités sont parfaitement exprimables et, le cas échéant, la cible pourra faire référence à tout autre profil de protection les couvrant (tel que [PP-CIP]).

1.3.4 Environnement matériel et logiciel

La sécurité de l'administration et de la supervision de la TOE repose sur son environnement, en particulier les postes utilisés pour l'administration distante.

Cet environnement doit:

- Reposer sur des postes d'administration distante de confiance.
- Contribuer à la sécurité des échanges entre les postes d'administration distante et la TOE.

2 Déclarations de conformité

2.1 Conformité de ce profil de protection

2.1.1 Conformité aux critères communs

Ce profil de protection est conforme à :

- La partie 2 des critères communs, version 3.1, révision 2, de septembre 2007 (cf. [CC2]).
- La partie 3 des critères communs, version 3.1, révision 2, de septembre 2007 (cf. [CC3]).

Aucune extension ou interprétation n'est retenue.

2.1.2 Conformité à un paquet d'assurance

Ce PP définit un ensemble d'exigences d'assurance correspondant au paquet EAL3 augmenté des composants suivants :

- ALC_FLR.3
- AVA_VAN.3

Ce niveau d'assurance sécurité est conforme au référentiel DCSSI « Processus de qualification d'un produit de sécurité - niveau standard » (cf. [QUA-STD]).

2.1.3 Conformité à un profil de protection

Ce profil de protection ne s'appuie sur aucun autre profil de protection.

2.2 Conformité des cibles de sécurité et profils de protection

Les ST et PP conformes à ce PP pourront annoncer un niveau de conformité « **démontrable** ».

Des notes d'application précisent quelles sont les hypothèses qui peuvent être transformées, partiellement ou en totalité, en OSP par les ST et PP conformes à ce PP. Ces notes d'application sont indiquées au niveau de chaque hypothèse concernée.

3 Définition du problème de sécurité

3.1 Biens

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

3.1.1 Biens protégés par la TOE

Lorsque le type de protection (partie *Protection*) est suivi de "(opt.)" pour optionnel, cela signifie que cette protection doit être fournie par la TOE, mais qu'elle n'est pas systématiquement appliquée par la TOE.

D.DONNEES_RESEAU_PRIVE

La TOE contribue à protéger des biens utilisateurs de type informations et services du réseau protégé, par le filtrage des flux susceptibles d'accéder ou de modifier ces biens.

Protection: confidentialité (opt.), intégrité (opt.) ou disponibilité (opt.)

3.1.2 Biens sensibles de la TOE

D.POLITIQUE_FILTRAGE

Les politiques de filtrage et les contextes de connexion définissent les traitements (filtrage implicite et services de sécurité) à effectuer sur les paquets IP traités par le firewall.

Cela inclut la politique d'audit des flux utilisateurs.

Protection:

- authenticité lorsque les politiques (et leurs contextes) transitent de l'endroit où l'administrateur les définit à distance vers le firewall;
- intégrité des politiques (et des contextes) stockées sur le firewall,
- cohérence entre la politique définie (et son contexte) et celle appliquée.
- confidentialité.

D.AUDIT_FLUX

Données générées par la politique d'audit pour permettre de retracer les flux traités par le firewall.

Protection: intégrité.

D.PARAM_CONFIG

Les paramètres de configuration du firewall comprennent entre autres:

- les adresses IP internes aux réseaux protégés et les tables de routage (configuration réseau);
- les données d'authentification et d'intégrité;
- les droits d'accès ;
- la politique d'audit des opérations d'administration.

Protection: confidentialité et intégrité.

D.AUDIT_ADMIN

Données générées par la politique d'audit pour permettre de retracer les opérations d'administration effectuées sur la TOE.

Protection: intégrité.

D.ALARMES

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

Protection: intégrité.

3.2 Menaces

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

Les différents agents menaçants sont :

- les attaquants internes : tout utilisateur autorisé du réseau protégé ;
- les attaquants externes : toute personne extérieure aux réseaux protégés.

Conformément à A.ADMIN, les administrateurs ne sont pas considérés comme des attaquants potentiels de la TOE.

3.2.1 Menaces sur le fonctionnement de la TOE

T.DYSFONCTIONNEMENT

Un attaquant met la TOE dans un état de dysfonctionnement qui contribue à rendre les services offerts par la TOE indisponibles ou la met dans un état non sûr.

Biens menacés : D.DONNEES_RESEAU_PRIVE, D.POLITIQUE_FILTRAGE, D.AUDIT_FLUX, D.PARAM_CONFIG, D.AUDIT_ADMIN, D.ALARMES.

3.2.2 Menaces sur la politique de filtrage

T.MODIFICATION_POL_FILTRAGE

Un attaquant modifie illégalement la politique de filtrage et/ou les contextes de connexion.

Bien menacé : D.POLITIQUE_FILTRAGE

T.DIVULGATION_POL_FILTRAGE

Un attaquant récupère illégalement la politique de filtrage et/ou les contextes de connexion.

Bien menacé : D.POLITIQUE_FILTRAGE

3.2.3 Menaces sur les paramètres de configuration

T.MODIFICATION_PARAMETRES

Un attaquant modifie illégalement les paramètres de configuration de la TOE.

Bien menacé : D.PARAM_CONFIG

T.DIVULGATION_PARAMETRES

Un attaquant accède illégalement aux paramètres de configuration de la TOE.

Bien menacé : D.PARAM_CONFIG

3.2.4 Menaces sur les traces d'audit des flux

T.MODIFICATION_AUDIT_FLUX

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

Bien menacé : D.AUDIT_FLUX

3.2.5 Menaces sur les alarmes

T.MODIFICATION_ALARMES

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

Bien menacé : D.ALARMES

3.2.6 Menaces sur les traces d'audit d'administration

T.MODIFICATION_AUDIT_ADMIN

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

Bien menacé : D.AUDIT_ADMIN

3.2.7 Menaces sur l'ensemble des biens lors du recyclage de la TOE

T.CHANGEMENT_CONTEXTE

Un attaquant ou un administrateur d'un nouveau réseau protégé, prend connaissance, par accès direct à la TOE, des biens sensibles de la TOE lors d'un changement de contexte d'utilisation (affectation du firewall à un nouveau réseau, maintenance,...).

Biens menacés : D.DONNEES_RESEAU_PRIVE, D.POLITIQUE_FILTRAGE, D.AUDIT_FLUX, D.PARAM_CONFIG, D.AUDIT_ADMIN, D.ALARMES.

3.3 Politiques de sécurité organisationnelles

Les politiques de sécurité organisationnelles présentes dans cette section permettent de définir les services rendus par la TOE au système d'information et les contraintes à remplir pour la Qualification niveau Standard des produits de sécurité par le SGDN/DCSSI.

3.3.1 Politiques relatives aux services offerts

OSP.FILTRAGE

La TOE doit appliquer la politique de filtrage définie par l'administrateur de sécurité, sur la base de la politique de sécurité du système d'information.

Dans le mode contextuel, la TOE doit pouvoir établir et appliquer à son niveau des règles de filtrage basées sur les caractéristiques des flux traités (par exemple: origine, destinataire, protocole applicatif).

La TOE doit également permettre de visualiser les règles de filtrage courantes.

OSP.AUDIT_FLUX

La TOE doit tracer les flux qu'elle traite de manière:

- à enregistrer au minimum les événements générés lors du rejet d'un flux;
- à permettre à l'administrateur d'ordonner chronologiquement les événements enregistrés;
- à permettre à l'administrateur d'attribuer un événement à un acteur;
- à permettre la visualisation des journaux d'audit et la sélection des événements enregistrés afin de s'assurer de la pertinence de la politique de filtrage et de sa bonne instanciation au niveau du firewall.

OSP.GESTION_ROLES

La TOE doit permettre de définir différents rôles d'agent / officier de sécurité, administrateur de sécurité, auditeur, administrateur système et réseau.

Elle permet également de fournir les traces d'audits des actions réalisées par ces rôles.

3.3.2 Politiques issues de la réglementation applicable

OSP.CRYPTO

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

3.4 Hypothèses

3.4.1 Hypothèses sur l'usage attendu de la TOE

A.AUDIT

Il est supposé que l'auditeur consulte régulièrement les événements d'audit générés par la TOE. La mémoire stockant les événements d'audit est gérée de telle sorte que les administrateurs ne perdent pas d'événements.

A.ALARME

Il est supposé que l'administrateur de sécurité analyse et traite les alarmes de sécurité générées et remontées par la TOE.

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

A.ADMIN

Les administrateurs sont des personnes non hostiles. Ils disposent des moyens nécessaires à la réalisation de leurs tâches, sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.

Du fait de cette hypothèse, ces administrateurs ne sont pas considérés comme des attaquants vis-à-vis des menaces identifiées dans ce document.

A.LOCAL

Les équipements contenant les services de la TOE (firewall), les équipements d'administration), ainsi que tous supports contenant les biens sensibles de la TOE (papier, disquettes, sauvegardes,...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

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

A.MAITRISE_CONFIGURATION

L'administrateur dispose des moyens de contrôler la configuration matérielle et logicielle de la TOE par rapport à un état de référence, ou de la régénérer dans un état sûr.

Cette hypothèse s'étend à la maîtrise du bien sensible "Politique de filtrage" dès lors que la TOE ne peut à elle seule garantir son intégrité.

A.STATION_ADMIN_SÛRE

Les stations utilisées par les administrateurs pour administrer à distance la TOE sont de confiance.

4 Objectifs de sécurité

4.1 Objectifs de sécurité pour la TOE

4.1.1 Objectifs sur les services de sécurité rendus par la TOE

O.APPLICATION_POL_FILTRAGE

La TOE doit appliquer la politique de filtrage spécifiée par l'administrateur et les règles de filtrage établies par la TOE (mode contextuel). Cette politique peut concerner à la fois les flux utilisateurs et les flux d'administration.

O.VISUALISATION_POL

La TOE doit permettre aux administrateurs de sécurité de visualiser unitairement la politique de filtrage et les contextes de connexion présents sur le firewall.

O.COHERENCE_POL

Dans le cas d'une administration à distance, la TOE doit garantir la cohérence entre la définition des politiques de filtrage et les politiques appliquées sur le firewall.

O.AUDIT_FLUX

La TOE doit tracer les flux qu'elle traite de manière:

- à enregistrer au minimum les événements générés lors du rejet d'un flux;
- à permettre à l'administrateur d'ordonner chronologiquement les événements enregistrés;
- à permettre à l'administrateur d'attribuer un événement à un acteur;
- à permettre la visualisation des journaux d'audit et la sélection des événements enregistrés afin de s'assurer de la pertinence de la politique de filtrage et de sa bonne instanciation au niveau du firewall.

O.GESTION_ROLES

La TOE doit permettre de définir les différents rôles et associer de manière sûre les rôles aux utilisateurs.

4.1.2 Objectifs de sécurité sur le fonctionnement de la TOE

4.1.2.1 Protection de la politique de filtrage

O.PROTECTION_POL_FILTRAGE

La TOE doit contrôler l'accès (consultation, modification) aux règles de filtrage et aux contextes de connexion sur le firewall.

4.1.2.2 Audit et alarmes

Flux

O.PROTECTION_AUDIT_FLUX

La TOE doit contrôler l'accès sur le firewall (consultation, modification) aux traces d'audit des flux qu'elle enregistre et doit permettre à un auditeur de détecter la perte d'événements d'audit des flux (en utilisant un compteur par exemple).

Événements d'administration

O.AUDIT_ADMIN

La TOE doit générer des traces d'audit des opérations effectuées par les administrateurs du firewall. La TOE doit permettre la visualisation de ces traces d'audit.

La génération des traces doit permettre l'imputabilité des événements d'administration enregistrés.

O.PROTECTION_AUDIT_ADMIN

La TOE doit contrôler l'accès sur le firewall (consultation, modification) aux traces d'audit d'administration qu'elle enregistre et doit permettre à un auditeur de détecter la perte d'événements d'audit d'administration (en utilisant un compteur par exemple).

Alarmes

O.ALARMES

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

O.PROTECTION_ALARMES

La TOE doit contrôler l'accès sur le firewall (consultation, modification) aux alarmes de sécurité (à destination des administrateurs de sécurité locaux ou à distance) qu'elle génère et doit permettre à un administrateur de sécurité de détecter la perte d'alarmes de sécurité (en utilisant un compteur par exemple).

4.1.2.3 Protection de l'administration distante

O.PROTECTION_FLUX_ADMIN

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

La TOE doit également contribuer à protéger les flux contre le rejeu.

4.1.2.4 Configuration de la TOE

O.PROTECTION_PARAM

La TOE doit contrôler l'accès sur le firewall (consultation, modification) aux paramètres de configuration, aux droits d'accès, aux données d'authentification et aux éléments permettant de gérer l'intégrité des flux d'administration.

4.1.2.5 Supervision de la TOE

O.SUPERVISION

La TOE doit permettre à l'administrateur système et réseau de consulter son état opérationnel.

O.IMPACT_SUPERVISION

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

4.1.2.6 Recyclage de la TOE

O.RECYCLAGE_TOE

La TOE doit fournir une fonctionnalité qui permet de rendre indisponibles ses biens sensibles préalablement à un changement de contexte d'utilisation: nouvelle affectation, maintenance,...

4.1.2.7 Identification et authentification des administrateurs

O.AUTHENTIFICATION_ADMIN

La TOE doit assurer l'identification et l'authentification des administrateurs de la TOE qui se connecte à la TOE en local ou à partir d'une station d'administration distante.

4.2 Objectifs de sécurité pour l'environnement opérationnel

4.2.1 Objectifs de sécurité sur la conception de la TOE

OE.CONCEPTION_CRYPTO

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

4.2.2 Objectifs de sécurité sur l'exploitation de la TOE

4.2.2.1 Environnement physique

OE.PROTECTION_LOCAL

Les équipements contenant les services de la TOE (firewall et équipements d'administration), ainsi que tous supports contenant les biens sensibles de la TOE (papier, disquettes, sauvegardes,...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

4.2.2.2 Administration de la TOE

OE.ADMIN

Les administrateurs doivent être formés aux tâches qu'ils ont à réaliser sur la TOE et être de confiance.

.

OE.STATION_ADMIN_SÛRE

Les stations utilisées par les administrateurs pour administrer à distance la TOE doivent être de confiance.

Elles doivent contribuer garantir à l'authenticité, l'intégrité et la confidentialité des flux d'administration à distance. La protection en confidentialité n'est pas systématiquement appliquée si les données passant dans le flux ne sont pas confidentielles.

4.2.2.3 Elles doivent également contribuer à protéger les flux contre le rejeu.Gestion des traces d'audit et des alarmes

OE.GESTION_TRACES_AUDIT

L'auditeur doit régulièrement analyser les événements d'audit enregistrés par la TOE et agir en conséquence. La mémoire stockant les événements d'audit est gérée de telle sorte que les administrateurs ne perdent pas d'événements.

En outre, les audits doivent faire l'objet de sauvegarde et d'archivage afin que l'impact de leur suppression accidentelle ou volontaire soit limité.

OE.TRAITE_ALARME

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

4.2.2.4 Contrôle de la TOE

OE.INTEGRITE_TOE

L'administrateur dispose des moyens de contrôler la configuration matérielle et logicielle de la TOE par rapport à un état de référence, ou de la régénérer dans un état sûr.

Cet objectif s'étend à la maîtrise du bien sensible "Politique de filtrage" dès lors que la TOE ne peut à elle seule garantir son intégrité.

4.3 Argumentaire

4.3.1 Couverture des menaces

4.3.1.1 Menaces sur le fonctionnement des services de la TOE

T.DYSFONCTIONNEMENT

Pour prévenir la menace, la TOE doit:

- aucune action

Pour se protéger, la TOE doit:

- aucune action

Pour détecter l'occurrence de la menace, la TOE doit:

- offrir un service de supervision (O.SUPERVISION) tout en ne dévoilant pas ses éléments sensibles (O.IMPACT_SUPERVISION).

Pour limiter l'impact de la menace, la TOE doit:

- pouvoir être remise dans un état précédemment validé (OE.INTEGRITE_TOE)

4.3.1.2 Menaces sur la politique de filtrage

T.MODIFICATION_POL_FILTRAGE

Pour prévenir la menace, la TOE doit:

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL)
- être utilisée par des administrateurs de confiance (OE.ADMIN)
- être administrée depuis des postes de confiance (OE.STATION_ADMIN_SÛRE)

Pour se protéger, la TOE doit:

- permettre de filtrer les flux d'administration (O.APPLICATION_POL_FILTRAGE)
- offrir un contrôle d'accès à ses objets sensibles (O.PROTECTION_POL_FILTRAGE)
- protéger les flux d'administration distante (O.PROTECTION_FLUX_ADMIN)
- authentifier l'administrateur de la TOE (O.AUTHENTIFICATION_ADMIN)

Pour détecter l'occurrence de la menace, la TOE doit:

- générer des traces d'audit et des alarmes (O.AUDIT_ADMIN, O.AUDIT_FLUX et O.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit:

- pouvoir être remise dans un état précédemment validé (OE.INTEGRITE_TOE)

T.DIVULGATION_POL_FILTRAGE

Pour prévenir la menace, la TOE doit:

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL)
- être utilisée par des administrateurs de confiance (OE.ADMIN)
- être administrée depuis des postes de confiance (OE.STATION_ADMIN_SÛRE)

Pour se protéger, la TOE doit:

- permettre de filtrer les flux d'administration (O.APPLICATION_POL_FILTRAGE)
- offrir un contrôle d'accès à ses objets sensibles (O.PROTECTION_POL_FILTRAGE)
- protéger les flux d'administration distante (O.PROTECTION_FLUX_ADMIN)
- authentifier l'administrateur de la TOE (O.AUTHENTIFICATION_ADMIN)

Pour détecter l'occurrence de la menace, la TOE doit:

- générer des traces d'audit et des alarmes (O.AUDIT_ADMIN, O.AUDIT_FLUX et O.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit:

- aucune action

4.3.1.3 Menaces sur les paramètres de configuration

T.MODIFICATION_PARAMETRES

Pour prévenir la menace, la TOE doit:

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL)
- être utilisée par des administrateurs de confiance (OE.ADMIN)
- être administrée depuis des postes de confiance (OE.STATION_ADMIN_SÛRE)

Pour se protéger, la TOE doit:

- permettre de filtrer les flux d'administration (O.APPLICATION_POL_FILTRAGE)
- offrir un contrôle d'accès à ses objets sensibles (O.PROTECTION_PARAM)
- protéger les flux d'administration distante (O.PROTECTION_FLUX_ADMIN)
- authentifier l'administrateur de la TOE (O.AUTHENTIFICATION_ADMIN)

Pour détecter l'occurrence de la menace, la TOE doit:

- générer des traces d'audit et des alarmes (O.AUDIT_ADMIN, O.AUDIT_FLUX et O.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit:

- pouvoir être remise dans un état précédemment validé (OE.INTEGRITE_TOE)

T.DIVULGATION_PARAMETRES

Pour prévenir la menace, la TOE doit:

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL)
- être utilisée par des administrateurs de confiance (OE.ADMIN)
- être administrée depuis des postes de confiance (OE.STATION_ADMIN_SÛRE)
- être recyclée lors d'un changement de contexte (O.RECYCLAGE_TOE)

Pour se protéger, la TOE doit:

- permettre de filtrer les flux d'administration (O.APPLICATION_POL_FILTRAGE)
- offrir un contrôle d'accès à ses objets sensibles (O.PROTECTION_PARAM)
- protéger les flux d'administration distante (O.PROTECTION_FLUX_ADMIN)
- authentifier l'administrateur de la TOE (O.AUTHENTIFICATION_ADMIN)

Pour détecter l'occurrence de la menace, la TOE doit:

- générer des traces d'audit et des alarmes (O.AUDIT_ADMIN, O.AUDIT_FLUX et O.ALARMES). L'administrateur de sécurité doit les analyser et les traiter (OE.TRAITE_ALARMES).

Pour limiter l'impact de la menace, la TOE doit:

- aucune action

4.3.1.4 Menaces sur les traces d'audit des flux

T.MODIFICATION_AUDIT_FLUX

Pour prévenir la menace, la TOE doit:

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL)
- être utilisée par des administrateurs de confiance (OE.ADMIN)
- être administrée depuis des postes de confiance (OE.STATION_ADMIN_SÛRE)

Pour se protéger, la TOE doit:

- permettre de filtrer les flux d'administration (O.APPLICATION_POL_FILTRAGE)
- offrir un contrôle d'accès à ses objets sensibles (O.PROTECTION_AUDIT_FLUX)
- protéger les flux d'administration distante (O.PROTECTION_FLUX_ADMIN)
- authentifier l'administrateur de la TOE (O.AUTHENTIFICATION_ADMIN)

Pour détecter l'occurrence de la menace, la TOE doit:

- permettre de détecter la perte de traces d'audits (O.PROTECTION_AUDIT_FLUX)

Pour limiter l'impact de la menace, la TOE doit:

- s'appuyer sur des mesures de sauvegarde et archivage des traces d'audit (OE.GESTION_TRACES_AUDIT)

4.3.1.5 Menaces sur les alarmes

T.MODIFICATION_ALARMES

Pour prévenir la menace, la TOE doit:

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL)
- être utilisée par des administrateurs de confiance (OE.ADMIN)
- être administrée depuis des postes de confiance (OE.STATION_ADMIN_SÛRE)

Pour se protéger, la TOE doit:

- permettre de filtrer les flux d'administration (O.APPLICATION_POL_FILTRAGE)
- offrir un contrôle d'accès à ses objets sensibles (O.PROTECTION_ALARMES)
- protéger les flux d'administration distante (O.PROTECTION_FLUX_ADMIN)
- authentifier l'administrateur de la TOE (O.AUTHENTIFICATION_ADMIN)

Pour détecter l'occurrence de la menace, la TOE doit:

- permettre de détecter la perte d'alarmes (O.PROTECTION_ALARMES)

Pour limiter l'impact de la menace, la TOE doit:

- aucune action

4.3.1.6 Menaces sur les traces d'audit d'administration

T.MODIFICATION_AUDIT_ADMIN

Pour prévenir la menace, la TOE doit:

- être déployée dans un local sécurisé (OE.PROTECTION_LOCAL)
- être utilisée par des administrateurs de confiance (OE.ADMIN)
- être utilisée sur des postes de confiance (OE.STATION_ADMIN_SÛRE)

Pour se protéger, la TOE doit:

- permettre de filtrer les flux d'administration (O.APPLICATION_POL_FILTRAGE)
- offrir un contrôle d'accès à ses objets sensibles (O.PROTECTION_AUDIT_ADMIN)
- protéger les flux d'administration distante (O.PROTECTION_FLUX_ADMIN)
- authentifier l'administrateur de la TOE (O.AUTHENTIFICATION_ADMIN)

Pour détecter l'occurrence de la menace, la TOE doit:

- permettre de détecter la perte de traces d'audits (O.PROTECTION_AUDIT_ADMIN)

Pour limiter l'impact de la menace, la TOE doit:

- s'appuyer sur des mesures de sauvegarde et archivage des traces d'audit (OE.GESTION_TRACES_AUDIT)

4.3.1.7 Menaces sur l'ensemble des biens lors du recyclage de la TOE

T.CHANGEMENT_CONTEXTE

Pour prévenir la menace, la TOE doit:

- fournir une fonctionnalité qui permet de rendre indisponibles ses biens sensibles préalablement à un changement de contexte d'utilisation: nouvelle affectation, maintenance,... (O.RECYCLAGE_TOE)

Pour se protéger, la TOE doit:

- aucune action

Pour détecter l'occurrence de la menace, la TOE doit:

- aucune action

Pour limiter l'impact de la menace, la TOE doit:

- aucune action

4.3.2 Couverture des politiques de sécurité organisationnelles

OSP.FILTRAGE

Cette OSP est directement traduite en objectifs sur les services de sécurité rendus par la TOE: O.APPLICATION_POL_FILTRAGE, O.VISUALISATION_POL, et enfin O.COHERENCE_POL dès lors que la gestion de la politique de filtrage est faite non pas directement sur le firewall, mais sur une station d'administration distante.

OSP.AUDIT_FLUX

Cette OSP est directement traduite en objectif sur les services de sécurité rendus par la TOE (O.AUDIT_FLUX)

OSP.GESTION_ROLES

Cette OSP est directement traduite par:

- l'objectif de gestion des rôles O.GESTION_ROLES
- l'objectif d'audit des actions effectuées par les administrateurs O.AUDIT_ADMIN

OSP.CRYPTO

Cette OSP est directement traduite en objectif sur la conception du produit OE.CONCEPTION_CRYPTO.

4.3.3 Couverture des hypothèses

A.ADMIN

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

A.LOCAL

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

A.AUDIT

Cette hypothèse se traduit par OE.GESTION_TRACES_AUDIT.

A.ALARME

Cette hypothèse se traduit par OE.TRAITE_ALARME.

A.MAITRISE_CONFIGURATION

Cette hypothèse se traduit par l'objectif OE.INTEGRITE_TOE

A.STATION_ADMIN_SÛRE

Cette hypothèse est couverte par OE.STATION_ADMIN_SÛRE

4.3.4 Tables de couverture avec les objectifs de sécurité

4.3.4.1 Couverture des menaces

Menaces	Objectifs de sécurité	Argumentaire
T.DYSFONCTIONNEMENT	O.SUPERVISION, OE.INTEGRITE_TOE, O.IMPACT_SUPERVISION	Section 4.3.1
T.MODIFICATION_POL_FILTRAGE	OE.PROTECTION_LOCAL, OE.ADMIN, OE.STATION_ADMIN_SÛRE, OE.INTEGRITE_TOE, OE.TRAITE_ALARME, O.AUTHENTIFICATION_ADMIN, O.PROTECTION_POL_FILTRAGE, O.PROTECTION_FLUX_ADMIN, O.APPLICATION_POL_FILTRAGE, O.AUDIT_ADMIN, O.AUDIT_FLUX, O.ALARMES	Section 4.3.1

Menaces	Objectifs de sécurité	Argumentaire
T.DIVULGATION_POL_FILTRAGE	OE.PROTECTION_LOCAL, OE.ADMIN, OE.STATION_ADMIN_SÛRE, OE.TRAITE_ALARME, O.AUTHENTIFICATION_ADMIN, O.APPLICATION_POL_FILTRAGE, O.PROTECTION_POL_FILTRAGE, O.PROTECTION_FLUX_ADMIN, O.AUDIT_ADMIN, O.AUDIT_FLUX, O.ALARMES	Section 4.3.1
T.MODIFICATION_PARAMETRES	OE.PROTECTION_LOCAL, OE.ADMIN, OE.STATION_ADMIN_SÛRE, OE.TRAITE_ALARME, O.AUTHENTIFICATION_ADMIN, O.APPLICATION_POL_FILTRAGE, O.PROTECTION_PARAM, O.AUDIT_ADMIN, O.AUDIT_FLUX, O.ALARMES, OE.INTEGRITE_TOE, O.PROTECTION_FLUX_ADMIN	Section 4.3.1
T.DIVULGATION_PARAMETRES	OE.PROTECTION_LOCAL, OE.ADMIN, OE.STATION_ADMIN_SÛRE, OE.TRAITE_ALARME, O.AUTHENTIFICATION_ADMIN, O.RECYCLAGE_TOE, O.APPLICATION_POL_FILTRAGE, O.PROTECTION_PARAM, O.AUDIT_ADMIN, O.AUDIT_FLUX, O.ALARMES, O.PROTECTION_FLUX_ADMIN	Section 4.3.1
T.MODIFICATION_AUDIT_FLUX	OE.PROTECTION_LOCAL, OE.ADMIN, OE.STATION_ADMIN_SÛRE, O.AUTHENTIFICATION_ADMIN, O.APPLICATION_POL_FILTRAGE, OE.GESTION_TRACES_AUDIT, O.PROTECTION_AUDIT_FLUX, O.PROTECTION_FLUX_ADMIN	Section 4.3.1
T.MODIFICATION_ALARMES	OE.PROTECTION_LOCAL, OE.ADMIN, OE.STATION_ADMIN_SÛRE, O.AUTHENTIFICATION_ADMIN, O.APPLICATION_POL_FILTRAGE, O.PROTECTION_FLUX_ADMIN, O.PROTECTION_ALARMES	Section 4.3.1
T.MODIFICATION_AUDIT_ADMIN	OE.PROTECTION_LOCAL, OE.ADMIN, OE.STATION_ADMIN_SÛRE, O.AUTHENTIFICATION_ADMIN, O.APPLICATION_POL_FILTRAGE, OE.GESTION_TRACES_AUDIT, O.PROTECTION_FLUX_ADMIN, O.PROTECTION_AUDIT_ADMIN	Section 4.3.1
T.CHANGEMENT_CONTEXTE	O.RECYCLAGE_TOE	Section 4.3.1

Tableau 1 menaces vers objectifs de sécurité

Objectifs de sécurité	Menaces
O.APPLICATION_POL_FILTRAGE	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES, T.MODIFICATION_AUDIT_FLUX, T.MODIFICATION_ALARMES, T.MODIFICATION_AUDIT_ADMIN
O.VISUALISATION_POL	
O.COHERENCE_POL	
O.AUDIT_FLUX	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES
O.GESTION_ROLES	
O.PROTECTION_POL_FILTRAGE	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE
O.PROTECTION_AUDIT_FLUX	T.MODIFICATION_AUDIT_FLUX
O.AUDIT_ADMIN	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES
O.PROTECTION_AUDIT_ADMIN	T.MODIFICATION_AUDIT_ADMIN

Objectifs de sécurité	Menaces
O.ALARMES	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES
O.PROTECTION_ALARMES	T.MODIFICATION_ALARMES
O.PROTECTION_FLUX_ADMIN	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES, T.MODIFICATION_AUDIT_FLUX, T.MODIFICATION_ALARMES, T.MODIFICATION_AUDIT_ADMIN
O.PROTECTION_PARAM	T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES
O.SUPERVISION	T.DYSFONCTIONNEMENT
O.IMPACT_SUPERVISION	T.DYSFONCTIONNEMENT
O.RECYCLAGE_TOE	T.CHANGEMENT_CONTEXTE, T.DIVULGATION_PARAMETRES
OE.STATION_ADMIN_SÛRE	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES, T.MODIFICATION_AUDIT_FLUX, T.MODIFICATION_ALARMES, T.MODIFICATION_AUDIT_ADMIN
O.AUTHENTIFICATION_ADMIN	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES, T.MODIFICATION_AUDIT_FLUX, T.MODIFICATION_ALARMES, T.MODIFICATION_AUDIT_ADMIN
OE.CONCEPTION_CRYPTO	
OE.PROTECTION_LOCAL	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES, T.MODIFICATION_AUDIT_FLUX, T.MODIFICATION_ALARMES, T.MODIFICATION_AUDIT_ADMIN
OE.ADMIN	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES, T.MODIFICATION_AUDIT_FLUX, T.MODIFICATION_ALARMES, T.MODIFICATION_AUDIT_ADMIN
OE.GESTION_TRACES_AUDIT	T.MODIFICATION_AUDIT_FLUX, T.MODIFICATION_AUDIT_ADMIN
OE.TRAITE_ALARME	T.MODIFICATION_POL_FILTRAGE, T.DIVULGATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES, T.DIVULGATION_PARAMETRES
OE.INTEGRITE_TOE	T.DYSFONCTIONNEMENT, T.MODIFICATION_POL_FILTRAGE, T.MODIFICATION_PARAMETRES

Tableau 2 objectifs de sécurité vers menaces

4.3.4.2 Couverture des hypothèses

Hypothèses	Objectifs de sécurité pour l'environnement	Argumentaire
A.ADMIN	OE.ADMIN	Section 4.3.3
A.LOCAL	OE.PROTECTION_LOCAL	Section 4.3.3
A.AUDIT	OE.GESTION_TRACES_AUDIT	Section 4.3.3
A.ALARME	OE.TRAITE_ALARME	Section 4.3.3
A.MAITRISE_CONFIGURATION	OE.INTEGRITE_TOE	Section 4.3.3

Hypothèses	Objectifs de sécurité pour l'environnement	Argumentaire
A.STATION_ADMIN_SÛRE	OE.STATION_ADMIN_SÛRE	Section 4.3.3

Tableau 3 hypothèses vers objectifs de sécurité pour l'environnement

Objectifs de sécurité pour l'environnement	Hypothèses
OE.CONCEPTION_CRYPTO	
OE.PROTECTION_LOCAL	A.LOCAL
OE.ADMIN	A.ADMIN
OE.STATION_ADMIN_SÛRE	A.STATION_ADMIN_SÛRE
OE.GESTION_TRACES_AUDIT	A.AUDIT
OE.TRAITE_ALARME	A.ALARME
OE.INTEGRITE_TOE	A.MAITRISE_CONFIGURATION

Tableau 4 objectifs de sécurité pour l'environnement vers hypothèses

4.3.4.3 Couverture des politiques de sécurité organisationnelles

Politiques de sécurité organi-sationnelles	Objectifs de sécurité	Argumentaire
OSP.FILTRAGE	O.APPLICATION_POL_FILTRAGE, O.COHERENCE_POL, O.VISUALISATION_POL	Section 4.3.2
OSP.AUDIT_FLUX	O.AUDIT_FLUX	Section 4.3.2
OSP.GESTION_ROLES	O.GESTION_ROLES, O.AUDIT_ADMIN	Section 4.3.2
OSP.CRYPTO	OE.CONCEPTION_CRYPTO	Section 4.3.2

Tableau 5 politiques de sécurité organisationnelles vers objectifs de sécurité

Objectifs de sécurité	Politiques de sécurité organisationnelles
O.APPLICATION_POL_FILTRAGE	OSP.FILTRAGE
O.VISUALISATION_POL	OSP.FILTRAGE
O.COHERENCE_POL	OSP.FILTRAGE
O.AUDIT_FLUX	OSP.AUDIT_FLUX
O.GESTION_ROLES	OSP.GESTION_ROLES
O.PROTECTION_POL_FILTRAGE	
O.PROTECTION_AUDIT_FLUX	
O.AUDIT_ADMIN	OSP.GESTION_ROLES
O.PROTECTION_AUDIT_ADMIN	
O.ALARMES	

Objectifs de sécurité	Politiques de sécurité organisationnelles
O.PROTECTION_ALARMES	
O.PROTECTION_FLUX_ADMIN	
O.PROTECTION_PARAM	
O.SUPERVISION	
O.IMPACT_SUPERVISION	
O.RECYCLAGE_TOE	
O.AUTHENTIFICATION_ADMIN	
OE.CONCEPTION_CRYPTO	OSP.CRYPTO
OE.PROTECTION_LOCAL	
OE.ADMIN	
OE.STATION_ADMIN_SÛRE	
OE.GESTION_TRACES_AUDIT	
OE.INTEGRITE_TOE	

Tableau 6 objectifs de sécurité vers politiques de sécurité organisationnelles

5 Définition des composants étendus

Sans objet.

6 Exigences de sécurité des TI

6.1 Définitions

Le schéma ci-après présente les interactions entres les éléments utilisés dans les SFR.

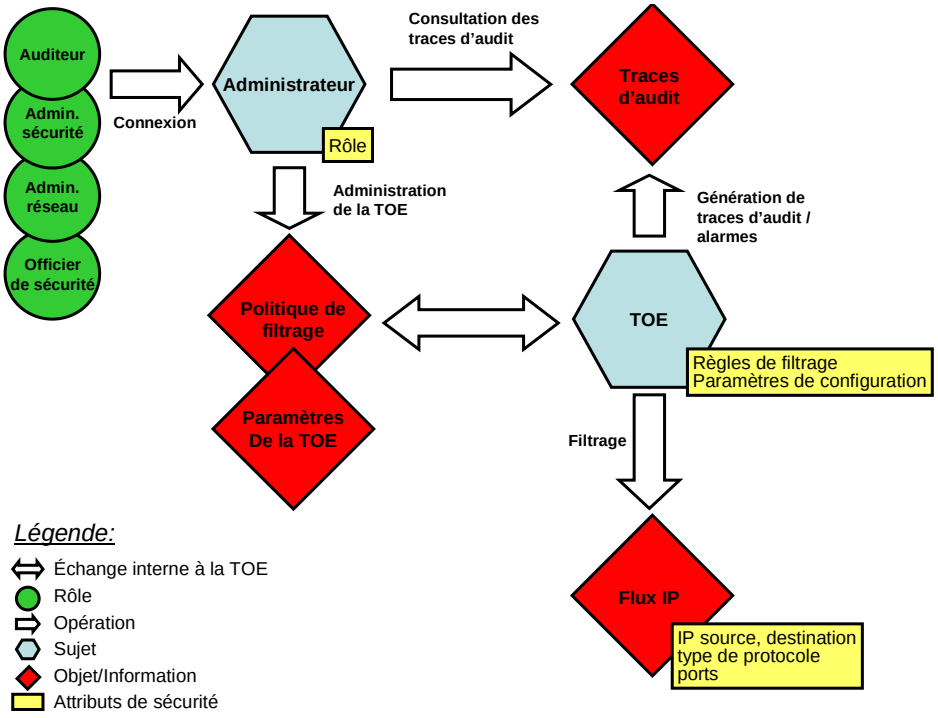

Figure 1: representation des interactions entre les elements definies dans les SFR

Ces éléments sont listés ci-après.

Sujets

- La TOE.
- Les administrateurs.

Objets

- Les règles de la politique de filtrage.
- Les biens sensibles du firewall.
- Les traces d'audit.
- Les paramètres de la TOE.

Informations

- Les flux IP utilisateurs.
- Les flux applicatifs sur TCP, UDP et ICMP.
- Les flux d'administrations.

Opérations

Opération concernant le contrôle des flux :

- Application de la politique de filtrage.

Opérations concernant l'accès aux règles de la politique de filtrage :

- Lire, insérer, modifier, supprimer.

Opérations concernant l'accès aux biens sensibles (les objets) du firewall :

- Effacer.

Attributs de sécurité

- Adresses IP source et destination des paquets IP.
- Types de protocole.
- Ports de communications.
- Rôle des administrateurs (agent/officier de sécurité, administrateur de sécurité, administrateur système et réseaux, auditeur).
- Paramètres de configuration de la TOE.

Entités externes

- Stations d'administration distantes.

6.2 Exigences de sécurité fonctionnelles pour la TOE

6.2.1 Services rendus par la TOE

6.2.1.1 Filtrage Flux

FDP_IFC.2-Filtrage_Flux Complete information flow control

FDP_IFC.2.1-Filtrage_Flux

The TSF shall enforce the **politique de filtrage (et les règles liées aux contextes de connexion en mode contextuel)** on

Subject:

- **la TOE.**

Information:

- **les flux IP utilisateurs,**
- **les flux applicatifs sur TCP, UDP et ICMP,**
- **les flux d'administration.**

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2-Filtrage_Flux

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

FDP_IFF.1-Filtrage_Flux Simple security attributes

FDP_IFF.1.1-Filtrage_Flux

The TSF shall enforce the **politique de filtrage (et les règles liées aux contextes de connexion en mode contextuel)** based on the following types of subject and information security attributes:

Subject security attributes:

- **règles de filtrage,**
- **paramètres de configuration de la TOE utilisés dans les règles de filtrage,**

Information Security attributes:

- **les adresses IP source et destination des paquets IP,**
- **les types de protocole,**
- **les ports de communication.**

Note d'application

Les ST conformes à ce PP devront préciser les paramètres de configuruation utilisés.

FDP_IFF.1.2-Filtrage_Flux

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

- **les attributs du paquet IP traité respectent les critères définis dans la politique de filtrage et/ou les règles de filtrage liées au contexte de connexion en mode contextuel.**

FDP_IFF.1.3-Filtrage_Flux

The TSF shall enforce the **aucune règle additionnelle**.

FDP_IFF.1.4-Filtrage_Flux

The TSF shall explicitly authorise an information flow based on the following rules:

- **une règle de filtrage autorise explicitement le passage du paquet IP.**

FDP_IFF.1.5-Filtrage_Flux

The TSF shall explicitly deny an information flow based on the following rules:

- **une règle de filtrage interdit explicitement le passage du paquet IP,**
- **aucune règle de filtrage n'a autorisé le passage du paquet IP.**

FMT_SMF.1-Visualisation_politique_filtrage Specification of management functions

FMT_SMF.1.1-Visualisation_politique_filtrage

The TSF shall be capable of performing the following management functions:

- **visualisation de la politique de filtrage et des contextes de connexion présents sur le firewall.**

6.2.1.2 Audit Flux

FAU_GEN.1-Audit_flux Audit data generation

FAU_GEN.1.1-Audit_flux

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 **not specified** level of audit; and

c) **au minimum les événements générés lors du rejet d'un flux.**

Raffinement non éditorial

Le niveau de détail de la trace d'audit (minimum, basic, detailed) dépend de l'évènement audité. Annexe A récapitule les traces minimales requises et établit le niveau d'audit associé.

Note d'application

Les ST conformes à ce PP devront préciser, s'il y a lieu, les autres événements audités.

FAU_GEN.1.2-Audit_flux

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, **les informations permettant à un auditeur de détecter la perte d'événements d'audit des flux (un compteur par exemple).**

Raffinement global

Les traces enregistrées doivent permettre notamment aux administrateurs de s'assurer de la pertinence de la politique de filtrage et de sa bonne instanciation au niveau du firewall.

FAU_GEN.2-Audit_flux User identity association

FAU_GEN.2.1-Audit_flux

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 non éditorial

On entend par 'identité des utilisateurs' l'adresse IP des émetteurs des flux.

FIA_UID.2-Flux User identification before any action

FIA_UID.2.1-Flux

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Raffinement global

On entend par 'utilisateur' les émetteurs et les destinataires des flux traités par le firewall identifiés par leurs adresses IP.

FPT_STM.1 Reliable time stamps

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

Raffinement global:

La fiabilité attendue de la base de temps est que seul l'administrateur de la TOE a le droit de la modifier ; la base de temps devant être fiable entre deux mises à jour par l'administrateur.

FAU_SAR.1-Audit_flux Audit review

FAU_SAR.1.1-Audit_flux
The TSF shall provide **les auditeurs** with the capability to read **les traces d'audit des flux traités par le firewall** from the audit records.

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

FAU_SAR.3-Audit_flux Selectable audit review

FAU_SAR.3.1-Audit_flux
The TSF shall provide the ability to apply **methods of sorting, ordering and searches** of audit data based on **la date et l'heure** et **[assignment: critères sélectionnés par l'auditeur]**.

Note d'application

Les ST conformes à ce PP devront préciser ces critères et les relations logiques utilisés.

6.2.1.3 Gestion Rôles

FMT_SMR.1 Security roles

FMT_SMR.1.1
The TSF shall maintain the roles**:**

- **agent/officier de sécurité,**
- **administrateur de sécurité,**
- **administrateur système et réseaux,**
- **auditeur.**

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

Note d'application

Une même personne peut être associée à plusieurs rôles. Dans le cas du firewall, une même personne pourrait être à la fois l'administrateur de sécurité et l'administrateur

système et réseau par exemple. Ces rôles peuvent être tenus localement sur le firewall ou à distance via une station d'administration.

FIA_UID.2-Administrateurs User identification before any action

FIA_UID.2.1-Administrateurs

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Raffinement global

Les « user » correspondent ici aux administrateurs; à ne pas confondre avec la possibilité de certains firewall de coupler le filtrage avec une identification/authentification des utilisateurs des réseaux.

FIA_UAU.2-Administrateurs User authentication before any action

FIA_UAU.2.1-Administrateurs

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Raffinement global

Cette exigence est relative à l'authentification des administrateurs pour l'administration du firewall.

Raffinement non éditorial

Le mécanisme d'authentification doit être conforme au référentiel [AUTH] de la DCSSI.

6.2.2 Fonctionnement de la TOE

6.2.2.1 Protection de la politique de filtrage

FDP_ACC.1-Règles_filtrage Subset access control

FDP_ACC.1.1-Règles_filtrage

The TSF shall enforce the **politique d'accès aux règles de filtrage** on

- **sujets: les administrateurs,**
- **objets: les règles de la politique de filtrage,**
- **opérations: lire, insérer, modifier, supprimer.**

FDP_ACF.1-Règles_filtrage Security attribute based access control

FDP_ACF.1.1-Règles_filtrage

The TSF shall enforce the **politique d'accès aux règles de filtrage** to objects based on the following:

- **sujets: les administrateurs sur la base de leur rôle,**
- **objets: les règles de la politique de filtrage.**

FDP_ACF.1.2-Règles_filtrage

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

- **l'insertion, la modification et la suppression (complète ou partielle) des règles de filtrage n'est autorisée qu'au rôle administrateur de sécurité;**
- **la lecture des règles de filtrage et des contextes de connexion n'est autorisée qu'aux rôles administrateur de sécurité**.

FDP_ACF.1.3-Règles_filtrage

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

Note d'application

Les ST conformes à ce PP devront indiquer les règles complémentaires utilisées ou préciser « pas de règles additionnelles ».

FDP_ACF.1.4-Règles_filtrage

The TSF shall explicitly deny access of subjects to objects based on the **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.

Note d'application

Les ST conformes à ce PP devront indiquer les règles complémentaires utilisées ou préciser « pas de règles additionnelles ».

Note d'application

Ces règles d'accès doivent être enrichies par le rédacteur de la cible de sécurité pour prendre en compte la capacité d'adaptation des règles par le firewall lui-même en fonction des contextes de connexion (mode contextuel).

6.2.2.2 Audit et alarmes

Protection des traces d'audit des flux

FAU_STG.1-Traces_audit_flux Protected audit trail storage

FAU_STG.1.1-Traces_audit_flux

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

FAU_STG.1.2-Traces_audit_flux

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

Evènements d'administration

FAU_GEN.1-Audit_admin Audit data generation

FAU_GEN.1.1-Audit_admin

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 **minimal or basic** level of audit **définis dans Annexe B avec le niveau d'audit associé** ; and

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

Note d'application

Le rédacteur de la cible de sécurité détaillera les autres évènements à auditer en fonction des exigences fonctionnelles sélectionnées. Il s'appuiera sur la partie 2 des Critères communs qui précise le type d'évènement à auditer pour chacun des composants pour le niveau de détail choisi dans FAU_GEN.1.1.

FAU_GEN.1.2-Audit_admin

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, **les informations permettant à un auditeur de détecter la perte d'événements d'audit des évènements d'administration (un compteur par exemple).**

FAU_GEN.2-Audit_admin User identity association

FAU_GEN.2.1-Audit_admin

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.

FAU_SAR.1-Audit_admin Audit review

FAU_SAR.1.1-Audit_admin

The TSF shall provide **les auditeurs** with the capability to read **les traces d'audit des évènements d'administration du firewall** from the audit records.

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

FAU_SAR.3-Audit_admin Selectable audit review

FAU_SAR.3.1-Audit_admin

The TSF shall provide the ability to apply **methods of sorting, ordering and searches** of audit data based on **des critères sélectionnés par l'auditeur**.

Note d'application

Les ST conformes à ce PP devront préciser ces critères et les relations logiques utilisés.

FAU_STG.1-Traces_audit_admin Protected audit trail storage

FAU_STG.1.1-Traces_audit_admin

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

FAU_STG.1.2-Traces_audit_admin

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

Alarmes

FAU_SAA.1-Alarmes Potential violation analysis

FAU_SAA.1.1-Alarmes

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

FAU_SAA.1.2-Alarmes

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of **événements d'audit** known to indicate a potential security violation;

b) **autres évenements**.

Note d'application

Les ST conformes à ce PP devront préciser les événements indiquant une violation potentielle de la politique de sécurité.

FAU_ARP.1-Alarmes Security alarms

FAU_ARP.1.1-Alarmes

The TSF shall **déclencher au minimum la remontée d'une alarme à l'administrateur de sécurité** upon detection of a potential security violation.

Note d'application

Les ST conformes à ce PP devront préciser, s'il y a lieu, les actions complémentaires mise en œuvre.

6.2.2.3 Protection de l'administration distante

Les exigences ci-après contribuent à l'établissement d'un canal sûr entre la TOE et une station d'administration distante.

FTP_ITC.1-Administration_distante Inter-TSF trusted channel

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

FTP_ITC.1.2-Administration_distante
The TSF shall permit **[selection: another trusted IT product]** to initiate communication via the trusted channel.

Raffinement non éditorial

« Another trusted IT product » désigne une station d'administration distante.

Note d'application

Les ST conformes à ce PP devront préciser le mécanisme utilisé.

FTP_ITC.1.3-Administration_distante
The TSF shall initiate communication via the trusted channel for **[assignment: l'administration ou la supervision de la TOE]**.

FPT_ITI.1-Administration_distante Inter-TSF detection of modification

FPT_ITI.1.1-Administration_distante
The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: **[assignment: détection de modifications, effacements, insertions dans les données d'administration]**.

Note d'application

Les ST conformes à ce PP devront préciser les anomalies prises en compte et les mécanismes de détection utilisés.

FPT_ITI.1.2-Administration_distante
The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform **[assignment: ignorer les données et émettre une alerte]** if modifications are detected.

FPT_RPL.1-Administration_distante Replay detection

FPT_RPL.1.1-Administration_distante
The TSF shall detect replay for the following entities: **[assignment: données d'administration échangées avec une station d'administration distante]**.

Note d'application

Les ST conformes à ce PP devront préciser les mécanismes utilisés.

FPT_RPL.1.2-Administration_distante
The TSF shall perform **[assignment: ignorer les données et émettre une alerte]** when replay is detected.

FPT_ITC.1-Administration_distante Inter-TSF confidentiality during transmission

FPT_ITC.1.1-Administration_distante
The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Note d'application

Les ST conformes à ce PP devront préciser les mécanismes utilisés.

FPT_TDC.1-Administration_distante Inter-TSF basic TSF data consistency

FPT_TDC.1.1-Administration_distante
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.

Note d'application

Les ST conformes à ce PP devront préciser les données échangées avec une station d'administration distante nécessitant d'être traduites.

FPT_TDC.1.2-Administration_distante
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.

Note d'application

Les ST conformes à ce PP devront préciser ces règles de traduction.

6.2.2.4 Configuration de la TOE

FMT_SMF.1-Configuration_TOE Specification of management functions

FMT_SMF.1.1-Configuration_TOE
The TSF shall be capable of performing the following management functions:

- **configuration des paramètres de la TOE (données d'identification et d'authentification, droits d'accès, heure du système, ...) ;**
- **configuration des paramètres système et réseau** ;
- **configuration de la politique de filtrage.**

FMT_MTD.1-Paramètres_système_réseau Management of TSF data

FMT_MTD.1.1-Paramètres_système_réseau
The TSF shall restrict the ability to **query and modify** the **paramètres de configuration réseau et système** et **heure du système** to **administrateurs système et réseau**.

FMT_MTD.1-Paramètres_TOE_Administrateur_sécurité Management of TSF data

FMT_MTD.1.1-Paramètres_TOE_Administrateur_sécurité
The TSF shall restrict the ability to **modify** the **données d'identification et d'authentification** et **droits d'accès** to **agent/officier de sécurité**.

FMT_MTD.1-Paramètres_TOE_Auditeur Management of TSF data

FMT_MTD.1.1-Paramètres_TOE_Auditeur
The TSF shall restrict the ability to **query** the **données d'identification et d'authentification** et **droits d'accès** to **auditeurs**.

6.2.2.5 Supervision de la TOE

FMT_SMF.1-Supervision Specification of management functions

FMT_SMF.1.1-Supervision
The TSF shall be capable of performing the following management functions:
- **supervision de l'état du firewall.**

FPT_ITC.1-Supervision Inter-TSF confidentiality during transmission

FPT_ITC.1.1-Supervision
The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Raffinement global

Les données exportées hors du contrôle de la TOE sont les données strictement nécessaires à la supervision, transmises à un équipement de supervision. Il faut s'assurer que ces données ne contiennent pas d'informations confidentielles ou sinon, les protéger.

6.2.2.6 Note d'application

Les ST conformes à ce PP devront préciser les mécanismes utilisés.Recyclage de la TOE

FDP_RIP.1-Recyclage_TOE Subset residual information protection

FDP_RIP.1.1-Recyclage_TOE

The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **tous les biens sensibles (politiques de filtrage, paramètres de configuration, traces d'audit, alarmes)**.

FDP_ACC.1-Recyclage_TOE Subset access control

FDP_ACC.1.1-Recyclage_TOE

The TSF shall enforce the **politique d'accès aux biens sensibles** on

- **sujets: les administrateurs,**
- **objets: les biens sensibles du firewall,**
- **opérations: effacer.**

Note d'application

La TOE offre une opération d'effacement des biens sensibles en cas de recyclage.

FDP_ACF.1-Recyclage_TOE Security attribute based access control

FDP_ACF.1.1-Recyclage_TOE

The TSF shall enforce the **politique d'accès aux biens sensibles** to objects based on the following:

- **sujets: les administrateurs sur la base de leur rôle,**
- **objets: les biens sensibles du firewall.**

FDP_ACF.1.2-Recyclage_TOE

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

- **L'effacement (complet ou partiel) des biens sensibles n'est autorisé qu'au rôle agent de sécurité.**

FDP_ACF.1.3-Recyclage_TOE

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

Note d'application

Les ST conformes à ce PP devront indiquer les règles complémentaires utilisées ou préciser « pas de règles additionnelles ».

FDP_ACF.1.4-Recyclage_TOE

The TSF shall explicitly deny access of subjects to objects based on the **[assignment:**

rules, based on security attributes, that explicitly deny access of subjects to objects].

Note d'application

Les ST conformes à ce PP devront indiquer les règles complémentaires utilisées ou préciser « pas de règles additionnelles ».

6.3 Exigences de sécurité d'assurance pour la TOE

Une TOE dont la ST est conforme à ce PP doit être évaluée au niveau EAL3 augmenté des composants ALC_FLR.3 et AVA_VAN.3 ce qui correspond au paquet d'assurance prévu pour une qualification au niveau standard d'une cible de sécurité (cf. [QUA-STD]) défini par la colonne « QS » du tableau suivant :

Classe d'assurance	Famille d'assurance	Composants d'assurance par niveau d'évaluation							
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	**QS**
Development	ADV_ARC		1	**1**	1	1	1	1	**1**
	ADV_FSP	1	2	**3**	4	5	5	6	**3**
	ADV_IMP				1	1	2	2	
	ADV_INT					2	3	3	
	ADV_SPM						1	1	
	ADV_TDS		1	**2**	3	4	5	6	**2**
Guidance documents	AGD_OPE	1	1	**1**	1	1	1	1	**1**
	AGD_PRE	1	1	**1**	1	1	1	1	**1**
Life-cycle support	ALC_CMC	1	2	**3**	4	4	5	5	**3**
	ALC_CMS	1	2	**3**	4	5	5	5	**3**
	ALC_DEL		1	**1**	1	1	1	1	**1**
	ALC_DVS			**1**	1	1	2	2	**1**
	ALC_FLR								**3**
	ALC_LCD			**1**	1	1	1	2	**1**
	ALC_TAT				1	2	3	3	
Security Target evaluation	ASE_CCL	1	1	**1**	1	1	1	1	**1**
	ASE_ECD	1	1	**1**	1	1	1	1	**1**
	ASE_INT	1	1	**1**	1	1	1	1	**1**
	ASE_OBJ	1	2	**2**	2	2	2	2	**2**
	ASE_REQ	1	2	**2**	2	2	2	2	**2**
	ASE_SPD		1	**1**	1	1	1	1	**1**
	ASE_TSS	1	1	**1**	1	1	1	1	**1**
Tests	ATE_COV		1	**2**	2	2	3	3	**2**
	ATE_DPT			**1**	2	3	3	4	**1**
	ATE_FUN		1	**1**	1	1	2	2	**1**
	ATE_IND	1	2	**2**	2	2	2	3	**2**
Vulnerability assessment	AVA_VAN	1	2	2	**3**	4	5	5	**3**

Tableau 7 Exigences pour une qualification au niveau standard d'une ST

Note d'application : les ST conformes à ce PP devront respecter le paquet d'assurance requis pour une qualification au niveau standard.

6.4 Argumentaire

6.4.1 Exigences de sécurité / Objectifs de sécurité

6.4.1.1 Couverture des objectifs de sécurité pour la TOE

Objectifs sur les services de sécurité rendus par la TOE

O.APPLICATION_POL_FILTRAGE

Cet objectif se traduit par les exigences:

- FDP_IFF.1-Filtrage_Flux qui permet de définir les règles minimales que doit respecter la politique de filtrage
- FDP_IFC.2-Filtrage_Flux qui demande à ce que la TOE applique cette politique de filtrage

O.VISUALISATION_POL

Cet objectif se traduit par l'exigence FMT_SMF.1-Visualisation_politique_filtrage qui nécessite la possibilité de visualiser les règles de filtrage et les contextes de connexion.

O.COHERENCE_POL

Cet objectif se traduit par FPT_TDC.1-Administration_distante pour assurer la cohérence entre la politique de filtrage définie sur la station d'administration distante et le firewall.

O.AUDIT_FLUX

Cet objectif est traduit par FAU_GEN.1-Audit_flux pour la génération des traces d'évènements sur les flux traités par le firewall, FAU_GEN.2-Audit_flux pour pouvoir imputer les événements à des émetteurs de ces flux. Pour réaliser ce dernier, les flux doivent être impérativement identifiés (FIA_UID.2-Flux). Les dates des événements audités étant enregistrées, la TOE doit de plus disposer d'une horloge fiable (FPT_STM.1).

La possibilité de consultation de ces traces d'audit des flux traités par le firewall est traduite par FAU_SAR.1-Audit_flux et FAU_SAR.3-Audit_flux.

O.GESTION_ROLES

L'objectif se traduit par l'exigence FMT_SMR.1 qui demande à ce que la TOE gère les différents rôles (administrateurs). Pour pourvoir gérer ces rôles, les administrateurs doivent impérativement être identifiés (FIA_UID.2-Administrateurs) et authentifiés (FIA_UAU.2-Administrateurs).

Objectifs de sécurité sur le fonctionnement de la TOE

Protection de la politique de filtrage

O.PROTECTION_POL_FILTRAGE

Cet objectif se traduit par les règles d'accès à la politique de filtrage (FDP_ACC.1-Règles_filtrage et FDP_ACF.1-Règles_filtrage).

Audit et alarmes

Flux

O.PROTECTION_AUDIT_FLUX

Cet objectif se traduit par FAU_STG.1-Traces_audit_flux qui exige la protection en intégrité des enregistrements d'événements d'audit. Le risque de perte d'enregistrement à cause du manque de mémoire n'est pas traité dans ce profil de protection en raison de l'hypothèse associée A.AUDIT.

Événements d'administration

O.AUDIT_ADMIN

Cet objectif est traduit par FAU_GEN.1-Audit_admin pour la génération des traces d'évènements sur les évènements d'administration du firewall, FAU_GEN.2-Audit_admin pour pouvoir imputer les événements aux administrateurs. Les administrateurs doivent être impérativement identifiés (FIA_UID.2-Administrateurs). Les dates des événements audités étant enregistrées, la TOE doit de plus disposer d'une horloge fiable (FPT_STM.1).

La possibilité de consultation de ces traces d'audit des événements d'administration du firewall est traduite par FAU_SAR.1-Audit_admin et FAU_SAR.3-Audit_admin.

O.PROTECTION_AUDIT_ADMIN

Cet objectif se traduit par FAU_STG.1-Traces_audit_admin qui protège en intégrité les enregistrements d'événements d'administration.

Alarmes

O.ALARMES

Cet objectif se traduit par FAU_ARP.1-Alarmes qui exige de lever une alarme de sécurité quand une violation potentielle de la sécurité est détectée et par FAU_SAA.1-Alarmes qui indique les règles utilisées pour détecter ces violations potentielles.

O.PROTECTION_ALARMES

Cet objectif se traduit par FAU_STG.1-Traces_audit_admin et FAU_STG.1-Traces_audit_flux qui protègent en intégrité les enregistrements d'événements.

Protection de l'administration distante

O.PROTECTION_FLUX_ADMIN

Cet objectif est traduit par les exigences de protection suivantes :

- FTP_ITC.1-Administration_distante et FPT_ITI.1-Administration_distante précise que la TOE permet l'établissement d'un canal sûr qui permet de contrôler l'intégrité des données d'administration échangées avec un site distant.
- FPT_RPL.1-Administration_distante précise que la TOE assure une protection contre le rejeu des données qu'elle échange avec des sites distants dans le cadre d'opérations d'administration ou de supervision distantes.
- FPT_ITC.1-Administration_distante précise que la TOE assure la confidentialité des données d'administration exportées vers un site distant.
- FPT_TDC.1-Administration_distante précise que les données nécessitent d'être traduites afin d'assurer la cohérence entre la station d'administration distante et la TOE et comment devront être définies les règles de traduction pour les mécanismes assurant la cohérence des données de la TSF.
- FIA_UID.2-Administrateurs et FIA_UAU.2-Administrateurs précisent que les administrateurs doivent impérativement être identifiés et authentifiés pour pourvoir réaliser des opérations d'administration.

Configuration de la TOE

O.PROTECTION_PARAM

Cet objectif est traduit par les exigences de protection suivantes:

- pour les paramètres de configuration réseau: FMT_MTD.1-Paramètres_système_réseau;
- pour les droits d'accès et les données d'authentification: FMT_MTD.1-Paramètres_TOE_Administrateur_sécurité pour les administrateurs de sécurité et FMT_MTD.1-Paramètres_TOE_Auditeur pour les auditeurs;

La fonctionnalité de configuration de ces paramètres est quant à elle couverte par FMT_SMF.1-Configuration_TOE.

Supervision de la TOE

O.SUPERVISION

Cet objectif est traduit par l'exigence FMT_SMF.1-Supervision qui exige la fourniture d'un service indiquant l'état du firewall.

O.IMPACT_SUPERVISION

Cet objectif est traduit par l'exigence FPT_ITC.1-Supervision qui exige de protéger les données exportées hors du contrôle du firewall si elles contiennent des informations confidentielles.

Recyclage de la TOE

O.RECYCLAGE_TOE

Cet objectif est traduit par les exigences suivantes :

- FDP_RIP.1-Recyclage_TOE qui exige que la TOE permette de rendre indisponible le contenu des ressources correspondant aux biens sensibles de la TOE ;
- FDP-ACC.1-Recyclage_TOE et FDP_ACF.1-Recyclage_TOE qui exigent des règles d'accès à l'opération d'effacement des biens sensibles.

O.AUTHENTIFICATION_ADMIN

Cet objectif est traduit par les exigences suivantes :

- FIA_UID.2-Administrateurs et FIA_UAU.2-Administrateurs qui précisent que les administrateurs doivent impérativement être identifiés et authentifiés pour pouvoir réaliser des opérations d'administration.

6.4.2 Tables de couverture entre les objectifs et exigences de sécurité

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.APPLICATION_POL_FILTRAGE	FDP_IFF.1-Filtrage_Flux, FDP_IFC.2-Filtrage_Flux	Section 6.3.1
O.VISUALISATION_POL	FMT_SMF.1-Visualisation_politique_filtrage	Section 6.3.1
O.COHERENCE_POL	FPT_TDC.1-Administration_distante	Section 6.3.1
O.AUDIT_FLUX	FAU_GEN.1-Audit_flux, FAU_GEN.2-Audit_flux, FPT_STM.1, FIA_UID.2-Flux, FAU_SAR.1-Audit_flux, FAU_SAR.3-Audit_flux	Section 6.3.1
O.GESTION_ROLES	FMT_SMR.1, FIA_UID.2-Administrateurs ; FIA_UAU.2-Administrateurs	Section 6.3.1
O.PROTECTION_POL_FILTRAGE	FDP_ACC.1-Règles_filtrage, FDP_ACF.1-Règles_filtrage	Section 6.3.1
O.PROTECTION_AUDIT_FLUX	FAU_STG.1-Traces_audit_flux	Section 6.3.1
O.AUDIT_ADMIN	FPT_STM.1, FAU_GEN.2-Audit_admin, FAU_GEN.1-Audit_admin, FAU_SAR.1-Audit_admin, FAU_SAR.3-Audit_admin, FIA_UID.2-Administrateurs	Section 6.3.1
O.PROTECTION_AUDIT_ADMIN	FAU_STG.1-Traces_audit_admin	Section 6.3.1
O.ALARMES	FAU_ARP.1-Alarmes, FAU_SAA.1-Alarmes	Section 6.3.1

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumen-taire
O.PROTECTION_ALARMES	FAU_STG.1-Traces_audit_flux, FAU_STG.1-Traces_audit_admin	Section 6.3.1
O.PROTECTION_FLUX_ADMIN	FTP_ITC.1-Administration_distante ; FPT_ITI.1-Administration_distante ; FPT_RPL.1-Administration_distante ; FPT_ITC.1-Administration_distante ; FPT_TDC.1-Administration_distante ; FIA_UID.2-Administrateurs ; FIA_UAU.2-Administrateurs	Section 6.3.1
O.PROTECTION_PARAM	FMT_MTD.1-Paramètres_système_réseau, FMT_MTD.1-Paramètres_TOE_Administrateur_sécurité, FMT_SMF.1-Configuration_TOE, FMT_MTD.1-Paramètres_TOE_Auditeur	Section 6.3.1
O.SUPERVISION	FMT_SMF.1-Supervision	Section 6.3.1
O.IMPACT_SUPERVISION	FPT_ITC.1-Supervision	Section 6.3.1
O.RECYCLAGE_TOE	FDP_RIP.1-Recyclage_TOE, FDP_ACC.1-Recyclage_TOE, FDP_ACF.1-Recyclage_TOE	Section 6.3.1
O.AUTHENTIFICATION_ADMIN	FIA_UID.2-Administrateurs ; FIA_UAU.2-Administrateurs	Section 6.3.1

Tableau 8 Argumentaire objectifs de sécurité vers les exigences fonctionnelles de la TOE

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_IFC.2-Filtrage_Flux	O.APPLICATION_POL_FILTRAGE
FDP_IFF.1-Filtrage_Flux	O.APPLICATION_POL_FILTRAGE
FMT_SMF.1-Visualisation_politique_filtrage	O.VISUALISATION_POL
FTP_ITC.1-Administration_distante	O.PROTECTION_FLUX_ADMIN
FPT_ITI.1-Administration_distante	O.PROTECTION_FLUX_ADMIN
FPT_RPL.1-Administration_distante	O.PROTECTION_FLUX_ADMIN
FPT_ITC.1-Administration_distante	O.PROTECTION_FLUX_ADMIN
FPT_TDC.1-Administration_distante	O.COHERENCE_POL ; O.PROTECTION_FLUX_ADMIN
FAU_GEN.1-Audit_flux	O.AUDIT_FLUX
FAU_GEN.2-Audit_flux	O.AUDIT_FLUX
FIA_UID.2-Flux	O.AUDIT_FLUX
FPT_STM.1	O.AUDIT_FLUX, O.AUDIT_ADMIN
FAU_SAR.1-Audit_flux	O.AUDIT_FLUX
FAU_SAR.3-Audit_flux	O.AUDIT_FLUX
FMT_SMR.1	O.GESTION_ROLES
FIA_UID.2-Administrateurs	O.GESTION_ROLES, O.AUDIT_ADMIN ; O.PROTECTION_FLUX_ADMIN ; O.AUTHENTIFICATION_ADMIN
FIA_UAU.2-Administrateurs	O.GESTION_ROLES ; O.PROTECTION_FLUX_ADMIN ; O.AUTHENTIFICATION_ADMIN
FDP_ACC.1-Règles_filtrage	O.PROTECTION_POL_FILTRAGE

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FDP_ACF.1-Règles_filtrage	O.PROTECTION_POL_FILTRAGE
FAU_STG.1-Traces_audit_flux	O.PROTECTION_AUDIT_FLUX, O.PROTECTION_ALARMES
FAU_GEN.1-Audit_admin	O.AUDIT_ADMIN
FAU_GEN.2-Audit_admin	O.AUDIT_ADMIN
FAU_SAR.1-Audit_admin	O.AUDIT_ADMIN
FAU_SAR.3-Audit_admin	O.AUDIT_ADMIN
FAU_STG.1-Traces_audit_admin	O.PROTECTION_AUDIT_ADMIN, O.PROTECTION_ALARMES
FAU_SAA.1-Alarmes	O.ALARMES
FAU_ARP.1-Alarmes	O.ALARMES
FMT_SMF.1-Configuration_TOE	O.PROTECTION_PARAM
FMT_MTD.1-Paramètres_système_réseau	O.PROTECTION_PARAM
FMT_MTD.1-Paramètres_TOE_Administrateur_sécurité	O.PROTECTION_PARAM
FMT_MTD.1-Paramètres_TOE_Auditeur	O.PROTECTION_PARAM
FMT_SMF.1-Supervision	O.SUPERVISION
FPT_ITC.1-Supervision	O.IMPACT_SUPERVISION
FDP_RIP.1-Recyclage_TOE	O.RECYCLAGE_TOE
FDP_ACC.1-Recyclage_TOE	O.RECYCLAGE_TOE
FDP_ACF.1-Recyclage_TOE	O.RECYCLAGE_TOE

Tableau 9 Argumentaire exigences fonctionnelles de la TOE vers objectifs de sécurité

6.4.3 Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances CC	Dépendances Satisfaites
FIA_UAU.2-Administrateurs	(FIA_UID.1)	FIA_UID.2-Administrateurs
FDP_IFC.2-Filtrage_Flux	(FDP_IFF.1)	FDP_IFF.1-Filtrage_Flux
FDP_IFF.1-Filtrage_Flux	(FDP_IFC.1) et (FMT_MSA.3)	FDP_IFC.2-Filtrage_Flux
FMT_SMF.1-Visualisation_politique_filtrage	Pas de dépendances	
FAU_GEN.1-Audit_flux	(FPT_STM.1)	FPT_STM.1
FAU_GEN.2-Audit_flux	(FAU_GEN.1) et (FIA_UID.1)	FAU_GEN.1-Audit_flux, FIA_UID.2-Flux
FIA_UID.2-Flux	Pas de dépendances	
FPT_STM.1	Pas de dépendances	
FAU_SAR.1-Audit_flux	(FAU_GEN.1)	FAU_GEN.1-Audit_flux
FAU_SAR.3-Audit_flux	(FAU_SAR.1)	FAU_SAR.1-Audit_flux

Exigences	Dépendances CC	Dépendances Satisfaites
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2-Administrateurs
FIA_UID.2-Administrateurs	Pas de dépendances	
FIA_UAU.2-Administrateurs	(FIA_UID.1)	FIA_UID.2-Administrateurs
FDP_ACC.1-Règles_filtrage	(FDP_ACF.1)	FDP_ACF.1-Règles_filtrage
FDP_ACF.1-Règles_filtrage	(FDP_ACC.1) et (FMT_MSA.3)	FDP_ACC.1-Règles_filtrage
FTP_ITC.1-Administration_distante	Pas de dépendances	
FPT_ITI.1-Administration_distante	Pas de dépendances	
FPT_RPL.1-Administration_distante	Pas de dépendances	
FPT_ITC.1-Administration_distante	Pas de dépendances	
FPT_TDC.1-Administration_distante	Pas de dépendances	
FMT_SMF.1-Configuration_TOE	Pas de dépendances	
FMT_MTD.1-Paramètres_système_réseau	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1-Configuration_TOE
FMT_MTD.1-Paramè-tres_TOE_Administrateur_sécurité	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1-Configuration_TOE
FMT_MTD.1-Paramètres_TOE_Auditeur	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1-Configuration_TOE
FMT_SMF.1-Supervision	Pas de dépendances	
FPT_ITC.1-Supervision	Pas de dépendances	
FDP_RIP.1-Recyclage_TOE	Pas de dépendances	
FDP_ACC.1-Recyclage_TOE	(FDP_ACF.1)	FDP_ACF.1-Recyclage_TOE
FDP_ACF.1-Recyclage_TOE	(FDP_ACC.1) et (FMT_MSA.3)	FDP_ACC.1-Recyclage_TOE
FAU_STG.1-Traces_audit_flux	(FAU_GEN.1)	FAU_GEN.1-Audit_flux
FAU_GEN.1-Audit_admin	(FPT_STM.1)	FPT_STM.1
FAU_GEN.2-Audit_admin	(FAU_GEN.1) et (FIA_UID.1)	FIA_UID.2-Administrateurs, FAU_GEN.1-Audit_admin
FAU_SAR.1-Audit_admin	(FAU_GEN.1)	FAU_GEN.1-Audit_admin
FAU_SAR.3-Audit_admin	(FAU_SAR.1)	FAU_SAR.1-Audit_admin
FAU_STG.1-Traces_audit_admin	(FAU_GEN.1)	FAU_GEN.1-Audit_admin
FAU_SAA.1-Alarmes	(FAU_GEN.1)	FAU_GEN.1-Audit_flux, FAU_GEN.1-Audit_admin
FAU_ARP.1-Alarmes	(FAU_SAA.1)	FAU_SAA.1-Alarmes

Tableau 10 Dépendances des exigences fonctionnelles

6.4.3.1 Argumentaire pour les dépendances non satisfaites

La dépendance FMT_MSA.3 de FDP_IFF.1-Filtrage_Flux n'est pas supportée. Dans le cadre de ce profil de protection, il n'est pas imposé de valeurs restrictives pour les attributs sur lesquels s'appuie la politique de filtrage. Il n'est pas en revanche exclu qu'un produit le fasse.

La dépendance FMT_MSA.3 de FDP_ACF.1-Règles_filtrage n'est pas supportée. Le profil de protection n'impose pas que la TOE prédéfinisse des valeurs par défaut des attributs de sécurité pour le contrôle d'accès à la politique de filtrage.

La dépendance FMT_MSA.3 de FDP_ACF.1-Biens_sensibles n'est pas supportée. Le profil de protection n'impose pas que la TOE prédéfinisse des valeurs par défaut des attributs de sécurité pour le contrôle d'accès aux biens sensibles.

6.4.4 Conformité à un PP

Sans objet.

6.4.5 Composants étendus

Sans objet.

Annexe A Compléments de description de la TOE

A.1 Fonctionnalités de la TOE

La fonctionnalité principale de la TOE est de fournir au système la capacité de restreindre les flux d'informations en provenance ou à destination d'un réseau protégé dans le but de protéger les ressources de ce réseau contre des attaques en provenance d'autres réseaux (via l'interconnexion où est mise en œuvre la TOE) :

- Application d'une politique de filtrage ;
- Audit/journalisation des flux IP.

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

- Gestion de la politique de filtrage ;
- Protection des opérations d'administration ;
- Audit des opérations d'administration et supervision ;
- Protection de l'accès aux paramètres de la TOE.

A.1.1 Services fournis par la TOE

Application de la politique de filtrage

La TOE est un firewall qui offre des fonctionnalités de filtrage des flux entre des réseaux IP, basées sur des règles permettant de mettre en œuvre la politique de sécurité du système d'information concerné. Pour bénéficier d'un filtrage optimum, la politique de sécurité doit être cohérente et non ambiguë. Deux types de filtrage peuvent être distingués :

- Le filtrage non contextuel : l'action de filtrage (acceptation, blocage, rejet, avec journalisation ou non) est déterminée en fonction du contenu d'un paquet réseau.
- Le filtrage contextuel : sur la base d'un premier filtrage non contextuel, la TOE établit un contexte et des règles de filtrage adaptées, basées sur les caractéristiques du flux identifié (origine, destinataire, protocoles). La connaissance de ce contexte permet à la TOE d'une part de gagner en performance, et d'autre part d'augmenter la pertinence du filtrage et sa précision.

Les fonctionnalités de filtrage, contextuel ou non, offertes par la TOE s'appliquent uniquement aux flux portés par le protocole IP et prennent en compte les couches réseau et transport.

Audit/journalisation des flux IP

Ce service permet de tracer tous les flux IP traités par la TOE. Il permet aussi la définition des événements à tracer et leur consultation.

A.1.2 Services nécessaires au bon fonctionnement de la TOE

A.1.1.1 Gestion des politiques de filtrage

Définition des politiques de filtrage

Seul un administrateur de sécurité est autorisé à définir la politique de filtrage. Il spécifie les règles de filtrage pour l'envoi ou la réception de données : acceptation, rejet et niveau de contrôle à effectuer.

Une politique de filtrage peut être définie localement, au niveau de l'administration locale du firewall, et à distance, sur une station d'administration distante. Dans ce dernier cas, la politique est distribuée au firewall. La cohérence entre la politique définie par l'administrateur de sécurité et celle se trouvant dans le firewall doit être assurée afin que la politique de filtrage mise en œuvre soit bien celle attendue et définie par l'administrateur de sécurité.

Protection de l'accès aux politiques de filtrage

Ce service permet de contrôler les différents types d'accès (modification, consultation) à la politique de filtrage et aux règles relatives aux contextes de sécurité, en mode contextuel, suivant le rôle de la personne authentifiée.

A.1.1.2 Protection des opérations d'administration

Le firewall peut être administré localement ou à distance. L'administration locale est une administration qui se fait directement sur la machine contenant les services du firewall, alors que l'administration à distance est une administration qui s'effectue au travers d'un réseau LAN ou WAN.

Authentification des administrateurs

Ce service permet d'authentifier tous les administrateurs qui effectuent des opérations d'administration sur le firewall.

Protection des flux d'administration à distance

Ce service permet de protéger en authenticité (incluant donc la couverture des attaques en rejeu) les flux de données échangées entre le firewall et la station d'administration pour effectuer des opérations d'administration à distance. Ce service permet aussi, le cas échéant, de protéger en confidentialité les flux d'administration. Cette protection concerne les flux d'administration de sécurité (politique de filtrage) et les flux d'administration système et réseau (paramètres de configuration).

A.1.1.3 Audit et supervision

Audit / journalisation des opérations d'administration

Ce service permet de tracer les opérations d'administration effectuées par l'administrateur sur le firewall, comme par exemple les modifications de la politique de filtrage. Il permet aussi la définition des événements à tracer et leur consultation.

Génération d'alarmes de sécurité

Ce service permet de générer des alarmes de sécurité pour signaler tout dysfonctionnement majeur du firewall. Il permet aussi à un administrateur de sécurité de définir les alarmes à générer et leur mode de diffusion et de consulter ces alarmes.

Supervision de la TOE

Ce service permet à un administrateur système et réseau de contrôler l'état de disponibilité du firewall (état de fonctionnement, niveaux d'utilisation des ressources, ...).

A.1.1.4 Protection de l'accès aux paramètres de configuration

Ce service permet de protéger (d'une attaque par réseau) les paramètres de configuration du firewall en confidentialité et en intégrité. Ces paramètres comprennent entre autres les paramètres de configuration réseau (données topologiques sur les réseaux protégés), les données d'authentification et les droits d'accès.

A.1.3 Rôles

Le fonctionnement de la TOE dans son environnement opérationnel manipule directement ou indirectement les rôles décrits ci-dessous. Il s'agit de rôles « logiques » dont l'attribution à des personnes distinctes ou non relève de la politique de sécurité de l'organisation qui met en œuvre la TOE.

Agent / Officier de sécurité

Il configure les rôles et les accès aux outils et fonctions d'administration. Il gère les moyens d'authentification pour accéder aux outils d'administration ou au firewall.

Administrateur de sécurité

Administrateur (local ou distant) du firewall. Il définit la politique de filtrage que va appliquer le firewall. Il définit les événements d'audit à tracer ainsi que les alarmes de sécurité à générer. De plus, il analyse, traite et supprime les alarmes de sécurité générées.

Auditeur

Son rôle est d'analyser et de gérer les événements d'audit concernant les activités sur les flux IP et les opérations d'administration.

Administrateur système et réseau

Administrateur responsable du système d'information sur lequel se trouve le firewall. Il est responsable du maintien en condition opérationnelle de la TOE (maintenance logicielle et matérielle comprises).

Il configure les paramètres réseaux du firewall et les paramètres systèmes qui sont liés aux contextes réseaux opérationnels à prendre en compte : il définit la topologie réseau globale mais ne définit pas la politique de filtrage applicable par le firewall.

Son rôle est aussi de contrôler l'état du firewall.

Utilisateur du réseau protégé

Utilisateur d'un réseau protégé connecté à un autre réseau à travers le firewall. Cet utilisateur peut, par l'intermédiaire d'applications, envoyer/recevoir des informations vers/d'un autre réseau via le firewall de son réseau.

Dans ce document, à moins de distinction spécifiquement exprimée, le rôle administrateur regroupe les rôles suivants : agent / officier de sécurité, administrateur de sécurité, auditeur et administrateur système et réseau.

A.2 Architecture de la TOE

Cette section présente l'architecture de la TOE sous deux aspects différents : aspect physique et aspect fonctionnel.

A.2.1 Architecture physique

La Figure 2 présente un exemple d'architecture physique d'interconnexion d'un réseau protégé à travers un firewall, architecture à partir de laquelle la TOE sera évaluée.

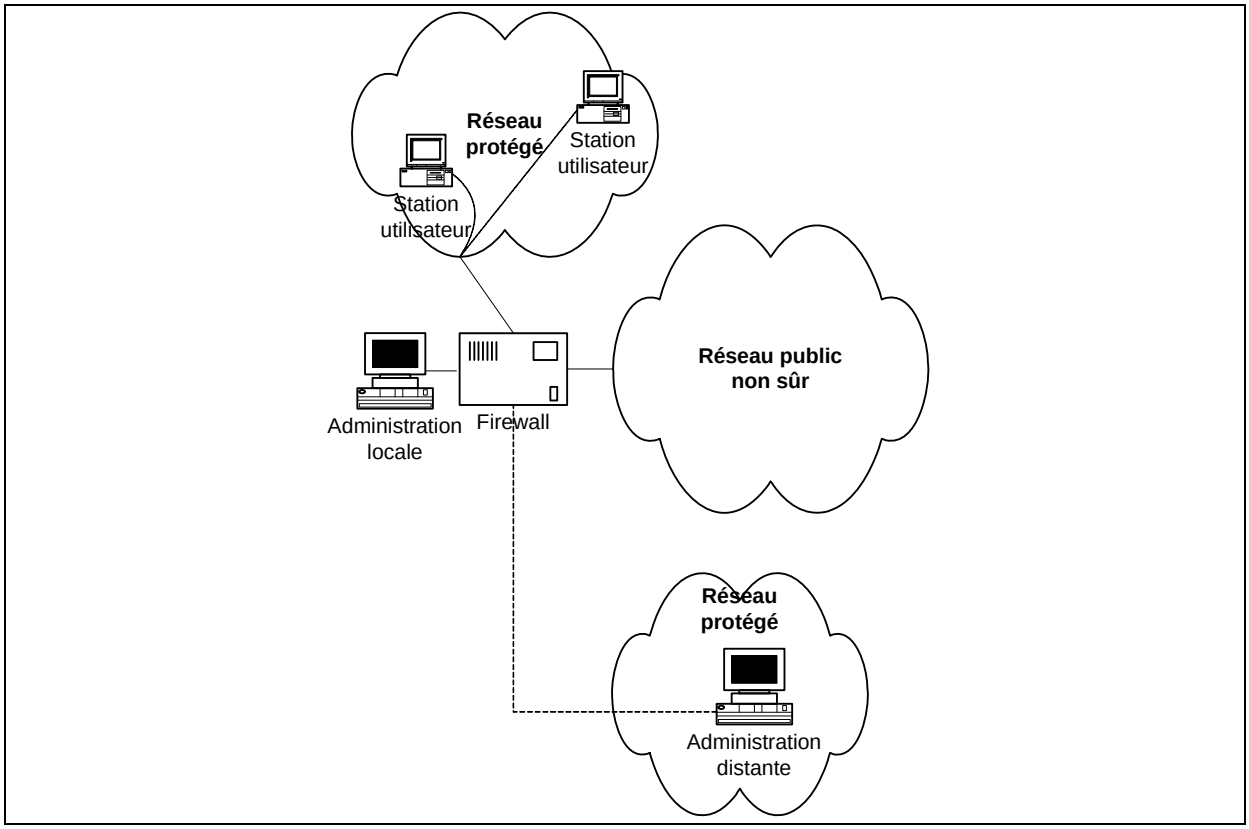

Figure 2 Exemple d'architecture possible d'une interconnexion avec firewall

Comme l'illustre la Figure 2, le firewall présente quatre interfaces externes logiques : une interface vers le réseau protégé, une interface vers le réseau public, une interface d'administration locale et une interface de télé-administration.

Le firewall assure ainsi seul l'interconnexion entre le réseau protégé et le réseau public. Mais il peut être inséré à l'intérieur d'une structure plus globale d'interconnexion de réseaux IP (cf. [PB-INT]) et permettre le cloisonnement du réseau protégé en plusieurs sous-réseaux, notamment en offrant une interface spécifique vers un sous-réseau de type DMZ. L'impact de cette capacité doit être étudié spécifiquement par le rédacteur de la cible de sécurité.

A.2.2 Architecture fonctionnelle

Les figures de cette section montrent les éléments qui constituent la TOE au niveau fonctionnel. Ces éléments apparaissent en grisé dans les figures. De plus, les biens apparaissent en italique. Les autres éléments sont extérieurs au périmètre de la TOE.

Ces schémas sont donnés à titre illustratif et forment une vue abstraite de l'architecture fonctionnelle de la TOE. L'ordonnancement des services présentés dans ces schémas ne correspond donc pas forcément à celui d'une implémentation donnée.

La Figure 3 présente les fonctionnalités qui concernent la gestion des rôles.

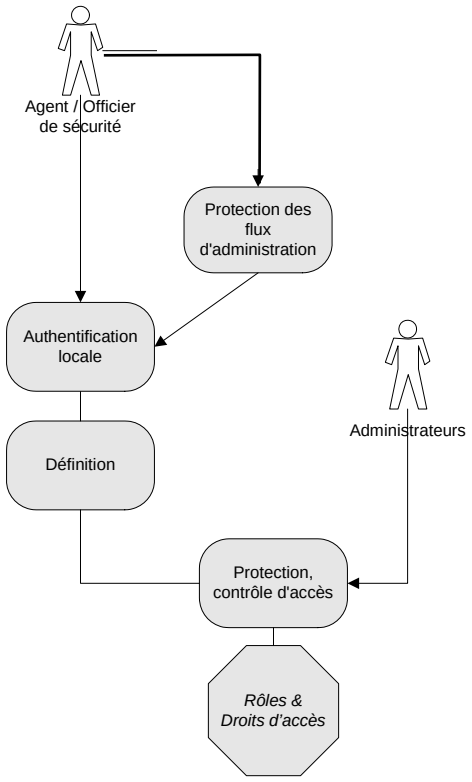

Figure 3 Gestion des rôles

La Figure 4 présente les fonctionnalités qui concernent la gestion de la politique de filtrage et des règles relatives aux contextes de connexion (en mode contextuel). Tous les services font partie de la TOE excepté celui d'authentification à distance de l'administrateur de sécurité. Le service nommé protection des flux d'administration comporte à la fois le service de protection en authenticité des flux d'administration à distance et celui de protection contre le rejeu des flux d'administration. Il en de même dans les schémas qui suivent.

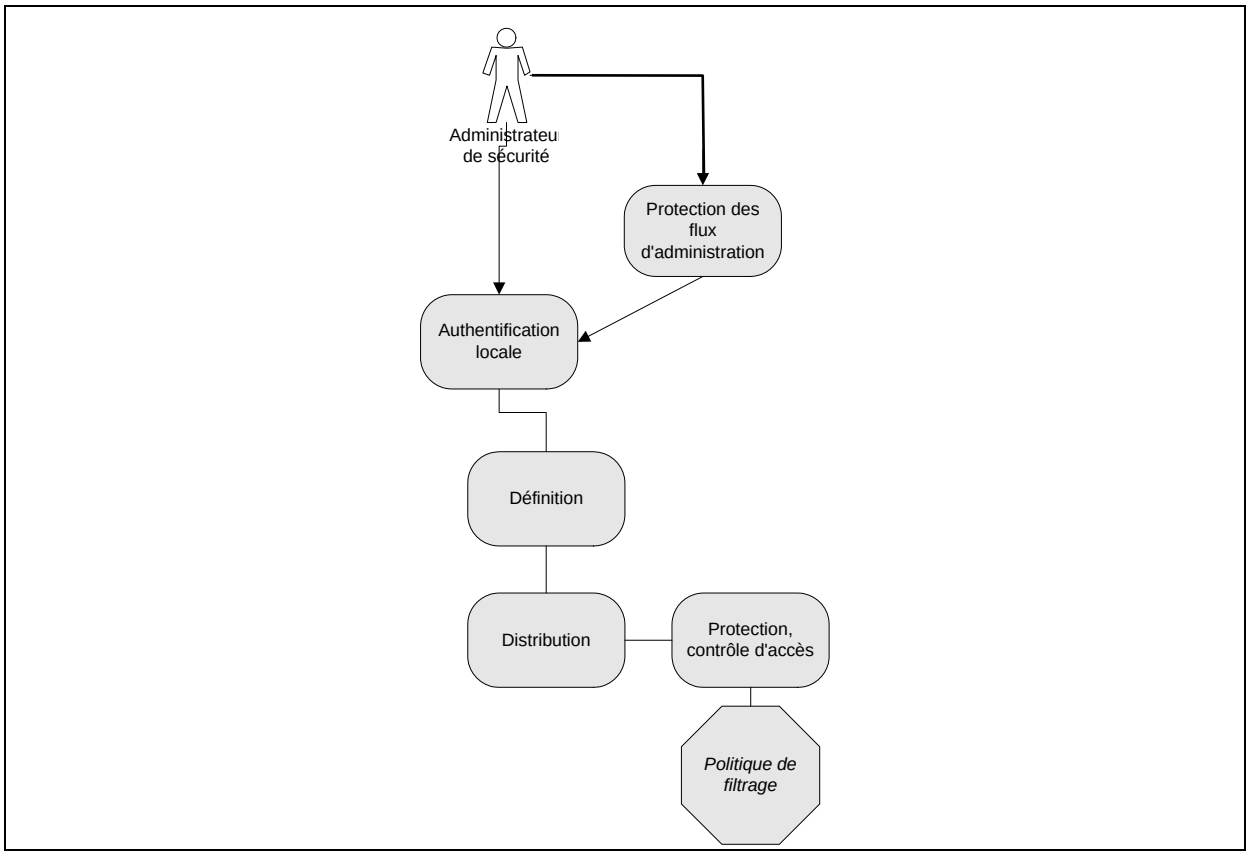

Figure 4 Gestion de la politique de filtrage

La Figure 5 présente les fonctionnalités qui concernent l'application de la politique de filtrage et des règles relatives aux contextes de connexion (en mode contextuel).

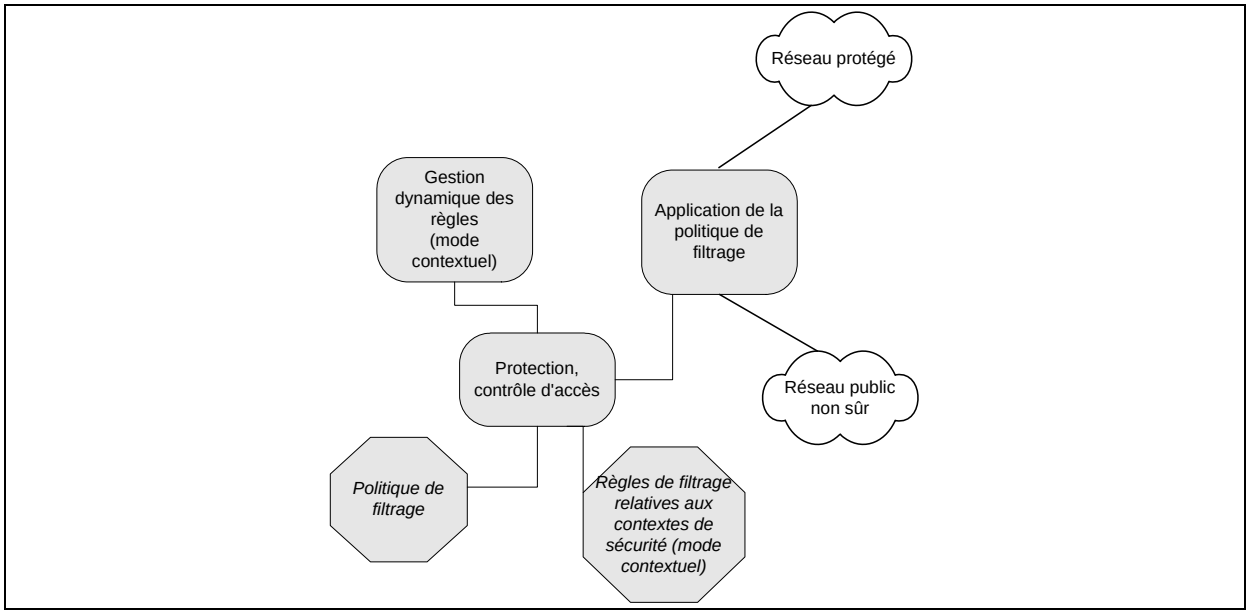

Figure 5 Application de la politique de filtrage

Au niveau de la configuration d'un firewall, l'authentification à distance de l'administrateur système et réseau ne fait pas partie de la TOE (Figure 6). Ce schéma ne présente pas tous les services de la TOE accédant en lecture aux paramètres de configuration, car ils sont nombreux. Ces services sont entre autres les services d'authentification locale, l'application de la politique de filtrage et tous les services qui consultent les droits d'accès et les adresses IP internes pour leur propre besoin.

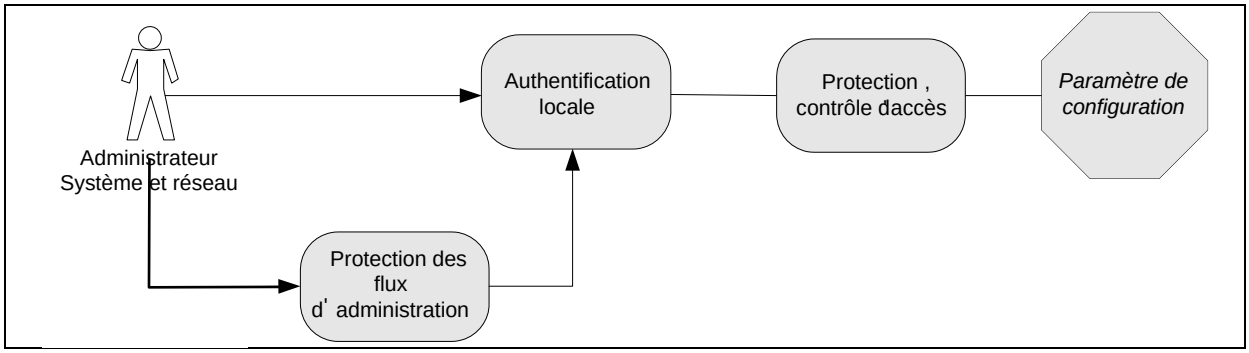

Figure 6 Configuration du firewall

Au niveau de l'audit, l'authentification à distance de l'auditeur et de l'administrateur de sécurité ne fait partie de la TOE (Figure 7).

La définition des événements à auditer (politique d'audit) relève dans la pratique :

- de la définition de la politique de filtrage en ce qui concerne les événements liés aux flux utilisateurs ;
- de la définition des paramètres de configuration en ce qui concerne les événements liés aux opérations d'administration.

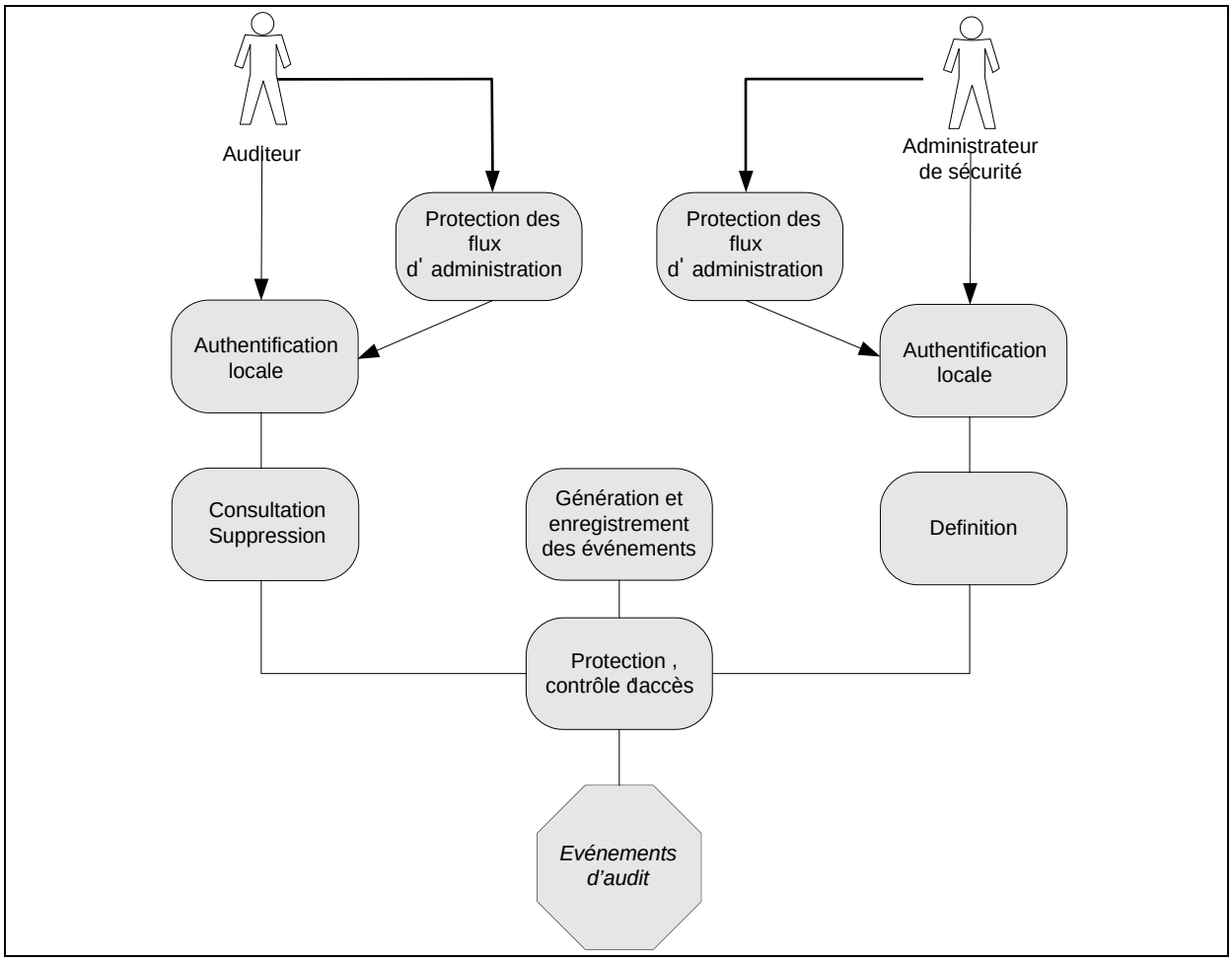

Figure 7 Gestion de l'audit

Au niveau des alarmes de sécurité, l'authentification à distance de l'administrateur de sécurité et le traitement des alarmes ne font pas partie de la TOE (Figure 8).

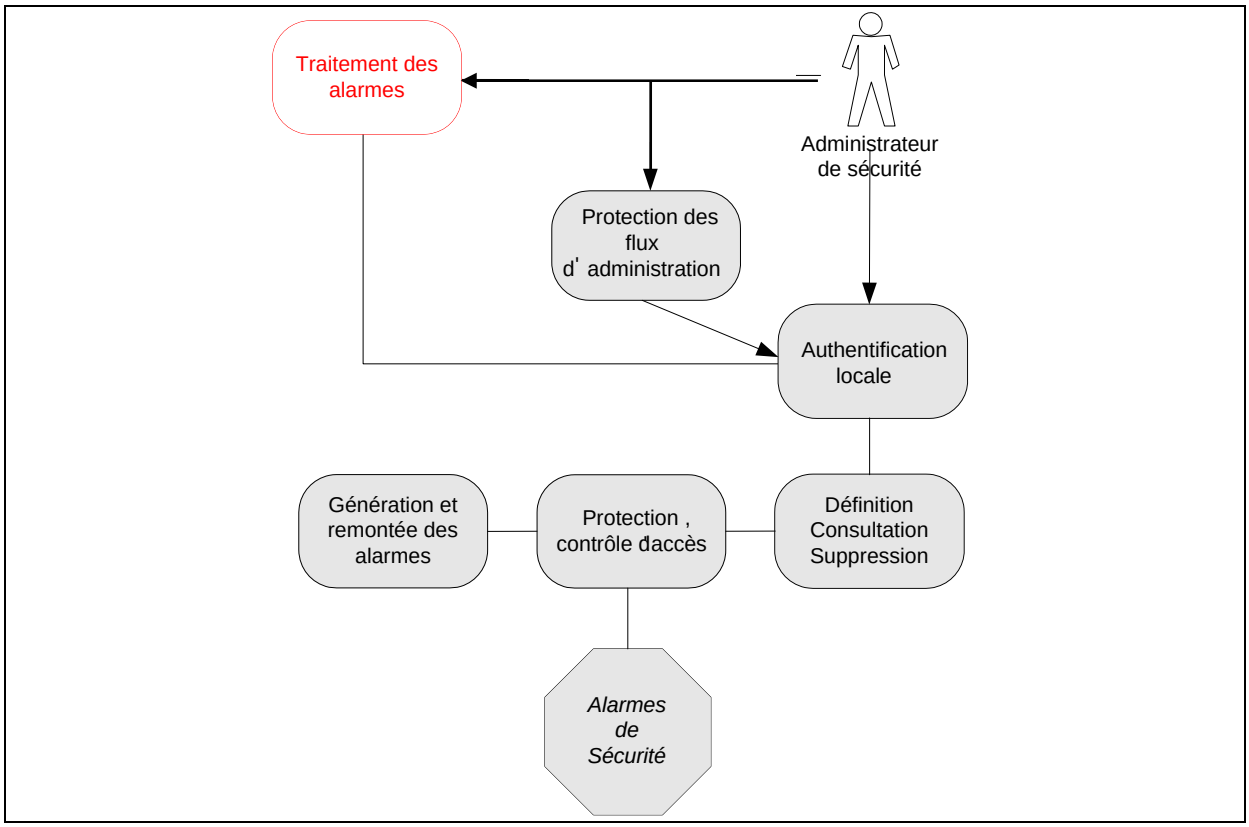

Figure 8 Gestion des alarmes de sécurité

Au niveau de la supervision, l'authentification à distance de l'administrateur système et réseau ne fait pas partie de la TOE (Figure 9).

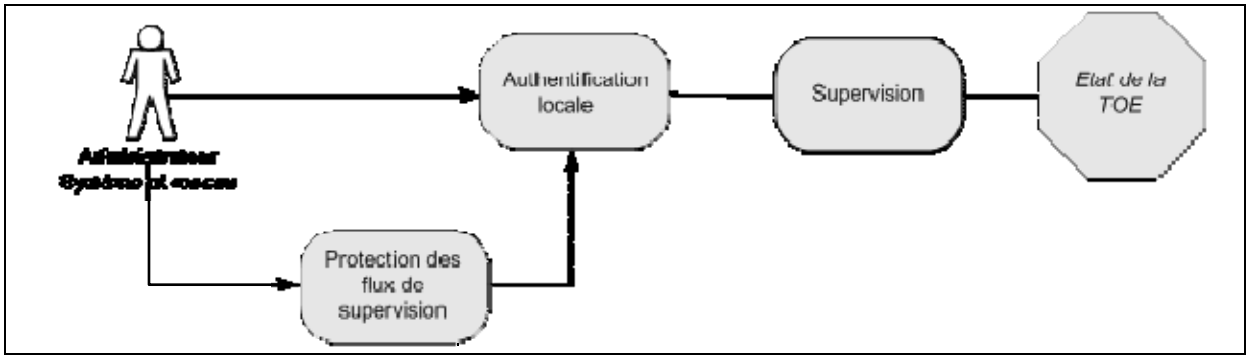

Figure 9 Supervision de la TOE

Annexe B Traces d'audits minimales et niveau associé

Pour chaque exigence fonctionnelle définie dans la partie 2 des CC v3.1r2, la prise en compte de certaines traces d'audit dans les exigences FAU_GEN est préconisée. Le tableau ci-dessous récapitule ces préconisations pour les exigences fonctionnelles retenues dans PP-FWIP et établit le niveau d'audit applicable.

Exigence PP-FWIP	**Préconisation CC partie 2**	**Niveau retenu**
FDP_IFC.2-Filtrage_Flux	N/A	N/A
FDP_IFF.1-Filtrage_Flux	a) Minimal: Decisions to permit requested information flows. b) Basic: All decisions on requests for information flow. c) Detailed: The specific security attributes used in making an information flow enforcement decision. d) Detailed: Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	Basic
FMT_SMF.1-Visualisation_politique_filtrage	a) Minimal: Use of the management functions.	Minimal
FAU_GEN.1-Audit_flux	N/A	
FAU_GEN.2-Audit_flux	N/A	
FIA_UID.2-Flux	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Basic
FPT_STM.1	a) Minimal: changes to the time; b) Detailed: providing a timestamp.	Minimal
FAU_SAR.1-Audit_flux	a) Basic: Reading of information from the audit records.	Basic
FAU_SAR.3-Audit_flux	a) Detailed: the parameters used for the viewing.	-
FMT_SMR.1	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	Minimal
FIA_UID.2-Administrateurs	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Basic
FIA_UAU.2-Administrateurs	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	Basic
FDP_ACC.1-Règles_filtrage	N/A	
FDP_ACF.1-Règles_filtrage	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Basic
FAU_STG.1-Traces_audit_flux	N/A	
FAU_GEN.1-Audit_admin	N/A	
FAU_GEN.2-Audit_admin	N/A	
FAU_SAR.1-Audit_admin	a) Basic: Reading of information from the audit records.	Basic

Exigence PP-FWIP	**Préconisation CC partie 2**	**Niveau retenu**
FAU_SAR.3-Audit_admin	a) Detailed: the parameters used for the viewing.	-
FAU_STG.1-Traces_audit_admin	N/A	
FAU_SAA.1-Alarmes	a) Minimal: Enabling and disabling of any of the analysis mechanisms; b) Minimal: Automated responses performed by the tool.	Minimal
FAU_ARP.1-Alarmes	a) Minimal: Actions taken due to potential security violations.	Minimal
FTP_ITC.1-Administration_distante	a) Minimal: Failure of the trusted channel functions. b) Minimal: Identification of the initiator and target of failed trusted channel functions. c) Basic: All attempted uses of the trusted channel functions. d) Basic: Identification of the initiator and target of all trusted channel functions.	Minimal
FPT_ITI.1-Administration_distante	a) Minimal: the detection of modification of transmitted TSF data. b) Basic: the action taken upon detection of modification of transmitted TSF data.	Basic
FPT_RPL.1-Administration_distante	a) Basic: Detected replay attacks. b) Detailed: Action to be taken based on the specific actions.	Detailed
FPT_ITC.1-Administration_distante	N/A	
FPT_TDC.1-Administration_distante	a) Minimal: Successful use of TSF data consistency mechanisms. b) Basic: Use of the TSF data consistency mechanisms. c) Basic: Identification of which TSF data have been interpreted. d) Basic: Detection of modified TSF data.	Basic
FMT_SMF.1-Configuration_TOE	a) Minimal: Use of the management functions.	Minimal
FMT_MTD.1-Paramètres_système_réseau	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1-Paramètres_TOE_Administrateur_sécurité	a) Basic: All modifications to the values of TSF data.	Basic
FMT_MTD.1-Paramètres_TOE_Auditeur	a) Basic: All modifications to the values of TSF data.	Basic
FMT_SMF.1-Supervision	a) Minimal: Use of the management functions.	Minimal
FPT_ITC.1-Supervision	N/A	
FDP_RIP.1-Recyclage_TOE	N/A	
FDP_ACC.1-Règles_filtrage	N/A	
FDP_ACF.1-Règles_filtrage	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Basic

Annexe C Définitions et acronymes

A.3 Acronymes

CC (Common Criteria) Critères Communs

EAL (Evaluation Assurance Level) Niveau d'assurance de l'évaluation. Un paquet composé de composants d'assurance tirés de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.

IP (Internet Protocol) Protocole Internet

IT (Information Technology) Technologie de l'information

OSP (Organisational security policies) Politiques de sécurité organisationnelles. Un ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.

PP (Protection Profile) Profil de protection. Un ensemble d'exigences de sécurité valables pour une catégorie de TOE, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

SF (Security Function) Fonction de sécurité. Une partie ou des parties de la TOE sur lesquelles on s'appuie pour appliquer un sous-ensemble étroitementimbriqué de règles tirées de la TSP.

SFP (Security Function Policy) Politique des fonctions de sécurité. La politique de sécurité appliquée par une Fonction de sécurité.

ST (Security Target) Cible de sécurité. Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une TOE identifiée.

TI Technologie de l'Information

TOE (Target Of Evaluation) Cible d'évaluation - Un produit ou un système TI et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.

TSF (TOE Security Functions) - Ensemble des fonctions de sécurité de la TOE. Un ensemble qui est constitué par tous les éléments matériels, logiciels et microprogrammés de la TOE sur lequel on doit s'appuyer pour l'application correcte de la TSP.

A.4 Définitions

Administrateur

Utilisateur autorisé à gérer tout ou une partie de la TOE. Il peut posséder des privilèges particuliers qui permettent de modifier la politique de sécurité de la TOE.

Authentification

Mesure de sécurité qui vérifie l'identité déclarée.

Authentification mutuelle

Mesure de sécurité qui permet pour chaque paire d'entités d'authentifier l'autre entité de la paire.

Environnement opérationnel

Environnement de la TOE lors de sa phase d'utilisation.

Politique de filtrage

Politique de sécurité définie pour la gestion des flux au niveau d'une interconnexion.

Règles de filtrage relatives à des contextes de connexion

Sur la base d'un premier filtrage non contextuel, règles de filtrage établies par la TOE, basées sur les caractéristiques du flux identifié (origine, destinataire, protocole applicatif). La connaissance de ce contexte permet à la TOE de s'affranchir des règles de filtrage explicites et ainsi de gagner en performance.

Raffiné éditorialement

Raffinement dans lequel une modification mineure est faite sur un élément d'exigence, telle que la reformulation d'une phrase pour des raisons de respect de la syntaxe. En aucun cas, cette modification ne change la signification de l'exigence.

Ce terme est défini dans [CC1]

Raffinement non éditorial

Raffinement qui permet d'ajouter des précisions ou de limiter l'ensemble des implémentations acceptables pour un élément d'exigence.

Raffinement global

Raffinement non éditorial qui s'applique à tous les éléments d'exigences d'un même composant.

Réseau protégé

Réseau interne à une entité (comme une entreprise ou un service) qui doit être protégé des flux arrivant de l'extérieur, et dont on doit maîtriser les flux sortants. C'est un réseau considéré comme sûr.

Réseau public

Réseau accessible à toute entité et toute personne qui ne peut être considéré comme sûr.

Annexe D Références

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2006, Version 3.1, Revision 1, CCMB-2006-09-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, September 2007, Version 3.1, Revision 2, CCMB-2007-09-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, September 2007, Version 3.1, Revision 2, CCMB-2007-09-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2007, Version 3.1, Revision 2, CCMB-2007-09-004.

[CRYPTO] Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse *standard*. http://www.ssi.gouv.fr/fr/sciences/publications

[CRYPTO_GESTION] Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications

[AUTH] Authentification : Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications

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

[PP-CIP] Profil de Protection, Chiffreur IP. Version 1.5, 3 février 2005, SGDN/DCSSI

[QUA-STD] Processus de qualification d'un produit de sécurité – Niveau *standard*. Version 1.1, 18 mars 2008, DCSSI, N°549/SGDN/DCSSI/SDR.

Annexe E Index