# Profil de protection Firewall d'interconnexion IP

| | | |
|---|---|---|
| **Version** | : | Version 2.2 |
| **Date** | : | 10 mars 2006 |
| **Classification** | : | Public |
| **Référence** | : | PP-FWIP |

# Historique du document

| Version | Date | Etat | 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 »<br>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 recommandations du rapport d'évaluation MELEZE_APE_1.1 | |

# Table des matières

# Table des figures

# Table des tables

# 1 Introduction

## 1.1 Identification du profil de protection

| | |
|---|---|
| **Titre :** | Profil de protection Firewall d'interconnexion IP |
| **Auteur :** | ARKOON, SGDN/DCSSI (Secrétariat Général de le Défense Nationale/Direction Centrale de la Sécurité des Systèmes d'Information) / Silicomp-AQL |
| **Version :** | Version 2.2 |
| **Commanditaires :** | DGE (Direction Générale des Entreprises) / ARKOON |
| **Version des CC :** | 2.3 |

Ce profil de protection est conforme aux parties 2 et 3 des Critères Communs ([CC2] et [CC3]).

Le niveau d'assurance de l'évaluation visé par ce profil de protection est EAL2+ (ou EAL2 augmenté) conformément au processus de qualification de niveau standard défini dans [QUA-STD].

Le niveau minimum de résistance des fonctions de sécurité visé par ce profil de protection est SOF-high, conformément également au processus de qualification de niveau standard défini dans [QUA-STD].

## 1.2 Présentation du profil de protection

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

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 en particulier à conserver, après l'interconnexion d'un réseau protégé, son niveau de sécurité initial.

Ce PP a été rédigé conformément aux attentes et aux préconisations du document [QUA-STD] qui définit le niveau standard comme correspondant à un premier niveau de qualité des produits de sécurité permettant la protection :

- des informations contre une atteinte à leurs disponibilité, intégrité et confidentialité,
- des systèmes contre une atteinte à leurs disponibilité et intégrité.

Par ailleurs, ce PP a été constitué sur la base d'un recueil de besoins de sécurité pour un produit de type firewall, à destination des organismes publics et privés.

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 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. |
| SOF | (Strength Of Function) Résistance des fonctions. La caractéristique d'une fonction de sécurité de la TOE exprimant les efforts minimum supposés nécessaires pour mettre en défaut le comportement de sécurité attendu par attaque directe des mécanismes de sécurité sous-jacents. |
| 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. |

## 1.4 Références


| | |
|---|---|
| [CC1] | Common Criteria for Information Technology Security Evaluation CCMB-2005-08-001, Part 1: Introduction and general model, Version 2.3, August 2005.Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 2.2, January 2004. CCIMB-2004-01-001. |
| [CC2] | Common Criteria for Information Technology Security Evaluation CCMB-2005-08-002, Part 2: Security functional requirements, Version 2.3, August 2005. |
| [CC3] | Common Criteria for Information Technology Security Evaluation CCMB-2005-08-003, Part 3: Security assurance requirements, Version 2.3, August 2005. |
| [CEM_PART1] | Common Criteria - Common Methodology for Information Technology Security Evaluation CEM-97/017, Part 1: Introduction and General Model, Version 0.6, 11 January 1997 (compliant with CC Version 1.0). |

| | |
|---|---|
| [CC1] | Common Criteria for Information Technology Security Evaluation CCMB-2005-08-001, Part 1: Introduction and general model, Version 2.3, August 2005.Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 2.2, January 2004. CCIMB-2004-01-001. |
| [CEM_PART2] | Common Criteria, Common Methodology for Information Technology Security Evaluation, CCMB-2005-08-004, Evaluation Methodology, Version 2.3, August 2005. |
| [CRYPTO] | Mécanismes de cryptographie : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, DCSSI, version 1.02 du 19/11/04. |
| [PB-INT] | Problématique d'interconnexion des réseaux IP. Version 1.8, mai 2003. 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 1.0, juillet 2003. DCSSI, 001591/SGDN/DCSSI/SDR. |

# 2 Description de la TOE

## 2.1 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.

### *2.1.1 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.

### *2.1.2 Services nécessaires au bon fonctionnement de la TOE*

#### 2.1.2.1 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.

#### 2.1.2.2 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 locale des administrateurs**

Ce service permet d'authentifier tous les administrateurs qui effectuent des opérations d'administration locale 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).

Ce service est divisé en deux parties qui sont toutes les deux incluses dans la TOE : l'une sur le firewall et l'autre sur la station d'administration.

#### 2.1.2.3 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, ...).

#### 2.1.2.4 Protection de l'accès aux paramètres de configuration

Ce service permet de protèger (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.

### *2.1.3 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 la suite du 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.

## 2.2 Architecture de la TOE

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

### *2.2.1 Architecture physique*

La Figure 1 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.

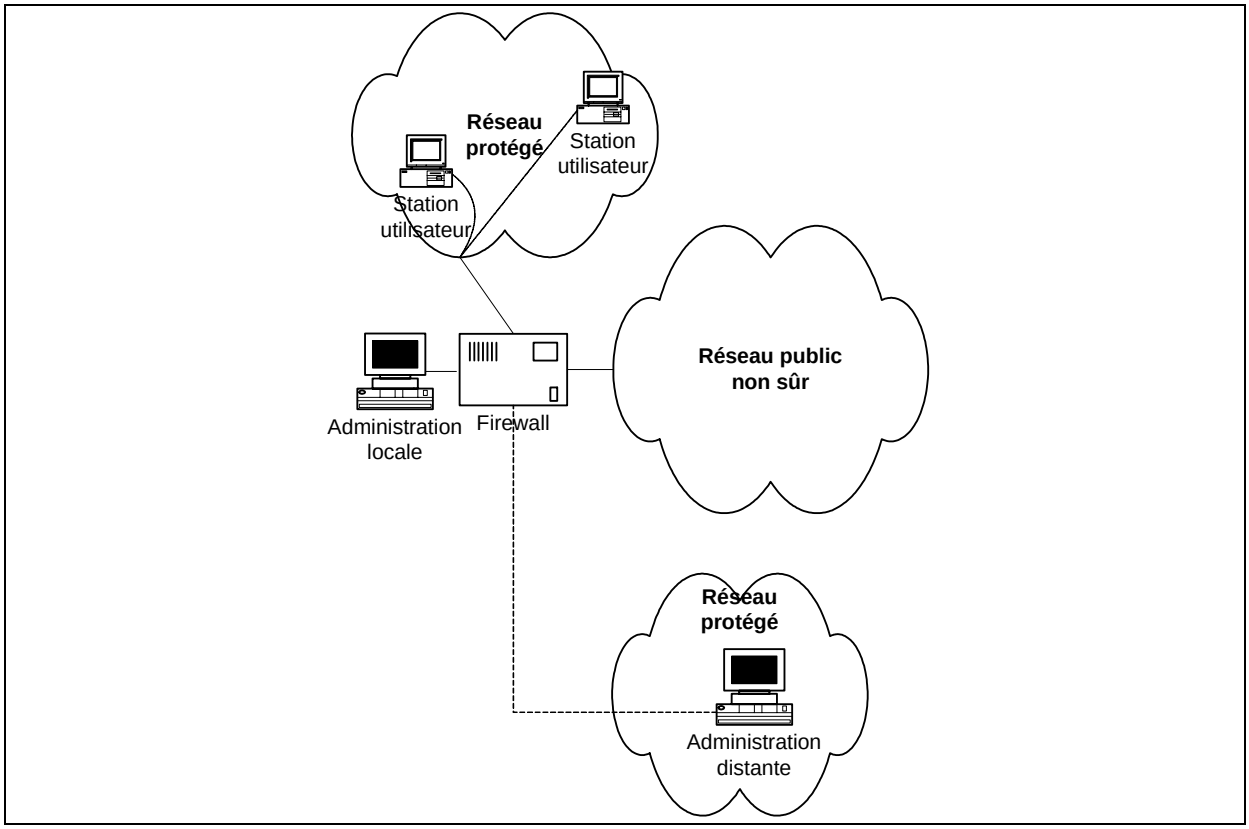


**Figure 1 Exemple d'architecture possible d'une interconnexion avec firewall**

Comme l'illustre la Figure 1, 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 téléadministration.

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.

### *2.2.2 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 2 présente les fonctionnalités qui concernent la gestion des rôles.

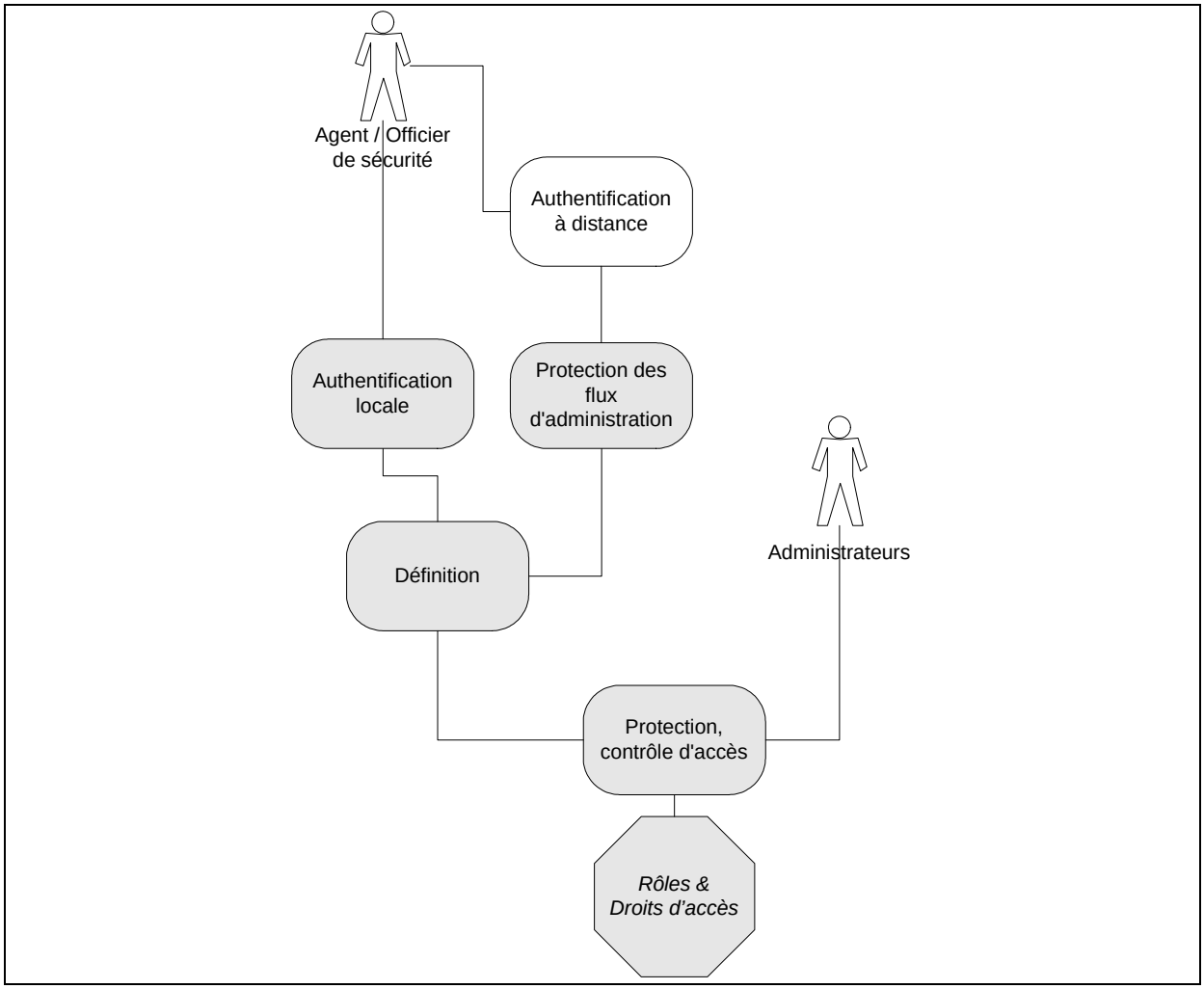


**Figure 2 Gestion des rôles**

La Figure 3 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.

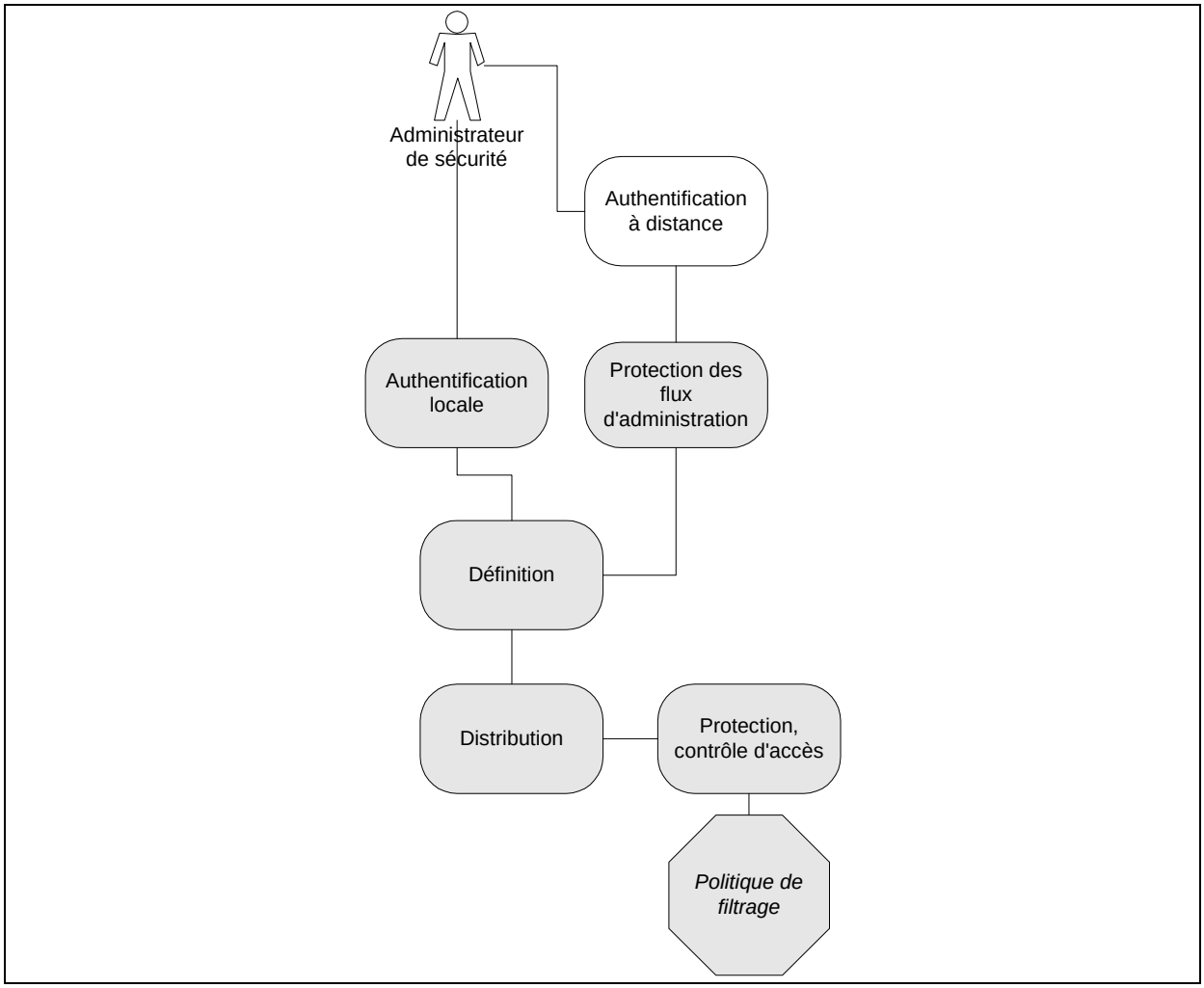


**Figure 3 Gestion de la politique de filtrage**

La Figure 4 présente les fonctionnalités qui concernent l'application de la politique de filtrage et des règles relatives aux contextes de connexion (en mode contextuel).

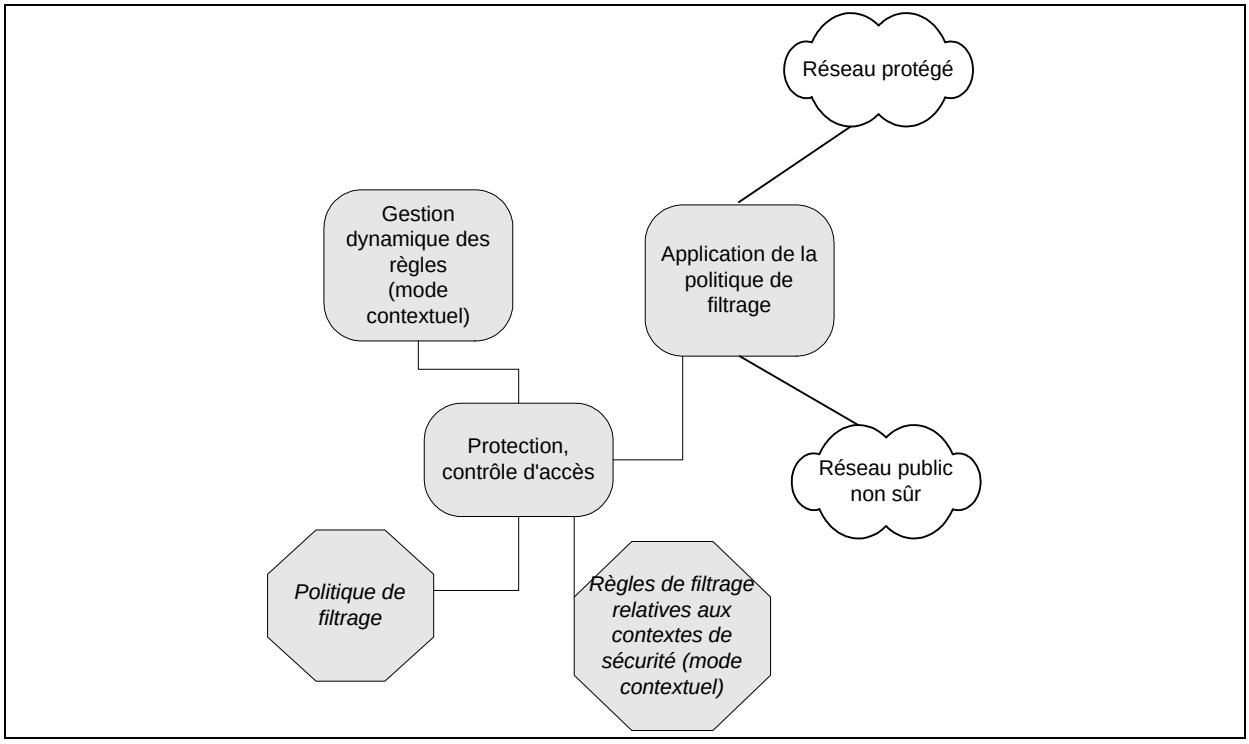


**Figure 4 Application de la politique de filtrage**

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 5). 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.

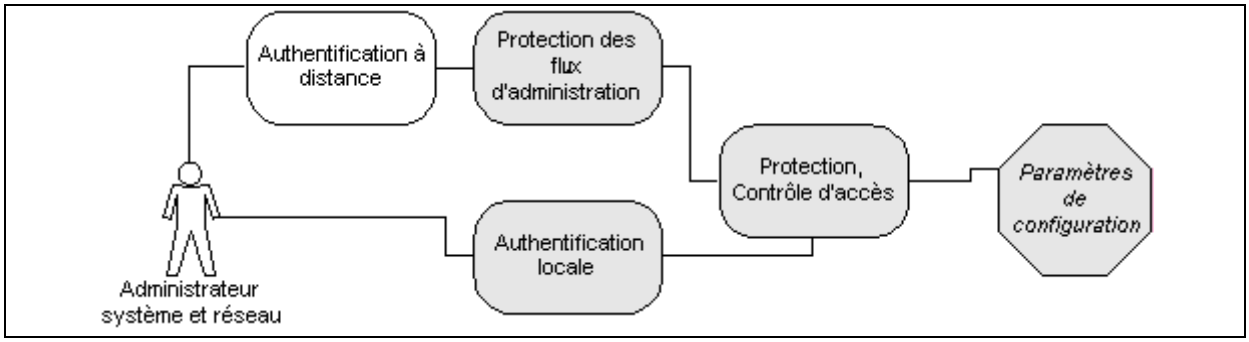


**Figure 5 Configuration du firewall**

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 6).

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.

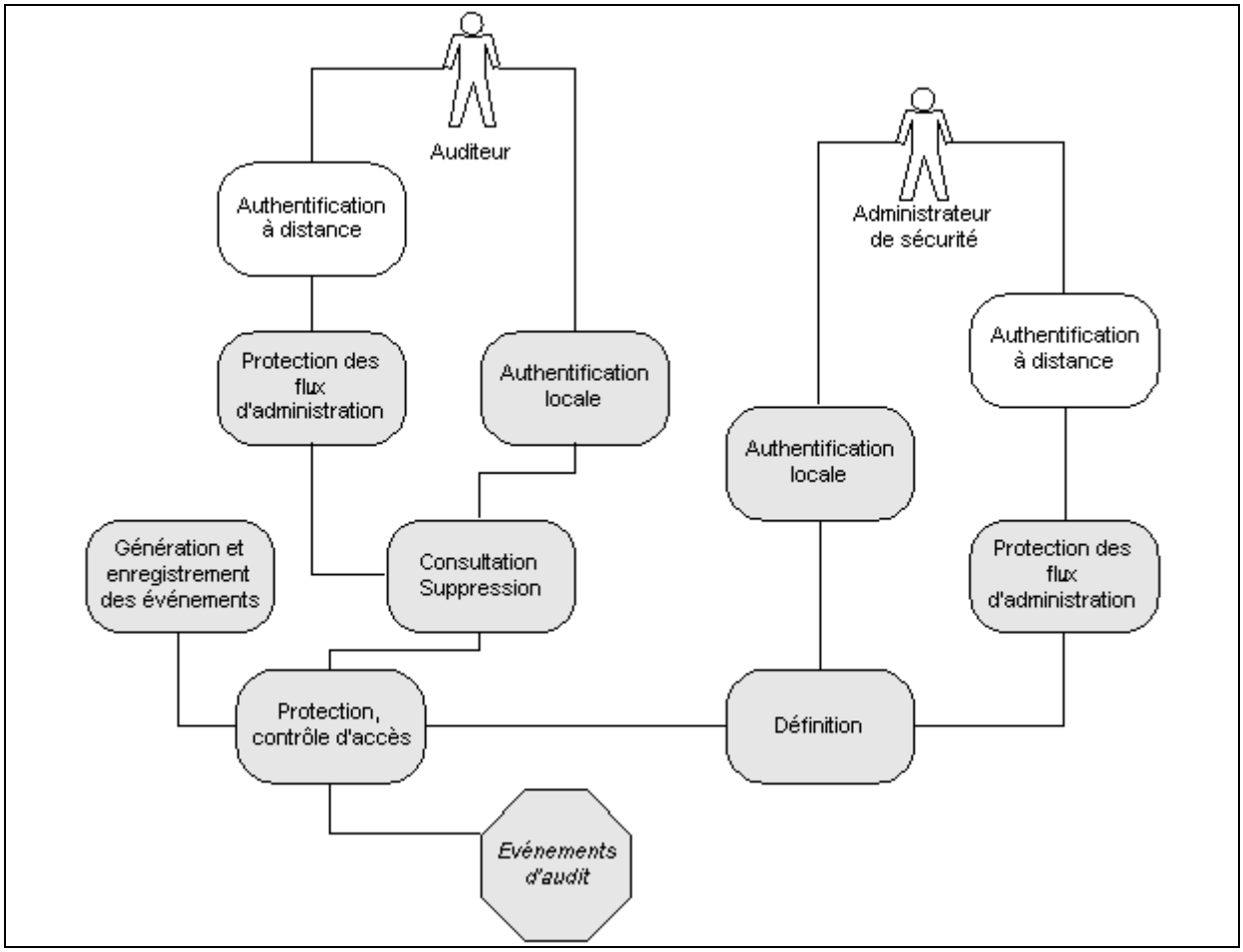


**Figure 6 Gestion de l'audit**

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 7).

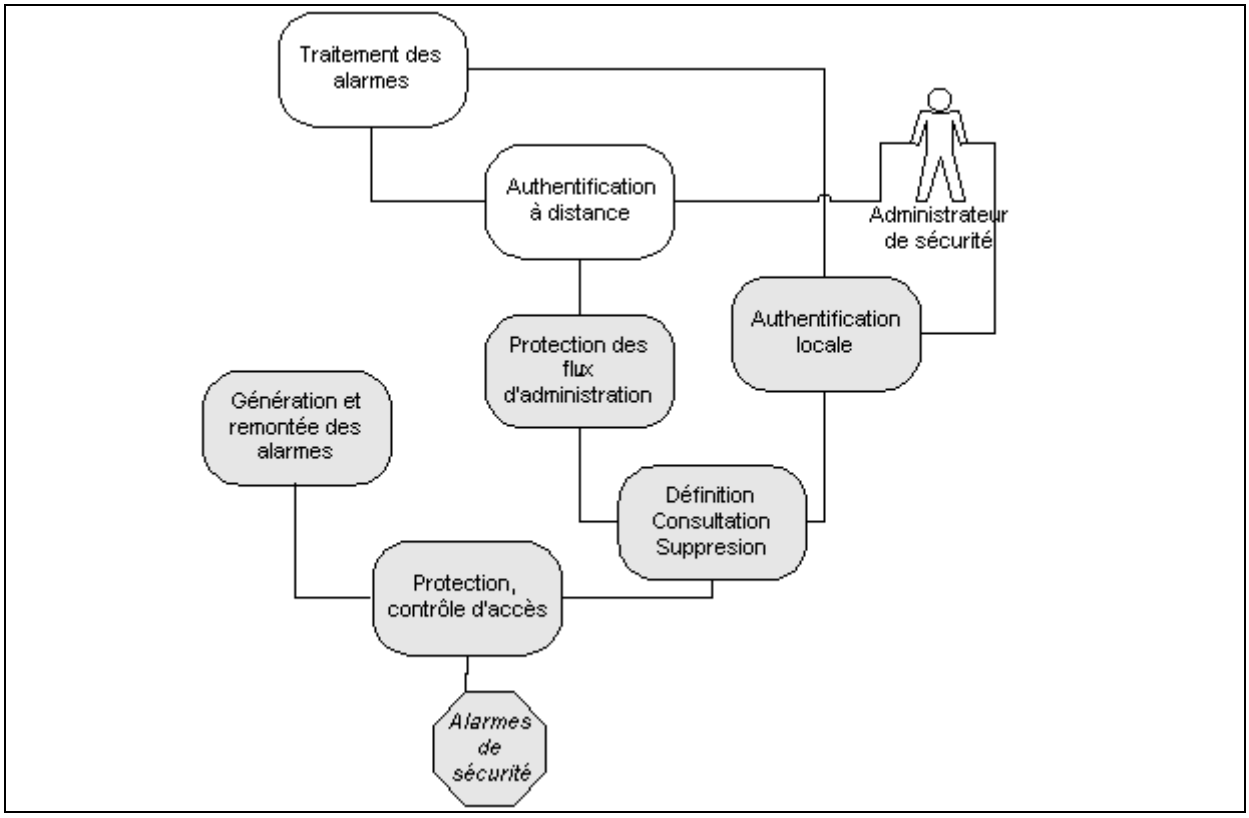


**Figure 7 Gestion des alarmes de sécurité**

Au niveau de la supervision, l'authentification à distance de l'administrateur système et réseau et la protection des flux de supervision ne font pas partie de la TOE (Figure 8).

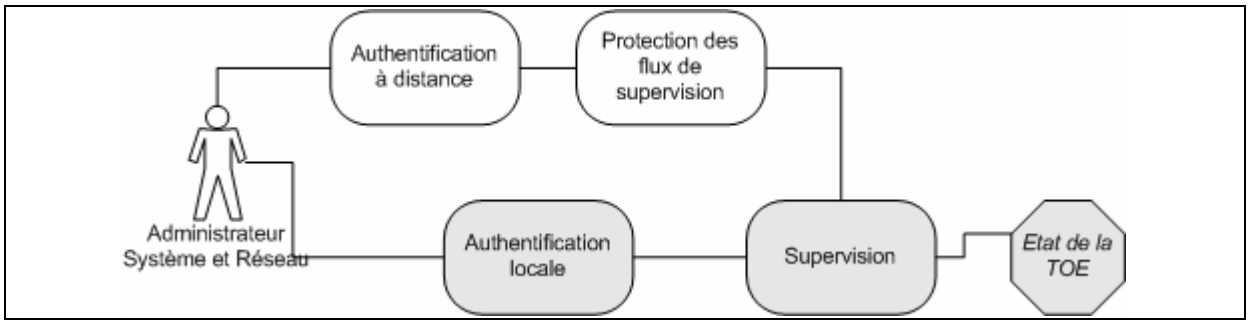


**Figure 8 Supervision de la TOE**

# 3 Environnement de sécurité de la TOE

## 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 Hypothèses

### *3.2.1 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.

### *3.2.2 Hypothèses sur l'environnement d'utilisation de la TOE*

**A.ADMIN**

Les administrateurs sont des personnes non hostiles. Elles disposent des moyens nécessaires à la réalisation de leurs tâches, sont formées 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 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.

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 regénérer 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.AUTHENTIFICATION_ADMIN_DISTANT**

L'environnement de la TOE permet d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants.

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

Les 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.

### *3.3.1 Menaces sur le fonctionnement des services 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.

### *3.3.2 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

### *3.3.3 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

### *3.3.4 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

### *3.3.5 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

### *3.3.6 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

### *3.3.7 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.

## 3.4 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.

**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.

**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.

# 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 définis au §2.1.3. 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 local (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 local 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).

**Evenements 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 local 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 local 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 garantir l'authenticité et la confidentialité des flux d'administration à distance. La protection en confidentialité n'est pas systématiquement appliquée si les données passant dans le flux ne sont pas confidentielles.

La TOE doit également protéger les flux contre le rejeu.

#### 4.1.2.4 Configuration de la TOE

**O.PROTECTION_PARAM**

La TOE doit contrôler l'accès local 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,...

## 4.2 Objectifs de sécurité pour l'environnement

### *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.AUTHENTIFICATION_ADMIN_DISTANT**

L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants.

#### 4.2.2.3 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 regénérer 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.

# 5 Exigences de sécurité des TI

## 5.1 Exigences de sécurité fonctionnelles pour la TOE

### *5.1.1 Services rendus par la TOE*

#### 5.1.1.1 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

- **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 TSC to flow to and from any subject in the TSC 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:

- **les adresses IP source et destination des paquets IP,**
- **les types de protocole,**
- **les ports de communication,**
- ***autres à définir par le rédacteur de la cible de sécurité.***

**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 provide the following **aucune capacité additionnelle**.

**FDP_IFF.1.5-Filtrage_Flux** The TSF shall explicitly authorise an information flow based on the following rules:

- ***règles d'acceptation à définir par le rédacteur de la cible de sécurité***

**FDP_IFF.1.6-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,**
- ***autres règles de refus à définir par le rédacteur de la cible de sécurité***.

**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 security management functions:

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

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

**FPT_TDC.1.1-** The TSF shall provide the capability to consistently interpret **la politique de filtrage par le firewall** when shared between the TSF and another trusted IT product.
**FPT_TDC.1.2-** The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

#### 5.1.1.2 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;**
- ***le rédacteur de la cible de sécurité détaillera les autres évènements à auditer***.

*Raffinement non éditorial:*

Le niveau de détail de la trace d'audit (minimum, basic, detailed) dépend de l'évènement audité. Le chapitre 7 récapitule les traces minimales requises et établit le niveau d'audit associé.

**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, 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** 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 identify itself before allowing any other TSF-mediated actions on behalf of that user.

*Raffinement global:*

On entend ici 'utilisateur' par les émétteurs 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 for its own use.

*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 perform **sorting, ordering and searches** of audit data based on **la date et l'heure** et **[assignment : criteria with logical relations]**.

#### 5.1.1.3 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 identify itself 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.

L'identification des administrateurs peut être locale ou issue du flux d'administration distante.

**FIA_UAU.2-Administrateurs_local User authentication before any action**

**FIA_UAU.2.1-Administrateurs_local** 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 locale du firewall. Pour l'administration distante, l'authentification de l'administrateur sur la station d'administration n'est pas incluse dans le périmètre de la TOE et est donc couverte par un objectif sur l'environnement. Concernant les exigences sur l'administration distante, se référer aux exigences fonctionnelles "Protection de l'administration distante".

### *5.1.2 Fonctionnement de la TOE*

#### 5.1.2.1 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 et auditeur**.

**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]**.

**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*

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).

#### 5.1.2.2 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 from unauthorised deletion.

**FAU_STG.1.2-Traces_audit_flux** The TSF shall be able to **prevent** unauthorised modifications to the 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 au chapitre 7 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, 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** 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 perform **sorting, ordering and searches** of audit data based on **des critères sélectionnés par l'auditeur**.

**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 from unauthorised deletion.

**FAU_STG.1.2-Traces_audit_admin** The TSF shall be able to **prevent** unauthorised modifications to the 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 TSP.

**FAU_SAA.1.2-Alarmes** The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of ***le rédacteur de la cible de sécurité doit défnir les événements à surveiller pour pouvoir soulever une alarme*** known to indicate a potential security violation;

b) ***tout autre évenement à définir par le rédacteur de la cible de sécurité qui pourrait déclencher une alarme***.

**FAU_ARP.1-Alarmes Security alarms**

**FAU_ARP.1.1-Alarmes** The TSF shall **déclencher la remontée d'une alarme à l'administrateur de sécurité** ***et toute autre action à définir par le rédacteur de la cible de sécurité*** upon detection of a potential security violation.

#### 5.1.2.3 Protection de l'administration distante

**FPT_ITT.1-Administration_distante Basic internal TSF data transfer protection**

**FPT_ITT.1.1-Administration_distante** The TSF shall protect TSF data from **disclosure and modification** when it is transmitted between separate parts of the TOE.

**FPT_ITT.3-Administration_distante TSF data integrity monitoring**

**FPT_ITT.3.1-Administration_distante** The TSF shall be able to detect **re-ordering of data, modification of data, substitution of data, deletion of data and au moins le rejeu des flux d'administration** for TSF data transmitted between separate parts of the TOE.

**FPT_ITT.3.2-Administration_distante** Upon detection of a data integrity error, the TSF shall take the following actions: ***le rédacteur de la cible de sécurité devra définir l'action à entreprendre***.

**FIA_UAU.2-Station_administration_distante User authentication before any action**

**FIA_UAU.2.1-Station_administration_distante** 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 pour l'administration distante du firewall. Cette exigence concerne l'authentification de la station d'administration vis-à-vis du firewall. Cette authentification peut être renforcée au niveau de la TOE par une authentification de l'administrateur directement auprès du firewall. Pour mémoire, l'authentification de l'administrateur distant vis-à-vis de la station d'administration distante relève de l'environnement de la TOE.

#### 5.1.2.4 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 security 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**.

#### 5.1.2.5 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 security 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 a remote 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.

#### 5.1.2.6 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]**.

**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]**.

## 5.2 Exigences de sécurité d'assurance pour la TOE

Le niveau des exigences de sécurité d'assurance est EAL2. L'EAL a été augmenté avec ADV_HLD.2, ADV_IMP.1(pour la partie de la TSF réalisant les exigences de la classe FCS), ADV_LLD.1(pour la partie de la TSF réalisant les exigences de la classe FCS), ALC_DVS.1, ALC_FLR.3, ALC_TAT.1(pour la partie de la TSF réalisant les exigences de la classe FCS), AVA_MSU.1 et AVA_VLA.2.

## 5.3 Exigences de sécurité pour l'environnement TI

### *5.3.1 Exigences fonctionnelles pour l'environnement TI*

#### 5.3.1.1 Administration distante

**FIA_UAU.2-Administration_distante User authentication before any action**

**FIA_UAU.2.1-Administration_distante** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

*Raffinement global:*

Il s'agit ici de l'authentification locale de l'administrateur sur la station d'administration distante.

# 6 Argumentaire

## 6.1 Argumentaire pour les objectifs de sécurité

### *6.1.1 Menaces*

#### 6.1.1.1 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'occurence 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)

#### 6.1.1.2 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)

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) et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurence 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)

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) et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurence 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

#### 6.1.1.3 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)

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) et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurence 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 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) et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurence 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

#### 6.1.1.4 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)

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) et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurence 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)

#### 6.1.1.5 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)

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) et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurence 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

#### 6.1.1.6 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)

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) et l'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT)

Pour détecter l'occurence 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)

#### 6.1.1.7 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'occurence de la menace, la TOE doit:

- aucune action

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

- aucune action

### *6.1.2 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.AUTHENTIFICATION_ADMIN_DISTANT** Cette hypothèse se traduit par OE.AUTHENTIFICATION_ADMIN_DISTANT

### *6.1.3 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.

### *6.1.4 Tables de couverture entre les éléments de l'environnement et les objectifs de securité*

| Menaces | Objectifs de sécurité | Argumentaire |
|---|---|---|
| T.DYSFONCTIONNEMENT | O.SUPERVISION, OE.INTEGRITE_TOE, O.IMPACT_SUPERVISION | Section 6.1.1 |
| T.MODIFICATION_POL_FILTRAGE | OE.PROTECTION_LOCAL, OE.ADMIN, OE.INTEGRITE_TOE, OE.TRAITE_ALARME, OE.AUTHENTIFICATION_ADMIN_DISTANT, O.PROTECTION_POL_FILTRAGE, O.PROTECTION_FLUX_ADMIN, O.APPLICATION_POL_FILTRAGE, O.AUDIT_ADMIN, O.AUDIT_FLUX, O.ALARMES | Section 6.1.1 |
| T.DIVULGATION_POL_FILTRAGE | OE.PROTECTION_LOCAL, OE.ADMIN, OE.TRAITE_ALARME, OE.AUTHENTIFICATION_ADMIN_DISTANT, O.APPLICATION_POL_FILTRAGE, O.PROTECTION_POL_FILTRAGE, O.PROTECTION_FLUX_ADMIN, O.AUDIT_ADMIN, O.AUDIT_FLUX, O.ALARMES | Section 6.1.1 |
| T.MODIFICATION_PARAMETRES | OE.PROTECTION_LOCAL, OE.ADMIN, OE.TRAITE_ALARME, OE.AUTHENTIFICATION_ADMIN_DISTANT, O.APPLICATION_POL_FILTRAGE, O.PROTECTION_PARAM, O.AUDIT_ADMIN, O.AUDIT_FLUX, O.ALARMES, OE.INTEGRITE_TOE, O.PROTECTION_FLUX_ADMIN | Section 6.1.1 |
| T.DIVULGATION_PARAMETRES | OE.PROTECTION_LOCAL, OE.ADMIN, OE.TRAITE_ALARME, OE.AUTHENTIFICATION_ADMIN_DISTANT, O.RECYCLAGE_TOE, O.APPLICATION_POL_FILTRAGE, O.PROTECTION_PARAM, O.AUDIT_ADMIN, O.AUDIT_FLUX, O.ALARMES, O.PROTECTION_FLUX_ADMIN | Section 6.1.1 |
| T.MODIFICATION_AUDIT_FLUX | OE.PROTECTION_LOCAL, OE.ADMIN, OE.AUTHENTIFICATION_ADMIN_DISTANT, O.APPLICATION_POL_FILTRAGE, OE.GESTION_TRACES_AUDIT, O.PROTECTION_AUDIT_FLUX, O.PROTECTION_FLUX_ADMIN | Section 6.1.1 |

| Menaces | Objectifs de sécurité | Argumentaire |
|---|---|---|
| T.MODIFICATION_ALARMES | OE.PROTECTION_LOCAL, OE.ADMIN, OE.AUTHENTIFICATION_ADMIN_DISTANT, O.APPLICATION_POL_FILTRAGE, O.PROTECTION_FLUX_ADMIN, O.PROTECTION_ALARMES | Section 6.1.1 |
| T.MODIFICATION_AUDIT_ADMIN | OE.PROTECTION_LOCAL, OE.ADMIN, OE.AUTHENTIFICATION_ADMIN_DISTANT, O.APPLICATION_POL_FILTRAGE, OE.GESTION_TRACES_AUDIT, O.PROTECTION_FLUX_ADMIN, O.PROTECTION_AUDIT_ADMIN | Section 6.1.1 |
| T.CHANGEMENT_CONTEXTE | O.RECYCLAGE_TOE | Section 6.1.1 |

**Tableau 1 Argumentaire 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 |
| 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.CONCEPTION_CRYPTO | |

| Objectifs de sécurité | Menaces |
|---|---|
| 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.AUTHENTIFICATION_ADMIN_DISTANT | 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 Argumentaire objectifs de sécurité vers menaces**

| Hypothèses | Objectifs de sécurité pour l'environnement | Argumentaire |
|---|---|---|
| A.ADMIN | OE.ADMIN | Section 6.1.2 |
| A.LOCAL | OE.PROTECTION_LOCAL | Section 6.1.2 |
| A.AUDIT | OE.GESTION_TRACES_AUDIT | Section 6.1.2 |
| A.ALARME | OE.TRAITE_ALARME | Section 6.1.2 |
| A.MAITRISE_CONFIGURATION | OE.INTEGRITE_TOE | Section 6.1.2 |
| A.AUTHENTIFICATION_ADMIN_DISTANT | OE.AUTHENTIFICATION_ADMIN_DISTANT | Section 6.1.2 |

**Tableau 3 Argumentaire 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.AUTHENTIFICATION_ADMIN_DISTANT | A.AUTHENTIFICATION_ADMIN_DISTANT |
| OE.GESTION_TRACES_AUDIT | A.AUDIT |
| OE.TRAITE_ALARME | A.ALARME |
| OE.INTEGRITE_TOE | A.MAITRISE_CONFIGURATION |

**Tableau 4 Argumentaire objectifs de sécurité pour l'environnement vers hypothèses**

| Politiques de sécurité organisationnelles | Objectifs de sécurité | Argumentaire |
|---|---|---|
| OSP.FILTRAGE | O.APPLICATION_POL_FILTRAGE, O.COHERENCE_POL, O.VISUALISATION_POL | Section 6.1.3 |
| OSP.AUDIT_FLUX | O.AUDIT_FLUX | Section 6.1.3 |
| OSP.GESTION_ROLES | O.GESTION_ROLES, O.AUDIT_ADMIN | Section 6.1.3 |
| OSP.CRYPTO | OE.CONCEPTION_CRYPTO | Section 6.1.3 |

**Tableau 5 Argumentaire 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 | |
| O.PROTECTION_ALARMES | |
| O.PROTECTION_FLUX_ADMIN | |
| O.PROTECTION_PARAM | |
| O.SUPERVISION | |
| O.IMPACT_SUPERVISION | |
| O.RECYCLAGE_TOE | |
| OE.CONCEPTION_CRYPTO | OSP.CRYPTO |
| OE.PROTECTION_LOCAL | |
| OE.ADMIN | |
| OE.AUTHENTIFICATION_ADMIN_DISTANT | |
| OE.GESTION_TRACES_AUDIT | |
| OE.INTEGRITE_TOE | |

**Tableau 6 Argumentaire objectifs de sécurité vers politiques de sécurité organisationnelles**

## 6.2 Argumentaire pour les exigences de sécurité

### *6.2.1 Objectifs*

#### 6.2.1.1 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). L'authentification locale des administrateurs est couverte par FIA_UAU.2-Administrateurs_local; l'authentification pour l'administration distante relève de FIA_UAU.2-Station_administration_distante.

**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.

Evenements 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 évenements 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 FPT_ITT.1-Administration_distante et FPT_ITT.3-Administration_distante sur la protection des données transmises entre le firewall et la station d'administration distante.

*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.

#### 6.2.1.2 Objectifs de sécurité pour l'environnement

**Objectifs de sécurité sur l'exploitation de la TOE**

*Administration de la TOE*

**OE.AUTHENTIFICATION_ADMIN_DISTANT** L'objectif est traduit directement par l'exigence d'authentification des administrateurs sur la station d'administration distante: FIA_UAU.2-Administration_distante.

### *6.2.2 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 6.2.1 |
| O.VISUALISATION_POL | FMT_SMF.1-Visualisation_politique_filtrage | Section 6.2.1 |
| O.COHERENCE_POL | FPT_TDC.1-Administration_distante | Section 6.2.1 |
| 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 6.2.1 |
| O.GESTION_ROLES | FMT_SMR.1, FIA_UID.2-Administrateurs, FIA_UAU.2-Administrateurs_local, FIA_UAU.2-Station_administration_distante | Section 6.2.1 |
| O.PROTECTION_POL_FILTRAGE | FDP_ACC.1-Règles_filtrage, FDP_ACF.1-Règles_filtrage | Section 6.2.1 |
| O.PROTECTION_AUDIT_FLUX | FAU_STG.1-Traces_audit_flux | Section 6.2.1 |
| 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 6.2.1 |
| O.PROTECTION_AUDIT_ADMIN | FAU_STG.1-Traces_audit_admin | Section 6.2.1 |
| O.ALARMES | FAU_ARP.1-Alarmes, FAU_SAA.1-Alarmes | Section 6.2.1 |
| O.PROTECTION_ALARMES | FAU_STG.1-Traces_audit_flux, FAU_STG.1-Traces_audit_admin | Section 6.2.1 |
| O.PROTECTION_FLUX_ADMIN | FPT_ITT.1-Administration_distante, FPT_ITT.3-Administration_distante | Section 6.2.1 |
| 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 6.2.1 |
| O.SUPERVISION | FMT_SMF.1-Supervision | Section 6.2.1 |

| Objectifs de sécurité | Exigences fonctionnelles pour la TOE | Argumentaire |
|---|---|---|
| O.IMPACT_SUPERVISION | FPT_ITC.1-Supervision | Section 6.2.1 |
| O.RECYCLAGE_TOE | FDP_RIP.1-Recyclage_TOE, FDP_ACC.1-Recyclage_TOE, FDP_ACF.1-Recyclage_TOE | Section 6.2.1 |

**Tableau 7 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 |
| FPT_TDC.1-Administration_distante | O.COHERENCE_POL |
| 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 |
| FIA_UAU.2-Administrateurs_local | O.GESTION_ROLES |
| FDP_ACC.1-Règles_filtrage | O.PROTECTION_POL_FILTRAGE |
| 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 |
| FPT_ITT.1-Administration_distante | O.PROTECTION_FLUX_ADMIN |
| FPT_ITT.3-Administration_distante | O.PROTECTION_FLUX_ADMIN |
| FIA_UAU.2-Station_administration_distante | O.GESTION_ROLES |
| 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 |

| Exigences fonctionnelles pour la TOE | Objectifs de sécurité |
|---|---|
| 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 8 Argumentaire exigences fonctionnelles de la TOE vers objectifs de sécurité**

| Objectifs de sécurité | Exigences de sécurité pour l'environnement | Argumentaire |
|---|---|---|
| OE.CONCEPTION_CRYPTO | | |
| OE.PROTECTION_LOCAL | | |
| OE.ADMIN | | |
| OE.AUTHENTIFICATION_ADMIN_DISTANT | FIA_UAU.2-Administration_distante | Section 6.2.1 |
| OE.GESTION_TRACES_AUDIT | | |
| OE.INTEGRITE_TOE | | |

**Tableau 9 Argumentaire exigences vers objectifs de sécurité pour l'environnement**

| Exigences de sécurité pour l'environnement | Objectifs de sécurité |
|---|---|
| FIA_UAU.2-Administration_distante | OE.AUTHENTIFICATION_ADMIN_DISTANT |

**Tableau 10 Argumentaire objectifs de sécurité pour l'environnement vers exigences**

### *6.2.3 Argumentaire pour l'EAL*

Le niveau d'assurance de ce PP est EAL2+, car il est requis par le processus de qualification standard [QUA-STD].

### *6.2.4 Argumentaire pour les augmentations à l'EAL*

#### 6.2.4.1 ADV_HLD.2 Security enforcing high-level design

Augmentation requise par le processus de qualification standard.

#### 6.2.4.2 ADV_IMP.1(pour la partie de la TSF réalisant les exigences de la classe FCS) Subset of the implementation of the TSF

Cette augmentation est requise par le processus de qualification standard et n'est valable que pour la classe fonctionnelle FCS.

#### 6.2.4.3 ADV_LLD.1(pour la partie de la TSF réalisant les exigences de la classe FCS) Descriptive low-level design

Cette augmentation est requise par le processus de qualification standard et n'est valable que pour la classe fonctionnelle FCS.

#### 6.2.4.4 ALC_DVS.1 Identification of security measures

Augmentation requise par le processus de qualification standard.

#### 6.2.4.5 ALC_FLR.3 Systematic flaw remediation

Augmentation requise par le processus de qualification standard.

#### 6.2.4.6 ALC_TAT.1(pour la partie de la TSF réalisant les exigences de la classe FCS) Well-defined development tools

Cette augmentation est requise par le processus de qualification standard et n'est valable que pour la classe fonctionnelle FCS.

#### 6.2.4.7 AVA_MSU.1 Examination of guidance

Augmentation requise par le processus de qualification standard.

#### 6.2.4.8 AVA_VLA.2 Independent vulnerability analysis

Augmentation requise par le processus de qualification standard.

### *6.2.5 Dépendances des exigences de sécurité fonctionnelles*

| Exigences | Dépendances CC | Dépendances Satisfaites |
|---|---|---|
| FIA_UAU.2-Administration_distante | (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 | |
| FPT_TDC.1-Administration_distante | 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 |
| FMT_SMR.1 | (FIA_UID.1) | FIA_UID.2-Administrateurs |
| FIA_UID.2-Administrateurs | Pas de dépendances | |
| FIA_UAU.2-Administrateurs_local | (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 |
| FPT_ITT.1-Administration_distante | Pas de dépendances | |
| FPT_ITT.3-Administration_distante | (FPT_ITT.1) | FPT_ITT.1-Administration_distante |
| FIA_UAU.2-Station_administration_distante | (FIA_UID.1) | FIA_UID.2-Flux |
| 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-Paramètres_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 |

| Exigences | Dépendances CC | Dépendances Satisfaites |
|---|---|---|
| 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 11 Dépendances des exigences fonctionnelles**

#### 6.2.5.1 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.

### *6.2.6 Dépendances des exigences de sécurité d'assurance*

| Exigences | Dépendances CC | Dépendances Satisfaites |
|---|---|---|
| ACM_CAP.2 | Pas de dépendances | |
| ADO_DEL.1 | Pas de dépendances | |
| ADO_IGS.1 | (AGD_ADM.1) | AGD_ADM.1 |
| ADV_FSP.1 | (ADV_RCR.1) | ADV_RCR.1 |
| ADV_HLD.2 | (ADV_FSP.1) et (ADV_RCR.1) | ADV_FSP.1, ADV_RCR.1 |
| ADV_IMP.1(pour la partie de la TSF réalisant les exigences de la classe FCS) | (ADV_LLD.1) et (ADV_RCR.1) et (ALC_TAT.1) | ADV_LLD.1(pour la partie de la TSF réalisant les exigences de la classe FCS), ADV_RCR.1, ALC_TAT.1(pour la partie de la TSF réalisant les exigences de la classe FCS) |
| ADV_LLD.1(pour la partie de la TSF réalisant les exigences de la classe FCS) | (ADV_HLD.2) et (ADV_RCR.1) | ADV_HLD.2, ADV_RCR.1 |
| ADV_RCR.1 | Pas de dépendances | |
| AGD_ADM.1 | (ADV_FSP.1) | ADV_FSP.1 |
| AGD_USR.1 | (ADV_FSP.1) | ADV_FSP.1 |
| ALC_DVS.1 | Pas de dépendances | |
| ALC_FLR.3 | Pas de dépendances | |
| ALC_TAT.1(pour la partie de la TSF réalisant les exigences de la classe FCS) | (ADV_IMP.1) | ADV_IMP.1(pour la partie de la TSF réalisant les exigences de la classe FCS) |
| ATE_COV.1 | (ADV_FSP.1) et (ATE_FUN.1) | ADV_FSP.1, ATE_FUN.1 |

| Exigences | Dépendances CC | Dépendances Satisfaites |
|---|---|---|
| ATE_FUN.1 | Pas de dépendances | |
| ATE_IND.2 | (ADV_FSP.1) et (AGD_ADM.1) et (AGD_USR.1) et (ATE_FUN.1) | ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1 |
| AVA_MSU.1 | (ADO_IGS.1) et (ADV_FSP.1) et (AGD_ADM.1) et (AGD_USR.1) | ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1 |
| AVA_SOF.1 | (ADV_FSP.1) et (ADV_HLD.1) | ADV_FSP.1, ADV_HLD.2 |
| AVA_VLA.2 | (ADV_FSP.1) et (ADV_HLD.2) et (ADV_IMP.1) et (ADV_LLD.1) et (AGD_ADM.1) et (AGD_USR.1) | ADV_FSP.1, ADV_HLD.2, ADV_IMP.1(pour la partie de la TSF réalisant les exigences de la classe FCS), ADV_LLD.1(pour la partie de la TSF réalisant les exigences de la classe FCS), AGD_ADM.1, AGD_USR.1 |

**Tableau 12 Dépendances des exigences d'assurance**

### *6.2.7 Argumentaire pour la résistance des fonctions*

Le niveau minimum de résistance est SOF-high, car il est requis par le processus de qualification standard [QUA-STD].

# 7 Traces d'audits minimales et niveau associé

Pour chaque exigence fonctionnelle définie dans la partie 2 des CC v2.2, 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.<br>b) Basic: All decisions on requests for information flow.<br>c) Detailed: The specific security attributes used in making an information flow enforcement decision.<br>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 |
| FPT_TDC.1-Administration_distante | a) Minimal: Successful use of TSF data consistency mechanisms.<br>b) Basic: Use of the TSF data consistency mechanisms. | Basic |

| | | |
|---|---|---|
| | c) Basic: Identification of which TSF data have been interpreted.<br>d) Basic: Detection of modified TSF data. | |
| 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;<br>b) Basic: All use of the user identification mechanism, including the user identity provided. | Basic |
| FPT_STM.1 | a) Minimal: changes to the time;<br>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;<br>b) Detailed: every use of the rights of a role. | Minimal |
| FIA_UID.2-Administrateurs | a) Minimal: Unsuccessful use | Basic |

| | | |
|---|---|---|
| | of the user identification mechanism, including the user identity provided;<br>b) Basic: All use of the user identification mechanism, including the user identity provided. | |
| FIA_UAU.2-Administrateurs_local | a) Minimal: Unsuccessful use of the authentication mechanism;<br>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.<br>b) Basic: All requests to perform an operation on an object covered by the SFP.<br>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 |

| | | |
|---|---|---|
| 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;<br>b) Minimal: Automated responses performed by the tool. | Minimal |
| FAU_ARP.1-Alarmes | a) Minimal: Actions taken due to imminent security violations. | Minimal |
| FPT_ITT.1-Administration_distante | N/A | |
| FPT_ITT.3-Administration_distante | a) Minimal: the detection of modification of TSF data;<br>b) Basic: the action taken following detection of an integrity error. | Basic |
| FIA_UAU.2-Station_administration_distante | a) Minimal: Unsuccessful use of the authentication mechanism;<br>b) Basic: All use of the authentication mechanism. | Basic |
| FMT_SMF.1-Configuration_TOE | a) Minimal: modifications to the group of users that are part of a role;<br>b) Detailed: every use of the rights of a role. | Minimal |
| FMT_MTD.1-Paramètres_système_réseau | a) Basic: All | Basic |

| | | |
|---|---|---|
| | modifications to the values of TSF data. | |
| 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.<br>b) Basic: All requests to perform an operation on an object covered by the SFP.<br>c) Detailed: The specific security attributes used in making an access check. | Basic |
| FIA_UAU.2-Administration_distante | a) Minimal: Unsuccessful use of the authentication mechanism;<br>b) Basic: All use of the authentication mechanism. | Basic |

# 8 Notice

Ce document a été majoritairement généré avec TL SET version 1.7, les Critères Communs version 2.2 avec les interprétations de janvier 2004 (incluant les interprétations: 137). L'outil d'édition sécuritaire de Trusted Logic est disponible sur www.trusted-logic.fr.

# 9 Glossaire

Cette annexe donne la définition des principaux termes utilisés dans ce document. Pour la définition des termes Critères Communs se référer à [CC1], § 2.3.

| | |
|---|---|
| **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. |
| **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. |

# 10 Index