Direction centrale de la sécurité des systèmes d'information

Profil de Protection
Pare-feu personnel
(PP-PFP)

Date de publication	**:**	2 mai 2006
Référence	**:**	PP-PFP
Version	**:**	1.4

Table des matières

1 Introduction

1.1 Identification

Titre : Profil de protection – Pare-feu Personnel

Référence : PP-PFP, version 1.4, 2 mai 2006

Auteur : Fidens

1.2 Contexte

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

L'objectif est de fournir un cadre administratif à la certification de pare-feu personnel pour les besoins des secteurs public et privé en vue de leur qualification.

1.3 Présentation générale de la cible d'évaluation

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

1.3.1 Type de la TOE

Le présent profil de protection exprime les objectifs de sécurité ainsi que les exigences fonctionnelles et d'assurance pour un pare-feu personnel (la TOE).

Ce pare-feu personnel est un composant logiciel installé sur un poste de travail et destiné à assurer le filtrage des flux réseau entrant et sortant de ce poste de travail.

1.3.2 Particularités / caractéristiques de sécurité de la TOE

Le pare-feu personnel a pour mission principale d'analyser et de filtrer les flux de données entrant et sortant d'un poste de travail pour protéger celui-ci contre :

- La diffusion de données locales du poste vers l'extérieur à l'insu de l'usager (via des chevaux de Troie, des espions logiciels, ...).
- la diffusion de données locales du poste vers l'extérieur via des services non autorisés par la politique de sécurité de l'organisation.
- Les attaques en provenance du réseau : exploitation illicite à distance de ressources locales, altération ou destruction à distance de données locales, saturation de ressources locales du poste (attaques de type déni de service).

Cette composante de filtrage des communications peut réaliser au minimum un filtrage

applicatif et un filtrage réseau. Le filtrage applicatif est associé à une fonction de contrôle d'intégrité des applications qui accèdent au réseau. Le filtrage réseau prend en compte la notion de filtrage contextuel ou comportemental[1].

Ce pare-feu personnel (PFP) a vocation à être installé et utilisé sur un poste de travail fixe ou nomade. Le poste nomade peut être utilisé dans ou hors des locaux de l'entreprise. Le politique de sécurité mise en oeuvre tient compte de cet environnement réseau.

Le poste de travail peut être multi-utilisateurs. Le PFP permet d'adapter la politique de sécurité en fonction des usagers du poste. L'usager peut être administrateur du poste.[2]

Dans certaines organisations, le PFP doit pouvoir fonctionner de manière transparente pour l'usager.

Une composante administration du PFP permet principalement de définir la politique de filtrage et les droits d'accès relatifs à cette politique. L'administration peut être faite par un administrateur, par un usager ou par les deux. Elle peut être réalisée localement sur le poste ou à distance depuis un centre d'administration.

Une composante journalisation et supervision permet de tracer les opérations relatives au fonctionnement et à l'administration du PFP et d'émettre des alarmes et cas de violation de la politique de sécurité. Elle permet aussi de tracer les flux réseau traités par le PFP. La supervision peut être locale sur le poste ou distante depuis un centre de supervision.

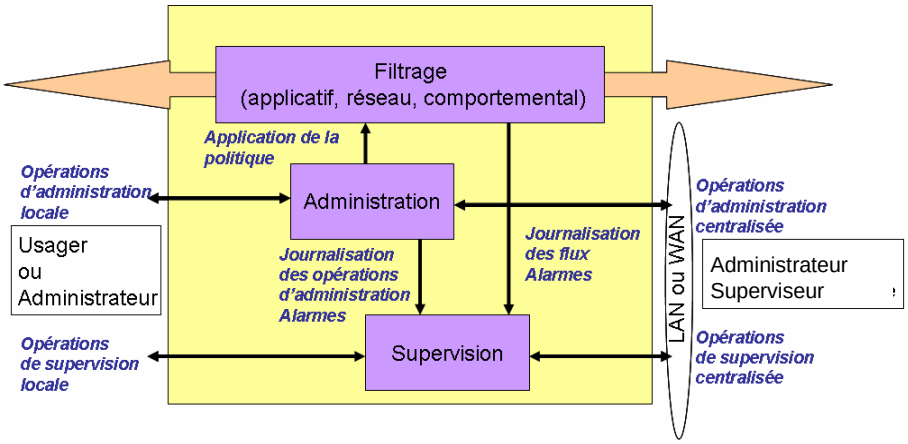

Figure 1 : schéma général de la TOE

1.3.3 Environnement matériel et logiciel

Pour fonctionner, la TOE s'appuie fortement sur le système d'exploitation utilisé sur le poste de travail à protéger.

[1] Par filtrage contextuel ou comportemental, on entend la capacité qu'a la TOE de filtrer un paquet en fonctions des paquets déjà reçus ou émis.

[2] Ce profil de protection fait la différence entre « l'usager », terme qui désigne une personne dont le rôle principal est d'utiliser le poste et « l'utilisateur », terme qui désigne une personne dont le rôle peut être celui d'un simple usager, d'un administrateur ou d'un superviseur.

Ce système d'exploitation doit permettre d'identifier les utilisateurs du poste de travail et doit contribuer à la protection de la TOE et ses données vis-à-vis de ces utilisateurs.

Le poste de travail doit disposer d'au moins une interface réseau et des logiciels associés.

1.4 Déclarations de conformité

Conformité de ce profil de protection :

Ce profil de protection est conforme à :

- La partie 2 des critères communs, version 3.0, révision 2, de juin 2005 (cf. [CC2]).
- La partie 3 des critères communs, version 3.0, révision 2, de juin 2005 (cf. [CC3]).

Aucune extension ou interprétation n'est retenue.

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

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

Conformité des cibles de sécurité et profils de protection :

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

Dans la mesure du possible, les auteurs de cible de sécurité ou de profil de protection qui souhaitent la conformité à ce PP, viseront un niveau de conformité « strict ».

Le niveau de conformité « démontrable » permet :

- d'annoncer une conformité à plusieurs profils de protection,
- de spécifier un paquet d'assurance plus élevé,
- de spécifier des exigences de sécurité fonctionnelles alternatives,
- de transformer un objectif de sécurité sur l'environnement opérationnel en un objectif de sécurité sur la TOE,
- de modifier les opérations du PP dans la mesure où elles sont plus restrictives.

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

2 Définition du problème de sécurité

2.1 Biens

La TOE offre des services visant à protéger le poste de travail contre la diffusion intempestive de données locales (attaques par cheval de Troie, KeyLogger, backdoor), contre l'exploitation à distance de ressources locales (temps CPU de la machine, attaque par rebond), contre la destruction ou l'altération de données locales à distance (attaques de type cheval de Troie, usurpation virale d'application, accès distant direct aux ressources statiques – système de fichiers - du poste de travail).

La TOE protège ces biens via :

- L'analyse et le filtrage de toutes les communications et connexions entrantes et sortantes (sur réseau local et distant) du poste de travail.
- La vérification de l'intégrité des applications "communicantes" du poste de travail sur lequel elle est installée.

2.1.1 Biens dans l'environnement opérationnel

2.1.1.1 Biens sensibles protégés par la TOE

Les biens protégés par la TOE sont :

D_data	Données stockées sur le poste de travail
D_appli	Les applications installées ou utilisables sur le poste de travail
D_services	Des services et les ressources logiques du poste de travail

D_data

Ce bien correspond aux données stockées sur le poste de travail dans des fichiers ou des bases de données. Ces données peuvent être des données utilisateurs ou des données de configuration ou de paramétrage des applications. Ces données peuvent être altérées ou rendues indisponibles par des accès extérieurs. Elles peuvent être exportées de manière illicite par un cheval de Troie.

Sensibilité : confidentialité, intégrité, disponibilité.

D_appli

Ce bien correspond aux applications, aux programmes et aux bibliothèques de programmes installés sur le poste et utilisés par les usagers. Ces applications peuvent être rendues indisponibles, altérées (insertion de chevaux de Troie) ou contenir des programmes espions (spyware).

Sensibilité : intégrité, disponibilité.

D_services

Des services ou ressources logiques du poste peuvent être protégées par la TOE. C'est notamment le cas de ressources du poste qui pourraient être saturées par des accès extérieurs répétés (attaques de type déni de service).

Sensibilité : disponibilité.

2.1.1.2 Biens sensibles de la TOE

Les biens sensibles de la TOE sont :

D_logiciel	La TOE elle-même en tant que logiciel.
D_filtre_flux	Règle de filtrage des flux de communications entrants ou sortants.
D_filtre_appli	Règle de filtrage des applications voulant réaliser des accès réseau.
D_param_config	Paramètres de configuration de la TOE.
D_param_CA	Paramètres de contrôle d'accès local ou distant à la TOE.
D_audit_flux	Données journalisées relatives à l'activité de communication du poste de travail (flux réseau).
D_audit_admin	Données journalisées relatives à l'administration, à la supervision et au fonctionnement de la TOE : démarrage, arrêt, modification de règles, de niveau d'alerte ou de paramètres...
D_alerte	Alertes générées sur détection de tentatives d'attaque.

D_logiciel

Ce bien sensible correspond à l'ensemble des programmes de la TOE. Ces programmes sont mémorisés et utilisés sur le poste.

Sensibilité : Intégrité, disponibilité.

D_filtre_flux

Une règle de filtrage des flux définit les traitements à effectuer sur les flux entrants et sortants du poste de travail afin de déterminer si ces flux sont autorisés ou non. Ces flux sont des flux portés par la pile protocolaire TCP/IP[3].

Ces règles sont mémorisées sur le poste, modifiables par les administrateurs et éventuellement par les usagers.

Sensibilité : confidentialité, intégrité.

D_filtre_appli

Une règle de filtrage des applications définit les traitements à effectuer lors des demandes de connexion vers l'extérieur des applications du poste de travail. Elle a pour but d'éviter la communication avec l'extérieur du poste de travail, de logiciels de type chevaux de Troie. Elle inclut un contrôle d'intégrité des applications pour éviter l'usurpation d'un logiciel autorisé par un logiciel malveillant, et le contrôle des communications demandées par l'application.

[3] Les ST conformes à ce PP devront spécifier les protocoles propriétaires ou non IP pris en compte.

Ces règles sont mémorisées sur le poste, modifiables par les administrateurs et éventuellement par les usagers.

Sensibilité : confidentialité, intégrité.

D_param_config

Les paramètres de configuration de la TOE regroupent notamment :

- La configuration générale de la TOE.
- Les paramètres relatifs à la journalisation et à la supervision : niveau des traces (log) produites par la TOE, fréquence de remontée des informations, niveau des alertes à envoyer, fréquence et adresse du serveur pour les mises à jour.
- Les paramètres relatifs à la politique d'administration.

Ces paramètres sont stockés localement et peuvent être modifiés localement (via l'IHM de la TOE) ou à distance (via l'interface d'administration distante).

Sensibilité : intégrité.

D_param_CA

Les paramètres de contrôle d'accès local et distant à la TOE regroupent les données utilisées pour le contrôle de l'accès à la TOE. Ces données peuvent notamment comprendre :

- Les données d'authentification des utilisateurs (usagers, administrateurs et superviseurs) pour l'accès local à l'interface de la TOE.
- Les données de l'authentification de l'administration et de la supervision centralisées.
- Les données de connexion (adresse de serveur, protocole d'échange des données de sécurité) pour l'administration et la supervision centralisées.
- Le niveau de visibilité de la TOE (accès local impossible ou partiel à l'interface de la TOE).

Ces paramètres sont stockés localement et peuvent être modifiés localement (via l'IHM de la TOE) ou à distance (via l'interface d'administration distante).

Sensibilité : confidentialité, intégrité.

D_audit_flux

La TOE fournit des données de supervision (données de connexion, adresses connectées, informations de connections sur les différents flux) dont l'exploitation peut être partielle, la transmission de ces données pouvant générer un trafic volumineux.

Ces données sont stockées et exploitées localement ou transmises à une entité de supervision.

Sensibilité : confidentialité, intégrité.

D_audit_admin

La TOE journalise des données relatives à son fonctionnement (démarrage, arrêt) et à son administration (modification de règles ou de paramètres).

Ces données sont stockées et exploitées localement ou transmises à une entité de supervision.

Sensibilité : confidentialité, intégrité.

D_alerte

La TOE génère des alertes dont la journalisation locale est systématique, et la transmission au centre de supervision configurable en fonction de leur gravité.

Un mécanisme permet de garantir la transmission de ces alertes en différé, pour permettre leur exploitation cohérente, y compris pour des postes de travail nomades connectés au centre d'administration de façon épisodique.

Sensibilité : intégrité, disponibilité.

Note d'application : les éditeurs de pare-feu personnel qui souhaitent protéger les alertes en confidentialité devront le spécifier dans les ST conformes à ce PP.

2.1.1.3 Tableau de synthèse

Le tableau ci-après résume les besoins de sécurité des différents biens sensibles identifiés :

	Confidentialité	Intégrité	Disponibilité
D_data	X	X	X
D_appli		X	X
D_service			X
D_logiciel		X	X
D_filtre_flux	X	X	
D_filtre_appli	X	X	
D_param_config		X	
D_param_CA	X	X	
D_audit_flux	X	X	
D_audit_admin	X	X	
D_alerte		X	X

Tableau 1 : sensibilité des différents biens

2.2 Utilisateurs

Les utilisateurs personnes physiques et les programmes informatiques qui accèdent à la TOE sont les suivants :

U_prog_local	Les programmes du poste qui interagissent avec la TOE.
U_prog_distant	Les programmes situés sur des systèmes distants qui interagissent avec la TOE au travers du réseau.
U_admin_sécu	Les administrateurs sécurité.
U_superviseur	Les superviseurs sécurité.
U_usager	Les usagers du poste.

U_prog_local

Il s'agit des programmes installés sur le poste hébergeant la TOE qui communiquent avec l'extérieur au travers de la TOE.

U_prog_distant

Il s'agit des programmes situés sur des systèmes distants qui interagissent au travers du réseau soit avec la TOE pour des besoins de supervision ou d'administration, soit avec le poste local au travers de la TOE pour des besoins applicatifs.

U_admin_sécu

L'administrateur sécurité est responsable de la définition et de l'administration au niveau de la TOE des règles de filtrage correspondant à la politique définie par l'agent (ou l'officier) de sécurité[4]. Il utilise pour remplir sa mission un accès local ou distant.

U_superviseur

Le superviseur sécurité contrôle et audite l'application par la TOE de la politique de filtrage définie au niveau des postes de travail au travers des alarmes et des données journalisées par la TOE. Il gère les alarmes remontées par la TOE. Il suit et analyse les événements de sécurité journalisés par la TOE. Il utilise pour remplir sa mission un accès local ou distant.

U_usager

L'usager utilise le poste de travail sur lequel est installée la TOE dans un contexte mono ou multi-utilisateurs. Selon la politique définie et autorisée par l'agent de sécurité, il peut :

- Assurer, seul ou en collaboration avec un administrateur de sécurité, l'administration de la TOE, ou au contraire n'avoir aucun regard sur celle-ci.
- Assurer, seul ou en collaboration avec le superviseur sécurité, la supervision de la TOE ou au contraire n'avoir aucun regard sur celle-ci.

2.3 Menaces

Typologie et origine des menaces

Les menaces peuvent avoir pour origine :

- Un dysfonctionnement de la TOE ou de l'environnement de la TOE (poste, réseau...).
- Un usager du poste hébergeant la TOE qui pourrait par malveillance (utilisation frauduleuse, abus de droits accordés) on par erreur (négligence, inadvertance, ignorance) porter atteinte au bon fonctionnement de la TOE.
- Un administrateur ou superviseur de sécurité qui pourrait par erreur (négligence, inadvertance) porter atteinte au bon fonctionnement de la TOE.
- Des personnes disposant d'un accès au réseau sur lequel est connecté le poste, qui peuvent agir de manière malveillante, abuser de droits qui leurs sont accordés ou commettre des erreurs. Ces personnes pourraient notamment :
    - Tenter d'accéder au poste ou d'en perturber le fonctionnement.
    - Intercepter ou altérer (modifier, supprimer, perturber, détourner) les communications (données d'administration, de supervision, d'alerte) entre ce poste et d'autres équipements.

[4] La notion d'agent (ou d'officier) de sécurité est définie dans la section A.4.2 de ce PP.

Potentiel d'attaque

On considère que les attaquants personnes physiques disposent d'un potentiel d'attaque de niveau **élémentaire** ce qui correspond à des personnes malintentionnées disposant des compétences informatiques d'un utilisateur averti.

Menaces non retenues

Ne sont pas prises en compte pour l'étude des menaces portant sur la TOE en exploitation :

- Les sinistres physiques, les événements naturels, les pertes de services essentiels, les perturbations dues au rayonnement.
- Les menaces que pourraient réaliser volontairement les administrateurs et superviseurs. Ceux-ci sont considérés comme n'étant pas hostiles.

2.3.1 Menaces relatives à la TOE en exploitation

Nota : les chiffres entre parenthèses correspondent à la numérotation utilisée par la méthode [EBIOS].

T_écoute_passive (19)

Un attaquant utilise le réseau sur lequel est connecté le poste hébergeant la TOE pour prendre connaissance de données échangées entre la TOE et un centre d'administration ou de supervision.

Biens concernés : D_filtre_flux, D_filtre_appli, D_param_CA, D_audit_flux, D_alerte.

Le risque lié à cette menace est important. Cette menace est retenue.

T_divulgation (23)

Un attaquant accède à des biens de la TOE sensibles en confidentialité et les utilise pour violer la politique de sécurité mise en oeuvre par la TOE.

Biens concernés : D_param_CA, D_filtre_flux, D_filtre_appli, D_audit_flux.

Le risque lié à cette menace est important. Cette menace est retenue.

T_origine (24)

Un attaquant transmet des informations à la TOE en usurpant l'identité d'un centre d'administration ou de supervision.

Un attaquant transmet des informations à un centre d'administration ou de supervision en usurpant l'identité de la TOE.

Biens concernés : D_data, D_appli, D_service, D_logiciel, D_filtre_flux, D_filtre_appli, D_param_config, D_param_CA, D_audit_flux, D_audit_admin, D_alerte.

Le risque lié à cette menace est important. Cette menace est retenue.

T_piégeage_logiciel (26)

Une personne mal intentionnée et ayant accès au poste modifie le logiciel pour désactiver ou modifier une de ses fonctions.

Biens concernés : D_logiciel, D_services

Le risque lié à cette menace est important mais sa faisabilité requiert un potentiel d'attaque

élevé. Cette menace est néanmoins retenue.

T_saturation (30)

Des attaques répétées et tracées conduisent à une saturation des journaux. Ces attaques peuvent être délibérées ou liées au dysfonctionnement d'un logiciel, être locales ou issues du réseau.

Biens concernés : D_audit_flux, D_audit_admin.

Des attaques répétées conduisent à une saturation d'un service de la TOE. Ces attaques peuvent être délibérées ou liées au dysfonctionnement d'un logiciel, être locales ou issues du réseau.

Biens concernés : D_services

Le risque lié à cette menace est important. Cette menace est retenue.

T_dysfonctionnement_logiciel (31)

Un dysfonctionnement de la TOE l'empêche de réaliser les fonctions de sécurité qu'elle doit assurer vis-à-vis du poste et des utilisateurs (usagers, administrateurs, superviseurs).

Ce dysfonctionnement peut se traduire par un blocage de la TOE empêchant d'accéder aux services offert par le poste.

Biens concernés : D_services.

Ce dysfonctionnement peut aussi se traduire par l'incapacité de la TOE à assurer un contrôle d'accès aux fonctions d'administration et de supervision, un contrôle des flux réseau et applicatifs, auquel cas, il y a potentiellement atteinte en confidentialité, intégrité, disponibilité de l'ensemble des biens sensibles de la TOE et du poste.

Biens concernés : D_data, D_appli, D_service, D_logiciel, D_filtre_flux, D_filtre_appli, D_param_config, D_param_CA, D_audit_flux, D_audit_admin, D_alerte

Le risque lié à cette menace est important. Cette menace est retenue.

T_altération_données (36)

Un attaquant altère (modification, suppression ou insertion) sur le poste hébergeant la TOE des biens sensibles de la TOE ou protégés par la TOE.

Un attaquant altère (modification, suppression ou insertion) des données liées à l'administration ou à la supervision lors de leur échange entre le poste hébergeant la TOE et un site distant.

Cet attaquant pourrait être par exemple un utilisateur local du poste ou une personne accédant à distance aux données mémorisées sur le poste ou échangées entre le poste et un site distant.

Biens concernés : D_data, D_appli, D_service, D_logiciel, D_filtre_flux, D_filtre_appli, D_param_config, D_param_CA, D_audit_flux, D_audit_admin, D_alerte.

Le risque lié à cette menace est important. Cette menace est retenue.

T_traitement_illicite (37)

Un attaquant récupère des données contenant des informations à caractère personnel et les utilise de manière malveillante.

Cet attaquant pourrait être par exemple un usager d'un poste multi-utilisateurs autorisé à

accéder aux journaux.

Cette action pourrait aussi avoir lieu lors du recyclage d'un poste de travail sur lequel le pare-feu est installé.

Biens concernés : D_audit_flux.

Le risque lié à cette menace est important. Cette menace est retenue.

T_erreur_utilisation (38)

Un usager ou un administrateur fait une erreur d'administration (modification de données) et provoque un dysfonctionnement de la TOE ou une altération de la politique de filtrage.

Biens concernés : D_filtre_flux, D_filtre_appli, D_param_config, D_param_CA, D_services.

Le risque lié à cette menace est important. Cette menace est retenue.

T_abus_droit (39)

Un utilisateur désactive volontairement une fonction de la TOE ce qui conduit à une violation de la politique de sécurité.

Biens concernés : D_param_config, D_param_CA.

Le risque lié à cette menace est important. Cette menace est retenue.

T_filtre_désactivation (39, 40)

Un programme malveillant ou un utilisateur pourrait désactiver, éventuellement de manière discrète, les fonctions de filtrage de la TOE et laisser ainsi le poste sans protection vis-à-vis de connexions illicites.

Biens concernés : D_filtre_flux, D_filtre_appli.

Le risque lié à cette menace est important. Cette menace est retenue.

T_usurpation_droit (40)

Une personne non autorisée pourrait accéder à la TOE ou à des fonctions de la TOE auxquelles elle n'a pas normalement accès et les utiliser pour modifier la politique de sécurité.

Exemples : usager accédant aux fonctions réservées à l'administrateur sécurité, personne accédant à une interface d'administration de la TOE laissée sans surveillance.

Un attaquant pourrait prendre connaissance des règles de filtrage de la TOE et disposer ainsi d'éléments lui permettant de violer la politique de sécurité mise en oeuvre par la TOE.

Attaquant : utilisateur du poste, personne accédant à distance aux données mémorisées sur le poste.

Biens concernés : D_filtre_flux, D_filtre_appli, D_param_config, D_param_CA.

Le risque lié à cette menace est important. Cette menace est retenue.

T_reniement_action (41)

Un utilisateur pourrait utiliser ses droits d'administration pour modifier la politique de sécurité appliquée par la TOE ou altérer le fonctionnement de la TOE puis nier avoir fait ces modifications.

Biens concernés : D_filtre_flux, D_filtre_appli.

Le risque lié à cette menace est important. Cette menace est retenue.

2.4 Politiques de sécurité organisationnelles (OSP)

2.4.1 Politiques relatives aux services offerts

OSP_filtrage

La TOE doit mettre en oeuvre un mécanisme de contrôle d'accès réseau basé sur des règles de filtrage. Elle doit permettre de définir plusieurs niveaux de filtrage. Ces règles de filtrage doivent prendre en compte l'environnement réseau du poste, les critères relatifs aux connexions, aux utilisateurs et aux applications. La TOE doit également permettre de faire du filtrage contextuel.

OSP_application_intégrité

La TOE doit permettre de contrôler l'intégrité des applications qui cherchent à réaliser des accès réseau ainsi que de détecter et signaler les applications qui ont été modifiées.

OSP_rôles

La TOE doit distinguer au minimum les rôles d'administrateur sécurité, de superviseur sécurité et d'usager. Elle doit permettre de tracer les actions réalisées par les titulaires de ces rôles.

OSP_admin

La TOE doit permettre d'administrer, localement ou à distance, sa configuration et les règles de filtrage. Toutes les règles de filtrage doivent pouvoir être visualisées. L'accès au module d'administration et l'utilisation des fonctions d'administration doivent être contrôlés.

OSP_supervision

LA TOE doit permettre de superviser, localement ou à distance, son fonctionnement. L'accès au module de supervision et l'utilisation des fonctions de supervision doivent être contrôlés. Seul le superviseur est autorisé à consulter et purger les journaux, aucun utilisateur n'a de droit en modification sur les journaux.

OSP_audit_admin

La TOE doit tracer les actions d'administration conduisant à une modification de la configuration de la TOE. Elle doit permettre de sélectionner, ordonner et visualiser ces données selon différents critères (date, acteur).

OSP_audit_flux

La TOE doit pouvoir tracer les flux qu'elle traite dans le cadre de la politique de sécurité. Elle doit permettre de sélectionner, ordonner et visualiser ces données selon différents critères (horodatage, acteur, adresse réseau, application, protocole, acceptation ou rejet du flux).

OSP_détection_violation

La TOE doit permettre, dans la mesure du possible, de détecter les tentatives de violation de la politique de sécurité et signaler toute tentative par l'émission d'une alarme.

OSP_configuration_sûre

La TOE doit pouvoir être réinstallée et reconfigurée permettant ainsi de disposer sur le poste d'une TOE dans un état sûr.

2.4.2 Politiques relatives à l'appréciation de la qualité de la TOE

OSP_EAL

La TOE doit être évaluée au niveau EAL2 augmenté des composants ADV_TDS.3**, ADV_IMP.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1 et AVA_VAN.3.

2.4.3 Politiques issues de la réglementation applicable

OSP_crypto

Les mécanismes cryptographiques de la TOE doivent être conformes aux exigences du référentiel cryptographique de la DCSSI pour le niveau de robustesse standard [CRYPT-STD].

2.5 Hypothèses

2.5.1 Hypothèses concernant le personnel

A_administrateurs_de_confiance

Les personnels chargés de l'administration ou de la supervision de la TOE et du poste hébergeant la TOE doivent être de confiance. Ils doivent disposer de la formation et des éléments nécessaires pour assurer correctement leur mission.

Personnels concernés[5] : administrateurs système, superviseurs système, administrateurs sécurité, superviseurs sécurité.

A_usager_non_privilégié

Les usagers du poste de travail hébergeant la TOE ne doivent pas avoir de privilège « Administrateur » ou équivalent au niveau de ce poste de travail.

2.5.2 Hypothèses concernant l'environnement TI

A_livraison_sûre

Le conditionnement, le transport et la livraison de la TOE doivent permettre de garantir l'authenticité et l'intégrité des supports d'installation et de la documentation de la TOE.

A_maîtrise_configuration

Les administrateurs de la TOE doivent disposer de moyens permettant de sauvegarder, contrôler par rapport à un état de référence et restaurer une configuration de la TOE.

Note d'application : les contributions de la TOE à cette hypothèse, si elles existent, devront

[5] Les notions d'administrateur système et de superviseur système sont définies dans la section A.4.2 de ce PP.

être mises en évidence dans les ST et PP conformes à ce PP sous la forme d'une OSP couvrant tout ou partie de cette hypothèse.

A_ressources_disponibles

Le poste hébergeant la TOE doit lui fournir les ressources nécessaires à son fonctionnement.

Ressources concernées : place disque, temps CPU, mémoire, bande passante, interface réseau et logiciels associés, IHM, horodatage.

A_poste_sûr

Le poste de travail hébergeant la TOE doit assurer une protection suffisante des éléments constituant la TOE (programmes, fichiers de données, journaux) et des éléments nécessaires à son fonctionnement (horodatage, éléments relatifs aux applications, aux utilisateurs, à la connexion).

A_type_environnement

L'environnement de la TOE doit mettre à la disposition de la TOE des éléments de confiance lui permettant de déterminer si le poste hébergeant la TOE est connecté dans ou hors de l'entreprise.

Note d'application : les contributions de la TOE à cette hypothèse, si elles existent, devront être mises en évidence dans les ST et PP conformes à ce PP sous la forme d'une OSP. La TOE pourrait par exemple déterminer qu'elle est dans l'entreprise par une authentification mutuelle avec un serveur d'authentification de l'entreprise.

A_filtrage_total

Le poste de travail hébergeant la TOE ne doit pas permettre de réaliser des connexions réseau, entrantes ou sortantes, court-circuitant la TOE et la politique de filtrage mise en oeuvre par la TOE.

Note d'application : les contributions de la TOE à cette hypothèse, si elles existent, devront être mises en évidence dans les ST et PP conformes à ce PP sous la forme d'une OSP couvrant tout ou partie de cette hypothèse.

A_poste_utilisateurs

L'environnement de la TOE doit assurer l'identification et l'authentification des utilisateurs (usagers, administrateurs, superviseurs) qui se connectent, localement ou à distance, au poste hébergeant la TOE et doit pouvoir fournir à la TOE les éléments de confiance relatifs à ces utilisateurs (identité, rôle) et nécessaires à son fonctionnement.

2.5.3 Hypothèses concernant l'environnement non TI

A_protection_physique

L'environnement de la TOE doit assurer une protection physique suffisante afin de limiter les risques d'attaque contre l'intégrité de la TOE (matériels et supports de données).

3 Objectifs de sécurité

3.1 Objectifs de sécurité pour le poste auxquels répond la TOE

OT_filtrage_niveaux

La TOE doit permettre de définir au minimum les niveaux de filtrage suivants :

- Un filtrage global appliqué dès le démarrage de la TOE indépendamment de toute connexion utilisateur. Ce filtrage est sous le contrôle de l'administrateur sécurité.
- Un filtrage utilisateur spécifique à un usager (ou à un groupe d'usagers), appliqué que cet usager est connecté. Ce filtrage est sous le contrôle de l'administrateur sécurité qui peut déléguer à cet usager le contrôle de tout ou partie de ce filtrage.
- Un filtrage adapté spécifique à un usager (ou à un groupe d'usagers), généré par un mécanisme d'apprentissage et contrôlé par cet usager. Ce mécanisme de filtrage peut être activé ou non par l'administrateur sécurité.

Le filtrage utilisateur et le filtrage adapté ne doivent pas être en contradiction avec le filtrage global.

OT_filtrage_critères

La TOE doit permettre de définir des règles de filtrage s'appuyant sur une combinaison logique de critères. Ces critères peuvent concerner :

- L'application : identification, lien entre application et protocoles.
- Le flux de communication : protocoles de communication[6], adresses réseau source ou destination, sens (entrant ou sortant), ports source ou destination, adresse MAC…
- L'usager : identité, rôle possédé.
- L'environnement réseau du poste : interface physique utilisée, zone de confiance (connexion dans ou hors de l'entreprise).
- Le contexte de la connexion (notion de filtrage contextuel).

OT_application_intégrité

La TOE doit permettre de contrôler l'intégrité des applications communicantes ainsi que détecter et signaler aux utilisateurs autorisés toute modification de ces applications.

3.2 Objectifs de sécurité pour la TOE

Nota : Le regroupement utilisé a pour seul but de faciliter la lecture des objectifs.

[6] Ce PP ne prend en compte que la pile protocolaire TCP/IP (cf. glossaire en annexe). Les protocoles propriétaires autres qu'IP seront définis par les ST conformes à ce PP.

3.2.1 Objectifs fonctionnels

OT_administration

La TOE doit permettre d'administrer, localement ou à distance, sa configuration et les règles de filtrage. Toute règle de filtrage appliquée par la TOE doit pouvoir être visualisée. L'accès à la fonction d'administration doit être limité à l'administrateur sécurité (U_admin_sécu).

OT_supervision

LA TOE doit permettre de superviser, localement ou à distance, son fonctionnement et les différents événements relatifs à sa sécurité. L'accès à la fonction de supervision doit être limité au superviseur sécurité (U_superviseur).

3.2.2 Identification, authentification, contrôle d'accès

OT_rôles

La TOE doit distinguer au minimum les rôles d'usager, d'administrateur sécurité, de superviseur sécurité.

OT_identification

LA TOE doit disposer d'un mécanisme lui permettant d'identifier de manière unique tout utilisateur des fonctions d'administration ou de supervision.

OT_authentification

La TOE doit authentifier les utilisateurs des fonctions d'administration et de supervision avant toute utilisation de ces fonctions.

OT_contrôle_accès

La TOE doit limiter l'accès aux fonctions d'administration ou de supervision aux seuls utilisateurs autorisés. Le contrôle d'accès doit couvrir : l'accès (consultation, modification, suppression) des paramètres, des règles de filtrage et des journaux, l'arrêt ou la désactivation de la TOE. Il doit être configurable par l'administrateur sécurité et s'appuyer sur les rôles définis au niveau de la TOE.

3.2.3 Sécurité des données de la TOE

OT_données_inaccessibilité

La TOE doit pouvoir rendre inaccessibles ses paramètres (de configuration, de contrôle d'accès) et règles de filtrage en cas de besoin (maintenance, désinstallation du logiciel, réaffectation du poste).

OT_journaux_protection

La TOE doit disposer d'un mécanisme permettant d'assurer la protection en intégrité et en confidentialité des journaux. Ce mécanisme doit permettre de détecter toute altération ou suppression d'un enregistrement d'audit et d'en informer les utilisateurs autorisés (superviseur de sécurité). Ce mécanisme doit aussi permettre de détecter toute atteinte d'un seuil critique de saturation des journaux et d'en informer les utilisateurs autorisés.

3.2.4 Sécurité des échanges d'administration ou de supervision

OT_échange_authentification

La TOE doit identifier et authentifier les sites distants avec lesquels elle communique dans le cadre des opérations d'administration ou de supervision distantes.

OT_échange_intégrité

La TOE doit assurer et contrôler l'intégrité des données qu'elle échange avec des sites distants dans le cadre des opérations d'administration ou de supervision distantes.

OT_échange_confidentialité

La TOE doit assurer la confidentialité des données qu'elle échange avec des sites distants dans le cadre d'opérations d'administration ou de supervision distantes.

OT_échange_rejeu

La TOE doit assurer la protection contre le rejeu des données qu'elle échange avec des sites distants dans le cadre d'opérations d'administration ou de supervision distantes.

3.2.5 Audit et journalisation

OT_audit_flux

La TOE doit pouvoir tracer et enregistrer des éléments relatifs aux flux qu'elle traite dans le cadre de la politique de sécurité. La granularité de ces traces doit être configurable par l'administrateur sécurité.

La TOE doit permettre aux utilisateurs autorisés de visualiser ces traces selon différents critères de sélection et de tri (date, usager, application, protocole, adresse, statut…).

OT_audit_exploitation

La TOE doit pouvoir tracer et enregistrer l'utilisation des fonctions d'administration et de supervision ainsi que les événements relatifs à son fonctionnement (démarrage et arrêt de la TOE, connexion et déconnexion des administrateurs et superviseurs…). La granularité de ces traces doit être configurable par l'administrateur sécurité.

La TOE doit permettre aux utilisateurs autorisés de visualiser ces traces selon différents critères de sélection et de tri (date, acteur, événement, résultat, site). La TOE doit aussi permettre aux utilisateurs autorisés de purger ces traces.

OT_alerte_détection

La TOE doit, dans la mesure du possible, détecter les tentatives d'intrusion ou de violation de la politique de sécurité ainsi que les risques de saturation et les signaler par l'émission d'une alarme à destination des utilisateurs autorisés. Ce mécanisme d'alerte doit être configurable par l'administrateur sécurité.

OT_alerte_réaction

La TOE doit régir elle-même ou permettre aux utilisateurs autorisés de réagir afin d'interdire rapidement tout accès réseau en cas d'alerte puis de revenir à l'état nominal antérieur. Ce mécanisme d'alerte doit être configurable par l'administrateur sécurité. Son usage doit pouvoir être tracé.

3.2.6 Fiabilité et disponibilité de la TOE

OT_intégrité

La TOE doit pouvoir contrôler l'intégrité de ses fonctions de filtrage, d'administration et de journalisation ainsi que de ses données de configuration et, en cas de détection d'une altération, la signaler par une alerte.

Note d'application : les ST et PP conformes à ce PP devront préciser quels sont les éléments (fonctions, données) sur lesquels portent ces contrôles et quels sont les mécanismes de contrôle d'intégrité utilisés.

OT_fonctionnement

La TOE doit permettre aux titulaires de rôles autorisés de connaître son état de fonctionnement.

OT_crypto

Les mécanismes cryptographiques de la TOE doivent être conformes aux exigences du référentiel cryptographique de la DCSSI pour le niveau de robustesse standard [CRYPT-STD].

3.3 Objectifs de sécurité pour l'environnement de développement

OD_EAL

La TOE doit être évaluée au niveau EAL2 augmenté des composants ADV_TDS.3**, ADV_IMP.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1 et AVA_VAN.3.

3.4 Objectifs de sécurité pour l'environnement opérationnel

3.4.1 Objectifs concernant le personnel

OE_administrateurs_de_confiance

Les personnels chargés de l'administration ou de la supervision de la TOE et du poste de travail doivent être de confiance. Ils doivent disposer de la formation et des éléments nécessaires pour assurer correctement leur mission.

OE_usager_non_privilégié

Les usagers du poste de travail hébergeant la TOE ne doivent pas avoir de privilège « Administrateur » ou équivalent au niveau de ce poste de travail.

3.4.2 Objectifs concernant l'environnement TI

OE_livraison_sûre

Le conditionnement, le transport et la livraison de la TOE doivent permettre de garantir l'authenticité et l'intégrité des supports d'installation et de la documentation de la TOE.

OE_maîtrise_configuration

Les administrateurs de la TOE doivent disposer de moyens permettant de sauvegarder la configuration de la TOE, de la contrôler par rapport à un état de référence et de la restaurer.

OE_ressources_disponibles

Le poste hébergeant la TOE doit lui fournir les ressources nécessaires à son fonctionnement : place disque, temps CPU, mémoire, bande passante, interfaces réseau, IHM, horodatage.

Note d'application : les ST et PP conformes à ce PP et les manuels des produits concernés devront fournir des recommandations quant aux dimensionnement des ressources nécessaires pour un fonctionnement correct de la TOE, en particulier au niveau de la place disque afin de limiter les risques de saturation des journaux d'audit de la TOE.

OE_poste_sûr

Le poste de travail hébergeant la TOE doit assurer une protection suffisante des éléments constituant la TOE (programmes, fichiers de données, journaux) ou nécessaires à son fonctionnement (heure, identification des applications et utilisateurs, éléments relatifs à la connexion).

OE_contexte_sûr

L'environnement de la TOE doit mettre à la disposition de la TOE avec un niveau de confiance suffisant les éléments nécessaires à son fonctionnement : informations relatives à la connexion, aux utilisateurs connectés localement, aux programmes locaux demandant à accéder au réseau.

Note d'application : les ST et PP conformes à ce PP pourront compléter cet objectif de sécurité pour l'environnement TI par un objectif de sécurité pour la TOE. En particulier, les manuels d'utilisation de la TOE devront clairement préciser ces éléments.

OE_type_environnement

L'environnement de la TOE doit mettre à la disposition de la TOE des éléments de confiance lui permettant de déterminer si le poste hébergeant la TOE est connecté dans ou hors de l'entreprise.

Note d'application : les ST et PP conformes à ce PP pourront remplacer cet objectif de sécurité pour l'environnement TI par un objectif de sécurité pour la TOE et revoir l'hypothèse associée. En particulier, les manuels d'utilisation de la TOE devront clairement préciser les éléments qui permettront d'identifier ce contexte.

OE_filtrage_total

Le poste de travail hébergeant la TOE ne doit pas permettre de réaliser des connexions réseau, entrantes ou sortantes, court-circuitant la TOE et la politique de filtrage mise en oeuvre par la TOE.

Nota : les ST et PP conformes à ce PP pourront remplacer cet objectif de sécurité pour l'environnement TI par un objectif de sécurité pour la TOE et revoir l'hypothèse associée.

OE_poste_utilisateurs

L'environnement de la TOE doit assurer l'identification et l'authentification des utilisateurs (usagers, administrateurs et superviseurs) qui se connectent, localement ou à distance, au poste hébergeant la TOE et doit pouvoir fournir à la TOE les éléments de confiance relatifs à

ces utilisateurs (identité, rôle) et nécessaires à son fonctionnement.

3.4.3 Objectifs concernant l'environnement non TI

OE_protection_physique

L'environnement de la TOE doit assurer une protection physique suffisante afin de limiter les risques d'attaque contre l'intégrité de la TOE (matériels et supports de données).

4 Exigences de sécurité des TI

4.1 Introduction

La TOE et son environnement peuvent être modélisés par le schéma ci-après. La TSF est un module supplémentaire qui n'est pas représentée sur ce schéma.

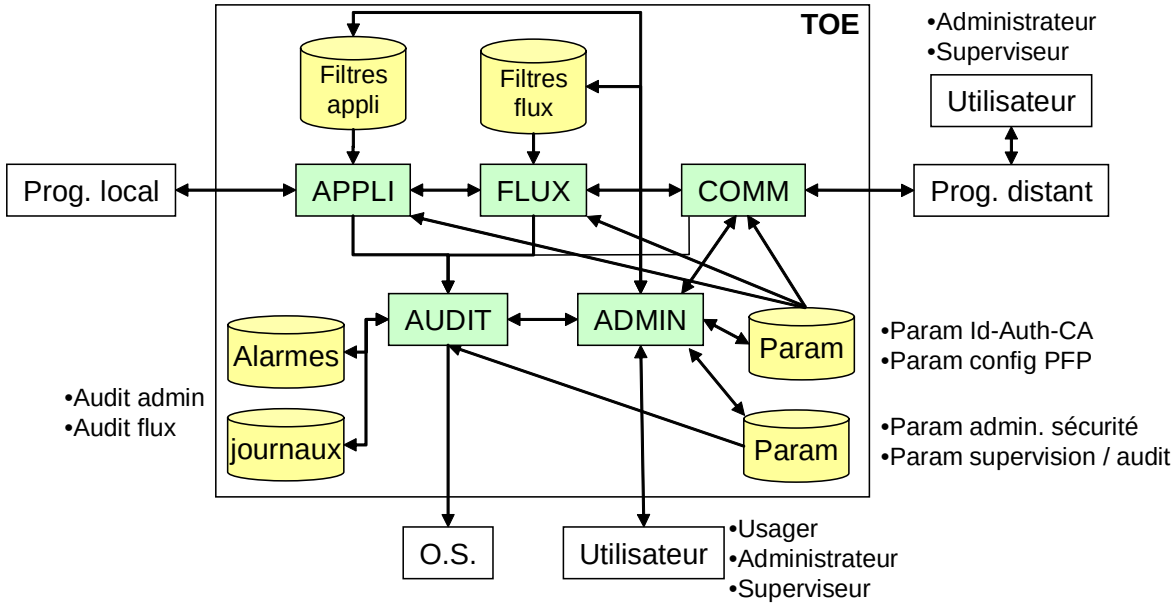

Figure 2 : modélisation de la TOE et de son environnement

Note d'application : Cette modélisation a pour unique objet de décrire le comportement de la TOE sur le plan de la sécurité. Elle n'impose aucune contrainte quant à l'architecture logicielle des produits et à son implémentation (nombre de modules et fonctions, structuration des données...). Les ST et PP conformes à ce PP pourront adapter ce modèle en fonction des produits concernés. Elles devront alors indiquer la correspondance entre les éléments du modèle adapté et ceux du modèle décrit ici.

4.1.1 Sujets

Les différents sujets de la TOE sont :

S_APPLI : Ce sujet met en oeuvre la politique de filtrage applicatif et le contrôle d'intégrité des applications. Il prend en compte le filtrage « adapté » (cf. A.5.1.1). Il peut générer des messages de trace et des alertes.

S_FLUX : Ce sujet met en oeuvre la politique de filtrage réseau. Il peut générer des messages de trace et des alertes.

S_AUDIT : Ce sujet met en oeuvre les fonctions de gestion des journaux d'audit et d'émission des alarmes et messages de trace.

S_ADMIN : Ce sujet met en oeuvre les fonctions d'administration et de supervision de la TOE. Il peut générer des messages de trace et des alertes.

S_COMM : Ce sujet met en oeuvre les fonctions de communication au travers du réseau avec des sites distants. Il peut générer des messages de trace et des alertes.

4.1.2 Objets

Les objets ci-après reprennent les biens sensibles de la TOE décrits dans la section 2.1.1.2 à l'exception de D_logiciel qui correspond à la TOE elle-même :

D_FILTRE_FLUX : règles de filtrage réseau.

D_FILTRE_APPLI : règles de filtrage applicatif et motifs d'intégrité des applications.

D_AUDIT_FLUX : messages de trace en rapport avec la politique de filtrage applicatif et réseau.

D_AUDIT_ADMIN : messages de trace en rapport avec les opérations d'administration, les opérations de supervision, le fonctionnement de la TOE.

D_ALERTE : messages d'alerte.

D_PARAM_CA : paramètres de contrôle d'accès à la TOE.

D_PARAM_CONFIG : paramètres de configuration de la TOE (paramètres liés à l'environnement de la TOE, à la configuration et au contexte réseau…).

Les objets ci-après n'apparaissent pas dans la section2.1.1.2. Ils correspondent à des biens propres à la TOE.

D_FLUX_IN : flux de communication entrants destinés à un programme local (hors TOE).

D_FLUX_OUT : flux de communication sortants émis par un programme local (hors TOE).

D_PARAM_SUPER : paramètres de configuration des fonctions de supervision d'audit et d'alerte (niveau de détail de l'audit, seuils d'alerte…).

D_PARAM_SÉCU : paramètres de configuration de la fonction d'administration sécurité ().

4.1.3 Opérations

Les opérations réalisées par les sujets sur les objets peuvent être regroupées dans les catégories suivantes :

C : cette opération correspond à la création ou à la génération de données (règle de filtrage, alarme, message d'audit, paramètre d'accès pour un usager).

W : cette opération correspond au stockage, à l'écriture, à la modification, à la mise à jour, à l'émission, à l'affichage ou à l'impression de données.

R : cette opération correspond à la lecture ou à la réception de données.

D : cette opération correspond à l'effacement, à la remise à zéro ou à la réinitialisation de données.

B : cette opération correspond à la sauvegarde de paramètres ou de règles de filtrages.

4.1.4 Attributs de sécurité

Attributs relatifs à l'identification et aux droits des usagers :

SA_IDENT : correspond à l'identité d'un sujet ou d'un objet.
Valeurs possibles pour un sujet : S_APPLI, S_FLUX, S_COMM, S_ADMIN, S_AUDIT.
Valeurs possibles pour un objet : D_FLUX_IN, D_FLUX_OUT, D_ALERTE, D_FILTRE_FLUX, D_FILTRE_APPLI, D_AUDIT_FLUX, D_AUDIT_ADMIN, D_PARAM_CONFIG, D_PARAM_CA, D_PARAM_SUPER, D_PARAM_SÉCU, S_APPLI, S_FLUX, S_COMM, S_ADMIN, S_AUDIT.

SA_RÔLE : correspond à un rôle. Valeurs possibles : ADMINISTRATEUR_SÉCURITÉ,

SUPERVISEUR_SÉCURITÉ, USAGER.

SA_USER : associé à un sujet, correspond à l'identité de l'utilisateur lié à ce sujet ; associé à un objet (par exemple un filtre applicatif), correspond à l'identité d'un utilisateur ayant des droits d'accès à cet objet.

SA_DROIT : correspond à un droit possédé par un usager. Valeurs possibles : AUDIT (droit pour cet usager de consulter les messages d'audit et d'alerte).

SA_CONNEXION : correspond à l'origine de la connexion pour un administrateur ou un superviseur. Valeurs possibles : « LOCALE » (connexion sur le poste) ou « DISTANTE » (connexion depuis un site distant).

Attributs relatifs au filtrage ou utilisés pour le filtrage :

SA_RÉSEAU : regroupe les attributs de sécurité relatifs aux paramètres réseau utilisées pour le filtrage : adresse source, adresse destination, port source (ou équivalent), port destination (ou équivalent), protocole, sens (entrant ou sortant), état (de la connexion, utilisé dans le cas du filtrage contextuel), adresse MAC.

Note d'application : les ST et PP conformes à ce PP devront fournir la liste exacte des paramètres réseau utilisés.

SA_ADAPTABILITÉ : permet de définir si un filtre (dont l'attribut SA_NIVEAU a la valeur « SPÉCIFIQUE ») est « PERMANENT » ou « ADAPTÉ » c'est à dire modifiable par l'usager.

SA_ENVIRONNEMENT : correspond à l'environnement réseau du poste. Valeurs possibles : « IN » pour les connexions réalisées dans l'entreprise, « OUT » pour les connexions réalisées depuis des locaux extérieurs à l'entreprise.

SA_MOTIF : correspond au motif d'intégrité calculé pour un programme, une alarme, ou un message d'audit.

SA_NIVEAU : permet de définir si un filtre est « GLOBAL » (i.e. valable pour tous) ou « SPÉCIFIQUE » à un usager.

SA_PROGRAMME : correspond à l'identité d'un programme.

4.1.5 Utilisateurs

Ces utilisateurs, programmes informatiques ou personnes physiques, sont définis dans la section 2.2 de ce document.

Propriétés de sécurité :

Ces utilisateurs disposent de propriétés de sécurité dont héritent les sujets avec lesquels ils établissent des liens :

Utilisateurs	Propriétés de sécurité associées
U_PROG_LOCAL	identité du programme, motif d'intégrité.
U_PROG_DISTANT	identité du programme, rôle.
U_ADMIN_SÉCU	identité de l'utilisateur, rôle, connexion.
U_SUPERVISEUR	identité de l'utilisateur, rôle, connexion.
U_USAGER	identité de l'utilisateur, rôle.

Tableau 2 : propriétés de sécurité des utilisateurs

Binding :

Les liens (*binding*) qu'il est possible d'établir entre les utilisateurs et des sujets sont les

suivants :

	S_ADMIN	S_COMM	S_APPLI	S_FLUX	S_AUDIT
U_PROG_LOCAL			X		
U_PROG_DISTANT		X			
U_ADMIN_SÉCU	X	X			
U_SUPERVISEUR	X	X			
U_USAGER	X				

Tableau 3 : liens utilisateur - sujet

4.1.6 Règles de contrôle d'accès

Les règles de contrôle d'accès par des sujets aux objets (ou à d'autres sujets considérés comme des objets) sont données dans le tableau ci-après.

Note d'application : les ST et PP conformes à ce PP devront préciser la manière dont ces règles de contrôle d'accès sont mises en oeuvre en fonction de la correspondance entre le modèle décrit dans ce PP et son adaptation.

Fonctions permises par la règle de contrôle d'accès	Sujets accédants	Objets accédés	Opérations	Autorisation d'accès si :
Chargement par la TOE des données utilisateurs et paramètres de configuration.	S_ADMIN	D_PARAM_CA D_PARAM_CONFIG D_PARAM_SÉCU D_PARAM_SUPER D_FLITRE_APPLI D_FILTRE_FLUX	R	SA_IDENT (sujet) = S_ADMIN & SA_IDENT (objet) = (D_PARAM_CA ou D_PARAM_SÉCU ou D_FLITRE_APPLI ou D_FILTRE_FLUX ou D_PARAM_SUPER ou D_PARAM_CONFIG)
Chargement par la TOE des paramètres d'audit.	S_AUDIT	D_PARAM_SUPER	R	SA_IDENT (sujet) = S_AUDIT & SA_IDENT (objet) = D_PARAM_SUPER
Chargement par la TOE des données utilisateurs et paramètres de configuration.	S_COMM	D_PARAM_CONFIG D_PARAM_CA	R	SA_IDENT (sujet) = S_COMM & SA_IDENT (objet) = (D_PARAM_CONFIG ou D_PARAM_CA)
Chargement par la TOE des règles de filtrage réseau et des paramètres.	S_FLUX	D_PARAM_CONFIG D_FILTRE_FLUX	R	SA_IDENT (sujet) = S_FLUX & SA_IDENT (objet) = (D_PARAM_CONFIG ou D_FILTRE_FLUX)
Chargement par la TOE des règles de filtrage applicatif et des paramètres.	S_APPLI	D_PARAM_CONFIG D_FILTRE_APPLI	R	SA_IDENT (sujet) = S_APPLI & SA_IDENT (objet) = (D_PARAM_CONFIG ou D_FILTRE_APPLI)
Gestion par l'administrateur sécurité des paramètres de sécurité et des règles de filtrage.	S_ADMIN	D_PARAM_CA D_PARAM_SÉCU D_FLITRE_APPLI D_FILTRE_FLUX	C / W / R / D	SA_IDENT (sujet) = S_ADMIN & SA_RÔLE (sujet) = ADMINISTRATEUR_SÉCURITÉ & SA_IDENT (objet) = (D_PARAM_CA ou D_PARAM_SÉCU ou D_FLITRE_APPLI ou D_FILTRE_FLUX)
Gestion par les usagers autorisés de leurs filtres spécifiques adaptés ou permanents.	S_ADMIN	D_FLITRE_APPLI	C / W / R / D	SA_IDENT (sujet) = S_ADMIN & SA_USER (sujet) = SA_USER (objet) & SA_ROLE (sujet) = USAGER & SA_NIVEAU (objet)= (SPÉCIFIQUE) & SA_ADAPTABILITÉ (objet) = (ADAPTÉ ou PERMANENT) & SA_IDENT (objet) = D_FILTRE_APPLI
Gestion par les superviseurs des paramètres d'audit et de supervision.	S_ADMIN	D_PARAM_SUPER	C / W / R / D	SA_IDENT (sujet) = S_ADMIN & SA_RÔLE (sujet) = SUPERVISEUR_SÉCURITÉ & SA_IDENT (objet) = D_PARAM_SUPER
Émission d'alarmes et de messages d'audit.	S_ADMIN S_COMM S_FLUX S_APPLI	S_AUDIT	W	SA_IDENT (sujet) = (S_ADMIN ou S_COMM ou S_APPLI ou S_FLUX) & SA_IDENT (objet) = S_AUDIT
Enregistrement des alertes et messages d'audit dans les journaux concernés.	S_AUDIT	D_ALERTE D_AUDIT_ADMIN D_AUDIT_FLUX	C	SA_IDENT (sujet) = S_AUDIT & SA_IDENT (objet) = (D_ALERTE ou D_AUDIT_ADMIN ou D_AUDIT_FLUX)

Fonctions permises par la règle de contrôle d'accès	Sujets accédants	Objets accédés	Opérations	Autorisation d'accès si :
Relayage des commandes passées des administrateurs et superviseurs distants.	S_COMM	S_ADMIN	W	SA_IDENT (sujet) = S_COMM & SA_RÔLE (sujet) = (ADMINISTRATEUR SÉCURITÉ ou SUPERVISEUR SÉCURITÉ) & SA_IDENT (objet) = S_ADMIN
Relayage des réponses aux commandes des administrateurs et superviseurs distants.	S_ADMIN	S_COMM	W	SA_IDENT (sujet) = S_ADMIN & SA_RÔLE (sujet) = (ADMINISTRATEUR SÉCURITÉ ou SUPERVISEUR SÉCURITÉ) & SA_IDENT (objet) = S_COMM
Relayage des commandes des superviseurs.	S_ADMIN	S_AUDIT	W	SA_IDENT (sujet) = S_ADMIN & SA_RÔLE (sujet) = SUPERVISEUR SÉCURITÉ & SA_IDENT (objet) = S_AUDIT
Relayage des demandes de lecture des messages d'audit et des alertes par les usagers autorisés.	S_ADMIN	S_AUDIT	W	SA_IDENT (sujet) = S_ADMIN & SA_RÔLE (sujet) = USAGER & SA_DROIT (sujet) = AUDIT & SA_IDENT (objet) = S_AUDIT
Lecture ou effacement des alertes et messages d'audit par les superviseurs sécurité.	S_AUDIT	D_ALERTE D_AUDIT_ADMIN D_AUDIT_FLUX	R / D	SA_IDENT (sujet) = S_AUDIT & SA_RÔLE (sujet) = SUPERVISEUR SÉCURITÉ & SA_IDENT (objet) = (D_ALERTE ou D_AUDIT_ADMIN ou D_AUDIT_FLUX)
Lecture des alertes et messages d'audit pour les usagers autorisés.	S_AUDIT	D_ALERTE D_AUDIT_FLUX	R	SA_IDENT (sujet) = S_AUDIT & SA_RÔLE (sujet) = USAGER & SA_DROIT (sujet) = AUDIT & SA_IDENT (objet) = (D_ALERTE ou D_AUDIT_FLUX)
Relayage des réponses aux commandes des superviseurs et demandes de lecture des messages d'audit et des alertes par les usagers autorisés.	S_AUDIT	S_ADMIN	W	SA_IDENT (sujet) = S_AUDIT & SA_IDENT (objet) = S_ADMIN
Sauvegarde des paramètres de la TOE	S_ADMIN	D_PARAM_CA D_PARAM_CONFIG D_PARAM_SÉCU D_PARAM_SUPER D_FLITRE_APPLI D_FILTRE_FLUX	B	SA_IDENT (sujet) = S_ADMIN & SA_RÔLE (sujet) = ADMINISTRATEUR SÉCURITÉ & SA_IDENT (objet) = (D_PARAM_CA ou D_PARAM_CONFIG ou D_PARAM_SÉCU ou D_PARAM_SUPER ou D_FLITRE_APPLI ou D_FILTRE_FLUX)
Relayage par la TOE des paquets entrants.	S_COMM	S_FLUX	W	SA_IDENT (sujet) = S_COMM & SA_IDENT (objet) = S_FLUX
Mise en oeuvre par la TOE des règles de filtrage réseau pour les paquets entrants ou sortants.	S_FLUX	S_COMM S_APPLI	W	SA_IDENT (sujet) = S_FLUX & SA_IDENT (objet) = (S_COMM ou S_APPLI) & SA_RÉSEAU (objet), SA_ENVIRONNEMENT (objet), SA_NIVEAU (objet), SA_ADAPTABILITÉ (objet) cohérents avec les règles définies dans D_FILTRE_FLUX
Mise en oeuvre par la TOE des règles de filtrage applicatif pour les paquets sortants.	S_APPLI	S_FLUX	W	SA_IDENT (sujet) = S_APPLI & SA_IDENT (objet) = S_FLUX & SA_RÉSEAU (sujet), SA_ENVIRONNEMENT (objet), SA_NIVEAU (objet), SA_ ADAPTABILITÉ (objet), SA_PROGRAMME (objet), SA_MOTIF (objet) cohérents avec les règles définies dans D_FILTRE_APPLI

Tableau 4 : règles de contrôle d'accès

4.2 Définition des composants étendus

Sans objet.

4.3 Exigences de sécurité fonctionnelles pour la TOE

Le regroupement utilisé pour structurer ces exigences s'appuie sur le regroupement utilisé pour les objectifs de sécurité pour la TOE. Il est le suivant :

- *Services rendus par la TOE (i.e. filtrage applicatif et filtrage réseau)*
- *Identification, authentification, accès à la TOE*
- *Sécurité des paramètres de la TOE et des règles de filtrage*
- *Sécurité des échanges d'administration et de supervision depuis un site distant*
- *Audit et sécurité des journaux*
- *Fiabilité de la TOE*
- *Autres exigences*

4.3.1 Services rendus par la TOE (filtrage applicatif et réseau)

Les exigences ci-après contribuent à la mise en oeuvre par la TOE de la politique de filtrage applicatif ou réseau.

FDP_ACC.1 (FRS) Access control (filtrage réseau des connexions sortantes)

Audit *- Refus ou acceptation de la demande d'accès (données associées : identité hérité de l'utilisateur, objet concerné, attributs de sécurité utilisés).*
Dépendances *FDP_ISA.1*

FDP_ACC.1.1 The TSF shall **[selection: allow, disallow]** an operation of a subject on an object **[selection: if, if and only if] [assignment: rules for operations, based on security attributes of the subjects and objects]**.

Raffinement *La TSF doit permettre au module de filtrage réseau (S_FLUX) d'accéder en écriture au module de communication (S_COMM) si et seulement si :*
1. *Les valeurs des attributs de sécurité associés à S_FLUX et hérités du paquet (D_FLUX_OUT) via S_APPLI permettent de sélectionner un ensemble de règles de filtrage dans D_FILTRE_FLUX.*
2. *Il n'existe aucune règle de filtrage sélectionnée interdisant ce flux*
3. *Il existe au moins une règle de filtrage sélectionnée autorisant ce flux.*

Attributs de sécurité utilisés : SA_RÉSEAU, SA_ENVIRONNEMENT, SA_PROGRAMME, SA_USER, SA_IDENT.

FDP_ACC.1 (FRE) Access control (filtrage réseau des connexions entrantes)

Audit *- Refus ou acceptation de la demande d'accès (données associées : identité hérité de l'utilisateur, objet concerné, attributs de sécurité utilisés).*
Dépendances *FDP_ISA.1*

FDP_ACC.1.1 The TSF shall **[selection: allow, disallow]** an operation of a subject on an object **[selection: if, if and only if] [assignment: rules for operations, based on security attributes of the subjects and objects]**.

Raffinement *La TSF doit permettre au module de filtrage réseau (S_FLUX) d'accéder en écriture au module de filtrage applicatif (S_APPLI) si et seulement si :*

1. *Les valeurs des attributs de sécurité associés à S_FLUX et hérités du paquet (D_FLUX_IN) via S_COMM permettent de sélectionner un ensemble de règles de filtrage dans D_FILTRE_FLUX.*
2. *Il n'existe aucune règle de filtrage sélectionnée interdisant ce flux*
3. *Il existe au moins une règle de filtrage sélectionnée autorisant ce flux.*

Attributs de sécurité utilisés : SA_RÉSEAU, SA_ENVIRONNEMENT, SA_IDENT.

FDP_ACC.1 (FAS) Access control (filtrage applicatif des connexions sortantes)

Audit *- Refus ou acceptation de la demande d'accès (données associées : identité hérité de l'utilisateur, objet concerné, attributs de sécurité utilisés).*

Dépendances *FDP_ISA.1*

FDP_ACC.1.1 The TSF shall **[selection: allow, disallow]** an operation of a subject on an object **[selection: if, if and only if] [assignment: rules for operations, based on security attributes of the subjects and objects]**.

Raffinement *La TSF doit permettre au module de filtrage applicatif (S_APPLI) d'accéder en écriture au module de filtrage réseau (S_FLUX) si et seulement si :*

1. *Les valeurs des attributs de sécurité associés à S_APPLI et hérités du paquet (D_FLUX_OUT) et du programme (U_PROG_LOC) permettent de sélectionner un ensemble de règles de filtrage dans D_FILTRE_APPLI.*
2. *Il n'existe aucune règle de filtrage sélectionnée interdisant ce flux*
3. *Il existe au moins une règle de filtrage sélectionnée autorisant ce flux.*

Attributs de sécurité utilisés : SA_PROGRAMME, SA_USER, SA_MOTIF, SA_RÉSEAU (port destination), SA_ENVIRONNEMENT, SA_IDENT.

FIA_TBR.1 (FAS) TSF binding rules (Filtrage applicatif des connexions sortantes)

Audit *- Refus d'établissement d'un lien pour un programme local (données associées : raison du refus, paramètres de sécurité utilisés et règle de sécurité utilisée pour accepter ou refuser l'établissement du lien).*

Dépendances *FIA_USB.1 (PL)*

FIA_TBR.1.1 The TSF shall deny a user binding to **[assignment: subject]** if **[assignment: rules based on one or more of user security properties, location of access, time of access, number of existing bindings of that user, other parameters]**.

Raffinement *La TSF doit interdire à tout programme local (U_PROG_LOCAL) d'établir un lien avec le module de filtrage applicatif (S_APPLI) si au moins une des conditions suivantes est remplie :*

1. *Il existe au moins une règle de filtrage applicatif (D_FILTRE_APPLI) qui, en fonction des propriétés de sécurité de ce programme, lui interdit d'établir un lien.*
2. *Il n'existe aucune règle de filtrage applicatif (D_FILTRE_APPLI) qui, en fonction des propriétés de sécurité de ce programme, l'autorise à établir un lien.*

3. Le motif d'intégrité calculé pour ce programme lors de la demande de connexion diffère du motif d'intégrité mémorisé par la TOE dans D_FILTRE_APPLI.
4. Autres conditions.

Note d'application :
Les ST conformes à ce PP devront préciser : la manière dont est calculer le motif d'intégrité ; les autres conditions retenues.

FCO_ETC.1 (FAE) Export of data and/or security attributes (filtrage applicatif des paquets entrants)

Audit *- Détail de la demande (données associées : règle de filtrage et attributs utilisés pour accepter ou refuser le paquet, statut (acceptation ou refus)).*
Dépendances *aucunes.*

FCO_ETC.1.1 The TSF shall enforce **[assignment: rules on whether export is allowed]** when **[assignment: subject]** exports **[assignment: list of data and/or security attributes]** to a user bound to that subject.

Raffinement *Quand le module de filtrage applicatif (S_APPLI) exporte des données vers un programme applicatif local (U_PROG_LOCAL), la TSF doit s'assurer du respect des règles ci-après :*
1. Les valeurs des attributs associés à S_APPLI et hérités du paquet (D_FLUX_IN) via S_FLUX sont conformes à au moins une règle de filtrage définie dans D_FILTRE_APPLI et autorisant ce flux.

FIA_UID.2 (PL) User identification (programme local)

Audit *- Connexion d'un programme local (données associées : identification du programme, contexte de la connexion).*
Dépendances *FIA_USB.1 (PL)*

FIA_UID.2.1 The TSF shall identify a user before the user can bind to **[assignment: subject]**.

Raffinement *La TSF doit identifier tout programme local (U_PROG_LOCAL) avant que celui-ci puisse établir un lien avec le module de filtrage applicatif (S_APPLI).*

FIA_USB.1 (PL) User-subject binding (programme local)

Audit *- Établissement d'un lien entre un programme local et un sujet (données associées : identification du programme, identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*
Dépendances *aucunes.*

FIA_USB.1.1 Upon binding a user to **[assignment: subject] [selection: the security attributes of the subject shall remain unchanged, the TSF shall change the values of security attributes of that subject as follows: [assignment: rules on how new values security attributes of that subject are determined from the user security properties of the user]]**.

Raffinement *Suite à l'établissement d'un lien entre un programme local (S_PROG_LOCAL) et le module de filtrage applicatif (S_APPLI), les attributs de sécurité de S_APPLI sont mis à jour à partir des propriétés de sécurité de S_PROG_LOCAL de la manière suivante :*

1. *SA_PROGRAMME = identité du programme*
2. *SA_MOTIF = valeur calculée par la TOE pour ce programme*
3. *SA_ENVIRONNEMENT = valeur correspondant à l'environnement réseau du poste (« IN » ou « OUT »). Cette valeur est fournie par le poste.*
4. *SA_USER = identité de l'utilisateur connecté sur le poste. Cette valeur est fournie par le poste.*
5. *SA_RÉSEAU prend les valeurs relatives à la connexion réseau. Ces valeurs sont déterminées par la TOE à partir des informations issues de la connexion réseau demandée.*

Note d'application :

Les ST conformes à ce PP devront préciser la manière dont est calculé le motif d'intégrité.

FIA_TOB.2 (PL) User-initiated termination of binding (programme local)

Audit *- Rupture (à l'initiative de l'utilisateur) d'un lien établi entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet).*

Dépendances *FIA_USB.1 (PL)*

FIA_TOB.2.1 The TSF shall allow a user to terminate a binding to **[assignment: subject]**.

Raffinement *La TSF doit permettre à chaque programme local (U_PROG_LOCAL) de rompre le lien avec le module de filtrage applicatif (S_APPLI).*

FIA_TOB.2.2 The TSF shall **[selection: leave the security attributes of the subject unchanged, terminate the subject, set the security attributes of the subject to [assignment: rules for setting the security attributes of the subject]]**.

Raffinement *La TSF doit soit laisser les attributs de sécurité du sujet inchangés, soit mettre fin au sujet, soit réinitialiser l'ensemble des valeurs pour les attributs de sécurité du module concerné (S_APPLI) de la manière suivante :*

1. *Pas de changement : SA_IDENT, SA_CONTEXTE*
2. *Remise à zéro : SA_PROGRAMME, SA_USER, SA_ENVIRONNEMENT, SA_RÉSEAU*

Note d'application :

Les ST conformes à ce PP devront préciser la solution retenue.

FIA_UID.1 (PD) Anonymous users (programme distant)

Audit *- Connexion d'un programme distant de manière anonyme (données associées : contexte de la connexion).*

Dépendances *FIA_USB.1 (PD)*

FDP_UID.1.1 The TSF shall allow users to bind to **[assignment: subject]** without identifying themselves.

Raffinement *La TSF doit permettre aux programmes distants (U_PROG_DISTANT) d'établir un lien avec le module de communication (S_COMM) sans s'identifier quand ces programmes n'ont pas pour but de communiquer avec le module d'administration et de supervision (S_ADMIN).*

FIA_USB.1 (PD) User-subject binding (programme distant)

Audit *- Établissement d'un lien entre un programme distant et un sujet (données associées : identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*

Dépendances *aucunes.*

FIA_USB.1.1 Upon binding a user to **[assignment: subject] [selection: the security attributes of the subject shall remain unchanged, the TSF shall change the values of security attributes of that subject as follows: [assignment: rules on how new values security attributes of that subject are determined from the user security properties of the user]]**.

Raffinement *Suite à l'établissement d'un lien entre un programme distant (S_PROG_DISTANT) et le module de communication (S_COMM), les attributs de sécurité de S_COMM sont mis à jour à partir de la manière suivante :*

1. *SA_ENVIRONNEMENT = valeur correspondant à l'environnement réseau du poste (« IN » ou « OUT »). Cette valeur est fournie par le poste.*
2. *SA_RÉSEAU prend les valeurs relatives à la connexion réseau. Ces valeurs sont déterminées par la TOE à partir des informations issues de la connexion réseau demandée.*

FIA_TOB.2 (PD) User-initiated termination of binding (programme distant)

Audit *- Rupture à l'initiative d'un programme distant d'un lien établi entre ce programme et un sujet (données associées : identification du sujet, caractéristiques de la connexion réseau).*

Dépendances *FIA_USB.1 (PD)*

FIA_TOB.2.1 The TSF shall allow a user to terminate a binding to **[assignment: subject]**.

Raffinement *La TSF doit permettre à un programme distant (U_PROG_DISTANT) de rompre le lien avec le module de communication (S_COMM).*

FIA_TOB.2.2 The TSF shall **[selection: leave the security attributes of the subject unchanged, terminate the subject, set the security attributes of the subject to [assignment: rules for setting the security attributes of the subject]]**.

Raffinement *La TSF doit soit laisser les attributs de sécurité du sujet inchangés, soit mettre fin au sujet, soit réinitialiser l'ensemble des valeurs pour les attributs de sécurité du module concerné (S_COMM) de la manière suivante :*

1. *Pas de changement : SA_IDENT, SA_CONTEXTE*
2. *Remise à zéro : SA_PROGRAMME, SA_USER, SA_ENVIRONNEMENT, SA_RÉSEAU*

Note d'application :

Les ST conformes à ce PP devront préciser la solution retenue.

4.3.2 Identification, authentification, accès à la TOE

Les exigences ci-après contribuent à la définition des utilisateurs, à la génération des données d'authentification ainsi qu'aux règles relatives à l'établissement ou la terminaison de sessions par les utilisateurs locaux ou distants.

FIA_URE.2 User registration with storage of authentication data

Audit *- Enregistrement d'un nouvel utilisateur.*
- Accès (réussi ou non, en lecture, écriture ou modification) aux propriétés de l'utilisateur.

Dépendances *FDP_ACC.1 (FI)*

FIA_URE.2.1 The TSF shall be able to register new users.

Raffinement *La TSF doit être capable d'enregistrer les nouveaux utilisateurs.*

FIA_URE.2.2 The TSF shall **[selection: obtain values for [assignment: user security properties] from the registering user, provide values for [assignment: user security properties] as follows: [assignment: rules for deriving security properties for the registering user]]**.

Raffinement *La TSF doit obtenir de l'administrateur sécurité qui effectue l'enregistrement des valeurs pour les propriétés de sécurité suivantes :*
1. l'identité de l'utilisateur.
2. le ou les rôles possédés par l'utilisateur.
Rôles possibles : ADMINISTRATEUR_SÉCURITÉ, SUPERVISEUR_SÉCURITÉ, USAGER.

FIA_URE.2.3 The TSF shall store these user security properties in **[assignment: object]**.

Raffinement *La TSF doit stocker l'ensemble des propriétés de sécurité relatives à l'utilisateur dans D_PARAM_CA.*

FIA_URE.2.4 The TSF shall **[selection: receive authentication data from the registering user, provide authentication data to the registering user, [assignment: other method to establish authentication data between the registering user and the TSF]]**.

Raffinement *La TSF doit :*
1. soit recevoir les données d'authentification de l'administrateur sécurité qui fait l'enregistrement.
2. soit s'appuyer sur une méthode spécifique de génération de données d'authentification.

Note d'application :
Les ST conformes à ce PP doivent préciser la méthode utilisée. Dans le cas d'une méthode spécifique, celle-ci doit être décrite.

FIA_URE.2.5 The TSF shall store this authentication data in **[assignment: object]**.

Raffinement *La TSF doit stocker les données d'authentification de l'utilisateur dans D_PARAM_CA.*

FIA_QAD.1 Verification of quality of authentication data

Audit *- Acceptation ou refus des données d'authentification fournies.*
Dépendances *FIA_URE.2 et*
FIA_USB.1 (UL) ou FIA_USB.1 (UD)

FIA_QAD.1.1 The TSF shall ensure that authentication data needed to bind to **[assignment: subject]** meets **[assignment: quality metric]**.

Raffinement *Lorsque les données d'authentification sont choisies par l'administrateur sécurité, la TSF doit s'assurer que les données d'authentification nécessaires à l'établissement d'un lien avec le module d'administration et de supervision (S_ADMIN) ou avec le module de communication (S_COMM) comportent :*
1. *un nombre minimum de caractères*
2. *différents types de caractères (lettres majuscules et minuscules, chiffres et caractères non alphanumériques).*

Note d'application :
Les ST conformes à ce PP devront préciser le nombre minimum de caractères et les conditions relatives au choix de ces caractères.
Les ST conformes à ce PP devront en outre indiquer s'il y a lieu les mécanismes cryptographiques utilisés pour protéger ces données d'authentification.

FIA_QAD.2 TSF generation of authentication data

Audit *- Génération de données d'authentification.*
Dépendances *FIA_URE.2 et*
FIA_USB.1 (UL) ou FIA_USB.1 (UD)

FIA_QAD.2.1 The TSF shall be able to generate authentication data that meets **[assignment: quality metric]**.

Raffinement *Si elle génère elle-même les données d'authentification, la TSF doit être capable de générer des données d'authentification aléatoires qui comportent un nombre minimum de caractères mélangeant lettres majuscules et minuscules, chiffres et caractères non alphanumériques.*

Note d'application :
Les ST conformes à ce PP devront préciser le nombre minimum de caractères, la méthode utilisée pour la génération des aléas.
Les ST conformes à ce PP devront en outre indiquer s'il y a lieu les mécanismes cryptographiques utilisés pour protéger ces données d'authentification.

FIA_QAD.2.2 The TSF shall enforce the use of this authentication data for authentication related to binding to **[assignment: subject]**.

Raffinement *Si elle génère elle-même les données d'authentification, la TSF doit garantir l'utilisation de ces données d'authentification pour établir le lien avec le*

module d'administration et de supervision (S_ADMIN) ou le module de communication (S_COMM).

FIA_UID.2 (UL) User identification (utilisateur local)

Audit *- Connexion d'un utilisateur local (données associées : identité de l'utilisateur, contexte de la connexion).*
Dépendances *FIA_USB.1 (UL)*

FIA_UID.2.1 The TSF shall identify a user before the user can bind to **[assignment: subject]**.

Raffinement *La TSF doit identifier tout utilisateur local avant que celui-ci puisse établir un lien avec le module d'administration et de supervision (S_ADMIN).*
Utilisateurs concernés : U_ADMIN_SÉCU, U_SUPERVISEUR, U_USAGER.

FIA_UID.2 (UD) User identification (utilisateur distant)

Audit *- Connexion d'un utilisateur distant (données associées : identité de l'utilisateur, contexte de la connexion).*
Dépendances *FIA_USB.1 (UD)*

FIA_UID.2.1 The TSF shall identify a user before the user can bind to **[assignment: subject]**.

Raffinement *La TSF doit identifier tout utilisateur distant avant que celui-ci puisse établir un lien avec le module de communication (S_COMM).*
Utilisateurs concernés : U_ADMIN_SÉCU, U_SUPERVISEUR.

FIA_UAU.1 (UL) User authentication by TSF (utilisateur local)

Audit *- Tentative (réussie ou non) d'authentification d'un utilisateur local.*
Dépendances *FIA_UID.2 (UL) et FIA_URE.2*

FIA_UAU.1.1 The TSF shall authenticate a user before the user can bind to **[assignment: subject]**.

Raffinement *La TSF doit authentifier tout utilisateur qui se connecte localement avant que celui-ci puisse établir un lien avec le module d'administration et de supervision (S_ADMIN).*
Utilisateurs concernés : U_ADMIN_SÉCU, U_SUPERVISEUR, U_USAGER.

FIA_UAU.1 (UD) User authentication by TSF (utilisateur distant)

Audit *- Tentative (réussie ou non) d'authentification d'un utilisateur distant.*
Dépendances *FIA_UID.2 (UD) et FIA_URE.2*

FIA_UAU.1.1 The TSF shall authenticate a user before the user can bind to **[assignment: subject]**.

Raffinement *La TSF doit authentifier tout utilisateur qui se connecte depuis un site distant avant que celui-ci puisse établir un lien avec le module de communication (S_COMM).*
Utilisateurs concernés : U_ADMIN_SÉCU, U_SUPERVISEUR.

FIA_UAU.6 Limited authentication feedback

Audit *- Pas de messages d'audit pour ce composant.*
Dépendances *FIA_UAU.1 (UL) ou FIA_UAU.1 (UD)*

FIA_UAU.6.1 The TSF shall provide only **[assignment: list of feedback]** to the user while the authentication is in progress.

Raffinement *A l'exception d'une possible information indiquant la frappe de caractères, la TSF ne doit fournir aucune information à l'utilisateur tant que celui-ci n'est pas complètement authentifié.*
Utilisateurs concernés : U_ADMIN_SÉCU, U_SUPERVISEUR, U_USAGER.
Note d'application :
Les ST conformes à ce PP devront préciser si une information (par exemple des « étoiles ») est transmise en retour à l'utilisateur ou non et si celle-ci permet ou non de compter les caractères saisis par l'utilisateur.

FIA_AFL.1 Authentication failure handling

Audit *- Atteinte ou dépassement d'un des seuils d'alerte lors de la connexion (données associées : seuil, nombre de tentatives).*
- Actions prises (émission d'une alerte, blocage de la connexion...).
Dépendances *FIA_UAU.1 (UL) et FIA_UAU.1 (UD)*

FIA_AFL.1.1 The TSF shall detect when **[assignment: positive integer]** unsuccessful authentication attempts occur related to **[selection: the same user, the same subject, [assignment: other common property of the unsuccessful authentication attempts]]**.

Raffinement *La TSF doit détecter les tentatives d'authentification infructueuses en rapport avec les conditions suivantes :*
1. *N1 (ou plus) tentatives erronées de connexion au module d'administration et de supervision (S_ADMIN) sous la même identité ou des identités différentes en moins de N2 minutes.*
2. *N3 (ou plus) tentatives erronées de connexion au module de communication (S_COMM) en moins de N4 minutes, quelle que soit l'identité utilisée.*

Note d'application :
Les ST conformes à ce PP devront préciser les valeurs choisies pour N1, N2, N3 et N4.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment: list of actions]**.

Raffinement *Lorsque les conditions précisées dans le point 1 ou 2 de l'exigence FIA_AFL.1.1 sont remplies, la TSF doit :*

1. *Émettre une alerte.*
2. *Prendre les actions définies par l'administrateur sécurité.*

Note d'application :

Les ST conformes à ce PP préciseront les actions que peut définir l'administrateur sécurité en réponse à un dépassement de seuil d'authentification.

FIA_TBR.1 (UL) TSF binding rules (utilisateur local)

Audit *- Refus d'établissement d'un lien entre un utilisateur et un sujet (données associées : raison du refus, paramètres de sécurité utilisés pour accepter ou refuser l'établissement du lien).*

Dépendances *FIA_USB.1 (UL)*

FIA_TBR.1.1 The TSF shall deny a user binding to **[assignment: subject]** if **[assignment: rules based on one or more of user security properties, location of access, time of access, number of existing bindings of that user, other parameters]**.

Raffinement *La TSF doit interdire à tout utilisateur local d'établir un lien avec le module d'administration et de supervision (S_ADMIN) si au moins une des conditions suivantes est remplie :*

1. *la valeur de l'attribut SA_USER (sujet) est égal à la valeur de identité fournie par l'utilisateur (i.e. un utilisateur est déjà connecté sous la même identité).*
2. *Autres conditions.*

Utilisateurs concernés : U_ADMIN_SÉCU, U_SUPERVISEUR, U_USAGER.

Note d'application :

Les ST conformes à ce PP devront préciser les autres conditions retenues.

FIA_TBR.1 (UD) TSF binding rules (utilisateur distant)

Audit *- Refus d'établissement d'un lien entre un utilisateur et un sujet (données associées : raison du refus, paramètres de sécurité utilisés pour accepter ou refuser l'établissement du lien).*

Dépendances *FIA_USB.1 (UD)*

FIA_TBR.1.1 The TSF shall deny a user binding to **[assignment: subject]** if **[assignment: rules based on one or more of user security properties, location of access, time of access, number of existing bindings of that user, other parameters]**.

Raffinement *La TSF doit interdire à tout utilisateur distant d'établir un lien avec le module de communication (S_COMM) si au moins une des conditions suivantes est remplie :*

1. *la valeur de l'attribut SA_USER (sujet) est égal à la valeur de la propriété identité de l'utilisateur (i.e. un utilisateur est déjà connecté sous la même identité).*
2. *L'attribut SA_ENVIRONNEMENT du sujet a pour valeur « OUT » (i.e. la connexion vient d'un site extérieur à l'entreprise).*
3. *Autres conditions.*

Utilisateurs : U_ADMIN_SÉCU, U_SUPERVISEUR.

Note d'application :

Les ST conformes à ce PP devront préciser les autres conditions retenues.

FIA_USB.1 (UL) User-subject binding (utilisateur local)

Audit *- Établissement d'un lien entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*

Dépendances *aucunes.*

FIA_USB.1.1 Upon binding a user to **[assignment: subject] [selection: the security attributes of the subject shall remain unchanged, the TSF shall change the values of security attributes of that subject as follows: [assignment: rules on how new values security attributes of that subject are determined from the user security properties of the user]]**.

Raffinement *Suite à l'établissement d'un lien entre un utilisateur connecté localement et le module d'administration et de supervision (S_ADMIN), les attributs de sécurité de S_ADMIN sont mis à jour à partir des propriétés de sécurité de l'utilisateur de la manière suivante :*

1. *SA_USER = identité de l'utilisateur (valeur issue de D_PARAM_CA)*
2. *SA_RÔLE = rôle possédé par l'utilisateur (valeur issue de D_PARAM_CA)*
3. *SA_CONNEXION = « LOCALE »*

Utilisateurs concernés : U_USAGER, U_SUPERVISEUR, U_ADMIN_SÉCU.

Note d'application :

Les ST conformes à ce PP devront préciser les conditions retenues.

FIA_USB.1 (UD) User-subject binding (utilisateur distant)

Audit *- Établissement d'un lien entre un utilisateur distant et un sujet (données associées : identification de l'utilisateur, identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*

Dépendances *aucunes.*

FIA_USB.1.1 Upon binding a user to **[assignment: subject] [selection: the security attributes of the subject shall remain unchanged, the TSF shall change the values of security attributes of that subject as follows: [assignment: rules on how new values security attributes of that subject are determined from the user security properties of the user]]**.

Raffinement *Suite à l'établissement d'un lien entre un utilisateur distant et le module de communication (S_COMM), les attributs de sécurité de S_COMM sont mis à jour à partir des propriétés de sécurité de l'utilisateur de la manière suivante :*

1. *SA_USER = identité de l'utilisateur (valeur issue de D_PARAM_CA)*
2. *SA_RÔLE = rôle possédé par l'utilisateur (valeur issue de D_PARAM_CA)*
3. *SA_CONNEXION = « DISTANTE »*

Utilisateurs concernés : U_SUPERVISEUR, U_ADMIN_SÉCU.

Les valeurs de ces attributs de sécurité sont transmises par S_COMM à S_ADMIN lors de toute demande d'action de la part de l'utilisateur connecté.

Note d'application :

Les ST conformes à ce PP devront préciser les conditions retenues.

FIA_TOB.1 (UD) TSF-initiated termination of binding (utilisateur distant)

Audit *- Rupture (à l'initiative de la TSF) du lien établi entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet, raison de la rupture).*

Dépendances *FIA_USB.1 (UD)*

FIA_TOB.1.1 The TSF shall terminate a binding to **[assignment: subject]** after **[selection: completion of [assignment: operation], [assignment: time interval of user inactivity], [assignment: other condition]]**.

Raffinement *La TSF doit mettre fin au lien établi entre l'utilisateur et le module de communication (S_COMM) dans les conditions suivantes :*

1. *Rupture de la connexion réseau entre le site distant et la TOE.*
2. *Arrêt de la TOE.*
3. *Suppression de l'utilisateur dans D_PARAMS_CA.*
4. *Rupture du canal sûr (suite à détection d'anomalie sur ce canal, par exemple) établi entre la TOE et le programme distant et utilisé par ce lien.*
5. *Autres conditions.*

Utilisateurs concernés : U_ADMIN_SÉCU, U_SUPERVISEUR.

Note d'application :

Les ST conformes à ce PP devront préciser les conditions pouvant conduire à une rupture du lien par la TSF.

FIA_TOB.1.2 The TSF shall **[selection: leave the security attributes of the subject unchanged, terminate the subject, set the security attributes of the subject to [assignment: rules for setting the security attributes of the subject]]**.

Raffinement *La TSF doit soit laisser les attributs de sécurité du sujet inchangés, soit mettre fin au sujet, soit réinitialiser l'ensemble des valeurs des attributs de sécurité du module concerné (S_COMM) de la manière suivante :*

1. *Pas de changement : SA_IDENT, SA_CONTEXTE*
2. *Remise à zéro : SA_PROGRAMME, SA_USER, SA_ENVIRONNEMENT, SA_RÉSEAU*

Note d'application :

Les ST conformes à ce PP devront préciser la solution retenue.

FIA_TOB.2 (UL) User-initiated termination of binding (utilisateur local)

Audit *- Rupture (à l'initiative de l'utilisateur) d'un lien établi entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet).*

Dépendances *FIA_USB.1 (UL)*

FIA_TOB.2.1 The TSF shall allow a user to terminate a binding to **[assignment: subject]**.

Raffinement *La TSF doit permettre à chaque utilisateur de rompre le lien avec le module d'administration (S_ADMIN).*
Utilisateurs concernés : U_ADMIN_SÉCU, U_SUPERVISEUR, U_USAGER.

FIA_TOB.2.2 The TSF shall **[selection: leave the security attributes of the subject unchanged, terminate the subject, set the security attributes of the subject to [assignment: rules for setting the security attributes of the subject]]**.

Raffinement *La TSF doit soit laisser les attributs de sécurité du sujet inchangés, soit mettre fin au sujet, soit réinitialiser l'ensemble des valeurs pour les attributs de sécurité du module concerné (S_ADMIN) de la manière suivante :*
1. *Pas de changement : SA_IDENT, SA_CONTEXTE*
2. *Remise à zéro : SA_PROGRAMME, SA_USER, SA_ENVIRONNEMENT, SA_RÉSEAU*

Note d'application :
Les ST conformes à ce PP devront préciser la solution retenue.

FIA_TOB.2 (UD) User-initiated termination of binding (utilisateur distant)

Audit *- Rupture à l'initiative d'un utilisateur distant d'un lien établi entre cet utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet).*
Dépendances *FIA_USB.1 (UD)*

FIA_TOB.2.1 The TSF shall allow a user to terminate a binding to **[assignment: subject]**.

Raffinement *La TSF doit permettre à chaque utilisateur de rompre le lien avec le module de communication (S_COMM).*
Utilisateurs concernés : U_ADMIN_SÉCU, U_SUPERVISEUR

FIA_TOB.2.2 The TSF shall **[selection: leave the security attributes of the subject unchanged, terminate the subject, set the security attributes of the subject to [assignment: rules for setting the security attributes of the subject]]**.

Raffinement *La TSF doit soit laisser les attributs de sécurité du sujet inchangés, soit mettre fin au sujet, soit réinitialiser l'ensemble des valeurs pour les attributs de sécurité du module concerné (S_COMM) de la manière suivante :*
3. *Pas de changement : SA_IDENT, SA_CONTEXTE*
4. *Remise à zéro : SA_PROGRAMME, SA_USER, SA_ENVIRONNEMENT, SA_RÉSEAU*

Note d'application :
Les ST conformes à ce PP devront préciser la solution retenue.

4.3.3 Sécurité des données de la TOE

Les exigences ci-après contribuent à la protection des données de la TOE.

FDP_ACC.1 (FI) Access control (contrôle d'accès interne à la TOE)

Audit *- Refus ou acceptation de la demande d'accès (données associées : identité héritée de l'utilisateur, objet concerné, attributs de sécurité utilisés).*
- Sauvegarde (données associées : résultat de l'opération, type de données sauvegardées).

Dépendances *FDP_ISA.1*

FDP_ACC.1.1 The TSF shall **[selection: allow, disallow]** an operation of a subject on an object **[selection: if, if and only if] [assignment: rules for operations, based on security attributes of the subjects and objects]**.

Raffinement *La TSF doit permettre une opération demandée par un sujet vis-à-vis d'un objet si et seulement si les attributs de sécurité associés à ce sujet et à cet objet respectent au moins une des règles d'autorisation définies dans le Tableau 4 : règles de contrôle d'accès.*

Note d'application :
Les ST conformes à ce PP devront compléter ce tableau.

FDP_ISA.1 Security attribute initialisation

Audit *- Création d'un objet ou d'un sujet (données associées : identité du sujet ou de l'objet + liste des attributs de sécurité).*

Dépendances *FDP_ACC.1 (FI) + FDP_ACC.1 (FAS) + FDP_ACC.1 (FRS) + FDP_ACC.1 (FRE)*

FDP_ISA.1.1 The TSF shall **[selection: use the following rules [assignment: rules] to assign an initial value, assign the value [assignment: value]]** to the security attribute **[assignment: security attribute]** whenever a **[assignment: object or subject]** is created.

Raffinement *La TSF doit utiliser les règles énoncées ci-après pour définir les attributs de sécurité lors de la création d'un objet ou d'un sujet :*

1. *Création d'un objet D_FILTRE_APPLI ou D_FILTRE_FLUX :*
    a. *lorsque l'attribut SA_RÔLE du sujet (S_ADMIN) est différent de « ADMINISTRATEUR SÉCURITÉ », l'attribut SA_NIVEAU prend pour valeur l'identité de l'utilisateur, l'attribut SA_ADAPTABILITÉ prend pour valeur « ADAPTÉ ».*
    b. *lorsque l'attribut SA_RÔLE du sujet (S_ADMIN) est « ADMINISTRATEUR SÉCURITÉ », l'attribut SA_NIVEAU prend pour valeur « GLOBAL ».*
    c. *Pour D_FILTRE_APPLI, l'attribut SA_MOTIF prend la valeur calculée par la TOE pour ce programme.*
2. *Création d'un objet D_AUDIT_FLUX ou D_AUDIT_ADMIN : l'attribut SA_MOTIF prend la valeur calculée par la TOE. Cet attribut permet de contrôler l'intégrité de l'objet et le chaînage de ce message avec les objets précédents de même type (i.e. D_AUDIT_FLUX ou D_AUDIT_ADMIN).*

Note d'application :
Les ST conformes à ce PP devront fournir la liste des autres règles mises en oeuvre pour l'initialisation des attributs de sécurité lors de la création de sujets ou d'objets.

Les ST conformes à ce PP devront préciser le mode de calcul du motif d'intégrité du programme et sur quel périmètre porte ce motif d'intégrité.
Les ST conformes à ce PP devront préciser le mode de calcul du motif d'intégrité correspondant à un objet D_AUDIT_FLUX ou D_AUDIT_ADMIN et sur quel périmètre porte ce motif d'intégrité.

FDP_MSA.1 Management of security attributes

Audit *- Toute demande (acceptées ou refusée) d'accès à un attribut de sécurité (données associées : identité du sujet, identité de l'utilisateur, objet, attribut, valeur, type d'accès demandé, statut ou résultat de la demande).*
Dépendances *FDP_ACC.1 (FI) + FDP_ACC.1 (FAS) + FDP_ACC.1 (FRS) + FDP_ACC.1 (FRE)*

FDP_MSA.1.1 The TSF determine if a subject is allowed to **[selection: query, modify, delete, [assignment: other types of access], [assignment: security attribute]]** or not, as follows: **[assignment: rules, based on the security attribute being accessed and the security attributes of the subject]**.

Raffinement *La TSF détermine si un sujet est autorisé ou n'est pas autorisé à réaliser des accès aux attributs de sécurité d'un objet en fonction des règles définies ci-après.*
D_FILTRE_APPLI, D_FILTRE_FLUX :
Pour pouvoir lire ou modifier les attributs de sécurité de ces objets, l'attribut SA_NIVEAU de l'objet doit avoir la valeur « SPÉCIFIQUE », l'attribut SA_USER du sujet et de l'objet doivent être égaux, l'attribut SA_ADAPTABILITÉ doit avoir la valeur « ADAPTÉ ».
D_PARAM_CA, D_PARAM_CONFIG :
Les attributs de sécurité de ces objets ne sont pas modifiables.
D_PARAM_SÉCU, D_PARAM_SUPER :
Les attributs de sécurité de ces objets ne sont pas modifiables.
D_AUDIT_FLUX, D_AUDIT_ADMIN, D_ALERTE :
Les attributs de sécurité de ces objets ne sont pas modifiables.
D_FLUX_IN, D_FLUX_OUT :
Pour pouvoir lire ou modifier les attributs de sécurité de ces objets, l'attribut de sécurité SA_IDENT du sujet doit avoir pour valeur « S_APPLI » ou « S_FLUX ».
Note d'application :
Les ST conformes à ce PP devront préciser ou compléter ces règles.

FPT_RIP.2 Removal after use

Audit *- Résultat de l'opération d'effacement demandée.*
Dépendances *aucunes.*

FPT_RIP.2.1 The TSF shall ensure that if **[assignment: list of operations]** are performed on **[assignment: list of objects]** the information in those objects is irretrievably removed.

Raffinement *La TSF doit garantir que toutes les informations contenues dans les objets suivants :*

D_FILTRE_APPLI, D_FILTRE_FLUX, D_PARAM_CA, D_AUDIT_FLUX
Sont rendues indisponibles lors des opérations suivantes :
1. *Désinstallation de la TOE.*
2. *Effacement ou suppression de ces objets.*

4.3.4 Sécurité des échanges d'administration ou de supervision

Les exigences ci-après contribuent à l'établissement d'un canal sûr entre la TOE et un site distant d'administration ou de supervision.

FIA_UID.2 (CS) User identification (canal sûr)

Audit *- Connexion d'un programme distant (données associées : identification du programme, contexte de la connexion).*
Dépendances *FIA_USB.1 (CS)*

FIA_UID.2.1 The TSF shall identify a user before the user can bind to **[assignment: subject]**.

Raffinement *La TSF doit identifier tout programme distant (U_PROG_DISTANT) qui veut communiquer avec le module d'administration et de supervision (S_ADMIN) avant que celui-ci puisse établir un lien avec le module de communication (S_COMM).*

FIA_UAU.1 (CS) User authentication by TSF (authentification mutuelle)

Audit *- Tentative (réussie ou non) d'authentification d'un programme distant.*
Dépendances *FIA_UID.2 (CS) et FIA_URE.2*

FIA_UAU.1.1 The TSF shall authenticate a user before the user can bind to **[assignment: subject]**.

Raffinement *La TSF doit authentifier tout programme distant (U_PROG_DISTANT) qui se connecte dans un but d'administration ou de supervision avant que celui-ci puisse établir un lien avec le module de communication (S_COMM).*

FIA_SUA.1 TSF authentication (authentification mutuelle)

Audit *- Authentification de la TOE auprès d'un programme distant (données associées : réussite ou échec de l'opération, identité du programme distant).*
Dépendances *FIA_USB.1 (CS)*

FIA_SUA.1.1 **[selection: Before, As, After]** a user binds to **[assignment: subject]** the **[selection: subject, TSF]** shall authenticate itself to that user.

Raffinement *Avant d'établir un lien entre le module de communication (S_COMM) et un programme distant (U_PROG_DISTANT) dans un but d'administration ou de supervision, la TOE doit s'authentifier auprès de ce programme.*
Note d'application :

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

FIA_USB.1 (CS) User-subject binding (canal sûr)

Audit *- Établissement d'un lien entre un programme distant et un sujet (données associées : identification du programme, identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*

Dépendances *aucunes.*

FIA_USB.1.1 Upon binding a user to **[assignment: subject] [selection: the security attributes of the subject shall remain unchanged, the TSF shall change the values of security attributes of that subject as follows: [assignment: rules on how new values security attributes of that subject are determined from the user security properties of the user]]**.

Raffinement *Suite à l'établissement d'un lien entre un programme distant (U_PROG_DISTANT) et le module de communication (S_COMM), les attributs de sécurité de S_COMM sont mis à jour à partir des propriétés de sécurité de S_PROG_DISTANT de la manière suivante :*

3. *SA_ENVIRONNEMENT = valeur correspondant à l'environnement réseau du poste (« IN » ou « OUT »). Cette valeur est fournie par le poste.*
4. *SA_RÉSEAU prend les valeurs relatives à la connexion réseau. Ces valeurs sont déterminées par la TOE à partir des informations issues de la connexion réseau demandée.*

FIA_TOB.1 (CS) TSF-initiated termination of binding (canal sûr))

Audit *- Rupture (à l'initiative de la TSF) du lien établi entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet, raison de la rupture).*

Dépendances *FIA_USB.1 (CS)*

FIA_TOB.1.1 The TSF shall terminate a binding to **[assignment: subject]** after **[selection: completion of [assignment: operation], [assignment: time interval of user inactivity], [assignment: other condition]]**.

Raffinement *La TSF doit mettre fin au lien établi entre un programme distant (U_PROG_DISTANT) et le module de communication (S_COMM) dans les conditions suivantes :*

1. *Rupture de la connexion réseau entre le site distant et la TOE.*
2. *Arrêt de la TOE.*
3. *Rupture du lien établi entre le module S_COMM et un utilisateur distant (U_ADMIN_SÉCU, U_SUPERVISEUR) au travers de ce canal sûr.*
4. *Autres conditions.*

Note d'application :

Les ST conformes à ce PP devront préciser les conditions pouvant conduire à une rupture du lien par la TSF.

FIA_TOB.1.2 The TSF shall **[selection: leave the security attributes of the subject unchanged, terminate the subject, set the security attributes of the subject to [assignment: rules for setting the security attributes of the subject]]**.

Raffinement *La TSF doit soit laisser les attributs de sécurité du sujet inchangés, soit mettre fin au sujet, soit réinitialiser l'ensemble des valeurs des attributs de sécurité du module concerné (S_COMM) de la manière suivante :*

3. Pas de changement : SA_IDENT, SA_CONTEXTE

4. Remise à zéro : SA_PROGRAMME, SA_USER, SA_ENVIRONNEMENT, SA_RÉSEAU

Note d'application :

Les ST conformes à ce PP devront préciser la solution retenue.

FIA_TOB.2 (CS) User-initiated termination of binding (canal sûr)

Audit *- Rupture à l'initiative d'un programme distant d'un lien établi entre ce programme distant et un sujet (données associées : identification du programme, identification du sujet).*

Dépendances *FIA_USB.1 (CS)*

FIA_TOB.2.1 The TSF shall allow a user to terminate a binding to **[assignment: subject]**.

Raffinement *La TSF doit permettre à un programme distant (U_PROG_DISTANT) de rompre le lien avec le module de communication (S_COMM).*

FIA_TOB.2.2 The TSF shall **[selection: leave the security attributes of the subject unchanged, terminate the subject, set the security attributes of the subject to [assignment: rules for setting the security attributes of the subject]]**.

Raffinement *La TSF doit soit laisser les attributs de sécurité du sujet inchangés, soit mettre fin au sujet, soit réinitialiser l'ensemble des valeurs pour les attributs de sécurité du module concerné (S_COMM) de la manière suivante :*

5. Pas de changement : SA_IDENT, SA_CONTEXTE

6. Remise à zéro : SA_PROGRAMME, SA_USER, SA_ENVIRONNEMENT, SA_RÉSEAU

Note d'application :

Les ST conformes à ce PP devront préciser la solution retenue.

FCO_ETC.1 (AMP) Export of data and/or security attributes (authentification mutuelle préalable)

Audit *- Détail de la demande d'exportation (données associées : identité du demandeur, site distant concerné, résultat de la demande (acceptation ou refus)).*

Dépendances *aucunes.*

FCO_ETC.1.1 The TSF shall enforce **[assignment: rules on whether export is allowed]** when **[assignment: subject]** exports **[assignment: list of data and/or security attributes]** to a user bound to that subject.

Itération 1 (communication entre la TOE et un superviseur distant) :

La TSF doit s'assurer du respect des règles ci-après avant d'autoriser le module de communication (S_COMM) à transmettre les données ci-après à un programme distant (U_PROG_DISTANT) auquel il est lié, quand ces données sont issues du module d'administration et de supervision (S_ADMIN).

1. *Il doit y avoir une authentification mutuelle préalable entre ce programme distant (U_PROG_DISTANT) et le module de communication (S_COMM).*
2. *SA_RÔLE (sujet) doit être égal à SUPERVISEUR_SÉCURITÉ et SA_IDENT (sujet) à S_COMM.*

Données concernées : D_AUDIT_FLUX, D_AUDIT_APPLI, D_PARAM_SUPER, D_ALERTE

Itération 2 (communication entre la TOE et un administrateur sécurité distant) :

La TSF doit s'assurer du respect des règles ci-après avant d'autoriser le module de communication (S_COMM) à transmettre les données ci-après à un programme distant (U_PROG_DISTANT) auquel il est lié, quand ces données sont issues du module d'administration et de supervision (S_ADMIN).

1. *Il doit y avoir une authentification mutuelle préalable entre ce programme distant (U_PROG_DISTANT) et le module de communication (S_COMM).*
2. *SA_RÔLE (sujet) doit être égal à ADMINISTRATEUR_SÉCURITÉ et SA_IDENT (sujet) à S_COMM.*

Données concernées : D_PARAM_SÉCU, D_PARAM_CA (sauf données d'authentification), D_AUDIT_FLUX, D_AUDIT_APPLI

FCO_ITC.1 Import without security attributes (authentification mutuelle préalable)

Audit *- Détail de la demande (données associées : règle de filtrage et attributs utilisés pour accepter ou refuser le paquet, statut (acceptation ou refus)).*

Dépendances *aucunes.*

FCO_ITC.1.1 The TSF shall enforce **[assignment: rules on whether import is allowed]** when **[assignment: subject]** imports **[assignment: list of data]** from a user bound to that subject.

Itération 1 (communication entre la TOE et un superviseur distant) :

La TSF doit s'assurer que les règles ci-après sont respectées lorsque le module de communication (S_COMM) importe les données ci-après depuis un programme distant (U_PROG_DISTANT) auquel il est lié, quand ces données sont destinées au module d'administration ou de supervision (S_ADMIN).

1. *Il doit y avoir une authentification mutuelle préalable entre ce programme distant (U_PROG_DISTANT) et le module de communication (S_COMM).*
2. *SA_RÔLE (sujet) doit être égal à SUPERVISEUR_SÉCURITÉ et SA_IDENT (sujet) à S_COMM.*

Données concernées : D_AUDIT_FLUX, D_AUDIT_APPLI, D_PARAM_SUPER, D_ALERTE

Itération 2 (communication entre la TOE et un administrateur sécurité distant) :

La TSF doit s'assurer que les règles ci-après sont respectées lorsque le module de communication (S_COMM) importe les données ci-après depuis un programme distant (U_PROG_DISTANT) auquel il est lié, quand ces données sont destinées au module d'administration ou de supervision (S_ADMIN).

1. *Il doit y avoir une authentification mutuelle préalable entre ce programme distant (U_PROG_DISTANT) et le module de communication (S_COMM).*
2. *SA_RÔLE (sujet) doit être égal à ADMINISTRATEUR_SÉCURITÉ et SA_IDENT (sujet) à S_COMM.*

Données concernées : D_PARAM_SÉCU, D_PARAM_CA (sauf données d'authentification), D_AUDIT_FLUX, D_AUDIT_APPLI

FCO_ITC.1.2 The data shall be imported without security attributes.

Raffinement Les données doivent être importées sans attribut de sécurité.

FCO_CED.1 Confidentiality of exported data (canal sûr)

Audit - Pas de messages d'audit pour ce composant.
Dépendances aucunes.

FCO_CED.1.1 The TSF shall protect the confidentiality of **[assignment: list of data and/or security attributes]** provided by **[assignment: subject]** to a user bound to that subject.

Raffinement La TSF doit protéger en confidentialité les données transmises au travers du réseau par le module de communication (S_COMM) à un programme distant (U_PROG_DISTANT) lié à ce sujet quand ces données sont issues du module d'administration et de supervision (S_ADMIN).
Données concernées : D_ALERTE, D_AUDIT_FLUX, D_AUDIT_APPLI, D_PARAM_CA, D_PARAM_CONFIG, D_PARAM_SÉCU, D_PARAM_SUPER

Note d'application :
Les ST conformes à ce PP devront préciser les mécanismes utilisés.

FCO_CID.1 Confidentiality of imported data (canal sûr)

Audit - Pas de message d'audit pour ce composant.
Dépendances aucune.

FCO_CID.1.1 The TSF shall assist in protecting the confidentiality of **[assignment: list of data and/or security attributes]** provided to **[assignment: subject]** by a user bound to that subject.

Raffinement La TSF doit contribuer à assurer la confidentialité des données importées par le module de communication (S_COMM) depuis un programme distant (U_PROG_DISTANT) auquel il est lié au travers du réseau, quand ces données sont destinées au module d'administration et de supervision (S_ADMIN).
Données concernées : D_PARAM_CA, D_PARAM_CONFIG, D_PARAM_SÉCU, D_PARAM_SUPER, D_RÈGLES_FLUX, D_RÈGLES_APPLI

Note d'application :
Les ST conformes à ce PP devront préciser les mécanismes utilisés pour assurer cette confidentialité.

FCO_IED.1 (CS) Integrity of exported data without recovery (canal sûr)

Audit *- Pas de messages d'audit pour ce composant.*
Dépendances *aucunes.*

FCO_IED.1.1 When **[assignment: subject]** transmits **[assignment: list of data and/or security attributes]** to a user bound to that subject, the TSF shall provide that user the means to detect **[selection: modification, deletion, insertion, replay, [assignment: other integrity]]** anomalies.

Raffinement *Quand le module de communication (S_COMM) transmet des données à un utilisateur auquel il est lié, la TSF doit fournir à cet utilisateur le moyen de détecter toute anomalie de type modification, effacement ou insertion de données.*
Données concernées : D_PARAM_CA, D_PARAM_CONFIG, D_PARAM_SÉCU, D_PARAM_SUPER, D_RÈGLES_FLUX, D_RÈGLES_APPLI, D_ALERTE, D_AUDIT_FLUX, D_AUDIT_APPLI
Utilisateurs concernés : U_PROG_DISTANT, U_ADMIN_SÉCU, U_SUPERVISEUR
Note d'application :
Les ST conformes à ce PP devront préciser les anomalies prises en compte et les mécanismes utilisés.

FCO_IID.1 Integrity of imported data without recovery (canal sûr)

Audit *- Toute anomalie détectée (données associées : identité de l'utilisateur personne physique, données altérées).*
Dépendances *aucunes.*

FCO_IID.1.1 The TSF shall monitor the integrity of **[assignment: list of data and/or security attributes]** provided to **[assignment: subject]** by a user bound to that subject for **[selection: modification, deletion, insertion, replay]** anomalies.

Raffinement *La TSF doit contrôler l'intégrité des données ci-après transmises au module de communication (S_COMM) par un programme distant (U_PROG_DISTANT) lié à ce sujet (S_COMM) quand ces données sont destinées au module d'administration et de supervision (S_ADMIN) afin de détecter toute altération, suppression, insertion ou re-jeu de ces données.*
Données concernées : D_PARAM_CA, D_PARAM_CONFIG, D_PARAM_SÉCU, D_PARAM_SUPER, D_RÈGLES_FLUX, D_RÈGLES_APPLI
Note d'application :
Les ST conformes à ce PP devront préciser les mécanismes utilisés.

FCO_IID.1.2 On detection of an anomaly the TSF shall discard the data and/or security attributes.

Raffinement *En cas de détection d'une anomalie, la TSF doit ignorer les données importées.*

4.3.5 Audit et journalisation

Les composants ci-après contribuent à la mise en oeuvre de la fonction d'audit, de la journalisation, de la détection des attaques et des réponses aux attaques.

FCO_IED.1 (AUD) Integrity of exported data without recovery (intégrité des données d'audit)

Audit *- Pas de messages d'audit pour ce composant.*
Dépendances *aucunes.*

FCO_IED.1.1 When **[assignment: subject]** transmits **[assignment: list of data and/or security attributes]** to a user bound to that subject, the TSF shall provide that user the means to detect **[selection: modification, deletion, insertion, replay, [assignment: other integrity]]** anomalies.

Raffinement *Quand le module d'administration (S_ADMIN) ou le module de communication (S_COMM) transmet des données à un utilisateur auquel il est lié, la TSF doit fournir à cet utilisateur le moyen de détecter toute anomalie de type modification, effacement ou insertion de données.*
Données concernées : D_ALERTE, D_AUDIT_FLUX, D_AUDIT_APPLI
Utilisateurs concernés : U_USAGER, U_SUPERVISEUR

Note d'application :
Les ST conformes à ce PP devront préciser les anomalies prises en compte et les mécanismes utilisés.

FAU_GEN.2 Audit data generation with time

Audit *- Pas de messages d'audit pour ce composant.*
Dépendances (FMI_TIM.1 ou (FCO_ITC.1 et FCO_IID.1)) et
FDP_ACC.1 (FI) ou FDP_ACC.1 (FAS) ou FDP_ACC.1 (FRE) ou FDP_ACC.1 (FRS) et
FPT_RSA.1 (AUD)

FAU_GEN.2.1 The TSF shall store an audit record in **[assignment: object]** of the following events: **[selection: start-up of the audit functions, shut-down of the audit functions, [assignment: rules for which other events will be audited]]**.

Raffinement *La TSF doit enregistrer un message d'audit dans le fichier d'audit lors de la survenue des événements suivants :*
1. *Démarrage de la fonction d'audit, arrêt de la fonction d'audit.*
2. *Opérations (définies pour chaque composant) donnant lieu à la création d'un message d'audit (voir Tableau 5 : liste des événements audités par composant).*
3. *Autres événements.*

Note d'application :
Les ST conformes à ce PP devront fournir la liste exacte des événements audités et des opérations donnant lieu à l'enregistrement d'un message d'audit.

Composant	*Messages d'audit associés*
FDP_ACC.1 (FRS)	*- Refus ou acceptation de la demande d'accès (données associées : identité hérité de l'utilisateur, objet concerné, attributs de sécurité utilisés).*
FDP_ACC.1 (FRE)	*- Refus ou acceptation de la demande d'accès (données associées : identité hérité de l'utilisateur, objet concerné, attributs de sécurité utilisés).*
FDP_ACC.1 (FAS)	*- Refus ou acceptation de la demande d'accès (données associées : identité hérité de l'utilisateur, objet concerné, attributs de sécurité utilisés).*
FIA_TBR.1 (FAS)	*- Refus d'établissement d'un lien pour un programme local (données associées : raison du*

	refus, paramètres de sécurité utilisés et règle de sécurité utilisée pour accepter ou refuser l'établissement du lien).
FCO_ETC.1 (FAE)	*- Détail de la demande (données associées : règle de filtrage et attributs utilisés pour accepter ou refuser le paquet, statut (acceptation ou refus)).*
FIA_UID.2 (PL)	*- Connexion d'un programme local (données associées : identification du programme, contexte de la connexion).*
FIA_USB.1 (PL)	*- Établissement d'un lien entre un programme local et un sujet (données associées : identification du programme, identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*
FIA_TOB.2 (PL)	*- Rupture (à l'initiative de l'utilisateur) d'un lien établi entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet).*
FIA_UID.1 (PD)	*- Connexion d'un programme distant de manière anonyme (données associées : contexte de la connexion).*
FIA_USB.1 (PD)	*- Établissement d'un lien entre un programme distant et un sujet (données associées : identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*
FIA_TOB.2 (PD)	*- Rupture à l'initiative d'un programme distant d'un lien établi entre ce programme et un sujet (données associées : identification du sujet, caractéristiques de la connexion réseau).*
FIA_URE.2	*- Enregistrement d'un nouvel utilisateur.* *- Accès (réussi ou non, en lecture, écriture ou modification) aux propriétés de l'utilisateur.*
FIA_QAD.1	*- Acceptation ou refus des données d'authentification fournies.*
FIA_QAD.2	*- Génération de données d'authentification.*
FIA_UID.2 (UL)	*- Connexion d'un utilisateur local (données associées : identité de l'utilisateur, contexte de la connexion).*
FIA_UID.2 (UD)	*- Connexion d'un utilisateur distant (données associées : identité de l'utilisateur, contexte de la connexion).*
FIA_UAU.1 (UL)	*- Tentative (réussie ou non) d'authentification d'un utilisateur local.*
FIA_UAU.1 (UD)	*- Tentative (réussie ou non) d'authentification d'un utilisateur distant.*
FIA_UAU.6	*- Pas de messages d'audit pour ce composant.*
FIA_AFL.1	*- Atteinte ou dépassement d'un des seuils d'alerte lors de la connexion (données associées : seuil, nombre de tentatives).* *- Actions prises (émission d'une alerte, blocage de la connexion...).*
FIA_TBR.1 (UL)	*- Refus d'établissement d'un lien entre un utilisateur et un sujet (données associées : raison du refus, paramètres de sécurité utilisés pour accepter ou refuser l'établissement du lien).*
FIA_TBR.1 (UD)	*- Refus d'établissement d'un lien entre un utilisateur et un sujet (données associées : raison du refus, paramètres de sécurité utilisés pour accepter ou refuser l'établissement du lien).*
FIA_USB.1 (UL)	*- Établissement d'un lien entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*
FIA_USB.1 (UD)	*- Établissement d'un lien entre un utilisateur distant et un sujet (données associées : identification de l'utilisateur, identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*
FIA_TOB.1 (UD)	*- Rupture (à l'initiative de la TSF) du lien établi entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet, raison de la rupture).*
FIA_TOB.2 (UL)	*- Rupture (à l'initiative de l'utilisateur) d'un lien établi entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet).*
FIA_TOB.2 (UD)	*- Rupture à l'initiative d'un utilisateur distant d'un lien établi entre cet utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet).*
FDP_ACC.1 (FI)	*- Refus ou acceptation de la demande d'accès (données associées : identité héritée de l'utilisateur, objet concerné, attributs de sécurité utilisés).* *- Sauvegarde (données associées : résultat de l'opération, type de données sauvegardées).*
FDP_ISA.1	*- Création d'un objet ou d'un sujet (données associées : identité du sujet ou de l'objet + liste des attributs de sécurité).*
FDP_MSA.1	*- Toute demande (acceptées ou refusée) d'accès à un attribut de sécurité (données associées : identité du sujet, identité de l'utilisateur, objet, attribut, valeur, type d'accès demandé, statut ou résultat de la demande).*
FPT_RIP.2	*- Résultat de l'opération d'effacement demandée.*
FIA_UID.2 (CS)	*- Connexion d'un programme distant (données associées : identification du programme, contexte de la connexion).*
FIA_UAU.1 (CS)	*- Tentative (réussie ou non) d'authentification d'un programme distant.*
FIA_SUA.1	*- Authentification de la TOE auprès d'un programme distant (données associées : réussite ou*

	échec de l'opération, identité du programme distant).
FIA_USB.1 (CS)	*- Établissement d'un lien entre un programme distant et un sujet (données associées : identification du programme, identification du sujet, valeurs des attributs de sécurité définis lors de l'établissement du lien).*
FIA_TOB.1 (CS)	*- Rupture (à l'initiative de la TSF) du lien établi entre un utilisateur et un sujet (données associées : identification de l'utilisateur, identification du sujet, raison de la rupture).*
FIA_TOB.2 (CS)	*- Rupture à l'initiative d'un programme distant d'un lien établi entre ce programme distant et un sujet (données associées : identification du programme, identification du sujet).*
FCO_ETC.1 (AMP)	*- Détail de la demande d'exportation (données associées : identité du demandeur, site distant concerné, résultat de la demande (acceptation ou refus)).*
FCO_ITC.1	*- Détail de la demande (données associées : règle de filtrage et attributs utilisés pour accepter ou refuser le paquet, statut (acceptation ou refus)).*
FCO_CED.1	*- Pas de messages d'audit pour ce composant.*
FCO_CID.1	*- Pas de message d'audit pour ce composant.*
FCO_IED.1 (CS)	*- Pas de messages d'audit pour ce composant.*
FCO_IID.1	*- Toute anomalie détectée (données associées : identité de l'utilisateur personne physique, données altérées).*
FCO_IED.1 (AUD)	*- Pas de messages d'audit pour ce composant.*
FAU_SAA.3	*- Pas de messages d'audit pour ce composant.*
FAU_ARP.1	*- Actions prise par la TSF suite à la détection d'une violation potentielle de la politique de sécurité (données associées : type de la violation, action prise).*
FPT_RSA.1 (AUD)	*- Atteinte de la taille maximale pour un fichier d'audit (données associées : taille atteinte).* *- Action(s) prise(s) par la TSF en cas d'atteinte de la taille maximale pour un fichier d'audit (données associées : fichier d'audit).*
FPT_TST.1	*- Résultats et détails des tests effectués.*
FPT_TST.2	*- Résultats et détails des tests effectués.*
FPT_RSA.1 (RES)	*- Atteinte d'un quota pour le nombre de connexions réseau simultanées (données associées : quota atteint).*
FMI_CHO.1	*- Pas de messages d'audit pour ce composant.*

Tableau 5 : liste des événements audités par composant

FAU_GEN.2.2 The TSF shall record within each audit record the following information:

a) Date and time of the event, type of event, values of **[assignment: security attributes of the subject]**, the **[selection: success, failure, [assignment: other outcome(s)]]** of the event; and

b) **[assignment: other information]**.

Raffinement *La TSF doit enregistrer dans chaque message d'audit les informations suivantes :*

1. *la date et l'heure de l'événement ou de l'opération,*
2. *le type de l'événement ou de l'opération,*
3. *la valeur des attributs de sécurité suivants du sujet : SA_RÔLE, SA_USER, SA_PROGRAMME, SA_IDENT,*
4. *le résultat de l'opération (succès ou échec),*
5. *toute autre information pertinente en rapport avec cette opération ou événement (voir Tableau 5 : liste des événements audités par composant).*

Note d'application :

Les ST conformes à ce PP devront fournir la liste détaillée et exhaustive des informations enregistrées.

FAU_SAA.3 Simple attack heuristics

Audit *- Pas de messages d'audit pour ce composant.*
Dépendances *FAU_GEN.1*

FAU_SAA.3.1 The TSF shall maintain an internal representation of the following signature events **[assignment: a subset of system events]** that may indicate a violation of the TSP.

Raffinement *La TSF doit pouvoir maintenir une représentation interne des événements caractéristiques ci-après qui peuvent indiquer une violation de la TSP.*

1. *Nombre de connexions simultanées depuis le réseau supérieur à N1.*
2. *Nombre de tentatives infructueuses de connexion depuis un même système distant supérieur à N2.*
3. *Autres événements.*

Note d'application :
Les ST conformes à ce PP devront fournir la liste des événements retenus et préciser les valeurs retenues pour N1 et N2.

FAU_SAA.3.2 The TSF shall compare the signature events against the record of system activity discernible from an examination of **[assignment: the information to be used to determine system activity]**.

Raffinement *La TSF doit comparer les événements caractéristiques à l'enregistrement de l'activité du système discernables par l'examen des messages d'audit générés par la TSF et les informations complémentaires mémorisées par la TSF.*
Note d'application :
Les ST conformes à ce PP devront préciser quelles sont ces informations.

FAU_SAA.3.3 The TSF shall indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Raffinement *En cas de détection d'une violation potentielle imminente de la politique de sécurité de la TOE, la TSF doit émettre une alerte.*

FAU_ARP.1 Security audit automatic response

Audit *- Actions prise par la TSF suite à la détection d'une violation potentielle de la politique de sécurité (données associées : type de la violation, action prise).*
Dépendances *FAU_SAA.1*

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

Raffinement *En cas de détection d'une violation potentielle de la politique de sécurité, la TSF doit prendre les actions définies par l'administrateur sécurité.*
Note d'application :
Les ST conformes à ce PP devront préciser les actions que peut sélectionner l'administrateur sécurité en réponse à une violation potentielle de la politique de sécurité.

FPT_RSA.1 (AUD) Maximum quotas for subjects and objects (fichiers d'audit)

Audit *- Atteinte de la taille maximale pour un fichier d'audit (données associées : taille atteinte).*
- Action(s) prise(s) par la TSF en cas d'atteinte de la taille maximale pour un fichier d'audit (données associées : fichier d'audit).
Dépendances *aucunes.*

FPT_RSA.1.1 The TSF shall enforce maximum quotas for **[selection: processing resources, storage resources, communication resources, [assignment: other resources]]** that **[assignment: list of subjects and/or objects]** can use **[selection: simultaneously, over a specified period of time]**.

Raffinement *La TSF doit contrôler que la taille des fichiers d'audit (D_AUDIT_FLUX, D_AUDIT_ADMIN) et d'alerte (D_ALERTE) ne dépasse pas les valeurs définies par l'administrateur sécurité dans D_PARAM_SUPER lorsque S_AUDIT écrit dans ces fichiers.*

Note d'application :
Les ST conformes à ce PP devront préciser quelles sont les valeurs possibles pour ces quotas.

FPT_RSA.1.2 The TSF shall **[assignment: action(s)]** when a maximum quota is **[selection: almost surpassed, surpassed]**.

Raffinement *La TSF doit émettre une alarme et prendre les actions définies par l'administrateur sécurité lorsque l'une de ces valeurs est atteinte.*

Note d'application :
Les ST conformes à ce PP devront préciser quelles sont les actions qui peuvent être définies par l'administrateur sécurité et prises par la TSF.

4.3.6 Fiabilité et disponibilité de la TOE

FPT_TST.1 TSF self-testing

Audit *- Résultats et détails des tests effectués.*
Dépendances *aucunes.*

FPT_TST.1.1 The TSF shall run a suite of tests **[selection: immediately after installation, during each start-up, periodically during normal operation, at the request of a subject, [assignment: other conditions]]** to demonstrate the correct operation of [selection: **[assignment: parts of the TSF], the TSF]**.

Raffinement *La TSF doit procéder à une suite de tests lors du démarrage de la TOE, périodiquement ou à la demande d'un utilisateur autorisé afin de démontrer le fonctionnement correct de l'ensemble de la TSF ou de certains de ses composants.*

Note d'application :
Les ST conformes à ce PP devront préciser les tests effectués et donner la liste des composants de la TSF qui sont testés.

FPT_TST.2 Integrity testing

Audit *- Résultats et détails des tests effectués.*
Dépendances *aucunes.*

FPT_TST.2.1 The TSF shall run a suite of tests **[selection: immediately after installation, during each start-up, periodically during normal operation, at the request of a subject, [assignment: other conditions]]** to verify the integrity of **[selection: the stored executable code of the TSF, [assignment: list of objects]]**.

Raffinement *La TSF doit procéder à une suite de tests lors du démarrage de la TOE, périodiquement ou à la demande d'un utilisateur autorisé afin de vérifier l'intégrité de l'ensemble de la TOE ou de certains de ses composants.*

Note d'application :
Les ST conformes à ce PP devront préciser les mécanismes utilisés pour réaliser ce contrôle d'intégrité et donner la liste des composants de la TOE dont l'intégrité est testée.

FPT_RSA.1 (RES) Maximum quotas for subjects and objects (accès rentrant)

Audit *- Atteinte d'un quota pour le nombre de connexions réseau simultanées (données associées : quota atteint).*
Dépendances *aucunes.*

FPT_RSA.1.1 The TSF shall enforce maximum quotas for **[selection: processing resources, storage resources, communication resources, [assignment: other resources]]** that **[assignment: list of subjects and/or objects]** can use **[selection: simultaneously, over a specified period of time]**.

Raffinement *La TSF doit appliquer des quotas maximums pour les accès réseau que les programmes distants (U_PROG_DISTANT) peuvent réaliser simultanément depuis des sites distants.*

Note d'application :
Les ST conformes à ce PP devront préciser quelles sont les valeurs possibles pour ces quotas.

FPT_RSA.1.2 The TSF shall **[assignment: action(s)]** when a maximum quotum is **[selection: almost surpassed, surpassed]**.

Raffinement *La TSF doit refuser toute connexion supplémentaire venant d'un site distant si le quota de connexions de ce type est atteint ou dépassé.*

4.3.7 Autres exigences

FMI_CHO.1 Choice

Audit *- Pas de messages d'audit pour ce composant.*
Dépendances *aucunes.*

FMI_CHO.1.1 **[assignment: set of SFRs]** or **[assignment: set of SFRs]**.

Raffinement *Les ST conformes à ce PP pourront choisir entre :*
1. FIA_QAD.1 et FIA_QAD.2 pour la génération des données d'authentification.

4.4 Exigences de sécurité d'assurance pour la TOE

SAR

La TOE doit être évaluée au niveau EAL2 augmenté des composants ADV_TDS.3**, ADV_IMP.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1 et AVA_VAN.3.

Ce qui correspond au paquet d'assurance prévu pour une qualification au niveau standard d'une cible de sécurité (cf. [QUALIF_STD]) défini par la colonne « QS » du tableau suivant :

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

Tableau 6 : exigences pour une qualification au niveau standard d'une ST

* Le composant ADV_IMP.1 est raffiné de la façon suivante : The sample of the implementation representation shall contain all the cryptographic mechanisms of the TOE.

** Le composant ADV_TDS.3 est raffiné de la façon suivante : The description of the design of the TSF in terms of modules could be limited to the cryptographic mechanisms of the

TOE.

*Note : le composant ADV_TDS.3** étant moins « exigeant » que ADV_TDS.3, une TOE conforme au paquet QS ne pourra prétendre qu'à la conformité au composant ADV_TDS.2 au titre des accords de reconnaissance.*

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

Pour un profil de protection, la classe d'assurance ASE (*security target evaluation*) et remplacée par le la clase APE (*protection profile evaluation*). Les composants équivalents pour un profil de protection sont les suivants :

Classe d'assurance	Famille d'assurance	Composants d'assurance par niveau d'évaluation							
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	**QS**
Protection Profile Evaluation	APE_CCL	1	**1**	1	1	1	1	1	**1**
	APE_ECD	1	**1**	1	1	1	1	1	**1**
	APE_INT	1	**1**	1	1	1	1	1	**1**
	APE_OBJ	1	**2**	2	2	2	2	2	**2**
	APE_REQ	1	**2**	2	2	2	2	2	**2**
	APE_SPD		**1**	1	1	1	1	1	**1**

Tableau 7 : exigences pour l'évaluation d'un profil de protection

5 Argumentaire

5.1 Objectifs de sécurité / Problème de sécurité

	T_écoute_passive	T_divulgation	T_origine	T_piégeage_logiciel	T_saturation	T_dysfonctionnement_logiciel	T_altération_données	T_traitement_illicite	T_erreur_utilisation	T_abus_droit	T_filtre_désactivation	T_usurpation_droit	T_reniement_action	OSP_filtrage	OSP_application_intégrité	OSP_rôles	OSP_admin	OSP_supervision	OSP_audit_admin	OSP_audit_flux	OSP_détection_violation	OSP_configuration_sûre	OSP_crypto	OSP_EAL	A_administrateurs_de_confiance	A_usager_non_privilégié	A_livraison_sûre	A_maîtrise_configuration	A_ressources_disponibles	A_poste_sûr	A_type_environnement	A_filtrage_total	A_poste_utilisateurs	A_protection_physique
OT_filtrage_niveaux					X									X																				
OT_filtrage_critères					X									X																				
OT_application_intégrité															X																			
OT_rôles																X																		
OT_administration			X				X		X	X	X	X	X				X																	
OT_supervision		X		X		X		X										X			X												
OT_identification		X						X			X	X																						
OT_authentification		X	X				X	X			X	X																						
OT_contrôle_accès		X					X	X		X																								
OT_données_inaccessibilité								X																										
OT_journaux_protection		X						X																										
OT_échange_authentification		X	X					X																										
OT_échange_intégrité			X																															
OT_échange_confidentialité	X							X																										
OT_échange_rejeu			X																															
OT_audit_flux				X	X		X		X											X														
OT_audit_exploitation		X	X	X	X		X	X	X	X	X	X	X			X	X	X	X		X													
OT_alerte_détection				X	X	X	X		X	X	X	X	X								X													
OT_alerte_réaction				X	X	X	X		X	X	X	X	X								X													
OT_intégrité				X			X																											
OT_fonctionnement				X		X																												
OT_crypto																							X											
OD_EAL						X			X															X	X		X							
OE_administrateurs_de_confiance									X	X	X		X												X									
OE_usager_non_privilégié																										X								
OE_livraison_sûre			X	X		X	X		X	X	X	X	X								X					X							
OE_maîtrise_configuration			X	X		X	X		X	X	X	X	X								X						X						
OE_ressources_disponibles					X																								X					
OE_poste_sûr		X		X			X	X																						X				
OE_contexte_sûr																														X	X			
OE_type_environnement																															X			
OE_filtrage_total																																X		
OE_poste_utilisateurs				X			X																										X	
OE_protection_physique																																		X

Tableau 8 : objectifs de sécurité / problèmes de sécurité

5.1.1 Couverture des menaces en environnement opérationnel

T_écoute_passive (19)

Protection :

OT_échange_confidentialité assure la protection en confidentialité des données échangées entre la TOE et un centre d'administration ou de supervision.

Détection :

Réponse :

T_divulgation (23)

Protection :

Au niveau réseau, **OT_échange_authentification** garantit que tout accès à des données a lieu depuis un site distant autorisé.

Au niveau du poste, les données (filtres, journaux, données d'authentification) sont protégées contre tout accès non autorisé via le poste (**OE_poste_sûr**) ou la TOE (**OT_journaux_protection**).

Au niveau de la TOE, **OT_supervision, OT_identification, OT_authentification, OT_contrôle_accès** protègent l'accès aux fonctions de supervision qui permettent d'accéder à ces données.

Détection :

OT_audit_exploitation permet de tracer tout accès à ces données au travers de la TOE via l'utilisation des fonctions d'administration ou de supervision et d'exploiter ces traces.

Réponse :

T_origine (24)

Protection :

OT_échange_authentification garantit que tout échange au travers du réseau a bien lieu entre la TOE et un site autorisé.

OT_authentification assure l'authentification des administrateurs et superviseurs et limite les risques d'usurpation.

OT_échange_intégrité et **OT_échange_rejeu** garantit que les données reçues par la TOE ne sont ni modifiées, ni contrefaites, ni rejouées et que les données transmises par la TOE ne le sont qu'à un système et un utilisateur autorisé.

Détection :

OT_audit_exploitation permet de tracer les actions des administrateurs ou superviseurs et d'exploiter ces traces. Cet objectif permet ainsi de détecter les tentatives de pénétration par force brute (essais de code d'accès), les tentatives d'envoi de données contrefaites ou modifiées.

Réponse :

OT_administration permet à l'administrateur de modifier les codes d'accès ou la configuration de la TOE afin d'augmenter ses protections vis-à-vis de cette menace.

OE_livraison_sûre et **OE_maîtrise_configuration** permettent de revenir à une configuration de confiance de la TOE si nécessaire.

T_piégeage_logiciel (26)

Protection :

OE_poste_utilisateurs assure un accès contrôlé au poste ce qui limite les risques d'occurrence de la menace. **OE_poste_sûr** garantit une protection des éléments (fichiers) de la TOE stockés sur le poste.

Détection :

OT_intégrité permet de détecter toute altération de la TOE ou perte de cohérence des données de la TOE (filtres, paramètres) puis de le signaler (**OT_alerte_détection** + **OT_supervision**). En exploitation, OT_intégrité ne permet pas de se prémunir contre un piégeage de la fonction de contrôle d'intégrité

elle-même (pas d'auto-contrôle possible en logiciel).

OT_fonctionnement permet de connaître l'état de fonctionnement de la TOE.

OT_audit_exploitation, OT_audit_flux et OT_alerte_détection permettent de détecter un dysfonctionnement éventuel de la TOE.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée au niveau du poste.

OE_livraison_sûre et **OE_maîtrise_configuration** permettent de revenir à une configuration de confiance de la TOE.

T_saturation (30)

Attaque des ressources du poste :

Protection :

OT_filtrage_niveau et **OT_filtrage_critères** permettent de bloquer des tentatives d'accès multiples vers une ressource du poste.

Détection :

OT_audit_exploitation, OT_audit_flux et OT_alerte_détection permettent de détecter les saturations du poste qui sont contrées par la TOE.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée.

Attaque de la TOE :

Protection :

OE_ressources_disponibles précisent quelles sont les ressources nécessaires pour un fonctionnement nominal correct de la TOE.

Détection :

OT_alerte_détection permet d'informer la supervision de la survenue de saturations.

OT_audit_exploitation, OT_audit_flux et OT_alerte_détection permettent aussi de détecter une éventuelle attaque de la TOE.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée au niveau du poste.

T_dysfonctionnement_logiciel (31)

Protection :

OD_EAL impose une évaluation qui permet d'avoir un niveau donné de confiance dans la TOE et son fonctionnement.

Détection :

OT_fonctionnement assure la détection de dysfonctionnements de la TOE (tels que la désactivation du filtrage ou le non fonctionnement des fonctions de sécurité) et leur signalement aux superviseurs se sécurité (**OT_supervision**).

OT_alerte_détection permet de détecter des violations de la politique de sécurité qui résulterait d'un dysfonctionnement.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée au niveau du poste.

OE_livraison_sûre et **OE_maîtrise_configuration** permettent de revenir à une configuration de confiance de la TOE.

T_altération_données (36)

Protection :

Le contrôle de l'accès au poste (**OE_poste_utilisateurs**), à la TOE (**OT_authentification**) et aux fonctions d'administration et de supervision (**OT_contrôle_accès**) limite les possibilités d'occurrence de cette menace.

OE_poste_sûr assure une protection par le poste des éléments constituant la TOE.

Détection :

OT_intégrité permet de détecter les pertes de cohérence des paramètres de la TOE ou des filtres définis.

OT_audit_exploitation, OT_audit_flux et OT_alerte_détection permettent de tracer les actions d'administration et de détecter une altération des paramètres ou des règles de filtrage.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée au niveau du poste.

OT_administration permet à l'administrateur de corriger toute règle ou paramètre altéré.

OE_livraison_sûre et **OE_maîtrise_configuration** permettent de revenir à une configuration de confiance de la TOE.

T_traitement_illicite (37)

Protection :

Au niveau réseau, **OT_échange_confidentialité** assure la protection en confidentialité des traces d'audit des flux lors de leur transmission entre la TOE et un centre de supervision. **OT_échange_authentification** garantit que les éléments tracés sont transmis à un site distant autorisé.

Au niveau du poste, les journaux sont protégés contre toute accès via le poste (**OE_poste_sûr**) ou via la TOE (**OT_journaux_protection**).

Au niveau de la TOE, **OT_supervision, OT_identification, OT_authentification, OT_contrôle_accès** protègent l'accès aux fonctions de supervision qui permettent d'accéder à ces données.

Dans le cas du recyclage d'un poste, **OT_données_inacessibilité** permet la destruction de toute donnée sensible.

Détection :

OT_audit_exploitation permet de tracer tout accès à ces données au travers de la

TOE via le mécanisme d'audit.

Réponse :

T_erreur_utilisation (38)

Protection :

OE_administrateurs_de_confiance limite le risque d'occurrence de cette menace du fait de personnel autorisé (formation et sensibilisation des personnels).

Il existe en outre une documentation requise par le niveau d'évaluation (**OD_EAL**) qui couvre l'utilisation et l'administration de la TOE.

Détection :

OT_audit_exploitation, OT_audit_flux et OT_alerte_détection permettent de tracer les actions d'administration et de détecter une altération des paramètres ou des règles de filtrage.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée au niveau du poste.

OT_admininstration permet à l'administrateur de corriger toute règle ou paramètre altéré.

OE_livraison_sûre et **OE_maîtrise_configuration** permettent de revenir à une configuration de confiance de la TOE.

T_abus_droit (39)

Prévention / protection :

OE_administrateurs_de_confiance limite le risque d'occurrence de cette menace du fait de personnel autorisé (formation et sensibilisation des personnels).

OT_contrôle_accès permet de limiter l'accès des utilisateurs aux seuls éléments utiles (données, fonctions) à leur mission.

Détection :

OT_audit_exploitation permet de tracer les actions d'administration et de détecter toute altération de paramètres ou règles de filtrage.

OT_alerte_détection permet de détecter des conséquences d'un abus de droit conduisant à un dysfonctionnement manifeste de la TOE ou à une violation majeure de la politique de sécurité.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée au niveau du poste.

OT_admininstration permet à l'administrateur de corriger toute règle ou paramètre altéré.

OE_livraison_sûre et **OE_maîtrise_configuration** permettent de revenir à une configuration de confiance de la TOE.

T_filtre_désactivation (39, 40)

Protection (usurpation) :

OT_identification et **OT_authentification** limite les risques d'usurpation.

Protection (abus) :

Le personnel d'administration et de supervision est de confiance (**OE_administrateurs_de_confiance**).

Détection :

OT_audit_exploitation permet de tracer les actions d'administration et de détecter toute altération de paramètres ou règles de filtrage.

OT_alerte_détection permet de détecter les conséquences d'une désactivation conduisant à un dysfonctionnement manifeste de la TOE ou à une violation majeure de la politique de sécurité.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée au niveau du poste.

OT_administration permet à l'administrateur de corriger toute règle ou paramètre altéré.

OE_livraison_sûre et **OE_maîtrise_configuration** permettent de revenir à une configuration de confiance de la TOE.

T_usurpation_droit (40)

Protection :

OT_identification et **OT_authentification** limite les risques d'usurpation.

Détection :

OT_audit_exploitation permet de tracer les actions d'administration et de détecter toute altération de paramètres ou règles de filtrage.

OT_alerte_détection permet de détecter les conséquences d'une usurpation conduisant à un dysfonctionnement manifeste de la TOE ou à une violation majeure de la politique de sécurité.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée au niveau du poste.

OT_admininstration permet à l'administrateur de corriger toute règle ou paramètre altéré.

OE_livraison_sûre et **OE_maîtrise_configuration** permettent de revenir à une configuration de confiance de la TOE.

T_reniement_action (41)

Protection :

OE_administrateurs_de_confiance limite le risque d'occurrence de cette menace du fait des personnels.

Détection :

OT_audit_exploitation permet de tracer les actions d'administration et de détecter toute altération de paramètres ou règles de filtrage.

OT_alerte_détection permet de détecter les conséquences d'une action conduisant à une violation de la politique de sécurité.

Réponse :

OT_alerte_réaction permet si nécessaire le blocage des accès réseau suite à une alerte détectée au niveau du poste.

OT_admininstration permet à l'administrateur de corriger toute règle ou paramètre altéré.

OE_livraison_sûre et **OE_maîtrise_configuration** permettent de revenir à une configuration de confiance de la TOE.

5.1.2 Couvertures des politiques de sécurité organisationnelles

OSP_filtrage

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OT_filtrage_critères qui définit les critères utilisés par les règles de filtrage.

OT_filtrage_niveaux qui définit les différents types de filtrage (global, utilisateur, spécifique)

OSP_application_intégrité

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OT_application_intégrité qui est dédié à la couverture de cette politique.

OSP_rôles

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OT_rôles qui est dédié à la couverture de cette politique.

Celui-ci est complété par **OT_audit_exploitation** pour le contrôle des actions des utilisateurs.

OSP_admin

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OT_admininstration qui est dédié à la couverture de cette politique.

Celui-ci est complété par **OT_audit_exploitation** pour le contrôle des actions d'administration.

OSP_supervision

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OT_supervision qui est dédié à la couverture de cette politique.

Celui-ci est complété par **OT_audit_exploitation** pour le contrôle des actions de supervision.

OSP_audit_admin

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OT_audit_exploitation qui couvre l'audit des actions réalisées dans le cadre de

l'administration ou de la supervision.

OSP_audit_flux

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OT_audit_flux qui est dédié à la couverture de cette politique.

OSP_détection_violation

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OT_alerte_détection qui est dédié à la couverture de cette politique.

OT_audit_exploitation et **OT_supervision** pour l'information quant à une alerte.

OT_alerte_réaction pour le traitement des alertes au niveau du poste.

OSP_configuration_sûre

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OE_livraison_sûre permet l'installation d'un exemplaire de confiance de la TOE.

OE_maîtrise_configuration garantit que les administrateurs disposent des moyens de sauvegarder une configuration sûre et de la restaurer.

OSP_EAL

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OD_EAL qui est dédié à la couverture de cette politique.

OSP_crypto

Cette politique de sécurité organisationnelle est mise en oeuvre par :

OT_crypto qui est dédié à la couverture de cette politique.

5.1.3 Couverture des hypothèses

A_administrateurs_de_confiance

L'objectif de sécurité **OE_administrateurs_de_confiance** est dédié à la couverture de cette hypothèse.

De plus, l'objectif **OD_EAL** renforce cette couverture en imposant la fourniture aux administrateurs et aux superviseurs d'une documentation adaptée.

A_usager_non_privilégié

L'objectif de sécurité **OE_usager_non_privilégié** est dédié à la couverture de cette hypothèse.

A_livraison_sûre

L'objectif de sécurité **OE_livraison_sûre** est dédié à la couverture de cette hypothèse.

De plus, l'objectif **OD_EAL** renforce cette couverture en garantissant la qualité des livrables.

A_maîtrise_configuration

L'objectif de sécurité **OE_maîtrise_configuration** est dédié à la couverture de cette hypothèse.

A_ressources_disponibles

L'objectif de sécurité **OE_ressources_disponibles** est dédié à la couverture de cette hypothèse.

A_poste_sûr

L'objectif de sécurité **OE_poste_sûr** est dédié à la couverture de cette hypothèse.

De plus, **OE_contexte_sûr** garantit que les données qui seront utilisées par la TOE correspondent aux données mises à sa disposition par son environnement.

A_type_environnement

L'objectif de sécurité **OE_type_environnement** est dédié à la couverture de cette hypothèse.

De plus, **OE_contexte_sûr** garantit que les données qui seront utilisées par la TOE correspondent aux données mises à sa disposition par son environnement.

A_filtrage_total

L'objectif de sécurité **OE_filtrage_total** est dédié à la couverture de cette hypothèse.

A_poste_utilisateurs

L'objectif de sécurité **OE_poste_utilisateurs** est dédié à la couverture de cette hypothèse.

A_protection_physique

L'objectif de sécurité **OE_protection_physique** est dédié à la couverture de cette hypothèse.

5.2 Exigences de sécurité / Objectifs de sécurité

5.2.1 Couverture des objectifs de sécurité pour la TOE

	OT_filtrage_niveaux	OT_filtrage_critères	OT_application_intégrité	OT_administration	OT_supervision	OT_rôles	OT_identification	OT_authentification	OT_contrôle_accès	OT_données_inaccessibilité	OT_journaux_protection	OT_échange_authentification	OT_échange_intégrité	OT_échange_confidentialité	OT_échange_rejeu	OT_audit_flux	OT_audit_exploitation	OT_alerte_détection	OT_alerte_réaction	OT_intégrité	OT_fonctionnement	OT_crypto
FDP_ACC.1 (FRS)	X	X																				
FDP_ACC.1 (FRE)	X	X																				
FDP_ACC.1 (FAS)	X	X	X																			
FIA_TBR.1 (FAS)	X	X	X																			
FCO_ETC.1 (FAE)	X	X																				
FIA_UID.2 (PL)	X	X	X																			
FIA_USB.1 (PL)	X	X																				
FIA_TOB.2 (PL)	X	X							X													
FIA_UID.1 (PD)	X	X																				
FIA_USB.1 (PD)	X	X																				
FIA_TOB.2 (PD)	X	X																				
FIA_URE.2				X	X	X	X	X														
FIA_QAD.1				X	X			X														X
FIA_QAD.2				X	X			X														X
FIA_UID.2 (UL)				X	X		X															
FIA_UID.2 (UD)				X	X		X															
FIA_UAU.1 (UL)				X	X			X														
FIA_UAU.1 (UD)				X	X			X														
FIA_UAU.6				X	X			X	X			X										
FIA_AFL.1				X	X													X	X			
FIA_TBR.1 (UD)				X	X																	
FIA_TBR.1 (UL)				X	X																	
FIA_USB.1 (UL)				X	X	X																
FIA_USB.1 (UD)				X	X	X																
FIA_TOB.1 (UD)				X	X				X													
FIA_TOB.2 (UL)				X	X				X													
FIA_TOB.2 (UD)				X	X				X													
FDP_ACC.1 (FI)				X	X				X		X						X					
FDP_ISA.1	X	X		X	X				X													
FDP_MSA.1	X	X		X	X				X													
FPT_RIP.2										X												
FIA_UID.2 (CS)												X										
FIA_UAU.1 (CS)												X										X
FIA_SUA.1												X										X
FIA_USB.1 (CS)												X	X	X	X							
FIA_TOB.1 (CS)									X			X	X	X	X							
FIA_TOB.2 (CS)									X			X	X	X	X							
FCO_ETC.1 (AMP)												X	X	X	X							
FCO_ITC.1				X	X							X	X	X	X							
FCO_CED.1														X								X
FCO_CID.1														X								X
FCO_IED.1 (CS)													X		X							X
FCO_IID.1													X		X							X
FCO_IED.1 (AUD)											X											
FAU_GEN.2																X	X					
FAU_SAA.3																		X				
FAU_ARP.1																			X			
FPT_RSA.1 (AUD)											X											
FPT_TST.1																					X	
FPT_TST.2																				X		
FPT_RSA.1 (RES)																		X	X			
FMI_CHO.1								X														

Tableau 9 : exigences fonctionnelles de sécurité / objectifs de sécurité pour la TOE

OT_filtrage_niveaux, OT_filtrage_critères

FIA_TBR.1 (FAS) et **FDP_ACC.1 (FAS)** définissent la mise en oeuvre des règles de filtrage applicatif pour les paquets sortants ; **FCO_ETC.1 (FAE)** définit la mise en oeuvre des règles de filtrage applicatif pour les paquets entrants.

FDP_ACC.1 (FRS) et **FDP_ACC.1 (FRE)** définissent la mise en oeuvre des règles de filtrage réseau pour les paquets sortants et entrants.

FIA_UID.1 (PD) précise que les programmes distants (autres que ceux destinés à l'administration ou à la supervision distantes) n'ont pas besoin de s'identifier avant l'établissement d'un lien avec la TOE.

FIA_UID.2 (PL) précise que les programmes locaux ont besoin de s'identifier avant l'établissement d'un lien avec la TOE.

FIA_USB.1 (PL) et **FIA_USB.1 (PD)** définissent les règles d'héritage des attributs de sécurité par le module de filtrage applicatif et le module de filtrage réseau.

FIA_TOB.2 (PL) et **FIA_TOB.2 (PD)** précisent les règles de réinitialisation des paramètres utilisés pour le filtrage.

FDP_ISA.1 et **FDP_MSA.1** précisent les règles relatives à la définition ou à la modification des attributs de sécurité.

OT_application_intégrité

FIA_UID.2 (PL) précise que les programmes locaux ont besoin de s'identifier avant l'établissement d'un lien avec la TOE.

FDP_ACC.1 (FAS) et **FIA_TBR.1 (FAS)** mettent en oeuvre le contrôle d'intégrité des applications cherchant à effectuer des connexions sortantes.**FIA_TBR.1 (FAS)** émet un message d'audit en cas d'altération d'une application.

OT_administration, OT_supervision

FIA_URE.2 précise les conditions d'enregistrement des utilisateurs ; **FIA_QAD.1** et **FIA_QAD.2** les critères relatifs aux données d'authentification des utilisateurs.

FIA_UID.2 (UL, UD) précise que la TOE doit commencer par identifier les utilisateurs préalablement à toute autre action ; **FIA_UAU.1 (UL, UD)** que la TOE doit authentifier les utilisateurs avant tout établissement d'un lien. **FIA_UAU.6** précise que la TOE ne fournit aucune information à l'utilisateur tant qu'il n'est pas authentifié. **FIA_AFL.1** précise les conditions de notification par la TOE des erreurs de connexion des utilisateurs.

FCO_ITC.1 précise les règles autorisant la transmission de données au module de communication.

FIA_TBR.1 (UL, UD) précisent les règles d'établissement d'un lien entre l'utilisateur et la TOE.

FIA_USB.1 (UL, UD) précisent les règles d'allocation des attributs de sécurité permettant aux utilisateurs autorisés d'accès aux fonctions qu'ils peuvent utiliser.

FDP_ACC.1 (FI) précise les règles permettant aux utilisateurs autorisés d'accéder aux données qu'ils doivent gérer.

FDP_ISA.1 et **FDP_MSA.1** précisent les règles relatives à la définition des attributs de sécurité.

FIA_TOB.1 (UD) et **FIA_TOB.2 (UL, UD)** définissent les conditions relatives à la

rupture de connexion entre un utilisateur et la TOE, rupture qui met fin aux autorisations d'accès pour cet utilisateur au travers du module d'administration et de supervision.

OT_rôles

FIA_URE.2 qui précise les conditions d'enregistrement des utilisateurs, précise aussi qu'un rôle peut être alloué à l'utilisateur et quels sont ces rôles.

FIA_USB.1 (UL, UD) précisent les règles d'allocation des attributs de sécurité (dont le rôle) permettant aux utilisateurs autorisés d'accès aux fonctions qu'ils peuvent utiliser.

OT_identification

FIA_URE.2 précise les conditions d'enregistrement des utilisateurs.

FIA_UID.2 (UL, UD) précise que la TOE doit commencer par identifier les utilisateurs préalablement à toute autre action.

OT_authentification

FIA_URE.2 qui précise les conditions d'enregistrement des utilisateurs, inclut aussi l'enregistrement des données d'authentification.

FIA_QAD.1 précise que la TOE contrôle la qualité des données d'authentification.

FIA_QAD.2 précise les conditions de génération par la TOE de données d'authentification.

FIA_UAU.1 (UL, UD) précise que la TOE doit authentifier les utilisateurs avant tout établissement d'un lien.

FMI_CHO.1 précise que le choix est laissé aux rédacteurs des ST entre la saisie des données d'authentification par l'administrateur sécurité et la génération des données d'authentification par la TOE.

FIA_UAU.6 précise que la TOE ne fournit aucune information à l'utilisateur tant qu'il n'est pas authentifié.

OT_contrôle_accès

FIA_UAU.6 précise que la TOE ne fournit aucune information à l'utilisateur tant qu'il n'est pas authentifié.

FDP_ACC.1 (FI) définit les conditions d'accès aux données et aux fonctions de la TOE.

FDP_ISA.1 et **FDP_MSA.1** précisent les règles relatives à la définition ou à la modification des attributs de sécurité.

FIA_TOB.2 (PL) définit les conditions de restriction d'accès d'un programme local à la TOE.

FIA_TOB.1 (CS), FIA_TOB.2 (CS) définissent les conditions de restriction d'accès d'un programme distant à la TOE pour l'établissement d'un canal de communication.

FIA_TOB.1 (UD) et **FIA_TOB.2 (UL, UD)** définissent les conditions relatives à la rupture de connexion entre un utilisateur et la TOE, rupture qui met fin aux autorisations d'accès pour cet utilisateur au travers du module d'administration et de supervision.

OT_données_inaccessibilité

FPT_RIP.2 précise qu'il est possible de rendre indisponible ou d'effacer les données sensibles de la TOE.

OT_journaux_protection

FDP_ACC.1 (FI) précise les règles de contrôles d'accès aux différents objets dont les journaux d'audit.

FPT_RSA.1 (AUD) précise que les journaux d'audit sont protégés contre tout risque de saturation et qu'une alarme est émise et des actions prises en cas d'atteinte d'un seuil critique.

FCO_IED.1 (AUD) précise que la TOE permet un contrôle d'intégrité des données d'audit transmises à un utilisateur autorisé.

OT_échange_authentification

FIA_UID.2 (CS) et **FIA_UAU.1 (CS)** précisent les conditions d'identification et d'authentification par la TOE d'un site distant (i.e. d'un programme distant).

FIA_SUA.1 précise que la TOE doit s'authentifier auprès des programmes distants pour l'établissement d'un canal sûr.

FCO_ETC.1 (AMP) et **FCO_ITC.1** précisent que la TOE doit s'assurer d'une authentification mutuelle entre la TOE et le site distant préalablement à tout échange.

FIA_USB.1 (CS) définit l'établissement du lien entre la TOE et le site distant.

FIA_TOB.1 (CS) et **FIA_TOB.2 (CS)** précisent les conditions de rupture du lien établi entre la TOE et un site distant dans le cadre d'un canal sûr.

FIA_UAU.6 précise que la TOE ne fournit aucune donnée à l'utilisateur (administrateur sécurité ou superviseur sécurité) tant qu'il n'est pas authentifié.

OT_échange_intégrité

FCO_ETC.1 (AMP) et **FCO_ITC.1** précisent que la TOE doit s'assurer d'une authentification mutuelle entre la TOE et le site distant préalablement à tout échange.

FCO_IID.1 précise que la TOE contrôle l'intégrité des données d'administration ou de supervision importées depuis un site distant.

FCO_IED.1 (CS) précise que la TOE permet de contrôler l'intégrité des données d'administration ou de supervision exportées vers un site distant.

FIA_USB.1 (CS) définit l'établissement du lien entre la TOE et le site distant.

FIA_TOB.1 (CS) et **FIA_TOB.2 (CS)** précisent les conditions de rupture du lien établi entre la TOE et un site distant dans le cadre d'un canal sûr.

OT_échange_confidentialité

FCO_ETC.1 (AMP) et **FCO_ITC.1** précisent que la TOE doit s'assurer d'une authentification mutuelle entre la TOE et le site distant préalablement à tout échange.

FCO_CID.1 précise que la TOE assure la confidentialité des données d'administration ou de supervision importées depuis un site distant.

FCO_CED.1 précise que la TOE assure la confidentialité des données d'administration ou de supervision exportées vers un site distant.

FIA_USB.1 (CS) définit l'établissement du lien entre la TOE et le site distant.

FIA_TOB.1 (CS) et **FIA_TOB.2 (CS)** précisent les conditions de rupture du lien établi entre la TOE et un site distant dans le cadre d'un canal sûr.

OT_échange_rejeu

FCO_ETC.1 (AMP) et **FCO_ITC.1** précisent que la TOE doit s'assurer d'une authentification mutuelle entre la TOE et le site distant préalablement à tout échange.

FCO_IED.1 (CS) précise que la TOE permet de contrôler l'intégrité des données d'administration ou de supervision exportées vers un site distant.

FCO_IID.1 précise que la TOE contrôle l'intégrité des données d'administration ou de supervision importées depuis un site distant.

FIA_USB.1 (CS) définit l'établissement du lien entre la TOE et le site distant.

FIA_TOB.1 (CS) et **FIA_TOB.2 (CS)** précisent les conditions de rupture du lien établi entre la TOE et un site distant dans le cadre d'un canal sûr.

OT_audit_flux

FAU_GEN.2 précise quels sont les événements audités et le contenu des messages d'audit.

OT_audit_exploitation

FAU_GEN.2 précise quels sont les événements audités et le contenu des messages d'audit.

FDP_ACC.1 (FI) précise les règles permettant aux utilisateurs autorisés de modifier les paramètres de l'audit et de la supervision dont la granularité de l'audit.

OT_alerte_détection

FAU_SAA.3 précise quels sont les événements considérés par la TOE comme des violations potentielles de la sécurité et qui doivent conduire à l'émission d'une alerte.

FIA_AFL.1 précise les conditions de notification par la TOE des erreurs de connexion des utilisateurs.

FPT_RSA.1 (RES) génère une alerte en cas de tentative de saturation de la TOE par des accès distants.

OT_alerte_réaction

FAU_ARP.1 précise que la TOE met en oeuvre automatiquement les actions définies par l'administrateur sécurité en cas de détection d'une violation de la sécurité.

FIA_AFL.1 précise les conditions de traitement par la TOE des erreurs de connexion des utilisateurs.

FPT_RSA.1 (RES) assure une protection contre les tentatives de saturation de la TOE par des accès distants.

OT_intégrité

FPT_TST.2 précise que l'intégrité de la TOE est contrôlée lors de son démarrage.

OT_fonctionnement

FPT_TST.1 précise que la TOE teste son fonctionnement lors de son démarrage, périodiquement ou à la demande d'un utilisateur autorisé.

OT_crypto

FIA_QAD.1, **FIA_QAD.2**, **FIA_UAU.1 (CS)** et **FIA_SUA.1** appliquent les règles définies par ce document.

De même que **FCO_CED.1**, **FCO_CID.1**, **FCO_IED.1 (CS)** et **FCO_IID.1**

5.2.2 Couverture des objectifs de sécurité pour l'environnement de développement

OD_EAL

Les exigences requises pour une qualification au niveau standard sont précisées dans la section 4.4 (cf. Tableau 6 : exigences pour une qualification au niveau standard d'une ST).

Elles sont complétées par les exigences requises pour l'évaluation d'un profil de protection (cf. Tableau 7 : exigences pour l'évaluation d'un profil de protection).

5.3 Dépendances

Les dépendances pour les composants fonctionnels sont les suivantes :

Composants	Dépendances	
FDP_ACC.1 (FRS)	FDP_ISA.1	Ce composant fait partie des composants retenus.
FDP_ACC.1 (FRE)	FDP_ISA.1	Ce composant fait partie des composants retenus.
FDP_ACC.1 (FAS)	FDP_ISA.1	Ce composant fait partie des composants retenus.
FIA_TBR.1 (FAS)	FIA_USB.1 (PL)	Ce composant fait partie des composants retenus.
FCO_ETC.1 (FAE)	Aucunes	
FIA_UID.2 (PL)	FIA_USB.1 (PL)	Ce composant fait partie des composants retenus.
FIA_USB.1 (PL)	Aucunes	
FIA_TOB.2 (PL)	FIA_USB.1 (PL)	Ce composant fait partie des composants retenus.
FIA_UID.1 (PD)	FIA_USB.1 (PD)	Ce composant fait partie des composants retenus.
FIA_USB.1 (PD)	Aucunes	
FIA_TOB.2 (PD)	FIA_USB.1 (PD)	Ce composant fait partie des composants retenus.
FIA_URE.2	FDP_ACC.1 (FI)	Ce composant fait partie des composants retenus.
FIA_QAD.1	FIA_URE.2 FIA_USB.1 (UL) FIA_USB.1 (UD)	Ces composants font partie des composants retenus.
FIA_QAD.2	FIA_URE.2 FIA_USB.1 (UL) FIA_USB.1 (UD)	Ces composants font partie des composants retenus.
FIA_UID.2 (UL)	FIA_USB.1 (UL)	Ce composant fait partie des composants retenus.
FIA_UID.2 (UD)	FIA_USB.1 (UD)	Ce composant fait partie des composants retenus.
FIA_UAU.1 (UL)	FIA_UID.2 (UL) FIA_URE.2	Ces composants font partie des composants retenus.
FIA_UAU.1 (UD)	FIA_UID.2 (UD) FIA_URE.2	Ces composants font partie des composants retenus.

Composants	Dépendances	
FIA_UAU.6	FIA_UAU.1 (UL) FIA_UAU.1 (UD)	Ces composants font partie des composants retenus.
FIA_AFL.1	FIA_UAU.1 (UL) FIA_UAU.1 (UD)	Ces composants font partie des composants retenus.
FIA_TBR.1 (UL)	FIA_USB.1 (UL)	Ce composant fait partie des composants retenus.
FIA_TBR.1 (UD)	FIA_USB.1 (UD)	Ce composant fait partie des composants retenus.
FIA_USB.1 (UL)	Aucunes	
FIA_USB.1 (UD)	Aucunes	
FIA_TOB.1 (UD)	FIA_USB.1 (UD)	Ce composant fait partie des composants retenus.
FIA_TOB.2 (UL)	FIA_USB.1 (UL)	Ce composant fait partie des composants retenus.
FIA_TOB.2 (UD)	FIA_USB.1 (UD)	Ce composant fait partie des composants retenus.
FDP_ACC.1 (FI)	FDP_ISA.1	Ce composant fait partie des composants retenus.
FDP_ISA.1	FDP_ACC.1 (FI) FDP_ACC.1 (FAS) FDP_ACC.1 (FRE) FDP_ACC.1 (FRS)	Ces composants font partie des composants retenus.
FDP_MSA.1	FDP_ACC.1 (FI) FDP_ACC.1 (FAS) FDP_ACC.1 (FRE) FDP_ACC.1 (FRS)	Ces composants font partie des composants retenus.
FPT_RIP.2	Aucunes	
FIA_UID.2 (CS)	FIA_USB.1 (CS)	Ce composant fait partie des composants retenus.
FIA_UAU.1 (CS)	FIA_UID.2 (CS) FIA_URE.2	Ces composants font partie des composants retenus.
FIA_SUA.1	FIA_USB.1 (CS)	Ce composant fait partie des composants retenus.
FIA_USB.1 (CS)	Aucunes	
FIA_TOB.1 (CS)	FIA_USB.1 (CS)	Ce composant fait partie des composants retenus.
FIA_TOB.2 (CS)	FIA_USB.1 (CS)	Ce composant fait partie des composants retenus.
FCO_ETC.1 (AMP)	Aucunes	
FCO_ITC.1	Aucunes	
FCO_CED.1	Aucunes	
FCO_CID.1	Aucunes	
FCO_IED.1 (CS)	Aucunes	
FCO_IID.1	Aucunes	
FCO_IED.1 (AUD)	Aucunes	
FAU_GEN.2	FDP_ACC.1 (FI) FDP_ACC.1 (FAS) FDP_ACC.1 (FRE) FDP_ACC.1 (FRS) FPT_RSA.1 (AUD) FMI_TIM.1	Ce composant fait partie des composants retenus. Ce composant fait partie des composants retenus. Ce composant fait partie des composants retenus. Ce composant fait partie des composants retenus. Ce composant fait partie des composants retenus. Ce composant n'est pas retenu mais La TOE obtient les données correspondantes du système d'exploitation qui assure la fonction d'horodatage.
FAU_SAA.3	FAU_GEN.1	Le composant FAU_GEN.2 hiérarchique à FAU_GEN.1 fait partie des composants retenus.
FAU_ARP.1	FAU_SAA.1	Le composant FAU_SAA.3 hiérarchique à FAU_SAA.1 fait partie des composants retenus.
FPT_RSA.1 (AUD)	Aucunes	
FPT_TST.1	Aucunes	
FPT_TST.2	Aucunes	
FPT_RSA.1 (RES)	Aucunes	

Composants	Dépendances	
FMI_CHO.1	Aucunes	

Tableau 10 : dépendances des composants fonctionnels

5.4 Conformité à un PP

Sans objet.

5.5 Composants étendus

Sans objet.

Annexe A Compléments de description de la TOE et de son environnement

A.1 Architecture de la TOE

Le schéma ci-après est un exemple possible d'architecture pour un PFP :

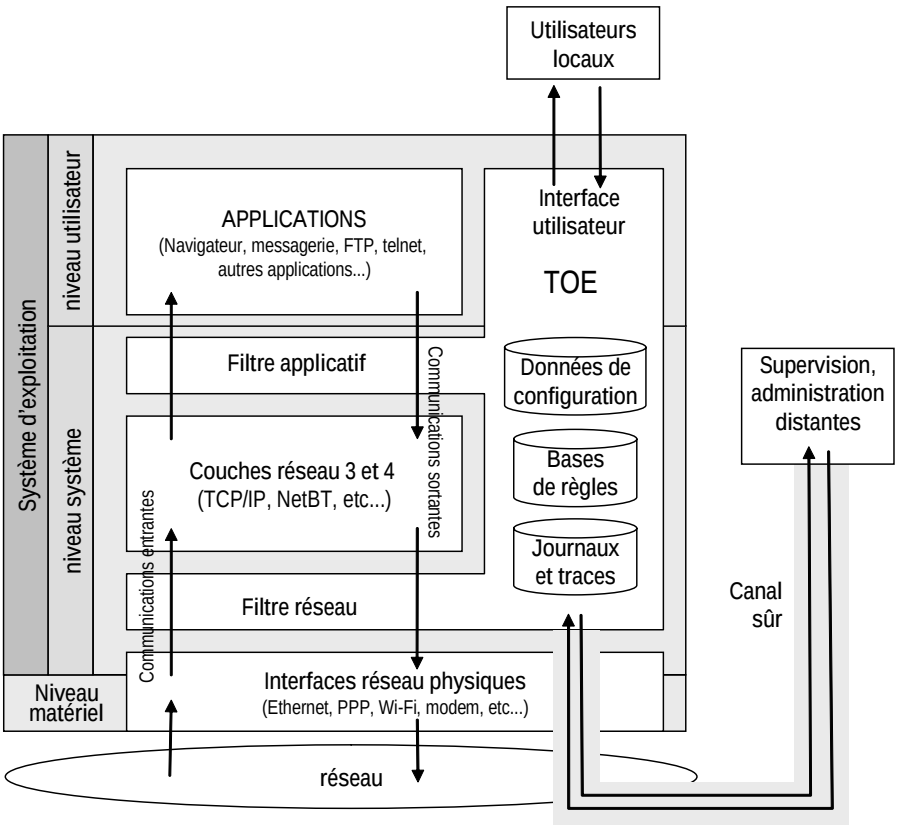

Figure 3 : schéma d'architecture de la TOE

La TOE réalise des échanges avec son environnement au travers des interfaces suivantes :

- Une interface « système » qui permet les interactions entre la TOE et les programmes du poste (système d'exploitation, autres programmes).
- Une interface « réseau » utilisée par les administrateurs et les superviseurs connectés à distance.
- Une « IHM locale » utilisée par les administrateurs, les superviseurs ou les usagers connectés localement sur le poste.

Les interfaces utilisées à titre « fonctionnel » ne sont pas indiquées dans cette liste.

Les ST conformes à ce PP devront préciser si la TOE fournit des drivers spécifiques utilisables à la place de ceux disponibles sur le poste.

A.2 Périmètre physique de la TOE

Le périmètre physique de la TOE comprend :

- Le kit d'installation de la TOE.
- La documentation associée.

A.3 Périmètre logique de la TOE

Le périmètre logique de la TOE comprend les composants suivants :

- Le ou les logiciels composant la TOE.
- Les paramètres d'administration de la TOE.
- Les règles de filtrage utilisées par la TOE.
- Les données de supervision, les alarmes et les journaux.

A.4 Rôles fonctionnels

Les différents rôles fonctionnels liés au fonctionnement du poste et de la TOE sont :

- L'agent (ou l'officier) de sécurité.
- L'administrateur système, réseau et bureautique.
- Le superviseur système.
- L'administrateur sécurité.
- Le superviseur sécurité.
- L'usager.

Nota : les rôles d'administration ou de supervision reconnus par la TOE et ceux reconnus par la machine hôte peuvent être indépendants. En particulier, un administrateur de la TOE n'est pas forcément administrateur de la machine hôte.

A.4.1 Rôles connus de la TOE

Les titulaires de ces rôles disposent d'un accès (local ou distant selon les cas) à la TOE pour remplir leur mission ou utiliser les droits dont ils disposent. Les rôles peuvent être affectés à des personnes différentes ou pas en fonction de la politique de sécurité choisie par l'organisation.

Ces rôles sont définis dans la section 2.2 de ce document.

A.4.2 Autres rôles

Les titulaires ces rôles n'ont pas besoin d'un accès à la TOE pour remplir leur mission.

Agent (ou officier) de sécurité

L'agent (ou l'officier) de sécurité définit la politique de filtrage qui doit être mise en oeuvre

par les administrateurs. Dans un contexte centralisé, il peut être responsable des équipes chargées de la supervision ou de l'administration de la sécurité.

Administrateur système

L'administrateur système est responsable de l'installation de la TOE en tant qu'application sur le poste de travail, du paramétrage et de l'administration du poste au niveau système et réseau. Il utilise pour remplir sa mission un accès local ou distant.

Superviseur système

Le superviseur système contrôle et audite l'administration système et réseau des postes de travail.

A.5 Fonctionnalités de la TOE

A.5.1 Services fournis par la TOE

A.5.1.1 Filtrage des communications

L'objectif principal du filtrage des communications est d'assurer un filtrage des flux au niveau de la pile protocolaire TCP/IP. Ce filtrage prend en compte les protocoles standard de la couche réseau (IP, ICMP), de la couche transport (TCP, UDP) et les protocoles standard des couches applicatives (5, 6 et 7).

La prise en compte des protocoles propriétaires non IP (NetBT par exemple) n'est pas l'objet du PP. Les ST conformes à ce PP devront indiquer le cas échéant les protocoles non IP pris en compte.

Le filtrage des communications met en oeuvre les filtrages suivants :

- Un filtrage basé sur l'analyse protocolaire des flux (conformité aux règles de filtrage définies à partir de critères tels que protocole, adresse source ou destination, port source ou destination, sens entrant ou sortant, adresse MAC, interface utilisée). Ce filtrage prend en compte le filtrage contextuel ou comportemental[7].
- Un filtrage basé sur l'analyse des applications communicantes (identification, lien entre programme et protocole).

Le filtrage doit aussi prendre en compte l'environnement réseau (connexion dans ou hors de l'entreprise).

Niveaux de filtrage :

La TOE offre trois niveaux de filtrage : global, utilisateur, adapté.

Le filtrage **global** est appliqué dès le démarrage du poste qu'un utilisateur soit connecté sur le poste ou non.

[7] Par filtrage contextuel ou comportemental, on entend la capacité qu'a la TOE de filtrer un paquet en fonctions des paquets déjà reçus ou émis.

Ce filtrage global est configurable lors de l'installation du PFP, modifiable et sous le contrôle de l'administrateur sécurité.

Un filtrage **utilisateur** qui est spécifique à un usager (ou à un groupe d'usagers). Il est appliqué dès que cet usager (ou tout usager du groupe) se connecte sur le poste.

Ce filtrage est sous le contrôle de l'administrateur sécurité qui peut déléguer à cet usager la possibilité de modifier tout ou partie de ce filtrage.

Un filtrage **adapté** qui est spécifique à un usager (ou à un groupe d'usager). Ce filtrage est généré par un mécanisme d'apprentissage qui permet à l'usager de construire une politique de filtrage adaptée à ses besoins par la validation des connexions « au fil de l'eau » au fur et à mesure de l'utilisation du poste.

Ce mécanisme permet une configuration intuitive du PFP, en évitant de présenter à l'usager des notions de sécurité ou de réseau complexes. Il limite les erreurs de configuration. Ce filtrage doit rester cohérent avec les politiques de filtrage créées par l'administrateur.

Le mécanisme d'apprentissage peut être activé ou désactivé par un administrateur.

Ces trois notions peuvent être représentées graphiquement comme suit :

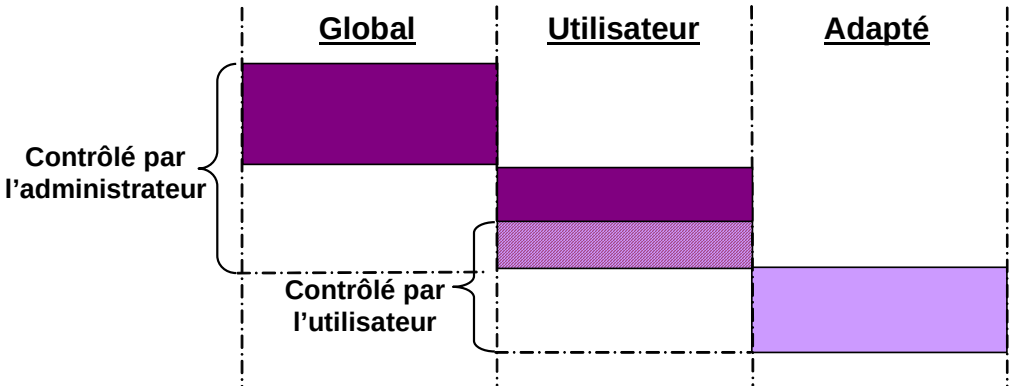

Figure 4 : niveaux de filtrage

A.5.1.2 Contrôle d'intégrité des applications

En support de la fonction de filtrage, le PFP permet de contrôler l'intégrité des applications communicantes.

Ce contrôle d'intégrité s'appuie sur des motifs d'intégrité qui permettent de détecter toute altération d'une application.

Les mécanismes utilisés pour ce contrôle d'intégrité des applications ne sont pas l'objet du PP. Ils devront être décrits dans les ST conformes à ce PP.

A.5.1.3 Protection contre les attaques

La TOE a la possibilité de réagir pour contrer certaines attaques, de type déni de service ou saturation, qui visent des ressources du poste.

L'administrateur sécurité a la possibilité de paramétrer les actions que la TOE devra prendre en réponse à ces attaques (par exemple, l'émission d'une alerte ou le blocage des flux).

A.5.2 Services nécessaires au bon fonctionnement de la TOE

Les services nécessaires au bon fonctionnement de la TOE sont l'administration et la supervision. Ces services peuvent être partagés entre différents rôles fonctionnels (cf. § 2.4.4).

A.5.2.1 Administration

L'administration du PFP peut être centralisée (par exemple quand le poste est connecté au réseau local de l'entreprise) ou locale (par exemple quand le poste est utilisé hors de l'entreprise ou lors des installations).

Elle comprend principalement la gestion des paramètres et des règles de filtrage. Elle concerne également la désactivation/réactivation de services de la TOE.

L'accès au service d'administration nécessite la possession d'un rôle spécifique qui doit être alloué aux personnes chargées de ce service.

Pour couvrir les différents modes d'organisation et de fonctionnement, l'administration du PFP doit pouvoir être effectuée :

- Par un administrateur appliquant la politique de l'entreprise, opérant localement ou de manière centralisée, sans contrôle de la part de l'usager.
- Par l'usager seul qui définit lui-même ses propres règles de filtrage.
- De manière collaborative entre l'administrateur qui définit des règles de base et l'usager qui les affine, par exemple selon un modèle d'apprentissage au fil de l'eau, en fonction des besoins de connexion des applications.

La possibilité pour l'usager de modifier la politique de sécurité est configurable par l'administrateur, depuis une liberté complète jusqu'à l'impossibilité totale de modifier la politique de sécurité.

Visibilité des paramètres de configuration et des règles de filtrage :

L'administrateur accède à l'intégralité de la configuration de la TOE, en particulier à l'ensemble des règles de filtrage et des paramètres propres aux flux analysés, y compris les règles et paramètres techniques qui pourraient être occultés à l'usager.

Un usager peut accéder aux règles de filtrage (de niveau utilisateur ou adapté) qui sont spécifique à cet usager. Cet accès doit être configurable par l'administrateur sécurité.

A.5.2.2 Supervision et journalisation

La supervision correspond à la capacité de visualiser des informations (journaux d'audit et messages d'audit, alertes, paramètres de supervision) depuis un site distant ou sur le poste. Elle doit pouvoir interopérer avec l'administration pour réagir à une alerte par exemple.

La journalisation correspond à l'enregistrement d'événements, critiques ou non critiques, dans un journal consultable en différé.

L'accès au service de supervision nécessite la possession d'un rôle spécifique qui doit être alloué aux personnes chargées de ce service.

Les informations enregistrées ou remontées peuvent être exploitées localement par l'usager, ou traitées par une personne responsable de la supervision. Une situation intermédiaire existe, où l'usager et le superviseur peuvent collaborer à l'exploitation des informations de supervision, des alarmes et des journaux.

La TOE permet de tracer :

- Les flux analysés et filtrés.
- Les opérations d'administration locales ou distantes.
- Les alertes générées sur détection de tentatives d'attaques.

L'exploitation des informations journalisées est paramétrable de manière à limiter les flux remontés vers l'entité de supervision ou présentés à l'utilisateur autorisé.

Le niveau des alertes remontées par la TOE peut être configuré de manière à limiter au nécessaire la quantité d'information.

La remontée des alarmes est configurable en fonction du contexte de la connexion (dans ou hors de l'entreprise) pour une information de l'usager ou du superviseur.

Un mécanisme peut permettre de réaliser le transfert des informations de supervision lorsque le poste est connecté au centre de supervision (remontée en différé pour les postes nomades).

A.5.3 Services de sécurisation de la TOE

A.5.3.1 Protections des fonctions d'administration et de supervision

La TOE dispose d'un mécanisme de contrôle d'accès aux fonctions qui relèvent de l'administration ou de la supervision : gestion des paramètres, des filtres, des journaux, arrêt de la TOE.

Ce mécanisme de contrôle d'accès s'appuie notamment sur l'utilisation de rôles, alloués aux utilisateurs autorisés.

Protection de l'administration et de la supervision distante :

La TOE identifie et authentifie les utilisateurs qui se connectent à l'interface d'administration ou de supervision et leur attribue un rôle en fonction de leur identité.

La TOE assure l'authenticité et l'intégrité des flux qu'elle transmet. Elle peut aussi assurer la confidentialité de ces flux. Elle contrôle l'intégrité et l'authenticité des flux qu'elle reçoit.

Elle dispose d'un mécanisme de protection contre les attaques par saturation visant les fonctions d'administration ou de supervision.

Protection de l'administration et de la supervision locale :

La TOE identifie et authentifie les utilisateurs qui se connectent à l'interface d'administration ou de supervision et leur attribue un rôle en fonction de leur identité.

A.5.3.2 Protection des journaux

La TOE assure un contrôle d'accès aux journaux en fonction des rôles possédés par l'utilisateur.

A.5.3.3 Protection de la TOE

La TOE doit :

- Contrôler l'intégrité de certains de ses composants et signaler toute perte d'intégrité détectée.
- Informer l'utilisateur (usager ou superviseur) de son état (actif ou inactif).

A.6 Environnement d'exploitation de la TOE

L'application pare-feu personnel est destinée à être installée sur un poste de travail équipé d'un système d'exploitation et disposant d'une ou de plusieurs interfaces réseau (Ethernet, WIFI, RTC, IRDA, USB...).

Ce poste de travail peut être partagé entre plusieurs utilisateurs ayant chacun un accès (compte utilisateur + mot de passe associé) personnel. Il peut être connecté directement au réseau de l'entreprise ou utilisé comme poste nomade.

Le nomadisme multiplie les contextes d'utilisation et les environnements réseau :

- Périodes : utilisation possible quels que soient le jour et l'heure.
- Conditions d'accès : accès ADSL ou RTC (FAI, Cybercafé, Hôtel), accès WIFI public (gare, train, aéroport...).

Les ST conformes à ce PP devront décrire précisément l'environnement d'exploitation. Elles devront en particulier indiquer les contraintes à respecter au niveau du poste : version du système d'exploitation, drivers à utiliser, ordre d'installation des logiciels...

A.7 Plate-forme d'évaluation de la TOE

La plate-forme d'évaluation de la TOE doit être représentative des cadres habituels d'utilisation, d'administration et de supervision de la TOE.

Elle doit comprendre au minimum :

- Le poste de travail hébergeant la TOE. Ce poste doit avoir au moins une interface réseau. Les drivers utilisés pour piloter les interfaces réseaux devront être ceux fournis avec la TOE ou recommandés par la documentation TOE.
- Un second poste de travail interconnecté avec le poste hébergeant la TOE. Ce poste permet de réaliser des échanges de données avec la TOE et d'évaluer la fonction de filtrage de la TOE.
- Un troisième poste de travail interconnecté avec le poste hébergeant la TOE. Ce

poste permet d'évaluer les fonctions d'administration et de supervision à distance.

- Un réseau auquel sont connectés ces postes qui permette de simuler les configurations réseau de l'environnement d'exploitation de la TOE.

Les ST conformes à ce PP devront décrire précisément la plate-forme à utiliser.

A.8 Fonctionnalités complémentaires possibles pour le PFP

Cette section présente des fonctionnalités complémentaires qui pourront être proposées par les industriels en réponses à des besoins spécifiques des usagers. Ces fonctionnalités ne sont pas prises en compte dans le cadre du présent PP mais pourront être intégrées dans les ST conformes à ce PP en développant l'analyse de sécurité associée.

Filtrage :

Les possibilités de filtrage suivantes n'ont pas été retenues :

- Filtrage horaire, filtrage d'URL, filtrage de contenu,
- Contrôle du téléchargement de fichiers.

Le filtrage est en outre limité aux connexions avec des systèmes hôtes : une connexion entre le poste et un disque amovible via un port USB ne sera pas prise en compte (alors qu'une connexion entre ce poste et un autre poste via ce même port USB et un modem sera prise en compte).

Désactivation temporaire du filtrage par l'usager :

La désactivation temporaire du filtrage par l'usager consiste à la faculté, offerte à l'usager, de désactiver temporairement des règles de filtrage afin de lui permettre de réaliser des communications qui sont, en temps normal, bloquées.

Cette fonction doit être sous le contrôle de l'administrateur sécurité qui doit pouvoir en autoriser la mise en oeuvre. La désactivation temporaire du filtrage par l'usager doit nécessiter l'utilisation d'un code et doit être auditée, de même que les communications réalisées dans ce mode de fonctionnement. Les règles désactivées par ce mécanisme doivent pouvoir être réactivées automatiquement à la fin de son utilisation.

Cette fonction peut aussi être mise en oeuvre par l'intermédiaire de mesures d'ordre organisationnel.

Mode d'apprentissage global :

Ce mode d'apprentissage permet de générer dynamiquement, en fonction des habitudes de connexion des différents usagers, une politique de filtrage pour le poste de travail qui pourra être affinée a posteriori par les administrateurs.

Confidentialité des processus de la TOE :

La confidentialité des processus de la TOE permet de masquer l'existence de la TOE sur un poste vis-à-vis des usagers ou d'attaquants.

Respect de la réglementation :

Par les moyens de protection des données qu'elle apporte, la TOE contribue au respect des lois et réglementations relatives à la protection des données sensibles à caractère personnel ou privé (cf. [L78]).

Annexe B Définitions et acronymes

B.1 Acronymes

PFP Pare-feu personnel

PP Profil de protection (*protection profile*)

ST Cible de sécurité (*security target*)

TOE Cible d'évaluation (*target of evaluation*)

TSF Fonctions de sécurité de la TOE (*TOE security functions*)

TSP Politique de sécurité de la TOE (*TOE security policy*)

B.2 Conventions utilisées

La liste ci-après fournit les racines utilisées pour les différents éléments.

Racine	Éléments désignés par cette racine
T_	Menaces (*threat*) concernant la TOE et l'environnement opérationnel de la TOE
TD_	Menaces (*threat*) concernant l'environnement de développement de la TOE
OSP_	Politiques de sécurité organisationnelles (*organisational security policy*)
A_	Hypothèses (*Assessment*)
OT_	Objectifs de sécurité pour la TOE
OE_	Objectifs de sécurité pour l'environnement opérationnel
OD_	Objectifs de sécurité pour l'environnement de développement
S_	Sujets de la TOE
SA_	Attributs de sécurité (*security attributes*)
D_	Biens sensibles et objets de la TOE
U_	Utilisateurs (programmes ou personnes physiques) interagissant avec la TOE

B.3 Définitions

Cible de sécurité (ST)

Document servant de référence à l'évaluation de la cible d'évaluation : le certificat délivré par la DCSSI attestera de la conformité du produit et de sa documentation aux exigences (fonctionnelles et d'assurance) formulées dans la cible de sécurité.

Cible d'évaluation (TOE)

Le produit à évaluer et sa documentation associée

Fonction de sécurité de la TOE (TSF)

Ensemble constitué par tous les éléments matériels, logiciels et microprogrammes de

la TOE sur lequel on doit s'appuyer pour l'application correcte de la TSP.

Pile protocolaire TCP/IP

Par « pile protocolaire TCP/IP », on entend les protocoles standard de la couche réseau (IP, ICMP), de la couche transport (TCP, UDP) et les protocoles standard des couches applicatives (5, 6 et 7).

Politique de sécurité de la TOE (TSP)

Ensemble de règles qui précisent comment gérer, protéger et distribuer les biens à l'intérieur d'une TOE.

Interprétation

Complément (clarification, correction, ou additif) aux Critères Communs ; la liste des interprétations est disponible sur le site : www.commoncriteriaportal.org

Annexe C Références

C.1 Références normatives

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, June 2005, Version 3.0, Revision 2, CCMB-2005-07-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, June 2005, Version 3.0, Revision 2, CCMB-2005-07-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, June 2005, Version 3.0, Revision 2, CCMB-2005-07-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, June 2005, Version 3.0, Revision 2, CCMB-2005-07-004.

[QUALIF_STD] Processus de qualification d'un produit de sécurité – Niveau *standard*. Version 1.0, juillet 2003. DCSSI, 001591/SGDN/DCSSI/SDR.

[CRYPT-STD] Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse *standard*. Version 1.02, 19/11/04. DCSSI, 2791/SGDN/DCSSI/SDS/Crypto.

C.2 Lois et règlements

[L78] Loi modifiée du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

C.3 Autres documents

[EBIOS] Méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité). Version 2 du 5 février 2004