

RESEAU DOMESTIQUE
PROFIL DE PROTECTION

V. Guilbeau, A. Le Baron, A. Puy & A. Tisserant

17 avril 2003

Table des matières

1	Introduction	4
1.1	Identification du profil de protection	4
1.2	Vue d'ensemble du profil de protection	4
2	Description de la cible d'évaluation	5
2.1	Définition	5
2.2	Parties	5
2.3	Flux	6
2.4	Interfaces	7
3	Environnement de sécurité	8
3.1	Sujets	8
3.1.1	Sujets physiques	8
3.1.2	Sujets exécutables	8
3.1.3	Rôles	8
3.2	Objets	9
3.2.1	Objets matériels	9
3.2.2	Objets immatériels	9
3.3	Opérations - Transactions	10
3.4	Politique de sécurité	10
3.4.1	Sujets - Objets matériels / Transactions	10
3.4.2	Sujets - Objets immatériels / Transactions	10
3.4.3	Filtrage des données	12
3.5	Hypothèses d'utilisation de la TOE	12
3.6	Menaces	13
3.6.1	Menaces externes	13
3.6.2	Menaces internes	14
3.7	Politiques de sécurité organisationnelles	15
4	Objectifs de sécurité	17
4.1	Objectifs de sécurité des technologies de l'information	17
4.2	Objectifs de sécurité de l'environnement	18

5	Exigences de sécurité	20
5.1	Exigences fonctionnelles	20
5.2	Texte des exigences fonctionnelles	20
5.2.1	Classe FAU : Audit de sécurité	20
5.2.2	Classe FDP : Protection des données de l'utilisateur	25
5.2.3	Classe FIA : Identification et Authentification	27
5.2.4	Classe FMT : Administration de la sécurité	28
5.2.5	Classe FTA : Accès à la TOE	29
5.3	Exigences d'assurance	31
6	Précisions	32
7	Argumentaire	33
7.1	Objectifs de sécurité de la TOE	33
7.1.1	Couverture des hypothèses	33
7.1.2	Couverture des menaces	34
7.1.3	Couverture des politiques de sécurité organisationnelles	37
7.1.4	Complétudes des objectifs de sécurité	38
7.1.5	Complétudes des objectifs de l'environnement	42
7.1.6	Récapitulatif des relations Menaces-Politiques-Objectifs- Hypothèses	44
7.2	Exigences fonctionnelles de la TOE	45
7.2.1	Argumentaire pour la classe FAU : Audit de sécurité	45
7.2.2	Argumentaire pour la classe FDP : Protection des don- nées de l'utilisateur	46
7.2.3	Argumentaire pour la classe FIA : Identification et authentification	47
7.2.4	Argumentaire pour la classe FMT : Administration de la sécurité	48
7.2.5	Argumentaire pour la classe FTA : Accès à la TOE	49
7.3	Satisfaction des objectifs de sécurité	50
7.4	Argumentaire des exigences d'assurance	50
7.5	Cohésion des exigences de sécurité	50

Table des figures

1	Exemple de réseau domestique dans un domicile particulier . . .	5
2	Les flux en présence	6
3	Objets immatériels type OS ou logiciel	11
4	Objets immatériels type données	11
5	Transactions autorisées entre sujets et objets immatériels . . .	11
6	Les utilisateurs de la TOE	15
7	Complétude des objectifs de sécurité et d'environnement . . .	44
8	Satisfaction des objectifs de sécurité	51

1 Introduction

1.1 Identification du profil de protection

Titre : Réseau Domestique - Mars 2003

Mots-Clés : réseau domestique, particuliers, PME

Enregistrement : non enregistré

Références à d'autres profils de protection : aucune

1.2 Vue d'ensemble du profil de protection

Ce profil de protection exprime les objectifs de sécurité ainsi que les exigences fonctionnelles d'assurance pour une cible d'évaluation (nommée ci-après TOE) constituée d'un réseau domestique.

Par la dénomination « réseau domestique », on entend ici un réseau de taille restreinte, tels que ceux que l'on peut rencontrer chez des particuliers ou encore dans certaines PME. Ces réseaux se développent rapidement, notamment du fait de la multiplication des périphériques qui peuvent s'y connecter et de l'émergence de techniques d'accès à hauts débits telles qu'ADSL.

Ce profil de protection a été établi en conformité avec les Critères Communs V2.1 (Août 1999).

2 Description de la cible d'évaluation

2.1 Définition

Un réseau domestique est constitué d'un nombre restreint d'ordinateurs ou autres périphériques reliés entre eux dans l'enceinte d'une propriété privée. Ils constituent ainsi un réseau interne, éventuellement connecté à un WAN.

Nous nous restreignons ici au cadre d'un réseau domestique répondant aux conditions suivantes :

- réseau interne situé dans le domicile d'un particulier, et propriété de ce dernier ;
- aucun protocole non filaire (802.11, HomeRF, Bluetooth, DECT...);
- réseau interne filaire quelconque (Ethernet, USB, ...);
- connexion ADSL pour l'accès à l'Internet *via* un modem relié à un seul routeur ;
- un seul point de connexion à l'Internet.

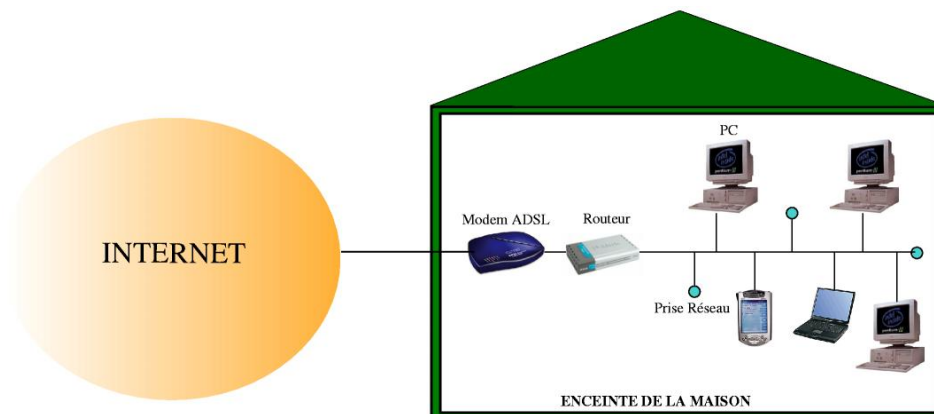


FIG. 1 – Exemple de réseau domestique dans un domicile particulier

2.2 Parties

Les parties en présence de la TOE sont :

- **La famille** logeant dans le domicile où est disposée la TOE, propriétaire de la TOE ;
- **Les personnes autorisées** à utiliser la TOE ;
- **Les personnes non autorisées** à utiliser la TOE.

2.3 Flux

Les flux en présence sont de trois types :

- **Flux internes** : flux circulant sur le réseau interne (entre les périphériques de la TOE) ;
- **Flux entrants** : flux provenant de l'extérieur vers le réseau interne ;
- **Flux sortants** : flux sortant du réseau interne vers l'extérieur.

On notera que les flux entrants et sortants peuvent être regroupés en deux catégories, suivant le mode de transmission qu'ils utilisent :

- **Flux internet** : flux empruntant nécessairement la connexion ADSL ;
- **Autres flux** : résultant de l'utilisation d'intermédiaires de stockage entre le réseau domestique et le monde extérieur (disquettes, ordinateur portable, cédéroms, appareils photos numériques...).

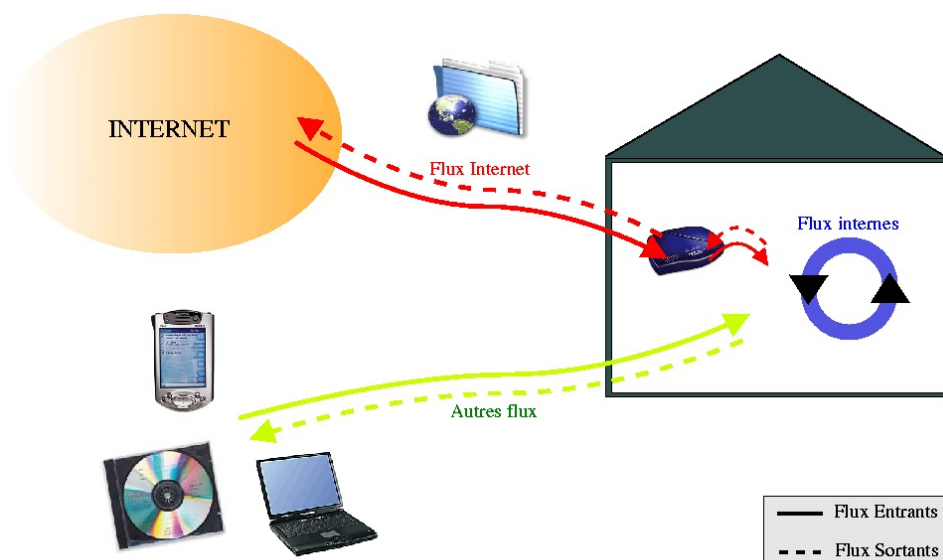


FIG. 2 – Les flux en présence

2.4 Interfaces

Les interfaces reliant la TOE au monde extérieur sont :

- **Les prises réseau**, disposées *intra muros* ;
- **Les périphériques** connectables à la TOE ;
- **La ligne téléphonique** à laquelle est reliée le modem ADSL.

3 Environnement de sécurité

3.1 Sujets

3.1.1 Sujets physiques

Les sujets physiques auxquels s'appliquent la politique de sécurité sont toutes les personnes ayant accès au réseau domestique. Il s'agit par exemple d'une famille constituée des deux parents et des enfants ainsi que des amis de la famille obtenant l'accès au réseau sur demande.

3.1.2 Sujets exécutables

Les principaux sujets exécutables sur lesquels peuvent agir les sujets physiques sont les suivants :

- **Le système d'exploitation** (type Linux par exemple) ainsi que **les applications d'administration associées**.
- **Les applications externes** : Ce sont celles qui peuvent communiquer avec l'extérieur de la TOE :
 - Clients mails (type Outlook) et messagerie (type ICQ)
 - Partage de fichiers en peer to peer (type Gnutella)
 - Navigateur internet
 - Client jeux vidéos en réseau
- **Les applications internes** : Ce sont celles qui ne peuvent pas communiquer avec l'extérieur de la TOE :
 - Les applications bureautiques et multimédia
 - Clients internes (de partage de fichiers et de jeux)

3.1.3 Rôles

On divise en trois types les rôles des sujets physiques ayant accès au réseau. Ces rôles seront repris dans la politique de sécurité organisationnelle (partie 3.7). Les rôles sont les suivants :

- **Administrateur** : ce rôle est tenu par un membre de la famille. Il est unique
- **Utilisateurs** : c'est le rôle tenu par les autres membres de la famille.

- Invité : toute personne n'ayant pas le rôle d'administrateur ou d'utilisateur se voit considéré comme invité (typiquement les amis de la famille) et ont des droits limités sur les objets.

3.2 Objets

3.2.1 Objets matériels

L'ensemble du matériel constituant la TOE :

- **Périphériques** connectables au réseau interne
 - Ordinateurs fixes et portables ;
 - Modem ADSL ;
 - Routeur, hubs, switches ;
 - Périphériques divers rattachables au réseau (caméra, imprimantes, ...).
- **Réseau filaire**
 - Câbles réseau ;
 - Prises Ethernet.

3.2.2 Objets immatériels

L'ensemble des données présentes dans la TOE :

- **Systèmes d'exploitation** utilisés par tous les périphériques connectables ;
- **Logiciels** correspondant aux applications externes définies précédemment.
- **Logiciels** correspondant aux applications internes définies précédemment.
- **Données personnelles** des utilisateurs (données privées, sensibles, dossiers de travail) ;
- **Données partagées** entre plusieurs utilisateurs de la TOE ;
- **Données publiques** à accès universel en lecture (partage de fichiers, . . .) ;

3.3 Opérations - Transactions

Les opérations réalisables sur les objets matériels au sein de la TOE sont les suivantes :

- **Mise hors service** : un utilisateur peut éteindre l'objet.
- **Mise en service** : un utilisateur peut mettre en service l'objet.
- **Connexion** : un utilisateur peut connecter l'objet au réseau interne.
- **Déconnexion** : un utilisateur peut déconnecter l'objet du réseau interne.

Les transactions possibles concernant les objets immatériels type système d'exploitation ou logiciel sont les suivantes :

- **Installation** : un utilisateur peut installer l'objet.
- **Exécution** : un utilisateur peut exécuter l'objet.
- **Modification** : un utilisateur peut modifier l'objet.
- **Destruction** : un utilisateur peut détruire l'objet.

Les transactions possibles concernant les objets immatériels type données sont les suivantes :

- **Listage** : un utilisateur peut connaître l'existence de la donnée.
- **Lecture** : un utilisateur peut visualiser le contenu de la donnée.
- **Écriture** : un utilisateur peut modifier le contenu de la donnée.
- **Destruction** : un utilisateur peut effacer la donnée.

3.4 Politique de sécurité

3.4.1 Sujets - Objets matériels / Transactions

Toutes les transactions sur les objets matériels sont réalisables par chacun des utilisateurs.

3.4.2 Sujets - Objets immatériels / Transactions

Les transactions possibles sur les objets immatériels sont notées de la manière suivante :

Installation	I
Éxecution	X
Modification	M
Destruction	D

FIG. 3 – Objets immatériels type OS ou logiciel

Listage	L
Lecture	R
Écriture	W
Destruction	D

FIG. 4 – Objets immatériels type données

Les droits des différents utilisateurs sur les objets immatériels sont décrits dans la figure 5. On considère les données privées et partagées autres que celles du sujet considéré, ce dernier ayant un accès total (LRWD) à ses données privées ainsi qu'aux données qu'il partage avec les autres sujet.

	Administrateur	Utilisateurs	Invité
Système d'exploitation	IXMD	X	X
Applications externes	IXMD	X	X
Applications internes	IXMD	IXMD	X
Données privées	-	-	-
Données partagées	LR	LR	-
Données publiques	LRWD	LRWD	LR

FIG. 5 – Transactions autorisées entre sujets et objets immatériels

Les droits des sujets exécutables sur les objets immatériels sont définis par les sujets physiques qui exécutent ces logiciels. Par exemple un logiciel multimédia aura les mêmes droits d'utilisation sur les fichiers multimédia que le sujet physique qui exécute le logiciel.

3.4.3 Filtrage des données

Les données transitant entre la TOE et Internet sont filtrées de la manière suivante :

- **Données sortantes**
 - Ne peuvent sortir de la TOE que des données en provenance des adresses MAC des objets matériels de la TOE, que ce soient les périphériques fixes de la TOE ou les périphériques se connectant via un compte invité.
- **Données rentrantes**
 - Ne peuvent rentrer dans la TOE que des données dont les ports de communication correspondent à ceux nécessaires aux applications externes autorisées.

3.5 Hypothèses d'utilisation de la TOE

H.USAGE :

La TOE est employée comme système d'information de la famille qui en est propriétaire. La connexion ADSL à l'Internet permet l'échange de données avec l'extérieur, de même que l'utilisation de périphériques de stockage mobiles.

H.UTILISATEURS :

La famille propriétaire de la TOE, ainsi que les utilisateurs qu'elle autorise, ne cherchent pas à compromettre la TOE volontairement.

H.VALEUR-BIENS-MATERIELS :

Les biens matériels sont évalués à leur valeur d'origine (incluant le prix d'achat, le coût d'installation...).

H.VALEUR-BIENS-IMMATERIELS :

Les biens immatériels sont supposés avoir une valeur non négligeable pour leurs propriétaires.

H.ACCES-DOMICILE :

Seules les personnes autorisées par au moins un membre de la famille propriétaire de la TOE peuvent obtenir un accès au domicile.

H.ACCES-PHYSIQUE-RESEAU-INTERNE :

Seules les personnes ayant accès au domicile ont un accès physique possible au réseau interne (prises réseau, périphériques...).

H.ACCES-INTERNET-ENTRANT :

La TOE est visible depuis l'extérieur, grâce à l'adresse IP affectée par le FAI au routeur relié au modem.

3.6 Menaces

3.6.1 Menaces externes

M.INTRUSION-PIRATE :

Un tiers obtient un accès illégal à la TOE. Cet accès résulte de l'utilisation de systèmes de détection de vulnérabilités automatisés, et n'est pas directement dirigé vers la TOE. Il ne nécessite par ailleurs que très peu d'expertise de la part de l'attaquant. Le tiers attaquant n'a pas de motivation particulière à viser cette TOE, et ne cherchera donc pas à tout prix à la pénétrer. Les biens mis en danger sont toutes les données immatérielles (logiciels, données, système), ainsi que le réseau interne (dénis de service).

M.INTRUSION-ESPION :

Un tiers mène une attaque ciblée pour obtenir un accès illégal à la TOE. Le choix précis de cette TOE répond à des motivations particulières, dans le cadre par exemple d'un espionnage industriel. Mener à bien ce genre d'attaque requiert une certaine expertise technique, et peut faire intervenir des systèmes de détection de vulnérabilités automatisés ciblés sur la TOE ainsi que des attaques nouvelles. Les biens visés sont ici les données immatérielles (données confidentielles, intégrité du système par installation de mouchards, ...) et éventuellement la disponibilité du réseau interne.

M.VIRUS :

Un virus ou tout autre logiciel malicieux s'introduit dans la TOE *via* la connexion Internet. Cette attaque n'est pas ciblée, et peut résulter en la corruption ou la destruction de données, et en la perturbation du fonctionnement de la TOE.

3.6.2 Menaces internes**M.NEGLIGENCE-MANIPULATION :**

Un utilisateur autorisé effectue une opération illicite portant atteinte à la TOE. Cet utilisateur n'a aucune motivation pour cette attaque, puisqu'elle est involontaire, ou du moins parce qu'il n'a pas conscience de son impact sur la TOE. Cette attaque peut prendre des formes distinctes :

- Mauvaise manipulation résultant en la corruption ou la destruction de données personnelles d'autrui ;
- Mise hors service d'un périphérique connectable à la TOE (modem ADSL, ordinateur,...).

Ces menaces ne nécessitent aucune expertise technique, et visent l'ensemble des biens à protéger de la TOE, y compris les données publiques sur lesquelles des restrictions peuvent être imposées (écriture, effacement).

M.NEGLIGENCE-INSTALLATION :

Un utilisateur autorisé installe un logiciel défectueux, vulnérable ou malicieux. L'attaquant n'a ici pas conscience de la dangerosité de son action. Tous les biens de la TOE peuvent être mis en danger, directement (destruction de données, mise hors service de périphériques) ou indirectement (création de nouvelles vulnérabilités exploitables).

3.7 Politiques de sécurité organisationnelles

P.ADMINISTRATEUR-UNIQUE :

Un et un seul membre de la famille se voit confier le titre d'administrateur de la TOE.

P.HIERARCHIE :

Les utilisateurs se répartissent comme indiqué figure 6.

P.MEMBRES :

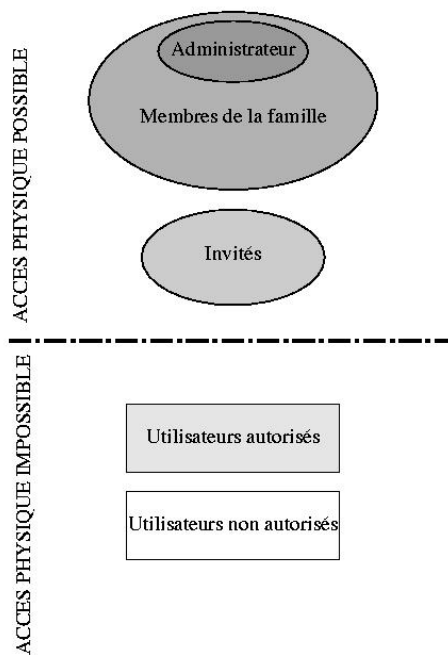


FIG. 6 – Les utilisateurs de la TOE

Les personnes vivant dans le domicile se voient attribuer le statut de membres de la famille, et sont reconnus comme tels par l'administrateur.

P.INVITES :

Les personnes pénétrant dans le domicile suite à l'autorisation d'un des membres de la famille au moins se voient attribuer le statut d'invités.

4 Objectifs de sécurité

4.1 Objectifs de sécurité des technologies de l'information

O.CONFIDENTIALITE-DONNEES-PRIVEES :

Les données privées ne sont consultables que par leur propriétaire.

O.CONFIDENTIALITE-DONNEES-PARTAGEES :

Une donnée partagée n'est consultable que par les utilisateurs d'un groupe d'utilisateurs précis associé à cette donnée et déterminé par l'administrateur. Les utilisateurs d'un tel groupe sont choisis parmi les invités ou les membres de la famille.

O.CONFIDENTIALITE-FLUX-INTERNES :

Les flux internes ne doivent pas sortir de l'environnement de la TOE.

O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE :

L'administrateur est unique et est authentifié par la TOE.

O.AUTHENTIFICATION-MEMBRES :

Les membres de la famille sont authentifiés personnellement par la TOE.

O.AUTHENTIFICATION-INVITES :

Quiconque a un accès physique et utilise la TOE sans authentification est un invité. Un membre de la famille pourra à ce titre être parfois considéré comme étant un invité.

O.INTEGRITE-DONNEES-PRIVEES :

Les données privées ne peuvent être modifiées que par leur propriétaire.

O.INTEGRITE-DONNEES-PARTAGEES :

Les données partagées ne peuvent être modifiées que par les utilisateurs qui peuvent les consulter.

O.INTEGRITE-DONNEES-PUBLIQUES :

Les données publiques ne peuvent en aucun cas être modifiées ou ajoutées par un utilisateur connecté *via* Internet. Seul l'administrateur peut les modifier ou les ajouter.

O.DISPONIBILITE :

L'ensemble des biens de la TOE (données, services, matériels) doit être disponible .

O.AUDIT :

La TOE doit proposer des moyens pour enregistrer et dater les événements, tout en identifiant leurs auteurs.

O.FILTRAGE :

La TOE exerce un contrôle des flux par filtrage, conformément à la politique de sécurité retenue pour le filtrage.

4.2 Objectifs de sécurité de l'environnement

O.USAGE :

La TOE est employée comme système d'information de la famille qui en est propriétaire.

O.UTILISATEURS :

La famille propriétaire de la TOE, ainsi que les utilisateurs qu'elle autorise, ne doivent pas compromettre la TOE volontairement.

O.ACCES-INTERNET-ENTRANT :

La TOE est visible depuis l'extérieur, grâce à l'adresse IP affectée par le FAI au routeur relié au modem.

O.VALEURS-BIENS :

Les biens matériels doivent être évalués à leur valeur d'origine.

O.VALEURS-BIENS-IMMATERIELS :

Les biens immatériels doivent se voir affecter une valeur non négligeable pour leurs propriétaires.

O.ENVIRONNEMENT :

Seules les personnes autorisées par au moins un membre de la famille propriétaire de la TOE peuvent obtenir un accès physique à la TOE.

5 Exigences de sécurité

5.1 Exigences fonctionnelles

Sigle	Description
FAU-ARP.1	Alarmes de sécurité
FAU-GEN.1	Génération de données d'audit
FAU-GEN.2	Lien avec l'identité de l'utilisateur
FAU-SAR.1	Revue d'audit
FAU-SAR.2	Revue d'audit restreinte
FAU-STG.1	Stockage de la trace d'audit
FAU-STG.4	Prévention des pertes de données d'audit
FDP-ACC.1	Contrôle d'accès partiel
FDP-ACF.1	Contrôle d'accès basé sur les attributs de sécurité
FDP-IFC.1	Politique de contrôle de flux
FDP-IFF.1	Attributs de sécurité simple
FIA-ATD.1	Définition des attributs de l'utilisateur
FIA-UAU.2	Authentification de l'utilisateur avant toute action
FIA-UID.2	Identification de l'utilisateur avant toute action
FMT-MOF.1	Administration du comportement des fonctions de sécurité
FMT-MSA.1	Administration des attributs de sécurité
FMT-MSA.2	Attributs de sécurité sûrs
FMT-MSA.3	Initialisation statique d'attribut
FMT-MTD.1	Administration des données de la TSF
FMT-SMR.1	Rôles de sécurité
FTA-SSL.1	Verrouillage de session, initié par la TSF
FTA-SSL.2	Verrouillage de session, initié par l'utilisateur
FTA-SSL.3	Clôture de session, initiée par la TSF
FTA-TAH.1	Historique des accès à la TOE

5.2 Texte des exigences fonctionnelles

5.2.1 Classe FAU : Audit de sécurité

FAU-ARP.1 Alarmes de sécurité

FAU-ARP.1.1 La TSF doit entreprendre [**les actions les moins perturbatrices**] dès la détection d'une violation potentielle de la sécurité.

Raffinement : *L'action la moins pénalisante correspond à la génération automatique d'une alarme. Le rédacteur de la cible de sécurité pourra ajouter des actions complémentaires à la génération de l'alarme.*

FAU-GEN.1 Génération de données d'audit

FAU-GEN.1.1 La TSF doit pouvoir générer un enregistrement d'audit des événements auditables suivants :

- Démarrage et arrêt des fonctions d'audit ;
- Tous les événements auditables pour le niveau d'audit [minimum, élémentaire, détaillé, non spécifié] ;
- Autres événements auditables définis spécifiquement

Raffinement : *Le tableau suivant liste tous les événements auditables. L'auteur de la cible de sécurité complétera éventuellement avec d'autres événements à auditer.*

Composant	Événements auditables
FAU-ARP.1	Actions entreprises à cause de violations imminentes de la sécurité.
FAU-GEN.1	-
FAU-GEN.2	-
FAU-SAR.1	Lecture d'informations à partir des enregistrements d'audit.
FAU-SAR.2	Essais infructueux de lecture d'informations à partir des enregistrements d'audit.
FAU-STG.1	-
FAU-STG.4	Actions entreprises à la suite d'une défaillance dans le stockage de l'audit.

Composant	Événements auditable
FDP-ACC.1	-
FDP-ACF.1	<p>Demandes réussies d'exécution d'une opération sur un objet couvert par la SFP ;</p> <p>Toutes les demandes d'exécution d'une opération sur un objet couvert par la SFP ;</p> <p>Les attributs de sécurité spécifiques utilisés pour vérifier un accès.</p>
FDP-IFC.1	-
FDP-IFF.1	<p>Décisions d'autoriser les flux d'information demandés ;</p> <p>Toutes les décisions relatives aux demandes de flux d'information ;</p> <p>Les attributs de sécurité spécifiques utilisés pour décider de la mise en œuvre d'un flux d'information ;</p> <p>Certains sous-ensembles spécifiques d'informations qui ont circulé conformément aux objectifs de la politique (e.g. audit de matériels en configuration dégradée).</p>
FIA-ATD.1	-
FIA-UAU.2	<p>Utilisation infructueuse du mécanisme d'authentification ;</p> <p>Toute utilisation du mécanisme d'authentification.</p>
FIA-UID.2	<p>Utilisation infructueuse du mécanisme d'identification de l'utilisateur, avec l'identité de l'utilisateur fournie ;</p> <p>Toute utilisation du mécanisme d'identification de l'utilisateur, avec l'identité de l'utilisateur fournie.</p>
FMT-MOF.1	Toutes les modifications dans le comportement des fonctions dans la TSF.
FMT-MSA.1	Toutes les modifications des valeurs des attributs de sécurité.
FMT-MSA.2	<p>Toutes les valeurs proposées et rejetées pour un attribut de sécurité ;</p> <p>Toutes les valeurs sûres proposées et acceptées pour un attribut de sécurité.</p>

Composant	Événements auditable
FMT-MSA.3	Les modifications de l'attribution par défaut des règles permissives ou restrictives ; Toutes les modifications des valeurs initiales des attributs de sécurité.
FMT-MTD.1	Toutes les modifications des valeurs des données de la TSF.
FMT-SMR.1	Les modifications du groupe des utilisateurs correspondant à un rôle ; Chaque utilisation des droits associés à un rôle.
FTA-SSL.1	Verrouillage d'une session interactive par le mécanisme de verrouillage d'une session ; Déverrouillage réussi d'une session interactive ; Toute tentative pour déverrouiller une session interactive.
FTA-SSL.2	cf FTA-SSL.1
FTA-SSL.3	Clôture d'une session interactive par le mécanisme de verrouillage de session.
FTA-TAH.1	-

- FAU-GEN.1.2 La TSF doit enregistrer au minimum les informations suivantes dans chaque enregistrement d'audit :
- Date et heure de l'événement, type d'événement, identité du sujet, ainsi que le résultat (succès ou échec) de l'événement ;
 - Pour chaque type d'événement d'audit, sur la base des définitions d'événements auditables contenues dans les composants fonctionnels inclus dans le PP ou la ST, les [autres informations d'audit pertinentes]

FAU-GEN.2 Lien avec l'identité de l'utilisateur

- FAU-GEN.2.1 La TSF doit pouvoir associer chaque événement auditable avec l'identité de l'utilisateur qui est à l'origine de l'événement.
- FAU-SAR.1 Revue d'audit**
- FAU-SAR.1.1 La TSF doit offrir aux utilisateurs autorisés la capacité de lire la liste des informations d'audit à partir des enregistrements d'audit.
- FAU-SAR.1.2 La TSF doit présenter les enregistrements d'audit d'une façon permettant à l'utilisateur de les interpréter.
- FAU-SAR.2 Revue d'audit restreinte**
- FAU-SAR.2.1 La TSF doit interdire à tous les utilisateurs le droit d'accès en lecture aux enregistrements d'audit, à l'exception de ceux à qui l'on a accordé un droit de lecture explicite.
- FAU-STG.1 Stockage de la trace d'audit**
- FAU-STG.1.1 La TSF doit protéger les enregistrements d'audit stockés contre une suppression non autorisée.
- FAU-STG.1.2 La TSF doit pouvoir empêcher et détecter les modifications effectuées sur les enregistrements d'audit.
- FAU-STG.4 Prévention des pertes de données d'audit**
- FAU-STG.4.1 Si la trace d'audit est pleine, la TSF doit ignorer les événements auditables ; empêcher les événements auditables, autres que ceux provoqués par l'utilisateur autorisé bénéficiant de droits spéciaux ; écraser les enregistrements d'audit les plus anciennement stockés et d'autres actions — définies par l'auteur de la cible de sécurité — à entreprendre en cas de défaillance du stockage de l'audit.

5.2.2 Classe FDP : Protection des données de l'utilisateur

FDP-ACC.1 Contrôle d'accès partiel

FDP-ACC.1.1 La TSF doit appliquer la SFP de contrôle d'accès aux listes des sujets, objets et opérations sur ces sujets et objets.

FDP-ACF.1 Contrôle d'accès basé sur les attributs de sécurité

FDP-ACF.1.1 La TSF doit appliquer la [affectation : SFP de contrôle d'accès] aux objets en se basant sur [affectation : *attributs de sécurité, groupes d'attributs de sécurité désignés*].

Raffinement : *L'auteur de la cible de sécurité complètera l'opération*

FDP-ACF.1.2 La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée : [affectation : *règles qui régissent les accès aux sujets contrôlés et aux objets contrôlés utilisant des opérations contrôlées sur des objets contrôlés*].

Raffinement : *L'auteur de la cible de sécurité complètera l'opération*

FDP-ACF.1.3 La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [affectation : *règles basées sur les attributs de sécurité, qui autorisent explicitement l'accès de sujets à des objets*].

Raffinement : *L'auteur de la cible de sécurité complètera l'opération*

FDP-ACF.1.4 La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de [affectation : *règles basées sur les attributs de sécurité, qui interdisent explicitement l'accès de sujets à des objets*].

Raffinement : L'auteur de la cible de sécurité complètera l'opération

FDP-IFC.1 Politique de contrôle de flux

FDP-IFC.1.1 La TSF doit appliquer la [affectation : *SFP de contrôle de flux d'information*] aux [affectation : *liste des sujets, des informations et des opérations couvertes par la SFP qui déclenchent le transfert d'informations contrôlées vers et en provenance de sujets contrôlés*].

Raffinement : L'auteur de la cible de sécurité complètera l'opération

FDP-IFF.1 Attributs de sécurité simple

FDP-IFF.1.1 La TSF doit appliquer la [affectation : *SFP de contrôle de flux d'information*] en fonction des types suivants d'attributs de sécurité de sujets et d'informations : [affectation : *le nombre minimum et le type des attributs de sécurité*].

Raffinement : L'auteur de la cible de sécurité complètera l'opération

FDP-IFF.1.2 La TSF doit autoriser un flux d'information entre un sujet contrôlé et des informations contrôlées par l'intermédiaire d'une opération contrôlée si les règles suivantes s'appliquent : [affectation : *pour chaque opération, les relations basées sur les attributs de sécurité qui doivent exister entre les attributs de sécurité du sujet et les attributs de sécurité des informations*].

Raffinement : L'auteur de la cible de sécurité complètera l'opération

FDP-IFF.1.3 La TSF doit appliquer les [affectation : *règles complémentaires de la SFP de contrôle de flux d'information*].

Raffinement : L'auteur de la cible de sécurité complètera l'opération

- FDP-IFF.1.4 La TSF doit fournir ce qui suit [affectation : *liste des capacités complémentaires de la SFP*].
Raffinement : *L'auteur de la cible de sécurité complètera l'opération*
- FDP-IFF.1.5 La TSF doit autoriser explicitement un flux d'information en fonction des règles suivantes : [affectation : *règles basées sur les attributs de sécurité, qui autorisent explicitement les flux d'information*].
Raffinement : *L'auteur de la cible de sécurité complètera l'opération*
- FDP-IFF.1.6 La TSF doit interdire explicitement un flux d'information en fonction des règles suivantes : [affectation : *règles basées sur les attributs de sécurité, qui interdisent explicitement les flux d'information*].
Raffinement : *L'auteur de la cible de sécurité complètera l'opération*

5.2.3 Classe FIA : Identification et Authentification

- FIA-ATD.1 Définition des attributs de l'utilisateur**
FIA-ATD.1.1 La TSF doit maintenir la liste suivante d'attributs de sécurité appartenant à des utilisateurs individuels : [affectation : *liste d'attributs de sécurité*].
- FIA-UAU.2 Authentification de l'utilisateur avant toute action**
FIA-UAU.2.1 La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.
- FIA-UID.2 Identification de l'utilisateur avant toute action**

FIA-UID.2.1 La TSF doit exiger que chaque utilisateur soit identifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.

5.2.4 Classe FMT : Administration de la sécurité

FMT-MOF.1 Administration du comportement des fonctions de sécurité

FMT-MOF.1.1 La TSF doit restreindre l'aptitude de [sélection : *déterminer le comportement, désactiver, activer, modifier le comportement*] des fonctions [affectation : *liste des fonctions*] aux [affectation : *rôles autorisés identifiés*].

FMT-MSA.1 Administration des attributs de sécurité

FMT-MSA.1.1 La TSF doit mettre en œuvre la ou les [affectation : *SFP de contrôle d'accès, SFP de contrôle de flux d'informations*] pour restreindre aux [affectation : *les rôles autorisés identifiés*] l'aptitude de [sélection : *changer la valeur par défaut, interroger, modifier, supprimer, [affectation : autres opérations]*] les attributs de sécurité [affectation : *liste des attributs de sécurité*].

FMT-MSA.2 Attributs de sécurité sûrs

FMT-MSA.2.1 La TSF garantir que seules des valeurs sûres sont acceptées pour les attributs de sécurité.

FMT-MSA.3 Initialisation statique d'attribut

FMT-MSA.3.1 La TSF doit mettre en œuvre la ou les [affectation : SFP de contrôle d'accès, SFP de contrôle de flux d'informations] afin de fournir des valeurs par défaut [sélection : *restrictives, permissives, autres propriétés*] pour les attributs de sécurité qui sont utilisés pour appliquer la SFP.

Raffinement *L'auteur de la cible de sécurité complètera l'opération*

FMT-MSA.3.2 La TSF doit permettre à [**l'administrateur**] de spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé.

FMT-MTD.1 Administration des données de la TSF

FMT-MTD.1.1 La TSF doit restreindre l'aptitude de [**changer une valeur par défaut, interroger, modifier, supprimer, effacer**] les [affectation : *liste des données de la TSF*] aux [affectation : *les rôles autorisés identifiés*].

Raffinement *L'auteur de la cible de sécurité complètera l'opération*

FMT-SMR.1 Rôles de sécurité

FMT-SMR.1.1 La TSF doit tenir à jour les rôles [affectation : *les rôles autorisés identifiés*].

Raffinement *L'auteur de la cible de sécurité complètera l'opération*

FMT-SMR.1.2 La TSF doit être capable d'associer des utilisateurs à des rôles.

5.2.5 Classe FTA : Accès à la TOE

FTA-SSL.1 Verrouillage de session, initié par la TSF

- FTA-SSL.1.1 La TSF doit verrouiller une session interactive à la suite de [affectation : *durée d'inactivité d'un utilisateur*] :
- en effaçant ou en écrasant le contenu des écrans d'affichage, les rendant ainsi illisibles ;
 - en désactivant tout moyen d'accès aux données de l'utilisateur ou d'affichage de celles-ci, excepté le déverrouillage de la session.
- Raffinement*
- FTA-SSL.1.2 La TSF doit exiger que les événements suivants interviennent avant le déverrouillage de la session : [**authentification de l'utilisateur**].
- FTA-SSL.2** **Verrouillage de session, initié par l'utilisateur**
- FTA-SSL.2.1 La TSF doit autoriser l'utilisateur à verrouiller sa propre session interactive :
- en effaçant ou en écrasant le contenu des écrans d'affichage, les rendant ainsi illisibles ;
 - en désactivant tout moyen d'accès aux données de l'utilisateur ou d'affichage de celles-ci, excepté le déverrouillage de la session.
- FTA-SSL.2.2 La TSF doit exiger que les événements suivants interviennent avant le déverrouillage de la session : [**authentification de l'utilisateur**].
- FTA-SSL.3** **Clôture de session, initiée par l'utilisateur**
- FTA-SSL.3.1 La TSF doit terminer une session interactive à la suite de [affectation : *période d'inactivité d'un utilisateur*].
- Raffinement*
- L'auteur de la cible de sécurité complètera l'opération*

FTA-TAH.1	Historique des accès à la TOE
FTA-TAH.1.1	Dès l'établissement réussi d'une session, la TSF doit afficher à l'attention de l'utilisateur [la date, l'heure, la méthode et le lieu] du dernier établissement réussi d'une session.
FTA-TAH.1.2	Dès l'établissement réussi d'une session, la TSF doit afficher [la date, l'heure, la méthode, le lieu] de la dernière tentative d'établissement infructueuse d'une session et le nombre de tentatives infructueuses depuis le dernier établissement réussi d'une session.
FTA-TAH.1.3	La TSF ne doit pas effacer les informations concernant l'historique des accès de l'interface utilisateur sans laisser à l'utilisateur la possibilité de revoir ces informations.

5.3 Exigences d'assurance

Le niveau d'assurance retenu est EAL2 augmenté des composants ALC-DVS.1, ATE-DPT.1 et AVA-MSU.1.

Classe Support au cycle de vie

ALC-DVS.1 Development Security

Classe Tests

ATE-DPT.1 Depth

Classe Estimation de vulnérabilités

AVA-MSU.1 Misuse

6 Précisions

Précisions au titre de l'organisation:

La TOE doit pouvoir, en cas de défaillance, retrouver son état opérationnel dans des délais acceptables pour les utilisateurs.

Précisions au titre des menaces:

Ce profil de protection ne prend pas en compte la menace d'intervention physique sur la TOE (destruction, altération).

7 Argumentaire

7.1 Objectifs de sécurité de la TOE

7.1.1 Couverture des hypothèses

H.USAGE

H.USAGE est couverte par l'objectif O.USAGE.

- O.USAGE exige que la TOE soit employée comme système d'information de la famille qui en est propriétaire.

H.UTILISATEURS

H.UTILISATEURS est couverte par l'objectif O.UTILISATEURS.

- O.UTILISATEURS exige que la famille propriétaire de la TOE ainsi que les utilisateurs qu'elle autorise ne cherchent pas à compromettre volontairement la TOE.

H.VALEUR-BIENS-MATERIELS

H.VALEUR-BIENS-MATERIELS est couverte par l'objectif O.VALEURS-BIENS-MATERIELS.

- O.VALEUR-BIENS-MATERIELS exige que les biens matériels soient évalués à leur valeur d'origine.

H.VALEUR-BIENS-IMMATERIELS

H.VALEUR-BIENS-IMMATERIELS est couverte par l'objectif O.VALEURS-BIENS-IMMATERIELS.

- O.VALEUR-BIENS-IMMATERIELS exige que les biens immatériels soient évalués de sorte à être affectés d'une valeur non négligeable pour leurs propriétaires.

H.ACCES-DOMICILE

H.ACCES-DOMICILE est couverte par l'objectif O.ENVIRONNEMENT.

- O.ENVIRONNEMENT exige que seules les personnes autorisées par un membre de la famille peuvent obtenir un accès physique à la TOE, c'est-à-dire un accès au domicile.

H.ACCES-PHYSIQUE-RESEAU-INTERNE

H.ACCES-PHYSIQUE-RESEAU-INTERNE est couverte par l'objectif O.ENVIRONNEMENT.

- O.ENVIRONNEMENT exige que seules les personnes autorisées par un membre de la famille peuvent obtenir un accès physique à la TOE, c'est-à-dire un accès au réseau interne.

H.ACCES-INTERNET-ENTRANT

H.ACCES-INTERNET-ENTRANT est couverte par l'objectif O.ACCES-INTERNET-ENTRANT.

- O.ACCES-INTERNET-ENTRANT exige que la TOE soit visible depuis l'extérieur grâce à une adresse IP affectée par le FAI au routeur.

7.1.2 Couverture des menaces**M.INTRUSION-PIRATE**

M.INTRUSION-PIRATE est couverte par les objectifs O.AUDIT, O.ACCES-INTERNET-ENTRANT, les objectifs O.INTEGRITE-*, O.CONFIDENTIALITE-*, O.DISPONIBILITE, O.FILTRAGE et O.AUTHENTIFICATION-* :

- O.AUDIT exige que les actions sur la TOE soient enregistrées et horodatées. Cela permettra de détecter des vulnérabilités et de mettre en place des solutions pour y remédier par la suite.
- O.ACCES-INTERNET-ENTRANT exige que l'attaquant qui cherche à s'introduire dans la TOE le fasse *via* le modem ADSL et la connexion

internet de la TOE, ce qui limite le nombre de vulnérabilités, donc les risques d'intrusion.

- O.CONFIDENTIALITE-* exige que les utilisateurs non autorisés à consulter une donnée ne peuvent pas y accéder.
- O.DISPONIBILITE exige que l'ensemble des biens de la TOE doit être disponible, ce qui couvre les dénis de service quels qu'ils soient.
- O.INTEGRITE-* exige que les utilisateurs non autorisés à modifier une donnée ne peuvent pas altérer son intégrité.
- O.FILTRAGE exige que les connexions non autorisées par la politique de sécurité ne puissent pas être établies.
- O.AUTHENTIFICATION-* exige que les utilisateurs s'authentifient pour accéder aux données non publiques.

M.INTRUSION-ESPION

M.INTRUSION-ESPION est couverte par les objectifs O.AUDIT, O.ACCES-INTERNET-ENTRANT, les objectifs O.INTEGRITE-*, O.CONFIDENTIALITE-*, O.DISPONIBILITE, O.FILTRAGE et O.AUTHENTIFICATION-* :

- O.AUDIT exige que les actions sur la TOE soient enregistrées et horodatées. Cela permettra de détecter des vulnérabilités et de mettre en place des solutions pour y remédier par la suite.
- O.ACCES-INTERNET-ENTRANT exige que l'attaquant qui cherche à s'introduire dans la TOE le fasse *via* le modem ADSL et la connexion internet de la TOE, ce qui limite le nombre de vulnérabilités, donc les risques d'intrusion.
- O.CONFIDENTIALITE-* exige que les utilisateurs non autorisés à consulter une donnée ne peuvent pas y accéder.
- O.DISPONIBILITE exige que l'ensemble des biens de la TOE doit être disponible, ce qui couvre les dénis de service quels qu'ils soient.
- O.INTEGRITE-* exige que les utilisateurs non autorisés à modifier une donnée ne peuvent pas altérer son intégrité.
- O.FILTRAGE exige que les connexions non autorisées par la politique de sécurité ne puissent pas être établies.
- O.AUTHENTIFICATION-* exige que les utilisateurs s'authentifient

pour accéder aux données non publiques.

M.VIRUS

M.VIRUS est couverte par les objectifs O.AUDIT, O.UTILISATEURS, O.CONFIDENTIALITE-*, O.DISPONIBILITE, O.FILTRAGE et O.INTEGRITE-* :

- O.AUDIT exige que les actions sur la TOE soient enregistrées et horodatées. Cela permettra de détecter les actions suspectes résultant de la contamination d'un bien de la TOE par un virus.
- O.UTILISATEURS exige que les utilisateurs autorisés de la TOE ne cherchent pas à compromettre la TOE.
- O.CONFIDENTIALITE-* exige qu'un utilisateur (le virus est un utilisateur invité) s'authentifie pour accéder à des données privées ou partagées.
- O.DISPONIBILITE exige que l'ensemble des biens de la TOE doit être disponible, ce qui couvre les dénis de service dûs à des virus.
- O.FILTRAGE exige que les connexions non autorisées par la politique de sécurité ne puissent pas être établies.
- O.INTEGRITE-* exige qu'un utilisateur (le virus est un utilisateur invité) s'authentifie pour altérer des données privées ou partagées.

M.NEGLIGENCE-MANIPULATION

M.NEGLIGENCE-MANIPULATION est couverte par les objectifs O.AUDIT, O.UTILISATEURS, O.DISPONIBILITE et O.INTEGRITE-* :

- O.AUDIT exige que les actions sur la TOE soient enregistrées et horodatées. Cela permettra de détecter une mauvaise manipulation, d'identifier son initiateur, et d'y remédier.
- O.UTILISATEURS exige que les utilisateurs autorisés de la TOE ne cherchent pas à compromettre la TOE.
- O.DISPONIBILITE exige que l'ensemble des biens de la TOE doit être disponible, ce qui couvre les mauvaises manipulations matérielles et logicielles.
- O.INTEGRITE-* exige qu'un utilisateur s'authentifie pour altérer des

données privées ou partagées, ce qui empêche un utilisateur de modifier des données sur lesquelles il n'a pas le droit.

7.1.3 Couverture des politiques de sécurité organisationnelles

P.ADMINISTRATEUR-UNIQUE

P.ADMINISTRATEUR-UNIQUE est couverte par l'objectif O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE :

- O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE exige que l'administrateur soit unique et soit authentifié par la TOE.

P.HIERARCHIE

P.HIERARCHIE est couverte par les objectifs O.USAGE, O.AUTHENTIFICATION-*, O.ACCES-INTERNET-ENTRANT et O.ENVIRONNEMENT :

- O.USAGE exige que la TOE soit employée comme système d'information de la famille, c'est-à-dire de l'administrateur et des membres de la famille.
- O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE exige que l'administrateur soit authentifié par la TOE.
- O.AUTHENTIFICATION-MEMBRES exige que les membres de la famille soient authentifiés par la TOE.
- O.AUTHENTIFICATION-INVITES exige que les invités soient authentifiés par la TOE.
- O.ACCES-INTERNET-ENTRANT exige qu'une personne n'ayant pas un accès physique à la TOE appartienne à la catégorie des utilisateurs (autorisés ou non).
- O.ENVIRONNEMENT exige que seuls les invités, les membres de la famille et l'administrateur aient un accès physique à la TOE.

P.MEMBRES

P.MEMBRES est couverte par l'objectif O.AUTHENTIFICATION-MEMBRES

- O.AUTHENTIFICATION-MEMBRES exige que les membres de la famille soient authentifiées par un mot de passe, délivré par l'adminis-

trateur.

P.INVITES

P.INVITES est couverte par les objectifs O.AUTHENTIFICATION-INVITES et O.ENVIRONNEMENT :

- O.ENVIRONNEMENT exige qu'une personne invitée a été au préalable autorisée par un membre de la famille propriétaire de la TOE.
- O.AUTHENTIFICATION-INVITES exige l'accès physique à la TOE pour pouvoir prétendre au statut d'invité.

7.1.4 Complétudes des objectifs de sécurité

O.CONFIDENTIALITE-*

O.CONFIDENTIALITE couvre les menaces M.INTRUSION-PIRATE, M.INTRUSION-ESPION et M.VIRUS :

- O.CONFIDENTIALITE-* couvre la menace M.INTRUSION-PIRATE car il exige que les utilisateurs non autorisés à consulter une donnée ne puissent pas y accéder.
- O.CONFIDENTIALITE-* couvre la menace M.INTRUSION-ESPION car il exige que les utilisateurs non autorisés à consulter une donnée ne puissent pas y accéder.
- O.CONFIDENTIALITE-* couvre la menace M.VIRUS car il exige que les utilisateurs s'authentifient pour accéder à des données privées ou partagées.

O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE

O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE couvre les menaces M.INTRUSION-PIRATE, M.INTRUSION-ESPION et satisfait les politiques P.ADMINISTRATEUR-UNIQUE et P.HIERARCHIE :

- O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE couvre la menace M.INTRUSION-PIRATE car il exige qu'un utilisateur s'authentifie pour accéder aux privilèges de l'administrateur.
- O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE couvre la

menace M.INTRUSION-ESPION car il exige qu'un utilisateur s'authentifie pour accéder aux privilèges de l'administrateur.

- O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE satisfait la politique P.ADMINISTRATEUR-UNIQUE car l'administrateur est unique.
- O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE satisfait la politique P.HIERARCHIE puisqu'il introduit la présence d'un administrateur.

O.AUTHENTIFICATION-MEMBRES

O.AUTHENTIFICATION-MEMBRES couvre les menaces M.INTRUSION-PIRATE, M.INTRUSION-ESPION et satisfait les politiques P.MEMBRES et P.HIERARCHIE :

- O.AUTHENTIFICATION-MEMBRES couvre la menace M.INTRUSION-PIRATE car il exige qu'un utilisateur s'authentifie pour accéder aux privilèges des membres.
- O.AUTHENTIFICATION-MEMBRES couvre la menace M.INTRUSION-ESPION car il exige qu'un utilisateur s'authentifie pour accéder aux privilèges des membres.
- O.AUTHENTIFICATION-MEMBRES satisfait la politique P.MEMBRES puisqu'il impose que les membres de la famille s'authentifient.
- O.AUTHENTIFICATION-MEMBRES satisfait la politique P.HIERARCHIE puisqu'il introduit la présence de membres de la famille.

O.AUTHENTIFICATION-INVITES

O.AUTHENTIFICATION-INVITES satisfait les politiques P.INVITES et P.HIERARCHIE :

- O.AUTHENTIFICATION-INVITES satisfait la politique P.INVITES puisqu'il impose qu'un membre ayant un accès physique à la TOE sans authentification est un invité.
- O.AUTHENTIFICATION-INVITES satisfait la politique P.HIERARCHIE puisqu'il introduit la présence d'invités.

O.INTEGRITE-DONNEES-PRIVEES

O.INTEGRITE-DONNEES-PRIVEES couvre les menaces M.INTRUSION-

PIRATE, M.INTRUSION-ESPION, M.VIRUS, M.NEGLIGENCE-MANIPULATION :

- O.INTEGRITE-DONNEES-PRIVEES couvre la menace M.INTRUSION-PIRATE car il exige que les utilisateurs non propriétaires d'une donnée privée ne puissent pas la modifier.
- O.INTEGRITE-DONNEES-PRIVEES couvre la menace M.INTRUSION-ESPION car il exige que les utilisateurs non propriétaires d'une donnée privée ne puissent pas la modifier.
- O.INTEGRITE-DONNEES-PRIVEES couvre la menace M.VIRUS car il exige que les utilisateurs s'authentifient pour modifier des données privées.
- O.INTEGRITE-DONNEES-PRIVEES couvre la menace M.NEGLIGENCE-MANIPULATION car il exige que les utilisateurs s'authentifient pour modifier des données privées.

O.INTEGRITE-DONNEES-PARTAGEES

O.INTEGRITE-DONNEES-PARTAGEES couvre les menaces M.INTRUSION-PIRATE, M.INTRUSION-ESPION, M.VIRUS, M.NEGLIGENCE-MANIPULATION :

- O.INTEGRITE-DONNEES-PARTAGEES couvre la menace M.INTRUSION-PIRATE car il exige que les utilisateurs non membres du groupe d'une donnée partagée ne puissent pas la modifier.
- O.INTEGRITE-DONNEES-PARTAGEES couvre la menace M.INTRUSION-ESPION car il exige que les utilisateurs non membres du groupe d'une donnée partagée ne puissent pas la modifier.
- O.INTEGRITE-DONNEES-PARTAGEES couvre la menace M.VIRUS car il exige que les utilisateurs s'authentifient pour modifier des données partagées.
- O.INTEGRITE-DONNEES-PARTAGEES couvre la menace M.NEGLIGENCE-MANIPULATION car il exige que les utilisateurs s'authentifient pour modifier des données partagées.

O.INTEGRITE-DONNEES-PUBLIQUES

O.INTEGRITE-DONNEES-PUBLIQUES couvre les menaces M.INTRUSION-PIRATE, M.INTRUSION-ESPION, M.VIRUS, M.NEGLIGENCE-MANIPULATION :

- O.INTEGRITE-DONNEES-PUBLIQUES couvre la menace M.INTRUSION-

PIRATE car il exige que l'administrateur seul puisse modifier les données publiques.

- O.INTEGRITE-DONNEES-PUBLIQUES couvre la menace M.INTRUSION-ESPION car il exige que l'administrateur seul puisse modifier les données publiques.
- O.INTEGRITE-DONNEES-PUBLIQUES couvre la menace M.VIRUS car il exige qu'un utilisateur s'authentifie comme administrateur pour modifier des données publiques.
- O.INTEGRITE-DONNEES-PUBLIQUES couvre la menace M.NEGLIGENCE-MANIPULATION car il exige qu'un utilisateur s'authentifie comme administrateur pour modifier des données publiques.

O.DISPONIBILITE

O.DISPONIBILITE couvre les menaces M.INTRUSION-PIRATE, M.INTRUSION-ESPION, M.VIRUS, M.NEGLIGENCE-MANIPULATION :

- O.DISPONIBILITE couvre la menace M.INTRUSION-PIRATE car il exige que les biens de la TOE soient disponibles.
- O.DISPONIBILITE couvre la menace M.INTRUSION-ESPION car il exige que les biens de la TOE soient disponibles.
- O.DISPONIBILITE couvre la menace M.VIRUS car il exige que les biens de la TOE soient disponibles.
- O.DISPONIBILITE couvre la menace M.NEGLIGENCE-MANIPULATION car il exige que les biens de la TOE soient disponibles.

O.AUDIT

O.AUDIT couvre les menaces M.INTRUSION-PIRATE, M.INTRUSION-ESPION, M.VIRUS, M.NEGLIGENCE-MANIPULATION :

- O.AUDIT couvre la menace M.INTRUSION-PIRATE car il exige que tout les événements intervenant sur la TOE soient enregistrés et horodatés, ce qui permet d'identifier les agissements d'un pirate.
- O.AUDIT couvre la menace M.INTRUSION-ESPION car il exige que tout les événements intervenant sur la TOE soient enregistrés et horodatés, ce qui permet d'identifier les agissements d'un espion.
- O.AUDIT couvre la menace M.INTRUSION-VIRUS car il exige que

tout les événements intervenant sur la TOE soient enregistrés et horodatés, ce qui permet de repérer les agissements d'un virus.

- O.AUDIT couvre la menace M.NEGLIGENCE-MANIPULATION car il exige que tout les événements intervenant sur la TOE soient enregistrés et horodatés, ce qui permet de corriger d'éventuelles négligences ou mauvaises manipulations.

O.FILTRAGE

O.FILTRAGE couvre les menaces M.INTRUSION-PIRATE, M.INTRUSION-ESPION, M.VIRUS :

- O.FILTRAGE couvre la menace M.INTRUSION-PIRATE car il exige que seuls les flux autorisés par la politique de sécurité puissent effectivement exister entre la TOE et l'internet.
- O.FILTRAGE couvre la menace M.INTRUSION-ESPION car il exige que seuls les flux autorisés par la politique de sécurité puissent effectivement exister entre la TOE et l'internet.
- O.FILTRAGE couvre la menace M.INTRUSION-VIRUS car il exige que seuls les flux autorisés par la politique de sécurité puissent effectivement exister entre la TOE et l'internet.

7.1.5 Complétudes des objectifs de l'environnement

O.USAGE

O.USAGE couvre l'hypothèse H.USAGE et satisfait la politique P.HIERARCHIE :

- O.USAGE couvre l'hypothèse H.USAGE puisqu'il impose que la TOE soit employée comme système d'information de la famille qui en est propriétaire.
- O.USAGE couvre la politique P.HIERARCHIE puisqu'il impose que la TOE soit employée comme système d'information de la famille, c'est-à-dire de l'administrateur et des membres de la famille.

O.UTILISATEURS

O.UTILISATEURS couvre l'hypothèse H.UTILISATEURS et les menaces M.VIRUS et M.NEGLIGENCE-MANIPULATION :

- O.UTILISATEURS couvre l'hypothèse H.UTILISATEURS puisqu'il impose que la famille propriétaire de la TOE, ainsi que les utilisateurs qu'elle autorise ne compromettent pas volontairement la TOE.
- O.UTILISATEURS couvre la menace M.VIRUS puisqu'elle implique qu'un utilisateur autorisé n'introduira pas de virus dans la TOE volontairement.
- O.UTILISATEURS couvre la menace M.NEGLIGENCE-MANIPULATION puisqu'elle implique qu'un utilisateur autorisé ne commettra pas de mauvaise manipulation de façon intentionnelle.

O.ACCES-INTERNET-ENTRANT

O.ACCES-INTERNET-ENTRANT couvre l'hypothèse H.ACCES-INTERNET-ENTRANT :

- O.ACCES-INTERNET-ENTRANT couvre l'hypothèse H.ACCES-INTERNET-ENTRANT puisqu'il impose que la TOE soit visible depuis l'extérieur grâce à l'adresse IP affectée par le FAI au routeur relié au modem.

O.VALEURS-BIENS-MATERIELS

O.VALEURS-BIENS-MATERIELS couvre l'hypothèse H.VALEURS-BIENS-MATERIELS :

- O.VALEURS-BIENS-MATERIELS couvre l'hypothèse H.VALEURS-BIENS-MATERIELS puisqu'il implique que les biens matériels soient évalués à leur valeur d'origine.

O.VALEURS-BIENS-IMMATERIELS

O.VALEURS-BIENS-IMMATERIELS couvre l'hypothèse H.VALEURS-BIENS-IMMATERIELS :

- O.VALEURS-BIENS-IMMATERIELS couvre l'hypothèse H.VALEURS-BIENS-MATERIELS puisqu'il implique que les biens immatériels aient une valeur non négligeable pour leurs propriétaires.

7.1.6 Récapitulatif des relations Menaces-Politiques-Objectifs-Hypothèses

	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i
M.INTRUSION-PIRATE	X	X	X	X	X	X	X	X	X		X	X			X			
M.INTRUSION-ESPION	X	X	X	X	X	X	X	X	X		X	X			X			
M.VIRUS	X	X	X				X	X	X	X	X	X		X				
M.NEGLIGENCE-MANIPULATION							X	X	X	X	X			X				
M.NEGLIGENCE-INSTALLATION																		
P.ADMINISTRATEUR-UNIQUE				X														
P.HIERARCHIE				X	X	X							X		X			X
P.MEMBRES					X													
P.INVITES						X												X
H.USAGE													X					
H.UTILISATEURS														X				
H.VALEUR-BIENS-MATERIELS																X		
H.VALEUR-BIENS-IMMATERIELS																	X	
H.ACCES-DOMICILE																		X
H.ACCES-PHYSIQUE-RESEAU-INTERNE																		X
H.ACCES-INTERNET-ENTRANT														X				

FIG. 7 – Complétude des objectifs de sécurité et d'environnement

- 1 O.CONFIDENTIALITE-DONNEES-PRIVEES
- 2 O.CONFIDENTIALITE-DONNEES-PARTAGEES
- 3 O.CONFIDENTIALITE-FLUX-INTERNES
- 4 O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE
- 5 O.AUTHENTIFICATION-MEMBRES
- 6 O.AUTHENTIFICATION-INVITES
- 7 O.INTEGRITE-DONNEES-PRIVEES
- 8 O.INTEGRITE-DONNEES-PARTAGEES
- 9 O.INTEGRITE-DONNEES-PUBLIQUES
- a O.DISPONIBILITE
- b O.AUDIT
- c O.FILTRAGE
- d O.USAGE
- e O.UTILISATEURS
- f O.ACCES-INTERNET-ENTRANT
- g O.VALEURS-BIENS-MAT
- h O.VALEURS-BIENS-IMM
- i O.ENVIRONNEMENT

Le tableau 7 montre que toutes les menaces, toutes les politiques et toutes les hypothèses sont couvertes par au moins un objectif de sécurité et

que chaque objectif de sécurité répond à au moins une menace, une politique ou une hypothèse.

7.2 Exigences fonctionnelles de la TOE

7.2.1 Argumentaire pour la classe FAU : Audit de sécurité

FAU-ARP.1 Alarmes de sécurité

Ce composant permet de générer des alarmes si une violation de la sécurité a été détectée, que ce soit des attaques externes ou une mauvaise manoeuvre de l'utilisateur. Il répond donc à l'objectif O.AUDIT.

FAU-GEN.1 Génération de données d'audit

Ce composant répond à O.AUDIT puisqu'il impose à la TSF de générer un journal d'audit.

FAU-GEN.2 Lien avec l'identité de l'utilisateur

Ce composant permet d'associer à tout événement auditable l'identité de l'utilisateur ou de l'opérateur qui aura réalisé cet événement. Il permet donc de savoir, pour chaque opération relevant de la sécurité, quelle entité l'a réalisée. Cette exigence couvre donc les objectifs O.AUDIT et O.AUTHENTIFICATION-*

FAU-SAR.1 Revue d'audit

Ce composant répond à O.AUDIT puisqu'il fournit les moyens nécessaires à l'analyse des enregistrements d'audit. En effet, cette exigence impose que toutes les données enregistrées dans le journal d'audit soient compréhensibles par un humain, donc par les opérateurs.

FAU-SAR.2 Revue d'audit restreinte

Ce composant répond à O.AUDIT puisqu'il exige qu'il n'y ait pas d'autres utilisateurs qui puissent lire les informations, à l'exception de ceux qui ont été identifiés dans le composant FAU-SAR.1

FAU-STG.1 Stockage de la trace d'audit

L'audit est protégé grâce à ce composant. Il permet de protéger la trace d'audit contre une suppression ou une modification non autorisée. Cette exigence répond à O.AUDIT., à O.INTEGRITE-DONNEES-PRIVEES et à O.CONFIDENTIALITE-DONNEES-PRIVEES.

FAU-STG.4 Prévention des pertes de données d'audit

Les données de l'audit sont préservées au cas où la trace d'audit est pleine. Ce composant définit les actions à entreprendre pour prévenir la perte de ces données et répond à l'objectif O.AUDIT et à l'objectif O.INTEFRITE-DONNEES-PRIVEES.

7.2.2 Argumentaire pour la classe FDP : Protection des données de l'utilisateur

FDP-ACC.1 Contrôle d'accès partiel

Ce composant joue un rôle essentiel dans l'objectif de protection des données. Chaque SFP de contrôle d'accès identifiée est mise en place pour un ensemble défini d'opérations qu'il est possible d'effectuer sur un ensemble défini d'objets de la TOE. Cette exigence répond ainsi ux objectifs O.CONFIDENTIALITE-* et O.INTEGRITE-*.

FDP-ACF.1 Contrôle d'accès basé sur les attributs de sécurité

Ce composant spécifie l'implémentation de la politique de contrôle d'accès définie dans FDP-ACC.1. Le composant permet à la TSF de mettre en oeuvre des accès basés sur les attributs de sécurité, il est indissociable du composant précédent. Il répond aux objectifs O.CONFIDENTIALITE-* et O.INTEGRITE-*.

FDP-IFC.1 Politique de contrôle de flux

Ce composant spécifie la politique de contrôle de flux mise en place. Il définit des sous-ensembles d'opérations possibles sur des sous-ensembles de flux. Il répond en particulier aux objectifs O.FILTRAGE et O.CONFIDENTIALITE-FLUX-INTERNES, et également à O.CONFIDENTIALITE-* à et O.INTEGRITE-

*

FDP-IFF.1 Attributs de sécurité simple

Ce composant complète le composant FDP-IFC.1, il impose des attributs de sécurité aux informations et aux sujets qui déclenchent les transferts d'information. Il spécifie les règles qui doivent être appliquées. Il répond aux objectifs O.CONFIDENTIALITE-* et O.INTEGRITE-*.

7.2.3 Argumentaire pour la classe FIA : Identification et authentification

FIA-ATD.1 Définition des attributs de l'utilisateur

Ce composant permet d'associer des attributs de sécurité à chaque utilisateur. Il est obligatoire pour pouvoir répondre aux objectifs d'authentification et de confidentialité des données privées. Il couvre les objectifs O.CONFIDENTIALITE-*, O.AUTHENTIFICATION-* et O.INTEGRITE-*.

FIA-UAU.2 Authentification de l'utilisateur avant toute action

Ce composant permet de répondre aux objectifs d'authentification définis. Il couvre les objectifs O.CONFIDENTIALITE-*, O.AUTHENTIFICATION-* et O.INTEGRITE-*.

FIA-UID.2 Identification de l'utilisateur avant toute action

Cela permet d'associer les attributs de sécurité correspondant à l'utilisateur (on considère que le statut d'invité est identifié). Il couvre les objectifs O.CONFIDENTIALITE-*, O.AUTHENTIFICATION-* et O.INTEGRITE-*.

7.2.4 Argumentaire pour la classe FMT : Administration de la sécurité

FMT-MOF.1 Administration du comportement des fonctions de sécurité

Ce composant permet de définir les droits des utilisateurs sur l'administration des fonctions de sécurité. Il répond à l'objectif O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE.

FMT-MSA.1 Administration des attributs de sécurité

Ce composant permet aux utilisateurs de gérer les attributs de sécurité spécifiés.

FMT-MSA.2 Attributs de sécurité sûrs

Ce composant garantit que les valeurs assignées aux attributs de sécurité sont valides par rapport à l'état sûr. Partant, les attributs de sécurité ne pourront pas être modifiés sans qu'ils répondent aux objectifs O.CONFIDENTIALITE-DONNEES-* et O.INTEGRITE-DONNEES*.

FMT-MSA.3 Initialisation statique de l'attribut

Ce composant garantit que les valeurs par défaut des attributs de sécurité sont de façon appropriée de nature soit permissive soit restrictive. Cette fonction est nécessaire afin d'initialiser correctement les attributs de sécurité des nouvelles données, de manière à ce qu'ils respectent les objectifs O.CONFIDENTIALITE-DONNEES-* et O.INTEGRITE-DONNEES*.

FMT-MTD.1 Administration des données de la TSF

Ce composant permet aux utilisateurs autorisés (ici, l'administrateur) de gérer les données de la TSF.

FMT-SMR.1 Rôles de sécurité

Ce composant spécifie les rôles par rapport à la sécurité que la TSF reconnaît. Il permet à la personne administrant les droits de la TOE d'être identifié comme tel.

7.2.5 Argumentaire pour la classe FTA : Accès à la TOE

FTA-SSL.1 Verrouillage de session, initié par la TSF

Ce composant permet le verrouillage, initié par le système, d'une session interactive à la suite d'une période d'inactivité spécifiée d'un utilisateur. Ceci permet de respecter les objectifs O.INTEGRITE-DONNEES-PRIVEES et O.INTEGRITE-DONNEES-PARTAGEES dans le cas d'une session restée ouverte d'un utilisateur.

FTA-SSL.2 Verrouillage de session, initié par l'utilisateur

Ce composant permet à l'utilisateur de verrouiller et déverrouiller ses propres sessions interactives.

FTA-SSL.3 Clôture de session, initiée par la TSF

Ce composant permet de terminer une session à la suite d'une période d'inactivité de l'utilisateur. Ceci permet de respecter les objectifs O.INTEGRITE-DONNEES-PRIVEES et O.INTEGRITE-DONNEES-PARTAGEES dans le cas d'une session restée ouverte d'un utilisateur.

FTA-TAH.1 Historique des accès de la TOE

Ce composant permet l'affichage des informations associées aux tentatives précédentes d'établissement d'une session. Il couvre l'objectif O.AUDIT.

7.3 Satisfaction des objectifs de sécurité

Le tableau 8 représente un récapitulatif de la satisfaction des objectifs de sécurité, en conservant les mêmes notations que précédemment pour les objectifs :

1	O.CONFIDENTIALITE-DONNEES-PRIVEES
2	O.CONFIDENTIALITE-DONNEES-PARTAGEES
3	O.CONFIDENTIALITE-FLUX-INTERNES
4	O.AUTHENTIFICATION-ADMINISTRATEUR-UNIQUE
5	O.AUTHENTIFICATION-MEMBRES
6	O.AUTHENTIFICATION-INVITES
7	O.INTEGRITE-DONNEES-PRIVEES
8	O.INTEGRITE-DONNEES-PARTAGEES
9	O.INTEGRITE-DONNEES-PUBLIQUES
a	O.DISPONIBILITE
b	O.AUDIT
c	O.FILTRAGE

7.4 Argumentaire des exigences d'assurance

La TOE doit protéger les biens qu'elle regroupe contre des attaquants disposant de compétences faibles (M.PIRATE) à moyennes (M.ESPION), et des moyens techniques et financiers limités. Le niveau EAL2 retenu, augmenté des composants ALC-DVS.1, ATE-DPT.1 et AVA-MSU.1, permet d'assurer :

- Une description fonctionnelle compartimentée des sous-systèmes de la TOE ;
- La recherche des vulnérabilités élémentaires ;
- La résistance à des attaquants disposant de moyens limités ;
- La recherche de vulnérabilités au niveau de chaque sous-système ;
- La réduction du risque dû à une erreur humaine qui nuirait à une fonction de sécurité de la TOE.

7.5 Cohésion des exigences de sécurité

La cohésion des exigences de sécurité est assurée si :

- toutes les dépendances des composants de sécurité sont satisfaites ;
- les composants de sécurité se supportent mutuellement ;
- les composants de sécurité forment un tout cohérent.

L'étude de la cohésion des exigences de sécurité n'a pas été effectuée dans le cadre de ce profil de protection.

	1	2	3	4	5	6	7	8	9	a	b	c
FAU-ARP.1											X	
FAU-GEN.1											X	
FAU-GEN.2				X	X	X					X	
FAU-SAR.1											X	
FAU-SAR.2											X	
FAU-STG.1	X			X							X	
FAU-STG.4				X							X	
FDP-ACC.1	X	X	X				X	X	X			
FDP-ACF.1	X	X	X				X	X	X			
FDP-IFC.1	X	X	X				X	X	X		X	X
FDP-IFF.1	X	X	X				X	X	X			
FIA-ATD.1	X	X	X	X	X	X	X	X	X			
FIA-UAU.2	X	X	X	X	X	X	X	X	X			
FIA-UID.1	X	X	X	X	X	X	X	X	X			
FMT-MOF.1				X								
FMT-MSA.1	X	X	X				X	X	X			
FMT-MSA.2	X	X	X				X	X	X			
FMT-MSA.3	X	X	X				X	X	X			
FMT-MTD.1	X	X	X				X	X	X			
FMT-SMR.1				X								
FTA-SSL.1	X	X		X	X	X	X	X	X			
FTA-SSL.2	X	X		X	X	X	X	X	X			
FTA-SSL.3	X	X		X	X	X	X	X	X	X		
FTA-TAH.1											X	

FIG. 8 – Satisfaction des objectifs de sécurité