FIREWALL A EXIGENCES ELEVEES

PROFIL DE PROTECTION

o o O o o

V2.2 - Septembre 1998

Enregistré par l'Organisme de Certification français sous la référence PP/9905

TABLE DES MATIERES

1. INTRODUCTION....1

1.1 Identification du profil de protection.... 1

1.2 Présentation du profil de protection.... 1

2. DESCRIPTION DE LA CIBLE D'EVALUATION....2

3. ENVIRONNEMENT DE SECURITE....3

3.1 Hypothèses d'utilisation de la TOE.... 3

3.2 Menaces.... 4

3.3 Politiques de sécurité organisationnelles.... 5

4. OBJECTIFS DE SECURITE....6

4.1 Objectifs de sécurité des technologies de l'information.... 6

4.2 Objectifs de sécurité de l'environnement.... 7

5. EXIGENCES DE SECURITE....8

5.1 Exigences fonctionnelles.... 8

5.2 Texte des exigences fonctionnelles.... 10

5.2.1 Classe Security Audit.... 10

5.2.2 Classe User Data Protection.... 14

5.2.3 Classe Identification and Authentication.... 17

5.2.4 Classe Security Management.... 19

5.2.5 Classe Protection of the TOE Security Functions.... 23

5.2.6 Classe TOE Access.... 24

5.2.7 Classe Trusted Path/Channels.... 25

5.3 Exigences d'assurance.... 26

6. PRECISIONS....26

7. GLOSSAIRE....27

8. ARGUMENTAIRE....29

8.1 Objectifs de sécurité de la TOE.... 29

8.1.1 Couvertures des hypothèses.... 29

8.1.2 Couverture des menaces.... 29

8.1.3 Couverture des politiques de sécurité organisationnelles.... 31

8.1.4 Complétude des objectifs de sécurité.... 32

8.1.4.1 Complétude des objectifs des technologies de l'information.... 32

8.1.4.2 Complétude des objectifs de l'environnement.... 34

8.1.5 Récapitulatif des relations Menaces-Politiques / Objectifs-Hypothèses.... 37

8.2 Exigences fonctionnelles de la TOE 38
8.2.1 Argumentaire pour la classe FAU : Security Audit 38
8.2.2 Argumentaire pour la classe FDP : User Data Protection 39
8.2.3 Argumentaire pour la classe FIA : Identification and Authentication 41
8.2.4 Argumentaire pour la classe FMT : Security Management 43
8.2.5 Argumentaire pour la classe FPT : Protection of the TOE Security Functions 45
8.2.6 Argumentaire pour la classe FTA : TOE Access 46
8.2.7 Argumentaire pour la classe FTP : Trusted Path/Channels 46
8.3 Satisfaction des objectifs de sécurité 48
8.4 Argumentaire des exigences d'assurance 50
8.5 Cohésion des exigences de sécurité 50
8.5.1 Dépendances des exigences fonctionnelles 50
8.5.2 Dépendances des exigences d'assurance 53
8.5.3 Support mutuel des composants de sécurité 54
8.5.4 Cohérence interne des composants de sécurité 58
8.5.4.1 FAU <-> FAU 59
8.5.4.2 FAU <-> FDP 60
8.5.4.3 FAU <-> FIA 61
8.5.4.4 FAU <-> FMT 62
8.5.4.5 FAU <-> FPT 63
8.5.4.6 FAU <-> FTA 65
8.5.4.7 FAU <-> FTP 65
8.5.4.8 FDP <-> FDP 66
8.5.4.9 FDP <-> FIA 67
8.5.4.10 FDP <-> FMT 68
8.5.4.11 FDP <-> FPT 69
8.5.4.12 FDP <-> FTA 69
8.5.4.13 FDP <-> FTP 69
8.5.4.14 FIA <-> FIA 70
8.5.4.15 FIA <-> FMT 71
8.5.4.16 FIA <-> FPT 72
8.5.4.17 FIA <-> FTA 72
8.5.4.18 FIA <-> FTP 73
8.5.4.19 FMT <-> FMT 73
8.5.4.20 FMT <-> FPT 75
8.5.4.21 FMT <-> FTA 75
8.5.4.22 FMT <-> FTP 76
8.5.4.23 FPT <-> FPT 76
8.5.4.24 FPT <-> FTA 77
8.5.4.25 FPT <-> FTP 77
8.5.4.26 FTA <-> FTA 78
8.5.4.27 FTA <-> FTP 78
8.5.5 Conclusion de l'analyse de cohésion 78

1. Introduction

1.1 Identification du profil de protection

Titre : Firewall à Exigences Elevées (FEE) - V2.2 - Septembre 1998

Enregistrement : PP/9905

Mots clés : firewall, filtrage de paquets, relais applicatif

Référence à d'autres profils de protection :

- PP FEE Firewall à Exigences Elevées - V1.4 - Mai 1998

1.2 Présentation du profil de protection

Ce profil de protection exprime les objectifs de sécurité ainsi que les exigences fonctionnelles et d'assurance pour une cible d'évaluation (nommée ci-après TOE) permettant d'assurer l'interconnexion de deux réseaux.

Cette TOE est destinée à fournir les mesures nécessaires visant à conserver, après interconnexion des deux réseaux, le niveau de sécurité atteint par chaque réseau considéré isolément.

Chacun des deux réseaux doit être soumis à une politique de sécurité. Les utilisateurs des deux réseaux qui communiquent via la TOE, respectent la politique de sécurité inhérente à leur réseau d'appartenance.

Ce profil de protection est conforme aux Critères Communs V2.0 (Mai 1998).

2. Description de la cible d'évaluation

Les utilisateurs de deux réseaux expriment le besoin d'interopérer pour des applications telles que la messagerie, ou d'accéder à des serveurs communs. Il est donc nécessaire d'ouvrir l'un vers l'autre les réseaux initialement non connectés. L'objet de la TOE est de fournir les fonctionnalités de sécurité visant à autoriser l'interconnexion des deux réseaux sans en dégrader le niveau de sécurité initial. La TOE est un firewall. Ce firewall est le seul point de passage entre les deux réseaux.

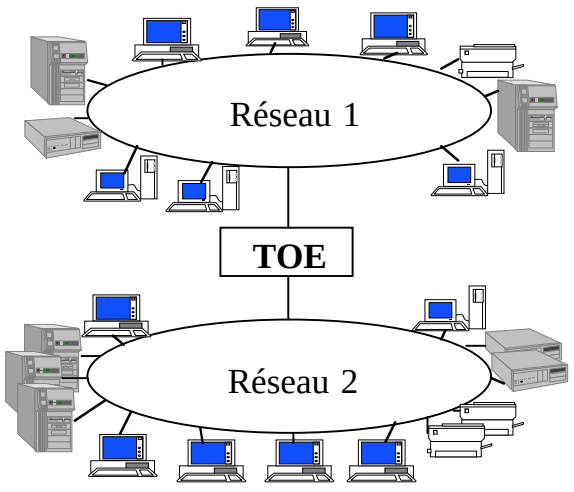
Pour autoriser une interconnexion sans dégradation du niveau de sécurité, la TOE offre des fonctionnalités de filtrage des communications entre les deux réseaux basées sur des règles définies conformément à la politique de sécurité mise en place :

- filtrage des paquets d'un réseau à l'autre,
- filtrage des applications entre utilisateurs de chaque réseau.

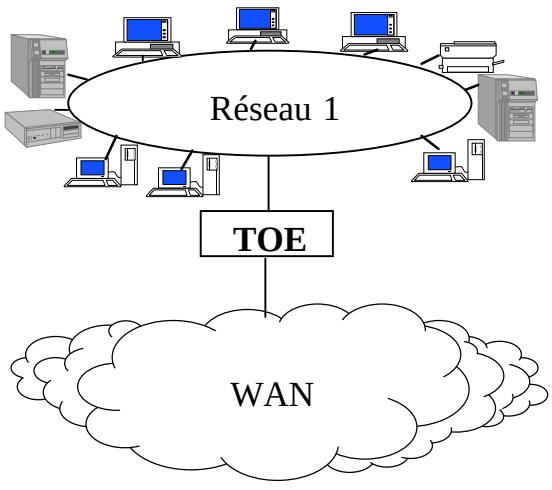
La TOE est également dotée de fonctionnalités de sécurité propres à assurer sa sécurité intrinsèque comme l'audit ou l'identification/authentification des opérateurs.

Le schéma suivant représente les deux types de configuration identifiés :

La TOE connecte deux réseaux locaux



La TOE connecte un réseau local à un réseau étendu



3. Environnement de sécurité

3.1 Hypothèses d'utilisation de la TOE

H. USAGE :

La TOE est le seul point de passage entre les deux réseaux. Les périphériques de connexion (modem) sont interdits sur les réseaux à protéger.

H.PERSONNEL :

Les opérateurs sont des personnes non hostiles et compétentes, et disposent des moyens nécessaires à leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la charge.

H.PERSONNE_EXT :

Une personne extérieure ayant un accès à la TOE, ne pourra le faire que conformément à la politique de sécurité mise en place.

H.INSTALLE :

La TOE est livrée et installée de manière à respecter la politique de sécurité régissant l'interconnexion des réseaux.

H.PROTECT_TOE :

La TOE se trouve dans un local protégé. Les moyens mis en oeuvre seront conformes à la politique de sécurité régissant l'interconnexion des réseaux .

3.2 Menaces

M.INTRUSION_RESEAU :

Un utilisateur du premier réseau s'introduit sur le second réseau via la TOE à des fins malveillantes.

Cette attaque peut impliquer une perte de confidentialité, d'intégrité ou de disponibilité des données protégées ou des ressources. Elle peut avoir différents impacts comme :

- l'accès à des services non autorisés,
- l'accès à de l'information sensible,
- la transmission d'informations sensibles,
- l'introduction d'informations non intègres,
- la saturation du réseau.

M.INTRUSION_TOE :

Un attaquant obtient un accès illégal à la TOE.

Cet attaquant peut donc, via un accès local ou distant à la TOE, modifier la configuration de la TOE, ajouter des accès non prévus, modifier les traces d'audit, saturer la TOE,...

M.MAUVAIS_OPE :

Un opérateur de la TOE négligent effectue une opération illicite sur la TOE.

Il est notamment possible qu'il :

- configure mal la TOE,
- ne relève pas l'audit.

M.VIRUS :

Un opérateur introduit, volontairement ou involontairement un logiciel non autorisé (notamment un virus) dans la TOE.

3.3 Politiques de sécurité organisationnelles

P.OPERATEUR :

Les opérateurs sont les seuls à avoir un accès direct à la TOE, après identification et authentification.

P.SECU_ADMIN :

Dans le cas d'un accès distant par un opérateur à la TOE, les communications doivent être protégées en confidentialité, en intégrité et en disponibilité.

P.TRACE :

Toutes les opérations jugées sensibles par l'opérateur doivent être auditées pour ensuite pouvoir être imputées aux entités qui les ont effectuées. Les données d'audit doivent faire l'objet d'un stockage.

P.ROLE :

Chaque opérateur ne doit avoir accès qu’aux fonctions de la TOE nécessaires à l'accomplissement de sa tâche dans le cadre du rôle qui lui est imparti.

P.SECU_INFO :

La TOE doit être capable de reconnaître et traiter les étiquettes de sécurité.

P.MAINTENANCE :

Avant toute intervention de maintenance, les informations sensibles contenues dans la TOE doivent être protégées.

4. Objectifs de sécurité

4.1 Objectifs de sécurité des technologies de l'information

O.I&A :

La TOE doit identifier de manière unique tous les opérateurs de la TOE et authentifier ces opérateurs préalablement à toute opération. Seuls les opérateurs doivent avoir un accès direct à la TOE.

O.CONFIG_TOE :

La TOE doit fournir aux opérateurs les fonctions nécessaires à l'accomplissement de leurs tâches.

O.ROLES :

La TOE ne doit pas permettre aux opérateurs d'effectuer des opérations qui ne sont pas de leur ressort.

O.PROTECT_DONNEES :

Les informations propres à la TOE et les informations utilisateurs stockées temporairement dans la TOE doivent être protégées contre les attaques visant leur confidentialité, leur intégrité et leur disponibilité[1].

O.ACCES_RESEAU :

La TOE doit fournir un contrôle d'accès entre les deux réseaux connectés en filtrant les accès en fonction de règles paramétrées par les opérateurs. Pour certains services, la TOE demande une authentification des utilisateurs.

Les règles utilisables portent sur l'identifiant des utilisateurs en communication, la nature de l'application mise en oeuvre, les commandes effectuées et leurs options, le contrôle des flux d'informations. Ces règles doivent pouvoir être complétées par l'exploitation des étiquettes de sécurité.

O.AUDIT :

[1] Les données sont disponibles si elles n'ont pas été détruites. La disponibilité des données n'inclut pas la disponibilité de la TOE et des fonctions qui permettent d'exploiter ces données.

La TOE doit fournir les moyens d'enregistrer les événements définis par les opérateurs, ainsi que les moyens nécessaires à l'analyse de ces enregistrements, de manière à permettre à l'exploitant chargé de l'analyse de ces traces de détecter les attaques ou tentatives d'attaques, de détecter les erreurs de configuration pouvant affaiblir la TOE, de savoir pour chaque opération relevant de la sécurité, quelle entité l'a réalisée.

4.2 Objectifs de sécurité de l'environnement

O.USAGE :

La TOE doit être le seul point de passage entre les deux réseaux.

O.PERSONNEL :

Les opérateurs doivent être des personnes non hostiles et compétentes, et disposer des moyens nécessaires à leurs tâches. Ils doivent être formés pour exécuter les opérations dont ils ont la charge.

O.PERSONNE_EXT :

Une personne extérieure ayant un accès à la TOE, ne devra pouvoir le faire que conformément à la politique de sécurité mise en place.

O.INSTALLE :

La TOE doit être livrée et installée de manière à respecter la politique de sécurité régissant l'interconnexion des réseaux.

O.PROTECT_TOE :

La TOE doit se trouver dans un local protégé. Les moyens mis en oeuvre doivent être conformes à la politique de sécurité régissant l'interconnexion des réseaux .

5. Exigences de sécurité

5.1 Exigences fonctionnelles

FAU_ARP.1	Security Alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.2	Guarantees of audit data availability
FAU_STG.3	Action in case of possible audit data loss
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_IFF.4	Partial elimination of illicit information flows
FDP_ITC.1	Import of user data without security attributes
FDP_ITT.1	Basic internal transfer protection
FDP_RIP.2	Full residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.3	Unforgeable authentication
FIA_UAU.4	Single-use authentication mechanisms
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
FMT_MOF.1	Management of security functions behaviour

FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_MTD.2	Management of limits on TSF data
FMT_REV.1	Revocation
FMT_SAE.1	Time-limited authorisation
FMT_SMR.2	Restrictions on security roles
FMT_SMR.3	Assuming roles
FPT_AMT.1	Abstract machine testing
FPT_RVM.1	Non-bypassability of the TSP
FPT_STM.1	Reliable time stamps
FPT_TST.1	TSF testing
FTA_MCS.1	Basic limitation on multiple concurrent sessions
FTA_SSL.3	TSF-initiated termination
FTA_TAH.1	TOE access history
FTA_TSE.1	TOE session establishment
FTP_TRP.1	Trusted path

5.2 Texte des exigences fonctionnelles

Dans le corps des composants fonctionnels ci-dessous, certaines opérations ont été complétées. Le choix des opérations résulte de l'expression du besoin. Pour les opérations non complétées, le raffinement indique que le choix est laissé au rédacteur de la cible de sécurité.

5.2.1 Classe Security Audit

FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall take [**the least disruptive action**] upon detection of a potential security violation.

Raffinement : *L'action la moins pénalisante correspond à la génération automatique d'une alarme et l'exécution de l'action associée à la possible violation de la politique de sécurité détectée. Les actions associées aux possibles violations de la politique de sécurité sont définies dans le composant FMT_MOF.1.*

FAU_GEN.1 Audit Data Generation

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

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

b) All auditable events for the [**detailed**] level of audit; and

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

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	Evénements auditables
FAU_ARP.1	• Actions taken due to imminent security violations.
FAU_GEN.1	• -
FAU_GEN.2	• -
FAU_SAA.1	• Enabling and disabling of any of the analysis mechanisms, • Automated responses performed by the tool.
FAU_SAR.1	• Reading of information from the audit records.
FAU_SAR.3	• The parameters used for the viewing.
FAU_SEL.1	• All modifications to the audit configuration that occur while the audit collection functions are operating.
FAU_STG.2	• -
FAU_STG.3	• Actions taken due to exceeding of a threshold.

Composant	Evénements auditables
FDP_ACC.2	• -
FDP_ACF.1	• All requests to perform an operation on an object covered by the SFP, • The specific security attributes used in making an access check.
FDP_IFC.2	• -
FDP_IFF.1	• All decisions on requests for information flow, • The specific security attributes used in making an information flow enforcement decision, • Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).
FDP_IFF.4	• The use of identified illicit information flow channels, • The use of identified illicit information flow channels with estimated maximum capacity exceeding a specified value.
FDP_ITC.1	• All attempts to import user data, including any security attributes, • The specification of security attributes for imported user data supplied by an authorised user.
FDP_ITT.1	• All attempts to transfer user data, including the protection method used and any errors that occurred.
FDP_RIP.2	• -
FDP_SDI.2	• All attempts to check the integrity of user data, including an indication of the results of the check, if performed, • The type of integrity error that occurred, • The action taken upon detection of an integrity error.
FIA_AFL.1	• The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_ATD.1	• -
FIA_SOS.1	• Rejection or acceptance by the TSF of any tested secret, • Identification of any changes to the defined quality metrics.
FIA_UAU.1	• All use of the authentication mechanism, • All TSF mediated actions performed before authentication of the user.
FIA_UAU.3	• Detection of fraudulent authentication data, • All immediate measures taken and results of checks on the fraudulent data.
FIA_UAU.4	• Attempts to reuse authentication data.

Composant	Evénements auditables
FIA_UID.2	• All use of the user identification mechanism, including the user identity provided.
FIA_USB.1	• Success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject).
FMT_MOF.1	• All modifications in the behaviour of the functions in the TSF.
FMT_MSA.1	• All modifications of the values of security attributes.
FMT_MSA.2	• All offered and rejected values for a security attribute, • All offered and accepted secure values for a security attribute.
FMT_MSA.3	• Modifications of the default setting of permissive or restrictive rules, • All modifications of the initial values of security attributes.
FMT_MTD.1	• All modifications to the values of TSF data.
FMT_MTD.2	• All modifications to the limits of TSF data, • All modifications in the actions to be taken in case of violation of the limits.
FMT_REV.1	• All attempts to revoke security attributes.
FMT_SAE.1	• Specification of the expiration time for an attribute, • Action taken due to attribute expiration.
FMT_SMR.2	• Modifications to the group of users that are part of a role, • Unsuccessful attempts to use a role due to the given conditions on the roles, • Every use of the rights of a role.
FMT_SMR.3	• Explicit request to assume a role.
FPT_AMT.1	• Execution of the tests of the underlying machine and the results of the tests.
FPT_RVM.1	• -
FPT_STM.1	• Changes to the time, • Providing a timestamp.
FPT_TST.1	• Execution of the TSF self tests and the results of the tests.
FTA_MCS.1	• Rejection of a new session based on the limitation of multiple concurrent sessions, • Capture of the number of currently concurrent user sessions and the user security attribute(s).
FTA_SSL.3	• Termination of an interactive session by the session locking mechanism.

Composant	Evénements auditables
FTA_TAH.1	• -
FTA_TSE.1	• All attempts at establishment of a user session, • Capture of the value of the selected access parameters (e.g. location of access, time of access).
FTP_TRP.1	• All attempted uses of the trusted path functions, • Identification of the user associated with all trusted path invocations, if available.

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

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

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

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

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

a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;

b) [assignment: *any other rules*].

Raffinement : L'auteur de la cible de sécurité complétera les opérations.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [**the opérateurs**] with the capability to read [**all audit information**] from the audit records.

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

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: *searches, sorting, ordering*] of audit data based on [assignment: *criteria with logical relations*].

Raffinement : L'auteur de la cible de sécurité complétera les opérations.

FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [**object identity, user identity, subject identity, host identity, event type**]

b) [assignment: *list of additional attributes that audit selectivity is based upon*].

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records*] audit records will be maintained when the following conditions occur: [selection: *audit storage exhaustion, failure, attack*].

Raffinement : L'auteur de la cible de sécurité complétera les opérations.

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall take [**the following action**] if the audit trail exceeds [assignment: *pre-defined limit*].

Raffinement : La TSF doit empêcher les occurrences d'actions auditables, exceptées celles des opérateurs qui ne seront pas auditées, en cas de saturation du journal d'audit.

L'auteur de la cible de sécurité complétera l'opération.

5.2.2 Classe User Data Protection

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [assignment: *access control SFP*] on [**any subjects and any objects**] and all operations among subjects and objects covered by the SFP.

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes, named groups of security attributes*].

Raffinement : L'auteur de la cible de sécurité complétera les opérations.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing*

access among controlled subjects and controlled objects using controlled operations on controlled objects].

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

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

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

FDP_IFC.2 Complete information flow control

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

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

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

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [

a) network origin identity of the communication flow (e.g., IP address) ;

b) network destination identity of the communication flow (e.g., IP address) ;

c) user origin identity of the communication flow (user name) (for authentication) ;

d) user destination identity of the communication flow (user name) ;

e) type of application (e.g., FTP, SQL, HTTP, SMTP, TELNET,...) ;

f) type of application command requested (e.g., FTP «get», SQL «select»,...) ;

g) format of the commands (e.g. lowercase, uppercase, length of commands,...);

h) date / time of the access ;

i) number, frequency and throughput of communication flow ;

j) labels ;

k) any other multiple attributes will be specified by the ST author].

Raffinement : *L'auteur de la cible de sécurité complétera la première opération et éventuellement la seconde.*

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

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

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

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

FDP_IFF.1.4 The TSF shall provide the following [assignment: *list of additional SFP capabilities*].

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

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

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

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

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

FDP_IFF.4 Partial elimination of illicit information flows

FDP_IFF.4.1 The TSF shall enforce the [assignment: *information flow control SFP*] to limit the capacity of [assignment: *non-empty list of types of illicit information flows*] to a [assignment: *maximum capacity*].

Raffinement : *L'auteur de la cible de sécurité complétera les opérations.*

FDP_IFF.4.2 The TSF shall prevent the following types of [assignment: *non-empty list of types of illicit information flows*].

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

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [assignment: *access control SFP and/or information flow control SFP*] when importing user data, controlled under the SFP, from outside of the TSC.

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

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [**control with an anti-virus**].

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the [**access control SFP(s) and information flow control SFP(s)**] to prevent the [**disclosure, modification and loss of use**] of user data when it is transmitted between physically-separated parts of the TOE.

FDP_RIP.2 Full residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**allocation of the resource to**] all objects.

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].

Raffinement : L'auteur de la cible de sécurité complétera les opérations.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*].

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

5.2.3 Classe Identification and Authentication

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 TSF shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

Raffinement : L'auteur de la cible de sécurité complétera les opérations.

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 : L'auteur de la cible de sécurité complétera l'opération.

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Raffinement : Pour ce composant, le « user » correspond aux utilisateurs de la TOE.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [**no operations**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Raffinement : Pour ce composant, le « user » correspond aux opérateurs de la TOE.

FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1 The TSF shall [**detect and prevent**] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall [**detect and prevent**] use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism(*s)].

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

Raffinement : Pour ce composant, le « user » correspond à la fois aux utilisateurs de la TOE et aux opérateurs.

FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Raffinement : Pour ce composant, le « user » correspond à la fois aux utilisateurs de la TOE et aux opérateurs.

5.2.4 Classe Security Management

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

Raffinement : *Le tableau suivant complète les trois opérations du composant. Chaque ligne correspond à une itération du composant dans laquelle :*

« Opération » correspond à : [selection: determine the behaviour of, disable, enable, modify the behaviour of],

« Fonction » correspond à : [assignment: list of functions],

« Rôle » correspond à : [assignment: the authorised identified roles].

Opération	Fonction	Rôle
determine the behaviour of	gestion des actions associées aux possibles violations de la politique de sécurité : - mise en mode bloqué de la TOE, - révocation des droits d'accès, - autres fonctions à définir par le rédacteur de la cible de sécurité.	administrateur
determine the behaviour of	sélection de la méthode de protection des données utilisateur transitant dans la TOE	administrateur

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

Raffinement : *Le tableau suivant complète les quatre opérations du composant. Chaque ligne correspond à une itération du composant dans laquelle :*

« Contrôle » correspond à : [assignment: access control SFP, information flow control SFP],

« Opération » correspond à : [selection: change_default, query, modify, delete, [assignment: other operations]],

« Attributs » correspond à : [assignment: list of security attributes],

« Rôle » correspond à : [assignment: the authorised identified roles].

Contrôle	Opération	Attributs	Rôle
access control SFP and information flow control SFP	query	tous les attributs de sécurité	opérateurs
access control SFP	initialise and modify	données d'authentification	administrateur
access control SFP and information flow control SFP	modify	tous les attributs de sécurité	administrateur

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [**access control SFP, information flow control SFP**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**administrateur**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

Raffinement : *Le tableau suivant complète les trois opérations du composant. Chaque ligne correspond à une itération du composant dans laquelle :*

« Opération » correspond à : [selection: change_default, query, modify, delete, clear, [assignment: other operations]],

« Données » correspond à : [assignment: list of TSF data],

« Rôle » correspond à : [assignment: the authorised identified roles].

Opération	Données	Rôle
create or empty	audit trail	administrateur
read or write	audit trail	exploitant sécurité
read	audit trail	opérateurs
use	audit review tools	administrateur

Opération	Données	Rôle
add, modify or delete	rules for monitoring the audited events	administrateur
add, modify or delete	group of users with read access right to the audit records	administrateur
maintain	rights to view/modify the audit events	administrateur
maintain	parameters that control the audit storage capability	administrateur
add, modify, delete	actions to be taken in case of imminent audit storage failure	exploitant sécurité
enable or disable	user account or point of entry	administrateur
display	TOE access parameters	opérateurs
modify	TOE access parameters	administrateur
manage	attributes used to make explicit access or denial based decision	administrateur
manage	threshold for unsuccessful authentication attempts	administrateur
configure	actions to be taken in the event of an authentication failure	administrateur
manage	metric used to verify the secrets	administrateur
manage	authentication data	administrateur
manage	list of actions that can be taken before the user is authenticated	administrateur
manage	user identities	administrateur
define	default subject security attributes	administrateur
manage	group of roles and their associated functions	administrateur
manage	group of users that are part of a role	administrateur
manage	conditions that the roles must satisfy	administrateur
install	TSF	administrateur
set or update	TSF configuration parameters	administrateur
manage	time	administrateur
configure	actions that require trusted path	administrateur
manage	anti-virus	administrateur

Opération	Données	Rôle
configure	actions to be taken upon the detection of an integrity error	administrateur
manage	maximum allowed number of concurrent user sessions	administrateur
specify	time of user inactivity after which termination of the interactive session occurs	administrateur
manage	session establishment conditions	administrateur
manage	lists of users, subjects, objects and other resources for which revocation is possible	administrateur
manage	revocation rules	administrateur
manage	list of security attributes for which expiration is to be supported	administrateur
define	actions to be taken if the expiration time has passed	administrateur

FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment: *actions to be taken*].

Raffinement : *Le tableau suivant complète les trois opérations du composant. Chaque ligne correspond à une itération du composant dans laquelle :*

« Données » correspond à : [assignment: list of TSF data],

« Rôle » correspond à : [assignment: the authorised identified roles],

« Action » correspond à : [assignment: actions to be taken].

Données	Rôle	Action
Limite du journal d'audit	Administrateur	Génération d'une alarme aux opérateurs

FMT_REV.1 Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [**users, subjects, objects**] within the TSC to [**the administrateur**].

FMT_REV.1.2 The TSF shall enforce the rules [**defined above**].

Raffinement : *Les attributs de sécurité d'un utilisateur, sujet ou objet peuvent être immédiatement révoqués par l'administrateur lorsqu'une violation de la politique de sécurité provoquée par cet utilisateur, sujet ou objet est suspectée.*

FMT_SAE.1 Time-limited authorisation

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*] to [**the administrateur**].

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

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.

Raffinement : *Seuls les attributs de sécurité des utilisateurs de la TOE peuvent avoir une date d'expiration. La liste de ces attributs sera définie par le rédacteur de la cible de sécurité.*

L 'auteur de la cible de sécurité complétera l'opération.

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles: [**administrateur et exploitant sécurité**].

Raffinement : *Ces deux rôles sont définis plus en détail dans le glossaire «(voir « opérateur de la cible d'évaluation »).*

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [assignment: *conditions for the different roles*] are satisfied.

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

FMT_SMR.3 Assuming roles

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: [**administrateur et exploitant sécurité**].

5.2.5 Classe Protection of the TOE Security Functions

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall run a suite of tests [**during initial start-up**] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests [**during initial start-up and at the request of the opérateurs**] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

Raffinement : Pour ce composant, « the authorised users » correspond à l'administrateur.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Raffinement : Pour ce composant, « the authorised users » correspond à l'administrateur.

5.2.6 Classe TOE Access

FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [**one**] sessions per user.

Raffinement : Pour ce composant, le « user » correspond aux opérateurs et aux utilisateurs de la TOE.

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**time interval of user inactivity**].

Raffinement : Pour ce composant, le « user » correspond aux opérateurs.

L'intervalle de temps d'inactivité d'un opérateur est paramétrable par l'administrateur.

FTA_TAH.1 TOE access history

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [**date, time, method, location**] of the last successful session establishment to the user.

Raffinement : Pour ce composant, le « user » correspond aux opérateurs.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [**date, time, method, location**] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

Raffinement : Pour ce composant, le « user » correspond aux opérateurs.

FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: *attributes*].

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

5.2.7 Classe Trusted Path/Channels

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [**remote**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

Raffinement : Pour ce composant, « the TSF remote users » correspond aux opérateurs.

FTP_TRP.1.2 The TSF shall permit [**the TSF remote users**] to initiate communication via the trusted path.

Raffinement : Pour ce composant, « the TSF remote users » correspond aux opérateurs.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication*, [assignment: *other services for which trusted path is required*]].

Raffinement : L'auteur de la cible de sécurité complétera l'opération.

5.3 Exigences d'assurance

Le niveau d'assurance retenu est **EAL5** augmenté des composants ALC_FLR.2 et AVA_VLA.4.

Classe Life cycle support

ALC_FLR.2 Flaw reporting procedures

Classe Vulnerability assessment

AVA_VLA.4 Highly resistant

Le niveau de résistance des fonctions de sécurité visé est « **élevé** » (SOF-high). Ce niveau devra être atteint par toutes les fonctions réalisées par un mécanisme de type probabilistique ou permutationel.

6. Précisions

Précisions au titre de l'organisation

Il est conseillé que les personnels extérieurs identifiés comme personnels de maintenance soient accompagnés par un opérateur.

Après une éventuelle défaillance de la TOE, il doit exister des moyens pour redémarrer la TOE dans un délai acceptable au plan opérationnel.

Précisions au titre du développement

La modification de la configuration de la TOE doit être possible dans un délai acceptable au plan opérationnel.

La TOE doit être logiquement transparente pour les utilisateurs connectés.

Précisions au titre des menaces

La menace consistant à exploiter les signaux parasites compromettants émis par la TOE ou à générer des signaux pour perturber la TOE n'est pas traitée dans le cadre de ce profil de protection car les signaux parasites compromettants ne sont pas pris en compte par les Critères Communs.

La menace d'intervention physique sur la TOE (vol total ou partiel, altération physique) n'est pas prise en compte dans le cadre de ce profil de protection. Elle est néanmoins couverte par l'objectif O.PROTECT_TOE.

7. Glossaire

Dans ce profil de protection sont utilisés les termes définis ci-dessous :

- accès direct : connexion locale ou distante pour administrer la TOE,
- attaque : violation ou tentative de violation de la politique de sécurité en vigueur,
- attaquant : utilisateur mais aussi toute autre entité non identifiée comme appartenant à la catégorie des utilisateurs réalisant ou tentant de réaliser une attaque,
- défaillance : cessation de l'aptitude d'un système à accomplir sa mission opérationnelle,
- étiquette de sécurité : label interprétable par la TOE fournissant des renseignements relatifs à la sécurité sur les données auxquelles il est associé,
- événement de sécurité : action portant sur une information sensible ou action mettant en oeuvre une fonction de sécurité,
- information sensible : information dont la divulgation et/ou la modification (incluant la destruction) entraîne une violation de la politique de sécurité,
- opération relevant de la sécurité : toute opération mettant en oeuvre la politique de sécurité en vigueur,
- opérateur de la cible d'évaluation : 2 rôles sont définis pour les aspects sécurité, *l'administrateur* qui administre la cible d'évaluation en configurant les différents paramètres conformément à la politique de sécurité en vigueur et *l'exploitant sécurité* qui analyse les résultats d'audit et transmet une proposition de changement des paramètres si besoin est. Ces rôles peuvent être assurés par une ou plusieurs personnes,
- réseau informatique : ensemble, géographiquement dispersé, de systèmes de traitement de données reliés entre eux pour échanger leurs données, et comprenant les composants des systèmes interconnectés et leurs interfaces avec les réseaux de données ou de communication utilisés.

  ⇒ un réseau informatique peut utiliser les services d'un seul ou plusieurs réseaux de communication ; plusieurs réseaux informatiques peuvent utiliser les services d'un réseau de communication commun;

  ⇒ un réseau informatique est appelé "local" s'il relie entre eux plusieurs équipements de traitement de données situés sur un même site.

- utilisateur : entité humaine ou machine autorisée à l'utilisation d'un équipement de traitement de données du réseau informatique.

8. Argumentaire

8.1 Objectifs de sécurité de la TOE

8.1.1 Couvertures des hypothèses

H.USAGE :

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

- O.USAGE exige que la TOE soit le seul point de passage entre les deux réseaux connectés.

H.PERSONNEL :

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

- O.PERSONNEL implique que les personnels sont compétents et non hostiles.

H.PERSONNE_EXT :

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

- O.PERSONNE_EXT implique que les personnes extérieures ne peuvent agir que conformément à la politique de sécurité mise en place.

H.INSTALLE :

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

- O.INSTALLE implique que la TOE est livrée et installée de manière à respecter la politique de sécurité régissant l'interconnexion des deux réseaux.

H.PROTECT_TOE :

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

- O.PROTECT_TOE implique que la TOE se trouve dans un local protégé.

8.1.2 Couverture des menaces

M.INTRUSION_RESEAU :

M.INTRUSION_RESEAU est couverte par les objectifs O.ACCES_RESEAU, O_USAGE et O.INSTALLE.

- O.ACCES_RESEAU exige que la TOE offre les fonctions de filtrage des flux d'information transitant par la TOE (et pour certains services des fonctions de contrôle de l'authentification des utilisateurs).
- O_USAGE limite la portée de cette menace car la TOE doit être le seul point de passage entre ces réseaux ce qui oblige un attaquant à transiter par la TOE.
- O.INSTALLE limite la portée de cette menace car il implique que la TOE est installée suivant une politique de sécurité prédéfinie incluant une politique de filtrage.

M.INTRUSION_TOE :

M.INTRUSION_TOE est couverte par les objectifs O.I&A, O.ROLES, O.PROTECT_DONNEES, O.AUDIT, O.INSTALLE, O.PERSONNE_EXT et O.PROTECT_TOE.

- O.I&A exige que la TOE identifie et authentifie de manière unique les opérateurs ayant un accès direct à la TOE (un attaquant n'aura donc pas d'identifiant défini et devra trouver l'authentifiant d'un opérateur).
- O.ROLES exige que la TOE permette aux opérateurs de n'accéder qu'aux fonctions nécessaires à l'accomplissement de leurs tâches.
- O.PROTECT_DONNEES exige que les données présentes dans la TOE soient protégées contre toute intervention illicite.
- O.AUDIT limite la portée de cette menace car il implique que tous les événements de sécurité sont audités. Cela permet donc, a posteriori, de détecter une éventuelle intrusion ou tentative d'intrusion dans la TOE.
- O.INSTALLE limite la portée de cette menace car il implique que la TOE est installée suivant une politique de sécurité prédéfinie.
- O.PERSONNE_EXT limite la portée de cette menace car il implique que tout personnel extérieur intervenant sur la TOE ne peut le faire que conformément à une politique de sécurité organisationnelle.
- O.PROTECT_TOE limite la portée de cette menace en limitant l'accès physique à la TOE aux seules personnes autorisées.

M.MAUVAIS_OPE :

M.MAUVAIS_OPE est couverte par les objectifs O.ROLES, O.PROTECT_DONNEES et O.PERSONNEL.

- O.ROLES exige que la TOE ne permette aux opérateurs d'accéder qu'aux fonctions nécessaires à l'accomplissement de leurs tâches.
- O.PROTECT_DONNEES exige que les données présentes dans la TOE soient protégées contre toute intervention illicite.
- O_PERSONNEL limite la portée de cette menace car il implique que les opérateurs sont des personnes de confiance, formées à leur métier.

M.VIRUS :

M.VIRUS est couverte par les objectifs O.PROTECT_DONNEES, O.CONFIG_TOE, O.ROLES, O.INSTALLE et O.PERSONNEL.

- O.PROTECT_DONNEES exige que les données présentes dans la TOE soient protégées contre toute intervention illicite.
- O.CONFIG_TOE exige que la TOE fournisse les fonctions nécessaires à l'accomplissement des tâches des opérateurs.
- O.ROLES exige que la TOE contrôle les droits d'écriture pour chaque opérateur.
- O.INSTALLE limite la portée de cette menace car il implique que la TOE est installée suivant une politique de sécurité prédéfinie.
- O_PERSONNEL limite la portée de cette menace car il implique que les opérateurs sont des personnes de confiance, formées à leur métier.

8.1.3 Couverture des politiques de sécurité organisationnelles

P.OPERATEUR :

P.OPERATEUR est couverte par les objectifs O.I&A, O.ROLES et O.PERSONNE_EXT.

- O.I&A exige que la TOE identifie et authentifie de manière unique les opérateurs ayant un accès direct à la TOE.
- O.ROLES exige que la TOE ne permette aux opérateurs d'accéder qu'aux fonctions nécessaires à l'accomplissement de leurs tâches.
- O.PERSONNE_EXT favorise l'application de cette politique car il implique que tout personnel extérieur intervenant sur la TOE ne peut le faire que conformément à une politique de sécurité organisationnelle.

P.SECU_ADMIN :

P.SECU_ADMIN est couverte par l'objectif O.CONFIG_TOE.

- O.CONFIG_TOE exige que la TOE fournisse les fonctions nécessaires à l'accomplissement des tâches des opérateurs.

P.TRACE :

P.TRACE est couverte par les objectifs O.AUDIT et O.PROTECT_DONNEES.

- O.AUDIT exige que la TOE fournisse les fonctions nécessaires à l'enregistrement de toute attaque ou tentative d'attaque.
- O.PROTECT_DONNEES exige que les données présentes dans la TOE, et en particulier le journal d'audit, soient protégées contre toute intervention illicite.

P.ROLE :

P.ROLE est couverte par les deux objectifs O.ROLES, O.CONFIG_TOE et O.PERSONNEL.

- O.ROLES demande à ce que la TOE ne permette aux opérateurs d'accéder qu'aux fonctions nécessaires à l'accomplissement de leurs tâches.
- O.CONFIG_TOE exige que la TOE fournisse les fonctions nécessaires à l'accomplissement des tâches des opérateurs.
- O_PERSONNEL favorise l'application de cette politique car il implique que les opérateurs sont des personnes de confiance, formées à leur métier.

P.SECU_INFO :

P.SECU_INFO est couverte par l'objectif O.ACCES_RESEAU.

- O.ACCES_RESEAU exige que la TOE offre les fonctions de filtrage nécessaires aux contrôles des flux d'informations pour ceux étiquetées transitant par la TOE.

P.MAINTENANCE :

P.MAINTENANCE est couverte par l'objectif O.PROTECT_DONNEES.

- O.PROTECT_DONNEES exige que les données présentes dans la TOE soient protégées contre toute intervention illicite.

8.1.4 Complétude des objectifs de sécurité

8.1.4.1 Complétude des objectifs des technologies de l'information

O.I&A :

O.I&A couvre la menace M.INTRUSION_TOE et satisfait la politique P.OPERATEUR.

- O.I&A couvre la menace M.INTRUSION_TOE car un attaquant ne pourra obtenir d'accès illégal à la TOE dès lors que sont demandées une identification et une authentification des utilisateurs ayant accès à la TOE,
- O.I&A satisfait la politique P.OPERATEUR car il limite les accès à la TOE aux seuls opérateurs.

O.CONFIG_TOE :

O.CONFIG_TOE couvre la menace M.VIRUS et satisfait les politiques P.ROLE et P.SECU_ADMIN.

- O.CONFIG_TOE couvre la menace M.VIRUS car il offre aux opérateurs une fonctionnalité de contrôle des données introduites dans la TOE,
- O.CONFIG_TOE satisfait la politique P.ROLE car il demande à la TOE de fournir les fonctions nécessaires à l'accomplissement des tâches des opérateurs,
- O.CONFIG_TOE satisfait la politique P.SECU_ADMIN car il permet à la TOE d'offrir aux opérateurs des communications sûres pour l'administration à distance.

O.ROLES :

O.ROLES couvre les menaces M.INTRUSION_TOE, M.MAUVAIS_OPE et M.VIRUS et satisfait les politiques P.ROLE et P.OPERATEUR.

- O.ROLES couvre la menace M.INTRUSION_TOE car un attaquant qui obtiendrait un accès direct à la TOE ne pourrait pas avoir accès à toutes les fonctions,
- O.ROLES couvre la menace M.MAUVAIS_OPE car un opérateur ne pourra effectuer une opération illicite que dans le rôle qui lui est imparti,
- O.ROLES couvre la menace M.VIRUS car il empêche un virus introduit par un opérateur d'altérer des données appartenant à un autre opérateur,
- O.ROLES satisfait la politique P.ROLE car il délimite les fonctions utilisables par chaque opérateur,
- O.ROLES satisfait la politique P.OPERATEUR car il limite l'accès aux fonctions de la TOE aux seuls opérateurs.

O.PROTECT_DONNEES :

O.PROTECT_DONNEES couvre les menaces M.INTRUSION_TOE, M.MAUVAIS_OPE et M.VIRUS et satisfait les politiques P.TRACE et P.MAINTENANCE.

- O.PROTECT_DONNEES couvre la menace M.INTRUSION_TOE car les données stockées dans la TOE sont protégées,
- O.PROTECT_DONNEES couvre la menace M.MAUVAIS_OPE car un opérateur ne pourra effectuer une opération illicite que dans les limites du rôle qui lui est imparti et des droits d'accès qu'il a sur les données,
- O.PROTECT_DONNEES couvre la menace M.VIRUS car il permet de protéger les données présentes dans la TOE contre toute intervention illicite, donc contre l'attaque d'un virus,
- O.PROTECT_DONNEES satisfait la politique P.TRACE car il permet de protéger les informations d'audit contenues dans la TOE,
- O.PROTECT_DONNEES satisfait la politique P.MAINTENANCE car il permet de protéger les données contenues dans la TOE pendant toute intervention de maintenance.

O.ACCES_RESEAU :

O.ACCES_RESEAU couvre la menace M.INTRUSION_RESEAU et satisfait la politique P.SECU_INFO.

- O.ACCES_RESEAU couvre la menace M.INTRUSION_RESEAU car il exige que la TOE filtre tout transfert de flux via la TOE ; il peut notamment empêcher un attaquant de traverser la TOE,
- O.ACCES_RESEAU satisfait la politique P.SECU_INFO car il exige que la TOE exploite des étiquettes de sécurité.

O.AUDIT :

O.AUDIT couvre la menace M.INTRUSION_TOE et satisfait la politique P.TRACE.

- O.AUDIT couvre la menace M.INTRUSION_TOE car il exige que la TOE trace les événements de sécurité, ce qui permet de détecter a posteriori une intrusion ou tentative d'intrusion,
- O.AUDIT satisfait la politique P.TRACE car il exige que la TOE offre les fonctions nécessaires à tout enregistrement d'événement de sécurité et à leur exploitation.

8.1.4.2 Complétude des objectifs de l'environnement

O.USAGE :

O.USAGE couvre la menace M.INTRUSION_RESEAU et l'hypothèse H.USAGE.

- O.USAGE couvre la menace M.INTRUSION_RESEAU car il exige que la TOE soit le seul point de passage entre les deux réseaux connectés. Il limite donc cette menace en imposant un contrôle sur toutes les tentatives d'intrusion.
- O.USAGE couvre l'hypothèse H.USAGE car il exige que la TOE soit le seul point de passage entre les deux réseaux connectés.

O.PERSONNEL :

O.PERSONNEL couvre les menaces M.MAUVAIS_OPE, M.VIRUS, l'hypothèse H.PERSONNEL et satisfait la politique P.ROLE.

- O.PERSONNEL couvre la menace M.MAUVAIS_OPE car il implique que les opérateurs sont des personnes non hostiles et compétentes, et qu'ils sont formés pour exécuter leurs tâches.
- O.PERSONNEL couvre la menace M.VIRUS car il implique que les opérateurs sont des personnes non hostiles. Ils ne vont donc pas volontairement introduire un virus dans la TOE.
- O.PERSONNEL satisfait la politique P.ROLE car il implique que les opérateurs disposent des moyens nécessaires à l'accomplissement de leurs tâches.
- O.PERSONNEL couvre l'hypothèse H.PERSONNEL car il implique que les opérateurs sont des personnes non hostiles et compétentes.

O.PERSONNE_EXT :

O.PERSONNE_EXT couvre la menace M.INTRUSION_TOE, l'hypothèse H.PERSONNE_EXT et satisfait la politique P.OPERATEUR.

- O.PERSONNE_EXT couvre la menace M.INTRUSION_TOE car il implique que l'accès de personnes extérieures à la TOE se fait conformément à la politique de sécurité, donc probablement accompagnées des opérateurs.
- O.PERSONNE_EXT satisfait la politique P.OPERATEUR car il implique que l'accès de personnes extérieures à la TOE se fait conformément à la politique de sécurité, donc probablement par les accès directs des opérateurs, surveillés par les opérateurs..
- O.PERSONNE_EXT couvre l'hypothèse H.PERSONNE_EXT car il implique que l'accès de personnes extérieures à la TOE se fait conformément à la politique de sécurité.

O.INSTALLE :

O.INSTALLE couvre les menaces M.INTRUSION_RESEAU, M.INTRUSION_TOE et M.VIRUS, et l'hypothèse H.INSTALLE.

- O.INSTALLE couvre la menace M.INTRUSION_RESEAU car il implique que la TOE est installée avec des paramètres de filtrage restrictifs, donc empêchant les intrusions.
- O.INSTALLE couvre la menace M.INTRUSION_TOE car il implique que la TOE est installée avec des paramètres d'accès réduits, donc empêchant les intrusions.
- O.INSTALLE couvre la menace M.VIRUS car il implique qu'il n'y a pas de virus ou logiciels non autorisés après l'installation de la TOE.
- O.INSTALLE couvre l'hypothèse H.INSTALLE puisqu'il implique que la TOE est livrée et installée de manière à respecter la politique de sécurité régissant l'interconnexion des deux réseaux.

O.PROTECT_TOE :

O.PROTECT_TOE couvre la menace M.INTRUSION_TOE et l'hypothèse H.PROTECT_TOE.

- O.PROTECT_TOE couvre la menace M.INTRUSION_TOE puisqu'il implique que la TOE se trouve dans un local protégé, donc empêchant les attaquants d'atteindre la TOE physiquement.
- O.PROTECT_TOE couvre l'hypothèse H.PROTECT_TOE puisqu'il implique que la TOE se trouve dans un local protégé.

8.1.5 Récapitulatif des relations Menaces-Politiques / Objectifs-Hypothèses

	O.I&A	O.CONFIG_TOE	O.ROLES	O.PROTECT_DONNEES	O.ACCES_RESEAU	O.AUDIT	O.USAGE	O.PERSONNEL	O.PERSONNE_EXT	O.INSTALLE	O.PROTECT_TOE
M.INTRUSION_RESEAU					X		X			X	
M.INTRUSION_TOE	X		X	X		X			X	X	X
M.MAUVAIS_OPE			X	X				X			
M.VIRUS		X	X	X				X		X	
P.OPERATEUR	X		X						X		
P.SECU_ADMIN		X									
P.TRACE				X		X					
P.ROLE		X	X					X			
P.SECU_INFO					X						
P.MAINTENANCE				X							
H.USAGE							X				
H.PERSONNEL								X			
H.PERSONNE_EXT									X		
H.INSTALLE										X	
H.PROTECT_TOE											X

Le tableau ci-dessus 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.

8.2 Exigences fonctionnelles de la TOE

8.2.1 Argumentaire pour la classe FAU : Security Audit

FAU_ARP.1 Security Alarms

Ce composant répond à l'objectif O.AUDIT puisqu'il permet de générer des alarmes si une violation de la sécurité a été détectée. Cette fonctionnalité satisfait à l'exigence «détecter les attaques ou tentative d'attaques» de l'objectif O.AUDIT.

Ce composant répond à l'objectif O.ACCES_RESEAU puisqu'il permet de détecter toute violation de la sécurité par un utilisateur.

FAU_GEN.1 Audit Data Generation

Ce composant est indispensable pour satisfaire à l'objectif O.AUDIT puisqu'il impose à la TSF de générer un journal d'audit.

Il permet également de définir le niveau d'audit (detailed) requis pour les composants fonctionnels utilisés dans ce PP. Seuls les composants fonctionnels pour lesquels l'audit est imposé par les CC seront audités ; ce PP n'étend pas la fonction d'audit à d'autres composants comme le propose l'élément FAU_GEN.1.1c.

FAU_GEN.2 User identity association

Ce composant répond à l'objectif O.AUDIT puisqu'il permet d'associer à tout événement auditable l'identité de l'utilisateur et 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.

FAU_SAA.1 Potential violation analysis

Ce composant participe à l'action de l'objectif O.AUDIT car il fournit les moyens nécessaires à l'analyse des enregistrements en proposant des règles de gestion des événements audités.

Ce composant répond à l'objectif O.ACCES_RESEAU puisqu'il permet de définir les règles qui mettront en évidence une violation ou tentative de violation de la politique de sécurité par un utilisateur.

FAU_SAR.1 Audit review

Ce composant répond à l'objectif 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 l'exploitant sécurité.

FAU_SAR.3 Selectable audit review

Ce composant répond à l'objectif O.AUDIT car il fournit des outils de revue des données d'audit, donc de ce fait fournit les moyens nécessaires à l'analyse des enregistrements des événements relevant de la sécurité.

Ce composant répond à l'objectif O.CONFIG_TOE puisqu'il fournit les outils nécessaires à l'exploitation des traces d'audit.

FAU_SEL.1 Selective audit

Ce composant répond à l'objectif O.AUDIT puisqu'il permet aux opérateurs de définir les événements auditables.

Ce composant répond à l'objectif O.CONFIG_TOE puisqu'il fournit les outils nécessaires au paramétrage des événements auditables.

FAU_STG.2 Guarantees of audit data availability

Ce composant répond à l'objectif O.AUDIT puisqu'il garantit que les enregistrements générés sont stockés dans un journal d'audit protégé contre la destruction ou la modification non autorisées. De plus, il limite les pertes des données d'audit en cas de saturation du journal d'audit ou de dysfonctionnement.

Ce composant répond à l'objectif O.PROTECT_DONNEES car il permet la protection du journal d'audit.

FAU_STG.3 Action in case of possible audit data loss

Ce composant répond à l'objectif O.AUDIT puisqu'il définit les actions à mener en cas de saturation du journal d'audit, de manière à perdre le minimum d'informations.

8.2.2 Argumentaire pour la classe FDP : User Data Protection

FDP_ACC.2 Complete access control

Ce composant répond directement à l'objectif O.ROLES puisqu'il permet un contrôle d'accès sur tous les objets et toutes les opérations. Ce composant empêche donc un opérateur d'effectuer des opérations qui ne sont pas de son ressort.

Ce composant répond à l'objectif O.PROTECT_DONNEES puisqu'il fournit un contrôle d'accès sur tous les objets de la TOE et empêche donc un opérateur ou un utilisateur mal intentionné de lire, modifier ou détruire les données contenues dans la TOE (données permanentes ou données temporaires), et qui ne lui appartiennent pas.

FDP_ACF.1 Security attribute based access control

Ce composant répond directement à l'objectif O.ROLES puisqu'il définit les règles de contrôle de la validité des opérations demandées. Ces règles sont basées sur l'identité des opérateurs et les caractéristiques des rôles. Ce composant permet donc d'autoriser ou d'interdire un accès par rapport aux valeurs des attributs définis des sujets utilisant la TOE.

Ce composant répond à l'objectif O.PROTECT_DONNEES puisqu'il permet de protéger en confidentialité, intégrité et disponibilité les données contenues dans la TOE en mettant en place un contrôle d'accès sur ces données.

FDP_IFC.2 Complete information flow control

Ce composant répond directement à l'objectif O.ACCES_RESEAU puisqu'il fournit un contrôle d'accès sur tous les objets et toutes les opérations transitant par la TOE.

Ce composant répond directement à l'objectif O.PROTECT_DONNEES puisqu'il fournit un contrôle d'accès sur toutes les données contenues dans la TOE.

FDP_IFF.1 Simple security attributes

Ce composant répond directement à l'objectif O.ACCES_RESEAU puisqu'il définit les paramètres sur lesquels le contrôle d'accès sera effectué, ainsi que les règles de contrôle d'accès.

FDP_IFF.4 Partial elimination of illicit information flows

Ce composant répond directement à l'objectif O.ACCES_RESEAU puisqu'il limite les canaux cachés. Il limite donc les communications qui ne seraient pas soumises au contrôle d'accès mis en place.

Ce composant répond indirectement à l'objectif O.PROTECT_DONNEES puisqu'il protège les informations contenues dans la TOE d'une divulgation illicite vers des sujets extérieurs.

FDP_ITC.1 Import of user data without security attributes

Ce composant répond directement à l'objectif O.PROTECT_DONNEES puisqu'il effectue un contrôle sur toutes les données importées, de manière à empêcher par exemple l'introduction d'un virus.

FDP_ITT.1 Basic internal transfer protection

Ce composant répond directement à l'objectif O.PROTECT_DONNEES puisqu'il protège dans la TOE les données des utilisateurs qui transitent en empêchant leur modification, leur lecture ou leur mise en indisponibilité.

FDP_RIP.2 Full residual information protection

Ce composant répond directement à l'objectif O.PROTECT_DONNEES puisqu'il rend indisponible toute donnée qui n'est plus utilisée et dont l'espace mémoire ou disque est réutilisé. Ceci empêche donc un utilisateur malveillant de relire des données auxquelles il ne doit pas avoir accès.

FDP_SDI.2 Stored data integrity monitoring and action

Ce composant répond directement à l'objectif O.PROTECT_DONNEES puisqu'il permet d'une part de détecter des erreurs d'intégrité sur les données contenues dans la TOE et d'autre part d'effectuer des opérations (à définir par le rédacteur de la cible de sécurité) en cas de perte d'intégrité de ces données.

8.2.3 Argumentaire pour la classe FIA : Identification and Authentication

FIA_AFL.1 Authentication failure handling

Ce composant est inclus pour supporter O.I&A car il définit les actions à exécuter en cas d'échec d'authentification. Ceci permet de limiter l'accès direct à la TOE aux seuls opérateurs : le fait de limiter le nombre de tentatives de connexions empêche un attaquant d'usurper l'identité d'un opérateur (par essais successifs).

Ce composant est inclus pour supporter O.ACCES_RESEAU car il définit les actions à exécuter en cas d'échec d'authentification. Ceci permet de limiter l'utilisation des services nécessitant une authentification aux seuls utilisateurs autorisés : le fait de limiter le nombre de tentatives de connexions empêche un attaquant d'usurper l'identité d'un utilisateur autorisé (par essais successifs).

FIA_ATD.1 User attribute definition

Ce composant est inclus pour supporter O.I&A car il associe à chaque opérateur un jeu d'attributs de sécurité, donc des attributs pour l'identification et l'authentification.

Ce composant est inclus pour supporter O.ROLES car il associe à chaque opérateur des attributs de sécurité lui permettant d'effectuer des opérations et lui interdisant l'accès à celles qu'il n'a pas à utiliser.

Ce composant est inclus pour supporter O.ACCES_RESEAU car il associe à chaque utilisateur un jeu d'attributs de sécurité, donc des attributs pour l'identification, l'authentification et le contrôle d'accès.

FIA_SOS.1 Verification of secrets

Ce composant est inclus pour supporter O.CONFIG_TOE car il fournit un mécanisme pour vérifier que les secrets correspondent bien à un niveau de qualité défini. C'est l'aspect "fourniture de mécanisme" qui justifie ce composant.

FIA_UAU.1 Timing of authentication

Ce composant est inclus pour supporter O.ACCES_RESEAU car il implique qu'un utilisateur peut exécuter un certain nombre d'actions sans être au préalable authentifié et doit être authentifié pour exécuter les autres.

Ce composant est inclus pour supporter O.I&A car il implique qu'un opérateur ne peut rien exécuter sans être au préalable authentifié.

FIA_UAU.3 Unforgeable authentication

Ce composant est inclus pour supporter O.I&A et O.ACCES_RESEAU (uniquement pour l'authentification) car il exige que le mécanisme d'authentification puisse détecter et prévenir l'utilisation de données d'authentification contrefaites ou copiées.

FIA_UAU.4 Single-use authentication mechanisms

Ce composant est inclus pour supporter O.I&A car il oblige l'utilisation d'un mécanisme d'authentification qui fonctionne avec une seule utilisation des données d'authentification.

FIA_UID.2 User identification before any action

Ce composant est inclus pour supporter O.I&A car il implique qu'un opérateur ne peut rien exécuter sans être au préalable identifié.

Ce composant est inclus pour supporter O.ACCES_RESEAU car il implique qu'un utilisateur ne peut rien exécuter sans être au préalable identifié.

Ce composant soutient l'objectif O.AUDIT puisqu'il permet d'associer à chaque utilisateur et opérateur un identifiant qui sera ensuite utilisé pour l'imputabilité dans le journal d'audit.

FIA_USB.1 User-subject binding

Ce composant est inclus pour supporter O.ROLES car il associe les attributs de sécurité d'un opérateur avec tout sujet agissant au nom de cet opérateur.

Ce composant est inclus pour supporter O.ACCES_RESEAU car il associe les attributs de sécurité d'un utilisateur avec tout sujet agissant au nom de cet utilisateur.

8.2.4 Argumentaire pour la classe FMT : Security Management

FMT_MOF.1 Management of security functions behaviour

Ce composant répond à l'objectif O.CONFIG_TOE puisqu'il fournit aux opérateurs des fonctions de gestion de la TOE, de manière à leur permettre de changer le comportement de la TOE selon les besoins (en cas de violation de la politique de sécurité par exemple).

Ce composant répond à l'objectif O.ROLES puisqu'il définit les attributions respectives de chacun des deux rôles prédéfinis.

Ce composant répond à l'objectif O.AUDIT puisqu'il permet de configurer la TOE dans un mode donné (par exemple le mode bloqué) lorsque une attaque/erreur ou une tentative d'attaque/d'erreur a été détectée.

Ce composant répond à l'objectif O.ACCES_RESEAU puisqu'il permet de répondre à une violation ou tentative de violation de la politique de sécurité par un utilisateur en modifiant le comportement de la TOE.

FMT_MSA.1 Management of security attributes

Ce composant répond à l'objectif O.CONFIG_TOE puisqu'il fournit aux opérateurs des fonctions de gestion des attributs de sécurité.

Ce composant répond à l'objectif O.ROLES puisqu'il définit les attributions respectives de chacun des deux rôles prédéfinis.

Ce composant répond aux objectifs O.I&A et O.ACCES_RESEAU puisqu'il fournit des fonctions de protection et d'initialisation des données d'authentification, et de protection des données de contrôle d'accès.

Ce composant répond à l'objectif O.PROTECT_DONNEES puisqu'il limite les accès aux attributs de sécurité aux opérateurs de la TOE.

FMT_MSA.2 Secure security attributes

Ce composant répond à l'objectif O.CONFIG_TOE puisqu'il fournit une fonction de contrôle des valeurs des attributs de sécurité, ce qui permet d'aider les opérateurs et de vérifier que les valeurs modifiées sont valides et permettent donc de respecter la politique de sécurité.

FMT_MSA.3 Static attribute initialisation

Ce composant répond directement à l'objectif O.CONFIG_TOE puisqu'il fournit à l'administrateur une fonctionnalité lui permettant de réaliser ses tâches. Cette fonctionnalité lui permet d'attribuer des valeurs par défaut aux attributs de sécurité des objets ou sujets créés.

Ce composant répond indirectement à l'objectif O.ROLES puisqu'il implique que les attributs associés aux objets de la TOE sont par défaut restrictifs, ce qui empêche un nouvel opérateur pour lequel l'administrateur n'a pas encore configuré les attributs de sécurité d'accéder à des opérations qui ne sont pas de son ressort.

Ce composant répond indirectement à l'objectif O.PROTECT_DONNEES puisqu'il implique que les attributs associés aux objets de la TOE sont par défaut restrictifs, ce qui empêche un opérateur d'accéder à des données nouvellement créées et qu'il n'a pas à connaître.

FMT_MTD.1 Management of TSF data

Ce composant répond à l'objectif O.CONFIG_TOE puisqu'il fournit aux opérateurs des fonctions de gestion des données de la TOE.

Ce composant répond à l'objectif O.ROLES puisqu'il définit les attributions respectives de chacun des deux rôles prédéfinis.

Ce composant répond à l'objectif O.AUDIT puisqu'il fournit des fonctions de gestion du journal d'audit, un contrôle d'accès sur le journal d'audit, …

Ce composant répond à l'objectif O.PROTECT_DONNEES car il permet la protection des données de la TOE en restreignant leur accès aux opérateurs.

FMT_MTD.2 Management of limits on TSF data

Ce composant répond à l'objectif O.CONFIG_TOE puisqu'il fournit à l'administrateur des fonctions de gestion des limites des données de la TOE.

Ce composant répond à l'objectif O.ROLES puisqu'il définit les attributions respectives de chacun des deux rôles prédéfinis.

Ce composant répond à l'objectif O.AUDIT puisqu'il permet de générer une alarme lorsque le journal d'audit est saturé. De plus il offre la possibilité à l'administrateur de prédéfinir la limite du taux de remplissage du journal d'audit qui, si elle est atteinte, déclenche une alarme.

FMT_REV.1 Revocation

Ce composant est inclus pour supporter l'objectif O.CONFIG_TOE puisque la révocation des droits d'accès fait partie des fonctionnalités nécessaires à l'administrateur pour configurer la TOE conformément à la politique de sécurité en vigueur.

Ce composant répond à l'objectif O.ROLES puisqu'il définit les attributions respectives de chacun des deux rôles prédéfinis.

Ce composant est inclus pour supporter les objectifs O.I&A et O.ACCES_RESEAU puisqu'il fournit un moyen de réaction immédiate pour l'administrateur en cas de détection ou de suspicion de violation de la politique de sécurité en vigueur : la révocation des droits d'accès.

FMT_SAE.1 Time-limited authorisation

Ce composant est inclus pour supporter l'objectif O.CONFIG_TOE. En effet, ce composant fournit à l'administrateur une fonction pour définir une durée maximale de validité d'un attribut de sécurité, ainsi que le comportement de la TOE lorsque la date d'expiration est dépassée.

Ce composant répond à l'objectif O.ROLES puisqu'il définit les attributions respectives de chacun des deux rôles prédéfinis.

Ce composant répond à l'objectif O.ACCES_RESEAU puisqu'il fournit un moyen de limitation des accès réseau (en posant une date d'expiration sur les attributs des utilisateurs), donc une limitation des attaques possibles.

FMT_SMR.2 Restrictions on security roles

Ce composant répond à l'objectif O.ROLES puisqu'il définit les deux rôles nécessaires à la gestion de la TOE.

Ce composant répond à l'objectif O.CONFIG_TOE puisqu'il fournit des fonctions de gestion des rôles.

FMT_SMR.3 Assuming roles

Ce composant répond à l'objectif O.ROLES puisqu'il empêche un opérateur qui n'a pas explicitement demandé à agir en tant que membre d'un rôle donné d'effectuer des opérations qu'il n'a pas à effectuer.

8.2.5 Argumentaire pour la classe FPT : Protection of the TOE Security Functions

FPT_AMT.1 Abstract machine testing

Ce composant est inclus pour supporter l'objectif O.PROTECT_DONNEES puisque l'auto-test de la TOE lors de son démarrage garantit son intégrité et son bon fonctionnement et permet donc à la TOE de remplir de façon satisfaisante sa mission opérationnelle de filtrage.

FPT_RVM.1 Non-bypassability of the TSP

Ce composant est inclus pour supporter tous les objectifs de sécurité des TI puisqu'il empêche le contournement des fonctions de sécurité.

FPT_STM.1 Reliable time stamps

Ce composant répond à l'objectif O.AUDIT puisqu'il permet d'avoir une heure sûre, ce qui implique que les informations concernant la date et l'heure dans les traces d'audit sont fiables.

Ce composant répond à l'objectif O.ACCES_RESEAU puisqu'il permet d'avoir une heure sûre pour la gestion des dates d'expiration des attributs de sécurité.

FPT_TST.1 TSF testing

Ce composant est inclus pour supporter l'objectif O.PROTECT_DONNEES. En effet, l'auto-test de la TOE lors de son démarrage garantit son intégrité et son bon fonctionnement et permet donc à la TOE de remplir de façon satisfaisante sa mission opérationnelle de filtrage.

Ce composant répond à l'objectif O.CONFIG_TOE puisqu'il fournit aux opérateurs une fonction de contrôle de la TOE, qui permet ainsi de vérifier que la TOE est opérationnelle.

8.2.6 Argumentaire pour la classe FTA : TOE Access

FTA_MCS.1 Basic limitation on multiple concurrent sessions

Ce composant est inclus pour supporter l'objectif O.ACCES_RESEAU puisqu'il permet, en limitant le nombre de sessions concurrentes d'un même utilisateur, d'empêcher une saturation du réseau.

FTA_SSL.3 TSF-initiated termination

Ce composant répond à l'objectif O.I&A puisqu'il empêche un attaquant d'utiliser la session d'un opérateur qui ne se serait pas déconnecté, et donc d'utiliser la TOE sans passer par une étape d'identification et d'authentification.

FTA_TAH.1 TOE access history

Ce composant répond indirectement à l'objectif O.I&A puisqu'il permet à un opérateur de détecter une intrusion ou tentative d'intrusion avec son identifiant, donc une violation de l'objectif O.I&A.

FTA_TSE.1 TOE session establishment

Ce composant répond directement à l'objectif O.I&A puisqu'il permet d'interdire l'accès à la TOE à partir d'attributs, donc à partir de l'identifiant fourni par exemple.

Ce composant répond indirectement à l'objectif O.CONFIG_TOE puisqu'il permet à l'administrateur de définir les conditions pour pouvoir établir une session sur la TOE.

8.2.7 Argumentaire pour la classe FTP : Trusted Path/Channels

FTP_TRP.1 Trusted path

Ce composant répond directement à l'objectif O.CONFIG_TOE puisqu'il permet aux opérateurs de se connecter à distance pour effectuer l'administration de la TOE, tout en ayant un chemin de confiance entre la TOE et leur terminal.

Ce composant répond directement à l'objectif O.I&A puisqu'il fournit un chemin sûr pour la connexion à distance des opérateurs, empêchant ainsi l'observation des données d'authentification et leur utilisation par un attaquant.

Ce composant répond directement à l'objectif O.PROTECT_DONNEES puisque l'utilisation d'un chemin de confiance pour l'administration à distance de la TOE permet la protection des données d'administration (protection en confidentialité et intégrité).

8.3 Satisfaction des objectifs de sécurité

Composant	Texte	O.I&A	O.CONFIG_TOE	O.ROLES	O.PROTECT_DONNEES	O.ACCES_RESEAU	O.AUDIT
FAU_ARP.1	Security Alarms					X	X
FAU_GEN.1	Audit data generation						X
FAU_GEN.2	User identity association						X
FAU_SAA.1	Potential violation analysis					X	X
FAU_SAR.1	Audit review						X
FAU_SAR.3	Selectable audit review		X				X
FAU_SEL.1	Selective audit		X				X
FAU_STG.2	Guarantees of audit data availability				X		X
FAU_STG.3	Action in case of possible audit data loss						X
FDP_ACC.2	Complete access control			X	X		
FDP_ACF.1	Security attribute based access control			X	X		
FDP_IFC.2	Complete information flow control				X	X	
FDP_IFF.1	Simple security attributes					X	
FDP_IFF.4	Partial elimination of illicit information flows				X	X	
FDP_ITC.1	Import of user data without security attributes				X		
FDP_ITT.1	Basic internal transfer protection				X		
FDP_RIP.2	Full residual information protection				X		
FDP_SDI.2	Stored data integrity monitoring and action				X		
FIA_AFL.1	Authentication failure handling	X				X	
FIA_ATD.1	User attribute definition	X		X		X	
FIA_SOS.1	Verification of secrets		X				

Composant	Texte	O.I&A	O.CONFIG_TOE	O.ROLES	O.PROTECT_DONNEES	O.ACCES_RESEAU	O.AUDIT
FIA_UAU.1	Timing of authentication	X				X	
FIA_UAU.3	Unforgeable authentication	X				X	
FIA_UAU.4	Single-use authentication mechanisms	X					
FIA_UID.2	User identification before any action	X				X	X
FIA_USB.1	User-subject binding			X		X	
FMT_MOF.1	Management of security functions behaviour		X	X		X	X
FMT_MSA.1	Management of security attributes	X	X	X	X	X	
FMT_MSA.2	Secure security attributes		X				
FMT_MSA.3	Static attribute initialisation		X	X	X		
FMT_MTD.1	Management of TSF data		X	X	X		X
FMT_MTD.2	Management of limits on TSF data		X	X			X
FMT_REV.1	Revocation	X	X	X		X	
FMT_SAE.1	Time-limited authorisation		X	X		X	
FMT_SMR.2	Restrictions on security roles		X	X			
FMT_SMR.3	Assuming roles			X			
FPT_AMT.1	Abstract machine testing				X		
FPT_RVM.1	Non-bypassability of the TSP	X	X	X	X	X	X
FPT_STM.1	Reliable time stamps					X	X
FPT_TST.1	TSF testing		X		X		
FTA_MCS.1	Basic limitation on multiple concurrent sessions					X	
FTA_SSL.3	TSF-initiated termination	X					
FTA_TAH.1	TOE access history	X					

Composant	Texte	O.I&A	O.CONFIG_TOE	O.ROLES	O.PROTECT_DONNEES	O.ACCES_RESEAU	O.AUDIT
FTA_TSE.1	TOE session establishment	X	X				
FTP_TRP.1	Trusted path	X	X		X		

8.4 Argumentaire des exigences d'assurance

La TOE doit protéger les réseaux et les informations qu'ils contiennent contre des attaquants disposant de compétences élevées et de moyens techniques et financiers importants. Le niveau EAL5 retenu, augmenté des deux composants ALC_FLR.2 et AVA_VLA.4 et le choix de SOF-high pour la résistance des fonctions de sécurité, permettent d'assurer :

- une visibilité complète sur le développement,
- une maîtrise complète de la TOE (documentation et code source entièrement disponibles),
- un processus de développement efficace pour la correction des anomalies détectées,
- des mécanismes résistants à des attaquants disposant de moyens importants.

8.5 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.

8.5.1 Dépendances des exigences fonctionnelles

Légende du tableau :

- case commentaires : « Ok (FAU_STG.2) » signifie que le composant est déjà inclus par le biais de l'inclusion du composant FAU_STG.2

- case commentaires : « Ok (EAL5) signifie que le composant sera traité par le niveau EAL5.

Composant fonctionnel	Dépendances	Commentaires
FAU_ARP.1	FAU_SAA.1	Ok
FAU_GEN.1	FPT_STM.1	Ok
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Ok Ok (FIA_UID.2)
FAU_SAA.1	FAU_GEN.1	Ok
FAU_SAR.1	FAU_GEN.1	Ok
FAU_SAR.3	FAU_SAR.1	Ok
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Ok Ok
FAU_STG.2	FAU_GEN.1	Ok
FAU_STG.3	FAU_STG.1	Ok (FAU_STG.2)
FDP_ACC.2	FDP_ACF.1	Ok
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Ok (FDP_ACC.2) Ok
FDP_IFC.2	FDP_IFF.1	Ok
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Ok (FDP_IFC.2) Ok
FDP_IFF.4	AVA_CCA.1 FDP_IFC.1	Ok (EAL5) Ok (FDP_IFC.2)
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	Ok (FDP_ACC.2) Ok (FDP_IFC.2) Ok
FDP_ITT.1	[FDP_ACC.1 or FDP_IFC.1]	Ok (FDP_ACC.2) Ok (FDP_IFC.2)
FDP_RIP.2	-	
FDP_SDI.2	-	
FIA_AFL.1	FIA_UAU.1	Ok
FIA_ATD.1	-	
FIA_SOS.1	-	
FIA_UAU.1	FIA_UID.1	Ok (FIA_UID.2)
FIA_UAU.3	-	

Composant fonctionnel	Dépendances	Commentaires
FIA_UAU.4	-	
FIA_UID.2	-	
FIA_USB.1	FIA_ATD.1	Ok
FMT_MOF.1	FMT_SMR.1	Ok (FMT_SMR.2)
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1	Ok (FDP_ACC.2) Ok (FDP_IFC.2) Ok (FMT_SMR.2)
FMT_MSA.2	ADV_SPM.1 [FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	Ok (ADV_SPM.3 inclus dans EAL5) Ok (FDP_ACC.2) Ok (FDP_IFC.2) Ok Ok (FMT_SMR.2)
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Ok Ok (FMT_SMR.2)
FMT_MTD.1	FMT_SMR.1	Ok (FMT_SMR.2)
FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	Ok Ok (FMT_SMR.2)
FMT_REV.1	FMT_SMR.1	Ok (FMT_SMR.2)
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	Ok (FMT_SMR.2) Ok
FMT_SMR.2	-	
FMT_SMR.3	FMT_SMR.1	Ok (FMT_SMR.2)
FPT_AMT.1	-	
FPT_RVM.1	-	
FPT_STM.1	-	
FPT_TST.1	FPT_AMT.1	Ok
FTA_MCS.1	FIA_UID.1	Ok (FIA_UID.2)
FTA_SSL.3	-	
FTA_TAH.1	-	
FTA_TSE.1	-	
FTP_TRP.1	-	

Toutes les dépendances des composants fonctionnels sont couvertes.

8.5.2 Dépendances des exigences d'assurance

Le niveau EAL5 est constitué d'un ensemble de composants d'assurance complet, c'est-à-dire que toutes les dépendances des composants inclus sont couvertes. Les dépendances des exigences d'assurance sont donc analysées uniquement pour les composants d'assurance ajoutés au niveau EAL5.

Composant d'assurance	Dépendances	Commentaire
ALC_FLR.2	-	-
AVA_VLA.4	ADV_FSP.1	Ok (ADV_FSP.3 inclus dans EAL5)
	ADV_HLD.2	Ok (ADV_HLD.3 inclus dans EAL5)
	ADV_IMP.1	Ok (ADV_IMP.2 inclus dans EAL5)
	ADV_LLD.1	Ok (inclus dans EAL5)
	AGD_ADM.1	Ok (inclus dans EAL5)
	AGD_USR.1	Ok (inclus dans EAL5)

Toutes les dépendances des composants d'assurance sont couvertes.

8.5.3 Support mutuel des composants de sécurité

Par définition et construction des CC, les composants d'assurance constituant le niveau EAL5 se supportent mutuellement. L'ajout de deux composants d'assurance (ALC_FLR.2 et AVA.VLA.4) ne change en rien le support mutuel des composants d'assurance.

Par définition, les composants d'assurance supportent les composants fonctionnels en fournissant l'assurance que ces composants fonctionnels seront bien mis en œuvre par la TOE.

Il reste donc à montrer que les composants fonctionnels retenus se supportent mutuellement. Le tableau suivant montre le support apporté par certains composants aux autres composants. Quatre formes de support ont été identifiées :

- un composant empêche le contournement d'un autre composant,
- un composant empêche l'altération d'un autre composant,
- un composant empêche la désactivation d'un autre composant
- un composant offre une fonctionnalité indispensable à un autre composant (ce cas est couvert par la couverture des dépendances entre composants et n'apparaît donc pas dans le tableau).

Les composants FPT_AMT.1 et FPT_TST.1 apportent un support contre l'altération à tous les composants. Les composants indiqués dans le tableau dans la colonne « Altération » viennent en complément de ces deux composants. Lorsque cette case est vide, cela signifie que seuls ces deux composants fournissent une protection contre l'altération.

	Composants fournissant une protection contre		
Composant	Contournement	Altération	Désactivation
FAU_ARP.1	FPT_RVM.1	FMT_MTD.1	FAU_GEN.1 FAU_SAA.1
FAU_GEN.1	FPT_RVM.1	FAU_STG.2 FMT_MTD.1	FAU_STG.2
FAU_GEN.2	FPT_RVM.1 FIA_UID.2	FMT_MSA.1 FMT_MTD.1	N/A
FAU_SAA.1	FPT_RVM.1	FMT_MTD.1	FAU_GEN.1
FAU_SAR.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FAU_SAR.3	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A

	Composants fournissant une protection contre		
Composant	Contournement	Altération	Désactivation
FAU_SEL.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	FAU_GEN.1
FAU_STG.2	FPT_RVM.1	FMT_MTD.1	N/A
FAU_STG.3	FPT_RVM.1	FAU_STG.2 FMT_MTD.1	FAU_GEN.1
FDP_ACC.2	FPT_RVM.1 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	N/A
FDP_ACF.1	FPT_RVM.1 FDP_ACC.2	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2
FDP_IFC.2	FPT_RVM.1 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	N/A
FDP_IFF.1	FPT_RVM.1 FDP_IFC.2	FMT_MSA.1 FMT_MTD.1	FDP_IFC.2
FDP_IFF.4	FPT_RVM.1 FDP_IFC.2	FMT_MSA.1 FMT_MTD.1	FDP_IFC.2
FDP_ITC.1	FPT_RVM.1 FDP_ACC.2 FDP_IFC.2	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2 FDP_IFC.2
FDP_ITT.1	FPT_RVM.1 FDP_ACC.2 FDP_IFC.2	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2 FDP_IFC.2
FDP_RIP.2	N/A	FMT_MTD.1	N/A
FDP_SDI.2	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2 FDP_IFC.2
FIA_AFL.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	FIA_UAU.1
FIA_ATD.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FIA_SOS.1	FPT_RVM.1	FMT_MTD.1	N/A
FIA_UAU.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FIA_UAU.3	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A

	Composants fournissant une protection contre		
Composant	Contournement	Altération	Désactivation
FIA_UAU.4	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FIA_UID.2	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FIA_USB.1	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	FIA_UID.2
FMT_MOF.1	FPT_RVM.1 FIA_UAU.1	FMT_MTD.1	N/A
FMT_MSA.1	FPT_RVM.1 FIA_UAU.1	FMT_MTD.1	N/A
FMT_MSA.2	FPT_RVM.1 FIA_UAU.1	FMT_MTD.1	N/A
FMT_MSA.3	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2 FDP_IFC.2
FMT_MTD.1	FDP_ACC.2 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2
FMT_MTD.2	FDP_ACC.2 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2
FMT_REV.1	FDP_ACC.2 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2
FMT_SAE.1	FDP_ACC.2 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	FDP_ACC.2
FMT_SMR.2	FPT_RVM.1 FIA_USB.1	FMT_MSA.1 FMT_MTD.1	N/A
FMT_SMR.3	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A
FPT_AMT.1	FPT_RVM.1	FMT_MTD.1	N/A
FPT_RVM.1	N/A	FMT_MTD.1	N/A
FPT_STM.1	N/A	FMT_MTD.1	N/A
FPT_TST.1	N/A	FMT_MTD.1	N/A
FTA_MCS.1	FPT_RVM.1 FIA_UID.2	FMT_MSA.1 FMT_MTD.1	FIA_UID.2
FTA_SSL.3	FPT_RVM.1	FMT_MSA.1 FMT_MTD.1	N/A

	Composants fournissant une protection contre		
Composant	Contournement	Altération	Désactivation
FTA_TAH.1	FPT_RVM.1 FIA_UAU.1	FMT_MSA.1 FMT_MTD.1	FIA_UAU.1
FTA_TSE.1	FPT_RVM.1 FIA_USB.1	FMT_MSA.1 FMT_MTD.1	N/A
FTP_TRP.1	FPT_RVM.1		N/A

« N/A » signifie « Non Applicable », c'est-à-dire que l'attaque considérée n'est pas valable :

- une attaque par contournement est « N/A » si l'exécution du composant fonctionnel en question se fait à la demande d'un opérateur, donc de manière non automatique (par exemple, FPT_TST.1) ou si le composant en question ne peut pas être contourné de part la construction de la TOE (par exemple, FDP_RIP.2).
- une attaque par désactivation est « N/A » si l'exécution du composant fonctionnel en question n'est pas dépendante de la configuration des fonctions de sécurité. Ce composant ne pourrait alors être désactivé que par modification des exécutables de la TOE.

Les attaques par contournement sont couvertes par les composants :

- FPT_RVM.1 qui assure le non-contournement des fonctions mettant en œuvre la politique de sécurité,
- FIA_UAU.1 qui assure l'authentification des opérateurs et utilisateurs,
- FIA_UID.2 qui assure l'identification des opérateurs et utilisateurs avant toute autre chose,
- FIA_USB.1 qui assure le lien entre une identité et un groupe d'attributs de sécurité,
- FDP_ACC.2 qui assure le contrôle d'accès sur toutes les opérations,
- FDP_IFC.2 qui assure le contrôle du flux d'information sur toutes les opérations.

Les attaques par altération sont couvertes par les composants :

- FMT_MSA.1 qui assure la protection des attributs de sécurité,
- FMT_MTD.1 qui assure la protection des données propres à la TOE,
- FAU_STG.2 qui assure la protection des données d'audit,
- FPT_AMT.1 qui assure la protection de l'intégrité de la TOE,
- FPT_TST.1 qui assure la protection de l'intégrité de la TOE.

Les attaques par désactivation sont couvertes par les composants :

- FAU_GEN.1 qui assure l'enregistrement des événements à auditer,
- FAU_SAA.1 qui assure la détection des violations de la politique de sécurité,
- FAU_STG.2 qui assure la protection du journal d'audit,
- FDP_ACC.2 qui assure le contrôle d'accès sur toutes les opérations,
- FDP_IFC.2 qui assure un contrôle de flux sur toutes les opérations,
- FIA_UAU.1 qui assure l'authentification avant toute autre chose des opérateurs et des utilisateurs dans certains cas,
- FIA_UID.2 qui associe un identifiant à chaque utilisateur.

8.5.4 Cohérence interne des composants de sécurité

Par définition et construction des CC, les composants d'assurance constituant le niveau EAL5 et les deux composants ajoutés forment un tout cohérent puisque toutes les dépendances sont couvertes.

Les composants fonctionnels forment un ensemble cohérent s'il n'existe pas deux composants qui soient incohérents l'un avec l'autre. Une recherche des dépendances entre composants est donc effectuée (tableaux), puis pour chaque dépendance identifiée, une analyse montre qu'il n'y a pas d'incohérence.

Une dépendance est identifiée entre deux composants s'ils traitent des notions similaires. Par exemple, les composants FAU_STG.2 et FAU_STG.3 ont une dépendance car ils traitent tous les deux de la saturation du journal d'audit : FAU_STG.2 pose une contrainte sur le journal de bord en cas de saturation et FAU_STG.3 définit ce qu'il faut faire en cas de saturation. La vérification de la cohérence de ces deux composants consiste à vérifier que les actions décrites dans FAU_STG.3 permettent de respecter la contrainte définie dans FAU_STG.2.

Légende des tableaux :

case grisée : relation déjà traitée (relation inverse) dans le même tableau

cc : pas d'incohérence possible de par la construction des CC (composants dont aucune opération n'a été complétée et qui sont dans la même classe ou liés par une dépendance)

O : dépendance identifiée, donc à analyser

x : relation analysée et n'ayant mis en évidence aucune dépendance entre les composants.

8.5.4.1 FAU <-> FAU

	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1	FAU_SAR.3	FAU_SEL.1	FAU_STG.2	FAU_STG.3
FAU_ARP.1		O	x	O	x	x	x	x	x
FAU_GEN.1			x	O	O	O	O	O	O
FAU_GEN.2				cc	x	cc	x	cc	x
FAU_SAA.1					x	cc	x	cc	x
FAU_SAR.1						x	x	x	x
FAU_SAR.3							x	cc	x
FAU_SEL.1								x	x
FAU_STG.2									O
FAU_STG.3									

- FAU_GEN.1 <-> (FAU_ARP.1, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.2, FAU_STG.3) : FAU_GEN.1 enregistre des informations générées ou gérées par les autres composants. Il n'y a donc pas d'incohérence entre ces composants.
- FAU_ARP.1 <-> FAU_SAA.1 : FAU_SAA.1 définit les règles pour mettre en évidence une possible violation de la politique de sécurité, FAU_ARP.1 définit les actions à faire lorsqu'une de ces violations est détectée. Ces deux composants sont donc cohérents.
- FAU_STG.2 <-> FAU_STG.3 : FAU_STG.3 définit l'action à effectuer en cas de saturation : empêcher les événements auditables de survenir, sauf ceux concernant les opérateurs. Ceci permet donc de ne pas perdre d'événements audités mémorisés dans le journal d'audit et est en conformité avec la contrainte de FAU_STG.2.

8.5.4.2 FAU <-> FDP

	FDP_ACC.2	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.4	FDP_ITC.1	FDP_ITT.1	FDP_RIP.2	FDP_SDI.2
FAU_ARP.1	x	x	x	x	x	x	x	x	x
FAU_GEN.1	x	O	x	O	O	O	O	x	O
FAU_GEN.2	x	x	x	x	x	x	x	x	x
FAU_SAA.1	x	x	x	x	x	x	x	x	x
FAU_SAR.1	O	x	x	x	x	x	x	x	x
FAU_SAR.3	x	x	x	x	x	x	x	x	x
FAU_SEL.1	x	x	x	x	x	x	x	x	x
FAU_STG.2	x	x	x	x	x	x	x	x	x
FAU_STG.3	x	x	x	x	x	x	x	x	x

- FAU_GEN.1 <-> (FDP_ACF.1, FDP_IFF.1, FDP_IFF.4, FDP_ITC.1, FDP_ITT.1, FDP_SDI.2) : FAU_GEN.1 enregistre des informations générées ou gérées par les autres composants. Il n'y a donc pas d'incohérence entre ces composants.
- FAU_SAR.1 <-> FDP_ACC.2 : FDP_ACC.2 fournit le contrôle d'accès qui permet de limiter la lecture du journal d'audit aux opérateurs (FAU_SAR.1). Il n'y a donc pas d'incohérence.

8.5.4.3 FAU <-> FIA

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.3	FIA_UAU.4	FIA_UID.2	FIA_USB.1
FAU_ARP.1	x	x	x	x	x	x	x	x
FAU_GEN.1	O	x	O	O	O	O	O	O
FAU_GEN.2	x	x	x	x	x	x	O	x
FAU_SAA.1	x	x	x	x	x	x	x	x
FAU_SAR.1	x	x	x	x	x	x	x	x
FAU_SAR.3	x	x	x	x	x	x	x	x
FAU_SEL.1	x	x	x	x	x	x	O	x
FAU_STG.2	x	x	x	x	x	x	x	x
FAU_STG.3	x	x	x	x	x	x	x	x

- FAU_GEN.1 <-> (FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.3, FIA_UAU.4, FIA_USB.1) : FAU_GEN.1 enregistre des informations générées ou gérées par les autres composants. Il n'y a donc pas d'incohérence entre ces composants.
- FAU_GEN.1 <-> FIA_UID.2 : Ces deux composants sont complémentaires : FIA_UID.2 fournit l'identifiant qui sera utilisé par FAU_GEN.1. Ces deux composants sont donc cohérents.
- FAU_GEN.2 <-> FIA_UID.2 : Ces deux composants sont complémentaires : FIA_UID.2 associe aux utilisateurs un identifiant qui sera utilisé par FAU_GEN.2. Ces deux composants sont donc cohérents.
- FAU_SEL.1 <-> FIA_UID.2 : Ces deux composants sont complémentaires : FIA_UID.2 associe aux utilisateurs un identifiant qui sera utilisé par FAU_SEL.1. Ces deux composants sont donc cohérents.

8.5.4.4 FAU <-> FMT

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SAE.1	FMT_SMR.2	FMT_SMR.3
FAU_ARP.1	O	x	x	x	x	x	O	x	x	x
FAU_GEN.1	O	O	O	O	O	O	O	O	O	O
FAU_GEN.2	x	x	x	x	x	x	x	x	x	x
FAU_SAA.1	x	x	x	x	O	x	x	x	x	x
FAU_SAR.1	x	x	x	x	O	x	x	x	x	x
FAU_SAR.3	x	x	x	x	O	x	x	x	x	x
FAU_SEL.1	x	x	x	x	O	x	x	x	x	x
FAU_STG.2	x	x	x	x	O	x	x	x	x	x
FAU_STG.3	x	x	x	x	O	O	x	x	x	x

- FAU_ARP.1 <-> FMT_MOF.1 : FMT_MOF.1 complète FAU_ARP.1 en définissant les actions à effectuer en cas de détection d'une possible violation de la politique de sécurité. Ces deux composants sont donc cohérents.
- FAU_ARP.1 <-> FMT_REV.1 : FMT_REV.1 définit la révocation des attributs de sécurité comme étant une réponse à une possible violation de la politique de sécurité. FAU_ARP.1, par le biais de FMT_MOF.1 définit des actions possibles en cas de violation de la politique de sécurité, dont la révocation des droits d'accès qui correspond à un sous-ensemble de la révocation des attributs de sécurité. Ces deux composants sont donc cohérents.
- FAU_GEN.1 <-> (FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1, FMT_SAE.1, FMT_SMR.2, FMT_SMR.3) : FAU_GEN.1 enregistre des informations générées ou gérées par les autres composants. Il n'y a donc pas d'incohérence entre ces composants.

- FAU_SAA.1 <-> FMT_MTD.1 : FAU_SAA.1 permet de définir une liste de règles pour détecter d'éventuelles violations de la politique de sécurité et FMT_MTD.1 permet à l'administrateur de gérer cette liste de règles. Ces deux composants sont donc cohérents.
- FAU_SAR.1 <-> FMT_MTD.1 : L'élément FAU_SAR.1.1 est inclus dans FMT_MTD.1. Il y a donc redondance d'information. Il n'y a aucune incohérence entre ces deux composants.
- FAU_SAR.3 <-> FMT_MTD.1 : FAU_SAR.3 fournit des outils pour l'analyse des traces d'audit et FMT_MTD.1 définit qui peut utiliser ces outils. Ces deux composants sont donc cohérents.
- FAU_SEL.1 <-> FMT_MTD.1 : FAU_SEL.1 définit des règles pour l'enregistrement des événements d'audit et FMT_MTD.1 permet à l'administrateur de gérer ces règles. Ces deux composants sont donc cohérents.
- FAU_STG.2 <-> FMT_MTD.1 : FAU_STG.2 demande une protection des données d'audit. FMT_MTD.1 protège ces données en limitant leur accès aux opérateurs. Ces deux composants sont donc cohérents.
- FAU_STG.3 <-> FMT_MTD.1 : FAU_STG.3 permet de définir une limite pour le journal d'audit et FMT_MTD.1 permet à l'administrateur de gérer cette limite. Ces deux composants sont donc cohérents.
- FAU_STG.3 <-> FMT_MTD.2 : FAU_STG.3 permet de définir une limite pour le journal d'audit et FMT_MTD.2 définit ce que la TOE doit faire lorsque cette limite est atteinte. Ces deux composants sont donc cohérents.

8.5.4.5 FAU <-> FPT

	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1	FAU_SAR.3	FAU_SEL.1	FAU_STG.2	FAU_STG.3
FPT_AMT.1	x	O	x	x	x	x	x	x	x
FPT_RVM.1	x	x	x	x	x	x	x	x	x
FPT_STM.1	x	O	cc	cc	x	cc	x	cc	x
FPT_TST.1	x	O	x	x	x	x	x	x	x

- FAU_GEN.1 <-> (FPT_AMT.1, FPT_TST.1) : FAU_GEN.1 enregistre des informations générées ou gérées par les autres composants. Il n'y a donc pas d'incohérence entre ces composants.
- FAU_GEN.1 <-> FPT_STM.1 : FPT_STM.1 permet à FAU_GEN.1 d'avoir une heure valide pour l'enregistrement des événements à auditer. Ces deux composants sont complémentaires et donc cohérents.

8.5.4.6 FAU <-> FTA

	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1	FAU_SAR.3	FAU_SEL.1	FAU_STG.2	FAU_STG.3
FTA_MCS.1	x	O	x	x	x	x	x	x	x
FTA_SSL.3	x	O	x	x	x	x	x	x	x
FTA_TAH.1	x	x	x	x	x	x	x	x	x
FTA_TSE.1	x	O	x	x	x	x	x	x	x

- FAU_GEN.1 <-> (FTA_MCS.1, FTA_SSL.3, FTA_TSE.1) : FAU_GEN.1 enregistre des informations générées ou gérées par les autres composants. Il n'y a donc pas d'incohérence entre ces composants.

8.5.4.7 FAU <-> FTP

	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1	FAU_SAR.3	FAU_SEL.1	FAU_STG.2	FAU_STG.3
FTP_TRP.1	x	O	x	x	x	x	x	x	x

- FAU_GEN.1 <-> FTP_TRP.1 : FAU_GEN.1 enregistre des informations générées ou gérées par FTP_TRP.1. Il n'y a donc pas d'incohérence entre ces composants.

8.5.4.8 FDP <-> FDP

	FDP_ACC.2	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.4	FDP_ITC.1	FDP_ITT.1	FDP_RIP.2	FDP_SDI.2
FDP_ACC.2		O	x	x	x	O	x	x	x
FDP_ACF.1			x	x	cc	x	x	x	cc
FDP_IFC.2				O	x	x	x	x	x
FDP_IFF.1					x	x	x	x	x
FDP_IFF.4						x	x	x	cc
FDP_ITC.1							x	x	x
FDP_ITT.1								x	O
FDP_RIP.2									x
FDP_SDI.2									

- FDP_ACC.2 <-> FDP_ACF.1 : FDP_ACF.1 complète FDP_ACC.2. Il n'y a pas d'incohérence entre ces deux composants.
- FDP_ACC.2 <-> FDP_ITC.1 : FDP_ITC.1 complète FDP_ACC.2 pour les données importées de l'extérieur de la TOE. Ces deux composants sont donc cohérents.
- FDP_IFC.2 <-> FDP_IFF.1 : FDP_IFF.1 complète FDP_IFC.2. Il n'y a pas d'incohérence entre ces deux composants.
- FDP_ITT.1 <-> FDP_SDI.2 : FDP_SDI.2 fournit une réponse à l'exigence « modification of user data » du composant FDP_ITT.1. Ces deux composants sont donc cohérents.

8.5.4.9 FDP <-> FIA

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.3	FIA_UAU.4	FIA_UID.2	FIA_USB.1
FDP_ACC.2	x	x	x	x	x	x	x	x
FDP_ACF.1	x	x	x	x	x	x	x	x
FDP_IFC.2	x	x	x	x	x	x	x	x
FDP_IFF.1	x	x	x	x	x	x	x	x
FDP_IFF.4	x	x	x	x	x	x	x	x
FDP_ITC.1	x	x	x	x	x	x	x	x
FDP_ITT.1	x	x	x	x	x	x	x	x
FDP_RIP.2	x	x	x	x	O	x	x	x
FDP_SDI.2	x	x	x	x	x	x	x	x

- FDP_RIP.2 <-> FIA_UAU.3 : FDP_RIP.2 assure que lors de la réallocation d'un objet, son contenu est effacé. Ceci est donc valable pour les mots de passe et empêche donc qu'ils soient recopiés. Ceci est donc cohérent avec FIA_UAU.3.

8.5.4.10 FDP <-> FMT

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SAE.1	FMT_SMR.2	FMT_SMR.3
FDP_ACC.2	O	O	x	O	O	x	O	O	x	x
FDP_ACF.1	O	O	x	O	O	x	x	x	x	x
FDP_IFC.2	x	x	x	x	x	x	x	x	x	x
FDP_IFF.1	x	x	x	x	O	x	x	x	x	x
FDP_IFF.4	x	x	x	x	x	x	x	x	x	x
FDP_ITC.1	x	x	x	x	O	x	x	x	x	x
FDP_ITT.1	x	x	x	x	x	x	x	x	x	x
FDP_RIP.2	x	x	x	x	x	x	x	x	x	x
FDP_SDI.2	x	x	x	x	O	x	x	x	x	x

- FDP_ACC.2 <-> (FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SAE.1) : Les six composants de la classe FMT fournissent des règles de contrôle d'accès. Ils sont donc cohérents avec le composants FDP_ACC.2.
- FDP_ACF.1 <-> (FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1) : Les quatre composants de la classe FMT fournissent des règles de contrôle d'accès. Ils sont donc cohérents avec le composants FDP_ACF.1.
- FDP_IFF.1 <-> FMT_MTD.1 : FMT_MTD.1 permet aux opérateurs de gérer les attributs permettant d'autoriser ou d'interdire les accès qui sont utilisés par FDP_IFF.1. Il n'y a donc pas d'incohérence entre ces deux composants.
- FDP_ITC.1 <-> FMT_MTD.1 : FDP_ITC.1 demande le contrôle par un antivirus des données utilisateur importées dans la TOE, FMT_MTD.1 définit qui gère cet antivirus. Ces deux composants sont cohérents.

- FDP_SDI.2 <-> FMT_MTD.1 : FDP_SDI.2 permet de définir une liste d'actions en cas d'erreur d'intégrité et FMT_MTD.1 permet à l'administrateur de gérer cette liste d'actions. Ces deux composants sont donc cohérents.

8.5.4.11 FDP <-> FPT

	FDP_ACC.2	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.4	FDP_ITC.1	FDP_ITT.1	FDP_RIP.2	FDP_SDI.2
FPT_AMT.1	x	x	x	x	x	x	x	x	x
FPT_RVM.1	x	x	x	x	x	x	x	x	x
FPT_STM.1	x	x	x	x	x	x	x	x	x
FPT_TST.1	x	x	x	x	x	x	x	x	x

8.5.4.12 FDP <-> FTA

	FDP_ACC.2	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FDP_IFF.4	FDP_ITC.1	FDP_ITT.1	FDP_RIP.2	FDP_SDI.2
FTA_MCS.1	x	x	x	x	x	x	x	x	x
FTA_SSL.3	x	x	x	x	x	x	x	x	x
FTA_TAH.1	x	x	x	x	x	x	x	x	x
FTA_TSE.1	x	x	x	x	x	x	x	x	x

8.5.4.13 FDP <-> FTP

	FDP_	FDP_	FDP_	FDP_	FDP_	FDP_	FDP_	FDP_	FDP_

	ACC.2	ACF.1	IFC.2	IFF.1	IFF.4	ITC.1	ITT.1	RIP.2	SDI.2
FTP_TRP.1	x	x	x	x	x	x	x	x	x

8.5.4.14 FIA <-> FIA

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.3	FIA_UAU.4	FIA_UID.2	FIA_USB.1
FIA_AFL.1		cc	cc	O	x	cc	x	x
FIA_ATD.1			cc	x	x	cc	x	x
FIA_SOS.1				x	x	cc	x	x
FIA_UAU.1					x	x	x	x
FIA_UAU.3						O	x	x
FIA_UAU.4							x	x
FIA_UID.2								x
FIA_USB.1								

- FIA_AFL.1 <-> FIA_UAU.1 : FIA_UAU.1 oblige les opérateurs et les utilisateurs dans certains cas à s'authentifier, et FIA_AFL.1 définit le comportement de la TOE en cas d'échecs successifs d'authentification. Il n'y a donc pas d'incohérence entre les deux composants.
- FIA_UAU.3 <-> FIA_UAU.4 : Ces deux composants contribuent à empêcher un attaquant de réutiliser des authentifiants qui ont déjà servi. Il n'y a donc pas d'incohérence entre ces deux composants.

8.5.4.15 FIA <-> FMT

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SAE.1	FMT_SMR.2	FMT_SMR.3
FIA_AFL.1	x	x	x	x	O	x	x	x	x	x
FIA_ATD.1	x	O	O	x	x	x	x	x	x	x
FIA_SOS.1	x	x	x	x	O	x	x	x	x	x
FIA_UAU.1	x	x	x	x	O	x	x	x	x	x
FIA_UAU.3	x	O	x	x	O	x	x	x	x	x
FIA_UAU.4	x	x	x	x	O	x	x	x	x	x
FIA_UID.2	x	x	x	x	x	x	x	x	x	x
FIA_USB.1	x	x	x	x	x	x	x	x	x	x

- FIA_ATD.1 <-> FMT_MSA.1 : Aucun de ces deux composants ne liste les attributs de sécurité, il n'y a donc pas d'incohérence.
- FIA_ATD.1 <-> FMT_MSA.2 : FMT_MSA.2 est complémentaire de FIA_ATD.1. Il n'y a donc pas d'incohérence entre ces deux composants.
- FMT_MTD.1 <-> (FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.3, FIA_UAU.4) : FMT_MTD.1 limite aux opérateurs la gestion des paramètres définis ou utilisés par les autres composants. Il n'y a donc pas d'incohérence.
- FIA_UAU.3 <-> FMT_MSA.1 : FMT_MSA.1 limite l'accès aux authentifiants aux opérateurs. Il est donc complémentaire du composant FIA_UAU.3 qui interdit la copie d'authentifiants. Il n'y a donc pas d'incohérence entre ces deux composants.

8.5.4.16 FIA <-> FPT

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.3	FIA_UAU.4	FIA_UID.2	FIA_USB.1
FPT_AMT.1	x	x	x	x	x	x	x	x
FPT_RVM.1	x	x	x	x	x	x	x	x
FPT_STM.1	x	x	x	x	x	x	x	x
FPT_TST.1	x	x	x	x	x	x	x	x

8.5.4.17 FIA <-> FTA

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.3	FIA_UAU.4	FIA_UID.2	FIA_USB.1
FTA_MCS.1	x	x	x	x	x	x	x	x
FTA_SSL.3	x	x	x	x	x	x	x	x
FTA_TAH.1	O	x	x	x	x	x	x	x
FTA_TSE.1	x	x	x	x	x	x	x	x

- FIA_AFL.1 <-> FTA_TAH.1 : FIA_AFL.1 définit le comportement de la TOE en cas d'échecs successifs d'authentification, et FTA_TAH.1 signale aux opérateurs les échecs d'authentification qui ont eu lieu depuis la dernière connexion réussie. Il n'y a donc pas d'incohérence entre les deux composants.

8.5.4.18 FIA <-> FTP

	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.3	FIA_UAU.4	FIA_UID.2	FIA_USB.1
FTP_TRP.1	x	x	x	x	O	x	x	x

- FIA_UAU.3 <-> FTP_TRP.1 : FIA_UAU.3 permet à la TOE de détecter et d'empêcher la copie d'authentifiants et FTP_TRP.1 permet de protéger les données échangées (dont les authentifiants). Ces deux composants sont complémentaires et donc cohérents.

8.5.4.19 FMT <-> FMT

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SAE.1	FMT_SMR.2	FMT_SMR.3
FMT_MOF.1		x	x	x	x	x	x	x	O	x
FMT_MSA.1			x	O	x	x	O	x	O	x
FMT_MSA.2				x	x	x	x	x	x	x
FMT_MSA.3					x	x	x	x	O	x
FMT_MTD.1						x	O	O	O	x
FMT_MTD.2							x	x	O	x
FMT_REV.1								x	O	x
FMT_SAE.1									O	x
FMT_SMR.2										O
FMT_SMR.3										

- FMT_MOF.1 <-> FMT_SMR.2 : FMT_MOF.1 définit des attributions de l'administrateur et l'exploitant sécurité. Ces attributions sont cohérentes avec la définition des rôles du composant FMT_SMR.2.
- FMT_MSA.1 <-> FMT_MSA.3 : FMT_MSA.1 permet à l'administrateur de lire et modifier les attributs de sécurité et à l'exploitant sécurité de lire uniquement ces données. FMT_MSA.3 permet à l'administrateur uniquement de modifier les valeurs par défaut des attributs de sécurité. Les deux composants permettent donc à l'administrateur de faire des modifications sur les attributs de sécurité et sont donc cohérents.
- FMT_MSA.1 <-> FMT_REV.1 : Ces deux composants limitent l'accès en écriture des attributs de sécurité à l'administrateur. Ces deux composants sont donc cohérents.
- FMT_MSA.1 <-> FMT_SMR.2 : FMT_MSA.1 définit des attributions de l'administrateur et l'exploitant sécurité. Ces attributions sont cohérentes avec la définition des rôles du composant FMT_SMR.2.
- FMT_MSA.3 <-> FMT_SMR.2 : FMT_MSA.3 définit des attributions pour l'administrateur. Ces attributions sont cohérentes avec la définition des rôles du composant FMT_SMR.2.
- FMT_MTD.1 <-> FMT_REV.1 : FMT_REV.1 permet à l'administrateur de révoquer des attributs de sécurité et FMT_MTD.1 permet à l'administrateur de définir les règles de révocation. Ces deux composants sont donc cohérents.
- FMT_MTD.1 <-> FMT_SAE.1 : FMT_SAE.1 permet à l'administrateur de définir une date d'expiration pour les attributs de sécurité et les actions à faire si cette date est atteinte. FMT_MTD.1 permet à l'administrateur de définir la liste des attributs qui peuvent avoir une date d'expiration et les actions associées. Ces deux composants sont donc cohérents.
- FMT_MTD.1 <-> FMT_SMR.2 : FMT_MTD.1 définit des attributions pour l'administrateur. Ces attributions sont cohérentes avec la définition des rôles du composant FMT_SMR.2.
- FMT_MTD.2 <-> FMT_SMR.2 : FMT_MTD.2 définit des attributions pour l'administrateur. Ces attributions sont cohérentes avec la définition des rôles du composant FMT_SMR.2.
- FMT_REV.1 <-> FMT_SMR.2 : FMT_REV.1 définit des attributions pour l'administrateur. Ces attributions sont cohérentes avec la définition des rôles du composant FMT_SMR.2.
- FMT_SAE.1 <-> FMT_SMR.2 : FMT_SAE.1 définit des attributions pour l'administrateur. Ces attributions sont cohérentes avec la définition des rôles du composant FMT_SMR.2.
- FMT_SMR.2 <-> FMT_SMR.3 : FMT_SMR.2 définit les deux rôles identifiés, FMT_SMR.3 implique qu'il faut une demande explicite pour endosser un rôle. Les rôles précisés dans ces deux composants sont les mêmes. Ces deux composants sont donc cohérents.

8.5.4.20 FMT <-> FPT

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SAE.1	FMT_SMR.2	FMT_SMR.3
FPT_AMT.1	x	x	x	x	x	x	x	x	x	x
FPT_RVM.1	x	x	x	x	x	x	x	x	x	x
FPT_STM.1	x	x	x	x	x	x	x	O	x	x
FPT_TST.1	x	x	x	x	x	x	x	x	x	x

- FMT_SAE.1 <-> FPT_STM.1 : FPT_SRM.1 permet à FMT_SAE.1 d'avoir une heure valide lui permettant de gérer correctement les dates d'expiration des attributs de sécurité. Ces deux composants sont donc cohérents.

8.5.4.21 FMT <-> FTA

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SAE.1	FMT_SMR.2	FMT_SMR.3
FTA_MCS.1	x	x	x	x	O	x	x	x	x	x
FTA_SSL.3	x	x	x	x	O	x	x	x	x	x
FTA_TAH.1	x	x	x	x	x	x	x	x	x	x
FTA_TSE.1	x	x	x	x	O	x	x	x	x	x

- FMT_MTD.1 <-> (FTA_MCS.1, FTA_SSL.3, FTA_TSE.1) : FMT_MTD.1 permet aux opérateurs de gérer des données utilisées par les autres composants. Il n'y a donc pas d'incohérences.

8.5.4.22 FMT <-> FTP

	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_REV.1	FMT_SAE.1	FMT_SMR.2	FMT_SMR.3
FTP_TRP.1	x	x	x	x	O	x	x	x	x	x

- FMT_MTD.1 <-> FTP_TRP.1 : FTP_TRP.1 permet de définir une liste d'actions nécessitant le chemin de confiance et FMT_MTD.1 permet à l'administrateur de gérer cette liste d'actions. Ces deux composants sont donc cohérents.

8.5.4.23 FPT <-> FPT

	FPT_AMT.1	FPT_RVM.1	FPT_STM.1	FPT_TST.1
FPT_AMT.1		x	x	O
FPT_RVM.1			x	x
FPT_STM.1				x
FPT_TST.1				

- FPT_AMT.1 <-> FPT_TST.1 : Ces deux composants sont complémentaires et permettent de montrer le bon fonctionnement de la TOE. Il n'y a pas d'incohérence entre ces deux composants.

8.5.4.24 FPT <-> FTA

	FPT_AMT.1	FPT_RVM.1	FPT_STM.1	FPT_TST.1
FTA_MCS.1	x	x	x	x
FTA_SSL.3	x	x	O	x
FTA_TAH.1	x	x	x	x
FTA_TSE.1	x	x	x	x

- FPT_STM.1 <-> FTA_SSL.3 : FPT_STM.1 permet d'avoir un temps sûr et donc des durées valides pour terminer la session d'un opérateur après une durée donnée d'inactivité et ainsi de répondre à FTA_SSL.3. Il n'y a donc pas d'incohérence entre ces deux composants.

8.5.4.25 FPT <-> FTP

	FPT_AMT.1	FPT_RVM.1	FPT_STM.1	FPT_TST.1
FTP_TRP.1	x	x	x	x

8.5.4.26 FTA <-> FTA

	FTA_MCS.1	FTA_SSL.3	FTA_TAH.1	FTA_TSE.1
FTA_MCS.1		x	x	x
FTA_SSL.3			x	x
FTA_TAH.1				x
FTA_TSE.1				

8.5.4.27 FTA <-> FTP

	FTA_MCS.1	FTA_SSL.3	FTA_TAH.1	FTA_TSE.1
FTP_TRP.1	x	x	x	x

8.5.5 Conclusion de l'analyse de cohésion

L'analyse de cohésion n'a mis en évidence aucun problème. Les exigences de sécurité forment donc un ensemble cohérent et se supportent mutuellement (« mutually supportive and internally consistent whole»).