PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2004/33

Arkoon Fast Firewall v3.0/11 avec certification-eal2-qualification package (configurations A200, A500, A2000 et A5000)

Paris, le 23 novembre 2004

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.
Toutefois, la certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Table des matières

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics. (article 7)
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (article 8)

Les procédures de certification sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)

Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle s'applique

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

[2] En novembre 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède et la Turquie.

jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le pare-feu **Arkoon Fast Firewall v3.0/11 avec certification-eal2-qualification package** développé par **Arkoon Network Security**.
Le produit a été évalué dans quatre configurations distinctes :

- A200
- A500
- A2000
- A5000

Le tableau suivant résume les composants matériels de ces quatre configurations :

	A200	A500	A2000	A5000
CPU	Via C3 667MHz	Intel P3 1GHz	Intel P3 2GHz	Intel P3 Bipro 1,2GHz
Memory	28Mo	56Mo	12Mo	12Mo/1Go
Hard Drive	20Go	40Go	40Go	36,7Go SCSI
PCMCIA slots	1	2	2	2
Flash	32Mo (System)	16Mo(Config) 32Mo(System)	16Mo(Config) 32Mo(System)	16Mo(Config) 32Mo(System)
Ethernet Ports	4	4	4	4
OS	AKS	AKS	AKS	AKS
Débit (Mb/s)	190	300	425	1700
Connections/s	5700	14400	23000	25000
Max. Conn. #	190000	450000	980000	2000000
Max. VPN #	50	500	10000	25000
AES Thrpt (Mb/s)	32	30	200	250

Tableau 1 - Configurations évaluées du pare-feu

1.2. Développeur

Arkoon Network Security

13A avenue Victor Hugo
69160 Lyon Tassin
France

1.3. Description du produit évalué

Le produit évalué est composé des éléments suivants :

- les composants logiciels du pare-feu, mettant en œuvre les fonctions de sécurité,
- une station d'administration et de supervision,
- un boîtier pare-feu (matériel) et la console d'administration.

Dans ce qui suit, nous distinguerons (cf §1.3.1) la console d'administration (cf Figure 2 – *FAST Appliance Console*) et la station d'administration (cf Figure 2 – *FAST Administration Station*). La première consiste en un écran et un clavier connecté sur le pare-feu, la seconde est reliée au pare-feu par un câble réseau. Cette dernière possède deux applications, l'une pour l'installation et le paramétrage (définition de la politique de sécurité) du pare-feu, la seconde pour la supervision du pare-feu et la remontée des journaux d'audit.

Le produit possède trois ports d'interface : le premier avec le réseau externe, le deuxième avec le réseau interne et le dernier avec le réseau d'administration. Pour les besoins de l'évaluation, la station d'administration est considérée dans le même local que le pare-feu, comme indiqué sur la figure suivante :

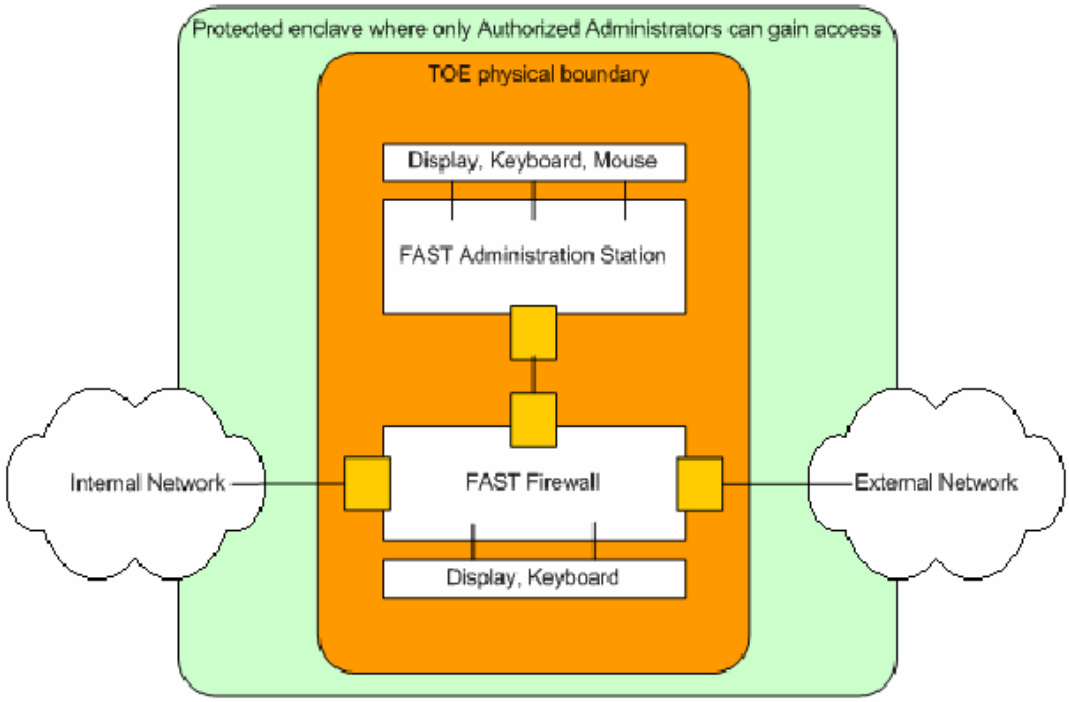

Figure 1 - Périmètre du produit évalué

Le produit met en œuvre quatre grandes familles de fonctions de sécurité : le cloisonnement réseau, l'audit, l'administration et la protection en intégrité des flux.

1.3.1. Architecture

Le produit est construit à partir des composants suivants :

- le *FAST Engine* qui met en œuvre les règles de la politique de sécurité du pare-feu en ce qui concerne les protocoles des couches transport et réseau (IP,

TCP, UDP et ICMP). Il fournit des mécanismes de limitation du nombre de connexions, des mécanismes de NAT[1] et des mécanismes d'authentification ;

- le *FAST Engine* inclut le *FAST Analyzer*, module permettant de mettre en œuvre la politique de sécurité pour les protocoles applicatifs (HTTP, FTP, SMTP et DNS) ;
- les *services de gestion* qui interagissent avec le *FAST Engine* et permettent de charger les configurations du pare-feu par les administrateurs ;
- les *services d'audit*, composés eux-mêmes de services de supervision du pare-feu au travers de journaux d'audit. Ces services préviennent les administrateurs en cas de détection d'événements pré-définis ;
- les *services d'authentification* ;
- une *console d'administration*, avec une interface utilisateur en ligne de commandes ;
- ainsi que d'autres modules ne faisant pas partie du périmètre de l'évaluation, comme : les VPN[2], le filtrage de contenu, la détection de virus, la gestion de la QoS[3], la gestion centralisée de plusieurs pare-feu Arkoon.

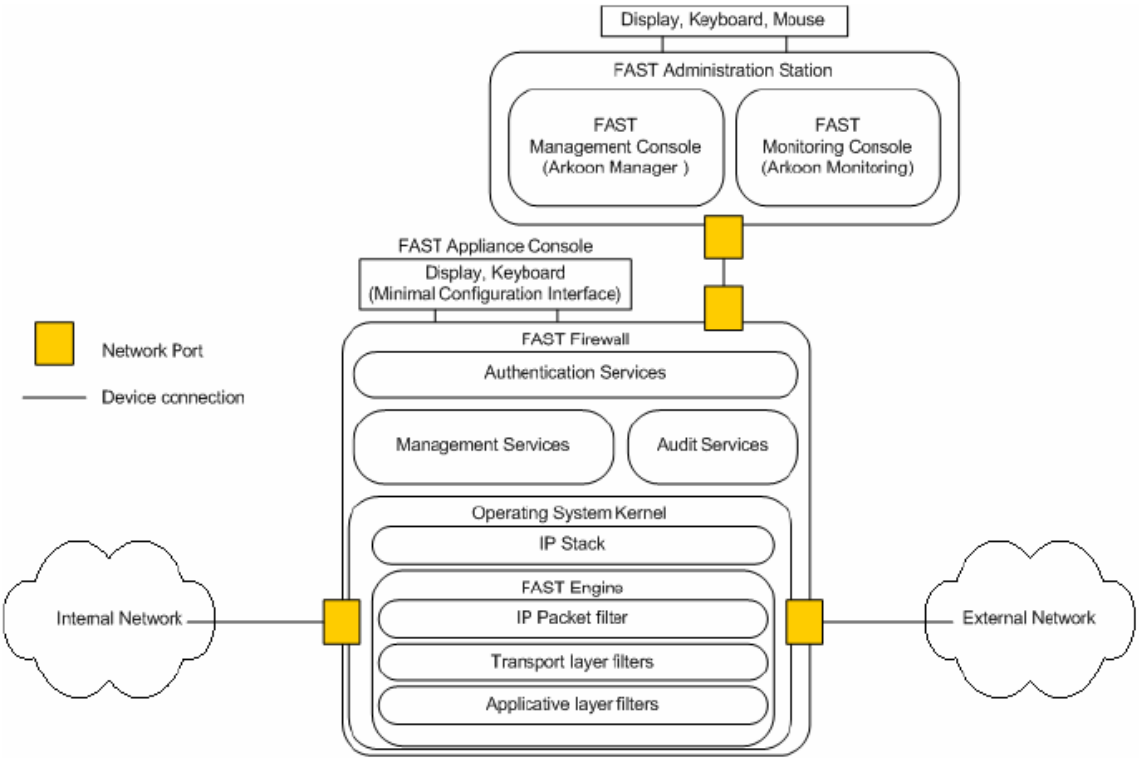

Figure 2 - Architecture du pare-feu

[1] Network Address Translation (Transcription d'adresse réseau)
[2] Virtual Private Network (réseau privé virtuel)
[3] Quality of Service (qualité de service)

L'administration du pare-feu peut se faire :

- à partir de la console d'administration (*FAST Appliance console*), en ligne de commandes,
- ou à partir des stations d'administration *FAST Management console* et *FAST Monitoring console* :
  - *FAST Management console* est installée sur la station d'administration et fournit une interface utilisateur graphique permettant de paramétrer la politique de sécurité du pare-feu,
  - *FAST Monitoring console* est aussi installée sur la station d'administration et est interfacée avec les services d'audit du pare-feu, fournissant une interface graphique sur les informations remontées par le pare-feu et ses journaux d'audit.

1.3.2. Périmètre et limites du produit évalué

Le périmètre du produit évalué est celui indiqué sur la figure 1.

2. L'évaluation

2.1. Commanditaire

Arkoon Network Security

13A avenue Victor Hugo
69160 Lyon Tassin
France

2.2. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.3. Centre d'évaluation

OPPIDA

13 route de la Minière
Bâtiment 134
78000 Versailles
France

Téléphone : +33 (0)1 30 83 27 95

Adresse électronique : cesti@oppida.fr

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation satisfont aux exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].

L'évaluation s'est déroulée de novembre 2003 à octobre 2004.

2.5.1. L'environnement de développement

Le produit est développé sur le site de :

Arkoon Network Security

13A avenue Victor Hugo
69160 Lyon Tassin
France

Les mesures de sécurité permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.
Un système de gestion de configuration est utilisé conformément au plan de gestion de configuration défini par le développeur du produit. Les procédures de génération permettent par ailleurs de s'assurer que les bons éléments de configuration sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures de développement et de gestion de configuration a été effectuée par une visite du site de Arkoon Network Security (cf Annexe 1).

Les procédures de correction d'anomalies décrivent la manière dont toute anomalie découverte sera suivie et corrigée, ainsi que la diffusion des informations et corrections relatives à ces anomalies, tant que le produit est maintenu par le développeur.
Ces procédures ont été évaluées, bien que le respect de ces procédures ne puisse pas être déterminé au moment de l'évaluation.

2.5.2. La conception du produit

La classe d'assurance ADV définit les exigences de raffinement des fonctions de sécurité du produit depuis les spécifications globales présentes dans la cible de sécurité [ST] jusqu'à l'implémentation de ces fonctions.

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit :
- spécifications fonctionnelles (FSP),
- conception de haut-niveau (HLD).

2.5.3. La livraison et l'installation

La livraison est considérée juste après le développement du produit. Le produit est livré aux clients d'Arkoon Network Security. La procédure de livraison utilisée [DEL] permet de détecter une modification du produit pendant la livraison. Les utilisateurs finaux – administrateurs, cf §2.5.4 – peuvent vérifier l'intégrité du produit livré en s'appuyant sur le guide de prise en main [AGD].

Les procédures d'installation, de génération et de démarrage [IGS] permettent d'obtenir la configuration évaluée du produit.

2.5.4. La documentation d'exploitation

Du point de vue de l'évaluation, les administrateurs correspondent aux rôles suivants (définis au paragraphe 2.3.2 de la cible de sécurité [ST]) :

- Pour la station d'administration :
  - administrateur *Read-only* : il administre le pare-feu depuis la station d'administration avec des droits d'accès restreints ;
  - administrateur *Read/Write* : il administre le pare-feu depuis la station d'administration avec des droits d'accès complets sur les fonctions de sécurité ;
- Pour la console d'administration :
  - *root* : il administre le pare-feu depuis la console d'administration avec des droits d'accès complets sur tout le produit.

Les guides des administrateurs [AGD] ont été fournis pour évaluation.

Les utilisateurs du pare-feu, autres que les administrateurs, sont soit des machines soit des individus utilisant une machine pour se connecter à un service à travers le pare-feu évalué. Ils n'ont aucune interface avec le pare-feu – hormis la configuration de leur propre poste (paramétrage du proxy HTTP dans son navigateur) –, puisque l'authentification possible de ces utilisateurs est hors périmètre d'évaluation.

2.5.5. Les tests fonctionnels

L'évaluateur a vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit sont reliées à au moins un test fonctionnel dans la documentation de test.
Les tests ont été réalisés sur une plate-forme représentative du produit en exploitation, dans les quatre configurations considérées (cf Tableau 1).

La plate-forme comprenait :

- une station d'administration, exécutant Windows 2000 Service Pack 4,
- une station cliente connectée sur le réseau « interne » (cf Figure 1), exécutant Windows 2000 Service Pack 4,
- un serveur connecté sur le réseau « interne », exécutant Mandrake version 8.2,
- une station connectée sur le réseau « externe », exécutant Mandrake version 8.2,
- et un pare-feu dans l'une des quatre configurations.

2.5.6. L'analyse de vulnérabilité

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement prises en compte dans la conception du produit.
L'évaluateur a également réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré.
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élémentaire**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du produit Arkoon Fast Firewall v3.0/11 avec certification-eal2-qualification package (configurations A200, A500, A2000 et A5000) pour les quatre configurations considérées.

3.2. Niveau d'évaluation

Le produit Arkoon Fast Firewall v3.0/11 avec certification-eal2-qualification package (configurations A200, A500, A2000 et A5000) a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL2**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_HLD.2	Security enforcing high-level design
ALC_DVS.1	Identification of security measures
ALC_FLR.3	Systematic flaw remediation
AVA_MSU.1	Examination of guidance
AVA_VLA.2	Independent vulnerability analysis

Tableau 2 - Augmentations

Pour tous les composants, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite
Class ACM	**Configuration management**	
ACM_CAP.2	Configuration items	Réussite
Class ADO	**Delivery and operation**	
ADO_DEL.1	Delivery procedures	Réussite
ADO_IGS.1	Installation, generation, and start-up	Réussite

[1] Annexe 3 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

	procedures	
Class ADV	**Development**	
ADV_FSP.1	Informal functional specification	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
Class ALC	**Life cycle support**	
ALC_DVS.1	Identification of security measures	Réussite
ALC_FLR.3	Systematic flaw remediation	Réussite
Class ATE	**Tests**	
ATE_COV.1	Evidence of coverage	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_MSU.1	Examination of guidance	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.2	Independent vulnerability analysis	Réussite

Tableau 3 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** suivantes[1]. Les opérations sur ces exigences sont décrites dans la cible de sécurité [ST].

- Audit data generation (FAU_GEN.1)
- Audit review (FAU_SAR.1)
- Selectable audit review (FAU_SAR.3)
- Protected audit trail storage (FAU_STG.1)
- Prevention of audit data loss (FAU_STG.4)
- Subset information flow control (FDP_IFC.1)
- Complete information flow control (FDP_IFC.2)
- Simple security attributes (FDP_IFF.1)
- Subset residual information protection (FDP_RIP.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- User identification before any action (FIA_UID.2)

[1] Annexe 2 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Management of TSF data (FMT_MTD.1)
- Security roles (FMT_SMR.1)
- Pseudonymity (FPR_PSE.1)
- Non-bypassability of the TSP (FPT_RVM.1)
- TSF domain separation (FPT_SEP.1)
- Reliable time stamps (FPT_STM.1)

3.4. Résistance des fonctions

Seules les fonctions d'authentification ont fait l'objet d'une estimation du niveau de résistance.
Le niveau de résistance des fonctions de sécurité est jugé **élevé** (**SOF-High**).

3.5. Analyse de la résistance des mécanismes cryptographiques

Il n'y a pas de mécanismes cryptographiques, aucune analyse n'a été menée par la DCSSI.

3.6. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

3.7. Reconnaissance internationale (CC RA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA].

3.8. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement se trouvant dans la cible de sécurité [ST] – repris en partie au paragraphe 3.9 du présent rapport – ainsi que les recommandations se trouvant dans les guides d'administration [AGD] et d'installation [IGS].
Les résultats de l'évaluation ne sont valables que dans les configurations spécifiées dans le présent rapport de certification.

3.9. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST] :

- le produit évalué et les stations d'administration doivent se trouver dans un environnement dont l'accès est contrôlé, interdisant l'accès à des personnes non autorisées (OE.PHYSEC, OE.LOCATE) ;
- L'environnement du produit évalué doit empêcher le re-jeu de l'authentification de l'administrateur vers le pare-feu (OE.SINUSE) ;

- le produit évalué ne doit contenir que des applications de sécurité et seulement les données nécessaires à leurs exploitations (OE.GENPUR) ;
- le produit évalué ne doit pas contenir de données publiques (OE.PUBLIC) ;
- les administrateurs sont des personnes de confiance. Ils sont formés et ils respectent les guides d'utilisation et d'administration du produit évalué (OE.NOEVIL, OE.ADMTRA et OE.GUIDAN) ;
- le flux d'information entre les réseaux dits « interne » et « externe » ne peut passer que par le produit évalué (OE.SINGEN) ;
- les utilisateurs ne peuvent accéder à distance aux fonctions d'administration du produit évalué par les réseaux dits « interne » et « externe » (OE.NOREMO).

3.10. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le produit Arkoon Fast Firewall v3.0/11 avec certification-eal2-qualification package (configurations A200, A500, A2000 et A5000) identifié au paragraphe 1.1 et décrit au paragraphe 1.3 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Visite du site de Arkoon Network Security

Le site de développement de Arkoon Network Security situé 13A avenue Victor Hugo, 69160 Lyon Tassin, a fait l'objet, dans le cadre de l'évaluation du produit Arkoon Fast Firewall v3.0/11 avec certification-eal2-qualification package (configurations A200, A500, A2000 et A5000), d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : ACM (ACM_CAP.2) ;
- la livraison : ADO (ADO_DEL.1) ;
- le support au cycle de vie : ALC (ALC_DVS.1 et ALC_FLR.3).

La visite par le centre d'évaluation, accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site. Les résultats de la visite se trouvent dans les rapports d'évaluation des tâches associées.

Annexe 2. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont données à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles du produit.

Class FAU	**Security audit**
Security audit data generation	
FAU_GEN.1	*Audit data generation* Ce composant définit le niveau des événements auditables et spécifie la liste des données que chaque enregistrement doit contenir.
Security audit review	
FAU_SAR.1	*Audit review* Le produit doit offrir aux utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]) la capacité de lire certaines informations (spécifiées dans la cible de sécurité [ST]) à partir des enregistrements d'audit.
FAU_SAR.3	*Selectable audit review* Les outils de revue d'audit doivent sélectionner, à partir de critères, les données d'audit à examiner.
Security audit event storage	
FAU_STG.1	*Protected audit trail storage* Les enregistrements d'audit doivent être protégés contre une suppression ou une modification non autorisées.
FAU_STG.4	*Prevention of audit data loss* Le produit doit entreprendre des actions (spécifiées dans le document [ST]) dans le cas où la trace d'audit est pleine.
Class FDP	**User data protection**
Information flow control policy	
FDP_IFC.1	*Subset information flow control* Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information, lesquelles sont spécifiées dans la cible de sécurité [ST] pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'informations.
FDP_IFC.2	*Complete information flow control* Chaque règle de contrôle de flux d'information identifiée doit traiter toutes les opérations sur les sujets et les informations couvertes par cette règle. Tous les flux d'information et toutes les opérations doivent être couverts par au moins une règle de contrôle de flux d'information identifiée. Conjointement avec le composant FPT_RVM.1, ceci correspond à l'aspect « systématiquement appelé » d'un moniteur de référence.
Information flow control functions	
FDP_IFF.1	*Simple security attributes* Ce composant impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la fonction et décrit comment les attributs de sécurité sont choisis par la fonction.
Residual information protection	

FDP_RIP.1	*Subset residual information protection* Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets lors de l'allocation ou de la désallocation de la ressource.
Class FIA	**Identification and authentication**
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
User authentication	
FIA_UAU.1	*Timing of authentication* Le produit autorise un utilisateur à exécuter certaines actions, spécifiées dans la cible de sécurité [ST], avant que son identité ne soit authentifiée.
User identification	
FIA_UID.2	*User identification before any action* Les utilisateurs doivent s'identifier avant que toute action ne soit autorisée.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Management of TSF data	
FMT_MTD.1	*Management of TSF data* Les utilisateurs autorisés peuvent gérer les données des fonctions de sécurité du produit.
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiés dans la cible de sécurité [ST]).
Class FPR	**Privacy**
Pseudonymity	
FPR_PSE.1	*Pseudonymity* Un ensemble d'utilisateurs ou de sujets doit être incapable de déterminer l'identité d'un utilisateur associé à un sujet ou à une opération, mais que cet utilisateur réponde quand même de ses actions.
Class FPT	**Protection of the TSF**
Reference mediation	
FPT_RVM.1	*Non-bypassability of the TSP* Les règles de sécurité du produit ne doivent pas pouvoir être contournées.
Domain separation	
FPT_SEP.1	*TSF domain separation* Le produit doit offrir un domaine protégé et distinct pour les fonctions de sécurité et procurer une séparation entre sujets.
Time stamps	

FPT_STM.1	*Reliable time stamps* Le produit doit fournir un horodatage fiable.

Annexe 3. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 4. Références documentaires du produit évalué

[AGD]	Guide de prise en main Référence AKV3-USR-IGS-GPEM Version 1.1.1.3 16 août 2004 Arkoon Network Security Guide d'administration Version 1.1.5.1 Arkoon Network Security Aide en ligne Arkoon Manager v3.0 Version 1.0.16.1 Arkoon Network Security Aide en ligne Arkoon Monitor v3.0 Version 1.0.7.1 Arkoon Network Security
[DEL]	Production, Intégration et Livraison Référence AKV3-ADO-DEL-PRO Version 1.2 20 juin 2004 Arkoon Network Security
[IGS]	Guide de prise en main Référence AKV3-USR-IGS-GPEM Version 1.1.1.3 16 août 2004 Arkoon Network Security Guide d'installation Référence AKV3-USR-IGS-EAL2 Version 1.1 17 août 2004 Arkoon Network Security
[RTE]	Rapport technique d'évaluation Référence OPPIDA/CESTI/OMEGA/RTE/2.0 Version 3.0 10 novembre 2004 OPPIDA
[ST]	Cible de sécurité publique Référence AKV3-CRT-EAL2-ST Version 2.7p 28 octobre 2004 Arkoon Network Security

	Cible de sécurité Référence AKV3-CRT-EAL2-ST Version 2.7 28 octobre 2004 Arkoon Network Security

Annexe 5. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CRY/I/01]	Instruction CRY/I/01 Analyse des mécanismes cryptographiques, DCSSI.
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, August 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, August 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, August 1999, version 2.1, réf: CCIMB-99-033. Le contenu des Critères Communs version 2.1 est identique à celui de la Norme Internationale ISO/IEC 15408:1999, comportant les trois documents suivants : ▪ ISO/IEC 15408-1: Part 1 Introduction and general model ; ▪ ISO/IEC 15408–2: Part 2 Security functional requirements ; ▪ ISO/IEC 15408–3: Part 3 Security assurance requirements.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, August 1999, version 1.0, ref CEM- 99/045.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, may 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr