PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2011/48

Logiciel FAST360, version 5.0/22

Paris, le 25 octobre 2011

Le directeur général adjoint de l'agence nationale
de la sécurité des systèmes d'information

Vice-amiral Michel Benedittini
[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.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2011/48

Nom du produit

Logiciel FAST360

Référence/version du produit

Version 5.0/22

Conformité à un profil de protection

[PP FWIP], version 2.2
« Profil de protection Firewall d'interconnexion IP »

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 3 augmenté

ALC_FLR.3, AVA_VLA.2

Développeur

ARKOON Network Security

1 place Verrazzano, 69009 Lyon, France

Commanditaire

ARKOON Network Security

1 place Verrazzano, 69009 Lyon, France

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France

Tél : +33 (0)1 30 14 19 00, mél : cesti@oppida.fr

Accords de reconnaissance applicables

CCRA **SOG-IS**

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 modifié. Ce décret indique que :

- L'agence nationale 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 disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « Logiciel FAST360, version 5.0/22 », développé par Arkoon Network Security, pour les *appliances* « UTM Arkoon FAST360 » et leur administration. Les appliance concernées appartiennent à la gamme Network Processor Appliances (Small, Medium et Large).

Ce produit est composé :

- d'une partie déployée sur l'*appliance* « UTM Arkoon FAST360 », qui réalise les fonctions de pare-feu, de serveur VPN/IPSEC, de détection et de prévention d'intrusions en temps réel, d'antivirus, d'antispyware, de serveur d'authentification…;
- des outils d'administration « Arkoon Management Tools », qui permettent de centraliser l'administration et la supervision d'une politique de sécurité réseau mise en œuvre par un ensemble d'*appliance*s « UTM Arkoon FAST360 », notamment en permettant de télédistribuer leurs configurations et d'automatiser leurs mises à jour.

1.2. Description du produit

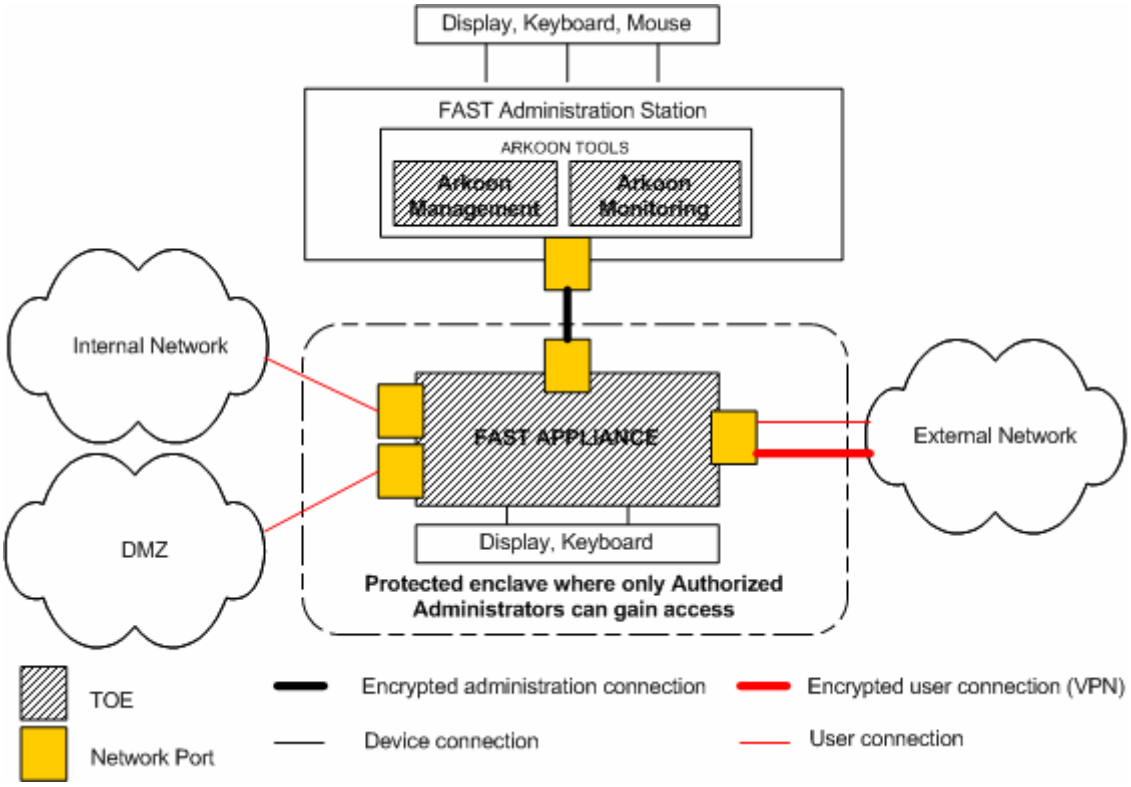
La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
Cette cible de sécurité est conforme au profil de protection « Firewall d'interconnexion IP » [PP_FWIP] et s'inspire du profil de protection, non certifié, « Chiffreur IP » [PP_CIP].

1.2.1. Architecture

Le logiciel FAST360 est constitué des éléments suivants :

- le système « Administration », qui permet de réaliser des opérations d'administration d'un parc d'*appliance* FAST360 ; ce système est lui-même composé :
  - du sous-système « Arkoon Manager », qui permet de gérer la configuration de l'*appliance* FAST360, dont notamment la configuration des composants qui mettent en œuvre les politiques de sécurité définies par l'administrateur ;
  - du sous-système « Arkoon Monitoring », qui permet de superviser l'*appliance* FAST360, c'est à dire de consulter/supprimer les journaux et alertes liés au trafic réseau et aux règles de sécurité établies par l'administrateur ;
- le système « Firewall » (FAST Engine), qui assure l'application des règles de filtrage, définies par le système « Administration », au trafic réseau transitant par l'*appliance*. Ce système « Firewall » s'appuie sur le moteur FAST (*Fast Applicative Shield Technology*) ;
- le système VPN (*Virtual Private Network*), qui offre la possibilité à des hôtes distants, statiques ou nomades, d'établir des tunnels IPSec avec l'*appliance* FAST360.

La figure suivante présente la cible d'évaluation (TOE) et son environnement.



L'*appliance* UTM Arkoon FAST360 est dotée de quatre interfaces réseau :

- une interface d'administration, qui relie l'*appliance* à sa station d'administration pour permettre son administration à distance ;
- une interface réseau externe, qui relie l'*appliance* à un réseau externe, considéré comme non sûr (Internet par exemple) ;
- une interface réseau interne qui relie l'*appliance* au réseau interne : le réseau protégé par l'*appliance* ;
- une interface réseau DMZ[1], qui relie l'*appliance* à un réseau DMZ où seules les machines devant être visibles depuis le réseau externe sont présentes.

[1] *Demilitarized zone*, zone démilitarisée

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- des services d'administration :
  - la gestion des comptes des administrateurs du produit ;
  - la journalisation et l'audit des opérations d'administration ;
  - la définition des politiques de sécurité appliquées par l'*appliance* ;
  - la gestion de la journalisation des flux ;
  - la supervision de l'*appliance* ;
  - la gestion des clés cryptographiques utilisées dans le cadre de l'authentification des administrateurs, et de la protection en confidentialité et en authenticité des flux VPN ;
- le filtrage des flux IP transitant par l'*appliance* entre réseaux externe, interne et DMZ, conformément à la politique de sécurité pare-feu définie par l'administrateur ;
- la protection de l'authenticité, de la confidentialité et l'intégrité des flux échangés au travers d'un réseau privé, conformément à la politique de sécurité VPN définie par l'administrateur :
  - la protection en confidentialité des données applicatives ;
  - la protection de l'authenticité des données applicatives ;
  - la protection en confidentialité des données topologiques ;
  - la protection de l'authenticité des données topologiques ;
  - le cloisonnement des flux en divisant un réseau privé en plusieurs sous-réseaux.

1.2.3. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version des composants du produit certifié est identifiable par les moyens suivants :

- pour le logiciel embarqué de la carte mémoire de l'*appliance*, dans le fichier « /etc/arkoon_version » ;
- pour l'outil Arkoon Manager, dans le menu « Aide > A propos » ;
- pour l'outil Arkoon Monitoring, dans le menu « ? > A propos d'Arkoon Monitoring ».

Les références complètes des composants certifiés constitutifs du produit, ainsi que leur format, sont fournies dans le tableau suivant :

Composants	Format de l'identification de la référence	Référence complète	
Logiciel embarqué de la carte mémoire de l'*appliance*	VERSION_MAJEURETYPE_YYMMDD_hhmm VERSION_MAJEURE/INC[-patch]	5.0MD_1100725_0230 5.0/22	
Outil Arkoon Manager	VERSION_MAJEURE-INC Build YYYYMMDDhhmmss	Windows JRE 1.6	5.0-22 Build 20110616185600
		Linux JRE 1.6	5.0-22 Build 20110616180328
Outil Arkoon Monitoring	VERSION_MAJEURE.YYMMDD.hhmm	Windows JRE 1.6	5.0.110616.1823
		Linux JRE 1.6	5.0.110616.1706

Pour les utilisateurs des distributions intermédiaires du produit (i.e. client de l'offre *Early Access Release* d'Arkoon), il doit être noté que la version certifiée correspond au *release candidate* n°6 de la version 5.0/22.

1.2.4. Cycle de vie

Le produit a été développé sur le site suivant :

ARKOON Network Security
1 place Verrazzano
69009 Lyon
France

Pour l'évaluation, seul le rôle « administrateur du produit » a été considéré (rôle « Toutes autorisation »). Le produit offre cependant la possibilité de répartir les droits d'administration entre les six rôles suivants :

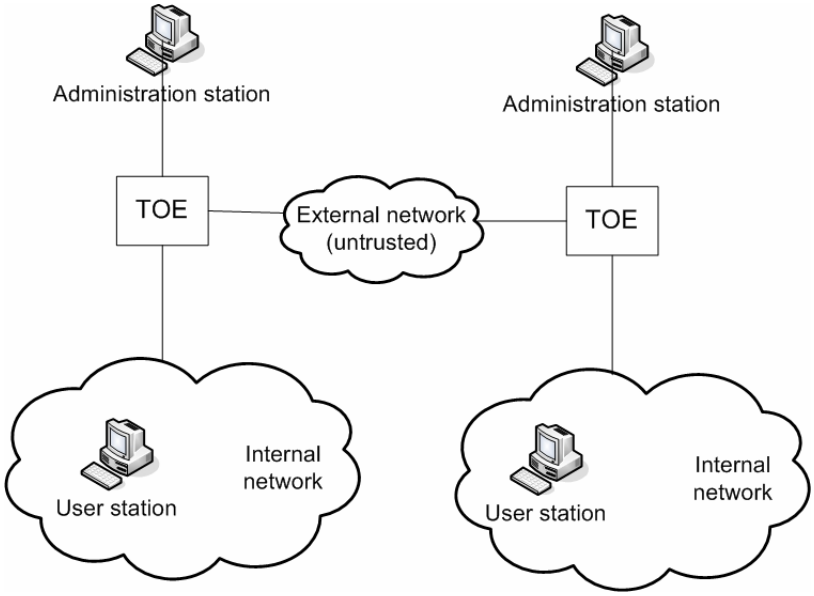
- agent de sécurité (également appelé officier de sécurité, ou responsable de sécurité) ;
- administrateur de sécurité ;
- superviseur sécurité ;
- administrateur système et réseau ;
- superviseur système et réseau ;
- auditeur système et réseau.

Si l'environnement de déploiement du produit le permet, il est recommandé d'utiliser des droits répartis pour éviter le cumul de privilèges.

1.2.5. Configuration évaluée

Le certificat porte sur la configuration du produit en mode “Sécurité renforcée” (voir le chapitre 1.3.9 du guide de première configuration du produit [GUIDES]), en appliquant les recommandations en matière de cryptographie décrites au chapitre 1.4 du guide de première configuration du produit ([GUIDES]).

La plateforme de tests mise en œuvre dans le cadre de cette évaluation est la suivante :



Les tests réalisés dans le cadre de cette évaluation ont porté sur :

- l’*appliance* ARKOON M1000, de la gamme Network Processor Appliances, série Medium ;
- et l’*appliance* ARKOON L3200, de la gamme Network Processor Appliances, série Large.

Les outils d’administration ont été installés dans les environnements suivants :

- Ubuntu Lenny/Sid avec les JRE 1.6 ;
- Windows XP SP3 avec les JRE 1.6 ;
- Windows Seven avec les JRE 1.6.

Note : ce certificat ne s’applique pas aux environnements des outils d’administration correspondant à des JRE[1] antérieurs à la version 1.6.

Des tests d’interopérabilité IPSec ont été réalisés à l’aide du produit VPN SafeNet SoftRemote v10.3.3.

[1] *Java Runtime Environment*

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 octobre 2011, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Dans le cadre du processus de qualification standard, la cotation des mécanismes cryptographiques (rapport [ANA-CRY]) et l'expertise de l'implémentation de la cryptographie (rapport [EXP-CRY]) ont été réalisées. Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VLA visé.

Le produit FAST360 autorise un grand nombre d'algorithmes cryptographiques et de tailles de clés à des fins de compatibilité avec des produits existants. Il est toutefois vivement recommandé de n'utiliser que les algorithmes et les tailles de clés suivants, proposés par défaut par le produit:

- AES en mode CBC avec des clés de 256 bits ;
- RSA avec des clés d'au minimum 4096 bits ;
- Diffie-Hellman avec des clés d'au minimum 2048 bits ;
- HMAC SHA-2 ou HMAC SHA-1.

2.4. Analyse du générateur d'aléas

Les mécanismes de génération d'aléas suivants ont été analysés dans le cadre de cette évaluation (rapports [ANA-CRY] et [EXP-CRY]) :

- génération d'aléas pour la négociation des clés de chiffrement IPSec ;
- génération d'aléas pour l'échange de données IPSec ;
- génération d'aléas pour la mise en œuvre du protocole TLS.

Ces mécanismes sont conformes au référentiel [REF-CRY].

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le « Logiciel FAST360, version 5.0/22» soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations relatives au mode « Sécurité renforcée » se trouvant dans les guides fournis [GUIDES], notamment :

- l'exploitation du produit doit être réalisée conformément aux référentiels cryptographique de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT], notamment concernant la génération et la gestion des clés réalisées hors TOE (OE.CRYPTO, OE.VPN.CRYPTO_EXT) ;
- les équipements sur lesquels le produit est déployé (*appliances* et postes d'administration), ainsi que tous les supports contenant des biens sensibles du produit (papier, disquettes, sauvegardes,...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs (OE.PROTECTION_LOCAL) ;
- l'initialisation des équipements sur lesquels le produit est déployé doit être réalisée à partir de postes d'administration directement connectée sur les équipements et dans le local protégé de l'*appliance* (OE.INITIALISATION_LOCAL) ;
- les administrateurs doivent être de confiance (OE.ADMIN) ;
- les événements d'audit et les alarmes de sécurité générés par le produit doivent être analysés régulièrement (OE.FW.ANALYSE_AUDIT, OE.VPN.ANALYSE_AUDIT, OE.FW.TRAITE_ALARMES, OE.VPN.TRAITE_ALARMES) ;
- les événements d'audit et les alarmes de sécurité générés par le produit doivent faire l'objet de mesures de sauvegarde et d'archivage (OE.FW.ANALYSE_AUDIT, OE.VPN.ANALYSE_AUDIT) ;
- l'environnement du produit doit permettre d'authentifier les administrateurs sur les postes d'administration (OE.AUTHENTIFICATION_ADMIN_DISTANT) ;
- l'administrateur doit disposer de moyens de contrôler la configuration matérielle et logicielle de l'*appliance* par rapport à un état de référence (OE.FW.INTEGRITE, OE.VPN.INTEGRITE).

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique 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] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2		
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**3**	Authorisation controls
	ACM_SCP			**1**	**2**	**3**	3	3	**1**	TOE CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**1**	Delivery procedures
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**1**	Informal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	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**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3		
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3		
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Examination of guidance
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - « ARKOON FAST360/5.0 - Cible de sécurité Critères Communs - Niveau EAL3+ », référence ST_ARKOON_FAST360_50, version 2.6, 14 septembre 2011.
[RTE]	Rapport technique d'évaluation : - « Rapport Technique d'Evaluation - Projet MEHETIA », référence OPPIDA/CESTI/MEHETIA/RTE, version 1.2, 17 octobre 2011.
[ANA-CRY]	« Cotation des mécanismes cryptographiques - Qualification MEHETIA », référence 2912 /ANSSI/ACE, 18 novembre 2010.
[EXP-CRY]	« Rapport d'expertise de l'implémentation de la cryptographie – MEHETIA », référence OPPIDA/CESTI/MEHETIA/CRYPTO/30, 5 mai 2011.
[CONF]	Liste de configuration documentaire : - « Liste des documents fournis pour l'évaluation CC », référence AKV5-LIST-DOCS-CERTIF, révision 2.4, 14 octobre 2011 ; Liste de configuration logicielle : - « Liste de configuration des sources du système », synchronisée avec la livraison du 27/06/11, référence liste-configuration_system, révision 1.5, 13 septembre 2011 ; - «Liste de configuration des sources des outils d'administration », référence. liste-configuration_tools, révision 1.5, 13 septembre 2011 ; Release Note : - « RELEASE NOTES ARKOON : UTM FAST360 v5.0/22 - AMC v5.0/22 », référence Release_Notes_FAST360_5_0_22_FR, version 5.0/22-20111014_1430, 14 octobre 2011, disponible sur le site http://client.arkoon.net.
[GUIDES]	Guides d'administration et d'installation du produit : - « ARKOON FAST360 UTM Appliances - Première Configuration », référence 20110919_1200, 19 septembre 2011 ; - « ARKOON FAST360 UTM Appliances - Guide d'administration », référence 20110919_1200, 19 septembre 2011.
[PP_CIP]	« Profil de protection Chiffreur IP », référence PP-CIP, version 1.5, 3 février 2005. *Ce PP n'est pas certifié.*
[PP_FWIP]	« Profil de protection Firewall d'interconnexion IP », référence PP-FWIP, version 2.2, 10 mars 2006. *Certifié par l'ANSSI sous la référence PP 2006/05.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[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 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010, voir www.ssi.gouv.fr