PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification PP 2006/05

Profil de Protection Firewall d'interconnexion IP (PP-FWIP)

Paris, le 10 octobre 2006,

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.
Un profil de protection est un document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité indépendants de leur technologie et de leur implémentation. Les produits ainsi définis satisfont les besoins de sécurité communs à un groupe d'utilisateurs.
La certification d'un profil de protection ne constitue pas en soi une recommandation de ce profil de protection par le centre de certification.

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 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 : 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 septembre 2006, 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, le Japon, la Norvège, les Pays-Bas, la Corée du Sud et l'Espagne ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Suède, la Turquie, la République Tchèque, Singapour, l'Inde et le Danemark.

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : Profil de protection Firewall d'interconnexion IP
Référence : PP-FWIP
Version : 2.2
Date : 10 mars 2006

1.2. Rédacteurs

Ce profil de protection a été rédigé par :

ARKOON Network Security

13A avenue Victor Hugo
69160 Lyon Tassin
France

SGDN/DCSSI

51 boulevard de La Tour-Maubourg
75007 Paris
France

Groupe Silicomp /AQL

1 rue de la châtaigneraie
CS 51766
35513 Cesson Sévigné Cedex
France

1.3. Description du profil de protection

1.3.1. Généralités

Le profil de protection a été rédigé dans le cadre d'un projet labellisé OPPIDUM subventionné par le ministère de l'économie, des finances et de l'industrie. Il est le résultat de réunions avec des utilisateurs et des développeurs de ce type de produit.
Ce profil de protection est conforme aux préconisations pour la qualification de produits de sécurité au niveau standard selon la version 2.3 des CC [QS-QR].

1.3.2. Périmètre de la cible d'évaluation

La cible d'évaluation (TOE), définie dans le profil de protection identifié en 1.1, permet d'assurer le filtrage des flux dans le cadre de l'interconnexion de réseaux IP. Cette TOE est destinée à participer à la mise en œuvre de la politique de sécurité associée à l'interconnexion

d'un réseau protégé avec un autre réseau. Elle vise en particulier à conserver, après l'interconnexion d'un réseau protégé, son niveau de sécurité initial.
La fonctionnalité principale de la TOE est de permettre la restriction des flux d'informations en provenance ou à destination d'un réseau protégé dans le but de protéger les ressources de ce réseau contre des attaques en provenance d'autres réseaux (via l'interconnexion où est mise en œuvre la TOE). Pour ce faire, elle fournit les services suivants :

- application d'une politique de filtrage ;
- audit/journalisation des flux IP.

De plus, pour son bon fonctionnement, la TOE requiert les services suivants :

- gestion de la politique de filtrage ;
- protection des opérations d'administration ;
- audit des opérations d'administration et supervision ;
- protection de l'accès aux paramètres de la TOE.

1.4. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies dans le profil de protection sont les suivantes :

- Security alarms (FAU_ARP.1)
- Audit data generation (FAU_GEN.1)
- User identity association (FAU_GEN.2)
- Potential violation analysis (FAU_SAA.1)
- Audit review (FAU_SAR.1)
- Selectable audit review (FAU_SAR.3)
- Protected audit trail storage (FAU_STG.1)
- Subset access control (FDP_ACC.1)
- Security attribute based access control (FDP_ACF.1)
- Complete information flow control (FDP_IFC.2)
- Simple security attributes (FDP_IFF.1)
- Subset residual information protection (FDP_RIP.1)
- User authentication before any action (FIA_UAU.2)
- User identification before any action (FIA_UID.2)
- Management of TSF data (FMT_MTD.1)
- Specification of Management Functions (FMT_SMF.1)
- Security roles (FMT_SMR.1)
- Inter-TSF trusted channel (FPT_ITC.1)
- Basic internal TSF data transfer protection (FPT_ITT.1)
- TSF data integrity monitoring (FPT_ITT.3)
- Reliable time stamps (FPT_STM.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)

Toutes les exigences fonctionnelles du profil de protection sont extraites de la partie 2 des Critères Communs [CC].

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL2**[1] **augmenté des composants d'assurance suivants** :

Composants	Descriptions
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1 *	Subset of the implementation of the TSF
ADV_LLD.1 *	Descriptive low-level design
ALC_DVS.1	Identification of security measures
ALC_FLR.3	Systematic flaw remediation
ALC_TAT.1 *	Well-defined development tools
AVA_MSU.1	Examination of guidance
AVA_VLA.2	Independent vulnerability analysis

Tableau 1 - Augmentations

(* Analyse restreinte aux mécanismes de nature cryptographique)

Le niveau de résistance exigé pour les fonctions de sécurité est **élevé** (**SOF-High**).
Toutes les exigences d'assurance du profil de protection sont extraites de la partie 3 des Critères Communs [CC].

1.6. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité sur l'environnement du profil de protection sont les suivants :

- Le référentiel de cryptographie de la DCSSI ([CRYPTO]) doit être respecté lors de la conception et l'exploitation de la TOE pour la gestion des clés (génération, destruction, consommation et distribution) et pour les fonctions de cryptographie utilisées dans la TOE, au niveau de résistance standard (OE.CONCEPTION_CRYPTO).
- Les équipements contenant les services de la TOE (firewall et équipements d'administration), ainsi que tout support contenant les biens sensibles de la TOE (papier, disquettes, sauvegardes,...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs (OE.PROTECTION_LOCAL).
- Les administrateurs doivent être formés aux tâches qu'ils ont à réaliser sur la TOE et être de confiance (OE.ADMIN) ;
- L'environnement de la TOE doit permettre d'authentifier l'administrateur de la TOE pour son accès aux équipements d'administration distants (OE.AUTHENTIFICATION_ADMIN_DISTANT).

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

- L’auditeur doit régulièrement analyser les événements d’audit enregistrés par la TOE et agir en conséquence. La mémoire stockant les événements d'audit est gérée de telle sorte que les administrateurs ne perdent pas d'événements. En outre, les audits doivent faire l'objet de sauvegardes et d'archivages afin que l'impact de leur suppression accidentelle ou volontaire soit limité (OE.GESTION_TRACES_AUDIT).
- L’administrateur de sécurité doit analyser et traiter les alarmes de sécurité générées et remontées par la TOE (OE.TRAITE_ALARME).
- L'administrateur doit disposer de moyens pour contrôler la configuration matérielle et logicielle de la TOE par rapport à un état de référence, ou pour la regénérer dans un état sûr. Cet objectif s'étend à la maîtrise du bien sensible "Politique de filtrage" dès lors que la TOE ne peut elle-même garantir son intégrité (OE.INTEGRITE_TOE).

2. L'évaluation

2.1. Centre d'évaluation

OPPIDA
4-6 avenue du Vieil Etang
Bât B
78180 Montigny Le Bretonneux
France

Adresse électronique : cesti@oppida.fr

2.2. Commanditaires

Ministère de l'Economie, des Finances et de l'Industrie / Direction Générale des Entreprises (DGE)
12, rue Villiot,
75572 Paris Cedex 12
France

ARKOON Network Security

13A avenue Victor Hugo
69160 Lyon Tassin
France

2.3. 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 le rapport technique d'évaluation [RTE].

2.4. Evaluation du profil de protection

L'évaluation du profil de protection a été menée sur la base des exigences de la classe APE définie dans la partie 3 des Critères Communs [CC] :

Class APE	Security Target evaluation
APE_DES.1	TOE description
APE_ENV.1	Security environment
APE_INT.1	ST introduction
APE_OBJ.1	Security objectives
APE_REQ.1	IT security requirements
APE_SRE.1	Explicitly stated IT security requirements

Tableau 2- Composants d'assurance de la classe APE

3. Conclusions de l'évaluation

3.1. Rapport technique d’évaluation

Le rapport technique d’évaluation [RTE] décrit les résultats détaillés de l’évaluation du profil de protection.

3.2. Niveau d'évaluation

Pour tous les composants de la classe APE, les verdicts suivants ont été émis :

Class APE	Protection profile evaluation	
APE_DES.1	TOE description	Réussite
APE_ENV.1	Security environment	Réussite
APE_INT.1	ST introduction	Réussite
APE_OBJ.1	Security objectives	Réussite
APE_REQ.1	IT security requirements	Réussite
APE_SRE.1	Explicitly stated IT security requirements	Réussite

Tableau 3 - Composants et verdicts associés

3.3. Recommandations et limitations d’usage

Le certificat d’un profil de protection ne s’applique qu’à la version évaluée du profil de protection.

3.4. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le profil de protection Profil de Protection Firewall d'interconnexion IP (PP-FWIP) identifié au paragraphe 1.1 du présent rapport **est conforme** aux exigences de la classe APE. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Niveaux d'assurance prédéfinis IS 15408 ou CC

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 2. Références

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td>[CC]</td><td>Critères Communs pour l’évaluation de la sécurité des technologies de l’information:
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.</td></tr>
<tr><td>[CEM]</td><td>Méthodologie d’évaluation de la sécurité des technologies de l’information:
Part 2: Evaluation Methodology, august 2005, version 2.3, ref CCMB-2005-08-004.</td></tr>
<tr><td>[IS 15408]</td><td>Norme Internationale ISO/IEC 15408:2005, comportant 3 documents :
IS 15408–1: (Part 1) Introduction and general model ;
IS 15408–2: (Part 2) Security functional requirements ;
IS 15408–3: (Part 3) Security assurance requirements ;</td></tr>
<tr><td>[RTE]</td><td>Projet : MELEZE - Rapport de fin de tâche APE, référence : OPPIDA/CESTI/ADB/759/2 – Version 2.0 du 28/08/06</td></tr>
<tr><td>[CRYPTO]</td><td>Mécanismes cryptographiques : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, DCSSI, version 1.02 du 19/11/04.</td></tr>
<tr><td>[QS-QR]</td><td>Processus de qualification d’un produit de sécurité – niveau standard, DCSSI, version 1.0 du 28 juillet 2003</td></tr>
</table>

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