Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/06

Suite logicielle IPS Firewall Netasq version 5

Paris, le 25 mars 2005.

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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 le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2005/06

Suite logicielle IPS Firewall Netasq version 5

Développeur : NETASQ

Critères Communs version 2.2

EAL2 Augmenté
(ADV_HLD.2, ADV_LLD.1*, ADV_IMP.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1*, AVA_MSU.1 et AVA_VLA.2)
*appliqués à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

Commanditaire : NETASQ

Centre d'évaluation : Silicomp-AQL

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] 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 mars 2005, 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 République Tchèque, la Suède, Singapour et la Turquie.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est la **Suite logicielle IPS Firewall Netasq version 5** développée par la société NETASQ.

1.2. Développeur

NETASQ

3, rue Archimède
59650 Villeneuve d'Ascq

1.3. Description du produit évalué

Le produit évalué est constitué du logiciel **IPS-Firewall version 5.1.4** exécuté dans des boîtiers appliances et du package **NETASQ administration suite (IHM) version 5.1.4** exécuté sur une station d'administration.

Les boîtiers appliances sont entièrement packagés par NETASQ, et afin de prendre en compte des paramétrages spécifiques aux différents boîtiers, la suite logicielle est compilée dans des « builds » différents S, M, L et XL.

La table suivante identifie les « builds » pouvant être installés dans les différents boîtiers appliances.

Build	Boîtier appliance
S	F25 F50
M	F200 F500
L	F1000 F2000
XL	F5000

1.3.1. Architecture et fonctionnalité du produit

Le boîtier appliance dans lequel s'exécute le logiciel **IPS-Firewall** est destiné à être utilisé en coupure entre plusieurs équipements afin de mettre en œuvre les politiques suivantes :

- politique de filtrage de flux entre les équipements ;
- politique de chiffrement VPN ;
- politique d'authentification préalable.

Ce logiciel inclut un noyau FreeBSD 4.7 avec les correctifs (patches) à jour, adapté et épuré par NETASQ.

Le boîtier appliance est connecté à la station d'administration, au travers d'un réseau, sur lequel s'exécute le package **NETASQ administration suite (IHM)** constitué de trois interfaces graphiques :

- **NETASQ Firewall Manager**, qui permet l'administration et la configuration des firewalls NETASQ ;
- **NETASQ Firewall Monitor**, qui permet la supervision et le monitoring des firewalls ;
- **NETASQ Firewall Reporter**, qui permet l'analyse des logs et reporting.

1.3.2. Politiques de sécurité mises en œuvre

La politique de filtrage de flux entre les équipements se fait sur la base des caractéristiques au niveau IP et transport et de l'identité des utilisateurs authentifiés. Elle permet d'assurer la limitation du débit de certains flux, d'imputer des flux et peut être configurée en fonction de la date et de l'heure.

La politique de chiffrement VPN gère l'authentification mutuelle des extrémités du tunnel et y assure la confidentialité et l'intégrité du contenu des flux.

La politique d'authentification préalable force l'authentification forte des administrateurs et des utilisateurs.

Le produit assure également la protection contre les attaques Internet. Cette protection est basée sur la technologie ASQ qui inclut un moteur d'analyse dynamique aux niveaux IP, transport et applicatif.

1.3.3. Périmètre et limites du produit évalué

Le produit évalué comprend les logiciels **IPS-Firewall** et **NETASQ administration suite (IHM)**. Les composantes matérielles des boîtiers appliances et celles de la station d'administration, ainsi que le système d'exploitation de la station d'administration ne font pas partie du périmètre d'évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

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

2.2. Commanditaire

NETASQ

3, rue Archimède
59650 Villeneuve d'Ascq

2.3. Centre d'évaluation

Silicomp-AQL

1 rue de la châtaigneraie
CS 51766
35517 Cesson Sévigné Cedex
France

Téléphone : +33 (0)2 99 12 50 00

Adresse électronique : cesti@aql.fr

2.4. Rapport technique d'évaluation

L'évaluation s'est déroulée du 6 juin 2004 au 9 mars 2005.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.5. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.

La cible de sécurité énonce explicitement deux exigences fonctionnelles de sécurité :

- Schedule security behaviour (FMT_MOF.SSB)
- Backup and restoration of TSF data (FMT_MTD.BRS)

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		Verdicts
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

2.6. Evaluation du produit

2.6.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL2[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL2	Structurally tested
+ADV_HLD.2	Security enforcing high-level design
+ADV_LLD.1*	Descriptive low-level design
+ADV_IMP.1*	Subset of the implementation of the TSF
+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

* les composants d'assurance ADV_LLD.1, ADV_IMP.1 et ALC_TAT.1 sont appliqués à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS.

2.6.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

NETASQ

3, rue Archimède
59650 Villeneuve d'Ascq

Les mesures de sécurité identifiées par l'évaluateur permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation lors du développement.

[1] Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

La vérification de l'application des mesures analysées a été effectuée lors d'une visite du site. (cf Annexe 1)

Des 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.

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_CAP.2	Configuration items	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.1	Identification of security measures	Réussite
ALC_FLR.3	Systematic flaw remediation	Réussite
ALC_TAT.1	Well-defined development tools	Réussite

2.6.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP) et conception de haut-niveau (HLD). Pour la partie du produit réalisant des opérations cryptographiques (classe FCS), cette analyse a aussi porté sur la conception de bas-niveau (LLD) et l'implémentation (IMP).

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :
Pour la fonctionnalité de filtrage :

- Complete information flow control (FDP_IFC.2)
- Simple security attributes (FDP_IFF.1)

Pour la fonctionnalité d'authentification :

- User identification before any action (FIA_UID.2)
- User authentication before any action (FIA_UAU.2)
- Multiple authentication mecanisms (FIA_UAU.5)

Pour la fonctionnalité de chiffrement :

- Subset information flow control (FDP_IFC.1)
- Basic data exchange confidentiality (FDP_UCT.1)
- Data exchange integrity (FDP_UIT.1)
- Simple security attributes (FDP_IFF.1)

Pour la fonctionnalité de VPN :

- Trusted Path (FTP_TRP.1)
- Multiple authentication mecanisms (FIA_UAU.5)
- Inter-TSF basic TSF consistency (FPT_TDC.1)

Pour la fonctionnalité de journalisation, d'audit et d'alarme:

- Audit data generation (FAU_GEN.1)
- User identity association (FAU_GEN.2)
- Audit review (FAU_SAR.1)
- Action in case of possible data loss (FAU_STG.3)
- Security alarms (FAU_ARP.1)
- Management of security functions behavior (FMT_MOF.1)
- Management of TSF data (FMT_MTD.1)
- Backup and restoration of TSF data (FMT_MTD.BRS)
- Security Alarms (FAU_ARP.1)
- Schedule security behaviour (FMT_MOF.SSB)

Pour la protection contre les attaques Internet :

- Complex heuristic attack (FAU_SAA.4)
- Security alarms (FAU_ARP.1)

Pour la protection contre l'utilisation impropre :

- Specification of management functions (FMT_SMF.1)
- Security roles (FMT_SMR.1)
- Complete access control (FDP_ACC.2)
- Management of security functions behavior (FMT_MOF.1)
- Management of TSF data (FMT_MTD.1)

Pour la protection de la cible d'évaluation:

- Basic internal TSF transfer protection (FPT_ITT.1)
- Trusted path (FTP_TRP.1)
- Multiple authentication mecanisms (FIA_UAU.5)

Pour le soutien de la sécurité:

- Cryptographic operation (FCS_COP.1)
- Reliable time stamp (FPT_STM.1)

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_FSP.1	Informal functional specification	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.1	Subset of the implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.6.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du produit entre le développeur et le client.

L'installation du produit correspond à la connexion et à la mise en fonctionnement du produit chez le client. Les procédures analysées [INSTALL] permettent d'obtenir la configuration évaluée du produit.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		**Verdicts**
ADO_DEL.1	Delivery procedure	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

2.6.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, les administrateurs du produit sont ceux qui définissent et implémentent les configurations du produit et les utilisateurs sont ceux qui utilisent le produit et ont besoin pour cela de s'authentifier.

L'évaluateur a analysé le guide d'administration [GUIDE] pour s'assurer qu'il permet d'exploiter le produit évalué d'une manière sécurisée. Ce guide qui est destiné aux administrateurs spécifie les instructions à donner aux utilisateurs pour l'utilisation sécurisée du produit.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		**Verdicts**
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.6.6. L'évaluation des tests fonctionnels

L'évaluateur a réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.

L'évaluateur a réalisé ses tests fonctionnels indépendants sur une plate-forme composée de deux boîtiers appliances F200 et F1000, d'une station d'administration avec la suite **NETASQ administration suite (IHM)** et de deux stations de travail sous Unix FreeBSD version 4.10.

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		**Verdicts**
ATE_COV.1	Evidence of coverage	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.6.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [INSTALL] [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

La cible de sécurité n'identifie aucun mécanisme probabilistique ou combinatoire non-crytpographique.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests sur la même plate-forme que les tests indépendants.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de **niveau élémentaire**.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.1	Examination of guidance	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.2	Independent vulnerability analysis	Réussite

2.6.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (Art. 8 du décret 2002-535)

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

L'administrateur du produit certifié devra s'assurer du respect des hypothèses de sécurité, détaillées dans la cible de sécurité [ST] et résumées ci-dessous :

- les boîtiers appliances sont installés et stockés de manière sécurisée ;
- le super-administrateur est le seul à pouvoir se connecter à la console locale des boîtiers ;
- les mots de passe utilisés sont gérés par une politique de création ou de contrôle ;
- la politique de contrôle de flux d'information est définie de manière complète, stricte, correcte et non ambiguë ;
- les administrateurs sont non-hostiles, compétents et formés par rapport à leurs responsabilités ;
- les boîtiers appliances sont installés comme seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de sécurité ;
- à part les fonctions de sécurité, les boîtiers appliance ne fournissent pas de service réseau autre que le routage et la translation d'adresse ;
- la cible d'évaluation ne dépend pas de services externes « en ligne » pour l'application de sa politique de contrôle de flux ;
- les stations d'administration à distance sont sécurisées ;
- les équipements réseaux avec lesquels le produit établit des tunnels VPN sont protégés de manière équivalente aux boîtiers appliances ;
- les postes sur lesquels s'exécutent les clients VPN sont protégés de manière équivalente aux boîtiers appliances.

L'administrateur du produit certifié devra :

- s'assurer que les ports USB physiquement présents sur les boîtiers appliances restent logiquement inaccessibles ;
- ajouter une règle spécifique s'il veut qu'une alarme soit générée à l'arrivée d'un paquet broadcast venant d'une adresse autre que 255.255.255.255 ;

- utiliser les algorithmes cryptographiques et les tailles de clés correspondant aux options spécifiées dans la cible de sécurité [ST §5.2.5.1.1] rappelées ici :

Opération cryptographique	***Algorithme***	***Taille des clés***
Signature et élaboration de clé	Diffie-Hellman	1536, 2048
Chiffrement/déchiffrement asymétrique	RSA	2048, 4096
Hachage univoque	HMAC-SH 1	160
Chiffrement / déchiffrement symétrique des paquest VPN	AES	128, 192, 256
	Triple DES	168
	Blowfish	128 à 256
	CAST	128
Chiffrement / déchiffrement symétrique des sessions d'administration	AES	128
Contrôle d'intégrité des sessions d'administration	HMAC-SH 1	160

L'administrateur devra également suivre les recommandations se trouvant dans les guides fournis [INSTALL] [GUIDE].

3.3. Reconnaissance européenne (SOG-IS)

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

3.4. Reconnaissance internationale (CC RA)

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

Annexe 1. Visite du site de développement de la société NETASQ à Villeneuve d'Ascq

Le site de développement de la société NETASQ situé à Villeneuve d'Ascq, a fait l'objet d'une visite par l'évaluateur le 10 novembre 2004 pour s'assurer de l'application des procédures de support au cycle de vie pour le produit Suite logicielle IPS Firewall Netasq version 5.

Ces procédures ont été fournies et analysées dans le cadre de la tâche d'évaluation suivante :

- ALC_DVS.1

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 2. 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 3. Références documentaires du produit évalué

[ST]	Firewalls NETASQ, évaluation de la suite logicielle IPS-Firewall version 5, NETASQ, réf : na-tn_ciblesec_fr.sxw, version 1.7 du 7 mars 2004 ;
[RTE]	Rapport technique d'évaluation – évaluation selon un paquet EAL2 , AQL, ref : NTQ002-RTE01-4.00, réf : 4.00 su 9 mars 2005
[INSTALL]	Quickstart – Comment installer votre IPS-Firewall NETASQ, NETASQ, réf : na_qs_v5_003 du 16 octobre 2003.
[GUIDE]	Manuel d'utilisation et de configuration administration suite v5, NETASQ, réf : na_ug_asv5_009_fr du 8 mars 2005 ; Manuel d'installation et de configuration – EZAdmin, NETASQ, réf : na_qs_ezadmin_002_fr.pdf du 17 octobre 2003 ; Manuel d'utilisation de reporter pro, NETASQ, réf : na_ug_ASvPRO_001_fr.pdf du 5 décembre 2003.
[Visite]	Rapport de visite Aspects organisationnels, AQL, réf : NTQ002-RAU01-1.00 du 16 novembre 2004.

Annexe 4. 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.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[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
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr