Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2014/72

Fonction de filtrage de la suite logicielle IPS-Firewall, version 9.1.0.5

Paris, le 21 octobre 2014

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

Contre-amiral Dominique RIBAN
[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 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-2014/72

Nom du produit

Fonction de filtrage de la suite logicielle IPS-Firewall

Référence/version du produit

Version 9.1.0.5

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_FLR.3

Développeur

NETASQ

Parc Scientifique de la Haute borne Parc Horizon, Bâtiment 6, Avenue de l'Horizon
59650 Villeneuve d'Ascq
France

Commanditaire

NETASQ

Parc Scientifique de la Haute borne Parc Horizon, Bâtiment 6, Avenue de l'Horizon
59650 Villeneuve d'Ascq
France

Centre d'évaluation

Oppida

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

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

L'évaluation porte sur la « Fonction de Filtrage de la Suite logicielle IPS-Firewall, version 9.1.0.5 » développée par la société NETASQ.

Il s'agit d'une brique logique intégrée à la suite logicielle « IPS-Firewall » embarquée dans les boîtiers « pare-feu – VPN » de la société NETASQ.

Le boîtier « pare-feu – VPN » offre des fonctionnalités de type pare-feu regroupant filtrage, détection d'attaques, gestion de la bande passante, gestion de la politique de sécurité, audit, imputabilité et authentification forte des administrateurs. Il offre également des fonctionnalités VPN (*Virtual Private Network* – Réseau Privé Virtuel : chiffrement et authentification) implémentant le protocole ESP (*Encapsuling Security Payload*) du standard IPSec en mode tunnel, sécurisant ainsi la transmission de données entre des sites distants.

De façon plus spécifique le rôle de la fonction de filtrage, consiste à filtrer les flux, entre différentes zones de confiance ; Typiquement un réseau non maîtrisé et un réseau de confiance comme schématisé dans la figure 1.

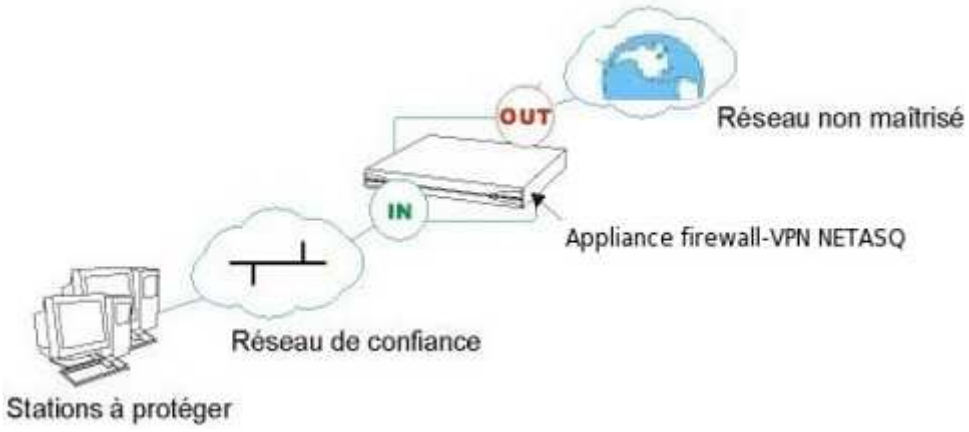

Figure 1 - Cas d'utilisation classique du produit

1.2. Description du produit

1.2.1. Introduction

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

1.2.2. Identification du produit

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

La version certifiée du produit est identifiable par :

- l'interface Web Manager : une fois connecté, la version de la TOE est indiquée en haut de la fenêtre d'administration ;
- l'interface Event Reporter : une fois connecté à l'application, l'onglet « Divers » regroupe les informations sur le pare-feu. La ligne intitulée « Nom du firewall » contient la version de la TOE ;
- l'interface Real-Time Monitor : une fois connecté à l'application, l'onglet « Dashboard » indique la version de la TOE ;
- la connexion directe en SSH sur la TOE permet également de vérifier la version qui est inscrite dans la bannière d'accueil.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par la TOE sont :

- le filtrage des flux entre les équipements ;
- la journalisation, l'audit et la remontée d'alarmes.

1.2.4. Architecture

La TOE est « la fonction de filtrage », qui est elle-même une brique du composant *Active Security Qualification* (ASQ). Ce dernier est l'un des différents composants de la suite logicielle « IPS-Firewall ». Cette suite inclut notamment un système d'exploitation basé sur le noyau « FreeBSD ».

La « Suite logicielle IPS-Firewall, version 9.1.0.5 » dans son ensemble a fait l'objet d'une évaluation menée conjointement à la présente et a été certifié au niveau EAL3 augmenté de ALC_CMC.4, ALC_CMS.4, ALC_FLR.3, AVA_VAN.3 (voir [ANSSI-CC-2014/70]).

Le schéma (Figure 2) montre l'architecture globale de la suite logicielle du produit avec le composant ASQ.

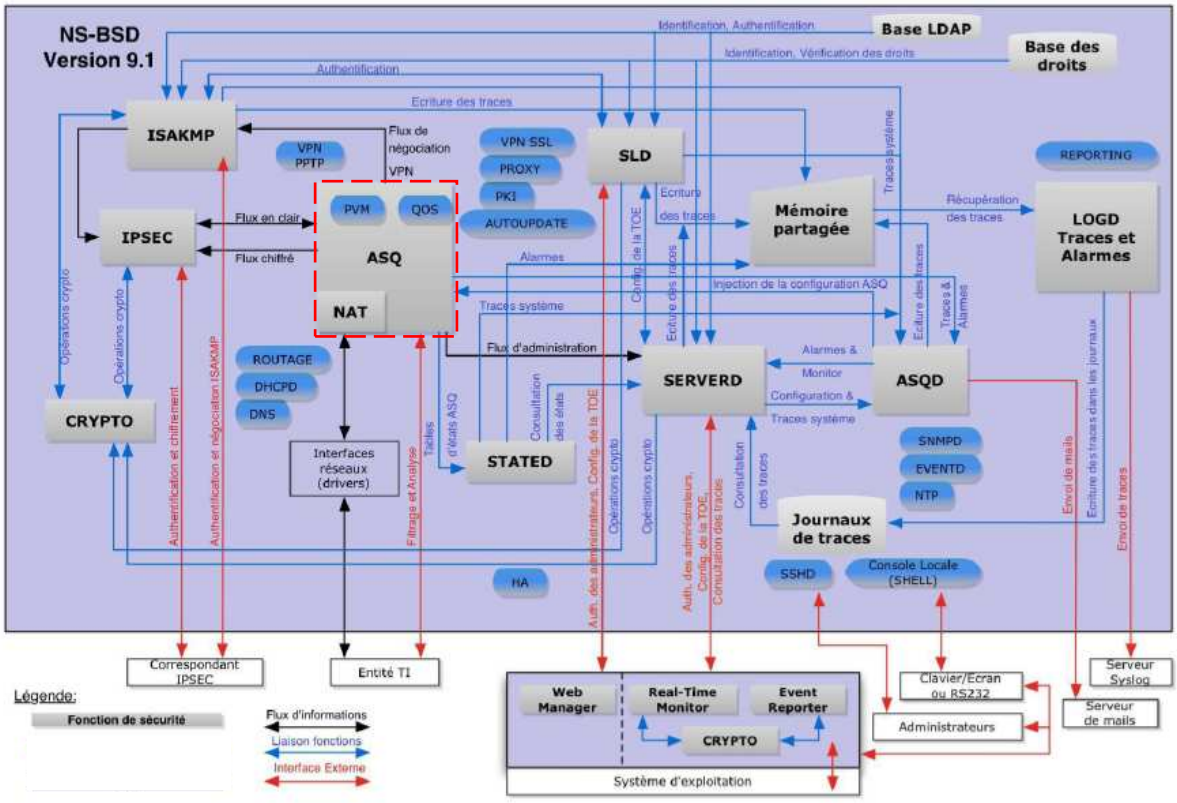

Figure 2 - Schéma des composants et interfaces de la TOE

Le schéma Figure 3 place la TOE dans son environnement et les différentes interconnexions.

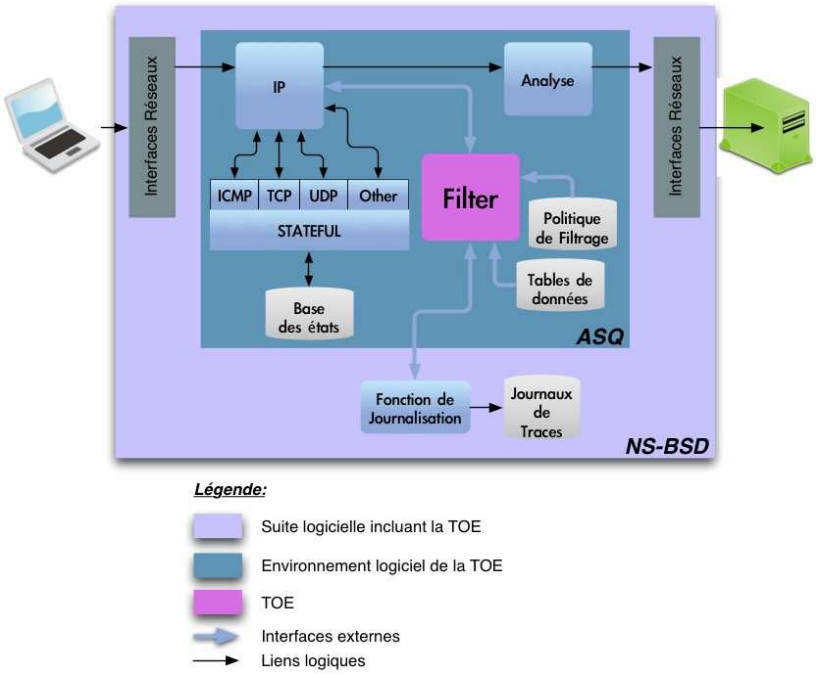

Figure 3 - Schéma des composants et interconnexions de la TOE

Le composant ASQ est en charge de l'application de la politique de filtrage des flux d'information et de leur analyse.

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

- **Développement** : développement du produit ;
- **Déploiement** : mise à disposition du produit aux clients ;
- **Installation** : installation du produit conformément aux recommandations fournies par NETASQ dans les guides (voir [GUIDES]) ;
- **Exploitation** : suivi du produit au jour le jour lorsqu'il est en production avec remontée éventuelle de bugs ;
- **Rebus** : destruction d'un produit obsolète ou défaillant.

Seules les phases de développement et de déploiement (réalisées par NETASQ) ont été évaluées.
Les phases d'installation, d'exploitation et de rebus sont réalisées par le client.

Le produit a été développé sur les sites suivants :

NETASQ

Parc Horizon – Bâtiment 6
Avenue de l'horizon
59650 Villeneuve d'Ascq
France

NETASQ

49 rue de Billancourt
92100 Boulogne-Billancourt
France

L'évaluateur a considéré comme administrateurs du produit les personnes réalisant les opérations d'administration de la sécurité et responsables de leur exécution conformément aux guides [GUIDES], et comme utilisateurs du produit les personnes utilisant des ressources informatiques des réseaux de confiance protégés par le produit.

La définition des profils administrateurs est du ressort d'un administrateur spécial, le « super-administrateur », qui intervient exclusivement lors des phases d'installation et de maintenance et est le seul habilité à se connecter, via la console locale, sur les boîtiers. Il doit être le seul responsable de l'accès dans les locaux où sont stockés les boîtiers.

1.2.6. Configuration évaluée

La configuration évaluée correspond à celle décrite dans le chapitre 2.5 de la cible de sécurité [ST]. Par ailleurs, la TOE a été configurée en désactivant les services suivants:

- les modules permettant la prise en charge des serveurs externes (ex : Kerberos, RADIUS, etc) ;
- le module de routage dynamique ;
- l'infrastructure à clés publiques (PKI) interne ;
- le module VPN SSL ;
- le cache DNS ;
- le moteur antivirus (ClamAV ou Kaspersky) ;
- le module Active Update.

Les tests ont été effectués sur la version 32 bits des boîtiers U250S et NG1000-A. La suite d'administration NETASQ version 9.1.0.5 a été installée sur un poste de travail sous Windows Seven 32 bits édition Professionnelle à jour avec tous les correctifs publiés par Microsoft. Le navigateur web utilisé pour le NETASQ Web Manager est Microsoft Internet Explorer version 9 à jour avec tous les correctifs publiés par Microsoft.

La plate-forme de test est schématisée ci-dessous.

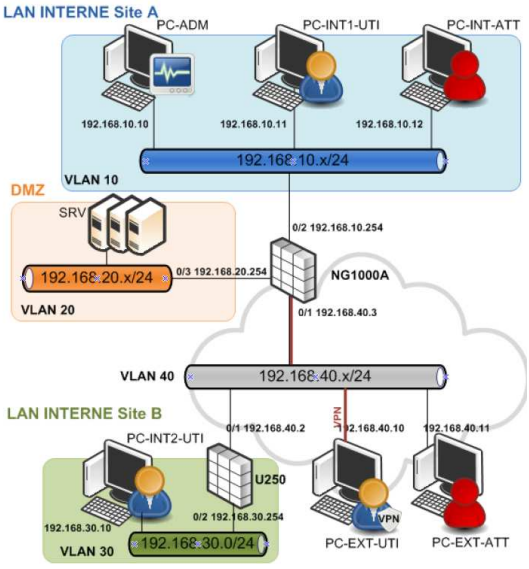

Figure 4 - Plate-forme de test

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 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 25 juillet 2014, 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

La TOE ne comporte pas de mécanismes cryptographiques.

2.4. Analyse du générateur d'aléas

La TOE ne comporte pas de générateur d'aléas.

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 la « Fonction Filtrage de la Suite logicielle IPS-Firewall, version 9.1.0.5 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté du composant ALC_FLR.3.

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 se trouvant dans les guides fournis [GUIDES], notamment :

- les boîtiers doivent être installés et stockés conformément à l'état de l'art concernant les dispositifs de sécurité sensibles ;
- les boîtiers doivent être installés de façon à constituer les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle des flux d'information ;
- soit les boîtiers doivent être dimensionnés en fonction des capacités des équipements adjacents, soit ces derniers doivent réaliser des fonctions de limitation du nombre de paquets par seconde transmis par les équipements du réseau protégé, positionnées légèrement en dessous des capacités maximales de traitement de chaque boîtier installé dans l'architecture réseau ;
- à part l'application des fonctions de sécurité, les boîtiers ne doivent pas fournir de service réseau autre que le routage et la translation d'adresse ;
- la politique de contrôle des flux d'informations à mettre en œuvre doit être définie, pour tous les équipements des réseaux de confiance à protéger, de manière complète, stricte, correcte et non ambiguë.

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 4+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Problem tracking CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**1**	Testing: basic 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_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**3**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : *Cible de sécurité fonction de filtrage - Suite logicielle IPS-Firewall Version 9.1,* *Référence* : NA_ASE_ciblesec_filter_v91, *Version* : 1.8, *Date* : 18/06/2014.
[RTE]	Rapport technique d'évaluation : *Rapport Technique d'Evaluation Projet GORA,* *Référence* : OPPIDA/CESTI/GORA/RTE, *Version* : 1.0, *Date* : 25/07/2014.
[CONF]	Listes de configuration du produit : - Référence : NA_ALC_sources_liste_9105, NETASQ ; - Liste des fournitures – Fonction de Filtrage & Suite logicielle IPS-Firewall version 9.1, Référence : NA_ALC_fournitures_v91, Version 1.10 datée du 16/06/2014, NETASQ.
[ANSSI-CC-2014/70]	Rapport de certification du produit : « Suite logicielle IPS-Firewall, version 9.1.0.5 »

[GUIDES]	Guide d'installation rapide (document livré avec le boîtier) : - NETASQ Firewall Multifonctions – Guide d'installation rapide – Série U ; Guide d'utilisation et de configuration de l'interface Web Manager : - NETASQ Firewall Multifonctions – Manuel d'utilisation et de configuration, Référence : nafrgde_FirewallUserGuide, Version 2.2-Firmware V9.1.3 datée de Juin 2014, NETASQ ; Guide d'utilisation et de configuration de l'interface Event Reporter : - NETASQ Event Reporter V9.1 – Manuel d'utilisation et de configuration, Référence : nafrgde_nereporter-v9.1, Version 9.1 datée d'Octobre 2013, NETASQ ; Guide d'utilisation et de configuration de l'interface Real-Time Monitor : - NETASQ Real-Time Monitor V9.0 – Manuel d'utilisation et de configuration, Référence : nafrgde_nrmonitor-v9.1, Version 9.1 datée d'Octobre 2013, NETASQ ; Guide de restauration logicielle par clé USB : - NETASQ Firewall Multifonctions – Restauration logicielle par clé USB, Référence : nafrgde_USB_Recovery, Version 1.1 datée d'Octobre 2013, NETASQ ; Guide de démontage du boîtier pour raison de confidentialité en cas de panne : - NETASQ – Option « Retour sécurisé », Référence : nafrtno_echange-securise, Version 1.2, NETASQ.

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF]	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 (RGS_B_1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_3), voir www.ssi.gouv.fr.