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-2014/70

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-2014/70

Nom du produit

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 3 augmenté

ALC_CMC.4, ALC_CMS.4, ALC_FLR.3, AVA_VAN.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

Le produit évalué est la « Suite logicielle IPS-Firewall, version 9.1.0.5 » développée par la société NETASQ.

Ce produit 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. Un cas d'utilisation classique du produit est décrit dans la figure ci-dessous.

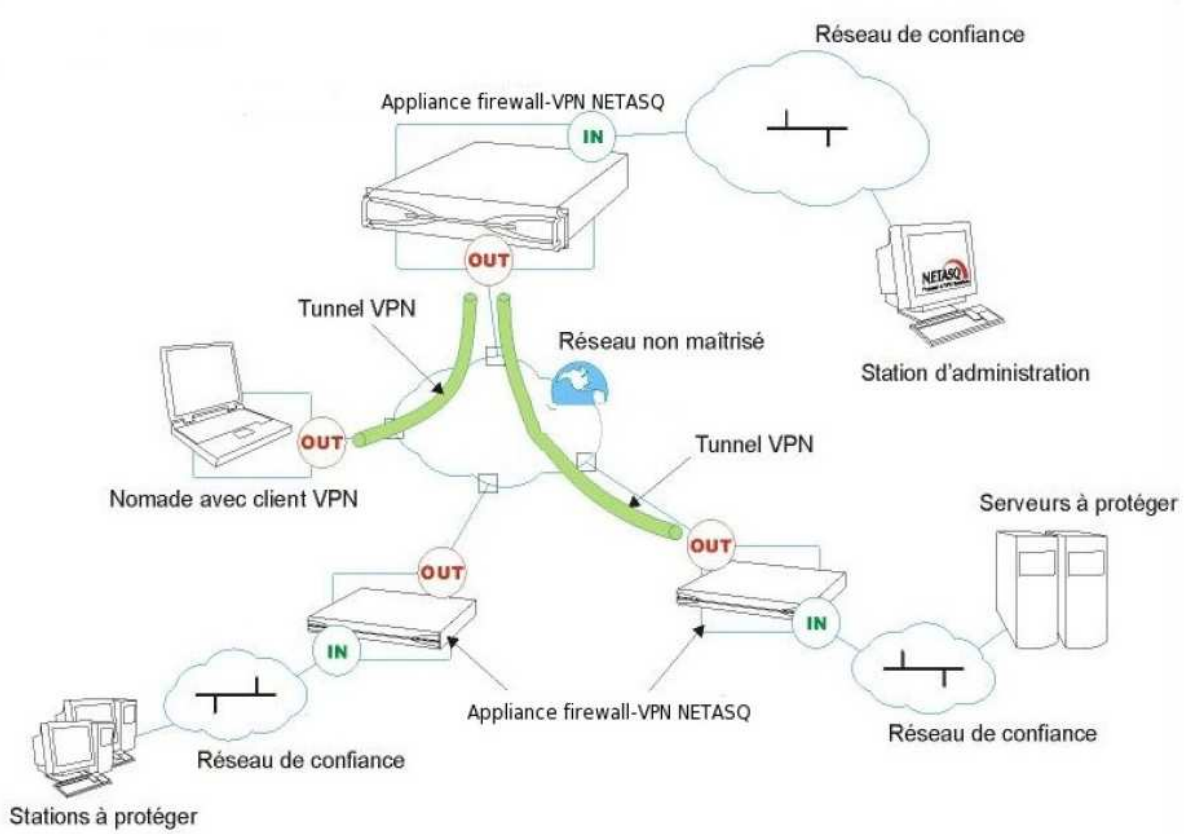

Figure 1 - Cas d'utilisation classique du produit

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].

Chaque boîtier IPS-Firewall NETASQ est identifié de manière unique au moyen d'un numéro de série. Il possède en outre une bi-clé et un certificat numérique interne. Chaque certificat inclut le numéro de série et le modèle du produit.

Une étiquette, collée sur chacun des boîtiers ainsi que sur le carton d'emballage, indique son modèle, son numéro de série, le code d'activation web du client (code qui permet l'activation du compte client dans l'espace client du site web NETASQ à partir duquel il est possible de télécharger la « Suite d'administration ») et un code barre contenant le numéro de série du produit.

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 le produit sont :
- le filtrage des flux ;
- le chiffrement (au niveau IP) entre les équipements ;
- la prévention des intrusions ;
- l'établissement des associations de sécurité ;
- la journalisation, l'audit et la remontée d'alarmes ;
- le contrôle d'accès aux opérations d'administration de la sécurité ;
- la sauvegarde et la restauration ;
- la protection des sessions d'administration.

1.2.4. Architecture

La TOE est constituée de deux packages applicatifs distincts :
- NS-BSD constitue le logiciel IPS-Firewall s'exécutant dans le boitier ;
- NETASQ Administration Suite est le logiciel s'exécutant sur les stations d'administration.

Le produit peut être décomposé en 13 sous-systèmes décris en gris dans la figure ci-dessous :

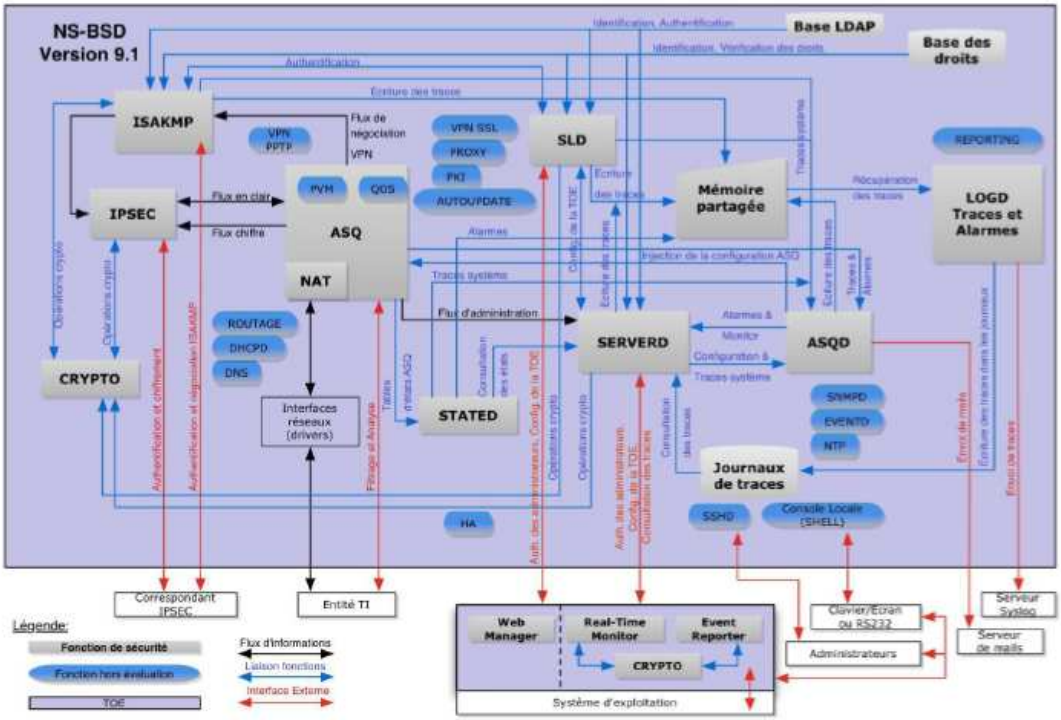

Figure 2- Architecture logique de la TOE

Le package NS-BSD est constitué des sous-systèmes suivants :

- ASQ est en charge de l'application de la politique de filtrage des flux d'information et de leur analyse ;
- ASQD collecte les traces générées par le sous-système ASQ et les transmet au sous-système LOGD. Dans le cas des alarmes, les données sont transmises au serveur d'administration SERVERD. L'autre rôle majeur d'ASQD est de transmettre la configuration de la politique d'analyse des attaques (action et niveau d'alarme), ainsi que la génération ou non de traces des flux acceptés par la politique de filtrage au sous-système ASQ ;
- STATED est en charge du monitoring des états ASQ, de la génération des alarmes lors des changements d'état des interfaces réseaux, etc. ;
- SLD permet une administration de l'IPS-Firewall par l'intermédiaire du client NETASQ Web Manager. Il permet ainsi d'offrir une interface d'administration Web au serveur d'administration SERVERD ;
- LDAP est composé d'une base de données de type annuaire LDAP contenant l'ensemble des informations relatives aux utilisateurs ;
- IPSEC est en charge de l'application de la politique de chiffrement. Celui-ci chiffre et authentifie les flux d'information, à partir d'un ensemble de règles de sécurité données (SPD) et d'associations de sécurité négociées (SAD). Il utilise pour cela le protocole ESP de la norme IPsec ;
- ISAKMP est en charge de la négociation des associations de sécurité en vue de l'application de la politique de chiffrement. Il négocie celles-ci selon le protocole IKE ;
- SERVERD permet l'interaction entre les clients IHM et la configuration de l'IPS-Firewall, mais également les remontées des informations pour le moniteur temps réel ou la consultation des journaux d'audit ;

- LOGD est en charge de la génération et de la consultation des traces générées par l'ensemble des autres sous-systèmes.

Le package NETASQ Administration Suite (IHM), qui s'exécute sur la station d'administration, est constitué de trois interfaces graphiques :

- NETASQ Web Manager, qui permet l'administration et la configuration des firewalls NETASQ ;
- NETASQ Event Reporter, qui permet la supervision et le monitoring d'un ou de plusieurs firewalls ;
- NETASQ Real-Time Monitor, qui permet la présentation de façon conviviale de l'état du système, les journaux d'alarme et permet de manipuler certaines informations stockées sur l'IPS-Firewall.

Enfin, la brique CRYPTO commune aux deux packages fournit les fonctions cryptographiques aux différents sous-systèmes.

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. Les guides associés sont référencés en annexe 2

Le produit a été développé sur les sites suivant :

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.

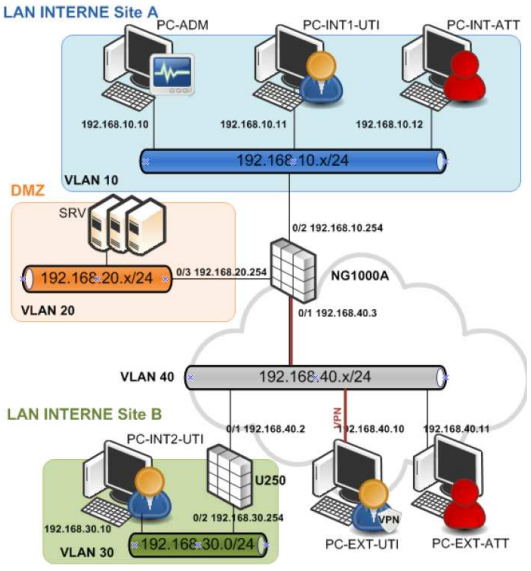

Figure 3 - Plate-forme de test

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 cotation des mécanismes cryptographiques a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations suivantes doivent être suivies :

- utilisation de la fonction de hachage sha-256 pour l'implémentation du protocole SRP ;
- utilisation d'IKEv2 ;
- utilisation de TLSv1.2.

Quoi qu'il en soit, les 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_VAN.3 visé.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-CRY]. 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_VAN.3 visé.

2.4. Analyse du générateur d'aléas

Le produit comporte un générateur d'aléas entrant dans le périmètre d'évaluation. Ce générateur a fait l'objet d'une analyse. Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Conformément au document [REF] la sortie du générateur matériel de nombres aléatoires subit un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

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 « 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 3 augmenté des composants ALC_CMC.4, ALC_CMS.4, ALC_FLR.3 et AVA_VAN.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 cible d'évaluation ne doit pas dépendre de services externes « en ligne » pour l'application de la politique de contrôle des flux d'information ;
- les équipements réseau avec lesquels la cible d'évaluation établit des tunnels VPN doivent être protégés de manière équivalente aux boîtiers;
- lors de l'installation de la cible d'évaluation ou pour des opérations de maintenance, le super-administrateur doit être le seul à être habilité à se connecter, via la console locale, sur les boîtiers ;
- tous les accès dans les locaux où sont stockés les boîtiers et toutes les interventions de maintenance sur les boîtiers doivent se faire sous la surveillance du super-administrateur ;

- les mots de passe des utilisateurs et des administrateurs doivent être gérés par une politique de création et de contrôle des mots de passe respectant les principes décrits dans les [GUIDES] ;
- 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 ;
- les administrateurs doivent être des personnes de confiance, compétentes et formées, disposant des moyens nécessaires à l'accomplissement de leurs tâches ;
- les stations d'administration distantes doivent être sécurisées, maintenues à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées, installées dans des locaux à accès protégé et doivent être exclusivement dédiées à l'administration de la cible d'évaluation et au stockage des sauvegardes ;
- les postes sur lesquels s'exécutent les clients VPN des utilisateurs autorisés doivent être protégés de manière équivalente aux stations d'administration distantes ;
- les algorithmes cryptographiques et les tailles de clés correspondant aux options spécifiées dans la cible de sécurité [ST, §5.2.5] et dans le guide d'utilisation de l'interface Web Manager (voir [GUIDES]), rappelées ici, doivent être utilisées :

Opération cryptographique	***Algorithme***	***Taille des clés***
Signature et élaboration de clés	Diffie-Hellman	2048, 3072, 4096
Chiffrement / déchiffrement asymétrique	RSA	2048, 4096
Hachage univoque	HMAC-SHA1	160
	HMAC-SHA2	256, 384, 512
	SHA2	256, 384, 512
Chiffrement / déchiffrement symétrique des paquets 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-SHA1	160

- il est nécessaire que les administrateurs soient sensibilisés à la complexité attendue d'un mot de passe étant donné que le niveau de force que donne l'indicateur de mot de passe ne correspond pas aux recommandations de l'ANSSI.

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
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural 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		
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**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : *Cible de sécurité - Suite logicielle IPS-Firewall Version 9.1* *Référence* : NA_ASE_ciblesec_v91 ; *Version* : 1.13 ; *Date* : 13/06/2014 ;
[RTE]	Rapport technique d'évaluation : *Rapport Technique d'Evaluation Projet GAIA* *Référence* : OPPIDA/CESTI/GAIA/RTE ; *Version* : 1.0 *Date* : 25/07/2014
[ANA-CRY]	*CC-CRYPTO-GAIAv2 0* *Référence* : OPPIDA/DOC/2014/BIW/673/2.0 ; *Version* : 2.0 *Date* : 18/06/2014
[EXP-CRY]	*CC-CRYPTO-GAIAv2 0* *Référence* : OPPIDA/DOC/2014/BIW/673/2.0 ; *Version* : 2.0 *Date* : 18/06/2014
[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.

[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.