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-2020/66

Stormshield Network Security UTM / NG-Firewall Software Suite (Version 3.7.9)

Paris, le 9 juillet 2020

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2020/66

Nom du produit

Stormshield Network Security UTM / NG-Firewall Software Suite

Référence/version du produit

Version 3.7.9

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 3 augmenté

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

Développeur

Stormshield

22 rue du Gouverneur Général Eboué
92130 Issy-Les-Moulineaux, France

Commanditaire

Stormshield

22 rue du Gouverneur Général Eboué
92130 Issy-Les-Moulineaux, France

Centre d'évaluation

Oppida

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

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.3.

SOG-IS

Ce certificat est reconnu au niveau EAL3 augmenté de ALC_CMS.4, ALC_CMC.4, ALC_FLR.3.

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 directeur général de l'Agence national de la sécurité des systèmes d'information 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 « Stormshield Network Security UTM / NG-Firewall Software Suite, version 3.7.9 » développé par *STORMSHIELD* et exécuté par les *appliances STORMSHIELD* suivantes : SN210, SN310, SNi40, SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100.

Les *appliances STORMSHIELD* offrent des fonctions de sécurité permettant d'interconnecter un ou plusieurs réseaux de confiance via un réseau non maitrisé sans dégrader le niveau de confiance. Les principales fonctions de sécurité peuvent être regroupées en deux catégories :

- la fonctionnalité de par-feu : regroupant filtrage, détection d'attaques, gestion de la bande passante, gestion de la politique de sécurité, audit, imputabilité et authentification forte des administrateurs ;
- la fonctionnalité VPN (*Virtual Private Network* – Réseau Privé Virtuel) 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.

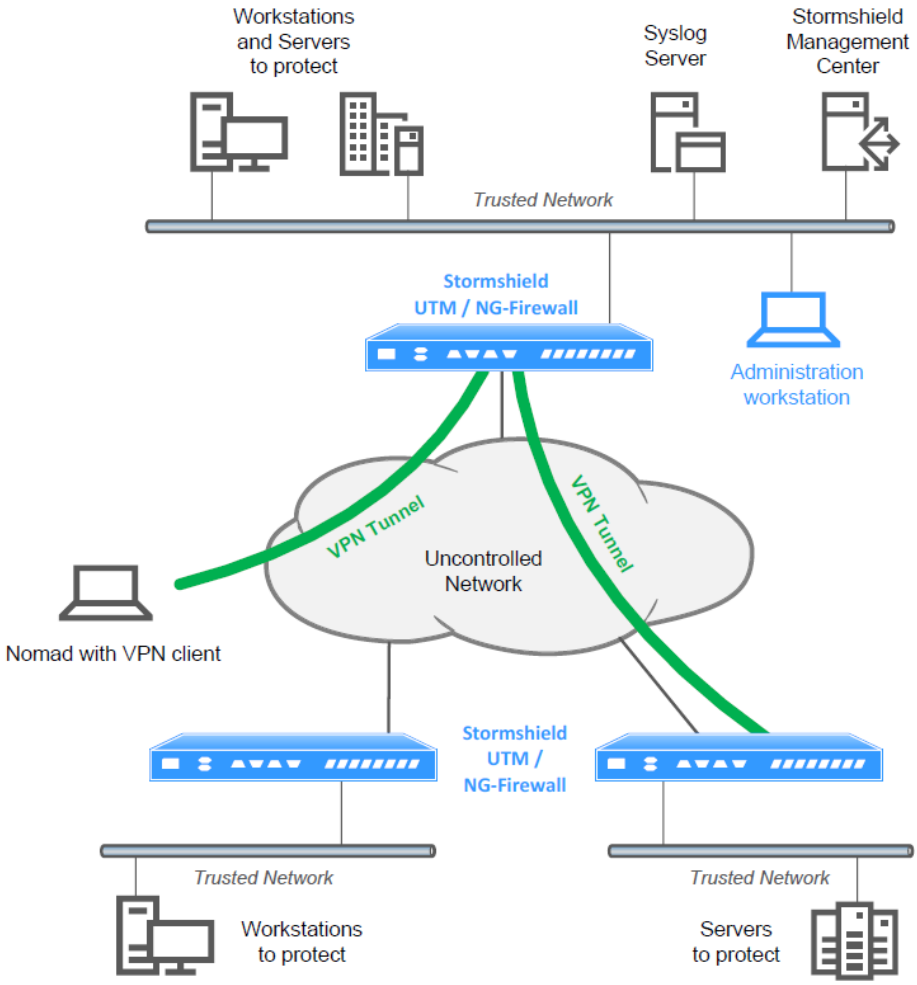

Figure 1 - Cas d'utilisation classique du produit

L'évaluation porte sur les parties logicielles suivantes :

- le *Stormshield Firmware* intégré dans l'*appliance STORMSHIELD*, réalisant le filtrage et le chiffrement ;
- le *Stormshield Web Manager* : logiciel permettant l'administration et la surveillance des *appliances*, et l'analyse des logs ;
- les connexions sécurisées entre l'*appliance*, le *Stormshield Web Manager*, le *Stormshield Management Center* et le serveur de log.

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. 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 réseau basée sur le moteur ASQ (*Active Security Qualification*) ;
- 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.

1.2.3. Architecture

Le produit est un package s'exécutant dans l'une des *appliances* listées en section 1.1. Ce dernier est composé des sous-systèmes suivants :

- ASQ en charge de l'application de la politique de filtrage des flux d'information et de leur analyse ;
- IPSEC en charge de l'application de la politique de chiffrement. Il 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 ;
- SERVERD le serveur d'administration, qui permet la configuration de l'IPS-Firewall et la consultation des journaux d'audit ;
- SLD le serveur web permettant l'administration de l'IPS-Firewall par l'intermédiaire d'une interface d'administration Web. Ce serveur web pour ces tâches d'administration se connecte au serveur d'administration SERVERD ;
- CAD le client d'administration vers SMC ;
- 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 ;

- IKE en charge de la négociation des associations de sécurité en vue de l'application de la politique de chiffrement ;
- LDAP est composé d'une base de données de type annuaire LDAP contenant l'ensemble des informations relatives aux utilisateurs ;
- LOGD en charge de la génération et de la consultation des traces générées par l'ensemble des autres sous-systèmes ;
- CRYPTO en charge de fournir les fonctions cryptographiques aux différents sous-systèmes.

1.2.4. 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 l'utilisateur connecté, la version de la TOE est indiquée en haut de la fenêtre d'administration ;
- en ligne de commande : une fois l'utilisateur connecté, la version est inscrite dans la bannière d'accueil.

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 *STORMSHIELD* 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.

L'évaluation du cycle de vie a porté sur le développement et le déploiement du produit, réalisés sur les sites suivants :

STORMSHIELD

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

STORMSHIELD

22 rue du Gouverneur Général Eboué
Immeuble Axium Bât. D – 2ème étage
92130 Issy-les-Moulineaux
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 », il a tous les droits et décide pour les autres administrateurs de leur octroyer un accès l'interface web de SMC et à l'interface web des firewalls. Il 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

Le certificat porte sur la configuration décrite dans le chapitre 2.3.1 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 ;
- le module de routage statique multicast ;
- l'infrastructure à clés publiques (PKI) interne ;
- le module VPN SSL (*Portal* and *Tunnel*) ;
- le cache DNS ;
- le moteur antivirus (*CLAMAV* ou *KASPERSKY*) ;
- le module Active Update ;
- les services SSH, DHCP, MPD et SNMPD ;
- le client DHCP ;
- le relai DHCP ;
- le *WiFi* pour les *appliances* équipées ;
- la géolocalisation et réputation IP/Host ;
- le contournement des capacités (« *bypass capabilities* ») pour le SNi40 ;
- toute règle IPS personnalisée ;
- les objets FQDN (nécessite un service DNS externe) ;
- les messages IPFIX.

Les tests ont été effectués sur les *appliances* SN210, SN510, SN910 et SN3000. Ces produits ont été jugés représentatifs de la gamme de produits. Ce certificat porte donc sur l'ensemble des boîtiers identifiés au paragraphe 1.1.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision5** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 février 2020, 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 incluant une expertise de l'implémentation [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 des générateurs d'aléas. Cette analyse n'a pas permis de mettre en évidence de biais statistiques. 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.

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 produit « Stormshield Network Security UTM / NG-Firewall Software Suite, 3.7.9» 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_CMS.4, ALC_CMC.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 :

- le mode de distribution des certificats est manuel (importation) ;
- les CRL doivent être régulièrement téléchargées depuis un serveur de CRL :
- le mode d'utilisation soumis à l'évaluation exclut le fait que la TOE s'appuie sur d'autres services tels que PKI, serveur DNS, DHCP, proxy. Les modules listés en 1.2.6 que Stormshield Network fournit en option pour la prise en charge de ces services sont désactivés par défaut et doivent le rester dans le cadre de la mise en œuvre de la configuration certifiée ;
- bien que supportée, la fonctionnalité IPv6 est désactivée par défaut et doit le rester dans le cadre de la mise en œuvre de la configuration certifiée ;
- les administrateurs et les utilisateurs IPSec sont gérés par l'annuaire LDAP interne. Des clients LDAP externes au boîtier *appliance firewall*-VPN ne doivent pas se connecter à cette base ;
- la possibilité offerte par la politique de filtrage d'associer à chaque règle de filtrage une inspection applicative (proxy HTTP, SMTP, POP3, FTP) et une programmation horaire ne doivent pas être utilisées ;
- l'option proposée par la politique de filtrage d'associer l'action « déchiffrer » (proxy SSL) à une règle de filtrage ne doit pas être employée.

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 lorsque les dépendances CC sont satisfaites. 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 EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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**	Authorisation controls
	ALC_CMS	1	2	3	4	5	5	5	**4**	Implementation representation 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 : - Stormshield Network Security UTM / NG-Firewall Software Suite Version 3 – EAL3+ Security Target, référence SN_ASE_sectarget_v3, version 3.9.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report Project: COEOS, référence D:\CESTI\CC\COEOS\RTE, version 1.0.
[EXP-CRY]	Qualification COEOS Expertise cryptographique, référence OPPIDA/CESTI/COEOS/CRYPTO/3.2, version 3.2.
[CONF]	Liste de configuration du produit : - SN_ALC_fournitures, version 3.7.
[GUIDES]	Guide d'installation du produit : - Guide Stormshield Management Center Présentation et Installation produits 2018, version 1.0, référence sns-fr-GammeSN_guide_installation-2018. - Guide Stormshield Management Center Guide d'installation, version 2.5, référence sns-fr-SMC-guide_d_installation-v2.5. Guide utilisation et de configuration du produit : - Guide Stormshield Network Security Manuel d'utilisation et de configuration, version 3, référence sns-fr-manuel_d'utilisation_et_de_configuration-v3. Guide d'administration du produit : - Guide Stormshield Management Center Guide d'administration, version 2.5, référence sns-fr-SMC-guide_d_administration-v2.5.

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
[NOTE 21]	Note d'application méthodologie pour l'évaluation d'une gamme de produits, version 1.0 du 1er février 2017, ANSSI.