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-CSPN-2018/22

ForcePoint Stonesoft Next Generation Firewall Version 5.10.14 build 14126 sur *appliance* NGF-325 avec SMC 6.2.5 build 10363

Paris, le 15 novembre 2018

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

Guillaume POUPARD
[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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2018/22**
Nom du produit **ForcePoint Stonesoft Next Generation Firewall**
Référence/version du produit **Forcepoint NGFW, Version 5.10.14 build 14126 sur *appliance* NGF-325 avec SMC 6.2.5 build 10363**
Catégorie de produit **Pare-feu**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Forcepoint** **9/11 Allée de l'Arche** **Courbevoie Cedex** **Paris La Défense 92671**
Développeur **Forcepoint** **9/11 Allée de l'Arche** **Courbevoie Cedex** **Paris La Défense 92671**
Centre d'évaluation **Amossys** **4 bis allée du bâtiment,** **35000 Rennes, France**
Fonctions de sécurité évaluées **Analyse du trafic** **Journalisation** **Contrôle d'accès** **Sécurisation des flux entre SMC et Pare-feu** **Mises à jour sécurisées**
Fonction(s) de sécurité non évaluées **Sans objet**
Restriction(s) d'usage **Oui (cf. §3.2)**

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 CSPN 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 « ForcePoint Stonesoft Next Generation Firewall, version 5.10.14 build *14126* sur appliance NGF-325 avec SMC 6.2.5 build 10363 » développé par *FORCEPOINT*.

Ce produit est un pare-feu. Il est déployé sous forme d'*appliance*, et communique avec un module d'administration *Stonesoft Management Center* (SMC).
Le produit permet principalement l'analyse et le filtrage du trafic de réseaux d'entreprise. Il inclut d'autres fonctionnalités de sécurité additionnelles, qui sont désactivées dans la version évaluée.
La figure 1 explicite l'architecture du produit.

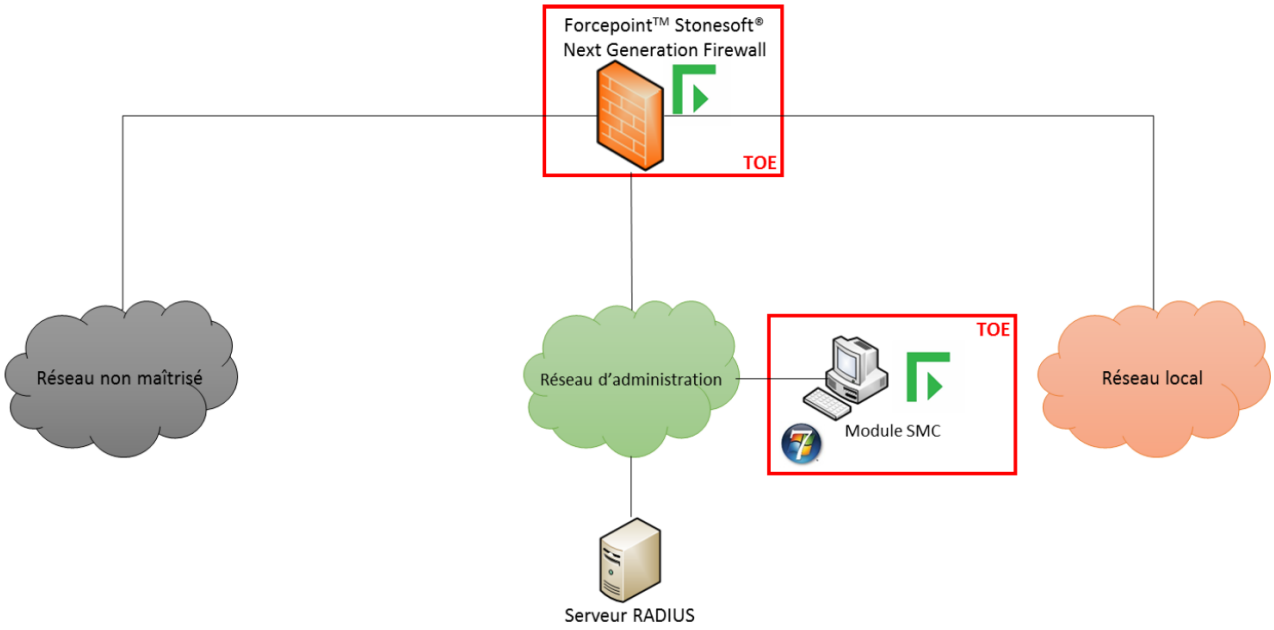

Figure 1 - Architecture Produit.

1.2. Description du produit évalué

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

1.2.1. Catégorie du produit

☐ 1 – détection d'intrusions
☐ 2 – anti-virus, protection contre les codes malicieux
☒ **3 – pare-feu**
☐ 4 – effacement de données
☐ 5 – administration et supervision de la sécurité
☐ 6 – identification, authentification et contrôle d'accès
☐ 7 – communication sécurisée
☐ 8 – messagerie sécurisée
☐ **9 – stockage sécurisé**
☐ 10 – environnement d'exécution sécurisé
☐ 11 – terminal de réception numérique (*Set top box*, STB)
☐ 12 – matériel et logiciel embarqué
☐ 13 – automate programmable industriel
☐ 99 – autre

1.2.2. Identification du produit

Nom du produit	ForcePoint Stonesoft Next Generation Firewall
Numéro de la version évaluée	5.10.14 build 14126 sur appliance NGF-325 avec SMC 6.2.5 build 10363

La version certifiée du produit peut être identifiée de la manière suivante :

- la version d'*appliance* (NGF-325) peut être vérifiée en regardant l'étiquette située sous l'*appliance* ;
- la version du pare-feu (5.10.14 build 14126) peut être récupérée au niveau du SMC, en cliquant sur un pare-feu détecté et en se reportant à la fenêtre « Info », comme montré sur la Figure 2 ;
- la version du SMC (6.2.5 build 10363) peut être récupérée lors du démarrage du client SMC, comme montré sur la Figure 3.

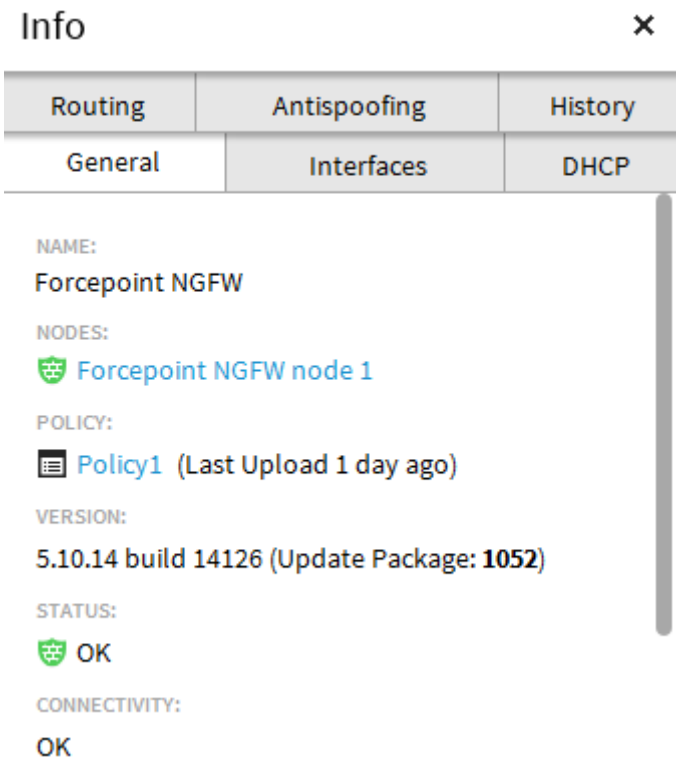

Figure 2 – Identification de la version du pare-feu.

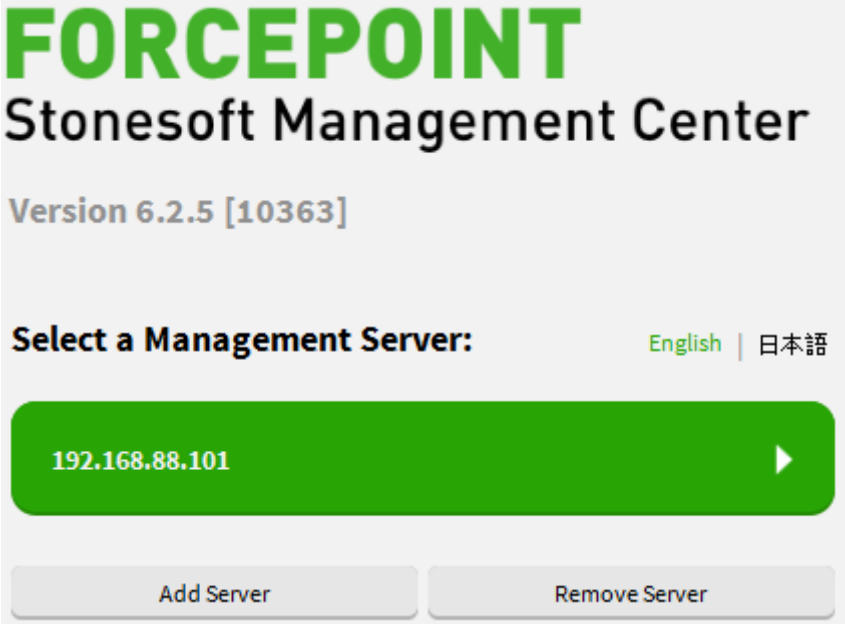

Figure 3 – Identification de la version du SMC

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :
- l'analyse du trafic ;
- la journalisation ;
- le contrôle d'accès ;
- la sécurisation des flux entre SMC et pare-feu ;
- les mises à jour sécurisées.

1.2.4. Configuration évaluée

La configuration évaluée est la version déployée sur *appliance* NGF-325.
Le présent rapport n'est *pas* applicable aux autres *appliances* embarquant le même logiciel :
- NGF-110 et NGF- 115 (débit inspection maximum : 400 Mbps) ;
- NGF-321 (débit inspection maximum : 700 Mbps) ;
- NGF-1035 (débit inspection maximum : 1 Gbps) ;
- NGF-1065 (débit inspection maximum : 3 Gbps) ;
- NGF-1401 (débit inspection maximum : 8 Gbps) ;
- NGF-1402 (débit inspection maximum : 14 Gbps) ;
- NGF-3207, NGF-3301, NGF-3305 et NGF-5206 (débit inspection maximum : 30 Gbps).

La plateforme de test est constituée des éléments suivants :
- le pare-feu sur *appliance* NGF-325 ;
- un poste Windows 7 contenant la partie serveur ainsi que la partie client du SMC, et un serveur de journalisation ;
- un poste Windows Server 2012 contenant un serveur RADIUS pour l'authentification des utilisateurs du SMC ;
- deux postes Kali Linux jouant le rôle d'attaquants sur le réseau local et le réseau d'administration ;
- un poste d'observation Kali Linux positionné entre le pare-feu et le routeur afin d'observer les communications réseau.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Le poste sur lequel le SMC est installé est configuré de la manière suivante :

- la partie serveur du SMC gère les communications avec le pare-feu ;
- un serveur de journalisation (LogServer) reçoit les évènements en provenance du pare-feu ;
- la partie client du SMC permet de visualiser les journaux du LogServer et permet également de se connecter à la partie serveur du SMC.

2.3.1.2. Description de l'installation et des non-conformités éventuelles

Le pare-feu a été directement livré sous forme d'*appliance*. Son installation n'a donc consisté qu'à relier les réseaux utilisés pour l'évaluation au boîtier.
Le développeur est ensuite venu dans les locaux de l'évaluateur afin de mettre à jour le *firmware* du pare-feu (et installer la version visée par cette évaluation).
Le SMC a été installé directement par l'évaluateur, à l'aide d'un programme fourni par le développeur.

2.3.1.3. Durée de l'installation

L'installation a duré une journée.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit. Il est tout de même présupposé que les utilisateurs soient familiarisés avec l'administration d'un pare-feu.

2.3.3. Revue du code source (facultative)

L'évaluation n'a pas fait l'objet d'une revue de code source, à l'exception des vérifications relatives à l'implémentation des mécanismes cryptographiques et aux générateurs d'aléas (voir paragraphes 2.4 et 2.5).

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur les dépendances logicielles du produit. Cependant aucune d'entre elles n'est exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.7. Accès aux développeurs

Le centre d'évaluation a eu accès aux développeurs pour répondre à des questions relatives à l'utilisation de la TOE.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Conformément aux [GUIDES] fournis, l'administrateur du produit devra mettre en œuvre les mesures suivantes :

- désactiver la suite TLS_RSA_WITH_AES_128_CBC_SHA256 ;

– modifier la politique de sécurité relative aux mots de passe afin de la mettre en cohérence avec les exigences de l'ANSSI [MDP].

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

2.3.8.3. Avis d'expert sur la facilité d'emploi

L'évaluateur n'a pas identifié de cas où le produit peut être configuré ou utilisé d'une manière non sécurisée.

2.3.8.4. Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité ou de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Les générateurs aléatoires du produit ont été analysés. Cette analyse n'a pas identifié de non-conformité ou de vulnérabilité exploitable.

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.

Ce certificat atteste que le produit « ForcePoint Stonesoft Next Generation Firewall, version 5.10.14 build *14126* sur appliance NGF-325 avec SMC 6.2.5 build 10363 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

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 spécifiés dans la cible de sécurité [CDS], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN - ForcepointTM Stonesoft® Next Generation Firewall* Référence : CSPN-ST-Forcepoint-NGFW ; Version : *1.04* ; Date : *26 Février 2018*
[RTE]	*Rapport Technique d'Évaluation CSPN - Produit Forcepoint NGFW - version 5.10.14* Référence : CSPN-RTE-Forcepoint-NGFW ; Version : 1.02 ; Date : *11 Octobre 2018*
[ANA-CRY]	*Expertise des mécanismes cryptographiques - Produit Forcepoint NGFW - version 5.10.14* Référence : CSPN-CRY-Forcepoint-NGFW ; Version : 1.02 ; Date : *20 Septembre 2018*
[GUIDES]	*Guide de référence* Référence : *ngfw_620_rg_smc-api_a_en-us* ; Version : *6.2 Révision A* ; Date : *2017* *Guide d'installation* Référence : *ngfw_620_ig_c_en-us* ; Version : *6.2 Révision C* ; Date : *2018* *Guide produit.* Référence : *ngfw_620_pg_b_en-us* ; Version : *version 6.2 Révision B* ; Date : *2018*

Annexe 2. Références 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.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr.
[MDP]	Note technique – Recommandations de sécurité relatives aux mots de passe, 5 juin 2012, ANSSI. https://www.ssi.gouv.fr/administration/guide/mot-de-passe/