

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité
des systèmes d'information

Bureau Qualifications et Agréments

Paris, le 27 DEC. 2018
N°8150 /ANSSI/SDE/PSS/BQA

**DECISION DE QUALIFICATION D'UN PRODUIT
AU NIVEAU ELEMENTAIRE**

***STONESOFT NGFW v.5.10.14 (build 14126) sur APPLIANCE NGF-325
avec le STONESOFT MANAGEMENT CENTER (SMC) v.6.2.5 (build 10363)***

***FORCEPOINT FRANCE
9/11, allée de l'Arche
92 671 COURBEVOIE Cedex***

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit.

Fiche 2 : Conditions, restrictions et limites de la qualification.

Fiche 3 : Base documentaire de la qualification.

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

Vu l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment son article 9 ;

Vu le décret n°2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », notamment son article 1^{er} ;

Vu le décret du 27 mars 2014 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Vu l'arrêté du 13 juin 2017 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques ;

Vu le *Processus de qualification d'un produit*,

Décide :

Art. 1 – Le produit fourni par la société *FORCEPOINT* portant le nom *STONESOFT NGFW v5.10.14 (build 14126) sur APPLIANCE NGF-325 avec le STONESOFT MANAGEMENT CENTER (SMC) v.6.2.5 (build 10363)*, respecte les règles fixées par le décret n° 2010-

112 du 2 février 2010 et est qualifié au niveau élémentaire sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.

Art. 2 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.

Art. 3 – La présente décision est valable pour une durée de trois ans.



Guillaume POUPARD
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information

Fiche 1

Description du produit

Désignation et versions

Le produit évalué est le *STONESOFT NGFW v5.10.14 (build 14126) sur APPLIANCE NGF-325 avec le STONESOFT MANAGEMENT CENTER (SMC) v.6.2.5 (build 10363)* développé par *FORCEPOINT*.

Ce produit est un pare-feu. Il est déployé sous forme d'*appliance*, et communique avec son module d'administration *STONESOFT MANAGEMENT CENTER (SMC)*.

Le produit permet principalement l'analyse et le filtrage du trafic de réseaux d'entreprise. Il inclut des fonctionnalités de sécurité additionnelles, qui sont désactivées dans la version évaluée.

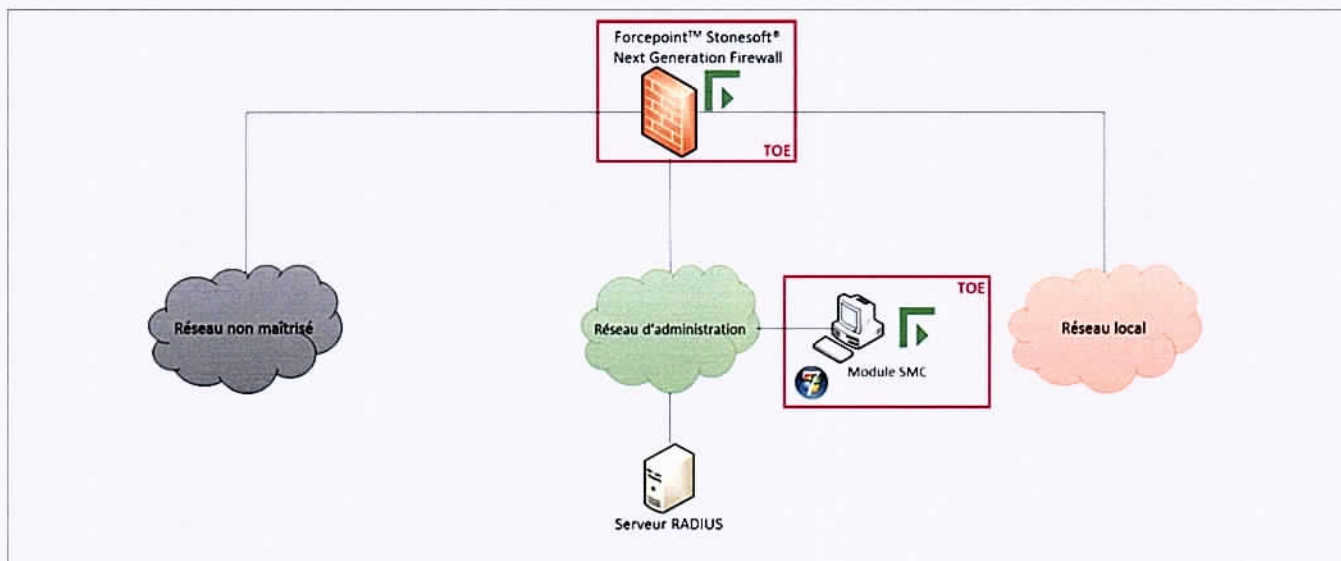


Figure 1. Cas d'usage classique du produit

Présentation générale

Les fonctions de sécurité évaluées uniquement sur la plateforme *NGF-325* 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.

Fiche 2

Conditions et limites de la qualification

Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que :

C1. H.PERSONNEL

Le pare-feu est administré par du personnel compétent, non hostile et correctement formé à son utilisation, respectant les guides et procédures. Cette condition concerne les rôles « Administrateur » et « Superviseur ».

C2. H.SERVICES_ADDITIONNELS

Seule la fonction de pare-feu est activée, tous les autres services (en particulier l'inspection en profondeur des flux ainsi que les services additionnels tels que VPN, antivirus, anti-spam, analyse des fichiers suspectés comme malveillants dans le *cloud*, etc.) étant désactivés.

C3. H.COUPURE

Les plateformes sont installées conformément à la politique d'interconnexion des réseaux en vigueur et sont les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de filtrage. De même, les plateformes déployées sont liées au dimensionnement du système et des flux à surveiller.

Les informations relatives au dimensionnement sont accessibles depuis la fiche technique suivante :

https://www.forcepoint.com/sites/default/files/resources/files/datasheet_next_gen_firewall_appliances_specs_en_0.pdf

C4. H.LOCAL_SÉCURISÉ

La plateforme est déployée dans un local dont les accès sont nominativement contrôlés.

C5. H.RÉSEAU_ADMIN_DÉDIÉ

L'administration et la supervision de la plateforme (*via* le module SMC) sont effectuées à partir d'un réseau séparé et dédié.

C6. H.SOURCE_HORAIRE

L'environnement informatique intègre une source de signaux horaires sécurisée permettant la datation des enregistrements d'audit. Le serveur de management centralisé fournit l'heure par le canal de management et se met à jour suivant la configuration choisie (le protocole NTP est le plus souvent utilisé).

C7. Conformément aux [GUIDES] fournis, l'administrateur du produit met en œuvre les mesures suivantes :

C7.a. désactiver la suite TLS_RSA_WITH_AES_128_CBC_SHA256 ;

C7.b. modifier la politique de sécurité relative aux mots de passe afin de la mettre en cohérence avec les exigences de l'ANSSI [MDP].

Limites

- L1.** La présente qualification ne s'applique qu'à la plateforme *NGF-325*, et n'est pas applicable aux plateformes suivantes :
- *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).
- L2.** L'actuelle version utilise des logiciels tierce partie (*POSTGRES*, *JAVA* ou *BOUNCYCASTLE*) intégrés au produit. Il est nécessaire que le développeur suive les impacts sur la sécurité du produit des éventuelles vulnérabilités les affectant et les prenne en compte pour la maintenance de qualification.

Fiche 3

Base documentaire de la qualification

Cadre réglementaire

[PROCESS_QUALIF_PROD]	<i>Processus de qualification d'un produit</i> , version 1.0 du 6 janvier 2017. Disponible sur : http://www.ssi.gouv.fr .
-----------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------

Documents rédigés par le centre d'évaluation

[RTE]	<i>Rapport Technique d'Évaluation CSPN - Produit FORCEPOINT NGFW - version 5.10.14</i> Référence : CSPN-RTE-FORCEPOINT-NGFW ; Version : 1.02 ; Date : 11 Octobre 2018
-------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[CERTIF]	Rapport de certification, référence : ANSSI-CSPN-2018/22 en date du : 15/11/2018
[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/

Guides d'utilisation et documentations techniques de l'industriel

[GUIDES]	<i>Guide de référence</i> Référence : ngfw_620_rg_smc-api_a_en-us ; Version : 6.2 Révision A ; Date : 2017 <i>Guide d'installation</i> Référence : ngfw_620_ig_c_en-us ; Version : 6.2 Révision C ; Date : 2018 <i>Guide produit.</i> Référence : ngfw_620_pg_b_en-us ; Version : version 6.2 Révision B ; Date : 2018
[CdS]	<i>Cible de sécurité CSPN - FORCEPOINT™ STONESOFT® NEXT GENERATION FIREWALL</i> Référence : CSPN-ST-FORCEPOINT-NGFW ; Version : 1.04 ; Date : 26 Février 2018