Cible de sécurité CSPN

Forcepoint™ Stonesoft® Next Generation Firewall

Catégorie « Pare-feu »

Référence : CSPN-ST-Forcepoint-NGFW-1.04
Date : le 08/09/2017
Code interne : ISY001

Siège : 4 bis allée du Bâtiment ● 35000 Rennes ● France ● www.amossys.fr
SIRET : 493 348 890 00036 ● **NAF** : 6202 A ● RCS Rennes B 493 348 890 ● SAS au capital de 38.000 Euros

FICHE D'EVOLUTIONS

Révision	Date	Description	Rédacteur
1.00	15/09/2016	Version originale	Antoine COUTANT
1.01	21/11/2016	Ajout du module LogServer dans le périmètre d'évaluation	Antoine COUTANT
1.02	01/06/2017	Mise à jour suite aux commentaires de l'ANSSI	Antoine COUTANT Alexandre DELOUP
1.03	08/09/2017	Mise à jour suite aux discussions avec l'ANSSI	David BRILLANT Antoine COUTANT Alexandre DELOUP Eric GOUSSET
1.04	26/02/2017	Mise à jour suite aux remarques de l'ANSSI	Alexandre DELOUP

Ce document est validé par Forcepoint.

SOMMAIRE

1. INTRODUCTION 4
1.1. Objet du document 4
1.2. Identification du produit 4
1.3. Références 4

2. DESCRIPTION DU PRODUIT 6
2.1. Description générale 6
2.2. Principe de fonctionnement 8
2.3. Description des dépendances 9
2.4. Description de l'environnement technique de fonctionnement 9
2.5. Périmètre de l'évaluation 10

3. PROBLEMATIQUE DE SECURITE 13
3.1. Description des utilisateurs typiques 13
3.2. Description des biens sensibles 13
3.3. Description des hypothèses sur l'environnement 14
3.4. Description des menaces 16
3.5. Description des fonctions de sécurité 17
3.6. Matrices de couverture 19
3.6.1. Menaces et biens sensibles 19
3.6.2. Menaces et fonctions de sécurité 19

4. ANNEXES 21
4.1. Cas particulier de la couche virtuelle 21
4.2. Spécifications materielles 23

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN[1] promu par l'ANSSI[2], du produit « Forcepoint™ Stonesoft® Next Generation Firewall » développé par la société **Forcepoint**.

La cible d'évaluation correspond au déploiement du module *NGFW* (sous forme d'*appliance* physique) ainsi que de son module d'administration (*SMC*[3]).

Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation de **Forcepoint**. Les mises à jour de ce document sont effectuées par **AMOSSYS**.

1.2. IDENTIFICATION DU PRODUIT

Editeur	**Forcepoint** 9/11 Allée de l'Arche - Courbevoie Cedex Paris La Défense 92671 - FRANCE
Lien vers l'organisation	https://www.forcepoint.com/
Nom commercial du produit	Forcepoint™ Stonesoft® Next Generation Firewall
Numéro de la version évaluée	*Appliance* NGF-325 contenant la version logicielle 5.10.10 composée de : - module pare-feu (NGFW) version 5.10.10 - module d'administration (SMC) version 6.2.1
Catégorie du produit	Pare-feu

Tableau 1 - Identification du produit évalué

1.3. REFERENCES

Pour la rédaction de la cible de sécurité, les documents suivants ont été consultés :

- Datasheet ForcepointTM Stonesoft® Next Generation Firewall[4] ;
- Next Generation Firewall 6.2.0 Product Guide[5] ;
- Next Generation Firewall 6.2.0 Installation Guide[6].

L'aide en ligne est disponible sur les liens suivants :

- http://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.2.0/index.html
- http://help.stonesoft.com/onlinehelp/StoneGate/SMC/index.html.

[1] Certification de Sécurité de Premier Niveau
[2] Agence nationale de la sécurité des systèmes d'information
[3] Security Management Center
[4] https://www.forcepoint.com/sites/default/files/resources/files/datasheet_next_gen_firewall_en_0.pdf
[5] https://kc.mcafee.com/corporate/index?page=content&id=PD26463
[6] https://kc.mcafee.com/corporate/index?page=content&id=PD26464

Les spécifications matérielles des *appliances* sont disponibles sur le lien suivant :

- https://www.forcepoint.com/product/network-security/forcepoint-ngfw

Les systèmes d'exploitation supportés sont disponibles dans les *release note* sur le lien suivant (cf p. 3, chapitre "System Requirements / Operating Systems") :

- https://support.forcepoint.com/DocumentsDisplayed?version=5.10&name=Stonesoft%20Next%20Generation%20Firewall%20(NGFW)

2. DESCRIPTION DU PRODUIT

2.1. DESCRIPTION GENERALE

Forcepoint™ Stonesoft® Next Generation Firewall (*NGFW*) protège les réseaux d'entreprise grâce à des contrôles de sécurité ultraperformants qui s'appuient sur des renseignements et bénéficient de mises à jour en temps réel en provenance de l'écosystème McAfee Security Connected. Cette solution est ainsi en mesure de proposer la solution de prévention des contournements la plus performante du marché, combinée à des fonctionnalités complètes de pare-feu nouvelle génération.

La solution *NGFW* repose sur une analyse approfondie des paquets ainsi qu'une série de fonctions de protection comprenant notamment :

- un contrôle granulaire des applications qui permet d'analyser précisément certaines fonctions des applications (comme interdire l'envoi de pièces jointes dans les systèmes de messagerie instantanée) ;
- un système de prévention des intrusions (IPS[7]) ;
- la solution Forcepoint AMD[8] qui est une solution de type sandboxing avec analyse des fichiers suspectés comme malicieux dans le cloud ;
- un réseau privé virtuel (VPN[9]) intégré (tunnels site à site ou site à *endpoint* qui permettent d'interconnecter plusieurs sites distants ou postes mobiles).

À cette conception unifiée à la fois efficace, extensible et hautement évolutive, viennent s'ajouter de puissantes technologies de protection contre les contournements (AET[10]) capables de décoder et de normaliser le trafic réseau, avant inspection et sur toutes les couches de protocoles, afin de détecter et de bloquer les mécanismes d'attaque les plus avancés.

La figure suivante représente l'équipement dans ses différents environnements possibles (boîtier physique, image dans un hyperviseur de virtualisation, logiciel à installer sur une machine avec le système d'exploitation durci Forcepoint™ Stonesoft® Next Generation Firewall).

Le logiciel est identique quel que soit la plateforme utilisée. En effet, le même binaire peut être utilisé pour des déploiements virtuels, logiciels ou même physiques (quel que soit le modèle d'*appliance* fourni par **Forcepoint**). L'annexe de ce document traite de la couche virtuelle (non soumise à l'évaluation) et est donnée à titre informatif.

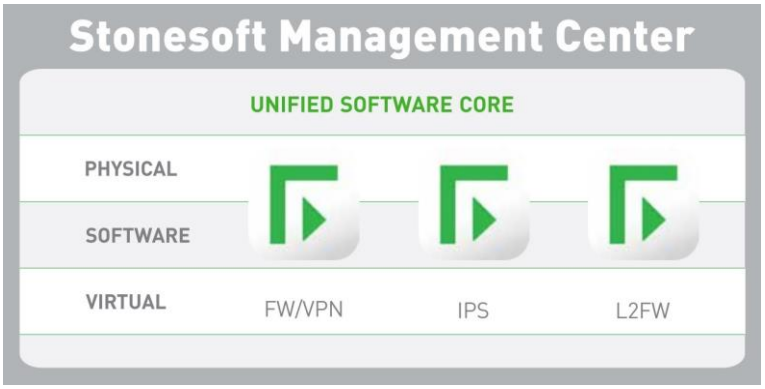

Figure 1 – Rôles fonctionnels

[7] Intrusion Prevention System
[8] Advanced Malware Detection
[9] Virtual Private Network
[10] Advanced Evasion Techniques

Le logiciel de base unifié (sur lequel se fonde Forcepoint™ Stonesoft® Next Generation Firewall) permet d'ajouter des fonctionnalités de sécurité et des capacités sans perturber un réseau. En effet, avec Forcepoint™ Stonesoft® Next Generation Firewall, une conception système unique exerce plusieurs rôles : pare-feu de la couche 2, pare-feu/VPN de la couche 3 et système IPS.

Le système à évaluer (la TOE[11]) sera constitué des deux composants principaux suivants :

- le pare-feu (*NGFW*) ;
- le module d'administration (*SMC*).

Les services additionnels (antivirus, antispam, analyse anti APT[12], etc.) ne font pas partie du périmètre d'évaluation et sont désactivés dans le cadre de l'évaluation.

[11] Target Of Evaluation
[12] Advanced Persistent Threat

2.2. PRINCIPE DE FONCTIONNEMENT

Globalement, le traitement d'un flux est représenté sur la figure suivante :

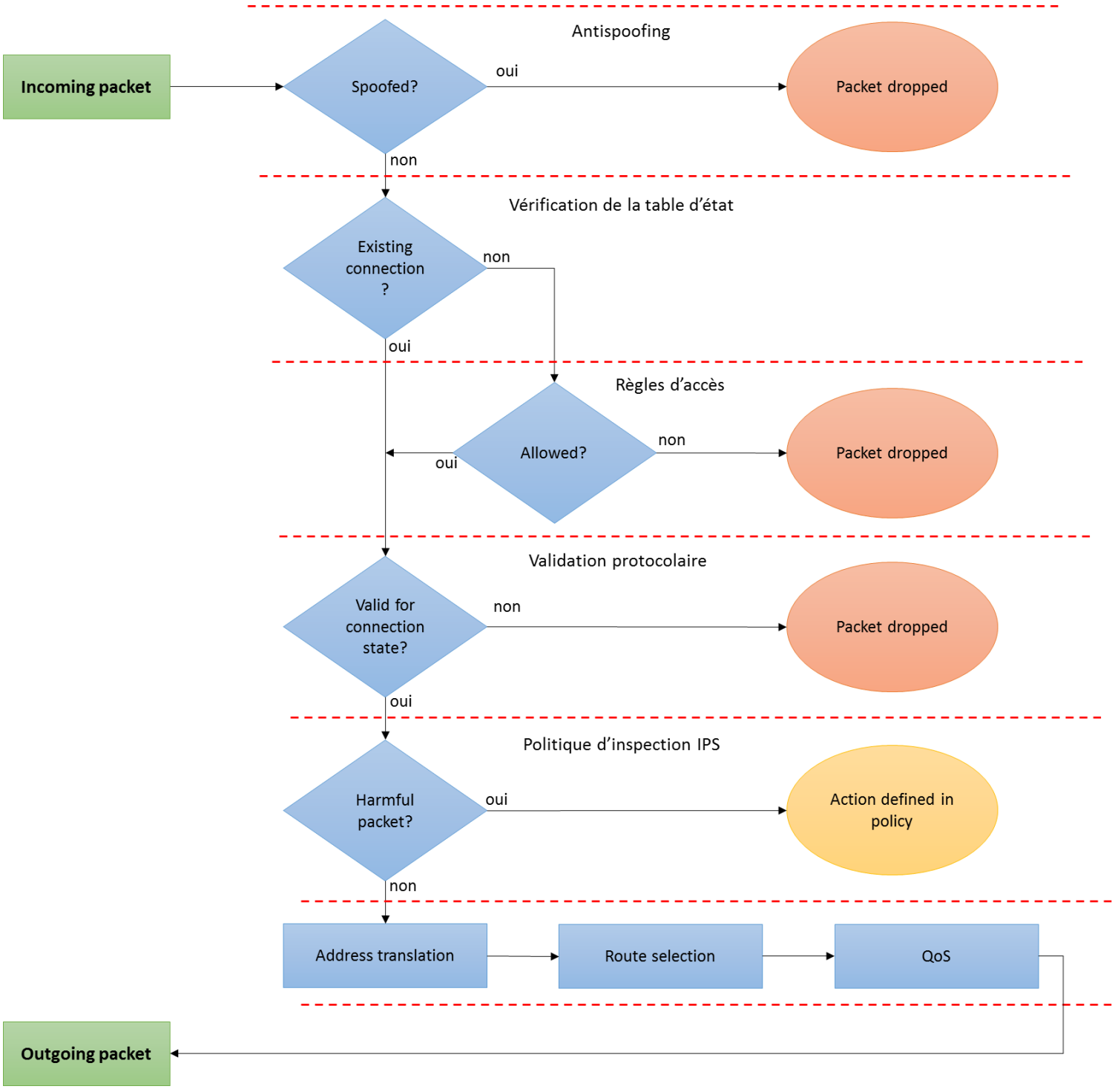

Figure 2 – Traitement d'un flux entrant

La fonction IPS sera désactivée dans le cadre de l'évaluation, puisqu'elle n'est pas utilisée par la fonctionnalité de pare-feu et ne remet ainsi pas en cause le fonctionnement du pare-feu.

2.3. DESCRIPTION DES DEPENDANCES

Forcepoint™ Stonesoft® Next Generation Firewall est une *appliance* dédiée, il n'y a donc aucune dépendance car elle est livrée préconfigurée avec les éléments nécessaires à son fonctionnement.

Seul le module SMC doit être installé sur un poste dédié.

2.4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

Le module d'administration (*SMC*) peut être installé sur les systèmes et versions d'exploitation suivants :

- Windows Server 2016 Standard and Datacenter editions
- Windows Server 2012 R2
- Windows Server 2008 R1 SP2 and R2 SP1
- Windows 7 SP1
- Windows 10
- CentOS 6
- CentOS 7
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- SUSE Linux Enterprise 11 SP3
- SUSE Linux Enterprise 12 SP1
- Ubuntu 14.04 LTS
- Ubuntu 16.04 LTS

Le support des systèmes d'exploitation récents est documenté dans toutes les nouvelles *release note* associée à une nouvelle version du NGFW.

Les équipements Forcepoint™ Stonesoft® Next Generation Firewall sont disponibles sous forme d'*appliances* dimensionnées selon leurs capacités de traitement :

- NGF-110 (débit inspection maximum : 400 Mbps)
- NGF 115 (débit inspection maximum : 400 Mbps)
- NGF-321 (débit inspection maximum : 700 Mbps)
- NGF-325 (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 (débit inspection maximum : 30 Gbps)

- NGF-3301 (débit inspection maximum : 30 Gbps)
- NGF-3305 (débit inspection maximum : 30 Gbps)
- NGF-5206 (débit inspection maximum : 30 Gbps)

L'administration des appliances se fait par un canal chiffré TLS 1.2 (AES256 ou AES128) et les boîtiers sont authentifiés par certificat (autorité de certification en ECDSA ou RSA). Le canal de communication le plus robuste (256 bits) est proposé par défaut lors de l'installation et est décrit au chapitre « Setting up » de la documentation en ligne[13].

2.5. PERIMETRE DE L'EVALUATION

L'*appliance* est livrée avec son propre système d'exploitation basé sur un système linux durci par les services R&D de **Forcepoint** ainsi que de modules nécessaires au fonctionnement de la solution. Le noyau linux (et les modules du noyau) est un système personnalisé minimaliste couvrant uniquement les besoins du NGFW. Plus précisément, les modules provenant directement de Debian sont les outils OS basiques tels que les commandes shell : ls, netstat, tcpdump, etc… ; le système de fichiers est personnalisé en lecture seule. De ce fait, le système d'exploitation est sécurisé par son design. Pour l'évaluation CSPN, **seul le modèle NGF-325 sera utilisé**[14]. Ses capacités fonctionnelles sont strictement identiques aux autres références citées précédemment.

Pour le SMC, l'installation sous Windows 7 SP1 (64 bits) est retenue. Ce poste dédié fera également office de serveur de journalisation (service LogServer).

[13] http://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.0.1/index.html#GUID-1787B5A9-C521-4FF6-AA5E-050C3CB7289B.html

[14] Ce modèle a été choisi pour sa représentativité des produits de Forcepoint.

La figure ci-dessous présente la plateforme d'évaluation CSPN (l'encadré rouge représente la cible d'évaluation) :

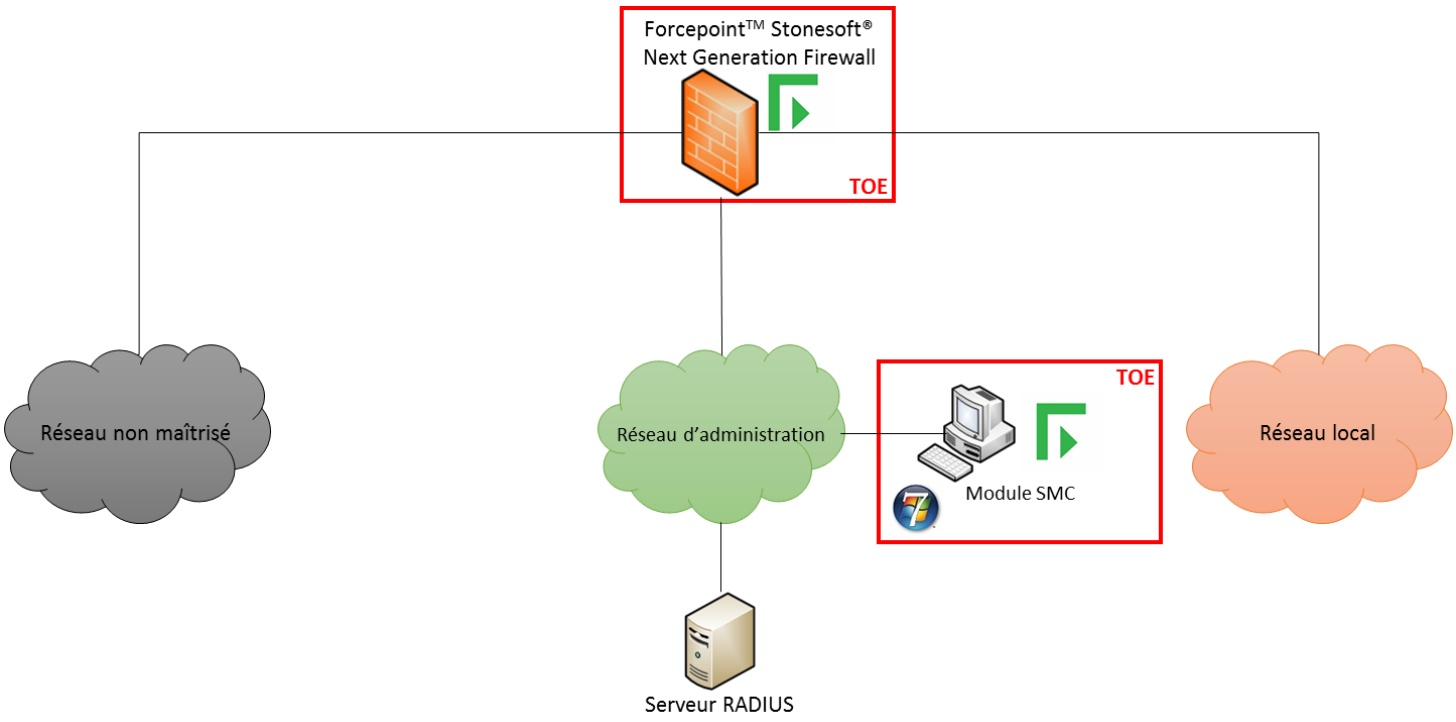

Figure 3 - Plateforme d'évaluation

La TOE (Forcepoint™ Stonesoft® Next Generation Firewall et le module SMC associé) est identifiée par des encadrés rouges. Trois réseaux sont présents :

- réseau non maitrisé : réseau non maitrisé par les administrateurs (Internet par exemple) ;
- réseau local : réseau protégé par Forcepoint™ Stonesoft® Next Generation Firewall, il contient les services que le pare-feu isole ;
- réseau d'administration : réseau où est situé le module SMC d'où les administrateurs peuvent gérer le pare-feu Forcepoint™ Stonesoft® Next Generation Firewall ainsi que le serveur RADIUS.

La séparation entre le réseau d'administration et le réseau opérationnel est choisie au moment de l'installation. Le réseau d'administration peut être cloisonné à une interface spécifique, un VLAN ou sur une interface de production. **Forcepoint** recommande une allocation d'interface spécifique pour le réseau d'administration (nominal et *backup*). Cette installation des différents réseaux est à réaliser par le client final au moment de l'installation de l'équipement.

Chacun de ces réseaux est susceptible de contenir un attaquant.

La TOE se compose des éléments suivants :

- ***L'Appliance Forcepoint NGFW*** dont le rôle est d'appliquer les règles de sécurité et dont la configuration évaluée est la suivante :
  - activation du suivi des connexions ;
  - politique de stockage des journaux paramétrée ;
  - désactivation de l'accès à l'interface en ligne de commande du moteur de pare-feu à partir du système d'exploitation, comme indiqué dans la documentation d'installation ;
  - désactivation des fonctionnalités VPN ainsi que des agents ou composants IPS associés à tous les protocoles ;
  - pas d'utilisation dans les règles de filtrage de l'option d'authentification des utilisateurs auprès du pare-feu (nécessite d'utiliser des VPN ou une authentification par telnet).

- **Le module d'administration *SMC*** qui est en charge de l'administration du pare-feu, de la collecte et la visualisation des journaux ainsi que de la supervision, la génération de rapports et alertes), est composée de :
  - un serveur d'administration ;
  - un serveur de journalisation et d'horodatage ;
  - une interface graphique.

Un serveur RADIUS utilisé pour l'authentification est également présent sur le réseau d'administration, mais est hors du périmètre de l'évaluation.

Le module d'administration (SMC) peut s'appuyer sur le serveur Radius pour authentifier les administrateurs. Les droits affectés aux administrateurs sont configurés directement sur le SMC de manière granulaire et par l'administrateur (tant pour les comptes locaux que Radius).

3.PROBLEMATIQUE DE SECURITE

3.1. DESCRIPTION DES UTILISATEURS TYPIQUES

Par définition, les utilisateurs sont les personnes et services applicatifs qui interagissent avec le produit évalué. Les rôles suivants sont pris en considération dans le cadre de l'évaluation :

- **Administrateur :** utilisateur disposant de tous les privilèges sur ForcepointTM Stonesoft® Next Generation Firewall. Il est donc en mesure de réaliser toutes les opérations de gestion, de maintenance et d'analyse des fonctions ;
- **Superviseur** : utilisateur autorisé à créer, modifier et mettre en œuvre des politiques et des règles de filtrage sur ForcepointTM Stonesoft® Next Generation Firewall ;
- **Exploitant** : utilisateur autorisé à gérer les statuts de Forcepoint™ Stonesoft® Next Generation Firewall, les événements de sécurité, les rapports d'audit.

Ces rôles utilisent le module SMC pour se connecter sur le Forcepoint™ Stonesoft® Next Generation Firewall. La description des rôles est disponible dans le chapitre 20 « Administrator Accounts » du document Stonesoft Next Generation Firewall 6.0 Product Guide.

Dans le cadre de l'évaluation les **postes utilisateurs**, dont les flux sont filtrés par la TOE, sont également considérés comme utilisateurs du produit, puisqu'ils interagissent avec le produit.

3.2. DESCRIPTION DES BIENS SENSIBLES

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon des critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité, confidentialité et authenticité.

Forcepoint™ Stonesoft® Next Generation Firewall contribue à protéger les biens sensibles suivants du système surveillé, sous réserve d'une politique de contrôle des flux correctement définie et réalisable mise en œuvre au niveau du système d'information dans sa globalité.

Un seul bloc fonctionnel participe au processus de filtrage et constitue donc un bien sensible :

- **B.FILTRAGE** : fonctionnalité de filtrage des flux.

  Besoin de sécurité : disponibilité.

Les biens protégés par le pare-feu Forcepoint™ Stonesoft® Next Generation Firewall sont les suivants :

- **B.SERVICES** : services proposés par les postes du (des) réseau(x) de confiance, les logiciels en écoute et leur configuration.

  Besoin de sécurité : disponibilité, intégrité, confidentialité.

- **B.TOPOLOGIE** : les informations de topologie du (des) réseau(x) de confiance.

  Besoin de sécurité : confidentialité.

D'autres biens sensibles, propres à Forcepoint™ Stonesoft® Next Generation Firewall, doivent également être considérés :

- **B.DONNÉES_CONFIGURATION** : ensemble des données d'identification et d'authentification des utilisateurs de Forcepoint™ Stonesoft® Next Generation Firewall ainsi que la gestion de leurs droits d'accès et les règles de filtrage de l'*appliance*.

Besoin de sécurité : disponibilité, intégrité, confidentialité.

- **B.JOURNAUX** : ensemble des traces générées par l'*appliance* et transmises au serveur de journalisation (service LogServer inclus dans le module SMC). Ces traces concernent la gestion de l'*appliance* (authentification des utilisateurs, actions d'administration ou de supervision) ainsi que les traces générées par le filtrage.

  Les communications entre *l'appliance* et le serveur de journalisation sont protégées en confidentialité et en intégrité par la mise en œuvre d'un chiffrement avec par défaut des clés de 256 bits en TLS 1.2 (TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384).

  Il est possible de désactiver le mode 256 bits et de redescendre en 128 bits en TLS 1.2 (TLS_RSA_WITH_AES_128_CBC_SHA) par configuration.

  Enfin, *l'appliance* et le serveur de journalisation s'authentifient mutuellement par certificat (autorité de certification interne en ECDSA par défaut ou RSA).

  Besoin de sécurité : intégrité, confidentialité, authenticité, disponibilité

- **B.FLUX_ADMINISTRATION** : flux d'administration de l'*appliance* à partir du module SMC installé sur le poste dédié, ainsi que les communications entre l'*appliance* et le serveur externe RADIUS.

  Besoin de sécurité : disponibilité, intégrité, confidentialité.

- **B.MISES_A_JOUR :** mises à jour du logiciel contenu dans Forcepoint™ Stonesoft® Next Generation Firewall.

  Besoin de sécurité : intégrité, authenticité.

- **B.ÉLÉMENTS_CRYPTO** : environnement de la TOE (Forcepoint™ Stonesoft® Next Generation Firewall et le module SMC) contenant un ensemble d'éléments cryptographiques servant notamment à sécuriser les communications liées aux opérations d'administration. Le module d'administration SMC contient une autorité de certification ECDSA signant des certificats pour chacun des pare feux associés : ces certificats permettent de chiffrer les communications liées aux opérations d'administration en AES-256 et intégrité SHA-512.

  Hors périmètre d'évaluation : il est possible d'installer une nouvelle AC sur le module SMC pour l'utiliser avec les *appliances*, auquel cas il est nécessaire de déployer de nouveaux certificats sur tous les équipements Forcepoint déployés sur le parc et administrés par ce module SMC. Dans ce dernier cas, le poste d'administration support du module SMC doit être déconnecté de tous les réseaux autres que le réseau d'administration.

  Besoin de sécurité : disponibilité, intégrité, confidentialité.

3.3. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement. Les hypothèses sur l'environnement de la TOE sont les suivantes :

- **H.PERSONNEL**

  La TOE est administrée par du personnel compétent, non hostile et correctement formé à son utilisation, respectant les guides et procédures. Cette hypothèse concerne les rôles « Administrateur » et « Superviseur ».

Hypothèse présentée au chapitre 20 du document "Stonesoft Next Generation Firewall 6.0 Product Guide".

- **H.SERVICES_ADDITIONNELS**

  Seule la fonction de pare-feu est activée, tous les autres services sont donc désactivés. Cette hypothèse concerne notamment la désactivation de l'inspection en profondeur ainsi que des services additionnels tels que VPN, antivirus, antispam, analyse des fichiers suspectés comme malveillants dans le cloud, etc.

  Hypothèse présentée au chapitre 49 du document "Stonesoft Next Generation Firewall 6.0 Product Guide" et notamment la section "Defining Access rule Action options".

- **H.COUPURE**

  Les *appliances* 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 *appliances* déployées sont liées au dimensionnement du système et des flux à surveiller. L'évaluation porte sur le déploiement d'un seul équipement (aucune redondance n'est testée).

  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

- **H.LOCAL_SÉCURISÉ**

  L'*appliance* est déployée dans un local dont les accès sont nominativement contrôlés.

  Hypothèse présentée au chapitre 4 du document "Stonesoft Next Generation Firewall 6.0 Product Guide".

- **H.RÉSEAU_ADMIN_DÉDIÉ**

  L'administration et la supervision de l'*appliance* (via le module SMC) est effectuée à partir d'un réseau séparé et dédié.

  Hypothèse présentée au chapitre 4 du document "Stonesoft Next Generation Firewall 6.0 Product Guide".

- **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).

  Dans le cadre de l'évaluation, la source horaire est fournie par la station d'administration hébergeant le module SMC.

  Hypothèse présentée au chapitre 26 du document "Stonesoft Next Generation Firewall 6.0 Product Guide" et notamment la section " Synchronizing engine times ".

3.4. DESCRIPTION DES MENACES

Par définition, une menace est une action ou un événement susceptible de porter préjudice à la sécurité de la cible évaluée.

Les agents menaçants considérés pour la CSPN sont les suivants :

- **utilisateur non autorisé** (attaquant humain ou entité informatique) qui interagit avec Forcepoint™ Stonesoft® Next Generation Firewall mais qui ne dispose pas d'accès légitime ;
- **utilisateur autorisé** disposant d'accès restreints sur Forcepoint™ Stonesoft® Next Generation Firewall (superviseur ou exploitant).

Les administrateurs (ceux disposant de tous les privilèges sur Forcepoint™ Stonesoft® Next Generation Firewall) ne sont pas considérés comme des attaquants. Les attaques physiques sur l'*appliance* ne sont également pas considérées pour l'évaluation CSPN.

Les attaquants peuvent être situés sur le réseau non maîtrisé, le réseau local ou le réseau d'administration.

Les menaces qui portent sur les biens sensibles de la TOE sont les suivantes :

- **M.CONTOURNEMENT_PARE_FEU**

  Un attaquant situé sur le réseau non maitrisé arrive à leurrer la fonctionnalité de filtrage des flux de Forcepoint™ Stonesoft® Next Generation Firewall pour accéder au SI du réseau surveillé. Cette attaque peut prendre la forme, par exemple, de l'utilisation d'adresse IP usurpée voire même de l'exploitation d'une faille ou d'une mauvaise configuration.

- **M.DÉNI_DE_SERVICE**

  Un attaquant parvient à mettre la TOE ou une de ses fonctions (pare-feu par exemple) en état de déni de service depuis le réseau non maitrisé.

- **M.ALTÉRATION**

  Un attaquant altère (modification ou suppression) des biens sensibles en intégrité de la TOE ou compromet des biens sensibles de la TOE en confidentialité. Les biens sensibles concernés sont les éléments cryptographiques, les journaux, la base des utilisateurs, la configuration et la politique du contrôle de flux.

- **M.EXFILTRATION**

  Un attaquant parvient à prendre connaissance des éléments cryptographiques, des journaux produits, des données de configuration ou de la politique de contrôle de flux.

- **M.ÉLÉVATION_PRIVILÈGES**

  Un attaquant disposant d'un accès restreint réussit à élever ses privilèges. À titre illustratif, un utilisateur ayant le rôle « exploitant » parvient à élever ses droits pour obtenir ceux d'un « superviseur » ou d'un « administrateur ».

- **M.UTILISATEUR_ILLICITE**

  Un attaquant ne disposant pas d'accès à la TOE parvient à effectuer des opérations illicites d'administration, de supervision ou d'exploitation en mettant en défaut les données d'authentification, le journal des événements de sécurité ou les paramètres de configuration. Cette menace peut prendre la forme d'une usurpation d'identité suite à des tentatives aléatoires répétées ou par le biais d'analyses de séquences d'authentification interceptées.

- **M.MITM_ADMIN**

  Un attaquant situé sur le réseau d'administration se place en homme-du-milieu entre l'*appliance* et le module SMC afin de porter atteinte en intégrité et/ou confidentialité aux données transitant sur ce lien.

- **M.MISE_A_JOUR_MALICIEUSE**

  Un attaquant parvient à forcer l'application d'une mise à jour malicieuse ou intercepte et modifie à son compte un flux de mise à jour légitime.

3.5. DESCRIPTION DES FONCTIONS DE SECURITE

Par définition, les fonctions de sécurité sont l'ensemble des mesures techniques et des mécanismes mis en œuvre par la TOE pour protéger de façon proportionnée les biens sensibles de la TOE contre les menaces identifiées.

Les fonctions de sécurité essentielles de la TOE sont les suivantes :

- **F.ANALYSE**

  Fonction de contrôle des flux d'informations du trafic traversant l'*appliance* Forcepoint™ Stonesoft® Next Generation Firewall. Cette dernière contrôle le flux de toutes les informations qui transitent par ses connexions réseau internes et externes pour mettre en œuvre la politique de sécurité du pare-feu à l'aide des éléments suivants :

  - règles d'accès fondées sur les adresses source et destination, ainsi que sur le protocole de la couche transport, celui de la couche application, le port source, le port de destination et l'interface sur laquelle le paquet arrive ; le suivi des connexions ; les résultats de l'authentification utilisateur et la durée de validité ;
  - règles permettant de décider d'accepter ou de rejeter des connexions chiffrées et non chiffrées ;
  - agents de protocole apportant des règles supplémentaires basées sur des mécanismes et des informations au niveau application. Ces agents de protocole permettent de renforcer la sécurité (conformité protocolaire) mais sont aussi nécessaires pour la translation d'adresse (NAT) pour les protocoles avec ouverture de ports dynamique (FTP, SIP…) ainsi que pour la redirection transparente des connexions. Alors que le moteur de pare-feu prend en charge de nombreux agents de protocole, l'évaluation se limite quant à elle aux agents des protocoles FTP, HTTP et SMTP.

  La règle de filtrage par défaut est présente dans le *template* de base, il s'agit d'une règle qui bloque le flux et qui stocke les logs. Sans règle, le boîtier bloque le flux d'une manière silencieuse.

  Tout paquet filtré (ayant le statut "*Discarded*") est bloqué *de facto* et ne sera donc pas traité par un autre service, ni réinjecté par un service dans la fonction de filtrage. En effet, il est assuré que tout paquet devant être ignoré par la TOE sera effectivement filtré et ne sera pas analysé a posteriori par un service externe à la fonction de filtrage.

  Une translation d'adresses réseau (NAT) est mise en œuvre entre des entités informatiques externes qui font transiter du trafic par la TOE, assurant que l'adresse IP des hôtes sur les réseaux internes est maintenue privée aux yeux des utilisateurs externes.

- **F.JOURNALISATION**

  La TOE permet de générer des enregistrements d'audit des événements de sécurité relatifs au trafic IP transitant par l'*appliance* Forcepoint™ Stonesoft® Next Generation Firewall ainsi que des enregistrements d'audit des modifications de la politique de

sécurité du pare-feu, de la gestion de l'*appliance* (authentification des utilisateurs, actions d'administration ou de supervision). La TOE permet également à l'administrateur autorisé (ou le superviseur autorisé) de définir les critères de sélection des événements du trafic IP à auditer. La TOE comporte un mécanisme empêchant la perte des données d'audit.
Les journaux sont générés par Forcepoint™ Stonesoft® Next Generation Firewall et envoyés au service LogServer (inclus dans le module SMC). En cas d'indisponibilité de LogServer, les logs sont bufferisés dans la partition `/var/spool` de Forcepoint™ Stonesoft® Next Generation Firewall.

- **F.CONTROLE_ACCÈS**

  Les utilisateurs (administrateurs, superviseurs et exploitants) accèdent au moteur de pare-feu (Forcepoint™ Stonesoft® Next Generation Firewall) via le serveur d'administration (module SMC) lequel fournit l'IHM permettant de gérer la politique de sécurité et les attributs d'authentification, les données et les fonctions de sécurité du moteur de pare-feu. Le moteur de pare-feu assure également que les fonctions de sécurité de confiance sont toujours appelées et ne peuvent pas être contournées.

  L'authentification est portée par le module SMC qui lui-même se base sur un mode d'authentification sous-jacent. Les modes d'authentification possibles des utilisateurs sont :

  - **Authentification sur une Base Locale** (les mots de passe sont stockés hachés (en sha512) et salés dans la base de données du module d'administration (SMC))
  - **Authentification via un serveur RADIUS** (méthodes supportées : PAP, CHAP, MSCHAP, MSCHAPv2 et EAP-MD5)
  - **Authentification TACACS** (méthodes supportées : ASCII, PAP, CHAP, MSCHAP)

  Toute solution d'authentification, supportant les protocoles d'authentification forte listés ci-dessus, peut être utilisée en lien avec le SMC.

  Remarque : seul le mode RADIUS est considéré dans la présente évaluation.

  La TOE permet donc d'identifier et d'authentifier nominativement les utilisateurs déclarés à accéder au système et de leur attribuer des droits en fonction de leur rôle.

  Il est possible de donner un accès direct au pare-feu à un administrateur (pour faire des diagnostics par exemple) en activant le protocole SSH (désactivé par défaut) et créer une règle de pare-feu afin d'autoriser cette connexion SSH. L'authentification de l'administrateur sur le pare-feu se fait à partir d'une base locale. Les mots de passe sont stockés hachés et salés dans un fichier accessible uniquement par le super utilisateur *root* du pare-feu. L'administrateur a la possibilité de changer le mot de passe depuis le module SMC.

- **F.FLUX_SÉCURISÉS**

  Les communications entre le pare-feu et le SMC sont protégées en confidentialité et en intégrité par l'utilisation d'un chiffrement avec par défaut des clés de 256 bits en TLS 1.2 (TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384). Il est toutefois possible de désactiver le mode 256 bits et de redescendre en 128 bits en TLS 1.2 (TLS_RSA_WITH_AES_128_CBC_SHA) par simple configuration. Enfin, les *appliances* et les composants de management s'authentifient mutuellement par certificat (autorité de certification interne en ECDSA par défaut ou RSA).

- **F.MISES_A_JOUR_SECURISÉES**

  Le processus de mise à jour de Forcepoint™ Stonesoft® Next Generation Firewall est authentifié et protégé en intégrité.

3.6. MATRICES DE COUVERTURE

3.6.1. Menaces et biens sensibles

La matrice suivante présente la couverture des menaces sur les biens sensibles (les lettres "D", "I", "C" et "A" représentent respectivement les besoins de Disponibilité, Intégrité, Confidentialité et Authenticité) :

	B.FITRAGE	B.SERVICES	B.TOPOLOGIE	B.DONNÉES_CONFIGURATION	B.JOURNAUX	B.FLUX_ADMINISTRATION	B.MISES_A_JOUR	B.ÉLÉMENTS_CRYPTO
M.CONTOURNEMENT_PARE_FEU		I	C					
M.DÉNI_DE_SERVICE	D	D		D				
M.ALTÉRATION				I	IA			I
M.EXFILTRATION		C		C	C			C
M.ÉLÉVATION_PRIVILÈGES				IC		IC		I
M.UTILISATEUR_ILLICITE	D			DIC	DIC			DI
M.MITM_ADMIN					A	IC		
M.MISE_A_JOUR_MALICIEUSE						I	IA	I
M.VOL_PARE_FEU		C		C	C			C

Tableau 2 - Couverture des biens sensibles par les menaces

3.6.2. Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

	F.ANALYSE	F.JOURNALISATION	F.CONTROLE_ACCÈS	F.FLUX_SÉCURISÉS	F.MISES_A_JOUR_SECURISÉES
M.CONTOURNEMENT_PARE_FEU	√				

	F.ANALYSE	F.JOURNALISATION	F.CONTROLE_ACCÈS	F.FLUX_SÉCURISÉS	F.MISES_A_JOUR_SECURISÉES
M.DÉNI_DE_SERVICE	√				
M.ALTÉRATION		√	√	√	
M.EXFILTRATION				√	
M.ÉLÉVATION_PRIVILÈGES		√	√		
M.UTILISATEUR_ILLICITE		√	√		
M.MITM_ADMIN				√	
M.MISE_A_JOUR_MALICIEUSE					√

Tableau 3 - Couverture des menaces par les fonctions de sécurité

4.ANNEXES

4.1. CAS PARTICULIER DE LA COUCHE VIRTUELLE

La couche virtuelle n'est pas soumise à l'évaluation. La présence de cette annexe se veut purement informative.

Dans la version soumise à l'évaluation, la couche virtuelle peut être un produit VMware ou KVM. Dans le premier cas, l'installation d'un boîtier peut être effectuée depuis une image ISO ou depuis une machine virtuelle déjà construite (OVA) et qui peut être importée telle quelle dans un hyperviseur vSphere. Dans le deuxième cas, l'installation d'un boîtier est effectuée depuis une image ISO.

Dans les deux cas, la solution permet d'effectuer un contrôle entre différents réseaux virtuels comme montre l'exemple simple ci-après.

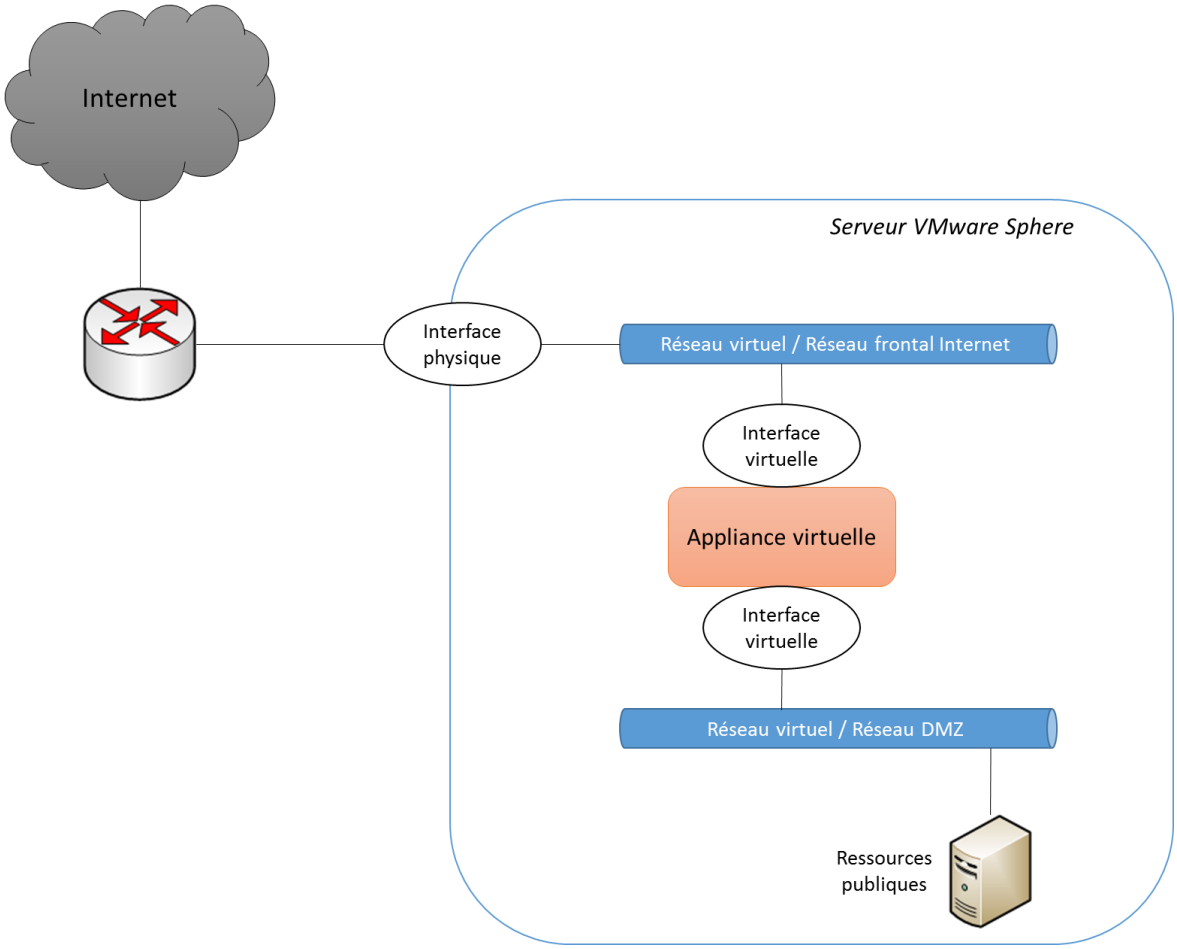

Figure 4 – Exemple de la solution utilisée sous environnement virtuel

4.2. SPECIFICATIONS MATERIELLES

Les tableaux ci-dessous présentent les spécifications matérielles des *appliances* NGFW de **Forcepoint**.

NGFW 110

NGFW 115

SPECIFICATIONS

PERFORMANCE*	110 & 115
NGFW Throughput (HTTP 21 kB payload)	150 Mbps
Maximum Firewall Throughput (UDP 1518 byte)	1.5 Gbps
Maximum Inspection Throughput (UDP 1518 byte)	400 Mbps
SSL Inspection (AES-256)	100 Mbps
Inspected Concurrent Connections	100,000
IPsec VPN Throughput (AES-128-GCM)	500 Mbps
IPsec VPN Tunnels	500
Mobile VPN Clients	Max 25
Maximum SSL VPN Portal Users	-
Concurrent Connections (No Inspection)	1 million
New TCP Connections/sec. (No Inspection)	10,000
64-Byte Packets/sec. (No Inspection)	240,000
VLAN Tagging	Unlimited[1]

PHYSICAL	110	115
Form Factor	Desktop	
Dimensions (W x H x D)	242 x 55 x 198mm 9.52 x 2.17 x 7.80in	
Net Weight (Without Modules)	1.1 kg 2.43lbs	
AC Power Supply	100–240 VAC 50–60 Hz, 36 W	
Typical Power Consumption	15 W	18 W
Maximum Power Consumption	32 W	38 W
Maximum BTU/hr.	109	130
MTBF (hr.)	120,000	
Operating Temperature	5–+40°C +41–+104°F	
Storage Temperature	-20–+70°C -4–+158°F	
Relative Humidity (Non-Condensing)	10%–90%	
Safety Certifications	CB, UL/EN60950	
EMI Certifications	FCC part 15, CE, EN55022, EN55024	

NETWORK INTERFACES	110	115
Fixed Ethernet Interfaces	10 x GE RJ45	
Gigabit Ethernet — Copper Ports	10	10-14
WiFi Capability	-	IEEE802.11ac/a/b/g/n
Network I/O Slots	0	1 mini module
Connectors	2 x USB, 1 x serial	

ORDERING	PART #
Forcepoint NGFW 110 Appliance	N110
Forcepoint NGFW 115 Appliance	N115
OPTIONAL SUBSCRIPTIONS	
URL Filtering for NGFW 110 and 115	FPWF3
Advanced Malware Detection for NGFW 110 and 115	FPAMD1
NETWORKING MODULES	
4 Port Gigabit Ethernet Mini Module	MMGE4
1 Port Gigabit Ethernet SFP Mini Module	MMGESFP
ACCESSORIES	
100 Series AC Power Supply	ACP110
100 Series Spare part Cfast (SLC)	ACM4

[1] Tagging is not available with switch ports 2-9.
[2] See NGFW Module Datasheet for details on modules and supported SFPs
[3] Supported only for 115 appliance
* Performance values reflect maximums measured under test conditions and may vary based on configuration and features enabled.

NGFW 321

NGFW 325

SPECIFICATIONS

PERFORMANCE*	321 & 325
NGFW Throughput (HTTP 21 kB payload)	200 Mbps
Maximum Firewall Throughput (UDP 1518 byte)	4 Gbps
Maximum Inspection Throughput (UDP 1518 byte)	700 Mbps
SSL Inspection (AES-256)	150 Mbps
Inspected Concurrent Connections	100,000
IPsec VPN Throughput (AES-128-GCM)	1 Gbps
IPsec VPN Tunnels	6000
Mobile VPN Clients	Unlimited
Maximum SSL VPN Portal Users	500
Concurrent Connections (No Inspection)	2 million
New TCP Connections/sec. (No Inspection)	15,000
64-Byte Packets/sec. (No Inspection)	800,000
VLAN Tagging	Unlimited
Virtual Contexts (default/maximum)	3/3

PHYSICAL	321	325
Form Factor	Desktop[1]	
Dimensions (W x H x D)	282 x 44 x 196mm 11.11 x 1.73 x 7.72in	305 x 44 x 196mm 12 x 1.73 x 7.72in
Net Weight (Without Modules)	1.8kg 3.97 lbs.	2.2kg 4.85 lbs.
AC Power Supply	100–240 VAC 50–60 Hz, 180 W	
Typical Power Consumption	18 W	22 W
Maximum Power Consumption	21 W	28 W
Maximum BTU/hr.	72	96
MTBF (hr.)	120,000	
Operating Temperature	0–+45°C +32–+113°F	
Storage Temperature	-20–+70°C -4–+158°F	
Relative Humidity (Non-Condensing)	10%–90%	
Safety Certifications	CB, UL/EN60950	
EMI Certifications	FCC part 15, CE, EN55022, EN55024	

NETWORK INTERFACES	321	325
Fixed Ethernet Interfaces	5 x GE RJ45	
Gigabit Ethernet — Copper Ports	5	5-13
WiFi Capability	0	IEEE802.11a/b/g/n
Network I/O Slots	0	2 mini modules
Connectors	2 x USB, 1 x serial	

ORDERING	PART #
Forcepoint NGFW 321 Appliance	N321
Forcepoint NGFW 325 Appliance	N325
OPTIONAL SUBSCRIPTIONS	
URL Filtering for NGFW 321 and 325	FPWF5
Advanced Malware Detection for NGFW 321 and 325	FPAMD2
NETWORKING MODULES [2,3]	
2 Port Gigabit Ethernet bypass Mini Module	MMGE2B
4 Port Fast Ethernet Switch Mini Module	MMFESW4
4 Port Gigabit Ethernet Mini Module	MMGE4
1 Port Gigabit Ethernet SFP Mini Module	MMGESFP
ACCESSORIES	
300 Series AC Power Supply	ACP32X
300 Series 19in Rack Mounting Kit	ACR32X
300 Series Spare part Cfast (SLC)	ACM8

[1] Optional rack mount kit available
[2] See NGFW Module Datasheet for details on modules and supported SFPs
[3] Supported only for 325 appliance
* Performance values reflect maximums measured under test conditions and may vary based on configuration and features enabled.

NGFW 1000 SERIES

SPECIFICATIONS

PERFORMANCE*	1035	1065
NGFW Throughput (HTTP 21 kB payload)	400 Mbps	1.2 Gbps
Maximum Firewall Throughput (UDP 1518 byte)	10 Gbps	20 Gbps
Maximum Inspection Throughput (UDP 1518 byte)	1 Gbps	3 Gbps
SSL Inspection (AES-256)	150 Mbps	500 Mbps
Inspected Concurrent Connections	150,000	1 million
IPsec VPN Throughput (AES-128-GCM)	1.2 Gbps	3 Gbps
IPsec VPN Tunnels	20,000	
Mobile VPN Clients	Unlimited	
Maximum SSL VPN Portal Users	1,000	2,000
Concurrent Connections (No Inspection)	5 million	8 million
New TCP Connections/sec. (No Inspection)	35,000	100,000
64-Byte Packets/sec. (No Inspection)	1.2 million	5 million
VLAN Tagging	Unlimited	
Virtual Contexts (default/maximum)	5/5	

PHYSICAL	1035	1065
Form Factor	1RU	
Dimensions (W x H x D)	426 x 44 x 300mm 16.77 x 1.73 x 11.81in	
Net Weight (Without Modules)	4.2kg 9.25 lbs.	
AC Power Supply	100–240 VAC 50–60 Hz, 180 W	
DC Typical Power option	-72 – -36 VDC, 200W dual feed	
Redundant power supply	-	
Typical Power Consumption	50 W	65 W
Maximum Power Consumption	95 W	90 W
Maximum BTU/hr.	256	307
MTBF (hr.)	120,000	
Operating Temperature	0–+40°C +32–+104°F	
Storage Temperature	-20–+70°C -4–+158°F	-20–+75°C -4–+167°F
Relative Humidity (Non-Condensing)	10%–95%	
Safety Certifications	CB, UL/EN60950	
EMI Certifications	FCC part 15, CE, EN55022, EN55024	

NETWORK INTERFACES	1035	1065
Fixed Ethernet Interfaces	4 x GE RJ45	
Gigabit Ethernet — Copper Ports	4-12	
10 Gigabit Ethernet ports (1065 Only)	0-4	
40 Gigabit Ethernet ports	-	
Network I/O Slots	1	
Connectors	2 x USB, 1 x serial	

ORDERING	PART #
Forcepoint NGFW 1035 Appliance, AC power supply	N1035
Forcepoint NGFW 1035 Appliance, DC power supply	N1035D
Forcepoint NGFW 1065 Appliance, AC power supply	N1065
Forcepoint NGFW 1065 Appliance, DC power supply	N1065D
OPTIONAL SUBSCRIPTIONS	
Web Filtering Feature Pack for NGFW 1035 and 1035 DC	FPWF9
Web Filtering Feature Pack for NGFW 1065 and 1065 DC	FPWF11
Advanced Malware Detection – NGFW 1035	FPAMD3
Advanced Malware Detection – NGFW 1065	FPAMD4
NETWORKING MODULES[1]	
4 Port Gigabit Ethernet RJ45 Module	M0G4
4 Port Gigabit Ethernet SFP Module	M0GF4
8 Port Gigabit Ethernet RJ45 Module	M0G8
2 Port 10 Gigabit Ethernet RJ45 Module (1065 Only)	M0102
2 Port 10 Gigabit Ethernet SFP+ Module (1065 Only)	M010F2
4 Port 10 Gigabit Ethernet SFP+ Module (1065 Only)	M010F4
2 Port Fiber Bypass LC Module	M0E2B
4 Port Gigabit Ethernet SX Fiber Bypass Module	M0GS4B
4 Port Gigabit Ethernet Bypass RJ45 Module	M0G4B
2 Port 10 Gigabit RJ45 Bypass Module (1065 Only)	M0102B
2 Port 10 Gigabit Ethernet Long Reach Bypass Module (1065 Only)	M010L2B
2 Port 10 Gigabit EthernetShort Reach Bypass Module (1065 Only)	M010L2B
ACCESSORIES	
1035 Spare part Cfast (SLC)	ACM8
1065 Spare part Cfast (SLC)	ACM16

[1] See NGFW Module Datasheet for details on modules and supported SFPs

NGFW 3301

NGFW 3305

SPECIFICATIONS

PERFORMANCE*	3301	3305
NGFW Throughput (HTTP 21 kB payload)	9 Gbps	15 Gbps
Maximum Firewall Throughput (UDP 1518 byte)	80 Gbps	160 Gbps
Maximum Inspection Throughput (UDP 1518 byte)	30 Gbps	
SSL Inspection (AES-256)	5 Gbps	14 Gbps
Inspected Concurrent Connections	12 million	15 million
IPsec VPN Throughput (AES-128-GCM)	18 Gbps	22 Gbps
IPsec VPN Tunnels	200,000	
Mobile VPN Clients	Unlimited	
Maximum SSL VPN Portal Users	20,000	30,000
Concurrent Connections (No Inspection)	30 million	50 million
New TCP Connections/sec. (No Inspection)	30,000	50,000
64-Byte Packets/sec. (No Inspection)	40 million	90 million
VLAN Tagging	Unlimited	
Virtual Contexts (default/maximum)	10/100	25/250

PHYSICAL	3301	3305
Form Factor	2RU	
Dimensions (W x H x D)	450 x 89 x 450mm 17.7 x 3.5 x 17.7in	437 x 89 x 450mm 17.2 x 3.5 x 17.7in
Net Weight (Without Modules)	12.4kg 27.3lbs.	
AC Power Supply	100–240 VAC 50–60 Hz, 650 W + 650 W	
DC Power Supply Option	-72 – -36 VDC, 650 W + 650 W	
Redundant Power Supply	Yes	
Typical Power Consumption	350 W	400 W
Maximum Power Consumption	450 W	500 W
Maximum BTU/hr.	1536	1706
MTBF (hr.)	100,000	
Operating Temperature	5–+40°C +41–+104°F	
Storage Temperature	-40–+70°C -4–+158°F	
Relative Humidity (Non-Condensing)	8%–90%	
Safety Certifications	CB, UL/EN60950	
EMI Certifications	FCC part 15, CE, EN55022, EN55024	

NETWORK INTERFACES	3301	3305
Fixed Ethernet Interfaces	2 x GE RJ45 Integrated 40G QSFP for 3305	
Gigabit Ethernet — Copper Ports	2-34	
10 Gigabit Ethernet ports	0-16	
40 Gigabit Ethernet ports	0-8	1-9
Network/ I/O Slots	4	
Connectors	4 x USB, 1 x serial, VGA, IPMI Ethernet	

ORDERING	PART #
Forcepoint NGFW 3301 Appliance	N3301
Forcepoint NGFW 3305 Appliance	N3305
OPTIONAL SUBSCRIPTIONS	
URL Filtering for NGFW 3301	FPWF17
URL Filtering for NGFW 3305	FPWF19
Advanced Malware Detection for NGFW 3301	FPAMD7
Advanced Malware Detection for NGFW 3305	FPAMD8
Virtual Contexts upgrade for NGFW 3301 (10-100)	FPVC100
Virtual Contexts upgrade for NGFW 3305 (25-250)	FPVC250
NETWORKING MODULES[1]	
2 Port 40 Gigabit Ethernet QSFP Module[2]	M040F2
2 Port 10 Gigabit Ethernet SFP+ Module	M010F2
4 port 10 Gigabit Ethernet SFP+ Module revision 2	M0E10F4
2 Port 10 Gigabit Ethernet RJ45 Module	M0102
4 Port Gigabit Ethernet SFP Module	M0GF4
8 Port Gigabit Ethernet RJ45 Module	M0G8
2 Port 10 Gigabit Ethernet Long Reach Bypass Module	M010L2B
2 Port 10 Gigabit Ethernet Short Reach Bypass Module	M010S2B
ACCESSORIES	
3300 Series Fan Kit	ACF33K
3300 Series Spare part SSD (MLC)	ACD400
Spare part AC power supply	ACP3300
Spare part DC power supply	ACPD3300

[1] See NGFW Module Datasheet for details on modules and supported SFPs
[2] NGFW engine release 5.10.3 or newer required
*Performance values reflect maximums measured under test conditions and may vary based on configuration and features enabled.

Fin du document