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-2013/10

## Fonction de Filtrage du boîtier PA 2050
## Version logicielle 5.0.4

*Paris, le 5 décembre 2013*

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

[Original signé]
Patrick Pailloux

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*<br>**ANSSI-CSPN-2013/10** |
| *Nom du produit*<br>**Fonction de Filtrage du boîtier PA 2050** |
| *Référence/version du produit*<br>**5.0.4** |
| *Catégorie de produit*<br>**Pare-feu** |
| *Critères d'évaluation et version*<br>**CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*** |
| *Développeur*<br>**Palo Alto Networks**<br>**3300 Olcott Street**<br>**Santa Clara, CA 95054**<br>**Etats-Unis d'Amérique** |
| *Commanditaire*<br>**Palo Alto Networks**<br>**Bâtiment A, étage 2**<br>**4 Boulevard des Îles**<br>**92120 Issy les Moulineaux** |
| *Centre d'évaluation*<br>**AMOSSYS**<br>**4 bis Allée du Bâtiment**<br>**35000 Rennes** |

# 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 « Fonction de Filtrage du boîtier PA 2050, version logicielle 5.0.4 » développée par la société Palo Alto Networks.

Le boîtier PA2050 est un pare-feu qui se présente sous la forme d'une *appliance*, et offre notamment des fonctions permettant l'identification des applications, des utilisateurs et du contenu des flux en provenance et à destination du réseau de l'entreprise.

Le produit offre les fonctionnalités suivantes :

- autoriser le trafic ;
- autoriser le trafic et rechercher des menaces, vulnérabilités et virus ;
- déchiffrer et inspecter le trafic ;
- refuser / bloquer le trafic (par exemple, refuser tout trafic en provenance de pays spécifiques) ;
- autoriser certaines applications ou fonctions, par exemple :
    - autoriser l'utilisation de *MSN* et *Google Task* mais bloquer l'utilisation de leurs fonctions respectives de transfert de fichiers ;
    - bloquer des applications indésirables comme le partage de fichier *P2P*[1] .

Les informations statistiques d'identification et de filtrage permettent à un administrateur d'affiner les stratégies de sécurité en fonction du trafic qui traverse le réseau.

Pour garantir un accès permanent aux fonctionnalités de gestion, les plateformes d'administration (*Control Plane*) et de gestion des données (flux réseau, évènements de sécurité et d'identification, *Data Plane*) sont physiquement séparées au sein de l'appliance (traitement et mémoire dédiés).

[1] *Peer to Peer* ou Pair à Pair.

## 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 – firewall** |
| ☐ 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 - matériel et logiciel embarqué |
| ☐ 99- Autres |

### *1.2.2. Identification du produit*

La version certifiée du produit est la version 5.0.4, identifiable depuis l'interface d'administration du produit dans le panneau « Informations générales » du Tableau de bord (voir figure 1).


**Figure 1 : Identification de la version du produit dans le tableau de bord de l'interface d'administration**

### *1.2.3. Services de sécurité*

Les services de sécurité fournis par le produit faisant l'objet de l'évaluation sont les suivants :

- filtrage des flux d'information transitant par le boîtier, en fonction des règles spécifiées dans la politique définie par l'administrateur, grâce notamment à des mécanismes permettant :
  - l'analyse des flux applicatifs : le produit identifie les paquets associés aux flux applicatifs transitant par le boîtier ainsi que les données incluses dans ces flux afin de leur appliquer la politique de filtrage ;
  - l'identification des utilisateurs : le produit identifie les utilisateurs d'applications en maintenant une table des utilisateurs de manière incrémentale et proactive grâce à la consultation des informations issues de différentes sources (journaux de connexions des contrôleurs de domaine par exemple) ;
- journalisation :
  - des évènements de sécurité relatifs au trafic IP transitant par le pare-feu et la détection de menaces, vulnérabilités et virus ;
  - des modifications de la politique de sécurité du pare-feu.

  Ces traces sont stockées localement ou envoyées de manière sécurisée vers un outil tiers distant (SIEM, archivage etc.) ;
- mise à jour : le produit dispose d'un mécanisme de mise à jour de la base des signatures applicatives lui permettant d'identifier les applications à l'origine des flux ;
- contrôle d'accès aux fonctions d'administration au moyen de rôles attribués aux utilisateurs autorisés.

### *1.2.4. Configuration évaluée*

Le modèle PA-2050 a été utilisé par l'évaluateur (Figure 2). Bien que cela n'ait pas été vérifié dans le cadre de l'évaluation, le même comportement peut être observé sur l'ensemble des boîtiers de la gamme *PA Series* aux dires du développeur.

PA-2050

1 Gbps firewall throughput (App-ID enabled[1])

500 Mbps threat prevention throughput

300 Mbps IPSec VPN throughput

250,000 max sessions

15,000 new sessions per second

2,000 IPSec VPN tunnels/tunnel interfaces

1,000 SSL VPN Users

10 virtual routers

1/6* virtual systems (base/max[2])

40 security zones

5,000 max number of policies

**Figure 2 : Boîtier PA-2050 utilisé pour l'évaluation**

# 2. L'évaluation

## 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. 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 a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit ne comportant pas de mécanismes cryptographiques.

## 2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

### *2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité*

#### 2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 3 « Argumentaire du produit »).

#### 2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 5 « Biens sensibles devant être protégés par le produit »).

#### 2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des menaces »).

#### 2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 7 « Description des fonctions de sécurité du produit »).

#### 2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 3.6 « Description des utilisateurs typiques concernés »).

### *2.3.2. Installation du produit*

#### 2.3.2.1. Plate-forme de test

La plate-forme de test est décrite dans la figure suivante :

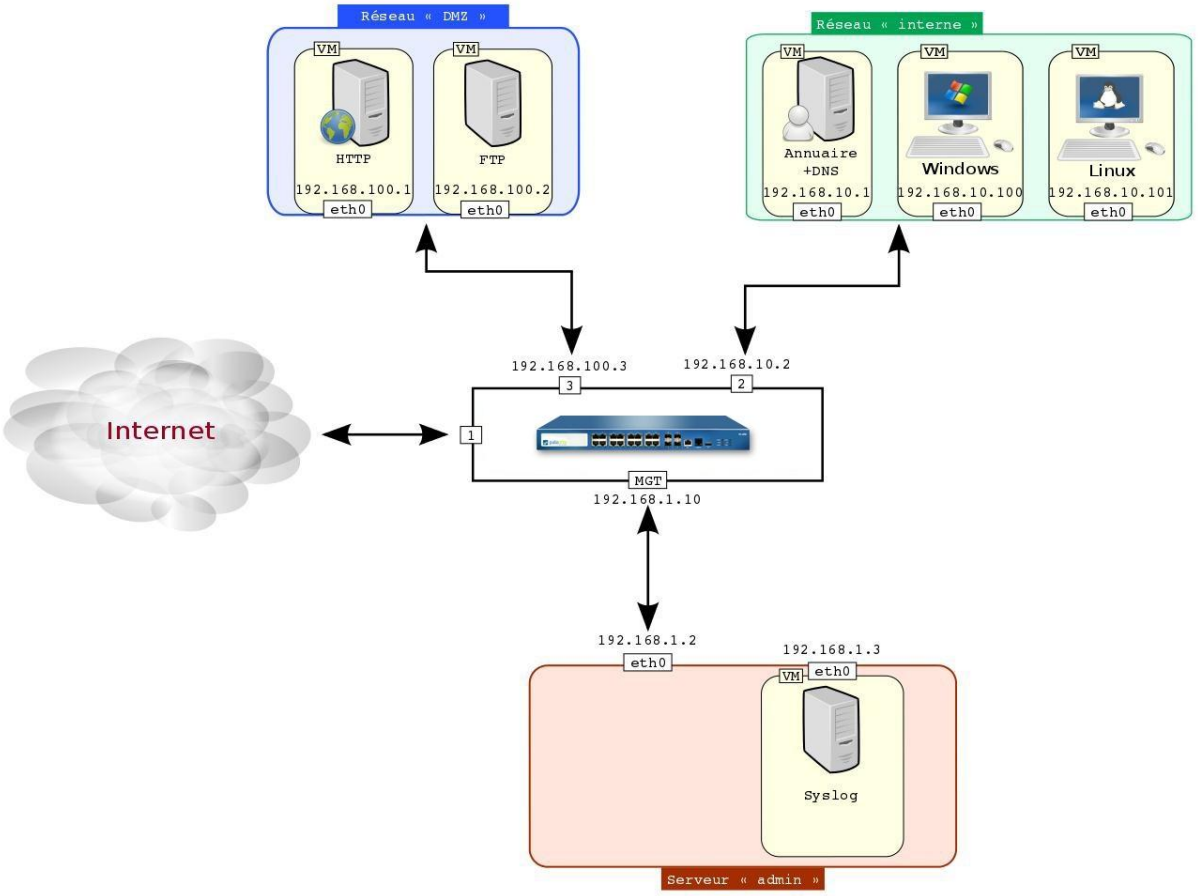


**Figure 3 : Schéma de la plate-forme d'évaluation**

Plusieurs réseaux ont été créés pour simuler l'infrastructure typique d'une entreprise.

- Le réseau local (nommé réseau « interne » sur la figure précédente) contient les postes clients ainsi qu'un serveur contrôleur de domaine *Active Directory*, mis en œuvre sur le système d'exploitation Windows Serveur 2008 R2 SP1 64 bits, pour l'authentification des utilisateurs. Sur le serveur Active Directory, un serveur DNS a également été installé.

  Deux postes clients ont été créés : un poste dont le système d'exploitation est Windows 7 SP1 PRO 64 bits et un poste dont le système d'exploitation est Debian wheezy 3.2.0-4 64 bits.

  Sur le contrôleur de domaine, deux utilisateurs ainsi qu'un groupe d'utilisateurs nommé « calendrier » ont été créés, auxquels ont été affectés des droits différents dans les politiques du pare-feu.

- Le réseau DMZ contient un serveur web (serveur dont le système d'exploitation est Debian lenny 2.6.32-5-686, sur lequel est installé le paquet apache2 en version 2.2.16-

6+squeeze7) et un serveur ftp (serveur dont le système d'exploitation est Debian lenny 2.6.32-5-686, sur lequel est installé le paquet proftpd-basic en version 1.3.3a-6squeeze6). Ce réseau contient les serveurs auxquels il est possible d'accéder depuis l'extérieur.

- Le réseau « admin » est le réseau depuis lequel les administrateurs du système d'information de l'entreprise se connectent pour le configurer. Un poste client dont le système d'exploitation est Windows 7 pro 32 bits a été installé dans ce réseau, connecté directement au port MGT du pare-feu.

Le pare-feu a un port connecté à chaque réseau ainsi qu'au réseau externe (réseau considéré comme n'étant pas de confiance).

#### 2.3.2.2. Particularités de paramétrage de l'environnement

L'interface de gestion de l'équipement propose un ensemble de configurations très étendues et interdépendantes. Chaque mécanisme de sécurité évalué fait l'objet d'une documentation à destination des administrateurs. Cependant, l'intervention d'un administrateur maîtrisant parfaitement les produits de ce constructeur est vivement recommandée pour s'assurer de la cohérence et du fonctionnement général du produit en environnement de production.

Plusieurs mécanismes doivent faire l'objet d'une attention particulière, faute de rendre le produit inopérant :

- Le mécanisme d'identification des utilisateurs proposé par le produit induit certaines contraintes architecturales de l'environnement du système d'information. Par exemple :
  - il est possible d'interfacer le produit avec un serveur d'annuaire existant. Pour cela, les paramètres de connexion à ce service doivent être cohérents avec la politique de filtrage mise en place par le pare-feu ;
  - les guides d'utilisation mentionnent la possibilité d'intégrer un agent au service d'annuaire interfacé au mécanisme d'identification. L'évaluateur recommande l'utilisation de cet agent facultatif afin d'offrir une réelle interface entre le produit et le serveur d'annuaire. L'installation de cet agent doit se faire sur un poste dédié, séparé du serveur Active Directory, ainsi que le recommande le développeur ;
  - le mécanisme d'identification figure parmi les services disposant d'une gestion de l'itinérance de service spécifique (voir *Figure 4 - Définition d'un itinéraire de service pour les communications avec l'agent*). Il est recommandé d'isoler la connexion entre le pare-feu et le serveur d'annuaire et de spécifier la zone hébergeant cette liaison dans l'interface d'administration. Un défaut de communication avec le service mènerait directement à un défaut du mécanisme d'identification utilisateur.
- Le mécanisme de filtrage applicatif du pare-feu est fourni avec un ensemble de filtres préconfigurés et maintenus par le développeur. Ces filtres régissent les critères d'utilisation de certains services grâce à un système de signatures et de prise en compte du contexte d'emploi. L'évaluateur a identifié certains services basés sur le protocole HTTPS que le produit, dans sa configuration par défaut, ne permet pas de prendre en compte. Pour cela, un service de déchiffrement protocolaire est intégré au produit. Son utilisation permet de pallier en partie les défauts du mécanisme de

détection en mettant en place une rupture de la session sécurisée originale, dans le but de pouvoir en maitriser le contenu. L'évaluateur recommande la configuration du mécanisme de déchiffrement - avec les réserves soulevées au 2.3.8, afin d'améliorer significativement la pertinence du filtrage applicatif.

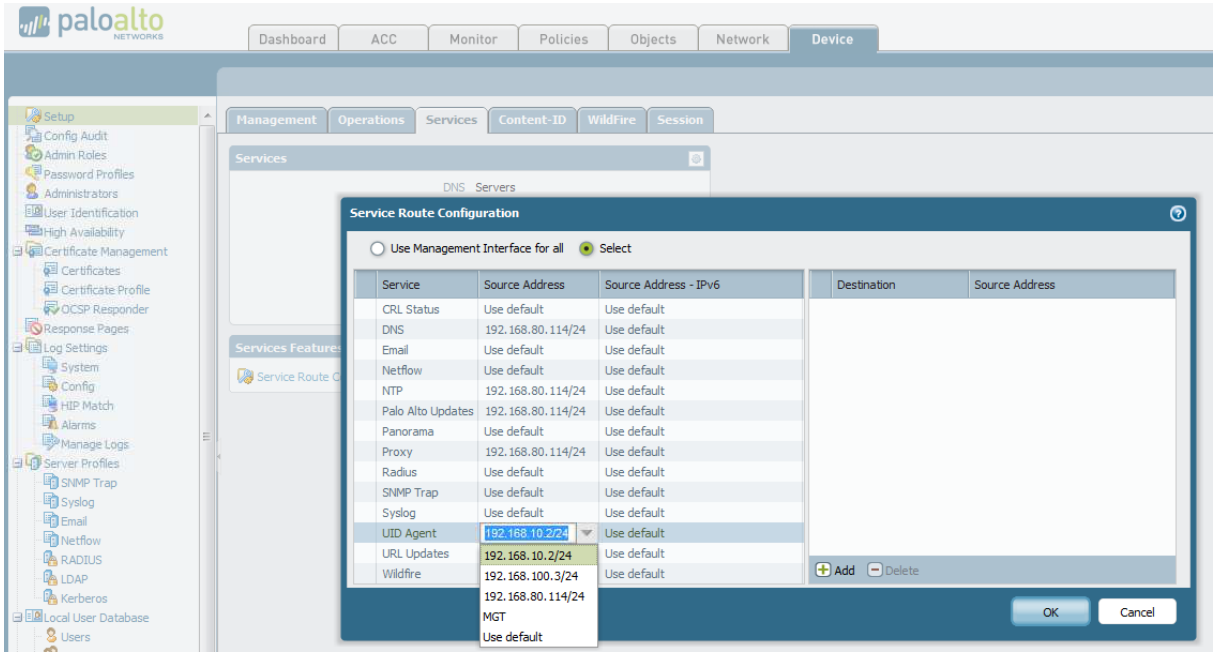


**Figure 4 - Définition d'un itinéraire de service pour les communications avec l'agent**

#### 2.3.2.3. Options d'installation retenues pour le produit

L'installation du pare-feu est décrite dans le guide [GSG].
L'évaluateur recommande :

- l'utilisation de zones distinctes, notamment pour les communications avec les serveurs d'annuaires ;
- la mise en place d'un agent User-ID sur le service d'annuaire ;
- la mise en place d'une politique de déchiffrement.

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

La plateforme d'évaluation est décrite au chapitre 2.3.2.1 (voir Figure 3 : Schéma de la plateforme d'évaluation).

Plusieurs réseaux ont été créés pour simuler la configuration typique d'une entreprise comme indiqué au chapitre 2.3.2.1.

Le port connecté au réseau d'administration est l'interface dédiée MGT : l'interface de configuration du pare-feu.
Pour configurer l'interface MGT, il suffit de connecter un équipement à ce port grâce à un câble RJ45 (configuration utilisée pour l'évaluation) ou au port console grâce à un câble série (la configuration du port série est fournie dans le guide [HRG]).

Les identifiants par défaut, que l'utilisateur doit présenter lors de la première connexion au pare-feu (par l'interface web ou par la console), doivent être changés par la suite.

Il faut ensuite configurer les interfaces du pare-feu qui seront connectées aux différents réseaux ainsi que les zones qui vont représenter les différents réseaux.
Dans le cadre de cette évaluation, les ports ont été configurés comme des interfaces de couche 3 reliées aux différentes zones.
Durant l'évaluation, la configuration IPv6 est restée désactivée au profit du protocole IPv4.

#### 2.3.2.5. Durée de l'installation

L'installation a nécessité deux jours avec l'assistance permanente du développeur.

#### 2.3.2.6. Notes et remarques diverses

D'un point de vue général, l'installation et la configuration du produit *PA Series* sont bien documentées ([GSG] pour un déploiement basique). Cependant, son utilisation et la compréhension de son fonctionnement sont moins aisées. D'une part, le chargement des pages de l'interface du pare-feu et la validation des paramètres sont très longs. D'autre part, certaines politiques de sécurité semblent provoquer des blocages du trafic qui ne sont signalés nulle part dans l'interface.
Le développeur a indiqué à l'évaluateur que les lenteurs dans le chargement des pages et les *commit* sont dus au modèle du pare-feu fourni pour l'évaluation (PA-2050) qui est ancien.

En outre l'évaluateur recommande une installation assistée par un intégrateur agréé par *Palo Alto Networks*, afin d'éviter que la configuration initiale ne soit incomplète ou défaillante.
Afin d'améliorer le filtrage du trafic et l'identification des applications, l'évaluateur recommande de mettre en place une politique de déchiffrement qui permettra d'identifier les applications contenues dans des flux chiffrés.

### *2.3.3. Analyse de la documentation*

L'évaluateur a eu accès à la documentation technique du produit [GUIDES].
La documentation fournie par le développeur est la suivante :

- la cible de sécurité ([CDS]) ;
- le guide de mise en route ([GSG]) ;
- le guide de l'administrateur ([AGF]) ;
- le guide de référence matériel ([HRG]) ;
- le guide de référence de l'interface en ligne de commande ([CLI-RG]).

La documentation fournie offre une description détaillée de l'ensemble des paramètres du pare-feu ([AGF]) et la description d'une configuration basique ([GSG]).
Le guide [CLI-RG] donne une description détaillée de l'ensemble des commandes utilisables lors de la connexion au pare-feu par l'interface série ou grâce au protocole SSH.
Le guide [HRG] donne des instructions pour l'installation et la maintenance du pare-feu au niveau matériel.

Dans l'ensemble, la documentation est lisible et détaillée mais elle ne permet pas de résoudre d'éventuels problèmes rencontrés lors de l'installation ou de l'administration du pare-feu (exemple : recherche d'informations concernant les zones bloquées par le pare-feu).

En effet, il est fortement recommandé que l'installation d'un pare feu de PaloAlto Networks soit réalisée par un intégrateur maitrisant ce produit. Ce pare-feu offre de multiples options qui peuvent être activées ou non après analyse par l'intégrateur de l'architecture à protéger.

La documentation est claire et aucune non-conformité n'a été relevée.

#### *2.3.4. Revue du code source (facultative)*

Sans objet.

#### *2.3.5. Fonctionnalités testées*

| Fonctionnalité | Résultat |
|---|---|
| Test du filtrage par adresse | **Réussite** |
| Test du filtrage par application | **Réussite** |
| Test du filtrage par service et port | **Réussite** |
| Test du filtrage par identification de l'utilisateur | **Réussite** |
| Test du mécanisme de mise à jour | **Réussite** |
| Test de l'application des rôles administrateur | **Réussite** |
| Test de la sécurisation des communications | **Réussite** |
| Test du filtrage du service Gmail | **Réussite sous conditions** |
| Test de l'identification des utilisateurs avec des règles utilisant des groupes de groupes | **Réussite** |

#### *2.3.6. Fonctionnalités non testées*

Sans objet.

#### *2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités*

Le bilan de l'analyse de la conformité est positif, aucune non-conformité n'a été identifiée. Cependant, le test du filtrage du service Gmail amène l'évaluateur à émettre une recommandation : afin que la pertinence du mécanisme de filtrage applicatif soit optimale, il est recommandé de mettre en place une politique de déchiffrement systématique, telle que présentée dans le rapport. Une attention particulière doit aussi être portée à la configuration de l'identification des utilisateurs (utilisation d'un agent et isolation de la connexion).

### *2.3.8. Avis d'expert sur le produit*

D'un point de vue général, l'installation et la configuration du produit *PA Series* sont bien documentées ([GSG] pour un déploiement basique). Cependant, son utilisation et la compréhension de son fonctionnement sont moins aisées. D'une part, le chargement des pages de l'interface du pare-feu et la validation des paramètres sont très longs. D'autre part, certaines politiques de sécurité semblent provoquer des blocages du trafic, dont l'application n'est indiquée nulle part dans l'interface.

En outre l'évaluateur recommande une installation assistée par un intégrateur agréé par *Palo Alto Networks*, afin d'éviter que la configuration initiale ne soit incomplète ou défaillante.

Au niveau fonctionnel, le produit offre un mécanisme de création de règles applicatives basées sur un ensemble de signatures plutôt complet. Certains filtres fournis, tels que *dl-free* ou *gmail*, sont cependant inadaptés à un usage opérationnel bien que fournis par défaut dans la configuration du produit. En effet, l'évaluateur a pu contourner ces filtres préconfigurés avec un niveau d'attaquant jugé faible.
Afin d'améliorer le filtrage du trafic et l'identification des applications, l'évaluateur recommande de mettre en place une politique de déchiffrement qui permettra d'identifier les applications contenues dans des flux chiffrés. Cette politique de déchiffrement doit être sélective et adaptée à la politique de sécurité de l'entreprise, par exemple à l'aide de listes blanches, afin de ne pas porter atteinte à la confidentialité de communications jugées sensibles.

Les tests ont montré que le mécanisme d'identification des utilisateurs peut subir des dysfonctionnements s'il n'est pas configuré correctement. L'évaluateur recommande ainsi l'utilisation de l'agent User-ID.

### *2.3.9. Analyse de la résistance des mécanismes et des fonctions*

#### 2.3.9.1. Liste des fonctions et des mécanismes testés

| Fonction et mécanisme |
|---|
| Test de résistance à la saturation FTP |
| Test de la résistance à une attaque par déni de service (DoS) |
| Test de la résistance du filtrage applicatif par l'adresse IP |
| Test de la robustesse de la confidentialité des communications liées au service de mise à jour |
| Test de la résistance du filtrage applicatif lors de l'utilisation d'un reverse proxy |
| Test de la résistance du filtrage applicatif lors de la fragmentation des paquets |

#### 2.3.9.2. Avis d'expert sur la résistance des mécanismes

Le pare-feu est efficace face à des attaques de type déni de service ou de saturation FTP. Par contre, il est vulnérable à une attaque par empoisonnement de cache ARP, ce qui l'empêche de router correctement le trafic (cette attaque est à minorer dans le sens où des contremesures simples peuvent être mises en place). Un test sur le filtrage applicatif a pu montrer qu'il est

aussi possible pour certaines applications, dans la configuration par défaut, de contourner le blocage en utilisant l'adresse IP du site web plutôt que son URL.

Sur la plateforme reconfigurée à l'aide du développeur, l'évaluateur a également pu montrer que le pare-feu souffre de faiblesses de détection face à des paquets réseaux segmentés au niveau TCP. Il est dans ce cas-ci possible de contourner le blocage dans une configuration n'offrant aucune protection contre cette attaque. Avec l'aide du développeur, l'évaluateur a identifié une configuration dans les guides permettant de se prémunir contre cette attaque par segmentation TCP.

### *2.3.10. Analyse des vulnérabilités (conception, construction…)*

#### 2.3.10.1. Liste des vulnérabilités connues

Les vulnérabilités publiques connues pour le produit ciblent des versions antérieures à celle évaluée et n'ont pu être testées par manque d'information sur les scénarios de reproduction des exploits associés.

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

Voir 2.3.9.2

### *2.3.11. Accès aux développeurs*

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

### *2.3.12. Analyse de la facilité d'emploi et préconisations*

#### 2.3.12.1. Cas où la sécurité est remise en cause

Moyennant le respect des recommandations évoquées ci-dessous, l'évaluateur n'a pas identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

#### 2.3.12.2. Recommandations pour une utilisation sûre du produit

La configuration par défaut du produit offre un niveau de protection faible. La configuration doit être maintenue à jour très régulièrement pour tenir compte des menaces existantes et à venir. Des connaissances avancées sont requises pour identifier de telles menaces et transcrire leur contexte d'application dans une règle ou une politique de sécurité. C'est pourquoi l'évaluateur recommande fortement l'assistance lors de la configuration du pare-feu par un intégrateur maîtrisant parfaitement les produits de la gamme *PA-Series.*

#### 2.3.12.3. Avis d'expert sur la facilité d'emploi

L'installation et la mise en route du produit sont aisées. Néanmoins, la configuration et la prise en main du produit pour une mise en œuvre efficace requièrent des connaissances avancées.

#### 2.3.12.4. Notes et remarques diverses

Néant.

## 2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.

## 2.5. Analyse du générateur d'aléas

Sans objet.

# 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 « Fonction de Filtrage du boîtier PA 2050, version logicielle 5.0.4 » 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 d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

# Annexe 1. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | *Cible de sécurité CSPN - Fonction de filtrage des boitiers pare-feux PA Series*<br>Référence : *PAO001-ST-1.02*<br>Version : *1.02*<br>Date : *21/05/2013* |
| [RTE] | *Rapport Technique d'Évaluation CSPN - Fonction de filtrage du boîtier PA-2050 version 5.0.4*<br>Référence : *CSPN-RTE-NIRZ2-2.00*<br>Version : *2.0*<br>Date : *03/10/2013* |
| [GUIDES] | Guides d'utilisation :<br>*Palo Alto Networks® - Guide de mise en route - PAN-OS 5.0*<br>Référence : *Getting_Started_Guide_PAN-OSv5.0_French*<br><br>*PA-2000 Series - Hardware Reference Guide*<br>Référence : *PA-2000_Hardware_Guide_RevF*<br><br>Guides d'administration :<br>*Palo Alto Networks - Guide de l'administrateur - Version 5.0*<br>Référence : *PA-5.0_Administrators_Guide_French*<br><br>*Palo Alto Networks - PAN-OS™ Command Line Interface - Reference Guide - Release 5.0*<br>Référence : *PAN-OS_5.0_CLI_Reference_Guide* |

# 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 (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011.<br><br>Documents disponibles sur www.ssi.gouv.fr |
| [GUIDES-ANSSI] | Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013.<br>Disponible sur www.ssi.gouv.fr/hygiene-informatique. |