PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2021/31

Pare-feu de nouvelle génération PA-5220 avec fonctionnalité App ID

Version 8.1.15

Paris, le 10 décembre 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2021/31**
Nom du produit **Pare-feu de nouvelle génération PA-5220 avec fonctionnalité App ID**
Référence/version du produit **Version 8.1.15**
Catégorie de produit **Pare-feu**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **PALO ALTO NETWORKS** 62 avenue Emile Zola - bâtiment A 92100 Boulogne-Billancourt
Développeur **PALO ALTO NETWORKS** 62 avenue Emile Zola - bâtiment A 92100 Boulogne-Billancourt
Centre d'évaluation **AMOSSYS** Immeuble le Ouessant 11 rue Maurice Fabre 35000 Rennes
Fonctions de sécurité évaluées Filtrage des flux réseau Journalisation Contrôle d'accès des utilisateurs Mises à jour sécurisées Sécurisation des flux d'administration
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Non (en bleu)

PREFACE

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est «Pare-feu de nouvelle génération PA-5220 avec fonctionnalité App ID, Version 8.1.15» développé par PALO ALTO NETWORKS.

Le produit est un pare-feu d'entreprise dit « nouvelle génération » (à identification applicative), commercialisé sous la forme d'une *appliance*. À la différence des pare-feus traditionnels qui bloquent les flux au niveau 2 à 4 de la couche OSI, la solution de PALO ALTO NETWORKS propose en outre une fonctionnalité d'identification des applications, des utilisateurs et du contenu du réseau de l'entreprise.

Il doit cependant être noté que le périmètre de la certification concerne le filtrage des niveaux 3 et 4, comme pour un pare-feu traditionnel, et ne porte donc pas sur le bon fonctionnement des composants spécifiques (App-ID permettant l'identification des applications, User-ID permettant l'identification des utilisateurs de ces applications et Content-ID permettant d'analyser le contenu de l'application). L'évaluation a en revanche étudié l'innocuité d'AppID, c'est-à-dire le risque qu'une potentielle vulnérabilité dans AppID permette d'entraver le fonctionnement du pare-feu et plus précisément le filtrage des niveaux 3 et 4.

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*

Produit	
Nom du produit	Pare-feu de nouvelle génération PA-5220 avec fonctionnalité App ID
Numéro de la version évaluée	8.1.15

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

- via l'interface *web* :
  - s'authentifier sur l'interface *web* du pare-feu,
  - vérifier le numéro de version dans l'onglet « *Dashboard* », encadré « *General Information* », champ « *Software Version* » ;
- via la CLI :
  - s'authentifier en SSH sur le pare-feu pour accéder à la CLI ;
  - entrer la commande show system info ;
  - vérifier le numéro de version indiqué après « sw-version ».

1.2.3 *Fonctions de sécurité*

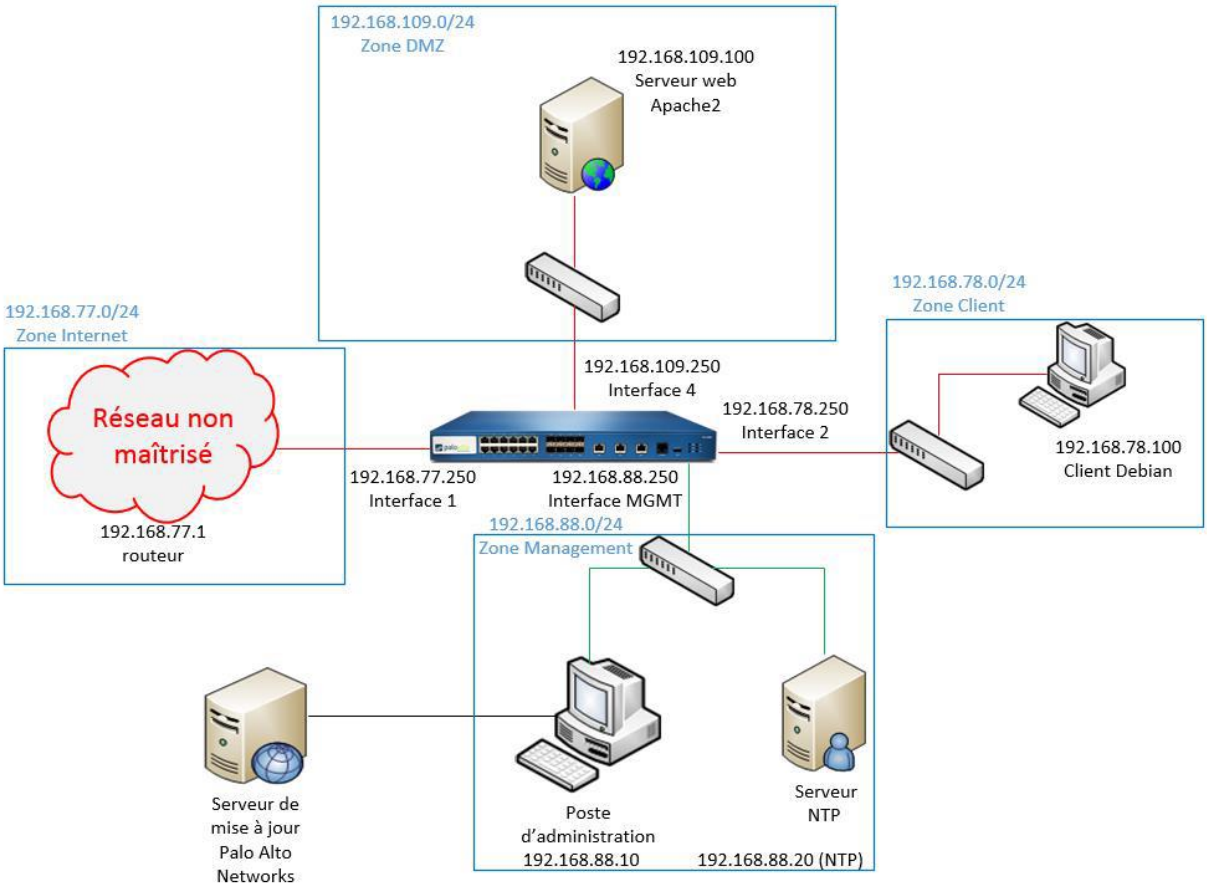
Les fonctions de sécurité évaluées du produit sont :

- le filtrage des flux réseau ;
- la journalisation ;
- le contrôle d'accès des utilisateurs ;
- les mises à jour sécurisées ;
- la sécurisation des flux d'administration.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à la configuration commerciale (sous forme d'*appliance*).

La plateforme de test est constituée des éléments suivants :



Cette plateforme est composée des postes suivants :

- un serveur web Apache2 version 2.4.25, installé sous Debian Stretch dans la DMZ ;
- un poste client sous Debian Stretch dans la zone client ;
- un serveur NTP sous Debian Stretch dans le VLAN de management ;
- un poste d'administration sous Windows Vista dans le VLAN de management.

La communication du VLAN Client et du VLAN DMZ avec l'extérieur s'effectue obligatoirement au travers du pare-feu.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

2.2 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 **Erreur ! Source du renvoi introuvable.**.

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

Le pare-feu a été livré sous forme d'*appliance*. Son installation a simplement consisté à relier les réseaux utilisés pour l'évaluation au boîtier.

L'évaluateur a ensuite effectué les étapes suivantes de configuration :
- activation du mode FIPS-CC ;
- création des zones ;
- adressage des interfaces ;
- configuration du *Virtual Router* ;
- configuration du NAT.

En plus de ces opérations, les opérations suivantes ont été effectuées afin de respecter les directives de [CDS] :
- suivi des bonnes pratiques de sécurité sur la protection de zone sur l'ensemble des zones de filtrage de la TOE (cf. [GUIDES], « *Best practices for securing your network from layer 4 and layer 7 evasions* ») ;
- désactivation du module IPS appelé « TP » ;
- suppression des signatures App-ID personnalisées.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

Le code source n'a pas fait l'objet d'une revue dans le cadre de cette l'évaluation.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

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

2.2.5 *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.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 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.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le **Erreur ! Source du renvoi introuvable.**.

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01]. Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

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 « Pare-feu de nouvelle génération PA-5220 avec fonctionnalité App ID, 8.1.15 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité **Erreur ! Source du renvoi introuvable.** pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et 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 **Erreur ! Source du renvoi introuvable.**, et suivre les recommandations se trouvant dans les guides fournis **Erreur ! Source du renvoi introuvable.**.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité - Pare-feu de nouvelle génération PA-5220 avec fonctionnalité App ID, version 8.1.15, référence CSPN-ST-PaloAlto_App-ID_Firewall, version 3.0.5, 6 août 2021.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Évaluation CSPN - Produit Pare-feu de nouvelle génération - version PA-5220, référence CSPN-RTE-PaloAlto_App-ID_Firewall-reprise, version 1.03, 26 octobre 2021.
[GUIDES]	Guides en ligne https://docs.paloaltonetworks.com/best-practices. En particulier : - *Best practices for securing administrative access* - https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/getting-started/best-practices-forsecuring-administrative-access.html - *Best practices for securing your network from layer 4 and layer 7 evasions* - https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-securing-your-network-from-layer-4-and-layer-7-evasions.html - *DoS and zone protection best practices* - https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices - *Zone protection profile* - https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/network/network-network-profiles-zone-protection.html (Pages consultées le 23 novembre 2021)

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 3.0, 12 avril 2021. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0, 6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.