Cible de sécurité CSPN

Fonction de filtrage des boitiers pare-feux PA Series

Référence : PAO001-ST-1.02

Date : le 21/05/2013

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

MAÎTRISE DU DOCUMENT

	SOCIETE	NOM	FONCTION	DATE	SIGNATURE
Contrôle technique	AMOSSYS	ACT	RTC	05/03/2013	[ORIGINAL SIGNE]
Contrôle qualité	AMOSSYS	JLR	RQCs	05/03/2013	[ORIGINAL SIGNE]
Approbation	AMOSSYS	ACT	RTC	21/05/2013	[ORIGINAL SIGNE]
Validation	PALO ALTO NETWORKS	Christophe ESTEBANEZ	Ingénieur Système	21/05/2013	[ORIGINAL SIGNE]

FICHE D'ÉVOLUTIONS

Révision	Date	Description	Rédacteur
0.10	25/01/2013	Création du document.	JLR
0.20	12/02/2013	Prise en compte des remarques de Palo Alto Networks.	JLR
0.30	15/02/2013	Modifications mineures.	JLR
1.00	22/02/2013	Modifications mineures suite aux remarques de Palo Alto Networks. Version diffusée à l'ANSSI.	JLR
1.01	05/03/2013	Prise en compte des remarques de l'ANSSI.	ALR
1.02	21/05/2013	Mise à jour de la version testée (chapitre 2)	ACT

SOMMAIRE

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation du pare-feu de nouvelle génération à identification applicative, développé par la société **Palo Alto Networks**, selon le schéma CSPN.

Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation de **Palo Alto Networks**. Les mises à jour de ce document sont effectuées par l'équipe projet d'**AMOSSYS**.

1.2. DOCUMENTS APPLICABLES

Ref.	Livrable
[CER-I-01.1]	*Méthodologie pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau.* N°1416/ANSSI/SR du 30 mai 2011.
[CER-I-02.1]	*Critères pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau.* N°1417/ANSSI/SR du 30 mai 2011.

1.1. GLOSSAIRE

Acronymes	Définitions
ACC	*Application Command Center*
CSPN	*Certification de Sécurité de Premier Niveau*
DoS	*Deny of Service*
NGFW	*Next Generation FireWall*
ST	*Security Target (Cible de sécurité)*
TOE	*Target Of Evaluation (Cible d'évaluation)*

2.IDENTIFICATION DU PRODUIT

Editeur	Palo Alto Networks
Lien vers l'organisation	http://www.paloaltonetworks.com/
Nom commercial du produit	*Appliance* PA-2050
Numéro de la version évaluée	Fonction de filtrage version 5.0.4
Catégorie du produit	Pare-feu

3. DESCRIPTION DU PRODUIT

3.1. DESCRIPTION GÉNÉRALE

Le produit est un pare-feu d'entreprise nouvelle génération à identification applicative commercialisé par la société **Palo Alto Networks** sous la forme d'une *appliance* et visant les entreprises de toute taille. À l'instar des pare-feu traditionnels qui bloquent les flux au niveau 2 et 4 de la couche OSI, la solution de **Palo Alto Networks** est destinée à sécuriser l'utilisation des applications de l'entreprise en identifiant les applications, les utilisateurs et le contenu du réseau de l'entreprise.

Pour cela, le produit intègre les trois technologies suivantes :

- **App-ID**, permettant l'identification des applications qui génèrent du trafic sur le réseau (indépendamment du port, du protocole, du chiffrement et de la technique évasive) ;
- **User-ID**, permettant l'identification des utilisateurs de ces applications ;
- **Content-ID**, permettant d'analyser le contenu de l'application pour y détecter d'éventuelles menaces, fichiers, schémas de données et activités Web.

Les informations statistiques d'identification et de filtrage permettent à un administrateur de créer des stratégies de sécurité en fonction du trafic qui traverse le réseau. Les réponses stratégiques peuvent être :

- 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 ;
    - etc.

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 (traitement et mémoire dédiés).

La figure ci-après présente l'architecture des pare-feux nouvelle génération de **Palo Alto Networks**.

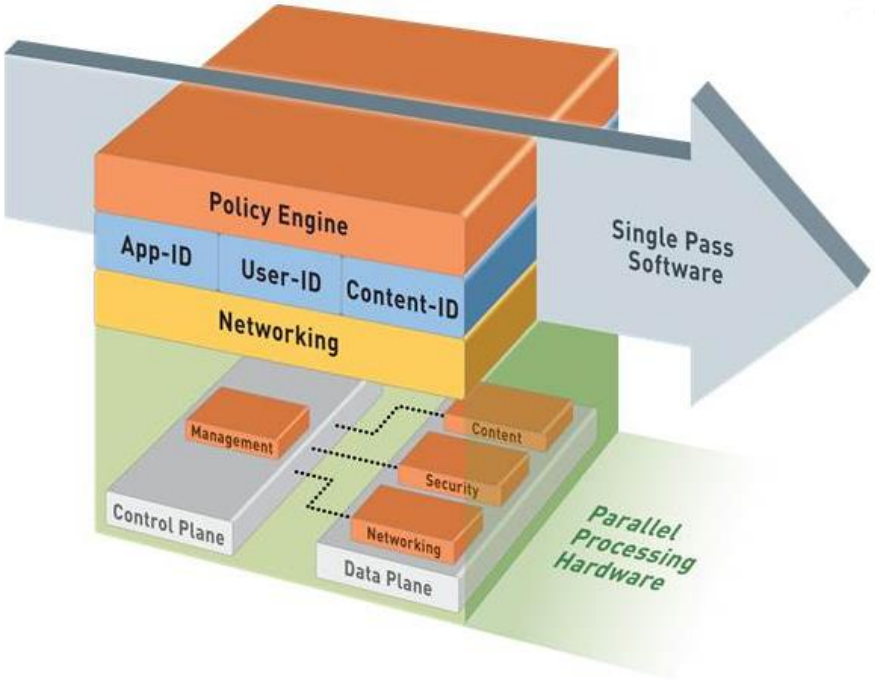

Figure 1 – Architecture des pare-feu nouvelle génération de Palo Alto Networks

3.2. DESCRIPTION DE LA MANIÈRE D'UTILISER LE PRODUIT

Le produit est destiné à contrôler l'utilisation des applications accédant au réseau d'une entreprise. Il assure notamment la prévention des intrusions, la protection anti-malware et le filtrage SSL. Il se base sur trois technologies « App-ID », « User-ID» et « Content-ID » pour identifier précisément une application, ses utilisateurs et son impact sur la sécurité.

Pour assurer ces fonctionnalités, le produit intègre :

- un **logiciel de filtrage** dynamique des flux en fonction :
  - des stratégies de sécurité spécifiées par l'administrateur ;
  - d'une liste d'URL autorisées[1] ;
  - du contenu des flux : les administrateurs peuvent mettre en œuvre des stratégies visant à réduire les risques liés à un transfert de fichiers ou de données ;
- un **module d'analyse** chargé d'identifier, à partir des flux autorisés qui transitent par le boîtier, les menaces et logiciels malveillants, au moyen :
  - d'un **système de prévention des intrusions** capable de détecter les failles de sécurité (connues et inconnues) du réseau, les vulnérabilités de la couche applicative, les dépassements de tampon, les attaques par refus de service ou par analyse de ports ;
  - d'un **antivirus réseau** permettant de bloquer les logiciels espions, y compris les virus PDF, les programmes malveillants dissimulés dans les fichiers compressés, dans le trafic Web (HTTP/HTTP compressé) ou qui circulent à travers des applications chiffrées ;
  - d'un **environnement de test virtuel** permettant d'exécuter les logiciels inconnus et de révéler une éventuelle menace.
- une **interface Web** permettant de visualiser l'activité des applications (ACC) et créer / déployer des stratégies de sécurité ;
- des outils de surveillance et de reporting.

Dans le cadre de l'évaluation CSPN, seules les fonctionnalités de filtrage à identification applicative (App-ID et User-ID) et d'administration du produit sont concernées par l'analyse.

[1] Les URL sont réparties en catégories (76 catégories disponibles) dans une base de données de filtrage des URL, permettant aux administrateurs d'appliquer des stratégies de navigation Web extrêmement précises.

3.3. DESCRIPTION DE L'ENVIRONNEMENT PRÉVU POUR SON UTILISATION

Palo Alto Networks propose plusieurs gammes de pare-feu de nouvelle génération :

- des équipements matériels (Séries PA-5000, PA-4000, PA-3000, PA-2000, PA-500 et PA-200 disposant chacun de modèles adaptés selon les besoins) ;
- des plateformes virtualisées (VM-100, VM-200, VM-300).

Les gammes diffèrent principalement en termes de performances (débits pare-feu, IPS, IPSec VPN), de capacité de virtualisation, de nombres d'interfaces et de politiques. La TOE et le système d'exploitation propriétaire, PAN-OS, sont embarqués dans ces produits.

Pour l'évaluation, le modèle PA-2050 est choisi (Figure 2).

La TOE est évaluée en tant que logiciel destiné à sécuriser l'utilisation des applications sur le réseau d'entreprise. Elle est démarrée au lancement de l'*appliance* PA-2050 et reste active jusqu'à son extinction.

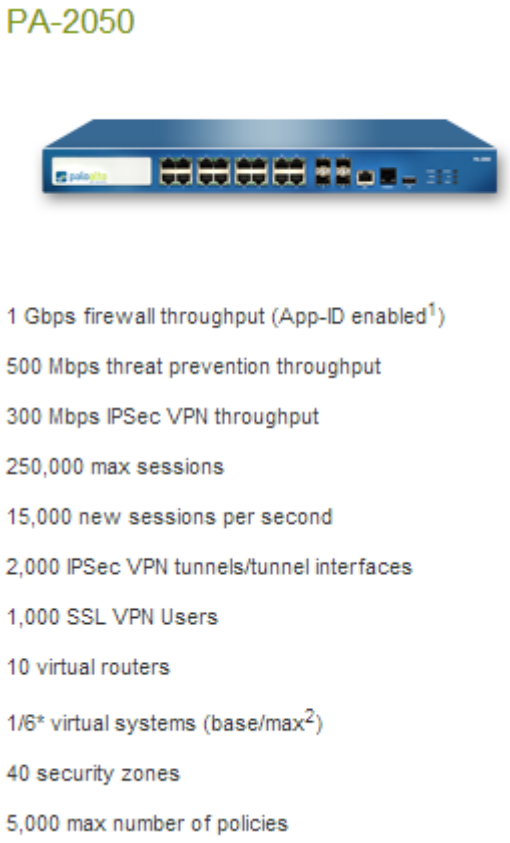

Figure 2 – Pare-feu de nouvelle génération (modèle PA-2050)

Quatre modes de fonctionnement sont possibles :

- en écoute : la TOE agit comme une sonde (connectée à un port mirroring) ;
- positionnée dans un carrefour stratégique du réseau : la TOE agit comme une passerelle de sécurité en coupure physique non intrusive de réseaux afin d'analyser tout le trafic entrant et sortant (optionnellement) d'un réseau local i.e. entre un réseau externe non maîtrisé (tel qu'Internet) et le réseau interne maîtrisé, de manière transparente et robuste, i.e. sans perte de paquet (Figure 3) ;
- en niveau 2 (couche liaison) ;
- en niveau 3 (couche réseau).

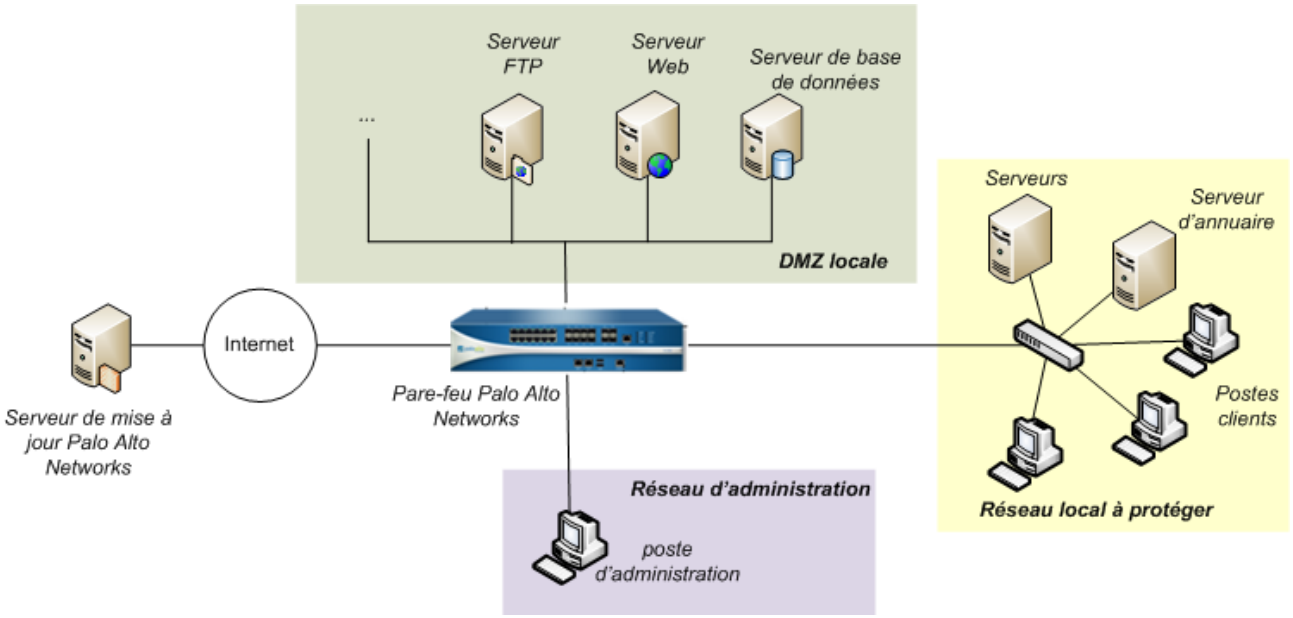

Figure 3 - Exemple d'architecture d'intégration du pare-feu Palo Alto Networks

3.4. DESCRIPTION DES HYPOTHÈSES SUR L'ENVIRONNEMENT

Les hypothèses sur l'environnement de la TOE sont les suivantes :

- **H.COUPURE**

  L'*appliance* est installée conformément à la politique d'interconnexion des réseaux en vigueur et est le seul point de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle des flux d'information.

- **H.SECURITE_PHYSIQUE**

  L'*appliance* est localisée dans un environnement physique sécurisé accessible des seules entités autorisées.

- **H.OS_SAIN**

  Toutes les dépendances nécessaires au fonctionnement de la TOE doivent être intègres. En particulier, le système d'exploitation support de l'*appliance* doit posséder des mécanismes de protection adéquats comme le contrôle d'accès et être à jour des correctifs en vigueur au moment de l'installation, sain et exempt de virus, chevaux de Troie, etc.

- **H.STATION_ADMIN**

  La station d'administration est sécurisée et maintenue à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées. Elle est installée dans un local à accès protégé et est exclusivement dédiée à l'administration de la TOE et au stockage des informations d'identification et de filtrage.

- **H.ADMIN_CONFIANCE**

  Les administrateurs en charge de la supervision sont des personnes non hostiles et compétentes, disposant des moyens nécessaires à l'accomplissement de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité.

- **H.POLITIQUE**

  La politique de contrôle des flux d'informations à mettre en œuvre est définie de manière complète, stricte et correcte. Autrement dit, tous les cas d'utilisation standards des équipements du réseau maîtrisé ont été envisagés lors de la définition des règles ; seuls les cas d'utilisation nécessaires des équipements sont autorisés ; les règles ne présentent pas de contradiction. En particulier, la configuration de la TOE doit évoluer dès qu'un changement est opéré dans le réseau local (configuration, augmentation/diminution du nombre d'hôtes ou des services, etc.).

3.5. DESCRIPTION DES DÉPENDANCES

La TOE est le logiciel de filtrage applicatif embarqué dans une *appliance* dédiée. Il n'y a donc aucune dépendance car celle-ci est livrée préconfigurée avec les éléments nécessaires à son fonctionnement.

3.6. DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNÉS

Le produit est totalement transparent pour les utilisateurs des réseaux à protéger.

Les rôles suivants seront pris en considération dans le cadre de l'analyse :

- ***Administrator :*** administrateur de l'*appliance* ayant un contrôle total sur le produit. Il a, entre autres, en charge la définition des stratégies de sécurité, la gestion des utilisateurs (rôles et droits d'accès) et le déploiement des mises à jour logicielles de la TOE ;
- ***Monitor :*** exploitant ayant en charge l'analyse des logs et alertes en sortie de la TOE et un accès en lecture à la configuration du pare-feu.

D'autres rôles et autorisations peuvent être définis pour les utilisateurs provenant du réseau d'administration mais ils ne seront pas considérés pour la présente évaluation.

3.7. DÉFINITION DU PÉRIMÈTRE DE L'ÉVALUATION

Les pare-feu de nouvelle génération de **Palo Alto Networks** se basent sur un traitement des flux en une seule passe dit « Single Pass Parallel Processing (SP3) » composé des trois briques principales « App-ID », « User-ID » et « Content-ID ».

La TOE se limite à l'application logicielle de filtrage à identification applicative (blocs orange et vert sur la Figure 4). Le module « Content-ID » est donc en dehors du périmètre de la TOE.

L'évaluation portera sur :

- le module « App-ID » de filtrage applicatif ;
- le module « User-ID» d'identification des utilisateurs ;
- la fonction de journalisation ;
- la fonction d'administration.

Est considéré hors TOE, le module « Content-ID » de détection des menaces.

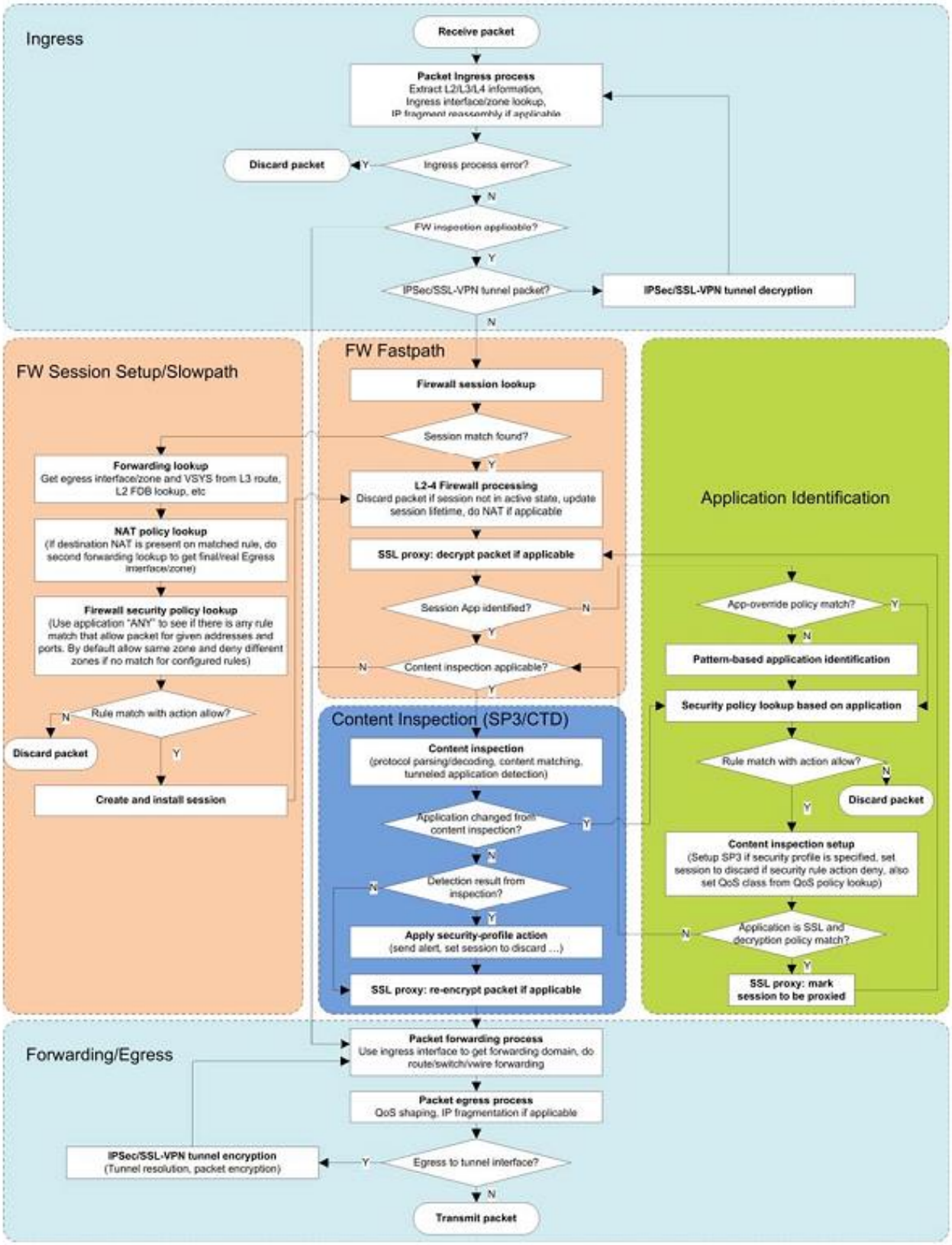

Figure 4 - Fonctionnement du pare-feu et périmètre de la TOE

La TOE est embarquée dans la plateforme matérielle PA-2050 installée au point de raccordement entre le réseau interne (maîtrisé) et le réseau externe (hostile) comme l'illustre la figure suivante.

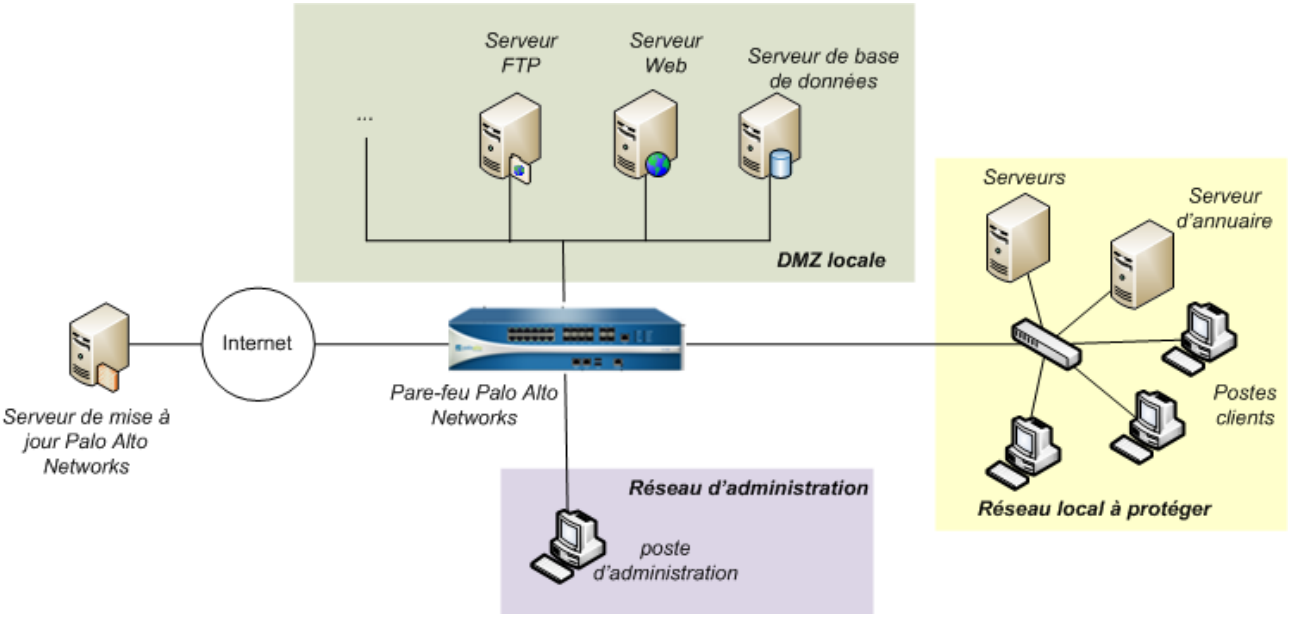

Figure 5 – Plateforme d'évaluation de la TOE

L'architecture proposée pour l'évaluation de la TOE comprend :

- la TOE (pare-feu nouvelle génération embarqué dans l'*appliance*) ;
- un *poste d'administrateur* pour la configuration, l'administration de la TOE et la visualisation des journaux ;
- un réseau local à protéger comprenant :
  - une DMZ contenant divers serveurs permettant de jouer différentes attaques lors de l'évaluation (attaques depuis l'extérieur sur *serveur web* Apache, *serveur FTP*, *serveur de base de données*, …);
  - un serveur d'annuaire permettant à la TOE d'identifier les utilisateurs (User-ID) ;
  - des *postes clients*.

4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

4.1. MATÉRIEL COMPATIBLE OU DÉDIÉ

La TOE est disponible sous forme d'*appliance* matérielle de différents types dimensionnée selon le débit (parefeu, IPS, IPSec VON), la capacité de virtualisation, les nombres d'interfaces et de politiques. Une version virtualisée est également disponible.

Pour l'évaluation, le modèle PA-2050 est choisi.

La TOE est incluse dans le boîtier PA-2050 livré par **Palo Alto Networks**.

4.2. SYSTÈME D'EXPLOITATION RETENU

La TOE est livrée avec son propre système d'exploitation qui est PAN-OS (système propriétaire orienté sécurité développé par **Palo Alto Networks**).

5.DESCRIPTION DES BIENS SENSIBLES

La fonction première de la TOE est de protéger le réseau local mais qui ne peut être considéré comme un bien sensible.

Les biens sensibles protégés par la TOE sont :

- **les données utiles au filtrage** :
  - les politiques de filtrage ;
  - la base de signatures applicatives ;
  - la base d'URL ;
  - les informations concernant les utilisateurs (dans le cas du module *User-ID*) ;
- **les paramètres de configuration** :
  - les fichiers de configuration et fichiers système de la TOE ;
  - les paramètres de sécurité propres à la TOE (en confidentialité et intégrité), dont les données d'authentification des *administrators* et *monitors* ;
- **les logs** générés par la TOE (i.e. les traces d'événements générés à l'issue d'une identification, d'un filtrage ou d'une modification de la politique du pare-feu).

Les biens sensibles protégés par l'environnement de la TOE sont :

- **les données utiles à la détection de menaces :**
  - la base de signatures virales ;
  - la base de vulnérabilités publiques.

6. DESCRIPTION DES MENACES

Les différents agents menaçants sont :

- attaquants internes : entités appartenant au réseau de confiance telles qu'un **utilisateur** ayant obtenu un accès illégitime à la TOE ;
- attaquants externes : entités n'appartenant pas au réseau de confiance telles que :
  - une **entité non autorisée** qui ne dispose pas d'accès légitime à la TOE ;
  - un **logiciel tiers** ne faisant pas partie de la TOE et qui cherche à introduire des attaques (virus ou dénis de service par exemple).

Les administrateurs ne sont pas considérés comme des attaquants.

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

- **M.CONTOURNEMENT**

  Une entité appartenant ou non au réseau de confiance parvient à contourner la politique de contrôle des flux d'informations.

- **M.EVENEMENT_NON_DETECTE**

  Une entité appartenant ou non au réseau de confiance parvient à masquer ses actions et compromettre les ressources sans être détectée (en provoquant la perte d'enregistrements d'audit ou en épuisant la capacité de stockage pour empêcher de futurs enregistrements).

- **M.ADMIN_ILLICITE**

  Une entité appartenant ou non au réseau de confiance parvient à effectuer des opérations d'administration illicites en mettant en défaut les données d'authentification ainsi que les paramètres de configuration de la TOE, ou en usurpant l'identité d'un administrateur suite à des tentatives aléatoires répétées, ou par le biais d'analyses de séquences d'authentification interceptées.

7. DESCRIPTION DES FONCTIONS DE SÉCURITÉ DU PRODUIT

Le produit ne permet pas directement d'assurer un besoin de sécurité en confidentialité ou intégrité sur un bien du SI à protéger. Il assure un besoin de disponibilité. En effet, la non-détection de menaces peut provoquer de graves conséquences sur la sécurité du réseau.

Par conséquent, le pare-feu contribue indirectement à la sécurité d'un système en sécurisant l'utilisation des applications. Les fonctions suivantes ne sont donc pas des fonctions de sécurité du point de vue de la TOE mais des fonctions de sécurité du point de vue du SI protégé par le pare-feu de **Palo Alto Networks**.

- **F1.FILTRAGE**

  La TOE applique un filtrage des flux d'informations transitant par le boîtier, en fonction des règles spécifiées dans la politique définie par l'administrateur.

- **F2.ANALYSE_FLUX**

  La TOE est capable d'identifier les paquets associés aux flux applicatifs transitant par le boîtier ainsi que les données incluses dans ces flux afin d'appliquer la politique de filtrage.

- **F3.IDENTIFICATION_UTILISATEUR**

  La TOE est capable d'identifier les utilisateurs d'applications. Pour cela, le produit maintient une table des utilisateurs en consultant de manière incrémentale et proactive les informations issues de différentes sources (logs de connexions des contrôleurs de domaine par exemple).

- **F4.JOURNALISATION**

  La TOE génère :

  - des évènements de sécurité relatifs au trafic IP transitant par le pare-feu et à la détection de menaces ;
  - des journaux relatifs aux modifications de la politique de sécurité du pare-feu.

  Ces traces sont journalisées localement ou envoyées vers un outil tiers distant (SIEM, archivage) de manière sécurisée.

- **F5.MISE_A_JOUR**

  La TOE 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.

- **F6.CONTROLE_ACCES**

  La TOE permet de contrôler l'accès aux fonctions qui relèvent de l'administration (gestion des stratégies, consultation des logs, accès aux données de configuration de la TOE, etc.) au moyen de rôles alloués aux utilisateurs autorisés. Les mots de passe des administrateurs sont hachés suivant le mécanisme MD5 et positionnés dans un fichier de configuration type xml, accessible uniquement par le Control Plane.

Fin du document

