Cible de sécurité CSPN

Pare-feu de nouvelle génération PA-5220 avec fonctionnalité App ID, version 8.1.15

Catégorie « Pare-Feu »

Référence : CSPN-ST-PaloAlto_App-ID_Firewall-3.0.5

Date : le 06/08/2021

Code interne : PAO002

Copyright AMOSSYS SAS

Siège : Immeuble Le Ouessant 3 ● 11 rue Maurice Fabre ● 35000 Rennes ● France ● www.amossys.fr

SIRET : 493 348 890 00051 ● **NAF** : 6202 A ● RCS Rennes B 493 348 890 ● SAS au capital de 38.000 Euros

SOMMAIRE

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], de l'*Appliance* Pare-Feu PA-5220 avec la fonctionnalité « App ID », développé par la société *Palo Alto Networks*.

La TOE[3] considérée est le pare-feu de nouvelle génération de *Palo Alto Networks* utilisant la fonctionnalité de filtrage « App ID », configurée en mode FIPS-CC.

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. IDENTIFICATION DU PRODUIT

Éditeur	**Palo Alto Networks** 3000 Tannery Way Santa Clara, CA 95054 Etats Unis d'Amérique
Lien vers l'organisation	https://www.paloaltonetworks.fr
Nom commercial du produit	Firewall PA-5220
Numéro de la version évaluée	PAN-OS version 8.1.15
Catégorie du produit	Pare-Feu

1.3. RÉFÉRENCES

Pour l'établissement de la présente cible de sécurité, les documents suivants ont été consultés :

[1] App-ID Tech Brief (https://www.paloaltonetworks.com/resources/techbriefs/app-id-tech-brief)

[2] Packet Flow Sequence in PAN-OS (https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081)

[3] Single Pass Parallel Processing Architecture whitepaper (https://www.paloaltonetworks.com/resources/whitepapers/single-pass-parallel-processing-architecture)

[4] PA-5200 Series description (https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-5200-series.html)

[1] Certification de Sécurité de Premier Niveau
[2] Agence nationale de la sécurité des systèmes d'information
[3] *Target Of Evaluation*

2. DESCRIPTION DU PRODUIT

2.1. 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 toutes tailles. À la différence 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.

La figure suivante (issue de [3]) présente le principe général de traitement du trafic :

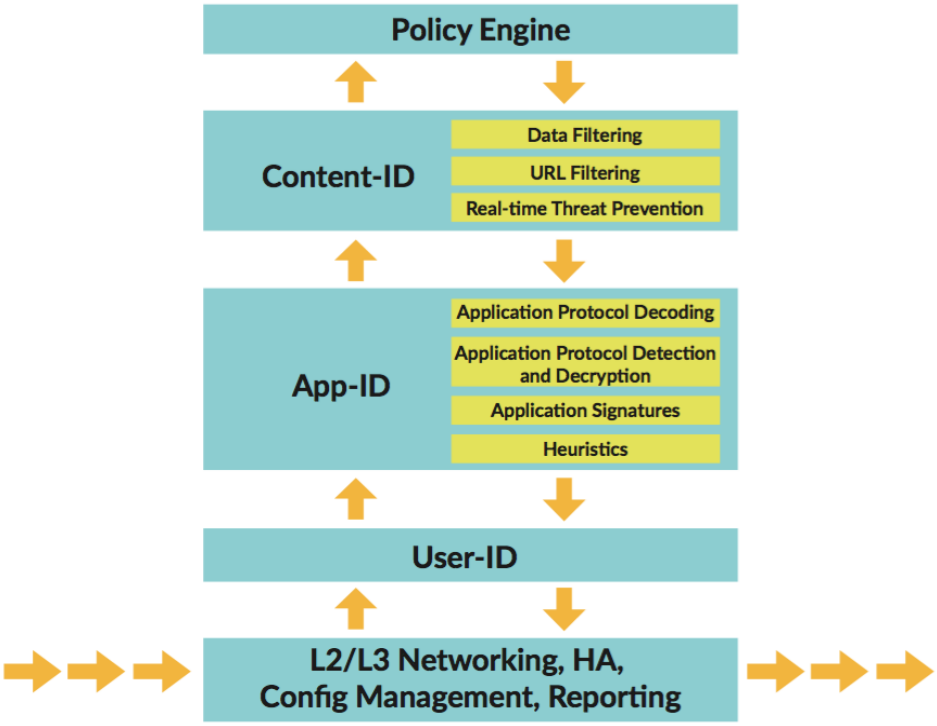

Figure 1 - Principe général de traitement du trafic

Les informations journalisées d'identification et de filtrage permettent à un administrateur de créer des stratégies de sécurité en fonction du trafic applicatif qui traverse le réseau. Les actions peuvent être, selon les choix de configuration :

- Autoriser le trafic ;
- Autoriser le trafic et rechercher des menaces, vulnérabilités et virus connus par *Palo Alto Networks*, ou analyser des fichiers potentiellement malveillants pour les identifier comme nouvelle menace ;
- Déchiffrer, décompresser et inspecter le trafic si nécessaire ;

- Refuser/bloquer le trafic (par exemple, refuser tout trafic en provenance de clients ou serveurs attribués à des utilisateurs, zones, réseaux, catégories de contenus, ou pays spécifiques) ;
- Autoriser certaines applications ou fonctions, par exemple :
    - autoriser l'utilisation de IRC et Google Talk mais bloquer l'utilisation de leurs fonctions respectives de transfert de fichiers,
    - bloquer des applications indésirables comme le partage de fichier P2P (Bittorrent, eMule, Gnutella, …),
    - rendre certaines applications « lecture uniquement » (exemple : Facebook, Twitter, DNP3, Siemens S7, Modbus, …),
    - etc.

La figure suivante présente l'architecture des pares-feux de nouvelle génération développés par *Palo Alto Networks* :

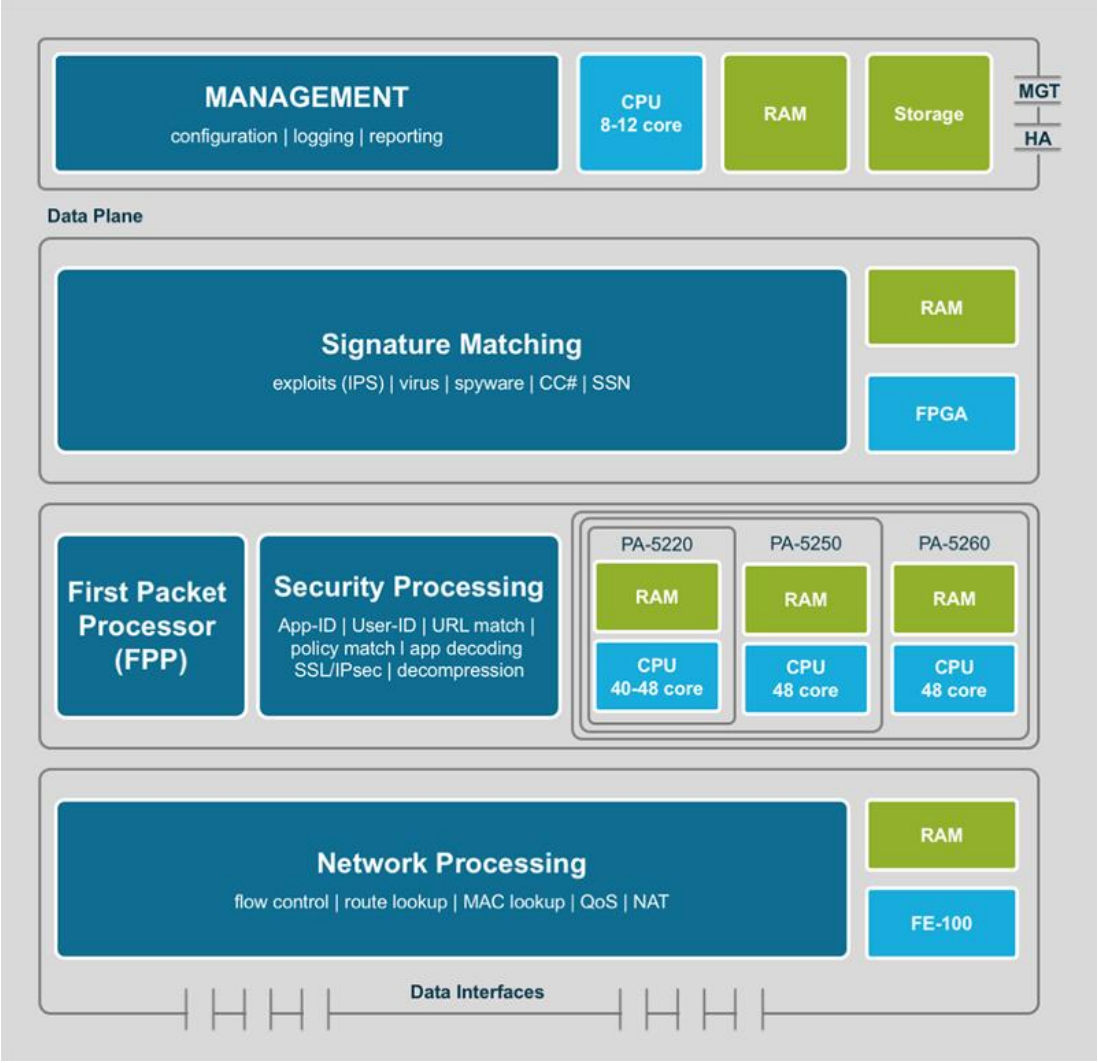

Figure 2 - Architecture des pare-feux de nouvelle génération de Palo Alto Networks

2.2. PRINCIPE DE FONCTIONNEMENT

Le produit est destiné à contrôler l'utilisation des applications accédant au réseau d'une entreprise. Il peut également assurer la prévention des intrusions ou attaques en déni de service, la protection anti-virus/anti-malwares (connus et à découvrir) et le filtrage SSL/TLS/SSH. Il se

base sur les trois technologies « App-ID », « User-ID » et « Content-ID » développées intégralement par *Palo Alto Networks* pour identifier précisément une application, ses utilisateurs et son impact sur la sécurité.

Pour assurer ces fonctionnalités, le produit intègre dans son logiciel PAN-OS:

- Un **module de filtrage** des flux en fonction :
  - des stratégies de sécurité spécifiées par l'administrateur,
  - de listes d'URL autorisés/interdits, utilisées par Content-ID, administrée par *Palo Alto Networks* ou gérée localement,
  - 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 à activer spécifiquement** 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 ;
- Une **interface SSH** permettant d'administrer la solution ;
- Des outils de surveillance et de génération de rapports, d'alarmes, d'alertes ;
- L'envoi de statistiques d'utilisation à Palo Alto Networks (fonctionnalité désactivée par défaut).

En effet, pour sécuriser les applications transitant par le réseau, les pare-feu nouvelle génération développés par *Palo Alto Networks* utilisent la fonctionnalité App-ID, éventuellement complété par le filtrage d'URL PAN-DB pour donner une visibilité sur l'application et les services Web afin de protéger un système d'information contre un éventail complet de risques légaux, réglementaires, de productivité et d'utilisation des ressources.

La fonctionnalité App-ID permet la visibilité des applications sur le réseau, pour permettre aux administrateurs d'identifier le comportement des applications, de comprendre leur fonctionnement et comprendre leurs caractéristiques comportementales pour déterminer leur risque relatif. Cette connaissance de l'application permet de créer et d'appliquer des règles de stratégie de sécurité pour autoriser, inspecter et ralentir/accélérer les applications souhaitées, tout en bloquant les applications indésirables. Lorsque des règles de stratégie sont définies pour autoriser le trafic, App-ID commence à identifier tout le trafic sans aucune configuration supplémentaire.

App-ID est un système breveté de classification de trafic (disponible uniquement dans le logiciel PAN-OS pour les pare-feux nouvelle génération de *Palo Alto Networks*) qui attribue les sessions réseau aux applications, indépendamment du port, du protocole, du chiffrement (SSH ou SSL) ou de toute autre tactique évasive utilisée par celle-ci. Cette fonctionnalité applique plusieurs mécanismes de classification au flux de trafic réseau pour identifier avec précision les applications par signatures d'application, par décodage de protocole d'application ou par heuristique.

App-ID identifie les applications traversant l'*appliance* de la façon suivante :

1. Le trafic est comparé à la politique pour vérifier s'il est autorisé sur le réseau surveillé.
2. Les signatures sont ensuite comparées au trafic autorisé pour identifier l'application en fonction de propriétés uniques d'application et des caractéristiques de la transaction associée. La signature détermine également si l'application est utilisée sur son port par défaut ou si elle utilise un port non standard. Si le trafic est autorisé par la stratégie, le trafic est ensuite potentiellement analysé pour détecter les menaces (via le module TP, TP est désactivé dans la version évaluée du produit) et continue d'être analysé pour identifier l'application de manière plus détaillée.
3. Si App-ID détermine que le chiffrement (SSL ou SSH) est en cours d'utilisation et qu'une règle de déchiffrement est configurée, la session est déchiffrée et les signatures d'application sont appliquées de nouveau sur le flux déchiffré.
4. Les décodeurs pour les protocoles connus sont ensuite utilisés pour rechercher des signatures contextuelles supplémentaires permettant de détecter d'autres applications qui peuvent être encapsulées à l'intérieur du protocole (par exemple, « Yahoo! Instant Messenger » utilisé sur HTTP). Les décodeurs valident que le trafic est conforme à la spécification du protocole et fournissent un support pour la traversée NAT et l'ouverture des trous d'emplacement dynamiques (*dynamic pinholes*) pour des applications telles que SIP et FTP.
5. Pour les applications qui sont particulièrement évasives et qui ne peuvent être identifiées grâce à une analyse de signature et de protocole, une analyse heuristique peut être utilisée pour déterminer l'identité de l'application (par exemple, Bittorrent, Skype).
6. Lorsque l'application est identifiée, la vérification de la politique détermine comment traiter l'application (bloquer ou autoriser) et éventuellement analyser les menaces, inspecter les transferts de fichiers non autorisés et les formats de données, ou optimiser à l'aide de règles de QoS (*Quality of Service*).

La figure suivante (issue de [1]) présente le principe de classification du trafic par App-ID :

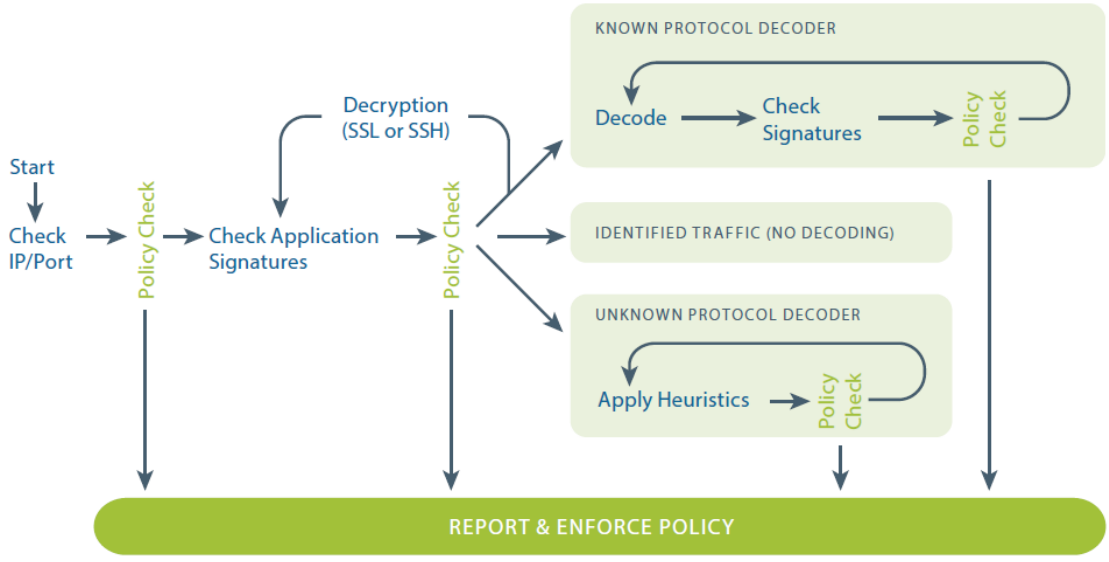

Figure 3 - Principe de classification du trafic par App-ID

La figure suivante (issue de [2]) présente le principe global de réception/analyse/transmission du trafic :

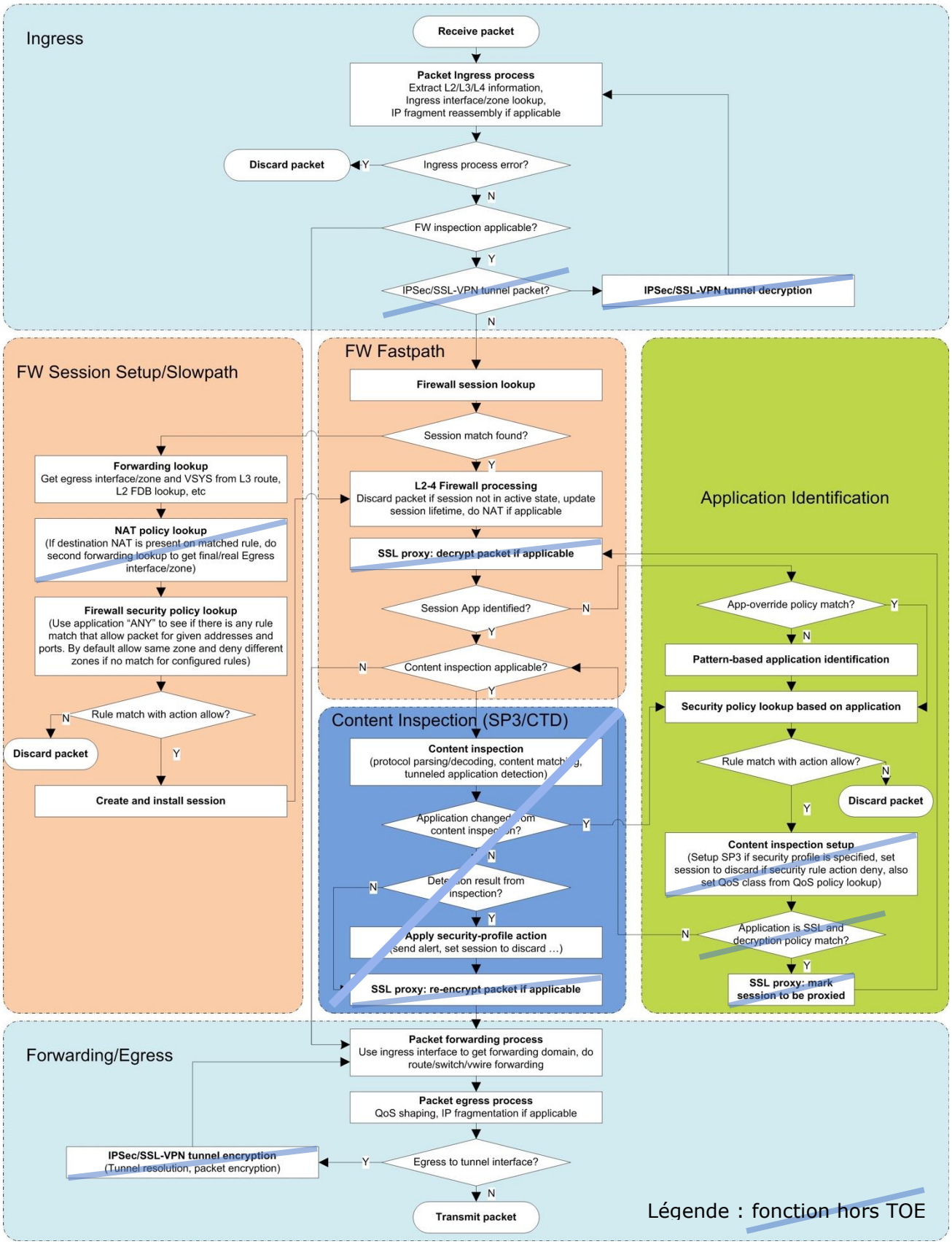

Figure 4 - Principe global de réception/analyse/transmission du trafic

Les traitements Ingress, FW Session Setup/Slowpath, FW Fastpath, Application Identification, Forwarding/Egress sont réalisées par le Data Plane par traitement logiciel et matériel spécifique.

Dans le cas où une application ne pourrait pas être détectée, l'utilisateur dispose de deux possibilités :

- Dans le cas d'une application commerciale, il peut capturer le trafic réseau et l'envoyer à *Palo Alto Networks* pour que des décodeurs spécifiques soient développés ;
- Dans le cas d'une application interne, il peut développer ses propres signatures applicatives en se basant sur les décodeurs accessibles afin que ces flux soient analysés ; Ces signatures personnalisées devront être mutuellement exclusives de toutes les autres signatures App-ID officielles (fournies par défaut par Palo Alto Networks) pour se prémunir d'une utilisation erronée d'App-ID voire son exploitation à des fins malicieuses. En effet, c'est la première signature identifiée dans un trafic donné qui sera celle retenue. Toutes les autres signatures de la liste, qui potentiellement pourraient correspondre au trafic mais qui sont analysées avec une priorité inférieure, ne seront pas retenues.

  Dans le cadre de cette évaluation, il est à noter que la création de signatures applicatives personnalisées n'est pas incluse dans la TOE.

Il est rappelé que, dans le cadre de l'évaluation CSPN, seule la fonctionnalité de filtrage à identification applicative (App-ID) est concernée par l'analyse. Néanmoins, il existe différents moteurs complémentaires comme TP (Threat Prevention), qui ont pour but notamment de protéger un serveur contre une attaque d'un client malveillant (par exemple via des injections de code, ce code pouvant être lui-même encodé).

2.3. DESCRIPTION DES DÉPENDANCES

Le produit est une *Appliance* dédiée dont le système d'exploitation (PAN-OS) est propriétaire et utilise une base Linux (Red Hat). D'autres outils open-source sont installés et distribués avec l'*Appliance* et sont listés sur https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings/pan-os-oss-listings/pan-os-8-1-open-source-software-oss-listing. La librairie SSL utilisée pour les fonctions de sécurité relatives à l'administration du produit devra être évaluée comme une librairie propriétaire (PANW-SSL).

L'administration de l'*Appliance* est réalisée depuis des réseaux et poste d'administration dédiés et isolés, connectés à l'interface dédiée d'administration. Le pare-feu nécessite également un accès à un serveur NTP et un serveur DNS depuis cette même interface. L'administration est généralement réalisée en utilisant les protocoles SSH ou HTTPS.

2.4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

Les pare-feux de nouvelle génération développés par *Palo Alto Networks* sont disponibles sous forme d'*Appliance* matérielle dimensionnée selon le débit, la capacité de virtualisation, les nombres d'interfaces et de politiques. Une version entièrement logicielle (VM) est également disponible.

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

- Des équipements matériels (séries PA-7000, PA-5200, PA-3200, PA-800 et PA-220 disposant chacun de modèles adaptés selon les besoins) ;
- Des plateformes virtualisées (VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000HV) utilisant les mêmes logiciels que les équipements matériels ;
- Des instances disponibles dans l'informatique en nuage (VMware ESXi, VMware NSX, Amazon Web Services, Azure, KVM, OpenStack, …).

Les gammes diffèrent principalement en termes de performances (débits pare-feu, sessions simultanées, IPS, IPSec VPN), de capacité de virtualisation d'administration, du nombre d'interfaces et de politiques configurées. Le logiciel PAN-OS est disponible simultanément pour toute la gamme matérielle et logicielle, ainsi que les mises à jour.

2.5. PÉRIMÈTRE DE L'ÉVALUATION

Le système à évaluer (la TOE) sera uniquement constituée du module d'administration intégré et de la fonction « App-ID ». Toutes les autres fonctionnalités seront désactivées pendant l'évaluation. Précisément ne seront pas activées : identification ou authentification des utilisateurs des flux à traiter, fonctions de chiffrement/déchiffrement des flux à filtrer, catégorisation dynamique des destinations des flux (filtrage d'URL), identification des menaces liées aux contenus (virus, malware, vulnérabilités).

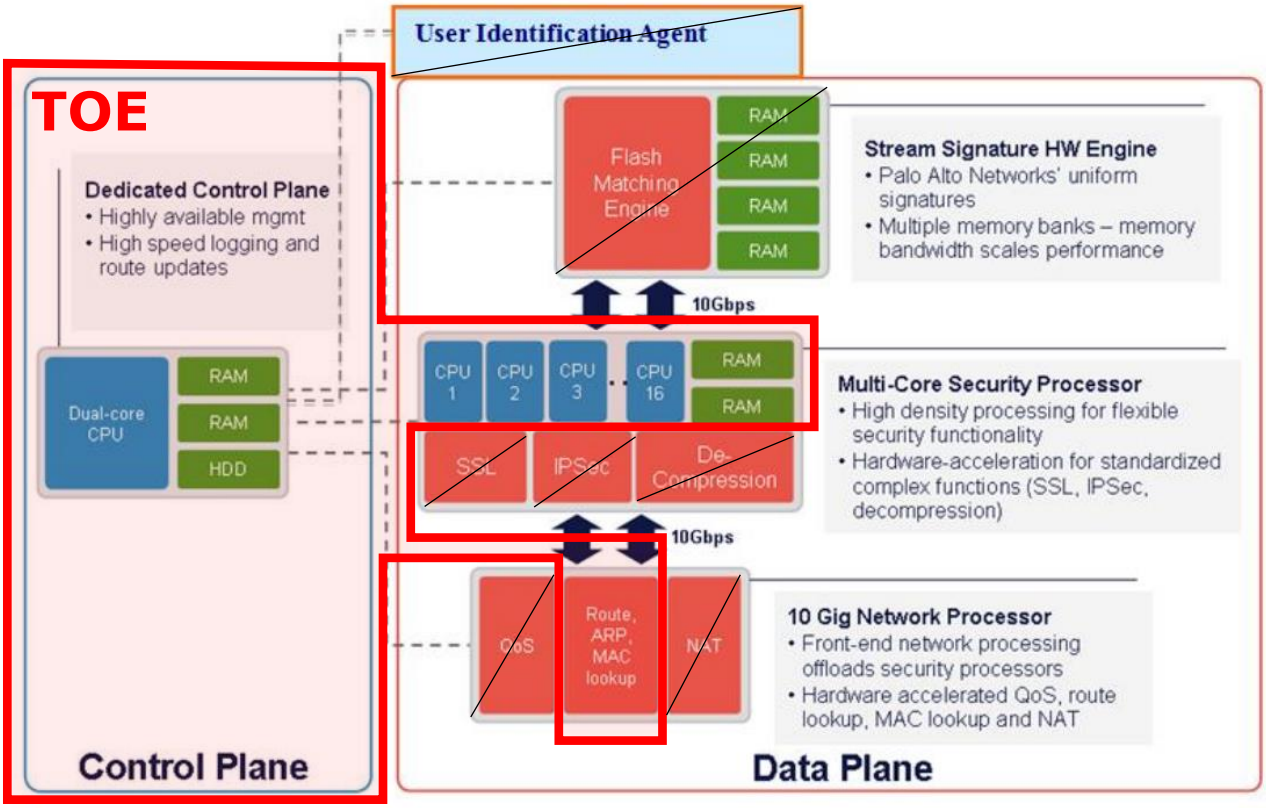

Figure 5 - Architecture de la TOE

La plateforme d'évaluation sera composée d'une *Appliance* PA-5220 déployée au sein d'un réseau local d'évaluation. **Le mode FIPS-CC sera activé sur l'*Appliance***.

L'*Appliance* PA-5220 sera mise en place entre différentes zones :

- Une DMZ hébergeant des services publics, accessible depuis le réseau non maîtrisé ;
- Un réseau local avec accès au réseau non maîtrisé et à la DMZ, mais inaccessible depuis le réseau non maîtrisé ;
- Un poste d'administration (Windows 10, dernière version Google Chrome) connecté à un réseau d'administration disposant uniquement d'un accès à l'interface d'administration dédiée de l'*Appliance* (interface "MGT" sur la figure 2) ou d'un accès par le port série disponible sur l'*Appliance* ;
- Un réseau non maîtrisé.

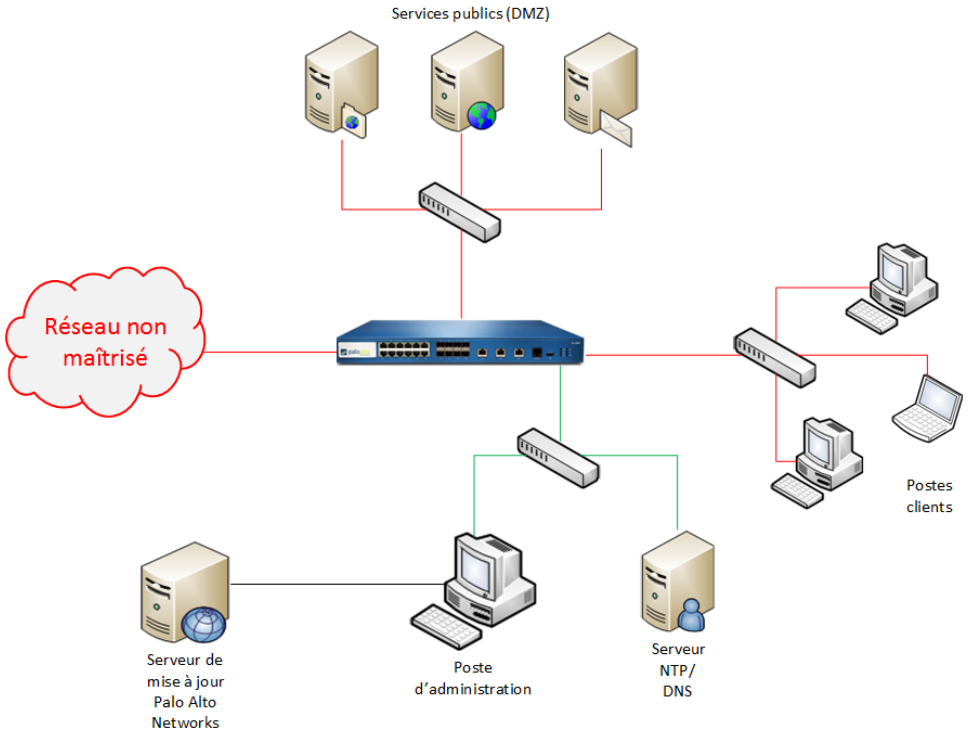

Figure 6 – Plateforme d'évaluation

Les flux réseaux identifiés sont les suivants :

- Les flux en vert sont les flux connectés aux interfaces d'administration ;
- Les flux en rouge sont les flux connectés aux interfaces de collecte et d'analyse.

La TOE évaluée devra se conformer à l'application des bonnes pratiques de sécurité pour la configuration, en suivant les recommandations suivantes : 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) :

- mettre en place une protection par zone sur l'ensemble des zones ;
- rejeter les paquets malformés ;
- rejeter les applications inconnues ;
- mettre en place un profil de protection pour bloquer les anomalies protocolaires ;
- etc.

Il est à noter que la certification ne vise pas à évaluer le bon fonctionnement d'AppID ni sa complexité d'utilisation.

3. PROBLÉMATIQUE DE SÉCURITÉ

3.1. DESCRIPTION DES UTILISATEURS TYPIQUES

Par définition, les utilisateurs concernent les personnes et services applicatifs qui interagissent avec le produit évalué.

Les rôles suivants sont prédéfinis et doivent être pris en considération dans le cadre de l'évaluation de sécurité :

- ***Superuser :*** utilisateur disposant de tous les privilèges sur le produit. Il est donc en mesure de réaliser toutes les opérations de gestion, de maintenance, d'ajout d'utilisateurs et d'analyse des fonctions ;
- ***Superuser (read-only)*** : accès en lecture à toutes les fonctionnalités du *Superuser* ;
- ***Device Administrator*** : utilisateur disposant de tous les privilèges sur le produit, sauf la création de nouveaux comptes utilisateurs ;
- ***Device Administrator (read-only)*** : accès en lecture à toutes les fonctionnalités du *Device Administrator*.

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. Pour les besoins de la problématique de sécurité d'un équipement de type pare-feu, un cinquième besoin de sécurité est rajouté : le non-rejeu.

L'*appliance* PA-5220 contribue à protéger les biens sensibles suivants du système surveillé, sous réserve d'une politique de contrôle des flux correctement définie et 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 réseaux.

  Besoin de sécurité : disponibilité.

Les biens protégés par la TOE sont les suivants :

- **B.SERVICES**

  Services proposés par les machines du(des) réseau(x) de confiance et accessibles depuis les autres zones réseaux, les logiciels en écoute et leur configuration.

  Besoin de sécurité : disponibilité, intégrité.

- **B.TOPOLOGIE**

  Informations de topologie du(des) réseau(x) de confiance.

  Besoin de sécurité : confidentialité.

D'autres biens sensibles, propres à la TOE ou son environnement, doivent également être considérés :

- **B.CONFIGURATION**

  Ensemble des données d'authentification et d'identification des utilisateurs, les éléments cryptographiques (certificats, clés, etc.) ainsi que la gestion de leurs droits d'accès et la configuration de la fonctionnalité App-ID : règles de filtrages, base de signatures applicatives, politiques à appliquer, etc.

  Besoin de sécurité : disponibilité, intégrité, confidentialité[4].

- **B.JOURNAUX**

  Ensemble des traces (événements, alertes, alarmes, etc.) générées localement par la fonctionnalité App-ID. Ces traces concernent la gestion de l'*appliance* (authentifications et actions des utilisateurs) ainsi que les traces générées par le filtrage. Les journaux sont générés localement et ne sont pas envoyés à des collecteurs distants.

  Besoin de sécurité : intégrité, confidentialité, disponibilité.

- **B.FLUX_ADMINISTRATION**

  Flux d'administration de l'*appliance*.

  Besoin de sécurité : intégrité, confidentialité, non-rejeu, authenticité.

- **B.MISES_À_JOUR**

  Mises à jour du logiciel contenu dans l'*appliance*.

  Besoin de sécurité : authenticité, intégrité, confidentialité.

3.3. DESCRIPTION DES HYPOTHÈSES 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 suivantes doivent être considérées :

- **H.PERSONNEL**

  La TOE est administrée par du personnel compétent, non hostile et correctement formé à son utilisation, respectant les guides et procédures.

- **H.SERVICES_ADDITIONNELS**

  Seule la fonctionnalité « App-ID » est activée, tous les autres services non-requis par celle-ci sont donc désactivés. Cette hypothèse concerne notamment la désactivation des services additionnels tels que User-ID, Content-ID, antivirus, etc.

- **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 filtrage. De même, l'*appliance* déployée est liée au dimensionnement du système et des flux à surveiller. L'évaluation porte sur le déploiement d'un seul équipement (aucune redondance n'est testée).

[4] La confidentialité est uniquement mise en place pour les paramètres de sécurité dans les fichiers de configuration (tout le fichier n'est pas chiffré).

- **H.LOCAL_SÉCURISÉ**

  L'*Appliance* est déployée dans un local dont les accès sont nominativement contrôlés et restreints.

- **H.RÉSEAU_ADMIN_DÉDIÉ**

  L'administration de l'*Appliance* est effectuée à partir d'un réseau séparé et dédié. Ce réseau permet l'administration courante de la TOE ainsi que les flux NTP/DNS et le déploiement de mises à jour via l'interface Web d'administration.

- **H.POSTE_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 ainsi qu'au stockage des informations d'identification et de filtrage.

- **H.RÉSEAU_ADMIN_DE_CONFIANCE**

  Le réseau d'administration de la TOE est considéré comme étant de confiance.

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 à considérer pour l'évaluation de sécurité doivent être les suivants :

- **utilisateur non autorisé** (attaquant humain ou entité informatique) qui interagit avec l'*appliance* mais qui ne dispose pas d'accès légitime ;
- **utilisateur autorisé** disposant d'accès restreints sur l'*appliance*.

Les administrateurs (rôle *Superuser* disposant de tous les privilèges sur la TOE) 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 ou 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 maîtrisé, arrive à leurrer la fonctionnalité de filtrage (la TOE) pour accéder au SI du réseau surveillé.

- **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 maîtrisé.

- **M.ALTÉRATION**

  Un attaquant, situé sur le réseau non maîtrisé, le réseau d'administration le réseau local, altère (modification ou suppression) des biens sensibles en intégrité de la TOE.

- **M.EXFILTRATION**

  Un attaquant, situé sur le réseau non maîtrisé, le réseau d'administration le réseau local, parvient à prendre connaissance des biens sensibles en confidentialité de la TOE.

- **M.MITM_ADMIN**

  Un attaquant, situé sur le réseau d'administration, se place en homme-du-milieu entre l'*appliance* et le poste administrateur afin de porter atteinte aux données transitant sur ce lien.

- **M.ÉLÉVATION_PRIVILÈGES**

  Un attaquant, situé sur le réseau d'administration et disposant d'un accès restreint à la TOE, réussit à élever ses privilèges.

- **M.ADMIN_ILLICITE**

  Un attaquant, situé sur le réseau non maîtrisé ou le réseau local et ne disposant pas d'accès à la TOE, parvient à effectuer des opérations illicites d'administration.

- **M.ÉVÉNEMENTS_NON_DETECTÉS**

  Un attaquant, situé sur le réseau non maîtrisé, le réseau d'administration ou le réseau local, parvient à masquer ses actions (en provoquant la perte d'enregistrements d'audit ou en épuisant la capacité de stockage pour empêcher de futurs enregistrements) et compromettre les ressources sans être détecté.

- **M.VOL_PARE_FEU**

  Un attaquant parvient à voler l'équipement contenant la TOE et à accéder à des informations protégées en confidentialité sans ouvrir l'*appliance*.

3.5. DESCRIPTION DES FONCTIONS DE SÉCURITÉ

Par définition, les fonctions de sécurité sont l'ensemble des mesures techniques et mécanismes mis en œuvre dans 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.FILTRAGE**

  Fonction de contrôle des flux applicatifs du trafic traversant l'*appliance*. 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 :

  - adresses source et destination ;
  - protocole de la couche transport ;
  - protocole de la couche application ;
  - ports source et destination ;
  - interface sur laquelle le paquet arrive ;
  - application utilisée.

  Le type d'application utilisée est déterminé via divers mécanismes internes à la TOE, présentés au §2.2 de ce document. Ces mécanismes font partie intégrante du moteur d'analyse et de filtrage.

- **F.JOURNALISATION**

  La TOE permet de générer des enregistrements d'audit des événements de sécurité relatifs au trafic applicatif transitant sur la TOE ainsi que des enregistrements d'audit des

modifications de la politique de sécurité du pare-feu, de la gestion de l'*appliance* (authentification et actions des administrateurs).

Les journaux sont stockés localement (sur l'*appliance*) dans une partition spécifique et dans un format propriétaire binaire. Ils sont visualisés à la demande via le poste d'administration dédié, et un contrôle d'accès logique mis en place par le système de fichiers permet de garantir leur confidentialité[5]. Des mécanismes de rotation des journaux sont mis en place par la TOE et configurés par les administrateurs.

- **F.CONTRÔLE_ACCÈS**

Les utilisateurs accèdent au moteur du pare-feu via la page d'administration dédiée, ou par l'accès SSH. Celle-ci fournit l'interface 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.

La TOE permet d'identifier et d'authentifier nominativement les utilisateurs déclarés à accéder au système et de leur attribuer des droits en fonction de leur rôle. Les utilisateurs peuvent s'authentifier en utilisant plusieurs modes (login/mot de passe, certificat, service tiers (radius, ldap, tacacs) : https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/firewall-administration/manage-firewall-administrators/administrative-authentication#idb2facbe5-5a97-4531-b655-1d41a9658953). Seuls les modes d'authentification par mot de passe et par certificat seront testés (*Local, Certificates*).

- **F.MISES_À_JOUR_SÉCURISÉES**

La TOE dispose d'un mécanisme de mise à jour logicielle et de la base des signatures applicatives lui permettant d'identifier les applications à l'origine des flux. Ces mises à jour sont effectuées depuis le réseau d'administration dédié.

Les mises à jour sont chiffrées (AES-256) et signées (RSA-2048). Sur le site web support.paloaltonetworks.com, il est possible de récupérer les binaires des mises à jour et de vérifier manuellement les hachés (aux formats MD5 et SHA256). Lorsque l'appliance reçoit un fichier de mise à jour, PAN-OS vérifie la signature et déchiffre les mises à jour en cas de succès de la vérification.

- **F.FLUX_ADMIN_SÉCURISÉS**

Les actions d'administration de la TOE peuvent être réalisées en ssh, ou au travers de la console Web.

Dans le cas où le mode FIPS-CC est activé (activé dans le cadre de l'évaluation[1]), les communications (flux d'administration en ligne de commande) sont réalisées en utilisant SSHv2. Pour la clé du serveur, par défaut une clé RSA 2048 est générée, modifiable par l'administrateur (conformément aux spécifications cryptographiques). Concernant les algorithmes de chiffrement, ils sont tous acceptés par défaut (de par la configuration en mode FIPS-CC du SSH) ;

Cf. https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3133.pdf). A cet égard, nous recommandons :

· aes-256gcm@openssh.com pour le chiffrement/intégrité
· ecdh-sha2-nistp256 pour l'échange de clés

Concernant, les communications (flux d'administration de la console web et les mises à jour) entre le pare-feu et le PC d'administration, elles sont protégées en confidentialité,

[5] Pas de confidentialité au sens « cryptographique ».

intégrité et anti-rejeu par le protocole TLS1.2, qui sera le seul protocole activé sur la TOE (https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/certificate-management/configure-an-ssltls-service-profile section « step 6 »). En activant le mode « FIPS-CC » du boitier et en n'activant que TLS1.2, les suites supportées sont celles présentées en Figure 8 : https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/certifications/enable-fips-and-common-criteria-support/change-the-operational-mode-to-fips-cc-mode. Il faut également noter qu'en activant ce mode les fonctions de sécurité présentées à l'url suivante sont activées :https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/certifications/fips-cc-security.

```
* TLSV1_2 Cipher Suites:
    Preferred:
                ECDHE-ECDSA-AES256-GCM-SHA384 ECDH-384 bits  256 bits      HTTP 302 Moved Temporarily - /php/login.php
    Accepted:
                ECDHE-ECDSA-AES256-GCM-SHA384 ECDH-384 bits  256 bits      HTTP 302 Moved Temporarily - /php/login.php
                ECDHE-ECDSA-AES128-GCM-SHA256 ECDH-256 bits  128 bits      HTTP 302 Moved Temporarily - /php/login.php

* TLSV1_1 Cipher Suites:
    Server rejected all cipher suites.

* TLSV1 Cipher Suites:
    Server rejected all cipher suites.

* SSLV3 Cipher Suites:
    Server rejected all cipher suites.
```

Figure 7 – Suites cryptographiques supportées en mode FIPS-CC (TLS1.2 only)

3.6. MATRICES DE COUVERTURES

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

	B.FILTRAGE	B.SERVICES	B.TOPOLOGIE	B.CONFIGURATION	B.JOURNAUX	B.FLUX_ADMINISTRATION	B.MISES_À_JOUR
M.CONTOURNEMENT_PARE_FEU		**I**	**C**				
M.DÉNI_DE_SERVICE	**D**	**D**		**D**			
M.ALTÉRATION				**I**	**ID**	**I**	**I**
M.EXFILTRATION				**C**	**C**	**C**	
M.MITM_ADMIN						**ICN**	**IAC**
M.ÉLÉVATION_PRIVILÈGES				**IC**		**C**	
M.ADMIN_ILLICITE	**D**	**DI**	**C**	**DIC**	**ICD**	**N**	
M.ÉVÉNEMENTS_NON_DETECTÉS					**I**		
M.VOL_PARE_FEU				**C**	**C**		

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

	F.FILTRAGE	F.JOURNALISATION	F.CONTROLE_ACCÈS	F.MISES_À_JOUR_SÉCURISÉES	F.FLUX_ADMIN_SÉCURISÉS
M.CONTOURNEMENT_PARE_FEU	√				
M.DÉNI_DE_SERVICE	√				
M.ALTÉRATION		√	√		√
M.EXFILTRATION			√		√
M.MITM_ADMIN			√	√	√
M.ÉLÉVATION_PRIVILÈGES		√	√		√
M.ADMIN_ILLICITE		√	√		
M.ÉVÉNEMENTS_NON_DETECTÉS	√			√	
M.VOL_PARE_FEU			√		

Fin du document