Déploiement, configuration et automatisation du module IPS/IDS des firewalls Palo Alto Networks chez Orange Réunion

Rapport d'alternance BUT3 Réseaux et Télécommunications, option Cybersécurité

Alternant : Jacob DUFOSSE

Tuteur entreprise : Jérémy TORTELLI, Architecte Réseaux IP

Tuteur universitaire : Laurent CHANE-KUANG-SANG

Période d'alternance : Septembre 2024 à juillet 2025

Entreprise : Orange Réunion, Direction Technique des Réseaux et Mobiles (DTRM), équipe réseaux IP

Année universitaire 2024-2025

Remerciements

Je tiens à exprimer ma profonde gratitude envers mon tuteur, Jérémy TORTELLI, pour son accompagnement bienveillant et sa confiance, ainsi qu'à l'ensemble de l'équipe Réseaux IP pour leur accueil et leur soutien tout au long de cette année.

Jeremy, merci pour ton passage de connaissance en réseaux, tes conseils très judicieux et aussi de m'avoir donné la latitude de monter en compétence dans des domaines qui me passionnent. Stéphane, merci pour ton aide, ta bonne humeur et toute ton énergie investie dans la défense de ce projet d'alternance pour une personne en reconversion. Bertrand, merci pour ta taquinerie et les grandes leçons humaines que tu m'as transmises cette année. Arnaud, merci pour tes conseils et toutes les techniques précieuses que tu as partagées avec moi. Johann, merci pour ton calme et ta rigueur qui m'ont beaucoup appris. Christian merci pour ton sourire et ta bonne humeur. Jean-François merci pour ton accueil dans l'équipe.

Cette expérience a confirmé mon intérêt pour la cybersécurité et m'a conforté dans mon choix d'orientation professionnelle, tout en m'ouvrant à l'envie d'approfondir mes connaissances en réseaux, cloud et automatisation.

J'ai de plus pu confirmer qu'il est tout à fait possible d'effectuer un retour réussi en entreprise après des années de travail à son compte.

Glossaire en annexe

Les termes techniques rencontrés dans ce rapport se trouvent dans le glossaire dans les annexes à partir de la page 47. Pour faciliter la lecture des liens hypertextes ont été ajoutés, vous pouvez ainsi facilement aller aux annexes pour y lire la définition des termes techniques. Bonne lecture.

Table des matières

I. Introduction

Présentation de l'entreprise Orange

Orange S.A., anciennement France Télécom, est l'un des principaux opérateurs de télécommunications au monde. Avec une présence dans 26 pays et plus de 266 millions de clients à l'échelle mondiale, le groupe propose une gamme complète de services de communication fixe et mobile, ainsi que des solutions numériques innovantes pour les particuliers et les entreprises.

À La Réunion, Orange est le leader historique des télécommunications, offrant des services de téléphonie fixe et mobile, d'accès à Internet haut débit et très haut débit, ainsi que des services de télévision et de contenus numériques. L'entreprise joue un rôle crucial dans le développement numérique de l'île, notamment à travers le déploiement de la fibre optique et des réseaux 4G/5G, contribuant ainsi à réduire la fracture numérique et à favoriser l'innovation technologique dans la région.

Orange Réunion emploie plus de 1000 collaborateurs répartis sur différents sites, dont le siège social situé à Saint-Denis. L'entreprise s'organise autour de plusieurs directions techniques et commerciales, chacune ayant des missions spécifiques pour assurer la qualité et la continuité des services proposés aux clients réunionnais.

Le département Réseaux IP : missions et organisation

Au sein d'Orange Réunion, le département Réseaux IP (Internet Protocol) relève de la Direction Technique des Réseaux et Mobiles (DTRM). Ce département joue un rôle fondamental dans l'infrastructure de communication de l'entreprise, assurant la conception, le déploiement, l'exploitation et la sécurisation des réseaux IP qui constituent l'épine dorsale des services numériques proposés par Orange.

Les principales missions du département Réseaux IP comprennent :

- **Conception et déploiement** des infrastructures réseau IP, incluant les routeurs, commutateurs et pares-feux
- **Administration et supervision** des équipements réseau pour garantir leur disponibilité et leurs performances
- **Sécurisation des infrastructures** contre les menaces informatiques et les cyberattaques
- **Gestion des interconnexions** avec les autres opérateurs et fournisseurs de services
- **Support technique** aux autres départements d'Orange et résolution des incidents réseau
- **Veille technologique** et évolution des infrastructures pour répondre aux besoins futurs

L'équipe Réseaux IP est composée d'ingénieurs et exploitants spécialisés, chacun apportant son expertise dans des domaines spécifiques. Cette équipe travaille en étroite collaboration avec d'autres départements, notamment l'équipe responsables des systèmes d'information (S.I), celle des équipements cœur de réseaux ou encore les équipes radio (RAN).

Positionnement personnel au sein de l'organisation

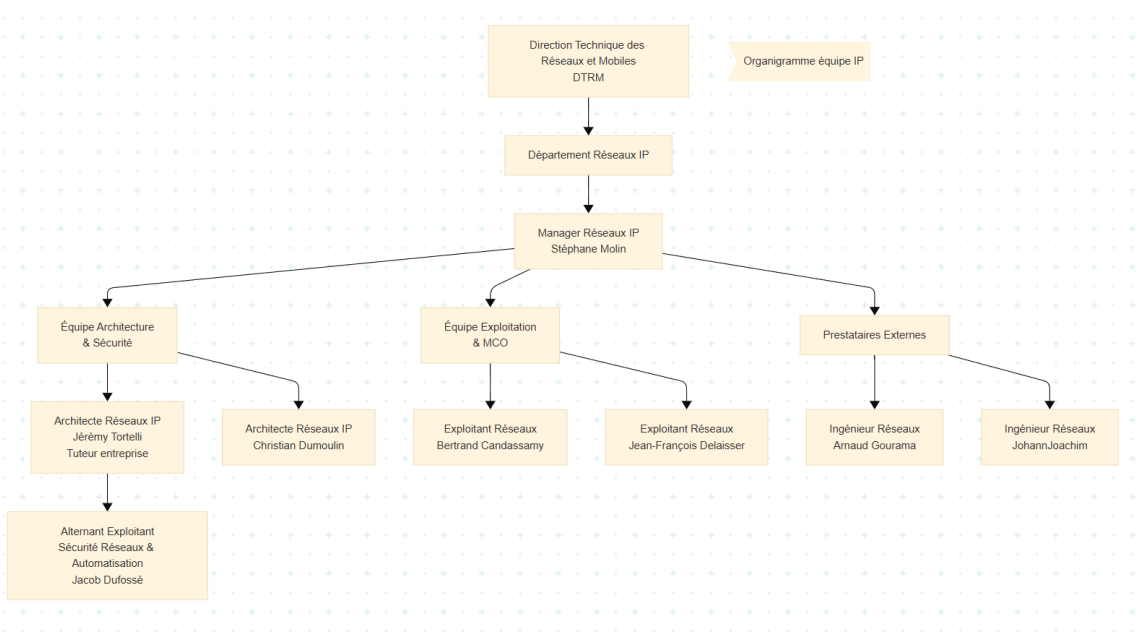


Figure 11 organigramme équipe réseaux IP DTRM

J'ai intégré l'équipe Réseaux IP en tant qu'alternant en BUT Réseaux et Télécommunications, option Cybersécurité. J'ai pu travailler directement avec les ingénieurs et exploitants responsables des réseaux et leur sécurité et cette position stratégique m'a offert une vision globale des enjeux des réseaux d'entreprise et télécom, tout en me permettant de contribuer concrètement aux projets de renforcement de la posture de sécurité d'Orange Réunion.

Contexte de l'alternance : enjeux de sécurité et importance des firewalls

Mon alternance s'est déroulée dans un contexte particulier pour Orange Réunion : la migration récente vers une nouvelle solution de pare-feu (firewall = équipements de sécurité réseau). En effet, l'entreprise a fait le choix stratégique de remplacer ses équipements de sécurité existants par des firewalls virtuels Palo Alto Networks, une solution de nouvelle génération offrant des capacités avancées de détection et de prévention des menaces.

Cette migration s'inscrit dans un contexte global d'évolution des cybermenaces :

- Une **sophistication croissante des attaques** informatiques, avec des techniques d'évasion de plus en plus élaborées
- Une **augmentation significative des attaques par déni de service** DOS et DDoS (attaque visant à surcharger les capacités des équipements réseaux) à destination des infrastructures critiques et les services web
- La **multiplication des vulnérabilités** dans les équipements, les applications et systèmes d'exploitation
- L'émergence de **nouvelles menaces liées à l'Internet des objets (IoT)** augmentant les vecteurs d'attaque (botnet)

Face à ces défis, les firewalls de nouvelle génération jouent un rôle crucial dans la stratégie de défense en profondeur d'Orange Réunion. Ils constituent la première ligne de défense du réseau, filtrant le trafic entrant et sortant, détectant les comportements suspects et bloquant les tentatives d'intrusion avant qu'elles ne puissent atteindre les systèmes internes.

Présentation de Palo Alto Networks et des outils associés

Palo Alto Networks est un leader mondial dans le domaine de la cybersécurité, reconnu pour ses solutions de pare-feu de nouvelle génération (NGFW : Next-Generation Firewall). Contrairement aux firewalls traditionnels qui se limitent au filtrage par ports et protocoles, les solutions Palo Alto intègrent des fonctionnalités avancées telles que :

- L'**inspection approfondie des paquets** de la couche réseau jusqu'à la couche applicative
- La **prévention des intrusions (IPS : Intrusion Prevention System)** et la **détection des menaces (IDS : Intrusion Detection System)**
- Le **filtrage d'URL** et le **contrôle des applications**
- La **protection contre les logiciels malveillants** et les menaces avancées
- L'**analyse du trafic chiffré** (**SSL/TLS**)

Dans l'environnement d'Orange Réunion, deux composants principaux de la solution Palo Alto ont été déployés :

1. **Les firewalls virtuels VM-Series** : Déployés sur l'infrastructure VMware ESXi, ces pares-feux virtuels offrent les mêmes fonctionnalités que leurs équivalents physiques.
2. **Panorama** : Cette plateforme centralisée de gestion permet d'administrer l'ensemble des firewalls Palo Alto depuis une interface unique.

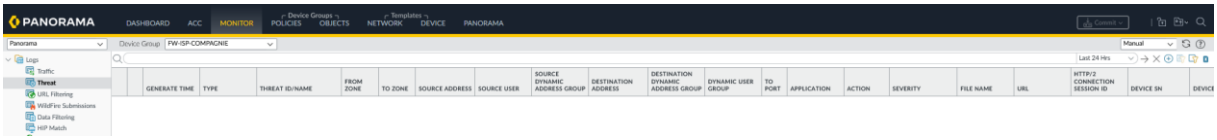


Figure 22 extrait de l'interface graphique web - Panorama

Pour administrer et exploiter ces solutions, plusieurs outils complémentaires sont utilisés :

- **VMware Vsphere** : Plateforme de gestion pour la virtualisation hébergeant les firewalls virtuels et Panorama
- **MobaXterm** : Application permettant l'accès sécurisé et à distance aux terminaux des équipements réseaux
- **Centreon** : Solution de supervision assurant le monitoring des performances et de la disponibilité des équipements
- **Loki / Syslog** : Solution de d'observabilité et de collecte des logs (enregistrements d'événements sur le réseau) sur de longues périodes

- **NetBackup** : Système de sauvegarde garantissant la protection des machines virtuelles et leurs configurations
- **GitLab** : Plateforme de gestion de code source utilisée pour le versioning des scripts d'automatisation

Problématique et mission principale

Dans ce contexte, la problématique centrale de mon alternance peut être formulée ainsi: **Comment optimiser la gestion et l'automatisation des opérations de sécurité réseau face à l'évolution constante des cybermenaces ?**

Cette problématique se décline en plusieurs questions :

- Comment configurer efficacement les firewalls Palo Alto pour maximiser la protection du réseau ?
- Comment exploiter pleinement les capacités du module de détection et de prévention des intrusions ?
- Comment automatiser les tâches récurrentes pour améliorer l'efficacité opérationnelle ?
- Comment documenter les processus pour assurer la pérennité des solutions mises en place ?

Pour répondre à ces questions, ma mission principale a consisté à configurer, exploiter et automatiser le module IPS/IDS des firewalls Palo Alto. Cette mission s'est articulée autour de trois axes majeurs :

1. **Configuration et optimisation du module** IPS/IDS: Mise en place des profils de protection DOS (denial of service) et CVE (common vulnerabilities and exposures), configuration des règles de sécurité, paramétrage des actions à entreprendre face aux différentes menaces.
2. **Exploitation et analyse** : Surveillance quotidienne des alertes, analyse des logs de sécurité, identification des faux positifs, prise de décision concernant le blocage des adresses IP malveillantes.
3. **Automatisation** : Développement de scripts Python et montée en compétence en API rest (interface de communication entre applications) et gitlab pour automatiser les tâches récurrentes.
4. **Documentation** : documentation des procédures et des configurations dans Confluence (outil de documentation collaboratif).

Cette mission s'inscrit dans la stratégie de sécurité d'Orange Réunion, visant à renforcer la protection de ses infrastructures critiques tout en optimisant les ressources humaines.

Passons tout d'abord à la description des tâches récurrentes avant de présenter plus en détails ma mission principale (module IPS/IDS) et son évolution vers l'automatisation.

II. Tâches quotidiennes et missions régulières

Au cours de mon alternance chez Orange Réunion, j'ai été impliqué dans diverses tâches opérationnelles et quotidiennes liées à la gestion des firewalls Palo Alto et à l'utilisation d'autres équipements.

Ces activités régulières m'ont permis de développer une compréhension pratique des missions classiques d'une équipe réseaux tel que le maintien en condition opérationnel (MCO) ou l'installation/configuration de nouveaux équipements, la gestion des certificats, le support, les astreintes ou encore le décommissionnement de matériel. Voici une liste et détails des missions quotidiennes qui m'ont été assignées :

Surveillance et analyse des logs de sécurité

Vérification quotidienne des alertes IPS/IDS

La surveillance des logs de sécurité constitue une responsabilité quotidienne essentielle. Chaque matin, j'analyse les alertes générées par le module IPS/IDS des firewalls Palo Alto, en priorisant celles de sévérité "critique" et "élevée".

Processus d'analyse structuré :

1. Consultation des alertes liées aux menaces via Panorama ("Monitor > Threats")
2. Filtrage par sévérité et période (dernières 24h)
3. Analyse des types de menaces et identification des adresses IP impliquées
4. Corrélation avec les événements antérieurs pour détecter des schémas d'attaque

Cette vigilance permet d'identifier rapidement les menaces potentielles avant qu'elles ne causent des dommages significatifs.

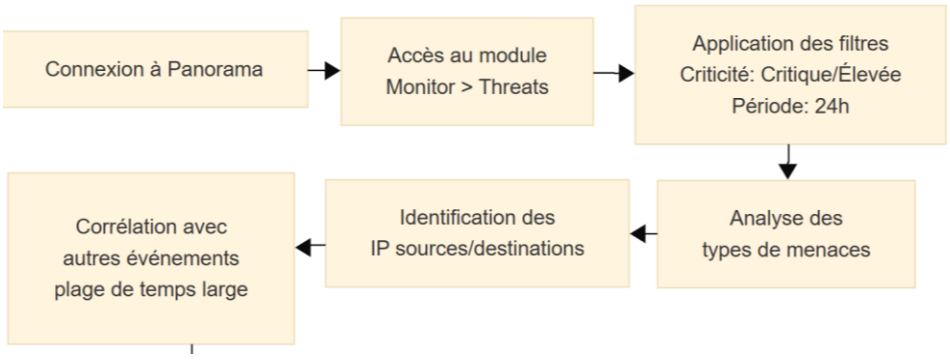


Figure 33 processus de vérification des logs de menaces sur firewalls Palo

Analyse des menaces détectées, faux positifs et prise de décision

Pour chaque alerte significative, je mène une analyse approfondie selon un processus structuré :

1. Examen des logs : Analyse du type de menace, signature IPS et contexte de détection
2. Recherche sur les CVE : Consultation des bases de données pour évaluer l'impact potentiel

3. Analyse comportementale : Vérification de l'origine (collaborateur ou externe) et recherche de schémas d'attaques sur différentes périodes
4. Évaluation du risque : Basée sur la criticité, les cibles visées, la localisation géographique et la temporalité et la variété de CVE utilisée

Les décisions prises sont proportionnées à l'analyse :

- Pour les faux positifs : documentation, communication à l'équipe et ajustement des règles IPS
- Pour les menaces réelles : blocage temporaire ou permanent de l'IP source, modification des règles de sécurité ou escalade à l'équipe de sécurité selon la gravité

Cette approche méthodique permet d'équilibrer protection et disponibilité des services.

Rapport des incidents de sécurité

Je transmets régulièrement à l'équipe IP un rapport synthétique des incidents de sécurité détectés par les firewalls, comprenant :

- Un résumé des adresses IP bloquées
- Les principales menaces détectées
- Un focus sur les incidents significatifs (attaquants persistants, nouvelles techniques d'attaque)

Ce rapport permet de maintenir une visibilité sur l'état de sécurité du réseau et d'identifier les tendances émergentes pour anticiper les évolutions nécessaires dans la configuration des firewalls.

Figure 44 exemple de courriel de rapport

Gestion des certificats

La gestion des certificats SSL/TLS sur Panorama et les firewalls constitue une mission récurrente essentielle pour le déchiffrement des flux. En effet un certificat SSL/TLS entre un client et le serveur final sert à chiffrer les échanges c'est-à-dire à les sécuriser. Or sur le firewall c'est l'inverse, le certificat sert à déchiffrer les flux. Les firewalls plus anciens se préoccupent de l'IP source et l'IP de destination, des ports. Mais avec les firewalls nouvelles génération on peut désormais analyser au niveau applicatif pour avoir des blocages beaucoup plus précis. Mais pour avoir accès au contenu du paquet sur cette couche, il faut déchiffrer le flux. D'où le besoin d'avoir le certificat pour le faire avant que le paquet soit autorisé à aller vers sa destination.

Processus de renouvellement et d'installation :

1. Récupération des certificats (DigiCert, Orange Internal CA ou équipements déjà mis à jour)
2. Import dans Panorama avec minimisation de l'impact sur les services
3. Association aux profils de déchiffrement
4. Validation du bon fonctionnement post-déploiement

Cette procédure standardisée garantit l'intégrité du déchiffrement SSL/TLS tout en maintenant la continuité des services.

Renouvellement et installation des certificats

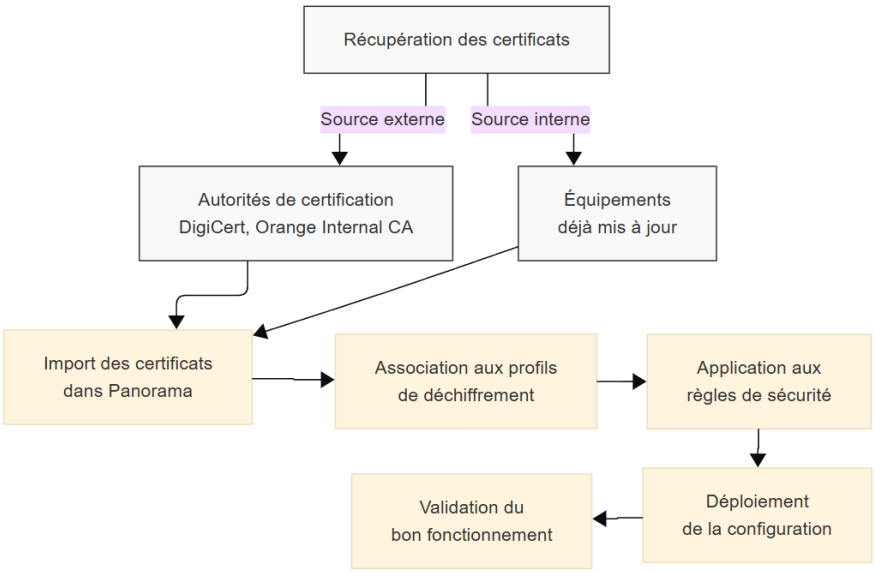


Figure 55 processus renouvellement / ajout certificat Panorama

Résolution des problèmes liés aux certificats expirés

Durant mon alternance, j'ai pris conscience que des certificats expirés ou mal configurés pourraient provoquer des interruptions de service, impactant directement la réputation et le chiffre d'affaires de l'entreprise. Pour prévenir ces risques, l'équipe IP a mis en place :

- Des notifications automatiques avant expiration

- Une planification rigoureuse des renouvellements
- Une coordination entre équipes pour les infrastructures multi-équipements

Maintenance des firewalls en condition opérationnelles (MCO)

La maintenance préventive et corrective des firewalls constitue une activité obligatoire pour garantir leur disponibilité et leurs performances optimales.

Vérification des synchronisations

Une tâche quotidienne essentielle consiste à vérifier la synchronisation des configurations entre:

- Panorama et les firewalls
- Les équipements primaires et secondaires dans l'architecture haute disponibilité

Cette vérification est critique car chaque firewall principal est accompagné d'un firewall secondaire de secours (équipement redondé), et leur configuration doit rester identique pour assurer une bascule transparente en cas de défaillance.

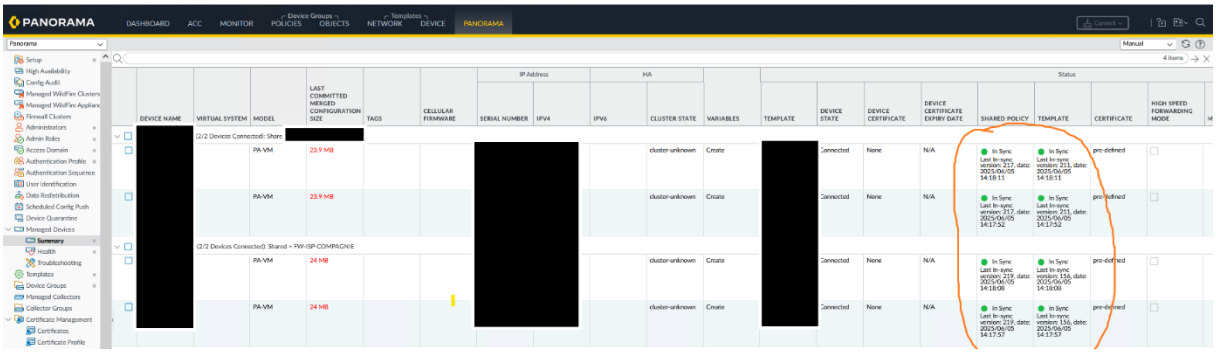


Figure 66 tableau de bord état des synchronisations équipements via Panorama

Résolution des problèmes de désynchronisation

Face aux désynchronisations entre Panorama et les firewalls ou entre membres d'une paire HA (high avaibility), j'applique une méthodologie structurée :

1. Identification du problème de désynchronisation
2. Application des méthodes standard (efficaces dans 90% des cas) – tel que regarder dans la fenêtre des commit si une personne n'a pas laissé des actions non enregistrées (cause la plus fréquente de désynchronisation).
3. Si nécessaire, analyse approfondie des logs de configuration, avant/après commit (appliquer les changements)
4. Mise en œuvre des correctifs appropriés comme commit ou resynchronisation manuelle
5. Validation du retour à l'état synchronisé
6. Documentation de l'incident et des solutions appliquées

Cette approche méthodique permet de résoudre efficacement les incidents de désynchronisation.

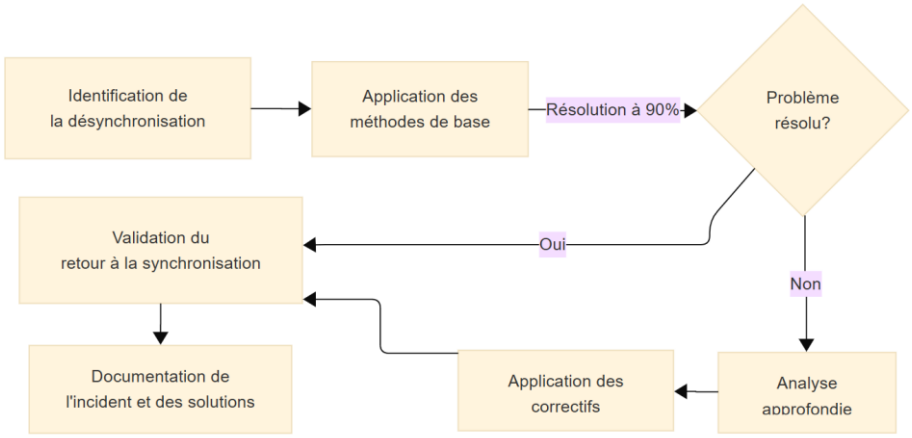


Figure 77 processus résolution de désynchronisation

Cette méthodologie m'a permis de résoudre efficacement plusieurs incidents de désynchronisation.

Mises à jour des équipements

La mise à jour des équipements est une opération critique nécessitant une approche réfléchie. Avant toute mise à jour, j'évalue désormais systématiquement :

- La nécessité réelle (présence de CVE critiques)
- L'impact potentiel sur les services
- Le rapport bénéfice/risque du changement de version

Mise à jour des bases de données de sécurité

J'ai implémenté l'automatisation des mises à jour des signatures IPS/antivirus et des bases de données CVE, essentielle pour maintenir l'efficacité des firewalls face aux menaces émergentes.

Mise à jour des OS

J'ai réalisé une mise à jour majeure de PAN-OS (système Palo) sur l'infrastructure Panorama, incluant :

- La rédaction de procédures détaillées sur Confluence
- La présentation en comité d'opération (COOP)
- La coordination avec le support Palo Alto et l'équipe SI

Cette expérience m'a permis de participer à un processus complet de résolution de problèmes techniques en environnement critique.

- Mise à jour de Panorama en standalone
  - Documentation Palo
    - documentation complète sur les mises à jour (pdf)
    - Liens vers les chapitres de références (web)
  - Procédure de mise à jour
    - 1. Faire la backup
    - 2. Choix de la mise à jour
      - Vérifiez la version actuelle
      - Vérifiez les versions de PAN-OS disponibles
      - Faites une revue de la nouvelle version
    - 3. Si User-id est activé (pas en usage pour le moment 09-04-2025)
    - 4. Mettez à jour les dynamics updates (anti virus, applications and threats) du Panorama
    - 5. Mise à jour des plugin VM (pas en usage pour le moment 09-04-2025)
    - 6. Mise à jour de PAN-OS
    - 7. Vérifiez le fonctionnement du Panorama après la mise à jour
    - 8. Revenez en arrière si problème

Figure 88 sommaire documentation de procédure de mise à jour Panorama

Gestion des règles de sécurité

La gestion des règles de sécurité constitue une activité centrale dans l'administration des firewalls, nécessitant rigueur et méthodologie.

Création et modification des règles selon les besoins

En réponse aux demandes des équipes métier et aux évolutions de l'infrastructure, j'ai créé et modifié des règles de sécurité :

1. Analyse des besoins exprimés et validation de leur légitimité
2. Conception de règles respectant le principe du moindre privilège
3. Implémentation dans Panorama avec une nomenclature appropriée
4. Déploiement en préproduction puis en production
5. Test de vérification de continuité des services (services toujours accessibles aux utilisateurs ?)
6. Suivi post-déploiement pour vérifier l'efficacité de la règle

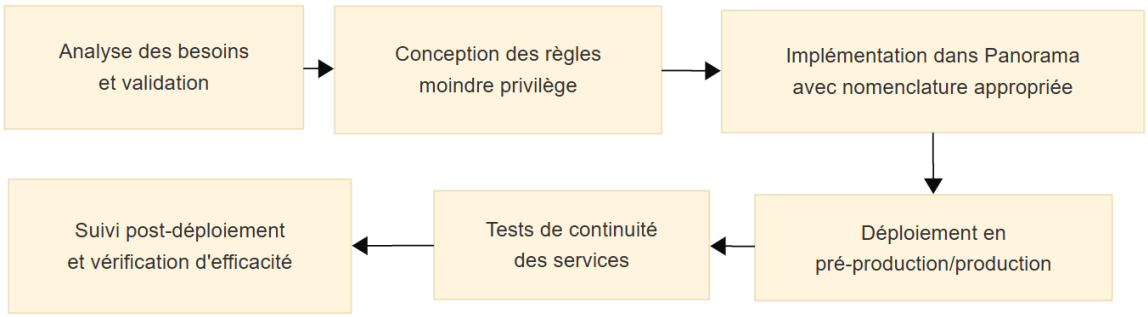


Figure 99 processus création règle de sécurité

Cette expérience m'a permis d'approfondir ma compréhension du fonctionnement des firewalls dans un environnement multi-constructeurs (Palo, Fortinet, F5), où l'ouverture d'un flux nécessite de retracer la chaîne complète d'équipements et de vérifier la configuration de chaque élément intermédiaire.

Documentation et communication

La documentation rigoureuse et la communication efficace sont essentielles pour assurer la pérennité des connaissances et la continuité des opérations.

Présentation du projet d'implémentation du module IPS/IDS

J'ai présenté le projet d'implémentation du module IPS/IDS aux équipes sécurité, architecture et SI après avoir réalisé une note de cadrage complète et une présentation PowerPoint détaillée.

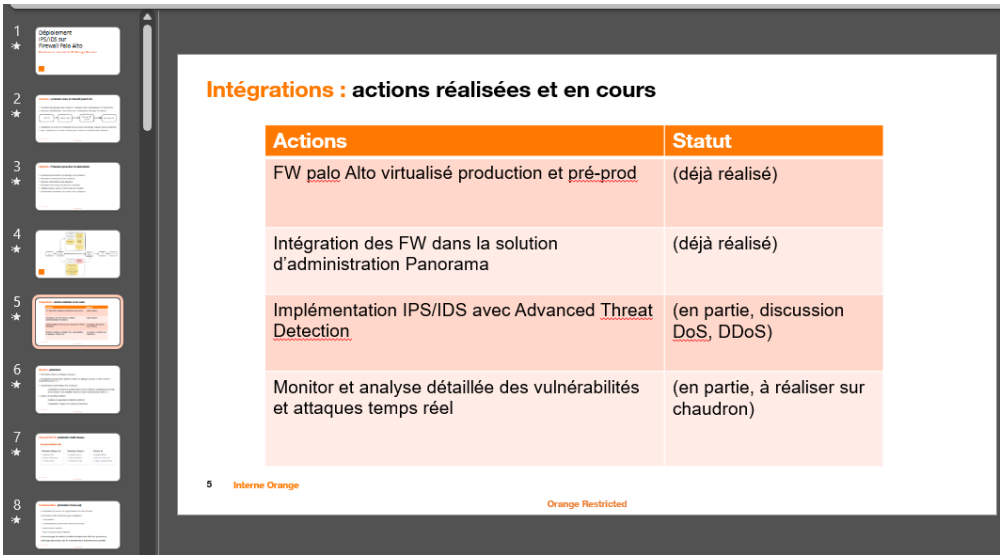


Figure 1010 Extrait de la présentation lancement de projet IDS/IPS : suivi et implémentation en cours

Mise à jour de la documentation technique sur Confluence

J'ai créé et maintenu une documentation structurée pour les équipements Palo Alto comprenant:

- Procédures détaillées pour les opérations courantes

- Tutoriels illustrés pour faciliter la prise en main
- Documentation des configurations et choix techniques

Cette documentation constitue un héritage durable de mon alternance, permettant le transfert de connaissances et la pérennisation des bonnes pratiques.

Figure 1111 Sommaire des documentations réalisées pour les équipements Palo Alto

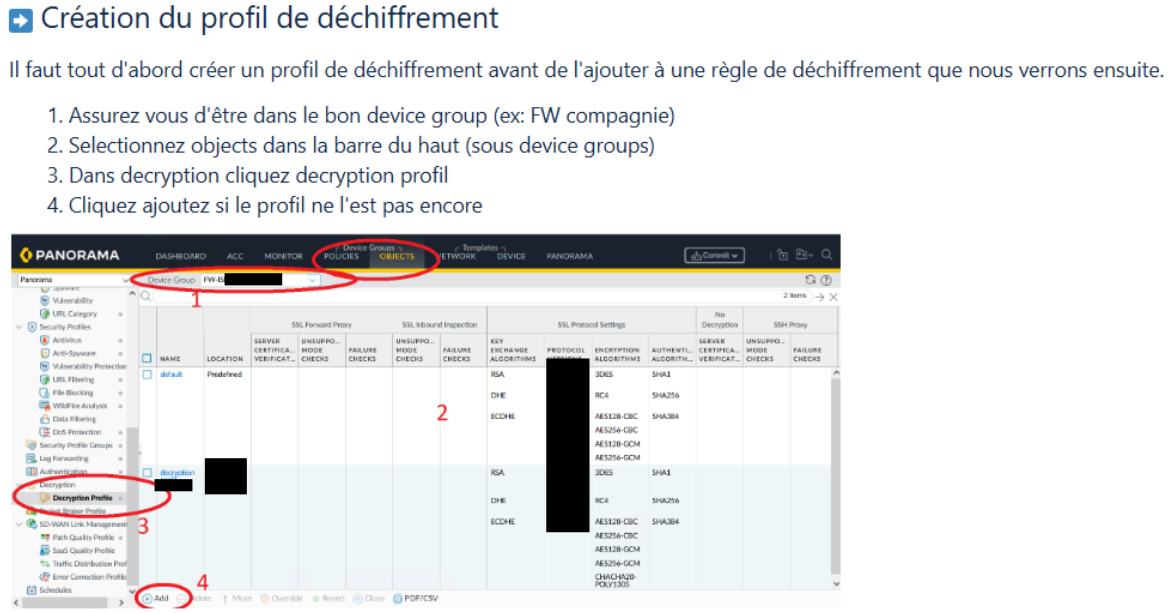


Figure 1212 Extrait de tutoriel de la configuration de la fonction d'analyse des menaces

Participation régulière aux réunions d'équipe

J'ai présenté hebdomadairement l'avancement des projets, partagé les incidents rencontrés et contribué aux discussions techniques sur l'évolution des solutions Palo Alto et leur automatisation.

Échanges avec les autres services

Mon rôle dans l'équipe Réseaux IP m'a permis d'échanger régulièrement avec les équipes SI pour :

- La création de machines virtuelles
- Les demandes d'autorisations de flux réseaux à travers le proxy externe (serveur intermédiaire entre réseau local et externe)

Les échanges avec les équipes SI m'ont offert une vision globale des enjeux de sécurité et m'ont sensibilisé aux défis propres aux grandes organisations, où les processus d'approbation transforment parfois un projet d'une journée en plusieurs semaines de travail.

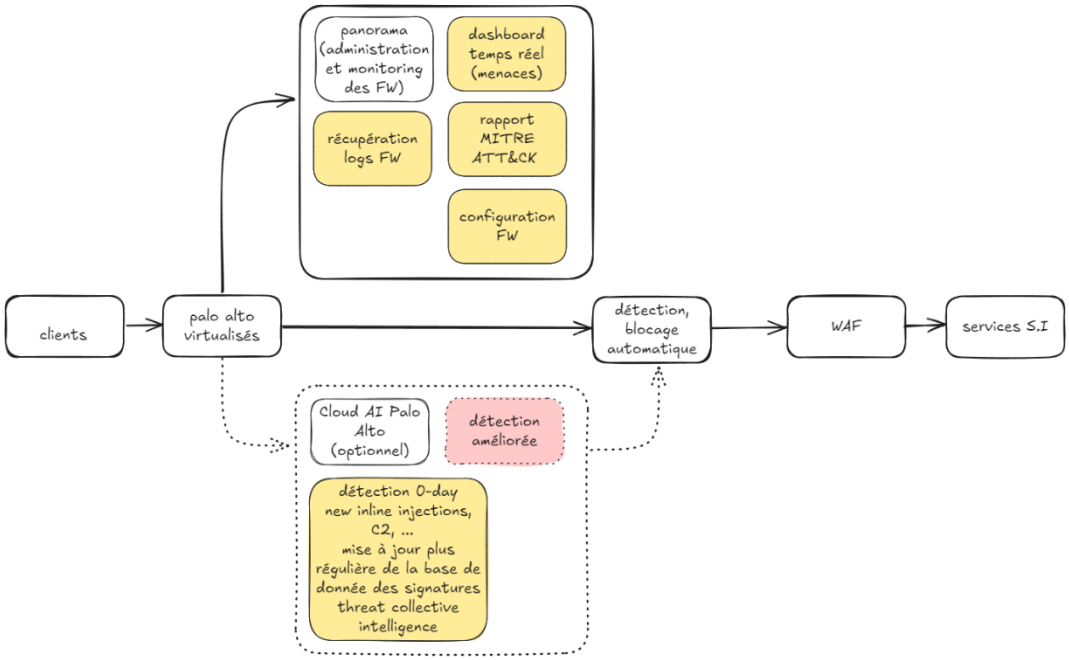
III. Déploiement et administration des firewalls Palo Alto et Panorama

Cette section présente l'architecture technique et les processus d'administration des firewalls Palo Alto. Bien que la mise en place initiale de cette infrastructure ait été réalisée avant mon arrivée, la compréhension approfondie de ces éléments a été essentielle pour mener à bien mes missions quotidiennes et mes projets d'amélioration.

Architecture technique et choix des solutions

L'infrastructure repose sur une architecture virtualisée de firewalls Palo Alto.

Voici un schéma simplifié du positionnement des firewall Palo de production et de Panorama (de nombreux éléments de réseau ne sont pas indiqués par confidentialité) :



Virtualisation et haute disponibilité

La solution déployée s'articule autour des composants suivants :

- **Firewalls virtuels VM-Series** : Déployés sur l'infrastructure VMware ESXi, ces pares-feux virtuels offrent l'ensemble des fonctionnalités de sécurité de nouvelle génération. Chaque site (Chaudron et Compagnie) dispose d'une paire de firewalls configurés en haute disponibilité active/passive.
- **Panorama** : Cette plateforme centralisée de gestion est également virtualisée. Elle permet d'administrer l'ensemble des firewalls depuis une interface unique, simplifiant considérablement les opérations de configuration et de supervision.
- **Infrastructure VMware** : L'ensemble de la solution Palo repose sur une infrastructure VMware ESXi et administré avec Vsphere, permettant la mobilité des machines virtuelles entre les hôtes physiques et facilitant les opérations de maintenance sans impact sur la disponibilité des services.

Cette architecture virtualisée présente plusieurs avantages stratégiques :

- **Flexibilité** : Possibilité d'ajuster les ressources allouées aux firewalls en fonction des besoins
- **Résilience** : Haute disponibilité des firewalls
- **Efficacité opérationnelle** : Gestion centralisée via Panorama et intégration avec les outils de supervision existants
- **Évolutivité** : Capacité à déployer rapidement de nouveaux firewalls virtuels selon les besoins

Configuration basique

La configuration des firewalls Palo Alto comprend plusieurs éléments de base essentiels que je vais détailler.

Adressage IP et interfaces

Les firewalls Palo Alto sont configurés avec plusieurs interfaces réseau (à travers lesquels les flux circulent), chacune associée à une zone de sécurité spécifique :

- Interfaces externes (zone untrust) connectées à Internet
- Interfaces internes (zone trust) connectées au réseau d'entreprise
- Interfaces de gestion pour l'administration des équipements et accès à l'API

Chaque interface est configurée avec une adresse IP statique et des paramètres réseau appropriés (masque de sous-réseau, passerelle par défaut). Les interfaces sont également associées à des profils de sécurité spécifiques en fonction de leur exposition aux menaces.

Routage et connectivité

Le routage sur les firewalls Palo Alto est configuré pour assurer la connectivité entre les différentes zones de sécurité et vers les réseaux externes et internes. Les routes configurées dans les équipements sont statiques mais elles peuvent l'être avec différents protocoles (tel que OSPF ou BGP).

Services d'infrastructure (DNS, RADIUS, proxy)

Les firewalls sont configurés pour utiliser plusieurs services d'infrastructure essentiels :

- **Serveurs DNS** internes pour la résolution de noms
- **Serveurs RADIUS** pour l'authentification des administrateurs
- **Serveurs proxy** pour les connexions sortantes vers Internet
- **Serveurs syslog** pour l'archivage des logs

Création de règles de sécurité

Les règles de sécurité constituent le cœur de la politique de filtrage des firewalls Palo Alto, définissant précisément quels flux sont autorisés, inspectés ou bloqués.

Structure des règles de sécurité

Les règles de sécurité Palo Alto sont structurées selon plusieurs critères :

- **Source** : Zone source, adresses IP des machines autorisées ou refusées, utilisateurs ou groupes d'origine du trafic
- **Destination** : Zone destination, adresses IP des machines destinataires ou FQDN de destination
- **Application** : Applications spécifiques identifiées par inspection approfondie
- **Service** : Ports et protocoles utilisés (https, http, etc.)
- **Action** : Allow, Deny, Drop, Reset
- **Profils de sécurité** : Antivirus, anti-spyware, vulnérabilités, filtrage URL, etc.
- **Logging** : Paramètres d'enregistrement des événements

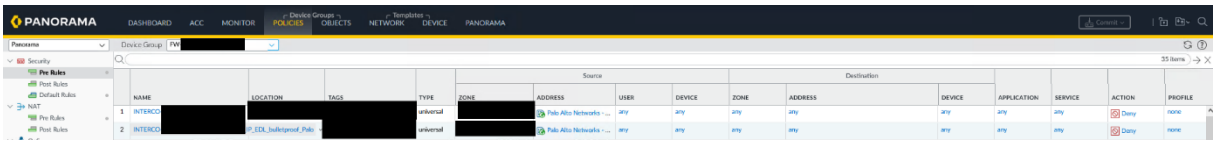


Figure 1313 Extrait du dashboard listes des règles sécurité

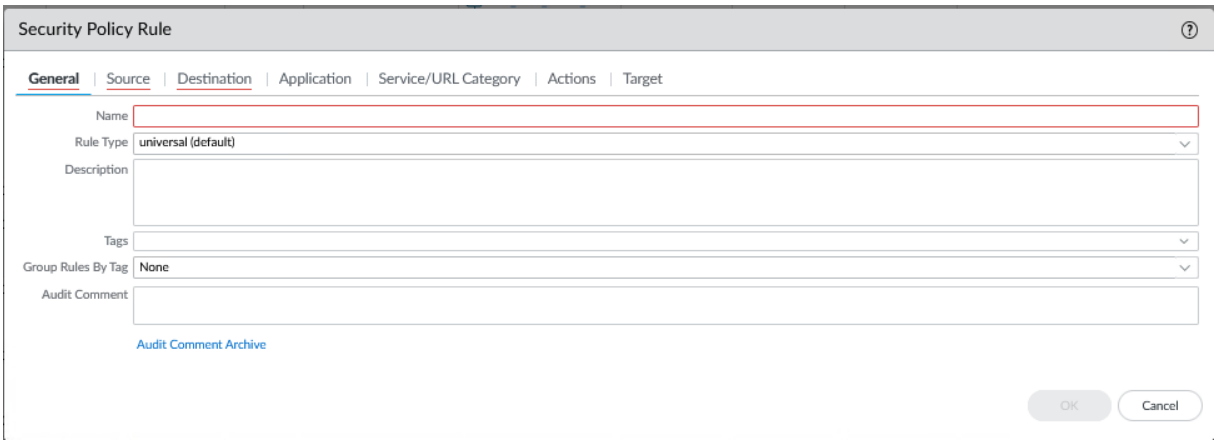


Figure 1414 Création d'une règle de sécurité

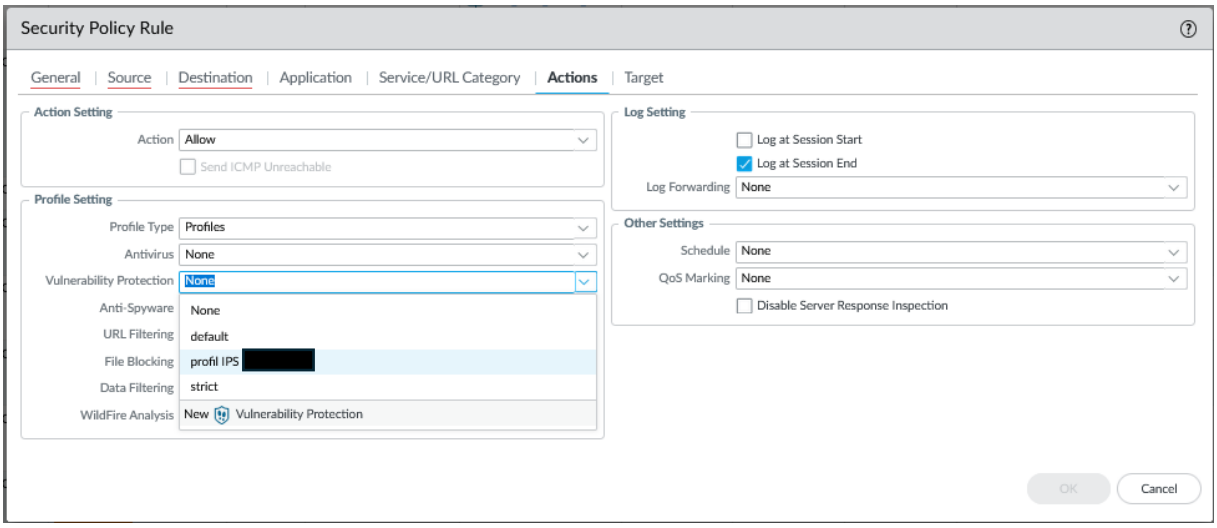


Figure 1515 Onglet pour la gestion des profils appliqués aux règles de sécurité

Cette structure granulaire permet un contrôle précis des flux réseau, au-delà des capacités des firewalls traditionnels.

Organisation des politiques de sécurité

Les règles sont organisées selon une hiérarchie logique pour optimiser à la fois la sécurité et les performances :

- Règles de blocage des menaces connues (listes noires via EDL builtin par exemple. Explication à la prochaine section)
- Règles spécifiques pour les services critiques
- Règles générales par catégorie de service
- Règle de blocage par défaut (deny-all)

Cette organisation permet d'appliquer le principe de sécurité du "moindre privilège" tout en maintenant une configuration lisible et maintenable.

Sauvegarde et restauration des configurations

La sauvegarde régulière des configurations est essentielle pour assurer la résilience de l'infrastructure de sécurité et permettre une restauration rapide en cas d'incident.

Plusieurs mécanismes complémentaires sont utilisés pour la sauvegarde des configurations :

- **Sauvegardes** de configuration générées automatiquement par Panorama avant chaque modification (enregistré sur l'équipement)
- **Exports manuels** des configurations via Panorama et téléchargeables hors équipement
- **Sauvegardes planifiées quotidiennement** via NetBackup pour l'ensemble de la machine virtuelle

Ces différentes couches de sauvegarde offrent une protection complète contre les risques de perte de configuration.

Procédures de restauration

Des procédures de restauration sont documentées pour différents scénarios :

1. Restauration d'une configuration précédente via l'interface Panorama
2. Restauration complète d'un firewall à partir d'une sauvegarde NetBackup
3. Reconstruction complète d'un firewall à partir des configurations exportées

Tests de performance et de basculement HA

Des tests réguliers sont effectués pour valider les performances des firewalls et leur capacité à maintenir la continuité de service en cas de défaillance.

Les performances des firewalls sont évaluées à l'aide de plusieurs outils et méthodes :

- IPerf pour mesurer le débit maximal dans différentes configurations
- Outils de génération de trafic pour simuler des charges réelles
- Surveillance des indicateurs de performance dans des conditions normales et de stress

Ces tests permettent de s'assurer que les firewalls disposent des ressources nécessaires pour traiter le trafic attendu sans devenir un goulot d'étranglement.

La fiabilité du mécanisme de haute disponibilité est vérifiée par des tests de basculement :

- Basculement planifié lors des fenêtres de maintenance
- Simulation de défaillance d'un firewall
- Tests de VMOTION pour valider la mobilité des machines virtuelles
- Mesure du temps de basculement et de l'impact sur les services

Supervision des firewalls

La supervision continue des firewalls est essentielle pour détecter rapidement les anomalies et maintenir un niveau optimal de performance et de sécurité.

Plusieurs outils complémentaires sont utilisés pour la supervision des firewalls :

- Centreon pour la surveillance des indicateurs de disponibilité et de performance
- Vsphere pour le monitoring des ressources virtualisées (CPU, mémoire, stockage)
- Panorama pour les indicateurs spécifiques aux Palo Alto
- Loki/syslog pour l'analyse approfondie des logs

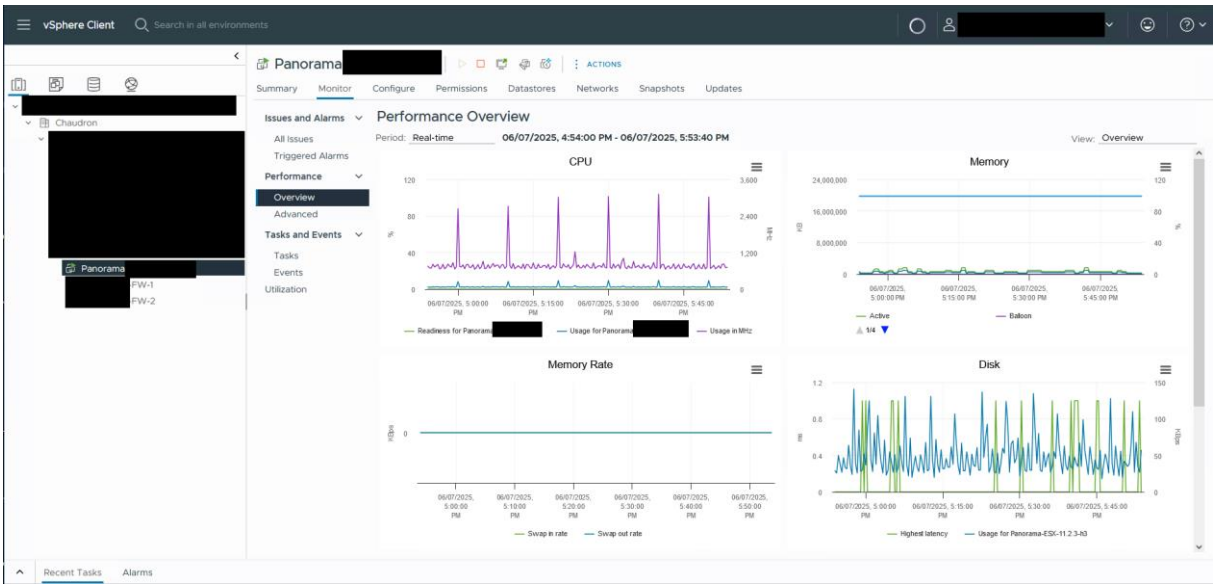


Figure 1616 Extrait de vSphere dashboard - surveillance VM panorama

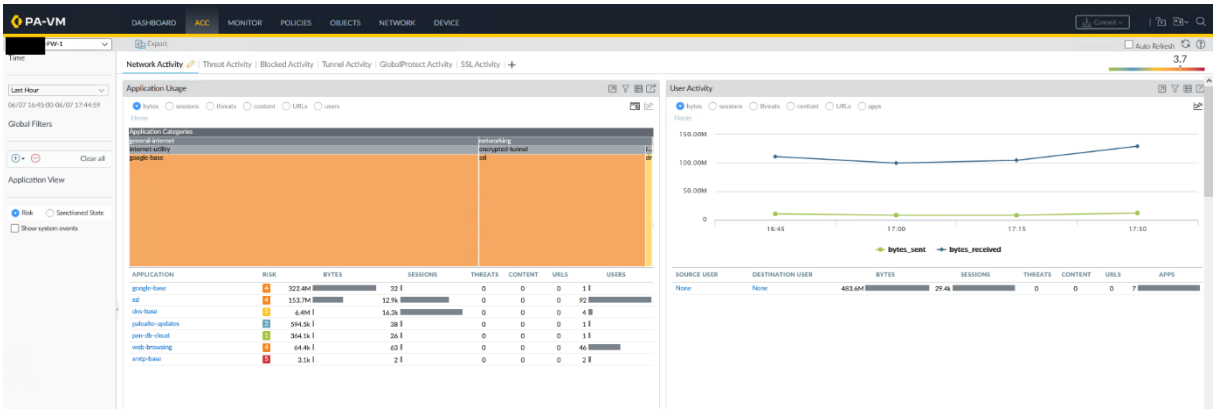


Figure 1717 Extrait interface monitoring réseaux Palo (directement depuis l'équipement lui-même)

Ces outils offrent une vision complète de l'état de santé de l'infrastructure de sécurité.

Indicateurs clés sur Centreon

Les principaux indicateurs surveillés comprennent :

- Disponibilité des firewalls et de leurs interfaces
- Utilisation des ressources (CPU, mémoire, sessions)
- Débit sur les différentes interfaces
- Latence de traitement des paquets
- État de synchronisation des paires HA
- Alertes de sécurité générées par les modules de protection

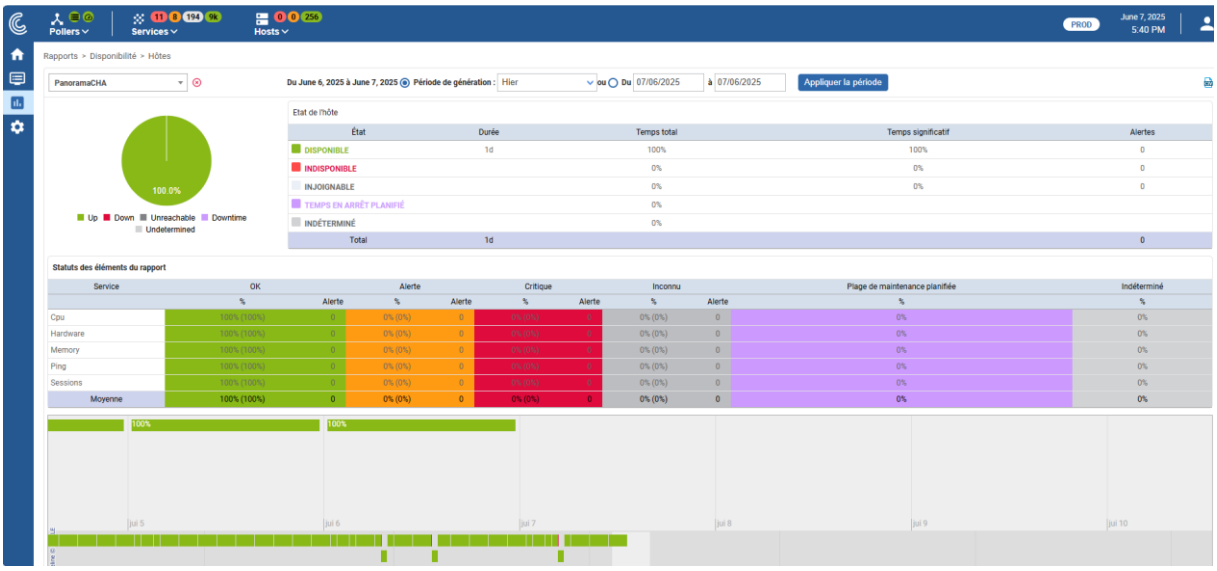


Figure 1818 Extrait de l'interface Centreon - supervision de Panorama

Des seuils d'alerte sont configurés pour chaque indicateur, permettant une détection précoce des problèmes. Des courriels sont reçus dès lors que les seuils sont dépassés, alertant tous les membres de l'équipe IP de l'état des équipements.

IV. Sécurisation du réseau avec le module IPS/IDS

Ma mission principale chez Orange a été de déployer, configurer et optimiser le module IPS/IDS "Advanced Threat Prevention" des firewalls Palo Alto. Ce projet s'est déroulé en trois phases : une phase initiale d'appropriation de la documentation, suivie de tests et de configurations en pré-production, puis enfin le déploiement et la configuration en production.

Présentation du module IPS/IDS : élément de stratégie de sécurité

Le module IPS/IDS constitue l'une des fonctionnalités les plus avancées des firewalls Palo Alto Networks. Contrairement aux firewalls traditionnels qui se limitent au filtrage par ports et protocoles, ce module permet une analyse approfondie du trafic réseau pour détecter et bloquer les tentatives d'intrusion en temps réel. Ce qui constitue une première ligne de surveillance et de défense en plus des autres équipements de sécurité présent dans l'infrastructure. Je rappelle que cet équipement fait la jonction entre internet et le réseau interne, il est donc fondamental en termes de sécurité.

Dans le contexte d'Orange Réunion, ce module joue un rôle central dans la stratégie de défense pour plusieurs raisons :

1. **Détection des menaces avancées** : Le module IPS/IDS permet d'identifier des attaques sophistiquées qui échapperaient aux mécanismes de filtrage traditionnels.
2. **Protection proactive** : Au-delà de la simple détection, le module peut bloquer automatiquement les tentatives d'intrusion et d'exploitation de CVE avant qu'elles n'atteignent leur cible, réduisant considérablement la fenêtre d'exposition aux menaces.

3. **Visibilité approfondie** : Les logs générés par le module offrent une visibilité précieuse sur les tentatives d'attaque, permettant d'analyser les techniques utilisées par les attaquants et d'adapter la posture de sécurité en conséquence.
4. **Réduction de la charge opérationnelle** : L'automatisation des réponses aux menaces courantes permet aux équipes de sécurité de se concentrer sur les incidents plus complexes nécessitant une expertise humaine.

Le module IPS/IDS de Palo Alto Networks se distingue par plusieurs caractéristiques avancées :

- Une base de données de signatures CVE / virus mise à jour quotidiennement par les chercheurs en sécurité de Palo Alto Networks

Des capacités d'analyse comportementale pour détecter des menaces zeroday, sans signature connue (option disponible dans la licence Advanced Threat Prevention, qui nécessite de transférer les logs vers le cloud Palo en temps réel – c'est une option qui n'a pas été retenue. Pour raisons de sécurité chez Orange les logs ne sont pas transférés à un tiers)

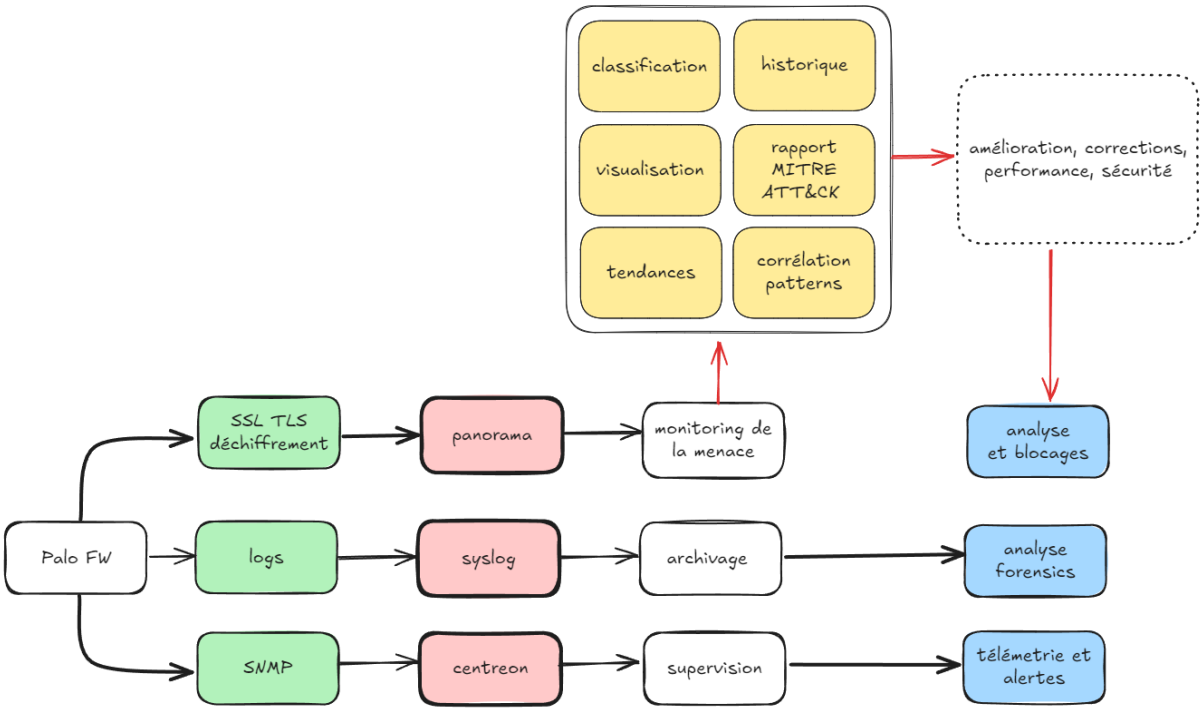
- Une intégration native avec les autres fonctionnalités de sécurité du firewall
- Des options de réponse granulaires, de la simple alerte au blocage automatique des adresses IP malveillantes

L'implémentation de ce module s'inscrit dans une approche globale de renforcement de la sécurité réseau, visant à protéger à la fois l'infrastructure interne et les services exposés sur Internet.

Configuration du monitoring des vulnérabilités

La configuration du monitoring des vulnérabilités constitue la première étape dans la mise en œuvre du module IPS/IDS. Cette configuration repose sur plusieurs éléments qui permettent une détection efficace des tentatives d'exploitation de vulnérabilités connues.

Architecture du monitoring des vulnérabilités et de la supervision



Le trafic réseau externe vers interne transite par les firewalls Palo Alto.

- Le module IPS/IDS analyse le trafic en temps réel en utilisant des signatures de menaces
- Les menaces détectées sont bloquées et/ou signalées.
- **Les événements de sécurité sont enregistrés et consultables** via Panorama (avec une limite de rétention configurée) mais aussi disponibles sur de plus grandes plages de temps via syslog et Loki

Déchiffrement des flux

Pour que le module IPS/IDS puisse analyser efficacement le trafic chiffré, la première étape est de configurer les certificats et le déchiffrement SSL/TLS.

Le processus de configuration du déchiffrement comprend plusieurs étapes techniques :

1. **Import des certificats** : J'ai importé les certificats des services exposés dans les firewalls Palo Alto. Cette étape est essentielle pour permettre au firewall de déchiffrer le trafic destiné à ces services.
2. **Création de profils de déchiffrement** : J'ai configuré des profils spécifiques définissant les paramètres du déchiffrement, notamment :
    a. Les versions de TLS autorisées (TLS 1.2 et 1.3)
    b. Les algorithmes de chiffrement acceptées (RSA par exemple)
3. **Configuration des règles de déchiffrement** : J'ai créé des règles précises pour définir quel trafic doit être déchiffré, en fonction de critères comme :
    a. Les zones source et destination
    b. Les adresses IP concernées
    c. Les applications et services

4. **Exclusions de déchiffrement** : Dans des cas spécifiques nous pouvons exclure certaines IP du déchiffrement (par exemple des IPs partenaires)
5. **On vérifie que le déchiffrement est effectif**

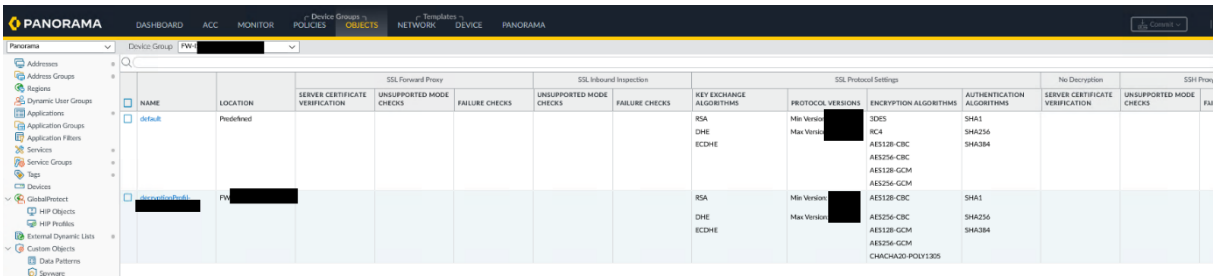


Figure 1919 Extrait des listes de profil de déchiffrement

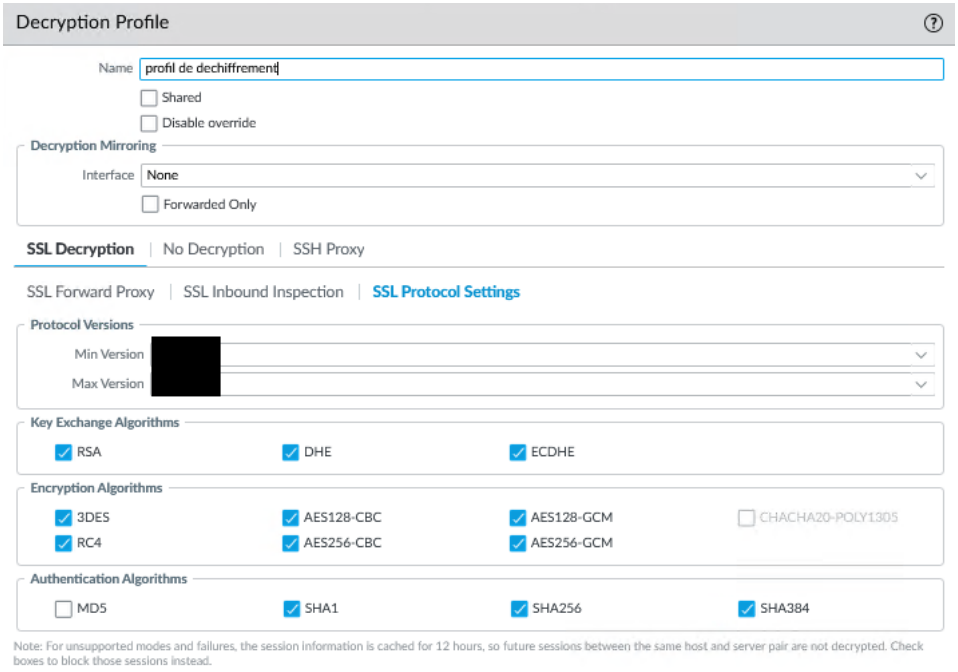


Figure 2020 Extrait de la configuration d'un profil de déchiffrement - algorithme chiffrement pris en charge

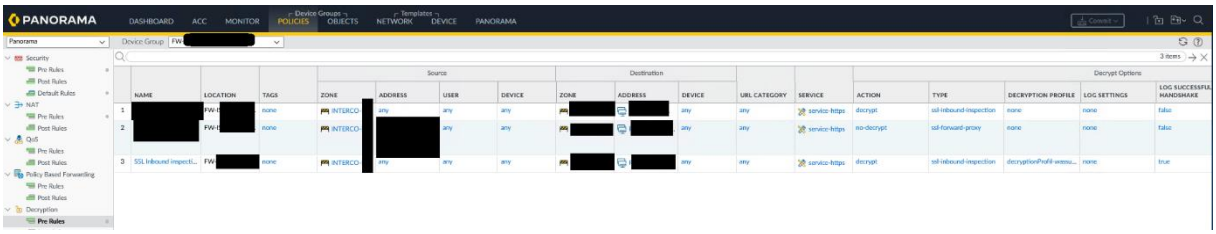


Figure 2121 Extrait de la liste des règles de déchiffrement

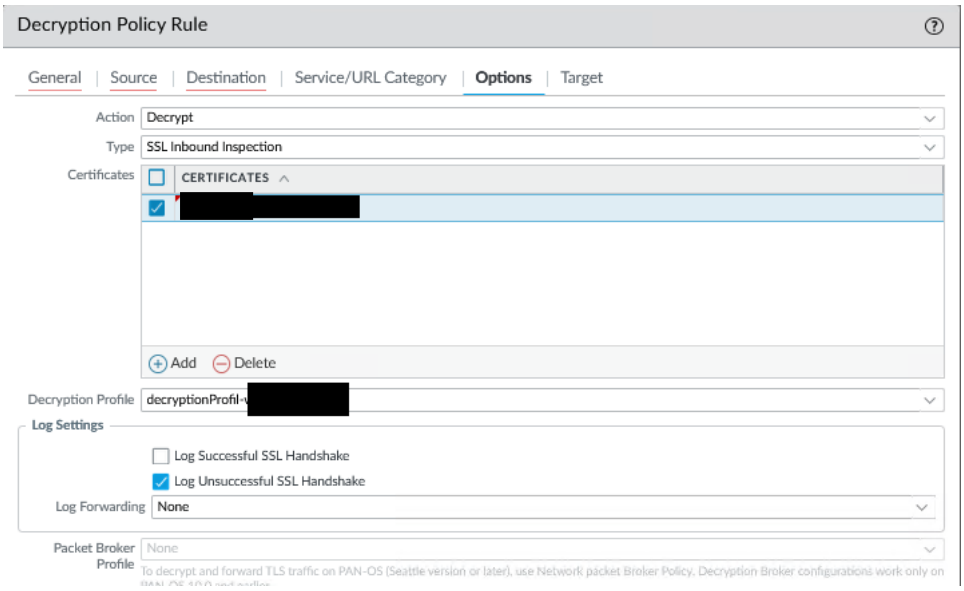
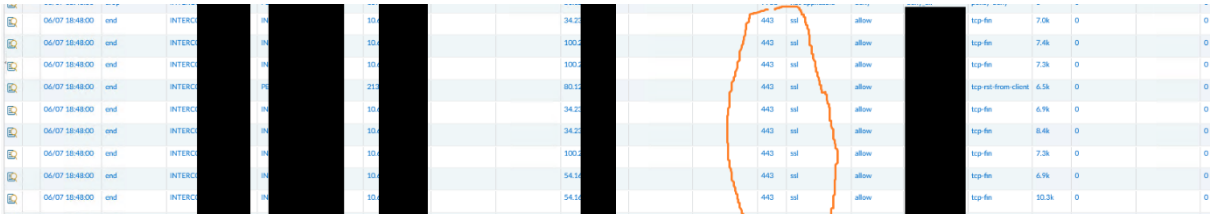
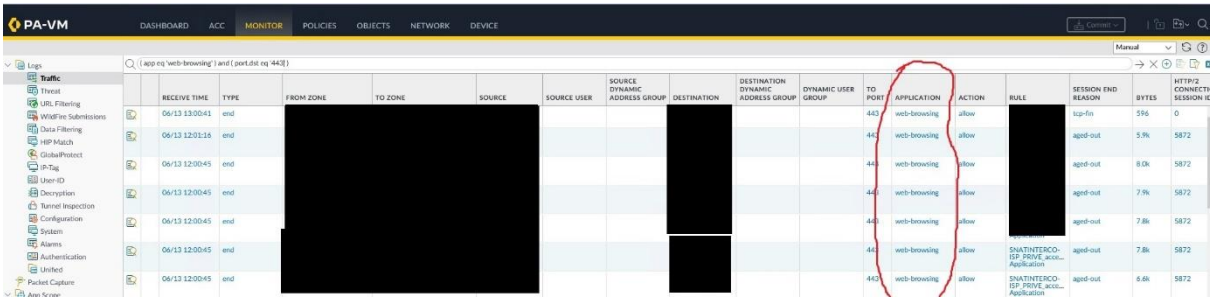


Figure 2222 Extrait de la configuration d'une règle de déchiffrement – choix du certificat associé au flux



Comme on peut le voir dans cette dernière capture, le flux n'est pas déchiffré car il est indiqué SSL (ce qui indique simplement le protocole de chiffrement). Si le flux était déchiffré nous pourrions savoir le type d'application utilisée pour l'échange (comme web-browsing par exemple). Voici une capture après déchiffrement fonctionnel.



On peut lire ici le type d'application qui est utilisée (web-browsing) ce qui indique que le flux est bien déchiffré.

A noter que cette configuration de déchiffrement est délicate car il faut vérifier l'impact sur les performances. Toutefois les équipements Palo étant dimensionnés de base pour des très grosses structures, le déchiffrement du trafic actuel chez Orange Réunion ne provoque très peu voire pas d'impact notable.

Profils de protection (CVE, sévérités, actions)

Après la configuration du déchiffrement, la création de profils de protection contre les vulnérabilités est essentielle. Adaptés aux besoins du S.I d'Orange Réunion (c'est-à-dire adapté aux différents systèmes d'exploitation et services), ces profils définissent les vulnérabilités surveillées et celles qui ne le sont pas, et les actions du firewall en cas de tentative d'exploitation.

Ces profils s'appuient sur des bases de données de vulnérabilités (CVE) que Palo Alto met à jour quotidiennement grâce à ses équipes de recherche (UNIT 42). Ces mises à jour se font aussi grâce aux données remontées par ses clients connectés au cloud, permettant une analyse collaborative et en temps réel des menaces. J'ai mis en place l'automatisation de la mise à jour de ces bases de données.

Exemples de CVE Windows disponibles dans la base :

Si le profil surveille les CVE Windows, le flux déchiffré est comparé aux signatures de la base de données Palo Alto. La capture ci-dessous illustre des exemples de CVE Windows surveillées.

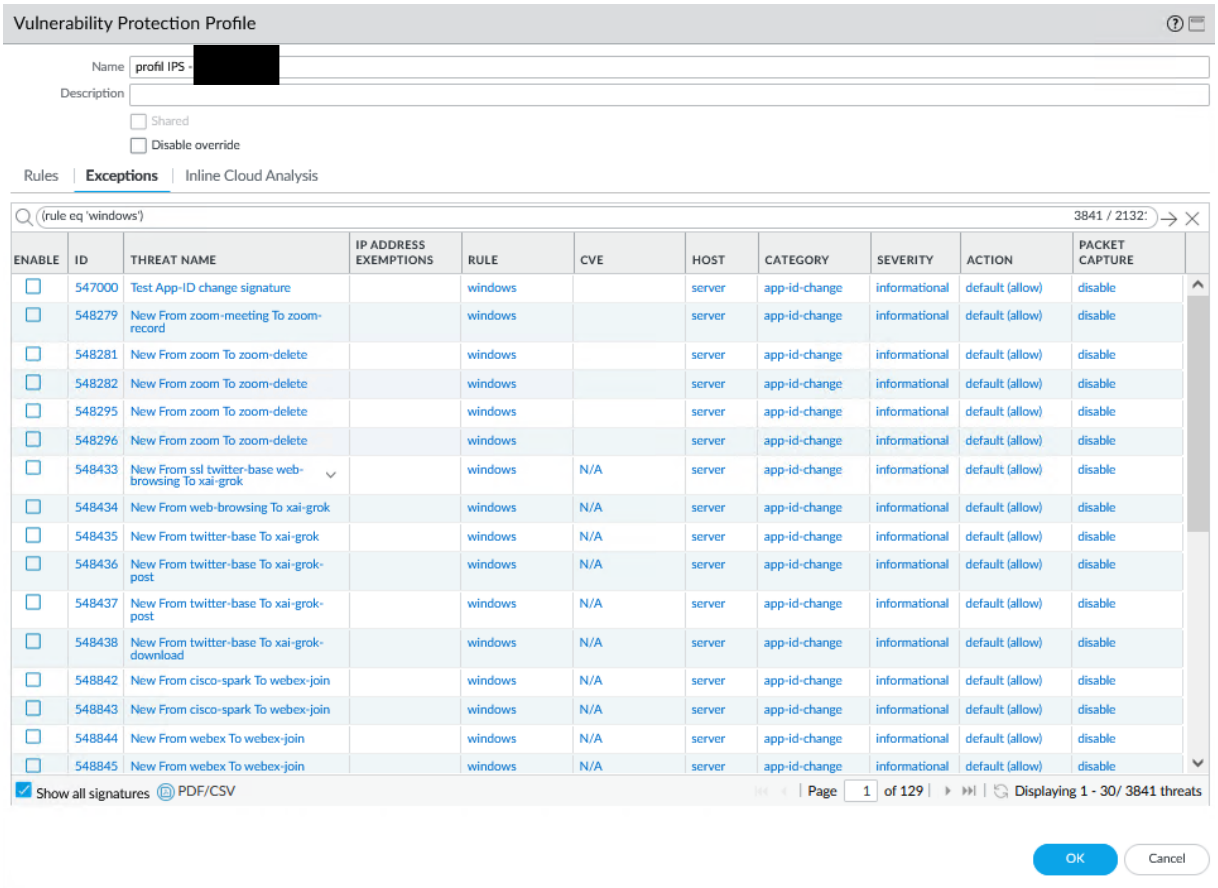


Figure 2323 Liste CVE Windows - extrait base de donnée Palo

Hiérarchie des règles de détection et d'action face aux CVE détectée

Les règles d'action suivent une approche hiérarchique basée sur la sévérité des vulnérabilités en quatre étapes.

Règles 1 et 2 : Les vulnérabilités critiques et hautes qui sont détectées dans les flux déchiffrés (selon la classification Palo) sont bloquées. Et même si l'OS ou service n'est pas présent dans l'architecture existante, l'adresse IP est bloquée.

Ce choix vise à contrer les tentatives d'attaques mais aussi à empêcher les attaquants d'explorer nos services, même si les CVE concernées ne concerne pas le S.I de Orange Réunion. En effet l'attaquant par l'utilisation d'une CVE critique a confirmé son intention malveillante.

Règle 3 : recherche les vulnérabilités de sévérité inférieure, mais conditionnellement à la présence du système, service ou application ciblé dans l'infrastructure. Cette approche, recommandée par Orange Cyberdéfense, optimise les performances en évitant une comparaison systématique avec l'ensemble de la base de données, particulièrement important pour les environnements à trafic élevé.

Règle 4 : compare les CVE restantes (ni critiques, ni hautes, ni liées à un système/application/service existant) avec l'ensemble de la base de données, en dernier recours.

1. **Règle pour les vulnérabilités critiques** :
    - Nom : "Rule Critical"
    - Menace : Any (toutes les menaces)
    - CVE : Any (toutes les CVE)
    - Type d'hôte : Server (serveurs)
    - Sévérité : Critical
    - Action : Block-IP (blocage de l'adresse IP source)
2. **Règle pour les vulnérabilités de sévérité élevée** :
    - Nom : "Rule High"
    - Menace : Any (toutes les menaces)
    - CVE : Any (toutes les CVE)
    - Type d'hôte : Server (serveurs)
    - Sévérité : High
    - Action : Block-IP (blocage de l'adresse IP source)
3. **Recherche de CVE pour les besoins spécifiques du S.I** :
    - Les profils de protection sont établis pour détecter en priorité les CVE exploitable sur les services, applications et systèmes existant dans le S.I de Orange.
    - Exemple : Si le S.I avait des OS Windows ou utilisait des gestionnaires d'API alors nous indiquerions en priorité dans les profils de comparer le trafic déchiffré avec la base de CVE de Windows et du gestionnaire d'API concerné.
4. **Règle de surveillance globale** :
    - Toutefois si aucune CVE n'a été trouvé dans les bases concernant les services spécifiques existant chez Orange, la dernière règle de surveillance indique de vérifier dans l'entièreté de la base de données.

Cette hiérarchisation des règles permet une réponse proportionnée aux menaces : actions strictes pour les vulnérabilités critiques, surveillance globale pour les autres, et optimisation des performances système.

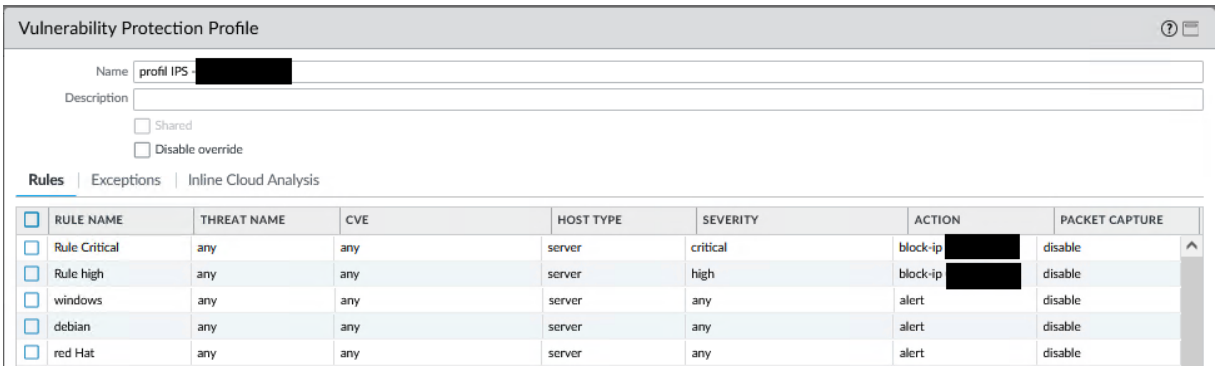


Figure 2424 Extrait de profil CVE et hiérarchie

Application des profils de vulnérabilités aux règles de sécurité (pour monitoring)

Après configuration, le profil de protection CVE est appliqué à un flux spécifique sur le firewall. Les paquets de ce flux sont déchiffrés puis analysés par rapport à la base de données de CVE. L'application du profil est visible dans la liste des règles par un logo dédié.

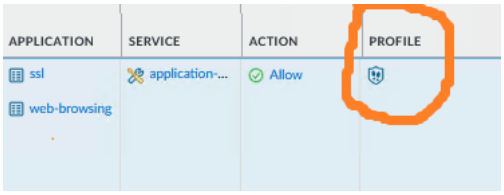


Figure 2525 Logo indiquant le déchiffrement du flux dans les règles de sécurité

La vérification du bon fonctionnement de l'analyse des menaces s'effectue via les logs. La capture ci-dessous confirme l'analyse effective des menaces.

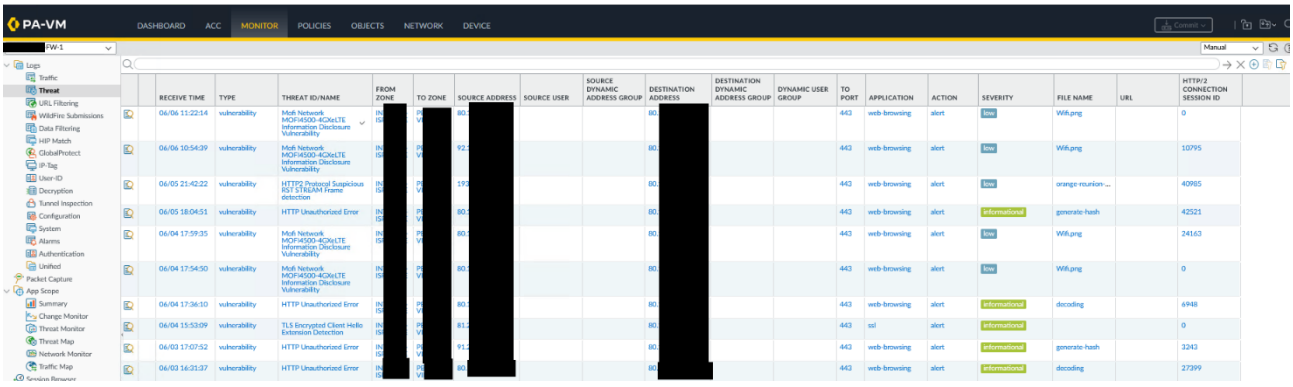


Figure 2626 Extrait des logs de menace

Analyse des logs et rapport

L'analyse des logs est essentielle à l'efficacité d'un système IPS/IDS. J'ai mis en place un processus manuel structuré d'analyse et de rapport pour optimiser l'exploitation de ces données et aider à la prise de décision.

Filtrage et analyse des logs

L'analyse des logs de menaces nécessite une approche méthodique pour gérer le volume important de données. J'ai donc créé des filtres spécialisés pour identifier rapidement les informations pertinentes. En voici quelques exemples :

Filtre pour les attaques critiques hors DoS :

```
( severity eq 'critical' ) and not ( name-of-threatid eq 'TCP
Flood' )
```

Ce filtre permet d'identifier les alertes critiques tout en excluant les nombreuses alertes de type DOS TCP Flood (attaque par saturation) qui peuvent masquer les menaces les plus importantes et plus élaborées.

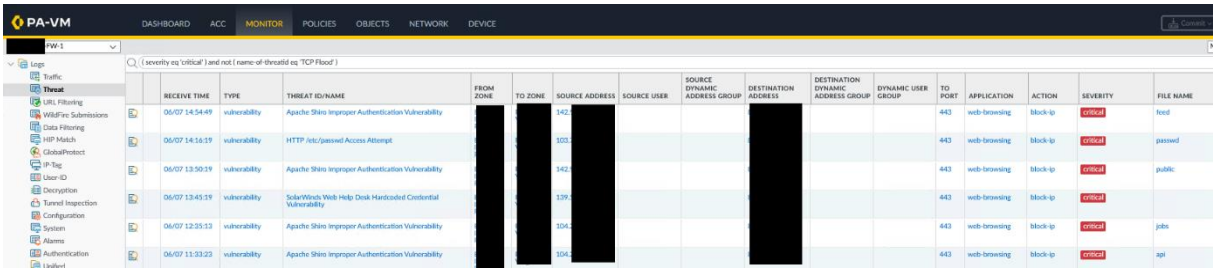


Figure 2727 Extrait des logs de menace filtrés

Filtre pour les scans Git :

```
( name-of-threatid eq 'Gitscanner Traffic Detected' )
```

Ce filtre détecte les scans de répertoires Git, souvent une phase de reconnaissance précédant des attaques plus sérieuses. Ces répertoires peuvent contenir des informations sensibles (secrets, clés API) laissées par inadvertance par les développeurs. L'objectif de ces reconnaissances est de cartographier l'infrastructure pour préparer des attaques futures.

La détection de ces activités de reconnaissance permet :

- D'identifier les adresses IP suspectes
- D'établir des corrélations avec d'autres attaques ultérieures
- De confirmer les intentions malveillantes avant d'appliquer des mesures de blocage

Cette approche progressive renforce la sécurité préventive sans bloquer les utilisateurs légitimes, et permet d'analyser les attaques ciblant l'infrastructure d'Orange. Ces filtres optimisent l'analyse quotidienne des logs, réduisant le temps d'identification des menaces parmi le volume important d'alertes.

Rapport et visualisation

Pour exploiter, comparer et présenter les données des logs, j'utilise aussi les rapports visuels préconfigurés de l'équipement, des graphiques configurables sur l'interface de l'équipement, ainsi qu'un script Python d'analyse automatisée que j'ai développé pour des rapports plus détaillés et la création de liste IP de blocage **(voir annexes page 50 à 53)**. Ces rapports (PDF, CSV ou image) facilitent la communication et la prise de décision.

Configuration de la protection DoS et des zones de protection

Outre la détection des vulnérabilités, la protection contre les attaques DOS est cruciale. J'ai configuré des mécanismes de protection DOS pour préserver la disponibilité des services d'Orange Réunion. Le principe est simple : bloquer une adresse IP après un nombre X de tentatives de connexion par seconde.

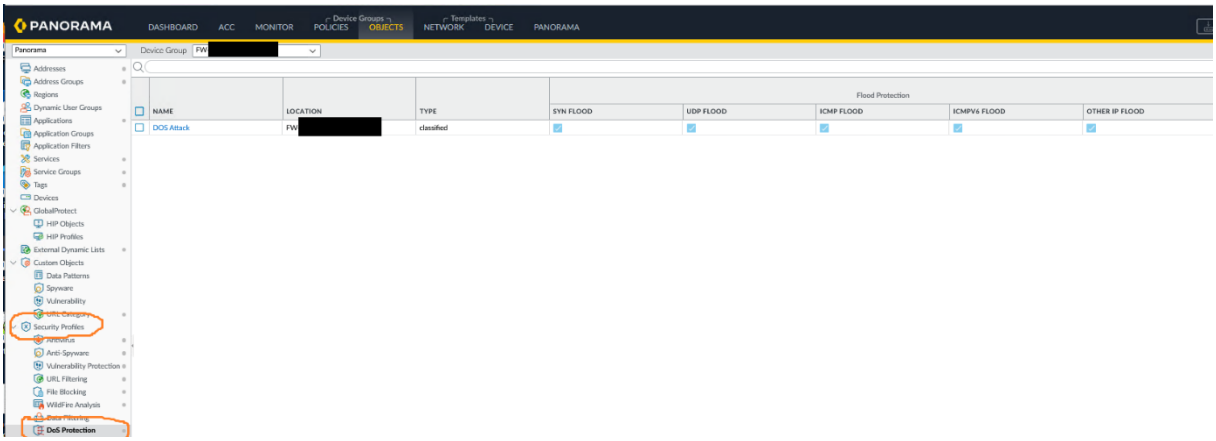


Figure 2828 Liste des DoS profile

Modes (AGGREGATE vs CLASSIFIED)

Palo Alto Networks propose deux modes principaux pour la protection contre les attaques DOS :

- **Mode AGGREGATE** : Dans ce mode, les seuils s'appliquent à l'ensemble du trafic d'une zone. Par exemple, si le seuil est fixé à 100 connexions par seconde (CPS), ce seuil s'applique au total des connexions de tous les utilisateurs vers tous les services de la zone, ce qui peut rapidement bloquer tous les accès aux services en cas d'attaque DDoS massive. C'est une mesure qui s'applique bien en seconde ligne de défense derrière des équipements dédiés à la gestion des attaques DDoS.
- **Mode CLASSIFIED** : Dans ce mode, les seuils s'appliquent individuellement à chaque flux spécifique. Par exemple, si le seuil est fixé à 100 CPS, chaque utilisateur peut établir jusqu'à 100 connexions par seconde vers chaque service distinct.

Après avoir étudié en détail les besoins spécifiques et la nature du trafic sur nos services critiques, j'ai choisi d'utiliser le mode **CLASSIFIED** pour la protection contre les attaques DOS.

Fonctionnement :

- Chaque flux ou utilisateur est surveillé indépendamment.
- Des seuils personnalisés (nombre de connexions par seconde) sont définis pour chaque flux / utilisateur
- Lorsqu'un flux/utilisateur dépasse ces seuils, des mesures de blocage ou de limitation sont appliquées uniquement à ce flux/utilisateur, sans affecter les autres.

Ce mode offre donc une détection plus précise des comportements anormaux. En optant pour cette approche, nous évitons de bloquer ou de limiter l'accès à l'ensemble des utilisateurs en cas

d'attaque ciblée ou d'activité malveillante d'un seul utilisateur. Cela permet une gestion plus fine et efficace de la sécurité, tout en maintenant la disponibilité des services pour la majorité des utilisateurs légitimes.

Création du profil DOS : Seuils (SYN FLOOD, UDP, ICMP) et temps de blocage

La protection DOS, comme les CVE, nécessite un profil. La configuration des seuils de blocage est délicate, nécessitant un équilibre entre sécurité et disponibilité, ainsi qu'une connaissance du SI et de son utilisation. L'accès aux outils d'analyse de trafic est essentiel. Après observation et ajustement, des seuils ont été définis pour éviter les faux positifs (exemples ci-dessous, non représentatifs des valeurs réelles d'Orange Réunion) :

1. **SYN FLOOD** (attaques visant à épuiser les ressources serveur par des connexions TCP incomplètes) :
    - Seuil d'alerte : 100 CPS (génération d'alertes à partir de 10 connexions par seconde)
    - Seuil maximal : 200 CPS (blocage complet de l'adresse IP)
    - Temps de blocage : 600 secondes (10 minutes)
2. **UDP / ICMP / Other IP FLOOD** (autres types d'attaques volumétriques) ont aussi leurs propres seuils.

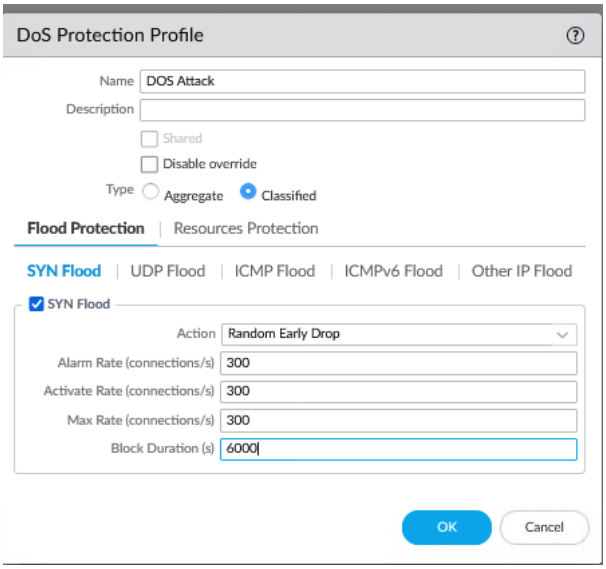


Figure 2929 Extrait de configuration du profil DOS (valeur arbitraire)

Création d'une règle DOS :

La création d'une règle DOS implique de définir la zone source, les adresses source à inclure/exclure (partenaires, services Orange), la destination, les services concernés (ex : https), et le profil DOS.

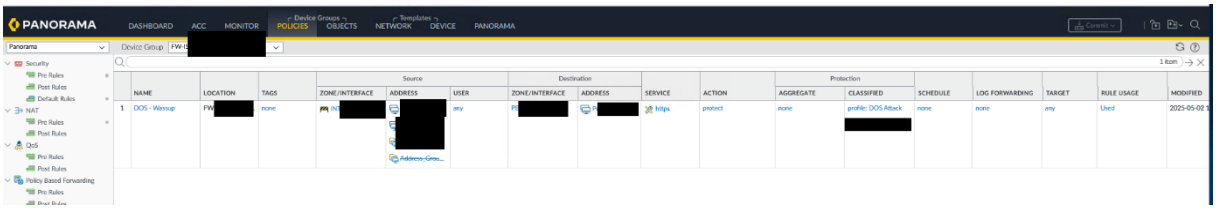


Figure 3030 Extrait des règles de protection DOS

Analyse sur l'utilisation de la règle DoS et BGP Flowspec

Limites des protections DOS sur firewall Palo Alto

Les fonctionnalités anti-DOS/DDoS intégrées aux firewalls Palo Alto ne constituent pas une solution de première ligne contre ces attaques. Bien qu'elles réduisent l'exposition, elles sont généralement précédées par :

- Des load balancers
- Des proxys dédiés
- Des équipements spécialisés anti-DDoS en amont

BGP Flowspec: une solution avancée contre les DDoS

Mes recherches durant l'alternance ont révélé que BGP Flowspec représente l'une des protections les plus efficaces contre les attaques volumétriques. Cette solution est particulièrement adaptée au contexte d'Orange Réunion, qui bénéficie d'Orange France comme fournisseur d'accès, facilitant ainsi son implémentation.

Fonctionnement de BGP Flowspec

Ce protocole opère selon le mécanisme suivant :

1. Lors d'une détection d'attaque, les équipements envoient automatiquement une alerte via BGP au routeur en amont
2. Ce routeur propage l'information sur toutes ses interfaces entrantes/sortantes
3. Le message se diffuse aux autres routeurs, y compris ceux d'autres fournisseurs compatibles avec BGP Flowspec
4. Les adresses IP impliquées dans l'attaque sont bloquées rapidement à la source, directement chez le fournisseur
5. Cette liste de blocage se propage via BGP à l'ensemble de l'infrastructure de routage

Cette approche représente probablement la solution la plus efficace contre les attaques DOS/DDoS à grande échelle.

Précisions techniques :

- BGP Flowspec (RFC 5575/8955) est une extension de BGP qui permet de distribuer des règles de filtrage de trafic plus granulaires que de simples préfixes IP
- Il permet de définir des règles basées sur plusieurs critères (IP source/destination, ports, protocoles, flags TCP, etc.)
- Les actions possibles incluent le drop, le rate-limiting, ou la redirection vers des scrubbing centers

Nuances à apporter :

- Tous les équipements réseau ne supportent pas BGP Flowspec, son déploiement nécessite des routeurs compatibles
- La propagation inter-opérateurs existe mais n'est pas automatique - elle dépend d'accords entre fournisseurs
- BGP Flowspec est particulièrement efficace pour les attaques volumétriques, mais moins pour certaines attaques applicatives sophistiquées

La solution BGP Flowspec serai pertinente à explorer contre les attaques volumétriques de type DDoS.

Configuration et utilisation des EDL builtin

Présentation des EDL et leur rôle dans la sécurité

Les External Dynamic Lists (EDL) sont un mécanisme puissant des firewalls Palo Alto qui permet de récupérer sur des serveurs web externes des listes d'adresses IP, d'URL ou d'autres objets, et de les utiliser dynamiquement dans les règles de sécurité. L'avantage majeur de ce système est qu'il permet de mettre à jour ces listes sans avoir à effectuer un commit.

Dans le cas des EDL built-in, il s'agit d'un cas particulier où Palo Alto Networks fournit directement des listes d'adresses IP malveillantes dans le cadre de la licence Advanced Threat Prevention. Ces listes sont intégrées à la base de données antivirus mise à jour quotidiennement, et constituent une source précieuse de renseignements sur les menaces.

Lors de mes recherches dans la documentation Palo Alto, j'ai découvert que ces listes étaient disponibles mais non exploitées dans notre infrastructure. Leur intégration représentait donc une opportunité significative d'amélioration de notre posture de sécurité sans coût supplémentaire.

Types de listes et leur pertinence

Palo Alto Networks fournit quatre catégories principales d'EDL built-in, chacune ciblant un type spécifique de menace :

- **Adresses IP à haut risque (High-Risk)** : Contient des adresses IP signalées comme malveillantes par des organisations tierces de confiance. Ces adresses sont associées à diverses activités suspectes mais n'ont pas été directement vérifiées par Palo Alto Networks.
- **Adresses IP malveillantes connues (Known-Malicious)** : Regroupe des adresses IP vérifiées comme malveillantes par les analyses WildFire et les recherches Unit 42 de Palo Alto Networks. Ces adresses sont utilisées presque exclusivement pour distribuer des logiciels malveillants ou pour des activités de commande et contrôle.
- **Adresses IP d'hébergeurs bulletproof (Bulletproof)** : Liste les adresses IP fournies par des hébergeurs qui imposent peu ou pas de restrictions sur le contenu, souvent utilisés par les attaquants pour héberger du contenu malveillant.

- **Adresses IP des nœuds de sortie Tor** : Identifie les nœuds de sortie du réseau Tor, qui peuvent être légitimes mais sont souvent associés à des activités malveillantes dans les environnements d'entreprise.

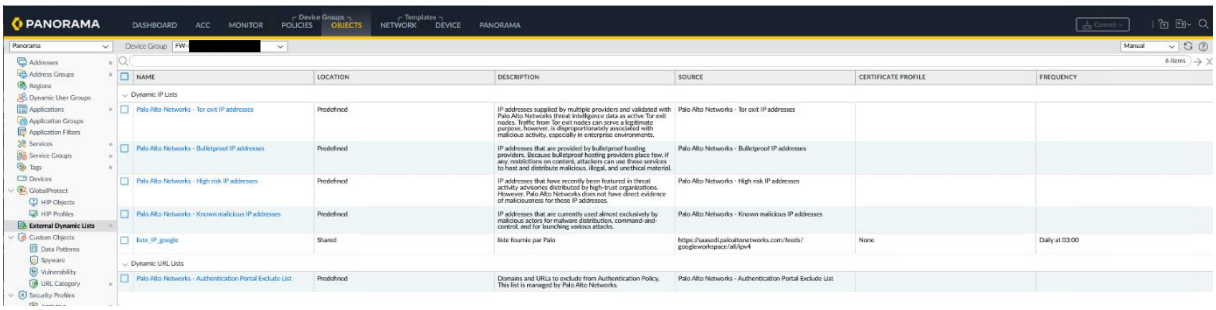


Figure 3131 Liste EDL Palo builtin - listes IP malveillantes

Après analyse, j'ai déterminé que les trois premières catégories étaient particulièrement pertinentes pour notre contexte et devaient être intégrées en priorité dans nos règles de blocage.

Implémentation dans les règles de sécurité

Pour exploiter efficacement ces listes, j'ai conçu une stratégie d'implémentation en plusieurs étapes :

1. **Activation des mises à jour** : Pour afficher les listes nous devions faire une mise à jour des bases de données anti-virus (que nous n'utilisions pas initialement car un autre équipement est dédié à la protection des couches applicatives, un WAF - Web Application Firewall).
2. **Création de règles de sécurité dédiées** : J'ai créé des règles de blocage spécifiques pour chaque type de liste, positionnées en tête de la politique de sécurité pour qu'elles soient efficaces.
3. **Séparation des listes** : Contrairement à une approche qui aurait consisté à regrouper toutes les listes dans une seule règle, j'ai délibérément créé une règle distincte pour chaque liste. Cette approche permet une analyse plus fine de l'efficacité de chaque liste via les compteurs de hits.

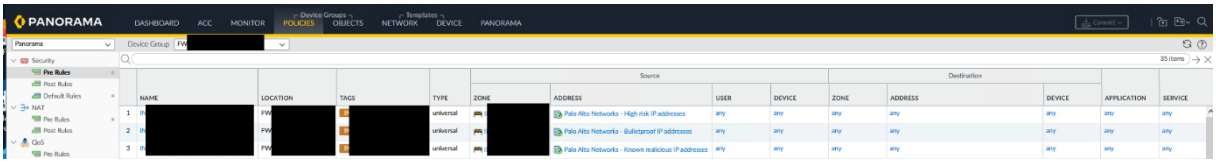


Figure 3232 Extrait des trois premières règles de sécurité pour filtrer les IPmalveillantes

Analyse de l'efficacité et résultats obtenus

Après la mise en place des règles EDL built-in, j'ai mis en place un suivi régulier pour évaluer leur efficacité :

1. **Analyse des hit counts** : les compteurs de hits sur chaque règle ont révélé que les listes "Known-Malicious" et "High-Risk" généraient le plus grand nombre de blocages, confirmant leur pertinence dans notre contexte. Et comme le montre le rapport d'analyse comparative statistique que j'ai réalisé, ces deux listes concentrent l'essentiel

des blocages, tandis que la liste "Bulletproof" n'a enregistré que peu de hit sur la période analysée.

2. **Rapport statistique** : J'ai effectué un rapport statistique analysant l'évolution des menaces avant et après ajout des EDL built-in. Ce rapport a démontré une réduction significative des tentatives de connexion suspectes après l'implémentation :
    - Réduction importante des alertes de sévérité moyenne en provenance de l'extérieur (hors France et Réunion)
    - Très forte diminution des alertes de sévérité moyenne pour les sources internationales
    - Forte baisse des alertes informationnelles
3. **Analyse des adresses uniques** : L'analyse comparative montre une évolution intéressante du nombre d'adresses IP uniques détectées :
    - Pour les attaques de type flood : réduction des adresses IP uniques
    - Pour les vulnérabilités hors TCP flood : légère augmentation des adresses IP uniques
    - Pour les sources internationales (hors France et Réunion) : réduction des adresses IP uniques
4. **Volumétrie globale** : La volumétrie totale des vulnérabilités hors TCP flood a significativement diminué, avec une baisse particulièrement marquée pour les alertes de sévérité moyenne.
5. **Faux positifs** : Un suivi attentif des faux positifs a été réalisé, en particulier concernant les alertes "HTTP Unauthorized Error" qui se répétaient fréquemment. L'analyse a montré que ces alertes n'ont pas d'impact significatif sur les résultats globaux ni sur les services légitimes. Cependant, il est important de communiquer ces faux positifs au SI afin qu'ils puissent vérifier si un défaut de mise à jour ou une autre anomalie applicative en est la cause.

L'intégration des EDL built-in a donc permis de bloquer efficacement les tentatives de connexion malveillantes, avec une réduction globale des alertes de X% pour les sources internationales, renforçant considérablement notre première ligne de défense contre les menaces connues.

Cette implémentation des EDL built-in illustre parfaitement comment la lecture des documentation et l'exploitation approfondie des fonctionnalités existantes peut significativement améliorer la posture de sécurité sans nécessiter d'investissements supplémentaires.

V. Automatisation des tâches de sécurité : une approche DevSecOps

Justification du besoin d'automatisation et gains attendus

L'administration quotidienne des firewalls Palo Alto implique de nombreuses tâches répétitives qui, bien qu'essentielles à la sécurité du réseau, consomment un temps considérable. Au cours

de mon alternance, j'ai rapidement identifié plusieurs processus manuels qui pouvaient bénéficier d'une automatisation :

- **Analyse des logs de menaces** : filtrage et évaluation de milliers d'alertes, nécessitant une corrélation sur plusieurs semaines de logs - tâche chronophage pour un analyste humain et peu efficiente comparée à un traitement automatisé
- **Génération des listes de blocage IP** issues de l'analyse des logs et leur implémentation dans les groupes d'adresses des firewalls
- **Génération de rapports de sécurité** pour les équipes techniques et managériales
- **Mise à jour des listes d'adresses** IP **d'autorisation**, notamment pour les services légitimes comme les robots de Google
- **Gestion et optimisation des règles de sécurité**

Face à ces constats, j'ai proposé une approche DevSecOps visant à automatiser ces tâches récurrentes. Cette démarche s'inscrit dans une vision plus large d'amélioration continue de la sécurité, où le code et l'automatisation deviennent des leviers d'efficacité opérationnelle.

Les gains attendus de cette automatisation sont multiples :

- **Gain de temps opérationnel** : Réduction du temps consacré aux tâches répétitives, permettant aux équipes de se concentrer sur des activités à plus forte valeur ajoutée
- **Amélioration de la réactivité** : Détection et réponse plus rapides aux menaces grâce à l'analyse automatisée et à la mise à jour dynamique des règles
- **Réduction des erreurs humaines** : Standardisation des processus d'analyse et de décision
- **Traçabilité accrue** : Historisation systématique des modifications via GitLab, facilitant les audits et le suivi des changements
- **Scalabilité** : Capacité à traiter un volume croissant d'alertes sans augmentation proportionnelle des ressources humaines
- **Transfert de connaissances** : Documentation implicite des processus à travers le code, facilitant la formation des nouveaux membres

Ce projet d'automatisation comporte un effort particulier sur la documentation, la traçabilité des actions, la maintenance du système et les procédures de debug en cas de défaillance.

Projets d'automatisation en cours : méthodes et avancement

Premier projet : Analyse automatisée des logs de menaces

Mon premier projet d'automatisation visait l'analyse des logs de menaces. J'ai développé un script fonctionnel générant des rapports et des listes de blocage à partir de l'historique des logs (plusieurs semaines). Ce script, utilisant un fichier CSV exporté de l'interface Palo Alto, offre différentes options d'analyse configurables via ligne de commande.

La VM dédiée à l'hébergement des scripts étant obsolète, une migration vers une nouvelle VM a été demandée (Python plus récent, accès GitLab, accès internet via proxy), ralentissant l'implémentation du script.

Entre temps le projet a été temporairement mis de côté pour un autre projet d'automatisation plus urgent, mais je souhaite le finaliser en intégrant une automatisation via l'API des Palo Alto, pour laquelle j'ai déjà réalisé des tests préliminaires.

Second projet : Automatisation des listes IP Googlebots

Entre-temps, un autre projet d'automatisation s'est présenté. Plusieurs adresses IP des robots crawler de Google aussi appelé googlebots, essentielles pour l'équipe marketing (pour référencement et revenus publicitaires) étaient bloquées par le firewall. Après investigation, nous avons identifié que les listes fournies par le département marketing étaient incomplètes - Google dispose en réalité de quatre listes d'IP pour ses robots, disponibles au format JSON sur developers.google.com.

La mise à jour manuelle de ces listes via l'interface CLI était trop chronophage, d'autant plus que ces listes peuvent changer fréquemment sans notification. Il fallait donc automatiser ce processus.

Réflexion sur l'approche d'automatisation

Deux approches principales ont été envisagées :

1. **Automatisation complète via Python et API Palo Alto** :
    a. Récupérer et parser les listes JSON avec python
    b. Les transformer en tableaux d'adresses IP
    c. Les pousser via l'API vers les groupes d'adresses du firewall
    d. Effectuer un commit
2. **Approche hybride avec EDL (External Dynamic Lists)** :
    a. Récupérer et parser les listes JSON via Python
    b. Générer des fichiers texte au format compatible EDL
    c. Héberger ces fichiers sur un serveur web interne
    d. Utiliser le système Palo des EDL pour récupérer la liste sans commit

J'ai opté pour la seconde approche, qui offre un meilleur équilibre entre automatisation et simplicité de maintenance.

Solution mise en œuvre

La solution que j'ai proposée et implémentée fonctionne ainsi :

1. Un script Python récupère les listes JSON des robots Google, les parse et les transforme en fichiers texte
2. Ces fichiers texte sont placés sur un serveur web interne https://adresseip/listeIP.txt
3. Le système EDL de Panorama requête ce serveur web et implémente dynamiquement les listes dans les règles de sécurité sans nécessiter de commit
4. En parallèle, les listes sont également versionnées dans GitLab pour assurer la traçabilité et permettre l'analyse historique

État d'avancement du projet

Actuellement disponible :

- VM script opérationnelle

- Autorisations proxy vers les sites concernés (paloaltonetworks.com et developers.google.com)
- Scripts de récupération et parsing des fichiers JSON
- Serveur web interne
- Script d'historisation vers GitLab

En cours de réalisation ou à venir :

- Fonction pour pousser les listes.txt sur le serveur web
- Ouverture des flux pour que Panorama puisse requêter le serveur web interne
- Documentation à jour sur l'ensemble du projet

Améliorations envisagées :

- **Mise en place des GitLab Runners dédiés (systèmes d'automatisation)**. *Les GitLab Runners dédiés sont des agents automatisés configurés pour exécuter des scripts de manière isolée et optimisée. Leur déploiement permet d'automatiser efficacement la compilation, les tests et le déploiement des applications, tout en assurant une meilleure gestion des ressources et une sécurité renforcée. Les GitLab Runners dédiés sont des agents automatisés configurés pour exécuter les pipelines CI/CD de manière isolée et optimisée. Leur déploiement permet d'automatiser efficacement la compilation, les tests et le déploiement des applications, tout en assurant une meilleure gestion des ressources et une sécurité renforcée.*
- **Implémentation d'une solution avancée de gestion des secrets (HashiCorp Vault**). ***HashiCorp Vault*** *serai utilisé pour stocker, gérer et distribuer en toute sécurité les secrets, tels que les clés API, mots de passe ou certificats. Cette solution garantit que les secrets sensibles ne sont pas exposés dans le code ou les scripts, renforçant ainsi la sécurité globale du système.*
- **Script de détection du % de changement dans la liste** à chaque mise à jour sur GitLab + alerting. *Un script serai déployé pour analyser les modifications apportées lors de chaque mise à jour dans GitLab, en calculant le pourcentage de changement dans la liste ou le contenu concerné. En cas de variation significative, des alertes sont générées pour permettre une réaction rapide, facilitant la détection d'éventuelles anomalies ou activités suspectes.*
- **Solution d'observabilité et surveillance**. *Une plateforme d'observabilité serai mise en place pour collecter, visualiser et analyser en temps réel les métriques, logs et événements du système. Cela permet de suivre la performance, détecter rapidement les incidents et assurer une maintenance proactive.*
- **Redondance du système de VM**

Architecture DevSecOps proposée

Séparation des rôles et flux unidirectionnels

L'architecture repose sur une séparation claire des responsabilités et une forte isolation de sécurité :

- GitLab : Plateforme centrale pour le stockage du code, la gestion des versions et le déploiement des scripts via des Runner. GitLab héberge les scripts d'automatisation et gère les secrets nécessaires à leur exécution.
- **VM Script** : Serveur dédié à l'exécution des scripts qui interagissent avec les équipements internes (firewalls Palo Alto, Panorama). Cette machine dispose d'accès Internet limités via un proxy.

Cette séparation permet d'établir des flux unidirectionnels et contrôlés :

- Les données externes sont récupérées par la VM Script, puis transmises à GitLab
- GitLab stocke ces données et les met à disposition des scripts
- Les scripts sont déployés sur la VM Script via des GitLab Runners
- La VM Script exécute les scripts mais n'interagit pas directement avec les équipements réseau
- Panorama a l'autorisation d'aller récupérer la liste texte sur l'adresse du serveur web, mais la VM ne peut rien effectuer en direction des firewalls ni de Panorama

Sécurité réseau renforcée

La sécurité de l'infrastructure d'automatisation a été une préoccupation centrale :

- **Canaux sécurisés SSL/TLS** : Communications chiffrées par certificat entre Panorama et le serveur web
- **Filtrage strict par firewall** : Règles précises limitant les flux réseau aux seuls échanges nécessaires
- **Authentification via TOKEN (jeton d'authentification)** : Accès sécurisé à GitLab
- **Rotation des secrets** : Procédure de renouvellement régulier des tokens

Gestion du code avec GitLab

GitLab constitue la pierre angulaire de l'approche DevSecOps. Grâce à ces projets d'automatisation j'ai pu commencer ma montée en compétence sur son utilisation avancée.

- **Centralisation sécurisée du code** : Repositories avec contrôles d'accès granulaires et protection des branches principales
- **Gestion des secrets** : Variables d'environnement sécurisées pour stocker les informations sensibles
- **Runners dédiés** : Exécution des scripts dans un environnement contrôlé. Les runners permettent d'éxécuter des scripts sur la VM (sans que les scripts soient présents sur la VM – ils sont dans gitlab).
- **Traçabilité complète** : Historique détaillé des modifications avec messages de commit explicites

Voir les fonctions et le code implémenté → en annexes page 53

Cette solution complète permet une mise à jour automatique et sécurisée des listes d'IP des robots google, tout en écoutant au mieux les besoins de l'équipe réseaux IP et résous un problème important pour l'équipe de marketing.

Méthodes et outils

Cette expérience m'a permis de développer une expertise technique sur divers outils en demande actuellement. J'ai utilisé stratégiquement tout ce qui est le plus en demande et ce qui permet d'augmenter la productivité.

Langages et bibliothèques

- **Python :** Développement des scripts d'automatisation avec utilisation des bibliothèques requests pour les appels API, json pour le parsing des données, subsystem et os pour faire appel de commandes bash comme CURL et utiliser des variables d'environnements lors de mes tests.
- **Bash :** utilisation de commande simple pour l'automatisation des t
- **JSON et CSV :** Manipulation de structures de données complexes pour le traitement des informations extraites des fichiers JSON et CSV

Outils DevSecOps

- **GitLab :** Gestion de version avec branches protégées, CI/CD pour le déploiement automatisé, et sécurisation des pipelines
- **API REST :** Interaction programmatique avec les systèmes Palo Alto et services externes Google
- **Confluence :** Pour la documentation collaborative

Méthodologie et bonnes pratiques

- **Clean Code :** Développement modulaire avec fonctions bien documentées et nommage explicite
- **Gestion des secrets :** Implémentation de variables d'environnement sécurisées
- **Documentation du code :** Commentaires détaillés expliquant la logique et les fonctionnalités

Outils d'assistance au développement

- **IA (Intelligence artificielle)** : Utilisation d'outils IA internes à Orange pour accélérer le développement, notamment pour la création d'un script d'analyse de logs de plus de 1300 lignes en une semaine. Pour les googlesbots qui étaient assez simples à réaliser je n'ai pratiquement utilisé ce procédé. Ces outils, non connectés au réseau externe, garantissent la sécurité des données traitées
- **VSCode :** Exploitation des extensions pour Python et Git
- **Debbug :** Utilisation de techniques de débogage pour identifier et résoudre les problèmes

Ces projets d'automatisation ont constitué une opportunité exceptionnelle d'appliquer mes connaissances en programmation et en sécurité, tout en développant une vision DevSecOps intégrée.

VI. Collaboration, communication et documentation

La réussite des projets de sécurité réseau repose non seulement sur l'expertise technique, mais aussi sur une collaboration efficace et une documentation rigoureuse. Comme je l'ai expliqué tout au long des sections précédentes, cette dimension a constitué une part importante de mon alternance.

Interactions avec les équipes

J'ai collaboré avec diverses équipes aux priorités et contraintes spécifiques :

Équipe Systèmes d'Information (SI)

Cette collaboration m'a permis de comprendre les contraintes applicatives et d'adapter les configurations réseau en conséquence

Consultants Orange Consulting (OCD)

J'ai bénéficié de formations sur Palo Alto, Panorama et IPS/IDS, incluant des ateliers techniques, un transfert de compétences sur les fonctionnalités avancées, et des revues conjointes de configurations.

Cette collaboration avec des experts externes a constitué une opportunité précieuse d'apprentissage sur une technologie premium largement utilisée à l'international.

Documentation et outils collaboratifs

Confluence a servi de plateforme centrale pour :

- Créer des espaces dédiés à chaque projet
- Centraliser la documentation technique
- Suivre l'avancement des projets

J'ai développé plusieurs types de documentation :

- **Tutoriels détaillés** sur la configuration du module IPS/IDS, la gestion des certificats, les mises à jour, et l'analyse des logs
- **Recueils de configurations** documentant les profils de protection, les zones de sécurité, et les règles pour services critiques
- **Processus formalisés** pour l'analyse des logs, le blocage d'IP malveillantes, et les décisions de mise à jour

Rapport et communication

J'ai maintenu une communication régulière avec l'équipe :

- Rapports quotidiens à mon tuteur
- Synthèses hebdomadaires des missions pour le management
- Partage systématique des incidents et modifications avec toute l'équipe pour assurer la continuité opérationnelle

Cette approche structurée de la documentation et de la communication a contribué à la pérennisation des connaissances et à l'harmonisation des pratiques au sein de l'équipe.

VII. Conclusion et perspectives

Au terme de cette alternance chez Orange Réunion, je dresse un bilan des réalisations accomplies et des perspectives d'évolution pour l'infrastructure de sécurité.

Synthèse des réalisations et des bénéfices

Cette année d'alternance a été marquée par plusieurs réalisations significatives qui ont contribué à renforcer la posture de sécurité d'Orange Réunion.

Amélioration de la posture de sécurité

L'optimisation du module IPS/IDS des firewalls Palo Alto a renforcé la protection du réseau grâce à :

- La mise en place des profils de protection CVE et de surveillance des menaces
- La configuration des profils DOS contre les attaques volumétriques
- L'intégration des EDL pour le blocage automatisé des adresses IP malveillantes
- L'analyse structurée des logs permettant d'identifier et bloquer les attaques ciblées

Gains d'efficacité grâce à l'automatisation

L'approche DevSecOps mise en œuvre a permis :

- L'automatisation de la mise à jour des listes d'adresses IP des robots Google
- Le traitement d'un volume croissant d'alertes via des scripts d'analyse
- La création d'une architecture d'automatisation évolutive

Documentation complète et structurée

La documentation technique élaborée constitue un héritage durable :

- Tutoriels détaillés sur la configuration du module IPS/IDS
- Recueils des configurations et choix techniques
- Processus formalisés pour le traitement des incidents
- Documentation des scripts d'automatisation

Cette documentation pérennise les connaissances au sein de l'équipe et réduit la dépendance aux expertises individuelles.

Limites et axes d'amélioration

L'architecture actuelle présente des opportunités d'amélioration :

- Protection DOS et DDoS à renforcer
- Intégration limitée avec les autres solutions de sécurité d'Orange France

- Absence d'automatisation dans la corrélation des événements de sécurité entre les différents équipements (ex : F5, proxy, Palo)
- Visibilité insuffisante sur les menaces persistantes avancées

Je préconise :

- La mise en place de processus supplémentaire dans la prévention des DDoS
- L'intégration avec un SIEM (Security Information and Event Management) local pour centraliser la corrélation des événements
- L'exploration de solutions d'analyse comportementale pour les menaces avancées
- La connexion au SOC d'Orange France pour une vision globale de la sécurité

Perspectives d'évolution

Au-delà des améliorations identifiées, plusieurs perspectives d'évolution se dessinent pour l'infrastructure de sécurité d'Orange Réunion.

Protection DDoS avancée (BGP Flowspec)

Une évolution majeure consisterait à renforcer la protection contre les attaques DDoS volumétriques en implémentant BGP Flowspec:

- Cette technologie permettrait de propager rapidement des règles de filtrage jusqu'aux routeurs de bordure, bloquant les attaques avant qu'elles n'atteignent les firewalls.
- L'intégration avec les mécanismes de détection existants créerait une défense en profondeur plus robuste.
- La capacité à répondre aux attaques volumétriques serait considérablement améliorée, protégeant ainsi la disponibilité des services critiques.

J'ai initié une étude de faisabilité sur cette solution, qui pourrait constituer un projet structurant pour l'année à venir.

Connexion avec le SOC Orange France

Une autre perspective prometteuse serait l'établissement d'une connexion avec le SOC (Security Operations Center) d'Orange France :

- Cette intégration permettrait de bénéficier d'une expertise étendue et d'une vision plus globale des menaces.
- Le partage d'informations tel que les logs de menaces renforcerait la capacité de détection précoce.
- L'accès à des ressources d'analyse avancées compléterait les capacités locales.

Des discussions préliminaires ont été engagées avec les équipes du SOC, et cette initiative pourrait se concrétiser dans les prochains mois.

Utilisation de l'IA pour l'analyse comportementale avancée des logs de menace

Enfin un projet que j'ai proposé et qui a pu commencer à être discuté avec l'équipe IA DATA, celle d'utiliser l'IA dans le processus d'analyse des logs de menaces afin d'obtenir tout comme mon

script python, une analyse fine, des détections de schémas d'attaques, des listes IPà bloquer et des rapports complets.

Compétences acquises et développées

Cette alternance m'a permis de développer un large éventail de compétences complémentaires:

Compétences techniques

- Maîtrise des firewalls Palo Alto et du module IPS/IDS
- Compréhension approfondie des mécanismes d'attaque et de défense
- Programmation Python pour l'automatisation des tâches de sécurité
- Utilisation des API REST pour l'intégration de systèmes hétérogènes
- Architecture réseau (zones, flux, segmentation)
- Utilisation avancée de l'IA pour développement de code

Compétences méthodologiques

- Documentation technique structurée
- Conception de processus d'automatisation
- Analyse systématique des logs et prise de décision
- Gestion de projet appliquée à la sécurité

Compétences relationnelles

- Communication avec différentes parties prenantes
- Collaboration en équipe pluridisciplinaire
- Présentation de sujets techniques complexes
- Gestion des priorités en environnement opérationnel

Compétences DevSecOps

- Intégration de la sécurité dans les processus d'automatisation
- Utilisation de GitLab pour la gestion du code
- Conception d'architectures sécurisées

Cette expérience a créé un pont entre mes connaissances théoriques universitaires et leur application concrète dans un environnement d'entreprise complexe.

Obstacles rencontrés

Au-delà des réalisations présentées dans ce rapport, mon parcours d'alternance a été jalonné de nombreux défis techniques et opérationnels.

Complexité technique et courbe d'apprentissage

La prise en main des équipements Palo Alto a représenté un défi majeur. Malgré mes connaissances préalables en réseaux, la documentation parfois fragmentée, les spécificités de

PAN-OS et les interactions avec l'infrastructure virtualisée ont exigé plusieurs semaines d'adaptation.

Défis opérationnels en environnement critique

Intervenir sur l'infrastructure d'un opérateur télécom implique des contraintes strictes. Par exemple, les fenêtres d'intervention importantes sont limitées, les processus de validation impliquent de multiples parties prenantes et les risques élevés d'impact sur les services critiques ont nécessité une approche méthodique incluant des plans de retour en arrière (rollback).

Défis d'automatisation et DevSecOps

L'implémentation (débutante) de l'approche DevSecOps a représenté un territoire inexploré, avec des contraintes d'accès réseau compliquant le déploiement des outils (il faut ouvrir des flux entre les différentes zones, ce qui nécessite d'interagir avec de nombreux équipements différents), plus une nécessaire montée en compétence sur GitLab.

Face à ces défis, j'ai appris à décomposer chaque projet en modules indépendants testables individuellement, ce qui m'a permis d'avancer méthodiquement.

Cette expérience m'a démontré que la maîtrise s'acquiert surtout par la confrontation méthodique aux problèmes réels, la persévérance face aux échecs initiaux et particulièrement grâce au développement d'une patience face aux difficultés techniques.

Lien entre les compétences acquises à l'université et leur application en entreprise

Les cours de sécurité réseau, programmation et administration système ont directement alimenté mes missions quotidiennes, tandis que la méthodologie de résolution de problèmes acquise en formation s'est révélée précieuse face aux défis techniques.

Réciproquement, cette immersion professionnelle a enrichi ma compréhension académique en l'ancrant dans des problématiques réelles. Les contraintes opérationnelles et les enjeux de sécurité d'un opérateur télécom ont donné une nouvelle dimension à mes connaissances théoriques.

Ressenti personnel sur l'alternance et les acquis professionnels

Cette année chez Orange Réunion a été particulièrement enrichissante. La confiance accordée par mon tuteur m'a permis de prendre des responsabilités significatives et de contribuer concrètement à l'amélioration de la sécurité de l'infrastructure.

J'ai apprécié la diversité des missions, alliant tâches opérationnelles et projets d'automatisation complexes. Cette polyvalence m'a offert une vision globale de la sécurité réseau et une compréhension des interactions entre les différentes composantes d'une infrastructure moderne.

Les défis techniques rencontrés ont stimulé ma créativité et ma capacité à résoudre des problèmes complexes. Au-delà des compétences techniques, cette alternance m'a permis de mûrir professionnellement dans ce nouveau domaine technologique que j'aborde en reconversion. J'ai développé mon sens des responsabilités et amélioré ma communication technique avec les différents professionnels du secteur.

VIII. Annexes

Glossaire des termes techniques

API (Application Programming Interface) : Interface permettant à différents logiciels de communiquer entre eux et d'échanger des données selon des règles prédéfinies.

APT (Advanced Persistent Threat) : Menace persistante avancée, type d'attaque où un attaquant établit une présence non détectée et prolongée dans un réseau ciblé.

BGP (Border Gateway Protocol) : est un protocole de routage utilisé pour échanger des informations de routage entre différents systèmes autonomes sur Internet

BGP Flowspec : Extension du protocole BGP permettant de distribuer des règles de filtrage du trafic réseau pour bloquer les attaques DDoS avant qu'elles n'atteignent leur cible.

Botnet : Réseau d'ordinateurs infectés contrôlés à distance par un attaquant, souvent utilisé pour des attaques DDoS.

Crawler Google : aussi appelé Googlebot, explore le web pour indexer les pages et améliorer la recherche sur Google.

Centreon : Plateforme de supervision et de monitoring des infrastructures informatiques.

CI/CD (Intégration Continue / Déploiement Continu) : pratique de développement logiciel qui automatise la construction, les tests et le déploiement des applications pour améliorer la rapidité et la fiabilité des livraisons.

CLI (Command Line Interface) : Interface en ligne de commande permettant d'interagir avec un système informatique via des commandes textuelles.

CSV (Comma-Separated Values) : est un format de fichier permettant de stocker des données tabulaires sous forme de texte, où chaque valeur est séparée par une virgule.

Commit : Action de valider et d'appliquer des modifications de configuration sur un équipement réseau ou dans un système de gestion de versions.

Contrôle des applications : Gestion et restriction de l'utilisation des logiciels ou applications sur un réseau ou un appareil.

Confluence : Logiciel de collaboration et de gestion de contenu en ligne.

CPS (Connections Per Second) : Nombre de connexions par seconde, métrique utilisée pour mesurer la charge sur un serveur ou un équipement réseau.

CVE (Common Vulnerabilities and Exposures) : Système de référencement standardisé des vulnérabilités de sécurité informatique connues.

DoS (Denial Of Service) : Attaque visant à rendre un service ou un réseau indisponible en le surchargeant de requêtes (venant d'une seule source).

DDoS (Distributed Denial of Service) : Attaque visant à rendre un service indisponible en le submergeant de requêtes provenant de multiples sources.

DevSecOps : Approche intégrant la sécurité dans le cycle de développement et d'exploitation des applications, combinant développement, sécurité et opérations.

DTRM (Direction Technique des Réseaux et Mobiles) : Division d'Orange responsable de la gestion technique des infrastructures réseau et mobile.

EDL (External Dynamic List) : Mécanisme permettant aux firewalls Palo Alto d'utiliser des listes d'adresses ou d'URL hébergées sur des serveurs externes.

ESXi : Hyperviseur de VMware permettant de créer et gérer des machines virtuelles directement sur le matériel physique sans nécessiter de système d'exploitation hôte.

Firewall : Équipement de sécurité filtrant le trafic réseau selon des règles prédéfinies pour protéger un réseau contre les accès non autorisés.

FQDN (Fully Qualified Domain Name) : Nom de domaine complet spécifiant la position exacte d'un hôte dans la hiérarchie DNS (ex: www.orange.fr).

GitLab : Plateforme de gestion de développement logiciel permettant le versioning du code, l'intégration continue et le déploiement continu.

GitLab Runner : Agent qui exécute les tâches d'intégration continue définies dans GitLab.

Googlebot : Robot d'indexation utilisé par Google pour explorer et indexer les pages web.

HA (High Availability) : Configuration en haute disponibilité permettant d'assurer la continuité de service en cas de défaillance d'un équipement.

HTTP Unauthorized Error : Erreur 401 indiquant qu'une authentification est nécessaire pour accéder à une ressource web.

ICMP (Internet Control Message Protocol) : Protocole utilisé pour diagnostiquer les problèmes de communication réseau, notamment via la commande ping.

IDS (Intrusion Detection System) : Système de détection d'intrusion qui surveille le trafic réseau pour identifier des activités suspectes.

IoC (Indicators of Compromise) : Indices techniques indiquant qu'un système a été compromis par une attaque informatique.

IoT (Internet of Things) : Internet des objets, désignant les appareils connectés à Internet autres que les ordinateurs traditionnels.

IP (Internet Protocol) : Protocole de communication fondamental d'Internet permettant l'adressage et le routage des paquets de données.

IPerf : Outil de test de performance réseau permettant de mesurer la bande passante maximale entre deux points.

IPS (Intrusion Prevention System) : Système de prévention d'intrusion capable non seulement de détecter mais aussi de bloquer automatiquement les tentatives d'intrusion.

JSON (JavaScript Object Notation) : Format de données textuelles utilisé pour l'échange d'informations structurées entre différents systèmes.

Load balancers : équipements qui répartissent le trafic réseau entre plusieurs serveurs pour optimiser la performance et la disponibilité des applications.

Logs : enregistrements chronologiques des événements et activités sur un système ou un réseau.

Loki : solution de gestion et d'analyse de logs conçue pour être intégrée avec Prometheus, permettant une recherche efficace et une visualisation des journaux. Prometheus est une plateforme de surveillance et d'alerte open source, principalement utilisée pour collecter, stocker et analyser des métriques en temps réel.

MCO (Maintien en Condition Opérationnelle) : Ensemble des activités visant à garantir le bon fonctionnement d'un système informatique.

MobaXterm : Terminal avancé pour Windows offrant des fonctionnalités multiples dont l'accès SSH, FTP, et X11.

NetBackup : Solution de sauvegarde d'entreprise développée par Veritas Technologies.

NGFW (Next-Generation Firewall) : Pare-feu de nouvelle génération intégrant des fonctionnalités avancées comme l'inspection approfondie des paquets et la détection d'intrusion.

NTLM (NT LAN Manager) : Protocole d'authentification Microsoft utilisé dans les environnements Windows.

OSPF (Open Shortest Path First) : est un protocole de routage dynamique utilisé pour déterminer le meilleur chemin dans un réseau informatique.

PAN-OS : Système d'exploitation des équipements Palo Alto Networks.

Panorama : Plateforme centralisée de gestion des firewalls Palo Alto Networks.

Proxy : Serveur intermédiaire agissant comme passerelle entre un utilisateur et Internet, pouvant filtrer les requêtes et masquer l'adresse IP de l'utilisateur.

RADIUS (Remote Authentication Dial-In User Service) : Protocole d'authentification, d'autorisation et de comptabilité pour les accès réseau.**RAN (Radio Access Network) :** Réseau d'accès radio permettant la connexion entre les appareils mobiles et le réseau principal.

REST (Representational State Transfer) : Style d'architecture pour les systèmes distribués, notamment utilisé pour les API web.

SIEM (Security Information and Event Management) : Solution permettant la collecte, l'analyse et la corrélation des événements de sécurité provenant de différentes sources.

SOC (Security Operations Center) : Centre opérationnel de sécurité chargé de surveiller et d'analyser la sécurité d'une organisation.

SSH (Secure Shell) : Protocole de communication sécurisé permettant l'accès distant à des équipements réseau.

SSL/TLS (Secure Sockets Layer/Transport Layer Security) : Protocoles cryptographiques assurant la sécurité des communications sur Internet.

SYN Flood : Type d'attaque DDoS exploitant le protocole TCP en envoyant un grand nombre de requêtes de connexion (SYN) sans les finaliser.

Syslog : Protocole standard pour la transmission de messages de journalisation dans un réseau informatique.

TCP (Transmission Control Protocol) : Protocole de communication fiable utilisé pour la transmission de données sur Internet.

TCP flood : est une attaque par déni de service qui submerge une cible en envoyant un grand nombre de paquets TCP pour la rendre inaccessible.

Token : Jeton d'authentification utilisé pour sécuriser l'accès aux API et aux services web.

Tor : Réseau d'anonymisation permettant de masquer l'origine du trafic Internet.

UDP (User Datagram Protocol) : Protocole de communication sans connexion utilisé pour des transmissions rapides mais moins fiables que TCP.

Unit 42 : Équipe de recherche en cybersécurité de Palo Alto Networks.

Filtrage URL : Processus de blocage ou d'autorisation d'accès à certains sites web en fonction de leur adresse URL (Uniform Resource Locator). L'URL c'est l'adresse web.

VM (Virtual Machine) : Machine virtuelle, émulation d'un système informatique complet.

VM-Series : Gamme de firewalls virtuels proposés par Palo Alto Networks.

VMware : Entreprise spécialisée dans les logiciels de virtualisation.

vMotion : Technologie VMware permettant de déplacer une machine virtuelle en fonctionnement d'un serveur physique à un autre sans interruption de service.

vSphere : Plateforme de virtualisation de VMware pour la gestion des infrastructures virtuelles.

Vulnérabilité : Faille de sécurité dans un système informatique pouvant être exploitée par un attaquant.

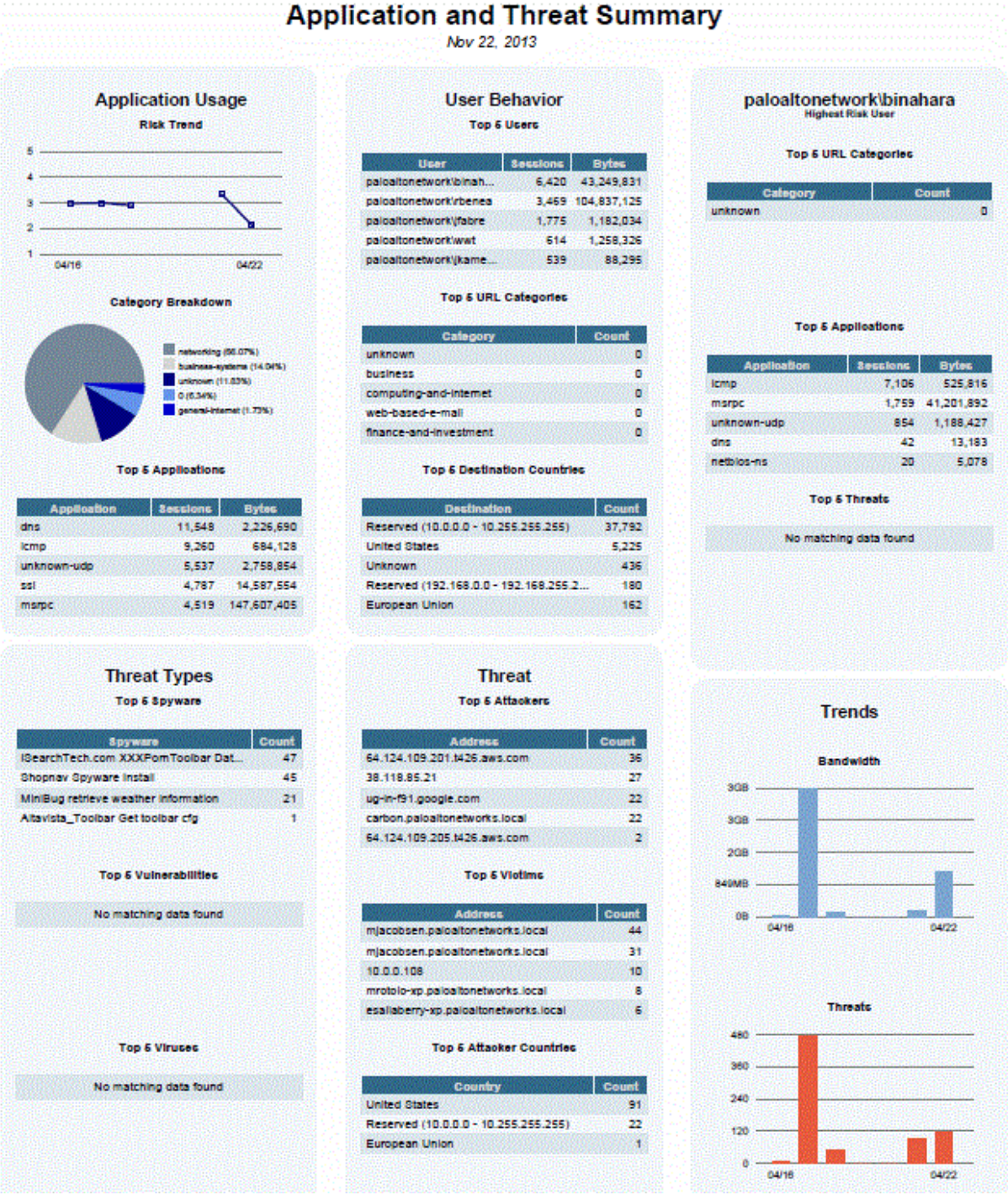
WAF (Web Application Firewall) : protège les applications web contre les attaques en filtrant et surveillant le trafic HTTP.

WildFire : Service cloud de Palo Alto Networks analysant les fichiers suspects pour détecter les logiciels malveillants inconnus.

Zone de sécurité : Segment logique d'un réseau défini dans un firewall, permettant d'appliquer des politiques de sécurité spécifiques.

Rapport de sécurité

Rapport autogénéré quotidiennement sur l'équipement (les données ne sont pas celles d'Orange)



Application and Threat Summary

Nov 22, 2013

Application Usage

Risk Trend

Category Breakdown

Top 5 Applications

Application	Sessions	Bytes
dns	11,548	2,226,690
icmp	9,260	684,128
unknown-udp	5,537	2,758,854
ssl	4,787	14,587,554
msrpc	4,519	147,607,405

User Behavior

Top 5 Users

User	Sessions	Bytes
paloaltonetwork\binah...	6,420	43,249,831
paloaltonetwork\rbenea	3,469	104,837,125
paloaltonetwork\jfabre	1,775	1,182,034
paloaltonetwork\wwt	614	1,258,326
paloaltonetwork\jkame...	539	88,295

Top 5 URL Categories

Category	Count
unknown	0
business	0
computing-and-internet	0
web-based-e-mail	0
finance-and-investment	0

Top 5 Destination Countries

Destination	Count
Reserved (10.0.0.0 - 10.255.255.255)	37,792
United States	5,225
Unknown	436
Reserved (192.168.0.0 - 192.168.255.2...	180
European Union	162

paloaltonetwork\binahara

Highest Risk User

Top 5 URL Categories

Category	Count
unknown	0

Top 5 Applications

Application	Sessions	Bytes
icmp	7,106	525,816
msrpc	1,759	41,201,892
unknown-udp	854	1,188,427
dns	42	13,183
netbios-ns	20	5,078

Top 5 Threats

No matching data found

Threat Types

Top 5 Spyware

Spyware	Count
ISearchTech.com XXXPornToolbar Dat...	47
Shopnav Spyware Install	45
MiniBug retrieve weather information	21
Altavista_Toolbar Get toolbar cfg	1

Top 5 Vulnerabilities

No matching data found

Top 5 Viruses

No matching data found

Threat

Top 5 Attackers

Address	Count
64.124.109.201.t426.aws.com	36
38.118.85.21	27
ug-in-f91.google.com	22
carbon.paloaltonetworks.local	22
64.124.109.205.t426.aws.com	2

Top 5 Victims

Address	Count
mjacobsen.paloaltonetworks.local	44
mjacobsen.paloaltonetworks.local	31
10.0.0.108	10
mrotolo-xp.paloaltonetworks.local	8
esaliaberry-xp.paloaltonetworks.local	6

Top 5 Attacker Countries

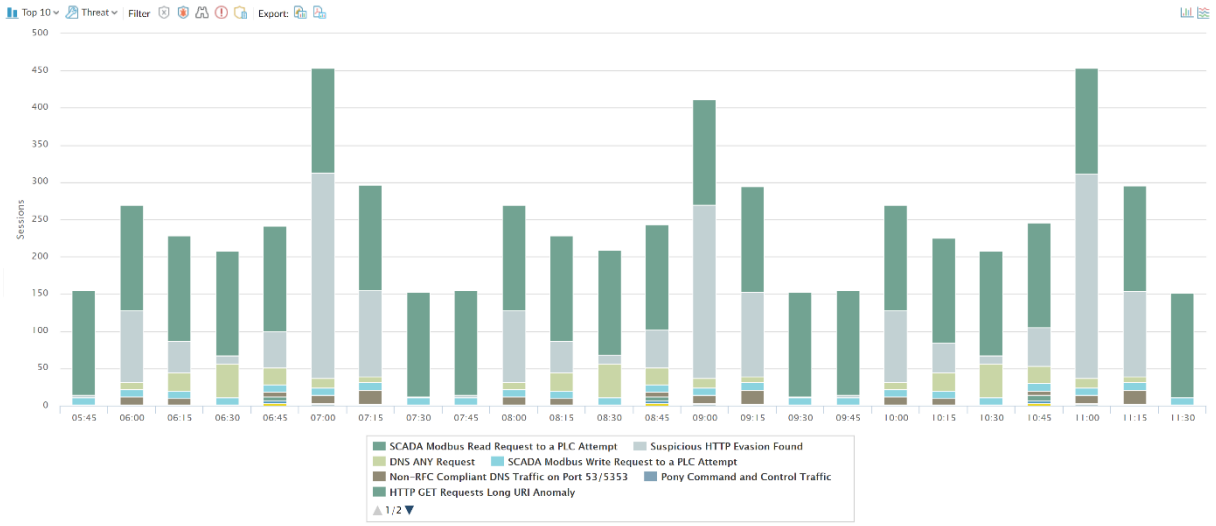
Country	Count
United States	91
Reserved (10.0.0.0 - 10.255.255.255)	22
European Union	1

Trends

Bandwidth

Threats

Graphique des menaces configurable et disponible dans l'interface graphique de l'équipement (les données ne sont pas celles d'Orange)

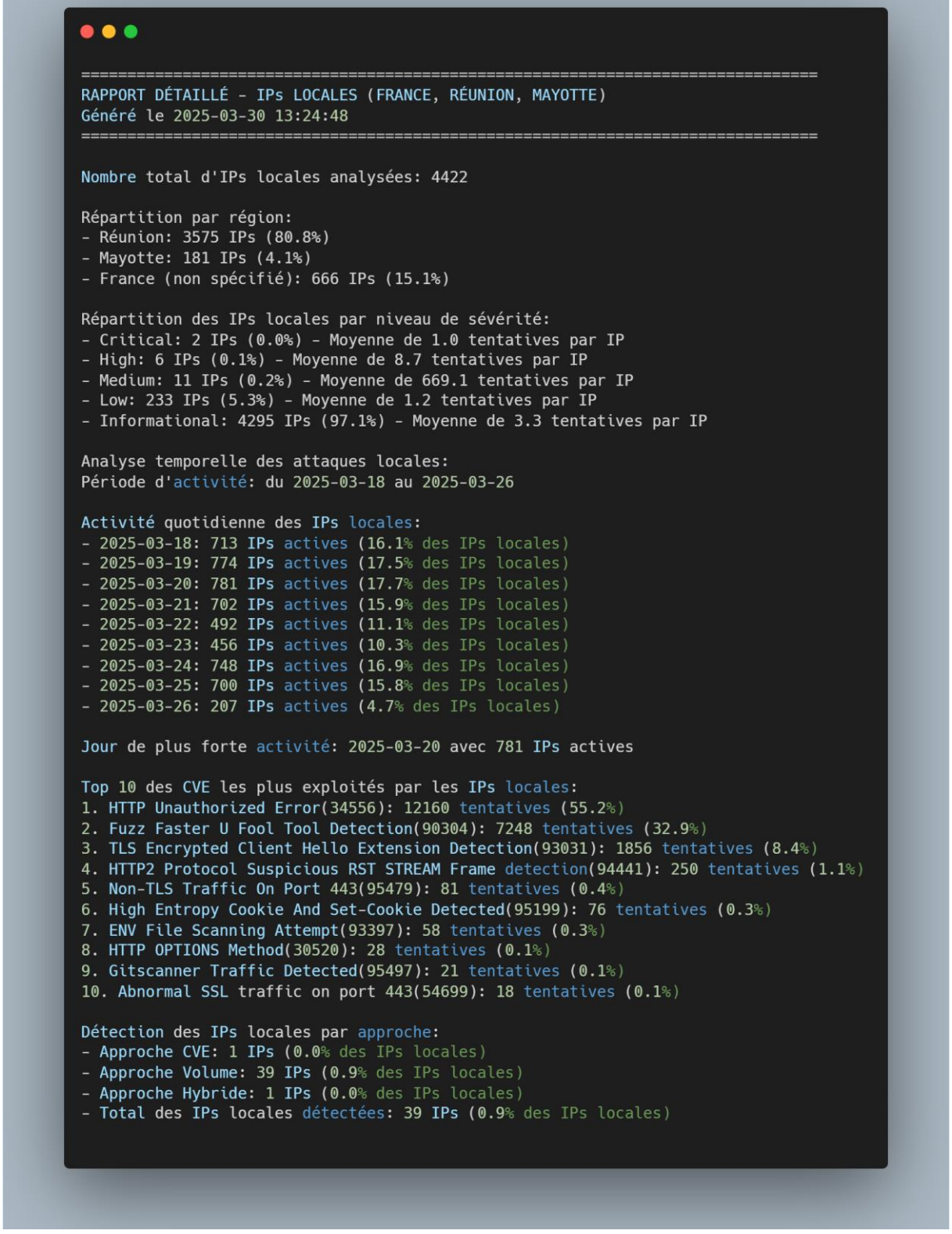

Top 10
Threat
Filter
Export:
Sessions
500
450
400
350
300
250
200
150
100
50
0
05:45
06:00
06:15
06:30
06:45
07:00
07:15
07:30
07:45
08:00
08:15
08:30
08:45
09:00
09:15
09:30
09:45
10:00
10:15
10:30
10:45
11:00
11:15
11:30
SCADA Modbus Read Request to a PLC Attempt
Suspicious HTTP Evasion Found
DNS ANY Request
SCADA Modbus Write Request to a PLC Attempt
Non-RFC Compliant DNS Traffic on Port 53/5353
Pony Command and Control Traffic
HTTP GET Requests Long URI Anomaly
1/2


Top 10
Incoming threats
Outgoing threats
Filter
Zoom In
Zoom Out
Export:
Last 6 hours
Last 12 hours
Last 24 hours
Last 7 days
Last 30 days
Last 60 days
Last 90 days

Généré par mon script d'analyse des menaces

```
┌──(kali㉿kali)-[~/Desktop/DATA-analyse]
└─$ /bin/bin/python3.12 /home/kali/Desktop/DATA-analyse/output/analyste-auto-3.py log\ -\ threats\ -\
6\ jours\ -\ du\ 1803\ au\ 2603.csv --threshold-cve 15 --threshold-attempts 30
Chargement des données depuis log - threats - 6 jours - du 1803 au 2603.csv...
Données chargées avec succès: 65534 entrées
Analyse des IPs avec plus de 15 CVE uniques ou plus de 30 tentatives...
Nombre total d'entrées de vulnérabilité: 32686
Nombre d'entrées de vulnérabilité (hors TCP flood): 32686
Période d'analyse: du 2025-03-18 01:42:39 au 2025-03-26 11:01:26

=== CLASSEMENT PAR NOMBRE DE CVE UNIQUES ===
Détecté 11 IPs ayant exploité plus de 15 CVE uniques sur la période.

Top 10 des IPs classées par nombre de CVE uniques :
1. IP: 212.56.35.99 - 25 CVE uniques exploités (131 tentatives au total)
   Première détection: 2025-03-18 02:51:30
   Dernière détection: 2025-03-26 07:07:34
   CVE le plus exploité: Gitscanner Traffic Detected(95497) (39 fois)

2. IP: 194.238.28.127 - 23 CVE uniques exploités (135 tentatives au total)
   Première détection: 2025-03-18 02:05:59
   Dernière détection: 2025-03-26 10:07:31
   CVE le plus exploité: Gitscanner Traffic Detected(95497) (24 fois)

3. IP: 37.60.249.107 - 23 CVE uniques exploités (257 tentatives au total)
   Première détection: 2025-03-18 02:06:49
   Dernière détection: 2025-03-26 09:09:25
   CVE le plus exploité: Gitscanner Traffic Detected(95497) (34 fois)

4. IP: 91.170.248.131 - 23 CVE uniques exploités (138 tentatives au total)
   Première détection: 2025-03-18 14:01:30
   Dernière détection: 2025-03-18 14:12:45
   CVE le plus exploité: HTTP Directory Traversal Request Attempt(30844) (17 fois)
```

```
... et 154 autres IPs. Voir le fichier exporté pour la liste complète.
Listes des IPs classées par CVE uniques exportées :
- Liste détaillée: output/block_list_by_cve_20250328_070712.txt
- Version CSV: output/block_list_by_cve_detailed_20250328_070712.csv
- Liste simple: output/block_list_by_cve_simple_20250328_070712.txt

Listes des IPs classées par nombre de tentatives exportées :
- Liste détaillée: output/block_list_by_attempts_20250328_070712.txt
- Version CSV: output/block_list_by_attempts_detailed_20250328_070712.csv
- Liste simple: output/block_list_by_attempts_simple_20250328_070712.txt

Résumé des résultats :
Nombre d'IPs dépassant le seuil de CVE uniques (15) : 11
Nombre d'IPs dépassant le seuil de tentatives (30) : 164
Nombre total d'IPs uniques à bloquer (combinant les deux critères) : 164

Listes exportées dans le répertoire : output

Terminé avec succès!
```



```
================================================================================
RAPPORT DÉTAILLÉ - IPs LOCALES (FRANCE, RÉUNION, MAYOTTE)
Généré le 2025-03-30 13:24:48
================================================================================

Nombre total d'IPs locales analysées: 4422

Répartition par région:
- Réunion: 3575 IPs (80.8%)
- Mayotte: 181 IPs (4.1%)
- France (non spécifié): 666 IPs (15.1%)

Répartition des IPs locales par niveau de sévérité:
- Critical: 2 IPs (0.0%) - Moyenne de 1.0 tentatives par IP
- High: 6 IPs (0.1%) - Moyenne de 8.7 tentatives par IP
- Medium: 11 IPs (0.2%) - Moyenne de 669.1 tentatives par IP
- Low: 233 IPs (5.3%) - Moyenne de 1.2 tentatives par IP
- Informational: 4295 IPs (97.1%) - Moyenne de 3.3 tentatives par IP

Analyse temporelle des attaques locales:
Période d'activité: du 2025-03-18 au 2025-03-26

Activité quotidienne des IPs locales:
- 2025-03-18: 713 IPs actives (16.1% des IPs locales)
- 2025-03-19: 774 IPs actives (17.5% des IPs locales)
- 2025-03-20: 781 IPs actives (17.7% des IPs locales)
- 2025-03-21: 702 IPs actives (15.9% des IPs locales)
- 2025-03-22: 492 IPs actives (11.1% des IPs locales)
- 2025-03-23: 456 IPs actives (10.3% des IPs locales)
- 2025-03-24: 748 IPs actives (16.9% des IPs locales)
- 2025-03-25: 700 IPs actives (15.8% des IPs locales)
- 2025-03-26: 207 IPs actives (4.7% des IPs locales)

Jour de plus forte activité: 2025-03-20 avec 781 IPs actives

Top 10 des CVE les plus exploités par les IPs locales:
1. HTTP Unauthorized Error(34556): 12160 tentatives (55.2%)
2. Fuzz Faster U Fool Tool Detection(90304): 7248 tentatives (32.9%)
3. TLS Encrypted Client Hello Extension Detection(93031): 1856 tentatives (8.4%)
4. HTTP2 Protocol Suspicious RST STREAM Frame detection(94441): 250 tentatives (1.1%)
5. Non-TLS Traffic On Port 443(95479): 81 tentatives (0.4%)
6. High Entropy Cookie And Set-Cookie Detected(95199): 76 tentatives (0.3%)
7. ENV File Scanning Attempt(93397): 58 tentatives (0.3%)
8. HTTP OPTIONS Method(30520): 28 tentatives (0.1%)
9. Gitscanner Traffic Detected(95497): 21 tentatives (0.1%)
10. Abnormal SSL traffic on port 443(54699): 18 tentatives (0.1%)

Détection des IPs locales par approche:
- Approche CVE: 1 IPs (0.0% des IPs locales)
- Approche Volume: 39 IPs (0.9% des IPs locales)
- Approche Hybride: 1 IPs (0.0% des IPs locales)
- Total des IPs locales détectées: 39 IPs (0.9% des IPs locales)
```

Extraits de code significatifs

1. Fonction récupération des données JSON via web

```python
import subprocess
import json

url_dict = {
    "liste_IP_google_bots":
"https://developers.google.com/search/apis/ipranges/googlebot.json",
    "liste_IP_google_crawlers":
"https://developers.google.com/search/apis/ipranges/special-crawlers.json",
    "liste_IP_google_user_triggered_fetchers":
"https://developers.google.com/search/apis/ipranges/user-triggered-fetchers.json",
    "liste_IP_google_user_triggered_fetchers_google":
"https://developers.google.com/search/apis/ipranges/user-triggered-fetchers-
google.json"
}

repositories_path = {
    "web_server" : "/var/www/html/",
    "git_folder" : "git_repo/panorama/"
}

def curl_get_JSON_with_subprocess(url):
    """Récupère les données JSON d'une URL via curl."""
    cmd = [
        "curl",
        "-v",  # Mode verbose (affiche les détails de la requête)
        "-L",  # Suivre les redirections
        "-k",  # Ignorer les erreurs de certificat SSL (à utiliser avec prudence)
        url
    ]
    try:
        result = subprocess.run(cmd, capture_output=True, text=True, check=True) #
check=True pour lever une exception en cas d'erreur
        json_data = json.loads(result.stdout)
        print("Contenu JSON formaté :")
        print(json.dumps(json_data, indent=4))
        # Enregistrement du JSON complet (facultatif - commenté pour éviter
l'écrasement)
        # with open('liste_IP_user-triggered-fetchers-google.json', "w") as f:
        #     f.write(result.stdout)
        print("Contenu récupéré avec succès!")
        return json_data
    except subprocess.CalledProcessError as e:
        print(f"Erreur curl (code {e.returncode}) : {e.stderr}")
        return None # Retourner None en cas d'erreur
    except json.JSONDecodeError:
        print("Le contenu n'est pas un JSON valide.")
        return None # Retourner None en cas d'erreur
    except Exception as e:
        print(f"Erreur lors de l'exécution de curl : {e}")
        return None # Retourner None en cas d'erreur
```

2. Fonction parsing du fichier JSON

```python
def parsing_json_data(json_data):
    """Analyse les données JSON et extrait les préfixes IPv4."""
    if json_data:
        ipv4_prefix_list = []
        prefixes_data = json_data.get("prefixes", [])  # Récupère la liste des
préfixes, ou une liste vide si 'prefixes' n'existe pas
        for prefix in prefixes_data:
            if "ipv4Prefix" in prefix:
                ipv4_prefix_list.append(prefix["ipv4Prefix"] + "\n")

        print("\nAdresses IP de la liste JSON :\n")
        for ip in ipv4_prefix_list:
            print(ip, end="") # Évite les sauts de ligne supplémentaires
        return ipv4_prefix_list # Retourne la liste des préfixes IPv4
    else:
        print("Aucun JSON valide récupéré.")
        return [] # Retourne une liste vide si json_data est None
```

3. Fonction création du fichier texte (intègre la copie vers les dossiers cibles : serveur web et dossier git)

En cours de réalisation – je travaille à la solution de copie sur les dossiers cibles qui actuellement n'est pas fonctionnelle car elle nécessite de rentrer le mot de passe sudo. Je cherche la solution la plus sécurisée actuellement.

```python
def write_list_IP(IP_list, filename, path):
    """Enregistre une liste d'adresses IP dans un fichier temporaire, puis la copie
dans le répertoire cible."""
    temp_filename = filename + ".txt"
    with open(temp_filename, "w") as f:
        f.writelines(IP_list)

    try:
        subprocess.run(["sudo", "cp", temp_filename, path], check=True)
        print(f"Fichier {temp_filename} copié avec succès dans /var/www/html/")
        os.remove(temp_filename) # Supprime le fichier temporaire
        print(f"Fichier temporaire {temp_filename} supprimé.")
    except subprocess.CalledProcessError as e:
        print(f"Erreur lors de la copie du fichier : {e}")
```

4. Historisation dans GitLab

```python
def push_to_gitlab(repo_path, commit_message=None):
    """Pousse les modifications vers le dépôt GitLab"""

    try:
        # Charger le dépôt existant
        repo = git.Repo(repo_path)

        # Ajouter tous les changements
        repo.git.add('--all')

        # Créer un message de commit avec horodatage
        if not commit_message:
            commit_message = f'Mise à jour liste_IP_google
{datetime.datetime.now().strftime("%Y-%m-%d %H:%M:%S")}'

        # Commit avec le message
        repo.index.commit(commit_message)

        # Pousser vers le remote 'origin'
        origin = repo.remote(name='origin')
        origin.push()

        print("Push vers GitLab réussi")
        return True
    except git.GitError as e:
        print(f"Erreur Git lors du push: {e}")
        return False
    except Exception as e:
        print(f"Erreur inattendue lors du push: {e}")
        return False
```

5. Intégration avec Panorama et EDL

La configuration dans Panorama comprend :

- Création d'un objet EDL pointant vers notre serveur web interne
- Intégration de cet objet dans les règles de sécurité appropriées
- Configuration de l'intervalle de mise à jour (daily)

Le système EDL va directement lire le fichier texte et implémenté les adresses IP dans le firewall (si l'EDL est utilisée sur une règle de sécurité – sinon les adresses sont simplement disponibles pour utilisation).

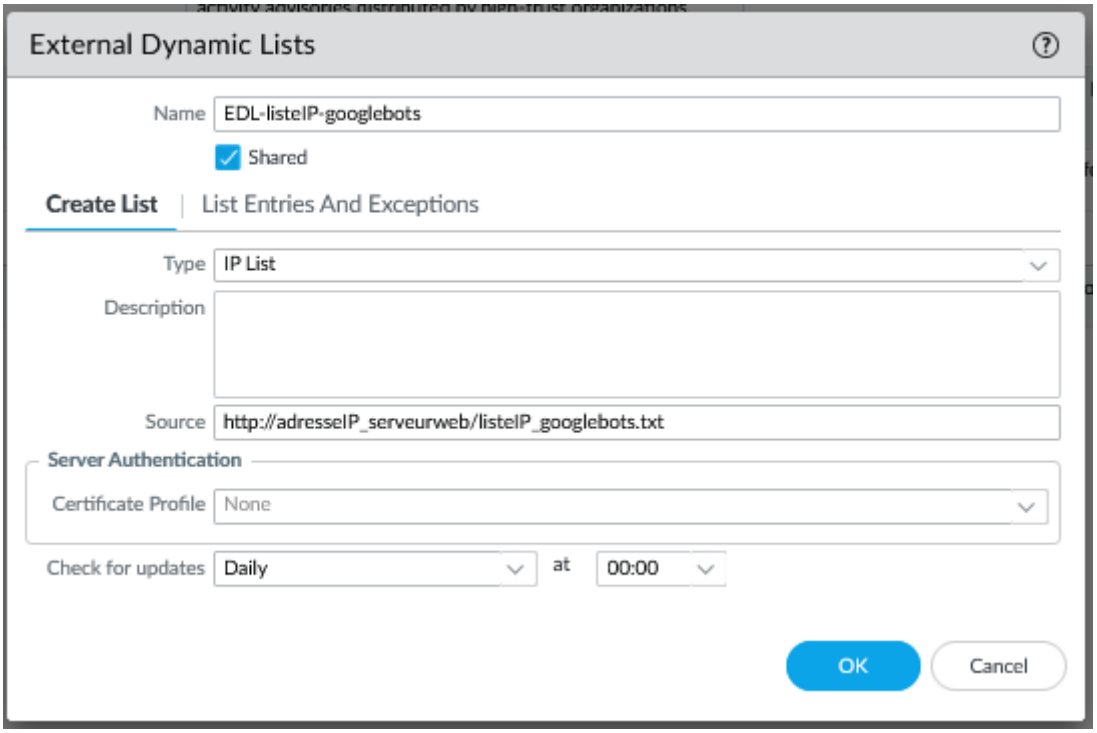
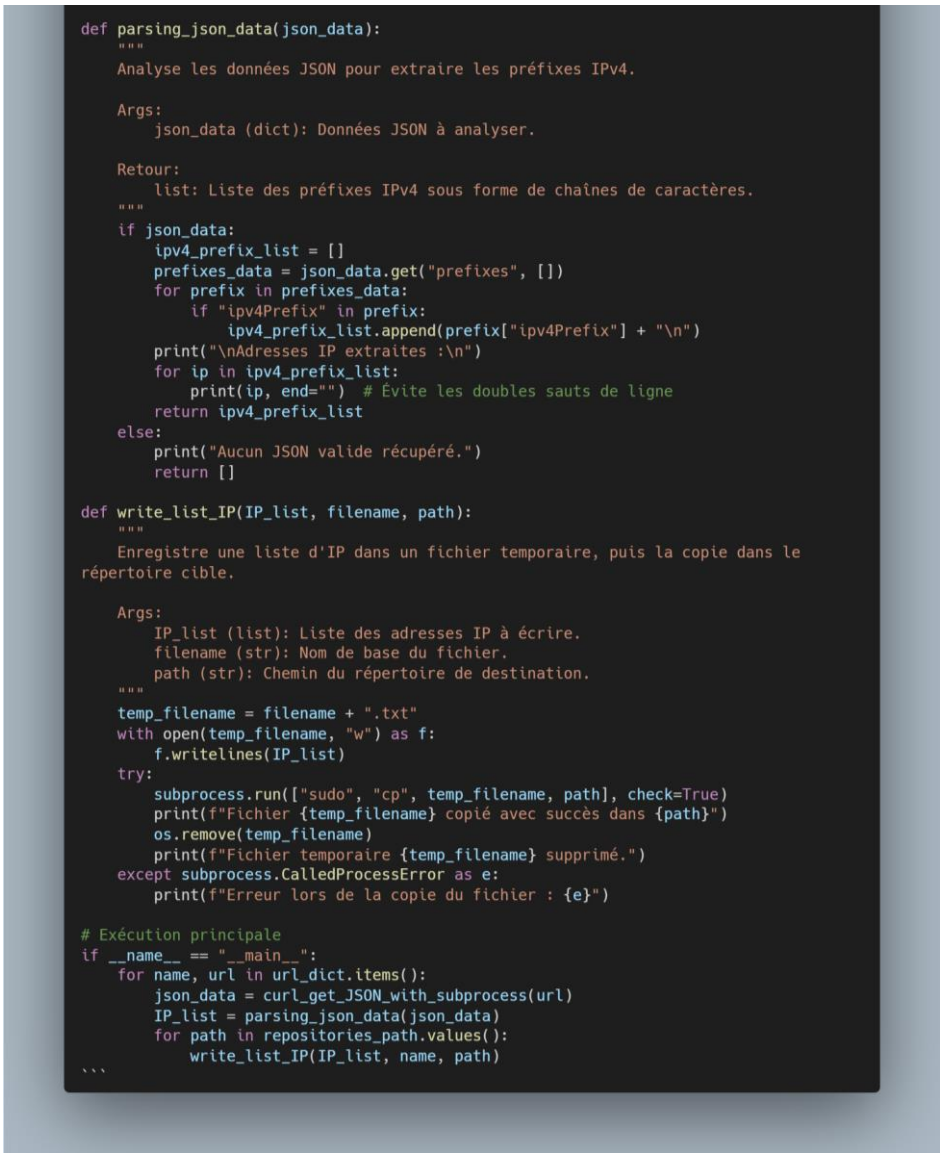


Figure 3333 Création de l'EDL googlebots et configuration de sa mise à jour

6. Code complet (manque encore l'intégration de la fonction push git)

```python
"""
Script pour récupérer et formater les plages d'adresses IP des crawlers Google.

Ce script utilise curl pour télécharger les données JSON des URLs spécifiées,
analyse ces données pour extraire les préfixes IPv4, puis enregistre ces adresses dans
des fichiers texte.

Fonctions principales :

- curl_get_JSON_with_subprocess(url): Récupère les données JSON d'une URL en utilisant
curl.
- parsing_json_data(json_data): Analyse les données JSON pour extraire les préfixes
IPv4.
- write_list_IP(IP_list, filename, path): Enregistre une liste d'IP dans un fichier,
puis le copie dans le répertoire cible.

Version : 1.2
Date : 2025-06-11
Développeur : Jacob Dufossé - Alternant Réseaux IP
"""

import subprocess
import json
import os

# Dictionnaire associant des noms à leurs URLs JSON respectives
url_dict = {
    "liste_IP_google_bots":
"https://developers.google.com/search/apis/ipranges/googlebot.json",
    "liste_IP_google_crawlers":
"https://developers.google.com/search/apis/ipranges/special-crawlers.json",
    "liste_IP_google_user_triggered_fetchers":
"https://developers.google.com/search/apis/ipranges/user-triggered-fetchers.json",
    "liste_IP_google_user_triggered_fetchers_google":
"https://developers.google.com/search/apis/ipranges/user-triggered-fetchers-
google.json"
}

# Chemins de stockage pour les fichiers
repositories_path = {
    "web_server": "/var/www/html/",
    "git_folder": "git_repo/panorama/"
}

def curl_get_JSON_with_subprocess(url):
    """
    Récupère les données JSON d'une URL en utilisant curl via subprocess.

    Args:
        url (str): L'URL à partir de laquelle récupérer les données JSON.

    Retour:
        dict ou None: Données JSON décodées ou None en cas d'erreur.
    """
    cmd = [
        "curl",
        "-v",  # Mode verbose pour le débogage
        "-L",  # Suivre les redirections
        "-k",  # Ignorer les erreurs SSL (attention à la sécurité)
        url
    ]
    try:
        result = subprocess.run(cmd, capture_output=True, text=True, check=True)
        json_data = json.loads(result.stdout)
        print("Contenu JSON formaté :")
        print(json.dumps(json_data, indent=4))
        # Optionnel : sauvegarde du JSON complet
        # with open('json_full_output.json', 'w') as f:
        #     f.write(result.stdout)
        print("Contenu récupéré avec succès !")
        return json_data
    except subprocess.CalledProcessError as e:
        print(f"Erreur curl (code {e.returncode}) : {e.stderr}")
        return None
    except json.JSONDecodeError:
        print("Le contenu n'est pas un JSON valide.")
        return None
    except Exception as e:
        print(f"Erreur lors de l'exécution de curl : {e}")
        return None
```



```python
def parsing_json_data(json_data):
    """
    Analyse les données JSON pour extraire les préfixes IPv4.

    Args:
        json_data (dict): Données JSON à analyser.

    Retour:
        list: Liste des préfixes IPv4 sous forme de chaînes de caractères.
    """
    if json_data:
        ipv4_prefix_list = []
        prefixes_data = json_data.get("prefixes", [])
        for prefix in prefixes_data:
            if "ipv4Prefix" in prefix:
                ipv4_prefix_list.append(prefix["ipv4Prefix"] + "\n")
        print("\nAdresses IP extraites :\n")
        for ip in ipv4_prefix_list:
            print(ip, end="")  # Évite les doubles sauts de ligne
        return ipv4_prefix_list
    else:
        print("Aucun JSON valide récupéré.")
        return []

def write_list_IP(IP_list, filename, path):
    """
    Enregistre une liste d'IP dans un fichier temporaire, puis la copie dans le
répertoire cible.

    Args:
        IP_list (list): Liste des adresses IP à écrire.
        filename (str): Nom de base du fichier.
        path (str): Chemin du répertoire de destination.
    """
    temp_filename = filename + ".txt"
    with open(temp_filename, "w") as f:
        f.writelines(IP_list)
    try:
        subprocess.run(["sudo", "cp", temp_filename, path], check=True)
        print(f"Fichier {temp_filename} copié avec succès dans {path}")
        os.remove(temp_filename)
        print(f"Fichier temporaire {temp_filename} supprimé.")
    except subprocess.CalledProcessError as e:
        print(f"Erreur lors de la copie du fichier : {e}")

# Exécution principale
if __name__ == "__main__":
    for name, url in url_dict.items():
        json_data = curl_get_JSON_with_subprocess(url)
        IP_list = parsing_json_data(json_data)
        for path in repositories_path.values():
            write_list_IP(IP_list, name, path)
```