Rapport d'alternance

Administrateur Réseaux et Sécurité chez Vizyon

Alban CALVO

3° année BUT Réseaux et Télécommunications

Septembre 2023 – Juin 2024

Tuteur enseignant : Lorraine Goeuriot

Tuteur en entreprise : Nicolas Kritter

Signature :

Remerciements

Avant tout, je tiens à remercier Monsieur Nicolas Kritter, de m'avoir accueilli au sein de son entreprise. Il m'a pris sous son aile et donné de précieux conseils tout au long de mon alternance.

Mes remerciements s'adressent aussi à Monsieur Guillaume Yziquel, pour m'avoir partagé ses connaissances et son expérience, ayant ainsi encouragé ma curiosité..

Également à Madame Nisrine Goumri, pour m'avoir permis de découvrir certains aspects du monde de l'entreprise. Ce qui m'encourage dans mon projet de monter mon entreprise à l'avenir.

Enfin je remercie tous les membres de l'équipe pédagogique du département Réseaux et Télécommunications de l'IUT1 de Grenoble pour m'avoir permis d'élargir mes compétences et mes connaissances durant ces 3 dernières années.

Merci

SOMMAIRE

INTRODUCTION

Dans le cadre de ma formation en BUT Réseaux et Télécommunications à l'IUT1 de Grenoble, j'ai choisi de m'orienter vers l'alternance en troisième année.

Au cours de mon BUT, j'ai opté pour la spécialisation en Cyber-sécurité. J'ai pris conscience de l'importance cruciale de ce domaine pour les entreprises, car leurs données les plus sensibles sont désormais stockées de manière informatisée. De surcroît, sans l'informatique et Internet, il est aujourd'hui difficile de gérer une entreprise de manière stable et pérenne.

J'ai donc choisi la voie de l'alternance afin d'acquérir dès que possible une expérience pratique en entreprise. Cette approche m'a également permis de mettre en application les connaissances théoriques acquises durant le BUT. J'ai pu apporter à Vizyon une perspective jeune et dynamique ainsi qu'une capacité à résoudre des problèmes complexes de manière autonome.

Je vais donc commencer par vous présenter l'entreprise, les missions que j'ai effectuées, et je conclurai par un retour sur cette expérience.

1. Présentation de l'entreprise

1.1. L'histoire de Vizyon

Vizyon est une entreprise, qui agit comme acteur du secteur de la téléradiologie. L'entreprise est située à La Tronche, au sein du bâtiment Biopolis de l'UGA. Ce bâtiment accueille de nombreuses entreprises tournées vers la recherche et le développement de nouvelles technologies dans le domaine de la santé.

L'entreprise a été fondée en 2019 par le Docteur Pierre Durand et Monsieur Le Bihan. Vizyon à été située dans plusieurs pays, en Suisse, en Turquie qu'elle à quittée en 2020, puis en France à La Tronche.

Vizyon est un acteur important du secteur de la téléradiologie, en effet elle apporte l'expertise de l'intelligence artificielle et de la blockchain. Elle gère plusieurs cabinets médicaux situés partout en France.

Vizyon met à disposition une plateforme pour les manipulateurs échographistes et les radiologues. Un patient vient au cabinet, le manipulateur réalise la radiographie et envoie

les images sur le PACS. Le radiologue quant à lui, décide de quel patient il va réaliser l'interprétation de la radio parmi une liste. Le radiologue a accès à l'image ainsi qu'un compte rendu généré par une intelligence artificielle. Les 2 IA principales sont Gleamer et Lunit. Après l'interprétation, le radiologue renvoie le dossier avec l'image et le compte rendu sur le RIS.

L'utilisation de la blockchain permet de sécuriser le transfert des données issues de l'acquisition d'images du centre vers la plateforme, entre les équipements de Radiologie et les serveurs **RIS** et **PACS**

Voici un peu de lexique relatif à l'entreprise :

Blockchain : C'est une technologie révolutionnaire qui permet de stocker et de transmettre des informations de manière transparente, sécurisée et décentralisée.

Blockchain : privée Une version restreinte de la technologie blockchain, limitée à un groupe restreint d'entités ou d'utilisateurs autorisés.

Instance DICOM : Une image médicale unique ou un ensemble de données liées, identifié par un code spécial appelé "Instance UID", utilisé pour distinguer entre les images au sein d'une série et d'une étude médicale.

PACS : Picture Archiving and Communication System est un système informatique qui gère le stockage, la visualisation et la distribution d'images médicales telles que les radiographies, les IRM, etc.

RIS : Radiology Information System est un système informatique utilisé pour gérer et organiser les informations liées aux examens radiologiques, patients, rendez-vous et rapports médicaux dans les départements de radiologie.

1.2. Contexte

La télé-radiologie est une spécialité médicale visant l'interprétation à distance d'images médicales telles que les radiographies, les scanners, les échographies, les IRM (Imagerie par Résonance Magnétique), etc. Grâce à cette approche, des radiologues spécialisés peuvent diagnostiquer et fournir des conseils aux médecins et aux patients sans avoir à se déplacer physiquement sur le site où les images ont été prises. La téléradiologie est particulièrement utile dans les zones géographiquement éloignées ou mal desservies par

les services médicaux spécialisés. Elle permet aussi aux patients d'accéder rapidement à l'expertise de radiologues qualifiés ce qui améliore la qualité des soins et accélère le processus de diagnostic et de traitement, chose particulièrement importante dans les situations d'urgence.

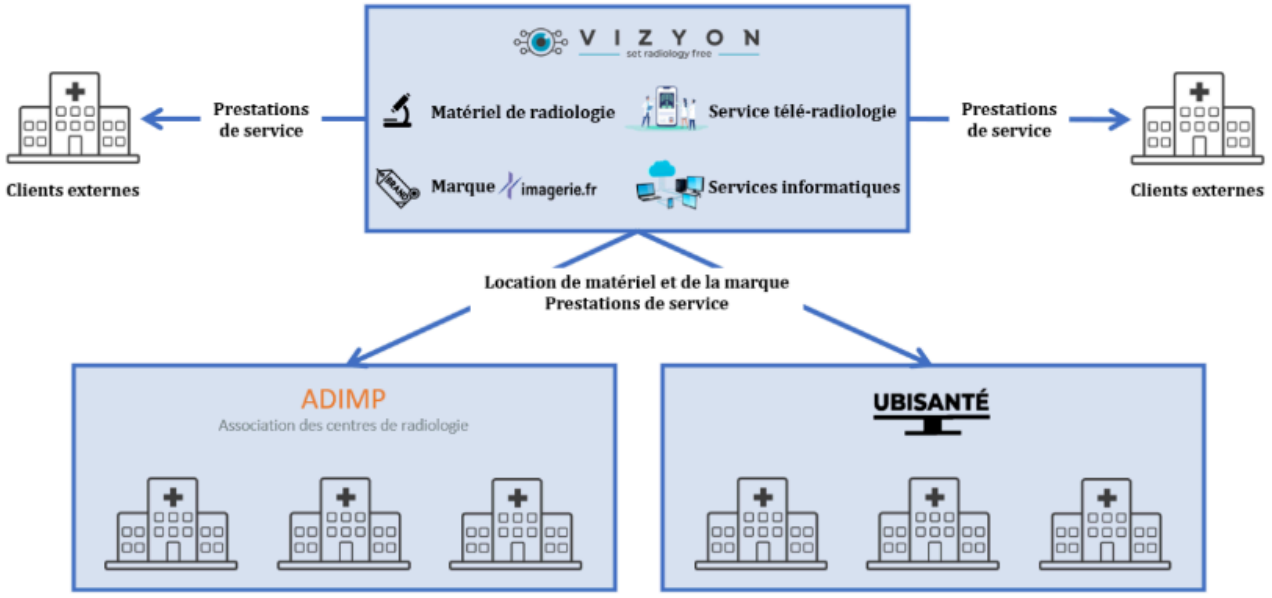
1.3. Structure et organisation

VIZYON développe une plateforme de télé-radiologie sécurisée par la blockchain et intégrant des algorithmes d'intelligence artificielle, afin de proposer un diagnostic rapide, de qualité et à prix abordable, partout dans le monde. La plateforme est actuellement utilisée en France, et en Afrique. La société prévoit aussi de la déployer dans d'autres pays au cours des prochaines années et de devenir un acteur majeur de la télé-radiologie au niveau mondial.

LES DIFFÉRENTES PRESTATIONS DE VIZYON :

- **Téléradiologie** : La téléradiologie est l'activité principale de Vizyon, représentant plus de 65% de ses revenus.
- **Services informatiques** : Vizyon propose des services informatiques complets pour optimiser les performances de la téléradiologie. Ces services englobent la gestion des données, l'utilisation de l'intelligence artificielle et le stockage sécurisé des radiographies et des comptes rendus médicaux dans le cloud. Les centres bénéficient également d'un support technique de la part de l'équipe de Vizyon pour résoudre rapidement les éventuelles erreurs et garantir une efficacité maximale du système. Ainsi, Vizyon offre une solution complète et personnalisée pour répondre aux besoins spécifiques de ses clients en matière de technologie et d'informatique médicale.
- **Leasing d'équipements médicaux** : Vizyon propose également des prestations de leasings en crédit bail en association avec des banques. Ces leasings regroupent différents équipements médicaux tels que des échographes, des tables de radiologie, et d'autres équipements essentiels à la pratique médicale de la radiologie. Cette prestation représente environ 5% du chiffre d'affaires de l'entreprise. Grâce à cette offre de leasing, les centres médicaux peuvent accéder à des équipements de pointe sans avoir à investir dans leur achats.
- **Location de la marque "Imagerie.fr"** : Vizyon loue la marque "Imagerie.fr" à tous les cabinets internes du groupe Imagerie.fr, appartenant à Ubisanté et à l'ADIMP. Cette prestation représente environ 2% du chiffre d'affaires de chaque centre, offrant une identité commune et unifiée au sein du groupe et renforçant leur image de marque et leur visibilité sur le marché.

Voici le schéma de la structure :



2. Les débuts de mon alternance

2.1. Comment j'ai trouvé cette alternance

J'ai trouvé cette alternance en répondant à une offre publiée sur Indeed. L'annonce demandait des compétences techniques en programmation, en réseaux et en scripting. Ayant acquis une solide expérience dans ces domaines grâce aux projets confiés par l'école, j'ai réalisé que cette opportunité correspondait parfaitement à mon profil. En raison de ma spécialisation en cybersécurité, j'ai également compris que les enjeux pour un acteur du secteur médical me permettraient de valoriser pleinement ces compétences. J'ai donc passé un entretien en visioconférence avec Madame Goumri et Monsieur Kritter

2.2. Mon intégration au sein de l'équipe

La première semaine, je me suis familiarisé avec les pratiques informatiques de l'entreprise. Mon tuteur en entreprise, Nicolas Kritter, est responsable du développement de l'application permettant aux radiologues de traiter les informations des patients. Les radiologues y entrent les données des patients et y sauvegardent les images de radiologie. L'application web leur permet d'interagir avec les systèmes RIS et PACS.

Il était donc essentiel que je comprenne l'architecture sous-jacente à cette infrastructure. Celle-ci comprend des machines virtuelles AWS et OVH, ainsi que les routeurs des cabinets médicaux qui permettent l'accès aux serveurs. J'ai passé la première semaine à lire la documentation, à observer mon environnement de travail et à étudier le fonctionnement des différentes machines.

Une fois cette première semaine écoulée, j'avais acquis une compréhension solide du fonctionnement de leur architecture réseau et des éléments tels que l'application web. J'ai ainsi pu commencer mon projet à long terme, qui consistait en la maintenance du réseau, sujet abordé dans mon étude de cas.

3. Missions / Travail

3.1. La liste des équipements réseaux et mise à jour

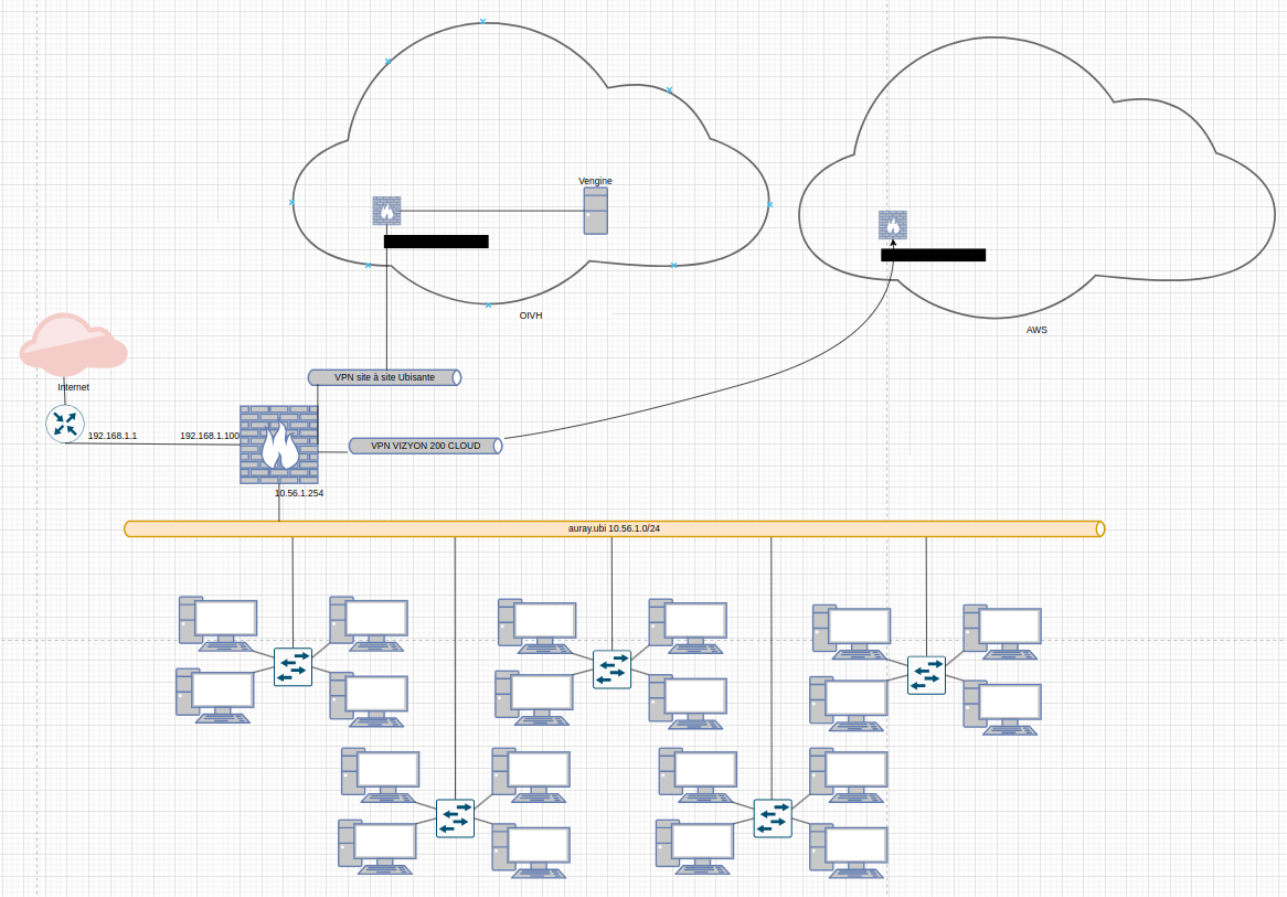
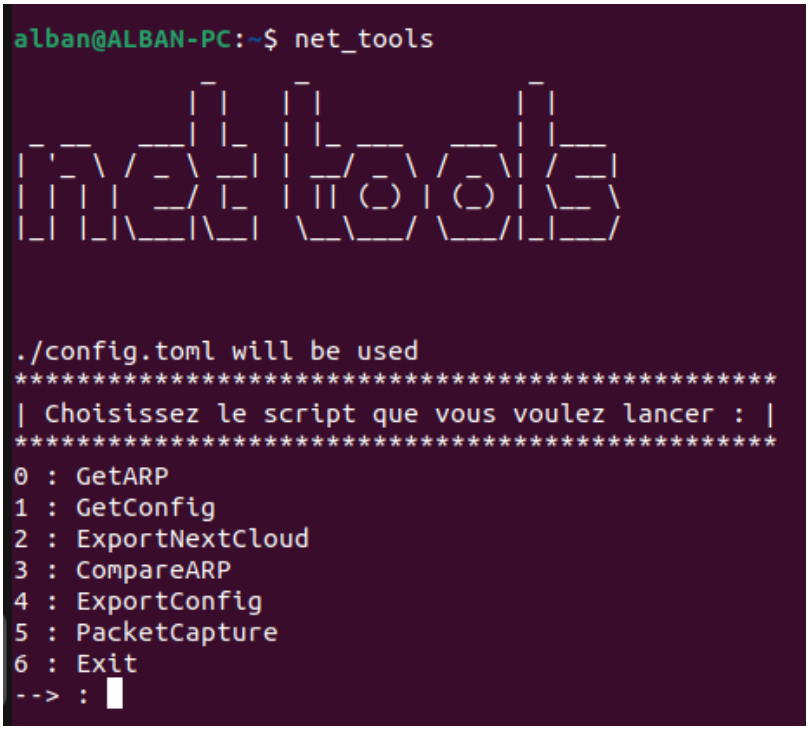


Schéma type cabinet

Voici le schéma d'un cabinet de radiologie, en l'occurrence celui d'Auray. Cette topologie est applicable à tous les autres cabinets. On peut donc observer plusieurs éléments à prendre en compte : les tunnels VPN à destination des clouds OVH et AWS représentés par les nuages, le trafic LAN en jaune et le trafic WAN à gauche du pare-feu à direction d'internet.

Durant cette alternance, j'ai pu constater la différence entre les travaux pratiques réalisés à l'école et la réalité en production. À mon arrivée chez Vizyon, j'ai commencé par établir une liste et un schéma du réseau actuel pour en comprendre le fonctionnement avant toute intervention.

Avant d'entreprendre quoi que ce soit, j'ai décidé de récupérer les fichiers de configuration des routeurs pfSense. Étant donné que j'avais onze routeurs à gérer, il n'était pas envisageable d'effectuer la même tâche de manière répétitive. J'ai donc automatisé ce processus. L'outil que j'ai développé à cet effet se nomme "net_tools" ou "Network Tools" selon la version. Cet outil Python me permet d'effectuer les tâches suivantes (voir capture)



:

Commandes de l'outil net_tools

Le script se base sur un fichier de configuration au format .TOML qui contient les répertoires destinés à stocker les fichiers créés ou récupérés. Il inclut également les informations concernant l'utilisateur distant à utiliser pour les connexions ainsi que les adresses des routeurs.

Une fois les configurations sauvegardées sur le cloud, j'ai entrepris une longue série de tests visant à les mettre à jour et à ajouter une liste blanche sur le LAN. Les routeurs des cabinets utilisaient la version 2.5.2 de pfSense Community Edition. Pour ce faire, j'ai proposé d'utiliser GNS3 afin de recréer partiellement l'infrastructure d'un cabinet. Le minimum requis était un routeur en version 2.5.2 avec la configuration d'un cabinet, un poste client, et un deuxième routeur en version 2.4.5 pour le tunnel VPN du routeur principal.

Lors de ces tests, j'ai commencé par configurer les listes blanches. J'ai créé des alias "Allowed_hosts" sur les routeurs puis sur GNS3. Ensuite, j'ai ajouté une règle autorisant uniquement les membres de la liste blanche à communiquer sur le LAN. J'ai vérifié que l'ajout de cette règle ne coupait pas l'accès aux ports d'administration du routeur. Étant donné que les routeurs sont géographiquement éloignés, je devais être particulièrement prudent pour ne jamais perdre l'accès. Les tests s'étant avérés concluants, j'ai pu intégrer ces listes blanches sur les routeurs.

Dans le cadre de la gestion des mises à jour, les tests suivants ont été réalisés :

- Mise à jour d'un pare-feu virtuel de la version 2.5.1 à la version 2.6.0, puis à la version 2.7.0.
- Mise à jour avec des packages installés.
- Mise à jour avec des packages désinstallés.
- Tests de changement du gestionnaire de packages et de ses branches (ou versions).

Après avoir mené ces tests sur un routeur virtuel, j'ai procédé à leur application sur un routeur physique de test. Suite à la réussite de la mise à jour sur le routeur de test, j'ai déployé cette mise à jour sur l'ensemble des routeurs. Pour éviter toute interruption de service en pleine journée, ces mises à jour ont été effectuées depuis mon domicile. À ce jour, la version des routeurs est pleinement à jour.

3.2. L'installation d'API et gestion distante en CLI

Ayant plusieurs routeurs à gérer, je devais trouver un moyen de les administrer tous simultanément lorsque cela était possible. C'est ainsi que j'ai eu l'idée de développer un outil en ligne de commande, codé en Python, appelé "pfsense-manager", disponible sur mon GitHub. Cet outil s'appuie sur l'API développée par Jared Hendrickson, installable sous forme de package `pkg` sur pfSense. Il s'agit d'une API REST qui accepte des commandes via des requêtes HTTP GET, POST, PUT et DELETE.

Mon outil m'a permis d'exécuter les tâches suivantes :

- `add-address` : Ajoute une adresse IP, une liste ou une plage à un alias existant.
- `add-package` : Installe un package sur le routeur distant.
- `add-rule` : Ajoute une règle sur un ou plusieurs routeurs.
- `create-certificate` : Crée un certificat sur le routeur.
- `create-config` : Crée un fichier de configuration à partir d'un fichier template.
- `create-vpn` : Crée un tunnel VPN entre le routeur client et le serveur VPN.
- `get-aliases` : Affiche les alias et leurs contenus sur la console.
- `install-api` : Installe l'API sur le routeur distant avant d'utiliser le package.
- `modify-rule` : Modifie une règle du pare-feu.
- `read-ca` : Affiche les autorités de certification du routeur.
- `read-certificates` : Affiche les certificats sur le routeur.
- `read-rules` : Affiche les règles des interfaces.
- `reboot-router` : Redémarre un routeur distant.
- `show-logs` : Affiche les logs systèmes et pare-feu sur la console.

Cet outil m'a permis de commencer la sécurisation du trafic réseau en ajoutant des règles aux pare-feu des routeurs pfSense. Pour ce faire, je devais d'abord analyser le trafic réseau actuel. J'ai donc développé un autre outil en Python qui permet de lancer la commande `tcpdump` sur un hôte Linux ou BSD distant, de récupérer la sortie au format `.pcap` sur ma machine grâce à la commande `scp`, et de l'ouvrir avec Wireshark sur ma machine. Cet outil s'appelle "packet-capture" et est également disponible sur mon GitHub si vous souhaitez consulter le code.

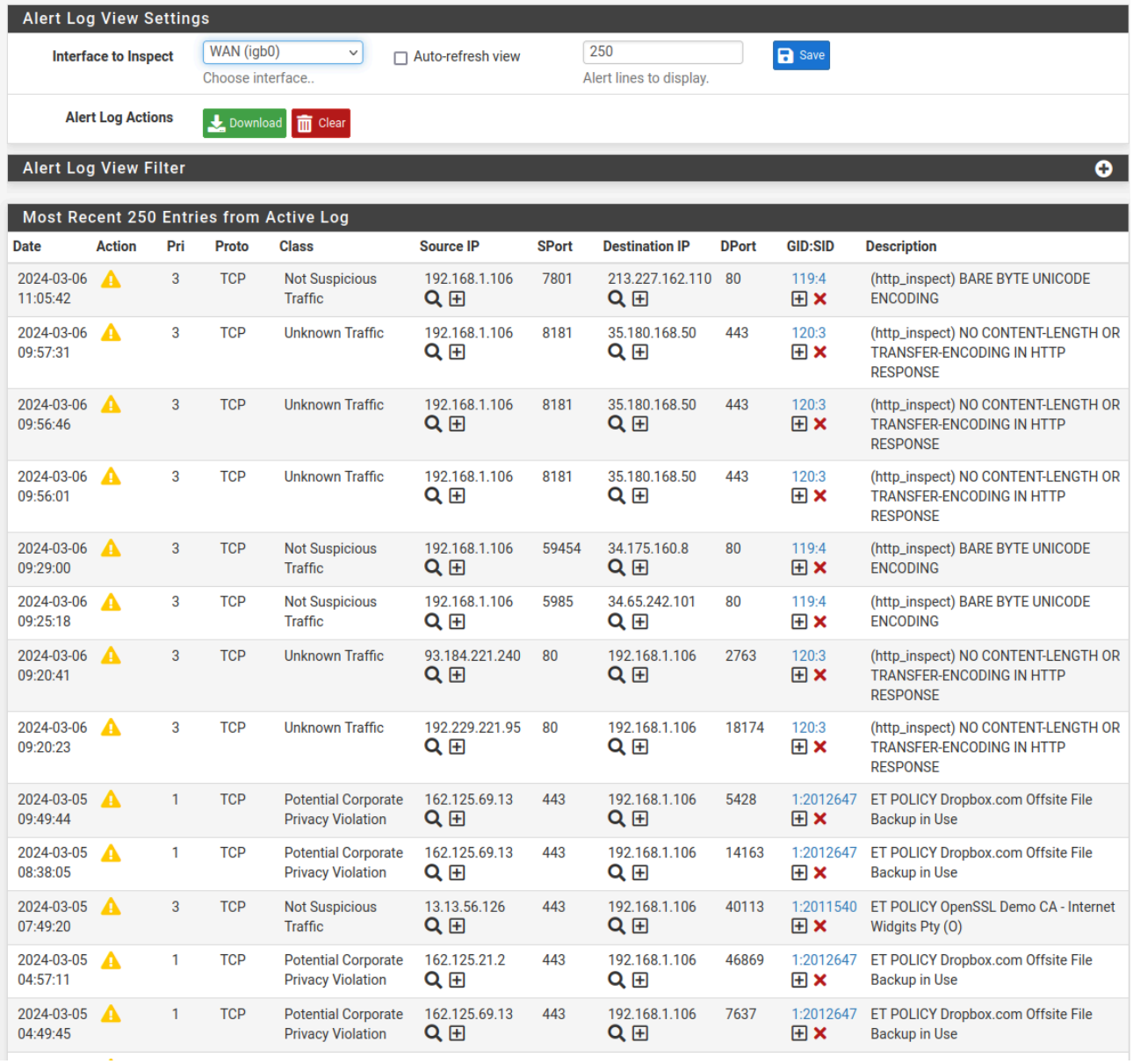
```
alban@ALBAN-PC:~$ packet-capture --help
Usage: packet-capture [OPTIONS]

Options:
  --hostip TEXT    The ip address of the remote host
  --hostname TEXT  The name of the remote host
  --port INTEGER   The ssh port on remote
  --hosts TEXT     The file that contains the list of hosts in hosts.toml
  --user TEXT      The user to make a ssh connection on remote
  --passwd TEXT    The passwd of user
  --passwds TEXT   The passwd.gpg file to for ssh connection
  --gnupg TEXT     The path to .gnupg folder to decrypt .json.gpg file
  --output TEXT    /path/to/folder that will contain .pcap files
  --timer TEXT     Timer of tcpdump command
  --help           Show this message and exit.
```

Commandes de l'outil packet-capture

Suite à une analyse des flux sur les interfaces LAN et WAN des routeurs, j'ai dressé une liste des adresses sources et destinations à autoriser avec Monsieur Kritter, ainsi que des ports pour les protocoles nécessaires.

Avant d'ajouter les règles, j'ai installé et configuré Suricata sur les routeurs. Suricata est un package que l'on peut installer sur pfSense pour analyser le trafic réseau. Je l'ai donc installé et configuré afin d'observer le trafic sur les interfaces LAN et WAN. Voici à quoi ressemble le système d'alertes de Suricata.

Cette configuration m'a permis de surveiller et d'analyser efficacement le trafic réseau, et d'ajuster les règles de sécurité en conséquence. Grâce à Suricata, j'ai pu identifier et réagir rapidement aux éventuelles menaces détectées sur le réseau.



Alert Log View Settings

Interface to Inspect: WAN (igb0) — Choose interface.. | Auto-refresh view | 250 — Alert lines to display. | Save

Alert Log Actions: Download | Clear

Alert Log View Filter

Most Recent 250 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-03-06 11:05:42	⚠	3	TCP	Not Suspicious Traffic	192.168.1.106	7801	213.227.162.110	80	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2024-03-06 09:57:31	⚠	3	TCP	Unknown Traffic	192.168.1.106	8181	35.180.168.50	443	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2024-03-06 09:56:46	⚠	3	TCP	Unknown Traffic	192.168.1.106	8181	35.180.168.50	443	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2024-03-06 09:56:01	⚠	3	TCP	Unknown Traffic	192.168.1.106	8181	35.180.168.50	443	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2024-03-06 09:29:00	⚠	3	TCP	Not Suspicious Traffic	192.168.1.106	59454	34.175.160.8	80	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2024-03-06 09:25:18	⚠	3	TCP	Not Suspicious Traffic	192.168.1.106	5985	34.65.242.101	80	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2024-03-06 09:20:41	⚠	3	TCP	Unknown Traffic	93.184.221.240	80	192.168.1.106	2763	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2024-03-06 09:20:23	⚠	3	TCP	Unknown Traffic	192.229.221.95	80	192.168.1.106	18174	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2024-03-05 09:49:44	⚠	1	TCP	Potential Corporate Privacy Violation	162.125.69.13	443	192.168.1.106	5428	1:2012647	ET POLICY Dropbox.com Offsite File Backup in Use
2024-03-05 08:38:05	⚠	1	TCP	Potential Corporate Privacy Violation	162.125.69.13	443	192.168.1.106	14163	1:2012647	ET POLICY Dropbox.com Offsite File Backup in Use
2024-03-05 07:49:20	⚠	3	TCP	Not Suspicious Traffic	13.13.56.126	443	192.168.1.106	40113	1:2011540	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
2024-03-05 04:57:11	⚠	1	TCP	Potential Corporate Privacy Violation	162.125.21.2	443	192.168.1.106	46869	1:2012647	ET POLICY Dropbox.com Offsite File Backup in Use
2024-03-05 04:49:45	⚠	1	TCP	Potential Corporate Privacy Violation	162.125.69.13	443	192.168.1.106	7637	1:2012647	ET POLICY Dropbox.com Offsite File Backup in Use

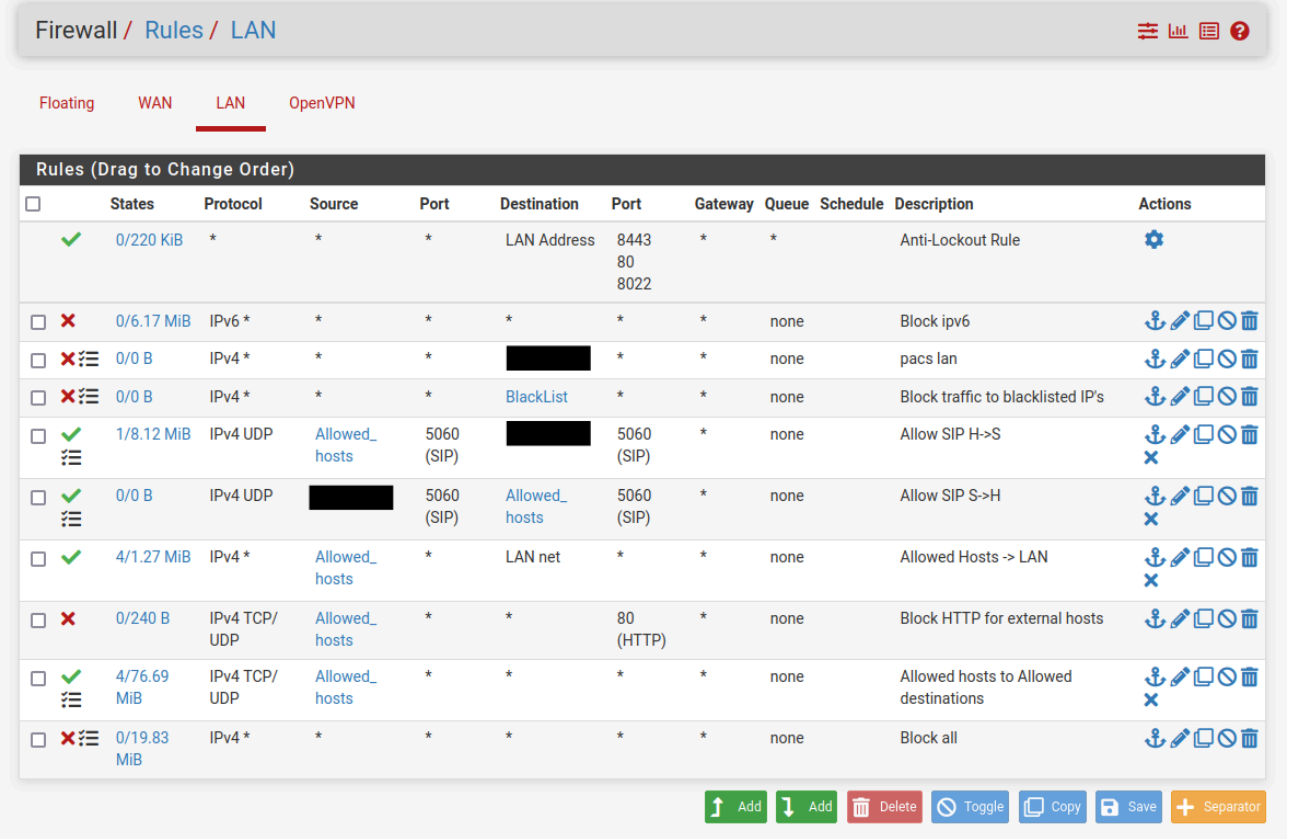
Alertes déclenchées par Suricata sur un routeur

Comme vous pouvez le constater, le nombre d'alertes est élevé. On y voit fréquemment des tentatives de connexion depuis l'extérieur ou depuis l'intérieur vers des sites frauduleux.

Suite à cette observation, j'ai ajouté des règles sur les interfaces LAN et WAN des routeurs. Étant donné que ces règles devaient être restrictives, j'ai appliqué l'ensemble des règles suivantes à tous les routeurs afin de normaliser le tout.

pfsense-manager add-rule --hosts ./hosts.toml --user admin --passwords ./ADMINS_PASSWD.json.gpg --gnupg ./.gnupg --description "Allow WEB" --dst @IP --dstport "80-443" --interface "lan" --protocol "tcp" --src "Allowed_hosts" --srcport "any"

Ces commandes illustrent comment mon outil permet de gérer et sécuriser efficacement le réseau en ajoutant, modifiant et appliquant des règles de pare-feu de manière standardisée sur l'ensemble des routeurs. Grâce à cette automatisation, j'ai pu garantir une configuration cohérente et sécurisée pour tous les sites gérés.



Règles ajoutées après utilisation du paquet pfsense-manager

3.3. Monitoring des pare-feu

En plus de la surveillance du réseau, il est crucial de surveiller le matériel. Il était donc nécessaire de mettre en place un système de monitoring pour nos routeurs et de disposer d'un serveur de logs. L'entreprise possédant déjà un serveur Nagios Core 4, je devais y ajouter les routeurs. Nagios utilise le protocole NRPE (Nagios Remote Plugin Executor). Le serveur envoie une requête sur le port 5666 d'une machine, et celle-ci y répond.

Dans notre cas particulier, le serveur avait une adresse IP publique tandis que les routeurs possédaient des adresses IP privées, ce qui rendait les routeurs inaccessibles pour le serveur, qui devait initier la connexion. Pour résoudre ce problème, nous avons choisi d'utiliser des tunnels SSH.

La solution consistait à établir des tunnels SSH pour permettre au serveur Nagios de communiquer avec les routeurs malgré la différence de réseau.

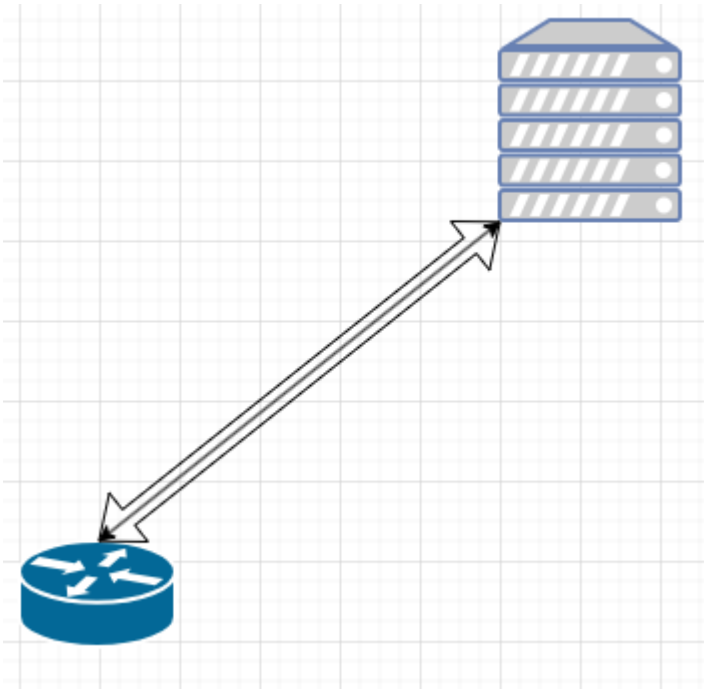


Schéma du lien ssh entre un routeur et le serveur Nagios

Sur ce schéma, la grande flèche représente le tunnel ssh et la plus petite le trafic NRPE.

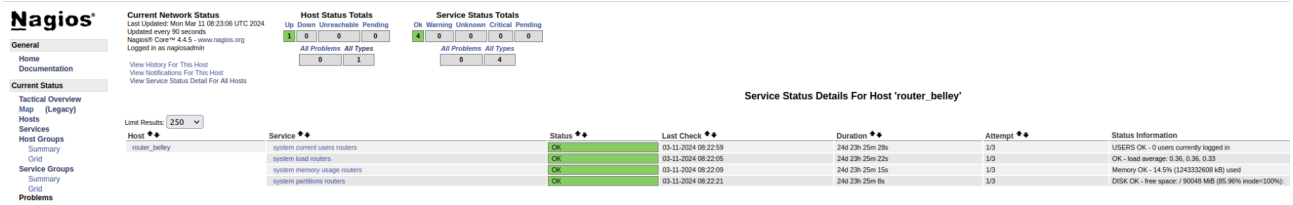
Commande autossh pour maintenir le tunnel:

/root/autossh -M 0 -N -o "ExitOnForwardFailure=yes" -o "ServerAliveInterval 30" -o "ServerAliveCountMax 3" -o "ConnectTimeout 10" -o "ExitOnForwardFailure yes" -i /root/.ssh/tunnelssh -R 6001:localhost:5666 [user]@[NAGIOS IP] -N -f &

La commande précédente montre le tunnel SSH créé depuis le routeur vers le serveur Nagios. Dans la configuration du serveur, nous indiquons à Nagios d'exécuter les requêtes sur localhost:6001. Grâce au tunnel, ce trafic est redirigé vers le port 5666 du routeur. La commande `autossh` garantit que le tunnel est recréé en cas de coupure, que ce soit à cause d'un redémarrage ou d'un timeout. Malheureusement, `autossh` est souvent instable sur FreeBSD, ce qui m'a obligé à trouver une autre solution.

J'ai choisi de faire transiter le trafic NRPE à travers le VPN. Pour cela, j'ai ajouté un client VPN sur le serveur Nagios, auquel une adresse IP est attribuée (par exemple : 1.2.3.4). Ensuite, j'ai spécifié au routeur de n'accepter que les requêtes NRPE provenant de cette adresse.

L'interface Nagios après l'ajout d'un routeur ressemble à ceci :



Interface Nagios avec l'état de la machine surveillée

On peut observer que Nagios va effectuer une requête via le protocole NRPE pour demander des informations au routeur. Il va ainsi solliciter l'état de plusieurs éléments tels que le taux d'utilisation de l'espace disque dur, de la mémoire vive, le nombre d'utilisateurs connectés et la charge de travail du routeur. Toutes ces données permettent de surveiller l'état général du routeur.

Une fois Nagios configuré pour surveiller les routeurs, j'ai entrepris la création d'un serveur ELK (Elasticsearch, Logstash, Kibana) afin d'assurer le stockage des logs sur une période prolongée. L'ensemble ELK permet de récupérer les logs d'une machine, de les stocker et de les consulter en indexant les données pour pouvoir les trier avec une large possibilité de filtres.

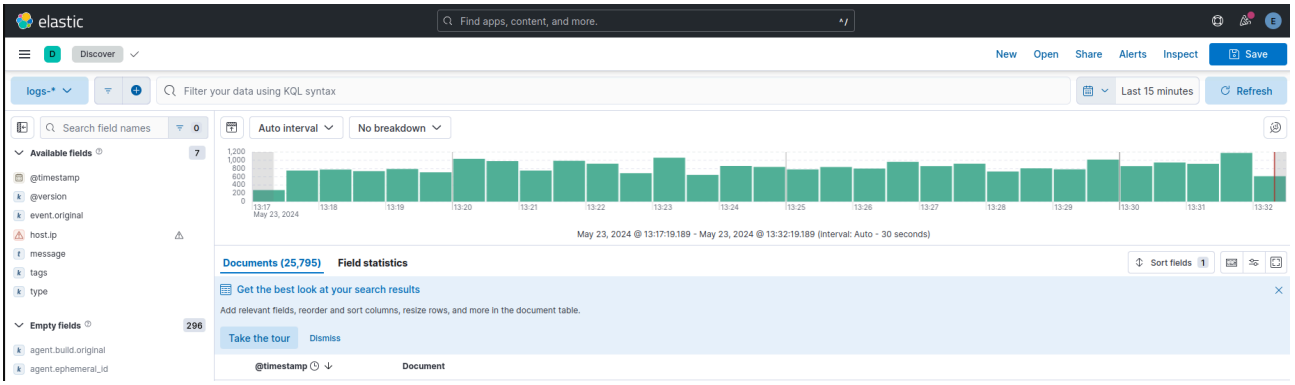
J'ai configuré tous les routeurs pour qu'ils envoient tous leurs logs vers mon serveur. Cependant, un nouveau problème est survenu. Pour chaque cabinet, le routeur passe par la box de l'opérateur. La source de l'envoi des logs pour mon serveur est donc la box de l'opérateur et non le routeur lui-même, en raison d'une translation d'adresse ou NAT effectuée en sortie de la box. Le problème réside dans le fait que l'adresse externe change fréquemment. Par conséquent, après une semaine, j'ai constaté un grand nombre

d'entrées invalides dans mes logs car les adresses ne correspondaient plus. Pour résoudre ce problème, j'ai décidé de connecter mon serveur ELK public à notre VPN principal. Cela a permis de stabiliser la source des logs.

Par la suite, j'ai pris la décision de séparer les logs en tables de vues pour faciliter la lecture et la compréhension des logs lors de leur analyse. Cette approche a permis d'améliorer significativement la lisibilité et l'interprétation des données enregistrées dans les logs.
. J'ai séparé ces tables par catégories qui sont :

- Logs généraux
- Logs Suricata interface WAN
- Logs Suricata interface LAN

Voici quelques exemples du rendu final :



Interface web ELK avec le retour des logs des routeurs

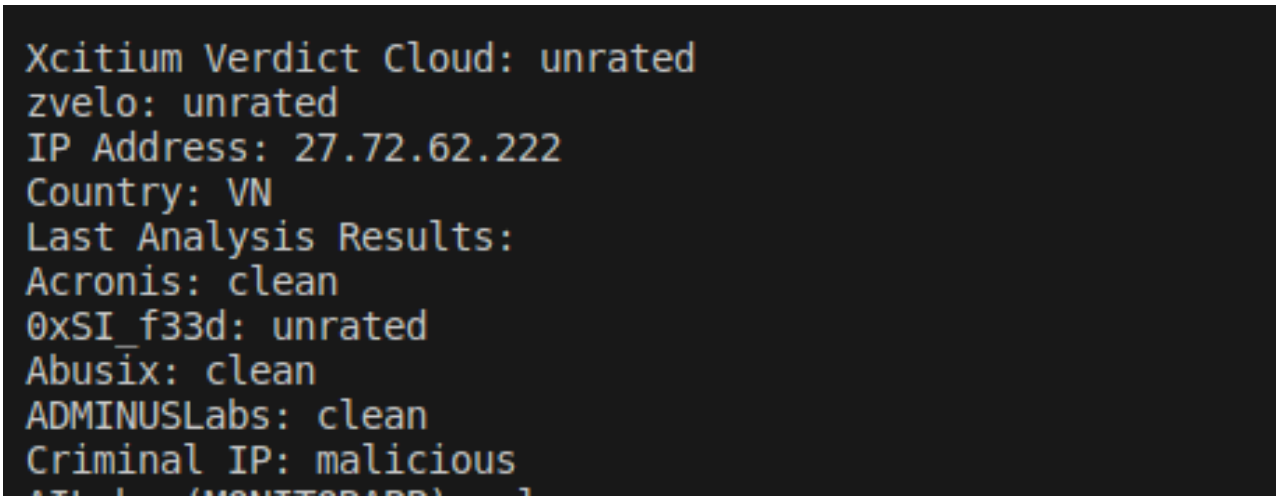
Face à la question de filtrer les adresses IP malveillantes, l'utilisation de Suricata pour bloquer automatiquement ces adresses est une solution envisageable. Cependant, il est important de noter qu'une telle approche peut entraîner le blocage d'adresses IP internes légitimes qui pourraient être la cible d'attaques extérieures. De plus, certaines adresses IP, comme celles de serveurs Microsoft, peuvent être identifiées à tort comme dangereuses par Suricata.

Pour contourner ce problème, j'ai développé un outil en Python qui récupère les logs générés par les alertes de Suricata sur ELK via son API REST. Cette approche présente l'avantage d'améliorer la sécurité en centralisant la récupération des logs sur ELK plutôt que de le faire directement sur les routeurs.

Mon script permet de spécifier pour quel routeur récupérer les logs. Ensuite, j'utilise l'API du site VirusTotal pour scanner chaque adresse IP et obtenir des informations sur sa

réputation. VirusTotal est un site web sur lequel des personnes peuvent signaler une adresse IP. Plus l'adresse est signalée, plus elle est catégorisée comme malicieuse. Les adresses IP malveillantes sont alors stockées dans une liste noire. Pour chaque adresse identifiée comme malicieuse, j'utilise mon paquet Python pfsense-manager pour les ajouter à un nouvel alias "BlackList" sur le routeur correspondant. Le trafic à destination de ces adresses est ainsi directement bloqué par une règle du pare-feu du routeur.

Cette approche permet une gestion efficace des adresses IP malveillantes tout en évitant les inconvénients potentiels de bloquer des adresses légitimes. De plus, elle offre une flexibilité et une personnalisation permettant d'adapter la politique de sécurité en fonction des besoins spécifiques de l'entreprise.



Extrait du résultat de l'utilisation de VirusTotal pour scanner une adresse IP

C'est une approche très bien pensée et sécurisée pour gérer les adresses IP malveillantes. Voici un résumé des étapes clés de votre processus :

1. Récupération des logs sur ELK : Vous récupérez les logs générés par les alertes de Suricata sur ELK via son API REST.

2. Analyse des adresses IP : Pour chaque adresse IP provenant des logs, vous utilisez l'API du site VirusTotal pour vérifier si elle est malicieuse. Vous stockez ensuite les adresses IP malveillantes dans une liste noire.

3. Vérification des adresses IP : Avant d'ajouter une adresse IP à la liste noire, vous vous assurez qu'elle ne correspond à aucun réseau ou machine appartenant à votre entreprise.

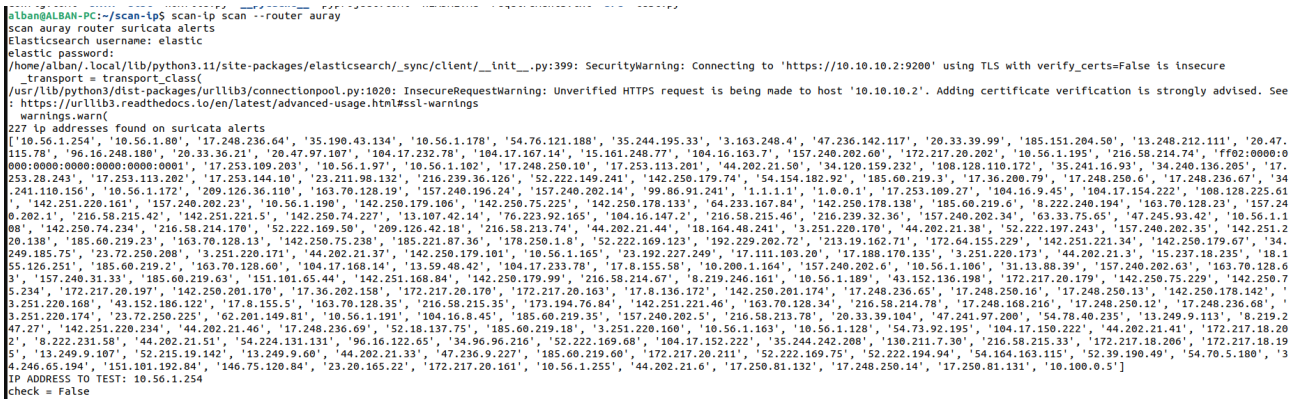
4. Gestion sécurisée des mots de passe : Vous avez mis en place une option dans votre script pour prendre en charge un fichier chiffré au format GPG contenant un mot de passe. Cela permet de stocker les mots de passe de manière sécurisée sur la machine.

5. Optimisation de l'utilisation de l'API : Pour optimiser l'utilisation de l'API de VirusTotal, chaque adresse IP testée est enregistrée dans une base de données, ce qui évite de les retester ultérieurement.

6. Gestion du quota d'utilisation de l'API : Étant donné que le site VirusTotal limite le nombre de requêtes par jour, vous prenez soin de gérer ce quota en enregistrant les adresses IP testées pour éviter de les retester inutilement.

Ces mesures garantissent une approche efficace et responsable dans la gestion des adresses IP malveillantes, tout en assurant la sécurité et la confidentialité des données et des processus.

Voici un exemple de l'exécution du script :



La mise en place d'une solution de secours pour le routeur central hébergé sur AWS est une étape cruciale pour garantir la continuité de service du réseau de Vizyon. Voici comment vous avez abordé cette tâche :

1. **Création d'une image de l'instance du routeur :** Comme il n'est pas possible de créer directement un clone de l'instance du routeur sur AWS, vous avez opté pour la création d'une image de l'instance existante. Cette image vous permet de rapidement déployer une nouvelle instance en cas de problème.

2. **Déploiement d'une instance de secours :** En cas de dysfonctionnement de l'instance principale, vous utilisez l'image précédemment créée pour déployer une nouvelle instance

de secours. Les adresses IP élastiques vous permettent de dissocier l'adresse IP publique de l'instance en panne et de l'associer à la nouvelle instance de secours. Ainsi, les autres routeurs ne remarquent pas de différence et se reconnectent automatiquement à la nouvelle instance, assurant ainsi la continuité de service du réseau.

Ce processus de secours garantit une haute disponibilité du routeur central, permettant ainsi de minimiser les interruptions de service et d'assurer une connectivité continue des tunnels VPN essentiels pour le fonctionnement des cabinets.

4. Bilan personnel, savoir et savoir être :

Savoir

Au cours de mon alternance en tant qu'administrateur Réseau spécialisé en cybersécurité, j'ai eu l'opportunité de développer et de renforcer une multitude de compétences techniques. Parmi celles-ci :

1. **Développement d'outils Python :**
   - **Automatisation des tâches :** J'ai créé plusieurs scripts en Python pour automatiser des tâches récurrentes, telles que la surveillance réseau, la gestion des configurations et les analyses de logs.
   - **Détection et prévention des intrusions :** J'ai développé des outils pour analyser les comportements réseau afin de détecter des anomalies et prévenir les intrusions.
   - **Analyse des vulnérabilités :** En utilisant des bibliothèques Python comme Scapy et Nmap, j'ai pu effectuer des analyses approfondies des vulnérabilités réseau.
2. **Gestion et administration réseau :**
   - **Configuration et maintenance :** J'ai participé activement à la configuration et à la maintenance des équipements réseau (routeurs, pare-feu).
   - **Sécurisation des réseaux :** J'ai mis en place des politiques de sécurité et configuré des solutions de pare-feu pour protéger les infrastructures réseau.
   - **Surveillance et diagnostic :** J'ai utilisé des outils de monitoring comme Nagios et Wireshark pour surveiller le trafic réseau et diagnostiquer les problèmes.

3. **Compétences en cybersécurité :**
   - **Implémentation de mesures de sécurité :** J'ai travaillé sur des projets visant à améliorer la sécurité des systèmes d'information, notamment à travers

l'installation et la configuration de systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS).
- **Connaissance des normes et des réglementations :** J'ai approfondi mes connaissances sur les normes de sécurité et veillé à leur application au sein de l'entreprise.

Savoir-être

Mon alternance m'a également permis de développer des compétences interpersonnelles et des qualités professionnelles essentielles :

1. **Travail en équipe :**
   - **Collaboration :** J'ai collaboré avec diverses personnes, notamment les équipes de développement et les équipes de support, pour assurer la sécurité et la fiabilité des infrastructures réseau.
   - **Communication :** J'ai appris à communiquer efficacement avec mes collègues, à partager des informations techniques de manière claire et concise, et à rédiger des rapports compréhensibles pour des non-spécialistes.
2. **Gestion du temps et organisation :**
   - **Priorisation des tâches :** J'ai acquis la capacité de prioriser les tâches en fonction de leur urgence et de leur importance, ce qui m'a permis de gérer efficacement mes projets.
   - **Autonomie :** J'ai développé une grande autonomie dans la gestion de mes missions, tout en sachant quand solliciter l'aide de mes supérieurs ou de mes collègues.
3. **Adaptabilité et résilience :**
   - **Réaction face aux incidents :** J'ai appris à réagir rapidement et efficacement face aux incidents de sécurité, en gardant mon calme et en adoptant une approche méthodique pour résoudre les problèmes.
   - **Apprentissage continu :** J'ai pris l'habitude de me tenir informé des dernières évolutions dans le domaine de la cybersécurité et de me former régulièrement sur les nouvelles technologies et techniques.
4. **Éthique professionnelle :**
   - **Confidentialité et intégrité :** J'ai respecté strictement les politiques de confidentialité et d'intégrité des données, assurant ainsi la protection des informations sensibles de l'entreprise.
   - **Responsabilité :** J'ai fait preuve de responsabilité dans toutes mes actions, en étant conscient de l'impact de mon travail sur la sécurité globale de l'entreprise.

5. Résumé / summary:

Lors de cette alternance, j'ai appris de nombreuses choses. J'ai appris à mettre en place mes compétences acquises à l'école au profit de l'entreprise. J'ai également appris de nouvelles connaissances et compétences.

J'ai eu l'occasion de perfectionner mon travail d'équipe lors des échanges avec les autres membres. Aussi, je me suis rendu compte qu'il fallait être prudent car chaque action à une conséquence, qu'elle soit bénéfique ou au contraire désastreuse. Cette alternance me conforte également dans mon choix de devenir RSSI (responsable de la sécurité des systèmes d'information) à l'avenir ou de monter mon entreprise de consulting et support informatique.

I learned a lot during my work-study placement. I learned how to apply the skills I'd acquired at school to the benefit of the company. I also learned new knowledge and skills.

I had the opportunity to perfect my teamwork through exchanges with other members. I also realized that you have to be careful, because every action has a consequence, whether it's beneficial or disastrous. This work-study experience has also confirmed my decision to become a CISO (Chief information security officer) in the future, or to set up my own consulting and IT support company.

Glossaire :

ELK : Elasticsearch, Logstash, Kibana, composent ELK. Kibana est l'interface web, Logstash est le serveur qui récupère les logs des machines et Elasticsearch est le serveur qui permet de manipuler les logs. Les 3 sont installer sur la même machine pour une question de simplicité.

Suricata : Outil installé sur une machine, qui génère des alertes lorsqu'il détecte un problème lors de connexions ou manipulations étranges sur une machine.

LAN : Local Area Network, c'est le réseau local.

WAN : Wide Area Network, c'est le réseau public ou extérieur.

GNS3 : Outil de virtualisation de réseaux informatique et équipements

BSD : Distribution d'OS (FreeBSD)

Wireshark : Outil de capture de paquets et analyse

scp : Commande linux qui copie des fichiers entre 2 machines distantes

GitHub : Plateforme de stockage de code et fichiers en ligne

SSH : Secure SHell (Accès au terminal du machine distante)

Nagios : Serveur de monitoring, surveillance de l'état des équipements