Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
Parcours cybersécurité

Mise en place d'une infrastructure de test d'intrusion

Dylan SBAIHI

Ministère de l'intérieur / DNPJ / D@TA-I

Responsable entreprise : Mr. Houssam MABROUK

Responsable académique : Pr. Éric WÜRBEL

2024

Table des matières

1 Remerciements

Je tiens à remercier l'équipe du D@TA-i (Département des Technologies Appliquées à l'Investigation) avec qui j'ai pu travailler durant ces 10 semaines, notamment l'équipe de développeurs en alternance, mon responsable du service public, Houssam MABROUK, Antoine TORRE, responsable du projet qui m'a été confié durant le stage, Sébastien BITTON, chef de section Expertise, et Nicolas ARISTIPE, chef du pôle SSI (Sécurité des Systèmes d'Information), qui ont fait preuve à mon égard d'un bon comportement, d'accompagnement et de soutien. J'ai pu constater des valeurs importantes de bien-vivre ensemble, une très bonne ambiance au sein de l'équipe et une gestion des problèmes et incidents très efficace.

2 Introduction

Je suis actuellement en stage au sein du pôle SSI du D@TA-I de la DNPJ (Direction Nationale de la Police Judiciaire). Ce pôle, réparti sur les sites de Marseille, Paris et Bordeaux, a pour mission l'homologation des systèmes d'information, le développement d'applications et la mise en place d'infrastructures réseau dédiées au réseau interministériel.

L'objectif de mon stage est de contribuer à la sécurisation des systèmes d'information au sein de ce pôle. Mes missions incluent la mise en place d'une infrastructure pour les tests d'intrusion et la configuration d'un VPN (Virtual Private Network) IPsec (Internet Protocol Security) pour les clients nomades. Le pôle SSI valide également les logiciels par des fiches techniques et des rapports de validation à la suite d'analyses de sécurité, participe au déploiement d'outils spécifiques à la SSI, réalise des audits et des tests d'intrusion pour les homologations de sécurité des applications internes, et innove en proposant des outils favorisant la sécurité des systèmes d'information.

Le rapport se déroulera comme suit : dans un premier temps, je présenterai le service au sein duquel j'ai effectué mon stage, puis le contexte et les enjeux de mes missions. J'expliquerai en détail le déroulement de chacune de mes missions. Enfin, je conclurai en faisant un bilan de mon expérience et des compétences acquises.

3 Présentation de la DNPJ et de son organisation

3.1 Présentation de la DNPJ

La Direction Nationale de la Police Judiciaire (DNPJ) est l'organisme principal qui supervise plusieurs sous-directions et départements. La DNPJ est chargée de coordonner l'ensemble des services d'investigation situés dans les DDPN (Directions Départementales de la Police Nationale) et les DIPN (Directions Interdépartementales de la Police Nationale). Elle est organisée en plusieurs entités pour assurer un fonctionnement optimal :

- **État-major** : Dirige les opérations et fixe les orientations stratégiques.
- **Sous-direction de la stratégie et du pilotage territorial** : Responsable de la planification et de la coordination stratégique.

- **Sous-direction des services opérationnels** : Gère les services de terrain qui mènent les investigations.
- **Sous-direction du soutien opérationnel** : Fournit le support logistique et technique nécessaire aux opérations.
- **Département de coopération internationale opérationnelle** : Facilite la collaboration avec les agences internationales.
- **Département des technologies appliquées à l'investigation** : Développe et implémente des technologies pour soutenir les investigations.

3.2 Présentation du D@TA-I

Depuis le 1er janvier 2021, la Direction Nationale de la Police Judiciaire (DNPJ) a mis en place le Département des Technologies Appliquées à l'Investigation (D@TA-i), chargé de coordonner l'ensemble des projets technologiques portés par la DNPJ, qu'ils soient destinés à l'ensemble de la communauté de l'investigation ou à une seule unité.

Figure 1: Logo du D@TA-i

D@TA-I, une sous-direction de la DNPJ, a pour mission d'animer les différentes communautés contribuant au succès des projets d'investigation, incluant les usagers de l'information et les administrateurs.

Elle se consacre à la gestion et à la sécurisation des systèmes d'information, en améliorant la performance et la fiabilité des infrastructures utilisées par les services d'investigation.

Face à des enjeux importants d'évolution, d'interopérabilité et aux attentes très fortes des agents, la création de D@TA-i autour de métiers complémentaires et interdépendants permet de consolider l'expertise, l'organisation et le professionnalisme de la DNPJ dans la prise en compte des projets technologiques majeurs pour l'investigation.

3.3 Organisation de D@TA-I

D@TA-I est dirigé par un chef de service et son adjoint, et se compose de six pôles de compétences ainsi que d'un état-major, regroupant plus de 200 personnels répartis sur différents sites : Paris, Nanterre, Le Chesnay, Pantin, Écully, Marseille, Rennes, Lille, Bordeaux et Mulhouse.

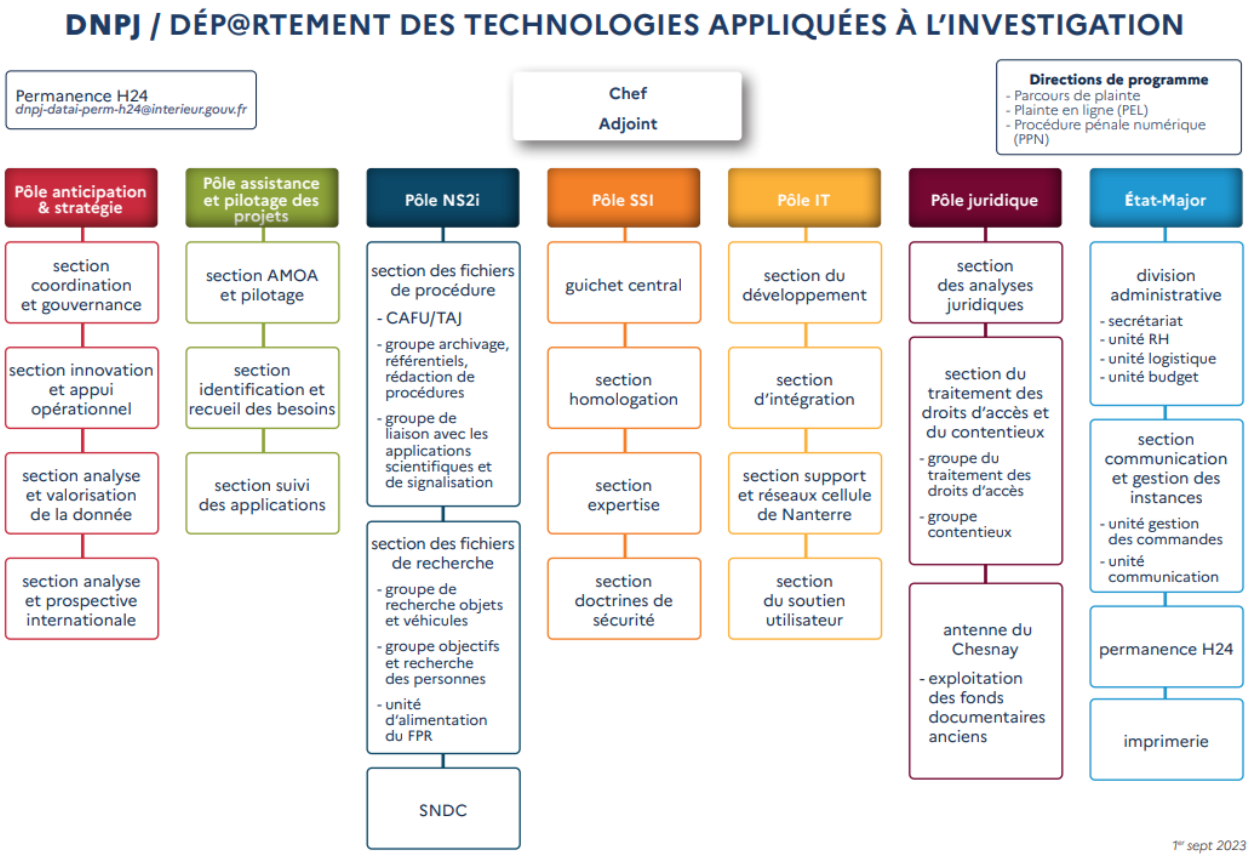


Figure 2 : Organigramme du D@TA-i

3.4 Mon Poste au sein de D@TA-I

Actuellement, je suis affecté au Pôle SSI, plus précisément dans la section Expertise. Cette section est responsable de la validation des logiciels (à travers des fiches techniques et des rapports de validation à la suite d'analyses de sécurité) et participe au déploiement d'outils spécifiques à la SSI.

Ma mission principale consiste à contribuer à la mise en place d'infrastructures réseau sécurisées pour effectuer des tests d'intrusion et ainsi garantir la sécurité des systèmes d'information.

4 Environnement de travail

Voici quelques photos de l'environnement de travail au sein du D@TA-i de Marseille. La pièce où je me trouve est occupée par les alternants et stagiaires, ce qui permet de maintenir une bonne ambiance ainsi qu'un certain confort grâce au fait d'être entouré de personnes plus ou moins du même âge. Les bureaux ont été installés récemment, ce qui fait que l'aménagement reste simple mais efficace.

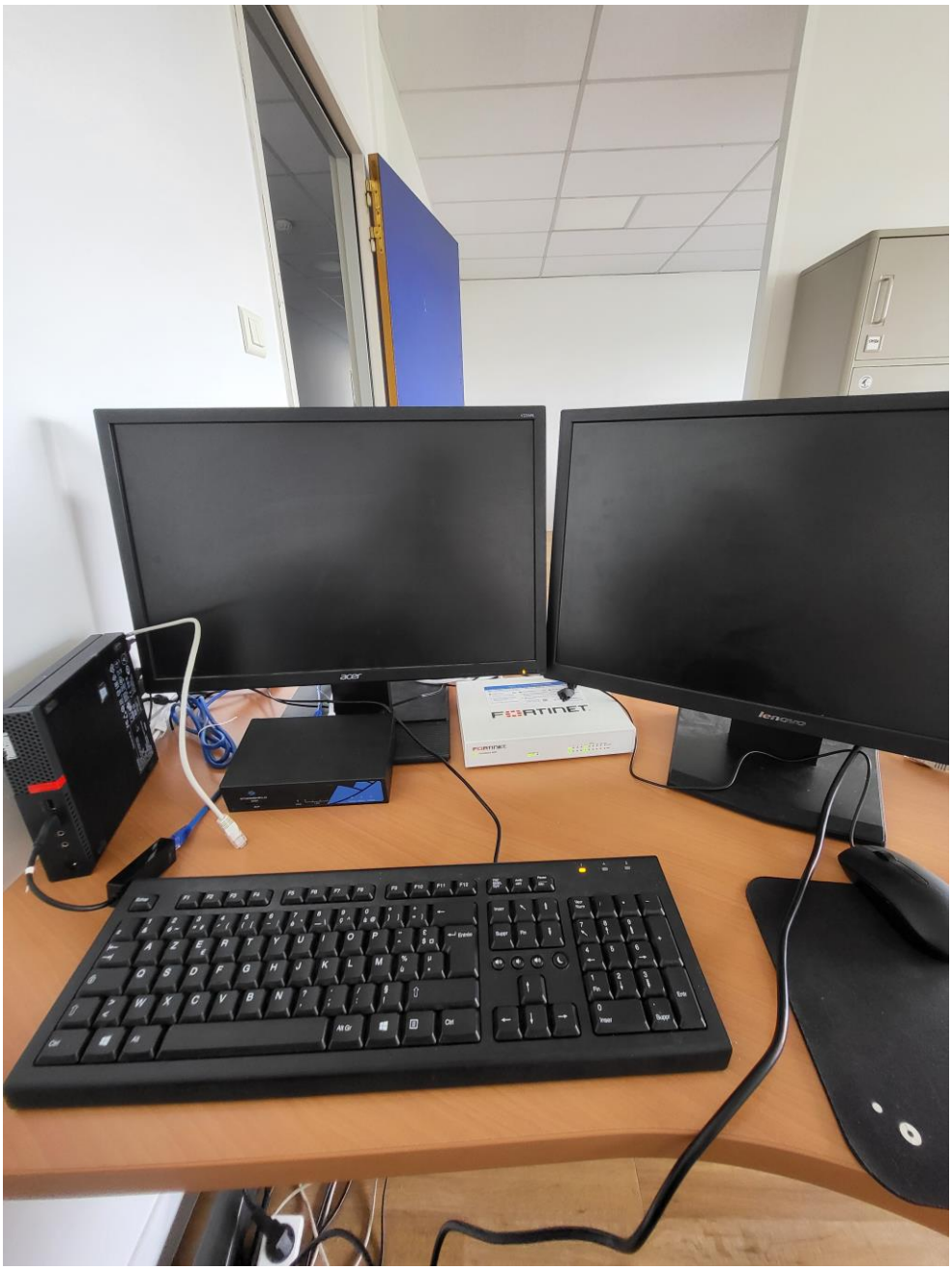
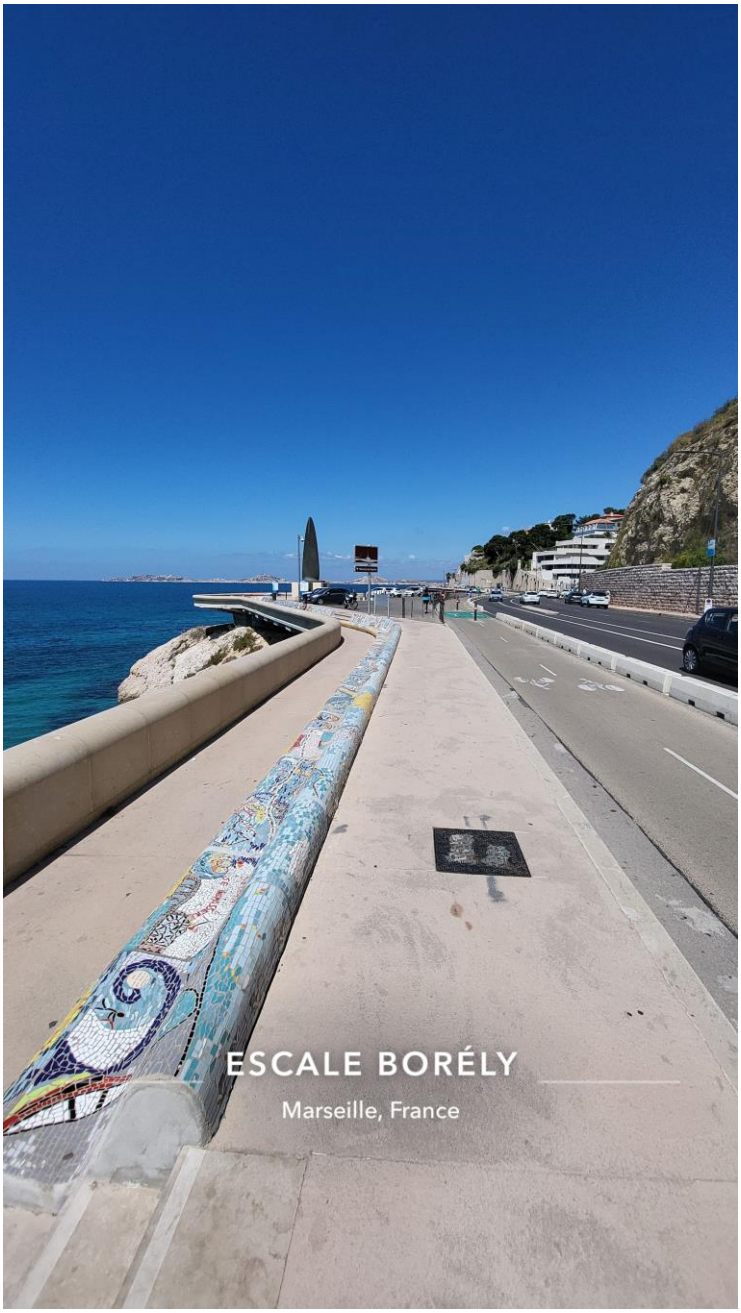


Figure 3 : mon bureau au sein du D@TA-i

Une journée type durant le stage : la journée commence dès le réveil à 6h00, étant donné que je commence à 9h00 et qu'il me faut en moyenne 1h10 de trajet, je pars à 7h45. Une fois arrivé, le chef de pôle, M. Nicolas ARISTIPE, est toujours présent, ainsi que les fonctionnaires (ingénieurs).

Vers 9h30 ou 10h00, l'équipe se regroupe dans la salle commune pour discuter brièvement de ce qu'il y a à faire, des problèmes rencontrés ou des nouveautés.

Entre 12h et 13h30, un footing est organisé, étant donné la proximité avec la corniche. Nous faisons donc un footing avant de manger.



Ensuite, je travaille sur le projet pour le reste de la matinée. En général, l'après-midi me permet de faire le point sur l'avancement du projet avec les cadres et de progresser sur les problèmes rencontrés.

Figure 4: ambiance au sein du D@TA-i

5 Diffusion restreinte

Pour des raisons de sécurité, certains aspects techniques du projet sont soumis à une diffusion restreinte. En conséquence, je ne pourrai pas aborder ces éléments en détail dans ce rapport.

6 Infrastructure dédiée au test d’intrusion

6.1.1 Objectif

Ce projet vise à développer une infrastructure spécialement conçue pour les tests d’intrusion, qui sera déployée sur les différents sites du pôle SSI.

Les tests d'intrusion, également connus sous le nom de "pentesting", sont des évaluations de sécurité cruciales où des experts en sécurité simulent des attaques malveillantes sur les systèmes informatiques afin d'identifier et d'exploiter les vulnérabilités.

Cela permet de renforcer la sécurité en prévenant les intrusions potentielles et en améliorant les mécanismes de défense de l'entreprise.

- **Appropriation du document technique** : Cette phase initiale est cruciale pour acquérir une compréhension approfondie des objectifs, des contraintes et des spécificités du projet. Le document technique sert de fondement à toutes les actions subséquentes en fournissant les directives et les standards à suivre.

- **Analyse et plan d'action** : À la suite de l’analyse du document technique, un plan d'action détaillé est élaboré. Ce plan définit les procédures et les étapes nécessaires pour la mise en place efficace de l'infrastructure de test.

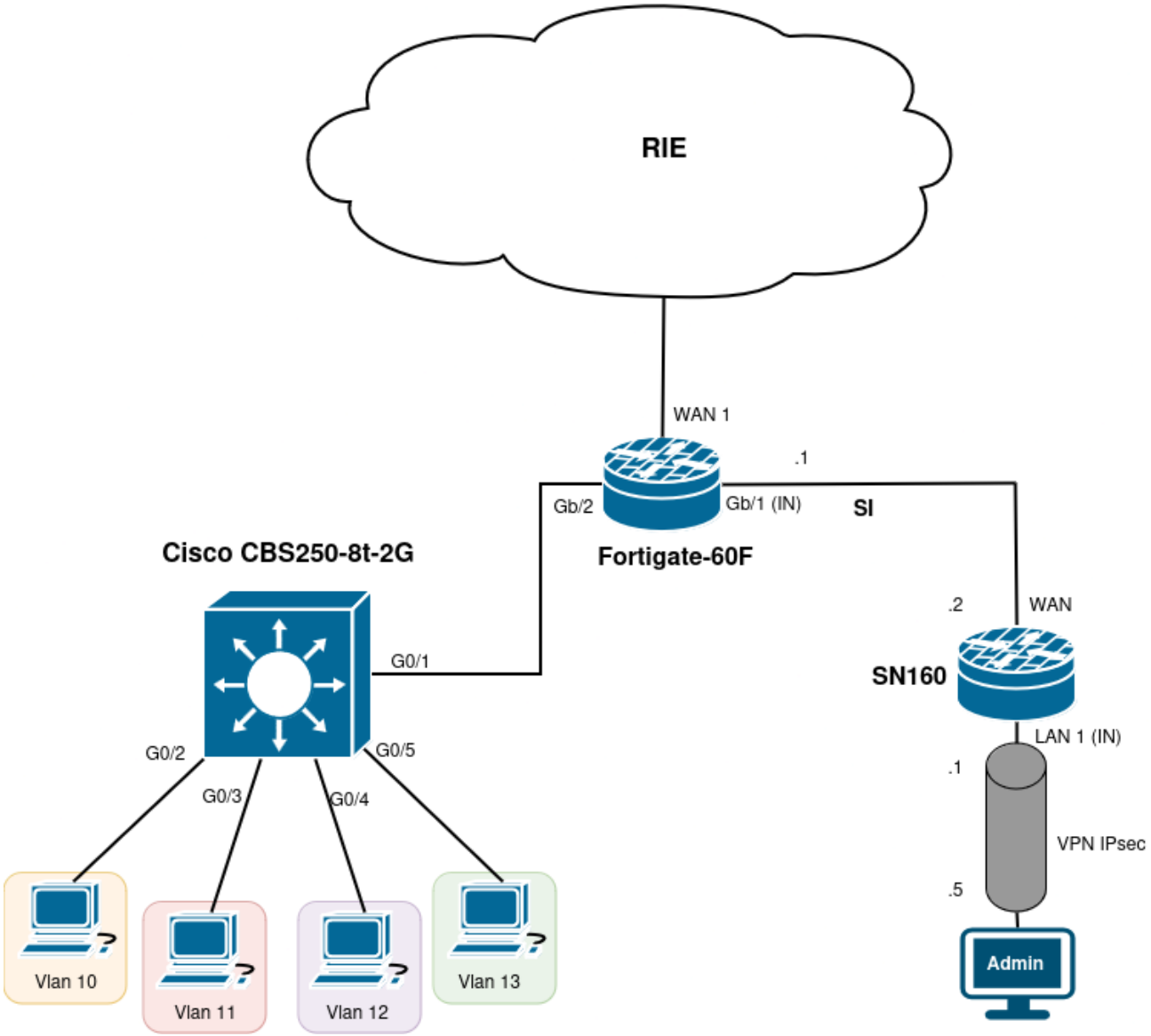
- **Réception et configuration de l'équipement** : Après la réception des équipements nécessaires, la phase de configuration commence. Cette étape est essentielle pour s'assurer que tous les composants matériels et logiciels sont correctement installés et configurés selon les spécifications du projet, permettant ainsi de réaliser des tests d’intrusion dans un environnement contrôlé et sécurisé.

Chaque étape de ce projet est conçue pour garantir que l'infrastructure de test d'intrusion soit robuste, sécurisée et capable de simuler des scénarios d'attaque réalistes, afin de préparer l'entreprise à mieux se défendre contre les cyberattaques.

6.1.2 Présentation de l'architecture

L'illustration ci-dessous présente l'architecture réseau conçue dans le cadre du projet, mettant en évidence la disposition des composants principaux tels que les firewalls, le switch, les PC, les VLAN et le VPN.

Elle montre également les flux de données entre ces éléments, assurant la sécurisation et l'optimisation des communications au sein de l'infrastructure. Conçue pour réaliser des tests d'intrusion, cette architecture n'est pas connectée à Internet, garantissant ainsi un environnement de test sécurisé et isolé.



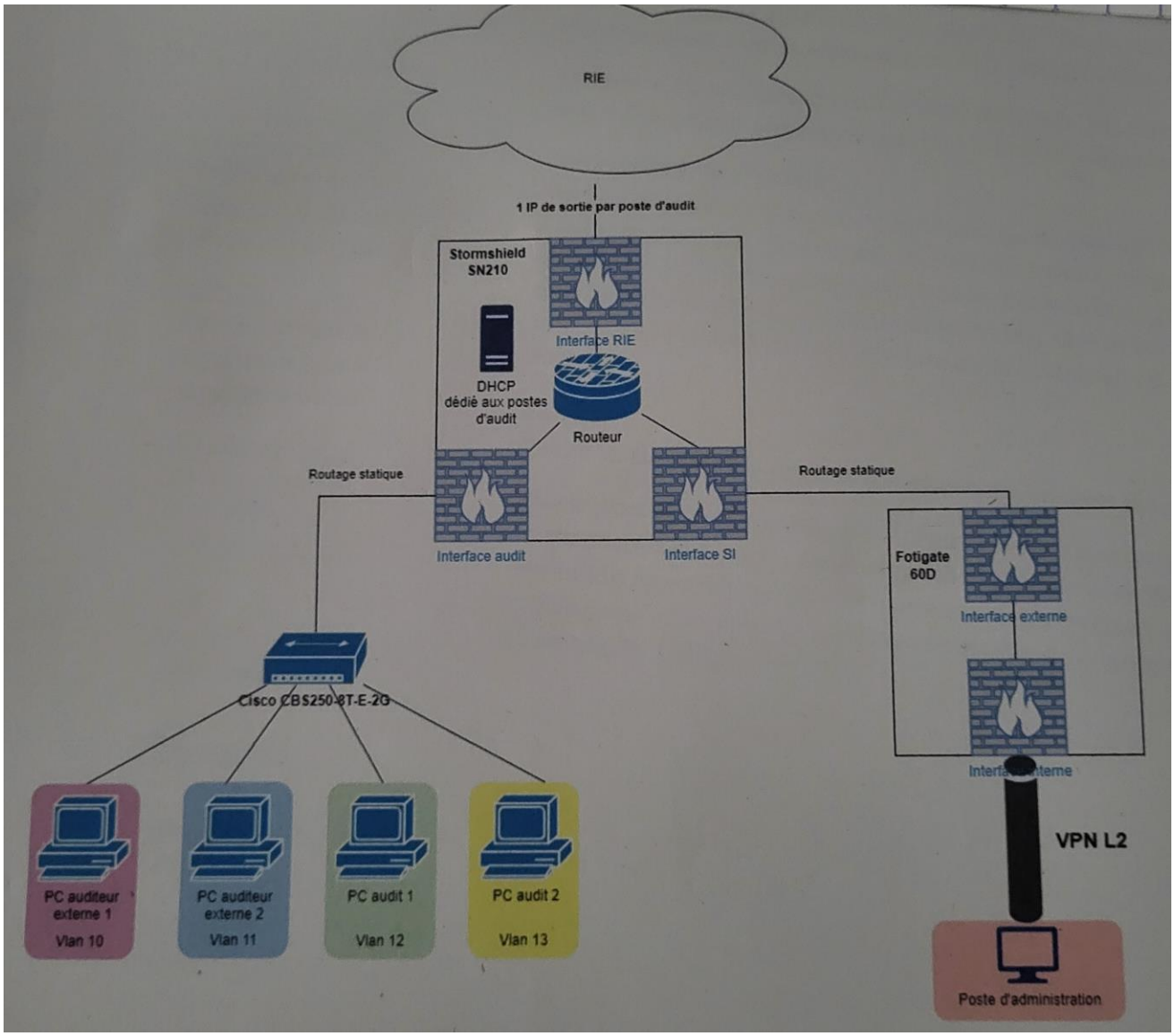


Figure 5: Schéma de l'infrastructure de test

6.1.3 Conception Réseau sous Packet Tracer et GNS3 avant déploiement

Étant donné que l'équipement n'était pas disponible à mon arrivée (il ne l'a été que deux semaines plus tard), j'ai dû réaliser l'architecture sous Packet Tracer et GNS3 (logiciels permettant la conception d'architectures réseau ainsi que la configuration des équipements). J'ai rencontré des contraintes, notamment avec Packet Tracer, car les équipements utilisés pour le projet ne sont pas intégrés dans le logiciel Cisco. De plus, pour GNS3, une licence était nécessaire pour pouvoir utiliser les VM de firewalls Stormshield ou Fortinet et les switchs Cisco.

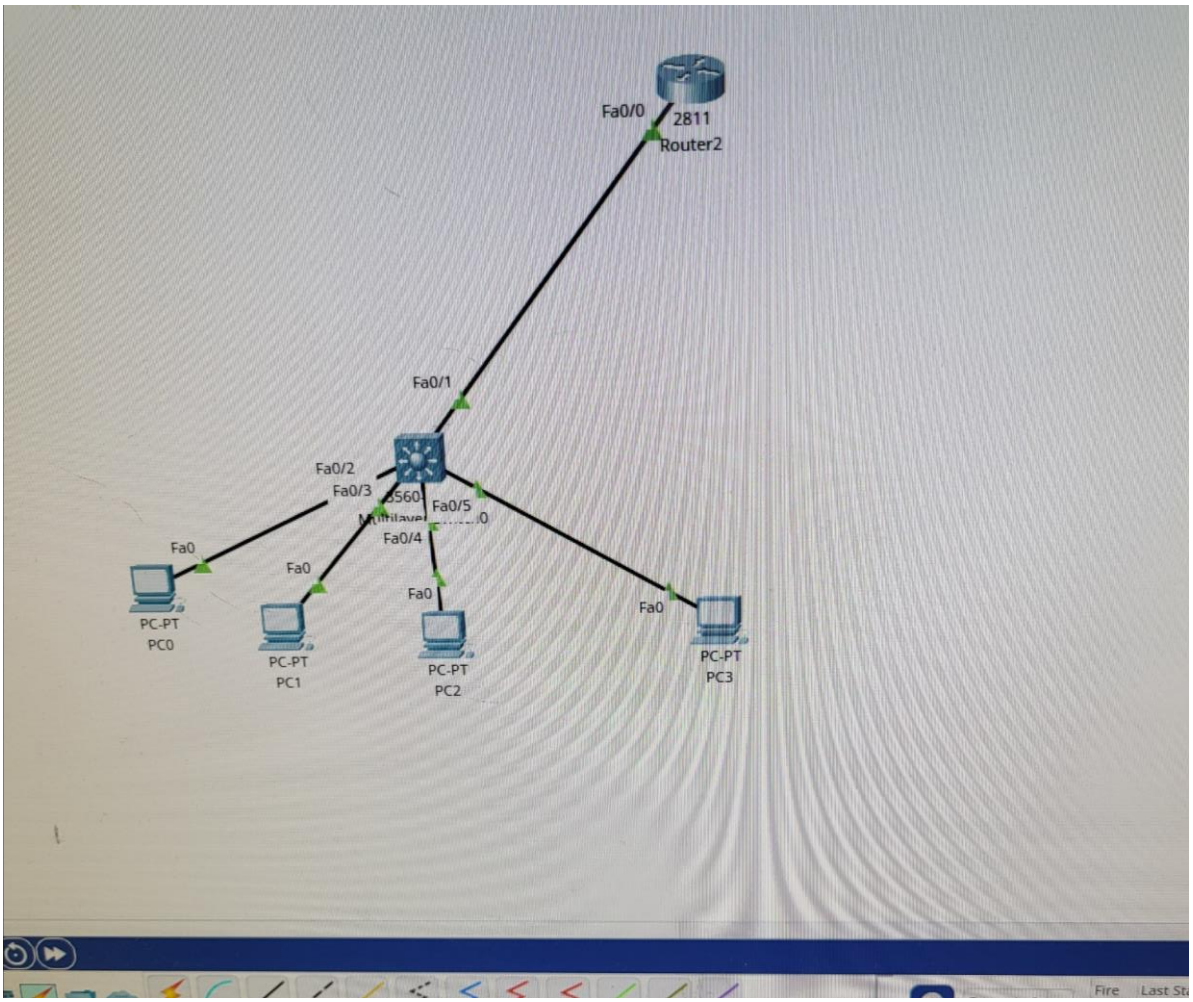


Figure 6: Illustration packet Tracer

Je n'ai donc pas pu réaliser cette première tâche comme prévu. En attendant l'arrivée des équipements, j'ai travaillé sur une feuille et effectué différentes tâches préparatoires telles que la configuration du switch, le plan d'adressage, et des réunions avec les responsables techniques pour discuter de certains éléments de l'architecture.

Figure 7: Logo de GNS3

Figure 8: Logo de Cisco Packet Tracer

6.2 Équipement et logiciel nécessaire

Pour la réalisation de ce projet, plusieurs équipements et logiciels ont été utilisés afin de créer une infrastructure sécurisée et performante.

En ce qui concerne les équipements, nous avons principalement employé un switch (commutateur, équipement réseau acheminant les données via les adresses MAC (Media Access Control, identifiant unique attribué à chaque interface réseau) et des firewalls (pare-feu, dispositifs de sécurité réseau qui surveillent et contrôlent le trafic réseau entrant et sortant pour protéger les systèmes contre les attaques) de marques différentes, Stormshield et Fortinet, représentant une surcouche de sécurité. Ces composants ont été choisis pour leur fiabilité et leurs capacités avancées en matière de sécurité et de gestion réseau.

Pour les logiciels, nous avons opté pour des outils d'analyse réseau, de virtualisation, et des clients VPN (Virtual Private Network, réseau privé virtuel permettant de sécuriser et de chiffrer les connexions à un réseau). VirtualBox (logiciel de virtualisation permettant de créer et de gérer des machines virtuelles sur un ordinateur hôte) a été utilisé pour la virtualisation des différents postes, permettant de simuler différentes configurations de réseau et d'environnement de manière efficace et contrôlée. De plus, des logiciels de client VPN ont été employés pour sécuriser et gérer les connexions, essentielles pour l'accès sécurisé aux ressources du réseau lors des phases de test.

Ces outils et équipements ont constitué la base matérielle et logicielle du projet, facilitant la conception, la simulation, et finalement la mise en œuvre de l'infrastructure réseau destinée aux tests d'intrusion.

6.2.1 Firewalls

6.2.2 Besoin de sécurité

L'implémentation de deux firewalls en cascade est une stratégie adoptée pour renforcer la sécurité en isolant le réseau administratif des potentielles attaques provenant du Réseau Interministériel de l'État (RIE) et du réseau d'audit. L'utilisation de firewalls de marques différentes augmente cette sécurité en diversifiant les technologies employées, ce qui réduit le risque d'exploitation de vulnérabilités communes susceptibles de compromettre l'ensemble de l'infrastructure réseau.

6.2.3 Firewall interne

L'idée initiale du projet était d'utiliser le firewall Fortinet 60F comme firewall interne. Il sera donc, selon le schéma de l'architecture du réseau, connecté au poste d'administration, et un VPN sera mis en place pour permettre une authentification sécurisée. Ainsi, l'accès au firewall interne sera limité au poste d'administration.

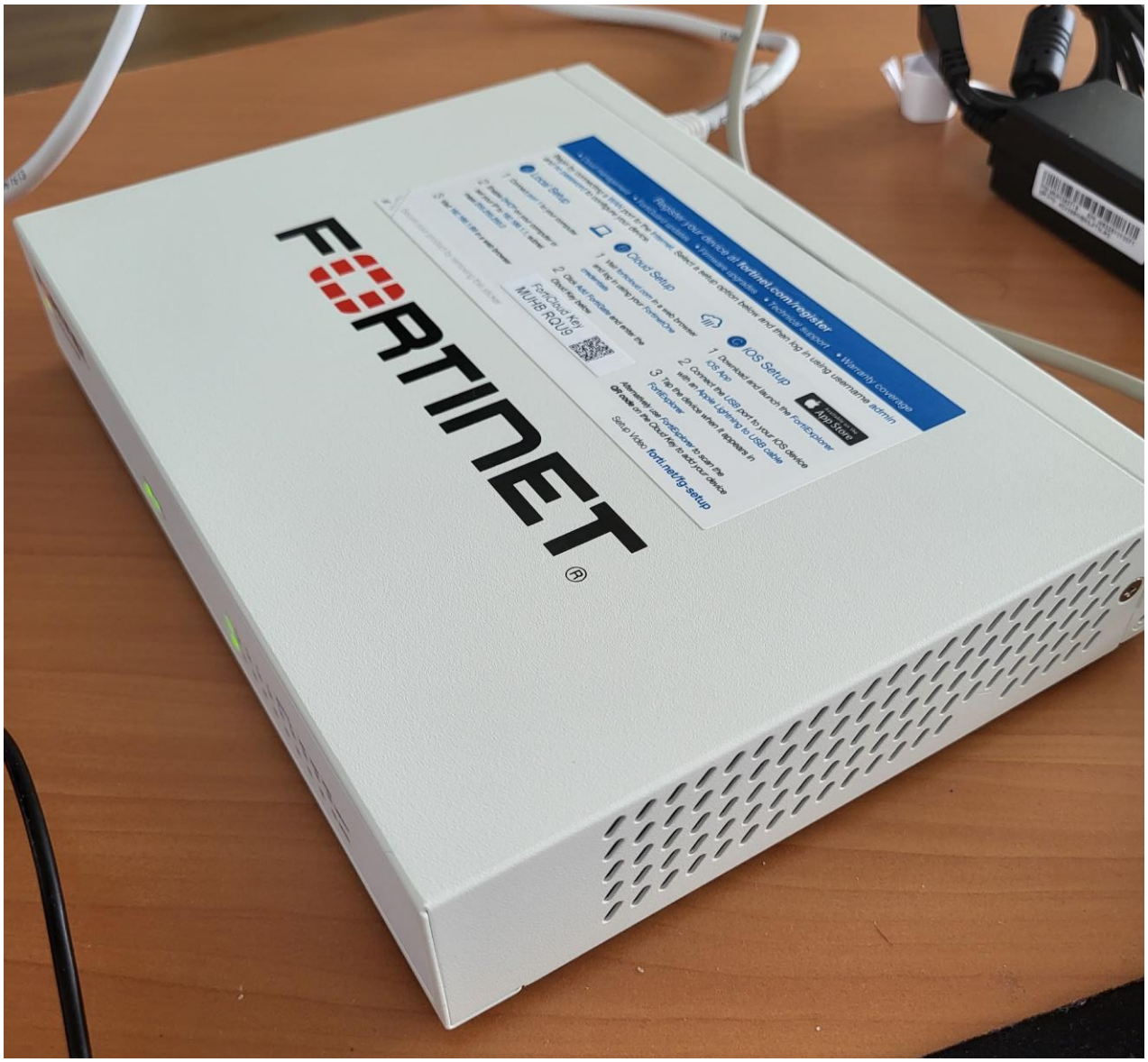


Figure 9: Firewall Fortinet 60F

6.2.4 Configuration de l'équipement (après les contraintes)

Le plus de cette mission est que, grâce au cours récent que nous avons eu sur les firewalls, notamment sur le firewall Stormshield SN160, j'ai pu être directement efficace et prendre en main l'environnement ainsi que les équipements de travail avec une certaine facilité.

Pour procéder à la bonne configuration des firewalls, je me suis donc inspiré des TPs effectués pendant les cours de M. Jean-Luc DAMOISEAU.

Premièrement, la mise en place d'une configuration de base était nécessaire, telle que : brancher le port **IN** uniquement sur un des ports **LAN** (Local Area Network, réseau local permettant de connecter plusieurs dispositifs au sein d'un espace limité) du pare-feu Stormshield pour permettre l'accès web via le réseau interne (administration).

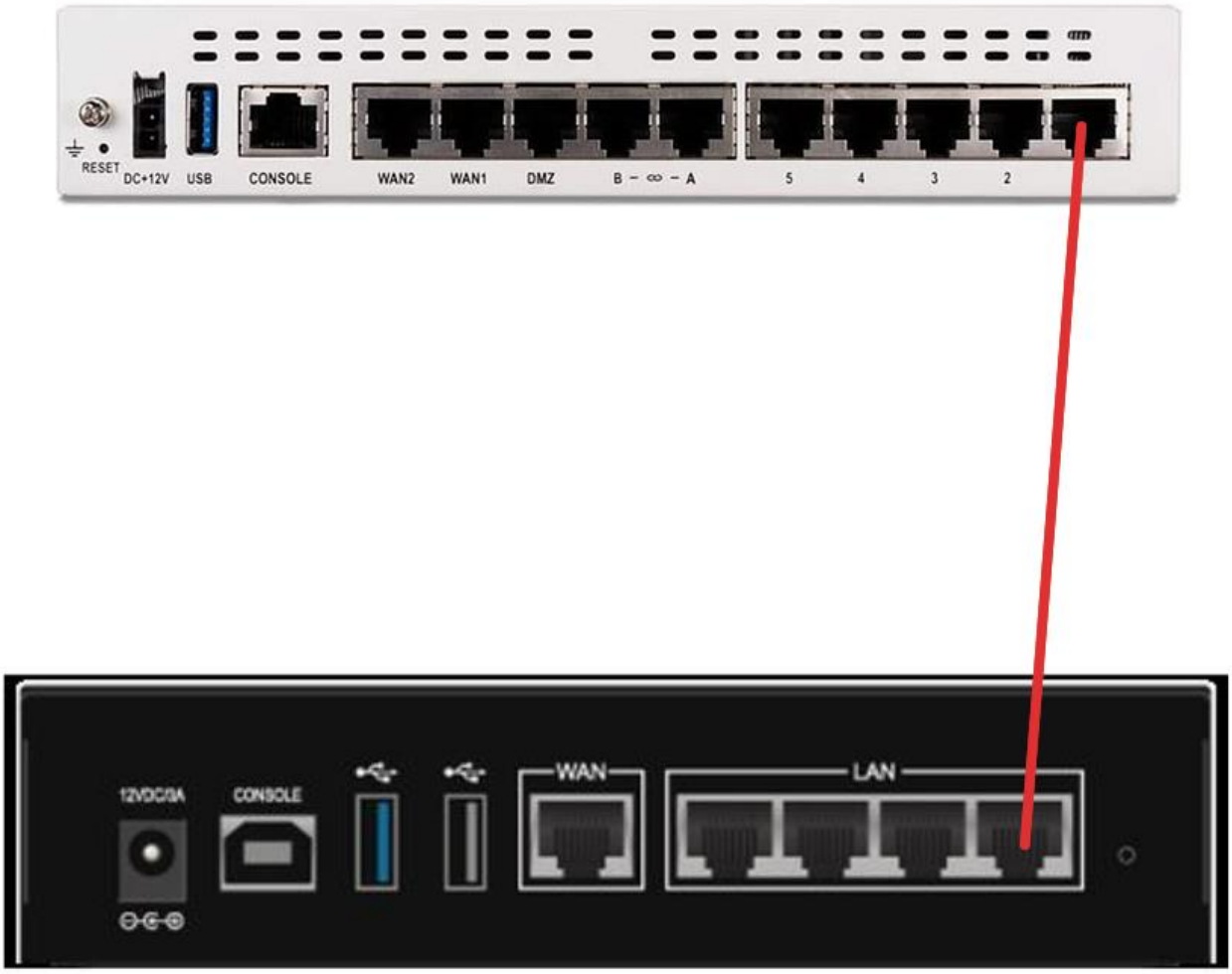


Figure 10: Architecture des firewalls

6.2.5 Firewall externe

Le Stormshield SN160 sera donc la **Gateway** (passerelle, dispositif qui connecte deux réseaux différents) permettant au réseau d'audit d'accéder aux différentes applications du RIE (Réseau Interministériel de l'État). Le rôle essentiel du firewall (pare-feu, dispositif de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant pour protéger les systèmes contre les attaques) externe est le filtrage des flux, limité à certains protocoles nécessaires à l'administration des postes d'audit (mise à jour des postes) et à l'accès aux ressources réseau du RIE.

Figure 111: Firewall Stormshield SN 160

Nous verrons plus tard dans les contraintes du projet pourquoi le Stormshield est devenu le pare-feu interne et le Fortinet le pare-feu externe. L'objectif est d'expliquer l'idée initiale du projet, puis de décrire les contraintes qui sont apparues plus tard.

6.2.6 Configuration de l'équipement (après les contraintes)

De même que pour le Stormshield, une configuration de base doit être mise en place pour le Fortinet (pare-feu de la marque Fortinet, utilisé comme pare-feu externe) et adaptée selon l'architecture réseau.

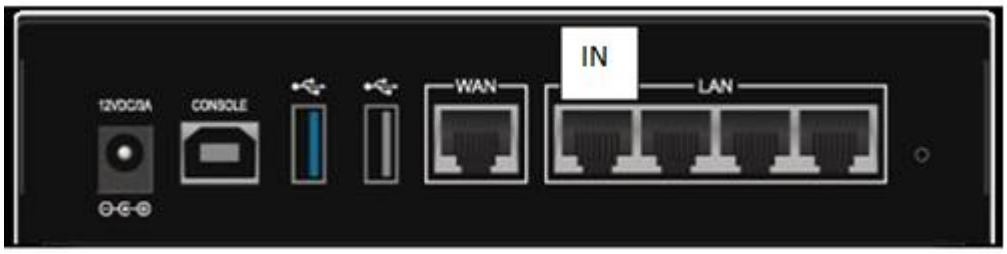


Figure 122: Port IN du Firewall Stormshield SN 160

Le changement du mot de passe administrateur est crucial, étant donné la faiblesse du mot de passe par défaut. Il est nécessaire de sécuriser l'accès au firewall avec un mot de passe plus robuste (au moins 15 caractères, entropie ≥ 100). Cela se fait dans la section : **SYSTÈME** > **CONFIGURATION** > **CONFIGURATION GÉNÉRALE**, politique de mot de passe.

Après avoir appliqué les modifications, allez dans **SYSTÈME** > **ADMINISTRATEURS** pour changer le mot de passe. La configuration des objets a ensuite été réalisée pour permettre la mise en place du tunnel **IPsec** (Internet Protocol Security, protocole de sécurité pour créer des connexions sécurisées sur un réseau). Cette configuration inclut :

- **Adresse du client IPsec** : Correspond à l'adresse du PC lorsque le tunnel sera activé.
- **Adresse IP du poste admin**.
- **Objets réseau** : Représentent le réseau du tunnel IPsec et le réseau interne.

Note : L'explication concernant pourquoi le VPN sera monté sur le Stormshield et non sur le Fortinet sera détaillée plus bas.

La configuration des règles de filtrage (ensemble de règles définissant quel trafic réseau est autorisé ou bloqué) permettant le trafic **IPsec** entre le poste admin et le firewall a été mise en place. Voici le tableau regroupant les règles utilisées :

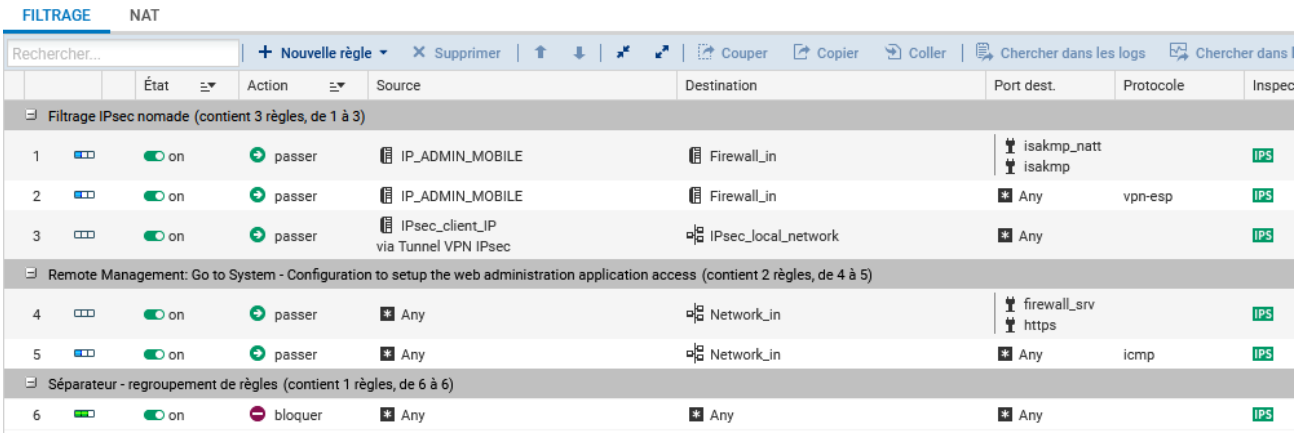


Figure 133: Règle de filtrage IPsec

Ensuite, la configuration d'une politique **IPsec** pour les **clients mobiles** (appareils comme les ordinateurs portables ou les téléphones mobiles qui se connectent au réseau depuis différents endroits) a été mise en place. Pour ce faire, j'ai utilisé comme support de travail le **TP Bonus de** M. Jean-Luc DAMOISEAU, qui portait notamment sur ce sujet. Pour des raisons de diffusion restreinte, je ne peux pas afficher la configuration du tunnel IPsec.

6.2.7 Switch Cisco

Pour notre infrastructure réseau, nous utilisons le **switch Cisco CB250-8T-2G** (commutateur réseau de la marque Cisco, modèle CB250-8T-2G), spécialement sélectionné pour sa capacité à gérer les **VLANs** (Virtual Local Area Network, réseau local virtuel permettant de segmenter un réseau en plusieurs sous-réseaux) et la **segmentation réseau**, ainsi que pour connecter efficacement les postes d'audit. Ce switch permet de structurer le réseau en segments distincts, améliorant ainsi la performance globale et la sécurité en isolant les flux de données critiques.

Figure 144: Switch Cisco CB250-8T-2G

Le commutateur **Cisco CB250-8T-E-2G** (modèle de switch de la marque Cisco) offre une configuration flexible avec 10 ports **Gigabit Ethernet** , incluant 8 ports **RJ45** (type de connecteur standard pour les connexions Ethernet) Gigabit pour des connexions Ethernet standard et 2 ports combinés **SFP** (Small Form-Factor Pluggable, module interchangeable pour l'ajout de différents types de connecteurs et de médias, adaptés pour des liaisons fibre optique), permettant une diversité de connexions réseau haut débit et fiables.

Figure 155:Module SFP

6.2.8 Besoin de sécurité

Segmenter le réseau en quatre **VLANs**, un pour chaque poste d'audit. Désactiver les ports et protocoles non essentiels tels que **CDP** (Cisco Discovery Protocol, protocole de découverte de dispositifs Cisco) et **VTP** (VLAN Trunking Protocol, protocole permettant de propager les informations de VLAN entre les switchs) pour minimiser les risques de sécurité. L'accès à l'administration du switch se fait via **SSHv2** (Secure Shell version 2, protocole de communication sécurisé pour accéder à distance aux équipements réseau), restreint à un seul port spécifique. Activer la sécurité des ports pour limiter l'accès

aux seules adresses **MAC** (Media Access Control, identifiant unique attribué à chaque interface réseau connue) connues des postes d'audit, en attendant de mettre en place une authentification forte (**802.1X**, standard pour l'authentification réseau basée sur les équipements).

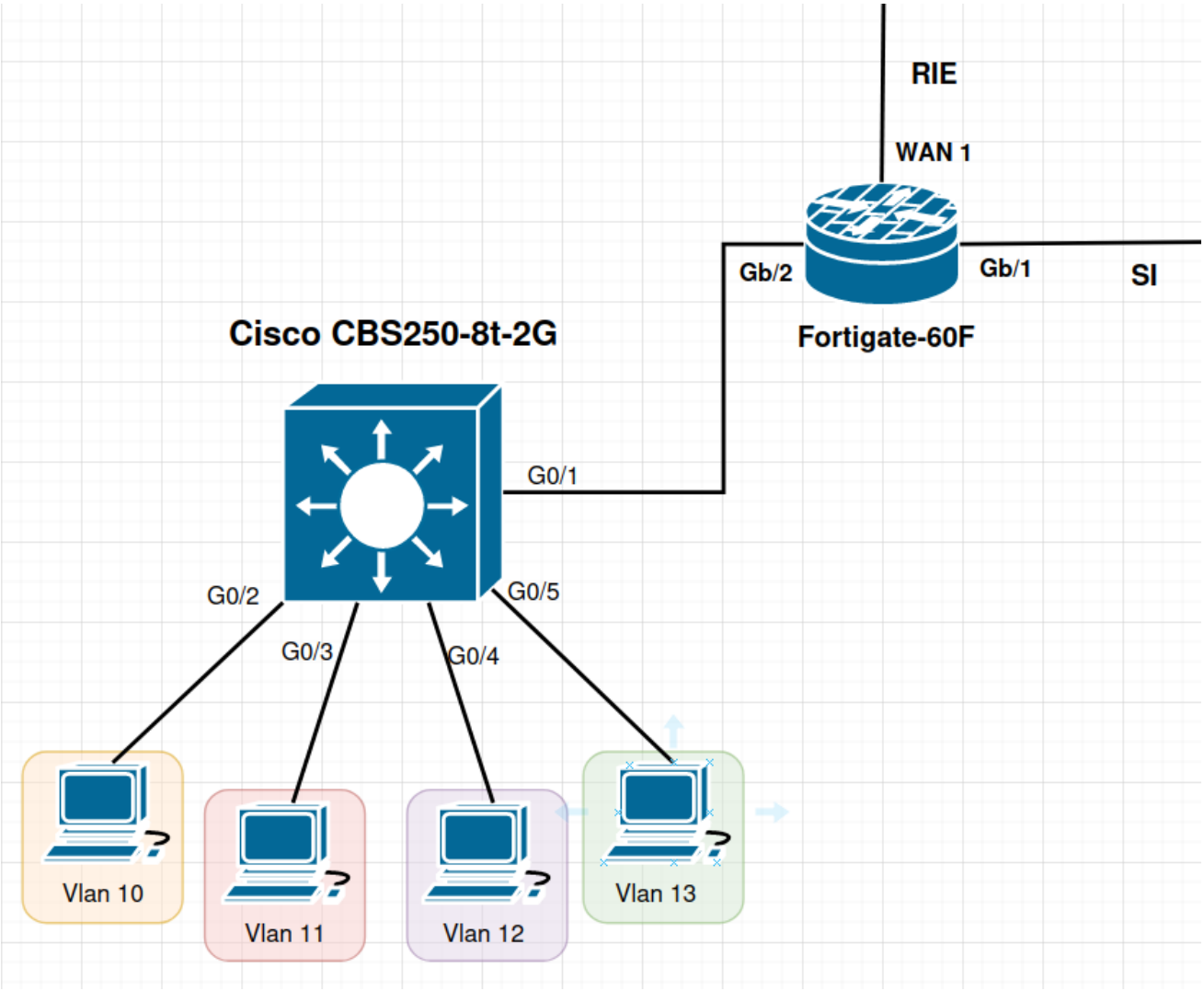


Figure 166: Shema de la partie réseau d'audit

6.2.9 Configuration du Switch

En attendant la réception de l'équipement, les exigences et la configuration prévue pour le **switch Cisco CB250-8T-2G** seront détaillées et enregistrées dans un fichier texte. Ce document sert à préparer et à structurer les paramètres de configuration essentiels tels que les **VLANs**, la **sécurité des ports** (mesures pour limiter l'accès aux ports réseau aux seules adresses MAC autorisées) et la **segmentation réseau**, garantissant une mise en œuvre rapide et efficace dès la disponibilité du switch. Le texte sera copié-collé une fois sur l'interface d'administration du switch.

```
Fichier    Modifier    Affichage

Switch(config)#interface vlan Z
Switch(config-if)#ip address x.x.x.x X.X.X.X
Switch(config-if)#no shut

Switch(config)#interface fastEthernet X/Y
Switch(config-if)#switchport
Switch(config-if)#switchport access vlan Z
Switch(config-if)#no shut
```

Figure 177: Exemple de Configuration depuis un fichier texte

Le fichier texte servira de **script de configuration (fichier texte)** lors de l'installation de l'infrastructure dans les différents sites de **D@TA-i** (Dép@rtement des Technologies Appliquées à l'Investigation). L'utilisation de logiciels tels que **mRemoteNG** (outil de gestion de connexions réseau permettant de centraliser et gérer les configurations des équipements réseau via différents protocoles) peut être envisagée pour centraliser la gestion des équipements réseau ainsi que leur configuration.

mRemoteNG
Multi-Remote Next Generation

Figure 188: Logiciel mRemoteNG

6.2.10 Poste Administrateur

Le poste d'administrateur constitue un élément crucial de l'**architecture réseau**, étant donné qu'il est le seul à avoir accès aux **firewalls**. Différents outils et logiciels, que je détaillerai dans les sections suivantes, seront nécessaires pour assurer cette gestion efficace.

6.2.11 Configuration du poste

Tout d'abord, le **système d'exploitation (OS, logiciel** de base qui permet à un ordinateur de fonctionner et de gérer les ressources matérielles et logicielles) utilisé sera **Windows 10 Édition Professionnelle** (version du système d'exploitation Windows 10 conçue pour les professionnels et les entreprises). En complément, **WSL 2** (Windows Subsystem for Linux version 2, fonctionnalité de Windows permettant d'exécuter des distributions Linux directement sur Windows) sera installé avec **Debian 12 (Bookworm) Édition Desktop** (distribution Linux connue pour sa stabilité et sa sécurité, version 12 codée "Bookworm" avec une interface graphique de bureau).

Figure 199: Illustration de Windows Subsystem for Linux

Figure 200: Logo de Debian 12 "Bookworm"

Pour mettre en place le **poste administrateur**, étant donné que mon poste fonctionne sur **Ubuntu** (distribution Linux populaire pour les environnements de bureau et serveur), j'ai mis en place une **MV (Machine Virtuelle)** (environnement simulé sur un ordinateur physique permettant d'exécuter un autre système d'exploitation en parallèle) **Windows 10 Pro** (version professionnelle du système d'exploitation Windows 10).

Figure 211: Logo de VIrtual Box

Figure 222: Logo de Windows 10 Pro

6.2.12 Sécurité du poste Admin

Pour garantir la **sécurité** (protection des systèmes informatiques contre les accès non autorisés et les menaces) du poste d'administrateur sous **Windows** (système d'exploitation développé par Microsoft), plusieurs mesures stratégiques sont mises en place :

- **Chiffrement du disque avec BitLocker en mode TPM + PIN** : Pour protéger les données stockées sur le disque dur, le chiffrement BitLocker est utilisé. Ce système utilise le module de plateforme sécurisée (TPM) pour stocker les clés de chiffrement de manière sécurisée, tout en nécessitant un PIN lors du démarrage. Cette combinaison assure que même en cas de vol physique du disque dur, les données restent inaccessibles sans les authentifications requises.

- **Utilisation de l'UAC (User Account Control)** : Le Contrôle de compte d'utilisateur est configuré pour demander le mot de passe administrateur pour toute action susceptible de modifier la configuration du système ou d'installer un logiciel. Cela minimise les risques d'actions malveillantes ou non autorisées, en s'assurant que seules les modifications approuvées par un administrateur puissent être effectuées.

- **Gestion des comptes** : Chaque administrateur de l'infrastructure dispose d'un compte utilisateur individuel pour les tâches quotidiennes et un compte administratif nominatif pour les opérations nécessitant des privilèges élevés. Cette séparation des privilèges aide à limiter les risques associés à l'utilisation excessive des droits administratifs.

- **Politiques de mot de passe** : Les mots de passe pour tous les comptes administratifs doivent comporter au moins 15 caractères aléatoires, incluant des majuscules, des minuscules, des chiffres et des symboles. Cette politique de mot de passe complexe vise à résister aux attaques de force brute et à d'autres formes de tentatives d'intrusion.

Ces mesures, combinées, fournissent une défense qui protège le poste administrateur contre diverses menaces, assurant ainsi l'intégrité et la sécurité de l'ensemble de l'infrastructure réseau.

6.2.13 Poste d'audit

Pour assurer une surveillance et un contrôle efficaces des réseaux au sein de l'entreprise, des postes d'audit spécifiques sont déployés. Ces postes sont essentiels pour réaliser des tests d'intrusion sur le Réseau Interministériel de l'État (RIE) et pour évaluer la robustesse de la sécurité en place. Pour maintenir la sécurité et l'intégrité du réseau tout en permettant ces activités d'audit, des règles strictes de pare-feu et des contrôles de flux sont mis en œuvre pour limiter les actions des postes d'audit à celles strictement nécessaires.

6.2.14 Configuration du poste

Les postes d'audit sont équipés de Windows 10, sur lesquels sont installés des outils de rédaction Microsoft, ainsi que la suite Office pour faciliter la documentation et la gestion des rapports d'audit. Chaque poste comprend également une machine virtuelle sous Kali Linux, un système d'exploitation largement utilisé pour les tests de pénétration et l'audit de sécurité, offrant ainsi aux auditeurs une gamme complète d'outils spécialisés pour leur travail.

Cette configuration spécifique permet aux auditeurs de disposer des ressources nécessaires pour effectuer des analyses approfondies tout en restant dans un environnement contrôlé et sécurisé. Les restrictions imposées par les règles de pare-feu et le contrôle des flux assurent que toutes les activités des postes d'audit sont minutieusement surveillées et restent conformes aux politiques de sécurité de l'entreprise.

6.2.15 Source NAT des PC d'audits

Pour optimiser la surveillance et l'identification des postes d'audit sur le Réseau Interministériel de l'État (RIE), une configuration de source NAT (Network Address Translation) sera mise en place. Cette configuration utilisera un pool d'adresses IP, attribuant une adresse IP unique à chaque poste d'audit. Ce dispositif permettra non seulement de mieux identifier chaque poste lorsqu'il interagit avec le RIE, mais également de maintenir une traçabilité précise des actions menées durant les tests d'intrusion.

L'utilisation de la source NAT avec un pool d'adresses IP distinctes pour chaque poste d'audit aide à renforcer les mesures de sécurité en permettant un contrôle et une gestion plus rigoureux des accès au réseau.

Cela garantit que toutes les activités entreprises par les postes d'audit sont clairement identifiées et associées à des adresses IP spécifiques, facilitant ainsi la détection rapide et efficace de toute anomalie ou comportement suspect sur le réseau.

6.2.16 Logiciel

Voici un récapitulatif et listage des logiciels utilisés pour les postes d'audit et d'administration, chacun étant spécifiquement sélectionné pour répondre aux exigences de sécurité et de fonctionnalité requises pour leurs rôles respectifs :

6.2.17 Logiciels pour le poste d'administration :

- **TheGreenBow VPN Client** : Ce logiciel client VPN est utilisé pour établir des connexions sécurisées et cryptées, permettant aux administrateurs d'accéder à distance aux ressources réseau critiques tout en maintenant une sécurité optimale.
- **Wireshark** : Utilisé pour l'analyse de réseau, Wireshark permet aux administrateurs de surveiller le trafic réseau en temps réel et de décomposer ces données pour identifier et résoudre les problèmes de réseau, ainsi que pour auditer les mesures de sécurité en place.

6.2.18 Logiciels pour le poste d'audit :

- **Kali Linux (VM)** : Chaque poste d'audit est équipé d'une machine virtuelle fonctionnant sous Kali Linux, une distribution Linux spécialisée dans les tests de pénétration et les audits de sécurité. Elle comprend une suite complète d'outils de sécurité pour l'analyse de vulnérabilités, les tests d'intrusion, et bien plus.
- **Microsoft Office** : Utilisé pour la documentation et la gestion des rapports d'audit, Office 365 offre aux auditeurs une plateforme flexible et intégrée pour créer, partager et collaborer sur les documents d'audit.

Ces logiciels jouent un rôle crucial dans la réalisation des activités quotidiennes des équipes d'audit et d'administration, en fournissant les outils nécessaires pour une gestion sécurisée et efficace de l'infrastructure réseau.

6.3 Shéma de l’architecture

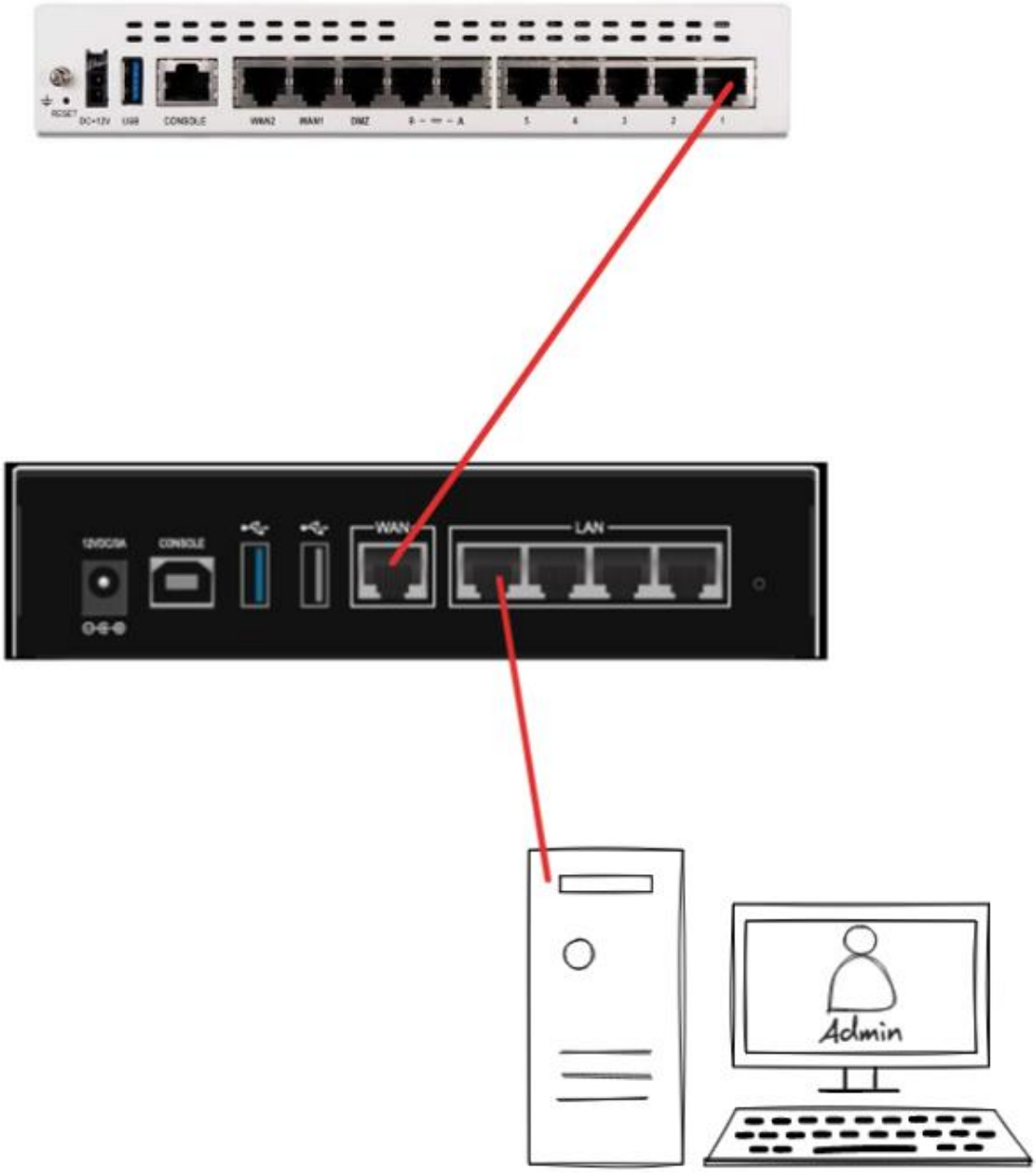


Figure 23: schéma de l’architecture coté réseau administrateur

6.4 Difficultés rencontrées

Plusieurs contraintes ont ralenti l'avancement du projet, affectant divers aspects de son développement et de sa mise en œuvre :

- **Réception des équipements** : Le retard dans la livraison des équipements nécessaires, tels que le switch Cisco, a retardé les phases initiales du projet, empêchant la réalisation des tests prévus dans les délais.

- **Configuration du VPN** : La configuration du VPN a présenté des défis significatifs, particulièrement avec l'utilisation du Fortinet comme firewall interne. Malgré plusieurs tentatives, l'établissement d'une connexion VPN stable sur ce dispositif a été infructueux, ce qui a nécessité une réévaluation des solutions techniques envisageables. De plus l'utilisation de certificats a été pour moi une difficulté notamment sur le Stormshield.

- **Problèmes de version et de modèle avec le Stormshield** : Le modèle de Stormshield utilisé, le SN160, a présenté des limitations en termes de configuration des interfaces physiques. Seuls un port WAN et un port IN pouvaient être configurés, les trois autres ports étant non configurables et attribués au bridge du firewall. De plus, des problèmes liés à la version du firmware (logiciel permanant stocker dans la mémoire non volatile ROM) ont également compliqué la mise en œuvre des fonctionnalités souhaitées.

- **Problème de logs sur le Stormshield SN160** : La nécessité d'une carte SD pour le stockage externe des logs a été un autre obstacle, limitant la capacité de surveillance et d'analyse des événements réseau.

- **Limitations du poste physique** : Les restrictions liées au poste physique ont limité la mise en œuvre à un poste administrateur uniquement, avec la configuration d'un poste d'audit sous Kali Linux achevée mais en attente de déploiement intégral.

- **Installation de l'infrastructure sur le switch du RIE** : Un imprévu externe, indépendant de notre contrôle, a entravé l'installation de l'infrastructure sur le switch du RIE au moment des tests, ce qui a empêché la réalisation des tests en conditions réelles.

Ces défis ont exigé des ajustements constants et une gestion flexible du projet pour s'adapter aux contraintes techniques et logistiques rencontrées.

6.5 Solution apportée

Voici une liste de solutions correspondant aux problèmes rencontrés :

- **Réception des équipements** : pré configuration du Switch via un fichier texte, recherche de solutions manquantes ou plus adaptés, documentation technique en amont.

- **Configuration du VPN** : utilisation du pare-feu Stromshield SN160 comme pare-feu interne permettant d'établir avec plus de faciliter le VPN IPsec pour le réseau Administrateur. Une solution temporaire a été de mettre en place une PSK (Pre-Shared Key ou clef partégé), a terme cela ne sera pas une solution à utiliser.

- **Problèmes de version et de modèle avec le Stormshield** : Le faite d'utiliser le Stormshield comme pare-feu interne permet d'éliminer la contrainte des trois ports nécessaires pour son utilisation initiale (pare-feu externe reliant 3 réseau différents), une mise à jour a dû être effectuer car le firmware disponible était une version ancienne et il était donc plus adaptés d'utiliser une version récente.

- **Problème de logs sur le Stormshield SN160** : l'utilisation d'un espace de stockage externe ou d'un server de log et obligatoire sur ce modèle de pare-feu, la solution prise en compte a été l'utilisation d'une carte SD.

- **Limitations du poste physique** : le poste administrateur à don été mis en priorité et donc la VM admin a été largement utilisé.

6.6 Conclusion de la mission

J'ai pu approfondir et partager des connaissances sur des aspects clés de la mise en place d'une infrastructure de sécurité informatique. Les échanges ont couvert des sujets variés, de la configuration des firewalls et des VPN à la gestion des logs, ainsi que l'optimisation des postes d'audit et administratifs. Cette interaction a été enrichissante pour comprendre les défis techniques et logistiques que comportent l'installation et la configuration de réseaux sécurisés dans un environnement interministériel. L'expérience que j'ai pu avoir notamment dans la gestion d'un projet et l'adaptabilité dans un environnement de travail me motive et va m'aider lors de mon alternance pour la 3-ème année de BUT.

7 Conclusion

En conclusion, la mise en place de cette infrastructure dédiée aux tests d'intrusion m'a permis de relever plusieurs défis techniques tout en posant une base solide pour des évaluations de sécurité approfondies. Les difficultés rencontrées, notamment la configuration des VPNs et l'intégration des équipements Fortinet et Stormshield, ont été formatrices et m'ont permis de mieux comprendre les interactions complexes entre ces systèmes.

Ces expériences m'ont aidé à surmonter les limitations matérielles et à optimiser la configuration de l'ensemble de l'architecture. L'infrastructure que j'ai développée est désormais fonctionnelle, adaptable et prête à soutenir des tests d'intrusion avancés. Elle me permettra de détecter et corriger efficacement les vulnérabilités, assurant ainsi la protection des environnements critiques tout en me préparant à de futures améliorations.

8 Glossaire

BUT, Bachelor Universitaire de Technologie

DNPJ, Direction Nationale de la Police Judiciaire

Pôle SSI, ensemble ou une structure dédiée à la Sécurité des Systèmes d'Information (SSI)

D@TA-i, Dép@rtement des Technologies Appliquées à l'Investigation

Section Expertise, déploiement d'outils spécifiques SSI, valide les logiciels, audit et test d'intrusion, innovation.

DIPN, (Directions Interdépartementales de la Police Nationale

DIPN, (Directions Interdépartementales de la Police Nationale

RIE, Réseau Interministérielle de l'Etat

UTM, (Unified Threat Management

Gateway, Paserelle permet de connecter deux réseaux.

Firewall (pare-feu), dispositif de sécurité réseau et filtre le trafic entrant et sortant

IPsec, Internet Protocol Security

IKE, (Internet Key Exchange version 1) Protocole pour échanger des clés de sécurité sur Internet, utilisé dans les VPN pour établir des connexions sécurisées.

IKEv2, (Internet Key Exchange version 2) Version améliorée d'IKE, offrant une configuration plus simple et une meilleure sécurité pour les connexions VPN.

SA, (Security Association) : Ensemble de paramètres de sécurité et de clés utilisés pour établir une connexion sécurisée entre deux parties.

ESP, (Encapsulating Security Payload) : Protocole de sécurité qui chiffre les données et les enveloppe dans les communications réseau pour assurer leur confidentialité.

PSK, PSK (Pre-Shared Key) : Clé secrète partagée utilisée pour authentifier et établir une connexion sécurisée entre deux parties.

Fortinet et Stormshield, Entreprises spécialisée dans la sécurité réseau, connue pour ses pare-feu et solutions de sécurité.

Stormshield SN 160, Modèle de pare-feu de la marque Stormshield, conçu pour protéger les réseaux des menaces externes.

NAT (Network Adress Translation), Technique qui modifie les adresses IP des paquets réseau pour permettre à plusieurs appareils de partager une seule adresse IP publique.

IP Pool, Gamme d'adresses IP disponibles à attribuer dynamiquement aux appareils sur un réseau.

VLAN, (Virtual Local Area Network) : Réseau local virtuel qui regroupe des appareils en fonction de leur fonction ou de leur emplacement, indépendamment de leur connexion physique.

802.1x, Protocole de contrôle d'accès réseau qui fournit une authentification des utilisateurs ou des appareils avant de leur permettre d'accéder au réseau.

SSHv2 (Secure Shell version 2), (Secure Shell version 2) : Protocole de réseau sécurisé pour se connecter à distance à des systèmes informatiques et les administrer de manière sécurisée.
TPM, (Trusted Platform Module) : Composant matériel sécurisé qui stocke des clés de cryptage et assure l'intégrité du système en vérifiant le démarrage et l'état du système.
BitLocker, Fonction de chiffrement de disque intégrée à Windows qui protège les données en chiffrant l'ensemble du disque dur.

9 Bibliographie