Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Stage de fin d'étude chez MIOS

Clément LANDIER

MIOS

Responsable entreprise : Guillaume GILABERT

Responsable académique : Eric SOCCORSI

2021

Table des matières

1 Introduction

Dans le cadre de mon DUT Réseaux et Télécoms, j'ai eu l'occasion d'effectuer un stage en entreprise d'une durée de 10 semaines, me permettant ainsi de mettre en application et de perfectionner les diverses compétences que j'ai acquis tout au long de mon parcours.

J'ai effectué mon stage chez Mios, dans le service IT qui conçoit des infrastructures système et réseau pour le compte d'autres entreprises.

Mon projet de stage avait pour but d'établir une liaison VPN (Virtual Private Network) entre les sites de Valence et d'Aix-en-Provence, permettant ainsi d'interconnecter le réseau des 2 sites, de plus j'avais pour mission de changer le plan d'adressage du site d'Aix afin de le rendre cohérent avec celui utilisé sur les autres sites de l'entreprise et de permettre la mise en place de VLANs (Virtual Local Area Network).

Ainsi nous allons d'abord détailler l'activité de l'entreprise, ensuite nous verrons l'étude que j'ai réalisé sur l'existant afin de faciliter le changement du plan d'adressage réseau et la mise en place des VLANs et enfin nous parlerons du déploiement du VPN.

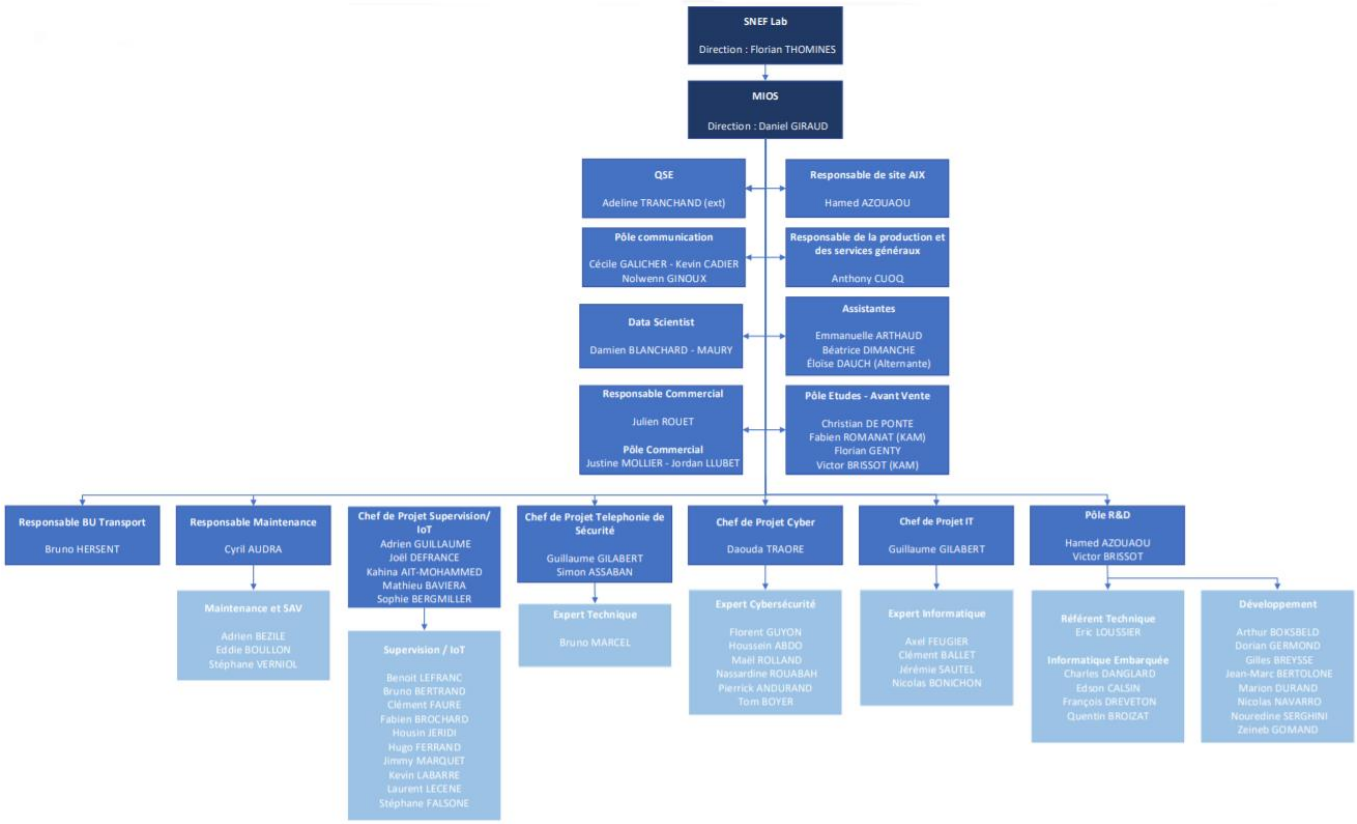
2 Présentation de l'entreprise

2.1 Histoire de l'entreprise

Créé en 1987 à Aix-en-Provence, MIOS est spécialisé dans le développement de solutions de téléphonie et de sonorisation de sécurité. MIOS est actuellement l'un des principaux fournisseurs de solutions de réseaux d'appels d'urgence pour les autoroutes et tunnels français. Première entreprise à développer une solution de gestion centralisée des appels et des équipements, MIOS a progressivement élargi son activité dans le domaine de la supervision puis dans le développement d'objets connectés multi protocoles.

En 2019, MIOS rejoint le Groupe SNEF en fusionnant avec le pôle d'expertise IT & IoT de Valence. Partageant la même approche, les deux entités combinent leurs compétences pour proposer à leurs clients des solutions dont ils ont la maîtrise. Parallèlement, MIOS a développé une expertise cyber sécurité afin de répondre aux enjeux et aux exigences métiers de ses clients. Rattaché à la Business Unit SNEF Lab. dédiée à l'innovation, MIOS accompagne la transformation digitale de ses clients en toute sécurité.

2.2 Organigramme



3 Présentation du sujet de stage

3.1 Énoncé du projet

Le but de mon stage était principalement la mise en place d'un VPN entre deux sites de l'entreprise, le premier sur Aix et le deuxième sur valence, le VPN permettra d'interconnecter les réseaux et ainsi d'accéder aux différentes ressources présentes sur les réseaux (Serveur de Stockage, Intranet,…) de manière sécurisée. La mise en place du VPN nécessitant de changer le routeur c'est aussi l'occasion de faire une refonte complète du réseau, notamment le remplacement des commutateurs présents étant assez vieux et peu rapides, la mise en place de VLANs permettant de réduire le domaine de broadcast et d'isoler les différents trafics présents sur le réseau tel que le trafic wifi ou des serveurs clients et ainsi d'augmenter la sécurité du réseau.

3.2 Problématique

Pour ce faire un changement du plan d'adressage est nécessaire, en effet celui utilisé en actuellement (192.168.0.0/24) permet seulement 254 adresses IP, ce qui en plus d'être très faible ne permet pas la mise en place des VLANs qui sont des sous réseaux.

Il est donc nécessaire de changer le plan d'adressage du réseau.

Dans ce but la première partie de mon stage a consisté à établir un plan du réseau et des différents équipements présents, et de réaliser un nouveau plan d'adressage prenant en compte les VLANs.

Je devrais aussi me familiariser avec le routeur/firewall Stormshield et apprendre à le configurer.

4 Travail réalisé

4.1 Étude et cartographie du réseau existant

Ma première mission consistait à établir un plan du réseau actuel de l'entreprise, le plan permettra de savoir précisément quels équipements sont connectés au réseau, ou ils se trouvent, et comment sont ils connectés, il permettra ainsi de faciliter le changement du plan d'adressage, en effet on pourra désormais savoir où se trouve les équipements dont la configuration doit être changée, de plus pour la mise en place des VLANs nous devons savoir quels équipements sont connectés sur quels ports des commutateurs.

Le plan du réseau a été réalisé grâce à l'outil Microsoft Visio, qui permet de faire différents types de diagrammes, notamment des diagrammes réseau, je me suis ainsi approprié cet outil pour réaliser mes diagrammes, j'ai ainsi appris à utiliser les différentes fonctionnalités du logiciel, notamment les stencils qui permettent d'importer des objets tels que des modèles de serveurs de constructeurs, ce qui permet de faire un diagramme plus détaillé et simple à lire.

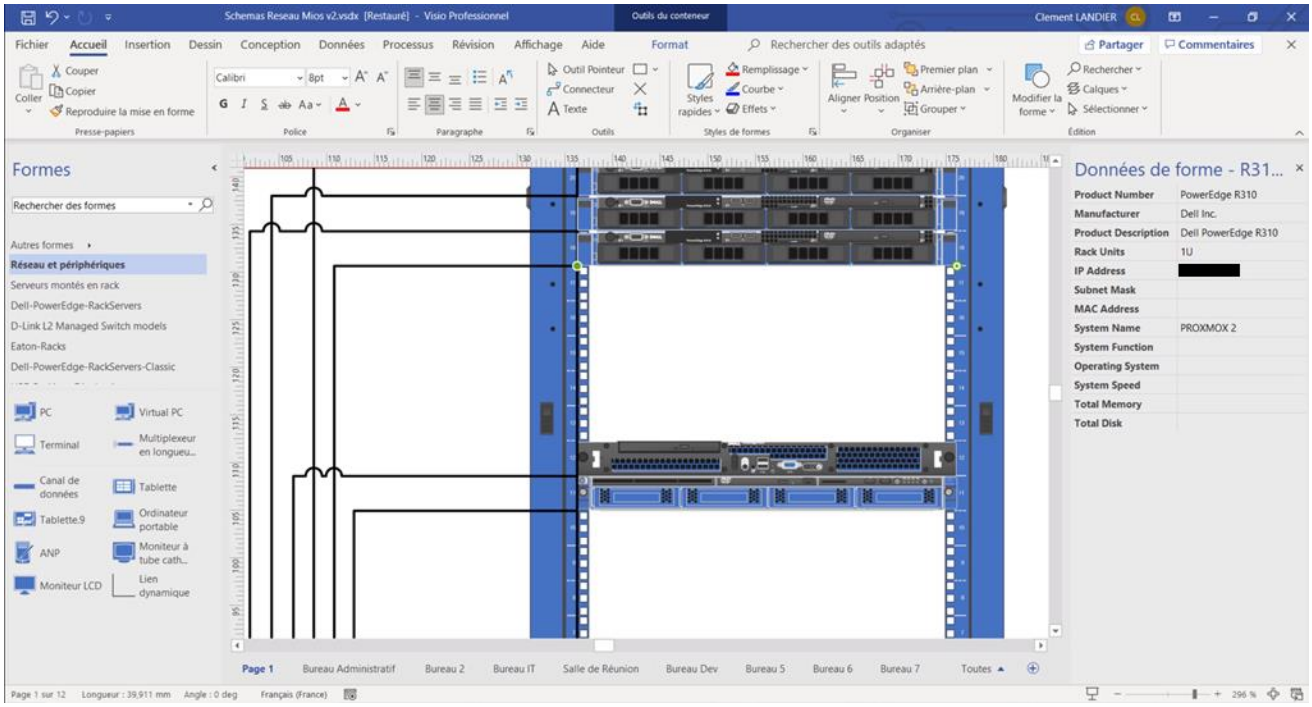


Figure 1 Outil Visio

Dans la réalisation de mon plan, j'ai été amené à faire un inventaire des différentes prises Ethernets présentes dans les locaux de l'entreprise, ainsi que de celles auquel les commutateurs sont connectés, cela permettra de mettre en place des VLANs sur les différents ports des commutateurs.

Port Switch	Label / conexion	Bureau	Equipement
Port 1	L048-04I	Poteau 3 Prise 3 Bureau Dev	Vide
Port 2	Alarme	Salle serveurs	Alarme
Port 3	L006/02T	Couloir	Imprimante
Port 4	L012-02I	Poteau 1 Prise 2 Bureau IT	PC Portable + TEL
Port 5	L012-01I	Poteau 1 Prise 1 Bureau IT	PC Portable
Port 6	L052/01T	Poteau 1 Prise 1 Bureau 5	Téléphone
Port 7	L056/01T	Poteau 2 Prise 2 Bureau 9	Vide
Port 8	L053/03T	Poteau 1 Prise 2 Bureau 6	Vide
Port 9	L056/03I	Poteau 3 Prise 1 Bureau 9	Mini Switch
Port 10	L008/01T	Poteau 2 Prise 2 Bureau Administratif	Vide
Port 11	L009/01T	Poteau 2 Prise 1 Bureau Administratif	Imprimante
Port 12	L010/01T	Poteau 2 Prise 2 Bureau 2	Vide
Port 13	Ls/01T		
Port 14	L056/03T	Poteau 2 Prise 4 Salle de réunion 2	Mini Switch
Port 15	L048-01I	Poteau 2 Prise 2 Bureau Dev	Mini Switch
Port 16	L052/02I	Poteau 2 Prise 2 Bureau 6	PC Fixe
Port 17	L011/02I	Poteau 3 Prise 2 Bureau IT	Vide
Port 18	L056/04T	Poteau 1 Prise 2 Salle de réunion 2	Borne VOIP Gigaset
Port 19	LO12-03T	Poteau 2 Prise 1 Salle de réunion	Mini Switch
Port 20	L050/04I	Poteau 5 Prise 3 Bureau Dev	Mini Switch
Port 21	L063/01T	Labo Integration	
Port 22	L063/02T		
Port 23	Switch 92	Salle serveurs	Switch 92
Port 24	LO51/01T	Salle serveurs	Switch4
SFP 25			
SFP 26			
SFP 27			
SFP 28			

Figure 2 Ports d'un des commutateurs

L'étude préliminaire du réseau a ainsi permis de mettre en évidence les équipements présents, les habitudes des utilisateurs du réseau et les sous réseaux présents, en effet la société Mios a différents clients dont les serveurs sont parfois présents temporairement dans les locaux de l'entreprise, d'autres clients ont quand a eux des serveurs de backup présents sur le réseau de l'entreprise, chacun d'entre eux est présent dans un sous réseau différent, il y a ainsi 290 sous réseaux que je devrais éviter lorsque je ferais mon plan d'adressage.

De plus mon étude a permis de se rendre compte qu'il y a par exemple 2 lignes internet : une ADSL et l'autre Fibre, 2 lignes téléphoniques, plusieurs serveurs de virtualisation avec différents services utilisés par les employés de l'entreprise telle qu'un serveur d'intégration continue utilisé par l'équipe de développeurs, l'étude a aussi permis de mieux comprendre comment fonctionne le réseau de téléphonie de l'entreprise.

J'ai aussi dû relever la configuration du routeur existant et notamment les différentes redirections de ports, qui permettent à du trafic venant de l'internet d'accéder à certains hôtes du réseau, et j'ai aussi testé si elle était réellement utile afin de supprimer celles qui n'étaient plus utilisées.

La suite de mon étude consister aussi a proposé un nouveau plan réseau prenant en compte les VLANs et n'empiétant pas sur les sous réseaux présents sur le site d'Aix ou les autres sites de l'entreprise.

Aix : 10.99.0.0/16

VLAN	ID	Plage d'adresses
Default	1	10.99.0.0/24
Vlan Sécurité	97	10.99.97.0/24
Vlan WiFi	98	10.99.98.0/24
Vlan VOIP	99	10.99.99.0/24
Vlan Serveurs	100	10.99.100.0/24
Vlan Administratif	101	10.99.101.0/24
Vlan IT	102	10.99.102.0/24
Vlan Réunion	103	10.99.103.0/24
Vlan Dev	104	10.99.104.0/24
VLAN IOT	105	10.99.105.0/24
Vlan Labo	106	10.99.106.0/24

Vlan 98 — 10.99.98.0/24

IP	Equipement	Details
10.99.98.1	Routeur	
10.99.98.2	Borne Wifi mioswifi1	
10.99.98.3	Borne Wifi mioswifi2	
10.99.98.4	Imprimante	
10.99.98.150 - 10.99.98.250	**DHCP**	

Figure 3 Propositions de plan d'adressage

À la fin de mon étude une réunion ayant pour but de discuter de l'état du réseau actuel ainsi que du déroulement des événements à venir a eu lieu, à cette occasion j'ai dû réaliser un PowerPoint présentant les résultats de mon étude, mes suggestions sur la démarche à suivre et une estimation du temps que prendrait la transition du plan d'adressage.

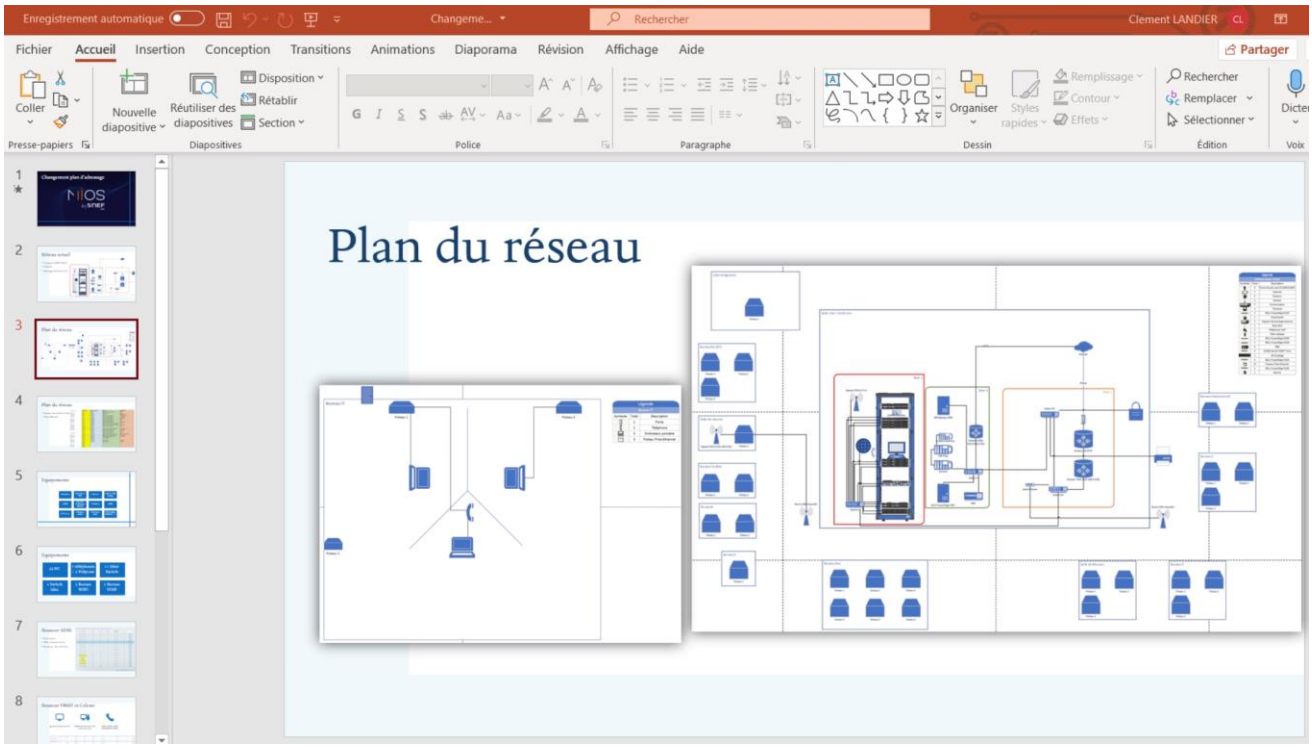


Figure 4 PowerPoint récapitulatif de l'étude réaliser

Suite a ma présentation il a été décidé que la mise en place du routeur/firewall Stormshield était plus importante que le changement d'adressage IP qui pourra être réalisé plus tard, de ce fait je me suis concentré sur la mise en place du Stormshield et le remplacement des commutateurs.

4.2 Installation et configuration basique du routeur

Le routeur/firewall Stormshield a pour but de remplacer le routeur actuel et d'ajouter de nouvelles fonctionnalités sur le réseau, notamment un VPN.

Avant de le déployer, j'ai d'abord effectué un ban de test sur mon bureau afin de me familiariser avec celui-ci et de ne pas avoir à le configurer le jour où il sera mis en service, évitant ainsi de couper l'accès internet pendant trop longtemps.

Après m'être connecté sur le routeur j'ai configuré les paramètres basiques tels que le compte administrateur et les adresses IP sur les différentes interfaces, j'ai ensuite ajouté les différentes routes présentes sur l'ancien routeur, et enfin j'ai configuré le serveur DHCP qui attribuera des adresses IP aux hôtes se connectant au réseau de l'entreprise.

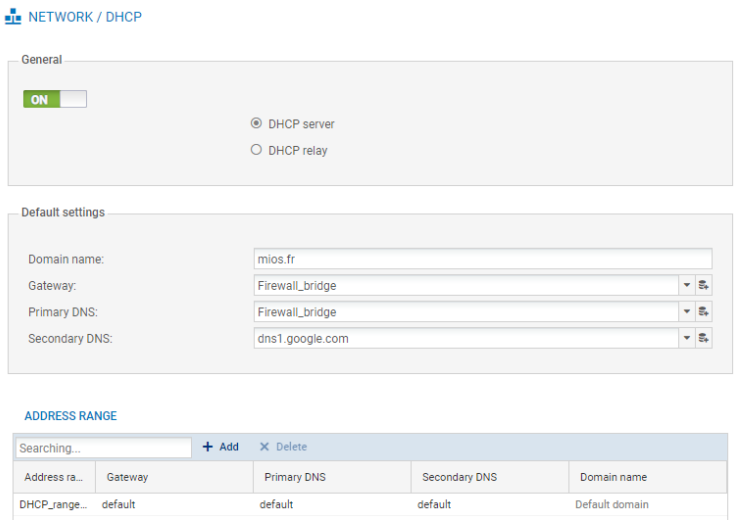


Figure 5 Configuration du DHCP

J'ai aussi configuré un serveur de cache DNS, le but d'un serveur DNS (Domain Name Server) est, à partir d'un nom de domaine, de retourner l'adresse IP correspondante, pour ce faire il cherche dans sa base de données qui comprend les correspondances nom de domaine vers adresse IP.

La première fois qu'un utilisateur veut accéder à un site internet, il doit d'abord récupérer son adresse IP avant de se connecter ce qui rajoute du délai au chargement de la page web, pour éviter cela le routeur propose de mettre en cache les requêtes effectuées par les hôtes du réseau ainsi si un hôte à déjà effectuer cette demande le routeur répondra à la place du serveur DNS, ce qui sera plus rapide, car il est situé sur le réseau proche des hôtes.

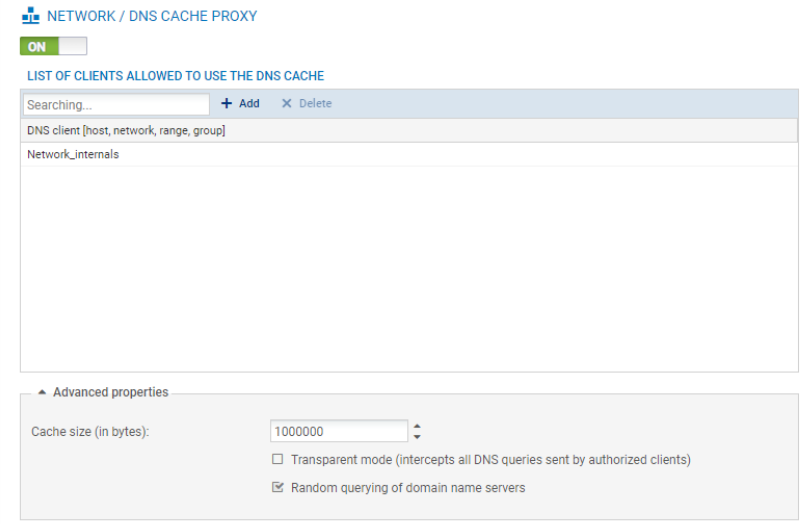


Figure 6 Configuration du Cache DNS

Une autre configuration importante que j'ai effectué sur le routeur est la configuration des logs, la mémoire interne du Stormshield étant limitée celui-ci stock les logs sur une carte SD externe que j'ai donc installé.

Après avoir configuré les paramètres vus précédemment ainsi que ceux que nous verrons dans les chapitres suivants j'ai procédé à l'installation du routeur dans la salle des serveurs, pour éviter de déranger les employés de l'entreprise j'ai effectué cette tâche durant la pause déjeuner et après avoir prévenu de l'interruption, du fait que j'avais déjà préparé et testé ma configuration le remplacement n'a duré que quelques minutes.

Figure 7 le Stormshield installer dans la baie serveur

4.3 Configuration du NAT et de la redirection de port sur le routeur

Le réseau de l'entreprise ayant plus d'adresse IP privée que d'adresse IP externe il est impossible d'assigner une adresse publique a chaque hôte du réseau, afin de résoudre ce problème on utilise une technique appeler NAT (Network Adress Translation) qui va permettre aux hôtes du réseau d'accéder à l'internet sans avoir une adresse IP publique dédiée.

Comme son nom l'indique, le NAT « traduit » des adresses, c'est-à-dire qu'il va remplacer une adresse IP privée par exemple en adresse IP publique. Dans notre cas c'est la déclinaison PAT (Port Adress Translation) qui nous intéresse celle-ci permet d'utiliser une seule adresse IP publique pour traduire plusieurs adresses IP privées pour cela le routeur va utiliser la technique de la surcharge de port, qui va ajouter comme fonctionnalité la possibilité de changer le port source, ce qui permet à plusieurs hôtes internes d'utiliser un même port source qui va ensuite être modifié par le routeur.

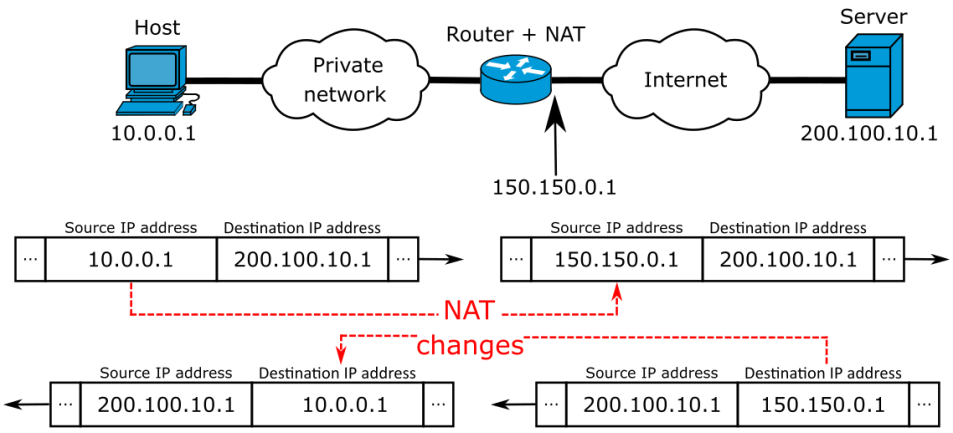


Figure 8 Schéma explicatif NAT

Sur le routeur Stormshield la configuration du NAT/PAT ce fait par l'ajout d'une simple règle qui dicte que tout le trafic à destination de l'internet verra son adresse IP source remplacée par celle du routeur et son port source par un port éphémère aléatoire il enregistrera ensuite cette correspondance port/hôte dans une table spécifique.

Inversement quand le routeur recevra un paquet sur l'un des ports éphémères il changera l'adresse IP de destination pour la remplacer par celle de l'hôte qui avait initié le trafic si celui-ci est présent dans la table, sinon le paquet seras détruit, car le routeur ne peut pas déterminer la destination réelle du paquet.

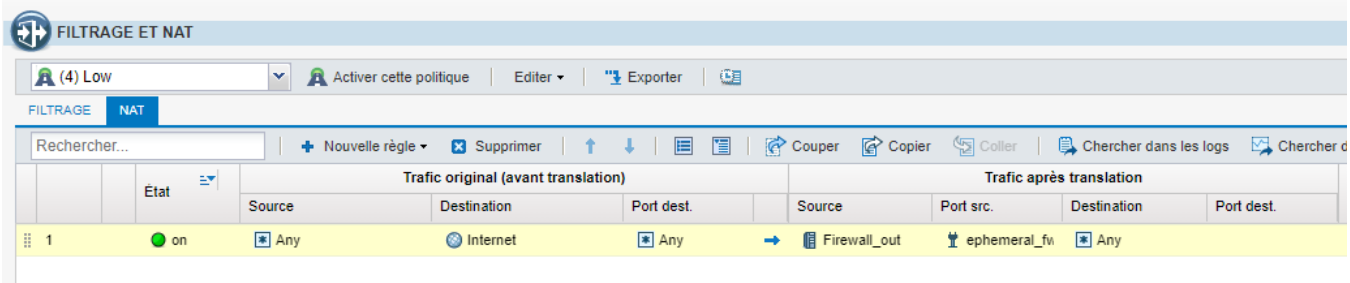


Figure 9 règle NAT sur le routeur

Comme nous venons de le voir, le NAT a pour avantage de nécessiter qu'une seule adresse IP publique pour permettre aux hôtes du réseau d'accéder à l'internet, il a aussi pour avantage d'augmenter la sécurité du réseau, car un ordinateur distant peut difficilement connaître la topologie du réseau.

Cependant, il a aussi des désavantages, certains protocoles nécessitant l'utilisation d'un port particulier auront du mal où ne pourront simplement pas fonctionner. De plus, les hôtes du réseau peuvent initier du trafic vers l'internet, mais l'inverse n'est pas possible.

Pour que des hôtes internet puissent initier du trafic sur un port donner nous devons donc configurer de la redirection de port, celle-ci permet d'instruire au routeur qu'un port externe spécifique devra correspondre à un port et un hôte interne.

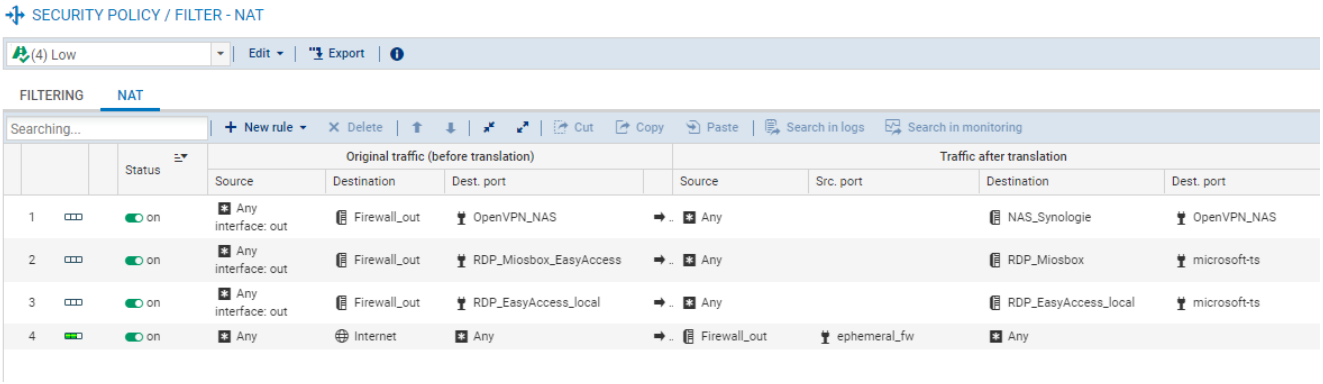


Figure 10 Règles NAT finale

Comme nous pouvons le voir sur la figure 7 le trafic provenant de l'interface externe ayant pour destination l'adresse IP externe du firewall et le port X (ici OpenVPN_NAS par exemple correspond à un port numéroter) verra son adresse IP de destination changer pour celle d'un hôte interne, de même son port peut être changé si besoin.

En conclusion, le NAT nous a permis de donner un accès internet à plusieurs postes sans qu'ils aient besoin d'avoir une adresse IP publique assignée, il a aussi permis d'élever la sécurité du réseau et n'a pas empêché l'accès depuis l'internet aux services qui doivent l'être.

4.4 Mise en place VPN IPSEC

La mise en place d'un VPN entre les sites d'Aix-en-Provence et de Valence et la mission principale du stage, le VPN permettra une interconnexion sécurisée entre les deux réseaux, il sera ainsi possible d'accéder aux ressources distantes sans les exposer sur l'internet, les employés pourront ainsi accéder aux NAS (Network Attached Storage) et autres serveurs présents sur le réseau distant.

IPSEC (Internet Protocol Security) est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP, il opère sur la couche 3 (Réseau) et remplace donc le protocole IP standard, le fait d'être à une couche aussi basse lui permet d'encrypter le trafic des couches supérieures de manière transparente pour les applications. Ainsi grâce à IPSEC le trafic ne pourra ni être lu, ni être modifié ce qui en garantie donc l'entière sécurité.

Afin que le VPN puisse fonctionner normalement il est essentiel que la configuration soit la même sur les deux routeurs Stormshield, j'ai donc effectué la configuration du VPN en collaboration avec une autre personne située elle sur le site de valence.

La première étape de la mise en place du VPN et de définir l'algorithme d'encryptions, dans notre cas c'est AES 256 (Advanced Encryption Standard) qui a été choisi, il s'agit d'un algorithme de chiffrement symétrique (utilisation d'une clé secrète) très réputé pour sa sûreté dans notre cas on utilise 256 bits, de par sa nature sécurisée il n'existe pas d'attaque possible autre que celle dite de brute force qui nécessiterait $\sim 2^{256}$ Opérations, ce qui est impraticable.

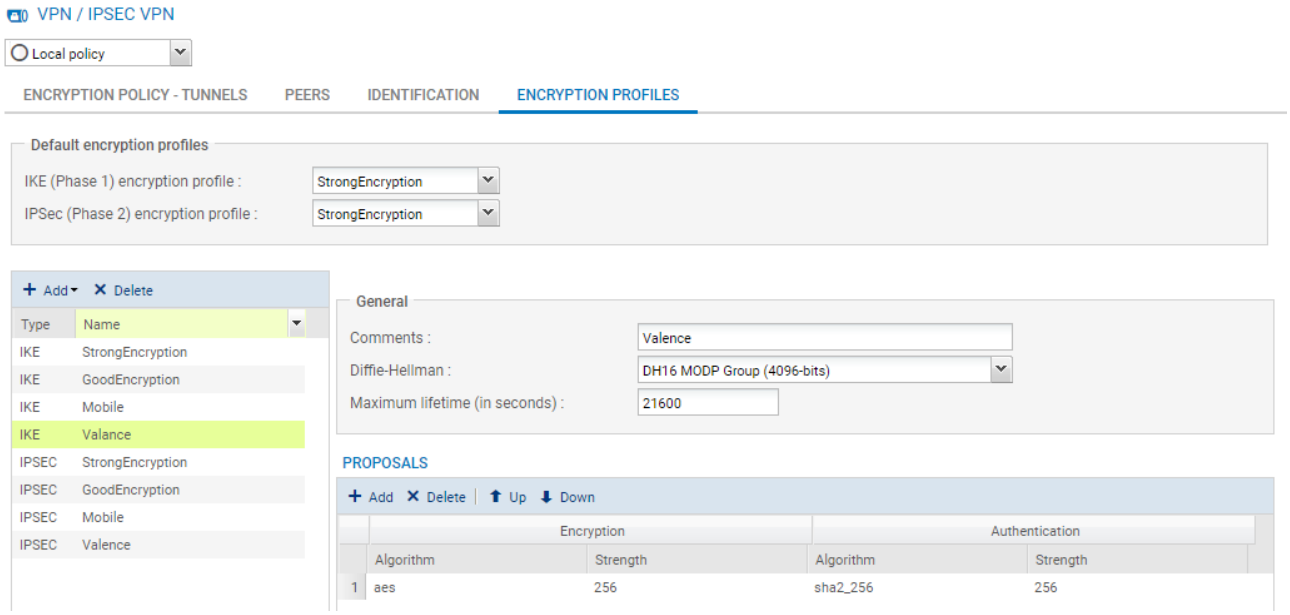


Figure 11 Configuration du profil d'encryptions

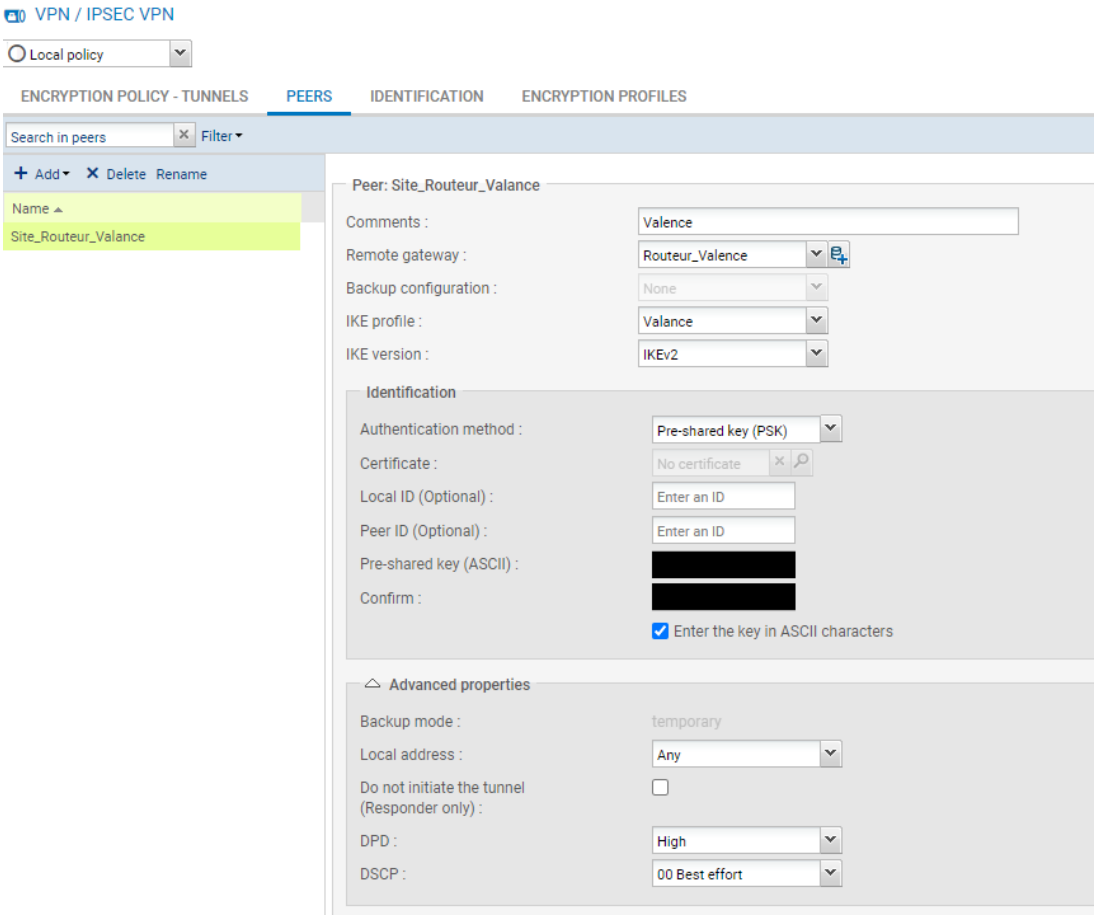


Figure 12 Configuration du pair

Il faut ensuite configurer le routeur distant et la méthode d'identification, dans notre cas nous avons choisi la méthode PSK (Pre-Shared Key) qui consiste simplement à définir une clé partagée connue d'avance par les deux routeurs formant le tunnel, ils chiffreront ainsi le trafic en utilisant cette même clé partagée sans avoir besoin d'effectuer un quelconque échange de clés préalable.

Une autre option que j'ai eu à configurer et le DPD (Dead Peer Détection) qui permet au routeur VPN de s'assurer que son Pair et toujours connecté, pour ce faire il utilise le mécanisme du Keepalive qui consiste simplement à envoyer un message à un intervalle de temps régulier pour vérifier que le lien entre les deux et toujours actif, dans mon cas l'utilisation du DPD a permis de résoudre un problème ou le VPN arrêtait de fonctionner après un certain temps, en effet DPD détecte maintenant toute déconnexion et rétabli la connexion si nécessaire.

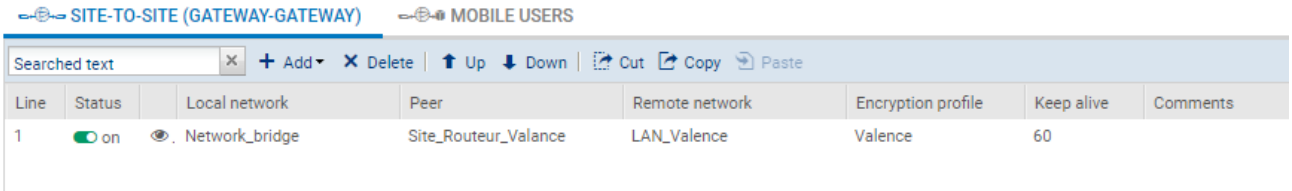


Figure 13 Configuration finale du VPN IPSEC

La dernière étape de la configuration du VPN IPSEC est de définir le réseau local et le réseau distant afin que le routeur sache quel trafic doit être routé sur le VPN, il suffit maintenant d'activer le VPN et d'enregistrer la configuration pour qu'un VPN se forme entre les deux routeurs de manière transparente pour les hôtes des deux réseaux.

4.5 Configuration de l'IPS

Le Stormshield étant avant tout un firewall possède de nombreuses options pour sécuriser le réseau, l'une d'elles et un IPS (Intrusion Prevention System), un IPS est un système qui analyse en temps réel le trafic réseau afin d'identifier et bloquer de potentielles attaques et d'émettre des alarmes pour alerter les administrateurs réseau.

La détection est principalement basée sur des signatures (motif, chaîne de caractère), le firewall compare les évènements observés avec des signatures qu'il possède et bloque le trafic suspect, une autre méthode est l'analyse protocolaire, le firewall vérifie que les paquets sont conformes avec les spécifications des protocoles auxquels ils appartiennent.

Cependant la détection n'est pas parfaite et de nombreuses alertes sont en réalité des faux positifs, ils peuvent donc bloquer malencontreusement des applications ou des trafics légitimes ce qui dans notre cas peut impacter les utilisateurs du réseau, pour éviter ce problème j'ai dû configurer l'IPS pour ne pas bloquer le trafic légitime.

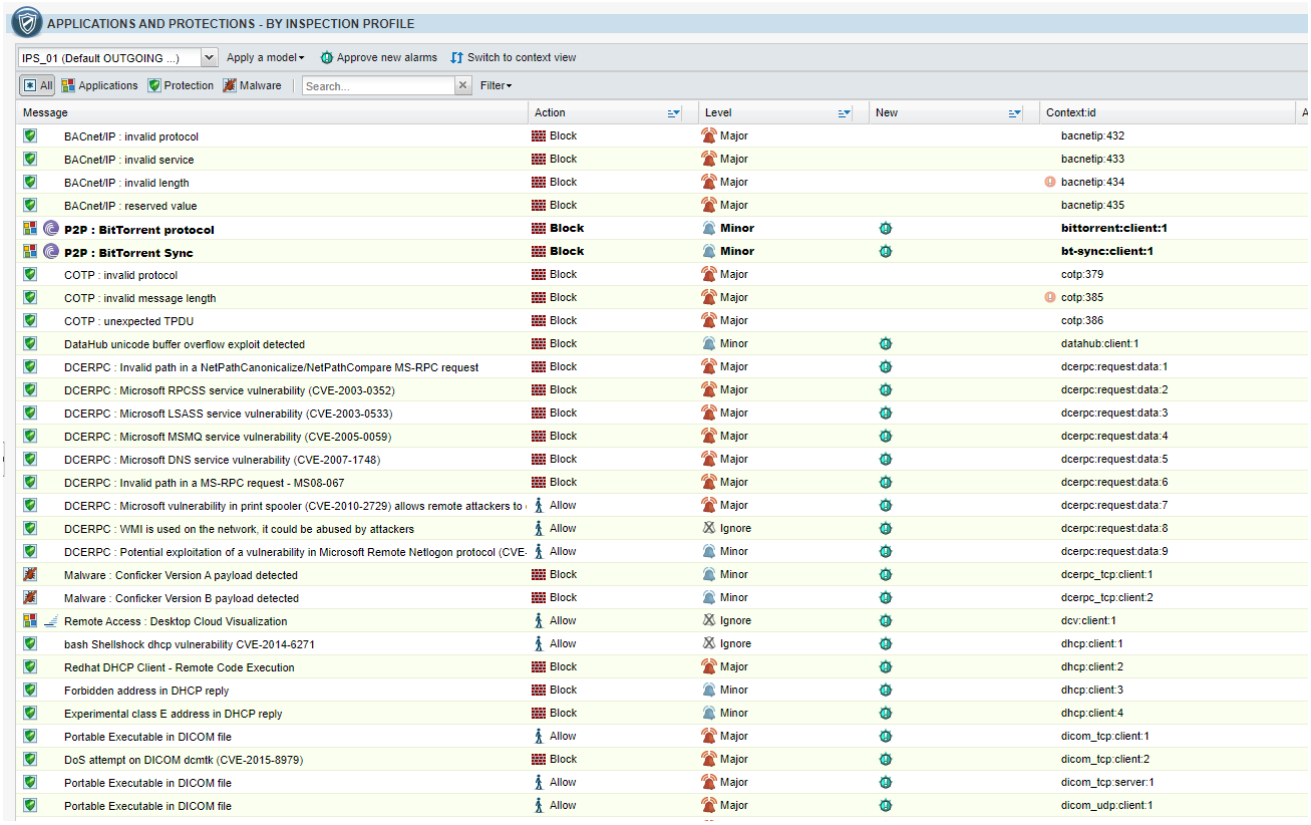
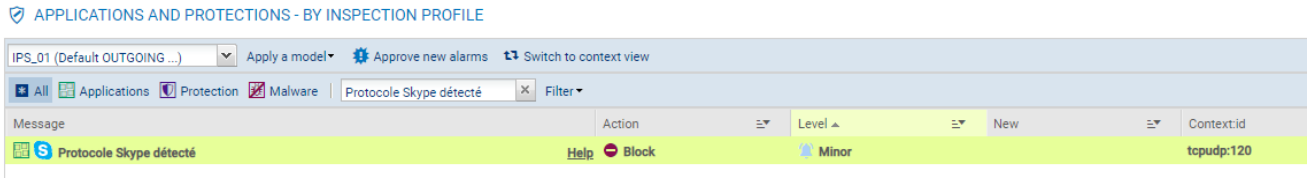


Figure 14 Configuration de l'IPS

Une des règles que j'ai eu à désactiver est la détection d'adresses usurpées, en effet il existe sur le réseau de nombreux sous réseaux utilisés pour des manipulations des serveurs clients ou pour des serveurs clients qui utilisent des sous-réseaux qui ne sont pas connus du routeur, avec la configuration par défaut le routeur bloquait ces sous réseaux, car il ne connaissait par leur existence, ce qui avait pour effet de bloquer leur accès au réseau.

D’autres protocoles et applications ont aussi été désactivés, par exemple le protocole d’échange de fichier pair-à-pair Bittotrent a été désactivé, car il est communément utilisé pour télécharger des œuvres piratées, à l’inverse l’application Skype était bloquée par défaut alors qu’elle est utilisée par certains employés, j’ai donc eu à la réactiver.



Après avoir déployé l’IPS on peut remarquer du trafic bloqué, si une partie de celui-ci peut sembler légitime il y a aussi beaucoup de tentatives d’attaques qui sont mises en évidence et bloquées par l’IPS. En effet du trafic non sollicité provenant de pays comme la Russie et le Vietnam est bloqué, car il peut s’apparenter à une attaque informatique.

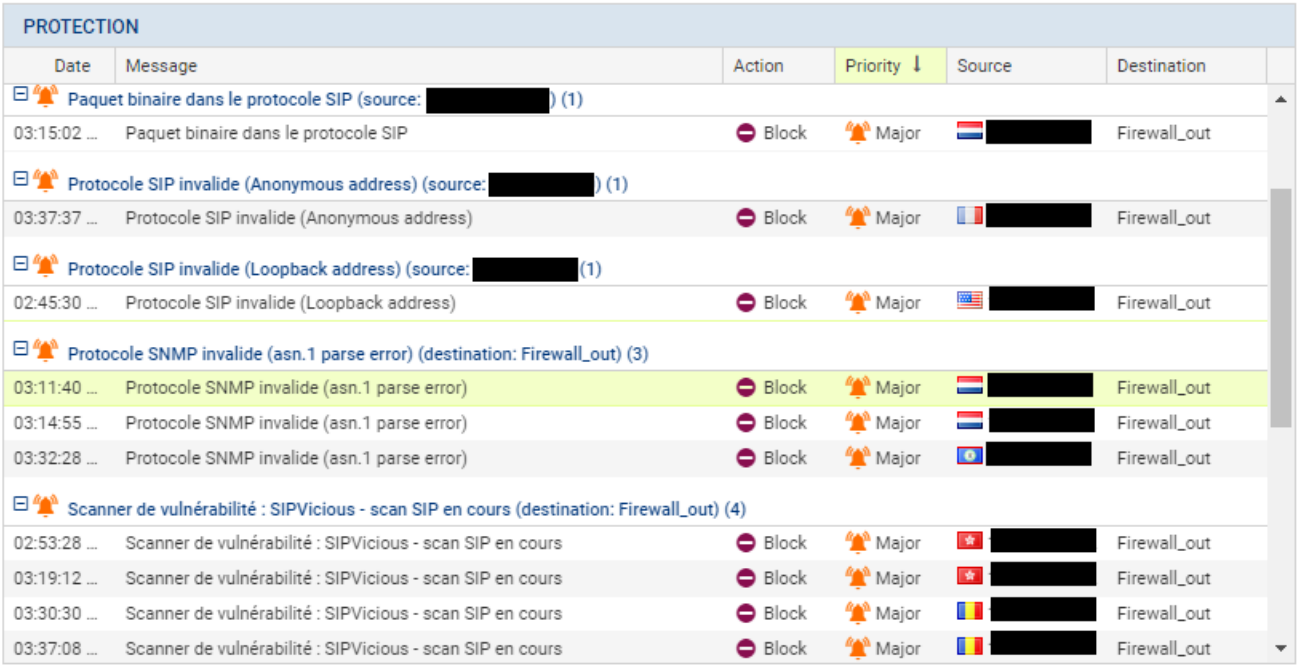


Figure 15 Tentative d'attaque bloquée par l'IPS

Les attaques bloquées sont diverses elles proviennent cependant souvent de scanneurs de ports, de services qui essaient de trouver des ports ouverts et services non sécurisés, un autre type d’attaques communes sont celles ou l’attaquant essaie des mots de passe souvent utilisés et peu sécurisés tel que les mots de passe par défaut.

Grâce à la mise en place du firewall et de l’IPS le réseau est maintenant bien plus sécurisé et les menaces potentielles sont bloquées avant qu’elles ne puissent atteindre leur cible.

4.6 Configuration de VLANs

Afin de séparer les différents trafics présents sur le réseau, d'augmenter la sécurité globale et de réduire l'impacte du trafic généré par les paquets broadcastés j'ai configuré des VLANs sur le routeur et les commutateurs.

Les VLAN (Virtual Local Area Network) sons des sous réseaux virtuels qui permettent de séparer le trafic dans différents sous réseaux cela peut permettre par exemple d'isoler les clients wifi du reste du réseau.

J'ai ainsi d'abord créé des interfaces virtuelles sur le routeur en définissent pour chaque VLAN un identifiant, et un sous réseau.

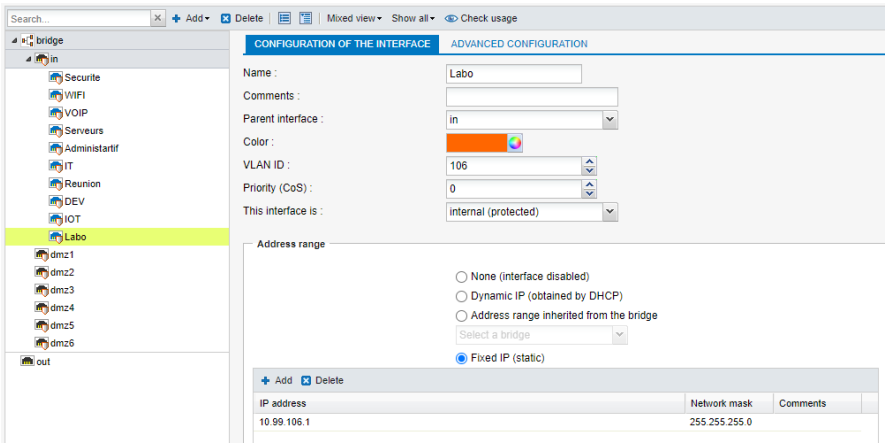


Figure 16 Configuration d'un VLAN sur le routeur

J'ai ensuite configuré les mêmes VLAN sur le commutateur, quand le commutateur recevra un paquet sur un port marqué comme « untagged » il ajoutera une étiquette à ce paquet qui définira à quel VLAN il appartient, cette étiquette sera ensuite utilisée par les autres commutateurs et le routeur pour savoir de quel VLAN le trafic provient.

VLAN Table

Display

ID	Name	Status	IP Config	IP Address	Untagged	Tagged
1	DEFAULT_VLAN	Port Based	Manual	[redacted]	23-24	1-22,25-28
97	Securite	Port Based	Disabled		2	23-24
98	WIFI	Port Based	Disabled		3	23-24
99	VOIP	Port Based	Disabled		None	1-28
100	Serveurs	Port Based	Disabled		None	23-24
101	Administratif	Port Based	Disabled		6,10-12	23-24
102	IT	Port Based	Disabled		4-5,17	23-24
103	Reunion	Port Based	Disabled		14,18-19	23-24
104	DEV	Port Based	Disabled		1,15,20	23-24
105	IOT	Port Based	Disabled		7-9,16	23-24

Figure 17 Configuration des VLANs sur le commutateur Aruba

Un port marque comme « tagged » pour un VLAN signifie qu'il laisse passer le trafic appartenant à cette VLAN, cela permet de laisser passer le trafic de plusieurs VLANs sur un port vers le routeur ou vers un autre commutateur.

J'ai ensuite configuré le serveur DHCP de manière à ce qu'il attribue des adresses IP en fonction des VLANs auxquels appartiennent les équipements.

4.7 Mise place VPN SSL

Tout comme le VPN IPSEC le VPN SSL (Secure Socket Layer) permet d'établir une connexion sécurisée entre deux équipements, dans notre cas il va permettre aux employées d'accéder au réseau interne de l'entreprise et aux équipements qui s'y trouvent depuis leur domicile ou tout autre réseau externe à l'entreprise.

Pour établir une connexion sécurisée celui-ci utilise des certificats privés pour le routeur et publics pour le client qui permettent de s'assurer que l'on communique bien avec la bonne personne et d'établir une connexion chiffrée.

L'utilisateur qui se connecte ce verra ensuite assigner une adresse IP dans un sous réseau créé à cet effet, et pourra communiquer avec les équipements présents sur le réseau de l'entreprise, l'entreprise elle n'aura pas accès au réseau de l'employé.

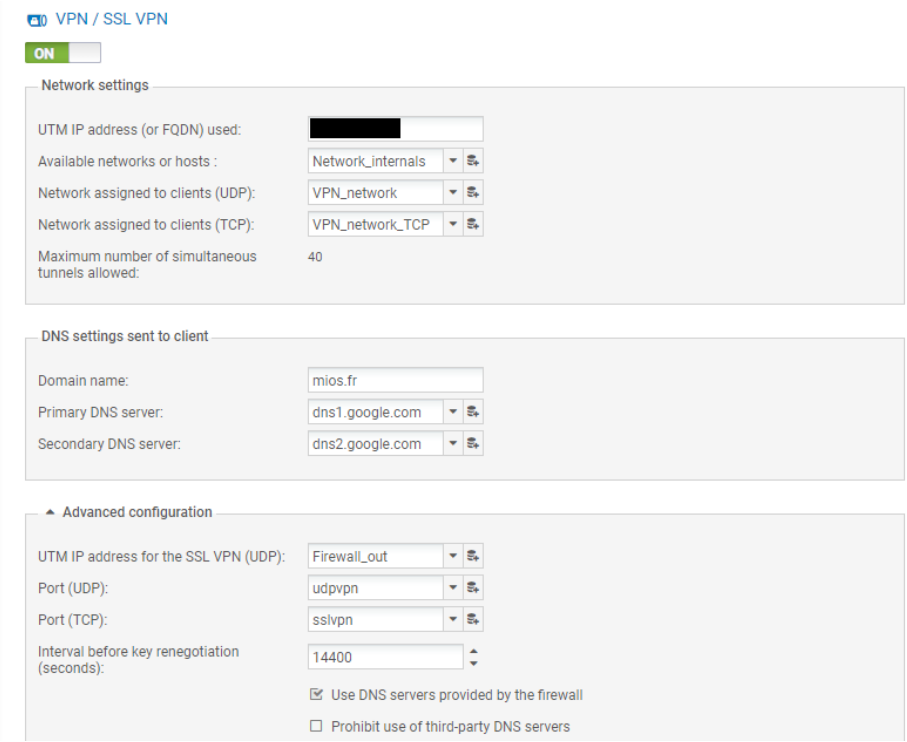


Figure 18 Configuration du VPN SSL

Avant que des utilisateurs puissent se connecter nous devons leur créer des comptes, pour cela nous pouvons connecter le Stormshield à un serveur Microsoft Active Directory, le routeur récupérera ensuite les comptes utilisateurs présents sur le serveur, il faudra ensuite définir les permissions des utilisateurs pour les autoriser à utiliser le VPN.

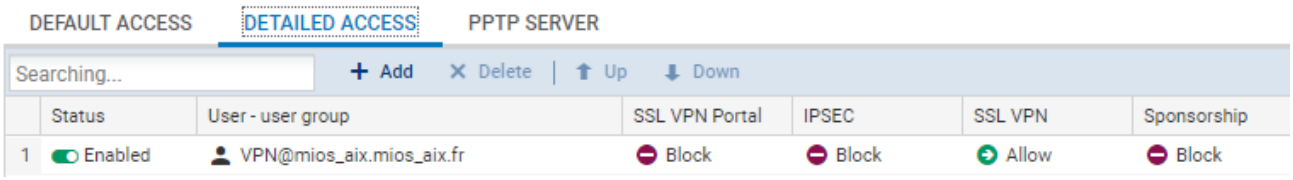


Figure 19 Configuration des permissions utilisateur

Pour se connecter l'utilisateur récupère un fichier contenant les informations de connexion générer par le routeur puis utilise une application de client VPN tel que « Stormshield Network SSL VPN Client » ou OpenVPN, il doit ensuite s'identifier avec un compte utilisateur.

5 Conclusion

Durant les 10 semaines de mon stage en entreprise, j'ai pu me familiariser avec le monde du travail et m'imprégner de son mode de fonctionnement.

J'ai acquis une meilleure compréhension des services présents sur un réseau d'entreprise ainsi que de l'utilisation qu'en font les employés, j'ai aussi appris à faire une étude et à schématiser un réseau en utilisant des outils professionnels.

De plus j'ai aussi pu apprendre quelles sont les méthodes de protection du réseau, notamment avec l'IPS que j'ai eu à configurer, j' ai aussi beaucoup appris sur les utilisations des services telles que les VPN, leur utilité en entreprise, leur fonctionnement, ainsi que leur configuration.

Mon stage m'a aussi permis de me familiariser avec le matériel de marque Stormshield et Aruba, qui sont couramment utilisés en entreprise, leur fonctionnement diffèrent parfois beaucoup du matériel que nous avons utilisé en TP et TD à l'IUT.

J'ai également pu mettre en pratique mes compétences acquises à l'IUT et ainsi d'ajouter une expérience et des cas d'utilisation qui me permettent de comprendre à quel point ces compétences sont essentielles dans le domaine des réseaux.

Ainsi, tout ce que j'ai vécu durant ces dix semaines a été une expérience très bénéfique qui m'aura permis de m'enrichir professionnellement tout en faisant un premier pas dans le monde du travail, qui m'intéresse de plus en plus. Cella m'a permis de me conforter dans mon projet professionnel qui est de devenir ingénieur réseaux.

6 Remerciements

Je tiens tout d'abord à remercier l'entreprise MIOS et plus particulièrement mon maître de stage Guillaume GILABERT de m'avoir accepté comme stagiaire et de m'avoir fait confiance tout au long de ce stage.

Je remercie également Yassine BOUASLA et Axel FEUGIER pour m'avoir guidé et conseillé durant mon stage.

De manière plus générale, je tiens à remercier les membres de l'équipe IT de Mios, ainsi que les employés du site d'Aix qui se sont montrés très accueillants.

7 Glossaire

VPN, *Virtual Private Network*, système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

ADSL, *Asymmetric Digital Subscriber Line*, technique de communication numérique.

VLAN, *Virtual Local Area Network*, Réseau LAN virtuel.

LAN, *Local Area Network*, réseau informatique où les hôtes s'envoient des trames au niveau de la couche de liaison sans utiliser d'accès à internet.

NAT, *Network Address Translation***,** capacité d'un routeur a faire correspondre des adresses IP à d'autres adresses IP.

PAT, *Port Adress Translation*, Extension du NAT ajoutant aussi la translation de ports.

NAS, *Network Attached Storage*, serveur de fichiers autonome, relié à un réseau, dont la principale fonction est le stockage de données.

IPSEC, *Internet Protocol Security*, cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques.

AES, *Advanced Encryption Standard*, algorithme de chiffrement symétrique.

PSK, *pre-shared key*, clé partagée qui a été précédemment échangée entre les deux parties à l'aide d'un canal sécurisé avant d'être utilisé.

DPD, *Dead Peer Detection*, mécanisme utilisé par des routeurs VPN IPSec pour détecter la perte de leur pair.

IPS, *Intrusion Prevention System*, Système de détection et prévention d'intrusion réseau.

SSL, *Secure Socket Layer*, protocoles de sécurisation des échanges par réseau informatique.

8 Bibliographie

Site WEB MIOS, https://mios.fr/

Microsoft Stencils, https://support.microsoft.com/en-us/office/find-more-shapes-and-stencils-0475ddea-2a0a-4dec-ab8c-7dda9e63bca9

Manuel Stormshield, https://documentation.stormshield.eu/SNS/v4/fr/Content/PDF/SNS-UserGuides/sns-fr-manuel_d_utilisation_et_de_configuration-v4.2.2.pdf

NAT, https://fr.wikipedia.org/wiki/Network_address_translation

Stormshield NAT, https://documentation.stormshield.eu/SNS/v3/fr/Content/HowTo_-_Implementing_a_NAT_rule/HT-NAT-rule.htm

Stormshield IPSEC, https://documentation.stormshield.eu/SNS/v3/fr/Content/HowTo_-_IPSec_VPN_-_Authentication_by_pre-shared_key/HOWTO-IPSec-preshared.htm

Usurpation d’adresse IP, https://securitykb.stormshield.eu/fr/b33df83f659c6ff9.html

David Burgermeister, Jonathan Krier , *Les systèmes de détection d'intrusions*, https://web.archive.org/web/20091007094552/http://dbprog.developpez.com/securite/ids/IDS.pdf