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

Etude de la sécurisation d'un réseau par la mise en œuvre d'une solution libre

Matthieu SUISSE

Centre Interdisciplinaire de Nanoscience de Marseille

Responsable entreprise : Mohammed KHABZAOUI

Responsable académique : Tin NGUYEN

2024

Table des matières

1/ Introduction

Dans l'optique de valider ma seconde année d'études de mon **BUT** Réseaux & Télécommunications, j'ai réalisé un stage dans le domaine des réseaux et de la cybersécurité d'une durée de 10 semaines, allant du 15 avril au 21 juin 2024 au sein du **CINaM** (Centre Interdisciplinaire de Nanoscience de Marseille) à Marseille.
Ce stage m'a permis de me former au domaine des réseaux et de la cybersécurité, domaine que j'apprécie particulièrement et qui vient parfaitement s'inscrire dans ma formation car il me donne la possibilité d'exploiter au mieux les connaissances acquises grâce à elle. J'ai notamment pour but de construire ma carrière professionnelle dans la cybersécurité et ces 10 semaines viennent me conforter dans l'idée de réaliser ce stage.

De nos jours, la sécurité d'un réseau au sein d'une entreprise est plus que cruciale. En effet, une entreprise détient des données qui peuvent être sensibles comme par exemples celles de ses clients et elles ne doivent sous aucun prétexte tomber entre les mains de personnes mal intentionnées. En l'occurrence dans le cadre de mon stage précisément, on parle d'un centre de recherche important. Il est normal que les recherches ne soient pas dévoilées publiquement parfois. C'est pourquoi la sécurité du réseau est d'une importance capitale.

Aujourd'hui et depuis l'arrivée de la norme 802.1X en 2001, la sécurité de beaucoup de réseaux d'entreprise se basent encore sur l'authentification par adresse **MAC** (Media Access Control) uniquement et à tort. Avec l'arrivée des dernières technologies, les ordinateurs portables deviennent de plus en plus fins et ne peuvent donc plus accueillir de port Ethernet car ceux-ci sont trop larges pour la finesse de l'appareil. Des adaptateurs ont été conçus afin de permettre à ces équipements de bénéficier d'un port Ethernet malgré tout mais ces adaptateurs possèdent leur propre adresse MAC. Ceci pose un problème de sécurité car si un adaptateur est autorisé sur le réseau alors peu importe l'équipement et la personne derrière, seul l'adresse MAC de l'adaptateur compte. Un individu mal intentionné peut s'introduire dans le réseau avec un adaptateur volé et ainsi accéder à de potentielles données sensibles.

L'enjeu de la sécurité réseau aujourd'hui est de s'adapter à ces nouvelles technologies afin de permettre une sécurité toujours plus optimale contre les potentielles menaces. C'est dans cet objectif que s'inscrit parfaitement mon projet au sein du CINaM. Ici, il est question d'ajouter une couche de vérification à celle par adresse MAC : la vérification par nom d'utilisateur et mot de passe. Elle rajoute une sécurité conséquente car elle permet même en cas d'adaptateur volé d'empêcher un intrus d'accéder au réseau car il n'est pas en possession d'un couple d'un nom d'utilisateur et d'un mot de passe valide.

C'est pourquoi l'étude de la sécurisation d'un réseau par la mise en œuvre d'une solution libre avec PacketFence m'a semblé être une mission particulièrement intéressante et formatrice car elle m'offre l'opportunité de développer mes compétences en matière de réseau et de sécurité des réseaux. De plus, elle s'applique dans un contexte où la cybersécurité devient de plus en plus importante de nos jours.
Cette dernière consiste-en :

- L'installation et l'administration d'un serveur PacketFence
- La mise en place d'un serveur **RADIUS** (Remote Authentication Dial-In User Service)
- Création et administration des comptes utilisateurs et machine avec **LDAP**
- Configuration, gestion et installations d'équipements actifs du réseau

Cette mission va me permettre à terme de mon stage de confirmer mes compétences et mes connaissances en matière de réseau, d'administration système ainsi qu'en cybersécurité.

Dans ce rapport, j'aborderai donc mon projet sur PacketFence dans un premier temps puis expliquerai les deux missions annexes que j'ai pu réaliser avant de conclure.

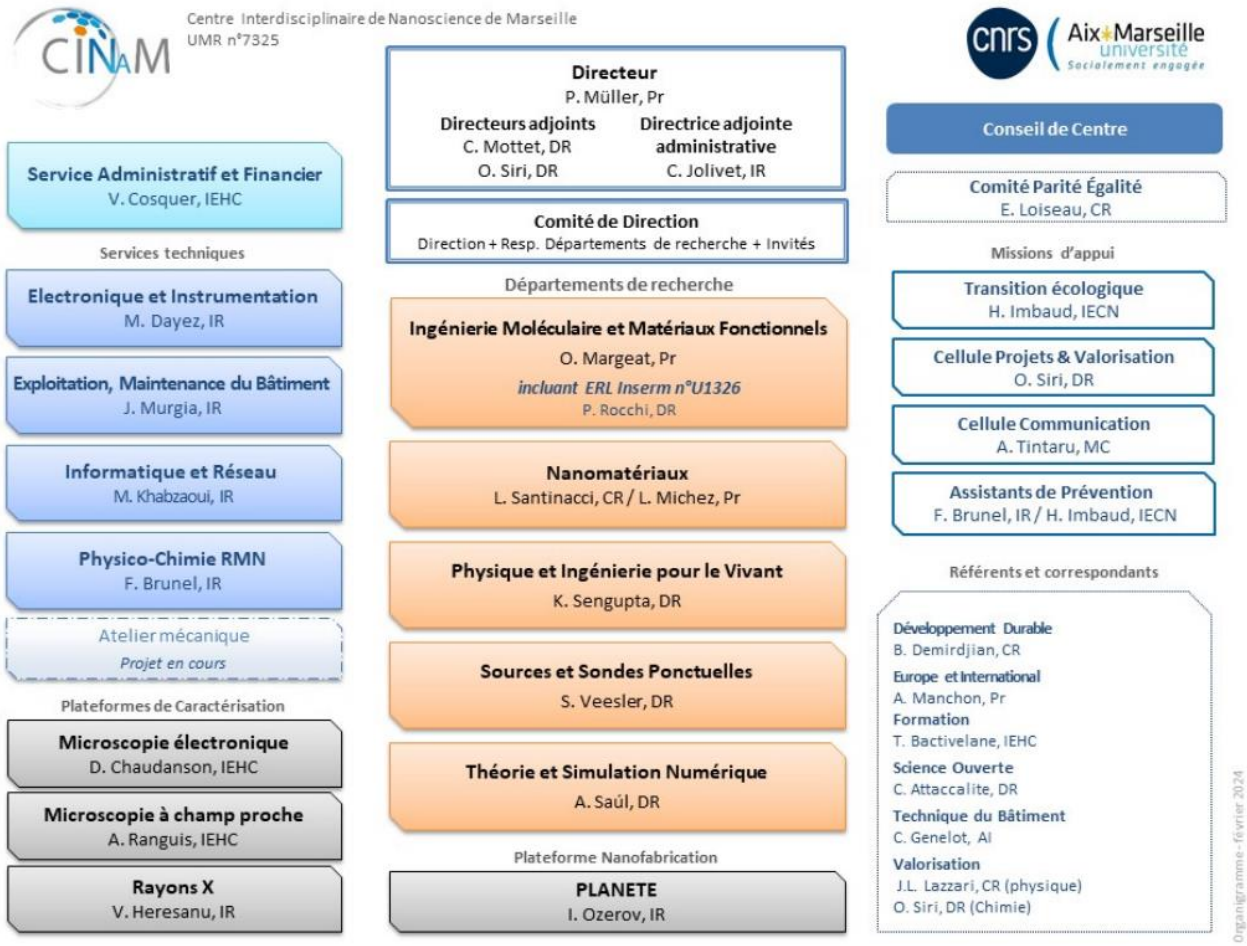
2 / Présentation de l'entreprise

2.1 La culture et l'activité du CINaM

Issu d'une collaboration entre le **CNRS** (Centre National de la Recherche Scientifique) et **AMU** (Aix-Marseille Université) en 2008, le CINaM centralise son activité sur l'ensemble des recherches concernant des systèmes dont une ou plusieurs dimensions sont de l'ordre du nanomètre (en sachant qu'un nanomètre correspond à un milliardième de mètre).

Ce centre rassemble des ingénieurs, des doctorants, des chercheurs, des stagiaires et bien d'autres venant des quatre coins du monde dans l'optique de faire avancer la nanoscience.

Les recherches qui y sont menées couvrent un large spectre, allant de la physique de la matière condensée à la chimie moléculaire. En effet, à l'échelle nanométrique les propriétés des matériaux diffèrent de celles qui prévalent aux échelles usuelles faisant du CINaM un laboratoire unique en son genre.



Organigramme du CINaM

2.2 Les locaux du CINaM

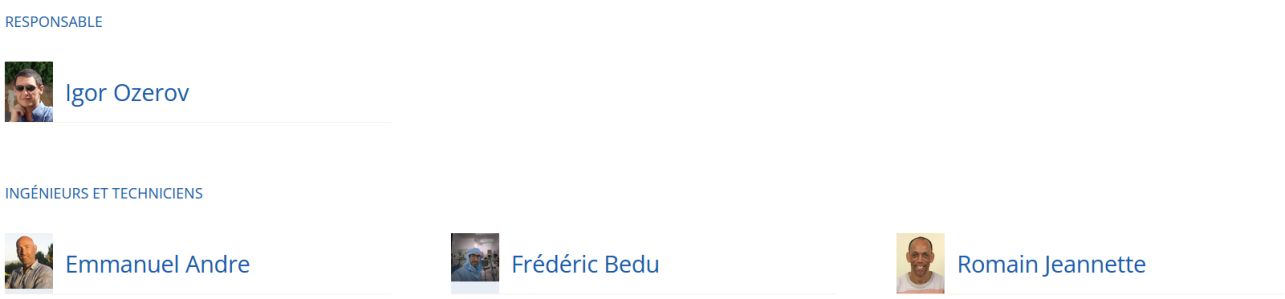
Le centre prend place dans un cadre de vie particulièrement exceptionnel puisqu'il se situe sur le campus de Luminy, au cœur du massif des calanques. En effet, l'occasion d'étudier et de mener ses recherches au sein d'un parc national avec une telle diversité est assez atypique pour un laboratoire. Le CINaM se base sur 3 bâtiments hébergeant chacun un domaine de recherche particulier. Le premier (figure 1) bâtiment héberge principalement les physiciens du laboratoire et est équipé de quelques équipements technologiques liés à la microscopie électronique. Le second bâtiment (figure 2) quant à lui regroupe sur quatre étages les chimistes du CINaM. Pour le dernier (figure 3), il s'agit de celui dans lequel j'ai eu l'occasion de travailler. Il se nomme PLANETE et héberge la plateforme technologique de micro et nanofabrication du CINaM. Les locaux du service informatique s'y trouvent et c'est pourquoi j'ai réalisé mon stage dans ce bâtiment précisément.

Premier bâtiment du CINaM (figure 1)

Second bâtiment du CINaM Aussi appelé TPR1 (figure 2)

Troisième bâtiment du CINaM Aussi appelé PLANETE (figure 3)

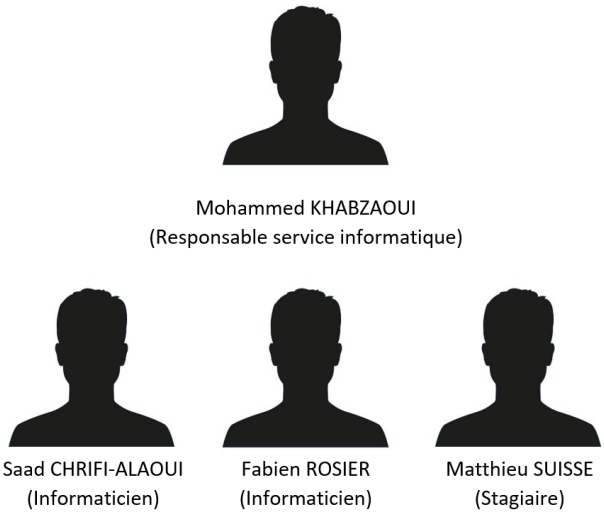
Pour répondre à la demande en nanolithographie, nanostructuration et en connectique des nano-objets, le CINaM accompagné du CNRS, d'AMU et d'un soutien des collectivités (ville de Marseille, Conseil Général des Bouches-du-Rhône, Conseil de la Région Sud Provence-Alpes-Côte d'Azur) a permis en 2006 la conception de la plateforme technologique PLANETE.
La plateforme contient une salle blanche de 250m^2 elle-même dotée d'équipements technologiques. Cette dernière est gérée par une équipe d'ingénieurs qui l'utilisent et en assurent le bon fonctionnement et le bon état en continu.



Organigramme du personnel scientifique de PLANETE

Entrée de la salle blanche

Pour le bon déroulement de mon stage, j'ai été assigné à un poste dans les locaux du service informatique. Les locaux sont séparés en trois pièces différentes : deux font office de bureaux et la dernière est assignée à une pièce de stockage pour divers équipements électroniques et informatiques.



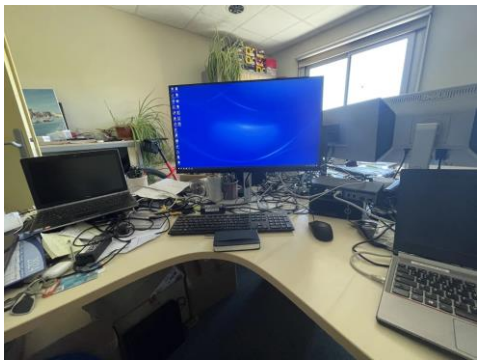
Organigramme du personnel du service informatique du CINaM

On retrouve sur l'organigramme mon responsable et mon tuteur de stage Mohammed KHABZAOUI. Il dirige l'ensemble du service informatique et intervient dans les trois différents bâtiments du CINaM pour corriger des soucis informatiques ou pour diriger des installations. Dans le service, j'ai co-travaillé avec Saad CHRIFI-ALAOUI et Fabien ROSIER qui ont le même rôle que Mohammed excepté la partie de responsable du service. Ils interviennent également et s'occupent notamment du service de tickets pour répondre aux besoins des utilisateurs. Ma présence dans le service a permis notamment de le renforcer afin d'alléger la tâche du reste du service.

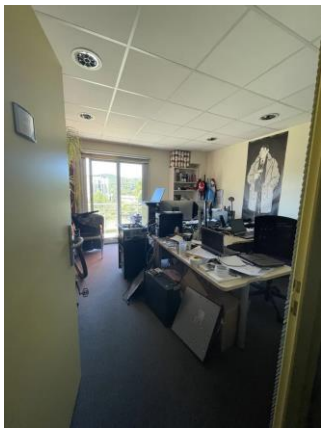
2.3 Les conditions de travail

J'ai pu retrouver dans ce stage une méthode de travail similaire à ce que nous avons appris dans notre formation au cours de petits projets organisés nommés **SAés**. L'objectif de celles-ci était de nous placer en situation d'entreprise dans laquelle nous avions un projet à rendre dans un temps imparti. Il était également important que mon maître de stage puisse voir mon avancement dans ce projet au fur et à mesure afin de pouvoir encadrer le projet. Cette communication apprise lors de mes SAés m'a notamment permis de rester sur une ligne directrice aussi claire que possible afin d'assurer le bon déroulé du projet.

En dehors des méthodes de travail acquises, j'ai eu la chance de collaborer dans un espace de travail très convivial ce qui permet la réalisation d'un travail productif. J'ai été assigné à un poste de travail avec Fabien ROSIER. Son expérience, la diversité de travail que nous avions ainsi que la proximité que nous partagions a permis d'avoir une bonne entente et une entraide au quotidien. Également les membres du laboratoire au quotidien ont été très bienveillants et agréables offrant des conditions de travail optimales.



Mon poste de travail



Bureau dans lequel j'ai travaillé

3/ Travail réalisé

Tout au long de mon stage, mon activité a été très diversifiée, intéressante et enrichissante. J'ai su développer mes compétences, mes connaissances, mon savoir-être mais également apprendre de nouvelles notions. Être mis en difficulté a su se révéler très instructif pour moi et m'a montré l'imprévu qu'il est possible de rencontrer dans la réalisation d'un projet dans le milieu professionnel.

Mon activité durant ce stage se divise en deux parties distinctes. La réalisation de mon travail s'est organisée et rythmée par de petits comptes-rendus expliqués à mon maître de stage afin de faire le point sur ce qui était fait et ce qui était à faire. Ainsi, la première partie de mon stage se résume à la conception et la mise en place d'un contrôleur d'accès réseau avec lequel j'ai pu utiliser notamment Windows Serveur et Linux pour le faire fonctionner. J'ai pu emprunter de l'équipement du service informatique à savoir des ordinateurs portables sur lesquels je pouvais expérimenter mon projet. La seconde partie de mon stage elle correspond plus à la configuration et mise en production de commutateurs dans le réseau du CINaM. J'ai utilisé des commutateurs HPE (Hewlett Packard Enterprise) ce qui a été très instructif pour moi car j'ai eu l'occasion de redécouvrir un nouvel environnement quelque peu différent de celui étudié pendant ma formation.

3.1 Le début de mon stage

Ce stage est ma première expérience professionnelle dans ce domaine. J'avais hâte de pouvoir mettre pour la première fois en application les connaissances théoriques et pratiques apprises lors de ma formation et d'en apprendre plus. Monsieur KHABZAOUI a su me placer dans de bonnes conditions afin d'appréhender mon stage de la meilleure manière possible et de me familiariser avec mon environnement de travail autant virtuel que physique. De plus, j'ai été présenté à l'ensemble du personnel administratif, scientifique et informatique, ce qui a permis de me mettre en confiance pour le début de ce stage.

Durant la première semaine, mon maître de stage m'a laissé prendre en main l'équipement que j'allais être amené à configurer, les logiciels et installer ce dont j'avais besoin. J'ai eu le champ libre pour me renseigner le plus possible concernant les sujets sur lesquels j'allais travailler dans l'objectif d'être le plus opérationnel.
Cette première semaine a été cruciale car elle m'a permis de me préparer convenablement et de bien comprendre l'objectif de mon projet. J'ai pris l'initiative de me renseigner à propos des sujets sur lesquels je suis moins à l'aise ou que je ne connais pas tel que Windows Server sur lequel je serais amené à travailler avec PacketFence, le protocole RADIUS que je ne connaissais pas auparavant ou encore les commutateurs HPE que je n'avais jamais eu l'occasion de manipuler. Ainsi j'ai pu établir un calendrier qui m'indiquait les lignes directrices de mon projet et de mon avancement dans mon apprentissage.

Semaine 1	Semaine 2	Semaine 3	Semaine 4	Semaine 5	Semaine 6	Semaine 7	Semaine 8	Semaine 9	Semaine 10
Conception du calendrier, Établir les objectifs du stage, Configuration de mon ordinateur personnel,	Découverte des switchs HPE, Découverte du protocole RADIUS, Découverte de FreeRADIUS	Approfondissement sur les switchs HPE, Tests sur un serveur FreeRADIUS, Révisions sur Windows Server	Configuration de switchs HPE, Mise en production des switchs configurés	Approfondissement de la configuration des switchs	Découverte de PacketFence, Tests sur PacketFence ZEN avec un serveur FreeRADIUS	Approfondissement sur PacketFence, Tests sur PacketFence version ISO avec un serveur FreeRADIUS	Tests sur PacketFence version ISO avec un serveur NPS sur Windows Server	Visite à la délégation pour observer un PacketFence opérationnel, Tests sur PacketFence version ISO avec un serveur NPS sur Windows Server	Finalisation de PacketFence version ISO avec un serveur NPS sur Windows Server

Calendrier de mes 10 semaines de stage au sein du CINaM

Comme attendu, certaines prévisions ne se sont pas passées comme prévu mais cela ne m'a pas empêché de tenir un avancement correct et continu concernant l'avancement du projet.

3.2 PacketFence

Mon projet s'organise autour de l'utilisation du logiciel PacketFence car il répond parfaitement aux attentes de mon maître de stage et au problème évoqué précédemment. PacketFence est un contrôleur d'accès réseau (**NAC**) entièrement libre et gratuit. Cette solution comprend un grand nombre de fonctionnalités avec notamment de la supervision réseau, la prise en charge de la norme 802.1X, scan de vulnérabilités ou encore la création d'un portail captif.

NAC est une solution de sécurité réseau offrant un contrôle d'accès sur un réseau donné à travers l'application de politiques de sécurité et de conditions. Elle implémente la norme 802.1X qui elle ajoute uniquement la fonctionnalité de s'authentifier. Un NAC lui permet notamment de retrouver cette authentification mais également de l'intégrité pour vérifier si un appareil répond à certaines exigences mises en place au préalable telles que la dernière version d'un système d'exploitation, une surveillance continue ou encore un contrôle d'accès dynamique permettant de placer les équipements dans un réseau ou un autre selon les paramètres.

Le logiciel s'organise à l'aide d'une documentation disponible sur le site web de PacketFence. On y retrouve un guide d'installation et de configuration ainsi qu'un manuel d'aide en cas d'erreur lors de l'installation ou de la configuration.

PacketFence se distingue des autres contrôleurs d'accès réseau par sa simplicité à l'installer. En effet, il peut être installé de trois manière distinctes : depuis une machine linux en faisant attention à la version du noyau (pour exemple si l'on utilise Debian, nous aurons alors besoin de Debian 11), sur une machine vierge avec une clé bootable où nous avons installé la version système d'exploitation de PacketFence et finalement sur une machine virtuelle avec la version ZEN (Zero Effort NAC) de PacketFence.

Après avoir essayé les trois solutions différentes, j'ai jugé qu'il était préférable d'opter pour la seconde solution à savoir d'utiliser une clé bootable et d'installer un système opérationnel avec PacketFence dedans. La raison pour laquelle j'ai opté pour cette solution est que parfois les dépendances ne sont pas toutes satisfaites laissant lieu à des erreurs impromptues. En l'occurrence ici, le système possède tout ce dont il a besoin permettant d'être sûr que nous n'avons rien oublié concernant ces dépendances. La solution ZEN sur machine virtuelle aussi correspondait mais j'ai trouvé qu'il était plus adapté de travailler sur une machine physique afin de pouvoir effectuer mes branchements de manière claire et précise avec le switch et les autres machines.

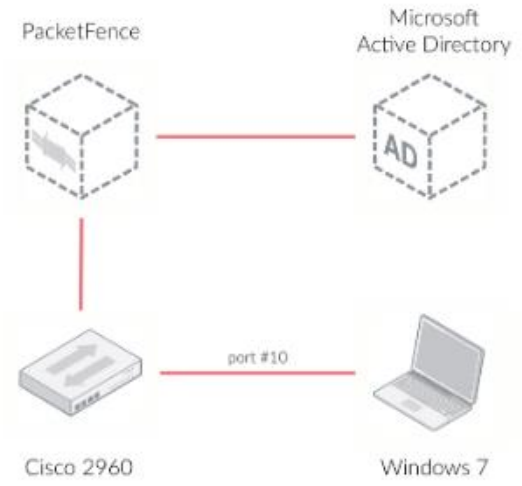


Schéma simplifié du fonctionnement de PacketFence

Comme l'indique la documentation de PacketFence et ce schéma, le logiciel fonctionne avec un serveur faisant principalement usage des services **AAA** (Authentication, Authorization, Accounting) et d'un service d'annuaire afin d'administrer des utilisateurs ou des machines. Ces derniers sont primordiaux lorsque l'on parle de sécuriser des réseaux et des systèmes informatiques. Ils permettent respectivement d'authentifier un utilisateur au moyen de divers protocoles, d'autoriser ou non l'accès à cet utilisateur en fonction du résultat de l'authentification puis finalement d'enregistrer une trace peu importe le résultat afin de savoir si quelqu'un a réalisé une tentative de connexion. Le service d'annuaire quant à lui est un service permettant d'organiser des données de manière claire et concise. Un protocole a été standardisé pour ces services, il s'agit de LDAP. Avec mon maître de stage, nous avons pu trouver qu'il existe deux solutions qui peuvent bien fonctionner avec PacketFence et répondre au besoin des services AAA et d'annuaire : FreeRADIUS et NPS. Ces deux solutions diffèrent sur un point principal : **NPS** est une solution fournie par Microsoft et payante tandis que FreeRADIUS est une solution libre d'utilisation et entièrement gratuite.

J'ai naturellement choisi d'opter pour une solution gratuite en premier lieu avant d'utiliser Windows Server.

3.2.1 FreeRADIUS

FreeRADIUS est un serveur RADIUS open source très utilisé à travers le monde pour l'utilisation de services AAA. Il implémente RADIUS, un protocole standardisé qui fonctionne sur le client-serveur. Un client RADIUS, souvent un équipement de réseau tel qu'un switch ou une borne Wi-Fi, envoie des requêtes UDP d'authentification, d'autorisation et de comptabilité au serveur RADIUS. FreeRADIUS propose ses avantages à savoir une haute flexibilité concernant la configuration, une grande scalabilité et finalement une grande compatibilité. Les fonctionnalités dont dispose FreeRADIUS sont multiples : au-delà des services AAA, on peut retrouver une possibilité d'ajouter des modules supplémentaires tels que **SQL** et LDAP parmi les plus connus. Son installation est assez simple et se fait uniquement sur des distributions Linux à l'aide des gestionnaires de paquets. En revanche, en vue de sa grande flexibilité, sa configuration devient elle aussi compliquée. La documentation de PacketFence est réalisée pour des cas de figure assez basiques où l'on utilise Windows Server ainsi qu'un commutateur de la marque Cisco. Il était donc très complexe d'essayer d'allier FreeRADIUS avec PacketFence et en prenant en compte que le CINaM utilise déjà un seveur Windows Active Directory, j'ai pris l'initiative de suivre la documentation de PacketFence et d'utiliser une solution sur un serveur Windows.

3.2.2 NPS avec Windows Server

NPS, de son vrai nom Network Policy Server, est une fonctionnalité de Windows Server qui à l'identique de FreeRADIUS implémente les services AAA au travers du protocole RADIUS. Cette fonctionnalité est présente depuis la version 2008 de Windows Server. Il offre une interface graphique intuitive pour configurer et administrer ce serveur, ce qui en fait une grande force. On retrouve des fonctionnalités similaires à celles présentes sur FreeRADIUS mais également certaines spécifiques à NPS comme son intégration particulière avec Active Directory permettant une configuration nettement plus simplifiée. La plus grande différence que j'ai pu observer réside dans la documentation où celle de Microsoft est officielle et très détaillée.

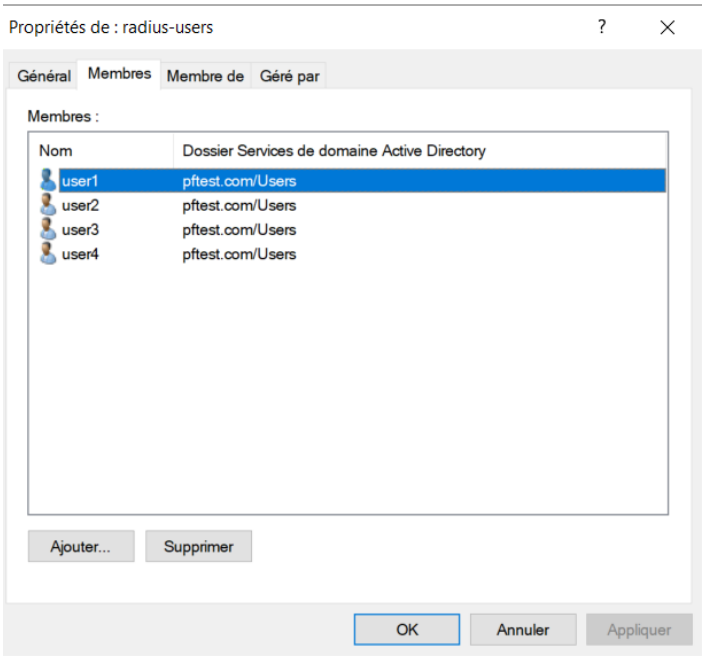
Active Directory est une solution de service d'annuaire propriétaire innovée par Microsoft. Elle intègre les services d'annuaire LDAP adaptés aux systèmes d'exploitation Windows. Néanmoins, cette solution permet facilement d'identifier, d'authentifier et d'administrer des machines fonctionnant sur macOS ou encore Linux. AD répertorie de manière claire et concise les éléments d'un réseau qu'il administre. Cette organisation hiérarchisée se divise en trois grandes catégories remarquables : les ressources, on retrouvera ici les périphériques comme les imprimantes ou les scanners, les services, on pensera ici aux services actifs sur le réseau comme le courrier électronique ou le DNS et finalement les utilisateurs.

Chaque objet est une entité unique sur le domaine et possède ses propres attributs. Il est possible de regrouper ces objets afin de leur faire partager des attributs simplement.

Pour la configuration et l'installation, d'un serveur NPS et Active Directory sur Windows Server, on peut facilement retrouver sur internet des tutoriels très bien guidés nous expliquant comment s'y prendre étape par étape afin de les installer chacun leur tour.

La force concernant l'intégration entre Active Directory et NPS se trouve dans le fait que RADIUS va pouvoir utiliser les groupes de machines et d'utilisateurs configurés dans le domaine AD que nous avons créé afin d'administrer ensuite les autorisations et interdictions. L'idée ici va être de créer un groupe de machine qui appartient au CINaM avec leur adresse MAC enregistrée afin de bien faire une première authentification sur le réseau. Une fois cette première authentification réalisée, la machine en question sera placée sur un Vlan qui permet simplement l'accès à internet n'offrant de ce fait aucun accès sur le réseau interne du CINaM.

La seconde authentification intervient lorsqu'un utilisateur s'authentifie sur une machine déjà authentifiée par PacketFence. On retrouve ici quelques pré-requis afin que cela fonctionne : il faut activer la fonctionnalité 802.1X sur la machine question et avoir enregistré un compte utilisateur dans le domaine AD. Tout cela se paramètre très simplement dans la fenêtre de configuration d'Active Directory. Une fois cela fait si l'utilisateur entre des informations d'identification valides, alors il sera dans sa session avec un accès à internet et au réseau interne du CINaM. Le cas échéant, l'utilisateur n'aura donc pas un accès autorisé et ne sera pas dans une session.

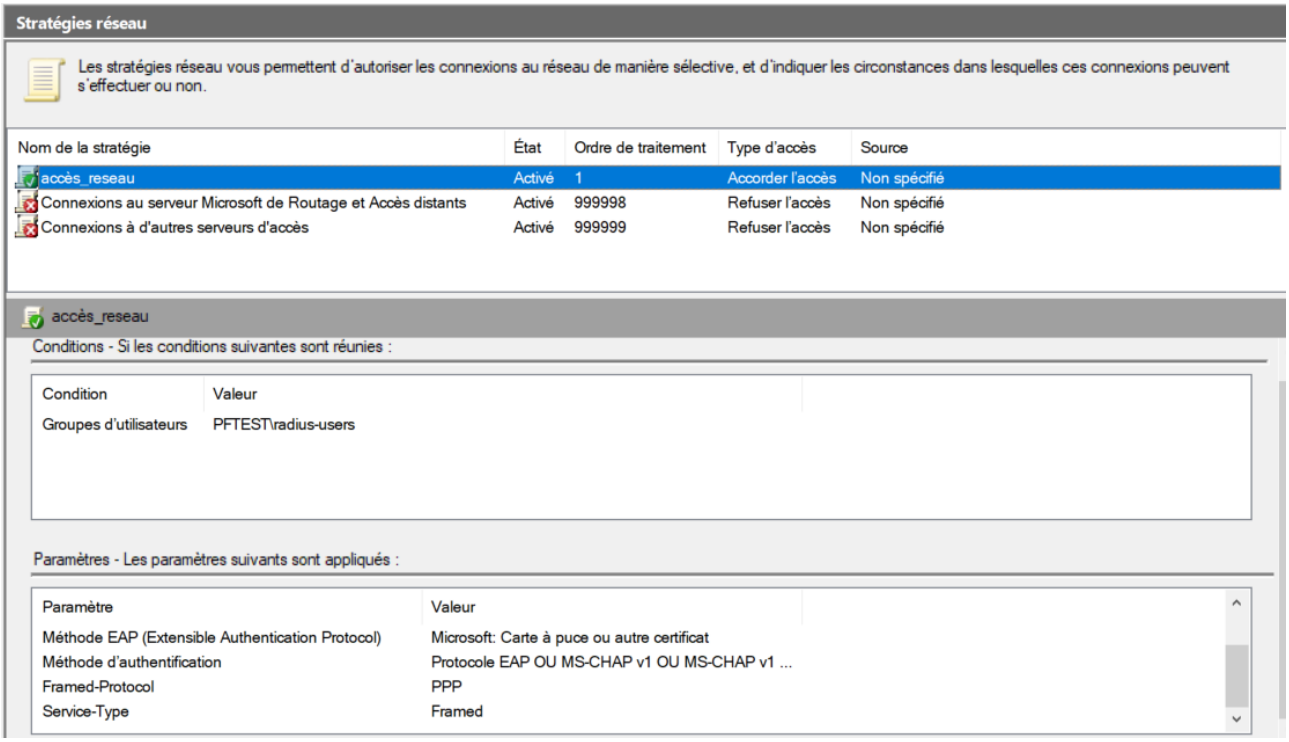


Groupe d'utilisateurs que l'on va autoriser à se connecter au réseau

La faille correspondant aux adresses MAC n'apparaît plus comme telle car désormais un utilisateur ne pourra plus avoir accès au réseau interne du CINaM uniquement via une adresse MAC mais également via un enregistrement avec un identifiant et un mot de passe que seule cette personne est censée connaître.

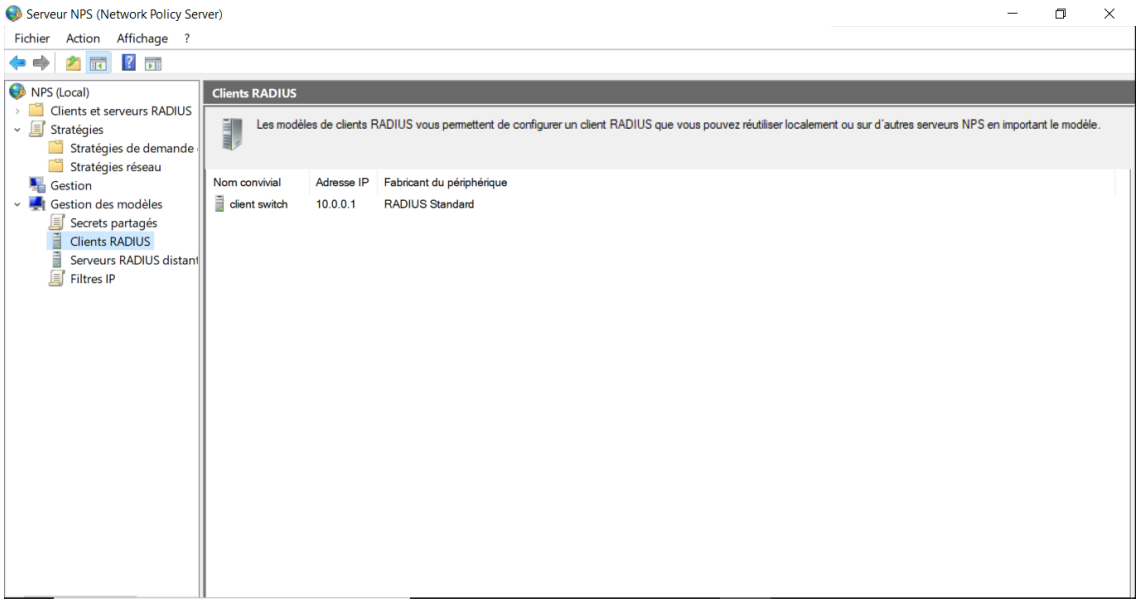
La seconde partie à configurer sur Windows Server est ensuite le serveur NPS. Le paramétrage se fait en trois étapes principales.

Dans un premier temps, il faut créer des stratégies réseau. Celles-ci correspondent aux groupes de machines ou d'utilisateurs auxquels on choisit de de donner ou de refuser un accès.



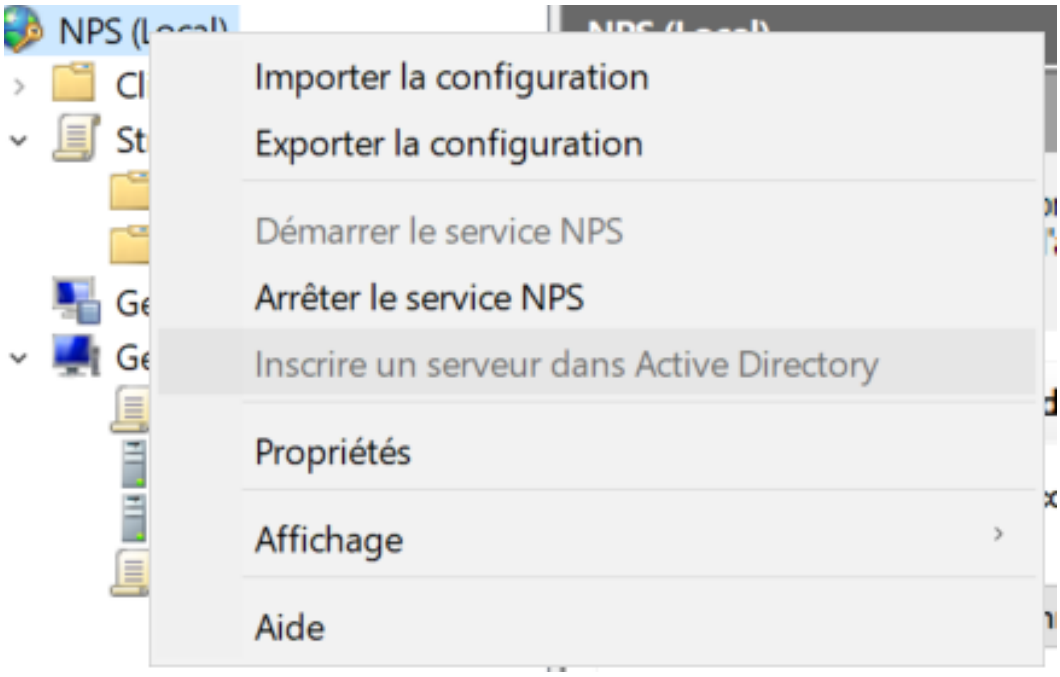
On définit une stratégie réseau avec les utilisateurs du groupe créé précédemment

La seconde étape de la configuration consiste à ajouter un client RADIUS. Ce système client correspond à l'équipement qui va venir interroger le serveur RADIUS en proposant les identifiants/mot de passe ou le matériel qui souhaite obtenir un accès. Ici pour cette configuration on vient renseigner l'adresse IP ainsi qu'un mot de passe appelé secret partagé qui permet d'authentifier les deux machines entre elles.



On définit le client RADIUS (commutateur)

La troisième étape se résume à inscrire le serveur dans le serveur Active Directory. Ceci permet de partager les groupes et utilisateurs créés dans le serveur AD afin d'appliquer les stratégies mises en place.



On inscrit le serveur NPS dans AD

3.2.3 Configuration et fonctionnement des commutateurs

Comme précisé dans le schéma, PacketFence fonctionne derrière un équipement réseau quelconque. Plus généralement et dans mon cas précisément, il est question d'appliquer le projet sur des commutateurs. Il sera question de reporter cette configuration plus tard sur des bornes Wi-Fi. Pour ce projet, j'ai eu l'opportunité de découvrir de nouveaux équipements réseau à savoir des commutateurs de la marque HPE. Leur fonctionnement n'est pas très différent d'un commutateur Cisco sur lesquels j'ai eu pour habitude de travailler durant ma formation. Néanmoins, on retrouvera quelques différences notamment sur les commandes de base pour manipuler l'équipement : "undo" qui remplacera la commande "no" sur Cisco ou "system-view" pour entrer en mode de configuration qui s'écrira "configure terminal" sur Cisco.
L'objectif sur ces commutateurs sont de créer des **VLANs** (Virtual Local Area Network), de paramétrer les ports et de configurer la discussion entre le commutateur et le serveur RADIUS.
La configuration s'effectue en plusieurs étapes. Dans un premier temps, il faut définir les différents VLANs afin de pouvoir ensuite attribuer les utilisateurs sur les différents VLANs correspondant. Concernant la configuration des ports, il faut activer et configurer la norme 802.1X , les configurer de sorte à ce qu'ils acceptent les requêtes pour le serveur RADIUS et finalement attribuer les bons VLANs aux ports.

```
port link-type hybrid
port hybrid vlan 20 25 126 tagged
port hybrid vlan 1700 untagged
```

Ici on attribue les VLANs au port. On commence par le placer sur un mode hybride permettant de faire passer des paquets taggés et des paquets non-taggés. Un paquet taggé est un paquet qui porte l'étiquette correspondant au VLAN auquel il appartient. Il permet une gestion efficace et segmentée du trafic dans un réseau complexe, qui dans la plupart des cas comprennent une infrastructure importante ou une segmentation élevée. Un paquet non-taggé quant à lui servira principalement pour assurer une compatibilité avec des périphériques qui ne prennent pas en charge ces tags ou bien pour simplifier le trafic.

```
dot1x
dot1x port-method multi-auth
dot1x auth-fail vlan 1700
dot1x timer tx-period 10
dot1x timer quiet-period 10
dot1x reauth-period 600
```

Ici on active le 802.1X sur le port et on le configure. On active le possibilité à plusieurs appareils différents de s'authentifier sur le même port, on place les appareils ayant échoué leur authentification sur le VLAN 1700 puis on met en place des comptes à rebours. Le premier permet de spécifier l'intervalle de temps entre les tentatives d'authentification. Toutes les 10 secondes, le switch initie une tentative d'authentification avec les équipements encore non authentifiés. Le second compte à rebours lui concerne les authentifications échouées. On attend donc également 10 secondes avant de réinitier une tentative d'authentification. L'objectif de mettre ces deux comptes à rebours est de s'assurer que toute connexion est bien terminée avant d'en initier une nouvelle. Le troisième quant à lui est quelque peu différent car il demande toutes les 600 secondes aux appareils déjà authentifiés de se réauthentifier. Cela fait office de sécurité afin de s'assurer assez régulièrement que l'on a toujours le bon appareil authentifié sur le réseau.

```
lldp enable
lldp tlv-enable system-description system-capabilities management-address
lldp notification enable
lldp med enable
lldp med config notification enable
```

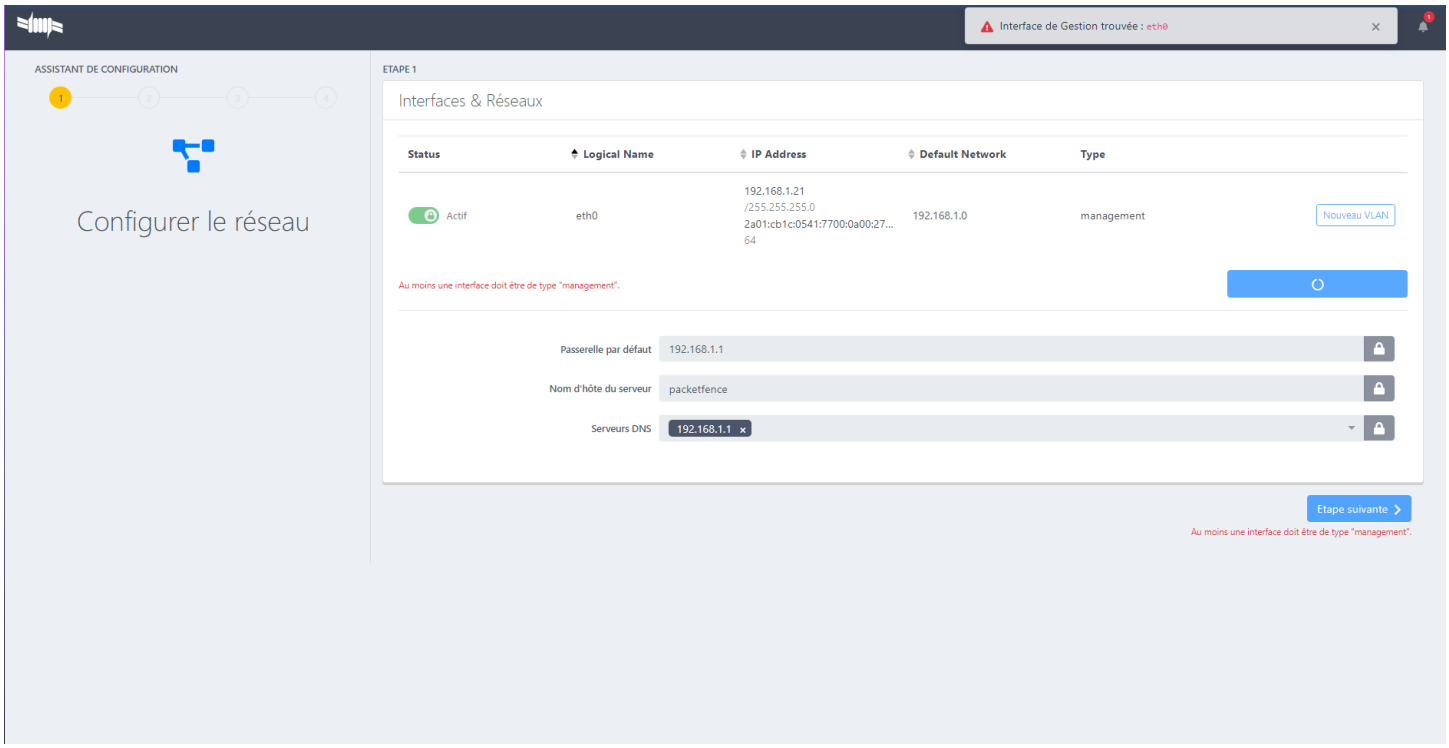
Pour cette dernière partie, nous avons configuré **LLDP**, autrement dit Link Layer Discovery Protocol. C'est un protocole de couche deux standardisé par l'**IEEE** sous le norme 802.1AB. Son seul et unique objectif est de permettre aux périphériques réseau d'annoncer leur présence et de recevoir les informations des autres périphériques connectés physiquement. Le protocole étant standardisé, il est compatible avec de nombreux équipements différents permettant d'utiliser le protocole même avec des commutateurs de marque différentes. LLDP permet la découverte des voisins à travers l'échange de trames de découverte. Ces trames sont envoyées à intervalles régulières pour garder à jour le voisinage de chaque périphérique. Elles contiennent des informations diverses comme le nom de l'appareil ou sur quel port est-il connecté. Les informations sont ensuite stockées dans une base de données locale à l'équipement réseau et y restent un temps limité.

Pour la configuration du port, j'ai configuré dans un premier temps les informations qui seront véhiculées dans les trames LLDP à savoir une description du système de l'appareil, les capacités du système et l'adresse de gestion du commutateur. J'ai activé les notification afin que d'alerter les changements de topologies réseau. Les deux dernières commandes elles permettent respectivement d'activer le protocole LLDP mais pour les équipements reliés aux médias notamment pour la voix sur **IP** (**VoIP**). La seconde commande elle permet l'envoi de notifications en cas de changement de configuration dans des dispositifs liés aux médias.

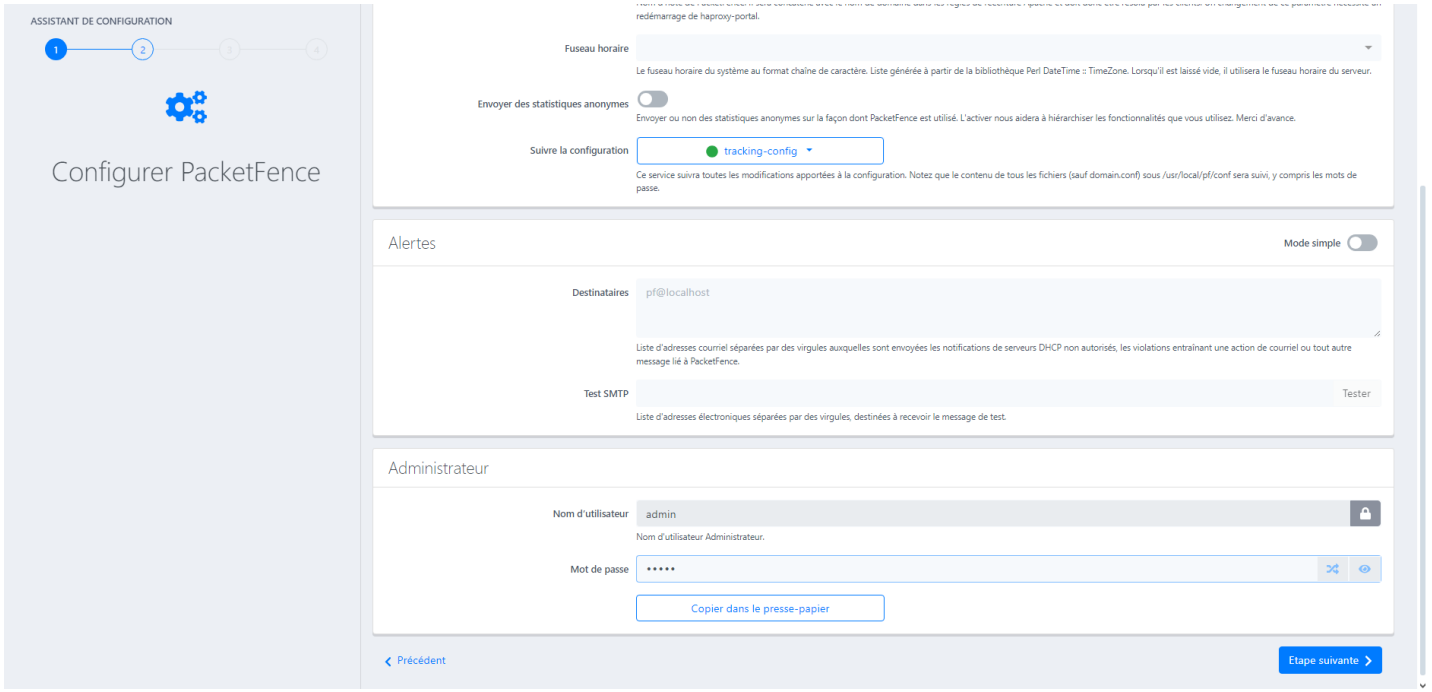
Pour finir, il ne reste plus qu'à configurer PacketFence afin de pouvoir finalement activer l'authentification lorsque l'on souhaite entrer sur le réseau.

3.2.4 Configuration et fonctionnement de PacketFence

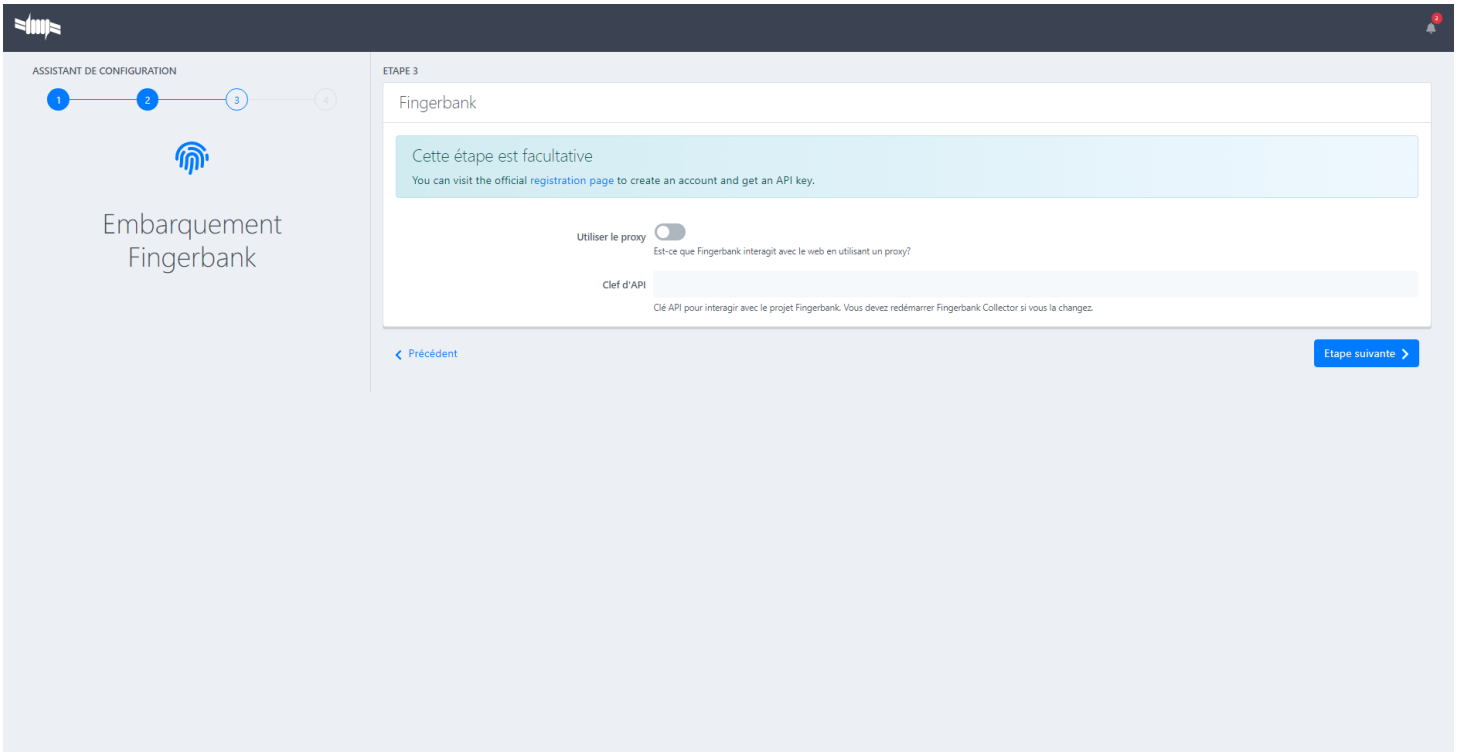
La configuration de PacketFence se fait uniquement via l'interface web. Lorsque l'on installe PacketFence, le port 1443 est ouvert et attend une connexion pour accéder à la configuration de PacketFence. La page de configuration nous permet d'annoncer en premier lieu une interface de management, c'est-à-dire l'interface de connexion par laquelle toutes les informations vont transiter. Cette interface doit être connectée au switch qui accueillera les appareils souhaitant s'authentifier et se connecter. Il y a ensuite 3 étapes qui demandent respectivement la configuration de la base de données de PacketFence en demandant notamment un mot de passe, un nom de domaine mais également nom d'hôte, une clé **API** Fingerbank dont nous n'avons pas besoin dans notre cas car nous ne faisons pas de l'IoT et finalement un récapitulatif de toute la configuration entrée pour vérifier ce que nous avons mis.



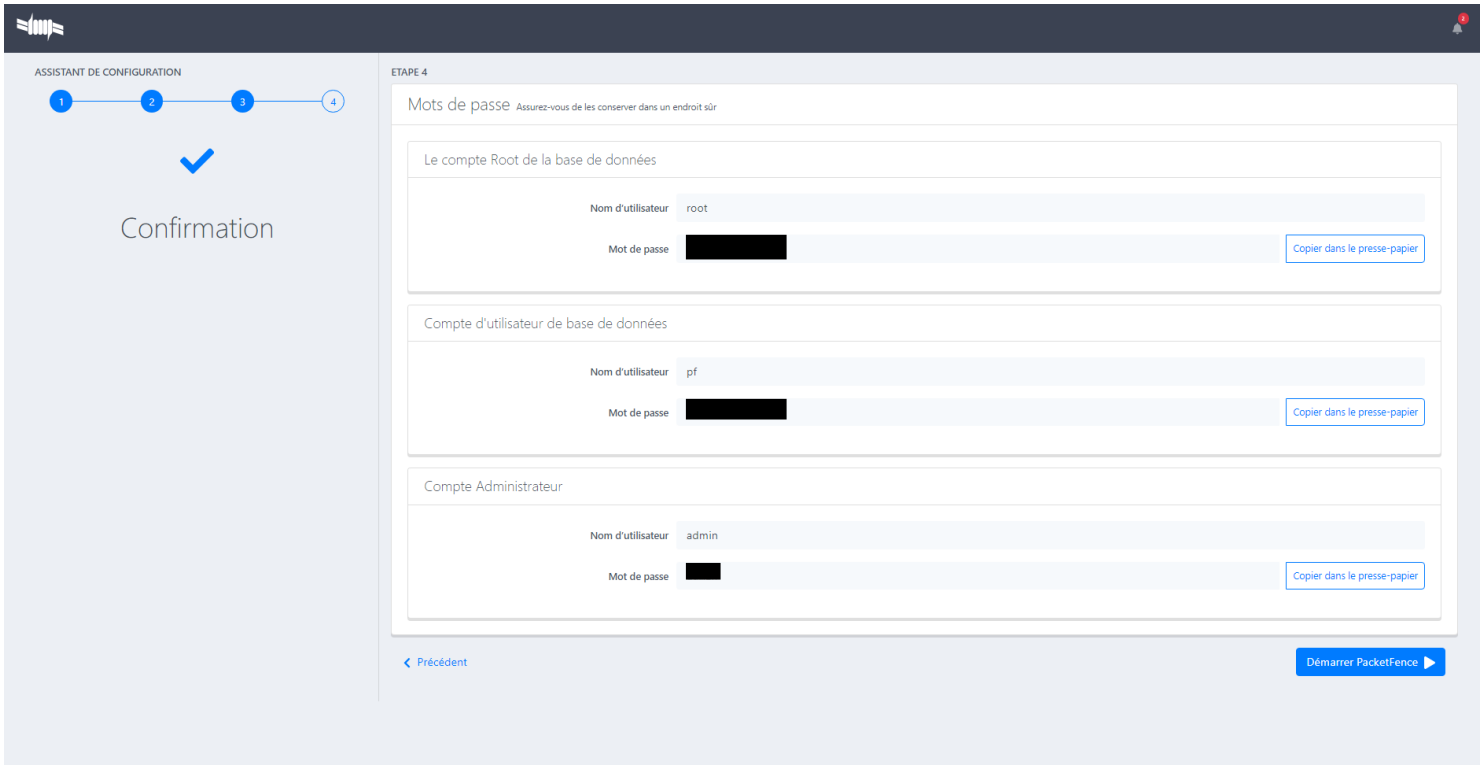
Etape n°1 de la configuration de PacketFence



Etape n°2 de la configuration de PacketFence

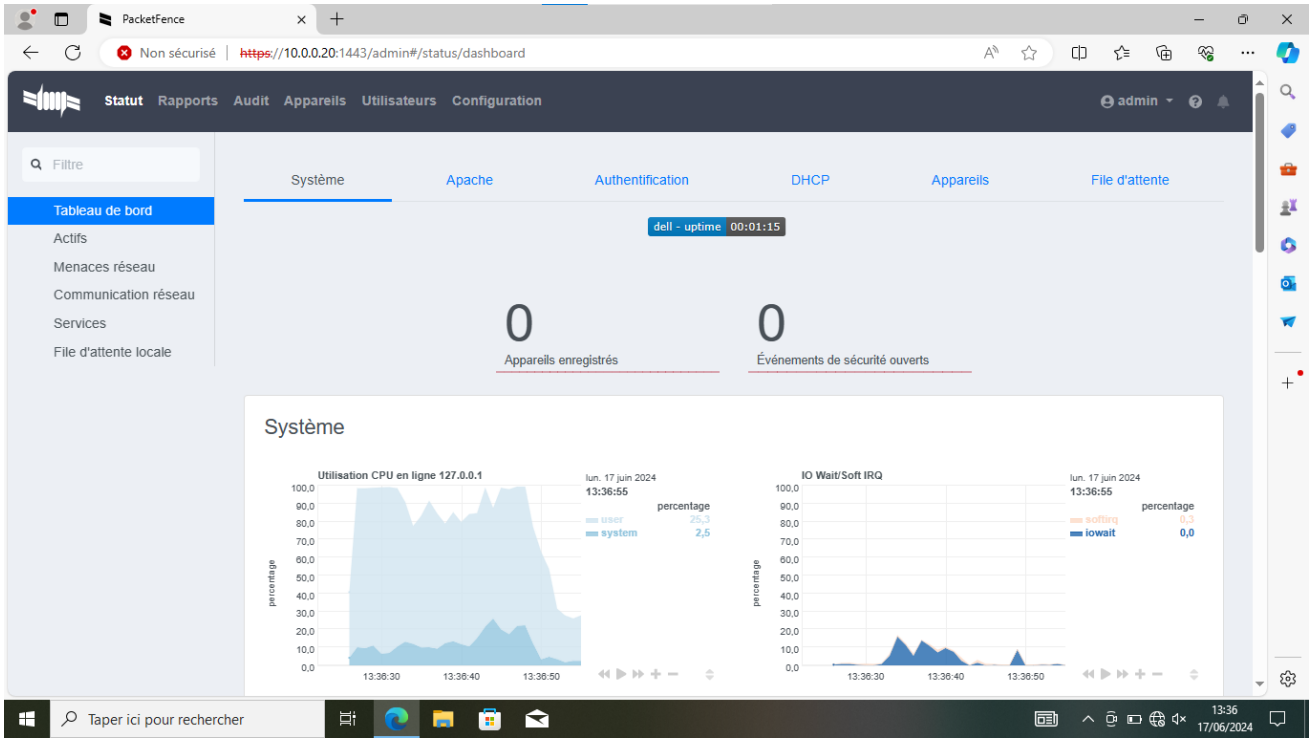


Etape n°3 de la configuration de PacketFence



Etape n°4 de la configuration de PacketFence

Une fois la pré-configuration réalisée, nous pouvons accéder à l'interface d'accueil en entrant notre identifiant et notre mot de passe administrateur.

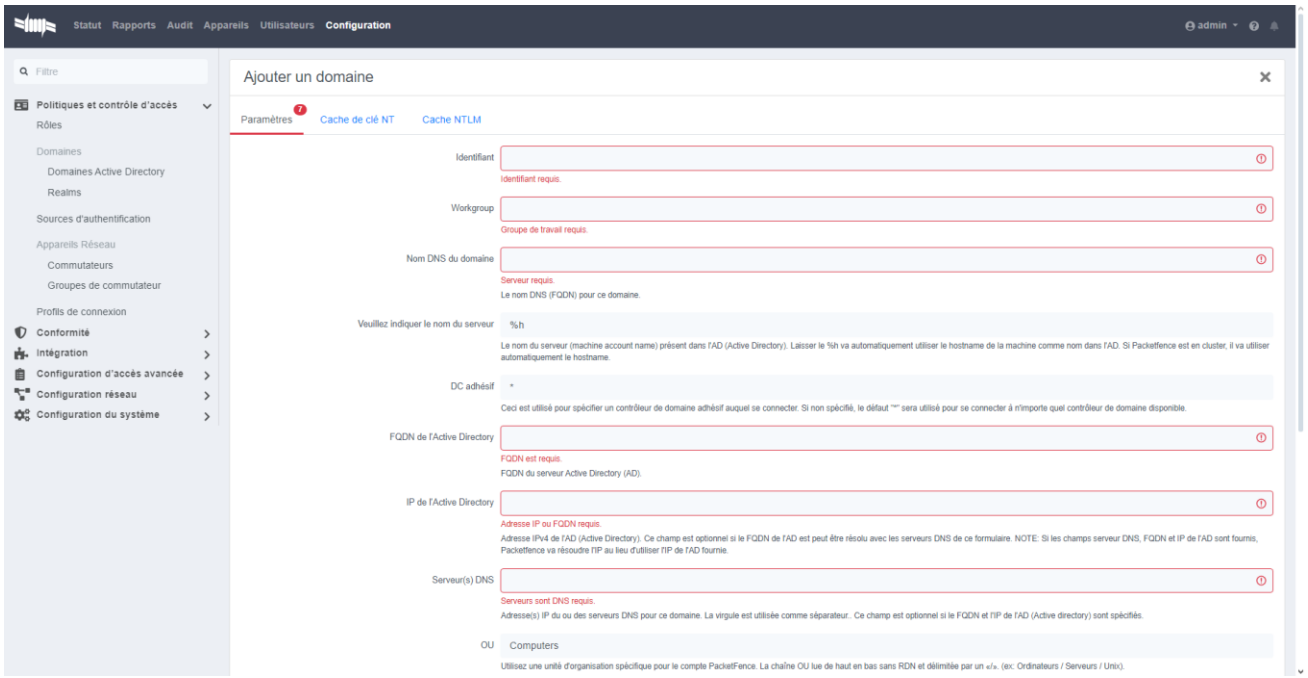


Page d'accueil de PacketFence

Cette page d'accueil nous fournit diverses informations utiles comme l'utilisation des ressources matérielles de la machine, l'affluence du trafic et d'autres informations.

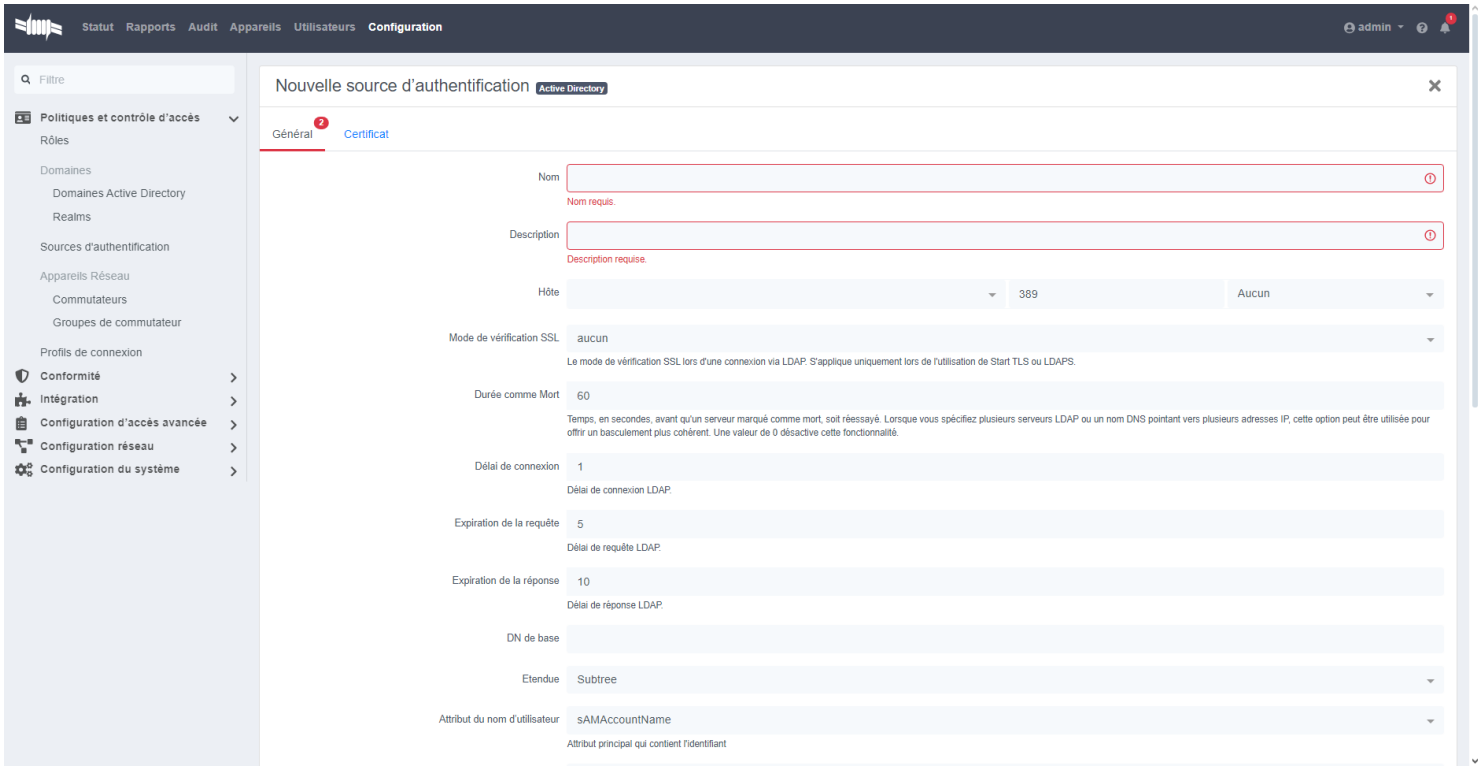
Dans l'onglet configuration, on retrouvera les différents paramètres qui sont configurables sur PacketFence.

Dans un premier temps, il faut ajouter PacketFence au domaine AD. Ceci permet à PacketFence d'accéder au domaine et d'avoir notamment accès au groupe que j'ai créé précédemment avec les 4 utilisateurs.



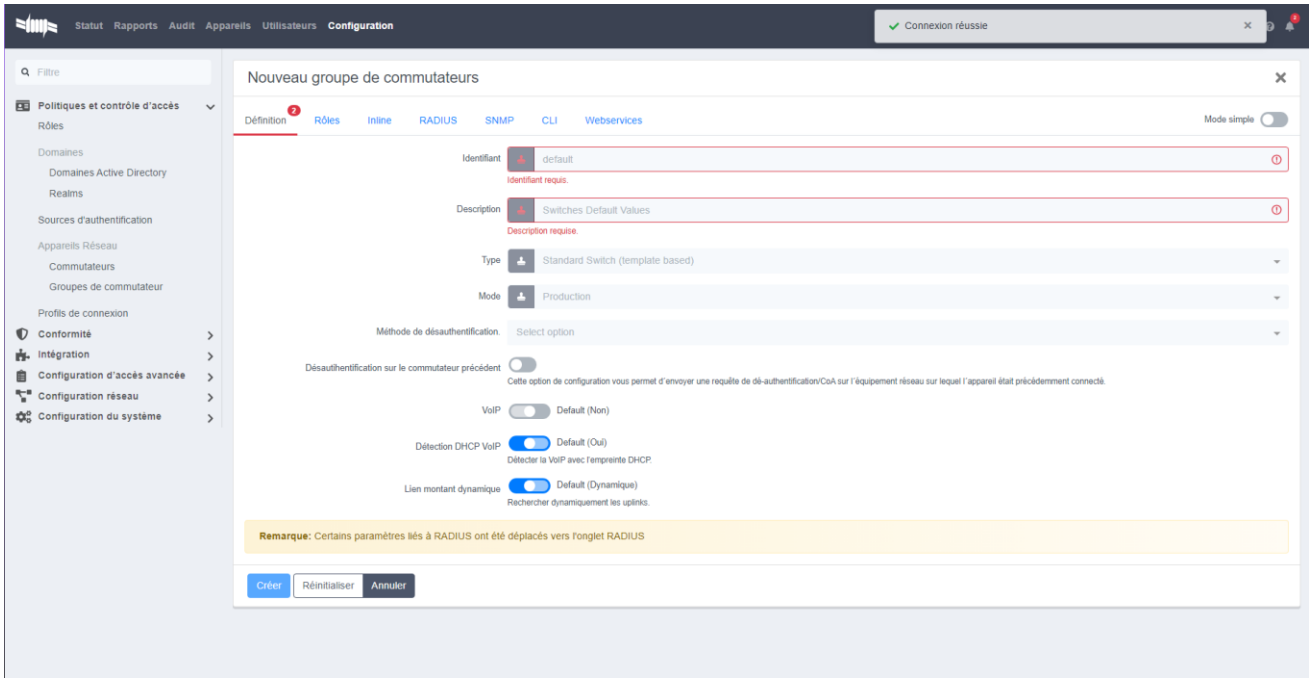
Page de configuration pour ajouter un domaine à PacketFence

Pour la seconde étape de la configuration, il faut ajouter une source d'authentification. Celle-ci va permettre de spécifier à PacketFence où il doit envoyer les demandes pour autoriser ou refuser les tentatives d'authentification. On configure la source d'authentification avec un Active Directory car c'est ce serveur qui centralise tout.



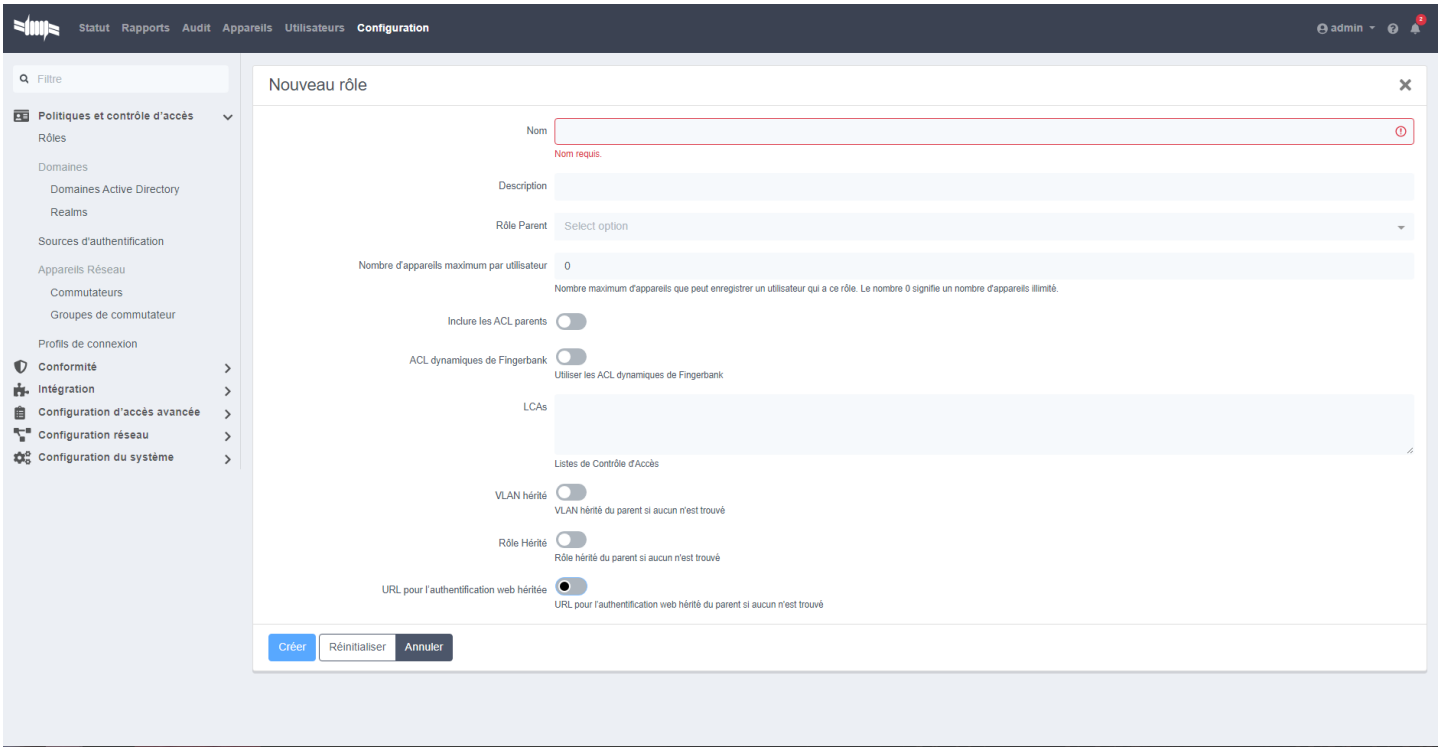
Page de configuration pour ajouter une source d'authentification dans PacketFence

Pour la suite de la configuration, nous allons configurer l'accès au commutateur depuis PacketFence afin qu'il identifie où envoyer les informations concernant la tentative d'authentification. Par la suite le commutateur saura avec les informations reçues accepter ou non dans un premier temps la connexion puis placer l'appareil dans le bon VLAN et le bon réseau de ce fait. Pour des raisons de simplicité et d'évolutivité pour le futur, il est conseillé de créer un groupe de commutateurs permettant après de venir l'agrémenter si l'on rajoute un commutateur dans le réseau.



Page de configuration pour ajouter un groupe de commutateurs dans PacketFence

Pour finaliser notre configuration sur PacketFence, nous devons mettre en place des rôles qui seront attribués par PacketFence pour administrer et classer chaque appareil qui se connecte. Ce rôle attribué permet d'attribuer celui qui l'a à un VLAN en particulier et pendant une durée déterminée. Il est également possible de fixer un nombre maximum d'utilisateurs qui possèdent le rôle en simultané.



Page de configuration pour ajouter un nouveau rôle dans PacketFence

A l'issue de cette configuration, nous pouvons donc nous connecter à travers une machine qui sera authentifiée puis l'utilisateur à son tour pour accéder au réseau dont il a besoin. A côté de ce projet, j'ai eu l'occasion de réaliser des missions annexes m'offrant des opportunités d'apprendre plus de choses différentes.

4/ Missions annexes

En parallèle de mon projet sur PacketFence, j'ai pu effectuer des missions annexes qui m'ont permis d'élargir mes compétences.

4.1 Configuration de commutateurs

La première mission annexe que j'ai pu réaliser a été de configurer des commutateurs afin de les envoyer en production par la suite. Dans ce genre de cas de figure, on récupère une base de fichier de configuration sur lequel on souhaite démarrer notre configuration. On effectue ensuite nos modifications sur le fichier brut. Avant de copier et coller l'intégralité du fichier dans un terminal sur notre commutateur.

L'objectif derrière cette manipulation réside uniquement dans le fait de gagner du temps. Ces commutateurs ne nécessitaient tous la même configuration globale. Quasiment uniquement leur adresse IP devait être modifiée.

Parmi ces commutateurs, j'ai pu découvrir une fonctionnalité très utilisée car très utile : le stacking. Cette fonctionnalité a pour objectif de faire fonctionner deux commutateurs ou plus ensemble. Ainsi ils ne représentent plus qu'un seul commutateur permettant de multiplier le nombre de ports par exemple. Ils partagent le même fichier de configuration offrant donc une supervision des deux commutateur simplifiée. Lorsque que deux commutateurs sont mis en stacking, nous devons leur attribuer un numéro de stack commençant à un pour le premier. Ce numéro s'affiche alors dans la configuration des ports : pour un commutateur avec le numéro un, son premier port aura pour identifiant Gigabit Ethernet 1/0/1 et pour un commutateur avec le numéro deux, son premier port aura pour identifiant Gigabit Ethernet 2/0/1. Le stacking ne peut néanmoins être effectué uniquement sur des commutateurs qui possèdent le même firmware, ou autrement dit qui possèdent la même version de leur logiciel. Autrement, il faut mettre à jour ou rétrograder l'un des deux afin de les placer au même niveau.

4.2 Configuration d'un domaine Active Directory

La seconde mission annexe qui m'a été attribué est de configurer et d'ajouter un ordinateur dans un domaine Active Directory. J'ai profité de cette mission annexe pour l'implémenter dans mon projet car j'utilisais déjà un serveur Active Directory avec PacketFence. Ajouter un ordinateur dans un domaine Active Directory permet diverses choses notamment une gestion centralisé depuis le serveur AD et une sécurité améliorée avec la mise en place de **GPOs** (Group Policy Object) qui permettent la mise en place de règles de contrôle et de sécurité afin de gérer les machines et les utilisateurs d'un domaine AD. Ces GPOs se configurent par les administrateurs et les personnes autorisées.

Lors de la réalisation de cette mission j'ai pu observer des erreurs potentielles qui peuvent pour certaines coûter la réinitialisation de la machine où le serveur se situe. Malgré ces erreurs, j'ai pu recommencer et apprendre où se situaient mes erreurs.

5/ Conclusion

Ce stage de 10 semaines a été d'une très grande richesse pour ma formation professionnelle. J'ai su développer mes compétences techniques et de savoir-être. J'ai apprécié travailler au sein du CINaM aux côtés de mon responsable Mohammed KHABZAOUI et de mes collègues de travail Fabien ROSIER et Saad CHRIFI-ALAOUI. Les échanges que j'ai pu avoir avec chacun d'entre eux ont été très précieux pour mon projet professionnel. J'ai pu l'affiner et être plus déterminé dans la poursuite de mes études.

L'étude de cas qui m'a été confiée a permis de mieux comprendre les enjeux qui se tiennent autour de la cybersécurité de nos jours et de mieux comprendre la solution libre qu'est PacketFence. Elle m'a permis d'approfondir mes connaissances sur la gestion d'un serveur Windows, d'Active Directory mais également sur la gestion d'un NAC. Les découvertes sur la norme 802.1X ont été très précieuses car elles s'inscrivent dans mon projet professionnel de travailler dans le monde de la cybersécurité.

Je suis également monté en compétences sur le plan du savoir-être. Le besoin de faire des petits rapports à mon responsable et d'être le plus concis et clair possible m'a été d'une grande aide. Notamment pour demander de l'aide, il est nécessaire d'être clair sur notre demande et de savoir bien expliquer le contexte dans lequel on se trouve pour aider notre interlocuteur à nous apporter la meilleure aide possible.

Ce stage a été très intéressant dans son ensemble en m'offrant une vision complète du travail en entreprise. Concernant mon projet professionnel, j'ai désormais pour objectif de poursuivre mes études dans une école d'ingénieur avec l'envie d'en apprendre toujours plus sur le domaine des réseaux et de la cybersécurité.

Le stage m'a également préparé à appréhender l'alternance que je vais effectuer lors de mon entrée en troisième année de BUT avec pour objectif de valider mon diplôme. Je suis donc très enthousiaste et optimiste à l'idée d'entrer dans la dernière année de mon BUT.

6 / Remerciements

Au terme de ces dix semaines de stage, je tiens à exprimer ma gratitude et présenter mes remerciements à toutes les personnes qui ont contribué de près ou de loin au bon déroulement et à la réussite de mon stage.

En premier lieu, je souhaiterais remercier le laboratoire du CINaM ainsi que tous les membres présents qui m'ont accueilli et mis en confiance au quotidien. J'ai pu évoluer au sein d'un organisme réputé ce qui m'a fourni un cadre de travail très confortable ainsi que la possibilité de découvrir et apprendre tout en restant en adéquation avec ma formation dans le domaine des Réseaux et de la Cybersécurité.

Je voudrais remercier Valérie JUVENAL pour l'aide qu'elle a su me fournir afin d'obtenir et de débuter mon stage dans les meilleures conditions possibles.

J'aimerais également remercier Fabien ROSIER et Saad CHRIFI-ALAOUI avec qui j'ai eu l'occasion de travailler en étroite collaboration et qui ont su m'accompagner dans mon apprentissage tout au long de mon stage. Les discussions partagées avec eux ont été très intéressantes et pleines de conseils professionnels et personnels qui m'accompagneront tout au long de ma carrière.

Je tiens ensuite à remercier grandement mon professeur référent Tin NGUYEN qui m'a accompagné tout au long de mon stage. J'ai pu bénéficier de ses précieux conseils qui m'ont mené vers la réussite de mon stage et de mon projet.

Finalement, j'aimerais sincèrement remercier Mohammed KHABZAOUI, mon maître de stage qui m'a accordé sa confiance pour ces 10 semaines de stage et a permis la réalisation de ce stage. Je tiens aussi à le remercier pour l'expérience que j'ai su acquérir à travers les différentes missions proposées. Je souhaiterais enfin le remercier pour sa disponibilité, sa bienveillance ainsi que son implication qu'il a su avoir dans l'objectif que ce stage soit une réussite totale autant pour moi que pour lui également.

7 / Glossaire

BUT, Bachelor Universitaire Technologique
CINaM, Centre Interdisciplinaire de Nanoscience de Marseille
MAC, Media Access Control
RADIUS, Remote Authentication Dial-In User Service
LDAP, Lightweight Directory Access Protocol
CNRS, Centre National de la Recherche Scientifique
AMU, Aix-Marseille Université
SAé, Situation d'apprentissage et d'évaluation
HPE, Hewlett Packard Enterprise
NAC, Network Access Control
AAA, Authentication, Authorization, Accounting
NPS, Network Policy Server
AD, Active Directory
macOS, système d'exploitation des ordinateurs de la marque Apple
Linux, système d'exploitation open source de type Unix
VLAN, Virtual Local Area Network
LLDP, Link Layer Discovery Protocol
IEEE, Institute of Electrical and Electronics Engineers
IP, Internet Protocol
VoIP, Voice over Internet Protocol
API, Application Programming Interface
GPO, Group Policy Object

8 / Sitographie

https://www.cinam.univ-mrs.fr/cinam/

https://www.packetfence.org

https://www.packetfence.org/doc/PacketFence_Network_Devices_Configuration_Guide.html#_hp

https://techhub.hpe.com/eginfolib/networking/docs/switches/WB/15-18/5998-8156_wb_2926_atmg/content/ch06s02.html

https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

https://freeradius.org