MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE
UNIVERSITE ABDELHAMID IBN BADIS MOSTAGANEM
Faculté des Sciences Exactes & de l'Informatique
Département de Mathématiques et d'Informatique
Filière Informatique

MEMOIRE DE FIN D'ETUDES

Pour l'Obtention du Diplôme de Master professionnalisant en Réseaux et Systèmes

La mise en place et la gestion d'un réseau informatique au sein de la FSEI

Présenté par :

- Gharbi Mohamed

Encadrée par :

- Dr.ROUKH Amine

Année universitaire 2018/2019

Dédicaces

Je dédie ce mémoire :

A mes très chers parents, qui ont toujours été là pour moi, « Vous avez tout sacrifié pour vos enfants n'épargnant ni santé ni efforts. Vous avez donné un magnifique modèle de labeur et de persévérance. Je suis redevable d'une éducation dont je suis fiers ».

Nous voudrions exprimer nos reconnaissances envers les amis et collègues qui nous ont apporté leur support moral et intellectuel tout au long de notre démarche.

Remerciements

Je tiens tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui m'a

Donné la force, la foi, et la patience d'accomplir ce Modeste travail.

En second lieu, je tiens à remercier mon encadrant DR. Amine ROUKH, son précieux

Conseil et son aide durant toute la période de travail.

Mes remerciements vont également à mes chers parents, que nulle dédicace ne peut exprimer

Mes sincères sentiments, pour leur patience illimitée, le

En témoignage de mon profond amour et respect pour leurs grands sacrifices.

Mes vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à ma recherche en acceptant d'examiner mon travail Et de l'enrichir par leurs propositions Enfin, je dis souvent que le trajet est aussi important que la destination. Cette dernière année m'a permis de bien comprendre la signification de cette phrase toute simple. Ce parcours, en effet, ne s'est pas réalisé sans défis et sans soulever de nombreuses questions pour

Lesquelles les réponses nécessitent de longues heures de travail

Résumé :

L'architecture représente la structure générale inhérente à un système informatique, et plus particulièrement l'organisation des différents éléments, que ceux-ci soient de type matériel ou logiciel. L'université des sciences exactes et de l'informatique de Mostaganem (FSEI) met à leur disposition son réseau qui est alors à la merci de tout genre d'utilisateurs! Pour améliorer ce réseau, une idée serait d'acquérir un mécanisme de conception qui soit à la fois robuste et fiable pour le réseau. L'objectif de notre travail consiste à proposer une architecteur réseau robuste, tolérante, flexible et fiable pour l'université FSEI, pour cela nous avons procédé à une étude de l'architecture actuelle, ainsi que les dispositifs d'interconnexion mis en place. Ce qui nous a permis de la critiquer et de suggérer des solutions et de choisir la technologie la plus appropriée pour répondre aux besoins de l'université afin de proposer une nouvelle architecture réseau qui donne une meilleure fluidité pour le trafic ainsi que sa fiabilité.

Mots clés : architecture réseau, Réseau de campus, VLANs, Pfsense.

Abstract :

The architecture represents the general structure inherent to a computer system, and more particularly the organization of the various elements, whether these are of hardware or software type. The university of the exact sciences and computer science of Mostaganem (FSEI) puts at their disposal its network which is then at the mercy of any kind of users! To improve this network, one idea would be to acquire a design mechanism that is both robust and reliable for the network. The objective of our work is to propose a robust, tolerant, flexible and reliable network architect for the FSEI University, for this we carried out a study of the current architecture, as well as the interconnection devices put in place. This allowed us to criticize and suggest solutions and choose the most appropriate technology to meet the University's needs in order to propose a new network architecture that provides a better flow for traffic and reliability.

Keywords: Network Architecture, Campus Network, VLANs, Pfsense.

Liste des figures

Liste des tableaux

Liste des abréviations

Abréviation	Expression Complète	Page
PAN	Personal Area Network	2
LAN	Local Area Network	3
HAN	Home Area Network	3
SAN	Storage Area Network	3
CAN	Campus Area Network	3
MAN	Metropolitan Area Network	4
WAN	Wide Area Network	4
VPN	Virtual Private Network	4
GAN	Global Area Network	5
STP	Shielded Twisted Pair	5
FTP	Foiled Twisted Pair	5
SFTP	Shielded Foiled Twisted Pair	5
SSTP	Shielded and Shielded Twisted Pair	5
IEEE	L'Institute of Electrical and Electronics Engineers	7
MAC	Media Access Control	8
CSMA/CD	Carrier Sense Multiple Access/Collision Detection	11
MAU	Multi Station Access Unit	11
FDDI	Fiber Distributed Data Interface	11
ITU	l'International Telecommunication Union	12
ISO	International Organization for Standardization	12
OSI	Open Systems Interconnection	12
RFC	Requests For Comments	13
TCP	Transmission Control Protocol	13

Sommaire

Sommaire

Sommaire

Introduction générale

Le besoin d'échanger des données se faisait sentir juste après l'apparition des ordinateurs, puis l'homme eut l'idée de les relier entre eux, c'est là où apparait le concept des réseaux informatiques. Les réseaux se sont développés pour pouvoir répondre à des exigences de communication entre systèmes terminaux très variés. Ils nécessitent la mise en œuvre de nombreux protocoles et fonctionnalités pour pouvoir rester évolutifs et être administrés sans qu'il soit nécessaire de recourir en permanence à des interventions manuelles. Les réseaux de grande taille peuvent se composer des réseaux campus, qui comprennent les utilisateurs connectés localement et des réseaux étendus (WAN) qui relient des campus.

La conception d'un réseau peut se révéler une tâche ardue. Pour que le réseau soit fiable et capable d'évoluer, nous devons garder à l'esprit que chacun des principaux composants précités possède ses exigences propres en matière de conception. Il est clair que la mise en place d'un réseau fait intervenir des environnements de plus en plus complexes, impliquant de nombreux types de supports de transmission, de protocoles et d'interconnexion à des réseaux. Une approche prudente peut néanmoins nous aider à éliminer une partie des difficultés liées à l'extension d'un réseau au fur et à mesure de son évolution.

Notre objectif consiste justement à gérer et mettre en place un réseau informatique de campus fiable au sein de la FSEI (faculté des sciences exactes et informatique de Mostaganem) afin d'assurer l'échange des informations. Un réseau flexible, robuste et interopérable qui répond au besoin de la faculté et qui facilite la connectivité entre les différentes départements afin de partager des données et d'utiliser les différentes ressources.

Nous examinons ensemble les différents chapitres qui composent ce mémoire et la démarche que nous adoptée pour traiter notre sujet. Notre rapport se subdivise en trois principaux chapitres :

Le premier chapitre aborde les généralités sur les réseaux informatiques dont la notion de la topologie réseau, qui est la description généralement schématique de l'agencement du réseau. Et l'architecture réseau et l'interconnexion. Il s'agit en particulier de comprendre les différences essentielles entre commutateur et routeur et de comprendre globalement le rôle des composants d'interconnexion.

Dans le deuxième chapitre, nous allons présenter l'université de Mostaganem où nous citrons l'architecture réseau actuel et ses inconvénients, ainsi nous passerons en revue les problèmes les plus couramment rencontrés pour son fonctionnement, où le but est de trouver une solution de conception optimisée d'une architecture plus rapide pour évoluer ce réseau afin qu'il soit fiable au niveau de la rapidité d'échange des données et tolérant au panne pour qu'il soit disponible à tous moment.

Le dernier chapitre nous présenterons la solution mise en place avec l'explication de sa réalisation ainsi que les tests de validation pour nous assurer que notre objectif a bien été atteint.

1. Introduction :

Les réseaux sont nés du besoin d'échanger des informations de manière simple et rapide entre des machines. En d'autres termes, les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux, et enfin des machines terminales, telles que les stations de travail à leur serveur [1].

Dans un premier temps, ces communications étaient uniquement destinées au transport des données informatiques, mais aujourd'hui avec l'intégration de la voix et de la vidéo, elles ne se limitent plus aux données mêmes si cela ne va pas sans difficulté.

Avant de nous attaquer aux infrastructures réseaux, reprenons quelques notions théoriques de base sur les réseaux informatiques en général.

2. Définition d'un réseau :

Un réseau a pour fonction de transporter les données d'une machine terminale vers une autre machine terminale. Pour ce faire, une série d'équipements et de processus sont nécessaires, allant de l'environnement matériel, utilisant des câbles terrestres ou des ondes radio, jusqu'à l'environnement logiciel constitué de protocoles, c'est-à-dire de règles permettant de décider de la façon de traiter les données transportées.

3. Définition de réseau informatique :

Un réseau informatique est l'interconnexion d'au moins deux ou plusieurs ordinateurs en vue d'échanger, de partager des données ou des ressources. En d'autre terme c'est une infrastructure de communication reliant des équipements informatiques *(*ordinateur, concentrateur, commutateur, routeur, imprimante...*)* permettant de partagé des ressources communes. Il est caractérisé par un aspect physique (câble véhiculant des signaux électriques) et un aspect logique (les logiciels qui réalisent les protocoles).

3.1. Les types de réseaux informatiques :

3.1.1. Réseau à l'échelle nanométrique :

Un réseau de communication à l'échelle nanométrique a des composants clés mis en œuvre à l'échelle nanométrique, y compris des supports de messages, et exploite des principes physiques différents des mécanismes de communication à l'échelle macroscopique. La communication à l'échelle nanométrique étend la communication à de très petits capteurs et actionneurs, comme ceux que l'on trouve dans les systèmes biologiques, et tend également à fonctionner dans des environnements trop difficiles pour une communication classique. [2]

3.1.2. Le réseau personnel (PAN) :

Un réseau personnel (PAN) est un réseau informatique utilisé pour la communication entre des ordinateurs et différents dispositifs technologiques de l'information proches d'une personne. Les ordinateurs personnels, les imprimantes, les télécopieurs, les téléphones, les

PDA, les scanners et même les consoles de jeux vidéo sont des exemples de périphériques utilisés dans un PAN. Un PAN peut inclure des périphériques câblés et sans fil. La portée d'un PAN s'étend généralement à 10 mètres. [3] Un PAN câblé est généralement construit avec des connexions USB et FireWire, tandis que des technologies telles que les communications Bluetooth et infrarouge forment généralement un PAN sans fil.

3.1.3. Le réseau local (LAN) :

Un réseau local (LAN) est un réseau qui connecte des ordinateurs et des périphériques dans une zone géographique limitée, telle qu'une maison, une école, un immeuble de bureaux ou un groupe de bâtiments rapproché. Chaque ordinateur ou périphérique du réseau est un nœud . Les réseaux locaux câblés sont très probablement basés sur la technologie Ethernet . Les normes plus récentes telles que ITU-T G.hn fournissent également un moyen de créer un réseau local câblé utilisant le câblage existant, tel que des câbles coaxiaux, des lignes téléphoniques et des lignes électriques. [4]

3.1.4. Home area network (HAN) :

Un réseau domestique (HAN) est un réseau local résidentiel utilisé pour la communication entre des périphériques numériques généralement déployés à la maison, généralement un petit nombre d'ordinateurs personnels et d'accessoires, tels que des imprimantes et des périphériques informatiques mobiles. Une fonction importante est le partage de l'accès à Internet, souvent un service à large bande via un fournisseur de télévision par câble ou de ligne d'abonné numérique (DSL). [5]

3.1.5. Réseau de zones de mémorisation (SAN) :

Un réseau de stockage (SAN) est un réseau dédié qui fournit un accès à un stockage de données consolidé au niveau du bloc. Les réseaux de stockage sont principalement utilisés pour rendre les périphériques de stockage, tels que les baies de disques, les bibliothèques de bandes et les librairies optiques, accessibles aux serveurs afin que les périphériques apparaissent comme des périphériques attachés localement au système d'exploitation. Un réseau de stockage possède généralement son propre réseau de périphériques de stockage qui ne sont généralement pas accessibles via le réseau local par d'autres périphériques. [6]

3.1.6. Réseau de campus (CAN) :

Un réseau de campus (CAN) est constitué d'une interconnexion de réseaux locaux dans une zone géographique limitée. Les équipements de réseau (commutateurs, routeurs) et les supports de transmission (fibre optique, installation de cuivre, câblage Cat5 , etc.) sont presque entièrement détenus par le locataire (propriétaire) du campus (entreprise, université, gouvernement, etc.). [7]

Par exemple, un réseau de campus universitaires est susceptible de relier divers bâtiments du campus afin de relier les collèges ou départements universitaires, la bibliothèque et les résidences pour étudiants.

3.1.7. Réseau dorsal :

Un réseau fédérateur fait partie d'une infrastructure de réseau informatique qui fournit un chemin pour l'échange d'informations entre différents réseaux locaux ou sous-réseaux. Une épine dorsale peut relier divers réseaux dans le même bâtiment, dans différents bâtiments ou sur une vaste zone. [8]

Par exemple le réseau fédérateur Internet [9], qui est l'ensemble des réseaux étendus (WAN) et des routeurs centraux qui relient tous les réseaux connectés à Internet.

3.1.8. Le réseau métropolitain (MAN) :

Le réseau métropolitain ou *Metropolitan Area Network* (MAN) est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments distants de quelques dizaines de kilomètres. [10]

3.1.9. Le réseau étendu (WAN) :

Un réseau étendu (WAN) est un réseau informatique qui couvre une grande zone géographique telle qu'une ville, un pays ou même une distance intercontinentale. Un réseau WAN utilise un canal de communication combinant de nombreux types de supports, tels que des lignes téléphoniques, des câbles et des ondes radio. Un réseau étendu utilise souvent des installations de transmission fournies par des entreprises de télécommunication ordinaires, telles que des compagnies de téléphone. Les technologies WAN fonctionnent généralement au niveau des trois couches inférieures du modèle de référence OSI : la couche physique , la couche liaison de données et la couche réseau. [11]

3.1.10. Réseau privé d'entreprise :

Un réseau privé d'entreprise est un réseau créé par une seule organisation pour interconnecter ses bureaux (sites de production, sièges sociaux, bureaux distants, magasins, etc.) afin de pouvoir partager des ressources informatiques.

3.1.11. Réseau privé virtuel (VPN) :

Un réseau privé virtuel (VPN) est un réseau superposé dans lequel certaines des liaisons entre les nœuds sont transportées par des connexions ouvertes ou des circuits virtuels dans un réseau plus important (par exemple, Internet) au lieu de fils physiques. Lorsque cela est le cas, les protocoles de couche de liaison de données du réseau virtuel sont tunnelés via le réseau plus vaste. Une application courante est la sécurité des communications via Internet, mais un VPN n'a pas besoin de fonctions de sécurité explicites, telles que l'authentification ou le cryptage du contenu. Les VPN, par exemple, peuvent être utilisés pour séparer le trafic de différentes communautés d'utilisateurs sur un réseau sous-jacent doté de fonctions de sécurité puissantes.

Le VPN peut offrir des performances optimales ou un accord de niveau de service (SLA) défini entre le client VPN et le fournisseur de services VPN. Généralement, un VPN a une topologie plus complexe que le point à point. [12]

3.1.12. Réseau global (GAN) :

Un réseau global (GAN) est un réseau utilisé pour prendre en charge la téléphonie mobile sur un nombre arbitraire de réseaux locaux sans fil, de zones de couverture par satellite, etc. Le principal défi des communications mobiles consiste à transférer les communications des utilisateurs d'une zone de couverture locale à l'autre. [13]

3.2. Les supports physiques d'interconnexion :

3.2.1. Le câble à paire torsadées :

Un câble à double paire torsadées (Twisted pair câble) décrit un modèle de câblage ou une ligne de transmission qui est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolant. Cette configuration a pour but de maintenir précisément la distance entre le fil et de diminuer la diaphonie. [14]

Ce type de câble est utilisé dans plusieurs cas mais nous nous parlerons dans le cas d'un réseau informatique, la longueur d'un segment de câble qui relie deux équipement ne peut pas dépasser 100m. Il existe cinq types de paire torsadée :

- **Paire torsadée non blindée (UTP en anglais):** dénomination officielle (U/UTP); elle n'est pas entourée d'un blindage protecteur. Ce type de câble est souvent utilisé pour le téléphone et les réseaux informatiques domestiques.
- **Paire torsadée blindée (STP en anglais):** dénomination officielle U/FTP. Chaque paire torsadée est entourée d'une couche conductrice de blindage, ce qui permet une meilleure protection contre les interférences. Elle est fréquemment utilisée dans les réseaux token ring.
- **Paire torsadée écrantée (FTP en anglais) :** officiellement connu sous la dénomination F/UTP. L'ensemble des paires torsadées ont un blindage commun assuré par une feuille d'aluminium, elle est placée entre la gaine extérieure et les quatre paires torsadées. On en fait usage pour le téléphone et les réseaux informatiques.
- **Paire torsadée écrantée et blindée (SFTP en anglais) :** nouvelle dénomination S/FTP. Ce câble est doté d'un double écran commun à toutes les paires.
- **Paire torsadée super blindée (SSTP en anglais) :** nouvellement connu sous la dénomination S/FTP. C'est un câble STP doté en plus d'un écran commun entre la gaine extérieur et les quatre paires.

Figure 1 – Paire Torsadée

3.2.2. Le câble coaxial :

Le câble coaxial est largement utilisé comme moyen de transmission. Ce type de câble est constitué de deux conducteurs concentriques : un conducteur central, le cœur, entouré d'un matériau isolant de forme cylindrique, enveloppé le plus souvent d'une tresse conductrice en cuivre. L'ensemble est enrobé d'une gaine isolante en matière plastique. Le terme coaxial vient du conducteur interne et du blindage externe partageant un axe géométrique. [15]

Il est utilisé pour transporter des signaux électriques à haute fréquence avec de faibles pertes. Il est utilisé dans des applications telles que les lignes téléphoniques principales, les câbles de réseau Internet à large bande , les bus de données informatiques à grande vitesse , le transport de signaux de télévision par câble et la connexion d' émetteurs et de récepteurs radio à leurs antennes .

On distingue deux types de câbles coaxiaux :

- le câble coaxial fin (thin Net) ou 10 base-2 mesure environ 6mm de diamètre, il est en mesure de transporter le signal à une distance de 185 mètres avant que le signal soit atténué.
- Le câble coaxial épais (thick Net) appelé aussi 10 base-5 grâce à la norme Ethernet qui l'emploi, mesure environ 12mm de diamètre, il est en mesure de transporter le signal à une distance de 500 mètres avant que le signal soit atténué.

Remarque : Pour le raccordement des machines avec les câbles coaxiaux, on utilise des connecteurs BNC.

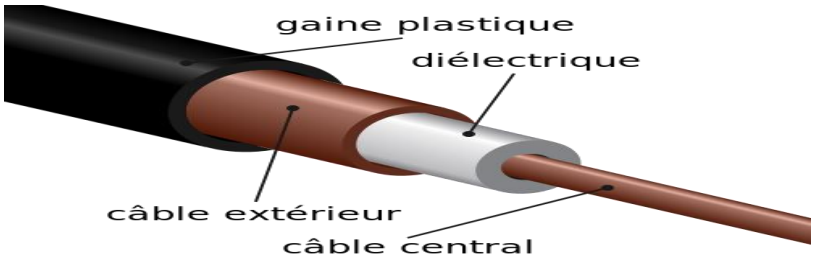

Figure 2 – Câble coaxial.

3.2.3. La Fibre Optique :

Une fibre optique est un fil en verre ou en plastique très fin qui à la propriété d'être un conducteur de la lumière et sert dans la transmission de données avec un débit supérieur à celui des autres supports. Elle est constituée du cœur, d'une gaine optique et d'une enveloppe protectrice. [16]

On distingue deux types de fibre optique :

- **La fibre multimode :** composée d'un cœur de diamètre variant entre 50 et 62.5 microns. Principalement utilisée dans les réseaux locaux, elle ne s'étend pas sur plus de deux kilomètres. Sa fenêtre d'émission est centrée sur 850, 1300 nanomètres. Elle supporte de très larges bandes passantes, offrant un débit pouvant aller jusqu'à 2.4Gbps, aussi elle

peut connecter plus de station que ne le permettent les autres câbles. L'inconvénient est qu'il est onéreux et difficile à installer.

- **La fibre monomode :** elle a un cœur extrêmement fin de diamètre 9 microns. La transmission des données y est assurée par des lasers optiques émettant des longueurs d'onde lumineuses de 1300 à 1550 nanomètres et par des amplificateurs optiques situés à intervalles régulier. C'est celle que l'on utilise sur les liaisons à longue portée car elles peuvent soutenir les hauts débits sur des distances de 600 à 2000 km par contre son câblage est onéreux et difficile à mettre en place.

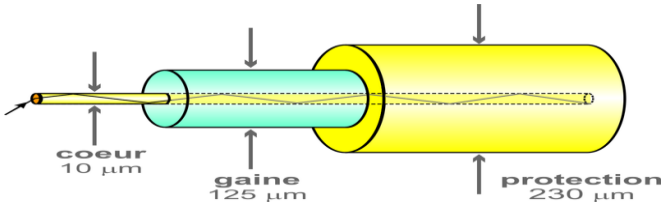

Figure 3 – La fibre optique.

3.2.4. Transmission sans fil :

Le Wi-Fi ou wifi est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11). Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, décodeur Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.

3.3. Les équipements d'interconnexion:

Afin de faciliter le choix entre les différents matériels d'interconnexion ci-dessus, nous allons passer en revue les divers caractéristiques de chacun. Nous allons ainsi préciser dans quelle mesure un matériel plutôt qu'un autre doit être utilisé.

3.3.1. Répéteur :

Un répéteur est un équipement qui permet d'étendre la longueur maximale d'un segment, en amplifiant le signal, en même temps qu'il permet d'interconnecter deux supports physiques différents. [17]

Le but de cet élément est d'augmenter la taille du réseau, il fonctionne au niveau de la couche 1 du modèle OSI. Il est transparent pour les stations de travail car il ne possède pas d'adresse Ethernet. Il offre un débit de 10 Mbits/s ; l'avantage de cet équipement est qu'il ne nécessite pas (ou très peu) d'administration. Par contre il ne diminue pas la charge du réseau, ne filtre pas les collisions, n'augmente pas la bande passante et n'offre pas de possibilité de réseau virtuel (voir figure 5).

Figure 4 – Répéteur.

3.3.2. Hub :

Le hub est un répéteur qui transmet le signal sur plus d'un port d'entrée-sortie. Lorsqu'il reçoit un signal sur un port, il le retransmet sur tous les autres ports. Il présente les mêmes inconvénients que le répéteur. Il assure en fonction annexe une auto-négociation du débit entre 10 et 100 Mbits/s, il est utilisé en extrémité du réseau et doit être couplé en un nombre maximum de 4 entre deux stations de travail (voir figure 6). [17]

Figure 5 – Hub.

3.3.3. Switch :

Aussi appelé commutateur, en général, les stations de travail d'un réseau Ethernet sont connectés directement à lui. Un commutateur relie les hôtes qui sont connectés à un port en lisant l'adresse MAC comprise dans les trames. Intervenant au niveau de la couche 2, il ouvre un circuit virtuel unique entre les nœuds d'origine et de destination, ce qui limite la communication à ces deux ports sans affecter le trafic des autres ports (voir figure 7). [17]

Figure 6 – Switch.

3.3.4. Routeur :

Aussi appelé commutateur de niveau 3 car il y effectue le routage et l'adressage, il permet d'interconnecter deux ou plusieurs réseaux. Possédant les mêmes composants de base qu'un ordinateur, le routeur sélectionne le chemin approprié (au travers de la table de routage) pour diriger les messages vers leurs destinations. Cet équipement est qualifié de fiable car il permet de choisir une autre route en cas de défaillance d'un lien ou d'un routeur sur le trajet qu'empreinte un paquet (voir figure 8). [17]

Figure 7 – Router.

3.3.5. Passerelle :

La passerelle relie des réseaux hétérogènes, elle dispose des fonctions d'adaptation et de conversion de protocoles à travers plusieurs couches de communication jusqu'à la couche application.

On distingue les passerelles de transport qui mettent en relation les flux de données d'un protocole de couche transport, les passerelles d'application qui quant à elles réalisent l'interconnexion entre applications de couches supérieures. [17] Malgré le fait que la passerelle est incontournable dans les grandes organisations, elle nécessite souvent une gestion importante.

3.3.6. Firewall :

Encore appelé pare-feu ou coupe feu, le pare feu c'est un système permettant de protéger un ordinateur des instruisons provenant du réseau. Très souvent pour sa mise en place, le firewall nécessite deux composants essentiels : deux routeurs qui filtrent les paquets ou datagrammes et une passerelle d'application qui renforce la sécurité. En général le filtrage de paquet est géré dans des tables configurées par l'administrateur, ces tables contiennent des listes des sources/destinations qui sont verrouillées et les règles de gestion des paquets arrivant de et allant vers d'autres machines. [17]

3.4. Topologie des réseaux :

La topologie est une façon d'agencer les équipements interconnectés dans un réseau local. La topologie peut comporter deux aspects :

3.4.1. Topologie physique :

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). Correspond à la façon dont les équipements du réseau local sont câblés. Autrement dit c'est la configuration spatiale du réseau.

On distingue généralement les topologies suivantes :

3.4.1.1. Topologie en bus :

Une topologie en bus est l'organisation la plus simple d'un réseau. Les nœuds sont connectés au câble de bus par des lignes de dérivation et des prises. Une ligne de dérivation est une connexion établie entre le périphérique et le câble principal (voir figure 1).

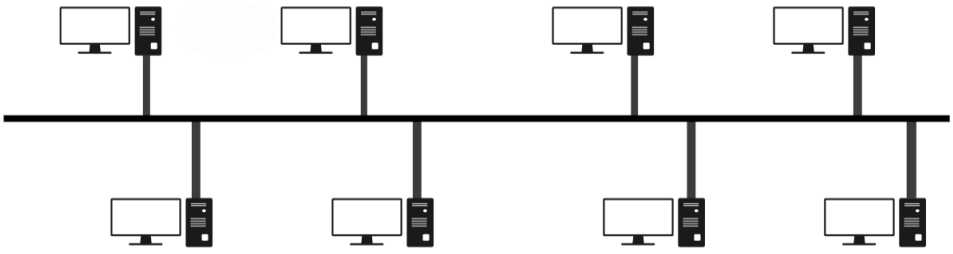

Figure 8 – Topologie en bus.

Les avantages d'une topologie de bus incluent la facilité d'installation. Les câbles dorsaux peuvent être posés le long du chemin le plus efficace, puis connectés aux nœuds par des lignes de chute de différentes longueurs. De cette manière, un bus utilise moins de câblage que les

topologies maillées ou en étoile. Alors que Les inconvénients incluent une reconnexion difficile et une isolation des pannes. De plus, un défaut ou une rupture du câble de bus interrompt toute transmission.

3.4.1.2. Topologie en étoile :

Dans une topologie en étoile, chaque périphérique dispose d'un lien point à point dédié uniquement vers un contrôleur central, généralement appelé concentrateur. Les appareils ne sont pas directement liés les uns aux autres. Contrairement à une topologie maillée, une topologie en étoile n'autorise pas le trafic direct entre les périphériques (voir figure 2).

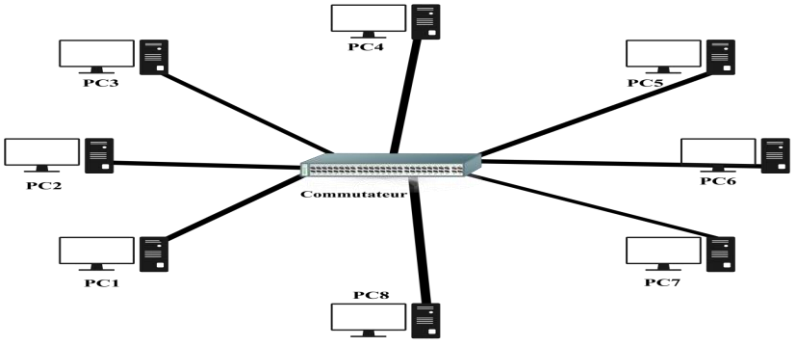

Figure 9 – Topologie en étoile.

L'avantage est que chaque périphérique n'a besoin que d'un lien et d'un port d'E / S pour le connecter à un nombre quelconque d'autres. Ce facteur facilite également l'installation et la reconfiguration. Les autres avantages incluent la robustesse. Si un lien échoue, seul ce lien est affecté. Tous les autres liens restent actifs**.**

3.4.1.3. Topologie en anneau :

Dans une topologie en anneau, chaque périphérique dispose d'une connexion point à point dédiée avec uniquement les deux périphériques de chaque côté. Un signal est transmis le long de l'anneau dans un sens, d'un périphérique à l'autre, jusqu'à ce qu'il atteigne sa destination. Chaque appareil de l'anneau intègre un répéteur.[18] Lorsqu'un appareil reçoit un signal destiné à un autre appareil, son répéteur régénère les bits et les transmet (voir la figure 3).

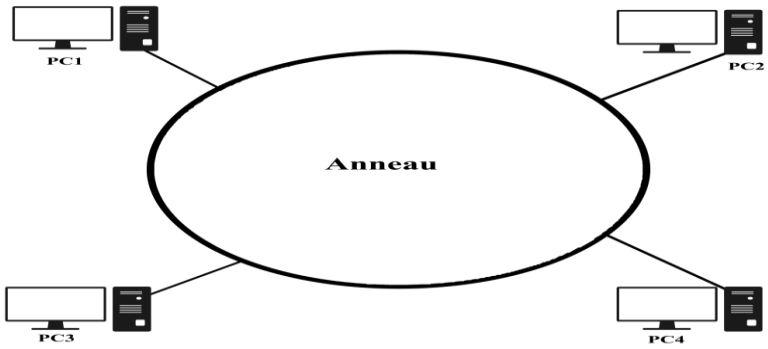

Figure 10 – Topologie en anneau.

3.4.2. Topologie logique :

La topologie logique désigne la manière dont les équipements communiquent en réseau. Dans cette topologie les plus courantes sont les suivantes :

3.4.2.1. Topologie Ethernet :

Ethernet est aujourd'hui l'un des réseaux les plus utilisées en local. Il repose sur une topologie physique en étoile. Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD, ce qui fait qu'il aura une très grande surveillance des données à transmettre pour éviter toute sorte de collision. Par conséquent un poste qui veut émettre doit vérifier si le canal est libre avant d'y émettre.

3.4.2.2. Topologie token ring :

Elle repose sur une topologie physique en Anneau (ring), il utilise la méthode d'accès par jeton (token). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre si un poste veut émettre, il doit attendre jusqu'à ce qu'il ait le jeton ; dans un réseau token ring, chaque nœud du réseau comprend un MAU (Multi Station Access Unit) qui peut recevoir les connexions des postes. Le signal qui circule est régénéré par chaque MAU.

Mettre en place un réseau token ring coûte chers, malgré la panne d'une station MAU provoque le disfonctionnement du réseau.

3.4.2.3. Topologie FDDI :

La technologie LAN FDDI (Fiber Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibre optiques.
Le FDDI est constitué de deux anneaux : un anneau primaire et anneau secondaire. L'anneau secondaire sert à rattraper les erreurs de l'anneau primaire ; le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner.

3.5. Les modèles de réseaux :

3.5.1. Le modèle OSI :

Le modèle d'interconnexion de systèmes ouverts (Open Systems Interconnection) fait l'objet d'une norme qui s'appelle 7498-1:1994 à l'ISO et X.200 à l'ITU (l'International Telecommunication Union) qui couvre tous les aspects des communications réseau. Le modèle OSI a pour objectif de montrer comment faciliter la communication entre différents systèmes sans nécessiter de modification de la logique du matériel et des logiciels sous-jacents. Il se compose de sept couches distinctes mais liées, chacune définissant une partie du processus de déplacement des informations sur un réseau (voir le tableau 1). [19]

3.5.1.1. Les 7 couches du modèle OSI :

Tableau 1 – les sept couches de modèle OSI

Nº des couches	Nom des couches	Définition
Couche 7	Application	Elle ne contient pas les applications utilisateurs, mais

		elle assure la communication, à l'aide de processus, entre les couches inférieures et les applications utilisateurs (transfert de fichiers, courrier électronique).
Couche 6	Présentation	Elle assure la mise en forme des données, la conversion des codes (ASCII, EBCDIC...), si nécessaire, pour délivrer à la couche application un message dans une syntaxe compréhensible. Elle peut aussi assurer le cryptage et la compression des données. C'est donc la première couche non impliquée dans le mécanisme de transfert d'informations.
Couche 5	Session	Elle assure l'échange des données, et la transaction entre deux applications distantes. Elle assure aussi la synchronisation et le séquencement de l'échange par la détection et la reprise de celui-ci en cas d'erreur.
Couche 4	Transport	Elle assure le contrôle du transfert de bout en bout des informations entre les deux systèmes d'extrémités, afin de rendre le transport transparent pour les couches supérieures. Elle assure le découpage des messages en paquets pour le compte de la couche réseau et les reconstitue pour les couches supérieures.
Couche 3	Réseau	Elle assure l'acheminement, le routage (choix du chemin à parcourir à partir des adresses), des blocs de données entre les deux systèmes d'extrémités, à travers des relais. Et elle définit la taille de ses blocs.
Couche 2	Liaison	Elle assure, le maintient de la connexion logique, le transfert des blocs de données (les trames et les paquets), la détection et la correction des erreurs dans ceux-ci.
Couche 1	Physique	Couche 1 Physique Elle assure l'établissement et le maintient de la liaison physique. Elle comprend donc les spécifications mécaniques (connecteurs) et les spécifications électriques (niveaux de tension).

3.5.2. Le modèle TCP/IP :

Le protocole TCP/IP a été inventé par **Vinton G. Cerf** et **Bob Kahn,** Il est décrit dans la **RFC1122**, qui date de 1989, il est utilisé sur le réseau Internet pour transmettre des données entre deux machines (protocole de transport) (voir le tableau 2).

- Le TCP prend à sa charge l'ouverture et le contrôle de la liaison entre deux ordinateurs.
- Le protocole d'adressage IP assure le routage des paquets de données. **[20]**

Tableau 2 – les couches de modèle TCP/IP

Nom des couches	Définition
Application	Le modèle TCP/IP n'a pas besoin des couches Session ni Présentation**.** La couche application contient des protocoles haut-niveaux : FTP pour le transfert de fichiers, SMTP pour les mails, HTTP pour le WWW, DNS pour les noms de domaine...
Transport	Tout comme pour le modèle OSI, la couche de transport permet aux hôtes source et destination de faire une conversation.
Internet	Le but de cette couche est de permettre d'injecter des paquets dans n'importe quel réseau et de faire en sorte qu'ils arrivent à destination**.**
Hôte réseau	Couche assez sombre, le modèle TCP/IP en dit peu sur cette couche excepté que l'hôte doit se connecter au réseau depuis certains protocoles de sorte à pouvoir envoyer des paquets IP à travers le réseau.

3.6. Les architectures réseaux :

3.6.1. Architecture centralisée :

C'est l'organisation la plus classique de l'administration, dans laquelle un seul manager (gestionnaire) contrôle toutes les ressources du réseau et les équipements distribués dans un réseau de télécommunication. Cette architecture présente l'avantage d'être facile à concevoir, mais en contrepartie elle s'avère inefficace dans le cas de réseaux étendus.

3.6.2. Architecture plate :

- Les postes dialoguent à travers 1 équipement (concentrateur, routeur,…).
- Plusieurs équipements peuvent être interconnectés. Ils utilisent le même protocole et le même débit. Les postes se partagent la bande passante.

3.6.3. Architecture hiérarchique :

- Pour permettre des dialogues simultanés, on fractionne les réseaux à plat en sous réseaux.
- Les sous réseaux sont reliés par des équipements d'interconnexion (routeurs, commutateurs.
- Les serveurs peuvent être utilement reliés aux routeurs pour être accessibles directement par chaque sous- réseau.

3.7. Réseau de campus :

3.7.1. Définition :

Un réseau de campus est un réseau propriété de LAN ou un ensemble de réseaux locaux interconnectés servant une entreprise, Le réseau de campus est généralement la partie de l'infrastructure réseau de l'entreprise qui fournit aux utilisateurs finaux et aux périphériques répartis sur un seul emplacement géographique, un accès aux services et ressources de communication réseau. Il peut s'agir d'un seul bâtiment ou d'un groupe de bâtiments répartis sur une zone géographique étendue. Normalement, l'entreprise qui possède le réseau du campus possède généralement les câbles physiques déployés sur le campus. Par conséquent, les concepteurs de réseau ont généralement tendance à concevoir la partie campus du réseau d'entreprise afin qu'elle soit optimisée pour l'architecture fonctionnelle la plus rapide fonctionnant sur une infrastructure physique à grande vitesse (1/10/40/100 Gbps). **[21]**

En outre, les entreprises peuvent également disposer de plusieurs blocs de campus dans le même emplacement géographique, en fonction du nombre d'utilisateurs présents dans l'emplacement, des objectifs et de la nature de l'entreprise. Dans la mesure du possible, la conception de réseaux de campus d'entreprise convergés modernes devrait tirer parti de l'ensemble commun suivant de principes d'ingénierie et d'architecture :

- Hiérarchie
- Modularité

3.7.2. Les caractéristiques :

L'évolution des besoins du réseau des clients, combinée aux problèmes de collision, de bande passante et de diffusion, a nécessité une nouvelle conception du campus. Les demandes accrues des utilisateurs et les applications complexes obligent les concepteurs de réseau à réfléchir d'avantage aux modèles de trafic au lieu de résoudre un problème de service isolé typique. Nous ne pouvons plus simplement penser à créer des sous-réseaux et à placer différents départements dans chaque sous-réseau. Nous devons créer un réseau qui permette à tout le monde d'atteindre facilement tous les services réseau.

En raison des nouvelles applications gourmandes en bande passante, de la vidéo et du son livrés au poste de travail, ainsi que de la charge de travail croissante sur Internet, le nouveau modèle de campus doit pouvoir fournir les éléments suivants:

Convergence rapide : Lorsqu'un changement de réseau a lieu, celui-ci doit pouvoir s'adapter très rapidement au changement et permettre aux données de se déplacer rapidement.

Chemins déterministes : Les utilisateurs doivent pouvoir accéder à une certaine zone du réseau sans faute.

Basculement déterministe : La conception du réseau doit comporter des dispositions garantissant que le réseau reste opérationnel même en cas de défaillance d'un lien.

Taille et débit évolutifs : Au fur et à mesure que des utilisateurs et de nouveaux périphériques sont ajoutés au réseau, l'infrastructure réseau doit être en mesure de gérer la nouvelle augmentation du trafic.

Applications centralisées : Les applications d'entreprise auxquelles tous les utilisateurs ont accès doivent être disponibles pour prendre en charge tous les utilisateurs de l'inter réseau.

Support multi protocole : Les réseaux de campus doivent prendre en charge plusieurs protocoles, à la fois routés et routés. Les protocoles routés sont utilisés pour envoyer des données utilisateur via l'inter réseau (par exemple, IP ou IPX). Les protocoles de routage sont utilisés pour envoyer des mises à jour du réseau entre routeurs, qui mettront à jour leurs tables de routage. Les exemples de protocoles de routage incluent RIP, le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) et OSPF (Open Shortest Path First).

Multidiffusion : La multidiffusion envoie une diffusion à un sous-réseau ou à un groupe d'utilisateurs défini. Les utilisateurs peuvent être placés dans des groupes de multidiffusion, par exemple pour la vidéoconférence.

QoS (quality of service) : Nous devons pouvoir hiérarchiser différents types de trafic.

3.7.3. Modèle de réseau hiérarchique :

Le modèle hiérarchique Cisco est utilisé pour aider à concevoir un inter-réseau hiérarchique évolutif, fiable et économique. Cisco définit trois couches de hiérarchie, chacune avec des fonctionnalités spécifiques.
Les trois couches sont les suivantes:

- Cœur
- Distribution
- Accès

Chaque couche a des responsabilités spécifiques. Rappelez-vous cependant que les trois couches sont logiques et pas nécessairement physiques. «Trois couches» ne signifient pas nécessairement «trois périphériques distincts». Avant d'examiner ces couches et leurs fonctions, considérons une conception hiérarchique commune, comme illustré à **la figure 11**.

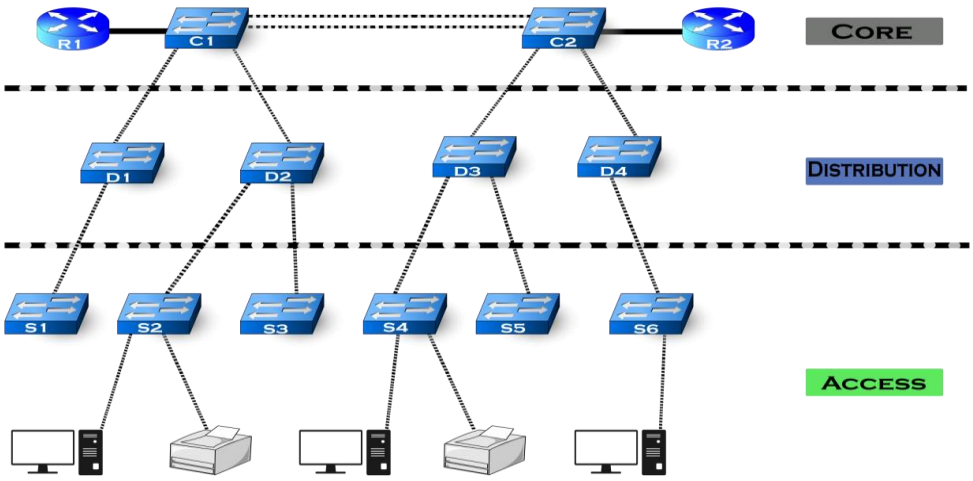

Figure 11 – Modèle hiérarchique à trois couches.

3.7.3.1. La couche cœur de réseau (Core Layer) :

La couche cœur et considérée comme étant le réseau fédérateur à haut débit de l'inter-réseau et assure la connexion aux ressources internet. Au sommet de la hiérarchie, la couche centrale est chargée de transporter de grandes quantités de trafic de manière fiable et rapide. Elle a pour seul objectif de permuter le trafic le plus rapidement possible. **[22]**

En cas de défaillance du noyau, chaque utilisateur peut être affecté. Par conséquent, la tolérance de panne sur cette couche est un problème. Il est probable que le cœur connaisse d'importants volumes de trafic. La vitesse et la latence sont donc des préoccupations majeures. Compte tenu de la fonction du noyau, nous pouvons maintenant examiner certaines caractéristiques de la conception à prendre en compte. Commençons par certaines choses qu'il ne faut pas les faire:

- Il ne faut pas faire rien pour ralentir le trafic. Cela inclut l'utilisation de listes d'accès, le routage entre les VLAN et le filtrage de paquets.
- Il faut évitez d'élargir le noyau lorsque l'inter réseau se développe (c'est-à-dire en ajoutant des routeurs) Si les performances deviennent un problème dans le noyau, privilégiez les mises à niveau par rapport à l'expansion.

Il faut assurer de certaines choses lors de la conception du noyau:

- Il faut concevoir le noyau pour une fiabilité élevée. Pensez aux technologies de liaison de données qui facilitent la vitesse et la redondance, telles que FDDI, FastEthernet (avec des liaisons redondantes), Gigabit Ethernet ou même ATM.
- Il faut concevoir le noyau avec rapidité. Le noyau devrait avoir très peu de latence.
- Il faut sélectionner les protocoles de routage avec des temps de convergence plus courts.
- Il faut concevoir la couche centrale en tant qu'environnement de commutation haute vitesse de couche 3 (L3) utilisant uniquement des services à accélération matérielle. Les conceptions de base de couche 3 sont supérieures à la couche 2 et à d'autres alternatives car elles fournissent:
- Convergence plus rapide autour d'une défaillance de lien ou de nœud.
- Évolutivité accrue car les relations entre voisins et le maillage sont réduits.
- utilisation plus efficace de la bande passante.

3.7.3.2. La couche de distribution (Distribution Layer) :

La couche de distribution est parfois appelée couche de groupe de travail et constitue le point de communication entre la couche d'accès et le cœur. La fonction principale de la couche de distribution est de fournir un routage, un filtrage et un accès au réseau étendu, ainsi que de déterminer comment les paquets peuvent accéder au cœur, si nécessaire. La couche de distribution doit déterminer le moyen le plus rapide de répondre aux demandes des utilisateurs (par exemple, la manière dont une demande de fichier est transmise à un serveur). Une fois que la couche de distribution a déterminé le meilleur chemin, elle transmet la demande à la couche principale. La couche centrale est alors responsable du transport rapide de la demande vers le service approprié. **[22]**

La couche de distribution est le lieu d'implémentation des stratégies pour le réseau. Ici, vous pouvez exercer une flexibilité considérable dans la définition du fonctionnement du réseau. En règle générale, les opérations suivantes doivent être effectuées au niveau de la couche de distribution:

- Implémentez des outils tels que des listes d'accès, le filtrage de paquets et la mise en file d'attente.
- Implémentez des stratégies de sécurité et de réseau, y compris la traduction d'adresses et les pare-feu.
- Redistribuez entre les protocoles de routage, y compris le routage statique.
- Route entre les VLAN et les autres fonctions de support de groupe de travail.
- Définir les domaines de diffusion et de multidiffusion. Les choses à éviter au niveau de la couche de distribution sont limitées aux fonctions qui appartiennent exclusivement à l'une des autres couches.

3.7.3.3. La couche d'accès (Access Layer) :

Cette couche est constituée des périphériques finaux tels que les ordinateurs, les imprimantes et les téléphones IP. Elle peut aussi contenir des routeurs, des commutateurs, des concentrateurs et des points d'accès sans fil. Le rôle de cette couche est de connecter et de contrôler l'accès des périphériques finaux au reste du réseau et de vérifier s'ils sont autorisés. Tout le trafic des services distants est géré par la couche de distribution. Les fonctions suivantes doivent être incluses dans cette couche:

- Poursuite du contrôle d'accès et des stratégies (depuis la couche de distribution).
- Création de domaines de collision distincts (segmentation).
- Connectivité du groupe de travail à la couche de distribution.
- Des technologies telles que le routage à la demande (DDR) et la commutation Ethernet sont fréquemment utilisées dans la couche d'accès. Le routage statique (au lieu des protocoles de routage dynamiques) est également présenté ici.

Les deux architectures de conception hiérarchique principales et communes des réseaux de campus d'entreprise sont les modèles de couches à trois et à deux niveaux :

3.7.3.4. Modèle à trois niveaux :

Ce modèle, illustré à **la figure 12**, est généralement utilisé dans les réseaux de grandes entreprises, construits à partir de plusieurs blocs de couche de distribution fonctionnelle.

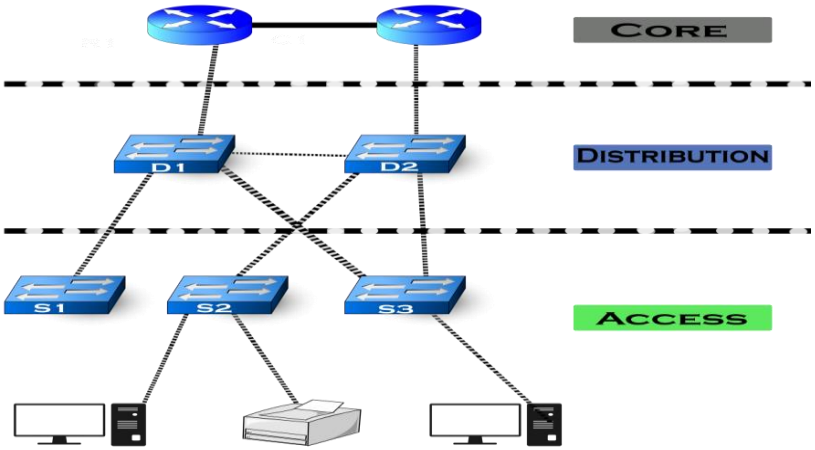

Figure 12 – Modèle de conception de réseau à trois niveaux.

3.7.3.5. Modèle à deux niveaux :

Ce modèle de conception, illustré à **la figure 13**, est plus adapté aux réseaux de campus de petite à moyenne taille (idéalement pas plus de trois blocs d'interruption fonctionnelle à interconnecter), où les fonctions de base et de distribution peuvent être combinées en une seule couche, également connu sous le nom d'architecture de distribution de noyau effondrée.

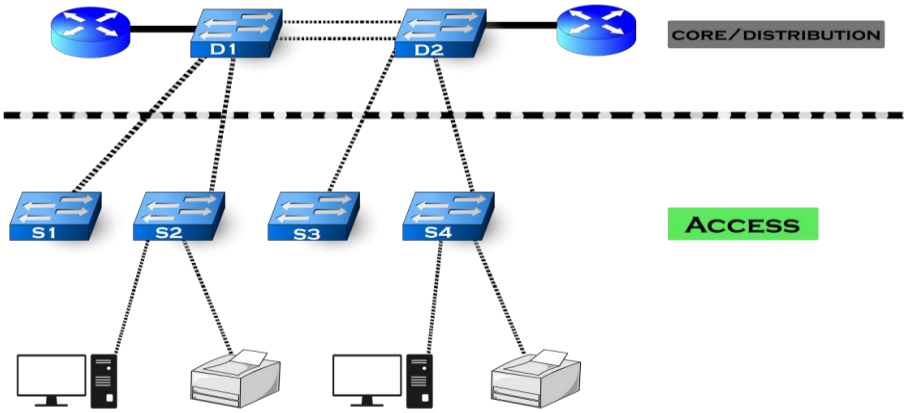

Figure 13 – Modèle de conception de réseau à deux niveaux.

3.7.3.6. Principes du modèle de réseau hiérarchique :

Pour mettre en place correctement un réseau hiérarchique, il faut commencer par étudier la couche d'accès et définir les périphériques finaux. Pour les autres couches, il faut étudier ces éléments :

- **Les liens agrégés :** il faut identifier les ports permettant la liaison entre les commutateurs de chaque couche et surtout estimer les débits nécessaires et disponibles pour mettre en place les liens agrégés permettant d'augmenter la bande passante disponible.
- **Les liens redondants :** en plus des liens agrégés, il faut prévoir des liens redondants permettant d'assurer la continuité de service sur la couche de distribution et la couche cœur de réseau en cas de défaillance d'un commutateur sur ces couches.

3.7.4. Modèle de réseau modulaire:

La conception modulaire rend le réseau plus évolutif et gérable en favorisant l'isolation du domaine de pannes et des modèles de trafic plus déterministe. Les modules du système sont les blocs de construction qui sont assemblés dans le plus grand campus. L'avantage de l'approche modulaire tient en grande partie à l'isolement qu'elle peut offrir. Les pannes qui se produisent dans un module peuvent être isolées du reste du réseau, ce qui simplifie la détection des problèmes et augmente la disponibilité globale du système. Les changements de réseau, les mises à niveau ou l'introduction de nouveaux services peuvent être effectués de manière contrôlée et par étapes, ce qui permet une plus grande flexibilité dans la maintenance et le fonctionnement du réseau du campus. Lorsqu'un module spécifique n'a plus une capacité suffisante ou manque d'une nouvelle fonction ou d'un nouveau service, il peut être mis à jour ou remplacé par un autre module ayant le même rôle structurel dans la conception hiérarchique globale. L'architecture du réseau du campus repose sur l'utilisation de blocs ou modules de base, reliés entre eux par l'intermédiaire du cœur du réseau. **La figure 14** illustre un réseau de campus typique ainsi que les différents modules fonctionnels dans le cadre de la conception d'architecture d'entreprise modulaire.

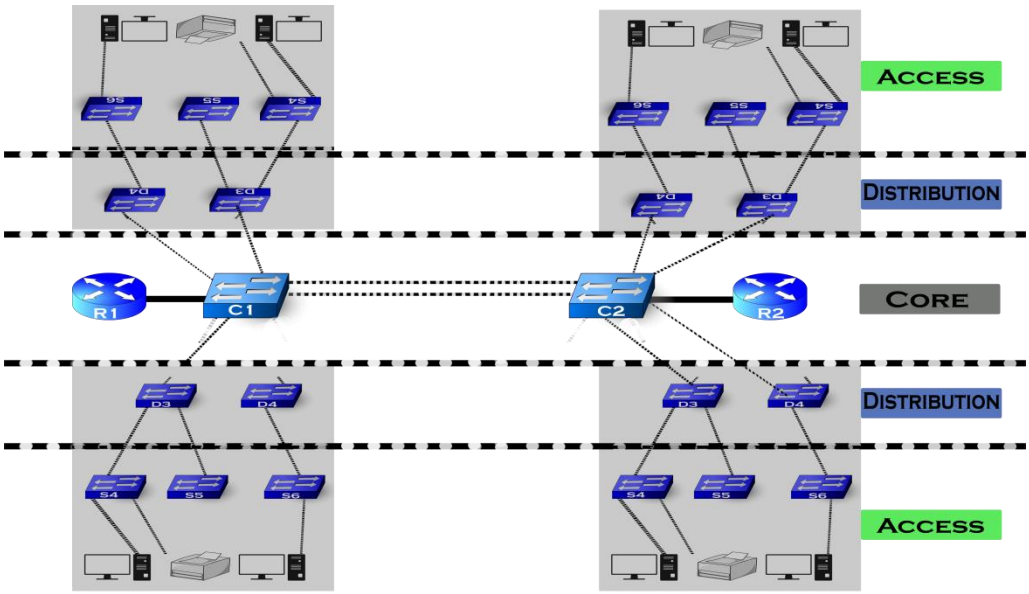

Figure 14 – Architecture typique d'un campus d'entreprise modulaire.

Remarque :

Au sein de chaque bloc fonctionnel de l'architecture d'entreprise modulaire, pour obtenir une conception structurée optimale, on doit appliquer le même principe de conception de réseau hiérarchique.

3.7.4.1. Modèle de conception Access-Distribution :

Le bloc accès-distribution (également appelé bloc de distribution) est probablement l'élément le plus familier de l'architecture du campus. C'est la composante fondamentale de la conception d'un campus. Concevoir correctement le bloc de distribution contribue dans une large mesure à garantir le succès et la stabilité de l'architecture globale. Le bloc de distribution d'accès est constitué de deux des trois niveaux hiérarchiques de l'architecture de

campus multicouches: les couches d'accès et de distribution. Bien que chacune de ces couches ait des exigences de service et de fonctionnalités spécifiques, ce sont les choix de conception du plan de contrôle de la topologie du réseau (tels que les protocoles de routage et de spanning tree) qui sont essentiels pour déterminer comment le bloc de distribution se colle et s'intègre dans l'architecture globale. Il existe actuellement trois choix de conception de base pour la configuration du bloc de distribution d'accès et du plan de contrôle associé:

- Multi-tier STP based (STP classique à plusieurs niveaux)
- Routed access (Accès routé)
- Virtual switch (Commutateur virtuel)

➢ **Bloc de distribution d'accès à plusieurs niveaux (Multi-tier STP based) :**

Ce modèle est le moyen classique ou traditionnel de connecter l'accès à la couche de distribution du réseau du campus. Dans ce modèle, les commutateurs de couche d'accès fonctionnent généralement en mode de couche 2 uniquement, et les commutateurs de couche de distribution fonctionnent en modes de couche 2 et de couche 3. Comme indiqué précédemment dans ce livre, la principale limitation de ce modèle est la confiance accordée au protocole STP (Spanning Tree Protocol) et au protocole FHRP (First Hop Redundancy Protocol).

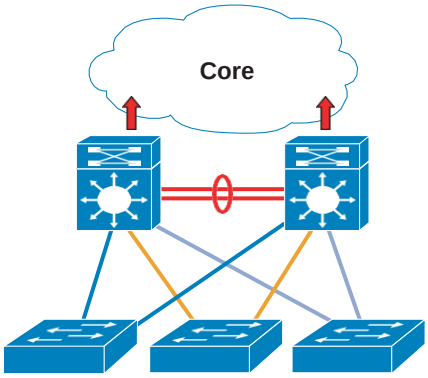

Figure 15 – Bloc de distribution d'accès à plusieurs niveaux sur le campus.

➢ **Routed access (Accès routé) :**

Comme configuration alternative au modèle de bloc de distribution multi-niveaux traditionnel, il existe un modèle dans lequel le commutateur d'accès agit comme un nœud de routage complet de couche 3 (fournit à la fois la commutation de couche 2 et de couche 3) et l'accès aux liaisons de liaison montante de couche 2 de distribution sont remplacés par des liens routés point à point de couche 3. Cette configuration alternative, dans laquelle la démarcation de couche 2/3 est déplacée du commutateur de distribution au commutateur d'accès, semble constituer un changement majeur dans la conception, mais constitue en réalité simplement une extension de la conception multi niveau recommandée (**voir la figure 16**).

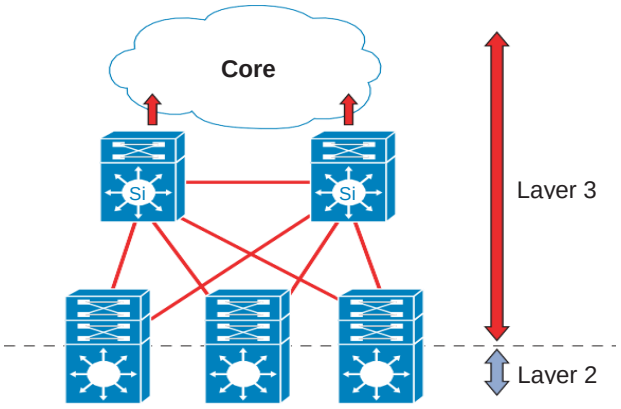

Figure 16 – Conception de bloc de distribution d'accès routé.

- **Virtual switch (Commutateur virtuel) :**

Ce modèle présente la conception la plus simple et la plus souple par rapport aux autres modèles déjà abordés. Avec l'introduction du concept de commutateur virtuel, la paire de commutateurs de distribution peut maintenant être configurée pour fonctionner en tant que commutateur logique unique, comme illustré à **la figure 17**, les concepteurs de réseau peuvent simplifier et améliorer la conception dans une large mesure. Cela offre un niveau plus élevé de résilience des nœuds et des chemins, ainsi qu'un temps de convergence réseau considérablement optimisé.

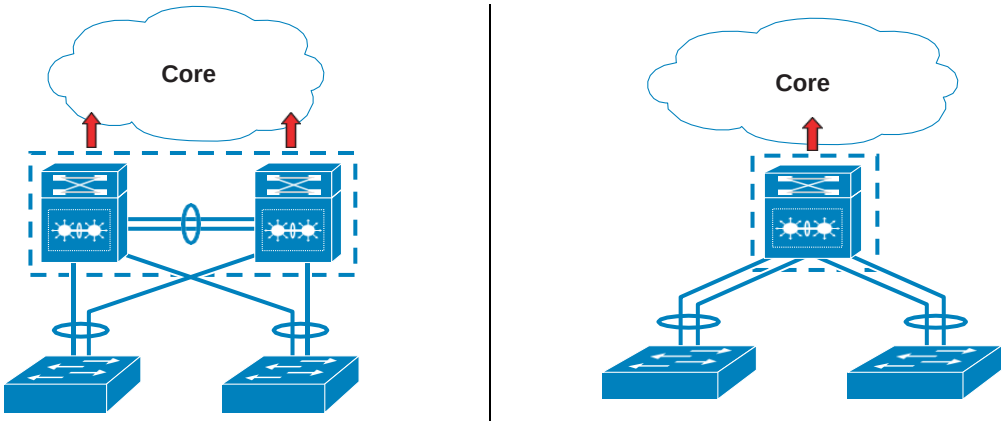

Figure 17 – Commutateur virtuel physique et logique.

Dans la section suivante on va donner la description des VLANs ainsi que les différents protocoles utilisés.

3.7.5. Concepts des Virtual LAN (VLAN) :

3.7.5.1. Définition :

Un réseau local virtuel (VLAN) est tout domaine de diffusion qui est divisé et isolé dans un réseau informatique à la couche de liaison de données (couche OSI 2). Les VLAN ont été uniformisés conformément à la spécification IEEE 802.1Q. Ils fonctionnent en appliquant des balises aux paquets réseau et en gérant ces balises dans des systèmes de réseau, créant ainsi l'apparence et la fonctionnalité du réseau. [23] C'est physiquement sur un seul réseau mais agit

comme s'il était divisé entre des réseaux séparés. De cette manière, les VLAN peuvent séparer les applications réseau bien qu'ils soient connectés au même réseau physique et sans nécessiter le déploiement de plusieurs ensembles de câblage et de périphériques réseau.

3.7.5.2. Les avantages de VLAN :

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- La réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN.
- les diffusions d'un serveur peuvent être limitées aux clients de ce serveur.
- La création de groupes de travail indépendants de l'infrastructure physique.
- possibilité de déplacer la station sans changer de réseau virtuel.

3.7.5.3. Les protocoles :

3.7.5.3.1. Protocole VTP :

VTP est un protocole propriétaire de CISCO, il est chargé de gérer les VLANs d'une manière centralisée et évite ainsi aux administrateurs du réseau de se connecter autant de fois qu'il y a de commutateurs dans un réseau pour ajouter, modifier ou supprimer la configuration d'un appelé serveur VTP, afin de distribuer ces informations de configuration VLAN d'un bout à l'autre du réseau commuté. Un tel protocole réduit les délais d'administration et de maintenance des réseaux VLAN. A noter que ce protocole s'applique au niveau de la couche liaison de données du modèle OSI.

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants [23] :

- **Le mode serveur :**
  - L'information est stockée dans la NVRAM.
  - Il défini le nom de domaine VTP.
  - Il peut ajouter, modifier ou supprimer un VLAN.
  - Il stocke la liste des VLANs du domaine VTP.
- **Le mode client :**
  - Il possède un nom de domaine.
  - Il stocke une liste de VLANs non modifiable.
- **Le mode transparent :**
  - Il ne participe pas aux domaines VTP du réseau.
  - Il transmet les paquets VTP via ses liens trunk.
  - Il possède sa propre liste de VLANs qu'il est possible de modifier.

Si une des conditions suivantes n'est pas respectée, le domaine de VTP ne sera pas valide et l'information ne se propagera pas :

- Il faut assigner le même nom de domaine de VTP à chaque commutateur.
- L'option trunk pour l'interconnexion des commutateurs doit être activée.

3.7.5.3.2. Protocole STP (Spanning-Tree Protocol) :

Le protocole STP est un protocole de couche 2 qui fonctionne sur des ponts et des commutateurs. La spécification du protocole STP est IEEE 802.1. L'objectif principal de ce protocole est de vérifier qu'aucune boucle n'est créée lorsqu'il y'a des chemins redondants dans le réseau car ces dernières sont fatales. **[23]**

Les commutateurs STP surveillent en permanence le réseau pour rechercher toutes les liaisons et s'assurer que des boucles ne se produisent pas en arrêtant les liaisons redondantes. Le protocole Spanning Tree exécute un algorithme appelé algorithme Spanning Tree. Les commutateurs choisissent un point de référence sur le réseau et calculent les chemins redondants vers ce point de référence. Après la découverte d'une boucle dans le réseau, l'algorithme Spanning Tree choisit un chemin sur lequel transférer des images et ferme les autres liens redondants afin d'empêcher que des images ne soient transférées le long de chemins en boucle. Le point de référence s'appelle le pont racine. Il ne peut y en avoir qu'un pont de racine.

Tout comme un réseau de campus d'entreprise tels que les réseaux de Googleplex ou du campus de Microsoft, un réseau de campus universitaires sert à connecter des différents départements et des bâtiments. La section suivante illustre quelques exemples des universités qui utilisent les campus.

3.7.6. Campus universitaires :

Les réseaux de campus universitaires interconnectent souvent des bâtiments variés, notamment des bâtiments administratifs, des bâtiments universitaires, des bibliothèques universitaires, des campus ou des centres d'étudiants, des résidences universitaires…etc. Cette section illustre quelques exemples des universités qui utilisent les campus tels que :

- **Réseau de l'université de Stanford :**

Le réseau universitaire de Stanford (SUNet) comprend des réseaux locaux dans des bâtiments et un réseau fédérateur qui connecte les réseaux locaux les uns aux autres et à des réseaux hors campus.

L'épine dorsale est conçue et exploitée par l'Université IT. Les services de réseau au sein de bâtiments individuels sont la responsabilité des départements qui occupent ces bâtiments, à moins que l'assistance ne soit achetée auprès du service informatique de l'Université.

Pour les bâtiments universitaires et administratifs, ils fournissent et prennent en charge l'infrastructure de communication de données à l'entrée des installations. Grâce au programme Net-to-Switch, ils fournissent une infrastructure de communication de données dans les bâtiments universitaires et administratifs. Pour les résidences d'étudiants, ils soutiennent l'infrastructure de communication de données aux points de service dans les chambres d'étudiants. La connectivité hors campus est maintenue via plusieurs connexions Internet et Internet2.

Pour les résidences d'étudiants, l'Université informatique prend en charge l'infrastructure de communication de données jusqu'au point de service de télécommunication (c.-à-d. La

prise murale) dans les chambres des étudiants. Le groupe d'informatique résidentielle au sein du département d'informatique académique des bibliothèques aide les étudiants à utiliser les services réseau dans les logements pour étudiants. Si nécessaire, Résidentiel Computing consulte et sollicite le soutien de l'Université IT. [24]

- **Réseau de l'université de MIT :**

En 1916, le MIT a quitté Boston pour s'installer à Cambridge, où le campus s'étend désormais sur plus de 1,6 km le long du côté de Cambridge de la Charles River. Le cœur du campus est constitué d'un groupe de bâtiments interconnectés, conçus par l'architecte W. Welles Bosworth (classe de 1889), qui facilitent l'interaction et la communication entre les écoles et les départements du MIT.

L'architecture du campus présente désormais une gamme de styles allant du néoclassique au moderniste, au brutaliste et au déconstructiviste. Parmi les points de repère intemporels du campus figurent des bâtiments conçus par des architectes de renom tels que Alvar Aalto, Frank Gehry, Steven Holl, IM Pei '40 et Eero Saarinen. À l'intérieur, il y a des installations ultramodernes qui soutiennent les efforts de recherche en cours du MIT dans plusieurs disciplines. Ces installations comprennent des laboratoires humides, des salles blanches et des espaces de fabrication, des souffleries, des laboratoires de tests de robots et, bientôt, un centre de nanotechnologie et d'imagerie avancée de 200 000 pieds carrés (18 581 m2).

Pour les étudiants, le campus dispose de 18 salles de séjour, chacune ayant sa propre personnalité et sa propre communauté. [25]

Il est clair que le réseau informatique mis en place afin de fournir des différents services pour assurer un bon fonctionnement des ressources informatique. La partie suivante illustre quelques services réseaux qui jouent un rôle essentiel dans la conception de réseau ainsi que le partage de l'information.

3.7.7. Les services réseaux :

Les services réseaux se basent sur des protocoles pour fournir des fonctionnalités qui sont accessibles par l'utilisateur au niveau de la couche 7 du modèle OSI (couche application). Comme services réseaux, on peut implémenter le service de résolution de noms (DNS), l'attribution d'adresse (DHCP), la messagerie, l'annuaire, le web, ...etc.

3.7.7.1. Domain Name System (DNS) :

Le DNS est un protocole indispensable au fonctionnement d'Internet. Non pas d'un point de vue technique, mais d'un point de vue de son utilisation. L'objectif du système de nom de domaine est de proposer une résolution à base de noms hiérarchique et distribués pour les hôtes IP connectés au réseau. Initialement le système permettait seulement de résoudre des noms en adresse IP, ainsi que des adresse IP en noms. [10]

Le système a progressivement évolué pour agir en tant que véritable service de localisation de ressources ; ainsi, aujourd'hui, un ordinateur peut interroger le service DNS pour trouver un serveur de messagerie correspondant à un domaine spécifique (enregistrement MX ou Mail

eXchanger), pour trouver un serveur Kerberos ou bien un serveur proxy internet ou encore localiser un serveur de licences Microsoft …et ainsi de suite.

Remarque :

DNS prend maintenant en charge IPv6 comme IPv4 pour identifier les objets au sein de l'arborescence logique.

- **Fonctionnement :**

Par exemple, pour un particulier, l'ordinateur obtient une adresse IP par le biais d'un box internet. Lorsque l'ordinateur privé demande à résoudre un nom DNS, tel que www.impots.gouv.fr, cette requête est envoyé par le box au serveur du FAI (Fournisseur d'Accès Internet).

Le service DNS du FAI agit ensuite seul pour interroger un des 13 serveurs racines internet, à la recherche des serveurs DNS qui gèrent la zone **fr**. Le serveur racine qui a connaissance du serveur qui gère la zone **fr** va renvoyer l'adresse IP du serveur DNS correspondant.

Le serveur du FAI va ensuite interroger le serveur qui gère la zone **fr** pour trouver celui qui gère la zone **gouv.fr**.

Et ainsi de suite, jusqu'à ce qu'il récupère l'adresse IP du serveur DNS qui gère la zone **impots.gouv.fr**. Une fois que le serveur DNS du FAI a obtenu l'information demandée, il la met en cache, puis la transmet au box internet, et ce dernier renvoie finalement l'adresse au client DNS du réseau local (**voir figure 18**).

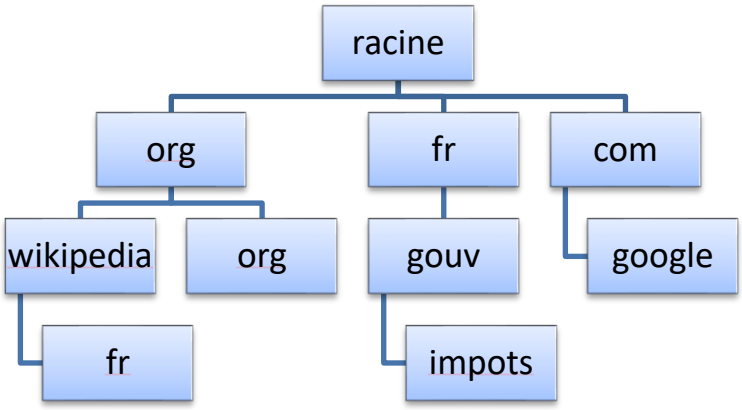

Figure 18 – l'arborescence des noms Internet (DNS).

3.7.7.2. Dynamic Host Configuration Protocol v4 (DHCPv4) :

Le service DHCP apparaît en 1993 comme une extension du protocole BOOTP créé en 1985. Un serveur DHCP a pour rôle de distribuer des adresses IP à des clients pour une durée déterminée. Au lieu d'affecter manuellement à chaque machine une adresse statique, ainsi que tous les paramètres tels que serveur de noms, passerelle par défaut, nom du réseau, un serveur DHCP alloue à chaque client un bail d'accès au réseau, pour une durée déterminée (durée du bail). Il passe en paramètres au client toutes les informations dont il a besoin. [26]

3.7.7.3. Messagerie :

Le courrier électronique est aujourd'hui l'une des applications les plus populaires du réseau. Utilisé pour des applications très variées : personnelles, professionnelles, associatives, politiques, etc. En fait, pour fonctionner, la messagerie électronique s'appuie principalement sur des serveurs de messagerie, des protocoles de transport ainsi que sur des protocoles de contenu. Le serveur de messagerie est un logiciel de courrier électronique ayant pour vocation de transférer les messages électroniques d'un serveur à un autre.

3.7.7.4. Annuaires :

Le service d'annuaire, sur un réseau TCP/IP utilise le protocole LDAP. Un annuaire électronique est une base de données spécialisée, dont la fonction première est de retourner un ou plusieurs attributs d'un objet grâce à de recherche multicritères. Contrairement aux SGBD, un annuaire est très performant en lecture mais l'est beaucoup moins en écriture. Il peut servir d'entrepôt pour centraliser des informations et les rendre disponibles via le réseau, à des applications, des systèmes d'exploitation ou des utilisateurs. La majorité des logiciels serveurs LDAP proposent un protocole de communication serveur-serveur pour assurer le service de réplication et de synchronisation des contenus, quand bien même la communication client-serveur est normalisée **[27]**.

3.7.7.5. Service web :

Un service Web est un système logiciel conçu pour prendre en charge une interaction interopérable de machine à machine sur un réseau. Il possède une interface décrite dans un format pouvant être traité par une machine (en particulier WSDL). D'autres systèmes interagissent avec le service Web de la manière spécifiée par sa description à l'aide de messages SOAP, généralement acheminés via HTTP avec une sérialisation XML associée à d'autres normes relatives au Web **[27]**.

4. Conclusion :

Ce chapitre nous a permis d’avoir une bonne compréhension des concepts de base et d’éclaircir les différentes idées du réseau LAN, nous avons vu les différents modèles de référence tel que OSI, ainsi que ses différentes couches et les éléments physiques qui le constituent en plus de ça nous avons définir de façon clair et détaillés le réseau de campus et les différentes types d’architecture.

Chapitre 2 : Etude de l'architecture existante et spécification des besoins

1. Introduction :

Ce chapitre sera réservé à l'étude du réseau existant dans la faculté des sciences exactes et de l'informatique (FSEI) de Mostaganem et aux améliorations proposées, d'abord nous allons évoquer un bref aperçu de l'université Abdelhamid Ibn Badis, Mostaganem (UMAB) en générale pour mieux connaitre sa structure et ses objectifs. Ensuite, nous allons étudier le réseau informatique et ses composants et nous essayerons de voir les points faibles du réseau et donné des suggestions afin d'amélioré sa fiabilité et de rendre le trafic plus efficace, pour pouvoir proposer d'éventuelles améliorations.

2. Présentation de l'université UMAB:

L'Université Abdelhamid Ibn Badis, Mostaganem (UMAB) a été créée en 1998 par Décret exécutif N° 98-220 du 07 Juillet 1998. Elle est située dans la ville de Mostaganem, au Nord-Ouest de l'Algérie. l'UMAB n'a cessé de relever les défis scientifiques et sociétaux. Une université dont la situation géographique lui offre une position stratégique. En effet, elle est à mi-distance des wilayas d'Oran, Relizane, Chlef et Mascara. **[28]**

3. L'historique de l'université :

L'histoire de l'université Abdelhamid Ibn Badis, Mostaganem se mêle intimement à celle de la région de Dahra. Fondé en 1978, cet établissement d'enseignement supérieur, a longtemps formé l'élite intellectuelle de la région ouest, et son influence est toujours marquante.

Auparavant, l'enseignement supérieur s'est implanté à Mostaganem dès 1969, avec la création de l'Institut de Technologie Agricole (I.T.A. de Mostaganem) qui formait des Ingénieurs en agronomie appliquée, et l'implantation en 1978 du Centre Universitaire de Mostaganem, qui a ouvert ses portes avec des formations supérieures en Biologie, en tronc commun de sciences médicales et en Chimie.

Depuis 1998, l'Université de Mostaganem a connu un essor très rapide de ses infrastructures et capacités, de ses personnels et de ses étudiants. Les efforts déployés par ses responsables, ses cadres et ses enseignants ont permis à l'UMAB de traverser avec succès une série d'étapes qualitatives qui ont fait de Mostaganem un véritable pôle universitaire rayonnant dans toute la région Ouest du pays et bien au-delà. **[28]**

Son parcours se résume comme suit :

- **1978**: Création du Centre Universitaire de Mostaganem **Décret n° 78-131 du 08 juin 1978 portant création du centre universitaire de Mostaganem.**
- **1984**: Organisation du Centre Universitaire de Mostaganem :
  - **a.** École Normale Supérieure en sciences fondamentales.
  - **b.** Institut National de l'Enseignement Supérieur de Biologie.
  - **c.** Institut National de l'Enseignement Supérieur de Chimie.
  - **d.** École Supérieure de l'Éducation Physique et Sportive.

- **1992**: Nouvelle organisation de l'institution :
  a. Centre Universitaire.
  b. École Normale Supérieure en sciences fondamentales.
  c. École Normale Supérieure en Éducation Physique et Sportive.
- **1997 :** Transfert de l'Institut National de Formation Supérieure en Agronomie (INFSA ex : ITA) du ministère de l'agriculture au centre universitaire de Mostaganem.
- **1998**: Passage de centre universitaire à l'université par décret :***Décret exécutif n°12-77 du 19 Rabie El Aouel 1433 correspondant au 12 février 2012 modifiant et complétant le décret exécutif n° 98-220 du 7 juillet 1998 portant création de l'université de Mostaganem.***
- **2000**: Transfert de l'Institut National de Formation Travaux Publics à l'Université de Mostaganem. (Ministère des travaux Publics).
- **2003**: Création de l'Institut des Sciences et Techniques des Activités Physiques et Sportives (STAPS).
- **2009**: Réorganisation de l'Université de Mostaganem (07 Facultés et 01 Institut).
- **2011**: Réorganisation de l'Université de Mostaganem (ouverture de la Faculté de Médecine).***Décret exécutif n°12-360 du 22 Dhou El Kaada 1433 correspondant au 08 octobre 2012 complétant le décret exécutif n° 98-220 du 13 Rabie El Aouel 1419 correspondant au 7 juillet 1998 portant création de l'université de Mostaganem.***
- **2013**: Restructuration des facultés de l'Université de Mostaganem en 08 facultés et 01 institut et (création de l'Ecole Normale Supérieure et l'Ecole Préparatoire en Sciences de la Nature et de la Vie).
- **2014:** Création de l'Ecole Normale Supérieure.
- **2016**: Réorganisation de l'Université de Mostaganem (09 Facultés et 01 Institut). ***Décret exécutif n°14-239 du 29 Chaoual 1435 correspondant au 25 Aout 2014 modifiant et complétant le décret exécutif n° 98-220 du 13 Rabie El Aouel 1419 correspondant au 7 juillet 1998 portant création de l'université de Mostaganem.*** **[29]**

Elle est composée actuellement de 9 facultés et d'un institut :

- La Faculté des sciences sociales (FSS) qui compte 2 départements (sciences humaines et sciences sociales).
- La Faculté de littérature arabe et des arts (FLAA) avec 3 départements (études littéraires et critiques, études linguistiques, arts visuels et arts de spectacles).
- La Faculté des langues étrangères (FLE) qui compte trois départements (français, anglais, espagnol).
- La Faculté des sciences économiques, commerciales et sciences de gestion (FSEGC) qui comprend 4 départements (sciences économiques, sciences commerciales, sciences de gestion, comptabilité et finances).
- La Faculté de droit et de sciences politiques (FDSP) avec 3 départements (droit public, droit privé, sciences politiques).
- La Faculté de médecine (FMED) qui comprend un seul département (médecine).
- La Faculté des sciences exactes et de l'informatique (FSEI) qui compte 2 départements (mathématiques et informatique, physique et chimie).

- La Faculté des sciences de la nature et de la vie (FSNV) comprenant 3 départements (agronomie, biologie, halieutique).
- La Faculté des sciences et de la technologie (FST) qui compte 4 départements (génie civil et architecture, génie des procédés, génie mécanique, génie électrique).
- L'institut d'éducation physique et sportive (IEPS) qui comprend 3 départements (éducation physique et sportive, entrainement sportif et activités motrices adaptées).

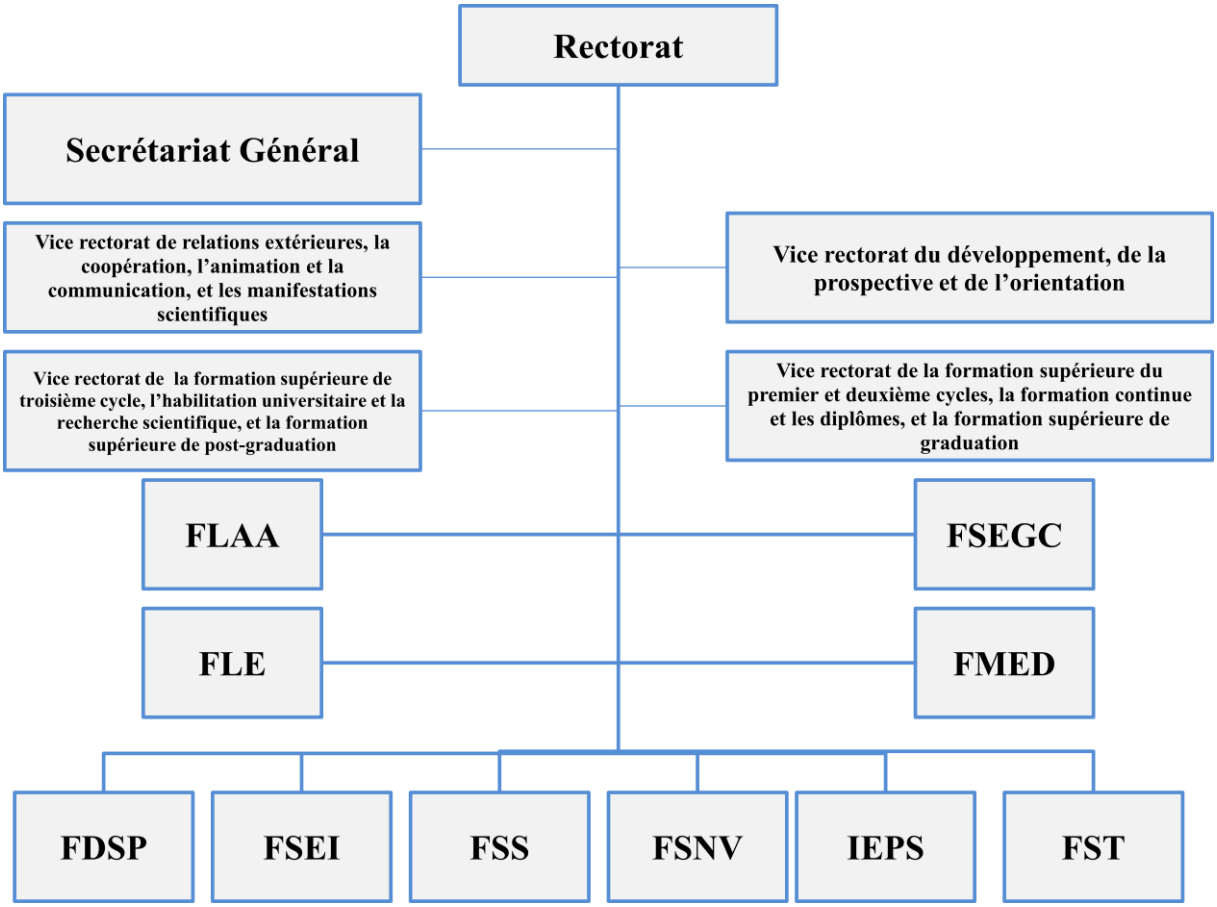

Figure 19 – l'organigramme de l'université UMAB.

L'Université de Mostaganem porte le nom d'Abdelhamid Ibn Badis, une figure emblématique du mouvement réformiste musulman en Algérie. Il était enseignant, philosophe, visionnaire musulman, journaliste, et révolutionnaire de la plume et du savoir. Une fête nationale 'YOUM EL ILM' ou « Journée du savoir » est célébrée en son honneur le 16 Avril de chaque année, commémorant la date de son décès.

4. Présentation du réseau informatique d'UMAB :

Le réseau informatique principal de l'université d'Abdelhamid Ibn Badis se situé au centre universitaire I.T.A est considéré comme étant un réseau de Backbone, il se charge de la gestion de toutes les ressources informatiques de l'université ainsi que de l'assurance de la continuité des services informatiques et de leurs maintenances, tels que le service pédagogique, la disponibilité de la connexion aux réseaux intranet et internet et l'exploitation des différents services offerts, et enfin la maintenance du parc informatique de l'université.

Chaque département, chaque laboratoire de recherche et chaque service administratif du rectorat et des facultés se sont vus dotés de l'outil internet qui se fait à partir du nœud central

domicilié au service des réseaux, via une liaison spécialisée de 100 Mbps sur un support en fibre optique monomode reliée au provider CERIST (Centre de Recherche sur l'Information Scientifique et Technique) pour intégrer le réseau universitaire ARN (Academic Research Network).

En menant un audit sur l'architecture réseau d'I.T.A, on a pu avoir l'architecture schématisée dans **la figure 20**, La salle machine du réseau local de l'I.T.A qui est le cœur du réseau, toutes les activités reposent sur cette salle, elle regroupe en un seul endroit les ressources nécessaires au bon fonctionnement du réseau, elle contient principalement 3 armoires, deux armoires contient l'ensemble des serveurs (tel que : serveur DNS, serveur Web…etc.), et l'autre est une armoire de brassage qui contient le routeur principale, le serveur pare-feu et des Switchs, éventuellement l'ensemble des convertisseurs media (FO/RJ45). Cette dernière sert à relier les différents sites/facultés de l'université UMAB par des fibres optiques et de servir une connexion internet à haut débit de 10 à 20 Mb/s par site. Chaque site a une armoire de brassage contenant un/des convertisseur(s) media, un/plusieurs Switch où sont reliés les différents équipements par des câbles informatiques.

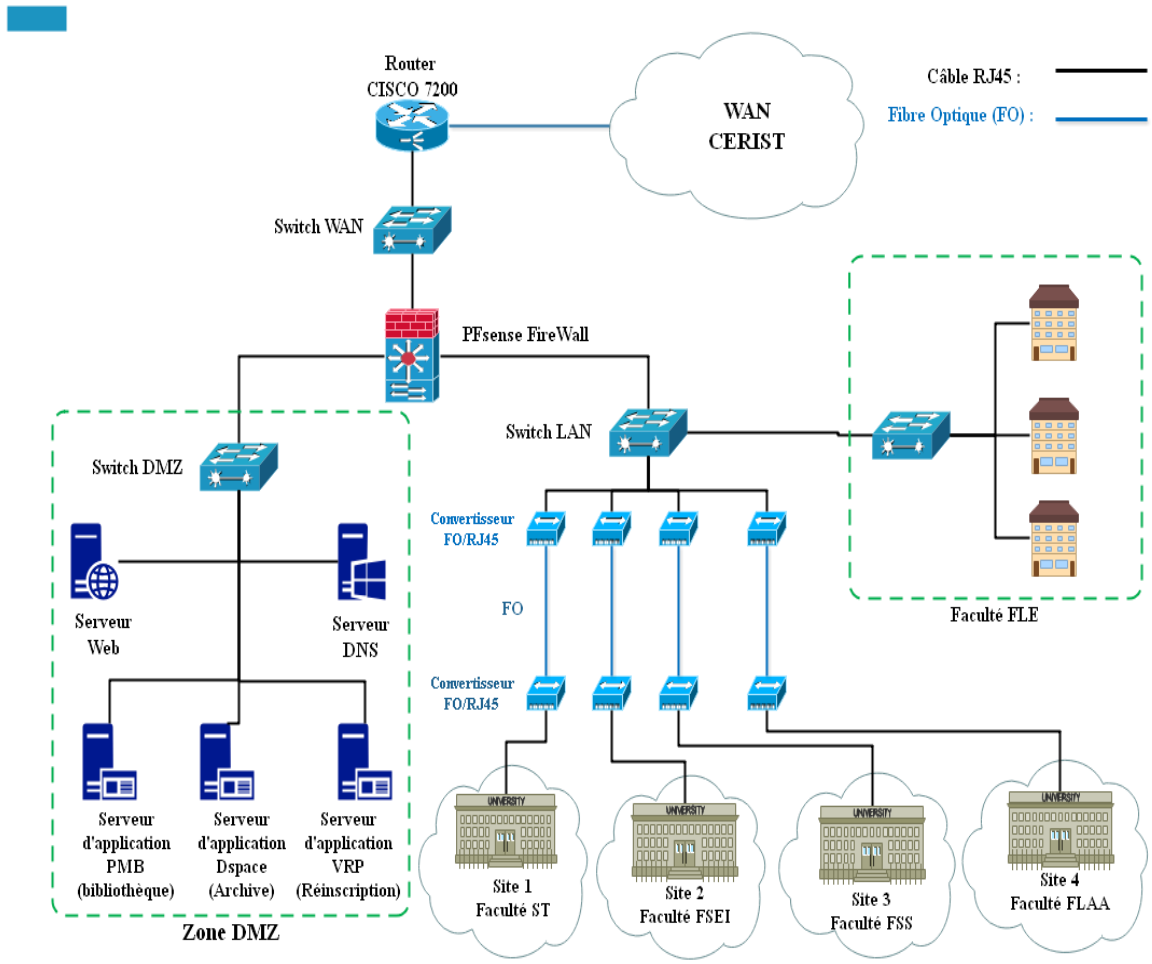

Figure 20 – Architecture du réseau du centre universitaire I.T.A.

L'architecture réseau s'appuie sur le modèle hiérarchique Cisco (vu au chapitre 1) à deux niveaux dont l'objectif était de fournir une connexion internet sécurisé, fiable et économique

aux différents sites universitaires et de faire en sorte que tous le trafic doit être surveillé et filtré par le centre informatique d'I.T.A.

Comme il est schématisé dans **la figure 20**, on trouve le pare-feu Pfsense qui se charge de filtrer les paquets entrants/sortants. Ce système de pare-feu permet aussi la gestion des VLANs car l'une de ces interfaces est reliée directement à un Switch LAN et que ce dernier offre une liaison vers les différents sites. En plus il est relié aussi à un Switch DMZ où on trouve l'ensemble des serveurs tels que serveur d'application PMB…etc.

5. Présentation de FSEI :

La Faculté des Sciences Exactes et de l'Informatique se consacre à l'enrichissement et à la transmission des connaissances au sein de ses départements. Composée de quatre départements : Mathématiques, Informatique, Physique, Chimie. La Faculté offre à plus de 1900 étudiants une formation de qualité dans les domaines des sciences de la matière et des mathématiques et informatique. Deux laboratoires de recherche résolument engagés dans une mission d'excellence nourrissent un enseignement supérieur de haut niveau.

Chacun des cinq départements (tronc commun en sciences exactes et informatique, informatique, physique, chimie et mathématiques) est dirigé par un chef de département, la **figure 21** illustre l'organigramme de la faculté.

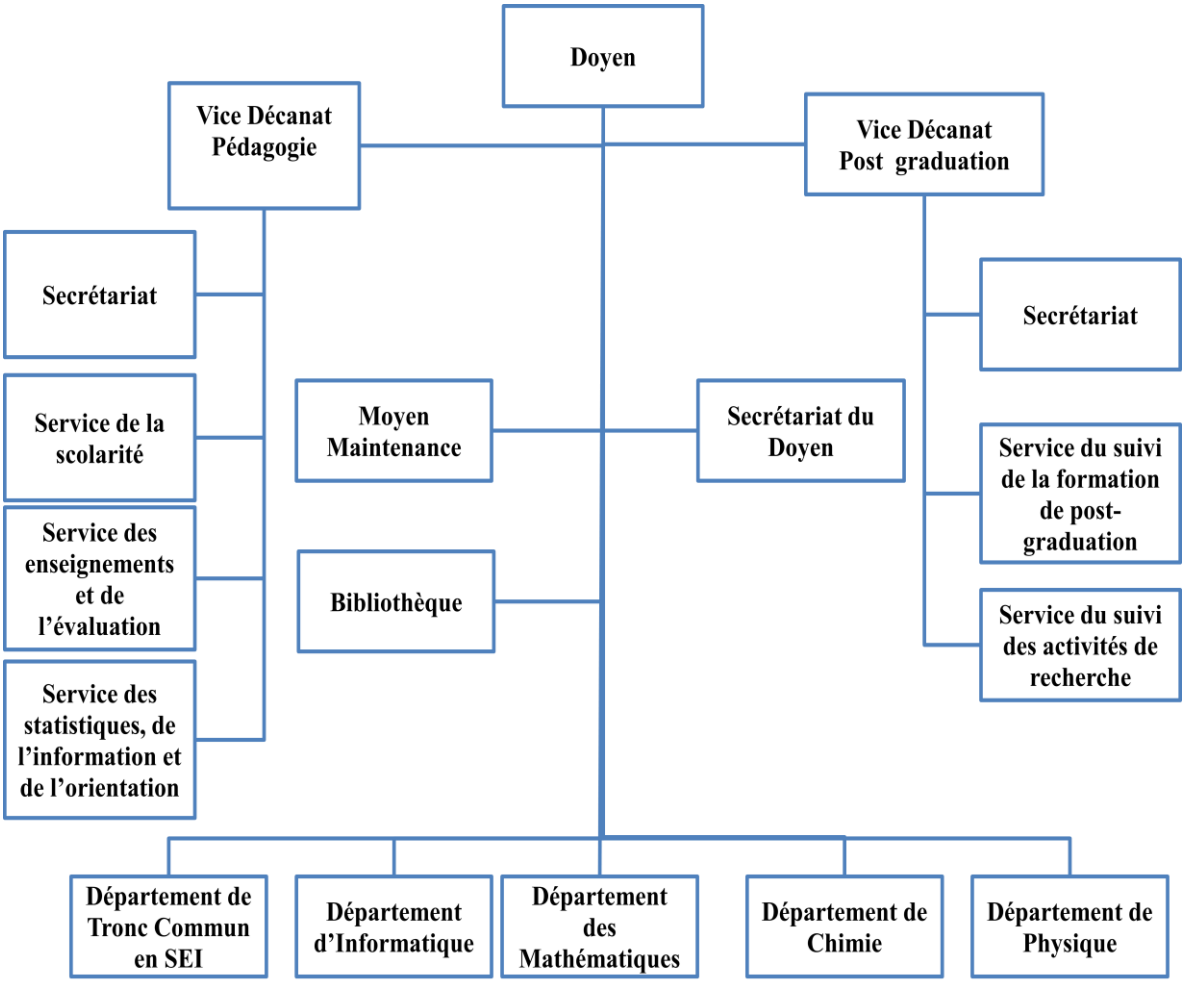

Figure 21 – L'organigramme de la faculté FSEI.

6. Présentation du réseau informatique de FSEI :

Le réseau informatique de la faculté FSEI est composé d'un réseau câblé et d'un réseau Wifi où l'accès à internet se fait via une liaison spécialisée de 10 à 20 Mbps sur un support en fibre optique monomode reliée au centre universitaire I.T.A.

Ce réseau informatique utilise un certain nombre de matériel informatiques pour la gestion quotidienne des enseignants et des étudiants où il y a deux solutions ont été utilisées pour sa mise en place:

- Un câblage filaire avec une topologie physique en étoile utilisant des câbles RJ45 UTP (Unshielded twisted pair) catégorie 6 pour la liaison entre les ordinateurs de bureau et le Switch (CISCO Catalyst 2960-24PC-L).
- Un réseau sans fil (Wifi) avec des points d'accès fournissant une vitesse théorique de 54Mbits/s destiné aux ordinateurs équipés d'une carte Wifi (IEEE 802.11), particulièrement les ordinateurs portables et les Smartphones.

La figure 22 illustre l'architecture du réseau actuel de la faculté :

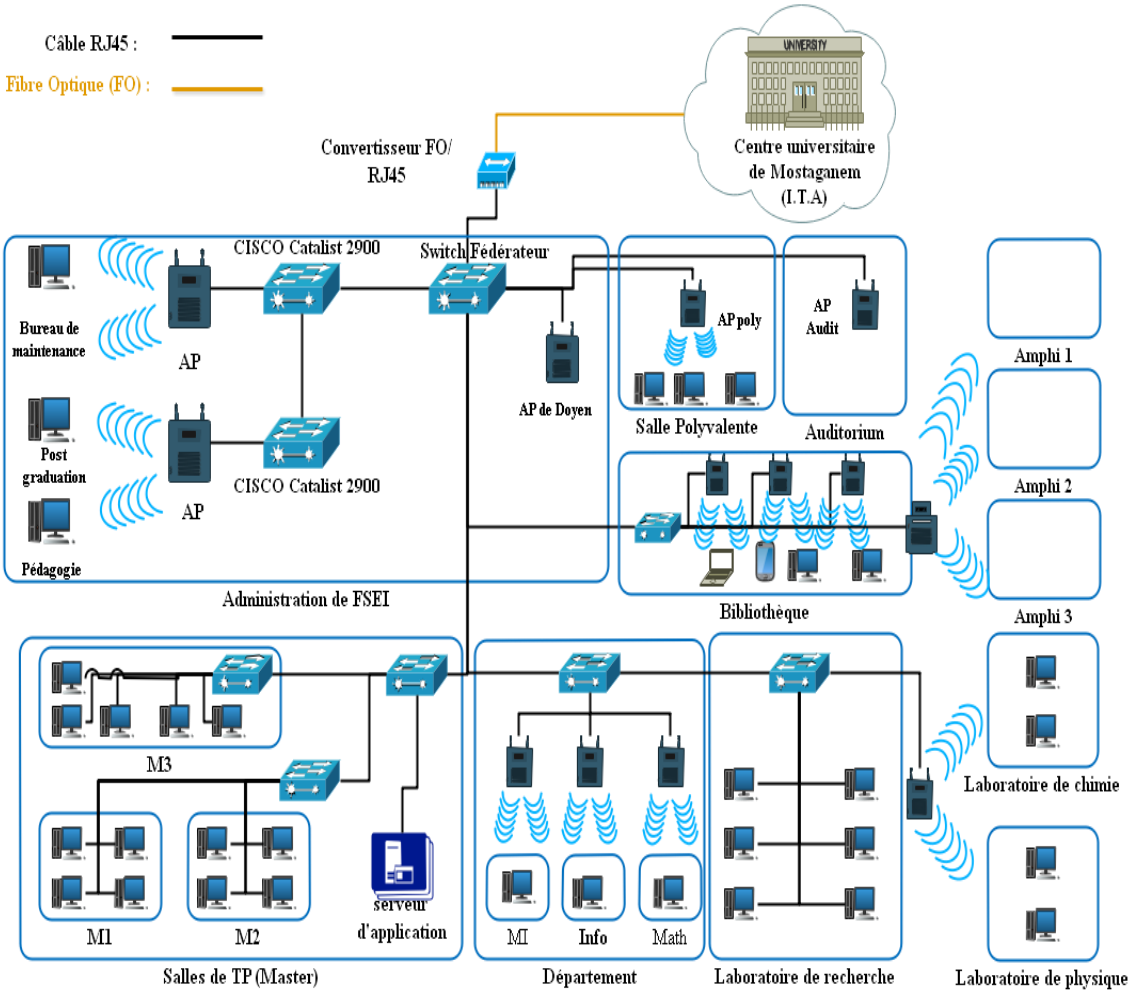

Figure 22 – Architecture du réseau actuel de FSEI.

6.1. Le parc informatique :

6.1.1. Environnement client :

Le parc informatique est composé de 44 ordinateurs de bureau équipés de processeur intel core i3 pour les salles de TP, Il faut également noter la présence circonstancielle d'ordinateurs portables au sein du parc informatique de la faculté, apportés et utilisé par des étudiants.

Tableau 3 – Caractéristiques des ordinateurs de FSEI.

Mémoire Ram	Capacité disque dur	Caractéristiques Processeur
2Go – 4Go	500 Go	3M Cache, 1.70 GHz

6.1.2. Environnement serveur :

La faculté ne dispose pas encore de serveurs, cependant la structure à un besoin assez pressant certain nombre de serveurs tel qu'un serveur de pare-feu pour contrôler le trafic du réseau et un serveur pour héberger un certain nombre de logiciels partagés. Notre étude prendra en compte cette préoccupation.

6.1.3. Les équipements d'interconnexion :

Les équipements d'interconnexion représentent le cœur du réseau dans une architecture. S'ils sont mal dimensionnés, ils pourront avoir des effets négatifs sur le trafic du réseau, pouvant entrainer la détérioration de celui-ci. Dans notre cas d'étude, l'infrastructure du réseau de FSEI ne comporte qu'un commutateur fédérateur (CISCO Catalyst 2960-24PC-L) de 24 ports Fast Ethernet et de 4 ports Gigabit Ethernet pour l'interconnexion des différents clients par des points d'accès (D-link DWL-2100AP) et des différents d'autres commutateurs de même modèle qui relient différents endroits, ainsi que des points d'accès Outdoor (DAP-3690) pour l'interconnexion des endroits qui n'ont pas accès filaire tels que les amphis et cafeteria.

- **CISCO Catalyst 2960-24PC-L :**

Est un commutateur Ethernet autonome à configuration fixe, qui fournit aux postes de travail une connectivité Fast Ethernet et Gigabit Ethernet, et permet la mise en œuvre de services LAN avancés au sein des réseaux d'entreprise et des réseaux d'agences. Il offre une sécurité intégrée avec contrôle d'admission par le réseau (NAC), qualité de service (QoS) évoluée, et résilience pour apporter des services intelligents à la périphérie du réseau **[30]** (voir la **figure 23**).

Figure 23 – Switch CISCO Catalyst 2960-24PC-L.

- **D-link DWL-2100AP :**

Est un point d'accès ultra-performant 802.11g destiné à être utilisé en intérieur. Il offre des vitesses réseau sans fil pouvant atteindre 108Mbps (en mode Turbo), tout en assurant

l'interopérabilité transparente avec le sans fil 802.11b existant. Avec ses taux de transfert de données élevés, sa sécurité accrue et sa fonction de passerelle intégrée, ce point d'accès est la solution sans fil idéale qui vous permet d'adopter une nouvelle technologie ultra-rapide tout en protégeant vos investissements passés grâce à l'interopérabilité avec votre équipement réseau actuel [31] (voir **figure 24**).

Figure 24 – point d'accès D-link DWL-2100AP.

- **D-link DAP-3690 :**

Le DAP-3690 est un point d'accès extérieur robuste, de forte puissance et conçu pour les environnements difficiles. Il constitue la solution idéale pour créer des points chauds ou pour étendre des réseaux sans fil en extérieur. [32]

Figure 25 – point d'accès D-link DAP-3690.

Tableau 4 – les équipements d'interconnexion de FSEI.

Equipement	Caractéristique	Nombre	Rôle
Switch	CISCO Catalyst 2960-24PC-L	8	Pour interconnecter les APs et les ordinateurs
Point d'accès (indoor)	D-link DWL-2100AP	12	Pour interconnecter les différents clients
Point d'accès (outdoor)	D-link DAP-3690	3	Pour interconnecter les amphis

7. Critique de l'existant :

L'étude du réseau de FSEI, nous à permis de déterminer un nombre important de contraintes pouvant réduire ses performances voir sa dégradation, on a :

- L'absence d'un serveur de pare-feu pour contrôler le trafic du réseau.
- L'absence d'un serveur DHCP pour la gestion de l'adressage.
- L'absence d'un serveur DNS qui permettra la résolution de nom dans le réseau local
- Le positionnement du point d'accès du Wifi ne permet pas de couvrir toute la zone de la faculté FSEI, par conséquent certains utilisateurs ne peuvent pas accéder à internet via Wifi.
- Tous les points d'accès sont ouverts, il n'y a aucune protection du Wifi est présente.
- Au niveau du réseau câblé, l'allocation des adresses se fait de façon dynamique sans une demande d'authentification, ce qui donne l'occasion à un individu quelconque de pouvoir accéder au réseau avec son ordinateur portable via un câble réseau d'un poste du réseau câblé.
- Un seul et unique domaine de diffusion ce qui implique une surcharge du réseau de la faculté, les machines communiquent sans cesse entre elles, le trafic réseaux devient lourd, ce qui ralenti nettement la communication sur le réseau et engendre une lourdeur mêmes sur les applications et machines clients.
- L'absence d'une segmentation du réseau en VLAN.
- La faculté ne dispose pas de serveur de messagerie interne.
- Manque de liaisons sécurisées (VPN) entre la faculté et le site principal (I.T.A) ou les autres sites.
- Absence d'un local technique approprié pour loger les équipements réseau (Switch, modem-routeur, serveurs).
- L'absence d'un serveur principal pour héberger les différentes applications partagées sur le réseau.

8. Spécification des besoins :

Suite à l'étude critique de l'existant plusieurs besoins ont été relevé, à savoir:

8.1. Besoins fonctionnels :

Les besoins fonctionnels expriment une action qui doit être menée sur l'infrastructure à définir en réponse à une demande. Dans ce cadre, nous allons :

- Déployer un serveur DHCP dans le but de centraliser la gestion de l'adressage et d'éviter des conflits d'adresses IP.
- Déployer un serveur DNS qui permettra la résolution de nom dans le réseau local.
- Déployer un serveur de mail pour la gestion de la messagerie local.
- Besoin de mettre en place un serveur pare-feu pour contrôler le trafic réseaux afin de protéger le réseau interne.
- Besoin d'élargir la portée du rayonnement du Wifi afin de couvrir toute la zone souhaité.
- Besoin d'authentifier toute personne souhaitant se connecter au réseau Wifi pour accéder à internet.
- Besoin de crypter de façon efficace les données circulant sur le réseau Wifi.
- Besoin de segmenter le réseau câblé en vlan ou en sous-réseau.
- Besoin de mettre en place un serveur pour les applications partagées.
- La nécessité d'avoir un local technique approprié pour les équipements réseaux.

8.2. Besoins non fonctionnels :

Les besoins non fonctionnels représentent les exigences implicites auquel le système doit répondre. Ainsi à part les besoins fondamentaux, notre réseau doit répondre aux critères suivants :

- La simplicité d'utilisation des services implémentés.
- La centralisation de l'administration.
- La sécurité des accès (local, mot de passe : longueur, caractères spéciaux, politique de réutilisation).
- La performance du réseau (temps de réponse).
- La disponibilité (heures de connexion).
- La fiabilité (moyenne de temps de bon fonctionnement, Le temps moyen de Rétablissement).

9. Conclusion :

L'étude de l'existant nous a permis de se familiariser avec le réseau actuel de la faculté FSEI, et de comprendre les détails de l'architecture profondément, et c'est ce qui nous a permis de voir les lacunes et les faiblesses du réseau. L'étude de ces lacunes va nous aider à proposer une solution pour palier à ses dernières. Dans la prochaine partie nous allons proposer notre solution à adopter et tracé nos objectifs afin de définir un plan de travail pour mettre en œuvre cette solution.

1. Introduction :

Dans le but d'interpréter et de compléter ce qui a été traité, dans ce chapitre nous allons proposer notre solution qui peut répondre mieux aux besoins précités dans le chapitre précédent où nous entamerons la partie pratique qui consiste à définir les différents outils que nous utiliserons ainsi que les installations et les configurations requises, où nous allons citer les différentes étapes à suivre pour la mise en œuvre de la solution proposée.

2. Spécification de la solution :

Parmi les architectures que nous avons vues au le chapitre 1, nous avons pris une décision de choisir le modèle hiérarchique en trois couches, il est l'approche de choix pour la conception de réseau. Il aide à la conception, au déploiement et à la maintenance d'un inter-réseau hiérarchique évolutif, digne de confiance et économique.

2.1. Présentation de l'architecture réseau proposé :

La proposition d'une nouvelle architecture du réseau local de FSEI et ceci dans le but de rendre le réseau plus fiable au niveau de la rapidité d'échange des données et tolérant au panne et de faciliter la préparation et le changement d'information entre les départements.

Dans cette nouvelle architecture, le réseau de la faculté est scindé en deux parties : le réseau local et la DMZ. Nous voyons également sur cette architecture la liaison avec le réseau public. Dans la nouvelle infrastructure, nous disposons de deux serveurs (SVR-DC et SRV-WEB) et un firewall (pfSense) sur lesquels sont déployés les différents services. Le routeur de l'opérateur joue le rôle de passerelle entre le réseau de la faculté et le réseau public. **La figure 26** montre notre architecture réseau que nous allons réaliser :

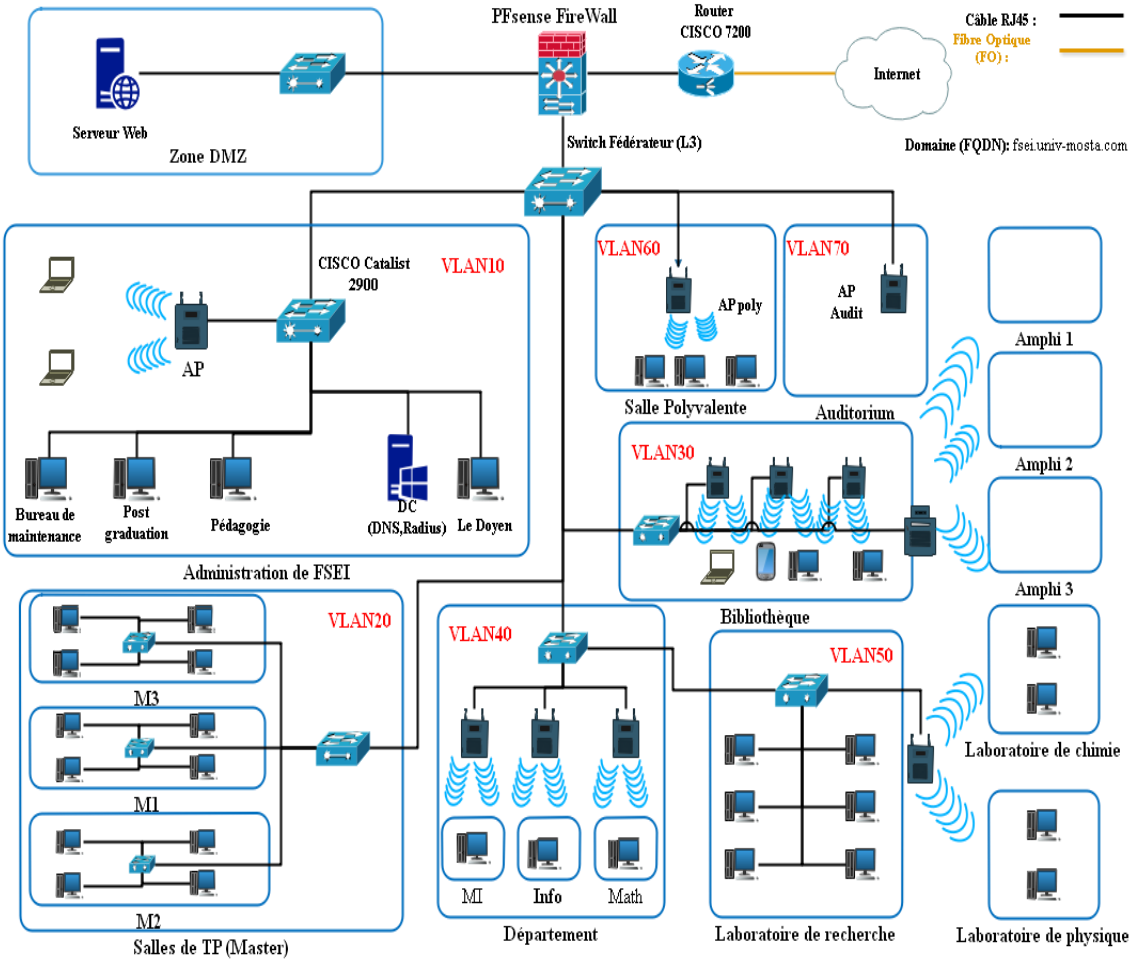

Figure 26 – la nouvelle architecture du réseau de FSEI

Dans cette nouvelle infrastructure, au niveau du réseau interne (LAN) nous disposons d'un commutateur (multi-Switch de niveau 3) sur lequel sont repartis les différents VLANs, la segmentation du réseau en utilisant les VLANs permettra de créer un ensemble logique isolé pour améliorer la sécurité du réseau en isolant les utilisateurs accédant aux données et applications sensibles.

Nous découpons le réseau LAN en plusieurs VLANs en utilisant la segmentation par sous-réseau. Chaque endroit de la faculté aurai son propre VLAN, et permettrait un échange d'informations plus rapide et sécurisé, augmentant ainsi la qualité de la bande passante.

Afin de réaliser le projet ENT (Espace Numérique de travail) de FSEI, nous avons mis en place un serveur web qui héberge l'ENT et nous avons installé et configuré un serveur AD DS qui va authentifier les utilisateurs afin de consulter à leur compte, stocke les informations de compte d'utilisateur et mettre en œuvre la politique de sécurité pour un domaine Windows. Ce dernier permet aussi de créer et de gérer des comptes utilisateur de manière centralisée et de fournir le service DNS.

2.2. Description de l'environnement de travail :

Les simulateurs de réseau sont d'excellentes ressources pour simuler certains scénarios, apprendre, obtenir des certifications et tout simplement de vieux tests. Il existe une variété de simulateurs disponibles dans la nature, mais les trois principaux que nous préférons utiliser pour différentes raisons sont VIRL, GNS3 et Packet Tracer. Lequel de ceux-ci est cependant préférable d'utiliser ? Dans ce projet nous allons utiliser GNS3 comme un simulateur préféré.

2.2.1. Comparaison entre VIRL, Packet Tracer et GNS3 :

Le premier simulateur VIRL (Virtual Internet Routing Lab) est une option pour apprendre, passer une certification ou valider une architecture avant sa mise en production. Le deuxième simulateur Packet Tracer, nous l'avons trouvé que c'était un excellent petit outil pour tester des idées de haut niveau. Il est un programme Cisco qui simule les périphériques réseau Cisco (routeurs, commutateurs). Cisco le fournit gratuitement aux centres de formation, aux étudiants, aux professionnels participant à la formation Cisco Networking Academy. Le GNS3 (Graphical Network Simulator) est l'émulateur préféré depuis si longtemps avec les études de Cisco. Il reste un excellent outil d'apprentissage et de préparation aux examens. Le tableau suivant montre la différence entre les trois simulateurs :

Tableau 5 - Comparaison entre VIRL, Packet Tracer et GNS3.

	VIRL	**Packet Tracer**	**GNS3**
Caractéristique	• Plus besoin d'acheter des équipements, faire des câblages qui peuvent te perdre du temps • VIRL fournit une application pratique de la préparation de certification de Cisco.	• Il dispose d'une large gamme de périphériques réseau. • Il simule extrêmement bien le comportement réel de l'équipement.	• GNS3 est Open Source, multiplateforme (Linux, Windows, MacOX), gratuit et fiable. • GNS3 est plus adapté pour les professionnels du réseau, puis les étudiants qui essaient de passer les examens de certification.

- Travaillant avec des images et des périphériques IOS modernes, nous pensons que VIRL est une très bonne suite. GNS3 a ses caractéristiques et fonctionnalités et est beaucoup plus facile à utiliser, beaucoup moins compliqué et nécessite beaucoup de ressources. Packet Tracer est un autre petit outil bien conçu qui peut être utilisé efficacement lors de tests et de scénarios rapides.

2.2.2. GNS3 :

GNS3 signifie Graphical Network Simulator, est un simulateur graphique de réseau qui permet l'émulation de réseaux complexe. Il est utilisé pour reproduire différentes systèmes d'exploitation dans un environnement virtuel. Il permet l'émulation en exécutant un IOS Cisco (Internetwork Operating Systems). **[30]**

- **Les composants du logiciel :**

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à:

- **Dynamips :** Emulateur d'IOS Cisco.
- **Dynagen :** Interface écrite en python et permettant l'interconnexion de plusieurs machines émulées.
- **Qemu :** Emulateur de système.
- **VMware :** Logiciel permettant la création de machines virtuelles.
- **Wireschark :** est un logiciel pour analyser les trames.

Grâce à ces composants, GNS3 nous permet :

- Le design de topologies réseaux de haute qualité et complexes.
- Emulation de plusieurs plate-formes de routeurs Cisco IOS, ou encore IPS, PIX et firewalls ASA.
- Simulation de switches Ethernet, ATM et Frame Relay.
- Connexion de réseaux simulés au monde réel.
- Capture de paquets grâce à Wireschark.

2.2.3. VMware Workstation:

VMWare Workstation est un logiciel à destination des professionnels. tout comme VMWare Player, il permet de créer des machines virtuelles et de les exécuter en même temps au-dessus d'un système d'exploitation hôte. Il propose toutefois quelques fonctionnalités plus poussées dont l'utilisateur final a rarement besoin, mais fort utiles aux professionnels de gestion de réseaux informatique.

2.3. Segmentation VLANs :

L'organisation réseau se fera en le segmentant à l'aide des VLANs. Chaque section du réseau représente un VLAN. Par conséquent, il y'aura naissance de 7 VLANs à savoir :

Administration, salle de TP, bibliothèque, département, laboratoire de recherche, salle polyvalente et l'auditorium.

2.3.1. Plan d'adressage :

Un réseau ne peut fonctionner sans une attribution et une configuration correcte de différentes adresses. Le plan d'adressage est la stratégie qui s'applique afin de permettre l'accessibilité des différentes entités d'un réseau de la manière la plus optimale.

L'objectif premier du plan d'adressage est d'éviter la duplication accidentelle des adresses, c'est-à-dire, il permet de désigner un équipement sans ambigüité, car une adresse IP affectée ne doit pas être réutilisée.

L'élaboration d'un plan d'adressage nécessite la prise en considération de certaines règles, telles que la classe d'adressage, la définition de sous-réseau, l'attribution statique et/ou dynamique des adresses.

2.3.2. Adressage des VLANs :

L'adressage du réseau local et de toutes les stations, se basera sur une adresse privée et c'est à partir de cette dernière que l'affectation des adresses IP pour l'ensemble des équipements et des VLANs va être accomplie. Les machines affiliées à un VLAN, vont

prendre toutes les adresses IP d'une même adresse sous-réseau. Le tableau suivant montre le plan d'adressage des VLANs :

Tableau 6 – Plan d'adressage des VLANs.

VLAN-id	Nom de VLAN	Adresse
10	Administration	10.10.0.0/16
20	Salle de TP	10.20.0.0/16
30	Bibliothèque	10.30.0.0/16
40	Département	10.40.0.0/16
50	Laboratoire de recherche	10.50.0.0/16
60	Salle polyvalente	10.60.0.0/16
70	Auditorium	10.70.0.0/16

3. Mise en place de la solution :

3.1. Partie matériel :

L'implémentation de notre solution doit se faire à travers des équipements de constructeur. Donc ce choix doit tenir compte de certaines compétences techniques d'une part et d'autre part de l'évolution du réseau car chaque constructeur dispose de sa technologie qui diffère les uns des autres.

Tableau 7 – Matériels utilisés.

Matériels	Quantité
Switch CISCO 3725 (L3)	1
Switch CISCO 3725 (L2)	7
Point d'accès DAP 2360	5
Router CISCO 7200	1
Serveur de pare-feu (pfSense)	2
Serveur contrôleur de domaine (AD DS)	1
Serveur web (apache)	1

3.1.1. Configuration du Switch :

La configuration d'un Switch se fait entre autre par CU (Command Line Interface). L'accès au CU se fait par console. Le port console permet de se connecter au CU du Switch même si celui-ci n'est pas déjà en réseau. Tout Switch Cisco a un port console qui est physiquement un port RJ-45. Un câble console relie un PC (via le port série ou USB) au Switch (via le port console). Une fois que le PC est physiquement connecté au port console du Switch, il faut installer et configurer un émulateur de terminal sur celui-ci. Les émulateurs de terminaux intègrent les supports pour Telnet et SSH qui permettent de configurer un Switch via le réseau.

3.1.2. Configuration de mot de passe et de nom du Switch :

Il faut savoir qu'IOS (International Standardization Organization) utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ce dispositif de sécurité, IOS peut accepter plusieurs mots de passe, ce qui nous permet d'établir différents privilèges d'accès au périphérique. Pour configurer le mot de passe et attribuer un nom au Switch, nous procédons comme suit:

```
Switch> enable
Switch# configure terminal
Switch (config)# enable secret passwd
Switch (config)# hostname switch_federateur
Switch_federateur (config)# line console 0
Switch_federateur (config-line)# password Pa$$w0rd
Switch_federateur (config-line)# login
Switch_federateur (config-line)# exit
Switch_federateur # do wr
```

3.1.3. Création de VLAN :

Nous créons un vlan en saisissant les commandes suivantes:

```
Switch_federateur # vlan database
Switch_federateur (vlan)# vlan tag_vlan  name  nom_vlan
Switch_federateur (vlan)#exit
```

Ou :

```
Switch_federateur # configure terminal
Switch_federateur (config)# vlan tag_vlan
Switch_federateur (config-vlan)# name nom_vlan
Switch_federateur (config-vlan)#end
```

3.1.4. Attribution des ports des commutateurs au VLANs :

C'est au niveau de chaque commutateur Accès que les ports vont être assignés aux différents VLANs existant. En effet, chaque port d'un commutateur appartiendra à un VLAN donné. Les commandes suivantes nous permettent d'associer un port à un VLAN en mode Accès :

```
Sw_administration (config)# interface fastethemet1/1
Sw_administration (config-if)# switchport mode access
Sw_administration (config-if)# switchport access vlan tag_vlan
```

- **Exemple: Configuration des VLANs statiques**
  - **Créer un VLAN 10 :**

Au niveau du Switch fédérateur (niveau 3) la création d'un vlan peux se faire par l'une des deux méthodes suivantes:

```
Switch_federateur # vlan database
Switch_federateur (vlan)# vlan 10 name Administration
Switch_federateur (vlan)# exit
```

Ou bien :

```
Switch_federateur # configure terminal
Switch_federateur (config)#vlan 10
Switch_federateur (config-vlan)# name Administration
Switch_federateur (config-vlan)#end
```

- **Ajouter un port au VLAN 10 :**

Au niveau du Switch d'accès (niveau 2) ajouter un ou plusieurs ports dans le vlan10, en utilisant la commande « range » pour sélectionner plusieurs ports:

```
Sw_administration (config)# interface fastethemet0/1
Sw_administration (config-if)# switchport mode access
Sw_administration (config-if)# switchport access vlan 10
Sw_administration (config-if)# end
```

```
sw_administration#show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                Fa1/12, Fa1/13, Fa1/14, Fa1/15
10   VLAN0010                         active    Fa1/1, Fa1/2, Fa1/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
sw_administration#
```

Figure 27 – création des VLANs avec des ports d'accès.

3.1.5. Configuration des liens trunk :

Un trunk est un lien entre deux équipements, le plus souvent entre deux switch, configuré de telle sorte que l'on peut y faire circuler des trames ethernet modifiées comportant des informations relatives au VLAN sur lequel elles transitent. Les commandes suivantes nous permettent d'associer un port à un vlan en mode trunk :

Au niveau switch fédérateur :

```
Switch_federateur # configure terminal
Switch_federateur (config)# switchport mode trunk
Switch_federateur (config)# switchport trunk encapsulation
dot1q
Switch_federateur (config)# no shutdown
```

Au niveau switch fédérateur :

```
Sw_administration # configure terminal
Sw_administration (config)# switchport mode trunk
Sw_administration (config)# switchport trunk encapsulation
dot1q
Sw_administration (config)# no shutdown
```

Remarque : les ports connectés entre les deux Switch doivent d'être configurer de la même façon.

3.1.6. Configuration des interfaces VLANs

La configuration des interfaces VLANs est faite au niveau du commutateur multifonction en donnant des adresses IP pour le VLAN (voir **figure 28**).

```
Switch_federateur(config)#interface vlan 10
Switch_federateur(config-if)#
*Mar  1 00:17:32.667: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, ch
anged state to up
Switch_federateur(config-if)#ip address 10.10.0.11 255.255.0.0
Switch_federateur(config-if)#no shutd
Switch_federateur(config-if)#no shutdown
Switch_federateur(config-if)#do wr
Building configuration...
[OK]
Switch_federateur(config-if)#
```

Figure 28 – configuration des interfaces VLANs.

Pour que le commutateur puisse router entre les VLAN, les interfaces VLAN doivent être configurées avec une adresse IP. Lorsque le commutateur reçoit un paquet destiné à un autre VLAN, il examine la table de routage afin de déterminer où transférer le paquet. Le paquet est ensuite transmis à l'interface VLAN de la destination. Il est à son tour envoyé au port où le périphérique final est connecté.

La commande suivante nous permet de voir notre table de routage :

```
Switch_federateur # show ip route
```

```
Switch_federateur#sh  ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/16 is subnetted, 7 subnets
C       10.10.0.0 is directly connected, Vlan10
C       10.30.0.0 is directly connected, Vlan30
C       10.20.0.0 is directly connected, Vlan20
C       10.40.0.0 is directly connected, Vlan40
C       10.60.0.0 is directly connected, Vlan60
C       10.50.0.0 is directly connected, Vlan50
C       10.70.0.0 is directly connected, Vlan70
Switch_federateur#
```

Figure 29 – la table de routage.

3.2. Partie logiciel :

3.2.1. Mise en place de pare-feu Pfsense :

➢ **Définition :**

Pfsense est un logiciel open source tournant sous FreeBSD. Il possède les fonctionnalités d'un pare-feu mais également d'un routeur. Il permet d'intégrer également de nouveaux services tels que l'intégration d'un portail captif, la mise en place d'un VPN, et bien d'autres.

➢ **Fonctionnalités Pfsense est :**

- Un fournisseur de services tel que :
  - Serveur de temps : NTPD.
  - Relais DNS.

- Serveur DHCP.
- Portail captif de connexion.

- Un routeur entre un WAN et un LAN, différents segments, VLANs, DMZs :
  - il implémente les protocoles RIP, OLSR, BGP.
  - il permet de mettre en place des VPNS : OpenVPN,IPsec, PPTP.
- Un firewall capable de :
  - faire de la traduction d'adresses : NAT, SNAT, DNAT.
  - faire du filtrage de paquets entre WAN et LAN et entre deux réseaux reliés par VPN.
  - faire de la QoS : « traffic shaper ».
  - faire du « load balanching » avec plusieurs connexions Internet.

➢ **Installation et Configuration :**

La distribution peut s'installer directement depuis une image ISO disponible sur pfsense.org. Pfsense peut s'installer sur plusieurs types de hardware. La configuration minimum recommandée :

- CPU : 1Ghz
- RAM : 1 Go
- Disque dur : 20Go
- Catre réseau : 2 (WAN et LAN, dans notre cas nous utiliserons 3 cartes réseaux où la 3ème est DMZ).

➢ **Installation :**

Pour procéder à l'installation de pfSense, il est nécessaire dans un premier temps de télécharger la distribution au format ISO. Après avoir préparé notre média, nous pouvons démarrer dessus et débuter la configuration :

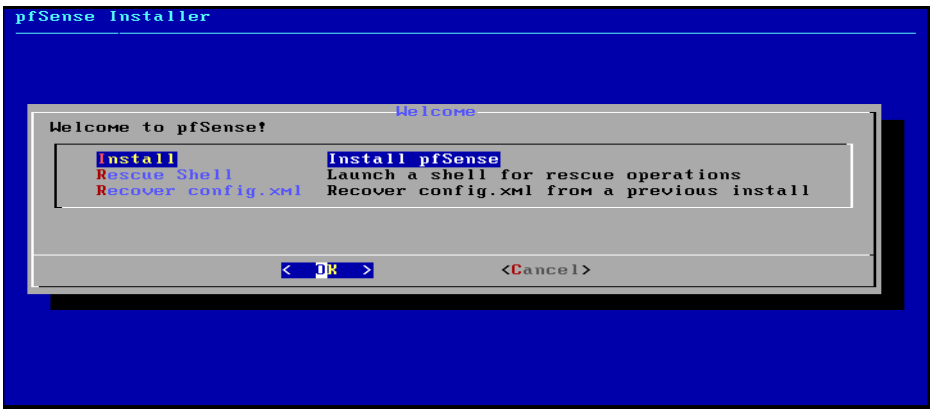

Figure 30 – installation Pfsense (étape 1).

- ➢ Sélectionnez « install pfSense »
- ➢ Sélectionnez votre clavier
- ➢ Sélectionnez auto pour le partitionnement des disques

Durant l'installation Pfsense va détecter automatiquement les listes des cartes réseaux disponibles, et va y attribuer respectivement em0, em1 et em2. Notez bien qu'il nécessite au moins deux cartes pour qu'il fonctionne correctement.

L'installation se termine ici, nous avons plein d'options à explorer (voir **la figure 31**). Par la suite toutes les configurations se font par l'intermédiaire d'une intuitive interface web.

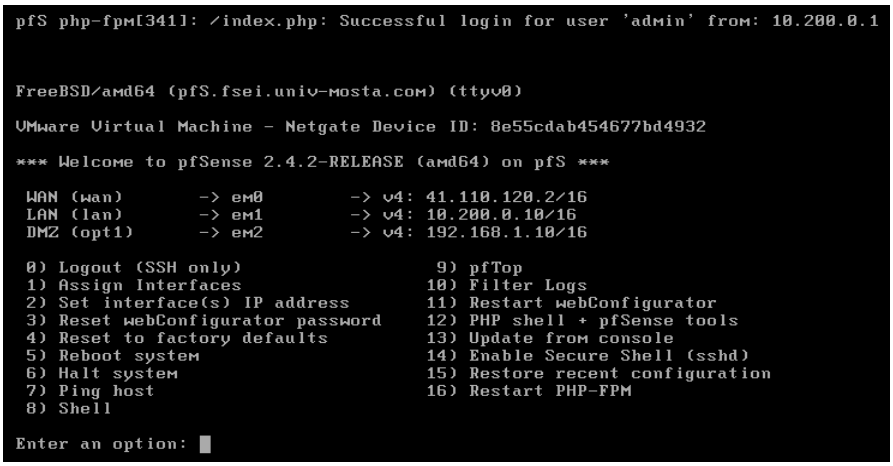

Figure 31 – L'écran d'accueil de Pfsense.

- **Configuration :**

Pour se connecter à l'interface de configuration nous utiliserons l'adresse IP de l'interface LAN, dans notre cas c'est http://10.200.0.10, le couple login/password par défaut est admin/pfsense.

Après authentification avec le login admin et le mot de passe, il est possible de finaliser la configuration. Elle se réalise en 9 étapes :

- Configuration du nom du boitier, du domaine, des serveurs DNS
- Configuration du serveur de temps
- Configuration de l'interface WAN
- Configuration de l'IP LAN
- Configuration du mot de passe admin
- Finalisation de l'installation

Notre Dashboard peut être personnalisé pour ressembler à cela :

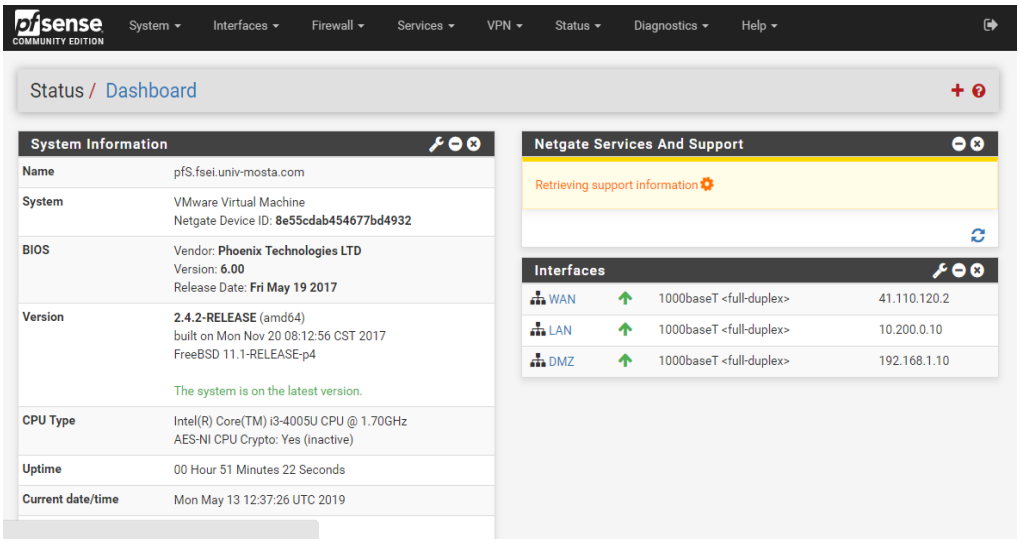

Figure 32 – Le Dashboard de Pfsense.

Le Dashboard permet d'avoir une vision complète sur l'état de santé de notre équipement : indicateurs sur l'état de nos interfaces, la charge du boitier, les sessions, les débits.

3.2.2. Mise en place de Windows serveur 2012 :

➢ **Présentation :**

Windows Server 2012 R2 est le résultat de toute l'expérience de Microsoft dans la fourniture de services dans le Cloud à l'échelle mondiale. Il représente à la fois un serveur de haut niveau pour les entreprises et une plateforme dans le Cloud. Il permet d'optimiser les performances pour les scénarios les plus stratégiques et protège contre des ruptures de services par l'utilisation d'options de récupération très fiables. Il réduit la complexité et les coûts grâce à une automatisation complète et à des solutions de virtualisation du réseau et du stockage sur du matériel standard. Enfin, il permet aux utilisateurs un accès à distance de n'importe où, à partir de n'importe quel appareil, tout en protégeant les informations de l'entreprise [30].

La gamme de produits Windows Server 2012 a été simplifiée afin de choisir plus facilement l'édition qui convient le mieux :

- Édition Datacenter pour les environnements de Cloud privés fortement virtualisés.
- Édition Standard pour les environnements peu ou pas virtualisés.
- Édition Essentials pour les petites entreprises comptant jusqu'à 25 utilisateurs, avec un serveur à 1 ou 2 processeurs.
- Édition Foundation pour les petites entreprises comptant jusqu'à 15 utilisateurs avec un serveur monoprocesseur.

Dans notre cas nous avons utilisé l'édition standard car c'est la mieux adaptée à notre environnement.

➢ **Installation et configuration du serveur Active Directory :**

- **Définition :**

Active Directory est le service d'annuaire de la famille Windows Server 2012. C'est un service réseau qui identifie toutes les ressources d'un réseau et met ces informations à la disposition des utilisateurs ainsi que des applications. Les services d'annuaires sont importants, car ils fournissent un moyen cohérent de nommer, décrire, localiser, administrer et sécuriser les informations relatives à ces ressources et d'y accéder. Lorsqu'un utilisateur recherche un dossier partagé sur le réseau, le service d'annuaire identifie la ressource et fournit l'information à l'utilisateur [32].

➢ **Les composants de l'Active Directory :**

Active directory se compose de plusieurs services dont [26] :

- **Active Directory Certificate Services (AD CS) :** Ces services fournissent les fonctions nécessaires pour émettre et révoquer les certificats numériques des utilisateurs, des ordinateurs clients et des serveurs.
- **Active Directory Domain Services (AD DS) :** Ces services AD DS procurent les services d'annuaire essentiels à l'établissement d'un domaine.
- **Active Directory Federation Services (AD FS) :** Ces services AD FS complètent les fonctionnalités d'authentification et de gestion d'accès des Services AD DS en les développant pour le World Wide Web.
- **Active Directory Lightweight Directory Services (AD LDS) :** Ces services AD LDS fournissent un magasin de données pour les applications fonctionnant avec l'annuaire qui

ne nécessitent pas les Services AD DS et qui n'ont pas besoin d'être déployées sur des contrôleurs de domaine.

- **Active Directory Rights Management Services (AD RMS) :** Ces services AD RMS procurent une couche destinée à protéger les informations d'une organisation et qui peut s'étendre hors de l'entreprise, protégeant ainsi les messages électroniques, les documents et les pages Web de l'intranet, contre tout accès non autorisé.

➢ **Configuration d'Active Directory**

La première étape consiste à configurer le nom de la machine et l'adresse IP du serveur local :

- Le nom de la machine est FSEI-DC.
- L'adresse IPv4 c'est une adresse statique de classe B : 10.10.0.50 (voir figure 33).

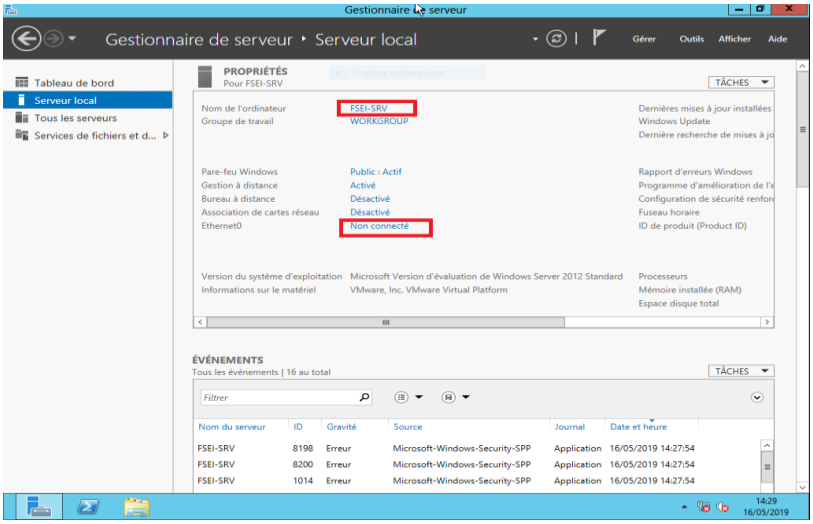

Figure 33 – Configuration du serveur local.

La deuxième étape comprend l'ajout du rôle d'Active Directory au serveur local (voir figure 3.5), pour cela nous allons :

- Depuis le gestionnaire de serveur, cliquer sur ajouter des rôles et fonctionnalités.
- Sélectionner le type d'installation " installation basée sur un rôle ou fonctionnalité ".
- Notre serveur et le seul du réseau, le choisir dans le pool de serveurs.
- Cocher le rôle service AD DS (Active Directory Domain Service).

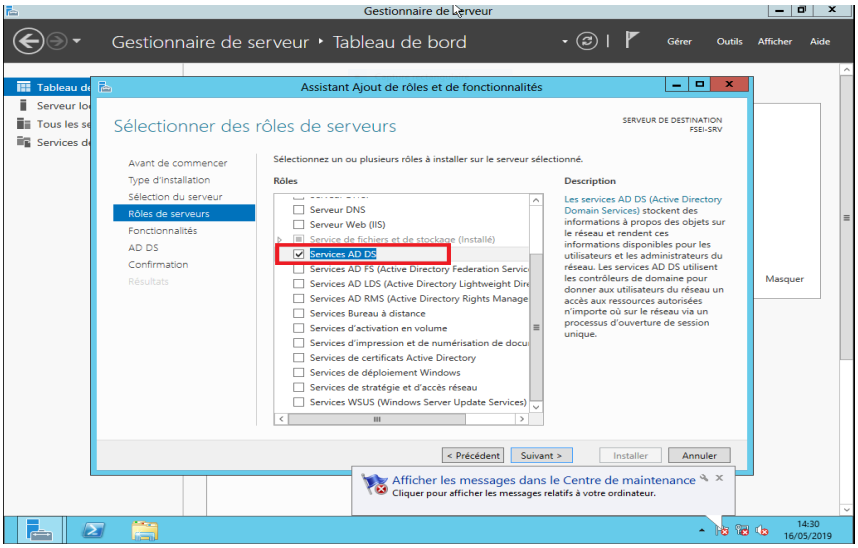

Figure 34 – l'ajout du rôle AD DS.

Apres l'installation d'Active Directory Domain Service, le système va redémarrer automatiquement. Dans la troisième, nous devons promouvoir ce serveur entant que contrôleur de domaine sinon le domaine ne sera pas créé (voir **la figure 35**).

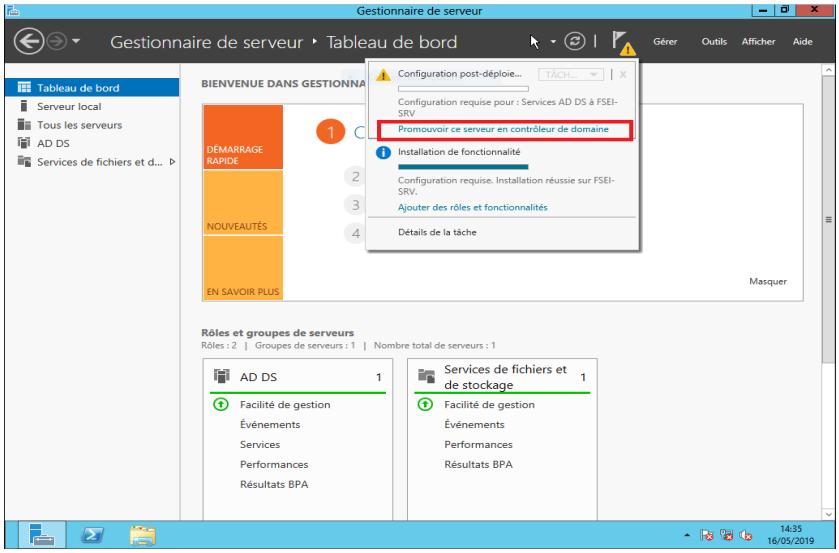

Figure 35 – Promouvoir le serveur en contrôleur de domaine.

Apres avoir cliqué sur " promouvoir ce serveur en contrôleur de domaine ", l'assistant nous demande de créer une nouvelle forêt sous le nom "fsei.univ-mosta.dz" (voir **la figure 36**).

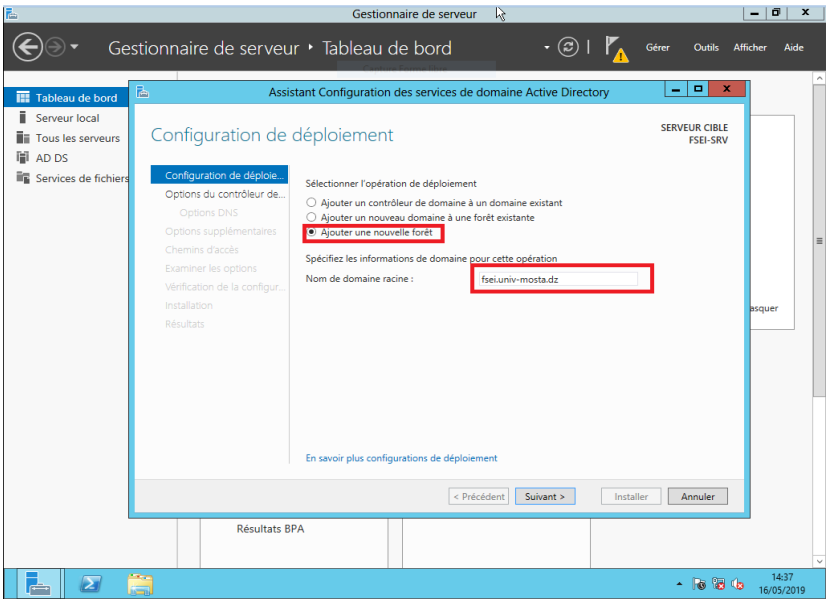

Figure 36 – Ajout d'une nouvelle forêt.

Lorsque la forêt et le domaine seront créés, le niveau fonctionnel de la nouvelle forêt est sélectionné par défaut, et nous laissons cocher l'ajout de la fonctionnalité du serveur DNS. Puis insérer le mot de passe du mode de restauration du service d'annuaire (DSRM) voir **la figure 37** :

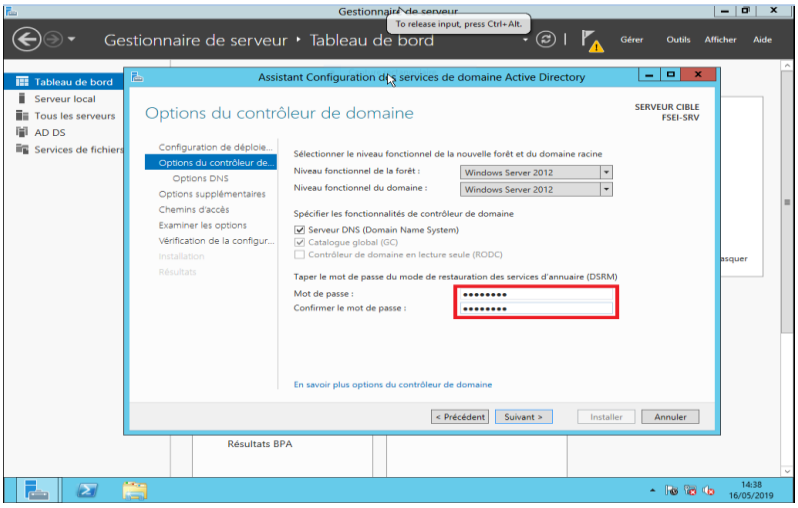

Figure 37 – Options de contrôleur de domaine.

Une erreur apparait sur l'écran suivant, ce message survient car aucun serveur DNS n'est installé sur la machine, nous cliquons simplement sur suivant pour le créer automatiquement, car c'est grâce à lui que les clients (postes utilisateurs ou serveurs membres du domaine) vont pouvoir trouver le serveur DC.

- Indiquer un nom NetBIOS au domaine "FSEI".
- Laisser les valeurs suivantes par défaut (NTDS et SYSVOL).
- L'installation est prête et un récapitulatif est affiché dans la figure 38 pour vérifier la configuration.

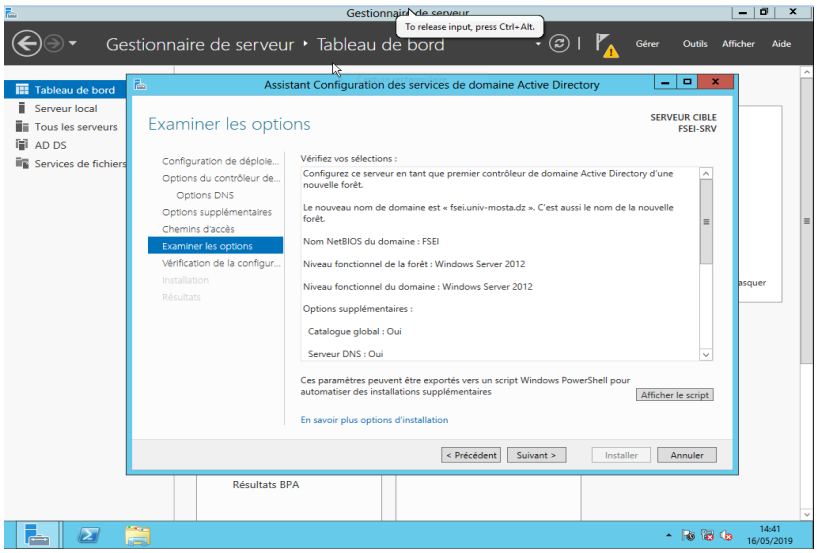

Figure 38 – Examiner les options.

Après configuration le serveur redémarre automatiquement, à présent, les outils de gestion d'active directory sont présents dans le menu outils, notre domaine est créé et l'ouverture de session se fait avec le compte administrateur du domaine " FSEI/Administrateur ".

4. Administration de la solution

4.1. Création et configuration du VLAN Pfsense :

Nous devons maintenant créer et configurer les 7 VLANs dans pfSense que nous avons crées avant dans le Switch fédérateur, pour ce faire Accédez à Interfaces-> Assignments et notez le nom du pilote de périphérique attribué à la carte réseau local. Dans notre cas, nous supposerons que le nom du pilote de périphérique est «em1» (voir **la figure 39**). L'interface LAN servira d'interface parent pour les interfaces VLAN que nous allons créer à l'étape suivante.

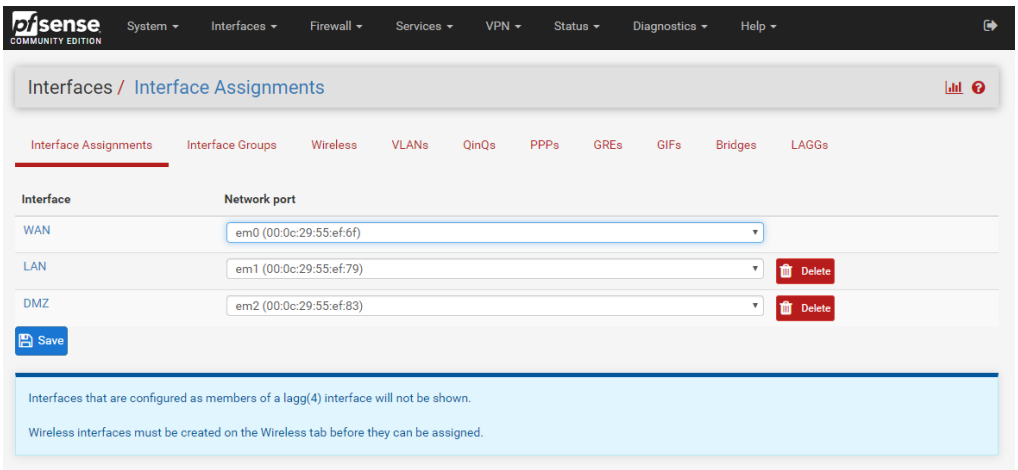

Figure 39 – l'affectation des interfaces.

Ensuite, accédez à Inerfaces-> Assignments-> VLANs et sélectionnez l'icône "+ Ajouter". Dans l'écran suivant, sélectionnez "em1", l'interface de la carte réseau local, parmi les options de la liste déroulante située sous "Interface parent", puis entrez la valeur 10 sous "Balise

VLAN". Ajoutez une description facultative pour ce VLAN sous «Description» où dans notre cas c'est le « VLAN10_administration », puis sélectionnez «Enregistrer» (voir **Figure 40**).

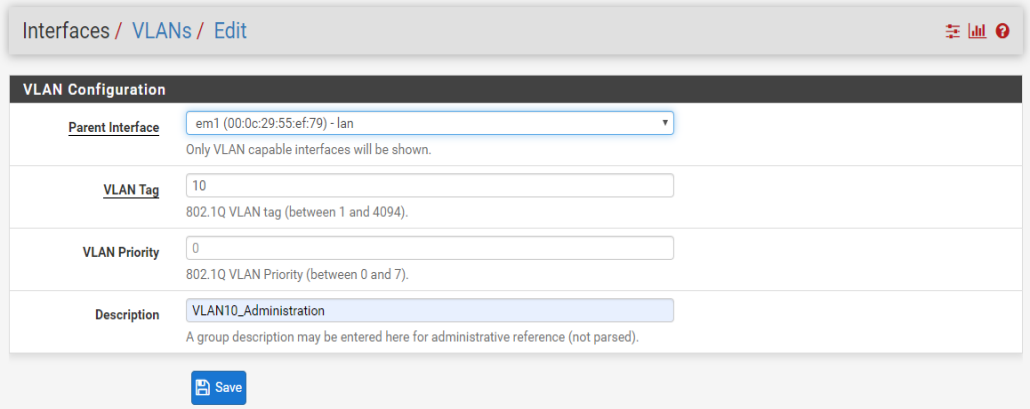

Figure 40 – création de VLAN 10 d'administration.

Après avoir créé l'interface VLAN, retournez dans Interfaces-> Assignments et sélectionnez l'icône "+ Ajouter" pour ajouter le "VLAN 10 sur em1-lan (VLAN10_administration)", puis sélectionnez "Enregistrer" (voir la **Figure 41**). pfSense va désigné le VLAN 10 comme une interface optionnelle ou «OPT».

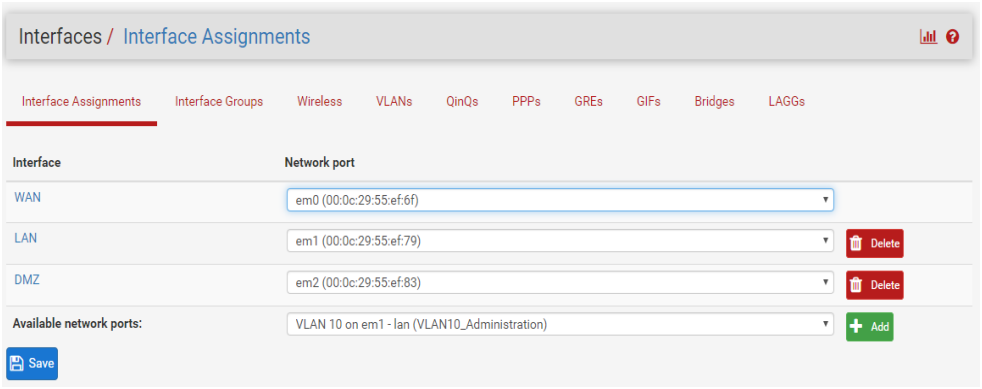

Figure 41 – affectation de l'interface VLAN 10.

Ensuite, nous supposons que pfSense a affecté le VLAN 10 à OPT2. Accédez à Interfaces-> OPT2 et sélectionnez «Activer l'interface». Sous «Description», remplacez «OPT2» par le nom de VLAN ce qui est « VLAN10_Administration », puis sélectionnez «IPv4 statique» parmi les options de la liste déroulante sous «Type de configuration IPv4». Nous allons utiliser le réseau 10.10.0.0/16 pour le VLAN 10 en attribuant l'adresse IP statique 10.10.0.2 sur cette interface et en sélectionnant le masque de réseau de «16» dans la section «Configuration IP statique». Les autres paramètres peuvent rester à leurs valeurs par défaut. Sélectionnez «Enregistrer» et «Appliquer les modifications» lorsque vous avez terminé (voir **la figure 42**). Maintenant, si nous revenons à Interfaces-> Assigments, le VLAN 10 sera répertorié et étiqueté avec la description que nous avons ajoutée lors de l'activation de l'interface lors des étapes précédentes.

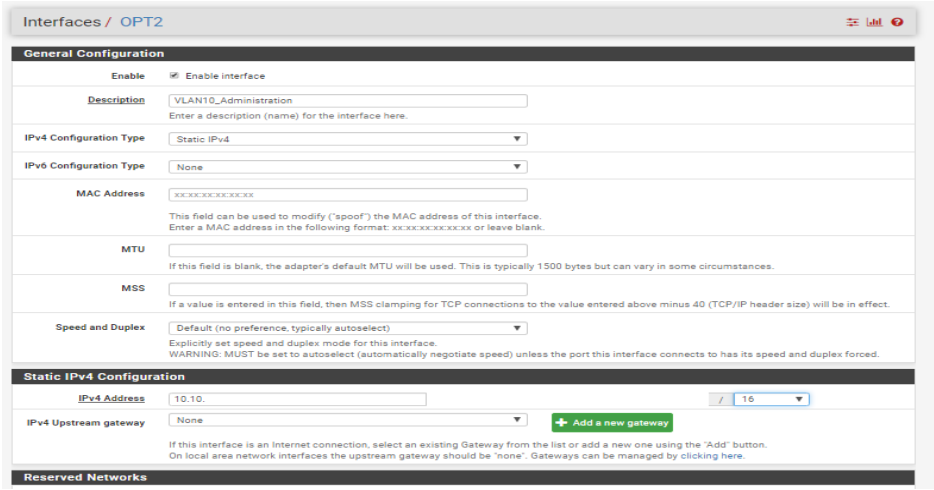

Figure 42 – configuration de VLAN 10.

4.1.1. Configuration des règles de pare-feu Pfsense :

Nous devons créer une règle de pare-feu pour nos VLANs afin que le trafic puisse passer de / vers l'interface de réseau étendu (WAN) et par extension, vers Internet. Naviguez vers Firewall-> Rules et sélectionnez le VLAN10_administration. Sélectionnez l'icône «Ajouter» (il n'existe actuellement aucune règle) pour créer une nouvelle règle. Dans notre cas, nous allons créer une règle de passe sortante simple pour tout protocole dans le VLAN10_administration, similaire à la configuration d'une règle de passe sortante de réseau local. Sélectionnez "any" parmi les options de la liste déroulante Sous "Protocole" et sous "Source", sélectionnez "VLAN10_administration net" parmi les options de la liste déroulante. Les autres paramètres peuvent rester à leurs valeurs par défaut. Sélectionnez «Enregistrer» et «Appliquer les modifications» lorsque vous avez terminé (voir **la figure 43**).

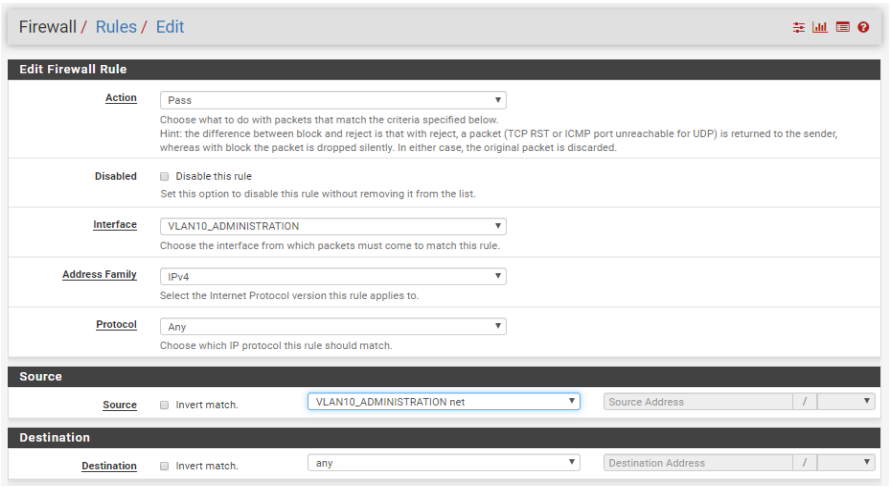

Figure 43 – Création des règles pour VLAN 10.

4.1.2. Configuration du serveur DHCP (Pfsense) :

Nous devons configurer un serveur DHCP pour les nouveaux VLANs que nous avons crées. Pour ce faire, Accédez à Services -> DHCP server et sélectionnez VLAN10_administration. Sélectionnez «Activer le serveur DHCP sur l'interface VLAN10_administration», puis entrez la plage d'adresses IP du réseau 10.10.0.0/16 que vous souhaitez que le serveur DHCP utilise sous «Plage». Enfin, pfSense utilisera l'adresse IP

attribuée à cette interface comme adresse de passerelle par défaut. Pour notre exemple, cette adresse sera 10.10.0.2. Les autres paramètres peuvent rester à leurs valeurs par défaut. Sélectionnez «Enregistrer» lorsque vous avez terminé (voir **la figure 44**).

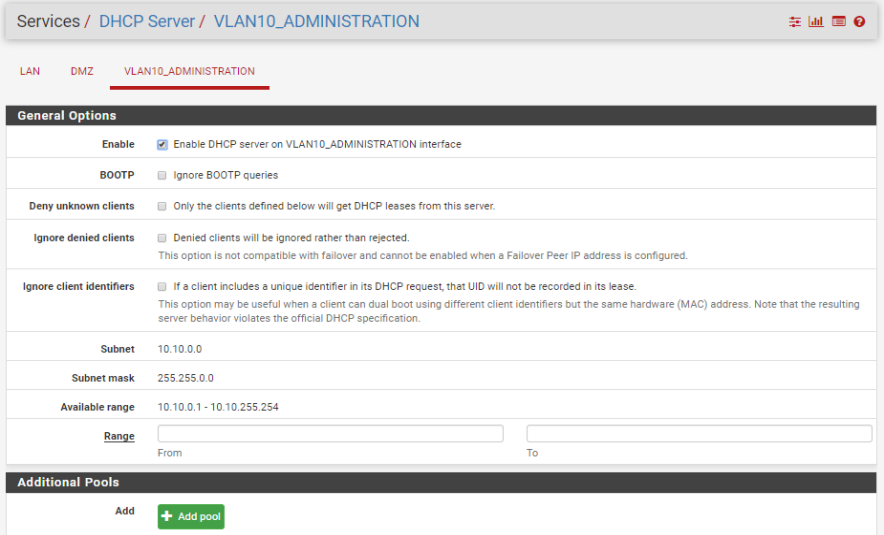

Figure 44 – configuration du serveur DHCP de VLAN 10.

4.2. Configuration de pfSense avec l'authentification Active Directory :

Avec pfSense, il est possible de déclarer la connexion à un AD pour authentifier les utilisateurs, pour déléguer l'administration du pare-feu. Par exemple, nous allons définir un groupe qui aura le droit de configurer le pare-feu, on va attribuer des droits à un groupe, et ce groupe correspond à un groupe de l'AD.

4.2.1. Déclarer l'annuaire Active Directory sur pfSense :

Première étape, nous devons connecter à la WebGUI de notre pfSense avec un compte administrateur. Ensuite cliquez sur le bouton « System » puis « User Manager » qui permet de gérer les utilisateurs et les groupes pfSense, ainsi que de configurer un serveur d'authentification. Puis cliquez sur l'onglet « authentification servers » (voir la figure 45).

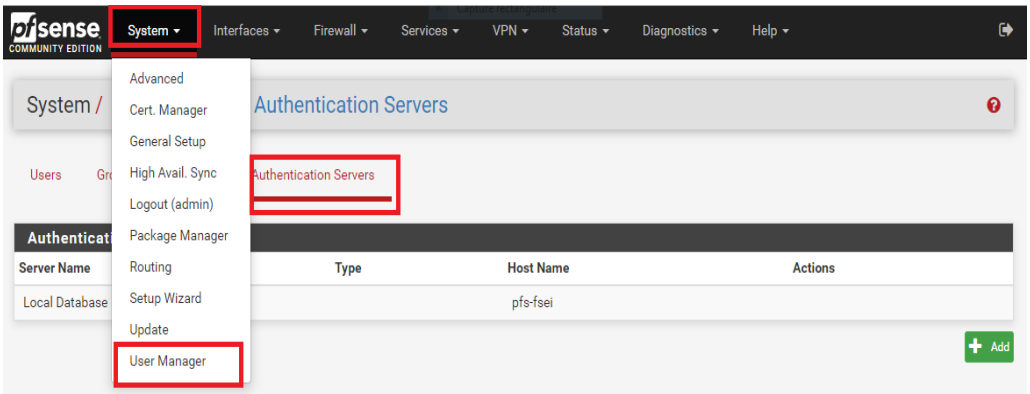

Figure 45 – interface de gestionnaire d'utilisateurs (pfSense).

L'écran ci-dessus montre l'onglet des serveurs où nous allons ajouter notre serveur AD DC dans pfsense pour l'authentification. Cliquer sur "+ add" pour ajouter le serveur AD DC (voir **la figure 46**).

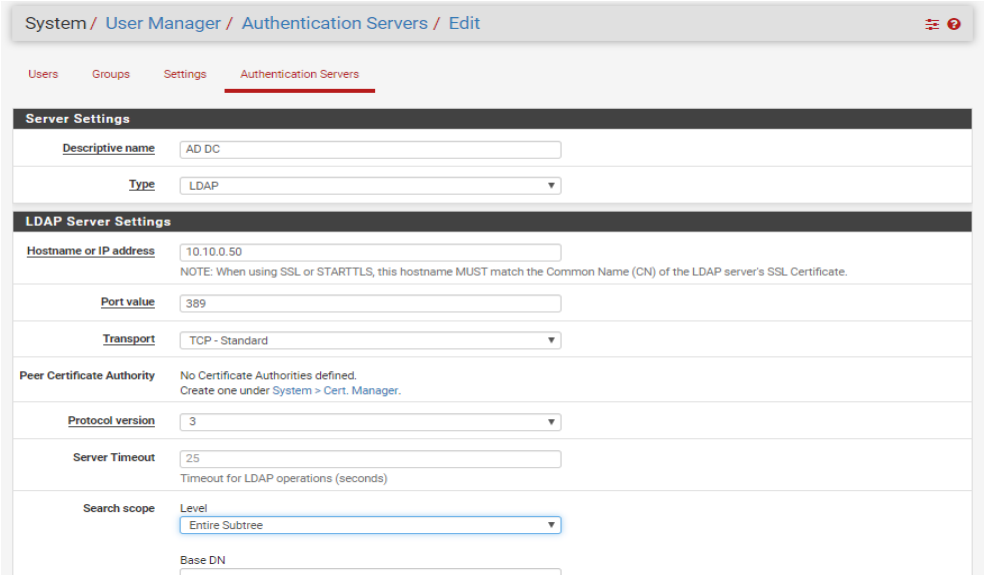

Figure 46 – l'ajout du serveur d'authentification AD DC.

Nom descriptif : nous pouvons entrer le nom de notre choix.
Type : Sélectionnez LDAP puisqu'il s'agit d'une authentification AD
Nom d'hôte ou adresse IP : nous pouvons taper le nom de domaine complet (FQDN) ou l'adresse IP de notre centre de distribution AD.
Valeur du port : Que ce soit par défaut
Transport : Valeur par défaut
Version du protocole : Valeur par défaut
Portée de la recherche : Sélectionner une sous-arborescence entière
DN de base : ici nous devons entrer les conteneurs de notre contrôleur de domaine. Assurez-vous de diviser les conteneurs correctement. Dans notre cas c'est « DC=fsei,DC=univ-mosta,DC=com ».
Conteneurs d'authentification : C'est ici que l'authentification s'intéresse. Par conséquent, assurez-vous de sélectionner ou de taper les conteneurs correctement. Dans notre cas c'est « OU=administrateurs,DC=fsei,DC=univ-mosta,DC=com ».

4.2.2. Configuration du serveur d'authentification AD DC :

Pour créer un compte avec un tel privilège, nous avons crée une unité d'organisation « administrateur », également appelé « OU » qui contient des utilisateurs et un groupe qui s'appelle « AD » contient les utilisateurs qui doivent avoir accès à pfSense.

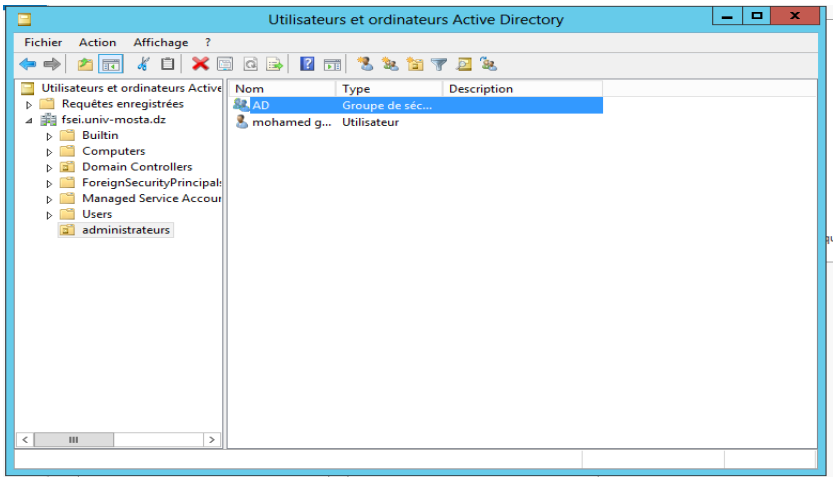

Figure 47 – configuration du serveur AD DC.

4.2.3. Déclarer le groupe local dans pfSense :

Dans pfSense, nous devons crée un groupe local qui aura le même nom que le groupe Active Directory, ceci permettra à pfSense de faire le lien entre les membres du groupe Active Directory et les droits positionnés sur le groupe pfSense.

Dans System, User Manager, accédez à l'onglet "Groups" et cliquez sur "Add" (voir la figure 48).

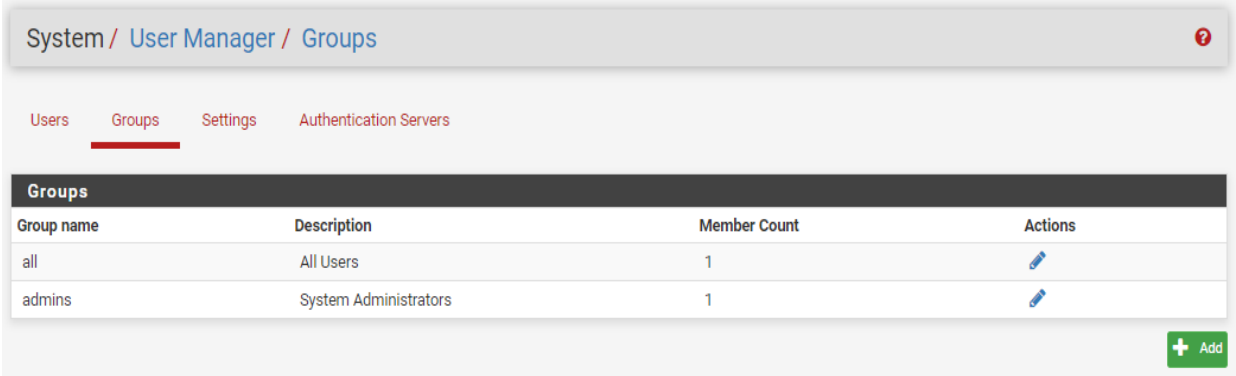

Figure 48 – les groupes locaux (pfSense).

Nommez ce groupe comme celui de l'AD, donc dans notre cas c'est "**AD**". Au niveau du scope, lorsqu'il s'agit d'un groupe Active Directory, il faut normalement indiquer "Remote" à la place de "Local" (voir la figure 49).

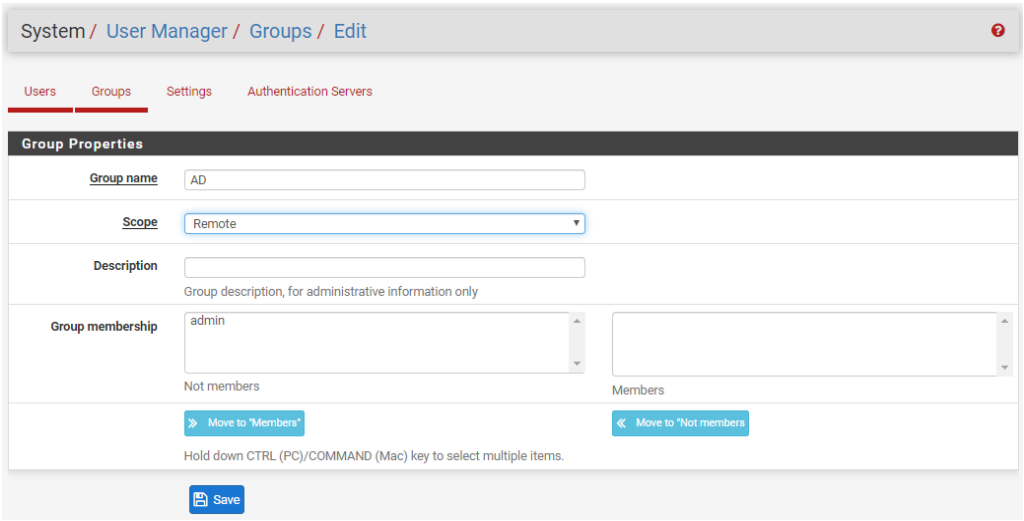

Figure 49 – création d'un groupe locale (pfSense).

Après l'enregistrement de ce groupe, nous devons l'attribuer des droits, pour ce faire cliquez sur l'icône en forme de crayon pour éditer le groupe fraîchement créé. Ensuite, toute la liste des privilèges apparaît, nous pouvons gérer finement les droits. C'est intéressant pour avoir une délégation précise (voir **la figure 50**).

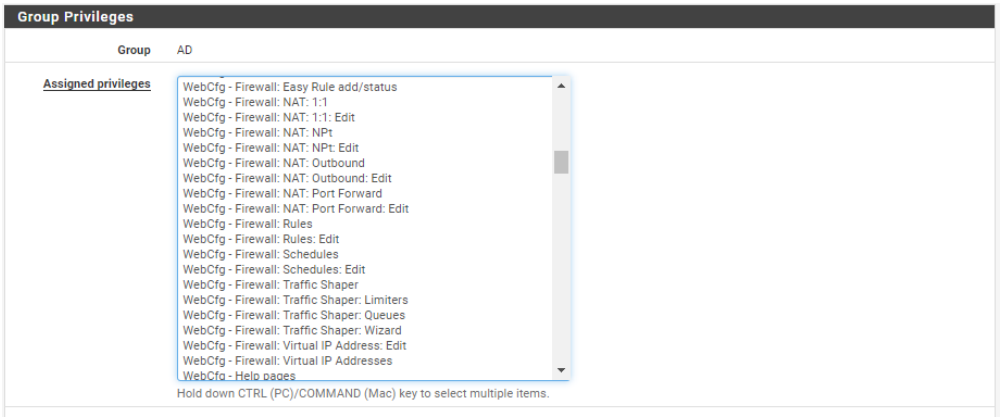

Figure 50 – les privilèges de groupe.

Maintenant, pour tester la connexion à la WebGUI pfSense avec un compte AD allez vers "*Diagnostics*", cliquez sur "*Authentication*". Nous devons choisir AD DC comme serveur d'authentification puis tester un login et un mot de passe qui est censé fonctionner. (Voir la figure 51) :

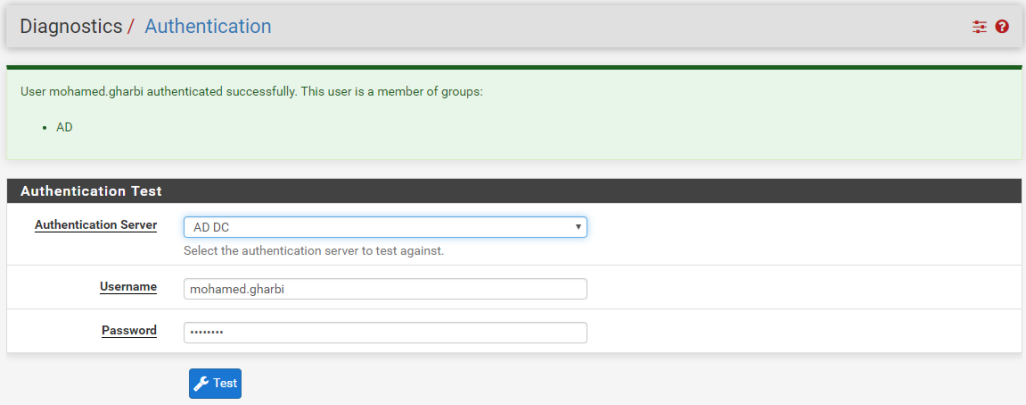

Figure 51 – teste de la connexion à la WebGUI pfSense avec un compte AD.

4.3. Gestion et administration des utilisateurs Active Directory :

4.3.1. Création des unités d'organisation :

Unité d'Organisation (OU) est un conteneur dans un domaine Microsoft Active Directory qui peut contenir des utilisateurs, des groupes et des ordinateurs. Il est la plus petite unité par laquelle, un administrateur peut affecter des paramètres de stratégie de groupe ou des autorisations de compte.

1. Pour créer une OU dans Active Directory, nous avons besoin d'ouvrir la console "Utilisateurs et Ordinateurs Active Directory ". nous pouvons la lancer depuis le *Gestionnaire de serveur* puis sous la rubrique *AD DS*. Un clic droit sur notre serveur puis on choisit *Utilisateurs et ordinateurs Active Directory* (voir **la figure 52**).

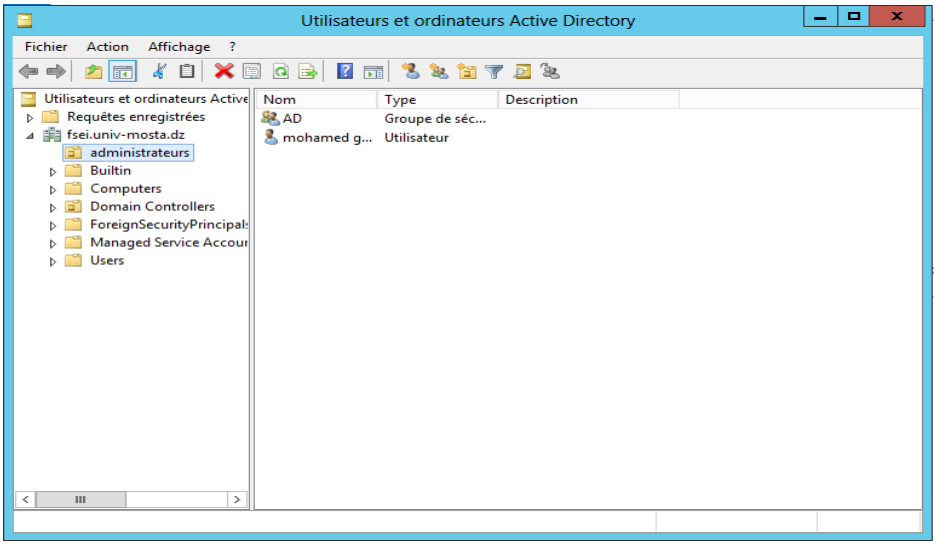

Figure 52 – Utilisateurs et ordinateurs Active Directory.

Nous allons créer une unité organisationnelle afin d'y mettre l'ensemble des utilisateurs et groupes mise en place pour ces utilisateurs dans le cadre de notre faculté. Nous allons créer 4 OU tels que : Administrateurs, enseignant, étudiant et personnel. Pour ce faire, un clic droite dans la fenêtre de droite, puis *Nouveau* et on choisit *Unité d'organisation* (voir **la figure 53**).

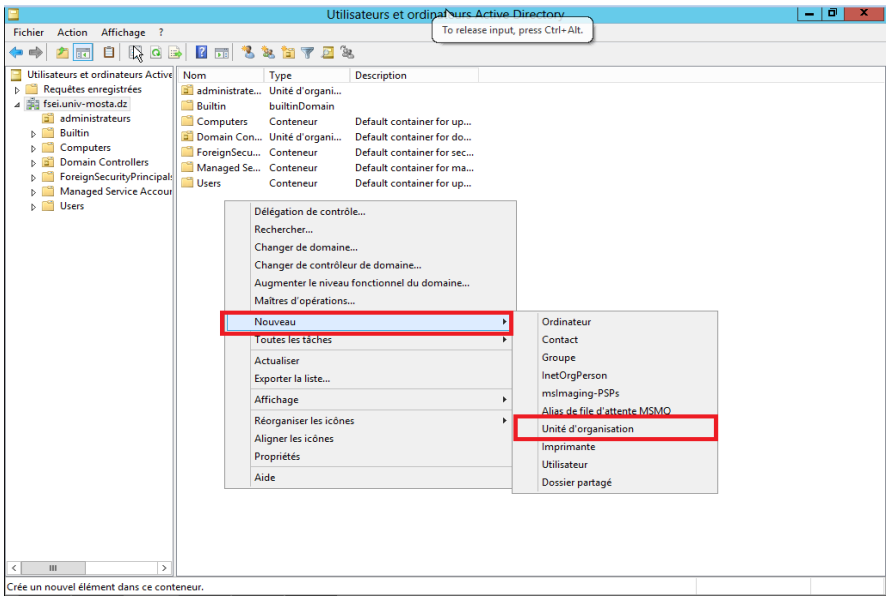

Figure 53 – création d'une unité d'organisation (OU).

4.3.2. Création des utilisateurs :

Nous avons créé des unités organisationnelles. Maintenant, nous pouvons créer les utilisateurs de notre faculté tels que les administrateurs, les enseignants et les étudiants pour appliquer après les stratégies de groupe. Pour ce faire, une clique droite ensuite *Nouveau* puis *Utilisateur*.

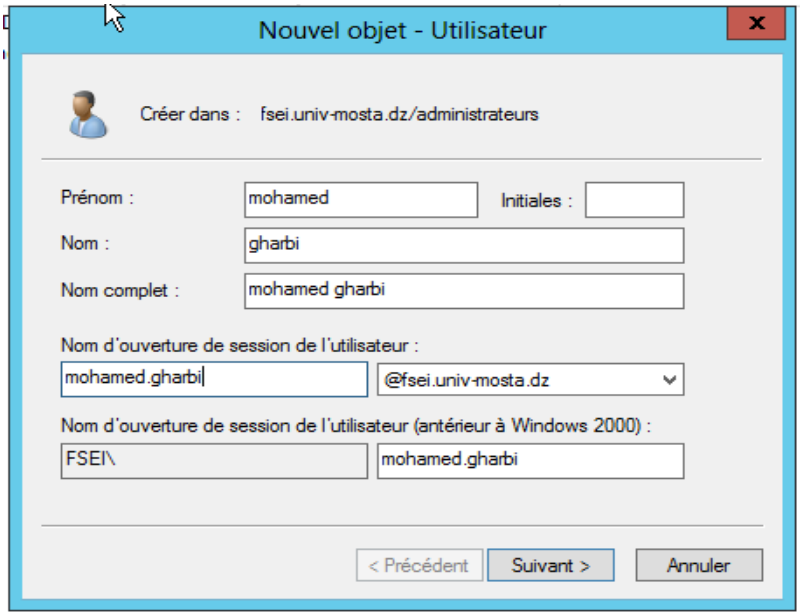

Figure 54 – Création des utilisateurs AD DS.

4.3.3. Implémentation des stratégies de groupe :

La Stratégie de Sécurité (Group Policy Object) est définit comme un ensemble des configurations et paramètres permettant la gestion des ordinateurs et des utilisateurs répertoriés dans un annuaire Active Directory. Une GPO est la manière la plus simple de configurer des paramètres appelés "Stratégies de Sécurité" qui seront appliqués sur des utilisateurs et des ordinateurs.

Après avoir créé les unités d'organisation de la faculté, Nous allons crée et appliqué par exemple une stratégie de groupe sur notre OU étudiant afin d'empêcher les étudiants d'exécuter des programmes et scripts sur les postes de travail. Notre GPO sera nommée «No_executer_Progrm ».

Pour ce faire, ouvrez la console de Gestion de stratégie de groupe > Ouvrez la liste déroulante (Forêt / Domaine / nom de votre domaine) > Clic droit sur l'OU étudiant > Créer un objet GPO dans ce domaine, et le lier ici…

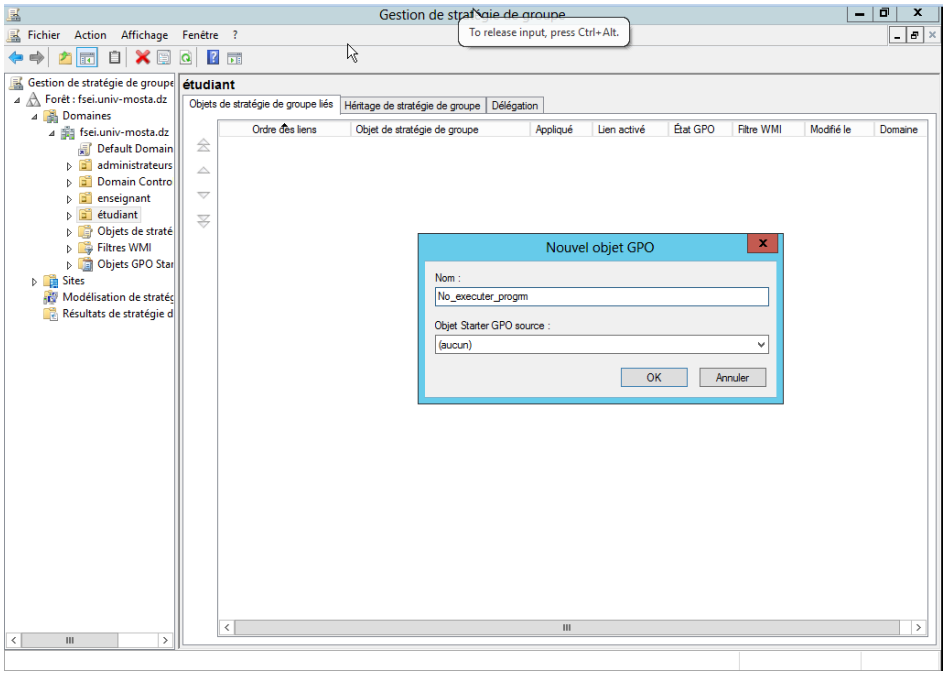

Figure 55 – création une stratégie de groupe (GPO).

La configuration de cette stratégie de groupe se fait à partir de la console éditeur de gestion des Stratégies de groupe. Développer **Configuration de l'ordinateur**, puis **Stratégie**, puis **Paramètre Windows**, puis **Paramètre de Sécurité**, puis **Stratégie de contrôle de l'application**, puis **AppLocker**. Nous allons réaliser 4 configurations qui sont :

1. Générer les règes par défaut : Faire un clic droit sur règles de l'exécutable (même chose pour règles de script) et cliquer soit sur « Créer des règles par défaut » ou sur « générer automatiquement les règles ». Dans notre cas, nous utilisons la deuxième option qui nous permet de spécifier le dossier d'analyse « Download » et à personnaliser les autorisations (voir **la figure 56**).

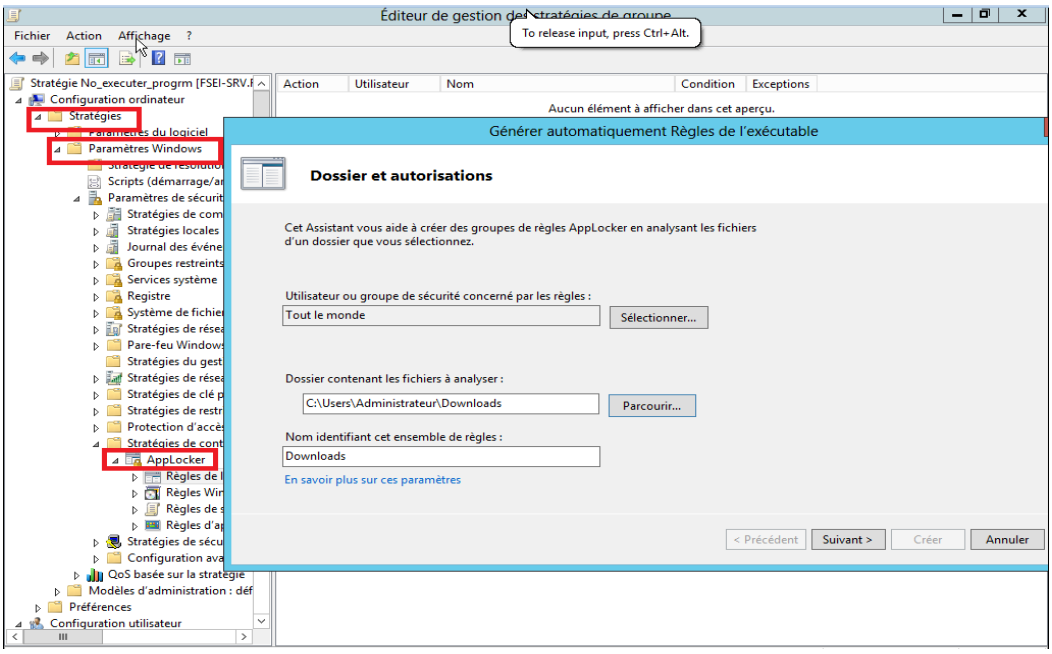

Figure 56 – Générer les règes par défaut.

2. Configurer les règles de l'exécutable (même procédure pour les règles de script) : clic droit sur règles de l'exécutable pour empêcher l'exécution des programme (règles de script pour empêcher l'exécution des scripts), puis cliquer sur « Créer une règle ». Dans la rubrique Autorisation, sélectionner « Refuser » et poursuivre les instructions.

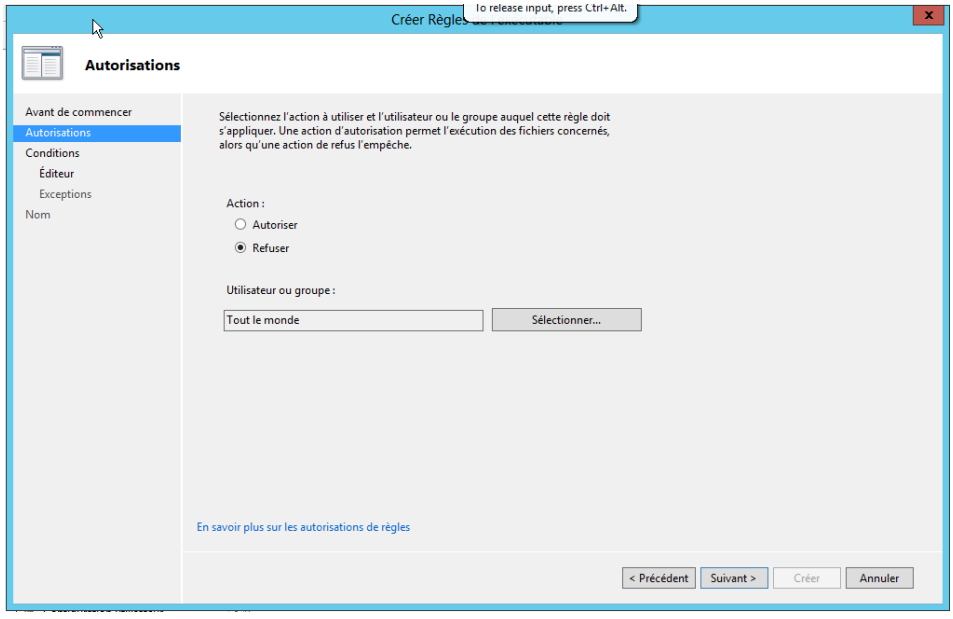

Figure 57 – Configurer les règles de l'exécutable.

3. Configuration de l'identité de l'application : Sélectionner Services système dans le Paramètre de sécurité, côté droit de la fenêtre, double clique sur Identité de l'application. Cocher Définir ce paramètre de stratégie et le mode de démarrage de service Automatique.

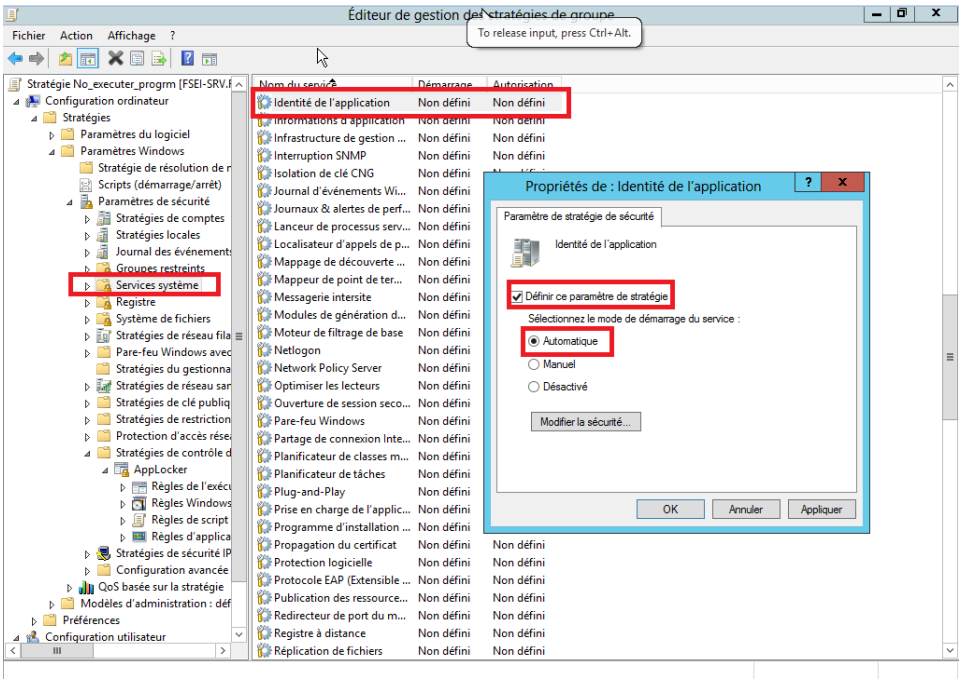

Figure 58 – Configuration de l'identité de l'application.

4. La configuration de mise en application des règles : Sélectionner AppLocker, coté droite de la fenêtre, cliquer sur le lien Configurer la mise en application des règles. Dans le cadre de ce projet, on coche Configurer pour appliquer les règles dans les rubriques Réglés de l'exécutable et règles de script.

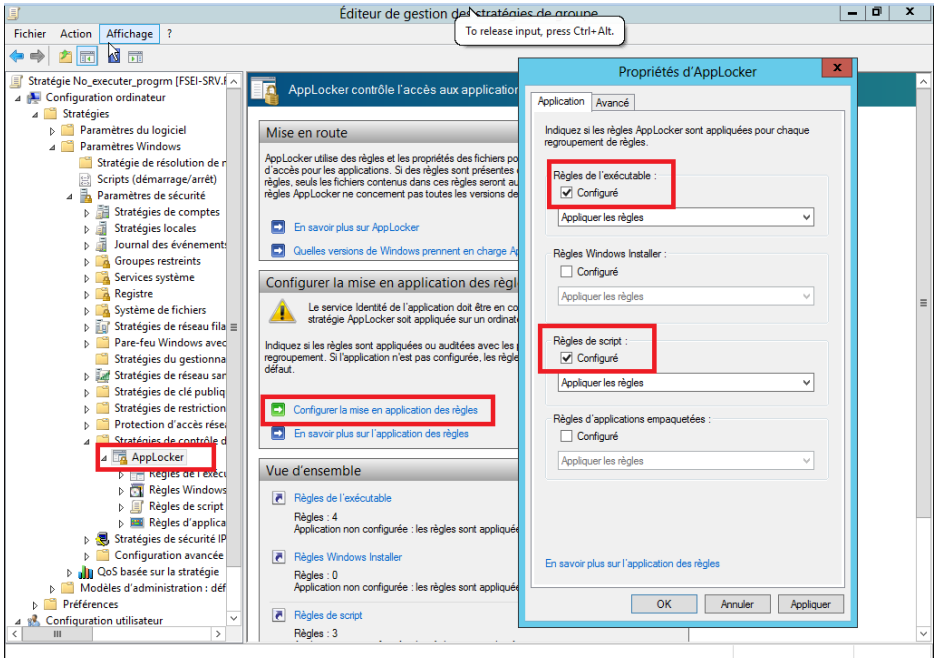

Figure 59 – La configuration de mise en application des règles.

4.4. Installation et configuration d'un serveur de stratégie réseau NPS (RADIUS) :

4.4.1. Définition :

NPS est l'implémentation Microsoft de la norme RADIUS spécifiée par l'IETF (Internet Engineering Task Force) dans les RFC 2865 et 2866. En tant que serveur RADIUS, NPS effectue une authentification, une autorisation et une comptabilité de connexion centralisées pour de nombreux types d'accès authentification de l'accès à distance par commutateur, réseau commuté et réseau privé virtuel (VPN) et connexions routeur à routeur. **[33]**

4.4.2. Installation NPS :

2. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'assistant Ajouter des rôles et des fonctionnalités s'ouvre.
3. Dans Avant de commencer, cliquez sur **Suivant**.
4. Dans Sélectionner le type d'installation, assurez-vous que l'installation **basée sur un rôle ou sur une fonctionnalité** est sélectionnée, puis cliquez sur **Suivant**.
5. Dans Sélectionner le serveur de destination, assurez-vous que **Sélectionner un serveur du pool de serveurs** est sélectionné.
6. Dans Pool de serveurs, assurez-vous que l'ordinateur local est sélectionné et cliquez sur **Suivant**.
7. Dans Sélectionner des rôles de serveur, dans **Rôles**, sélectionnez **Stratégie de réseau et services d'accès.** Une boîte de dialogue s'ouvre pour vous demander si elle doit ajouter les fonctionnalités requises pour la stratégie de réseau et les services d'accès.
8. Cliquez sur **Ajouter des fonctionnalités**, puis sur **Suivant.**
9. Dans Sélectionner des fonctionnalités, cliquez sur **Suivant**, puis dans Services de stratégie et d'accès réseau, passez en revue les informations fournies et cliquez sur **Suivant**.
10. Dans Sélectionner les services de rôle, cliquez **sur Serveur de stratégie réseau**.
11. Pour les fonctionnalités requises pour le serveur de stratégie réseau, cliquez sur **Ajouter des fonctionnalités,** puis sur **Suivant**.
12. Dans Confirmer les sélections d'installation, cliquez sur **Redémarrer automatiquement le serveur de destination si nécessaire**.
13. Cliquez sur **Oui** pour confirmer la sélection, puis cliquez sur **Installer**. La page Progression de l'installation affiche l'état pendant le processus d'installation.
14. Cliquez sur **Fermer (voir la figure 54)**.

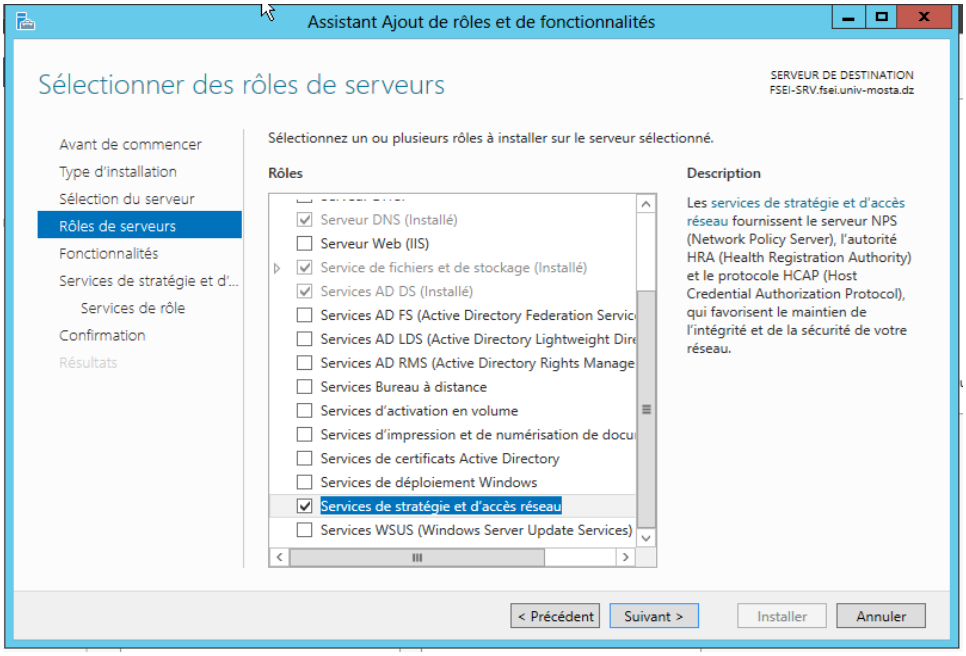

Figure 60 – installation de rôle NPS.

4.4.3. Configuration NPS:

Après avoir installé NPS, nous configurons NPS pour gérer toutes les tâches d'authentification, d'autorisation et de comptabilité.

Première étape, nous enregistrons le serveur dans Active Directory afin qu'il soit autorisé à accéder aux informations du compte d'utilisateur lors du traitement des demandes de connexion.

1. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Serveur de stratégie réseau**. La console NPS s'ouvre.
2. Dans la console NPS, cliquez avec le bouton droit de la souris sur **NPS (Local)**, puis cliquez sur **Enregistrer le serveur dans Active Directory** pour le sélectionner. La boîte de dialogue Network Policy Server s'ouvre.
3. Dans la boîte de dialogue Network Policy Server, cliquez deux fois sur **OK (voir la figure 55)**.

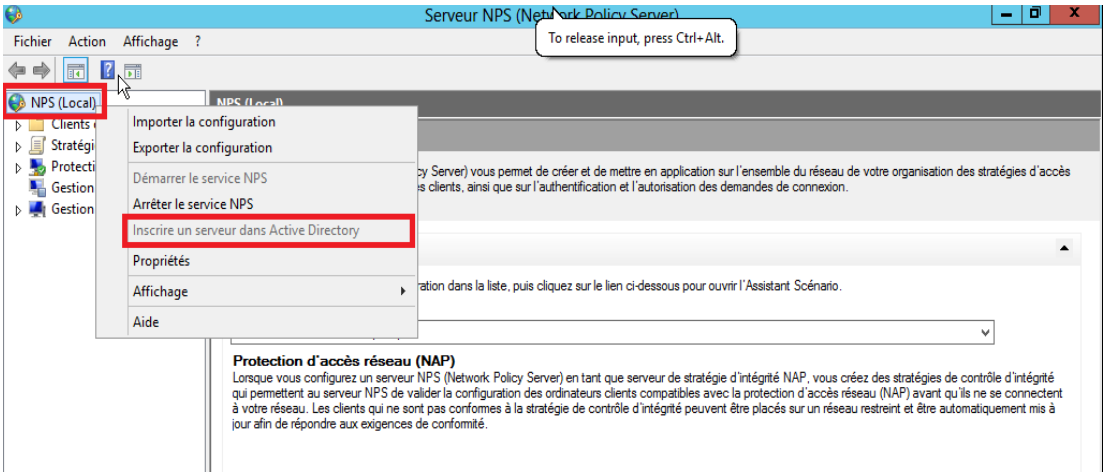

Figure 61 – Enregistrer le serveur NPS dans Active Directory.

- **Configurer un point d'accès sans fil en tant que serveur NPS RADIUS Client :**

Dans cette procédure, nous configurons un point d'accès, également appelé un *serveur d'accès réseau (NAS)*, comme un RADIUS client.

1. Sur le serveur NPS, dans **le Gestionnaire de serveur**, cliquez sur **outils**, puis cliquez sur **Network Policy Server**. Le serveur NPS aligner-dans s'ouvre.
2. Dans le serveur NPS aligner-, double-cliquez-cliquez sur **Clients et serveurs RADIUS**. Clique-droite sur **Clients RADIUS**, puis cliquez sur **New**.
3. Dans **nouveau Client RADIUS**, vérifiez que le **activer ce client RADIUS** case à cocher est activée.
4. Dans **nouveau Client RADIUS**, dans **nom convivial**, nous ajoutons tous les point d'accès sans fil situés dans la faculté, par exemple le point d'accès de VLAN6 de la salle de polyvalente nommé VLAN6_WIFI_AP.
5. Dans **adresse (IP ou DNS)**, tapez l'adresse IP ou le nom de domaine complet (FQDN) pour le serveur NAS, dans notre cas c'est 10.60.0.2.
6. Dans **nouveau Client RADIUS**, dans **Secret partagé**, nous choisissons **manuel**, puis dans **secret partagé**, tapez le mot de passe fort qui est aussi entré sur le NAS. Retapez le secret partagé dans **confirmer le secret partagé**.
7. Cliquez sur **OK**. Notre NAS s'affiche dans la liste des clients RADIUS configuré sur le serveur NPS (voir **la figure 56**).

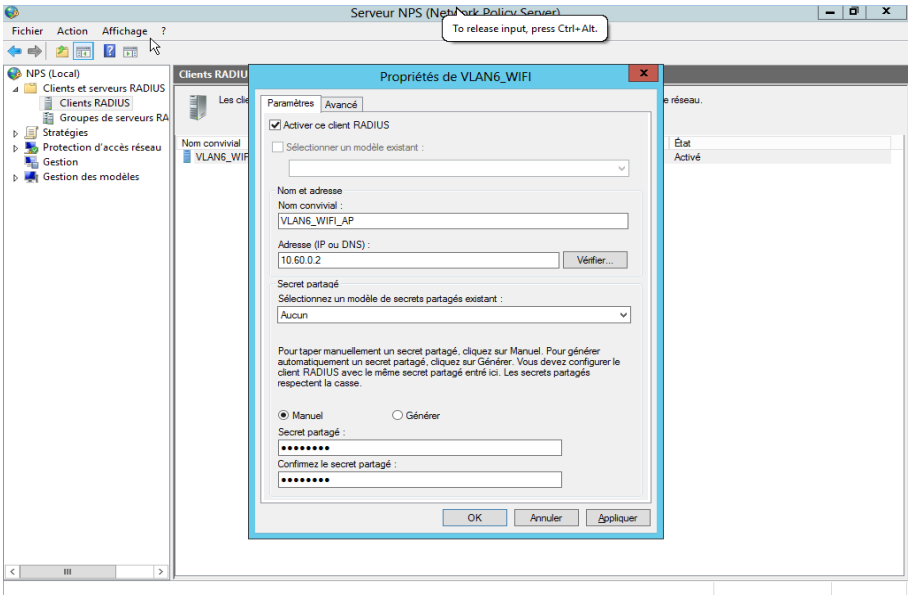

Figure 62 – l'ajout un point d'accès en tant que RADIUS client.

- **Création des stratégies du serveur NPS pour 802.1 X sans fil à l'aide d'un Assistant :**

Dans cette procédure, nous configurons NPS en tant que serveur RADIUS sur le réseau de notre faculté. Sur le serveur NPS, nous devons définir une stratégie qui autorise uniquement les utilisateurs d'un groupe spécifique à accéder au réseau.

1. Dans la console NPS, dans Configuration standard, assurez-vous que le **serveur RADIUS pour les connexions câblés ou sans fil 802.1X** est sélectionné.

2. Cliquez sur **Configurer 802.1X**. L'assistant Configurer 802.1X s'ouvre (voir **la figure 57**).

Figure 63 – configurer 802.1X.

3. Sur le **spécifier des commutateurs de 802. 1 X** page d'Assistant, en **clients RADIUS**, tous les commutateurs des points d'accès sans fil que nous avons ajoutés en tant que Clients RADIUS sont affichés. dans ce cas là nous choisissons les APs selon besoins et notre configuration.
4. Dans **spécifier des groupes d'utilisateur**, cliquez sur **ajouter**, ici nous tapons le nom du groupe de sécurité que nous avez configuré pour nos clients sans fil dans Active Directory Users par exemple le groupe « AD ».
5. Suivez les instructions de l'assistant pour terminer la création de la nouvelle stratégie.

4.5. Mise en place du portail captif (captive portal) :

4.5.1. Définition :

Un portail captif est un service web mis en place dans un réseau pour authentifier les utilisateurs. Tous les utilisateurs de ce réseau LAN devront forcément accéder à ce portail dit « captif » et s'y authentifier pour ensuite pouvoir accéder à l'internet. Si l'authentification n'est pas effectuée ou abandonnée, la connexion internet ne sera pas établie pour l'utilisateur concerné.

4.5.2. Configuration :

Dans l'interface principale de pfSense, cliquez sur le menu « Services », puis sur l'option « Captive portal ». La configuration de ce portail se faire en plusieurs étapes. Nous devons une zone dans laquelle le portail captif sera actif puis configurer cette zone, dans notre cas nous allons créer plusieurs zones selon notre faculté telle que « WIFI_poly », « WIFI_audit » et « WIFI_cafe ». Pour ce faire, cliquez sur le bouton vert « Add » un assistant de création va alors s'ouvrir :

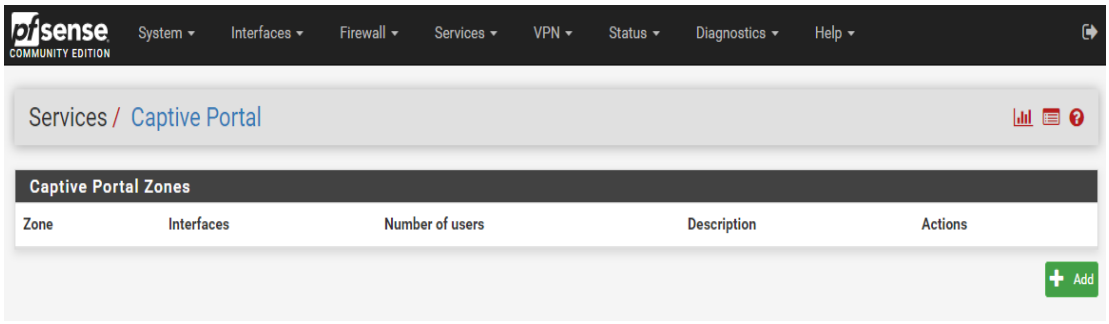

Figure 64 – Les zones de portail captif.

Il faut dans un premier temps donner un nom à cette zone et une description, le nom de la zone est obligatoire :

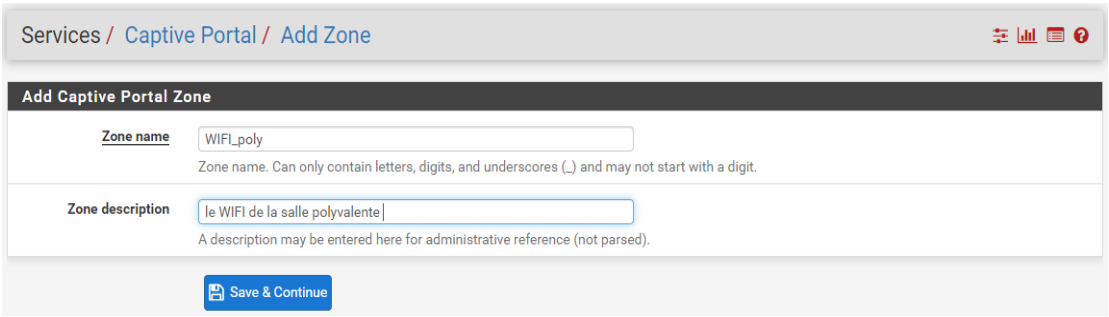

Figure 65 – l'ajout d'une zone du portail captif (captive portal).

Cliquez sur le bouton « Save & continue » pour passer à la suite de la configuration – c'est à partir de cet instant que ça devient plus intéressant mais aussi plus complexe.

Pour accéder aux paramètres du portail captif, il nous faut activer ce portail, en cochant la case à côté de « Enable captive portal ».

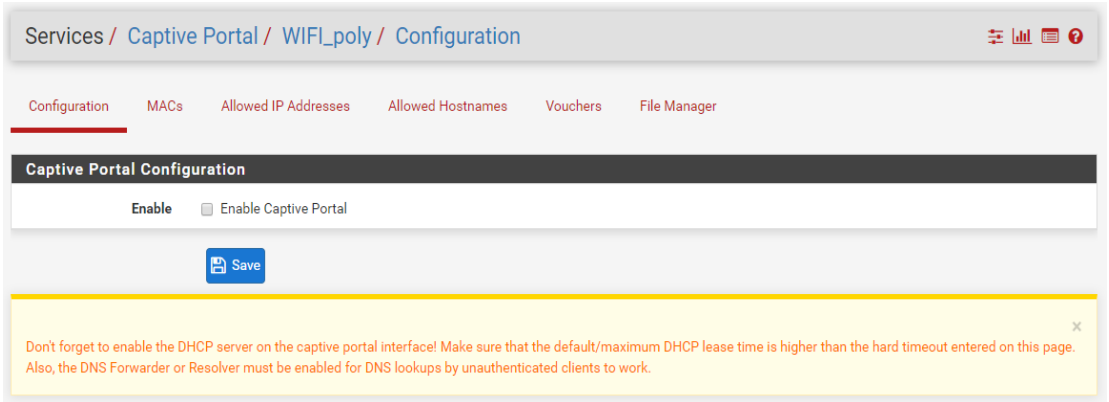

Figure 66 – configuration du portail captif (1).

Ainsi, tous les paramètres de configuration du portail captif vont s'afficher.

Dans l'ordre des options importantes et quasi obligatoires :

- **interfaces :** il s'agit là de quelle interface sur laquelle le portail captif sera exploité – il faut cliquer sur l'interface correspondant à votre LAN (ici, LAN)
- **maximum concurrent connections :** limite le nombre de connexion en même temps sur le portail captif ; si cette limite est dépassée, le portail captif ne sera pas accessible par les

autres clients, jusqu'à temps qu'une place se libère. Laissez vide si vous ne souhaitez pas de limites

- **idle timeout :** délai en minutes à laquelle les clients seront déconnectés s'ils n'ont pas eu / effectué d'activité. Laissez vide si vous ne souhaitez pas de limites
- **hard timeout :** délai en minutes pour forcer la déconnexion des utilisateurs, qu'importe leur activité

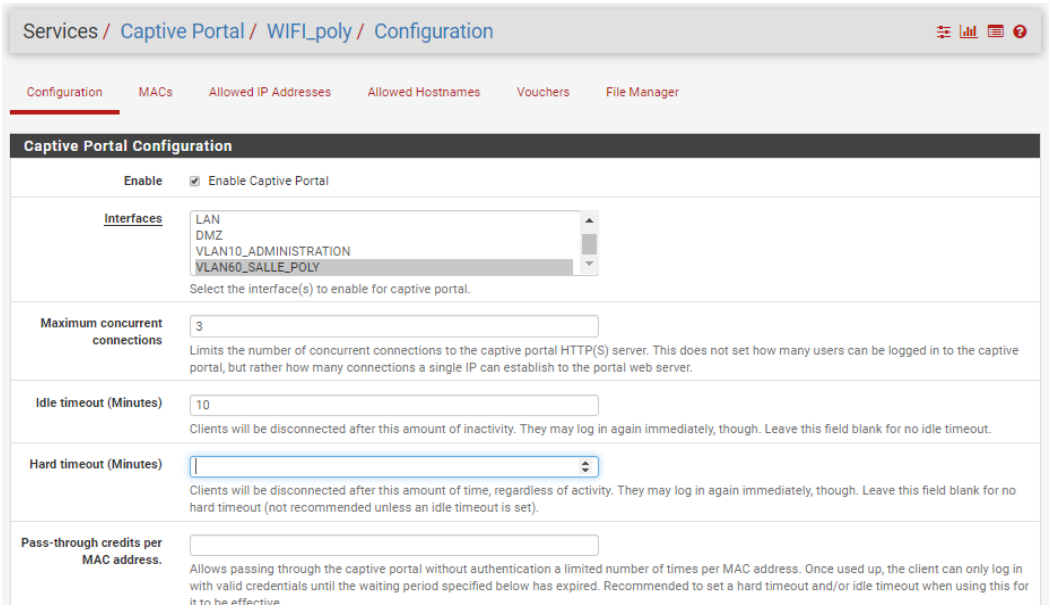

Figure 67 – configuration du portail captif (2).

Dans la rubrique « **Authentification** ». C'est dans cette partie que nous devons faut choisir le mode d'authentification de nos clients où dans notre cas nous allons utiliser le serveur RADIUS que nous avons crée pour connecter ce portail avec notre annuaire (ou encore LDAP) et qui veut dire que l'utilisateur doit être membre de la faculté pour qu'il puisse utiliser la connexion internet. Pour ce faire, cliquer sur « **RADIUS Authentication** », nous devons citer l'adresse IP du serveur et le secret partagé (voir **la figure 68**).

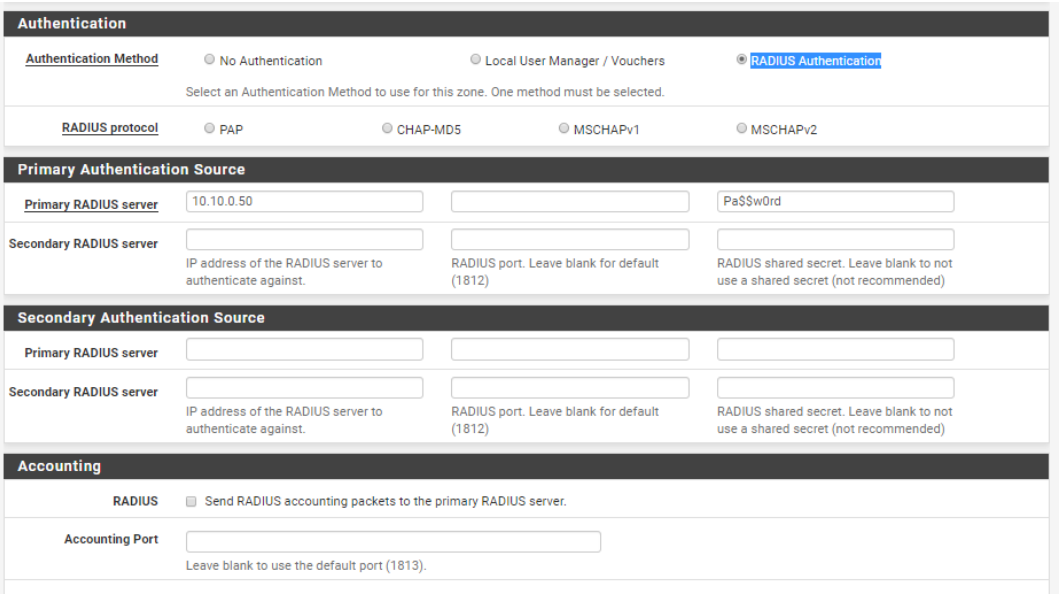

Figure 68 – configuration du portail captif (2).

5. Teste et validation de la solution :

5.1. Vérification du routage inter VLAN :

A l'aide de la commande « show IP interface brief », nous pouvons avoir les Switchs Virtuelle Interface (SVI) comme ceci :

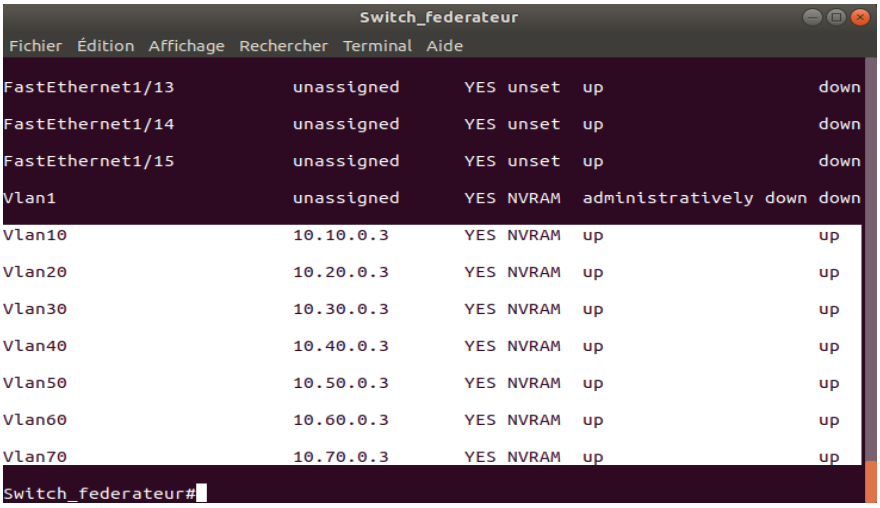

Figure 69 – les Switchs Virtuelle Interface (SVI).

5.2. Vérification de la distribution des adresses IP avec le DHCP :

Le serveur DHCP dans pfSense transmettra les adresses aux clients DHCP et les configurera automatiquement pour l'accès au réseau. Par défaut, le serveur DHCP est activé sur chaque interface VLAN que nous avons crée (voir **la figure 70**).

Côté serveur :

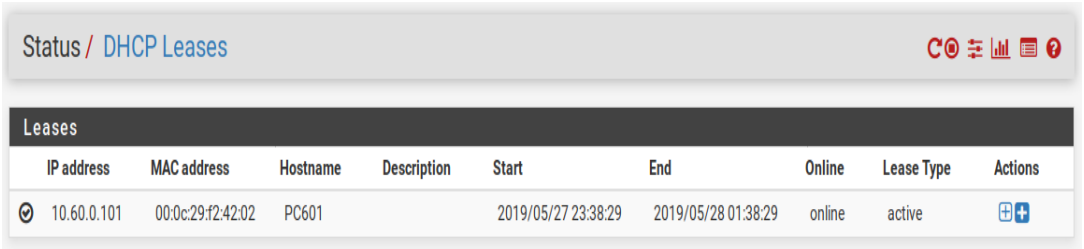

Figure 70 – la distribution des adresses IP avec le DHCP (côté serveur).

Côté client :

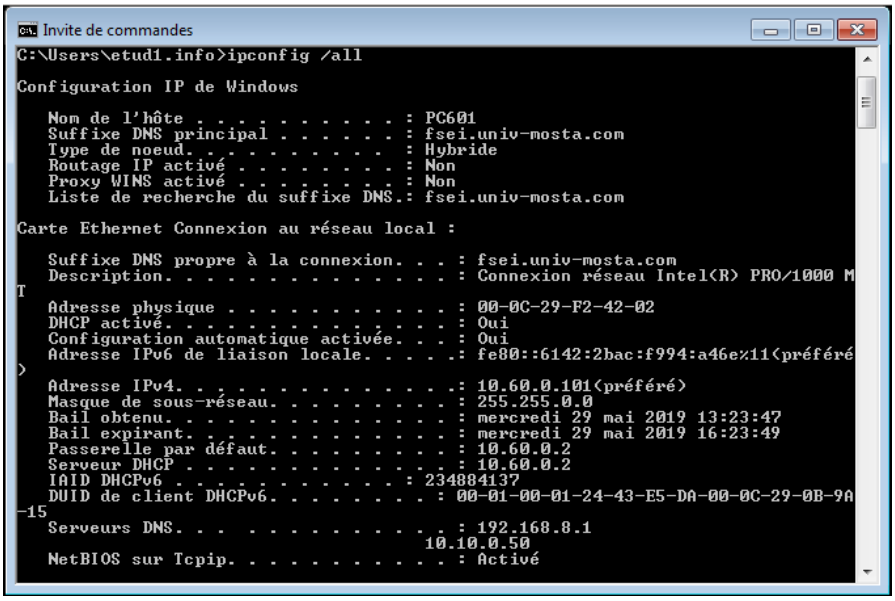

Figure 71 – la distribution des adresses IP avec le DHCP (côté client).

5.3. Vérification de la communication entre les PCs :

A ce stade, nous vérifions l'accessibilité des différents équipements dans un même réseau mais dans deux VLANs distincts à partir du PC-1 « 10.10.0.104 » situé dans le VLAN 10 en essayant de pinger le PC-3 « 10.20.0.102 » situé dans le VLAN 20.

La figure 72 illustre le succès du test effectué entre les différents VLANs :

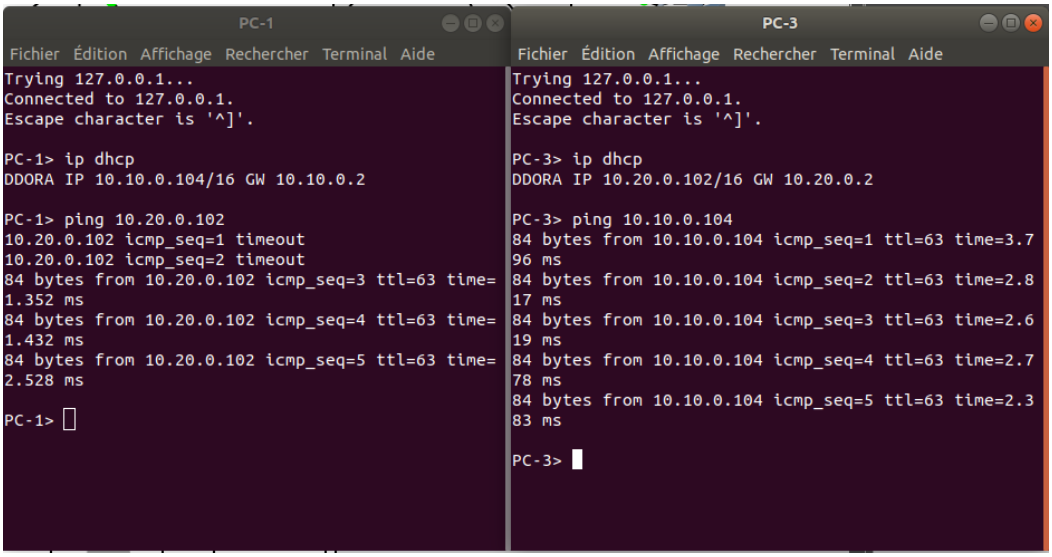

Figure 72 – Vérification de la communication entre les PCs.

5.4. Teste du portail captif:

Après avoir configurer notre portail captif et créer les différentes zones telles que « WIFI_poly », nous allons maintenant tester la connectivité. Cet exemple a été appliqué au niveau du VLAN 6 de la salle polyvalente, donc chaque utilisateur qui veut connecter à travers le point d'accès de ce VLAN, il doit saisie son identifiant et le mot de passe pour pouvoir accéder à internet (voir **la figure 73**).

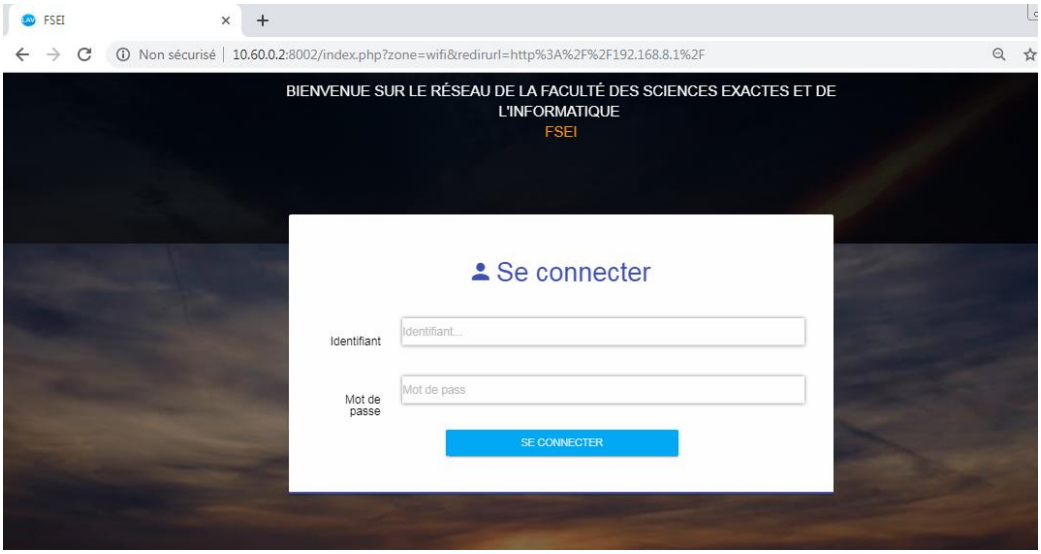

Figure 73 – l'interface du portail captif (captive portal).

5.5. Ajout du poste client dans le domaine Active Directory :

- Dans l'écran d'**accueil**, tapez **Panneau de configuration**, puis appuyez sur Entrée.
- Accédez à **Système et sécurité**, puis cliquez sur **Système**.
- Sous **Paramètres du nom de l'ordinateur, du domaine et du groupe de travail**, cliquez sur **Modifier les paramètres**.
- Sous l'onglet **Nom de l'ordinateur**, cliquez sur **Modifier** (voir **la figure 74**).

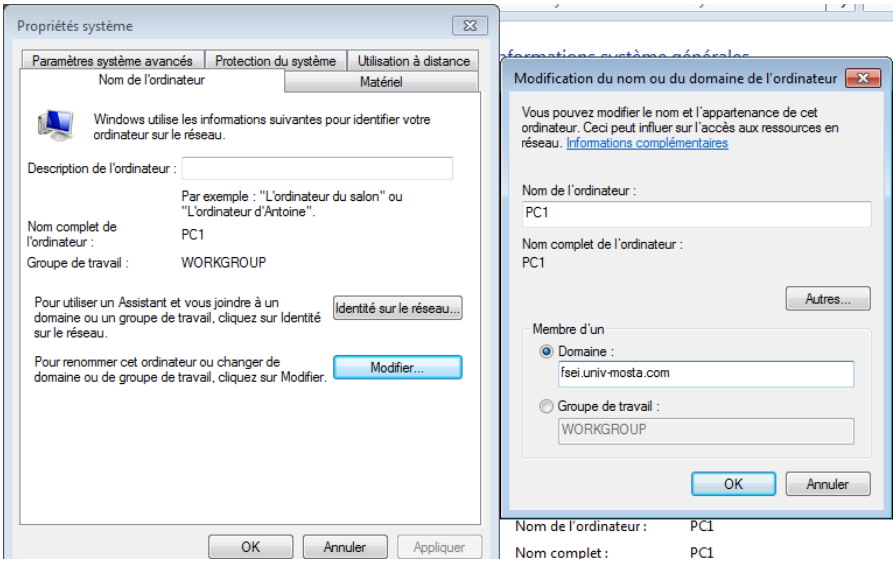

Figure 74 – Ajout du poste client dans le domaine Active Directory (étape 1).

- Sous **Membre d'un**, sous **Domaine**, nous tapons le nom notre domaine qui est « fsei.univ-mosta.com », puis cliquez sur **OK**.

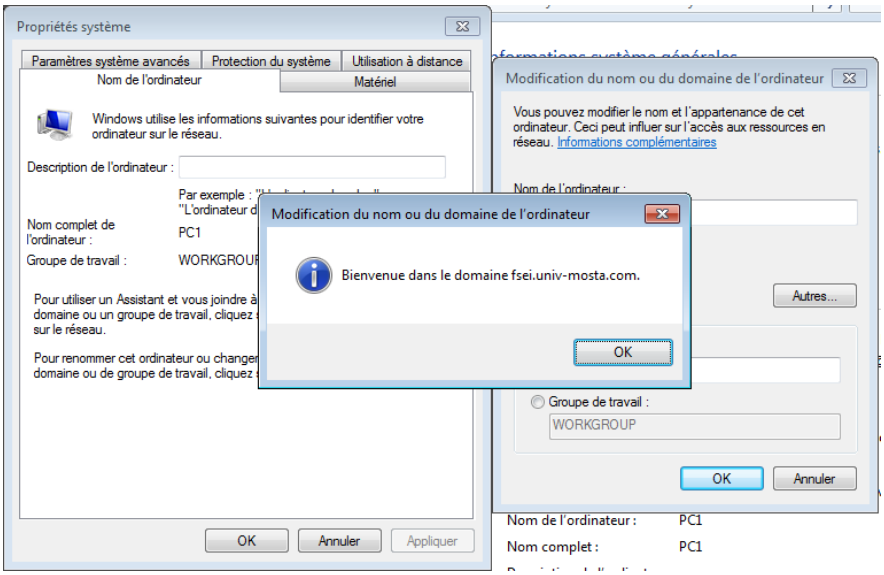

Figure 75 – Ajout du poste client dans le domaine Active Directory (étape 2).

5.6. Teste des stratégies de groupe :

Après avoir joindre les portes de travail au domaine, Nous allons maintenant appliquer la stratégie de groupe que nous avons configuré qui consiste à empêcher les étudiants d'exécuter des programmes et scripts sur les postes de travail (voir la figure 76).

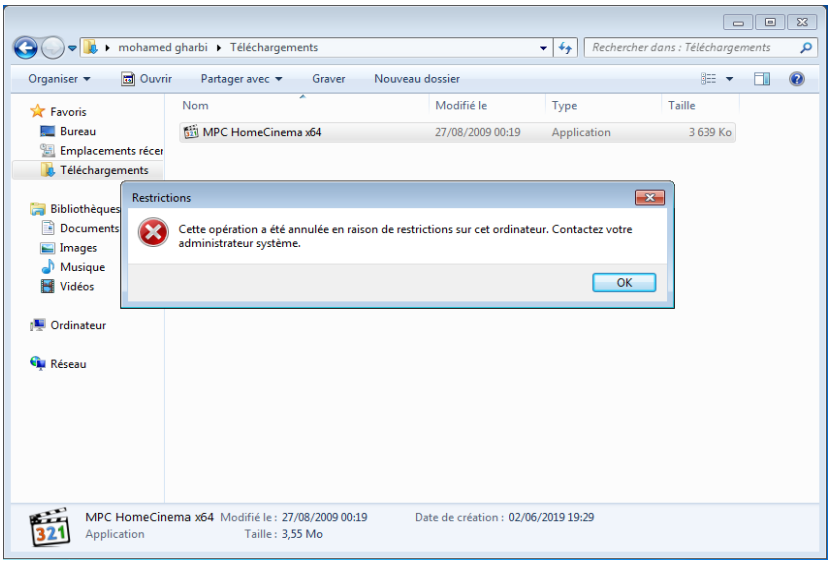

Figure 76 – Application de la stratégie de groupe (GPO).

5.7. Teste de la connexion à l'ENT de la faculté :

Un espace numérique de travail (ENT) est un portail internet éducatif permettant à chaque membre de la communauté éducative d'un établissement scolaire, d'accéder, via un point d'entrée unique et sécurisé, à un bouquet de services numériques en relation avec ses activités.

Nous avons réalisé un site web dynamique (ENT) qui répond aux exigences de nos divers utilisateurs cibles en leur offrant un contenu intéressant et des caractéristiques techniques à leurs niveaux, pour qu'ils puissent accomplir leurs tâches.

Les objectifs sont donc de favoriser le partage et la communication de ressources et de pratiques en fournissant à chaque utilisateur un espace de travail et de stockage dont les ressources sont accessibles à tout moment de n'importe quel lieu pourvu d'une connexion internet. Deuxièmement, l'objectif est de diversifier les ressources et supports pédagogique mais aussi d'améliorer le suivi individuel grâce à des dispositifs tel que le soutien, les programmes personnalisés ou les ressources éducatives en ligne.

Pour accéder à notre ENT, il suffit de taper « fsei.univ-mosta.com » (voir **la figure 77**).

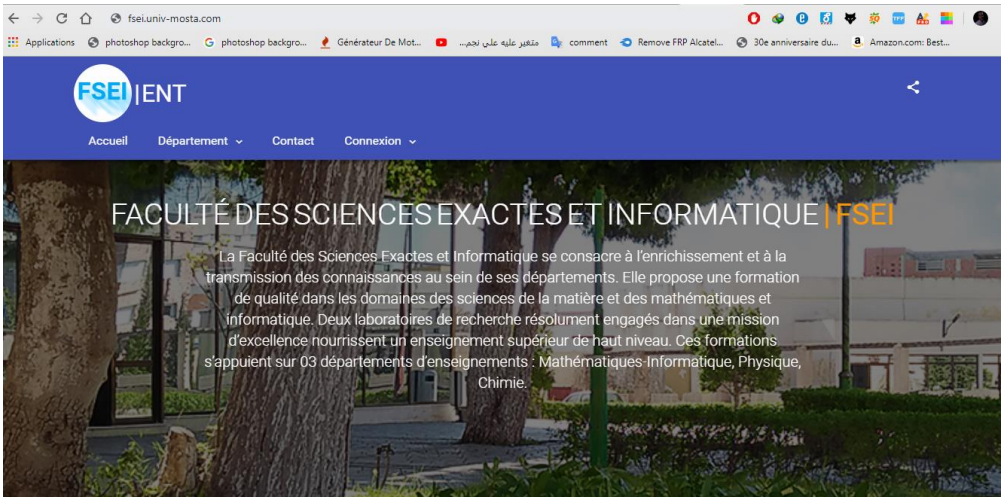

Figure 77 – Espace numérique de travail (ENT) de FSEI.

Au niveau de sous-réseau DMZ, nous avons mis en place un serveur web (Apache) qui contient notre plateforme l'ENT. L'authentification au l'ENT va se faire à travers notre AD DS. Lorsque l'utilisateur (étudiant ou enseignant) veut consulter son compte, il doit saisir son identifie et mot de passe et choisir sa spécialité pour qu'il puisse y connecter. Pour tester la connexion nous avons créé un utilisateur où son nom complet est « mohamed gharbi », cet étudiant appartient à l'OU « info » qui est elle-même dans l'OU « étudiant » (voir **la figure 78**).

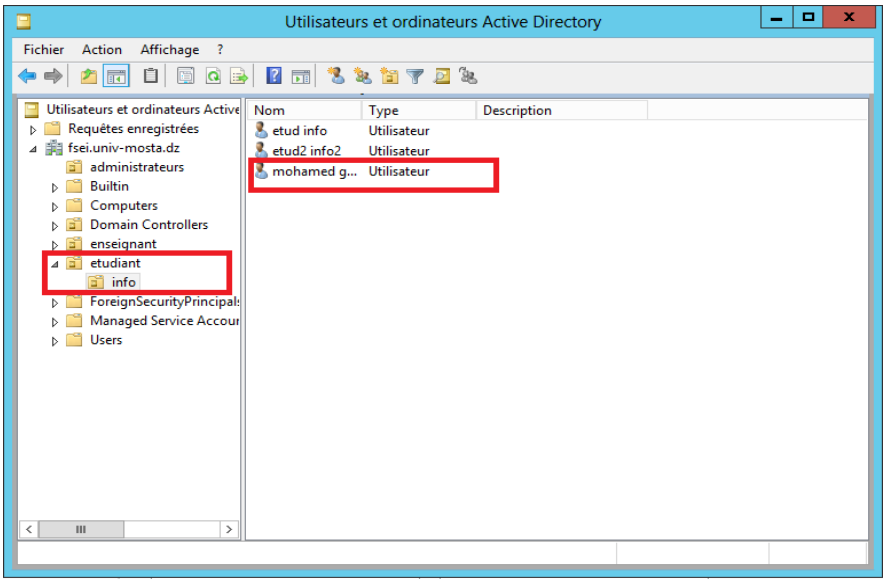

Figure 78 – Utilisateurs et ordinateurs Active Directory.

L'étudiant doit saisir son identifie et mot de passe et choisir sa spécialité pour qu'il puisse y connecter (voir **la figure 79**).

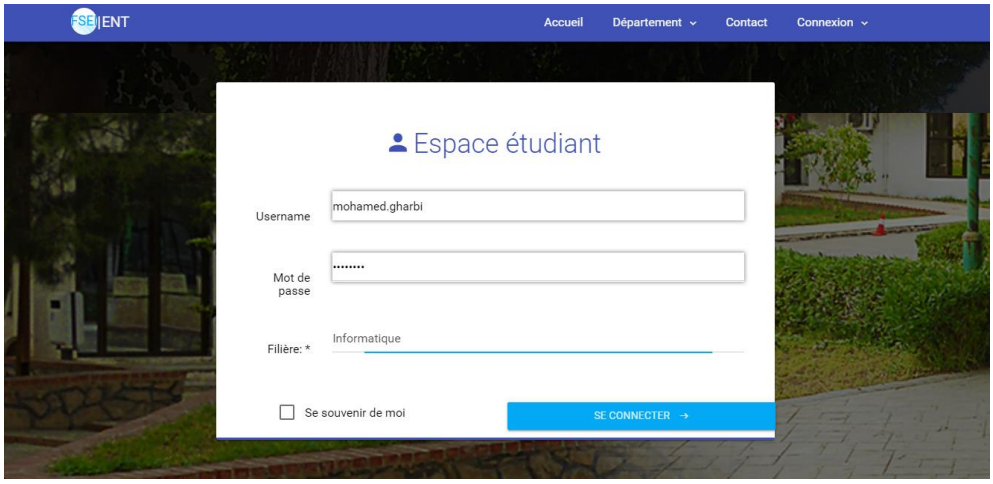

Figure 79 – Espace étudiant Authentification (ENT).

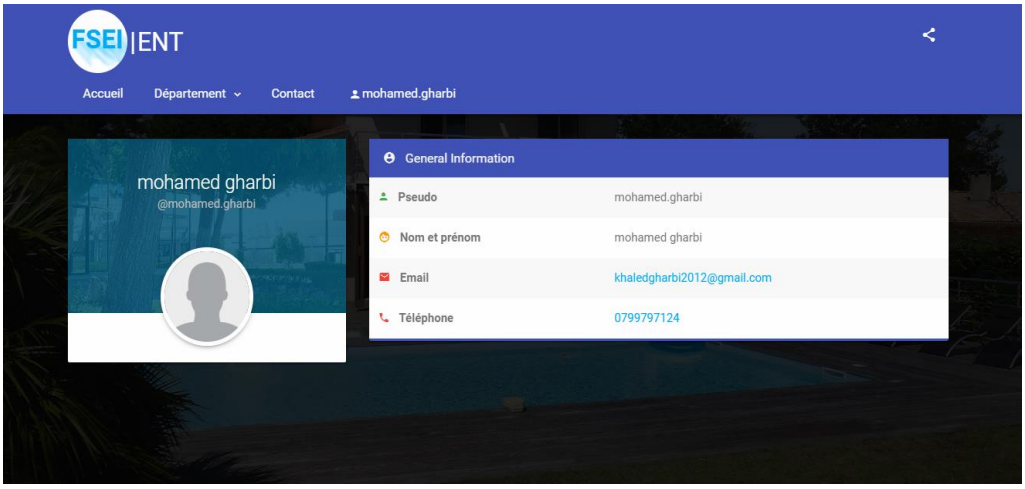

Figure 80 – Compte étudiant (ENT).

6. Conclusion :

Dans ce chapitre nous avons présenté une brève description de la nouvelle architecture réseau que nous avons proposé et les améliorations que nous avons apporté pour donner un plus au fonctionnement réseau de la faculté, nous avons mis en place un serveur de pare-feu pour contrôler et sécuriser notre réseau, nous avons mis en place aussi un serveur Microsoft AD DS afin de créer et de gérer des comptes utilisateur de manière centralisée, nous avons segmenté le réseau de la faculté en VLAN dans un Switch Fédérateur d'une manière à avoir un réseau fluide, une bande passante optimisée et une organisation souple.

Conclusion générale et perspectives:

Le travail présenté dans ce mémoire de Master s'est porte sur La mise en place et la gestion d'un réseau informatique au sein de la FSEI

La définition d'un réseau de campus n'a jamais été simple, mais la description courante est un groupe de segments de réseau local au sein d'un bâtiment ou un groupe de bâtiments qui se connectent pour former un seul réseau. En règle générale, l'université possède l'ensemble du réseau, y compris le câblage entre les différents départements. Ce réseau local (LAN) utilise généralement les technologies Ethernet, Token Ring ou FDDI (Fibre Distributed Data Interface). Le principal défi des administrateurs de réseau consiste à faire en sorte que le réseau du campus fonctionne efficacement. Pour ce faire, ils doivent comprendre les réseaux de campus actuels ainsi que les nouveaux réseaux de campus émergents.

Par conséquent, dans ce projet nous avons vue les notions de bases sur les réseaux informatiques dont la notion de la topologie réseau et les différents types de réseau qui peuvent être réalisés ainsi que l'architecture réseau et l'interconnexion. Nous avons découvris aussi les exigences actuelles et futures des inter-réseaux de campus.

Nous avons ensuite étudié l'architecture existante du réseau où nous avons expliqué les avantages et les inconvénients de celui-ci, ce qui nous a permis de critiqué cette architecture et de suggérer quelques solutions afin de proposé une nouvelle avec une meilleur fiabilité, fluidité et sécurité du réseau.

Dans la nouvelle architecture, nous avons mis en place des serveurs tels que serveur de pare-feu (pfSnese), AD DS et serveur Web, La mise en place du réseau local virtuel (VLAN) nous a permis de segmenter le réseau de FSEI. Ce travail d'une part n'a pas été facile du point de vu conception car il fallait comprendre le fonctionnement des équipements Cisco et leur fonctionnalité, afin d'augmenter les performances du réseau.

Ainsi, après avoir atteint notre objectif nous souhaitons par la suite travailler sur la plateforme ENT pour but de moderniser l'enseignement et la pédagogie, de saisir et de mettre à la disposition des étudiants, des enseignants, des personnels administratifs et plus généralement de tous les membres de la communauté éducative de l'enseignement supérieur, en fonction des habilitations de chaque usager, des contenus éducatifs et pédagogiques, des informations administratives, relatives aux enseignements et au fonctionnement de l'établissement ainsi que de la documentation en ligne.

L'intérêt principal que nous avons tiré de cette étude est que nous avons bien affronté la vie professionnelle de notre domaine. Nous avons évalué les différentes étapes de réalisation d'un projet ainsi que les techniques développées par les spécialistes du domaine pour assurer l' efficacité et la bonne réalisation des travaux en se limitant aux ressources et à des durées de temps exactes. Nous avons pu voir la complexité de la mise en route d'un nouveau projet et de sa rapide évolution qui nous a appris à mieux nous organiser afin d'être capable de finaliser notre travail.

Bibliographie :

[1] : Pujolle Guy, Les Réseaux**,** 3e Edition mise à jour par Eyrolles, à Paris, 2000, Page 13

[2] : Bush, SF (2010). *Réseaux de communication à l'échelle nanométrique*. Maison Artech. ISBN 978-1-60807-003-9 .

[3] : Margaret Rouse. "Réseau personnel (PAN)" . *TechTarget*. Récupéré le 29 janvier 2011.

[4] : "La nouvelle norme globale pour la maison entièrement en réseau" . *Journal de l'UIT-T*. ITU . 2008-12-12. Archivé de l'original le 2009-02-21.

[5] : https://en.wikipedia.org/wiki/Home_network

[6] : https://en.wikipedia.org/wiki/Storage_area_network

[7] : Gary A. Donahue (June 2007). *Network Warrior*. O'Reilly. p. 5.

[8] : "Réseaux dorsaux" . Chapitre 8. Angelfire.com/ut/cnst/Chap8.html. Récupéré le 2 octobre 2013.

[9] : http://www.tech-faq.com/internet-backbone.html

[10] : Réseaux informatiques – notions fondamentales – 5ème Edition crée par José DORDOIGNE, 2013 en France, page 34.

[11] : *"A WAN Is a Wide Area Network. Here's How They Work". lifewire.com/wide-area-network-816383*

[12] : Mason, Andrew G. (2002). *Cisco Secure Virtual Private Network*. Cisco Press. p. 7.

[13] : https://en.wikipedia.org/wiki/IEEE_802.20

[14] : McBee, David Barnett, David Groth, Jim (2004). (3rd ed.). San Francisco: SYBEX. page. 11.

[15] :https://web.archive.org/web/20110728162909/http://www.belden.com/pdfs/Techpprs/CoaxialCablesandApplications.pdf

[16] : https://www.blackbox.fr/fr-fr/page/27220/Information/Technique/black-box-explique/Cables-fibre-optique/constitution-dun-cble-fibre-optique

[17] : https://www.memoireonline.com/11/11/4952/m_Conception-et-deploiement-dune-architecture-reseau-securisee--cas-de-SUPEMIR0.html

[18] : Data communications and networking I Behrouz A Forouzan. - 4th ed, page 45-48.

[19] : https://whatis.techtarget.com/fr/definition/Modele-OSI

[20] : https://www.livinginternet.com/i/ii_tcpip.htm

[21] : https://searchsdn.techtarget.com/definition/campus-network

[22] : Edwards, Wade. CCNP Complete Study Guide (642-801, 642-811, 642-821, 642-831). Sybex. © 2005

[23] : VAUCAMPS A, "cisco CCNA", ENI édition, 2010.

[24] : https://uit.stanford.edu/service/network

[25] : https://en.wikipedia.org/wiki/Massachusetts_Institute_of_Technology

[26] : https://searchnetworking.techtarget.com/definition/DHCP

[27] : https://docplayer.fr/1179366-Active-directory-qu-est-ce-qu-un-service-d-annuaire.html

[28] : https://www.univ-mosta.dz/histoire-de-luniversite/

[29] : https://www.univ-mosta.dz/actes-reglementaires/

[30] : A.Ksiks. Etude et simulation sur GNS3 du service MP-BGP/VPN-IP, 2011.

[31] : Fiche sur la licence de Windows Server 2012 R2. Microsoft.com.

[32] : Service d'annuaire Active Directory. DIRECTION RECHERCHE ET INGENIERIE DE FORMATION, p 6.

[33] : https://docs.microsoft.com/en-us/windows-server