

Sommaire

Introduction générale.....	8
Chapitre 1	10
Présentation générale.....	10
1. Présentation de l'établissement d'accueil :	11
2. Présentation du Sujet :.....	12
2.1. Etude de l'existant :.....	12
2.2. Critique de l'existant :	16
2.3. Solutions retenu :.....	16
Chapitre 2 : ETAT DE L'ART.....	19
Introduction :.....	20
1. WI-FI :.....	20
2 .Catégories de réseaux :.....	21
2.1 WPAN :.....	21
2.2 WMAN :.....	22
2.3 WWAN :	22
2.4 WLAN :.....	22
2.5 WRAN :.....	22
2.5 Différentes Normes de WI-FI :	23
3-Equipement Wi-Fi :.....	26
3-1 Point d'accès :	26
3-2 Modems :	27
3-3 Routeurs :	28
4- Sécurité Wi-Fi :.....	28
4-1 WEP :.....	28
4.2 WPA.....	29

4.3 WPA2 :	29
4.4 802.1x :	30
Firewall.....	31
1-Définition :	31
2-Catégories de pare-feu :	31
2-1 Pare-feu sans état (<i>stateless firewall</i>) :	31
2-2 Pare-feu à états (<i>stateful firewall</i>) :	32
2-3 Pare-feu applicatif :	32
2-4 Pare-feu identifiant :	33
2-5 Pare-feu personnel :	33
2-6 Portail captif :	34
3 Fonctionnement générale :	34
Conclusion :	35
Chapitre 3	36
Présentation des outils	36
Introduction :	37
I. Freeradius :	37
1. Définition :	37
2. Caractéristiques :	38
3. Principe de fonctionnement :	39
4. Principe de protocole 802.1X(EAP) :	41
1. Définition :	41
2. Authentification basé sur le contrôle de port :	42
a. Port non contrôlé :	42
b. port contrôlé :	43
3. Protocole EAP :	43
4. Les paquets EAP :	43

5. Séquence d'authentification d'une session 802.1X/EAP :	47
II. PfSense :	48
1. Introduction :	48
2. Descriptions :	48
3. Services proposés :	49
4. Principe de fonctionnements :	49
Conclusion :	50
Chapitre 4	51
Réalisations	51
I. Environnement matériels et logiciel :	52
1. Points d'accès :	52
2. Machine Client :	52
3. Machine Serveur :	52
4. Les logiciels :	52
5. Présentations des machines virtuelles :	53
III. Travail réalisé :	54
Radius	54
1. Installations FreeRadius :	54
2. Configuration de FreeRadius:	55
a. Configuration de la base de données	56
b. Configuration de fichier :	59
3. creation de certificats :	63
4. Test de fonctionnement :	63
5. Configuration de point d'accès et configuration de connexion de SMC:	64
a. Configuration du point d'accès :	64
b. connexion au réseau sans fil :	66
PfSense	71

1. Installation de PfSense :	71
2. Configuration de PfSense :.....	73
a. Configuration DHCP :	75
b. Configuration de squid proxy server :.....	76
c. Configuration de SquidGuard Proxy Filter :	77
d. Configuration Firewall	79
e. Configuration de Captive Portal :	80
3. Test de fonctionnement :	82
a. DHCP	82
b. Test squid proxy server :	82
c. Test SquidGuard proxy filter :	83
d. Test Firewall & Portal captive :	84
Conclusion générale	85

Liste des figures

Figure 1:ARCHITECTURE DE RESEAU DE L' ISET	14
Figure 2 :SOLUTIONS RETENU	17
Figure 3:schéma simplifié de solution retenu	18
Figure 4:Emplacement proposé des points d'accès.....	18
Figure 5 :Mode de topologies sans fil 802.11	24
Figure 6:Mode d'infrastructure	25
Figure 7:Mode ad hoc	25
Figure 8 :point d'accée.....	26
Figure 9 :principe du WEP.....	28
Figure 10:Pare-feu passerelle entre LAN et WAN	34
Figure 11:Pare-feu routeur, avec une zone DMZ.....	35
Figure 12:mécanisme générale de Freeradius	37
Figure 13:changements password par étape.....	40
Figure 14:architecture réseau	41
Figure 15:port non controlé.....	42
Figure 16:Port Contrôlé.....	43
Figure 17: EAP-TLS	46
Figure 18:Diagramme de séquence d'authentification.....	47
Figure 19:fonctionnement de portal captive.....	50
Figure 20:laréponse Access-Accept	56
Figure 21:creation de user radius	57
Figure 22:Creation de table radcheck.....	57
Figure 23:Ajoute des utilisateurs.....	58
Figure 24:mettre une authentification EAP	58
Figure 25:nasname	58
Figure 26:Test NTRadPing	63
Figure 27:test surDebian	64
Figure 28:interface de point d'accès	64
Figure 29:configuration de SMC.....	65
Figure 30:unutilisateurfreeradius	66
Figure 31:gestionnaire de certificat.....	66
Figure 32:importer de certificat.....	67

Figure 33:installation certificat client.....	67
Figure 34:certificat importé.....	68
Figure 35:installation de certificat de serveur	68
Figure 36:protection clé privé	69
Figure 37:connexion au réseau sans fil	69
Figure 38:les paramètre de connexion	70
Figure 39:choisi le méthode d'authentification.....	70
Figure 40:booter le pfSense.....	71
Figure 41:etape2 d'installation.....	72
Figure 42:configuration console.....	72
Figure 43:installation rapide.....	73
Figure 44:1eretapes de configuration	73
Figure 45:adressage De LAN	74
Figure 46:Accédé a l'interface de pfSense.....	74
Figure 47:configuration de DNS server	75
Figure 48:configuration de DHCP	75
Figure 49:ajoute deux utilisateurs sur squid.....	76
Figure 50:authentificationmethod	76
Figure 51:configuration de Alias.....	79
Figure 52:ajoute d'un rule	79
Figure 53:ajoute de groupe.....	80
Figure 54:ajout utilisateurs.....	81
Figure 55:filtrage d'adresse Mac.....	81
Figure 56:test DHCP	82
Figure 57:test proxy	83
Figure 58:test de blacklist.....	83
Figure 59:inetrface portal captive sur XP	84
Figure 60:blocage Mac.....	84

Liste des tableaux

Tableau 1:Les Types Des Paquet Radius	38
Tableau 2: les types des paquets EAP	44
Tableau 3: Méthode d'authentification	45
Tableau 4 :caractéristiques de point d'accès	52

INTRODUCTION GENERALE

Les réseaux sans fil rencontrent aujourd'hui un succès important car ils permettent de déployer des moyens de transmission sans contrainte d'immobilité liée aux câblages et aux prises, la promotion actuelle de ce type de solution est uniquement axée sur les avantages qu'elle procure : facilité et rapidité d'installation, coût inférieur à un système filaire, mobilité, accès partagé à des services de haut débit.

Vu l'importance et l'obligation de l'élaboration d'un pare-feu, chaque organisme doit établir un pare-feu pour la sécurité informatique périodiquement afin d'identifier ses sources de menace et ces dégâts informationnels.

Bien que cette technologie semble aux premiers abords parfaite et sans soucis, la réalité est plus dure, due surtout au problème de la protection de ces réseaux sans fil, même vis-à-vis d'attaque simple. La nature de signal transmis (ondes électro magnétiques) rend difficile, voire impossible la maîtrise complète de la propagation. En conséquent, il est assez facile d'écouter les messages et même de s'introduire sur de tels réseaux ; il est donc nécessaire de définir pour les réseaux sans fil une politique de sécurité stricte reposant sur des mécanismes, si possible sans failles, tel que l'authentification, le contrôle d'intégrité et le chiffrement avec la configuration d'un firewall qui est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet).

Le travail que nous présentons dans le cadre du projet de fin d'étude consiste à l'étude du sécurisation d'un réseau sans fil existant afin d'améliorer en premier lieu sa portée et ensuite passer au déploiement d'une solution de sécurité des réseaux sans fil « Wi-Fi » de **L'ISSET DE TOZEUR**. Notre travail va consister à sécuriser un réseau Wi-Fi en mode infrastructure en mettant en place un serveur d'authentification freeradius et configuration d'un firewall PfSense.

Le présent rapport est de ce fait la synthèse des étapes de mise en œuvre de cette application, il s'articule autour de quatre principaux chapitres. Le premier chapitre est consacré à la présentation de l'organisme d'accueil et consacré à l'étude de l'existant **ISSET de Tozeur**. Le

deuxième chapitre nous présentons des généralités sur les réseaux sans fil « Wi-Fi » et les différentes catégories de firewall son principe, son fonctionnement, et l'état de l'art de mécanismes de sécurité. Dans le troisième chapitreont réservé la présentation des outils. En fin le dernier chapitre présente la réalisation de notre travail par des imprimes écran.

CHAPITRE 1

PRESENTATION GENERALE

1. PRESENTATION DE L'ETABLISSEMENT D'ACCUEIL :

L'ISSET de Tozeur est un établissement d'enseignement supérieur, dont l'objectif est de former les étudiants dans plusieurs disciplines. Les sciences de l'informatique forment un domaine indispensable pour la formation. Pour cela, cet établissement offre des locaux et des moyens pour parvenir à réaliser cet objectif.

L'Institut supérieur des Etudes Technologique de Tozeur a été créé par le décret 2004-2204 du 14 septembre 2004. Les cours ont démarré le 16 septembre 2004. Il fait partie d'un réseau d'établissements.

Il s'agit du premier établissement d'enseignement supérieur dans la région, il a donc pour mission et pour responsabilité de répondre aux besoins en formation continue et d'ouvrir les horizons aux travailleurs. (Développement de cours de soir)

L'ISSET assure une formation Supérieure Technologique dans les spécialités Maintenance Industrielle, Mécatronique Auto, Climatisation Industrielle, Réseaux & Service Informatique, Multimédia & Développement des d'informations, Electricité Industrielle, Électronique Industrielle, Automatismes & Informatique Industrielle, Travaux Publics, Bâtiments et Topographie & Géomatique à **l'ISSET de Tozeur**.

L'ISSET de Tozeur propose une formation de licence dans les spécialités suivantes :

➤ Génie Civil : Licence appliquée en Génie Civil

Les spécialités :

- Travaux Publics
- Bâtiments
- Topographie et Géomatique

➤ **Technologies de l'Informatique : Licence appliquée en Technologies de l'Informatique**

Les spécialités :

- Multimédia et Développement Web (MDW)
- Réseaux et Services Informatiques (RSI) :

➤ **Génie Mécanique : Licence appliquée en Génie Mécanique**

Les spécialités :

- Maintenance Industrielle
- Mécatronique
- Climatisation Industrielle
- Energie et Génie Climatique (Licence Co-construite)

➤ **Génie Électrique : Licence appliquée en Génie Electrique**

Les spécialités :

- Electricité Industrielle
- Electronique Industrielle
- Automatismes et Informatique Industrielle

2. PRESENTATION DU SUJET :

2.1. Etude de l'existant :

L'ISSET de Tozeur dispose d'un réseau informatique comportant les éléments suivants :

Laboratoires : 10 laboratoires d'enseignement et 2 salles d'accès libre (salle étudiants et salle enseignants).

Salle serveurs : 2 serveurs (server Linux RedHat et l'autre équipé de Windows Server 2003),
1 routeur modem, 2 modem ADSL, Armoire réseau).

L'ISET de Tozeur est relié par une fibre optique avec l'opérateur de Tunisie Télécom, ce type de connexion internet offre un haut débit sa vitesse arrive jusqu'à 1Gb/s.

Il existe deux types de fibre optique :

- **Fibre optique multimodes** : Les fibres multimodes (dites MMF, pour Multi Mode Fiber), ont été les premières sur le marché. Elles ont pour caractéristique de transporter plusieurs modes (trajets lumineux). Du fait de la dispersion modale, on constate un étalement temporel du signal proportionnel à la longueur de la fibre. En conséquence, elles sont utilisées uniquement pour des bas débits ou de courtes distances.
- **Fibre optique monomodes** : Pour de plus longues distances et/ou de plus hauts débits, on préfère utiliser des fibres monomodes (dites SMF, pour *Single Mode Fiber*), qui sont technologiquement plus avancées car plus fines.

Chaque poste est connecté à l'aide d'un câble à paire torsadé avec connecteur RJ45 à l'un des commutateurs communs de niveau 1 situé au niveau d'une salle serveur dans une armoire de brassage. Chaque commutateur possède 24 ports.

Les commutateurs niveau 1 se rassemblent au niveau d'un commutateur fédérateur niveau 1. Les commutateurs fédérateur niveau 1 se rassemblent au niveau de commutateur niveau 2, ce dernier doit se connecter à un routeur.

La distance entre commutateur fédérateur niveau 1 et commutateur niveau 2 est plus ou moins éloignée (environ 100m), pour cela le concepteur réseau a choisi d'utiliser une connexion à fibres optiques.

Le commutateur fédérateur niveau 2 contient 24 ports RJ45 et deux ports fibre optique et le commutateur du niveau 1 contient 24 ports qui rassemblent tous les départements et l'administration.

Il existe un autre commutateur commun niveau 1 qui connecte le serveur proxy et le serveur contrôleur de domaine qui est de sa part connecté à l'aide d'un câble paire torsadé au commutateur fédérateur niveau 2.

Le routeur de l'ISET de Tozeur est connecté au WAN Tunisie Télécom à l'aide d'une connexion ADSL (câble téléphonique RJ11).

La figure suivante décrit l'architecture du réseau de l'ISET de Tozeur :

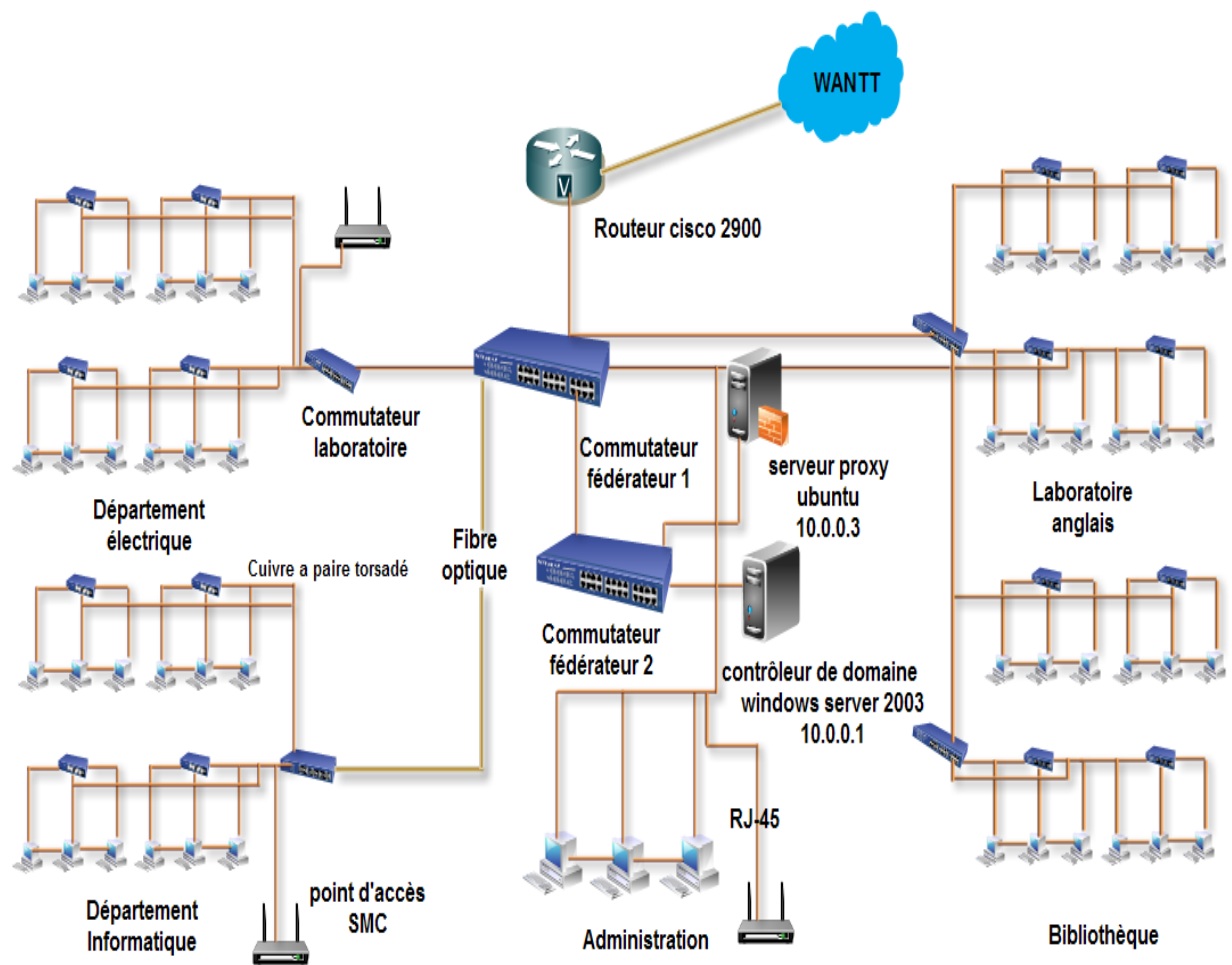


Figure 1: ARCHITECTURE DE RESEAU DE L'ISET

L'architecture de l'ISET est bien riche d'équipements réseau et de serveurs comme présenté par la figure précédente, on cite donc :

- **Les routeurs :**

L'ISET est dotée d'un routeur Cisco 2900 Séries Integrated Services Routers (ISR), il offre une connectivité hautement sécurisée avec une intégration multi-services qui peut transformer le lieu de travail avec un large éventail de services intégrés, un support riche-media, et une efficacité opérationnelle. Le routeur est un équipement de couche 3 du modèle OSI. Il ne doit pas être confondu avec un commutateur (couche 2).

- **Un serveur proxy :**

Est un ordinateur exécutant un programme passerelle à laquelle les programmes internet des autres machines du réseau local s'adressent pour leurs requêtes. Le Proxy fait la requête en son **nom sur internet puis transmet la réponse au demandeur.**

- **Serveur DHCP :**

C'est un serveur qui permet d'attribuer des adresse IP aux machines qui sont connectés au réseau local de l'ISET.

- **Serveur DNS :**

Le Domain Name System est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.

- **Point d'accès :**

Un point d'accès Wifi est un équipement réseau qui permet à votre ordinateur de se connecter sur le réseau sans fil.

Il existe 3 point d'accès a Iset Tozeur :

-SMC

-D_Link

-Dep_info

2.2. Critique de l'existant :

Le réseau sans fil de **ISET** n'est pas sécurisé. La maintenance de ce réseau est faite d'une manière manuelle par le personnel.

Le réseau wifi il est ouvert, tous les gens ce quel que soit les étudiants ou les étrangers permet de se connecter au réseau de l'ISET Tozeur ce que provoque des trouble sur le réseau ,et ce que permet au pirate d'écouter et modifier toutes les communications circulant sue le réseau .

L'emplacement des points d'accès est placé d'une manière aléatoire

Il existe trois point d'accès sont placé comme suit :

-Un point d'accès dans l'administration

-Un point d'accès dans le département technologies d'informatique

-Un point d'accès dans le département mécanique

Lorsque un étudiant se déplace dans l'ISET il n'a pas la possibilité de reste connecter sur le réseau par ce que il n'existe pas la technologie d'itinérance entre les point d'accès.

Dans l'architecture de réseau de l'ISET il n'existe pas une machine firewall, son rôle consiste à filtrer tous les paquets et les trames sur les réseaux et aussi permet de contrôler les accès aux sites web malveillants.

2.3. Solutions retenu :

Nous proposons une solution qui consiste à mettre en place une architecture de sécurité réseau sans fil basé sur l'authentification permet de :

-Gérer l'authentification des utilisateurs (login +mot de passe).

-Protéger les identités et les informations transmis des utilisateurs.

-Contrôle de stratégie : l'administrateur peut contrôler les stratégies de

Compte via un domaine existant.

Il est nécessaire donc de sécuriser tous les points d'accès dans L'ISET par le mode WPA2/AES.

Il faut configurer une machine linux comme étant une machine firewall permet de filtrer les paquets et pour obtenir une bonne sécurité au réseau.

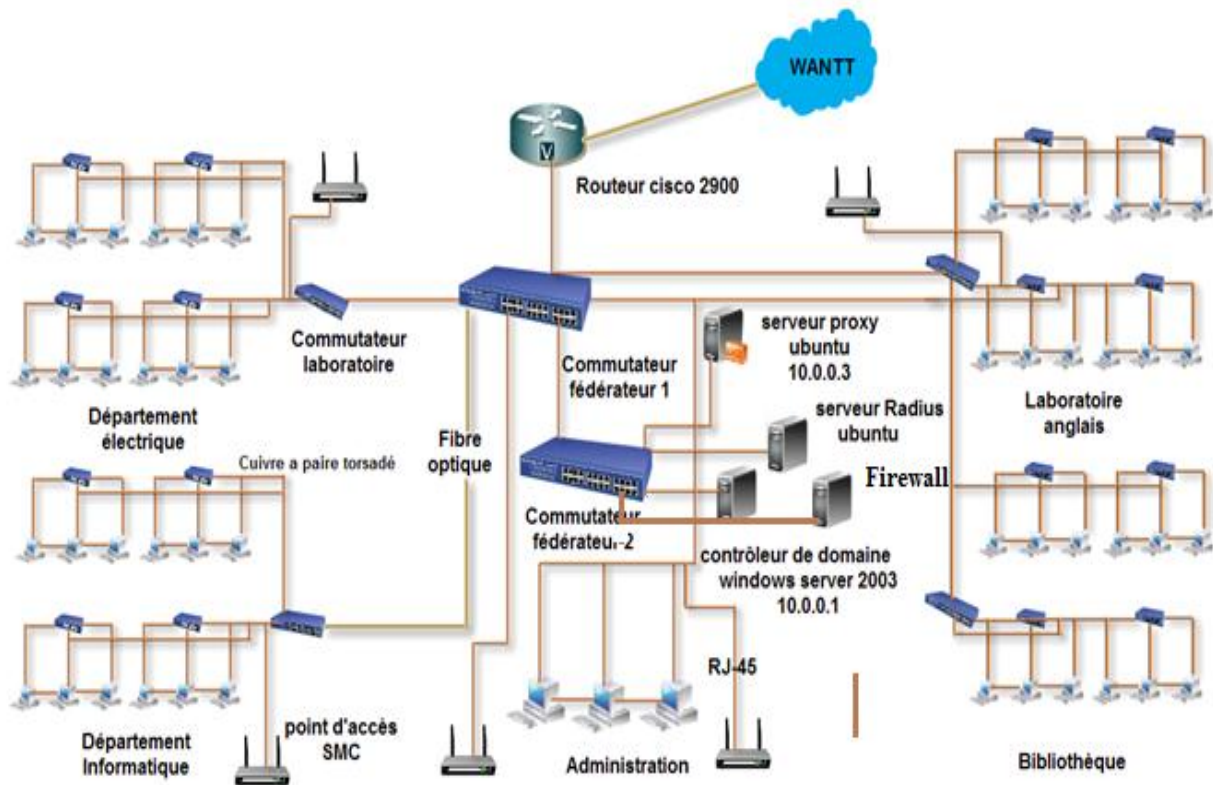


Figure 2 :SOLUTIONS RETENU

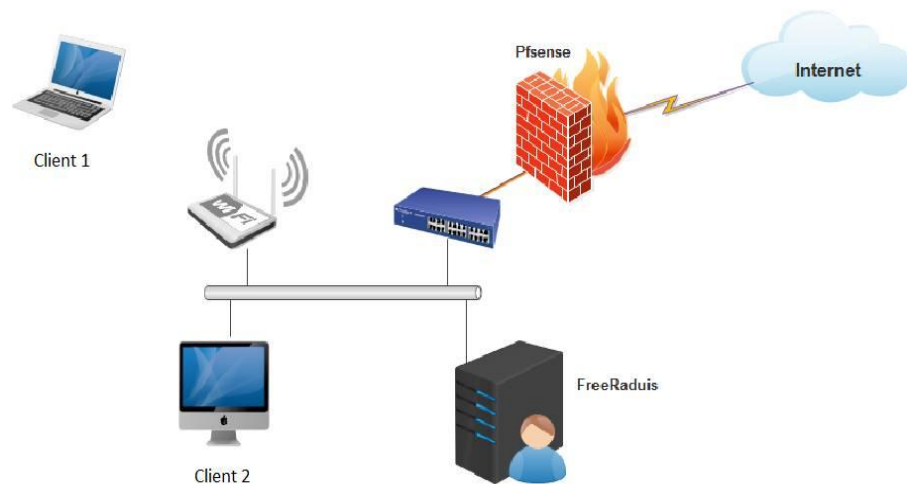


Figure 3:schéma simplifié de solution retenu

Pour atteindre de couverture totale de L'ISET nous avons proposées emplacements des points d'accès.

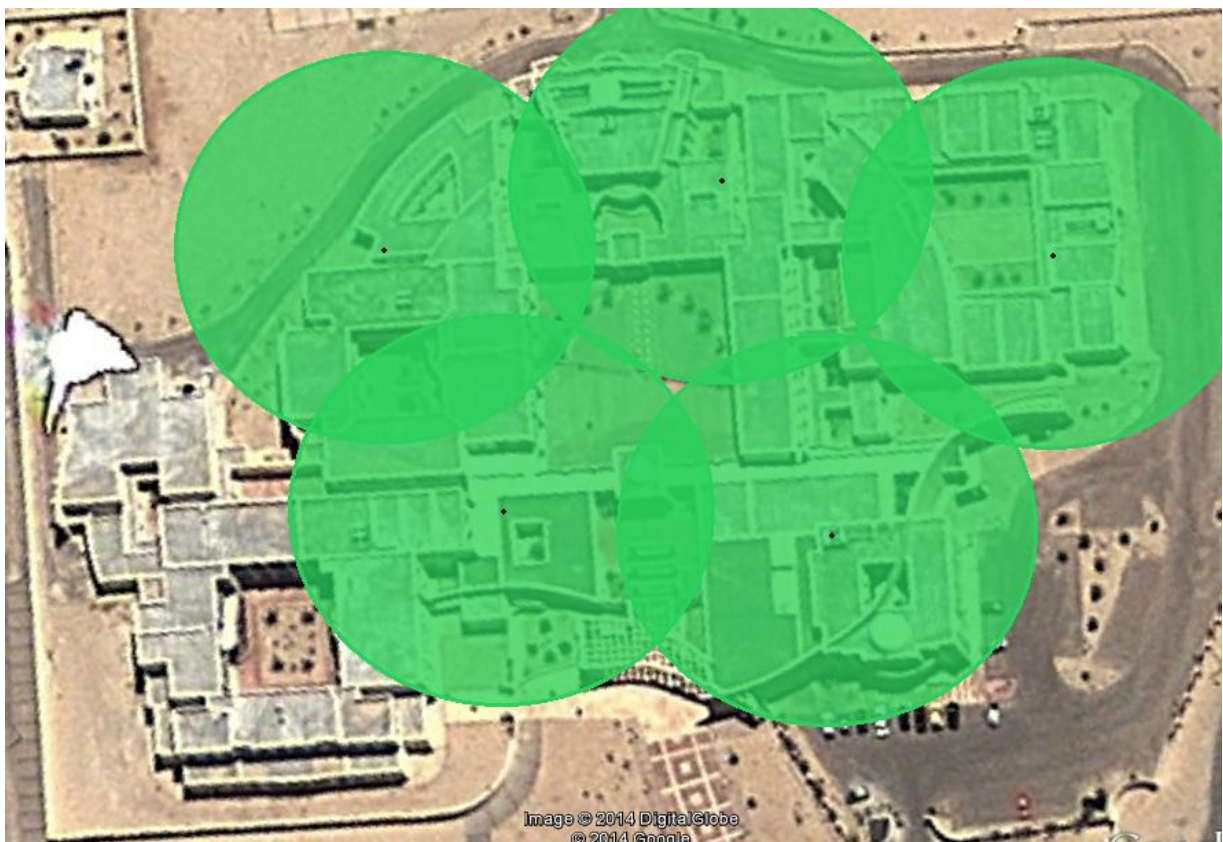


Figure 4:Emplacement proposé des points d'accès

CHAPITRE 2 : ETAT DE L'ART

Introduction :

Dans ce chapitre, nous commençons par la présentation des différents types de technologies sans fil. Ensuite nous passons à une petite tournée sur les protocoles de sécurité. Pour finir avec la définition du rôle d'un serveur radius et aussi on va présenter les différents catégories de firewall et son principe de fonctionnement générales

1. WI-FI :

Définition :

Un réseau sans fil (en anglais Wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux (ordinateur portable) peuvent communiquer sans liaison filaire.

Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

➤ Avantages WI-FI :

- **Mobilité**

Les utilisateurs sont généralement satisfaits des libertés offertes par un réseau sans fil et de fait sont plus enclins à utiliser le matériel informatique.

- **Facilité et souplesse**

Un réseau sans fil peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.

- **Coût**

Si leur installation est parfois un peu plus coûteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits ; sur le moyen terme, l'investissement est facilement rentabilisé.

- **Évolutivité**

Les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins

➤ **Inconvénients de Wi-Fi :**

▪ **Complexité**

Le premier problème auquel l'administrateur réseau est confronté est la diversité des compétences nécessaires à la mise en œuvre d'un réseau Wi-Fi. Il faut prendre en considération les problèmes de transmission radio, un éventuel audit du site, l'intégration de l'existant (réseau câblés, mais peut être aussi les quelques ilots Wi-Fi déjà en place), le respect de régulation, le support effectif des standards actuels et à venir, l'administration de ce futur réseau, le monitoring du trafic.

▪ **Qualité et continuité du signal**

Ces notions ne sont pas garanties du fait des problèmes pouvant venir des interférences, du matériel et de l'environnement.

▪ **Sécurité**

La sécurité des réseaux sans fil n'est pas encore tout à fait fiable du fait que cette technologie est novatrice. Elle est une préoccupation critique d'un administrateur réseau confronté au Wi-Fi, d'une part parce que les faiblesses des technologies ont été largement traitées sur Internet, d'autre part parce qu'il s'agit d'une approche effectivement nouvelle du sujet, et qui présente une grande diversité.

2 .Catégories de réseaux :

2.1 WPAN :

Le réseau personnel sans fil (appelé également réseau individuel sans fil ou réseau domestique sans fil et noté WPAN pour **W**ireless **P**ersonal **A**rea **N**etwork) concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à Permettre la liaison sans fil entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN : Bluetooth, Home RF, La technologie ZigBee

2.2 WMAN :

Le réseau métropolitain sans fil (**WMAN** pour *Wireless Metropolitan Area Network*) est connu sous le nom de **Boucle Locale Radio (BLR)**. Les WMAN sont basés sur la norme *IEEE 802.16*. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.

Trois grandes familles des réseaux sans fils métropolitains : Wi MAX, Les réseaux mobiles de 3e génération, MBWA

2.3 WWAN :

Le réseau étendu sans fil (**WWAN** pour *Wireless Wide Area Network*) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes :

- **GSM** (*Global System for Mobile Communication* ou en français *Groupe Spécial Mobile*)
- **GPRS** (*General Packet Radio Service*)
- **UMTS** (*Universal Mobile Telecommunication System*)

2.4 WLAN :

Le réseau local sans fil (noté **WLAN** pour *Wireless Local Area Network*) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-deux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :

Le Wifi (ou *IEEE 802.11*), soutenu par l'alliance WECA (*Wireless Ethernet Compatibility Alliance*) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètre

2.5 WRAN :

La publication de la norme *IEEE 802.22* intervient 7 ans après la création d'un groupe de travail chargé de la mise en œuvre d'une norme « Réseau régional sans fil ». Ce nouveau standard, qui exploite les bandes de radiodiffusion télévisuelle dans la gamme des hautes VHF et des basses UHF, « pourra être utilisé pour apporter l'accès à Internet à large bande (haut-débit) -de manière fiable et sécurisée- dans de vastes ensembles régionaux qui n'y ont

pas encore accès » indique l'IEEE dans un communiqué. « L'utilisation des « espaces blancs » entre les canaux occupés par les chaînes de télévision n'entraînera pas d'interférences avec la réception de celles-ci.»

2.5 Différentes Normes de WI-FI :

Le terme Wi-Fi se généralisait pour l'ensemble des normes 802.11 dont la certification est prise en charge par la WECA (devenue Wi-Fi Alliance). Le Wi-Fi couvre de nombreuses normes différentes qui ont toutes le préfixe 802.11. Un suffixe sous forme de lettre permet de distinguer les normes entre elles. Pour les particuliers, il existe en tout cinq normes différentes : 802.11a/b/g/n/ac. Chacune représente une évolution par rapport à la précédente.

802.11	Bande de fréquence	Débit théorique maximal	Portée	Congestion	Largeur canal	MIMO
A	5 GHz	54 Mbps	Faible	Faible	20 MHz	Non
B	2,4 GHz	11 Mbps	Correcte	Elevée	20 MHz	Non
G	2,4 GHz	54 Mbps	Correcte	Elevée	20 MHz	Non
n	2,4 GHz et 5 GHz	De 72 à 450 Mbps	Bonne	Elevée et faible	20 ou 40 MHz	Oui
ac	5 GHz	De 433 à 1300 Mbps	Bonne	Faible	40 ou 80 MHz	Oui

Les normes 802.11a/b/g sont celles qui posent le moins de problèmes puisque leur fonctionnement est simple. La première fonctionne dans la bande des 5 GHz, et c'est ce qui lui permet d'avoir un débit élevé pour l'époque, à 54 Mbps. Cependant, sa portée est faible puisque plus une fréquence est élevée et plus sa portée diminue. En revanche, **l'avantage de la bande des 5 GHz est sa faible congestion (= moins d'interférences) qui permet, dans les faits, d'atteindre des débits plus élevés et une meilleure stabilité de la connexion.** Pour information, la bande des 2,4 GHz est

congestionnée puisque de nombreux appareils l'utilisent également : les micro-ondes, les téléphones DECT ou encore les appareils Bluetooth.

Wi-Fi 802.11n : il permet à un appareil de disposer de plusieurs antennes pour envoyer et recevoir les informations. De base, un appareil dispose d'une seule antenne pour télécharger les informations (download) et pour les émettre (upload). Avec le MIMO 2×2, un appareil dispose alors de deux antennes. On peut monter actuellement jusqu'à 3×3 (3 antennes en réception et 3 en émission) ou des configurations plus exotiques comme 3×2 (3 pour la réception et 2 pour l'émission). Passer à 2 antennes (MIMO 2×2) permet de doubler le débit par rapport à une seule antenne.

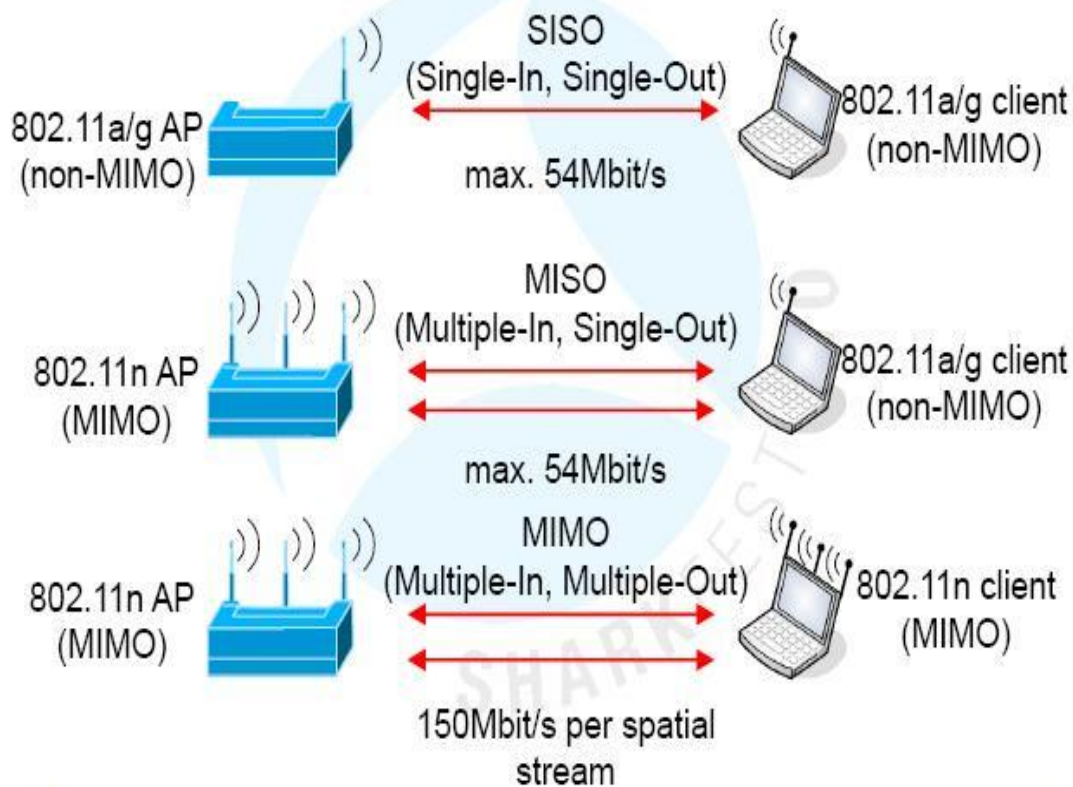


Figure 5 : Mode de topologies sans fil 802.11

- **Le mode infrastructure** dans lequel les clients sans fils sont connectés à un point d'accès. Il s'agit généralement du mode par défaut des cartes 802.11b.

Mode d'infrastructure

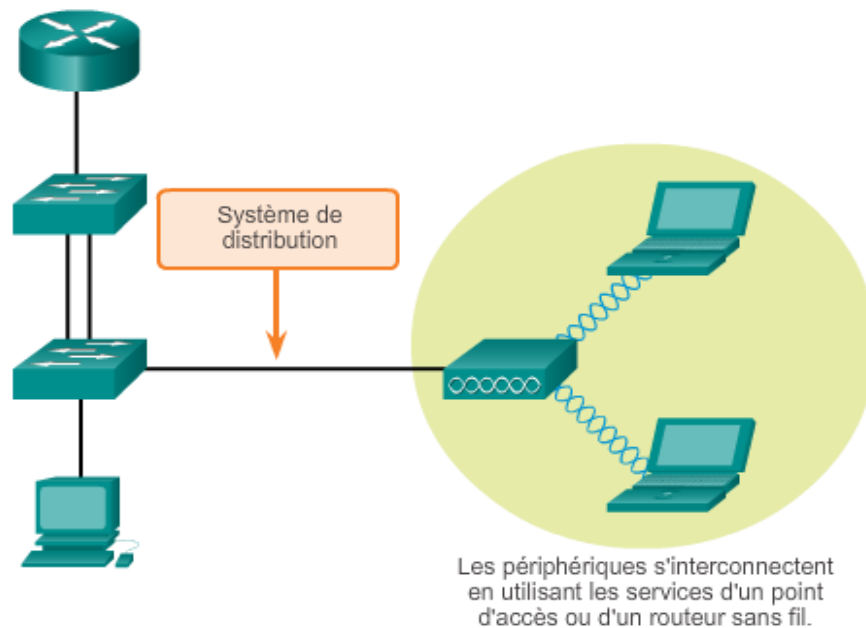


Figure 6:Mode d'infrastructure

- **Le mode ad hoc** dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès

Mode ad hoc

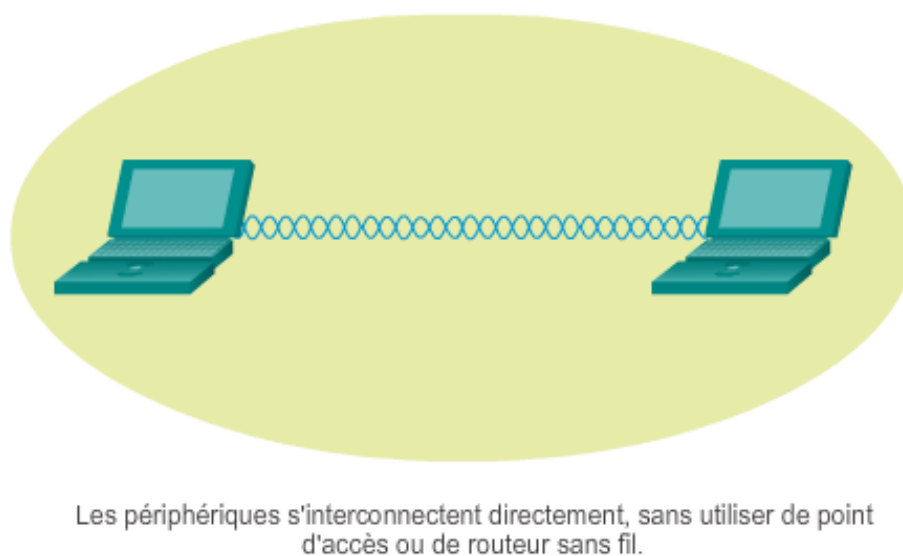


Figure 7:Mode ad hoc

3-EQUIPEMENT WI-FI :

L'installation d'un réseau Wifi nous permettra de surfer sur l'Internet sans fil. Le Wi-Fi utilisant la radio comme support de communication, il faut des périphériques particuliers pour transformer les données informatiques en signaux radio et vice-versa. Ces appareils transforment un signal numérique (des 1 et des 0), provenant d'un ordinateur ou d'un réseau filaire, en signal analogique (à valeurs réelles) envoyé vers une antenne, à l'émission, et inversement à la réception. Il s'agit donc d'un modem (MODulateur/DEModulateur), qui a la même fonction qu'un bon vieux modem téléphonique.

3-1 Point d'accès :

Dans le domaine des [réseaux de télécommunications](#), est un endroit équipé d'une structure ad-hoc permettant de se connecter matériellement à un réseau filaire ou radio, en suivant une procédure logicielle à l'aide d'un terminal

Le support physique étant les ondes radio, on ne peut pas empêcher les stations non destinataires de recevoir les trames émises, d'où l'analogie avec le hub. Les APS sont nécessaires lorsque le réseau sans fil fonctionne en mode infrastructure. Ce sont en fait des boîtes qui contiennent une carte Wi-Fi comme on en trouve sur les stations, une ou plusieurs antennes et du logiciel embarqué dans une puce pour gérer tout cela. Le logiciel présent permet de fournir des services supplémentaires liés à la sécurité et l'identification des autres AP connectés. Il est possible de transformer un ordinateur équipé d'une carte Wi-Fi en point d'accès, par simple adjonction de programmes



Figure 8 :point d'accée

3-2 Modems :

Le **modem** est le périphérique utilisé pour transférer des informations entre plusieurs ordinateurs via un support de transmission filaire (lignes téléphoniques par exemple). Les ordinateurs fonctionnent de façon numérique, ils utilisent le codage binaire (une série de 0 et de 1), mais les lignes téléphoniques sont analogiques. Les signaux numériques passent d'une valeur à une autre, il n'y a pas de milieu, de moitié, c'est du « *Tout Ou Rien* » (un ou zéro). Les signaux analogiques par contre n'évoluent pas « par pas », ils évoluent de façon continue.

3-3 Routeurs :

Un **routeur** est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles. Il y a habituellement confusion entre routeur et relais, car dans les réseaux Ethernet les routeurs opèrent au niveau de la couche 3 du modèle OSI².

4- Sécurité Wi-Fi :

4-1 WEP :

WEP (Wired Equivalent Privacy) est un protocole pour sécuriser les réseaux sans fil de type Wi-Fi. Les réseaux sans fil diffusant les messages échangés par ondes radioélectriques sont particulièrement sensibles aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans fil une confidentialité comparable à celle d'un réseau local filaire classique.

Le principe du WEP consiste à définir dans un premier temps la clé secrète. Cette clé doit être déclarée au niveau du point d'accès et des clients. Elle sert à créer un nombre pseudo aléatoire d'une longueur égale à la longueur de la trame. Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire comme masque grâce à un OU Exclusif entre ce nombre et la trame. Il utilise RC4 pour le chiffrement et CRC-32 pour l'intégrité.

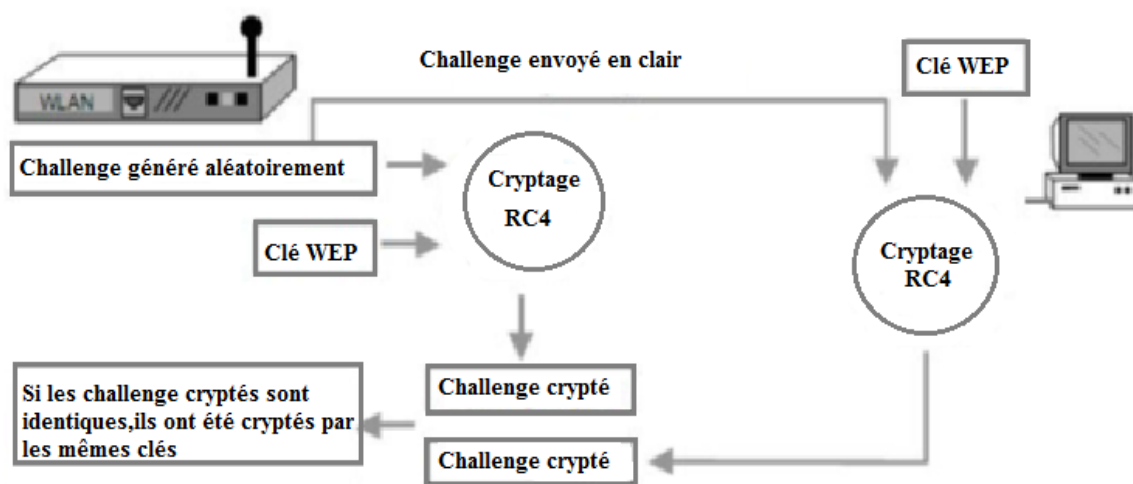


Figure 9 : principe du WEP

4.2 WPA

WPA (Wi-Fi Protected Access) est un autre protocole de sécurisation des réseaux sans fil offrant une meilleure sécurité que le WEP car il est destiné à en combler les faiblesses.

Le WPA permet un meilleur cryptage de données qu'avec le WEP car il utilise des clés TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) dites dynamiques et permet l'authentification des utilisateurs et utilise MIC pour l'intégrité. Ainsi, le WPA permet d'utiliser une clé par station connectée à un réseau sans fil, alors que le WEP lui utilisait la même clé pour tout le réseau sans fil. Les clés WPA sont en effet générées et distribuées de façon automatique par le point d'accès sans fil qui doit être compatible avec le WPA.

TKIP (Temporal Key Integrity Protocol)

Protocole permettant le cryptage et le contrôle d'intégrité des données. Ce protocole utilise toujours le RC4 (d'où sa comptabilité avec le WEP) comme algorithme de cryptage avec une clé de 128 bits, par contre l'IV passe à 48 bits. De plus il y a une clé par station (et non une pour tout le réseau avec WEP), cette clé est générée et change automatiquement de façon périodique. Le contrôle d'intégrité des données s'effectue par un code de hachage de 8 octets appelé MIC (**M**essage **I**ntegrity**C**ode) ou Michael. Ce code porte aussi les adresses MAC, ce qui évite de modifier ou forger des trames. De plus, il utilise un numéro de séquence sur les paquets, permettant un contrôle de bon séquençement.

4.3 WPA2 :

Ce standard reprend la grande majorité des principes et protocoles apportés par WPA, avec une différence notoire dans le cas du chiffrement l'intégration de l'algorithme AES. Les protocoles de chiffrement WEP et TKIP sont toujours présents. Deux autres méthodes de chiffrement sont aussi inclus dans IEEE 802.11i en plus des chiffrements WEP et TKIP.

- **WPA personnel (WPA-Personal)** : connu également sous le nom de mode à secret partagé ou WPA-PSK (Pre-shared key), WPA personnel est conçu pour les réseaux personnels ou de petites entreprises, car il n'y a pas besoin d'utiliser un serveur d'authentification. Chaque équipement du réseau sans fil s'authentifie auprès du point d'accès en utilisant la même clé sur 256 bits.

- **WPA entreprise (WPA-Enterprise)** : connu également sous le nom de mode WPA-802.1X ou WPA-EAP, WPA entreprise est conçu pour les réseaux d'entreprise et demande à ce que l'on installe un serveur d'authentification RADIUS. C'est plus compliqué à mettre en place, mais offre plus de sécurité, car cette méthode ne repose pas sur des phrases secrètes, vulnérables aux attaques par dictionnaire. Le protocole EAP (Extensible Authentication Protocol) est utilisé pour l'authentification. EAP existe en plusieurs variantes, dont EAP-TLS, EAP-TTLS et EAP-SIM.

4.4 802.1x :

Le protocole 802.1x est une solution de sécurisation d'un réseau mis au point par l'organisme de standardisation IEEE en 2001. Il a pour but de contrôler l'accès à un réseau filaire ou sans fil grâce à un serveur d'authentification. Le standard permet de mettre en relation le serveur d'authentification et le système à authentifier par des séquences par des échanges EAP. Le protocole 802.1x va donc unifier les différentes méthodes d'authentification sous la même bannière.

Le protocole fonctionne à partir de trois éléments :

- **Le client (supplicant)** : c'est le système à authentifier c'est-à-dire l'élément qui désire se connecter sur le réseau.

- **Le contrôleur (point d'accès)** : ou système authenticateur c'est-à-dire l'élément qui va demander l'authentification.

- **Le serveur d'authentification** : Ce serveur d'authentification est en général un serveur Radius. Selon la requête du suppliant.

FIREWALL

1-Définition :

Un firewall (ou pare-feu) est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).

Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.



2-CATEGORIES DE PARE-FEU :

Les pare-feux sont un des plus vieux équipements de sécurité informatique et, en tant que tels, ils ont été soumis à de nombreuses évolutions. Suivant la génération du pare-feu ou son rôle précis, on peut les classer en différentes catégories.

2-1 Pare-feu sans état (*stateless firewall*) :

C'est le plus vieux dispositif de filtrage réseau, introduit sur les routeurs. Il regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées. Ces règles peuvent avoir des noms très différents en fonction du pare-feu :

- « [ACL](#) » pour *Access Control List* (certains pare-feux [Cisco](#)),
- politique ou *policy* (pare-feu [Juniper](#)/Netscreen),

- filtres,
- règles ou *rules*,
- etc.

La configuration de ces dispositifs est souvent complexe et l'absence de prise en compte des machines à états des protocoles réseaux ne permet pas d'obtenir une finesse du filtrage très évoluée. Ces pare-feux ont donc tendance à tomber en désuétude mais restent présents sur certains routeurs ou systèmes d'exploitation.

2-2 Pare-feu à états (*stateful firewall*) :

Certains protocoles dits « à états » comme TCP introduisent une notion de connexion. Les pare-feux à états vérifient la conformité des paquets à une connexion en cours. C'est-à-dire qu'ils vérifient que chaque paquet d'une connexion est bien la suite du précédent paquet et la réponse à un paquet dans l'autre sens. Ils savent aussi filtrer intelligemment les paquets ICMP qui servent à la signalisation des flux IP.

Enfin, si les ACL autorisent un paquet UDP caractérisé par un quadruplet (ip_src, port_src, ip_dst, port_dst) à passer, un tel pare-feu autorisera la réponse caractérisée par un quadruplet inversé, sans avoir à écrire une ACL inverse. Ceci est fondamental pour le bon fonctionnement de tous les protocoles fondés sur l'UDP, comme DNS par exemple. Ce mécanisme apporte en fiabilité puisqu'il est plus sélectif quant à la nature du trafic autorisé. Cependant dans le cas d'UDP, cette caractéristique peut être utilisée pour établir des connexions directes (P2P) entre deux machines (comme le fait Skype par exemple).

2-3 PARE-FEU APPLICATIF :

Dernière génération de pare-feu, ils vérifient la complète conformité du paquet à un protocole attendu. Par exemple, ce type de pare-feu permet de vérifier que seul le protocole HTTP passe par le port TCP 80. Ce traitement est très gourmand en temps de calcul dès que le débit devient très important. Il est justifié par le fait que de plus en plus de protocoles réseaux utilisent un tunnel TCP afin de contourner le filtrage par ports.

Une autre raison de l'inspection applicative est l'ouverture de ports dynamique. Certains protocoles comme FTP, en mode passif, échangent entre le client et le serveur des adresses IP ou des ports TCP/UDP. Ces protocoles sont dits « à contenu sale » ou « passant difficilement les pare-feux » car ils échangent au niveau applicatif (FTP) des informations du niveau IP (échange d'adresses) ou du niveau TCP (échange de ports). Ce qui transgresse le principe de

la séparation des couches réseaux. Pour cette raison, les protocoles « à contenu sale » passent difficilement voire pas du tout les règles de NAT ...dynamiques, à moins qu'une inspection applicative ne soit faite sur ce protocole.

Chaque type de pare-feu sait inspecter un nombre limité d'applications. Chaque application est gérée par un module différent pour pouvoir les activer ou les désactiver. La terminologie pour le concept de module est différente pour chaque type de pare-feu : par exemple : Le protocole HTTP permet d'accéder en lecture sur un serveur par une commande GET, et en écriture par une commande PUT. Un pare-feu applicatif va être en mesure d'analyser une connexion HTTP et de n'autoriser les commandes PUT qu'à un nombre restreint de machines.

2-4 PARE-FEU IDENTIFIANT :

Un pare-feu réalise l'identification des connexions passant à travers le filtre IP. L'administrateur peut ainsi définir les règles de filtrage par utilisateur et non plus par adresse IP ou adresse MAC, et ainsi suivre l'activité réseau par utilisateur.

Plusieurs méthodes différentes existent qui reposent sur des associations entre IP et utilisateurs réalisées par des moyens variés. On peut par exemple citer authpf (sous OpenBSD) qui utilise ssh pour faire l'association. Une autre méthode est l'identification connexion par connexion (sans avoir cette association IP = utilisateur et donc sans compromis sur la sécurité), réalisée par exemple par la suite NuFW, qui permet d'identifier également sur des machines multi-utilisateurs.

On pourra également citer Cyberoam qui fournit un pare-feu entièrement basé sur l'identité (en réalité en réalisant des associations adresse MAC = utilisateur) ou Check Point avec l'option NAC Blade qui permet de créer des règles dynamiques basée sur l'authentification Kerberos d'un utilisateur, l'identité de son poste ainsi que son niveau de sécurité (présence d'antivirus, de patches particuliers).

2-5 PARE-FEU PERSONNEL :

Les pare-feux personnels, généralement installés sur une machine de travail, agissent comme un pare-feu à états. Bien souvent, ils vérifient aussi quel programme est à l'origine des données. Le but est de lutter contre les virus informatiques et les logiciels espions.

2-6 Portail captif :

Les portails captifs sont des pare-feux dont le but est d'intercepter les usagers d'un réseau de consultation afin de leur présenter une page web spéciale (par exemple : avertissement, charte d'utilisation, demande d'authentification, etc.) avant de les laisser accéder à Internet. Ils sont utilisés pour assurer la traçabilité des connexions et/ou limiter l'utilisation abusive des moyens d'accès. On les déploie essentiellement dans le cadre de réseaux de consultation Internet mutualisés filaires ou Wi-Fi.

3 FONCTIONNEMENT GENERALE :

Le pare-feu était jusqu'à ces dernières années considéré comme une des pierres angulaires de la sécurité d'un réseau informatique (il perd en importance au fur et à mesure que les communications basculent vers le HTTP sur SSL, court-circuitant tout filtrage). Il permet d'appliquer une politique d'accès aux ressources réseau (serveurs).

Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).

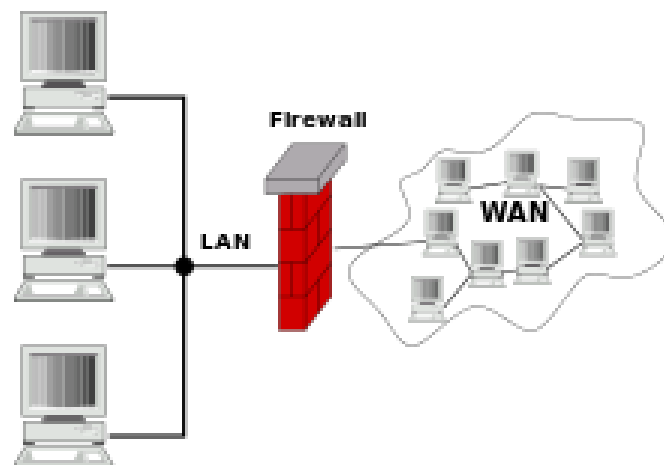


Figure 10:Pare-feu passerelle entre LAN et WAN

Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège.

Le filtrage se fait selon divers critères. Les plus courants sont :

- l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.) ;

- les options contenues dans les données (fragmentation, validité, etc.) ;
- les données elles-mêmes (taille, correspondance à un motif, etc.) ;
- les utilisateurs pour les plus récents.

Un pare-feu fait souvent office de routeur et permet ainsi d'isoler le réseau en plusieurs zones de sécurité appelées zones démilitarisées ou DMZ. Ces zones sont séparées suivant le niveau de confiance qu'on leur porte.

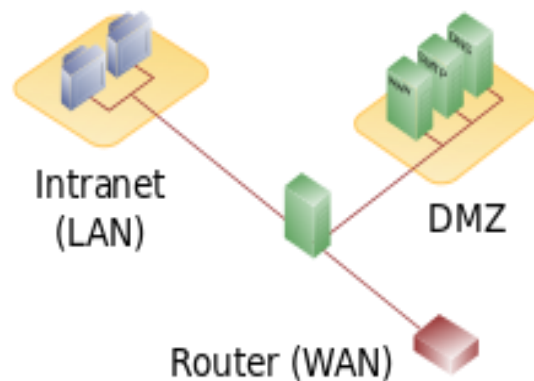


Figure 11:Pare-feu routeur, avec une zone DMZ

Enfin, le pare-feu est également souvent extrémité de tunnel [IPsec](#) ou [SSL](#). L'intégration du filtrage de flux et de la gestion du tunnel est en effet nécessaire pour pouvoir à la fois protéger le trafic en confidentialité et intégrité et filtrer ce qui passe dans le tunnel. C'est le cas notamment de plusieurs produits du commerce nommés dans la liste ci-dessous.

CONCLUSION :

Dans ce chapitre nous avons commencé par la présentation de différent type de réseaux sans fils. Ensuite, nous avons introduit les protocoles de sécurité et nous avons présenté les différentes catégories de firewall et son principe de fonctionnement.

CHAPITRE 3

PRESENTATION DES OUTILS

INTRODUCTION :

Dans ce chapitre on va représenter les différents outils qu'on va l'étudier, tel que son rôle et son principe de fonctionnements

I. FREERADIUS :

1. DEFINITION :

FreeRadius (*RemoteAuthentication Dial-In User Service*) est un serveur Radius libre sous licence BSD soutenu par la société Network Radius SARL. Le protocole RADIUS permet de centraliser les informations d'authentification des utilisateurs. Ces informations sont stockées dans une base de données. Elles sont sollicitées lorsque le client (*l'utilisateur*) tente d'établir une session. La requête est alors transmise à un serveur (*client ou nas*) qui soumet la requête d'authentification au serveur radius central. Cet exemple peut être illustré avec les réseaux wifi de grande envergure. Les utilisateurs sont stockés dans la base de données du serveur radius. L'opérateur dispose de plusieurs points d'accès pour proposer son service sans fil. Lorsqu'un client se connecte avec ses identifiants, ces derniers sont soumis à la borne wifi. Cette dernière transmet la requête d'authentification au serveur RADIUS central qui répond favorablement ou non à la requête initiale.

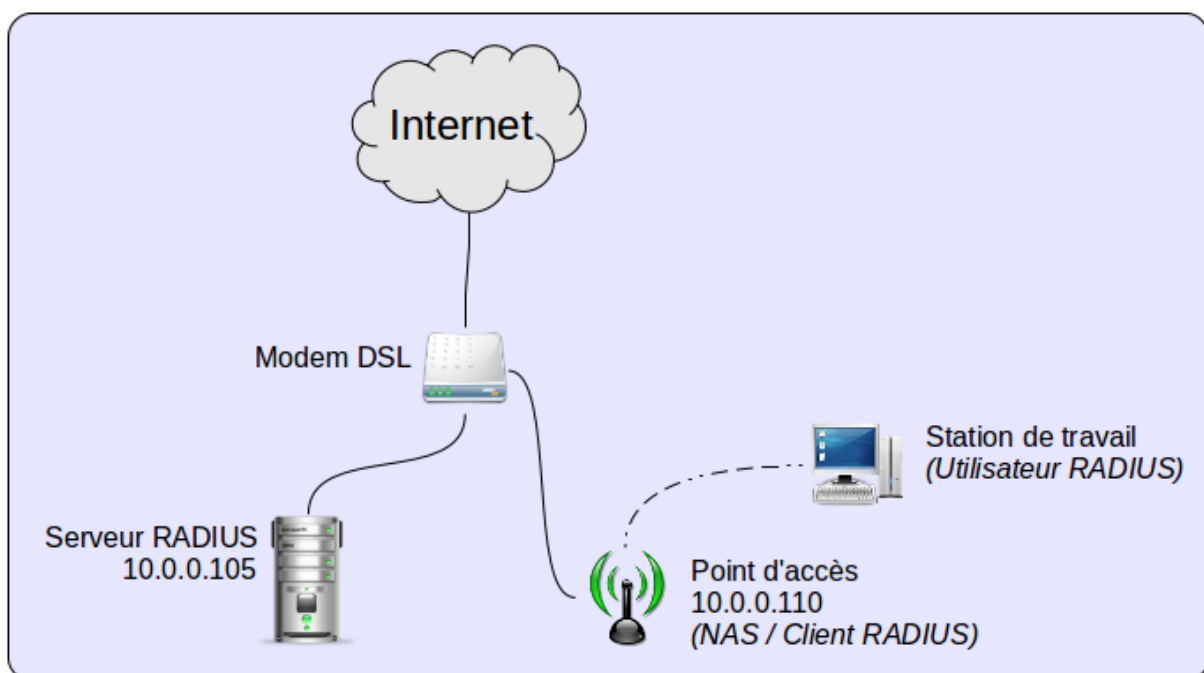


Figure 12:mécanisme générale de Freeradius

2. Caractéristiques :

Radius utilise le protocole « AAA »

- Authentification (Authentication) : vérification de l'identité d'un utilisateur.
- Autorisation (Authorization) : droits accordés à un utilisateur (accès à une partie d'un réseau, à des fichiers, le droit d'écriture...).
- Comptabilité (Accounting) : informations récoltées pendant toute la durée de la session, après identification de l'utilisateur.

Le protocole est basé sur des échanges requêtes/réponses avec les clients Radius, c'est-à-dire les NAS. Il n'y a jamais de communication directe entre le poste de travail et le serveur.

Les ports utilisés seront :

1812 pour recevoir les requêtes d'authentification et d'autorisation.

1813 pour recevoir les requêtes de comptabilité.

RADIUS utilise le protocole UDP sur le port 1812 pour le transport de ses données.

Pour l'authentification il y a quatre types de paquets :

Access-Request	Envoyé par le contrôleur d'accès, contenant les informations sur le client (login/mot de passe, ...).
Access-Accept	Envoyé par le serveur dans le cas où l'authentification est un succès.
Access-Reject	Envoyé par le serveur dans le cas où l'authentification est un échec, ou si il souhaite fermer la connexion
Access-Challenge	Envoyé par le serveur pour demander des informations complémentaires, et donc la réémission d'un paquet Access-Request.

Tableau 1:Les Types Des Paquet Radius

Le serveur RADIUS supporte plusieurs méthodes parmi lesquelles le mode :

➤ PAP (PasswordAuthentication Protocol) :

Le protocole PAP est, comme son nom l'indique, un protocole d'authentification par mot de passe.

Le principe du protocole PAP consiste à envoyer l'identifiant et le mot de passe en clair à travers le réseau. Si le mot de passe correspond, alors l'accès est autorisé.

➤ CHAP (Challenge Handshake Authentication Protocol) :

Le protocole CHAP, est un protocole d'authentification basé sur la résolution d'un « défi » (en anglais « challenge »), c'est-à-dire une séquence à chiffrer avec une clé et la comparaison de la séquence chiffrée ainsi envoyée.

Le protocole CHAP améliore le protocole PAP dans la mesure où le mot de passe n'est plus transmis en clair sur le réseau.

➤ MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) :

Microsoft a mis au point une version spécifique de CHAP, baptisée MS-CHAP améliorant globalement la sécurité.

En effet, le protocole CHAP implique que l'ensemble des mots de passe des utilisateurs soient stockés en clair sur le serveur, ce qui constitue une vulnérabilité potentielle.

Ainsi MS-CHAP propose une fonction de hachage propriétaire permettant de stocker un hash intermédiaire du mot de passe sur le serveur. Lorsque la machine distante répond au défi, elle doit ainsi préalablement hacher le mot de passe à l'aide de l'algorithme propriétaire.

3. Principe de fonctionnement :

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
- Le NAS achemine la demande au serveur RADIUS.
- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur.

Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :

- **ACCEPT** : l'identification a réussi ;
- **REJECT** : l'identification a échoué ;
- **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « challenge »).
- **CHANGE PASSWORD** : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

Suivant le schéma de la figure, c'est l'utilisateur qui va envoyé (1) vers le serveur Radius les éléments d'authentification (certificat, identifiant, mot de passe...). Cependant, il ne communique pas directement avec le serveur et d'ailleurs, il ne le connaît pas. C'est le NAS qui va servir d'intermédiaire (2), car il connaît l'adresse du serveur.

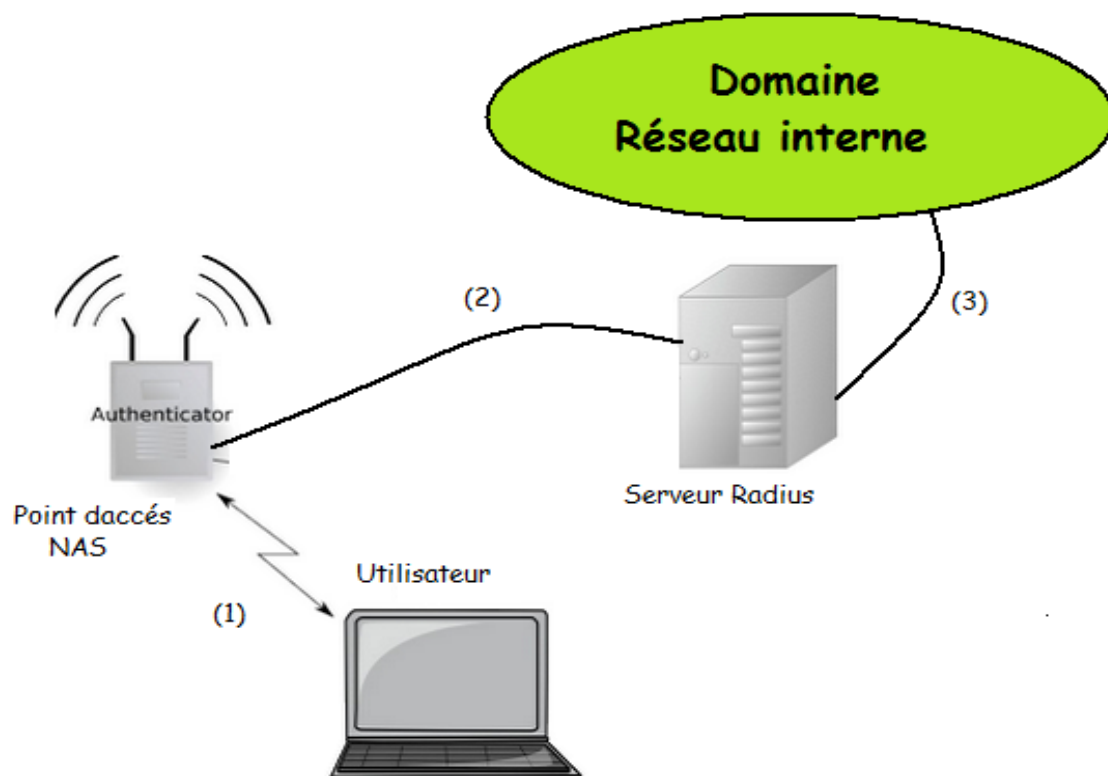


Figure 13: changements password par étape

4. Principe de protocole 802.1X(EAP) :

1. Définition :

Le protocole 802.1X a pour but d'authentifier un client afin de lui autoriser l'accès à un réseau.

On utilise le protocole EAP (Extensible Authentication Protocol) et un serveur d'authentification qui est généralement un serveur RADIUS.

Le protocole 802.1X implique une communication indirecte entre le poste de travail et le serveur Radius, cette communication s'établit d'abord entre le poste de travail et le NAS

(Point d'accès) en s'appuyant sur le protocole EAP, puis entre le NAS (point d'accès) et le serveur Radius, par encapsulation, en s'appuyant sur le protocole Radius.

Le protocole EAP est utilisé pour transporter le protocole d'authentification qu'on veut utiliser (TLS, PEAP...).

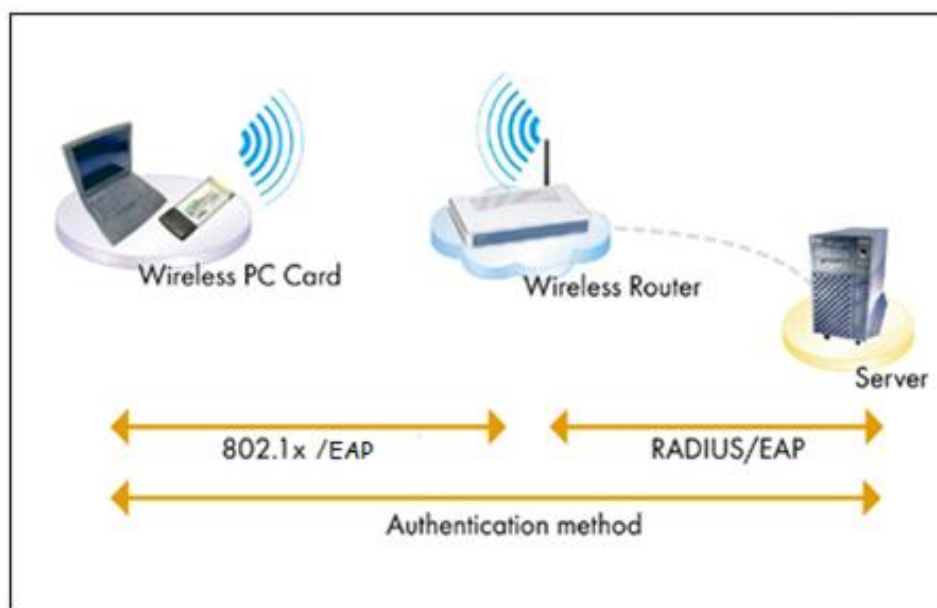


Figure 14:architecture réseau

Le point d'accès sert alors d'intermédiaire entre les deux parties et encapsule les paquets EAP venant du client dans les paquets du protocole Radius. Et c'est avec ce protocole qu'il communique avec le serveur.

Entre le poste de travail et l'équipement réseau, le protocole est appelé « EAP over WAN » (EAPoW)

2. Authentification basé sur le contrôle de port :

Dans notre cas le système authenticateur est le point d'accès qui fait office de relais entre les ordinateurs portables et le serveur d'authentification (Radius). La principale innovation amenée par le standard 802.1X consiste à scinder le port d'accès physique au réseau en deux ports logiques, qui sont connectés en parallèle sur le port physique. Le premier port logique est dit « contrôlé », et peut prendre deux états « ouvert » ou « fermé ».

Le deuxième port logique est, lui, toujours accessible mais il ne gère que les trames spécifiques à 802.1X.

Lorsque l'utilisateur (client) découvre le point d'accès (client Radius), ce dernier ne lui ouvre pas de port, jusqu'à ce que le l'utilisateur (client) soit authentifié par le serveur radius. Seul le trafic nécessaire à 802.1x sera toléré avant une authentification réussie.

a. Port non contrôlé :

Par défaut le trafic est autorisé sur le port du contrôleur d'accès, mais uniquement en direction du serveur d'authentification.

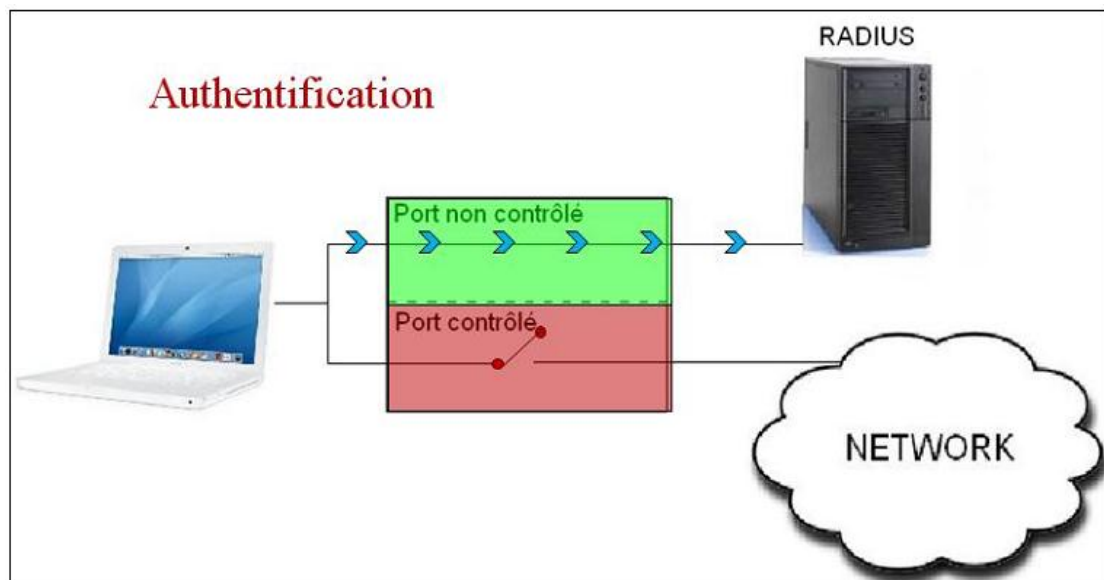


Figure 15:port non contrôlé

b. port contrôlé :

Une fois que l'authentification du client est réalisée, et si celui-ci est autorisé à accéder au réseau, alors le port est ouvert en direction du réseau.

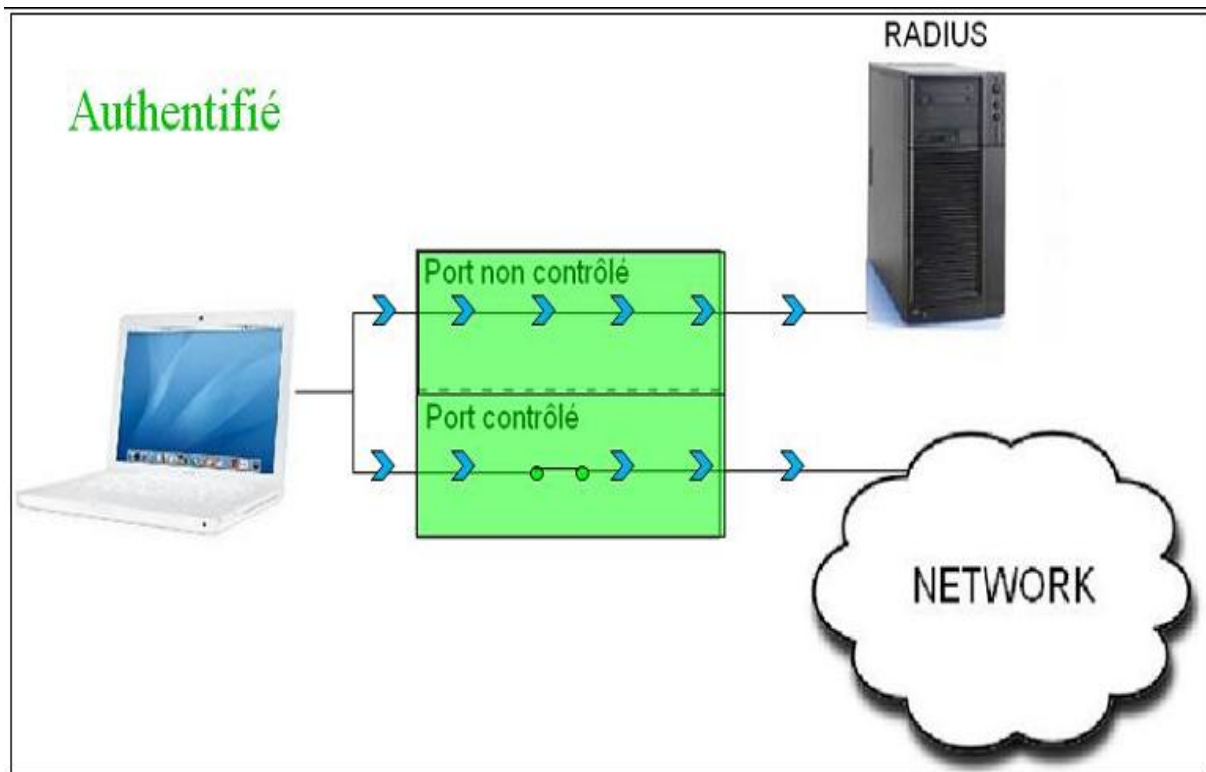


Figure 16:Port Contrôlé

3. Protocole EAP :

La communication entre l'équipement réseau (authenticator) et le serveur d'authentification est assurée par le protocole EAP (Extensible Authentication Protocol), le 802.1X ne fournissant qu'un cadre fonctionnel à l'interaction entre les équipements. Ce protocole EAP est un protocole de transport des informations d'authentification et permet d'utiliser différentes méthodes d'authentification.

Le domaine d'application de ce protocole correspond donc à tous les modes de connexion pouvant être considérés comme des connexions dites point à point telles que : connexion réseau sans fil entre un poste utilisateur et une borne d'accès, connexion filaire entre un poste utilisateur et point d'accès.

4. Les paquets EAP :

Un message EAP peut être de quatre types/code :

Request	Le système authentificateur émet une requête d'information.
Response	Réponse du système à authentifier à un paquet Request.
Success	Le système authentificateur indique une authentification réussie.
Failure	Le système authentificateur indique un échec de l'authentification.

Tableau 2: les types des paquets EAP

Il existe plusieurs méthodes d'authentification portées par les paquets EAP.

Ces principaux mécanismes sont de trois types différents :

- Méthode par mot de passe.
- Méthode par certificats.
- Méthode par carte à puce

C'est pourquoi il existe de multiples extensions EAP permettant un niveau de confidentialité convenable.

Ce tableau décrit plus en profondeur les méthodes suivant :

Type EAP	Méthode d'authentification	Remarques
EAP-MD5	Login/Mot de passe	Facile à implémenter. Supporté par beaucoup de serveur. Utilise les mots de passe en clair. Pas d'authentification mutuelle.
EAP-TLS	Certificat	Utilisation de certificats pour le serveur et les clients. Solide mais plus compliqué à gérer à cause des certificats. Authentification mutuelle entre le serveur et le client.
EAP-TTLS	Login/Mot de passe	Création d'un tunnel TLS. Supporte PAP, CHAP, MSCHAP. Certificat obligatoire coté serveur, optionnel coté client. Authentification mutuelle.
EAP-PEAP	Login/Mot de passe	Similaire à EAP-TTLS. Création d'un tunnel TLS.

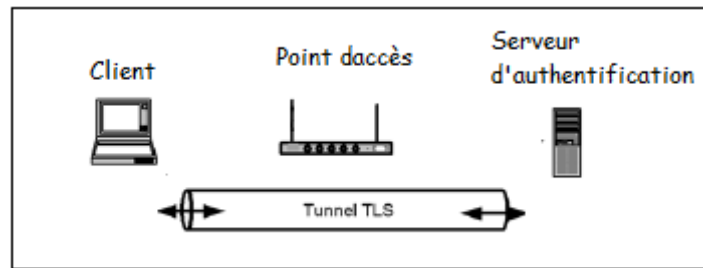
Tableau 3: Méthode d'authentification

- Méthode par certificat :

Pour l'authentification nous aurons choisi la méthode par certificat qui est basé sur EAP-TLS, EAP-PEAP :

- **EAP-TLS :**

TLS dispose de trois fonctions : l'authentification du serveur, l'authentification du client et le chiffrement.

**Figure 17: EAP-TLS**

Le chiffrement dont il est question ici a pour but de créer un tunnel protégé dans lequel passeront les données sensibles une fois que l'authentification sera faite.

TLS est un protocole d'authentification mutuelle par certificat du client et du serveur. Chacun doit donc posséder un certificat qu'il envoie à l'autre qui l'authentifie.

- **Le protocole EAP/PEAP :**

PEAP est un protocole qui a été développé par Microsoft, Cisco et RSA Security pour pallier le principal problème d'EAP/TLS, à savoir la nécessité de distribuer des certificats à tous les utilisateurs ou machines.

Comme avec EAP/TLS, c'est une authentification mutuelle qui s'établit entre le client et le serveur. Mais cette fois, elle est asymétrique. Le serveur sera authentifié par son certificat auprès du client qui, lui-même, s'authentifiera auprès du serveur par la présentation d'un identifiant et d'un mot de passe.

Seul le serveur a besoin d'un certificat. Mais les clients doivent tout de même installer le certificat de l'autorité qui a émis le certificat du serveur. Cela permet de s'assurer que les mots de passe sont envoyés au bon serveur.

Comme un mot de passe va être envoyé par le client au serveur, il faudra bien que ce dernier le valide en fonction d'une base d'authentification qu'il pourra interroger. Le serveur Radius devra donc être paramétré de manière à pouvoir valider le mot de passe.

En principe, si on décide d'utiliser PEAP, cela signifie que cette base existe déjà, en général, il s'agit d'une base Windows.

5. Séquence d'authentification d'une session 802.1X/EAP :

Avant la connexion du système à authentifier au port physique du système authenticateur, le port contrôlé de ce dernier est bloqué, et seul le port non contrôlé est accessible.

Lorsque le système à authentifier se connecte au port physique du système authenticateur, il reçoit un paquet EAP l'invitant à s'authentifier.

Sa réponse est reçue sur le port non contrôlé du système authenticateur, puis est retransmise au serveur d'authentification par ce dernier.

Par la suite, un dialogue s'établit entre le serveur d'authentification et le système à authentifier par le biais du relais offert par le port non contrôlé du système authenticateur.

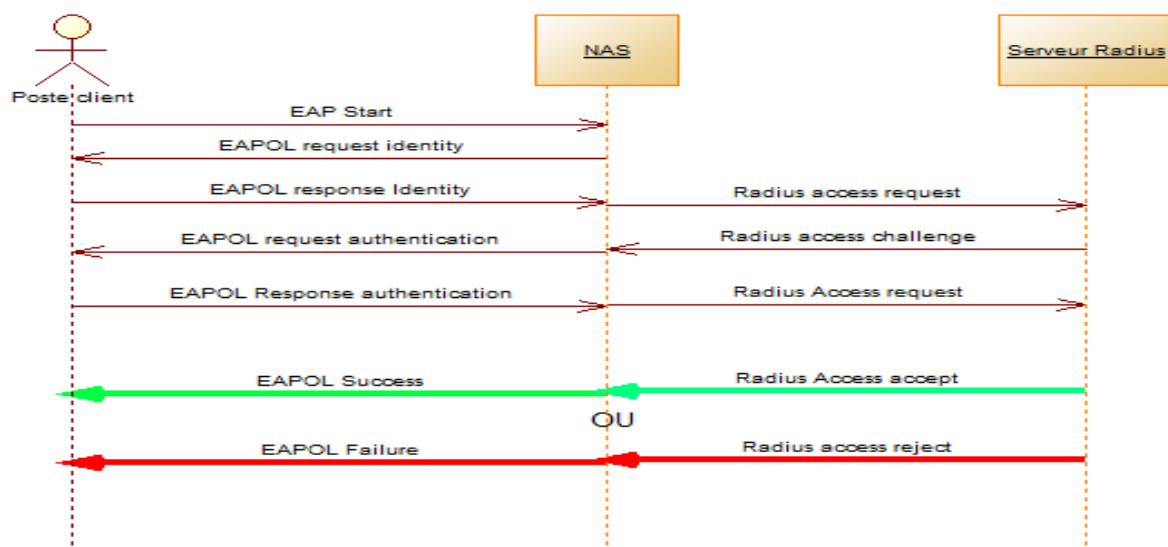


Figure 18:Diagramme de séquence d'authentification

II. PFSENSE :

1. Introduction :

Nous avons décidé d'étudier les principaux services fournis par l'excellent routeur/Pare-feu.

PfSense. C'est un système Open source basé sur le système d'exploitation FreeBSD, réputé pour être extrêmement stable. De plus, PfSense ne réinvente pas la poudre puisqu'il reprend le cœur du Routeur/Firewall m0n0wall (<http://m0n0.ch/wall/>) et y ajoute ses propres fonctionnalités.

C'est précisément de cette partie dont nous allons traiter dans ce document la distribution PfSense propose en cela une multitude d'outils Open Sources permettant à l'administrateur réseau d'optimiser ses tâches.

Au début d'année 2009, PfSense a sorti un livre blanc payant nommé : Guide Book : the Definitive Guide, qui relate de tout ce qui concerne PfSense. Notre volonté n'est pas de le copier mais d'avoir une approche basée sur le retour d'expérience. Ainsi nos parties sont constituées d'une présentation de la technologie concernée, des solutions techniques associées (comparaison si besoin) et d'une mise en pratique. Notre analyse est en somme la problématique suivante : comment mettre en place tel ou tel service intégré PfSense en pratique.

2. Descriptions :

PfSense est un portail captif à base de Linux FreeBSD. Ses avantages principaux sont :

- 1 => Sa Disponibilité (Base FreeBSD, loadbalancing, etc...) ;
- 2 => Sa confidentialité (HTTPS Web GUI, HTTPS authentication, IPSEC, PPTP, etc...) ;
- 3 => Ses possibilités de suivi et audits ;
- 4 => Sa mise à jour (système upgradable, packages visibles et téléchargeables directement depuis l'interface d'administration web, etc...) ;
- 5 => Simplicité d'administration et d'installation ;

6 => Autonomie complète.

En gros, un portail sécurisé avec fonctions de firewall sous une distribution libre et simple d'utilisation pour des personnes initiées aux problématiques réseaux.

3. Services proposés :

Ceci parmi les services de PfSense :

- Portail Captif
- VPN site à site (OpenVPN)
- Répartition de charge avec Load Balancer
- Vlans Virtuelles
- Partage de bande passante TrafficShaper
- Filtrages des sites Web
- Blocage de sites Web
- Squid
- SquidGuard
- NAT (Network Adresse Translation)
- Proxy transparent qui joue le rôle de serveur mandataire

4. Principe de fonctionnements :

Le client se connecte au réseau par l'intermédiaire d'une connexion filaire ou au point d'accès pour du wifi. Ensuite un serveur DHCP lui fournit une adresse IP ainsi que les paramètres de la configuration du réseau. A ce moment-là, le client à juste accès au réseau entre lui et la passerelle, cette dernière lui interdisant, pour l'instant, l'accès au reste du réseau. Lorsque le client va effectuer sa première requête de type web en HTTP ou HTTPS, la passerelle le redirige vers une page web d'authentification qui lui permet de s'authentifier grâce à un login et un mot de passe. Cette page est cryptée à l'aide du protocole SSL pour sécuriser le transfert du login et du mot de passe. Le système d'authentification va alors contacter une base de données contenant la liste des utilisateurs autorisés à accéder au réseau.

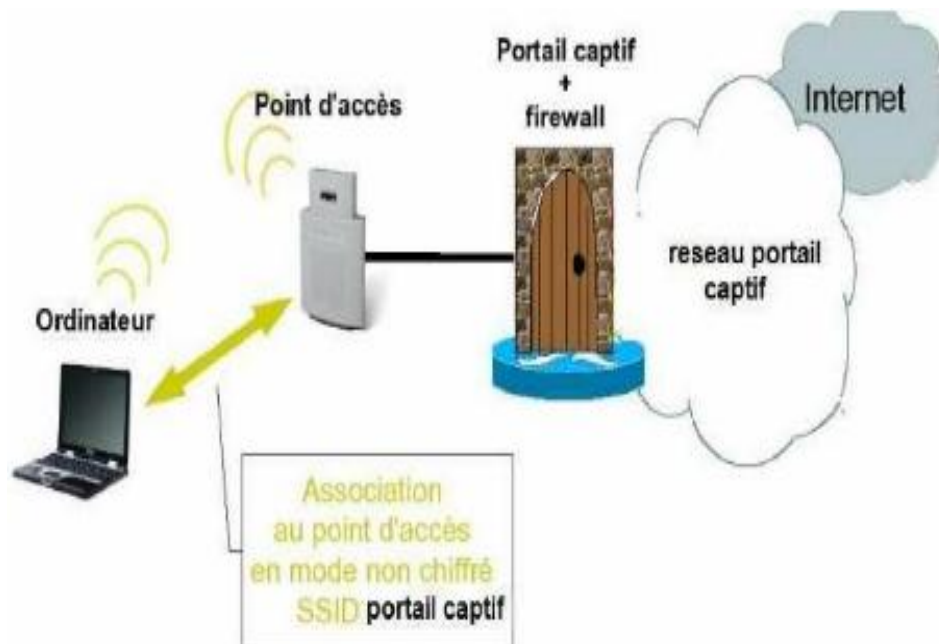


Figure 19: fonctionnement de portail captif

CONCLUSION :

Dans ce chapitre on a connu le definition de freeradius et ses carecterstiquetelque aussi son principe de fonctionnement .et dans une deuxieme titre on a étudié le description de pfsense et ses services .

CHAPITRE 4

REALISATIONS

I. ENVIRONNEMENT MATERIELS ET LOGICIEL :**1. Points d'accès :**

<i>Point d'accès</i>	SMC SMCWEBS-N
<i>Portée expérimentale</i>	25m
Connecteurs	Ethernet - RJ45 Femelle
Modes de fonctionnement	Mode point d'accès Mode Ethernet client
Puissance antenne	2Dbi
Cryptage	WEP, WPA, WPA-PSK, WPA2-PSK

Tableau 4 :caractéristiques de point d'accès**2. Machine Client :**

- Marque : DELL
- Processeur : Intel(R) Core™ i5-2430M CPU @ 2.10 GHz
- Mémoire vive : 6 Go
- Système d'exploitation : Windows 7 édition Intégrale
- Type du system : 32 bits

3. Machine Serveur :

- Marque : Acer
- Processeur : Intel® Core™ i3 4005 CPU @ 1.70 GHz
- Mémoire vive : 4 Go
- Type de System : 32 bits
- Système d'exploitation : Windows 7 édition Intégrale

4. Les logiciels :

- ✓ **VirtualBox** : Est un logiciel libre de virtualisation publié par Oracle et un hyperviseur de type 2 il permet d'installer une ou plusieurs machines virtuel sur une même machine physique.

- ✓ **NTRadPing** : C'est une application Windows qui test le service FreeRadius

5. Présentations des machines virtuelles :

- **Machine Debian** : c'est une machine de base linux configuré comme un serveur Radius avec les caractéristiques suivant :
 - ✓ Fichier iso Debian 7.8.0 32 bits (500.000 Ko)
 - ✓ Mémoire vive 750 MO
 - ✓ Carte de bouclage Microsoft
- **Machine PfSense** : c'est une machine a base BSD configure comme un serveur Firewall avec les caractéristiques suivant :
 - ✓ Fichier iso pfSense CE-2.3 32 bits (566.920 Ko)
 - ✓ Mémoire Vive 512 Mo
 - ✓ Carte de bouclage Microsoft
 - ✓ Carte Qualcomm Atheros AR5BWB222 Wireless Network Adapter
- **Machine Windows XP** : c'est une machine Windows configure comme étant une machine Client de serveur pfSense avec les caractéristiques suivants :
 - ✓ Fichier iso Windows XP-French (628.75 Mo)
 - ✓ Mémoire vive 256 MO
 - ✓ Carte de bouclage Microsoft

III. TRAVAIL REALISE :

RADIUS

Dans ce chapitre on va représenter comment on a configuré et installer Freeradius et le PfSense a l'aide de lignes de commandes et des imprimés écrans

1. Installations FreeRadius :

- **Installation Apache**

Nous avons installé en premier lieu le serveur apache par la commande :

- ✓ Sudo apt-get install apache2

Maintenant nous allons ouvrir notre navigateur et nous allons sur la page <http://localhost>. Si vous voyez le message « It works! » c'est que vous avez réussi et Apache fonctionne parfaitement.

- **Installation de MySQL**

Le deuxième serveur configuré est **mysql**et l'installation peut être faite en deux lignes de commande :

- ✓ Sudo apt-get install mysql-server
- ✓ Sudo apt-get install mysql-client

- **Installation ldap**

Nous allons installer le daemon serveur **slapd** d'OpenLDAP et le paquet **ldap-utils**, un paquet contenant des utilitaires de gestion de LDAP avec la commande :

- ✓ Sudo apt-get install slapd ldap-utils.

- **Installation Webmin**

Le dernière serveur qui nous avons installé est configurer est **Webmin** et l'installation peut être faite par les commandes suivantes :

- ✓ `sudo apt-get install perllibnet-ssleay-perlopenssllibauthen-pam-perllibpam-runtime libio-pty-perl apt-show-versions python`
- ✓ `wget http://prdownloads.sourceforge.net/webmin/webmin_1.580_all.deb`
- ✓ `sudo dpkg -i webmin_1.580_all.deb`

Nous allons exécuter les commandes suivantes pour installer le serveur Freeradius ainsi que d'autres serveurs nécessaires à son fonctionnement :

- ✓ `Sudo apt-get install freeradius freeradius-utils`
- ✓ `Sudo apt-get install freeradius-mysql`

2. Configuration de FreeRadius:

Après l'installation de Freeradius on va faire un test interne et on configure quelque fichier :

Users :

Est le fichier des utilisateurs. Un utilisateur est défini par son nom et sa méthode d'authentification (en fonction des méthodes, ce fichier peut contenir des mots de passe).

On ajoute un nouvel utilisateur dans le fichier users

On ouvre le fichier users avec l'éditeur gedit et avec la commande

`#gedit users`

On va écrire la ligne suivante pour ajouter l'utilisateur "tozeur" :

"tozeur" Cleartext-Password : "hello"

clients.conf:

Pour définir et paramétrer le dialogue avec les authentificateurs. Ici sont recensés les authentificateurs via un nom, une adresse IP et un secret partagé. D'autres informations optionnelles peuvent être ajoutées pour éviter les connexions simultanées d'un même utilisateur.

Le mot de passe ou le secret par défaut est **testing123** on le trouve dans le fichier **clients.conf** et on peut le modifier

On ouvre le fichier users avec l'éditeur gedit et avec la commande

#geditclients.conf

On va redémarrer le serveur FreeRadius avec la commande :

#service freeradius restart

Pour tester l'utilisateur 'tozeur' il faut :

-Lancer le FreeRADIUS en mode « debug » avec la commande : **#freeradius -X**

-ouvrir un autre terminal et écrire la commande :

#radtesttozeur hello 127.0.0.1 0 testing123

Nous devrions obtenir la réponse :

```
root@debian:/etc/freeradius# radtest tozeur hello 127.0.0.1 0 testing123
Sending Access-Request of id 249 to 127.0.0.1 port 1812
  User-Name = "tozeur"
  User-Password = "hello"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=249, length=20
root@debian:/etc/freeradius# █
```

Figure 20: la réponse Access-Accept

a. Configuration de la base de données

Dans un premier temps, on se connecte au serveur MySQL et on crée une nouvelle base de données qui va s'appeler « radius ». Ensuite on va ajouter un utilisateur et un client à la base de données, après avoir importé les différentes tables depuis les SQL que FREERADIUS propose.

- **Connexion au serveur MySQL et création de la base de donnée :**

On crée la base de données « radius » avec la commande **createdatabase radius;**

On passe ensuite à la création de l'utilisateur radius. On lui attribue tous les droits sur la base de données « radius ». Cet utilisateur est optionnel car je peux aussi utiliser root pour les échanges entre le serveur radius et la base de données.

- **Création de l'utilisateur radius et attribution des droits :**


```
mysql> create user 'radius'@'localhost' identified by 'passer';  
Query OK, 0 rows affected (0.00 sec)
```

Figure 21:creation de user radius

- **Importation des tables depuis le serveur freeRADIUS :**

Les fichiers de configuration du serveur freeRADIUS se trouvent dans le répertoire /etc/freeradius.

Ce répertoire contient un répertoire /etc/freeradius/sql/mysql qui contient à son tour tous les fichiers SQL que nous allons importer à savoir schema.sql et nas.sql. Nous allons, depuis la base de données, importer les deux fichiers qui vont créer automatiquement les tables dans notre base de données radius :

```
mysql> use radius;  
Database changed  
mysql> source /etc/freeradius/sql/mysql/schema.sql;
```

Figure 22:Creation de table radcheck

Une description des différentes tables :

La table nas : contient la liste des NAS, c'est-à-dire des clients RADIUS. Elle remplace le fichier traditionnel clients.conf

La table radacct :contient les informations qu'un NAS retourne en cas d'accounting

La table radcheck : permet de vérifier une option d'un utilisateur comme le mot de passe, par exemple, quand on utilise PEAP ou TTL

option de groupe

La table radgroupreply : permet de retourner une option de groupe

La table radpostauth : contient les informations sur chaque authentification réussie.

La table radreply : permet de retourner une option pour l'utilisateur.

La table usergroup : permet de faire la liaison entre le nom d'utilisateur et son groupe.

Quand on utilise freeRADIUS avec une base de données, la gestion des utilisateurs est un peu différente : chaque utilisateur est rattaché un groupe. Ce qui fait qu'il y a les options de groupe et les options pour l'utilisateur.

- **Ajout d'un utilisateur (ou compte utilisateur)**

Les utilisateurs doivent être ajoutés dans la table radcheck. Voici les différents champs à renseigner :

On ajoute deux nouveaux utilisateurs :

```
mysql> insert into radcheck (username,attribute,op,value) values ("nadhmi","cleartext-password","=", "passer");
Query OK, 1 row affected (0.01 sec)

mysql> insert into radcheck (username,attribute,op,value) values ("atef","cleartext-password","=", "passer");
Query OK, 1 row affected (0.01 sec)
```

Figure 23:Ajoute des utilisateurs

Il faut ensuite ajouter le type d'authentification que l'utilisateur va utiliser. Dans notre cas, c'est le type EAP-TLS

```
mysql> insert into radcheck (username,attribute,op,value) values ("nadhmi","Auth-Type",":=", "EAP-TLS");
Query OK, 1 row affected (0.00 sec)

mysql> insert into radcheck (username,attribute,op,value) values ("atef","Auth-Type",":=", "EAP-TLS");
Query OK, 1 row affected (0.01 sec)
```

Figure 24:mettre une authentification EAP

Ajout de NAS :

```
mysql> insert into nas (nasname,shortname,ports,secret) values ("192.168.1.254","SMC","1812","passer");
Query OK, 1 row affected (0.01 sec)
```

Figure 25:nasname

b. Configuration de fichier :

on se déplace dans le répertoire /etc/freeradius pour effectuer toutes les modifications nécessaires pour la prise en compte de notre base de données MySQL. Les fichiers à modifier sont :

- radiusd.conf
- sites-available/default
- sql.conf
- eap.conf

• Configuration de fichier radiused.conf :

Pour la configuration globale du serveur. Ce fichier est découpé en deux grandes parties, d'abord les paramètres propres au démon (interfaces d'écoute, port, etc.), puis une partie définition des modules (définition et configuration des modules d'authentification disponibles hormis ceux du type EAP qui sont traités séparément, des modules de journalisation, de relayage des requêtes, etc.).

```
listen {
type = auth
ipaddr = *
port = 0

}
listen {
ipaddr = *
port = 0
type = acct
}
#$INCLUDE clients.conf
$INCLUDE ${confdir}/modules/
$INCLUDE eap.conf
$INCLUDE sql.conf
$INCLUDE sql/mysql/counter.conf
$INCLUDE sites-enabled/
```

✓ Configuration de fichier sites/available-default :

Le fichier fourni par défaut l'activer par les commandes suivants :

```
authorize {

preprocess
```

```
eap {  
    ok = return  
    sql  
    authenticate {  
        Auth-Type CHAP {  
            chap  
        }  
    }  
    eap  
    session {  
        sql  
    }  
}
```

✓ **Configuration de fichier sql.conf :**

Nous allons ouvrir et modifier le fichier **/etc/freeradius/sql.conf** par la commande suivante :

```
#gedit sql.conf
```

Le fichier s'ouvre, je vais vérifier tous ces lignes :

```
Sql {  
    database = "mysql"  
    driver = "rlm_sql_${database}"  
    server = "localhost"  
    login = "radius"  
    password = "motdepasse_sql"
```

```
radius_db = "radius"  
acct_table1 = "radacct"  
acct_table2 = "radacct"
```

```
postauth_table = "radpostauth"
authcheck_table = "radcheck"
authreply_table = "radreply"
groupcheck_table = "radgroupcheck"
groupreply_table = "radgroupreply"
usergroup_table = "radusergroup"
deletestalesessions = yes
sqltrace = no
sqltracefile = ${logdir}/sqltrace.sql
num_sql_socks = 5
    connect_failure_retry_delay = 60
readclients = yes
nas_table = "nas"
$INCLUDE sql/${database}/dialup.conf
}
```

✓ Configuration de fichier eap.conf :

Pour la configuration des méthodes EAP d'authentification. Le contenu de ce fichier était au départ inclus dans la partie module du fichier « radiusd.conf » mais les développeurs ont préféré le séparer pour des raisons de lisibilité car il devenait de plus en plus volumineux du fait du nombre de méthodes d'authentification EAP différentes. En fonction des méthodes EAP que le serveur devra supporter dans son environnement de production il y aura éventuellement certains paramètres à configurer. Par exemple dans le cas d'une authentification via EAP-TLS, il faudra indiquer le répertoire contenant le certificat du serveur (qu'il enverra au supplicant) et la clé privée avec le mot de passe associé, celui contenant le certificat de l'autorité (qui permettra de vérifier le certificat fourni par le supplicant), indiquer si le serveur doit vérifier un fichier contenant les certificats révoqués ou encore s'il faut vérifier que le nom de l'utilisateur correspond au nom du propriétaire du certificat fourni.

Le fichier eap.conf :

Nous allons ouvrir le fichier /etc/freeradius/eap.conf avec la commande :

```
gediteap.conf
```

Nous spécifions que l'on veut utiliser EAP-TLS et non MD5 et on trouve dans la ligne 22 :

```
default_eap_type = tls
```

Après on configure EAP-TLS, il faut que l'on enlève les commentaires (les # devant) à partir de la ligne 122 et on modifie les chemins des certificats

```
eap {  
  
    default_eap_type = tls  
  
    timer_expire = 60  
  
    cisco_accounting_username_bug = no  
  
    tls {  
  
        certdir = ${confdir}/certs  
  
        cadir = ${confdir}/certs  
  
        private_key_password = passer  
  
        private_key_file = ${certdir}/server@galorius.tn-key.pem  
  
        certificate_file = ${certdir}/server@galorius.tn-cert.pem  
  
        CA_file = ${cadir}/TEST-FREERADIUS-cacert.pem  
  
        dh_file = ${certdir}/dh  
  
        random_file = ${certdir}/random  
  
        CA_path = ${cadir}
```

```
cipher_list = "DEFAULT"
```

```
}
```

```
}
```

3.creation de certificats :

4. Test de fonctionnement :

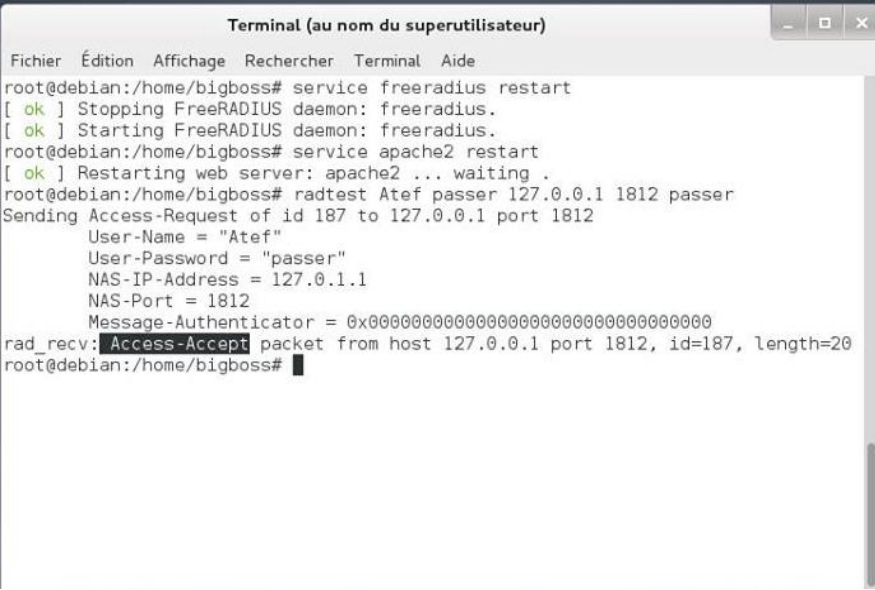
Dans cet étape on va faire un test interne de FreeRadius a l'aide de NTRadPing.

On attribue au serveur Debian l'adresse IP 192.168.2.150 et pour la machine 192.168.2.11

On utilise une carte de bouclage pour la machine client, désactiver le pare-feu et faire un ping entre le serveur et la machine et vice-versa



Figure 26:Test NTRadPing



```

Terminal (au nom du superutilisateur)
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@debian:/home/bigboss# service freeradius restart
[ ok ] Stopping FreeRADIUS daemon: freeradius.
[ ok ] Starting FreeRADIUS daemon: freeradius.
root@debian:/home/bigboss# service apache2 restart
[ ok ] Restarting web server: apache2 ... waiting .
root@debian:/home/bigboss# radtest Atef passer 127.0.0.1 1812 passer
Sending Access-Request of id 187 to 127.0.0.1 port 1812
    User-Name = "Atef"
    User-Password = "passer"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 1812
    Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=187, length=20
root@debian:/home/bigboss#

```

Figure 27:test surDebian

Le « Access-Accept » qu'on a à la fin ici montre que notre serveur écoute bien sur son adresse IP : il fonctionne aussi bien en local que sur son adresse Ethernet.

5. Configuration de point d'accès et configuration de connexion de SMC:

a.Configuration du point d'accès :

Le point d'accès doit être connecté au serveur FreeRADIUS via un câble Ethernet. On se connecte à son interface graphique en tapant dans la barre du navigateur 192.168.2.1 (adresse du point d'accès) et on a l'interface suivante:



Figure 28:interface de point d'accès

Après on fixe l'adresse IP de serveur radius 192.168.2.150 et la mode de sécurité WPA2 avec l'algorithme de cryptage AES

SMC Networks SMCWEBS-N

Setup Wizard Operation Mode Network Settings **Wireless Settings** Administration

Wireless Security and Encryption Settings
The Wireless Security and Encryption Settings page allows you to make detailed security configurations to prevent unauthorized access and monitoring.

Select SSID
SSID Choice SMC ▼

"SMC"
Security Mode WPA2 ▼

WPA
WPA Algorithms ☐ TKIP ☒ AES ☐ TKIPAES
Key Renewal Interval 3600 seconds
PMK Cache Period 10 minute
Pre-Authentication ☒ Disable ☐ Enable

Radius Server
IP Address 192.168.2.150
Port 1812
Shared Secret
8~63 ASCII or 64 Hexadecimal
Session Timeout 0

Copyright © 2010 SMC Inc. All Rights Reserved

Figure 29:configuration de SMC

Après chaque modification on clique sur « save » et on redémarre le point d'accès pour qu'il prenne en compte les modifications. Pour redémarrer, on va dans « System Tools » puis « Reboot » et je clique ensuite sur le bouton « Reboot »

On ajoute dans la table « radcheck » de la base de données radius un utilisateur « FREERADIUS-CLIENT » qui est l'utilisateur à qui est destiné le certificat du client :

```
mysql> insert into radcheck (username,attribute,op,value)
-> values ("FREERADIUS-CLIENT","Cleartext-Password",":=", "passer");
Query OK, 1 row affected (0.04 sec)

mysql> insert into radcheck (username,attribute,op,value)
-> values ("FREERADIUS-CLIENT","Auth-Type",":=", "EAP");
Query OK, 1 row affected (0.04 sec)

mysql> insert into radcheck (username,attribute,op,value)
-> values ("FREERADIUS-CLIENT","EAP-Type",":=", "EAP-TLS");
Query OK, 1 row affected (0.01 sec)
```

Figure 30:unutilisateurfreeradius

b. connexion au réseau sans fil :

sur la machine client windows 7 on accede au CMD on tape la commande suivant **certmgr.msc** pour acceder au gestionnaire de certificat

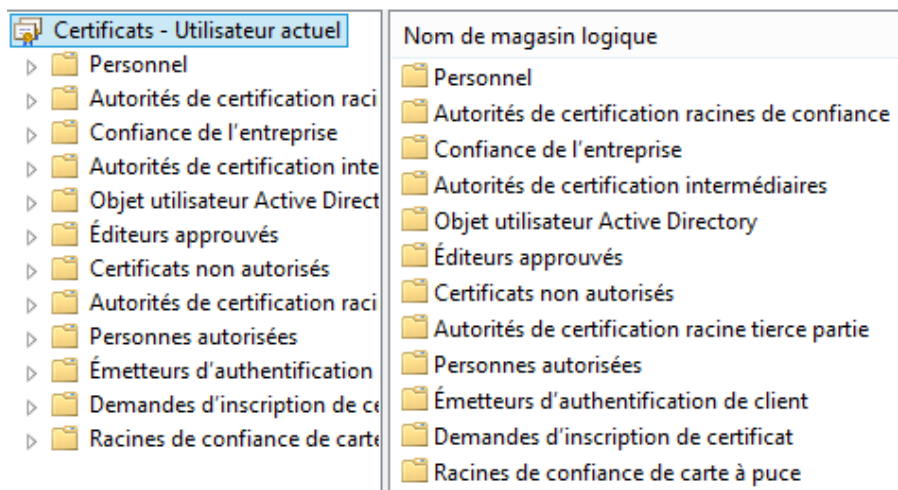


Figure 31:gestionnaire de certificat

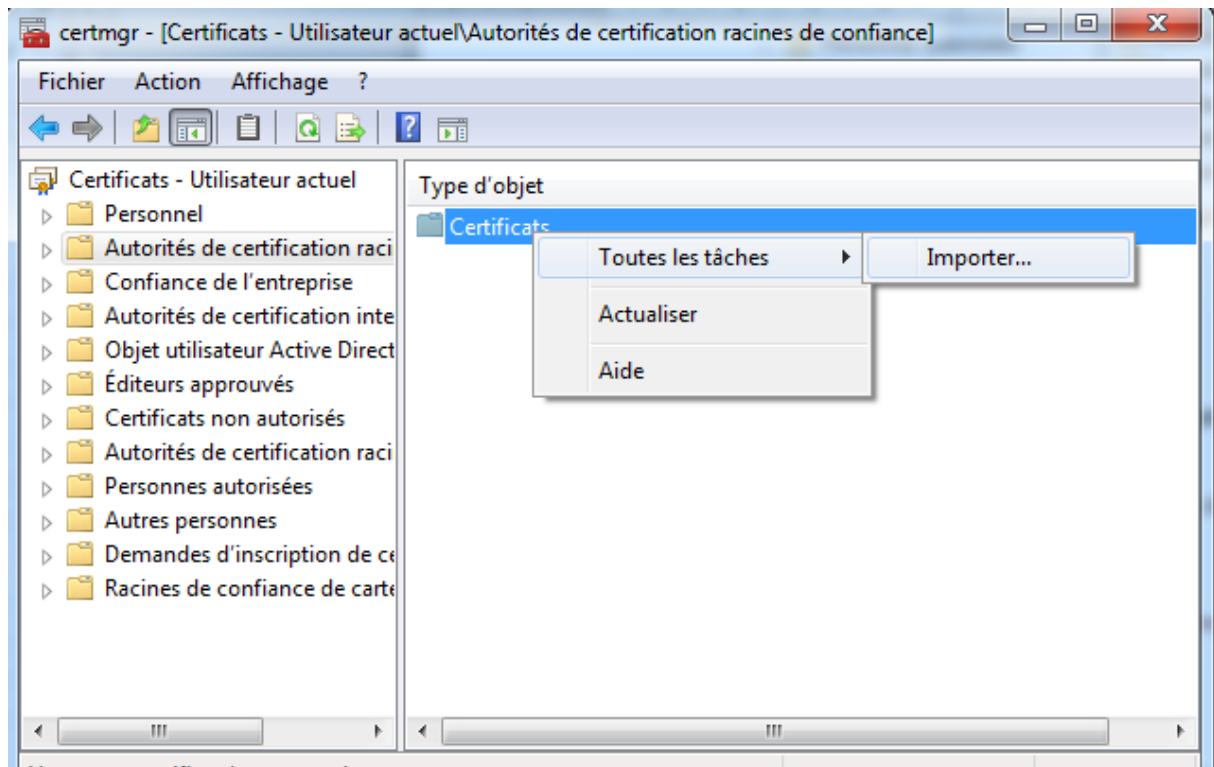


Figure 32:importer de certificat

Puis on installe le certificat de client

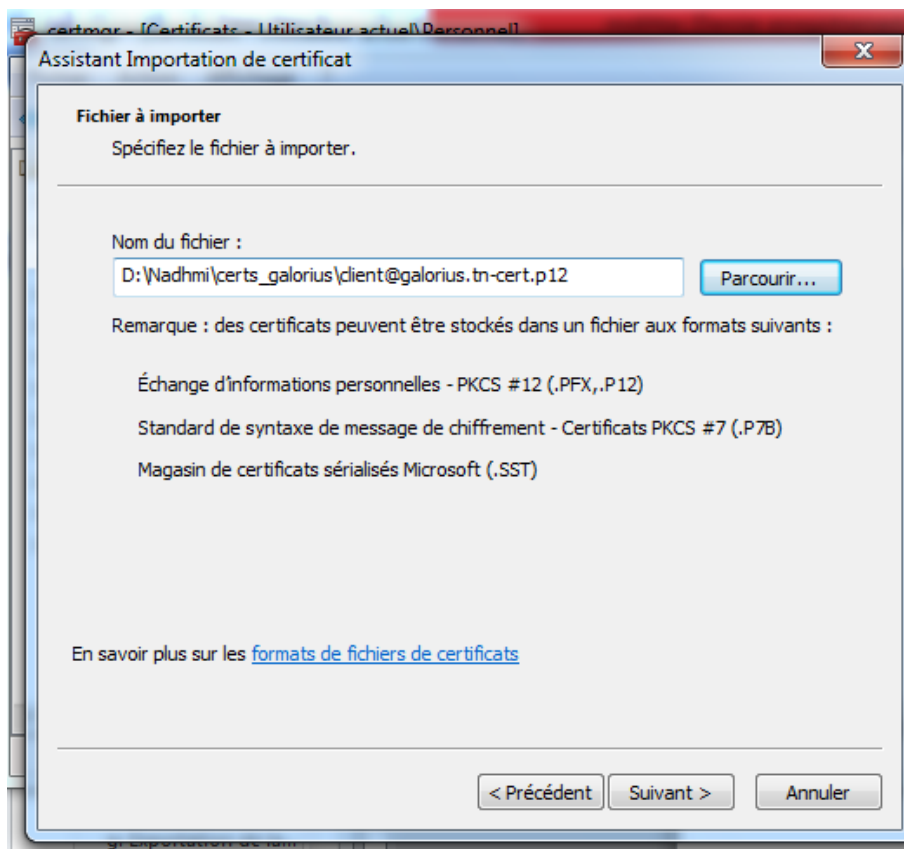


Figure 33:installation certificat client

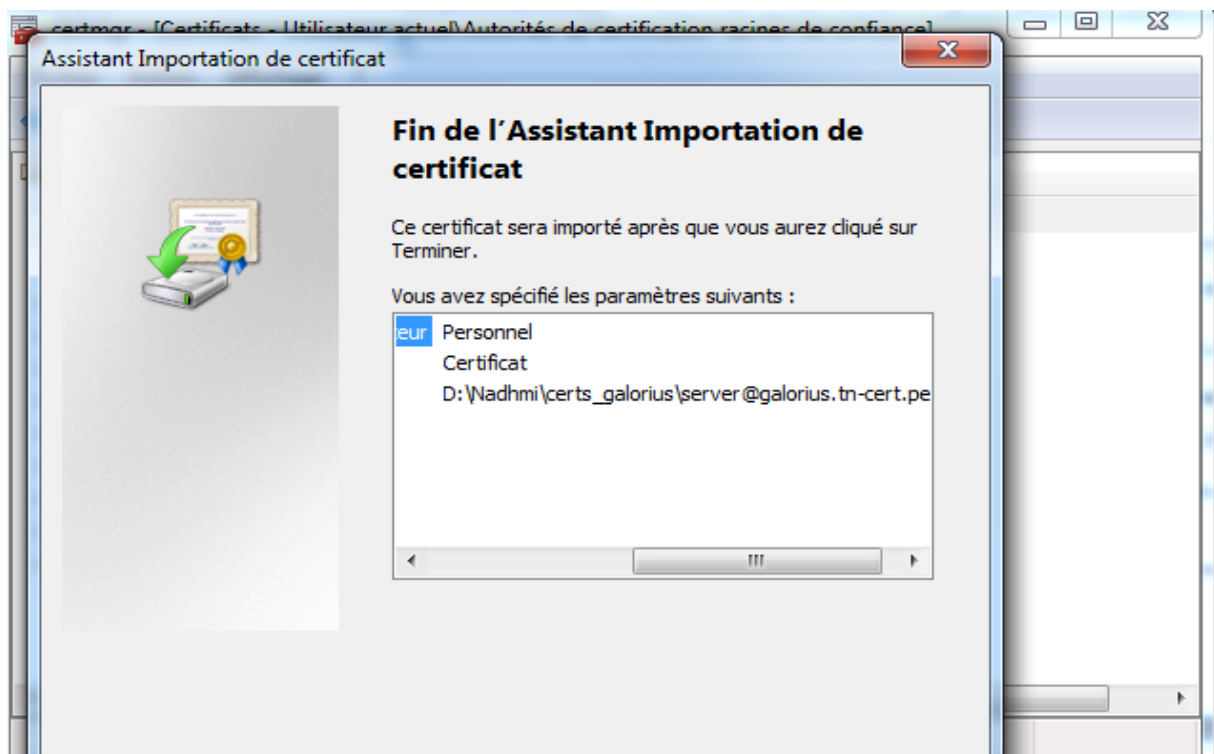


Figure 34:certificat importé

➤ **Installation du certificat du serveur**

Même procédure pour installer le certificat de serveur

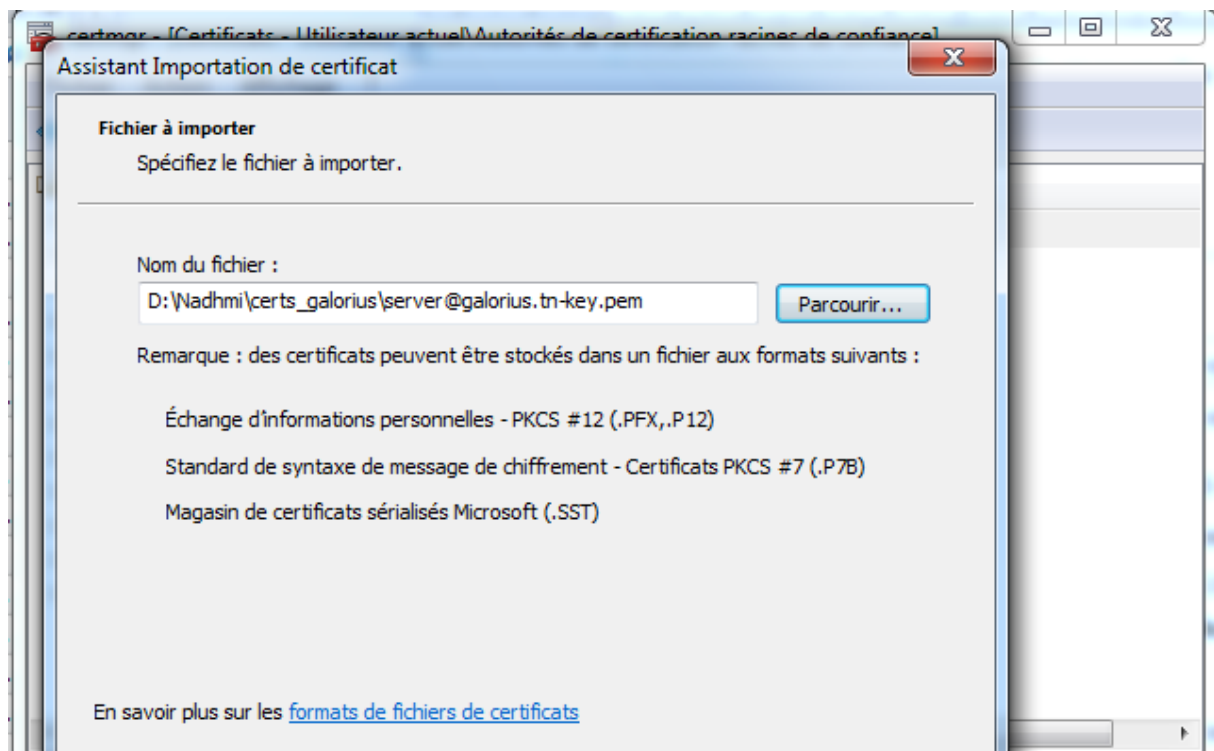


Figure 35:installation de certificat de serveur

Protection de clé privée

Pour maintenir la sécurité, la clé privée a été protégée avec un mot de passe.

Tapez le mot de passe pour la clé privée.

Mot de passe :

•••••

☐ Afficher le mot de passe

Options d'importation :

- ☐ Activer la protection renforcée de clé privée. Une confirmation vous est demandée à chaque utilisation de la clé privée par une application, si vous activez cette option.
- ☐ Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement.
- ☒ Indure toutes les propriétés étendues.

Figure 36:protection clé privé

➤ **Connexion au réseau sans fil SMC**

Tous nos certificats étant installés, passons maintenant à la connexion au Wifi proprement dit. Pour cela, nous devons configurer le réseau sans fil manuellement en ajoutant les certificats pour qu'ils soient pris en compte :

Paramètres => Panneau de configuration => Réseau et Internet => Centre Réseau et Partage => Configurer une nouvelle connexion ou un nouveau réseau :

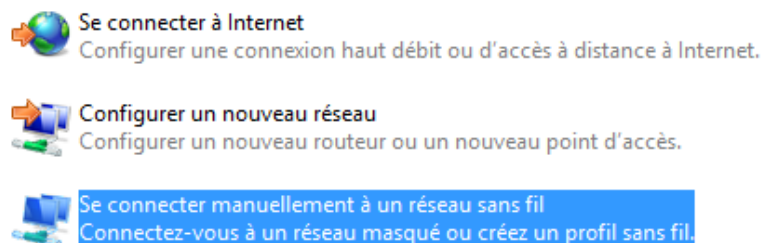


Figure 37:connexion au réseau sans fil

SSID : smc
Type de réseau : Point d'accès
Disponibilité du réseau : Tous les utilisateurs

☒ Me connecter automatiquement lorsque ce réseau est à portée

☐ Rechercher d'autres réseaux sans fil tout en étant connecté à réseau

☐ Me connecter même si le réseau ne diffuse pas son nom (SSID)

Figure 38:les paramètre de connexion

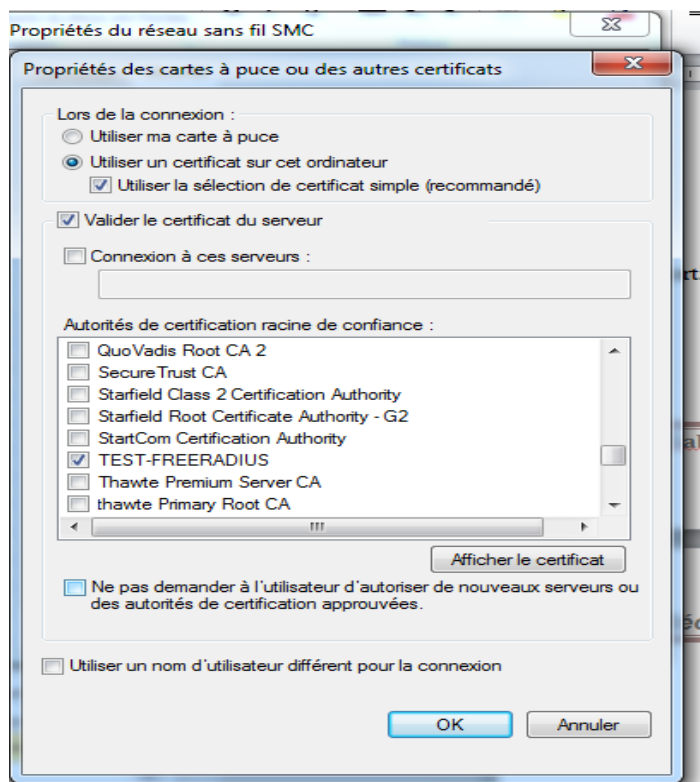


Figure 39:choisi le méthode d'authentification

PFSENSE

1. Installation de PfSense :

Lors du démarrage de l'ordinateur avec le CD ou l'ISO monté, un menu de boot apparaît. Selon les besoins on peut choisir de démarrer Pfsense avec certaines options activées. Si aucune touche n'est appuyée, Pfsense bootera avec les options par défauts (choix 1) au bout de 8 secondes.

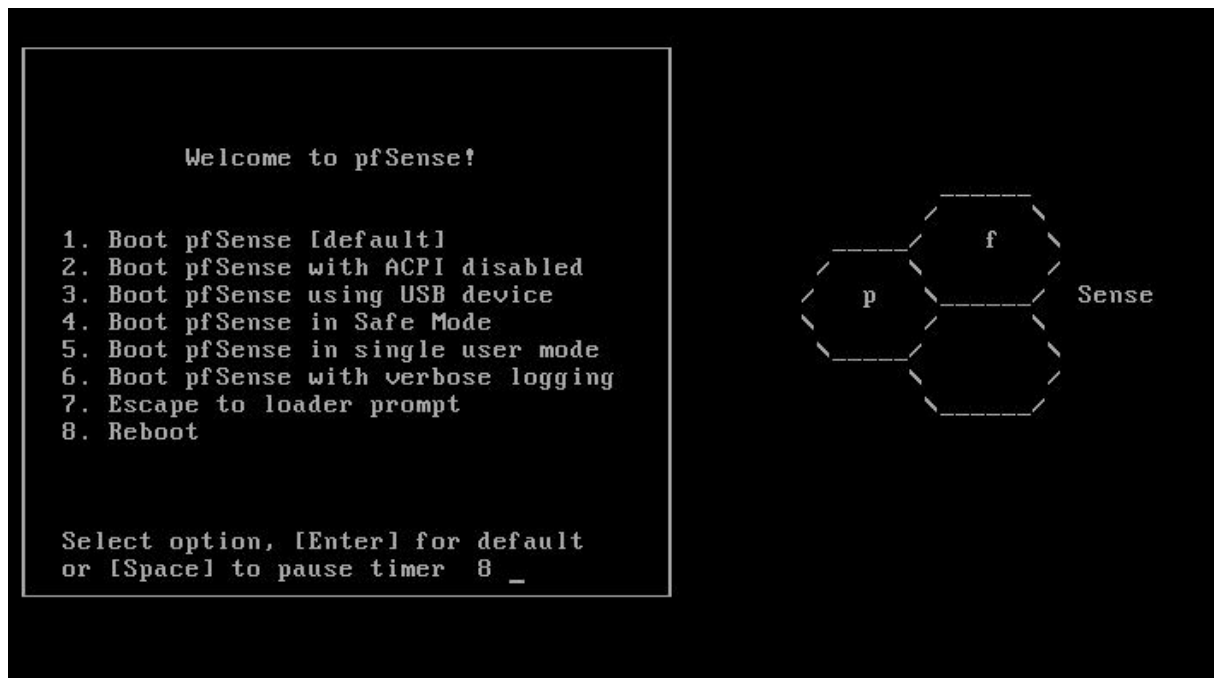
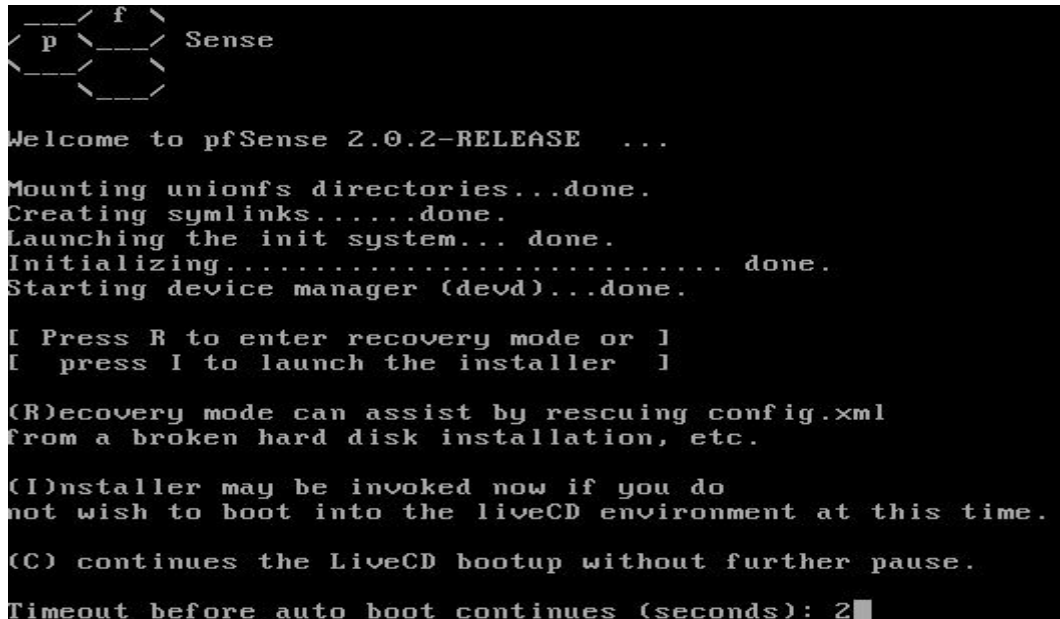


Figure 40:booter le pfSense

Appuyez sur « **Entrée** » pour booter avec les options par défaut.



```

Welcome to pfSense 2.0.2-RELEASE ...

Mounting unionfs directories...done.
Creating symlinks.....done.
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...done.

[ Press R to enter recovery mode or ]
[ press I to launch the installer ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

(I)nstaller may be invoked now if you do
not wish to boot into the liveCD environment at this time.

(C)ontinues the LiveCD bootup without further pause.

Timeout before auto boot continues (seconds): 2
```

Figure 41:etape2 d'installation

Appuyer rapidement sur la touche « **I** » afin de démarrer l'installation.

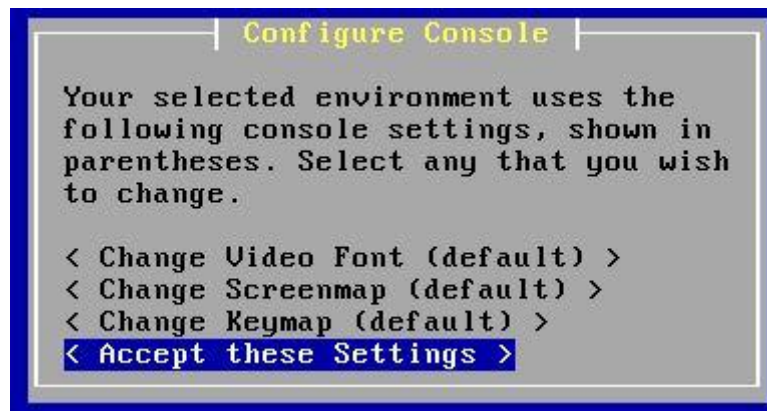


Figure 42:configuration console

On choisit « **Quick/Easy Install** » pour procéder à l'installation rapide.

Le message qui suit, nous informe que le disque dur sera formaté et toutes les données présentes dessus seront effacées. On sélectionne « **OK** » et on continue.

L'installation débute et copie les fichiers nécessaires sur le disque dur, nous devons par la suite choisir quel type de kernel nous voulons installer, étant sur un ordinateur nous choisissons le « **Standard Kernel** ».

Une fois l'installation finie, on choisit « **Reboot** » et nous redémarrons sur notre nouvelle installation.

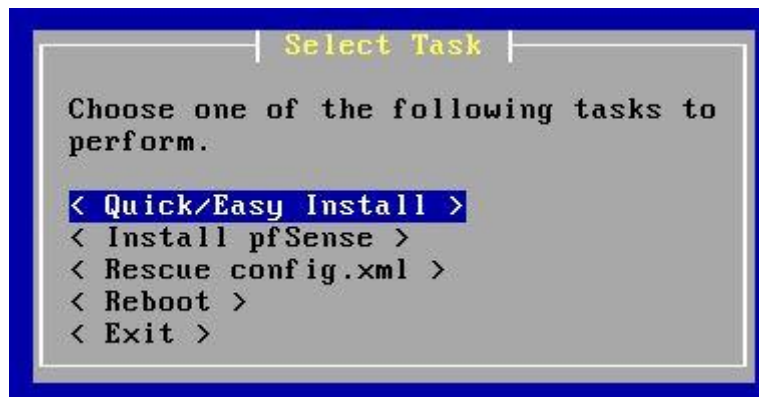


Figure 43:installation rapide

2. Configuration de PfSense :

Lors du premier démarrage de PfSense, il faut configurer les différentes interfaces (WAN, LAN, DMZ, etc..).

```
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3-RELEASE i386 Mon Apr 11 18:12:06 CDT 2016
Bootup complete

FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3-RELEASE-pfSense (i386) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 10.10.12.104/8
LAN (lan)      -> em1          -> v4: 192.168.2.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Figure 44:1eretapes de configuration

Puis on tape sur 2 pour configurer l'adresse IP on donne l'adresse 192.168.2.1 au réseau LAN

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.2.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
    255.255.0.0   = 16
    255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Figure 45:adressage De LAN

Après l'adressage, sur le navigateur de Google Chrome on attribue l'adresse IP 192.168.2.1 pour accéder a l'interface de PfSense.



Figure 46:Accédé a l'interface de pfSense

On configure le nom de domaine et on les adresse de DNS server

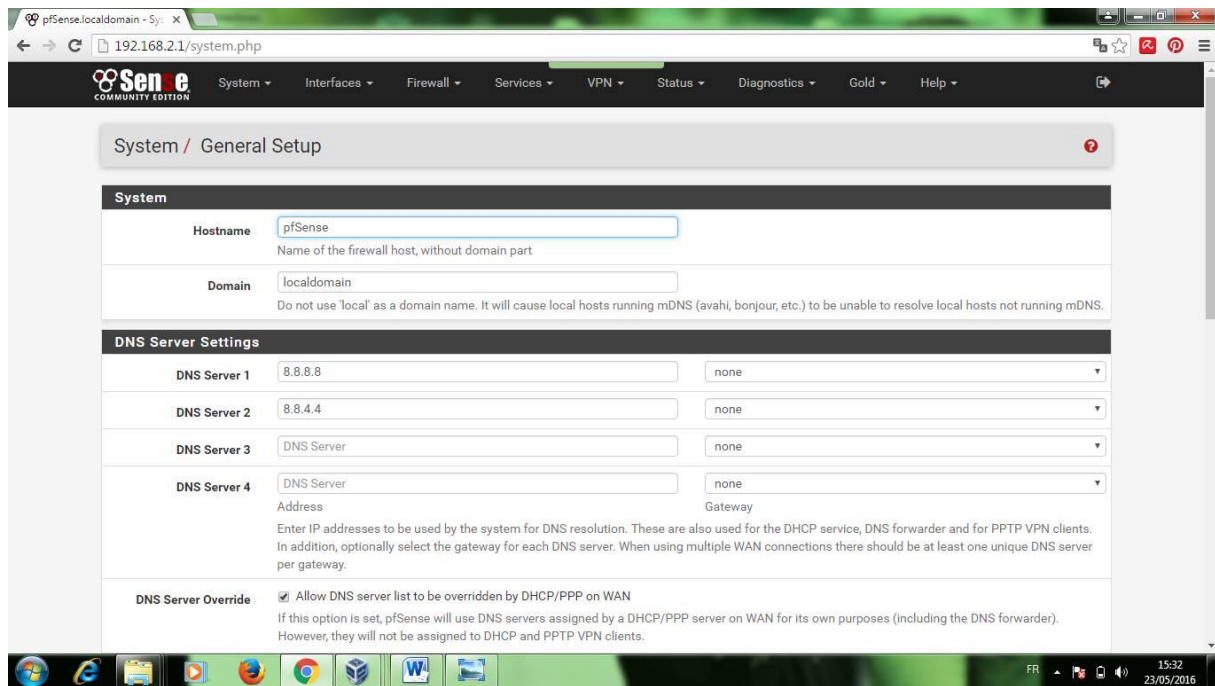


Figure 47:configuration de DNS server

a. Configuration DHCP :

Dans cette étape on va configurer un serveur DHCP sur pfSense qui va attribuer des adresses IP aux machines client qui se connecte à ce réseau local. On lui donne une plage entre 192.168.2.10 et 192.168.2.99

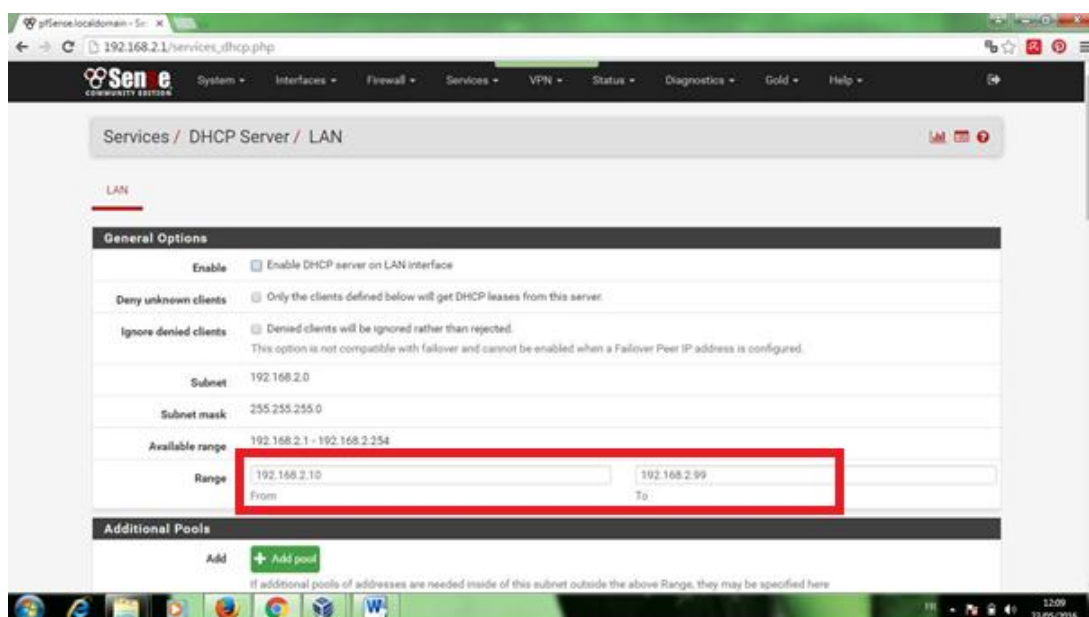


Figure 48:configuration de DHCP

b. Configuration de squid proxy server :

Dans une première étape on ajoute le service squid proxy server à travers de system> package Manager >installed Packages>Install squid

Après l'installation de service Squid on ajoute deux utilisateurs Atef et Nadhmi

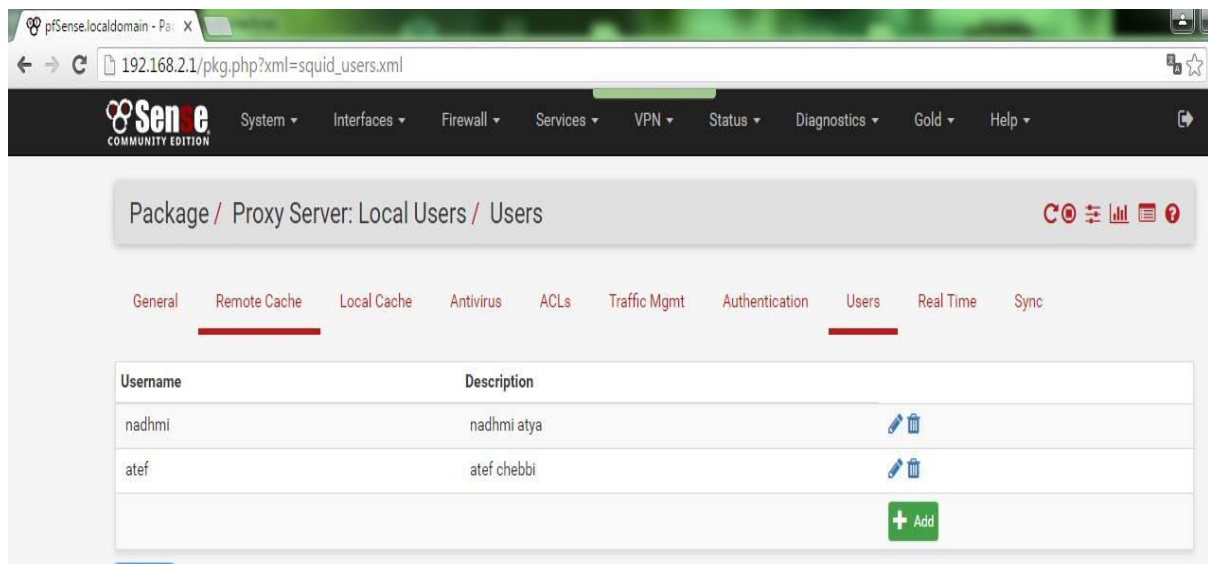


Figure 49:ajoute deux utilisateurs sur squid

Puis on attribue une authentification local pour que le machine client peut se connecte au service squid

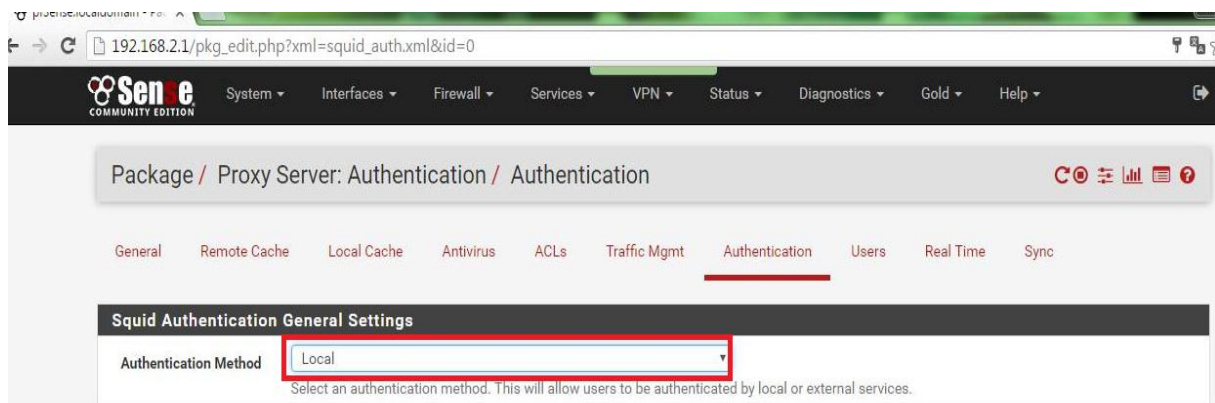
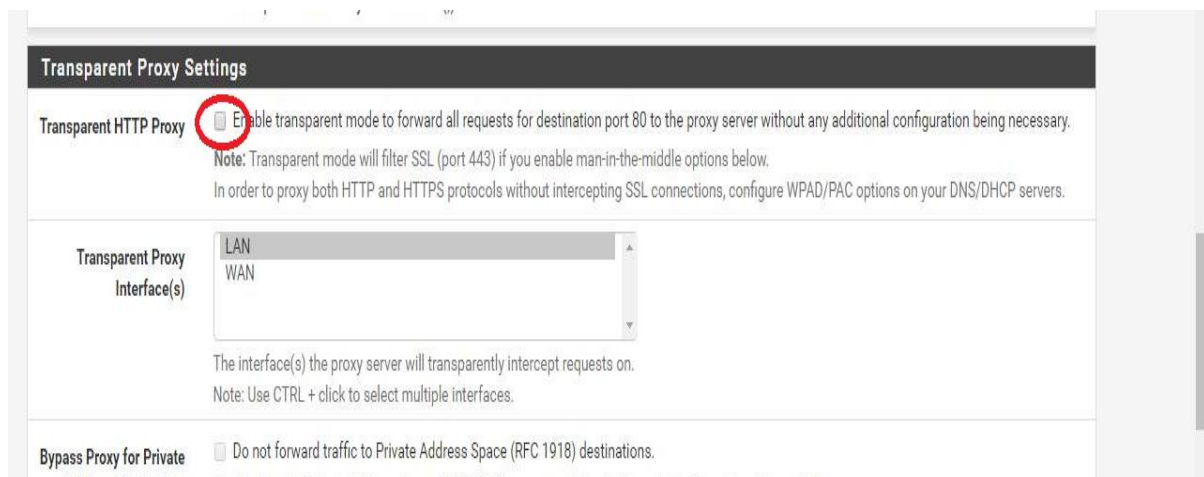


Figure 50:authentificationmethod

Pour que le service squid se marche bien il faut tout d'abord décocher Transparent http Proxy



FigdecocherEnable

c. Configuration de SquidGuard Proxy Filter :

Même principe que squid proxy on installe le service SquidGuard Proxy Filter.

Dans cette étapes on va configurer le Blacklist ceci qui permet de bloquer des sites Web précisé selon le choix d'administrateurs.

Sur le « General setting » on ajoute une Blacklist :



Fig :Blaclist

Puis on télécharger le lien de Blacklist

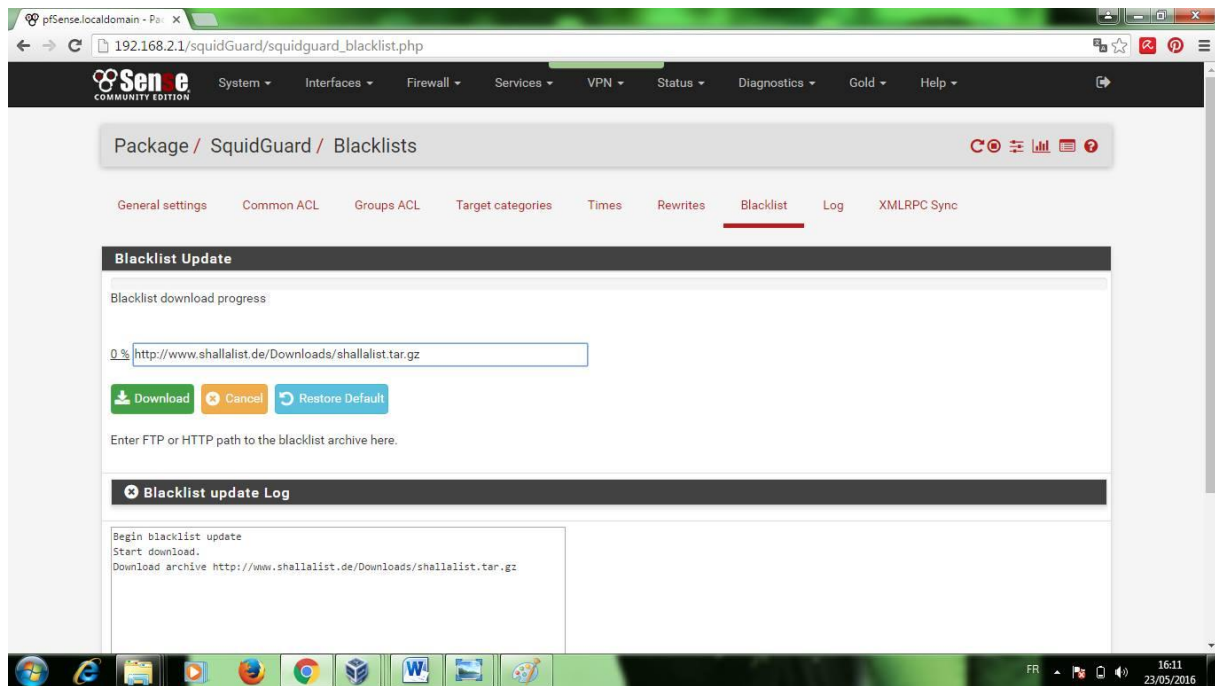


Fig : téléchargement de Blacklist

On accède au « Common ACL » pour choisir des listes de sites web qu'on va le bloquer à partir de Blacklist qu'on a téléchargé ,et dans cette exemple on a choisi les sites de chat et de piratage comme montre le figure suivant :

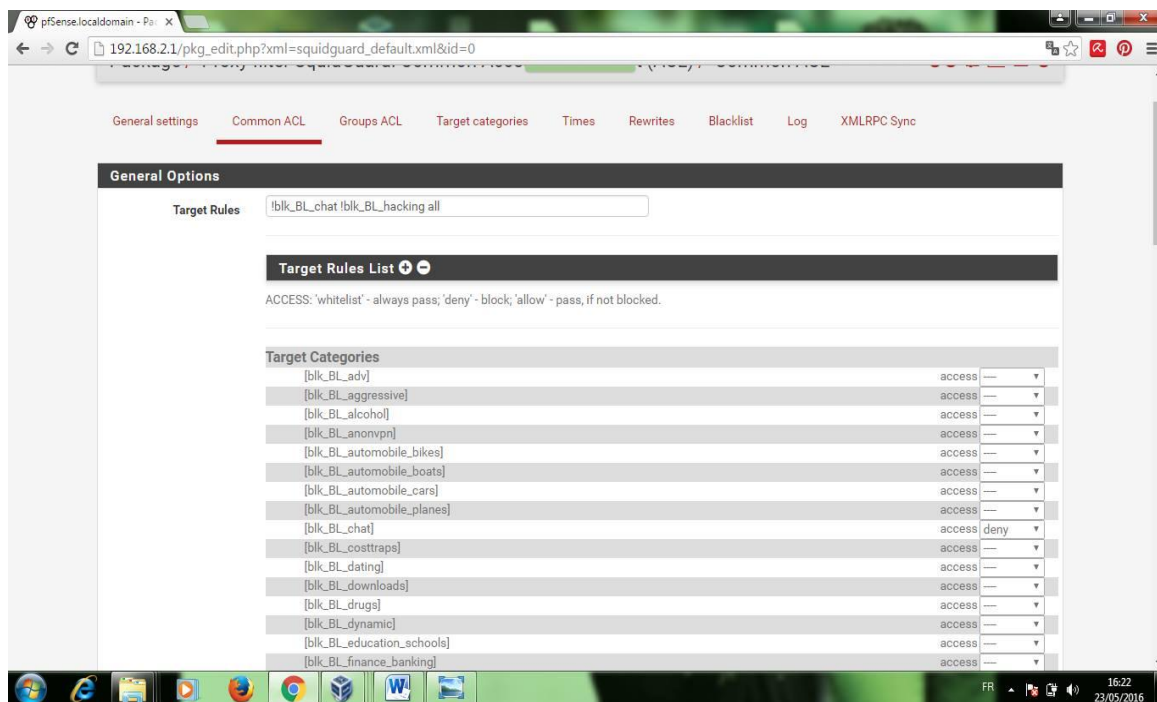


Fig :choisi de trajet catégories

d. Configuration Firewall

Dans cette étape on va configurer le firewall sur pfSense.

Sur « Alias » on va configurer le nom, le type et l'adresse qu'on va le bloqué

Dans cet exemple on a choisi de bloquer le site de Facebook comme montre le schéma suivant

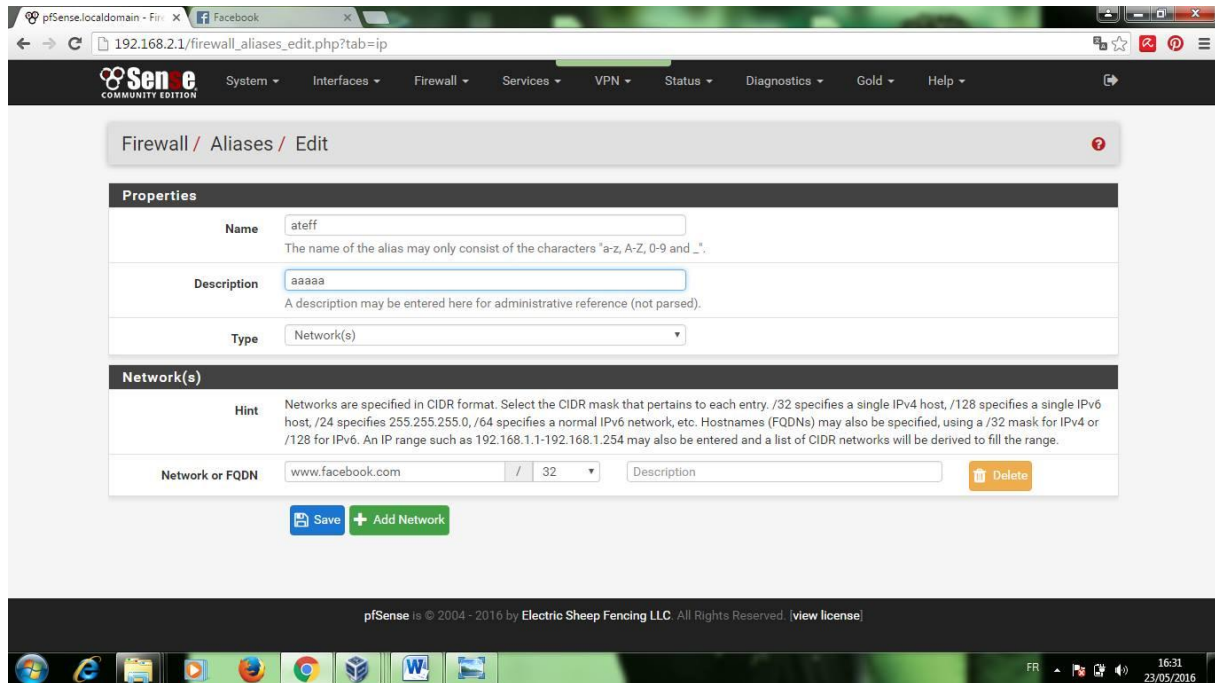


Figure 51:configuration de Alias

Sur firewall > Rules > LAN on ajoute nouveau rule avec la méthode blocage

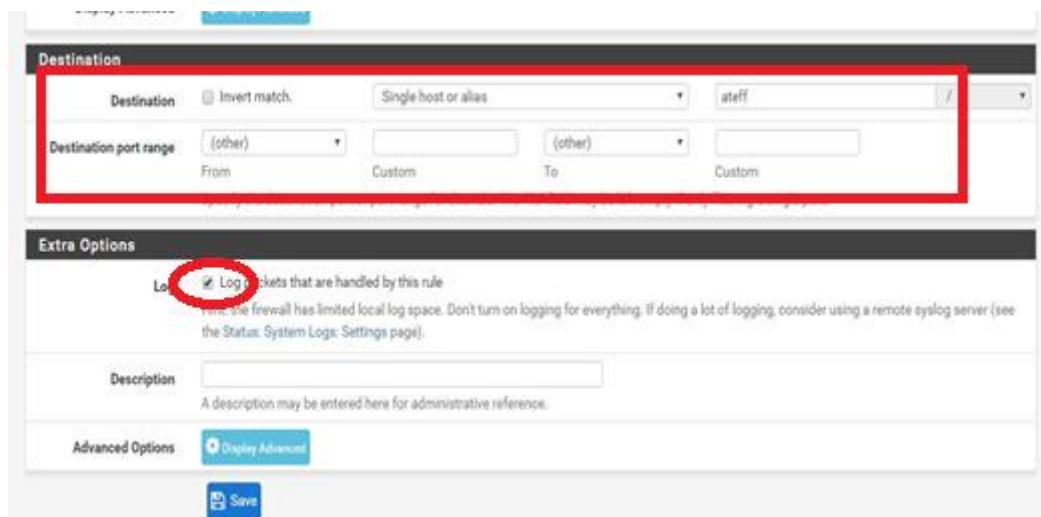


Figure 52:ajoute d'un rule

e. Configuration de Captive Portal :

La captive portale offre plusieurs services, et dans cette étape nous avons travaillé sur l'ajout des utilisateurs et de créations de la zone ainsi que le filtrage par adresse MAC.

Dans le System >users Managers on ajoute un « groupe_nadhmi »

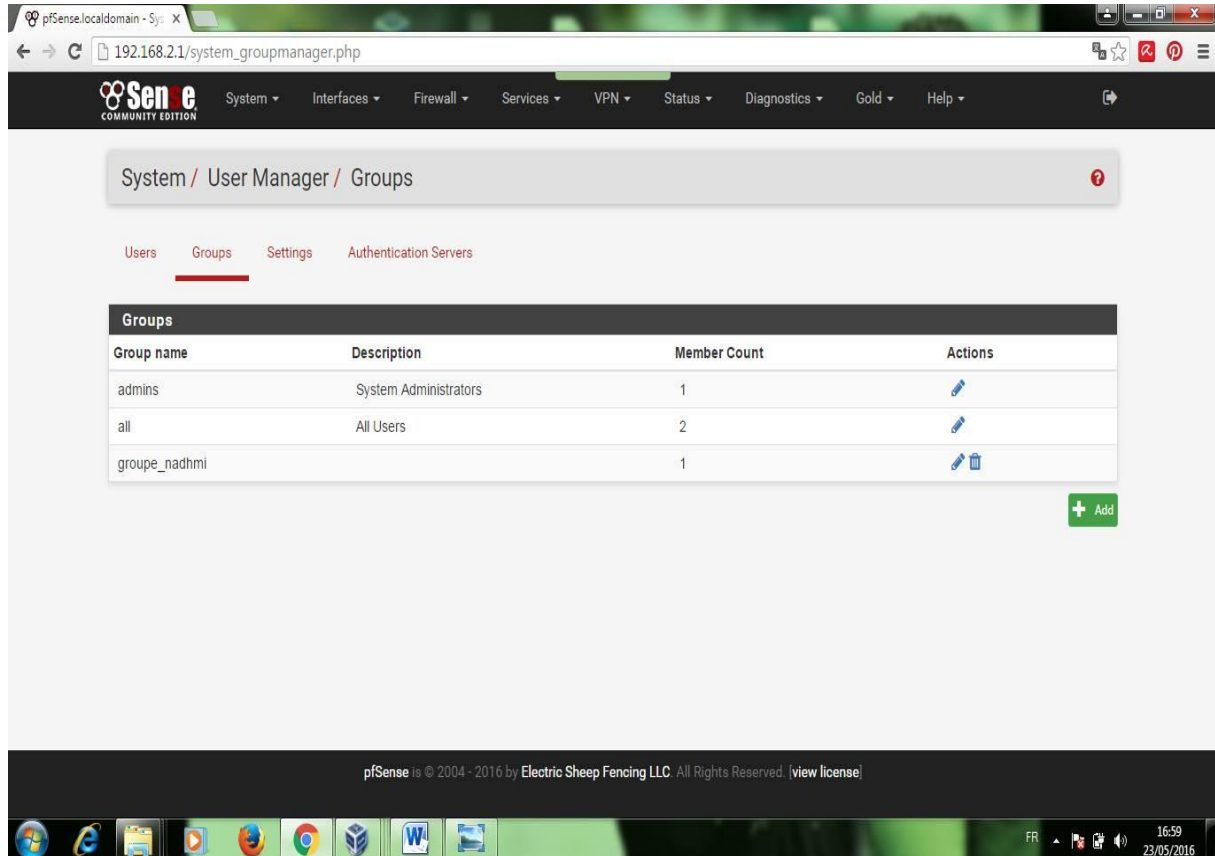


Figure 53:ajoute de groupe

Après l'ajout de groupe on ajoute un utilisateurs « atef » et on l'attribue son login et mot de passe

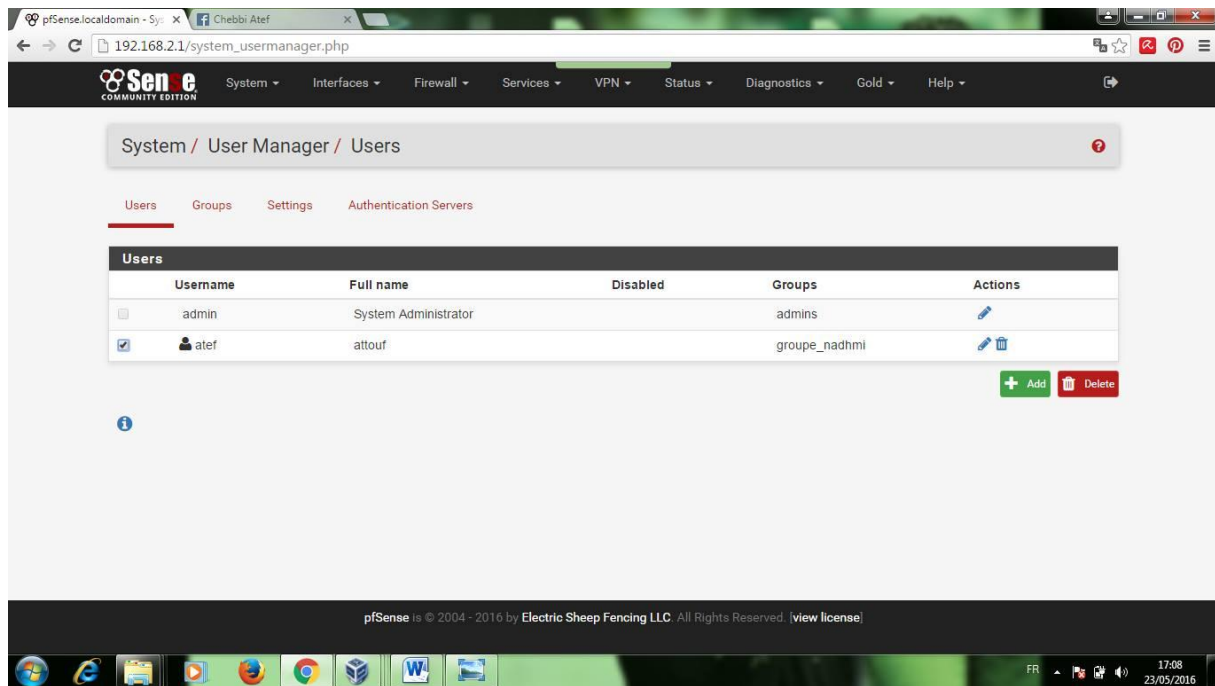


Figure 54:ajout utilisateurs

Après ces configuration on va filtrer l'accès par l'adresse MAC ,on va accéder au service portail captif puis au zone qu'on a créé récemment puis sur MAC on ajoute nouveau table et on le remplir comme le schéma indiqué suivant :

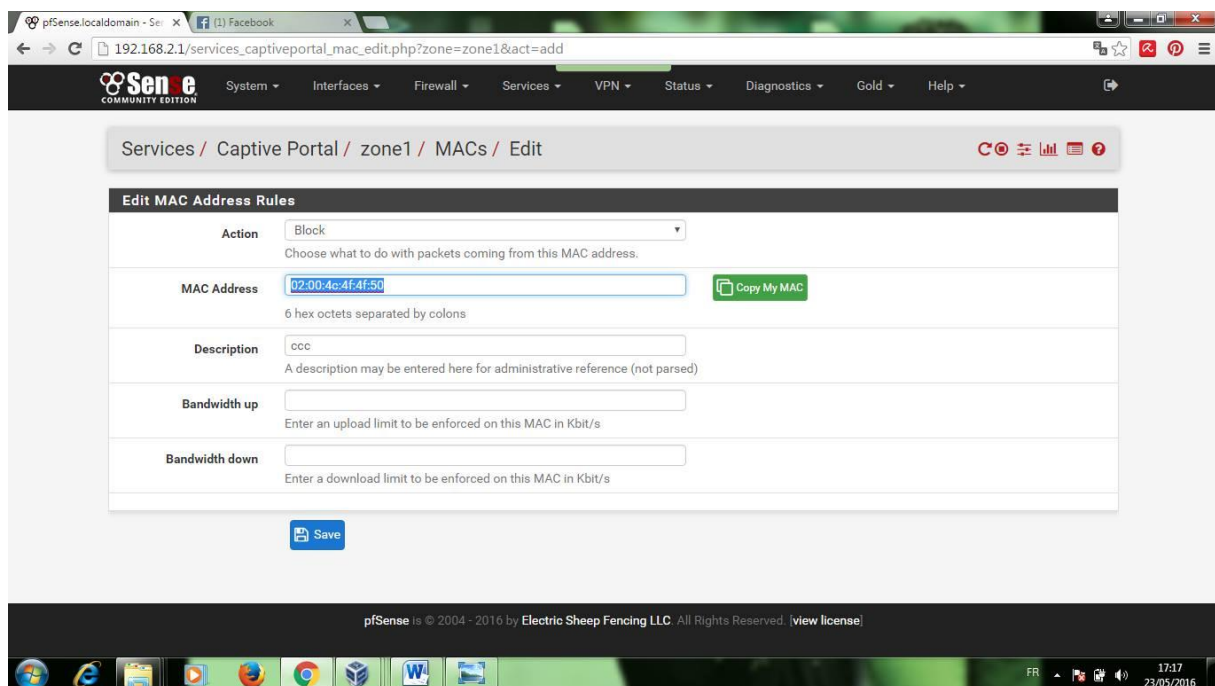
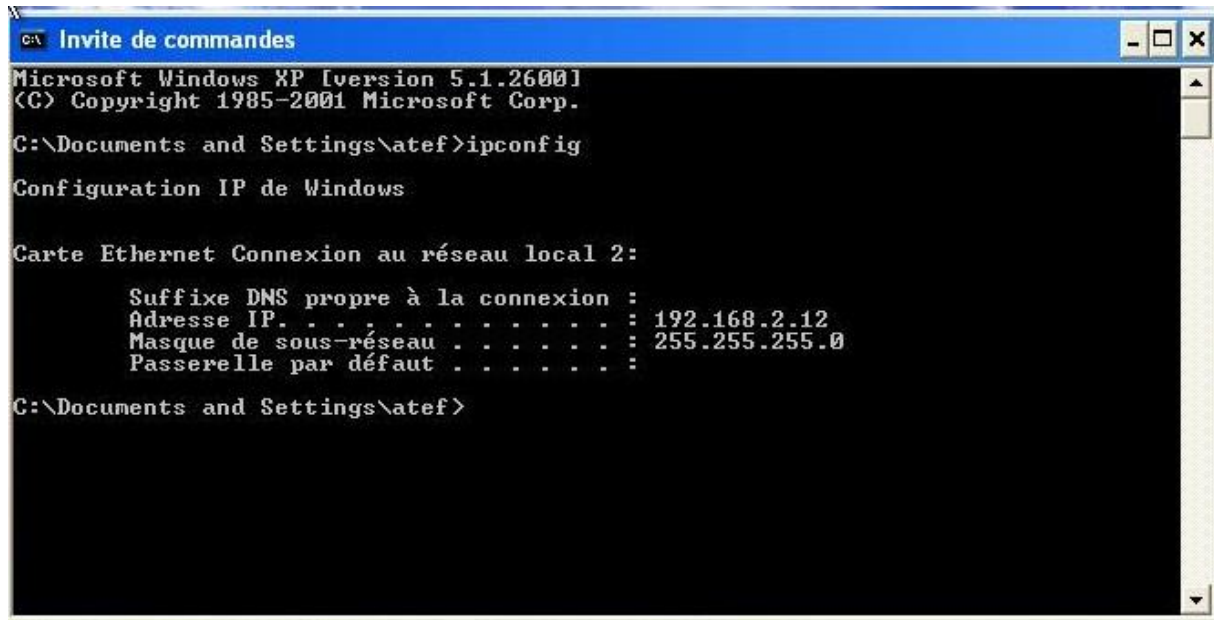


Figure 55:filtrage d'adresse Mac

3.Test de fonctionnement :

a. DHCP

sur la machine Client Windows XP on accède au menu démarrer puis CMD on tape la commande « ipconfig » on remarque que le serveur DHCP de pfSense a lui attribuer l'adresse IP suivant 192.168.2.12 sa ce qui valide que le serveur DHCP se fonctionne correctement .



```
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\atef>ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au réseau local 2:
    Suffixe DNS propre à la connexion :
    Adresse IP. . . . . : 192.168.2.12
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . :

C:\Documents and Settings\atef>
```

Figure 56:test DHCP

b.Test squid proxy server :

Sur le paramètre de navigateur de la machine client Windows XP on change la méthode d'accès internet en proxy et en lui attribue l'adresse IP se de serveur pfSense 192.168.2.1 avec le port 3128 puis on aller la barre de rechercher on tape l'adresse Google et remarque que le navigateur affiche un fenêtre demandant un login et un mot de passe .

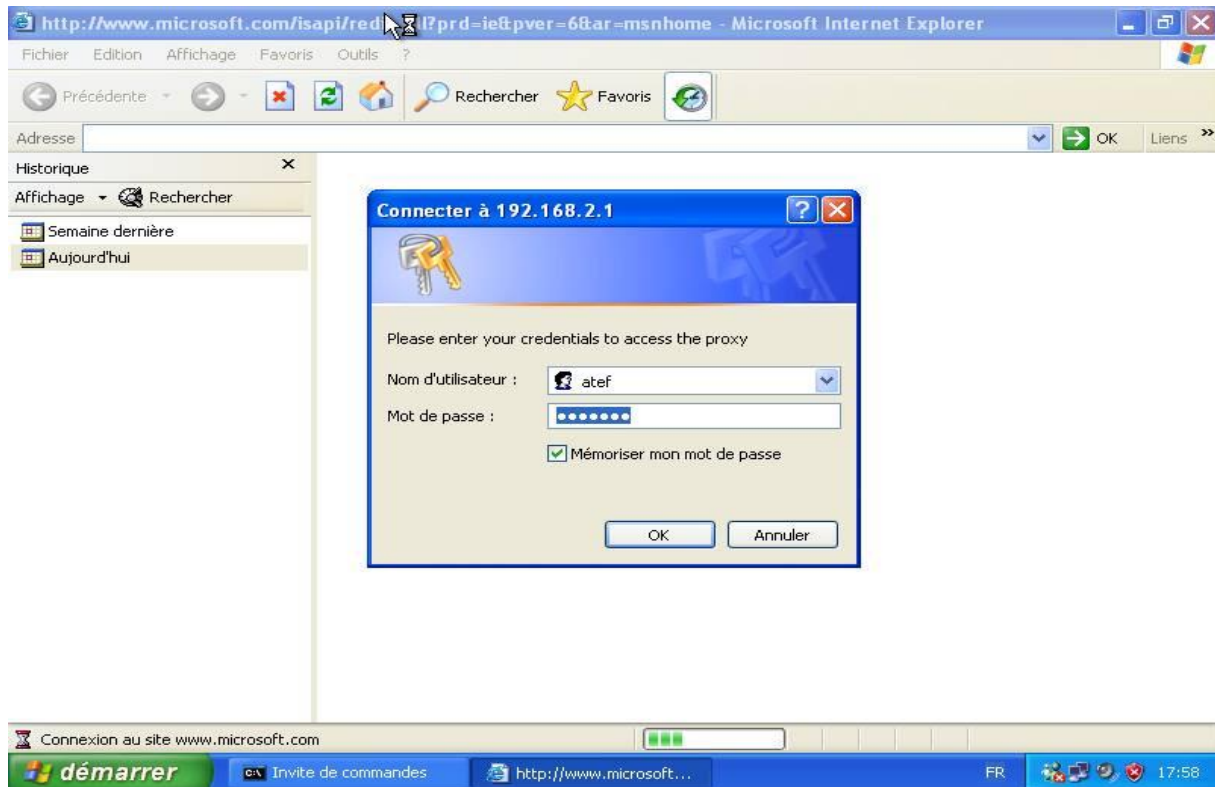


Figure 57: test proxy

c. TestSquidGuard proxy filter :

sur le navigateur de la machine client on accède aux sites web de chat, le navigateur nous répond pas le message suivant :

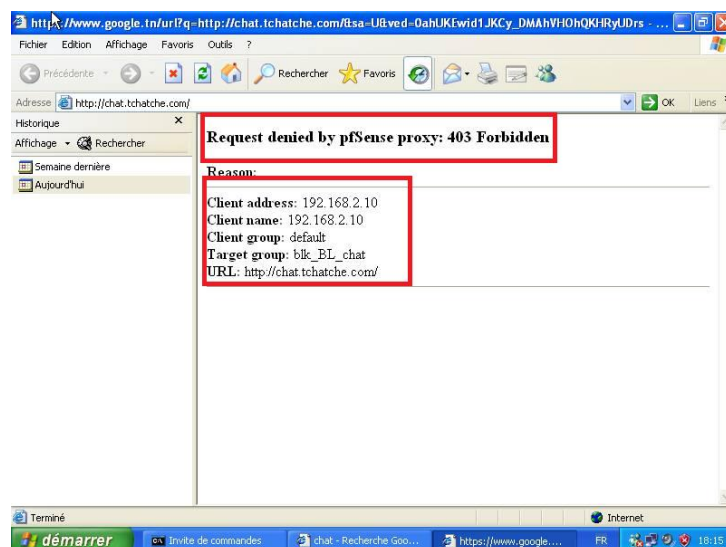


Figure 58: test de blacklist

d. Test Firewall & Portal captive :

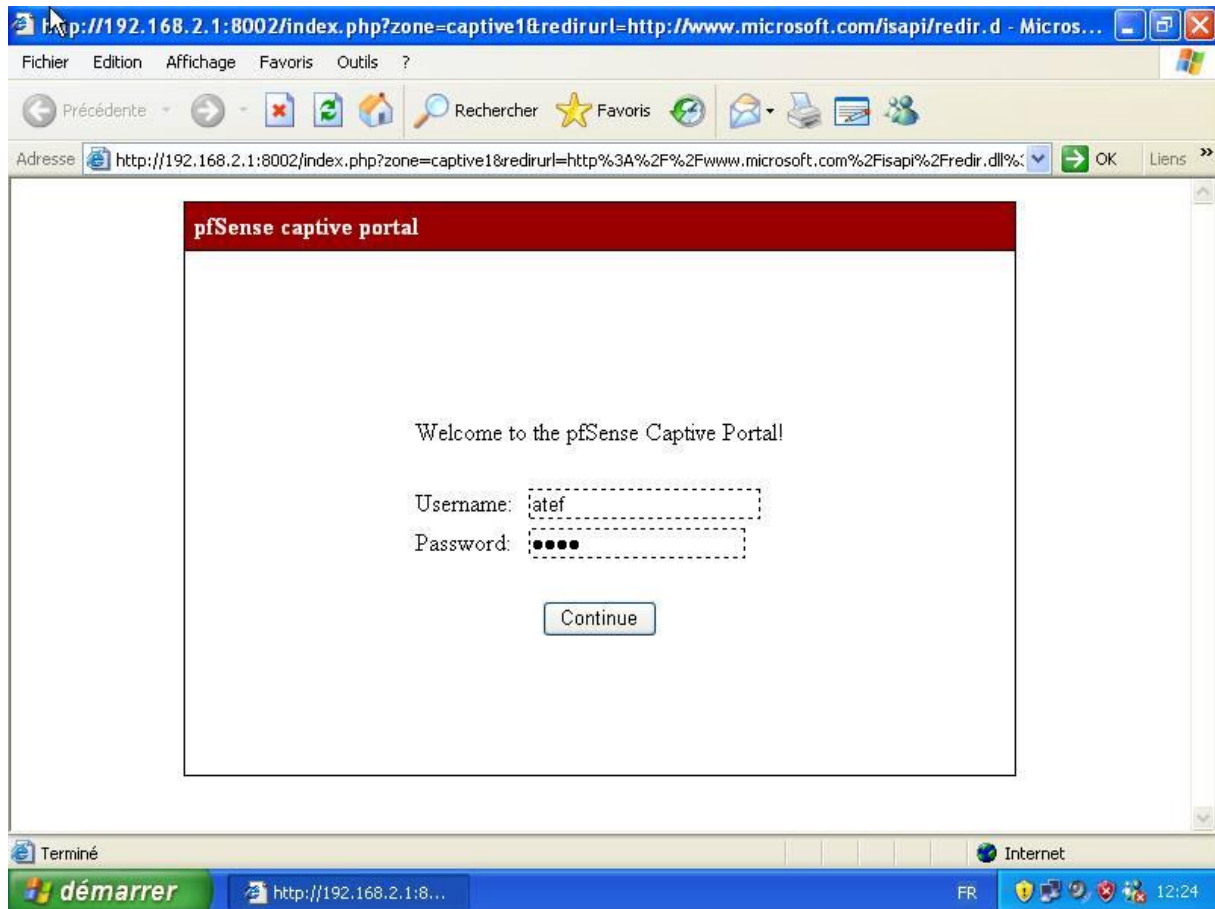


Figure 59:intrface portal captive sur XP

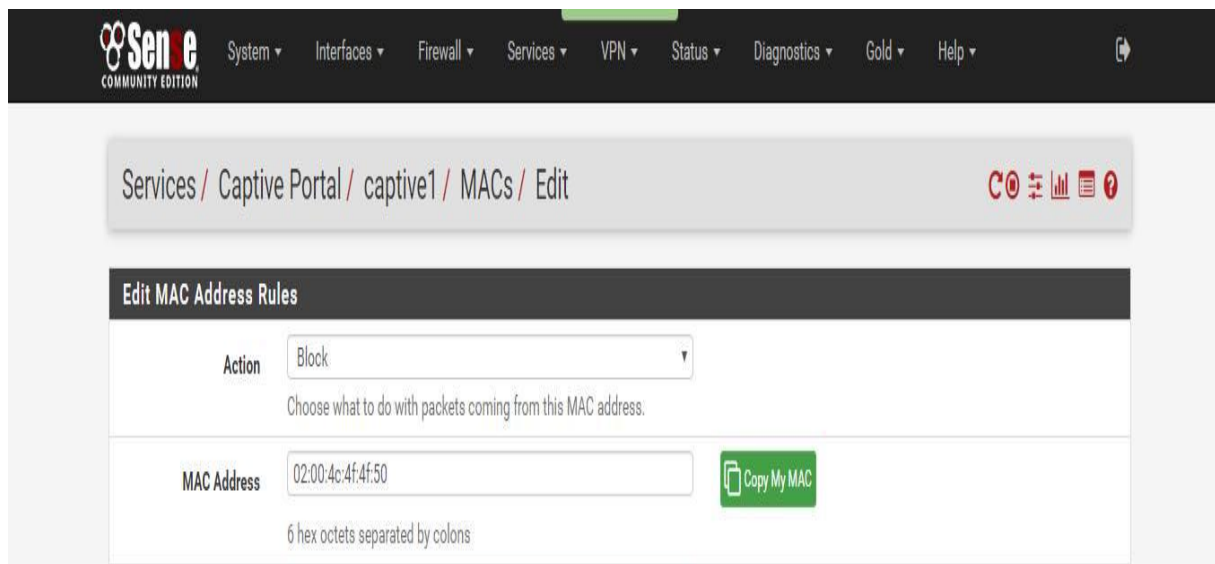


Figure 60:blocage Mac

CONCLUSION GENERALE

Notre projet de fin d'étude a porté sur la sécurisation d'un réseau sans fil et la configuration d'un firewall.

Ce projet s'est avéré bénéfique car il nous a initiés à la sécurité réseau tout en prenant connaissance du métier d'administrateur de sécurité réseau et les approches des règles de sécurité. Il nous a appris à mettre en application le savoir acquis durant nos études supérieures, à connaître l'importance de l'esprit d'équipe dans un projet et à avoir l'opportunité d'être encadrés et guidés.

Certes, nous avons rencontré quelques difficultés pour réaliser notre projet telles que la découverte d'un nouveau domaine de compétence, l'utilisation des nouveaux outils et apprendre à réaliser une bonne manipulation des configurations de réseau. Cependant, le fait qu'on s'est trouvé dans un contexte professionnel et nécessitant une expertise, nous a permis de surmonter ces difficultés et de pouvoir relier l'aspect théorique et l'aspect pratique et réaliser un réseau sans fil sécurisé avec le serveur Freeradius et la protection, la sécurisation et la détection d'attaque réseau avec PfSense.

Ce projet était l'occasion pour découvrir les problèmes liés à la sécurité des réseau sans fil et nous a permis d'avoir une bonne expérience dans la réalisation d'une application en passant par les différentes étapes de configuration .

Enfin, nous espérons que ce projet aura la chance de s'enrichir et d'être amélioré dans des futurs projets.