

REPUBLIQUE DU SENEGAL



Un peuple - un but - une foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR DE LA RECHERCHE ET
DE L'INNOVATION

DIRECTION GENERALE DE L'ENSEIGNEMENT SUPERIEUR

DIRECTION DE L'ENSEIGNEMENT SUPERIEUR PRIVE

ECOLE SUPERIEURE DE TECHNOLOGIE ET DE MANAGEMENT



MEMOIRE DE FIN DE CYCLE

Pour l'obtention de la Licence en **TELEINFORMATIQUE**

Option **Télécommunications et Réseaux**

INTITULE

**Etude et mise en œuvre de solution contre les
intrusions réseau**

Présenté et soutenu par :
M. Abdoulaye GUEYE

Sous la direction de :
Dr. Mamadou Mansour KHOUMA

2023-2024

A LA MEMOIRE DE

Tous ceux qui ont contribué à notre éducation, à notre formation et à notre réussite et qui ne sont plus là malheureusement :

- Mon père Djibril GUEYE
- Ma tante Fatou NDAW

Paix à leur âme et que Dieu les accueille au paradis. Amine.

DEDICACES

C'est avec profonde gratitude et sincères mots, que nous dédions ce modeste travail de fin d'étude à ma chère sœur Ndèye Anna GUEYE et mon frère Papa Doudou GUEYE qui ont sacrifié leurs vies pour notre réussite et ils nous ont éclairé le chemin par leurs conseils judicieux. On espère qu'un jour, nous pourrons leur rendre un peu de ce qu'ils ont fait pour nous, que Dieu leur prête bonheur et longue vie.

REMERCIEMENTS

Nous tenons tout d'abord à remercier ALLAH le tout puissant de nous avoir donné, la force et le courage, la santé, les moyens afin de pouvoir accomplir ce modeste travail.

Nous adressons particulièrement notre reconnaissance envers Dr Mansour KHOUMA notre encadreur, professeur à l'ESTM, pour son suivi. Les discussions que nous avons partagées ont permis d'orienter notre travail d'une manière pertinente. Nous le remercions aussi pour sa disponibilité à encadrer ce travail à travers ses critiques et ses propositions d'amélioration.

Nous tenons à présenter nos remerciements à Lamine HAIDARA, au Dr Anthony TONFACK et à tous nos enseignants si compétents pour nous avoir soutenus dans la poursuite de notre formation.

Nous remercions toute la famille ainsi que nos amis(es) pour les encouragements incroyables tout au long de ce travail.

Enfin nous remercions toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce mémoire, ainsi qu'au bon déroulement de ce projet, et dont les noms ne figurent pas dans ce mémoire.

AVANT-PROPOS

Créée en 2001, l'ESTM (Ecole Supérieure de Technologie et de Management de Dakar) est une école d'ingénieurs spécialisés entre autres dans les domaines de l'informatique, des télécommunications et du management des entreprises. Ayant un corps professoral professionnel et expérimenté, elle a pour mission de former et de délivrer des formations reconnues, innovantes et de qualité à ses étudiants, mais c'est aussi de les accompagner dans leur insertion professionnelle et dans la construction d'une belle carrière ! S'appuyant sur le système LMD, l'ESTM délivre des diplômes en Licence, Master en s'inspirant des normes exigées par le CAMES (Centre Africain et Malgache pour l'Enseignement Supérieur).

Pour l'obtention de la licence en Réseaux et Télécommunications, l'ESTM exige aux étudiants la rédaction d'un mémoire de fin de cycle. C'est dans ce cadre que nous avons élaboré ce document qui a pour sujet : **Etude et mise en œuvre de solution contre les intrusions réseau**

La supervision va permettre une détection des actions qui essaient de collecter la confidentialité de l'utilisateur ou les informations sur une ressource. La détection d'intrusion peut être effectuée manuellement ou automatiquement. Dans le processus de détection d'intrusion manuelle, un analyste humain procède à l'examen de fichiers de logs à la recherche de tout signe suspect pouvant indiquer une intrusion. Mais dans le cas d'une détection d'intrusion automatique le système crée des bips pour alerter les administrateurs afin qu'ils puissent y remédier.

RESUME

Le renforcement de la sécurité informatique est devenu une nécessité primordiale vu l'apparition des diverses formes d'attaques informatiques de nos jours. Et ce sont les réseaux d'entreprises, d'institutions, de gouvernements qui ont le plus besoin de cette sécurisation car elles sont fréquemment les cibles des attaques d'intrusion. Les pare-feux sont très populaires en tant qu'outils permettant d'élaborer efficacement des stratégies pour sécuriser un réseau informatique. Un firewall offre au système une protection d'un réseau interne, contre un certain nombre d'intrusions venant de l'extérieur, grâce à des techniques de filtrage rapides et intelligentes.

L'objectif de ce travail est la mise en place d'un firewall open source « pfsense » comme solution. Ce pare-feu offre un panel de fonctionnalités de type NAT, DHCP, ...etc., auquel nous avons utilisé « kali linux » pour jouer le rôle de client pour l'intrusion.

En somme le pare-feu est une solution de premier choix, mais il nécessite quand même une intervention humaine.

ABSTRACT

Strengthening computer security has become a primary necessity given the emergence of various forms of computer attacks nowadays. And it is the networks of companies, institutions, governments that need this security the most because they are frequently the targets of intrusion attacks. Firewalls are very popular as tools for effectively developing strategies to secure a computer network. A firewall offers the system protection of an internal network, against a certain number of intrusions coming from outside, thanks to fast and intelligent filtering techniques.

The objective of this work is the implementation of an open source firewall "pfsense" as a solution. This firewall offers a range of features such as NAT, DHCP, ... etc., to which we used "kali linux" to play the role of client for the intrusion.

In short, the firewall is a first-class solution, but it still requires human intervention.

Table des matières

A LA MEMOIRE DE.....	1
DEDICACES	2
REMERCIEMENTS	3
AVANT-PROPOS.....	4
RESUME	5
ABSTRACT.....	6
LISTE DES FIGURES.....	11
LISTE DES TABLEAUX	13
GLOSSAIRES	14
INTRODUCTION GENERALE	16
CHAPITRE I : CADRE THEORIQUE ET CADRE METHODOLOGIQUE	18
I - Cadre Théorique.....	18
1.1 Problématique.....	18
1.2 Objectif de la recherche.....	18
1.3 Hypothèse de recherches	19
1.4 Pertinence du Sujet.....	19
II Cadre Méthodologique	20
2.1 Cadre de l'étude	20
2.2 Délimitation du champ de l'étude.....	21
2.3 Technique d'investigation	21
2.4 Difficultés rencontrées.....	21
CHAPITRE II : CADRE CONCEPTUEL.....	22
III Rappel sur le réseau et la sécurité	22
3.1 Rappel sur les réseaux	22
3.1.1 Définition des réseaux informatiques.....	22
3.1.1.1 Les type de réseaux.....	22
3.1.1.2 Définition des réseaux sans fil.....	23
3.1.1.3 Les Réseaux WPAN (Wireless Personale Area Network)	23
3.1.1.4 Les réseaux LAN (Local Area Network)	23
3.1.1.5 Les réseaux WLAN (Wireless Local Area Network)	24
3.1.1.6 Les réseaux WMAN (Wireless Metropolitan Area Network)	24

3.1.1.7 Les réseaux MAN	24
3.1.1.8 Les réseaux locaux WAN.....	24
3.1.1.9 Les attaques réseaux	25
3.1.1.10 Les attaques réseaux sans fil.....	25
3.1.1.11 L'interception des données.....	25
3.1.1.12 L'usurpation d'adresse IP	25
3.1.1.13 Les réseaux VLAN (Virtual Local Area Network).....	25
3.1.1.14 Les réseaux locaux sans fils (WIFI)	26
3.1.2 Catégories des réseaux informatiques	26
3.1.2.1 Les réseaux P2P (Peer to Peer où pair à pair).....	26
3.1.2.2 Les réseaux serveurs/clients	26
3.1.3 Les différent types de topologie réseau	26
3.1.3.1 Définition du topologie réseau.....	26
3.1.3.2 Topologie en bus.....	26
3.1.3.3 Topologie en étoile.....	27
3.1.3.4 Topologie en anneau	28
3.1.3.5 Topologie en arbre	28
3.1.4 Les différents types de routages	29
3.1.4.1 Définition du concept Routage	29
3.1.4.2 Routage statique.....	29
3.1.4.3 Routage Dynamique	29
3.1.4.4 Le routage centralisé.....	30
3.1.5 La norme du modèle OSI	30
3.1.5.1 Définition.....	30
3.1.5.2 Les différentes couches du modèle OSI	30
3.1.5.3 La couche physique	31
3.1.5.4 La couche liaison de données	31
3.1.5.5 La couche Réseau	31
3.1.5.6 La couche Transport	32
3.1.5.7 La couche Session.....	32
3.1.5.8 La couche Présentation	33
3.1.5.9 Couche Application	33
3.1.5.10 Le modèle TCP/IP	34
3.1.6 Définition de la cryptographie.....	34

3.1.6.1 Les différents types de cryptographies	34
3.1.6.2 La cryptographie symétrique	35
3.1.6.3 La cryptographie asymétrique	35
3.1.7 Définition d'un serveurs Proxy	35
3.1.7.1 Serveur proxy niveau application et circuit	35
3.1.7.2 Serveur proxy dédié ou générique	36
3.1.8 Les réseaux privés virtuels (VPN).....	36
III.2 Rappels sur la sécurité	36
3.2.1 Définition de la sécurité informatique	36
3.2.1.1 Types de sécurité informatique	37
3.2.1.2 Différence entre sécurité des informations et sécurité informatique	37
3.2.1 Les objectifs spécifiques de la sécurité	37
3.2.2 Les différents types d'attaques.....	39
3.2.3 Les techniques d'attaques	40
IV Généralités sur les systèmes de détection et de prévention.....	41
4.1 Présentation des systèmes de détections d'intrusion.....	41
4.1.1 Les différents types de détection d'intrusion	41
4.1.2 Classification des systèmes de détection d'intrusion.....	42
4.2 Présentation des systèmes de prévention d'intrusion.....	43
4.2.1 Les différents types de système de préventions d'intrusions.....	44
4.2.2 La différence entre IPS et IDS.....	45
4.3 Choix de la solution.....	45
4.3.1 La sécurité améliorée.....	45
4.3.2 Automatisation des taches	46
4.3.3 La conformité aux règles	46
4.3.4 Les raisons de choix de solution.....	46
CHAPITRE III : MISE EN OEUVRE DE LA SOLUTION	48
4.4 Présentation de la solution retenue	48
4.4.1 Architecture de Solution.....	48
4.4.2 Déploiement	49
4.4.3 Présentation de Suricata	50
4.4.4 Présentation de Snort.....	50
4.4.5 Présentation de OSSEC	50
4.5.6 Outil technologie mise en œuvre.....	51

CONCLUSION :	71
BIBLIOGRAPHIE ET WEBOGRAPHIE :	72

LISTE DES FIGURES

Figure 1 Réseau sans fil lié par Bluetooth	23
Figure 2 Périphérique communiquant par Ethernet	24
Figure 3 Communication sans fil par Wi-Fi.....	24
Figure 4 Topologie en bus.....	27
Figure 5 Topologie en étoile	27
Figure 6 Topologie en anneau	28
Figure 7 Topologie en arbre	29
Figure 8 Déploiement et fonctionnement de pfsense.....	50
Figure 9 Clique avec Advanced	52
Figure 10 Remplir les espaces vides	53
Figure 11 Remplir les champs vides	53
Figure 12 Confirmation de bonne configuration.....	54
Figure 13 Interface de Thunderbird	54
Figure 14 Remplir les informations	54
Figure 15 Enregistrement de l'utilisateur dans la base	55
Figure 16 Domaine du serveur entrant et sortant.....	55
Figure 17 Compte créer.....	56
Figure 18 Enregistrement d'un utilisateur dans la base	57
Figure 19 Compte créer.....	57
Figure 20 Envois email via pfsense	58
Figure 21 Début de l'installation de Snort	58
Figure 22 Recherche et installation de snort.....	59
Figure 23 Procédure d'installation de snort	59
Figure 24 Installation de snort	60
Figure 25 Début de la configuration	61
Figure 26 Accès aux paramètres globaux	62
Figure 27 Création d'un compte Snort.....	62
Figure 28 Connexions dans snort.....	63
Figure 29 Générons un « Oinkcode »	63
Figure 30 code générer pour pfsense	63
Figure 31 Début de la configuration	64
Figure 32 téléchargement des mises à jour de Snort.....	65

Figure 33 Téléchargements effectuer	65
Figure 34 Configuration de l'interface et création des alertes.....	66
Figure 35 Cliquez sur LAN Catégories	67
Figure 36 Configurer de Snort	67
Figure 37 Kali linux pour l'intrusion.....	68
Figure 38 Détection des intrusions avec Pfsense	68
Figure 39 Accès sur captive portail.....	69
Figure 40 Renseignement des champs vides.....	69
Figure 41 Option LAN pour continuer	70

LISTE DES TABLEAUX

Tableau 1 Couche du Modèle OSI	30
Tableau 2 (gauche) de découpage en couche du modèle OSI.....	34
Tableau (droite) découpage du Modèle TCP/IP.....	34
Tableau 3 Comparaison de solution	51

GLOSSAIRES

CSA: Cisco Security Agent

DOS: Denial of Service

DMZ: Demilitarized Zone

DNS: Domain Name System

EAP: Extensible Authentication Protocol

HTTP: Hypertext Transfer Protocol

HIPS: Host Based Intrusion Detection System

HIDS : System de détection et intrusion sur les hôtes

IP: Internet Protocol

IPSEC: Internet Protocol Security

ISS: Internet Security System

IPS: Intrusion Prevention System

IDS: Intrusion Detection System

KIPS: Kernel Intrusion Prevention System

LDAP: Lightweight Directory Access Protocol

NIDS: Network Intrusion Detection System

NNIDS: Network Node Intrusion Detection system

NIPS : System de protection contre les intrusions en réseaux

OSI: Open system interconnect

SNORT: The Open-Source Network Intrusion Detection System.

SNMP: Simple Network Management Protocol

TCP: Transmission Control Protocol

UDP: Unit Datagram Protocol

VPN : Virtual Private Network

INTRODUCTION GENERALE

Avant la diffusion des connexions inter-réseaux qui entraîna l'internet tel que nous la connaissons, la majeure partie des réseaux étaient limités à des communications entre les mêmes postes de ce réseau. Quelques réseaux avaient des passerelles ou des ponts les reliant entre eux, mais la plupart du temps ils étaient conçus pour un usage unique. Une méthode déjà utilisée dans les réseaux de télécommunication reposait sur un ordinateur central raccordé à ses terminaux via de longues lignes.

La sécurité informatique protège l'intégrité des informations comme les attaques, systèmes de transfert de fichiers, évalue le trafic réseaux, et les données des entreprises, les dommages causés ou les accès non autorisés. Donc la sécurité de l'information est un mécanisme d'authentification et de contrôle d'accès dont a besoin une entreprise afin de construire un système sécurisé déterminant et éliminant ces vulnérabilités.

Pour pallier aux besoins des entreprises, l'administration de réseau ne cesse d'évoluer pour s'équiper avec de nouvelle technologie récente qui peuvent faire face aux attaques afin de pouvoir améliorer la sécurité des données et leurs transferts.

Les entreprises ont un rôle très important actuellement mais ont cependant besoin de la surveillance des informaticiens spécialisés en sécurité informatique, de plus en plus d'équipement avec des technologies de pointes qui leurs permettent de bien gérer leur infrastructure (serveur, imprimante, téléphonie IP, Ordinateur). Il est difficile d'administrer un réseau informatique avec l'ensemble des équipements car les administrateurs ont beaucoup de tâches à effectuer.

Le but de notre mémoire est de mettre en place un système de détection d'intrusion de réseau qui est un mécanisme destiné à repérer les activités anormales ou suspectes sur la cible analysée (réseau ou hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées. Pour notre documentation il a fallu recourir à la recherche documentaire comme technique d'investigation.

Pour bien mener à notre but, il s'agira de réaliser une étude approfondie sur la supervision du trafic réseau et détecter des anomalies dans le réseau. Notre étude sera répartie en trois parties : la première partie sera sur le cadre théorique et méthodologique, la deuxième partie sera basée

sur le cadre conceptuel et enfin la troisième partie portera sur l'étude et la mise en œuvre de notre outil de supervision.

CHAPITRE I : CADRE THEORIQUE ET CADRE METHODOLOGIQUE

I - Cadre Théorique.

1.1 Problématique

Le réseau informatique est un ensemble d'équipement (router, modem, switch) qu'utilise les entreprises pour interconnecter leurs équipements réseaux. Avec la modernisation et la technologie elles évoluent au fur et à mesure et ont donc besoins de sécurisées leurs données et leurs informations. Avoir un pare-feu dans une entreprise est un moyen de lutter efficacement pour lutter contre les menaces. Le fait est de constater que même si elles sont équipées de matériels adéquat, ces systèmes sont souvent confrontés à de nombreuses difficultés comme, les pannes, la baisse de performance, et aux problèmes liés aux ressources. Pour la prévention des intrusions l'entreprise peut sécuriser les environs en faisant l'acquisition d'une clôture et d'un portail, mais aussi en isolant les éléments dangereux par des marquages. Se protéger contre les intrus empêchent que des informations sensibles et des données personnelles tombent entre les mains des personnes extérieures et protègent aussi les périphériques physiques.

Pourquoi utiliser des technologies IPS ou IDS pour sécuriser les entreprises ?

Pourquoi doit-on installer un système de détection d'intrusion pour les entreprises ?

L'ensemble de ces questions constituent la problématique de notre sujet.

Nous allons passer aux objectifs de recherches.

1.2 Objectif de la recherche

Notre objectif de recherche débute avec l'objectif général suivis de l'objectif spécifiques.

Notre objectif général est de mettre en place un système de détection d'intrusion avec des alertes pour évaluer le trafic réseaux afin de détecter des intrus avec des outils open source et les étudiée, et savoir comment les installées et voir comment ils fonctionnent au sein du réseau et d'avoir les possibilités qu'ils offrent afin de faire une étude approfondie sur notre objectif spécifique.

Les objectifs spécifiques sont les suivants :

- Surveiller les machines hôtes et étudier le trafic
- Etudier et analyser les suspects pendant un temps
- Vérifier l'état du réseau

Cette section a constitué nos objectifs de recherches. Entre temps il devient nécessaire de déterminer un ensemble d'hypothèse à émettre afin de répondre à la question posée.

1.3 Hypothèse de recherches

Pour apportés des solutions aux problèmes, nôtre travail consistera à mettre en place un mécanisme de surveillance et de supervision afin de réduire les risques entre l'apparition d'un problème et son traitement et d'effectuer un signal pour les alertes suspects. Ainsi nos recherches seront basées sur :

La surveillance du trafic réseau

La vérification des composants du système

La mise en alerte en cas de problème ou d'intrus

Les actions à effectuer en fonction des alertes et voyant

Le choix de notre solution sera basé sur plusieurs critère dépendant de ce que nous allons présenter au fur et à mesure de notre étude.

1.4 Pertinence du Sujet

Les systèmes de détections d'intrusions sont intéressants à étudier car ils apportent beaucoup de solutions, ils peuvent être des pare-feu conçus dans le but de contrer les attaques et les intrusions non identifiés. Ils sont devenus un élément clé dans un avenir prévisible en ce qui concerne la sécurité des entreprises car de nos jours toutes les entreprises sont confrontées à l'insécurité et aux attaques pouvant mener à leurs pertes.

Au cours des dernières années, beaucoup de société ont été victimes d'attaques et certains ont perdus beaucoup de clients. De nos jours la sécurité est l'une des branches les plus importantes

dans le domaine de l'informatique il est présent dans la (programmation web, sécurisation des fichiers, le réseau) pour s'assurer qu'au qu'une perte ne se fasse.

Cette étude vise à contribuer et à aider les grandes ou petites sociétés à protéger leurs données et leurs éviter des pertes de clients et de sécurisé leurs données en utilisant la technologie moderne.

Ce premier chapitre nous permettra d'apprendre l'ensemble des questions soulevé par le sujet. Maintenant nous allons passer au cadre méthodologique du sujet.

II Cadre Méthodologique

De nos jours les réseaux informatiques sont indispensables pour les entreprises car ils facilitent l'échange des données via des logiciels qui effectuent des taches afin de permettre une communication (VOIP, courriel, serveurs de fichiers, serveurs DHCP). Ces entreprises subissent des attaques pouvant entrainer des pertes ou des collectes de données. Mais les systèmes de détection, et prévention d'intrusions, sont conçu pour contrer ces attaques et trouver des solutions à ces attaques. Ils sont largement répandus pour la sécurité de ces systèmes informatiques puisqu' ils permettent à la fois de détecter et de répondre à une attaque en temps réel ou en hors-ligne.

Dans cette partie nous allons d'abord présenter le cadre d'utilisation de détection d'intrusions puis délimiter notre champ de recherches, ensuite nous parler des techniques d'investigations utilisées et enfin les difficultés rencontrées durant nos recherches.

2.1 Cadre de l'étude

Notre étude se focalise sur les réseaux informatiques. Toutes entreprises à besoin d'échange d'information elle a une valeur qui doit être convenablement protégé entre autres (ces données, ces utilisateurs, et son fonctionnement). L'approche de la sécurité de l'information permet de protéger l'information des menaces qui pourraient corrompre sa qualité tout en garantissant à la continuité des activités de l'entreprise, en minimisant les pertes et en maximisant le retour sur l'investissement et les opportunités.

2.2 Délimitation du champ de l'étude

Cette étude se focalise principalement sur la surveillance des systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) qui surveillent notre réseau en permanence afin d'identifier les incidents potentiels entraînant une violation des données.

Ils consignent les informations afférentes dans des journaux, résolvent les incidents et les signalent aux administrateurs chargés de la sécurité. Les systèmes de détection d'intrusions, sont des systèmes software ou hardware conçus afin de pouvoir automatiser le monitoring d'événements survenant dans un réseau ou sur une machine particulière.

Système IPS considère le paquet inoffensif, il le transmet sous forme d'un élément traditionnel de couches 2 ou 3 du réseau. Les utilisateurs finals ne doivent en ressentir aucun effet. Cependant, lorsque le système IPS détecte un trafic douteux il doit pouvoir activer un mécanisme de réponse adéquat en un temps record. L'IPS doit aussi, offrir un moyen de diminuer considérablement l'utilisation des ressources humaines nécessaires au bon fonctionnement des IDS.

2.3 Technique d'investigation

La technique adoptée pour réaliser ce travail est la recherche documentaire en faisant recours aux sites internet et aux anciens mémoires relatant de ce sujet. Cette partie nous a permis de connaître l'ensemble des techniques d'investigations auxquelles nous avons eu recours durant la conception de ce mémoire.

2.4 Difficultés rencontrées

Au cours de nos recherches, nous avons eu à rencontrer quelques difficultés dont les plus mémorables sont :

- Les difficultés rencontrées pendant la rédaction du mémoire
- Les informations parfois pas très pertinentes lors de la consultation d'autre ouvrage.
- L'installation de l'iso de pfsense qui a nécessité une autre machine

CHAPITRE II : CADRE CONCEPTUEL

III Rappel sur le réseau et la sécurité

3.1 Rappel sur les réseaux

3.1.1 Définition des réseaux informatiques

Les réseaux informatiques sont des périphériques électronique (ordinateurs, imprimantes, tablettes) capables d'échanger des informations grâce à des lignes physiques puis les transmettre sous format de données numériques. Ces réseaux informatiques sont indispensables pour les entreprises, car les systèmes d'exploitation, les logiciels informatiques, les serveurs, les routeurs et les switches, utilisent des protocoles réseaux afin de faire parvenir l'information à destination. Pour qu'ils puissent communiquer ils utilisent des protocoles réseaux pour mieux parvenir les informations à destination. L'objectif est de permettre aux composants électroniques, matériels et logiciels de communiquer entre eux à travers des protocoles normalisés du modèle OSI de façon à ce que l'usage du réseau soit le plus efficace possible à ses utilisateurs.

Un réseau informatique peut avoir plusieurs objectifs distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.)
- La communication entre personnes (courrier électronique, réseaux sociaux etc.)
- La communication entre processus (entre des ordinateurs industriels par exemple etc.)
- Une garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données)
- Le jeu vidéo multi-joueurs
- Téléchargement des fichiers et applications.

3.1.1.1 Les type de réseaux

On distingue plusieurs catégories de réseaux selon leurs infrastructures, et leurs fonctionnements, en fonction des systèmes informatiques ou encore de leurs technologies

3.1.1.2 Définition des réseaux sans fil

Les réseaux sans fil, comme des réseaux à travers lesquels les périphériques peuvent communiquer sans liaison filaire. Ils sont basés sur une liaison utilisant des ondes radioélectriques (radio et infrarouges) en un lieu où est placé des antennes.

3.1.1.3 Les Réseaux WPAN (Wireless Personale Area Network)

Un réseau WPAN est un réseau personnel qui couvre une plage d'espace limitée entre dix et trente mètres selon la capacité des appareils utilisés pour sa connexion. Ils peuvent être connectés à partir d'ordinateurs, de téléphones portables, d'imprimantes et d'appareils photo. Par exemple (Bluetooth, HomeRF).



Figure 1 Réseau sans fil lié par Bluetooth

3.1.1.4 Les réseaux LAN (Local Area Network)

C'est un ensemble d'appareils informatiques appartenant à une même organisation et qui sont reliés par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Il se trouve dans un espace limité, comme une pièce, un ou un ensemble de bâtiments. La vitesse de transfert de ces réseaux peut varier entre (10 Mbps pour l'Ethernet, et 1 Gbps pour les FDDI ou Gigabit Ethernet).

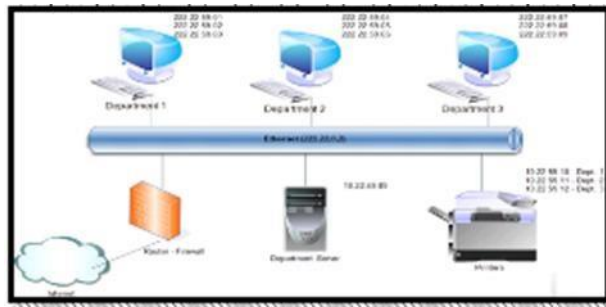


Figure 2 Périphérique communiquant par Ethernet

3.1.1.5 Les réseaux WLAN (Wireless Local Area Network)

Ces réseaux permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Ils permettent de relier entre eux les terminaux présents dans la zone de couverture. On peut citer comme exemple la technologie Wi-Fi.



Figure 3 Communication sans fil par Wi-Fi

3.1.1.6 Les réseaux WMAN (Wireless Metropolitan Area Network)

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.

3.1.1.7 Les réseaux MAN

C'est une Infrastructure réseau qui couvre une zone plus vaste qu'un LAN, mais moins étendue qu'un WAN (par exemple, une ville). Les MAN sont généralement gérées par une seule entité, comme une grande entreprise. En général le câble coaxial est le support physique le plus utilisé dans ce type de réseau il peut être public ou privé sa norme est IEEE-802.6.

3.1.1.8 Les réseaux locaux WAN

Un réseau étendu WAN est un réseau informatique couvrant une grande zone géographique, permettant de relier plusieurs pays où continent et de nombreux serveurs et succursales

internationales utilisent un WAN pour connecter les réseaux de leurs entreprises. Le plus grand WAN actuellement est le réseau Internet.

3.1.1.9 Les attaques réseaux

Ce sont des attaques répandues qui ont pour but d'intercepter les communications entre de tierces personnes, sans que ces utilisateurs ne se doutent que le canal a été compromis. Les hackers utilisent souvent ce type d'attaque car ils peuvent utiliser et écouter le trafic qui se passent entre les ordinateurs de l'entreprise et une machine tierce.

3.1.1.10 Les attaques réseaux sans fil

C'est l'attaque la plus classique. Elle consiste à écouter les transmissions des différents utilisateurs d'un réseau sans fil, et de récupérer n'importe quelle donnée transitant sur ce réseau si elles ne sont pas cryptées.

3.1.1.11 L'interception des données

Par défaut un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous, et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour une entreprise l'enjeu stratégique est très important.

3.1.1.12 L'usurpation d'adresse IP

Est une technique de piratage informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.

3.1.1.13 Les réseaux VLAN (Virtual Local Area Network)

Les vlan sont des réseaux virtuels dans lesquels un réseau physique peut-être subdivisé en plusieurs réseaux logiques. La norme 802.1Q fut sortie par Cisco et l'implémenta aussi dans ses switches avec la possibilité sur certains switches Cisco de décider quel 'trunk' effectuer entre le ISL ou le 802.1Q.

3.1.1.14 Les réseaux locaux sans fils (WIFI)

Un réseau sans fil est un réseau numérique dans lequel les différents postes communiquent par ondes radio ou sans liaisons filaire. Ces réseaux nous offrent une possibilité d'être connecté en un périmètre géographique étendue.

Ces technologies se distinguent par leur fréquence, leur débit, ainsi que leur transmission. Ils relient très facilement des périphériques informatiques d'une dizaine de mètres ou de kilomètres.

3.1.2 Catégories des réseaux informatiques

On distingue deux types de réseaux qui sont les suivants :

3.1.2.1 Les réseaux P2P (Peer to Peer où pair à pair)

Les logiciels clients et ceux des serveurs sont généralement exécutés sur des ordinateurs distincts, mais un seul des deux peut tenir simultanément ces doubles rôles. Ils arrivent que les ordinateurs fassent à la fois office de client et de serveur sur le réseau.

3.1.2.2 Les réseaux serveurs/clients

Sur un réseau à architecture client-serveur, tous les ordinateur (client) sont connectés à un ordinateur central (le serveur de réseau), une machine généralement très puissante en termes de capacité, elle est utilisée pour le partage de connexion, les logiciels centralisés et les fichiers.

3.1.3 Les différent types de topologie réseau

3.1.3.1 Définition du topologie réseau

La topologie d'un réseau correspond à son architecture physique, en ce sens où leur structure détermine leur type. Les architectures suivantes ont effectivement été utilisées dans des réseaux informatiques grand public ou d'entreprise.

3.1.3.2 Topologie en bus

Une topologie en bus est une configuration réseau dans laquelle chaque ordinateur et chaque périphérique réseau sont connectés à un seul câble ou à un réseau fédérateur. Selon le type de

carte réseau utilisé dans chaque ordinateur de la topologie en bus, un câble coaxial ou un câble réseau RJ-45 est utilisé pour les connecter ensemble.



Figure 4 Topologie en bus

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. Elle est cependant vulnérable car si l'une des connexions est défectueuses, l'ensemble du réseau est affecté.

3.1.3.3 Topologie en étoile

C'est la topologie la plus courante actuellement elle est omniprésente, elle est très souple en matière de gestion et dépannage de réseau, la panne d'un nœud ne perturbe pas le fonctionnement global du réseau. En revanche un commutateur (switch) qui relie tous les nœuds constitue un point unique de défaillance, une panne à ce niveau rend le réseau totalement inutilisable. Le réseau Ethernet est un exemple de topologie en étoile. L'inconvénient principal de cette topologie réside dans la longueur des câbles utilisés.

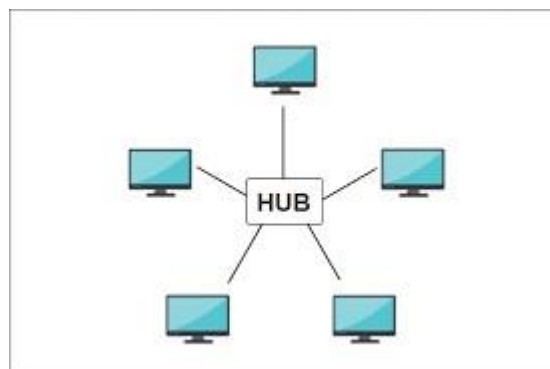


Figure 5 Topologie en étoile

Contrairement à la topologie en bus les topologies en étoiles sont moins vulnérables car une connexion peut être débranchée sans que le reste des périphériques du réseau ne soient paralysés, elles ont besoin d'un hub pour pouvoir fonctionner.

3.1.3.4 Topologie en anneau

La topologie en anneau est une configuration réseau dans laquelle les connexions de périphériques créent un chemin de données circulaire. Chaque appareil du réseau est entièrement connecté à deux autres, l'avant et l'arrière, formant ainsi un seul chemin continu pour transmettre le signal, comme les points dans un cercle. Cette topologie peut également être appelée topologie active.

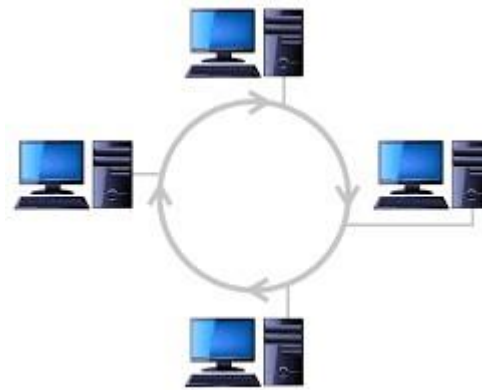


Figure 6 Topologie en anneau

La topologie en anneau connecte chaque périphérique à exactement deux périphériques formant un seul chemin continu similaire à un anneau.

3.1.3.5 Topologie en arbre

Une topologie en arbre peut également être décrite comme une combinaison des topologies en étoile et en bus. Le nœud primaire ou racine est connecté à un ou plusieurs nœuds secondaires, qui sont connectés à des nœuds tertiaires, formant ainsi une structure hiérarchique ou arborescente.

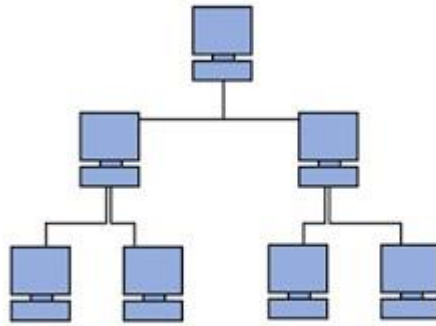


Figure 7 Topologie en arbre

La topologie en anneau est moins fiable car la défaillance d'un appareil peut perturber l'ensemble du réseau. La topologie en anneau est moins chère que la topologie en arbre.

3.1.4 Les différents types de routages

3.1.4.1 Définition du concept Routage

Le routage est une règle intégrée dans les logiciels qui permettent aux routeurs de passer des informations entre les réseaux. Ce protocole de routage permet également aux routeurs de déterminer les itinéraires disponibles ainsi que de déterminer les itinéraires les plus efficaces pour le trafic réseau.

3.1.4.2 Routage statique

Le routage statique est une forme de routage qui permet d'ajouter des informations dans la table de routage de façon manuel à chaque modification topologique du réseau.

On utilise ce type de routage quand on veut spécifier le chemin que doit emprunter la route pour arriver à destination ou du routeur prochain, plutôt que des informations provenant du trafic de routage dynamique.

3.1.4.3 Routage Dynamique

Le routage dynamique utilise plusieurs algorithmes et protocoles pour fonctionner. Le routage dynamique permet aux routeurs de sélectionner les chemins en fonction des changements de disposition du réseau logique en temps réel. Les protocoles de routages (RIPv2, OSPF, EIGRP).

3.1.4.4 Le routage centralisé

Le modèle de routage centralisé est un modèle de routage dans lequel le routage est effectué de manière centralisée à l'aide d'une base de données centralisée. En d'autres termes, la table de routage est conservée à un seul nœud "central", qui doit être consulté lorsque d'autres nœuds doivent prendre une décision de routage.

3.1.5 La norme du modèle OSI

3.1.5.1 Définition

Le modèle OSI (Open System Interconnections) est un modèle générique et standard d'architecture d'un réseau en 7 couches, élaboré par l'organisme ISO (Organisation Internationale de normalisation) en 1984.

La mise en évidence de ces différentes couches se base sur les caractéristiques suivantes qui étaient recherchées par l'ISO :

- Création d'une couche lorsqu'un niveau d'abstraction est nécessaire.
- Définition précise des services et opérations de chaque couche.
- Définition des opérations de chaque couche en s'appuyant sur des protocoles normalisés.
- Choix des frontières entre couches de manière à minimiser le flux d'information aux interfaces.
- Définition d'une couche supplémentaire lorsque des opérations d'ordre différent doivent être réalisées.

3.1.5.2 Les différentes couches du modèle OSI

Le modèle standard OSI comporte 7 couches et chacune joue un rôle important dans l'acheminement des données.

Tableau 1 Couche du Modèle OSI

N°	Couches modèle OSI	Protocole de chaque couche
7	Application	DNS, FTP, http, IMAP, POP3, SMTP, SNMP
6	Présentation	AFP, ASN.1, ASCII, MIME, SMB

5	Session	AppleTalk, ISO 8327 / CCITT X.225
4	Transport	ATP, TCP, UDP, SCTP
3	Réseau	ARP, CLNP, DDP, ICMP, IGMP, IP
2	Liaison	PPP, RADIUS, RNIS, Wi-Fi, Bluetooth
1	Physique	Matériel et parfois propre aux constructeurs

3.1.5.3 La couche physique

Comme son nom l'indique, la couche physique est responsable de l'équipement qui facilite le transfert des données, comme les câbles et les routeurs installés sur le réseau. Sans normes, la transmission entre les appareils de différents fabricants est impossible. Matériaux propres aux constructeurs.

3.1.5.4 La couche liaison de données

Spécifie comment les données sont expédiées entre deux nœuds/routeurs dans une distance d'un saut. Elle est responsable du multiplexage des données, du contrôle d'erreurs, de l'accès au media ainsi d'assurer la liaison point à point où multipoint dans un réseau de communication.

- La norme Bluetooth est une norme de télécommunications permettant l'échange bidirectionnel de données à courte distance en utilisant des ondes radio UHF sur la bande de fréquence de 2,4 GHz. Son but est de simplifier les connexions entre les appareils électroniques à proximité en supprimant des liaisons filaires.
- Le wifi (Wireless Fidelity) est une technologie de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenue un moyen d'accès à haut débit à Internet. Il est basé sur la norme IEEE 802.11 (ISO/CEI 8802-11).

3.1.5.5 La couche Réseau

Lorsque l'on communique au sein d'un même réseau, la couche réseau est inutile, mais la plupart des utilisateurs se connectent à d'autres réseaux, tels que les réseaux dans le cloud. Lorsque les données traversent différents réseaux, la couche réseau est chargée de créer de petits paquets de données acheminés vers leur destination, puis reconstruits sur l'appareil du destinataire.

Protocol Ipv4 (Internet protocol version 4) La version 4 du protocole Internet est la quatrième version du protocole Internet. C'est l'un des protocoles de base des méthodes d'interconnexion de réseaux basées sur des normes dans Internet et d'autres réseaux à commutation de paquets.

ICMP (Internet Control Message Protocol) est l'un des protocoles fondamentaux constituant la suite des protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible

3.1.5.6 La couche Transport

Cette couche est chargée du transport des données, de leur découpage en paquets, du contrôle de flux, de la conservation de l'ordre des paquets et de la gestion des éventuelles erreurs de transmission.

- **TCP (Transmission Control Protocol)** est situé au-dessus de IP. Les applications transmettent des flux de données sur une connexion réseau. TCP découpe le flux d'octets en segments dont la taille dépend de la MTU du réseau sous-jacent (couche liaison de données).
- **UDP (Protocole de Datagramme Utilisateur)** est un des principaux protocoles de télécommunication utilisés par Internet qui n'est pas sécurisé le rôle de ce protocole est de permettre la transmission de données (sous forme de datagrammes) de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port.

3.1.5.7 La couche Session

Pour communiquer entre deux appareils, une application doit d'abord créer une session, qui est unique à l'utilisateur et l'identifie sur le serveur distant. Lorsque de gros volumes de données sont transférés, la session est chargée de s'assurer que le fichier est transféré dans son intégralité que la retransmission est établie si les données sont incomplètes.

- **NetBIOS (Network Basic Input Output System)** Ce n'est pas un protocole réseau, mais un système de nommage et une interface logicielle qui permet d'établir des sessions entre différents ordinateurs d'un réseau.
- **RPC (Remote procedure call)** Chaque message d'appel est associé à un message de réponse. Le protocole RPC est un protocole de transmission de messages qui

implémente d'autres protocoles non RPC tels que le traitement par lots et la diffusion d'appels distants.

3.1.5.8 La couche Présentation

La couche application affiche des informations aux utilisateurs, mais la couche présentation est celle qui prépare les données pour qu'elles puissent être affichées à l'utilisateur. La communication avec un serveur Web via HTTPS utilise des informations chiffrées. La couche présentation est responsable de l'encodage et du décodage des informations afin qu'elles puissent être affichées en clair.

- **Protocol ASCII (American Standard Code for Information Interchange)** est le format le plus courant des fichiers texte dans les ordinateurs et sur Internet. Dans un fichier ASCII, chaque caractère alphabétique, numérique ou spécial est représenté par un nombre binaire sur 7 bits une chaîne composée de sept 0 ou 1.
- **Protocole SMB (Server Message Block)** est un protocole permettant le partage de ressources sur des réseaux locaux avec des PC sous Windows La version 2 de SMB est apparue dans Vista, Windows 7 et Windows 8.

3.1.5.9 Couche Application

C'est la seule couche qui interagit directement avec les données de l'utilisateur. Les applications logicielles comme les navigateurs web et les logiciels de messageries se servent de la couche applicative pour initier des communications. Toute fois les applications ne font pas partie de la couche application.

- **Protocole SMTP (Simple Mail Transfer Protocole)** est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique il utilise le port (25).
- **POP3 (Post Office Protocol version 3)** permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant (le serveur POP). Les personnes n'étant pas connectées en permanence à Internet afin peuvent consulter les mails reçus hors connexion il utilise le port (110).
- **DNS (Domain Name System)** Le Domain Name System ou DNS est un service informatique distribué qui résout les noms de domaine Internet en adresse IP

3.1.5.10 Le modèle TCP/IP

TCP/IP est un protocole de liaison de données utilisé sur Internet pour permettre aux ordinateurs et autres appareils d'envoyer et de recevoir des données. L'acronyme TCP/IP signifie 'Transmission Control Protocol Internet Protocol'. Il permet aux appareils connectés à Internet de communiquer entre eux via les réseaux.

Tableau 2 (gauche) de découpage en couche du modèle OSI

Tableau (droite) découpage du Modèle TCP/IP

Modèle OSI		Modèle TCP/IP	
7	Application	4	Application
6	Présentation		
5	Session		
4	Transport	3	Transport (TCP)
3	Réseaux	2	Internet (IP)
2	Liaison de donnée	1	Accès au réseau
1	Physique		

3.1.6 Définition de la cryptographie

La cryptographie permet l'échange sûr des renseignements privés et confidentiels. On peut également utiliser la cryptographie pour assurer l'authentification, la non-répudiation et l'intégrité de l'information, grâce à un processus cryptographique spécial appelé signature numérique.

3.1.6.1 Les différents types de cryptographies

Il existe deux types de chiffrement ou de protocole de routage selon leur degré de chiffrement et leur technologie. La Cryptographie symétrique et celle asymétrique.

3.1.6.2 La cryptographie symétrique

Elle a été très longtemps utilisée pour le chiffrement des messages sensé être confidentiel. Dans le chiffrement à clé symétrique ou clé secrète, c'est la même clé qui sert à la fois à chiffrer et à déchiffrer un message.

Les différents types de chiffrements cryptographiques.

- Advanced Encryptions Standard (AES) : standard de chiffrement avancé C'est l'algorithme de chiffrement actuellement le plus utilisé et le plus sûr.
- Data Encryptions Standard (DES), est un algorithme de chiffrement symétrique par bloc utilisant des clés de 56 bits. Il n'est plus recommandé aujourd'hui, car il est lent à l'exécution et de son espace de clés trop petit, permettant une attaque systématique en un temps raisonnable.
- International Data Encryptions Algorithme (IDEA) : Une clé de chiffrement longue de 128 bits choisie aléatoirement est utilisée pour le chiffrement des données. La même clé secrète est requise pour le déchiffrement. L'algorithme consiste à appliquer huit fois une même transformation suivie d'une transformation finale appelée demi-ronde.

3.1.6.3 La cryptographie asymétrique

La cryptographie asymétrique est utilisée dans le but de garantir la confidentialité d'une donnée, ou d'assurer la sécurité, et établir l'authenticité d'une transaction en employant une technique de chiffrement. Il utilise une clé privée et un autre public pour éviter le déchiffrement du message avant destination.

3.1.7 Définition d'un serveurs Proxy

Le serveur proxy est un serveur intermédiaire qui sépare les utilisateurs des sites Web sur lesquels ils naviguent. Ils assurent différents niveaux de fonctionnalité, de sécurité et de confidentialité, selon le type d'utilisation, vos besoins ou la politique de votre entreprise.

3.1.7.1 Serveur proxy niveau application et circuit

- **Proxy de niveau application (Application-Levels-Proxy)** :il utilise la couche7 du modèle OSI. Ainsi, ce type de serveur proxy dispose de fonctions dont le but est d'analyser des

paquets de données, de bloquer, de modifier, et de transmettre en fonction des règles préconfigurées et filtré les applications.

- **Proxy de niveau circuit (Circuit-Levels-Proxy)** : il fonctionne sur la couche de transport (niveau 4) du modèle de référence OSI et ne peut pas analyser des paquets de données. Il est en général utilisé comme un module de filtre et de pare-feu il permet de filtrer des paquets de données via des ports et des adresses il ne peut pas influencer la communication. Les paquets de données sont soit transmis soit bloqués.

3.1.7.2 Serveur proxy dédié ou générique

- **Proxy dédié** : un serveur proxy dédié définit un protocole de communication particulier. En général, ces serveurs proxy fonctionnent parallèlement aux protocoles tels que HTTP, FTP ou SMTP.

- **Proxy générique** : à l'inverse des proxys dédiés, un serveur proxy générique n'est pas spécialisé et est utilisé pour plusieurs protocoles de communication (SMTP, HTTP).

3.1.8 Les réseaux privés virtuels (VPN)

C'est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

III.2 Rappels sur la sécurité

3.2.1 Définition de la sécurité informatique

La sécurité informatique est un terme utilisé pour décrire l'ensemble des stratégies, méthodes, solutions, et outils utilisés pour protéger la confidentialité, l'intégrité, la disponibilité des données, et ressources numériques d'une entreprise. Cette stratégie s'appuie sur une combinaison de technologies avancées et de ressources humaines pour prévenir, détecter et neutraliser une multitude de cybermenaces et de cyberattaques. Elle couvre la protection de l'ensemble des systèmes matériels, des applications logicielles, ainsi que du réseau et de ses différents composants, comme les datacenters physiques ou basés dans le cloud.

3.2.1.1 Types de sécurité informatique

La sécurité informatique est une mesure ou outil destiné à protéger les ressources numériques d'une entreprise. Elle comprend plusieurs aspects dont entre autres :

- **La cybersécurité** : qui a pour but de protéger les ressources numériques d'une entreprise (réseaux, systèmes, ordinateurs, données, serveurs, etc.) contre les cyberattaques.
- **La sécurité des Endpoint** : ou protection des end points, est l'approche qui vise à protéger les end points (ordinateurs de bureau, ordinateurs portables, terminaux mobiles, etc.) contre les activités malveillantes.
- **La sécurité du cloud** : regroupe la stratégie et les solutions de protection contre les cybermenaces de l'infrastructure cloud, ainsi que de tout service ou application hébergé dans l'environnement cloud.
- **La sécurité du réseau** : désigne les outils, les technologies et les processus utilisés pour protéger le réseau et l'infrastructure critique contre les cyberattaques et les activités malveillantes. Elle inclut un ensemble de mesures préventives et défensives conçues pour refuser tout accès non autorisé aux ressources et aux données.
- **La sécurité de l'IoT** : est une subdivision de la cybersécurité qui couvre la protection, la surveillance et la neutralisation des menaces ciblant l'(IOT) et le réseau de ces terminaux connectés qui collectent, stockent et partagent des données via Internet.

3.2.1.2 Différence entre sécurité des informations et sécurité informatique

- **La sécurité de l'information** : elle consiste à protéger un système informatique contre toute violation, intrusion, dégradation ou vol de données au sein du système d'information (serveurs, courriel, données).
- **La sécurité Informatique** : elle consiste à protéger un système informatique contre toute violation, intrusion, dégradation ou vol de données au sein du système informatique.

3.2.1 Les objectifs spécifiques de la sécurité

L'arrivée d'internet et des nouvelles technologies ont permis de développer et d'améliorer de manière considérable la communication. Cependant, ces nouvelles technologies ne sont pas invulnérables, les failles de sécurités sont fréquentes, c'est ainsi que la question de la sécurité des réseaux a pris une place importante dans la société actuelle.

Authentification et identification

L'authentification des services permet de bien assurer qu'une communication est authentique dans les réseaux. On distingue généralement deux types d'authentification :

- L'authentification d'un tiers consiste à prouver son identité
- Et l'authentification de la source des données sert à prouver que les données reçues viennent bien d'un tel émetteur déclaré.

Avec la vulnérabilité constamment liée à l'utilisation des mots de passe, il est important de recourir aux mécanismes très robustes tels que l'authentification par des certificats [ISO9594], des clés publiques [River78] ou à travers des centres de distribution des clés [RFC1510].

La confidentialité

La confidentialité est un service de sécurité qui assure l'autorisation d'une seule personne à prendre la connaissance des données. En général on utilise un algorithme cryptographique de chiffrement des données concernées pour avoir ce service. Si seul les données sont chiffrées, une oreille espionne peut tout de même écouter les informations de l'en-tête, elle peut ainsi, à partir des adresses source et destination, identifier les tiers communicants et analyser leur communication : fréquence des envois, quantité de données échangée, etc. Il y a de protection contre l'analyse de trafic quand en plus de la confidentialité, on garantit l'impossibilité de connaître ces informations.

Protection d'identités

La vérification efficace des événements liés à la sécurité se fonde aussi sur la capacité d'identifier chaque utilisateur. Il est très nécessaire que chaque utilisateur de l'internet ait une identité distincte, qui est une combinaison qui donne le nom de l'utilisateur et possiblement celui de son Pc, de son organisation et son pays. Comme nous l'avons défini avant au niveau de la première catégorie active de la sécurité, la connaissance de ces informations par un tiers malveillant peut être considérée à la vie privée des usagers.

Contrôle d'accès

La demande d'accès distant sécurisé vers les réseaux privés des entreprises a poussée à la majorité des entreprises à adapter des solutions de sécurité basées sur des points d'accès situés

aux frontières des réseaux privés. Ces points d'accès sont aussi très intéressants dans le sens où ils constituent un point unique et la sécurité peut être imposée. Ils donnent des renseignements de trafic, des statistiques sur ce trafic, et encore toutes les connexions entre les deux réseaux.

Attitude des entreprises face aux risques

Prendre conscience de la menace et identifier les risques devient important. Les entreprises adoptent, en général un ensemble de mesures préventives parmi lesquelles la gestion et le transfert des risques figurent en bonne place. Le recours à l'assurance constitue l'ultime filet de sécurité des entreprises.

3.2.2 Les différents types d'attaques

Dans cette section, nous allons nous concentrer sur les différents types d'attaques les plus courantes existant sur les appareils mobiles Android, mais également sur les divers types de menaces mettant en danger la sécurité des appareils mobiles. Ces différentes menaces venant généralement de pirates, escrocs, hackers, peuvent perturber le fonctionnement d'un appareil mobile, modifier les données d'un utilisateur et également transmettre des données, comme le ferait un logiciel malveillant les hackers ne manquent pas d'imagination pour mettre à mal la sécurité des utilisateurs et de certaines entreprises.

Les attaques par rebond

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les attaques par rebond (par opposition aux attaques directes), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui.

Les logiciels malveillants

Un logiciel malveillant, c'est un logiciel qui est installé sur un ordinateur sans le consentement de son propriétaire. La famille des logiciels malveillants est très vaste : elle comprend notamment les virus furtifs, qui s'attaquent aux logiciels antivirus pour les rendre incapables de détecter d'autres virus, et les logiciels espions, qui récoltent des informations sur les utilisateurs. Ces logiciels servent à attaquer un système permettant aux hackers d'accéder à l'ordinateur. Les virus macro infectent les fichiers Microsoft et Excel et compromettent les données, tandis que les vers se propagent dans les boîtes emails.

3.2.3 Les techniques d'attaques

Protection par mot de passe

Les attaques de mot de passe constituent l'une des formes les plus courantes de violation des données d'entreprise et personnelles. Une attaque de mot de passe est tout simplement une tentative de vol de mot de passe par un hacker. En 2020, 81 % des violations de données étaient dues à des informations d'identification compromises. Dans la mesure où les mots de passe ne peuvent comporter qu'un nombre limité de lettres et de chiffres, ils deviennent de moins en moins sécurisés.

Attaque Hybride

Les attaques hybrides visent particulièrement les mots de passe constitués d'un mot traditionnel et suivi d'une lettre ou d'un chiffre tel que (marechal6). Il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire. Il existe enfin des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs.

Exemple d'attaques Hybrides

L'ingénierie sociale consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau en demandant de réinitialiser le mot de passe.

Attaque par Réflexion

La technique dite attaque par réflexion (en anglais smurf) est basée sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau.

Attaque par Usurpation d'Adresse IP

L'usurpation d'adresse IP est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

IV Généralités sur les systèmes de détection et de prévention

Définition

Les systèmes de détection et de prévention d'intrusions permettent de repérer et d'empêcher l'intrusion d'un utilisateur malveillant dans un système distribué comme une grille informatique ou un réseau en nuage.

4.1 Présentation des systèmes de détections d'intrusion

Définition

Un système de détection d'intrusion (IDS) est chargé d'identifier les attaques et les techniques et est souvent déployé hors bande en mode écoute seule afin qu'il puisse analyser tout le trafic et générer des événements d'intrusion à partir de trafic suspect ou malveillant.

4.1.1 Les différents types de détection d'intrusion

Host Intrusion Detection Systems (HIDS)

Un HIDS (**Host Intrusion Détection System**) sont les systèmes de détection d'intrusions réseaux, où des systèmes de sécurité des réseaux informatiques utilisés pour se protéger contre les virus, les logiciels espions et les logiciels malveillants et d'autres types de fichiers malveillants.

Network-based Intrusion Detection system (NIDS)

Les NIDS (Network-based intrusion détection system) est un système de détection d'intrusion réseau qui observe le trafic sur une branche du afin d'y repérer des tentatives d'attaques, soit à partir des signatures soit en identifiant les comportements anormaux.

Wireless Intrusion Detection System

Ce type de système de détection d'intrusion permet de détecter et d'avertir sur les attaques spécifiques liées aux réseaux sans-fils.

Système de détection d'intrusion basé sur un protocole PIDS

Un système de détection d'intrusion basé sur un protocole PIDS est principalement implémenté sur un serveur Web. La fonction d'un PIDS est d'examiner le flux de communication entre les différents appareils sur un réseau ainsi que ses ressources en ligne. Il surveille et évalue la transmission des données via HTTP et HTTPS.

4.1.2 Classification des systèmes de détection d'intrusion

Les systèmes de détection d'intrusion peuvent également être classés en deux catégories à savoir actifs et passifs.

IDS actif

Également appelé système de détection et de prévention des intrusions IDPS, un IDS actif examine le trafic à la recherche d'activités suspectes. Il est automatisé pour bloquer les activités malveillantes à l'aide d'adresses IP bloquantes et restreindre l'accès non autorisé aux données sensibles sans intervention humaine.

Détection d'intrusion basée sur les signatures

Un système IDS peut identifier une attaque en la vérifiant pour un comportement ou un modèle spécifique comme des signatures malveillantes, des séquences d'octets.

Détection basée sur la réputation

C'est à ce moment qu'un IDS peut détecter les cyberattaques en fonction de leurs scores de réputation. Si le score est bon, le trafic obtiendra un laissez-passer, mais si ce n'est pas le cas, le système vous informera immédiatement pour agir.

SNORT

Protégez votre réseau avec un puissant logiciel de détection open source - Snort. Cet IPS utilise un ensemble de règles pour définir les activités malveillantes sur le réseau et trouver des paquets pour générer des alertes pour les utilisateurs.

IDS passif

Contrairement à un IDS actif qui a la capacité de bloquer les adresses IP face à une activité suspecte, un IDS passif ne peut qu'alerter l'administrateur pour une enquête plus approfondie après avoir détecté une activité suspecte.

Avantage des systèmes de détection d'intrusion

- Pouvoir surveiller des événements locaux jusqu'au host, détecter des attaques qui ne sont pas vues par NIDS
- Le trafic réseau est crypté lorsque les sources des informations des host-based sont générées avant d'arriver à destination.

Inconvénients des systèmes de détection d'intrusion

- NIDS ne peut pas analyser des informations chiffrées (cryptées). Ce problème a lieu dans les organisations utilisant le VPN.
- Il est difficile à traiter tous les paquets circulant sur un grand réseau. De plus il ne peut pas reconnaître des attaques pendant le temps de haut trafic.

4.2 Présentation des systèmes de prévention d'intrusion

Définition

Un système de prévention des intrusions (IPS) est une forme de sécurité réseau qui sert à détecter et prévenir les menaces identifiées. Les systèmes de préventions des intrusions surveillent en permanence votre réseau, recherchant les éventuels actes de malveillance et capturent des informations à leur sujet. L'IPS signale ces événements aux administrateurs du système et prend des mesures préventives, telles que la fermeture des points d'accès et la reconfiguration des firewalls pour empêcher de futures attaques.

Les administrateurs de sécurité de réseau ont besoin d'aide en ce qui concerne la surveillance du trafic. Il y a de nouvelles menaces chaque jour, et même la plupart des systèmes de sécurité de réseau de haute technologie ne peuvent pas prédire les virus les plus récents. Cependant, les systèmes de prévention des intrusions travaillent constamment à résoudre les comportements suspects sur les réseaux. Utilisation d'un système de prévention d'intrusion permet d'éliminer le trafic et les pirates indésirables.

4.2.1 Les différents types de système de préventions d'intrusions

Intrusion Prevention Network-Based System

Pour la sécurité du réseau, un système de prévention d'intrusion basée sur le réseau (PIN) dispose d'un réseau, à la recherche d'activités suspectes à travers une analyse de données de protocole. Un NIPS identifie et bloque les attaques sur le réseau.

Système de prévention des intrusions basé sur l'hôte (HIPS)

Ce logiciel réside sur l'ordinateur client ou le serveur et surveille les événements et les fichiers sur le dispositif.

Systèmes de prévention des intrusions sans fil

Comme un NIPS, le système de prévention des intrusions sans fil (WIPS) cherche trafic suspect en évaluant les protocoles réseau. Cependant, un WIPS surveille un réseau sans fil. Un WIPS utilise couramment un appareil qui surveille les activités non autorisées, comme l'abus de points d'accès. Par exemple, il protège contre quelqu'un d'autre en utilisant votre réseau sans fil pour obtenir de l'information privée. Un WIPS empêche contre les intrus et travaille pour démasquer les criminels, empêchant ainsi d'autres attaques.

La détection d'intrusion basée sur noyau KIPS

Les KIPS (Kernel Intrusion Prévention Système) leur particularité est de s'exécuter dans le noyau d'une machine pour y bloquer toute activité suspecte. Ils peuvent également interdire l'OS d'exécuter un appel système qui ouvrirait un Shell de commandes. Puisqu'un KIPS analyse les appels systèmes ils ralentissent l'exécution c'est pour quoi ils sont moins utilisés.

Avantage des systèmes de préventions d'intrusion

- Supprimera ou remplacera tout contenu malveillant rester sur le réseau suite à une attaque.
- Mettra fin à la session TCP qui est exploitée et bloquer l'adresse IP source ou le compte utilisateur fautif pour empêcher l'accès non éthique à toute application, hôte cible ou ressource réseau.

Inconvénients des systèmes de préventions d'intrusions

- Ils bloquent toute activité qui lui semble suspect, mais n'étant pas fiable à 100% donc ils ne bloquent pas tous les trafics ils bloquent quelques-uns.
- Ils laissent parfois passer certaines attaques sans les repérés et permettent donc aux pirates d'attaques d'un PC.

4.2.2 La différence entre IPS et IDS

La différence entre l'IPS et l'IDS est l'action prise lorsqu'un incident potentiel est détecté.

- Un IPS est un système de prévention des intrusions qui contrôlent l'accès à un réseau informatique et le protègent contre les abus et les attaques. Ces systèmes sont conçus pour surveiller les données d'intrusion et prendre les mesures nécessaires pour éviter qu'une attaque ne se déclenche.
- Un IDS est un système de détection des intrusions qui n'est pas conçus pour bloquer les attaques. Ils se contentent de surveiller le réseau et d'envoyer des alertes aux administrateurs si une menace potentielle est détectée.

4.3 Choix de la solution

Pour la supervision du trafic réseau au niveau des entreprises ou des sociétés, nous avons choisi PFSENSE comme étant un outil excellent à mettre en place.

Notre choix s'est basé sur les points forts de ce pare-feu notamment sa haute disponibilité (HA) qui permet aux infrastructures ou bien à un service d'être joignable il possède une interface graphique qui est facile à configurer et facilite la tâche aux administrateurs réseaux afin d'effectuer toutes les configurations possibles et d'éviter des attaques.

4.3.1 La sécurité améliorée

Pfsense est un système IPS et IDS qui contribue à améliorer la posture de sécurité de votre organisation en vous aidant à détecter les vulnérabilités, les attaques, et les empêcher d'infiltrer vos systèmes, appareils connectés aux réseaux.

4.3.2 Automatisation des tâches

L'utilisation des solutions IDS et IPS permettent d'automatiser les tâches de sécurité. Les systèmes vous aideront à automatiser ces tâches pour vous libérer du temps consacré à la croissance de votre entreprise. Cela réduit non seulement les efforts, mais également les coûts.

4.3.3 La conformité aux règles

IDS et IPS vous aident à protéger les données de vos clients et de votre entreprise et vous assistent lors des audits. Il vous permet de respecter les règles de conformité et d'éviter les sanctions.

4.3.4 Les raisons de choix de solution

Pfsense est un excellent pare-feu et dans certains cas aussi il se comporte comme un routeur donc il est le pare-feu le plus important pour les entreprises pour :

Sa force

Pfsense possède de nombreuses fonctionnalités et capacités avancées qui garantissent qu'il suit toujours les règles par défaut ou personnalisées. Il filtre également le trafic séparément, qu'il provienne de votre réseau interne d'appareils ou de l'Internet ouvert, vous permettant de définir des règles et des politiques différentes pour chacun.

Sa flexibilité

Étant donné que le pare-feu pfsense vous permet d'ajouter et d'intégrer des fonctionnalités supplémentaires sous forme de code, il est suffisamment flexible pour fonctionner à la fois comme pare-feu de base et comme système de sécurité complet.

Avec pfsense, vous pouvez inclure la détection et la prévention des intrusions IPS / IDS pour intercepter les pirates qui tentent d'accéder à votre réseau, ainsi que le blocage de liste de masse, où vous introduisez une base de données de sites infestés de logiciels malveillants connus, adresses IP malveillantes et sites de pirates informatiques au cas où il y aurait une intrusion.

Il est Open-Source

C'est un logiciel dont l'intégralité du code est à portée de main au public pour l'examiner et le modifier sans se soucier de la violation du droit d'auteur. Le logiciel open source est une initiative publique collaborative, où toute personne qualifiée peut contribuer à l'amélioration du logiciel et faire vérifier son travail par d'autres pour la qualité et l'authenticité.

CHAPITRE III : MISE EN OEUVRE DE LA SOLUTION

4.4 Présentation de la solution retenue

Pfsense est l'un des pare-feux les plus utilisés dans les entreprises pour sa fiabilité et son efficacité liés aux besoins et la sécurisation des données. C'est un système d'exploitation orienté professionnel, à la fois dans l'environnement domestique avec des utilisateurs avancés et dans les petites et moyennes entreprises pour diviser efficacement leur réseau et disposer de certains services.

Contrairement aux autres pare-feu, Pfsense possède une interface graphique complète et intuitive, permettant aux administrateurs de bien gérer/configurer les options possibles. C'est donc un système d'exploitation très fiable pour les entreprises car il consomme très peu de ressources.

Un autre de ces points forts sont les mises à jour continues que nous avons, à la fois du côté du système d'exploitation de base, ainsi que de tous les packages que nous pourrions installer en plus. Dans un pare-feu exposé à Internet, il est très important d'avoir des mises à jour pour éviter les failles de sécurité qui pourraient être trouvées.

Avec la possibilité d'installer des logiciels supplémentaires, nous pourrions disposer d'un puissant IDS / IPS (système de détection et de prévention des intrusions) tel que Snort ou Suricata et aussi, installer une troisième carte pour la DMZ. Nous pourrions filtrer les paquets rapidement de façons très avancées, en fonction du matériel, nous pourrions donc avoir des bandes passantes supérieures à 10 gbps. Pfsense dispose d'une part d'un pare-feu puissant pour atténuer et ou bloquer les attaques Dos et DDoS.

4.4.1 Architecture de Solution

Le firewall Pfsense est un pare-feu open source basée sur le système d'exploitation **FreeBSD**. Sa fonction est d'assurer la sécurité d'un périmètre. Il comporte l'équivalent libre des outils et services utilisés sur des routeurs propriétaires.

En plus du pare-feu, il offre des fonctionnalités comme par exemple :

- Authentification RADIUS

- Translation d'adresses (NAT)
- Serveur DNS
- Serveur DHCP
- Portail captif
- VPN IPsec, OpenVPN

Installation de Pfsense avec 3 interfaces réseau :

- Interface **DMZ**
- Interface **LAN**
- Interface **WAN**

Ce qu'il vous faut :

- Oracle VM Virtual Box ou VMWare (nous utiliserons ce dernier)
- Firewall pfsense

4.4.2 Déploiement

Pfsense fonctionne sur une architecture de 86 bits, mais est compatible avec les processeurs 64 bits les plus récents. Il peut être installé sur quasiment toutes les plates-formes cloud comme amazon. Pour procéder à l'installation de Pfsense, il est nécessaire de télécharger le fichier au format ISO

Il faut utiliser la bonne version de l'ISO en fonction de votre processeur.

Indépendamment du nombre de processeurs et de cœurs (nous recommandons 1 CPU et 4 cœurs) avec au minimum une (RAM de 4 Go), il faut également ajouter une deuxième carte réseau, car nous aurons le WAN Internet et le LAN.

Nous installerons la solution et ensuite la configuration de Pfsense.

Dans notre travail nous utiliserons des machines hôtes afin de pouvoir communiquer avec le serveur et ensuite VMWare pour le déploiement.

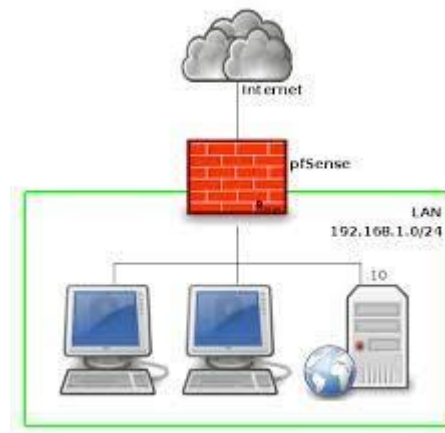


Figure 8 Déploiement et fonctionnement de pfSense

PfSense utilise un pare-feu SPI (Stateful Packet Inspection) basé sur certaines règles. Nous pouvons filtrer les paquets rapidement de manière très avancée, en fonction du matériel, et pouvoir atteindre des bandes passantes supérieures à 10 Gbps. Grâce à l'interface utilisateur, nous pourrions créer des « alias » pour avoir des groupes d'adresses IP et de ports, pour les appliquer ultérieurement aux règles, et de cette façon, ne pas avoir des centaines de règles dans le pare-feu, il est très important de savoir quoi nous filtrons et maintenons les règles correctement mises à jour.

4.4.3 Présentation de Suricata

Suricata est un logiciel open source de détection d'intrusion (IDS), de prévention d'intrusion (IPS), et de supervision de sécurité réseau (NSM). Il est développé par la fondation OISF (Open Information Security Foundation). Suricata permet l'inspection des Paquets plus en profondeur.

4.4.4 Présentation de Snort

Le système de détection et de prévention des intrusions (IDS/IPS) Snort est capable d'effectuer une analyse du trafic et un enregistrement des paquets sur les réseaux IP. Il effectue l'analyse des protocoles, la recherche et la mise en correspondance des contenus.

4.4.5 Présentation de OSSEC

OSSEC est un HIDS (Host Intrusion Détection System). Son rôle est de détecter les comportements anormaux sur une machine. Il collecte les infos qui lui sont envoyées par les

équipements connecté. Il utilise des signatures pour détecter les anomalies. Un agent est installé sur chaque machines. Nous allons vous expliquer comment mettre celui-ci en place dans les lignes suivantes :

Tableau 3 Comparaison de solution

Solutions	Points fort	Point Faible
Pfsense	<ul style="list-style-type: none"> -Filtrage des sources de destinations au - peut niveau des adresses IP, protocole et UDP TCP -Capacité à limiter le nombre de sécurité ou fait règle par règle. des recherches -Pfsense utilise pf0 pour filtrer un système d'exploitation qui initie la connexion utilisant des systèmes FreeBSD 	<ul style="list-style-type: none"> La mauvaise configuration port causer des problèmes -Mettre en danger en ayant pas connexion trop métriser la
SURICATA	<ul style="list-style-type: none"> -Analyse protocolaire -Interaction avec les transferts de fichiers -performance élevé 	<ul style="list-style-type: none"> -Mono serveur -Vulnérabilités des sondes Taux positifs
SNORT	<ul style="list-style-type: none"> -Base de signature importante -Documentation riche -Couplage avec d'autres outils -Moteur de détection Mis à jour régulière de la signature 	<ul style="list-style-type: none"> -Vulnérabilités des ondes -nombreuses fonctionnalités payantes -Avoir des connaissances en sécurité
OSSEC	<ul style="list-style-type: none"> -Vérification de l'intégrité de la solution -Surveillances de journal -Détection de rootkit 	<ul style="list-style-type: none"> -Manques informations sur les alertes -vulnérabilités des sondes

4.5.6 Outil technologie mise en œuvre

Pour installer pfsense nous aurons besoin de télécharger le fichier iso dans le site officiel de pfsense et crée une machine virtuelle dans VMware

Nous allons configuration des protocoles SMTP, IMAP, et POP3 pour la notification par Email sur pfsense. Avant d'établir cette notification il faudra configurer quelques protocoles qui nous seront indispensable et nous permettra de configurer la notification par E-mail. Tout d'abord la machine virtuelle utilisée est Debian 11.

Configurer le Protocole DNS et vérifier s'il fonctionne après en utilisant nslookup.

Configuration de postfix qui est un serveur de messagerie électronique qui permet d'accéder aux mails après configuration.

Configuration de Dovecot qui est un serveur IMAP et POP3 destiné à fonctionner sur plusieurs systèmes d'exploitation comme (Linux/UNIX, FreeBSD, MacOS).

Faire en sorte que la machine hôte et le serveur puissent communiquer.

Après avoir fini de configurer les services cités on entre dans l'interface graphique de pfsense et on clique sur Advanced.

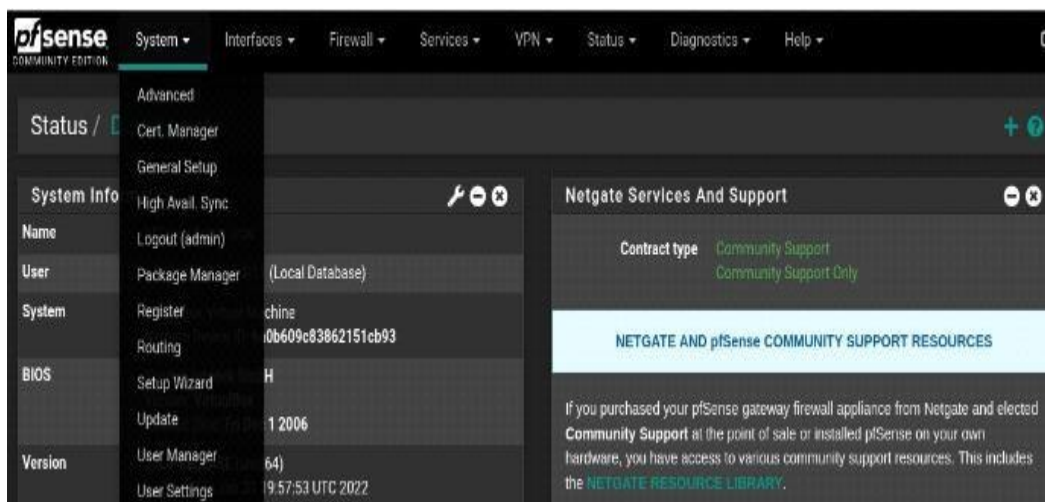


Figure 9 Clique avec Advanced

Après cela on appuie sur Notifications puis on renseigne les champs vides. L'adresse IPv4 du serveur SMTP et le port utilisé pour envoyer les notifications, ainsi que le délai de connexion.

System / Advanced / Notifications

Admin Access Firewall & NAT Networking Miscellaneous System Tunables **Notifications**

General Settings

Certificate Expiration ☒ Enable daily notifications of expired and soon-to-expire certificates.
When enabled, the firewall will check CA and Certificate expiration times daily and file notices when expired or soon-to-expire entries are detected.

Ignore Revoked ☐ Ignore notifications for revoked certificates.
When enabled, the firewall will NOT check expiring for revoked (at least once) certificates.

Certificate Expiration Threshold 27
The number of days at which a certificate lifetime is considered to be expiring soon and worthy of notification. Default is 27 days.

E-Mail

Disable SMTP ☐ Disable SMTP Notifications
Check this option to disable SMTP notifications but preserve the settings below. Some other mechanisms, such as packages, may need these settings in place to function.

E-Mail server 192.168.1.11
This is the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent.

SMTP Port of E-Mail server 25
This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps).

Connection timeout to E-Mail server 10
This is how many seconds it will wait for the SMTP server to connect. Default is 20s.

Secure SMTP Connection ☐ Enable SMTP over SSL/TLS

Figure 10 Remplir les espaces vides

Toujours sur le renseignement des champs disponibles en mettant les deux emails créer et en mettant le nom de celui qui recevra l'email ou la notification puis cliquez sur TEST SMTP settings si c'est bien configuré vous verrez la notification sur Thunderbird qui vous permettra d'entrer les deux emails d'envoyer des emails a ces deux utilisateurs.

Validate SSL/TLS ☒ Validate the SSL/TLS certificate presented by the server.
When disabled, the server certificate will not be validated. Encryption will still be used if available, but the identity of the server will not be confirmed.

From e-mail address laye@pfsense.net
This is the e-mail address that will appear in the from field.

Notification E-Mail address queye@pfsense.net
Enter the e-mail address to send email notifications to.

Notification E-Mail auth username (optional) queye
Enter the e-mail address username for SMTP authentication.

Notification E-Mail auth password [masked] [masked]
Enter the e-mail account password for SMTP authentication. Confirm

Notification E-Mail auth mechanism PLAIN
Select the authentication mechanism used by the SMTP server. Most work with PLAIN, some servers like Exchange or Office365 might require LOGIN.

Test SMTP Settings [Test SMTP Settings](#)
A test notification will be sent even if the service is marked as disabled. The last SAVED values will be used, not necessarily the values entered here.

Figure 11 Remplir les champs vides

Comme on le voit ici le message a été envoyé avec succès.



Figure 12 Confirmation de bonne configuration

Alors vérifions si nous avons reçus la notification par e-mail envoyé par pfsense avec Thunderbird.



Figure 13 Interface de Thunderbird

Après avoir cliqué sur E-mail on entre les informations des utilisateurs et leurs emails respectifs.

Figure 14 Remplir les informations

Avec une notification en couleur verte Thunderbird nous montre que cet utilisateur est bien enregistré parmi dans la base de données.

✓ The following settings were found by probing the given server:

Manual configuration

INCOMING SERVER

Protocol: IMAP

Hostname: debian.pfsense.net

Port: 143

Connection security: None

Authentication method: Normal password

Username: laye

OUTGOING SERVER

Hostname: debian.pfsense.net

Port: 25

Connection security: None

Authentication method: Normal password

Username: laye

Advanced config

Re-test Cancel Done

Figure 15 Enregistrement de l'utilisateur dans la base

Warning!

Incoming settings:

debian.pfsense.net does not use encryption.

Insecure mail servers do not use encrypted connections to protect your passwords and private information. By connecting to this server you could expose your password and private information.

Outgoing settings:

debian.pfsense.net does not use encryption.

Insecure mail servers do not use encrypted connections to protect your passwords and private information. By connecting to this server you could expose your password and private information.

Thunderbird can allow you to get to your mail using the provided configurations. However, you should contact your administrator or email provider regarding these improper connections. See the [Thunderbird FAQ](#) for more information.

☒ I understand the risks

Change Settings Confirm

Figure 16 Domaine du serveur entrant et sortant

Le compte a été créé avec succès. On clique sur le bouton « finish » pour terminer.

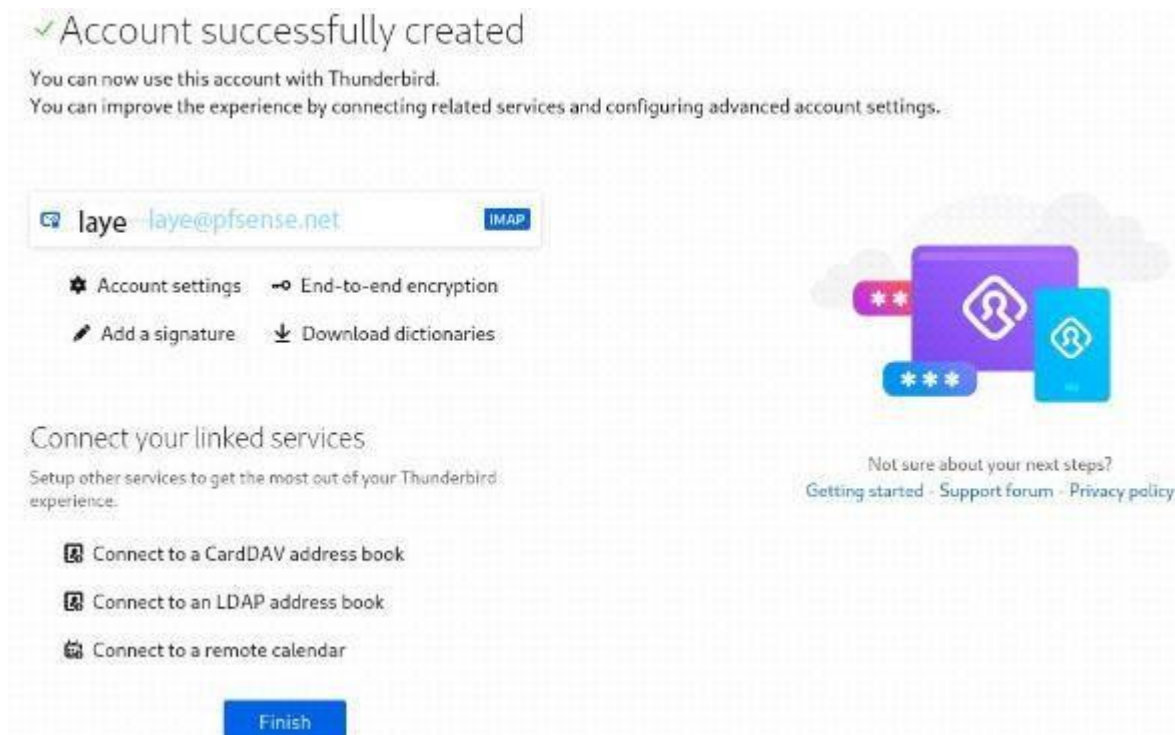


Figure 17 Compte créer

On passe à l'étape de création de l'e-mail du deuxième utilisateur.

The screenshot displays the 'Set Up Your Existing Email Address' form. The title is followed by instructions: 'To use your current email address fill in your credentials. Thunderbird will automatically search for a working and recommended server configuration.' The form contains three input fields: 'Your full name' with the value 'gueye', 'Email address' with the value 'gueye@pfsense.net', and 'Password' with masked characters. Each field has an information icon to its right. Below the password field is a checked checkbox labeled 'Remember password'. To the right of the form is a cartoon illustration of a blue, blob-like character with a single eye, wearing a blue shirt and holding a small blue object.

✓ The following settings were found by probing the given server:

Manual configuration

INCOMING SERVER

Protocol: IMAP

Hostname: debian.pfsense.net

Port: 143

Connection security: None

Authentication method: Normal password

Username: gueye

OUTGOING SERVER

Hostname: debian.pfsense.net

Port: 25

Connection security: None

Authentication method: Normal password

Username: gueye

[Advanced config](#)

Re-test Cancel Done

Figure 18 Enregistrement d'un utilisateur dans la base

✓ Account successfully created

You can now use this account with Thunderbird.
You can improve the experience by connecting related services and configuring advanced account settings.

gueye gueye@pfsense.net IMAP

⚙ Account settings 🔒 End-to-end encryption
✍ Add a signature ⬇ Download dictionaries

Connect your linked services
Setup other services to get the most out of your Thunderbird experience.

🔗 Connect to a CardDAV address book
🔗 Connect to an LDAP address book
🔗 Connect to a remote calendar

Finish

Not sure about your next steps?
[Getting started](#) · [Support forum](#) · [Privacy policy](#)

Figure 19 Compte créer

Voici les e-mails et les notifications que pfsense nous a envoyé.



Figure 20 Envois email via pfsense

Fin de la configuration et la notification par E-mail avec pfsense.

Configuration de SNORT sur pfsense avec Kali linux.

Installation de Snort pour la détection d'intrusion avec alerte. Tout d'abord veuillez-vous authentifier avant d'accéder à l'interface web de pfsense où vous allez cliquer sur « System > Package Manager »

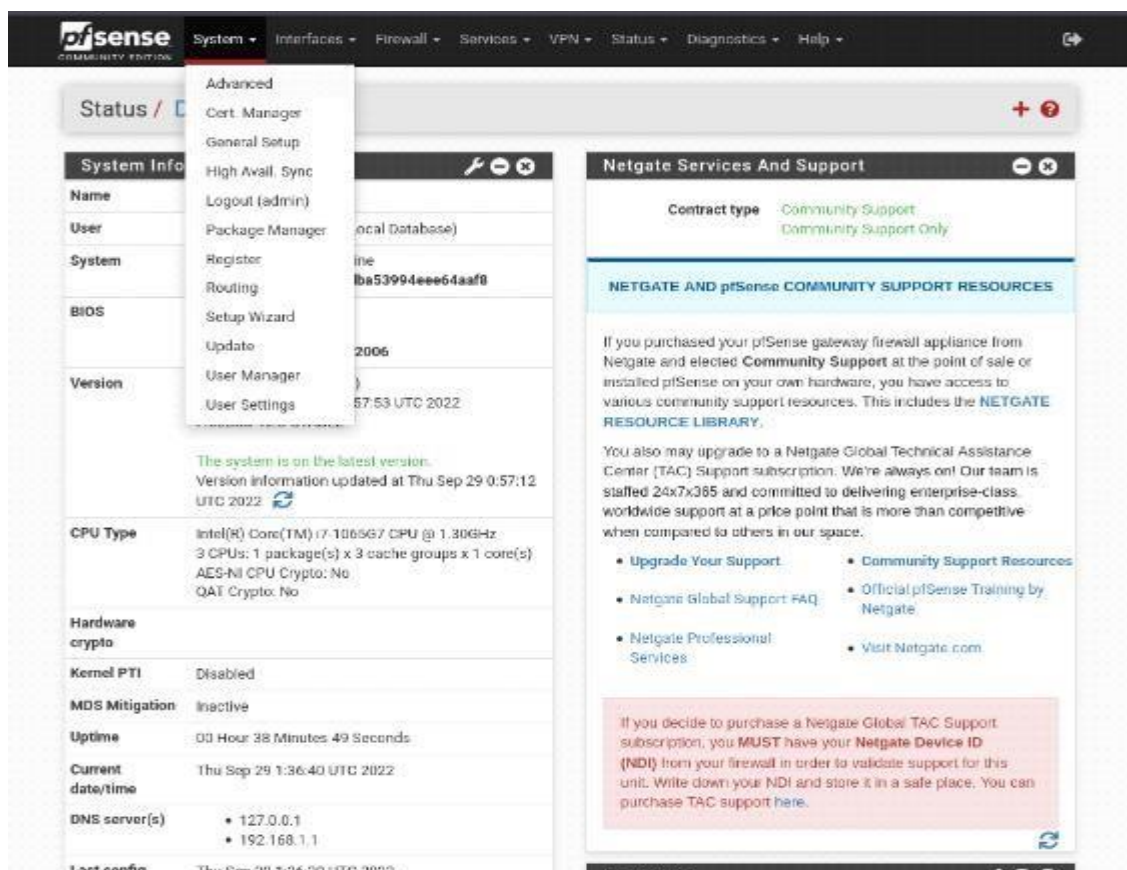


Figure 21 Début de l'installation de Snort

Puis ensuite sur la barre de recherche on tape le mot SNORT puis on procède à l'installation de SNORT.

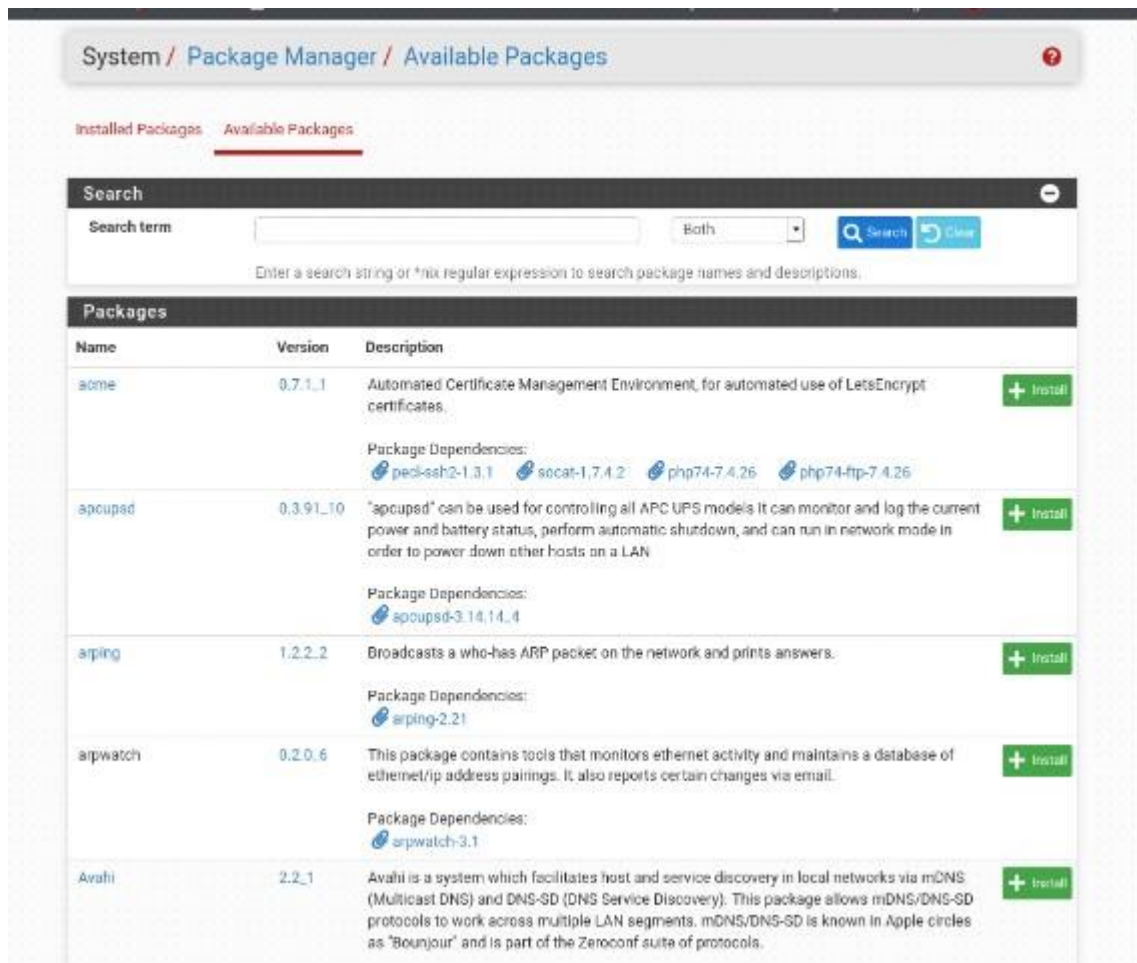


Figure 22 Recherche et installation de snort

Après avoir fait la recherche de SNORT dans la barre de recherche on clique sur Install pour l'installation. PfSense propose la dernière version de SNORT donc il suffit juste de l'installer.

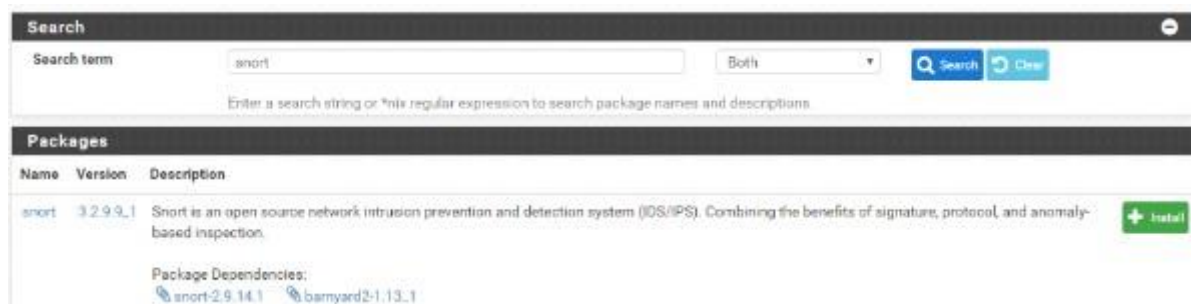


Figure 23 Procédure d'installation de snort

Voici SNORT après avoir fini son installation il figure parmi les listes des paquets installés.

pfSense COMMUNITY EDITION System • Interfaces • Firewall • Services • VPN • Status • Diagnostics • Help •

System / Package Manager / Installed Packages

Installed Packages Available Packages

Name	Category	Version	Description	Actions
✓ mailreport	mail	3.6.3_3	Allows you to setup periodic e-mail reports containing command output, and log file contents.	
✓ snmptt	net-mgmt	1.0.0_1	SNMPTT (SNMP Trap Translator) is an SNMP trap handler written in Perl for use with the Net-SNMP. Easy to setup and use. Package Dependencies: snmptt-1.4.2_1	
✓ snort	security	4.1.6	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.20	
✓ suricata	security	6.0.4_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF. Package Dependencies: suricata-6.0.4	

= Update ✓ = Current
 = Remove = Information = Reinstall
 No new version available.
 Package is configured but not (fully) installed or deprecated

Figure 24 Installation de snort

Sur les menus qui s'affichent dans l'interface web cliquer sur « Services vous verrez les paquets déjà installés pour y accéder et cliquer sur SNORT.

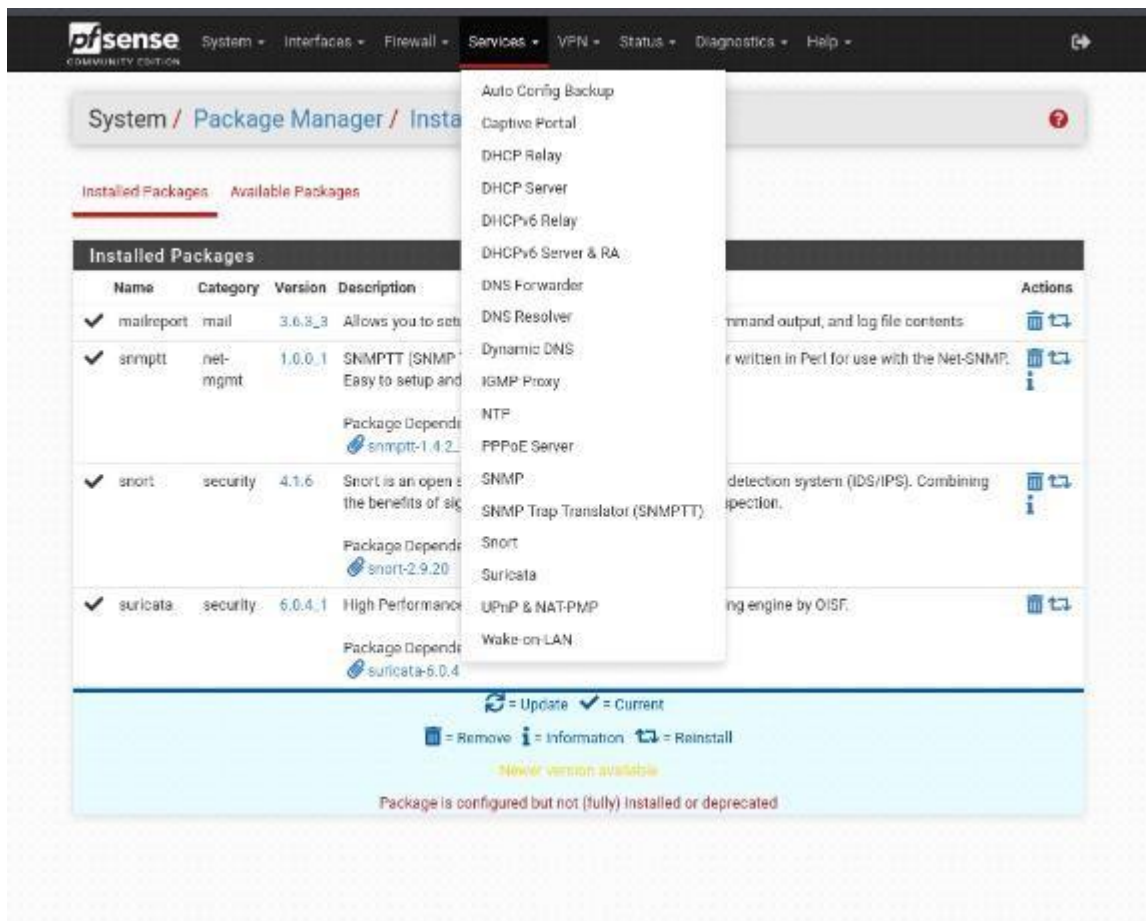


Figure 25 Début de la configuration

Avant d'ajouter une interface Snort il faudra configurer Snort dans « Global Setting » avec un « Oinkcode » qui se trouve dans leur site et pour y insérer le hash généré.

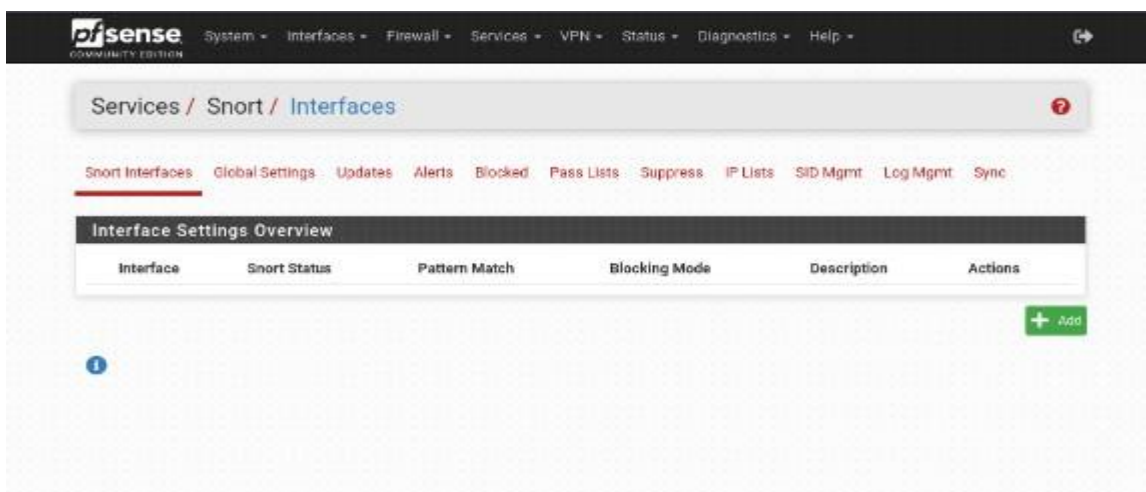


Figure 26 Accès aux paramètres globaux

Après avoir cliqué sur Services Snort Global Settings avant de commencer l'installation veuillez-vous inscrire sur Snort car nous auront besoin d'un code générer directement dans votre compte Snort.

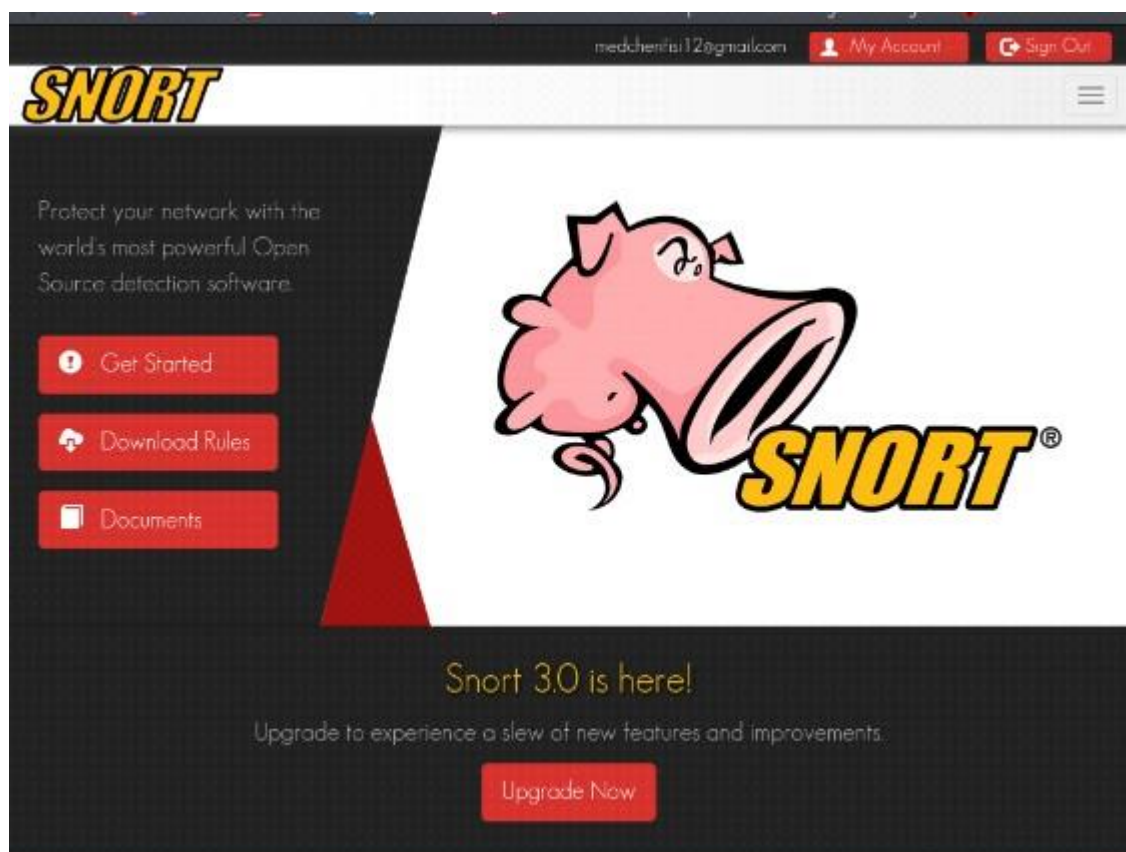


Figure 27 Création d'un compte Snort

Voici après avoir créé le compte connectons-nous avec ce compte puis accéder à votre oinkcode.



Figure 28 Connections dans snort

Le Oinkcode permet de générer un code permettant de configurer de Snort dans l'interface web de pfsense.



Figure 29 Générons un « Oinkcode »

Ce code générer nous sera utile dans la partie suivante pour la configuration de Snort.

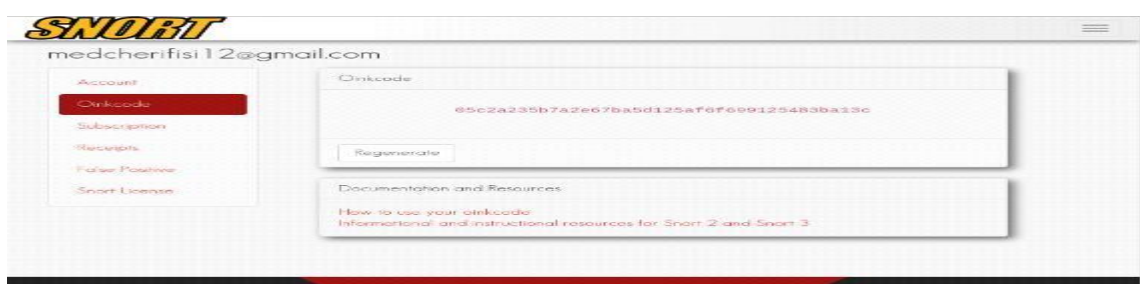


Figure 30 code générer pour pfsense

Copier le Oinkcode qui se trouve au niveau de Snort et le coller ici. La configuration consiste à activer quelques options

Services / Snort / Global Settings

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Snort Subscriber Rules

Enable Snort VRT ☒ Click to enable download of Snort free Registered User or paid Subscriber rules

Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)

Snort Oinkmaster Code
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☒ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open ☒ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐ Click to enable download of Emerging Threats Pro rules

Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

Enable OpenAppID ☐ Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.

Figure 31 Début de la configuration

FEODO Tracker Botnet C2 IP Rules

Enable FEODO Tracker Botnet C2 IP Rules ☐ Click to enable download of FEODO Tracker Botnet C2 IP rules

Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an banking Trojan used by cybercriminals to commit banking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet.

Rules Update Settings

Update Interval Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Update Start Time
Enter the rule update start time in 24-hour format (HH-MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:06 and choosing 12 Hours for the interval, the rules will update at 00:06 and 12:06 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

Hide Deprecated Rules Categories ☐ Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

Disable SSL Peer Verification ☐ Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

General Settings

Remove Blocked Hosts Interval Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.

Remove Blocked Hosts After Deinstall ☐ Click to clear all blocked hosts added by Snort when removing the package. Default is checked.

Keep Snort Settings After Deinstall ☒ Click to retain Snort settings after package removal.

Startup/Shutdown Logging ☐ Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Téléchargeons les mises à jour de Snort afin qu'il prenne en compte les modifications effectuées.

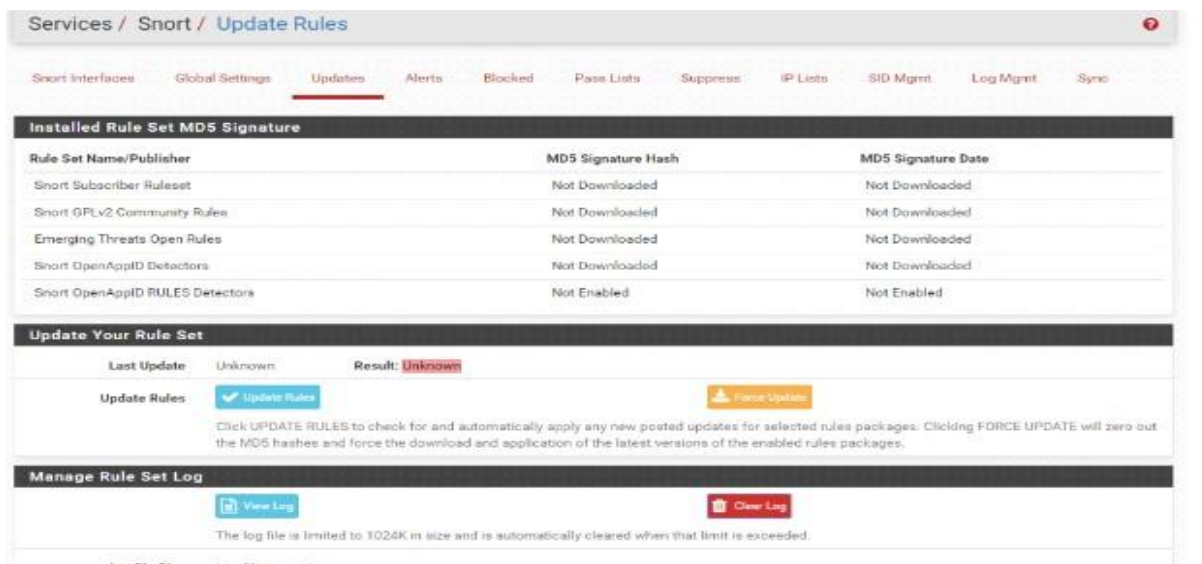


Figure 32 téléchargement des mises à jour de Snort

Comme on peut le voir sur cette image ci-dessous les mises à jour ont bien été télécharger.

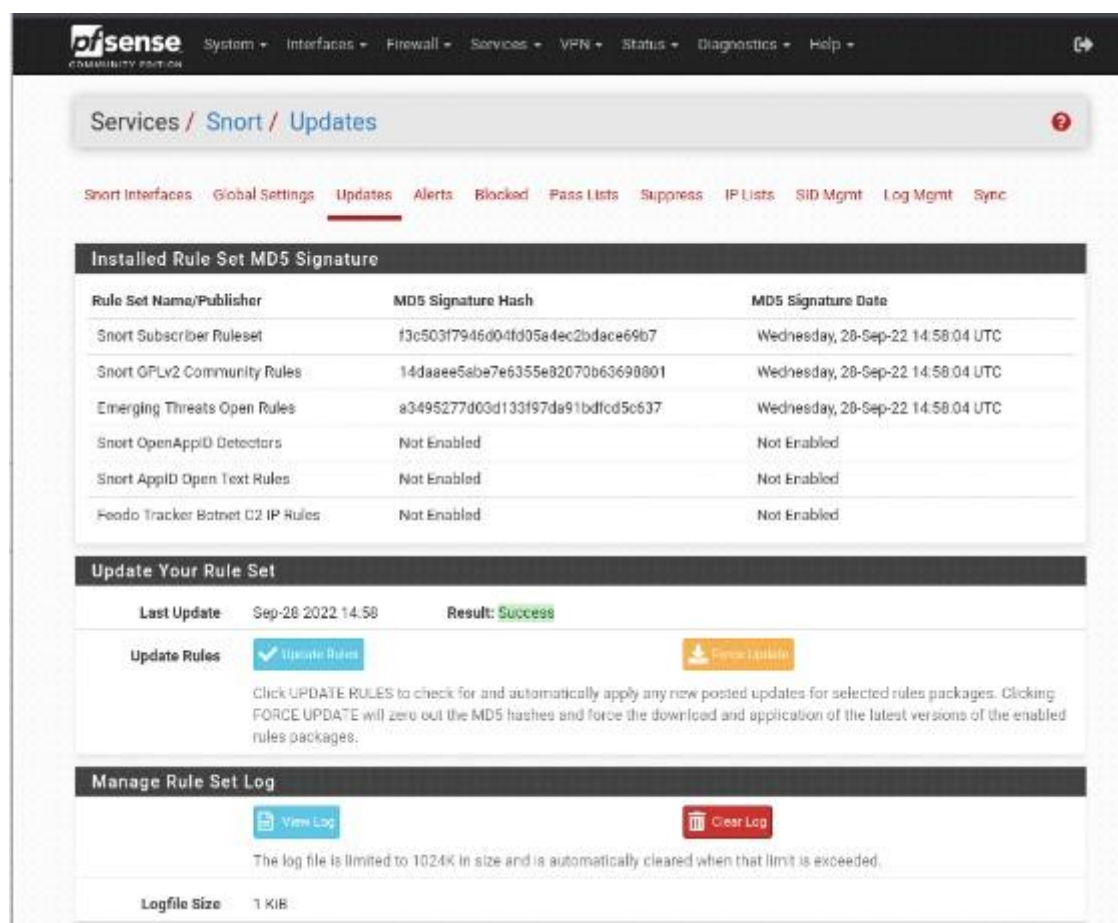



Figure 33 Téléchargements effectuer



System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Services / Snort / WAN - Interface Settings

[Snort Interfaces](#)
[Global Settings](#)
[Updates](#)
[Alerts](#)
[Blocked](#)
[Pass Lists](#)
[Suppress](#)
[IP Lists](#)
[SID Mgmt](#)
[Log Mgmt](#)
[Sync](#)

WAN Settings

General Settings

Enable

☒ Enable Interface

Interface

LAN (em1)

Choose the interface where this Snort instance will inspect traffic.

Description

Interface LAN

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log

☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.

System Log Facility

LOG_AUTH

Select system log Facility to use for reporting. Default is LOG_AUTH.

System Log Priority

LOG_ALERT

Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.

Enable Packet Captures

☐ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file.

Enable Unified2

☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging

Figure 34 Configuration de l'interface et création des alertes

66

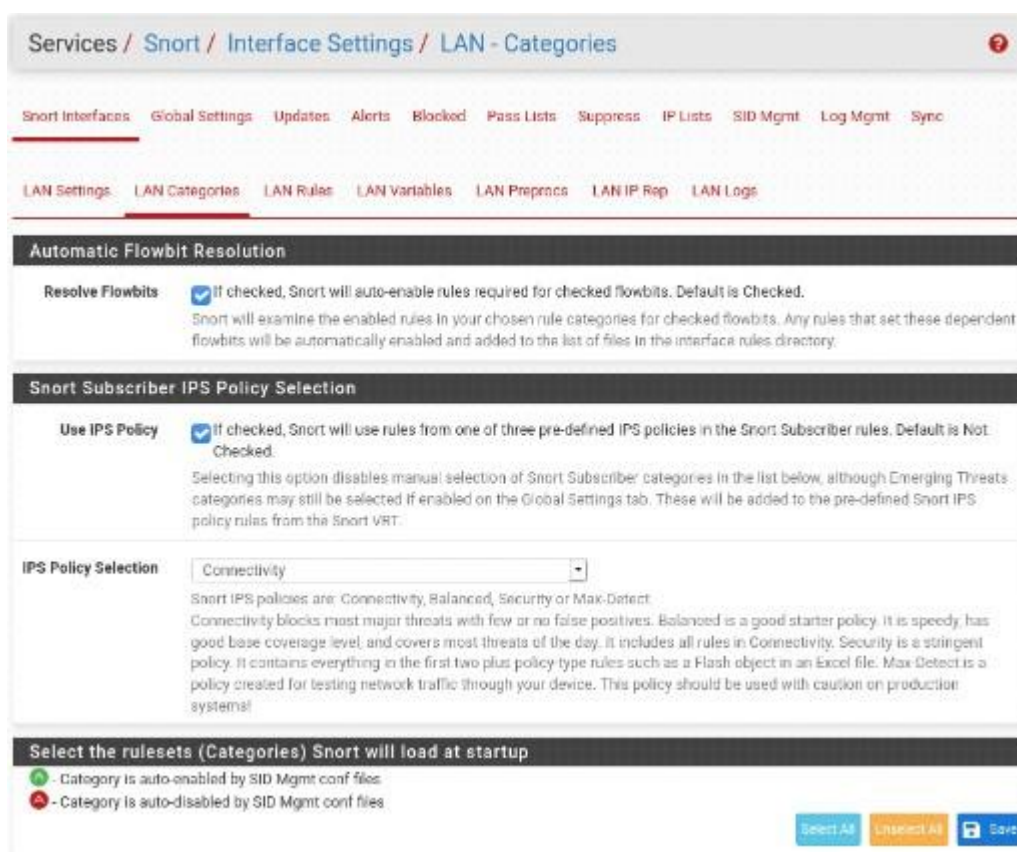


Figure 35 Clique sur LAN Catégories

Après avoir terminé la configuration on passe à l'enregistrement. On valide, et on retourne à la liste des interfaces de Snort pour appuyer sur **Start**.



Figure 36 Configurer de Snort

Nous utiliserons Kali linux et nmap permet de scanner et de tester des intrusions qui sont compatible avec Snort.

```

root@kali:~# nmap -T4 -A -v 192.168.1.17
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-29 03:57 CEST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:57
Completed NSE at 03:57, 0.00s elapsed
Initiating NSE at 03:57
Completed NSE at 03:57, 0.00s elapsed
Initiating NSE at 03:57
Completed NSE at 03:57, 0.00s elapsed
Initiating ARP Ping Scan at 03:57
Scanning 192.168.1.17 [1 port]
Completed ARP Ping Scan at 03:57, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:57
Completed Parallel DNS resolution of 1 host. at 03:57, 0.00s elapsed
Initiating SYN Stealth Scan at 03:57
Scanning pfSense.home.arpa (192.168.1.17) [1000 ports]
Discovered open port 53/tcp on 192.168.1.17
Discovered open port 80/tcp on 192.168.1.17
Completed SYN Stealth Scan at 03:57, 4.91s elapsed (1000 total ports)
Initiating Service scan at 03:57
Scanning 2 services on pfSense.home.arpa (192.168.1.17)

```

Figure 37 Kali linux pour l'intrusion

Les triangles jaunes signifient qu'il y a eu des attaques ou des intrusions et que pfsense a réussi à les bloqués. Cela veut dire que l'action effectuer ici est une alerte.

Services / Snort / Alerts

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Alert Log View Settings

Interface to Inspect: LAN (em1) Auto-refresh: ☐ Alert lines to display: 500 Save

Alert Log Actions: Download Clear

Alert Log View Filter

5 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-09-29 02:01:28	⚠	3	TCP	Unknown Traffic	192.168.1.20	50422	192.168.1.17	80	119:34	(http_inspect) TOO MANY PIPELINED REQUESTS
2022-09-29 02:01:27	⚠	3	TCP	Unknown Traffic	192.168.1.20	50420	192.168.1.17	80	119:34	(http_inspect) TOO MANY PIPELINED REQUESTS
2022-09-29 02:01:10	⚠	3	TCP	Unknown Traffic	192.168.1.20	50418	192.168.1.17	80	119:34	(http_inspect) TOO MANY PIPELINED REQUESTS
2022-09-29 02:01:08	⚠	3	TCP	Unknown Traffic	192.168.1.20	50416	192.168.1.17	80	119:34	(http_inspect) TOO MANY PIPELINED REQUESTS
2022-09-29 02:00:44	⚠	3	TCP	Unknown Traffic	192.168.1.20	50378	192.168.1.17	80	119:31	(http_inspect) UNKNOWN METHOD

Figure 38 Détection des intrusions avec Pfsense

Fin de la configuration de SNORT

Début de configuration d'un portail captif avec Kali linux.

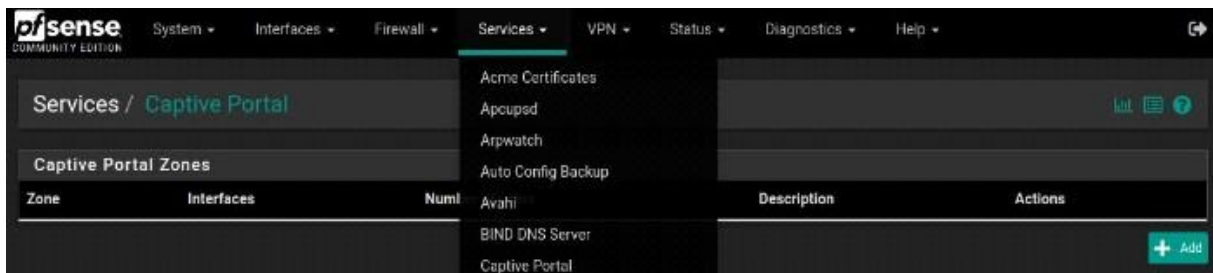


Figure 39 Accès sur captive portail

Après avoir cliquer sur services et captive portail on donne le nom de la zone et sa description puis on sauvegarde.

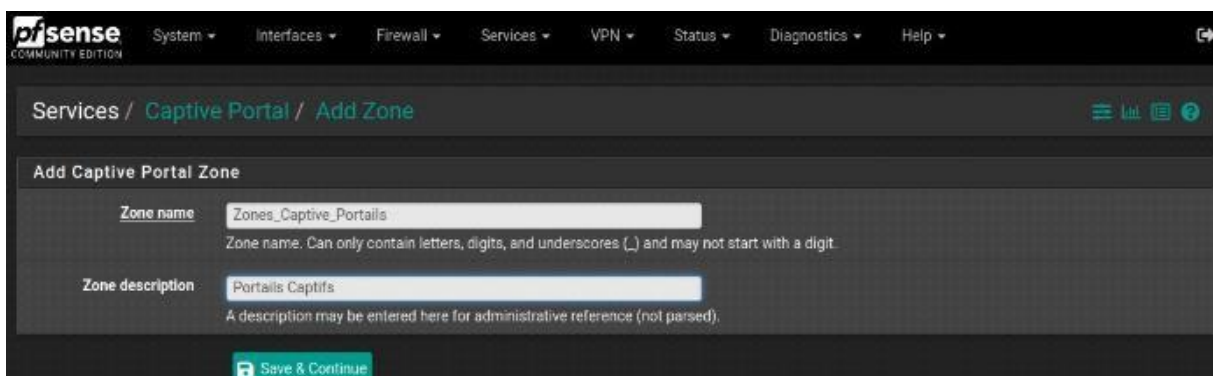
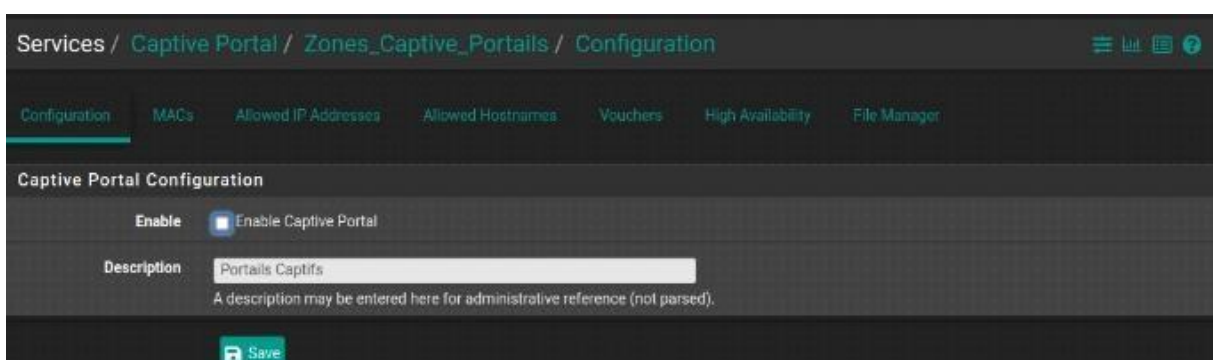


Figure 40 Renseignement des champs vides

Cochons la case **Enable Captive Portail** pour activer le portail captif afin de commencer la configuration.



Après avoir cocher Enable Captive Portail alors on choisit le LAN de pfSense pour continuer.

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal / Zones_Captive_Portails / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

Captive Portal Configuration

Enable ☒ Enable Captive Portal

Description Portails Captifs
A description may be entered here for administrative reference (not parsed).

Interfaces WAN
LAN
Select the interface(s) to enable for captive portal.

Maximum concurrent connections 1
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

Idle timeout (Minutes) 5
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Figure 41 Option LAN pour continuer

CONCLUSION :

Pour garder les équipements réseaux des entreprises à jour et préserver leurs intégrités, les administrateurs de réseaux doivent effectuer des mises à jour régulières afin de garder les données pour les entreprises et les récupérer ultérieurement via les serveurs.

La meilleure des options est la sécurité des systèmes qui convient parfaitement aux entreprises qui ont toujours besoin de sécuriser leurs données et les informations sensibles pouvant les affecter et même donner accès à des intrus pour infecter leurs travaux. La sécurité informatique joue un rôle très important dans l'informatique car elle permet une authentification plus stricte afin d'éviter des attaques et mieux protéger les entreprises.

Les IPS et IDS sont utilisés dans beaucoup d'entreprises car avec les différents types d'attaques qui existent de nos jours ces entreprises ont besoin de beaucoup de protocoles afin d'assurer la sécurité et éviter des brutes forces qui mettra en danger les entreprises concernées.

Ce chapitre nous a permis de mieux comprendre les différents types de réseaux et protocoles, ces services utilisent des dispositifs et des technologies de grandes qualités. Il nous a aussi permis de nous familiariser avec les routeurs, en connaissant ces différents composants, son rôle et de savoir comment établir une liaison distante entre un routeur et son administrateur.

BIBLIOGRAPHIE ET WEBOGRAPHIE :

<https://www.pfsense.org/download/?section=downloads> : Consulté le 01/07/2024 à 21h30mn

<http://labrat.fr/article/installation-de-pfsense.html> : Consulté le 01/07/2024 à 21h40mn

<https://www.osnet.eu/fr/content/pfsense-definitive-guide-tout-sur-pfsense4> : Consulté le 02/07/2024 à 19h00mn

<https://www.memoireonline.com/11/19/11308/Etude-pour-la-securisation-dun-reseau-par-lamise-en-place-dun-pare-feu-open-source-cas-de.html>: Consulté le 21/07/2024 à 19h15mn

<https://fr.wikipedia.org/wiki/FreeBSD>: Consulté le 02/08/2024 à 20h00mn

https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_d%C3%A9tection_d%27intrusion: Consulté le 03/08/2024 à 19h30mn

<https://web.maths.unsw.edu.au/~lafaye/CCM/attaques/methodologie.htm>: Consulté le 07/08/2024 à 20h30mn

