الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière Télécommunication
Spécialité : Réseaux & Télécommunications

Présenté par

SANOGO M'pèrè Moussa
&
MOHAMED VADEL SIDI MOHAMED EL GHALGHAMY Imane

Mise en place d'une sécurité réseau basé sur le pare-feu OPNsense

Proposé par : M.MEHDI Marouane & M. YALAOUI Moussa

Année Universitaire 2022-2023

Remerciement

Nous tenons à exprimer notre profonde gratitude à Allah qui nous a guidé et donné le courage pour mener à bien ce travail.

Nous remercions vivement et chaleureusement monsieur Yalaoui Moussa pour nous avoir assistée, soutenu ainsi que pour l'intérêt qu'il a porté à la réalisation de ce projet.

On remercie également monsieur Mehdi Merouane pour son aide, ses conseils et son orientation durant notre cycle universitaire.

Nous adressons nos sincères remerciements aux membres du jury pour l'examination de notre travail.

Nos remerciements s'adressent à tous ceux qui ont contribués de près ou de loin.

Dédicace

Nous dédions ce travail à nos parents pour leur soutien indéfectible durant nos parcours académiques sans quoi on n'aurait pas pu arriver jusqu'ici.

Nous dédions ce travail également à nos amis, camarades de classe et professeurs du département qui ont beaucoup contribué à notre formation.

ملخص

الإنترنت) ، مما يعني أن **WAN (** شبكة الشركة ، المعروفة باسم شبكة المنطقة المحلية ، هي أساس شبكة المنطقة الواسعة إتقانها شرط لا غنى عنه لمسؤول الشبكة. لضمان حسن سيرها ، من الضروري ضمان حمايتها للقضاء على أي محاولة اقتحام يمكن أن تسبب مشاكل هائلة مثل فشل خوادم الشبكة المحلية مما يؤدي إلى توقف الخدمات التي تقدمها الشبكة المحلية. يعد جدار الحماية أحد الحلول التي يمكن أن تساعد في التغلب على هذه المشكلة. وبالتالي فإن حلنا المقترح هو نظام جدار وهو جدار حماية مفتوح المصدر يقدم ميزات مثيرة للاهتمام. أنشأنا شبكة محلية مكونة من خادم **OPNsense** حماية يسمى مصادقة سمح لنا بمصادقة المستخدمين الذين يريدون الانتقال إلى الإنترنت من خلال بوابة مقيدة ، وهو خادم بريد يضمن بواسطة نشره كنظام لمنع التسلل وكشفه. **OPNsense** تبادل الرسائل داخل الشبكة وتأمين كل شيء باستخدام جدار حماية لقد طبقنا أيضًا بعض قواعد وقيود التصفية لتحسين التحكم في المستخدمين. الاختبارات التي تم إجراؤها في هذا العمل تثبت صحة الحل المقترح.

Résumé

Le réseau d'entreprise communément appelé réseau local LAN est la base du réseau étendu WAN(internet), ce qui fait que sa maîtrise est sine qua non pour un administrateur réseau. Pour assurer son bon fonctionnement il faut s'assurer de sa protection pour faire vouer toute tentative d'intrusion qui peut causer d'énormes problèmes comme la panne des serveurs du réseau local entraînant un arrêt des services offerts par le réseau local.

Le firewall est une des solutions qui peut aider à pallier ce problème. Ainsi notre solution proposée est un système de firewall appelé OPNsense qui est un firewall open source offrant des fonctionnalités intéressantes. Nous avons mis en place un réseau local composé d'un serveur d'authentification qui nous a permis d'authentifier les utilisateurs qui veulent partir sur internet à travers un portail captif, d'un serveur de messagerie qui garantit l'échange des messages au sein du réseau et sécuriser le tout avec le pare-feu OPNsense en le déployant comme un système de prévention et de détection d'intrusion. Nous avons aussi mis en place quelques règles de filtrage ainsi que des restrictions pour mieux contrôler les utilisateurs. Les tests effectués dans ce travail, valide la solution proposée.

Mots clés : LAN, WAN, OPNsense, DNS, zenarmor, zimbra, plugins

Abstract

The corporate network, commonly referred to as the LAN (local area network), is the foundation of the WAN (wide area network), making its mastery a sine qua non for any network administrator. To ensure its smooth operation, it must be protected against any intrusion attempts, which can cause huge problems, such as the failure of LAN servers, leading to a shutdown of LAN services.

The firewall is one of the solutions that can help alleviate this problem. So our proposed solution is a firewall system called OPNsense, an open source firewall offering some interesting features. We set up a local area network consisting of an authentication server to authenticate users wishing to access the Internet via a captive portal, a mail server to guarantee the exchange of messages within the network, and the OPNsense firewall, deployed as an intrusion prevention and detection system. We also implemented a number of filtering rules and restrictions to better control users. The tests carried out in this work validate the proposed solution.

Keywords: LAN, WAN, OPNsense, zimbra, zenarmor, DNS, plugin.

Liste des acronymes

ACL: Access Control List

ADSL: Asymetric Digital Subscriber Line

ARP: Address Resolution Protocol

ASPF: Application Specific Packet Filtering

CARP: Common Address Redundancy Protocol

CentOS: Community Enterprise Linux Operating System

CPU: Central Processing Unit

DHCP: Dynamic Host Configuring Protocol

DMZ: Demilitarised Zone

DNS: Domain Name System

DoS: Denied of Service

FEC : fichier des écritures comptables

FQDN : Fully Qualified Domain Name

FTP : File Transfert Protocol

GIF : format d'échange d'images

GRE: Generic Routing Encapsulation

HDD: Hard Disk Drive

HTTP: Hyper Text Transfert Protocol

HTTPS: Hyper Text Transfert Protocol Secure

ICMP: Internet Control Message Protocol

IDS: Intrusion Detection System

IMAP: Internet Mail Access Protocol

IP: Internet Protocol

IPS: Intrusion Prevention System

LACP: Link Aggregation Control Protocol

LAGG: Link Aggregation

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol

NGFW: Next Generation Firewall

OS: Operating System

PC: Personal Computer

PHP: Hypertext Pre-processor

POP 3: Post Office Protocol

RAM: Random Access Memory

RHEL: Red Hat Enterprise Linux

SNMP: Simple Network Management Protocol

SQL: Structured Query Language

SSD: Solid State Drive

SSL: Secure Socket Layer

TCP : Transport Control Protocol

TLS : Sécurité de la couche de transport

UDP: User Datagram Protocol

VPN: Virtual Private Network

VRRP: Virtual Router Redundancy Protocol

WAN: Wide Area Network

WEB: World Wide Web

Wi-Fi: Wireless Fidelity

Liste des figures

Liste des tableaux

Sommaire

Introduction Générale

Avec l'avènement de l'ère numérique, toutes les entreprises sont dépendantes des réseaux informatiques, spécialement des réseaux locaux. Certains services de l'entreprise exigent un accès au réseau WAN(internet) non seulement pour le bon déroulement des activités de l'entreprise mais aussi dans le but de rester en contact avec les partenaires distants. Ces activités peuvent constituer un danger pour l'entreprise car le réseau WAN n'est pas sécurisé raison pour laquelle les entreprises sont confrontées à une variété de menaces comme les attaques par déni de service (DoS), les intrusions malveillantes, les fuites de données sensibles etc… Plus la taille de l'entreprise est grande, plus il est difficile de gérer les trafics entrants et sortants, plus la configuration du réseau devient complexe et plus le risque d'exposition est élevé.

Cependant la mise en place d'une sécurité robuste est essentielle pour protéger les réseaux contre ces menaces potentielles. La notion de sécurité est devenue un sujet de recherche très important et elle englobe d'une part les appareils de sécurité et d'autre part une architecture inébranlable face aux menaces. Ainsi, l'un des aspects les plus fondamentaux de la sécurité réseau est le pare-feu. Le pare-feu joue un rôle essentiel en tant que première ligne de défense contre les attaques provenant de l'extérieur et permet de contrôler le flux de trafic entre les réseaux. Il agit comme une barrière de sécurité en analysant le trafic entrant et sortant, en filtrant les paquets de données et en appliquant des règles de sécurité spécifiques.
Il peut limiter ou interdire l'accès à certains services non agréés par l'entreprise donnant ainsi un contrôle sur les activités qui y déroulent dans son enceinte.
C'est dans ce cadre que s'inscrit notre projet de fin d'études qui consiste à mettre en place un système de sécurité de réseaux basé sur le pare-feu "OPNsense", réalisé au sein du centre des systèmes, réseaux d'information, de communication, de télé-enseignement au niveau de l'université de Blida 1.
Notre travail consiste tout d'abord à mettre en place un réseau local composé d'un serveur d'authentification, d'un serveur DNS et d'un serveur de messagerie et par la suite implémenter le pare-feu OPNsense au bord de notre réseau. Pour mener à bien ce travail, nous parlerons dans un premier temps de la généralité sur la sécurité réseau y compris les menaces et les pare-feu, puis on étudiera le pare-feu OPNsense en évoquant ses fonctionnalités de base et enfin la dernière partie sera purement pratique car elle sera complètement axée sur la réalisation de notre projet.

Chapitre 1 : Sécurité réseau et firewall

1.1 Introduction

Dans le monde interconnecté d'aujourd'hui, la sécurité des réseaux informatiques est devenue une préoccupation majeure.
L'utilisation croissante d'Internet, qui était à l'origine destiné à connecter les individus, a malheureusement entraîné une augmentation des dangers et des menaces.
Les pirates informatiques sont constamment à l'affût, cherchant à escroquer et à pirater les utilisateurs mal protégés.
Pour préserver cette communication devenue indispensable à travers le monde, il est impératif de mettre en place des solutions qui renforcent la sécurité des systèmes informatiques. Parmi ces solutions, le déploiement de pare-feu (firewall) à la frontière des réseaux informatiques est l'une des plus essentielles.

Ce chapitre fera l'objet d'une étude minutieuse sur la Sécurite Réseau et le firewall ainsi que quelques exemples de firewall.

1.2 Réseau Informatique

Un réseau informatique est un ensemble d'ordinateurs et de dispositifs interconnectés qui permettent le partage des ressources et la communication entre eux.
Il s'agit d'une infrastructure qui facilite l'échange d'informations, de données et de services entre les utilisateurs et les systèmes connectés.
Les réseaux informatiques peuvent être de différentes tailles et configurations [11]:

- **Reseaux locaux (LAN) :** limités à un seul emplacement, tels que des bureaux ou des campus universitaires.
- **Réseaux étendus (WAN) :** couvrir de vastes zones géographiques, en reliant plusieurs sites distants.

1.3 Protocole

Les protocoles de réseau jouent un rôle crucial dans la communication entre les appareils connectés. Les protocoles de réseau sont des ensembles de règles et de normes qui définissent comment les données sont transmises, formatées, routées et reçues sur le réseau.

- **Protocole IP :** Le protocole Internet (IP) est l'un des protocoles de réseau les plus utilisés. Il permet l'adressage des appareils et le routage des paquets de données sur Internet. Le protocole IP fonctionne en attribuant des adresses IP uniques à chaque appareil connecté au réseau.

- **Protocole TCP :** Il assure la transmission fiable des données en découpant les informations en petits paquets, en les envoyant et en s'assurant qu'ils sont reçus correctement et dans l'ordre.

- **Protocole UDP :** un protocole permettant l'envoi sans connexion de datagrammes dans des réseaux basés sur le protocole IP.

- **Protocole FTP :** Il s'agit donc d'un protocole utilisé pour transférer des fichiers d'un ordinateur à un serveur ou d'un serveur à un ordinateur.

Le protocole FTP utilise 2 ports (20, 21).

- **Protocole HTTP : est** un protocole servant à transmettre des documents hypermédias, comme HTML. Le protocole HTTP utilise le port 80.

- **Protocole ARP : est** un protocole effectuant la traduction d'une adresse IPv4 en une adresse MAC.

- **Protocole ICMP : est** un protocole de la couche réseau utilisé par les périphériques réseau pour diagnostiquer les problèmes de communication du réseau.

- **Protocole SNMP :** désigne un protocole standard de communication. Il est principalement employé pour le transfert du courrier électronique et il utilise le port 25.

- **Protocole IMAP :** désigne un protocole permettant l'accès direct à ses courriels sur un serveur de messagerie et il utilise le port 143.

- **Protocole POP 3 :** est un protocole standard utilisé pour récupérer les courriers électroniques d'une boîte aux lettres distante sur un serveur de messagerie et il utilise le port 110.

- **Protocole LDAP** : permet de rechercher, de modifier ou d'authentifier d'importants volumes de données, d'informations et d'éléments dans des services d'annuaires distribués, mais aussi de gérer la communication avec les bases de données desdits annuaires. Il utilise le port 636.

1.4 Serveur

Le terme serveur désigne le rôle joué par un appareil matériel destiné à offrir des services à des clients en réseaux. Les services que peut rendre un serveur sont nombreux, on peut citer parmi les plus importants :

- **Serveur DNS :** un système d'application dont le rôle est de traduire les noms de domaine des sites internet en adresses IP qui peuvent être comprises par l'ordinateur qui l'utilise.

- **Serveur de Messagerie :** Il permet de recevoir les mails adressés à un collaborateur et de les garder en mémoire jusqu'à ce que la personne concernée puisse y avoir accès. Pour les entreprises, c'est aussi l'opportunité de créer une communauté via les boîtes mail individuelles en donnant accès, sous réserve de validation par la personne concernée, aux calendriers, aux absences et aux groupes de travail d'un même service.

- **Serveur D'Authentification :** est un type spécifique de serveur qui gère le processus d'authentification des utilisateurs et des appareils qui souhaitent accéder à un système, à un réseau ou à des ressources protégées. Il agit comme une passerelle sécurisée entre les utilisateurs et les ressources auxquelles ils cherchent à accéder.

- **Serveur WEB :** est un type de serveur informatique qui héberge des sites web et fournit des pages web aux utilisateurs qui les demandent via un navigateur web. Il est responsable

du stockage, du traitement et de la livraison des fichiers et des ressources qui composent les sites web.

- **Serveur de Fichier** : Le serveur de fichiers a pour rôle d'héberger et de donner accès aux fichiers partagés par les ordinateurs connectés en réseau.

1.5 La sécurité des réseaux

Fait référence à l'ensemble des mesures et des pratiques mises en place pour protéger les réseaux informatiques contre les menaces, les attaques et les vulnérabilités.
Elle vise à garantir la **confidentialité**, **l'intégrité** et la **disponibilité des données,** des ressources et des services du réseau.

1.6 Les Attaques

Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables. Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée.
Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques. Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques afin de mieux s'y préparer [12].

1.6.1 Technique D'attaque

Les hackers utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes [13] :

- **Les Attaque Direct :** C'est la plus simple des attaques. L'hacker attaque directement sa victime à partir de son ordinateur (figure 1.1). En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrables, et un grand nombre de ces logiciels envoie directement les paquets à la victime.

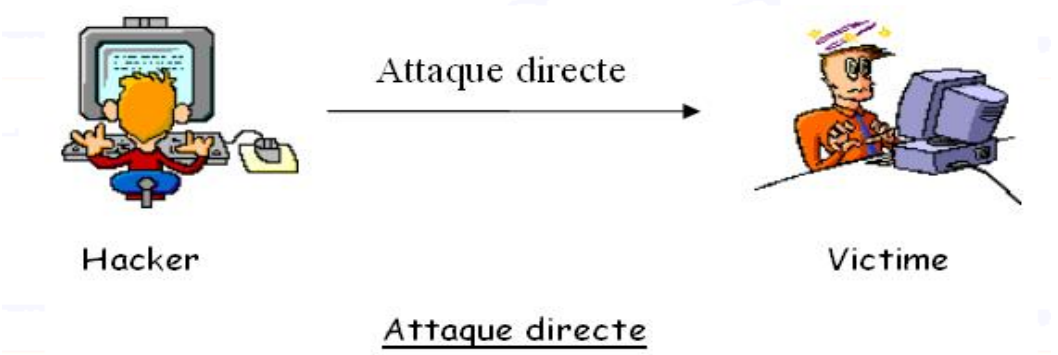

Figure 1. 1 : Attaque direct

Lorsque l'on se fait attaquer de la sorte, il y a de grandes chances pour que l'on puisse remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

➢ **Les Attaque Indirect Par Rebond :** Cette attaque est très prisée des hackers (figure 1.2) . En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) de l'hacker ;
- Éventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...) pour attaquer. Le principe en lui-même, est simple : Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime d'où le terme de rebond.

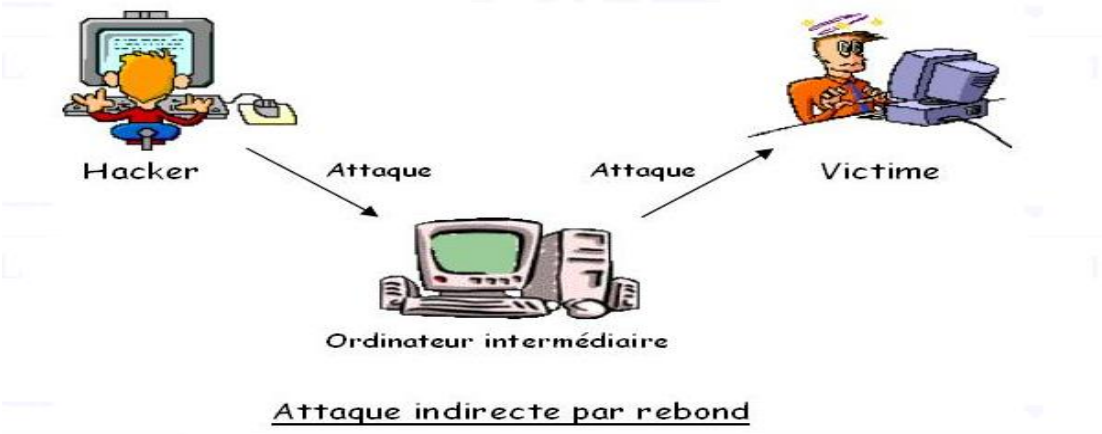

Figure 1. 2 : Attaque indirecte par rebond[]

Si vous êtes victime de ce genre d'attaque, il n'est pas facile de remonter à la source. Au plus simple, vous remontrez à l'ordinateur intermédiaire.

- **Les Attaque Indirect Par Réponse :** Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue de l'hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

1.6.2 Type D'Attaque Réseau

1.6.2.1 Attaque passive sur le Réseau :

Activités comme le wiretapping (écoute en ligne) et l'idle scan (méthode de balayage des ports TCP), conçues pour intercepter le trafic passant par le réseau [14].

1.6.2.2 Attaque Active Sur Le Réseau :

Activités telles que les attaques par déni de service (DoS, Denial of Service) et les injections SQL, où l'auteur tente d'exécuter des commandes pour perturber le fonctionnement normal du réseau [14].

1.7 Dispositif de Protection

Un dispositif de protection des attaques réseau est un ensemble de mesures et de technologies conçues pour sécuriser les réseaux informatiques contre les attaques malveillantes. Parmi les dispositifs de protection les plus couramment utilisés, citons :

- Les pare-feu ;
- Les systèmes d'authentification et de contrôle d'accès ;
- Les réseaux privés virtuels (VPN) ;
- Antivirus ;
- Serveur Mandataire (PROXY) ;
- Systèmes de détection d'intrusions.

Chacun de ces dispositifs joue un rôle spécifique dans la sécurisation des réseaux et dans la prévention des attaques, dans ce travaille on va se focaliser sur le pare-feu (firewall)**.**

1.8 Définition du firewall

Un pare-feu est une forme de protection qui permet à un réseau de se connecter à Internet tout en maintenant un certain degré de sécurité (figure 1.3). Les firewalls sont des dispositifs ou des programmes qui contrôlent le flux du trafic réseau entre les réseaux ou les hôtes qui adoptent différentes postures de sécurité.

Il existe plusieurs types de pare-feu, chacun ayant des capacités différentes pour analyser le trafic réseau et autoriser ou bloquer des instances spécifiques en comparant les caractéristiques du trafic aux politiques existantes. Comprendre les capacités de chaque type de pare-feu, ainsi que la conception de politiques de pare-feu et l'acquisition de technologies de pare-feu qui répondent efficacement aux besoins d'une organisation, sont essentiels pour assurer la protection des flux du trafic réseau [1].

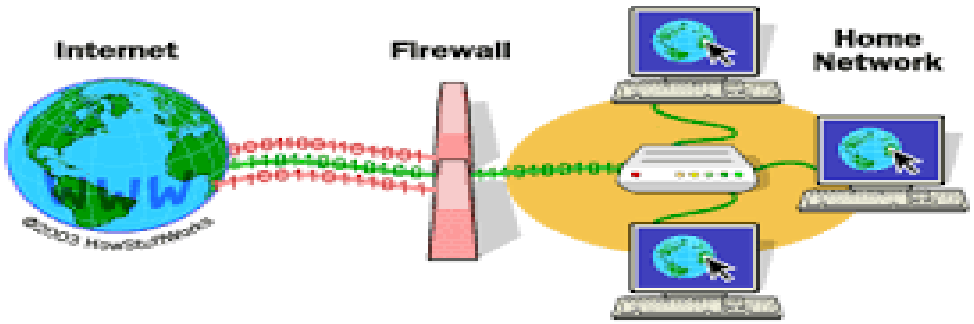

Figure 1. 3 : protection du LAN par le firewall[1]

1.9 Concepts de base des zones de sécurité du firewall

Une zone de sécurité est un ensemble d'un ou plusieurs segments de réseau nécessitant la régulation du trafic entrant et sortant par le biais de politiques. Les zones de sécurité sont des entités logiques auxquelles une ou plusieurs interfaces sont liées. Vous pouvez définir plusieurs zones de sécurité, dont vous déterminez le nombre exact en fonction des besoins de votre réseau (généralement 4). Tous les ordinateurs d'une zone de sécurité configurée sur un pare-feu sont considérés comme "dignes de confiance" et la communication entre eux n'est pas affectée par

le pare-feu. Cependant, la communication entre les réseaux séparés par un pare-feu doit suivre les politiques configurées sur le pare-feu [2].

1.10 Les différentes zones du firewall

1.10.1 Zone de confiance (Trust Zone)

La zone intérieure ou de confiance est également appelée zone privée. Comme son nom l'indique, cette zone contient des actifs et des systèmes qui ne doivent pas être accessibles à quiconque en dehors de l'organisation. Cela inclut les postes de travail des utilisateurs, les imprimantes, les serveurs non publics et tout ce qui est considéré comme une ressource interne. Les appareils trouvés ici ont des adresses IP privées attribuées dans le réseau (c'est une zone fiable).

1.10.2 Zone non fiable (Untrust zone)

La zone extérieure ou non fiable est également connue sous le nom de zone publique. Cette zone est considérée comme étant hors du contrôle d'une organisation et peut être considérée simplement comme l'Internet public (c'est une zone non fiable).

1.10.3 Zone DMZ

La troisième zone de sécurité de base est appelée DMZ, ou zone démilitarisée (figure 1.4). Les ressources dans la DMZ nécessitent un accès externe depuis la zone extérieure. Il est courant de voir des serveurs publics dans la DMZ, tels que des serveurs de messagerie, Web ou d'applications. Une DMZ permet un accès public à ces ressources sans mettre en danger les ressources privées de la zone intérieure [2].

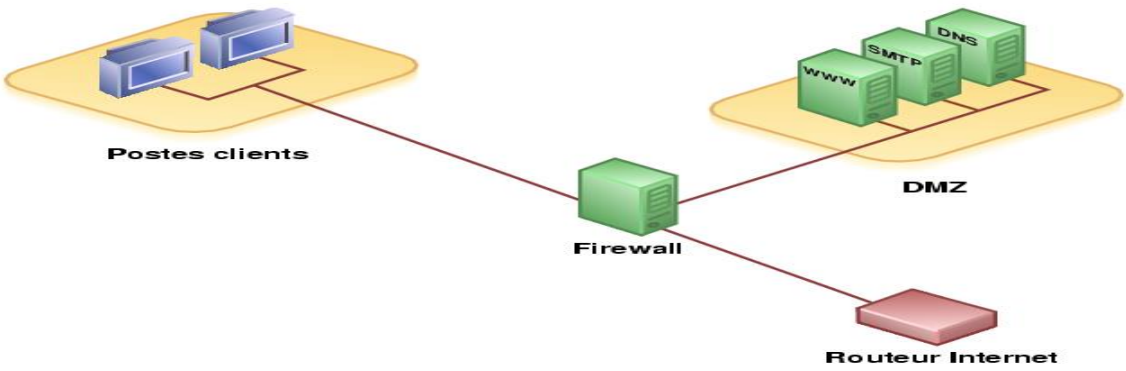

Figure 1. 4 : Zone DMZ[2]

1.10.4 Zone de sécurité locale

La zone locale représente le pare-feu lui-même. Les paquets activement envoyés par le pare-feu peuvent être considérés comme étant envoyés depuis la zone locale. Les paquets qui nécessitent une réponse et un traitement par le pare-feu (non transmis) peuvent être considérés comme provenant de la zone locale. Aucune interface ne peut être ajoutée à la zone locale, mais toutes les interfaces de service sur le pare-feu appartiennent à la zone locale. En raison des caractéristiques particulières de la zone locale, dans les scénarios où l'appareil doit transmettre et recevoir des paquets, vous devez activer la politique de sécurité entre la zone locale et la zone de sécurité où réside l'appareil pair [3].

1.11 Communication interzone : politique de sécurité

La fonction de base d'un pare-feu est de contrôler l'accès des données entrant et sortant du réseau. Il protège un réseau spécifique contre les attaques de réseaux non fiables et permet également une communication légitime entre deux réseaux. Un pare-feu utilise généralement une politique de sécurité pour mettre en œuvre la fonction précédente. La politique de sécurité consiste en des conditions de correspondance (telles que les 5 tuples, les utilisateurs et les plages de temps) et les actions. Après avoir reçu le trafic, le pare-feu identifie les attributs de trafic (tels que les 5 tuples, les utilisateurs et les plages horaires) et fait correspondre les attributs de trafic avec les conditions correspondantes de la politique de sécurité. Si toutes les conditions de la politique de sécurité sont satisfaites, le trafic correspond à la politique de sécurité. Dans ce cas, l'appareil effectue les actions suivantes :

- ➢ Si l'action est "autorisée" et que la détection de la sécurité du contenu n'est pas configurée, le trafic est autorisé à passer.
- ➢ Si l'action est "autorisée" et que la détection de la sécurité du contenu est configurée, l'appareil détermine s'il autorise le trafic en fonction du résultat de la détection de la sécurité du contenu.
- ➢ Si l'action est définie sur "refuser", le trafic n'est pas autorisé à passer [3].

1.11.1 Processus de mise en correspondance des politiques de sécurité

Le principe de conception de base d'un pare-feu est de "refuser tout le trafic par défaut, sauf indication contraire". Cela garantit que le pare-feu peut protéger la cyber sécurité une fois qu'il

est connecté au réseau. Pour autoriser un certain trafic, créez une politique de sécurité. Généralement, plusieurs politiques de sécurité sont configurées pour différents trafics de service. Le processus de mise en correspondance des politiques de sécurité est le suivant :

Le fait que le trafic dans la même zone de sécurité et le trafic entre différentes zones de sécurité soit contrôlé par la politique de sécurité par défaut est décrit comme suit [3] :

- ➢ Le trafic entre les différentes zones de sécurité (y compris, mais sans s'y limiter, le trafic envoyé par les pare-feu et le trafic reçu par les pare-feu) est contrôlé par la politique de sécurité par défaut.
- ➢ Par défaut, le trafic dans la même zone de sécurité n'est pas contrôlé par la politique de sécurité par défaut, et l'action de transfert par défaut est "autoriser". Si le trafic dans la même zone de sécurité doit être contrôlé par la politique de sécurité par défaut, vous pouvez activer cette fonction si nécessaire. Après son activation, la configuration de la politique de sécurité par défaut prendra effet sur le trafic dans la même zone de sécurité, y compris les actions de la sécurité par défaut et la fonction de journalisation.
- ➢ L'action par défaut et la fonction de journalisation (y compris les journaux de correspondance de politique, les journaux de session, les journaux de trafic) peuvent être modifiées dans la politique de sécurité par défaut.

1.12 Politiques de filtrage de zone

Dans le cas des zones de sécurité réseau, un pare-feu applique la politique de contrôle d'accès, en déterminant quel trafic est autorisé à passer entre les zones configurées. Avec cette implémentation commune à quatre zones, plusieurs stratégies de filtrage de zone recommandées doivent être en place :

- ❖ **De l'intérieur vers l'extérieur et de l'intérieur vers la DMZ** : le trafic provenant de l'intérieur est inspecté lorsqu'il se déplace vers l'extérieur ou vers la DMZ. Les exemples incluent un employé demandant une page Web à partir d'un serveur Web public ou accédant à n'importe quelle ressource dans la DMZ. Ce type de trafic est autorisé avec très peu de restrictions, voire aucune [2].

- ❖ **De l'extérieur vers l'intérieur** : le trafic provenant de l'extérieur et se dirigeant vers l'intérieur est complètement bloqué, à moins que le trafic ne réponde à une demande d'une ressource interne. Par exemple, si un utilisateur interne demande une page Web à partir

d'un serveur Web public, ce trafic de l'extérieur vers l'intérieur est autorisé. Les connexions provenant du réseau public qui ne sont pas une réponse à une requête seront refusées [2].

- **DMZ vers l'intérieur** : le trafic provenant de la DMZ et se dirigeant vers l'intérieur est également complètement bloqué, à moins que le trafic ne soit une réponse à une demande légitime de l'intérieur [2].

- **De l'extérieur vers la DMZ** : le trafic provenant de l'extérieur et se dirigeant vers la DMZ est inspecté par le pare-feu et sélectivement autorisé ou refusé. Des types de trafic spécifiques peuvent être transmis, tels que le trafic de courrier électronique, HTTP, HTTPS ou DNS. Notez également que les réponses de la DMZ vers l'extérieur seront dynamiquement autorisées. En d'autres termes, le pare-feu ouvrira dynamiquement un port pour autoriser le trafic requis de la DMZ vers l'extérieur selon les besoins [2].

- **DMZ vers l'extérieur** : le trafic provenant de la DMZ et se dirigeant vers l'extérieur est autorisé de manière sélective en fonction des exigences de service et des règles de pare-feu. Par exemple, s'il existe un serveur de messagerie dans la DMZ qui doit se répliquer avec un serveur de messagerie situé à un autre emplacement, la politique de pare-feu doit autoriser ce type de trafic [2].

1.13 Principes du filtrage

Les systèmes de filtrage de paquets acheminent les paquets entre les hôtes internes et externes, mais ils le font de manière sélective. Ils autorisent ou bloquent certains types de paquets d'une manière qui reflète la politique de sécurité d'un site.

Le type de routeur utilisé dans un pare-feu à filtrage de paquets est connu sous le nom de routeur de filtrage. Chaque paquet comporte un ensemble d'en-têtes contenant certaines informations. Les principales sont les suivantes : l'adresse IP source, l'adresse IP de destination, protocole (si le paquet est un paquet TCP, UDP ou ICMP), port source TCP ou UDP, port de destination TCP ou UDP, type de message ICMP, taille du paquet. Le routeur peut également regarder les données situées plus loin dans le paquet, au-delà des en-têtes ; cela lui permet, par exemple, de filtrer les paquets sur la base d'informations plus détaillées (comme le nom de la page web demandée) et de vérifier que les paquets semblent être formatés comme prévu pour leur port de destination. Le routeur peut également s'assurer que le paquet est valide

(qu'il a bien la taille qu'il prétend avoir et qu'il est de taille légale, par exemple), ce qui permet d'éviter un certain nombre d'attaques par déni de service basées sur des paquets mal formés. En outre, le routeur sait des choses sur le paquet qui ne sont pas reflétées dans le paquet lui-même, telles que : l'interface sur laquelle le paquet arrive, l'interface sur laquelle le paquet sortira etc…

Enfin, un routeur qui garde la trace des paquets qu'il a vus connaît certains faits historiques utiles, tels que :

- ➢ Si ce paquet semble être une réponse à un autre paquet (c'est-à-dire que sa source était la destination d'un paquet récent et que sa destination est la même que celle du paquet précédent) destination d'un paquet récent et que sa destination est la source de cet autre paquet)
- ➢ Combien d'autres paquets ont été vus récemment en provenance ou à destination du même hôte ?
- ➢ Si ce paquet est identique à un paquet vu récemment
- ➢ Si ce paquet fait partie d'un paquet plus important qui a été divisé en plusieurs parties (fragmenté).

Pour comprendre le fonctionnement du filtrage de paquets, examinons la différence entre un routeur ordinaire et un routeur de filtrage. Un routeur ordinaire examine simplement l'adresse de destination de chaque paquet et choisit le meilleur moyen qu'il connaît pour envoyer ce

paquet vers cette destination. La décision sur la manière de traiter le paquet est basée uniquement sur sa destination. Il y a deux possibilités : le routeur sait comment envoyer le paquet vers sa destination, et il le fait ; ou le routeur ne sait pas comment envoyer le paquet vers sa destination, et il oublie l'existence du paquet et envoie un message ICMP "destination inaccessible" à la source du paquet.

Un routeur de filtrage, en revanche, examine les paquets de plus près. En plus de déterminer s'il peut ou non s'il peut ou non acheminer un paquet vers sa destination, un routeur de filtrage détermine également s'il doit ou non le faire. Les mentions "doit" ou "ne doit pas" sont déterminées en fonction de la nature du paquet ou "ne devrait pas" sont déterminés par la politique de sécurité du site, que le routeur de filtrage a été configuré pour appliquer.

Une fois qu'il a examiné toutes les informations, un routeur de filtrage de paquets simple peut faire l'une des choses suivantes :

- ➢ Envoyer le paquet à la destination prévue.
- ➢ Laisser tomber le paquet - l'oublier, sans en avertir l'expéditeur.
- ➢ Rejeter le paquet - refuser de le transmettre et renvoyer une erreur à l'expéditeur.
- ➢ Enregistrer des informations sur le paquet.
- ➢ Déclencher une alarme pour avertir immédiatement quelqu'un de la présence du paquet.

Les routeurs plus sophistiqués peuvent également être en mesure de faire une ou plusieurs de ces choses :

- ➢ Modifier le paquet (par exemple, pour effectuer une traduction d'adresse réseau).
- ➢ Envoyer le paquet vers une destination autre que celle à laquelle il était destiné (par exemple, pour forcer les transactions à passer par un serveur mandataire ou effectuer un équilibrage de charge).
- ➢ Modifier les règles de filtrage (par exemple, pour accepter les réponses à un paquet UDP ou pour refuser tout trafic en provenance d'un site qui a envoyé des paquets hostiles). Le fait que les serveurs de certains services Internet résident à certains numéros de port permet au routeur de bloquer ou d'autoriser certains types de connexions simplement en spécifiant le numéro de port approprié (par exemple, le port TCP 23 pour les connexions Telnet) dans l'ensemble des règles spécifiées pour le filtrage des paquets.

Les dispositifs qui examinent le contenu des paquets, plutôt que leurs en-têtes, sont souvent appelés filtres de paquets intelligents. En pratique, presque tous les filtres de paquets avec état sont également capables de regarder le contenu des paquets, et beaucoup sont également capables de modifier le contenu des paquets, de sorte que vous pouvez voir toutes ces capacités regroupées sous le titre "filtrage de paquets avec état". Cependant, on peut légitimement parler de "filtre de paquets avec état" sans avoir la capacité de filtrer ou de modifier le contenu de manière avancée [4].

1.14 Avantages du filtrage de paquets

Le filtrage de paquets a beaucoup d’avantages :

- ➢ Un routeur de dépistage peut contribuer à protéger un réseau entier : Si un seul routeur relie votre site à l'internet, le filtrage des paquets sur ce routeur vous permet d'améliorer considérablement la sécurité de votre réseau, quelle que soit la taille de votre site.

- ➢ Le filtrage simple de paquet est très efficace : Le filtrage simple des paquets ne nécessitant de prêter attention qu'à quelques en-têtes de paquets, il peut être effectué avec un très faible surcoût très peu de frais généraux. Il faut pour cela configurer le firewall avec des règles de filtrage généralement appelées ACL (Access Control List).
- ➢ Le filtrage de paquet avec état : Ce mécanisme se veut meilleur que le monde précédent en apportant une capacité de filtrage applicatif tout en restant au niveau de la couche transport/session. Le filtrage dynamique ajoute la prise en compte de l'historique au simple filtrage de paquet : l'idée de base étant qu'avec un échange client/serveur si un paquet est passé dans un sens il en passera un dans l'autre (commutation de la source et destination du couple IP/port pour les paquets TCP/UDP). Diverses temporisations sont introduites : poignées de main TCP, fermeture de connexion ou de session. Ce mode permet de générer à la volée des règles temporaires de filtrage des paquets. Ces dernières disparaissent lorsqu'aucun paquet ne passe pendant un délai configuré ou avec la fermeture de la session en TCP (RST, FIN). Le filtrage adaptatif recherche, en outre, des signatures dans le segment de données des paquets afin de déterminer le type et l'état du protocole applicatif transporté et de procéder ainsi à des vérifications de cohérences. C'est dans cette catégorie que l'on peut ranger le terme de « stateful inspection » utilisé par divers éditeurs [4].

1.15. Les inconvénients du filtrage des paquets

Bien que le filtrage de paquets offre de nombreux avantages, il présente également certains inconvénients.

- ➢ Les outils de filtrage actuels ne sont pas parfaits ;
- ➢ Les règles de filtrage des paquets ont tendance à être difficiles à configurer. Bien qu'il y ait un certain degré de difficulté, il va de la de l'esprit à l'impossibilité de se creuser les méninges.
- ➢ Les capacités de filtrage des paquets de nombreux produits sont incomplètes, ce qui rend difficile, voire impossible, la mise en œuvre de certains types de filtres très souhaitables.
- ➢ Le filtrage des paquets réduit les performances du routeur ;
- ➢ Certaines politiques ne peuvent pas être facilement appliquées par des routeurs de filtrage de paquets normaux [4].

1.16 Context de l'ASPF (Application Specific Packet Filtering firewall)

Dans le modèle TCP/IP, la couche application fournit des services d'application réseau communs, tels que Telnet, HTTP et FTP. Les protocoles de couche application peuvent être classés en protocoles de couche application monocanal et multicanaux en fonction du nombre de ports occupés.

- ➢ Protocole de couche application monocanal : protocole qui n'occupe qu'un seul port lors de la communication. Par exemple, Telnet n'occupe que le port 23 et HTTP n'occupe que le port 80.
- ➢ Protocole de couche application multicanal : protocole qui occupe deux ports ou plus pendant la communication. Par exemple, dans FTP en mode passif, le port 21 et un port aléatoire sont occupés.

Les pare-feu traditionnels à filtrage de paquets présentent les inconvénients suivants pour le contrôle d'accès multi canal du protocole de couche application :

- ➢ Les pare-feu de filtrage de paquets traditionnels ne peuvent mettre en œuvre qu'un contrôle d'accès simple.
- ➢ Les pare-feu de filtrage de paquets traditionnels ne peuvent bloquer les données d'application que pour certains protocoles à canal unique qui utilisent des ports fixes.

Les protocoles multicanaux doivent négocier l'adresse et le port de la connexion de canal de données suivante en fonction du résultat de la négociation. Les adresses IP et les ports des canaux de données sont négociés dynamiquement et ne peuvent pas être connus de l'administrateur. Par conséquent, des politiques de sécurité précises ne peuvent pas être formulées. Pour assurer le bon établissement des canaux de données, tous les ports doivent être ouverts. Cela peut provoquer des attaques sur le serveur ou le client [3].

Application de l'ASPF dans les protocoles d'application multicanaux

ASPF est utilisé pour filtrer les paquets dans la couche application.

En détectant les informations d'adresse et de port transportées au niveau de la couche d'application des paquets de négociation, le pare-feu génère automatiquement une entrée de carte de serveur correspondante. Lorsque le premier paquet d'un canal de données traverse le pare-feu, le pare-feu génère une session basée sur l'entrée de mappage du serveur pour autoriser les paquets suivants dans le canal de données, ce qui équivaut à créer automatiquement une politique de sécurité raffinée. Pour toutes les connexions d'un protocole d'application spécifié,

ASPF conserve les informations d'état de chaque connexion et détermine dynamiquement s'il faut autoriser les paquets de données à traverser le pare-feu ou rejeter les paquets de données[3].

1.17 Les types de firewall

1.17.1 Les firewalls bridge

Ils sont relativement répandus. Ils agissent comme de véritables câbles réseau avec la fonction supplémentaire de filtrage, d'où leur nom de pont. Leurs interfaces n'ont pas d'adresse IP, et se contentent de transférer les paquets d'une interface à l'autre en appliquant des règles prédéfinies. Cette absence est particulièrement utile, car elle signifie que le pare-feu est indétectable pour un pirate ordinaire. En effet, lorsqu'une requête ARP est envoyée sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que "renvoyer" les paquets, il sera totalement invisible sur le réseau. Il est donc impossible de diriger une attaque contre le pare-feu, car aucun paquet ne sera traité par le pare-feu comme sa propre destination. La seule façon de le contourner est donc d'outrepasser ses règles de suppression. Tout attaquant doit donc "suivre" ses règles et essayer de le contourner [5].

- **Les Avantages**

➢ Impossible de l'éviter (les paquets passeront par ses interfaces).

➢ Peu coûteux [6].

- **Inconvénients**

➢ Possibilité de le contourner (il suffit de passer outre ses règles).

➢ Configuration souvent contraignante.

➢ Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless) [6].

1.17.2 Les firewalls matériels

On les trouve souvent sur les routeurs achetés sur le marché auprès de grands fabricants tels que Cisco ou Nortel. Ils sont intégrés directement dans la machine, ils agissent donc comme une "boîte noire" et s'intègrent parfaitement au matériel. Leur configuration est souvent relativement difficile, mais leur avantage est que leur interaction avec les autres fonctionnalités

du routeur est simplifiée par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en termes de configuration, ils sont également vulnérables aux attaques, car ils sont présents dans la “boîte noire” qu’est le routeur. De plus, comme ils sont souvent étroitement liés au matériel, l’accès à leur code est assez difficile. Son administration est souvent plus simple que celle des firewalls bridge [5].

- **Avantage :**

➢ Intégré au matériel réseau.

➢ Administration relativement simple.

➢ Bon niveau de sécurité.

- **Inconvénients :**

➢ Dépendant du constructeur pour les mises à jour.

➢ Souvent peu flexibles.

1.17.3 Les firewalls logiciels

Le firewall logiciel est installé directement sur un ordinateur ou un serveur et chargé de la sécurité du réseau, il joue un rôle similaire au firewall matériel mais de façon locale.
Il fonctionne avec une grande variété d’autres solutions de sécurité technologique pour fournir une sécurité plus robuste et cohérente aux entreprises de toutes tailles [5].

1.17.4 Les firewalls personnels

Ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelquefois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final. Il est installé dans des appareils informatiques comme n'importe quel autre logiciel qui peut être personnalisé.

- **Avantage :**

➢ Sécurité en bout de chaîne (le poste client).

➢ Personnalisable assez facilement.

- **Inconvénients :**

➢ Facilement contournable.

➢ Difficiles à départager de par leur nombre énorme.

1.18 Comparaison entre firewall matériel et firewall logiciel

Il est important d'être aussi éduqué sur les différences entre les deux types pare-feu lorsque vous faites ce choix important. On cite quelques-unes des plus grandes différences entre les deux types de firewall [5] :

Paramètres	Firewall logiciel	Firewall matériel
Protection large ou granulaire	Fournit une protection granulaire pour tous les appareils individuels du réseau	Protège le réseau dans son ensemble
Complexe contre simplicité	Plus simple à configurer, à modifier et à entretenir	Nécessite un personnel qualifié et une proximité physique avec le centre de données
Coût élevé vs faible coût	Peu coûteux à déployer et à entretenir	Investissement initial élevé en matériel et investissement continu en personnel qualifié
Inconvénient vs commodité	Le firewall logiciel est difficile à contourner et a très peu d'effet sur l'expérience utilisateur	Le firewall matériel est souvent contourné par les employés qui recherchent une connexion plus rapide et plus fiable ou un accès à certains sites restreints
Expertise vs convivialité	Le firewall logiciel est facile à utiliser et conçu pour être facilement géré par n'importe qui	Le firewall matériel nécessite des connaissances informatiques avancées pour l'installation et la gestion

Tableau 1. 1 : Comparaison entre firewall matériel et firewall logiciel[5]

1.19 Intérêts et limites du pare-feu

Avantage

- ➢ Avec une architecture réseau cohérente, on bénéficie d'une centralisation dans la gestion des flux réseaux.

- ➢ De plus, avec un plan d'adressage correct, la configuration du pare-feu est peu ou pas sensible au facteur d'échelle (règles identiques pour 10 comme 10000 équipements protégés).
- ➢ L'utilisation de la journalisation offre une capacité d'audit du trafic réseau et peut donc fournir des traces robustes en cas d'incident, si le pare-feu n'est pas lui-même une des cibles.
- ➢ Enfin le pare-feu permet de relâcher les contraintes de mise à jour rapide de l'ensemble d'un parc en cas de vulnérabilité sur un service réseau : il est possible de maintenir une certaine protection des équipements non vitaux au prix de la dégradation du service avec la mise en place d'un filtrage [7].

Limites d'un Firewall

Malgré qu'un firewall permet de restreindre l'accès à un point unique, mais il reste incapable devant certaines situations :

- ➢ **La protection contre la menace interne** :

Les utilisateurs internes ayant accès à une ressource non protégée peuvent voler ou détruire des données sans jamais approcher le firewall.

- ➢ **La protection contre des connexions ne passant pas par le firewall :**

Un firewall ne peut contrôler efficacement que le trafic qui passe par lui : il ne peut systématiquement rien faire contre les connexions qui lui échappent. Il est fréquent de constater que des utilisateurs "experts" ou administrateurs mettent en place leur propre "entrée de service" à l'intérieur du réseau.

- ➢ De par sa fonction, le pare-feu est un point névralgique de l'architecture de sécurité avec de fortes contraintes de disponibilité. Il existe des solutions permettant la synchronisation de l'état des pare-feu, comme l'élection du routeur avec VRRP (Virtual Router Redundancy Protocol).

➢ Enfin une bonne gestion d'un pare-feu nécessite la compréhension des protocoles filtrés surtout lorsque les interactions deviennent complexes comme dans les cas FTP, H323...avec le transport de paramètres de connexion dans le segment de données.

➢ **La protection contre les nouvelles menaces :**

Un firewall est destiné à protéger le réseau de l'entreprise contre des menaces connues. La mise en place d'un firewall doit impérativement s'accompagner d'une politique de mise à jour régulière.

1.20 Le pare-feu de nouvelle génération

Pour que le pare-feu redevienne la pierre angulaire de la sécurité des réseaux d'entreprise, les NGFW "règlent le problème à la base". Les NGFW classent le trafic réseau d'une organisation en fonction de l'identité de l'application afin d'accorder l'accès aux utilisateurs et de fournir aux administrateurs la visibilité et le contrôle de tous les types d'applications, y compris les applications web, les applications SaaS (Software as a Service) et les applications patrimoniales. Les exigences fonctionnelles essentielles d'un NGFW efficace sont les suivantes :

➢ Identifier les applications indépendamment du port, du protocole, des techniques d'évasion ou du protocole Secure Sockets Layer de cryptage SSL (Secure Sockets Layer) avant de faire quoi que ce soit d'autre

➢ Fournir une visibilité granulaire et un contrôle basé sur des les applications, y compris les fonctions des applications individuelles

➢ Identifier précisément les utilisateurs et utiliser ensuite les informations comme attribut pour le contrôle des politiques

➢ Fournir une protection en temps réel contre un large éventail de menaces, y compris celles qui opèrent au niveau de la couche application

➢ Intégrer les fonctions traditionnelles de pare-feu et de prévention des intrusions dans le réseau

➢ Prendre en charge les déploiements en ligne avec une dégradation de performance.

1.21 Les firewall logiciels

❖ **Zone Alarm Free**

L'un des premiers pare-feu apparus sous Windows pour offrir une meilleure protection aux machines utilisant cet OS (figure 1.5). Il constitue une ligne de défense solide pour tous les utilisateurs connectés à des lignes ADSL et à des modems câble.

L'interface graphique de Zone Alarm Free est hautement dynamique. Elle laisse le contrôle aux utilisateurs sur leurs données. La dernière version du logiciel permet la détection de trafic suspect, le masquage de ports ouverts et des mises à jour de sécurité. En bonus, les utilisateurs de Zone Alarm Free bénéficient d'un espace offert de 5 Go de sauvegarde en ligne via 1 Drive [8].

Figure 1. 5 : Zone Alarm Free

❖ Comodo firewall

L'une des solutions pare-feu les plus reconnues pour leur efficacité (figure 1.6). Ce logiciel personnel est sûrement le meilleur choix pour les utilisateurs qui désirent des fonctionnalités pare-feu plus poussées. Comodo Firewall est compatible avec les PC sous systèmes d'exploitation Windows. L'interface du logiciel a une configuration simplifiée et interactive pour rendre l'expérience utilisateur agréable et la prise en main facile. Avec ses fonctionnalités si particulières, Comodo Firewall est désormais disponible en version gratuite et en version payante [8].

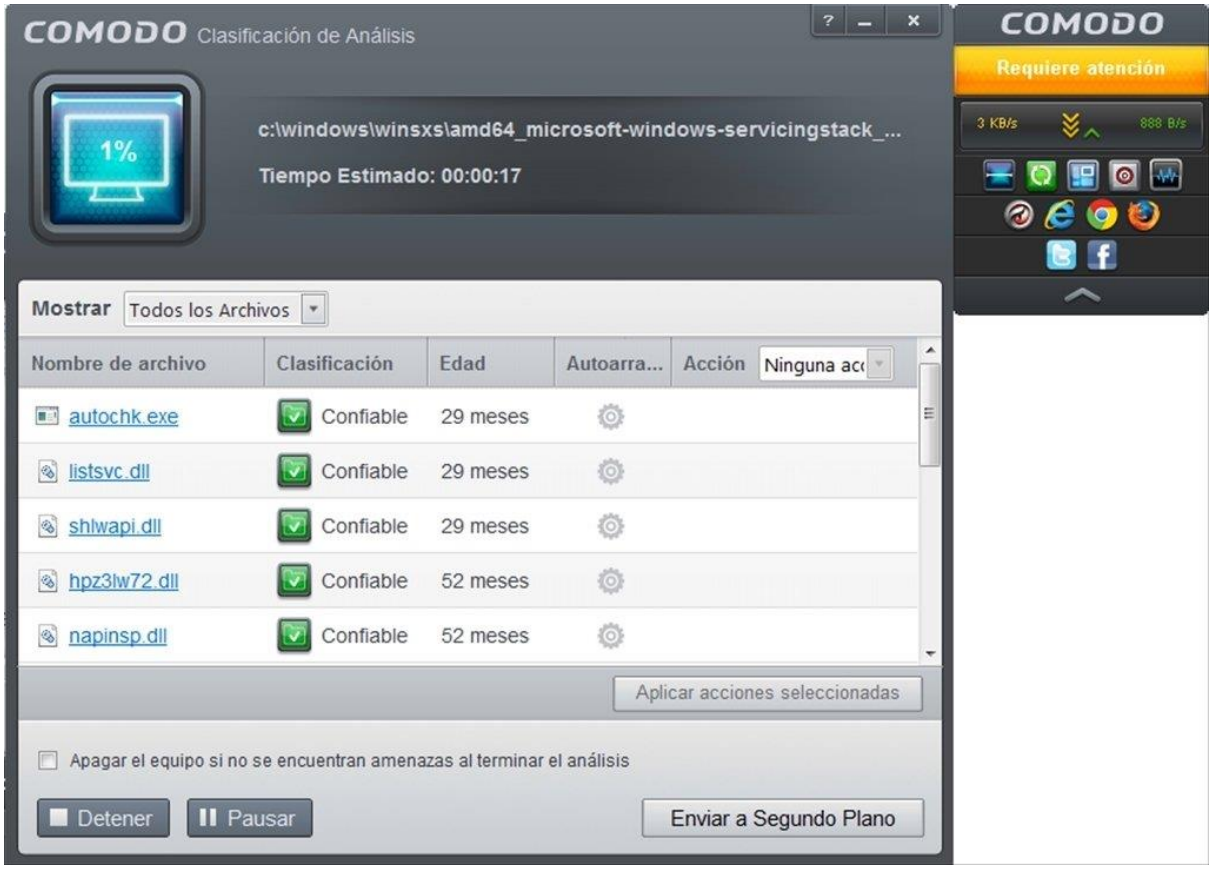

Figure 1. 6 : Comodo Firewall

- **Kerio control**

Réservé en partie aux professionnels des entreprises, le logiciel Kerio Control est une plateforme qui vous permet d'assurer la sécurité totale du système de connexion réseau de votre entreprise (figure 1.7). Grâce à ses différentes fonctionnalités, il gère toutes les menaces entrantes et sortantes de votre réseau de connexion. Kerio Control dispose de nombreux outils dont : une solution antivirus qui protège votre réseau de l'attaque des virus, un dispositif de filtrage qui bloque des contenus web indésirables, un réseau VPN qui assure le lien entre votre siège social et vos succursales et enfin un outil de gestion efficace de la bande passante et des flux. Kerio Control Firewall vous offre aussi des outils efficaces et pratiques qui bloquent toute tentative d'infiltration en protégeant votre réseau optimisant ainsi son bon fonctionnement [9].

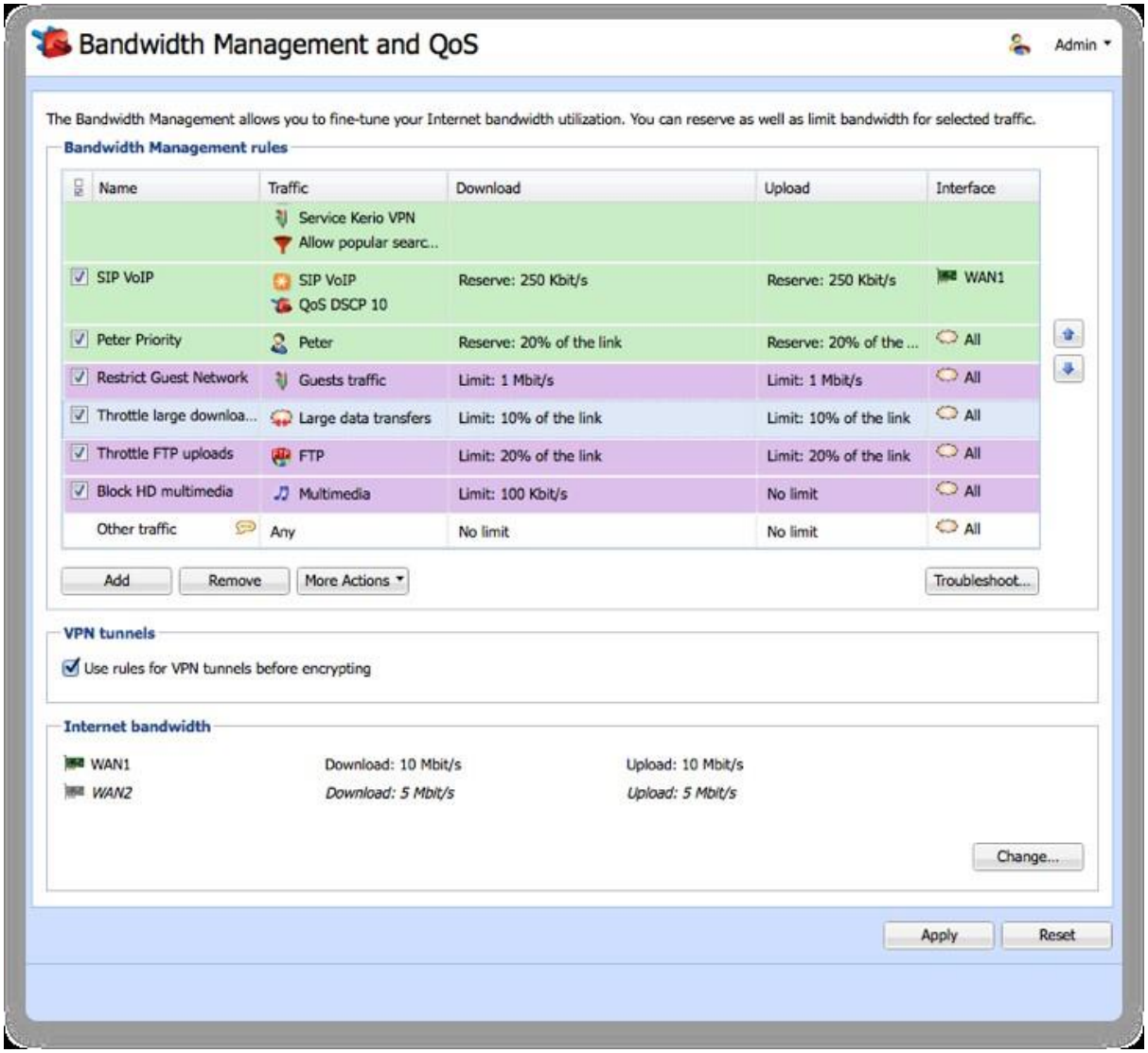

Figure 1. 7 : Kerio control

❖ OPNsense

OPNsense dispose d'une interface Web et peut être utilisé sur la plate-forme x86-64 (figure 1.8). En plus d'agir comme un pare-feu, il dispose de capacités de mise en forme du trafic, d'équilibrage de charge et de réseau privé virtuel, et d'autres peuvent être ajoutées via des plugins. OPNsense offre des fonctionnalités de pare-feu de nouvelle génération utilisant zenarmor [10].

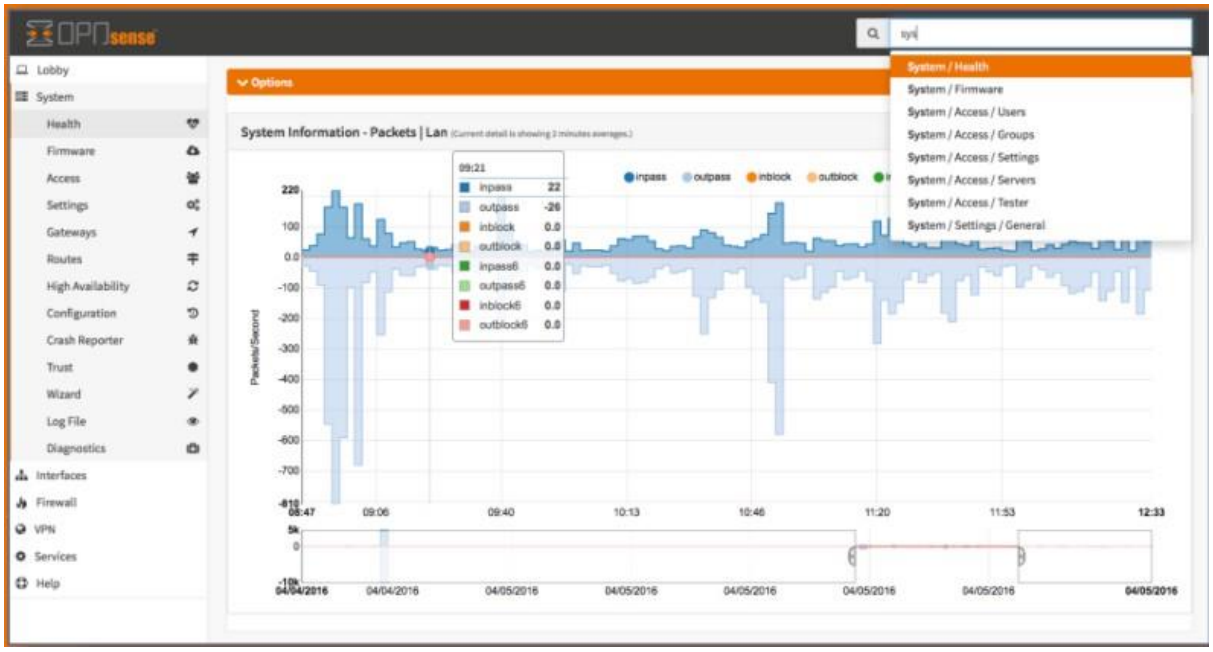

Figure 1. 8 : Interface d'OPNsense

1.22. Conclusion

Dans ce chapitre, nous avons parlé de la sécurité du réseau d'une manière générale et des firewalls de manière détaillée avec quelques exemples. On remarque également l'importance des politiques de sécurité mises en place dans les firewalls qui facilitent beaucoup le filtrage des paquets, ainsi que l'architecture des firewalls qui dépend de la nécessité c'est à dire le "comment" ou le "ou" du déploiement du firewall.

L'ensemble de toutes ces connaissances nous aide à mieux choisir et déployer le firewall dans un réseau mais aussi avec des politiques de sécurité bien réfléchies (bien configurées).

Cependant, certes le firewall est un outil qui permet de sécuriser un réseau informatique mais il n'est pas certain. Seul, il ne peut pas protéger complètement le réseau, il existe d'autres appareils de protection.

Chapitre 2 : Etude du firewall OPNsense

2.1. Introduction

Comme mentionné dans le chapitre précédent, notre choix s'est porté sur le firewall OPNsense, ce chapitre nous parlera brièvement de l'histoire d'OPNsense, son installation et les configurations de base. Avant d'installer et de configurer votre propre installation OPNsense, il est essentiel de connaître certains concepts et de savoir comment le projet OPNsense a été lancé. Nous découvrirons également FreeBSD, tout en explorant les fonctionnalités d'OPNsense et les scénarios de déploiement typiques dans lesquels nous pouvons l'utiliser.
Dans ce chapitre, nous allons couvrir les principaux sujets suivants :

- ➢ Histoire d'OPNsense
- ➢ FreeBSD
- ➢ Pourquoi OPNsense ?
- ➢ Fonctionnalités et déploiements courants.

2.2. Un peu d'histoire

En 2014, un groupe de développeurs courageux a décidé de se séparer de PFsense et de m0n0wall et a lancé le projet OPNsense. La première version officielle a été publiée en janvier 2015, héritant d'une grande partie du code de ses prédécesseurs. Néanmoins, avec un plan très ambitieux pour changer la façon dont beaucoup de choses étaient faites, OPNsense s'est rapidement imposé comme une alternative à PFsense et a reçu une recommandation importante du fondateur de m0n0wall, Manuel Kasper, encourageant les utilisateurs de son projet à migrer vers OPNsense. Ce fut le début de l'un des meilleurs projets de pare-feu open source.

2.3. FreeBSD

FreeBSD est un système d'exploitation libre et gratuit. C'est un système de type Unix, mais différent de Linux, c'est un système d'exploitation complet, comprenant le noyau, les pilotes, et d'autres utilitaires et applications utilisateur. Linux ne comprend que le noyau et les pilotes, et tout le reste est construit en tant que distribution ou simplement distro. Le projet FreeBSD

jouit d'une excellente réputation en matière de sécurité, et une équipe dédiée s'en occupe au niveau du code. Cela lui a permis d'acquérir la réputation d'un système d'exploitation très sûr. De nombreuses entreprises l'ont fait - MacOs, iOS et d'autres systèmes d'exploitation d'APPLE sont basés sur le code FreeBSD, les PlayStation 3 et 4 de Sony l'utilisent, et de nombreux appareils de réseau l'utilisent également. Si vous avez un iPhone, il utilise également un système d'exploitation basé sur FreeBSD.
Maintenant que nous connaissons le système d'exploitation d'OPNsense, examinons les raisons pour lesquelles nous devons l'envisager pour notre pare-feu réseau.

2.4 Pourquoi OPNsense

A cause de la limitation de ses prédécesseurs tels que m0n0wall, PFsense, etc… OPNsense est venu avec beaucoup de nouveautés. Parmi les caractéristiques clés pour lesquelles on doit choisir OPNsense, il y a : une interface web GUI sans accès root direct au système d'exploitation, IDS et IPS avec support netmap, d'excellents plugins disponibles, des sauvegardes cloud, etc.… pour n'en citer que quelques-unes. La liste s'allonge avec chaque nouvelle version.

2.5 Installation et configuration de base d'OPNsense

2.5.1 Architectures matérielles prises en charge

OPNsense est disponible pour les architectures de microprocesseur x86-64 (amd64) bits. Les installations complètes sur des cartes mémoire SD, des disques à semi-conducteurs (SSD) ou des disques durs (HDD) sont destinées à OPNsense.

2.5.2 Exigences matérielles recommandées

La spécification recommandée pour exécuter toutes les fonctionnalités standard d'OPNsense signifie que chaque fonctionnalité est fonctionnelle et convient à la plupart des cas d'utilisation.

Processeur	Processeur multicœur 1,5 GHz
RAM	8GHz
Méthode d'installation	Console série ou vidéo(vga)
Installer la cible	120 Go de SSD

Tableau 2. 1 : Exigences matérielles recommandées [10]

2.5.3 Préparation du démarrage du système

Le processus de démarrage de l'installation d'OPNsense nous permet d'exécuter plusieurs étapes de configuration facultatives.

Si tout se passe bien, vous devez avoir une interface comme celle-là. Par défaut, pour se connecter, il faut mettre l'utilisateur "root" avec le mot de passe "OPNsense" que nous pouvons changer quand on le voudra.

La menue console comprend 13 options, voir la figure ci-dessous (figure 2.1).

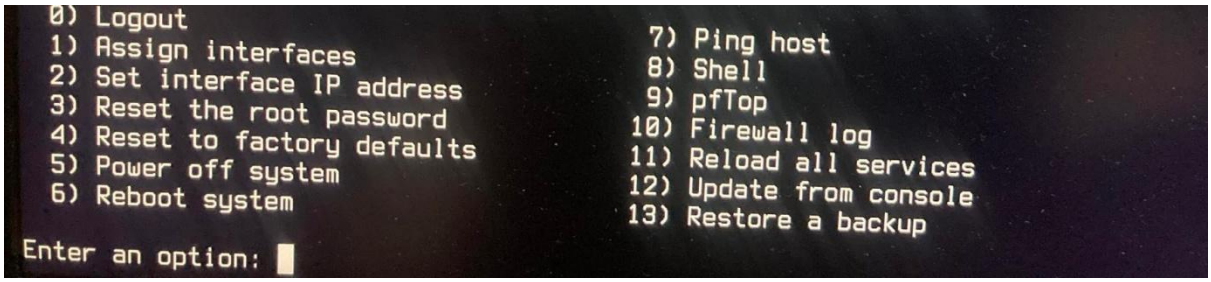

Figure 2. 1 : Les menus du pare-feu OPNsense

Parmi ces options, on peut pinger, redémarrer, définir une adresse IP, attribuer des interfaces, éteindre le firewall etc… On peut évidemment manipuler notre OPNsense via l'interface console mais pour faire juste des choses basiques, si on veut une configuration plus complète et simple, on doit accéder à l'interface graphique.

- **Option 1 :**

  On choisit la carte réseau pour notre interface LAN et WAN (figure 2.2, figure 2.3).

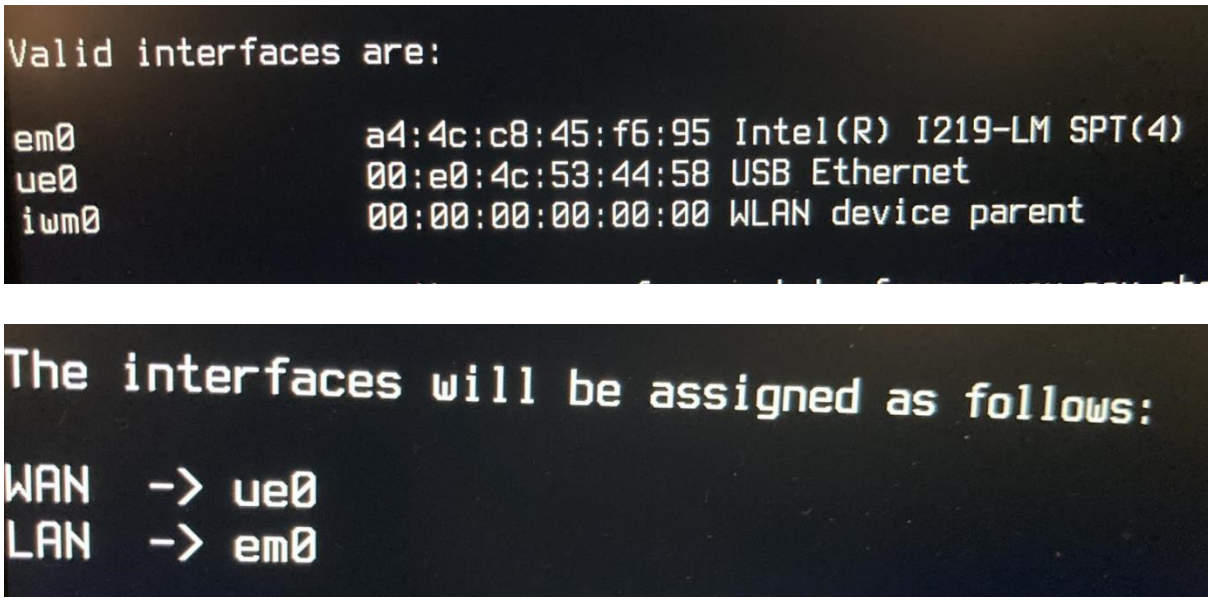

Figure 2. 2 : Attribution des interfaces

- **Option 2 :** On définit l'adresse IP des interfaces attribuées (figure 2.3).

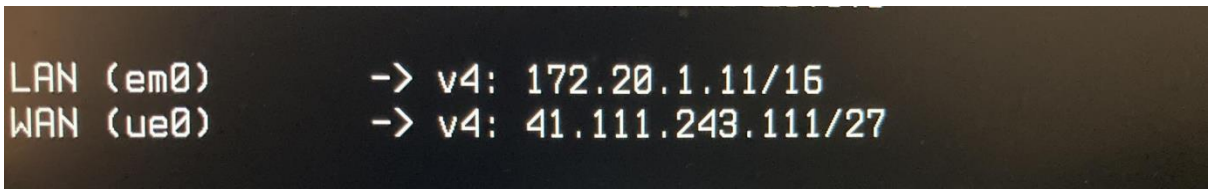

Figure 2. 3 : Définition des adresses IP

- **Option 8 :** On a également une interface Shell qui nous permet de le configurer avec des commandes tapées dans le terminal root. On pourrait aussi tester la connectivité entre le pare-feu et les hôtes via l'interface Shell (figure 2.4).

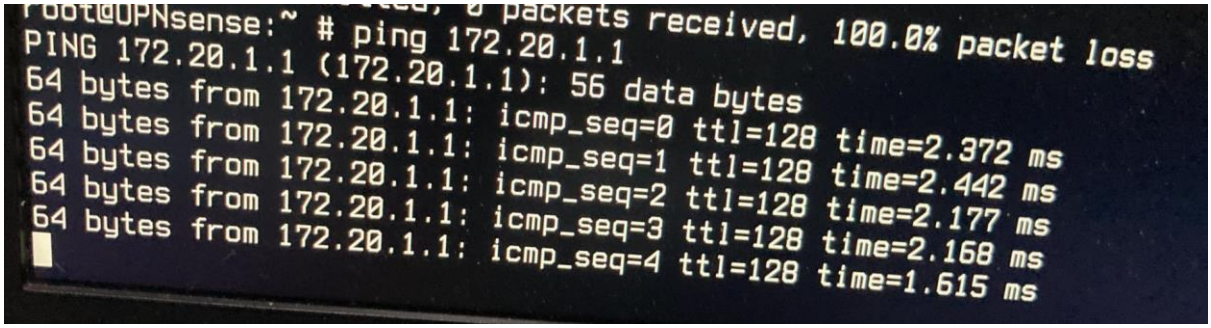

Figure 2. 4 : Test de connectivité

2.5.5 Interface graphique

Par défaut, l'adresse IP du LAN est 192.168.1.1 que nous avons modifié. A travers cette adresse (celle que nous avons définies), on pourra accéder à l'interface graphique de notre firewall qui présente beaucoup plus d'options que l'interface console (figure 2.5).

Il suffit juste de taper sur un navigateur quelconque d'un pc client le l'adresse IP pour accéder à l'interface graphique.

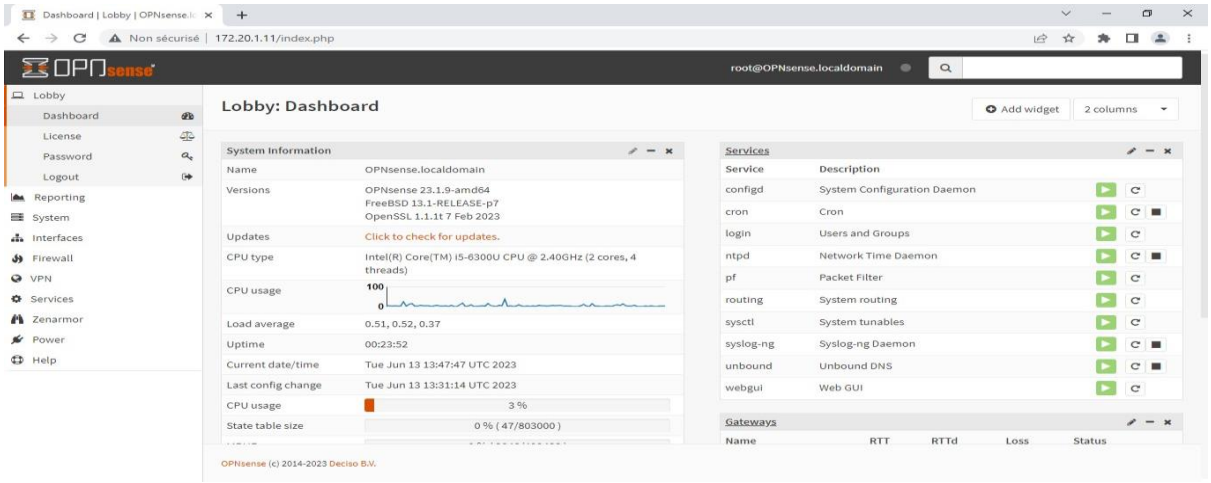

Figure 2. 5 : Interface graphique

Pour le bon fonctionnement d'OPNsense, on doit configurer le "wizard" (l'assistant). Il se trouve dans "system" (figure 2.6).

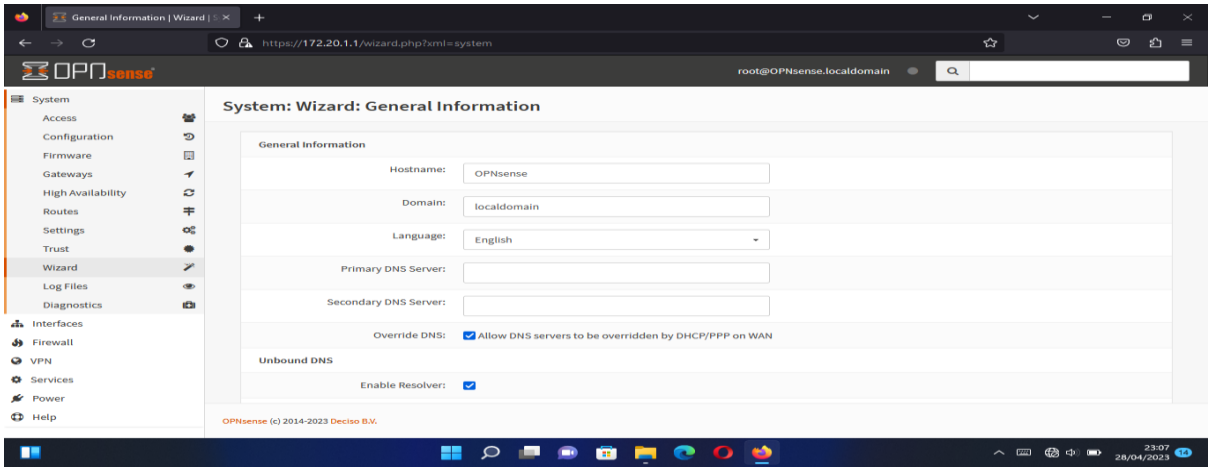

Figure 2. 6 : Configuration du wizard

Ainsi on remplit les différents champs jusqu'à la fin et juste après on aura notre firewall prêt à l'utilisation. Après cette étape, on va voir si on a des mises à jours à faire, si c'est le cas on le fait sinon on passe (figure 2.7).

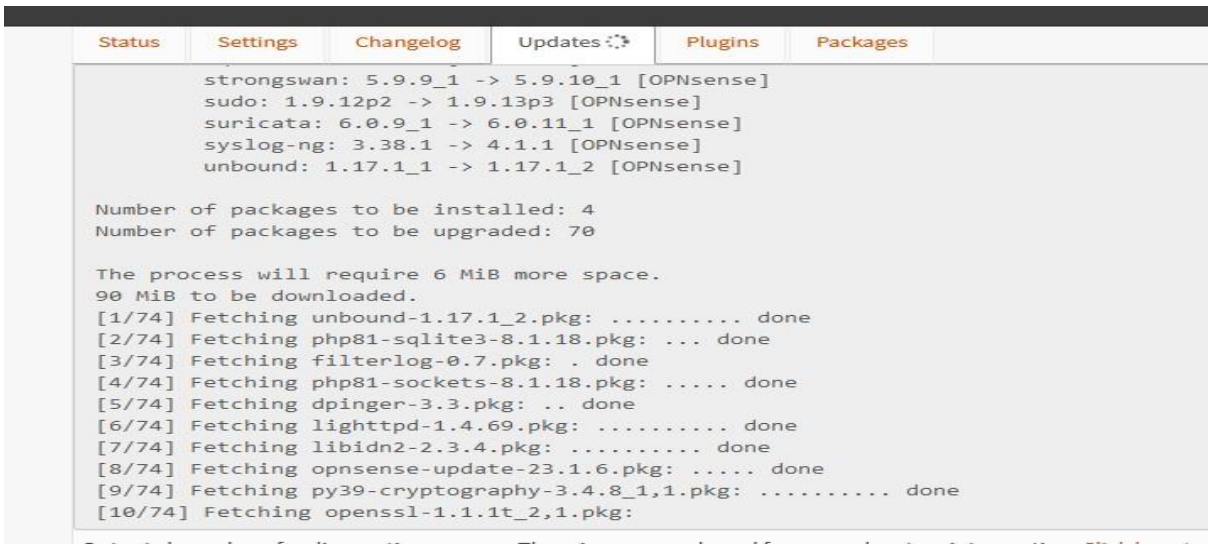

Figure 2. 7 : Mise à jour d'OPNsense

En plus des interfaces LAN et WAN, on a différents autres types d'interfaces présentes dans OPNsense (figure 2.8).

Figure 2. 8 : Les interfaces disponibles d'OPNsense

2.6 Gestion d'interface

En tant que solution de pare-feu complète, OPNsense prend en charge de nombreux types d'interfaces réseau qui sont :

- **Pont** : Un pont peut connecter deux interfaces réseau différentes dans le même segment de réseau. Par exemple, vous pouvez connecter une interface LAN connectée par câble avec une interface wifi à l'aide d'un pont (figure 2.9). De cette façon, l'appareil connecté dans les deux interfaces s'appuiera sur le même domaine de diffusion ou un même segment de réseau[4].

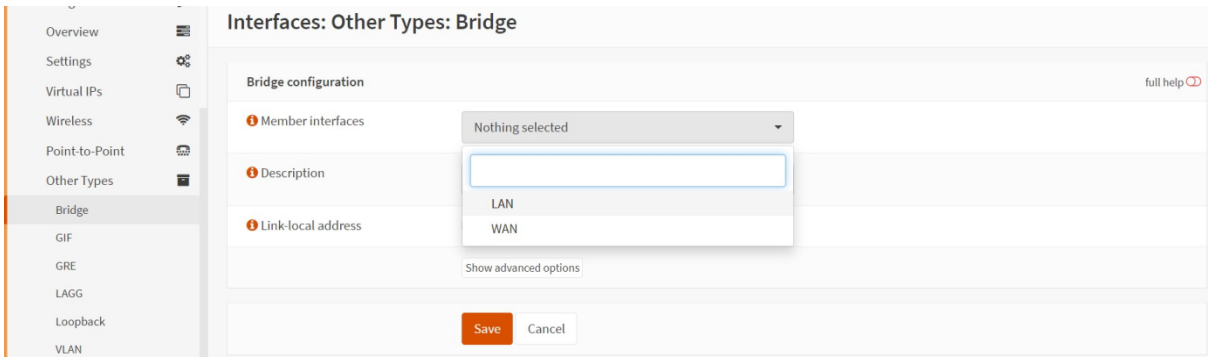

Figure 2. 9 : Interface bridge

❖ Interface de tunnel générique (GIF)

L'interface de tunnel générique est un type de configuration d'interface qui peut être utilisé pour tunneliser ipv6 via ipv4. Un exemple de son utilisation est de le configurer avec le courtier de tunnel ipv6 de Hurricane Electric, avec lequel vous pouvez accéder à Internet ipv6 en utilisant une connexion ipv4 existante [4].

❖ Encapsulation de routage générique(GRE)

L'encapsulation de routage générique est une configuration réseau qui permet à deux hôtes de tunneliser le trafic sans chiffrement. Un exemple de son utilisation est lorsque vous devez traverser certains protocoles qui ne sont pas pris en charge par le système intermédiaire [4].

❖ Agrégation de liens(LAGG)

L'agrégation de liens, également connue sous le nom de canal de port, peut fournir, comme son nom l'indique, une agrégation à l'aide de plusieurs interfaces réseau. Il peut être utilisé pour

augmenter la bande passante dans les réseaux locaux avec la condition préalable d'un appareil compatible, comme un commutateur, par exemple. Il peut prendre en charge le basculement puisqu'au moins une interface est active. Pour exécuter ces fonctions, LAGG devra être configuré des deux côtés de la connexion, avec le même protocole. Les protocoles actuels pris en charge par OPNsense sont les suivants (figure 2.10) : LACP, FEC, Failover, Load Balance, Round Robin [4].

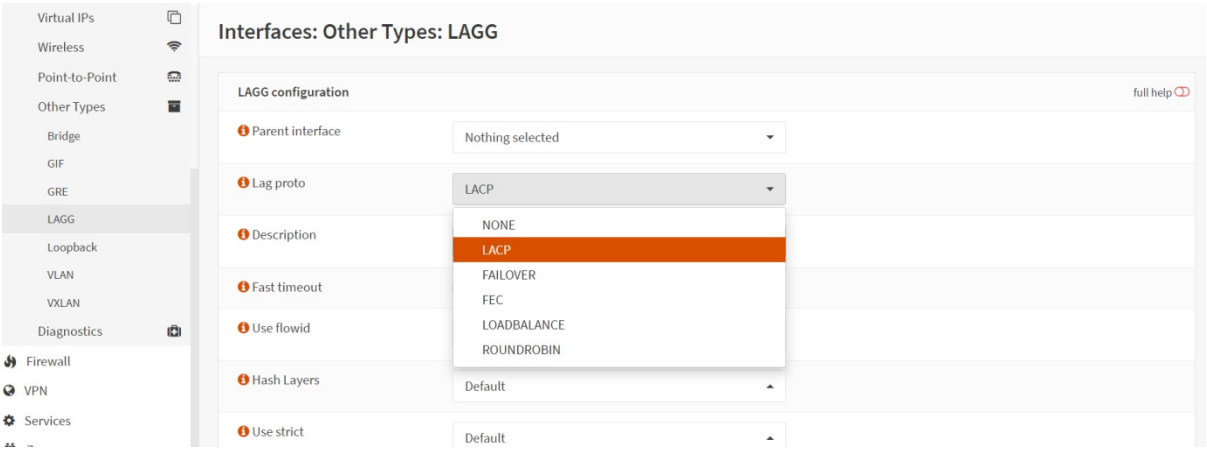

Figure 2. 10 : Interface LAGG

- **Interface de bouclage (Loop back)**

Le bouclage est une interface virtuelle couramment utilisée pour tester les communications locales dans un hôte. Vous pouvez facilement le tester en essayant d'envoyer un ping à l'adresse 127.0.0.1 (ou ::1 pour ipv6)[4].

- **Interface VLAN (802.1Q)**

La norme 802.1Q de l'IEEE, également connue sous le nom de Dot1q, est une norme de réseau permettant de prendre en charge les réseaux locaux virtuels (VLAN). Cette fonction est très utile lorsque nous devons définir différents réseaux à l'aide d'une seule interface de réseau physique, avec laquelle nous pouvons séparer les paquets provenant de différentes sources de réseau, en utilisant l'étiquetage VLAN (figure 2.11).

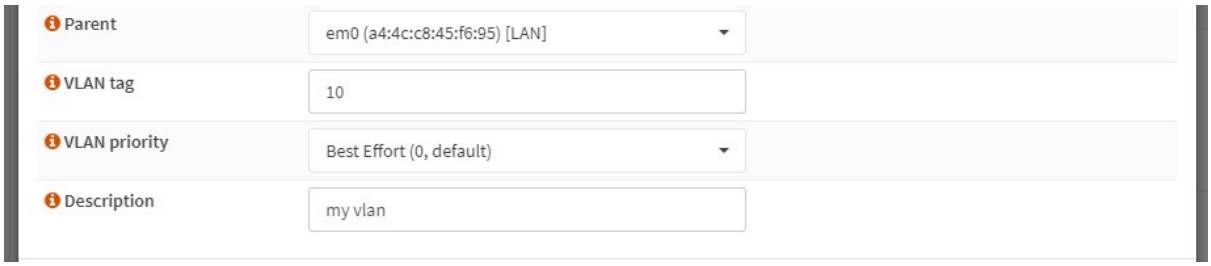

Figure 2. 11 : Interface Vlan

- **LAN virtuel extensible VxLAN**

Le réseau local extensible virtuel a été créé pour surmonter les limitations du vlan à l'ère du cloud. Il peut adresser jusqu'à 16 millions de réseaux logiques, tandis que vlan ne peut en faire que 4096. La plupart des technologies de virtualisation modernes le prennent en charge et son utilisation est plus courante dans les scénarios cloud.

2.7 firewall

2.7.1 Les règles

Dans l'option "firewall" puis "rules" on verra les différentes règles qu'on pourra créer que ce soit avec notre LAN, WAN ou Loop back … Voir la figure ci-dessous (figure 2.12)

Figure 2. 12 : Les règles par défaut d'OPNsense

Ceux-ci sont les règles par défaut qui permettent un accès internet aux hôtes du réseau local. Bien sûr on pourra modifier ces règles, tout comme on pourra en ajouter d'autres pour plus de sécurité. La création de nouvelles règles fera l'objet des prochains chapitres.

2.7.2 Les services

Il y a aussi différents services disponibles qu'on pourra configurer (figure 2.13).

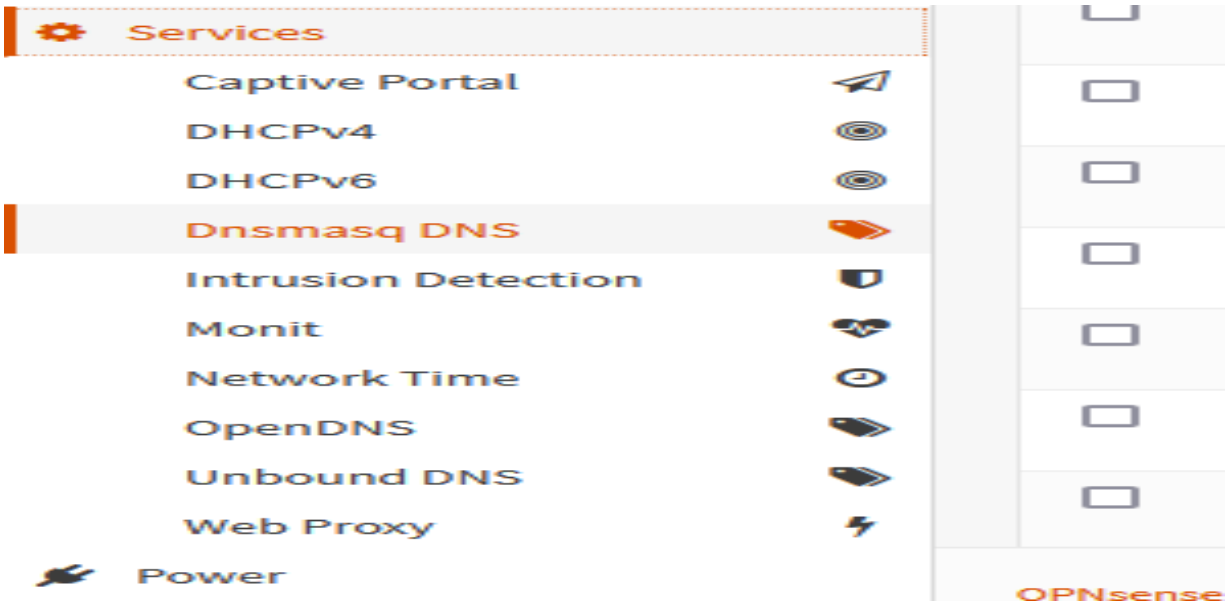

Figure 2. 13 : Les différents services d'OPNsense

2.7.3 Portail captif

Le portail captif vous permet de forcer l'authentification ou la redirection vers une page cliquable pour l'accès au réseau (figure 2.14). Ceci est couramment utilisé sur les réseaux de points d'accès, mais est également largement utilisé dans les réseaux d'entreprise pour une couche de sécurité supplémentaire sur l'accès sans fil ou Internet [15].

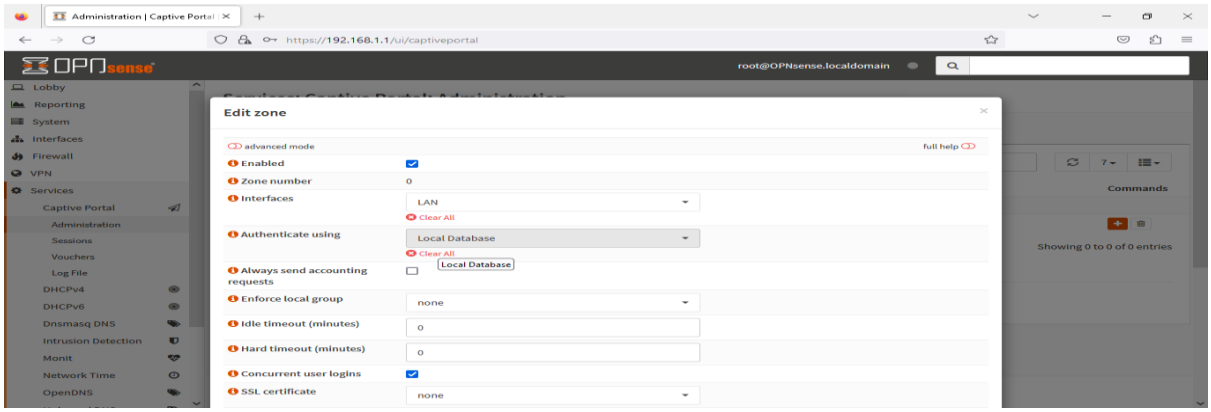

Figure 2. 14 : Le portail captif

2.7.4 Serveur et relais DHCP

Le protocole de configuration dynamique des hôtes (DHCP), comme son nom l'indique, est un protocole permettant de louer des adresses IP à des hôtes dans un réseau. OPNsense possède à la fois des capacités de serveur et de relais ; le plus courant, le serveur DHCP, est utilisé pour définir un pool d'adresses configuré dynamiquement pour les hôtes du réseau. Le second est utilisé lorsque les hôtes ne peuvent pas accéder directement au serveur DHCP, par exemple si le serveur DHCP repose sur un autre segment de réseau (figure 2.15)[4].

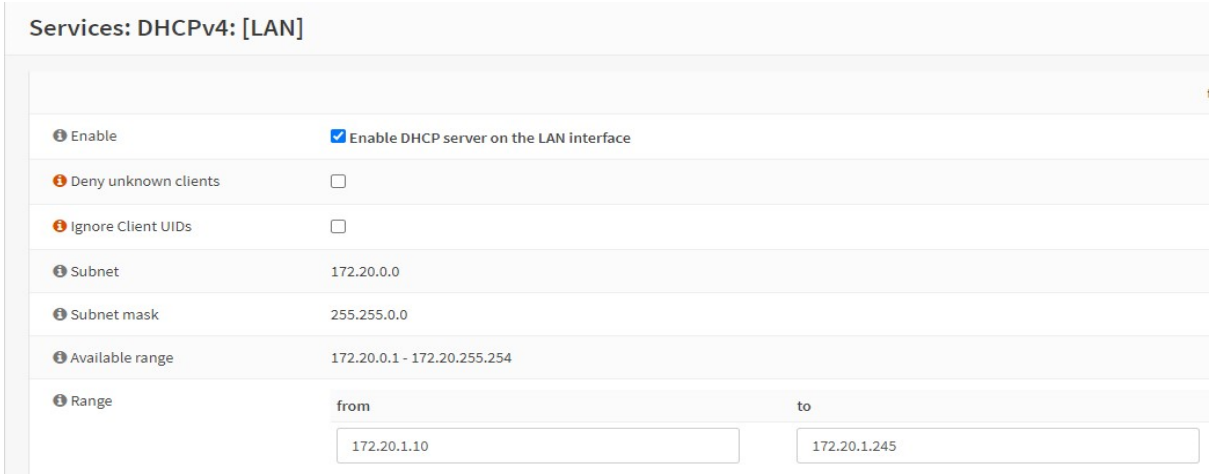

Figure 2. 15 : Le serveur DHCP

2.7.5 Système de prévention des intrusions

C'est l'une des améliorations les plus significatives d'OPNsense par rapport à PFsense (figure 2.16). Le service utilisé pour OPNsense est suricata. Contrairement à Snort qui était utilisé dans le PFsense, le système IPS en ligne d'OPNsense est basé sur Suricata et utilise Netmap pour améliorer les performances et minimiser l'utilisation du processeur. Ce système d'inspection approfondie des paquets est très puissant et peut être utilisé pour atténuer les menaces de sécurité à la vitesse du fil [15].

Figure 2. 16 : Système de détection d'intrusion

2.7.6 Proxy de mise en cache de transfert

Ceci est également connu sous le nom de proxy Web. Ce service est natif d'OPNsense ; il peut être utilisé pour mettre en cache des composants de sites Web tels que JavaScript, CSS, images, polices, etc. Vous pouvez également l'utiliser pour contrôler l'accès à Internet à l'aide de l'authentification, bloquer le site Web avec des listes de blocage, créer des listes de contrôle d'accès de base et intercepter le trafic HTTPS/SSL en mode transparent (figure 2.17) [15].

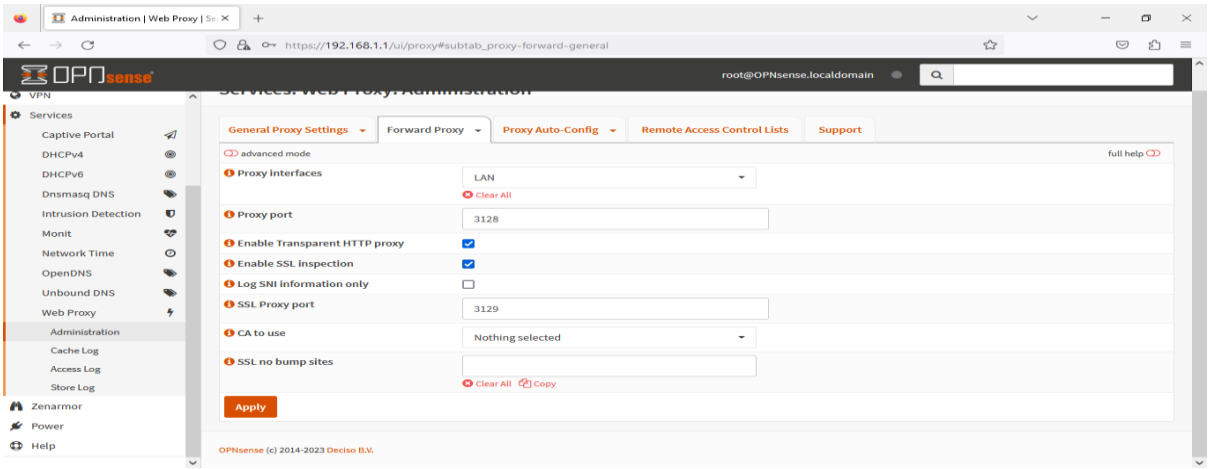

Figure 2. 17 : La fonction proxy

2.8 Autres fonctionnalités de base

Les fonctionnalités de base d'OPNsense sont toutes fournies avec l'installation par défaut d'OPNsense, sans aucun plugin. Les principales fonctionnalités sont les suivantes :

2.8.1 Pare-feu à inspection dynamique

Un pare-feu avec état est un pare-feu qui garde une trace de l'état des connexions réseau (telles que les flux TCP, les communications UDP) qui le traversent. OPNsense propose le regroupement des règles de pare-feu par catégorie, une fonctionnalité intéressante pour les configurations réseau plus exigeantes.

2.8.2 Modélisation de trafic

OPNsense utilise un autre composant du pare-feu, ipfw, le filtrage de paquets natif de FreeBSD, pour classer et prioriser les paquets pour la mise en forme du trafic.Avec la modélisation de trafic, vous pourrez limiter et réserver la bande passante et prioriser le trafic de qualité de service (QoS) (figure 2.18, figure 2.19)[4].

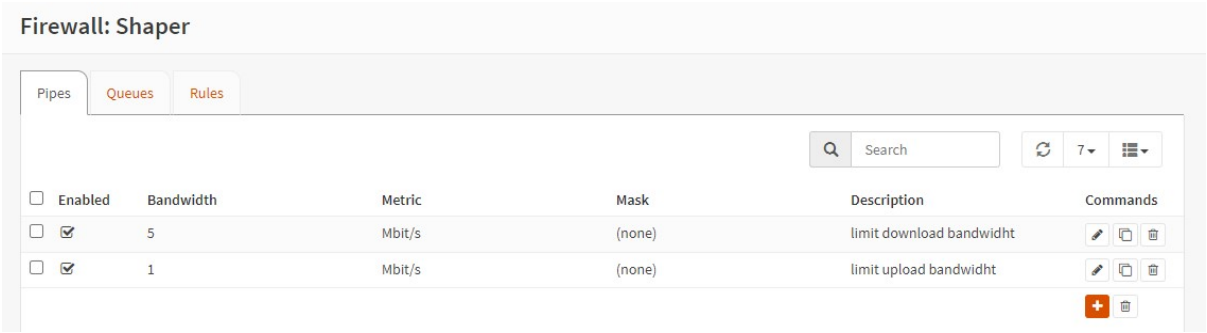

Figure 2. 18 : Définition de la bande passante

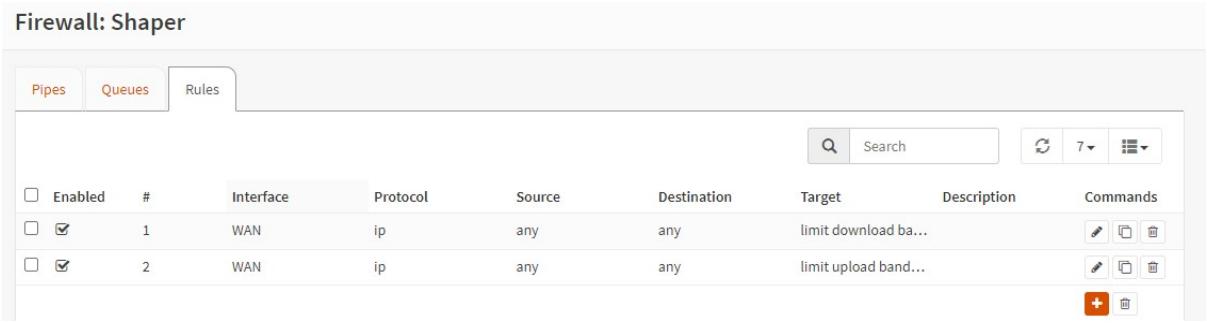

Figure 2. 19 : Modélisation du trafic

Ici, on a deux règles qui permettent de limiter la bande passante de téléchargement et de télé versement respectivement.

- La 1ere règle limite la bande passante de téléchargement à 5Mbits.
- La 2eme règle limite la bande passante de télé versement à 1Mbits.

2.8.3 Redirecteur DNS

Le système de noms de domaine (DNS) est la base de notre Internet moderne, sans quoi nous aurions besoin de connaître l'adresse IP de chaque site Web pour y accéder. Le serveur DNS et le redirecteur se chargent de résoudre les domaines en adresses IP. OPNsense a plus d'un service natif pour faire ce travail, Unbound et Dnsmasq ; les deux sont des résolveurs. Pour activer un serveur DNS, tel que bind, vous devrez installer le plugin bind.

2.8.4 Réseau privé virtuel(VPN)

Les options VPN disponibles dans le noyau OPNsense sont IPsec et OpenVPN (figure 2.20). Les deux peuvent être utilisés comme configurations de site à site et de client à site pour connecter un utilisateur en toute sécurité sur Internet.

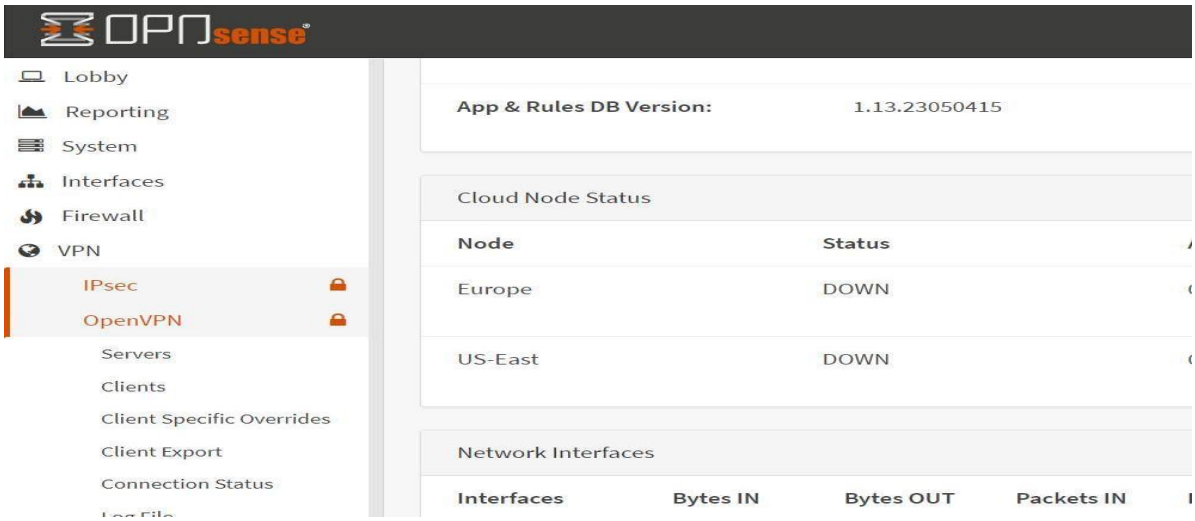

Figure 2. 20 : Les vpn disponibles

2.8.5 Haute disponibilité (CARP)

OPNsense utilise le protocole de redondance d'adresse commune ou CARP pour le basculement matériel. Deux pare-feu ou plus peuvent être configurés en tant que groupe de basculement. Si une interface tombe en panne sur le primaire ou si le primaire se déconnecte

entièrement, le secondaire devient actif. L'utilisation de cette fonctionnalité puissante d'OPNsense crée un pare-feu entièrement redondant avec un basculement automatique et transparent. Lors du passage au réseau de secours, les connexions resteront actives avec une interruption minimale pour les utilisateurs [15].

2.8.6 Sauvegarde sur le cloud

OPNsense prend en charge la sauvegarde cloud cryptée de votre configuration avec la possibilité de conserver les sauvegardes des fichiers plus anciens (histoire). À cette fin, le support de Google Drive a été intégré dans l'interface utilisateur [15].

2.8.7 Exportation et analyses Netflow - Insight

Netflow est une fonctionnalité de surveillance, inventée par Cisco, elle est implémentée dans le noyau FreeBSD avec ng_netflow (Netgraphe). Étant donné que Netgraph est une implémentation du noyau, il est très rapide avec peu de surcharge par rapport à softflow ou pfflowd. Alors que de nombreuses solutions de surveillance telles que Nagios, Cacti et vnstat ne capturent que les statistiques de trafic, Netflow capture les flux de paquets complets, y compris la source, l'adresse IP de destination et le numéro de port. OPNsense offre un support complet pour exporter les données Netflow vers des collecteurs externes ainsi qu'un analyseur complet appelé Insight pour le sur-boîte analyse et suivi en direct. OPNsense est la seule solution open source avec un analyseur Netflow intégré dans son interface utilisateur graphique [15].

2.9 Les plugins

OPNsense nous offre la possibilité d’installer plusieurs plugins en fonction de notre besoin, comme mentionné précédemment, chaque nouvelle mise à jour arrive avec de nouveaux plugins donc avec de nouvelles fonctionnalités.
Dans ce travail, le plugin qui nous intéresse est le plugin zenarmor.

2.9.1 Installation du plugin Zenarmor

2.9.2 Pare-feu de nouvelle génération avec zenarmor

Zenarmor est un plugin pour le pare-feu OPNsense qui fournit des fonctionnalités de pointe de nouvelle génération. Si vous recherchez des fonctionnalités telles que le contrôle d’application,

Analyse du réseau et Contrôle TLS, Zenarmor est le produit que vous recherchez. Zenarmor renforce votre pare-feu avec les fonctionnalités de nouvelle génération suivantes :

- ➢ Contrôle des applications ;
- ➢ Contrôle des applications cloud (contrôles Web 2.0) ;
- ➢ Analyse avancée du réseau ;
- ➢ Filtrage Web et sécurité ;
- ➢ Renseignements sur les menaces dans le cloud ;
- ➢ Filtrage et création de rapports basés sur l'utilisateur ;
- ➢ Intégration Active Directory ;
- ➢ API RESTful ;
- ➢ Gestion et rapports centralisés basés sur le cloud ;
- ➢ Mise en forme et hiérarchisation du trafic basé sur les applications / catégories Web ;
- ➢ Filtrage basé sur des politiques et QoS ;
- ➢ Prévention des menaces chiffrées ;
- ➢ Inspection TLS complète de tous les ports (pour chaque port TCP, pas seulement HTTPS) [15].

Alors pour l'installation, on se rend dans système>Firmware>Plugins, puis on tape 'os-sensei' dans la barre de recherche pour avoir les plugins qui permettent d'installer zenarmor (figure 2.21). Les 3 plugins qui permettent d'installer zenarmor sont : os-sensei ; os-sensei-agent ; os-sensei-updater.

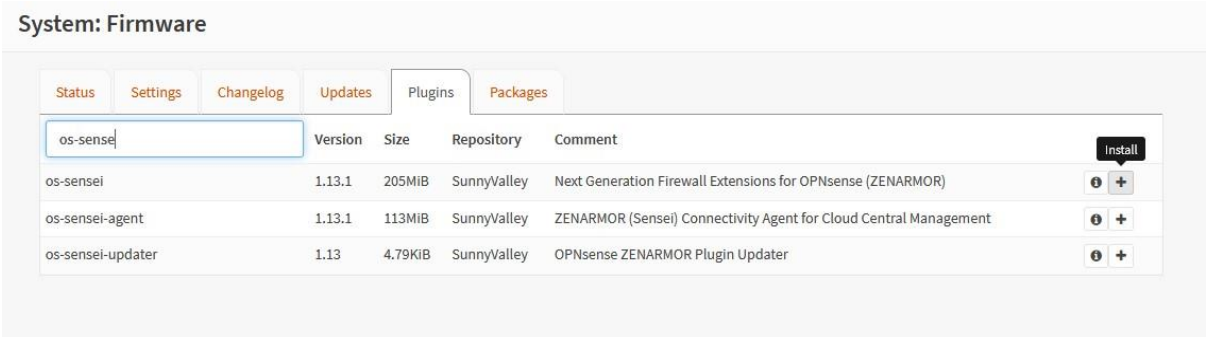

Figure 2. 21 : Les plugins de zenarmor

2.9.3 Installation des plugins de zenarmor

Ces trois plugins doivent être installés un à un, voir la figure ci-dessous (figure 2.22).

```
***GOT REQUEST TO INSTALL***
Currently running OPNsense 23.1.7_3 at Sun May 21 12:09:48 UTC 2023
Updating OPNsense repository catalogue...
OPNsense repository is up to date.
Updating SunnyValley repository catalogue...
SunnyValley repository is up to date.
All repositories are up to date.
The following 3 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
        os-sensei: 1.13.1 [SunnyValley]
        os-sensei-updater: 1.13 [SunnyValley]
        ubench: 0.32 [SunnyValley]

Number of packages to be installed: 3

The process will require 205 MiB more space.
52 MiB to be downloaded.
[1/3] Fetching ubench-0.32.pkg: . done
[2/3] Fetching os-sensei-updater-1.13.pkg: . done
[3/3] Fetching os-sensei-1.13.1.pkg: .
```

Figure 2. 22 : Installation des plugins de zenarmor

Après l'installation de ces plugins, on actualise la page pour avoir Zenarmor en bas parmi les options à gauche (figure 2.23).

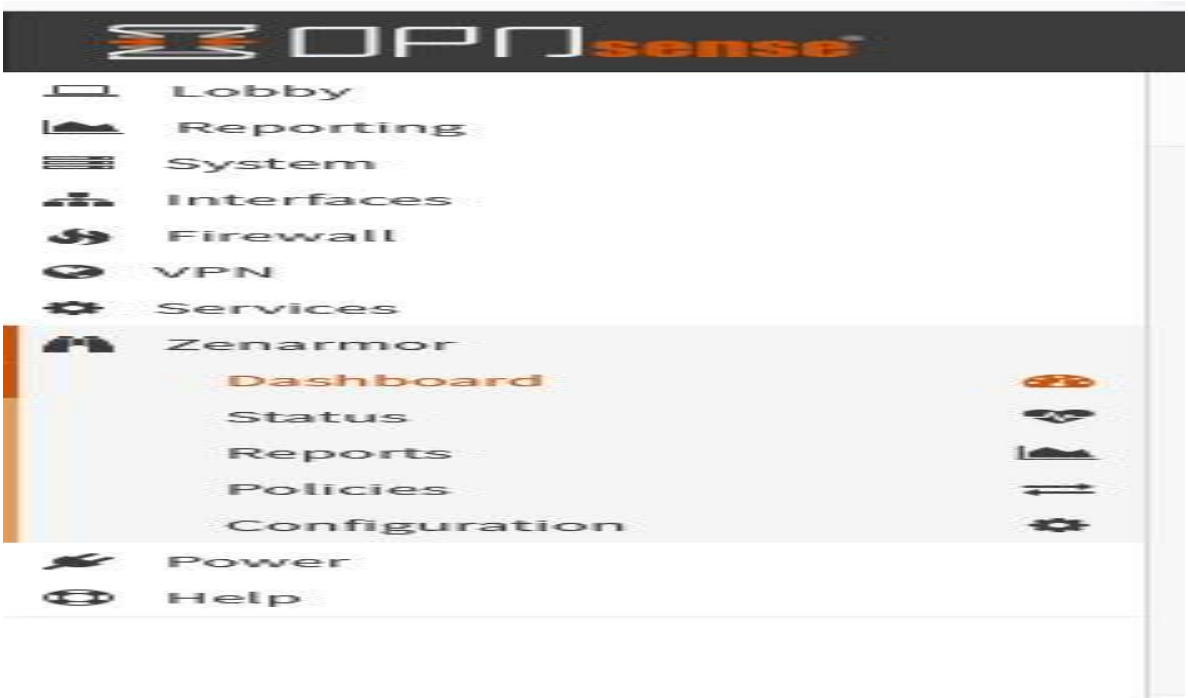

Figure 2. 23 : les menus de zenarmor

Bienvenue dans Zenarmor, qui contient ses propres menus comme on peut le voir dans l'image ci-dessus (figure 2.23). Une fois installée, zenarmor a besoin d'une configuration minimale pour fonctionner.

On sautera sur plusieurs de ces étapes et vous montrera que l'essentiel.

Figure 2. 24 : Début de la configuration minimale de zenarmor

Ci-dessus (figure 2.24) est la configuration de la base de données des rapports. Elle permet d'afficher des statistiques des différentes activités qui passent par notre firewall.

Après cette dernière configuration, on va maintenant choisir le mode de déploiement de notre firewall, ici vous pouvez voir dans l'image ci-dessous (figure 2.25) qu'on le déploie comme routeur sur la couche 3 du modèle OSI, puis on choisit l'interface à protéger (dans notre cas on a choisi LAN(em0) qui est l'interface de notre réseau LAN.

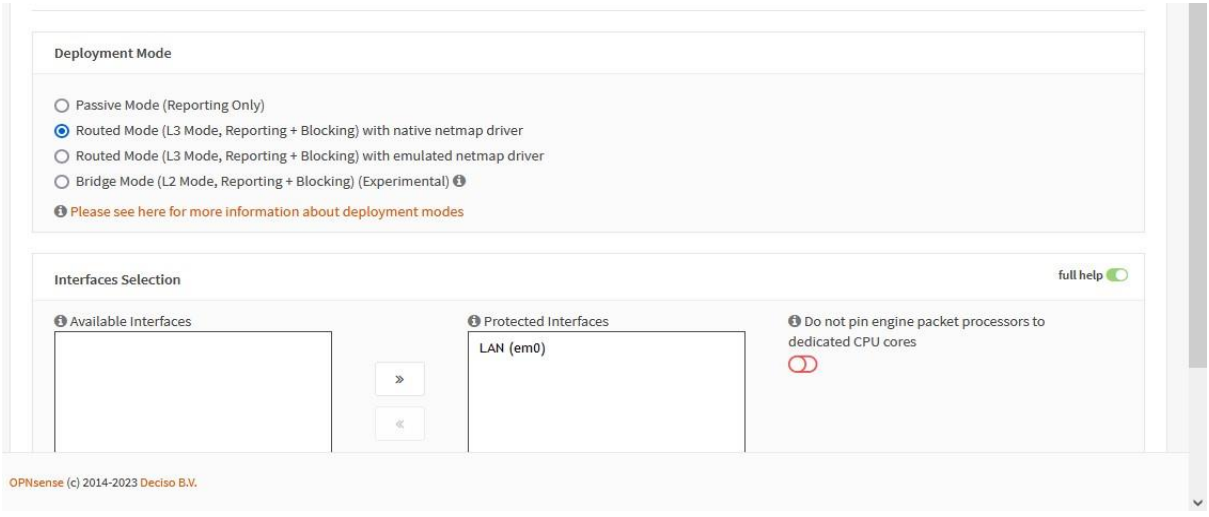

Figure 2. 25 : Mode de déploiement d'OPNsense

Puis maintenant on doit déterminer la taille du déploiement (en d'autres termes la taille de notre LAN). On a un petit réseau c'est pourquoi on a choisi 25(hôtes) mais on pourrait également choisir 15(hôtes) (figure 2.26)

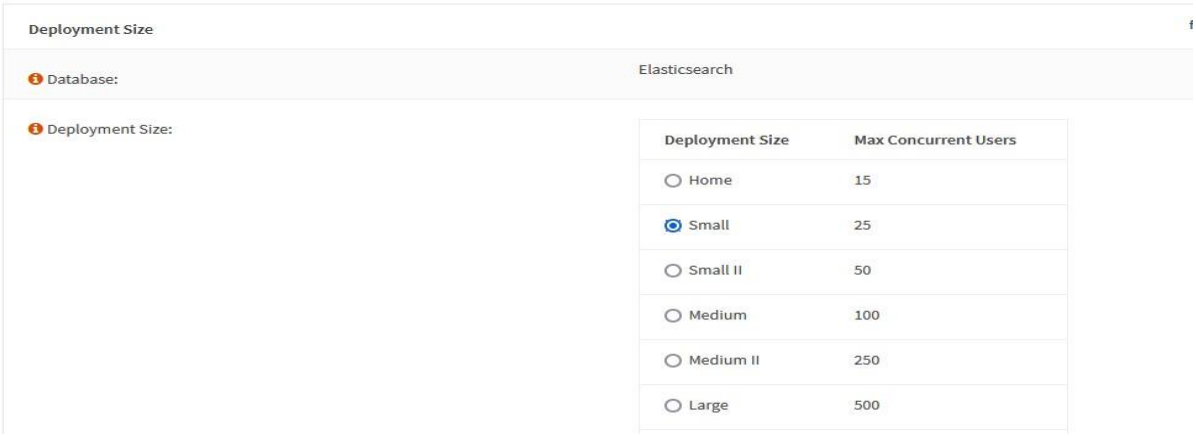

Figure 2. 26 : La taille du réseau

Enfin la configuration minimale de zenarmor prend fin, et on peut constater qu'il a été bien configuré à travers l'image ci-dessous (figure 2.27).

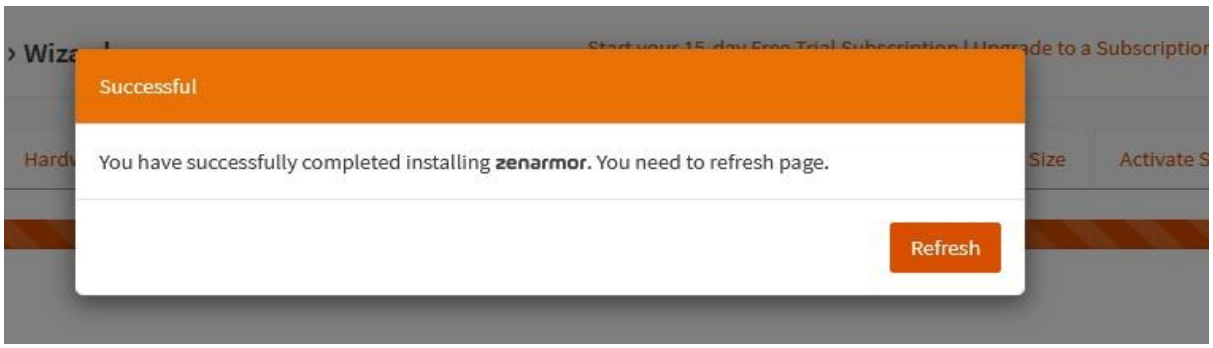

Figure 2. 27 : Finition de la configuration minimale d'OPNsense

Ci-dessous, une image du plugin après installation et configuration (figure 2.28)

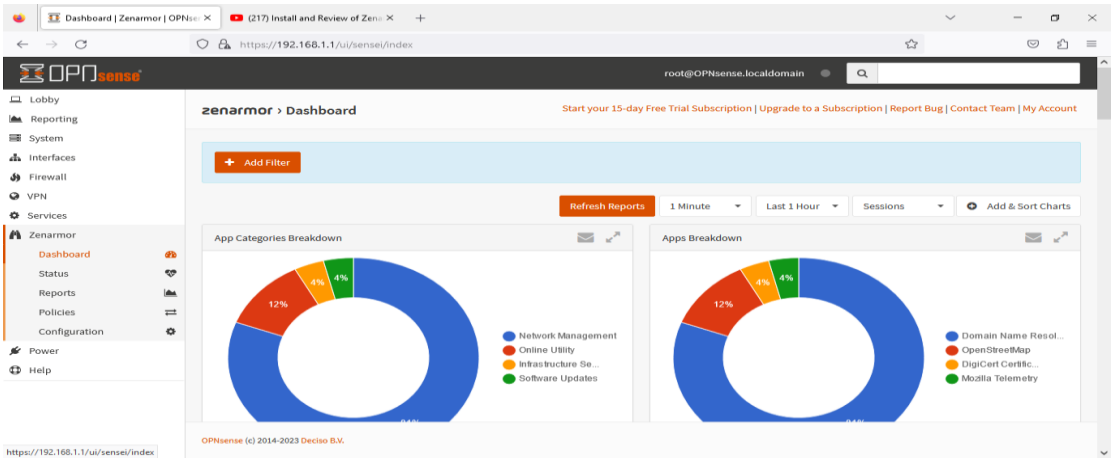

Figure 2. 28 : Le Dashboard de zenarmor

Notre firewall est maintenant prêt pour l'emploi.

2.10 Conclusion

Dans ce chapitre, on a parlé d'OPNsense théoriquement aussi bien que pratiquement. On a décrit brièvement les fonctionnalités de base d'OPNsense avec quelques exemples pratiques et on a installé et configuré le plugin zenarmor qui va beaucoup nous aider dans la suite de notre travail. C'est un chapitre clé, qui nous a permis d'avoir dans un premier temps des connaissances générales pratiques sur les firewalls et dans un second temps la maîtrise de ce puissant firewall open source. L'exploitation de ces connaissances fera l'objet du prochain chapitre

Chapitre 3 : Mise en œuvre

3.1 Introduction

Dans le chapitre précédent, on a vu les principales fonctionnalités de base d'OPNsense, et différentes étapes pour son utilisation. Dans ce chapitre, nous allons mettre en place nos différents serveurs, nous assurer de leur liaison avec le pare-feu, ainsi que leur bonne administration. D'une manière brève, ce chapitre est axé sur la création, la configuration et la sécurité de notre réseau local avec le pare-feu OPNsense tout en établissant des tests.

3.2 Architecture globale

Notre projet consiste à mettre en place un réseau d'entreprise ainsi que d'en assurer la sécurité par le pare-feu OPNsense. Pour faire ce travail, nous avons utilisé de nombreux outils comme phpldapadmin, des distributions linux (Ubuntu et CentOS), le pare-feu OPNsense, ainsi que d'autres logiciels. On va configurer OPNsense puis valider ses fonctionnalités en établissant une série de test qui dépendent du :

- ➢ Contrôle de notre réseau d'entreprise
- ➢ Autorisation et contrôle à l'accès au WAN
- ➢ Limitation des droits des utilisateurs
- ➢ Restrictions à l'accès des employés aux sites nuisibles.

La figure ci-dessous (Figure 3.1**)** représente l'architecture globale de notre réseau local, elle comprend :

- ➢ Un routeur relié au réseau WAN ;
- ➢ OPNsense ;
- ➢ Un commutateur qui relie les clients ;
- ➢ Deux postes clients.

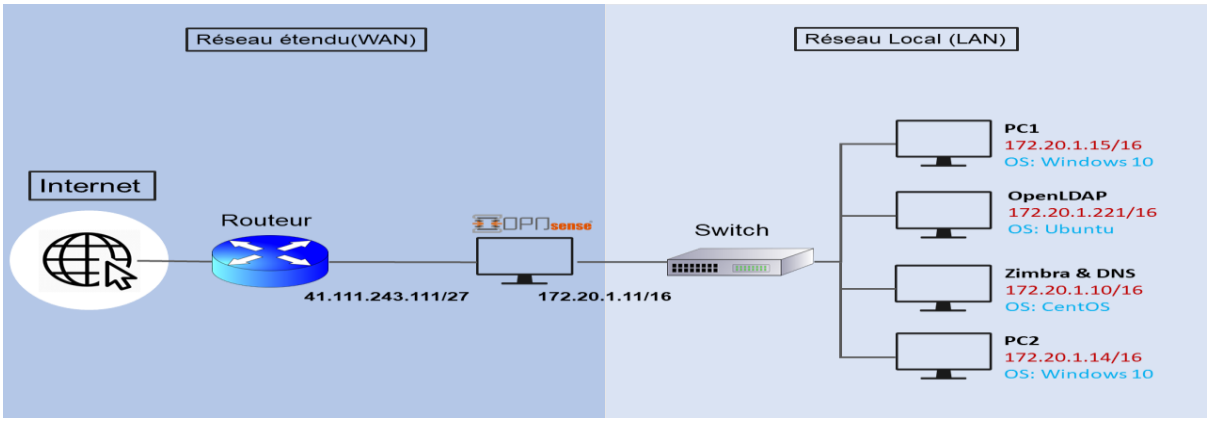

Figure 3. 1 : L'architecture globale

3.3 Description des outils utilisés

3.3.1 Phpldapadmin

Phpldapadmin est une interface écrite en PHP qui permet de modifier facilement et via une interface conviviale un annuaire OpenLDAP. Elle permet de gérer plusieurs annuaires LDAP et implémente plusieurs modes d'authentification [16].

3.3.2 CentOS

CentOS (**C**ommunity **ent**erprise **O**perating **S**ystem) est une distribution GNU/Linux destinée aux serveurs (et aux postes de travail). Tous ses paquets, à l'exception du logo, sont des paquets compilés à partir des sources de la distribution RHEL (Red Hat Enterprise Linux), éditée par la société Red Hat. Elle est donc quasiment identique à celle-ci et se veut 100 % compatible d'un point de vue binaire [17].

3.3.3 Ubuntu

Ubuntu est un système d'exploitation GNU/Linux fondé sur Debian. Il est développé, commercialisé et maintenu pour les ordinateurs individuels, les serveurs etc…

3.4 Réalisation

3.4.1 Installation et configuration de notre serveur d'authentification

Il y a plusieurs moyens d'authentifier les utilisateurs de notre réseau local lorsqu'ils veulent partir sur internet comme authentification par un serveur radius, active directory ou OpenLDAP.

Dans ce travail, le serveur d'authentification est OpenLDAP.

- Tout d'abord avant de commencer ce travail, on installe le système d'exploitation Ubuntu qui est une distribution de Linux. Après la bonne installation de celle-ci, on s'assure également de sa bonne configuration.
- On doit maintenant télécharger les paquets OpenLDAP (figure 3.2), pour faire ça, on va sur terminal puis on met à jour les paquets disponibles sur notre Ubuntu. Après on introduit la commande suivante : "apt-get install slapd ldap-utils"

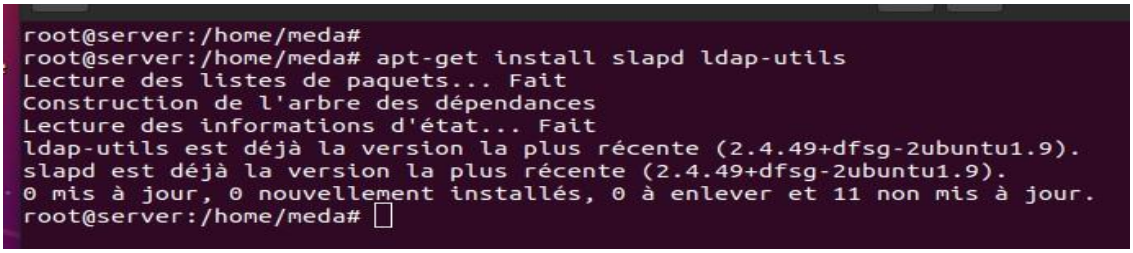

Figure 3. 2 : Packet d'installation d'OpenLDAP

Les paquets sont déjà installés. Une fois les paquets installés, on s'attaque maintenant à la configuration. Ci-dessous sont les images de configuration (figure 3.3).

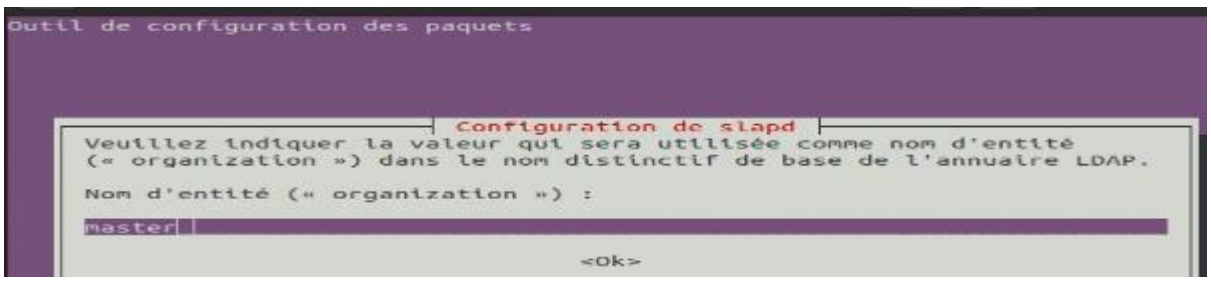

Figure 3. 3 : Définition du nom de l'entité

On crée un compte administrateur puis on l'attribue un mot de passe comme dans la figure en bas (figure 3.4).

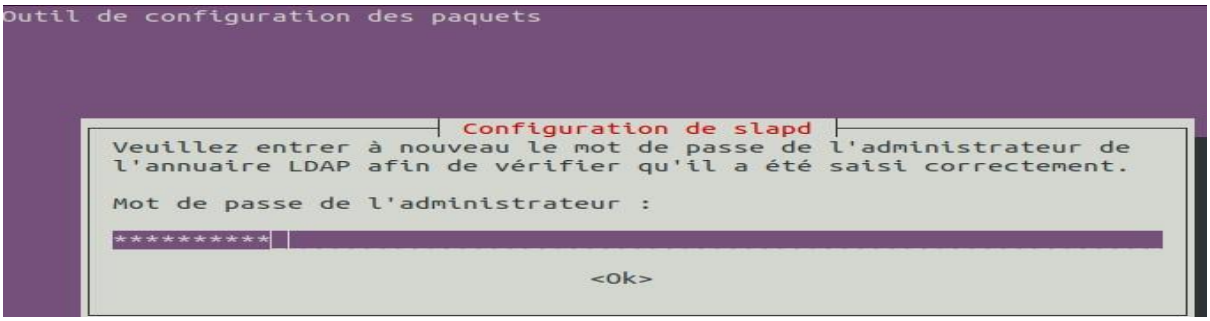

Figure 3. 4 : Définition du compte administrateur

On crée un nom de domaine (figure 3.5) ici le nom de domaine est “ldap.com”.

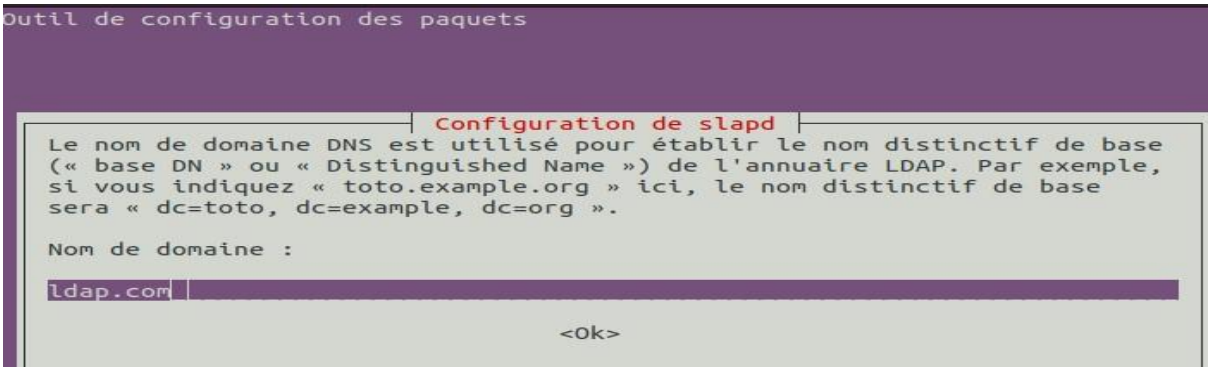

Figure 3. 5 : Définition du nom de domaine

Puis après la configuration on tape la commande “ldapsearch -x” pour voir s’il a été bien configuré. Voir figure 3.6.

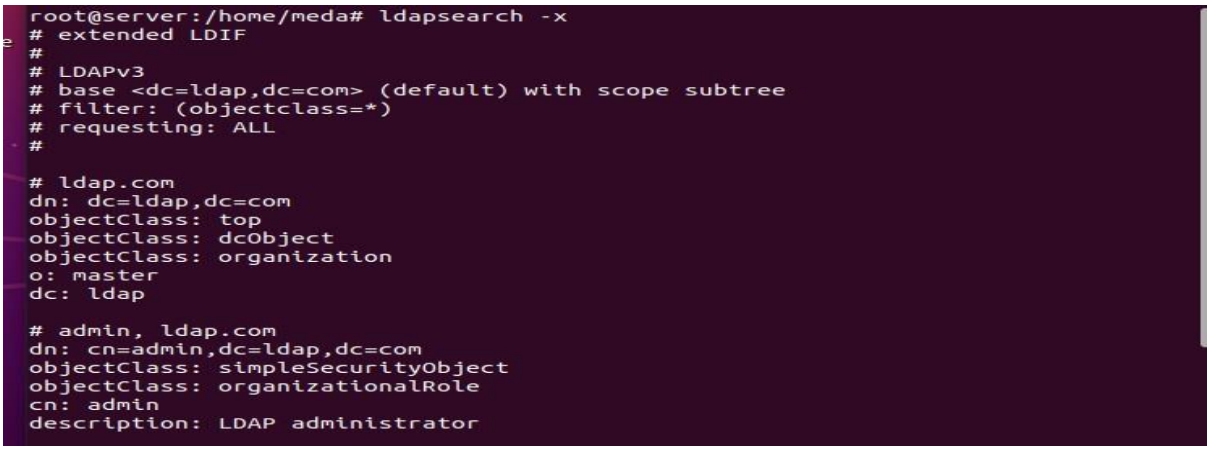

Figure 3. 6 : Validation de la configuration d’OpenLDAP

On voit qu'il a été bien configuré et on utilise LDAP version 3.

Tout ce qu'on a vu jusqu'à présent se fait avec l'interface shell, pour une manipulation plus fluide et simple on va devoir passer à une interface graphique. Pour cela, on a besoin de l'outil phpldapadmin.

3.4.2 Installation et configuration de phpldapadmin

Comme la fois précédente, on télécharge les paquets phpldapadmin et on les installe en tapant la commande (figure 3.7) "apt-get install phpldapadmin"

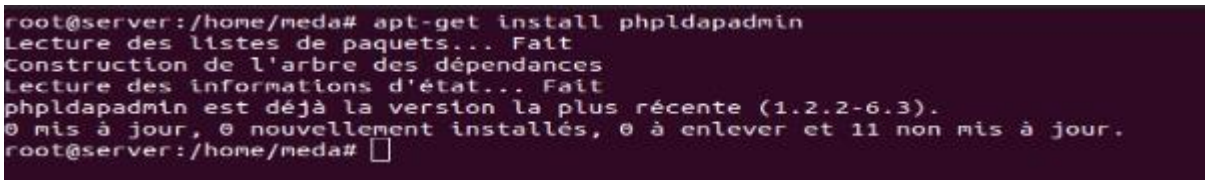

Figure 3. 7 : Installation de phpldapadmin

Les paquets sont déjà installés. On doit maintenant modifier le fichier de configuration de phpldapadmin pour qu'il se connecte au serveur LDAP en tapant la commande "gedit /etc/phpldapadmin/config.php". Voir figure 3.8.

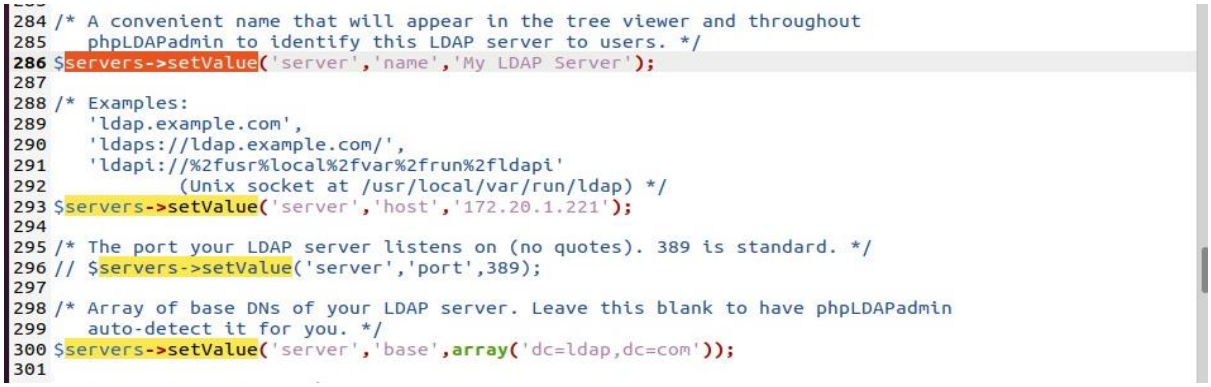

Figure 3. 8 : Configuration du fichier named

On modifie les informations suivantes :

- ➢ Le nom du serveur (My LDAP server) ;
- ➢ L'adresse du serveur qui va nous permettre d'accéder à l'interface graphique (172.20.1.221) ;

- Port de LDAP (389) ;
- Le nom de domaine (ldap.com).

Après ces modifications, on redémarre le service apache2.

Maintenant pour accéder à l'interface graphique de notre serveur LDAP, il suffit tout simplement de taper dans la barre de recherche du navigateur cette url "https://172.20.1.221/phpldapadmin/".

Pour se connecter(figure3.9), on utilise la base DN qu'on a configurée depuis le début c'est à dire "cn=admin,dc=ldap,dc=com" suivi du mot de passe administrateur (on se connecte en tant qu'administrateur).

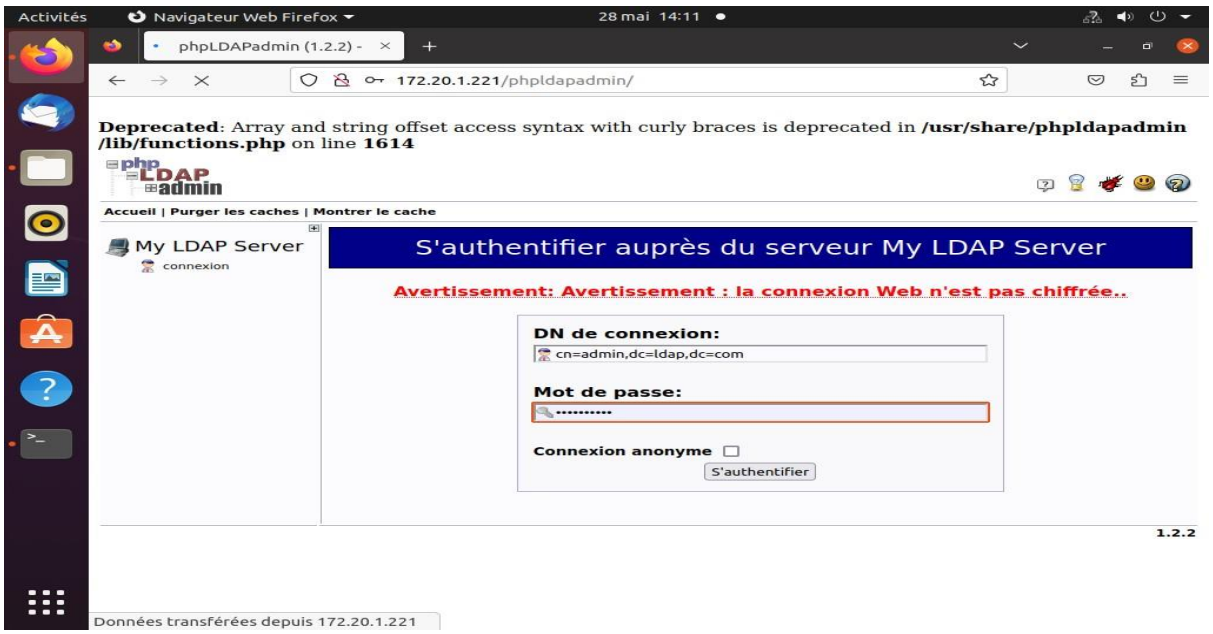

Figure 3. 9 : Interface graphique d'OpenLDAP

Après l'authentification, on peut maintenant faire tout ce qu'on veut avec notre serveur ldap y compris création des groupes des utilisateurs des calendriers etc… Dans ce travail, ce qui nous intéresse est la création des groupes et d'y ajouter des utilisateurs (figure 3.10).

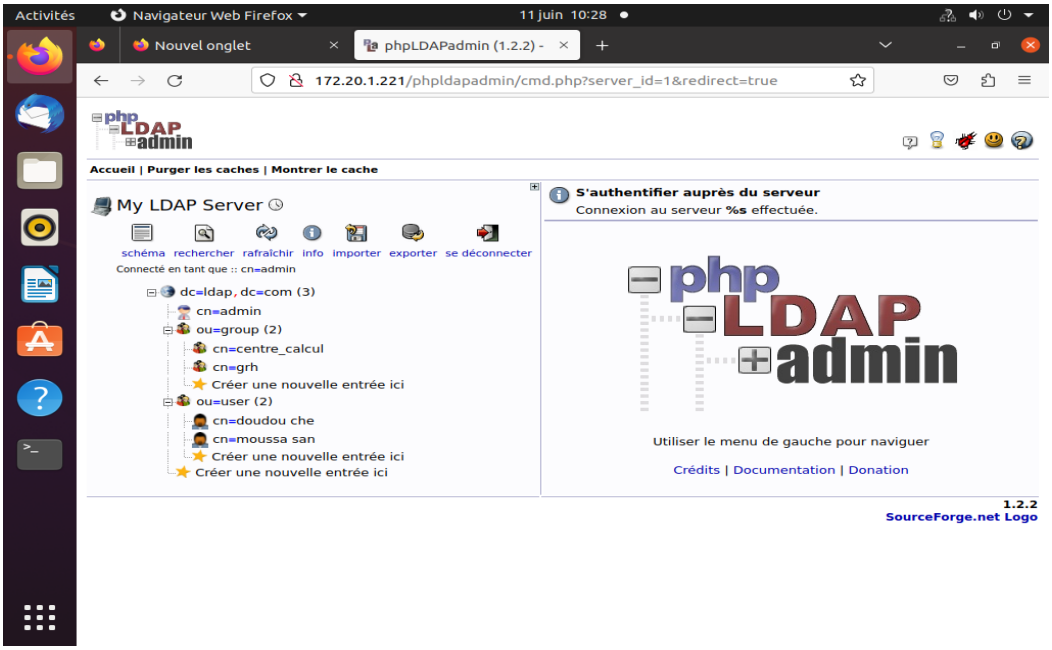

Figure 3. 10 : Les groupes et utilisateurs crées dans OpenLDAP

On a créé deux groupes (centre de calcul et départ Electro) et deux utilisateurs (moussa san et doudou che).

La dernière étape consiste à lier notre serveur d'authentification à notre pare-feu pour que chaque utilisateur du réseau local s'authentifie lorsqu'il veut avoir accès à internet. Pour ce faire, il y a une fonctionnalité dans OPNsense qu'on va utiliser. On va dans system>access>servers puis on entre les informations suivantes :

- ➢ Nom de l'authentification ;
- ➢ Adresse IP du serveur d'authentification ;
- ➢ Port ;
- ➢ Base DN de LDAP (cn=admin, dc=ldap, dc=com) ainsi que le mot de passe ;
- ➢ Introduire les groupes et les utilisateurs créés dans notre serveur ldap.

Puis sauvegarder la configuration (figure 3.11).

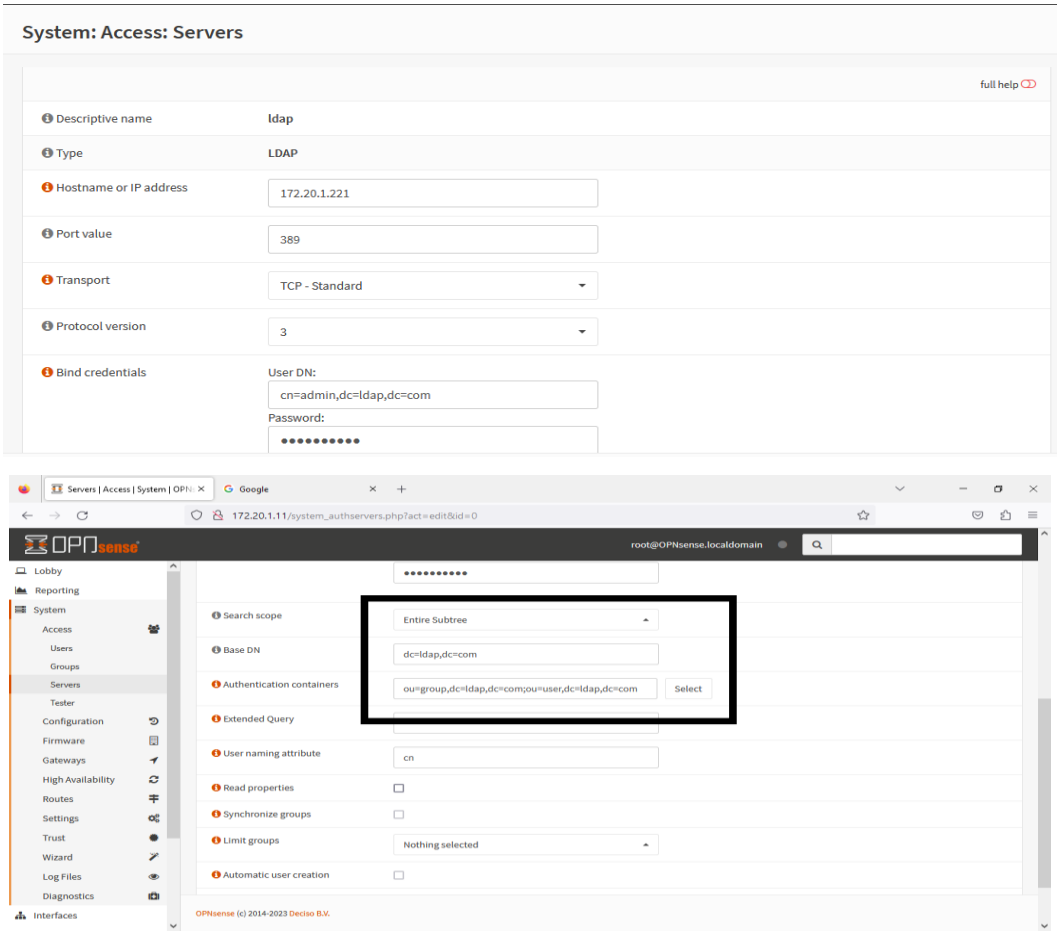

Figure 3. 11 : Liaison du pare-feu avec le serveur OpenLDAP

On vient de configurer notre serveur au niveau de notre pare-feu, maintenant on va faire un test (figure 3.12) pour voir si c'est bien configuré.

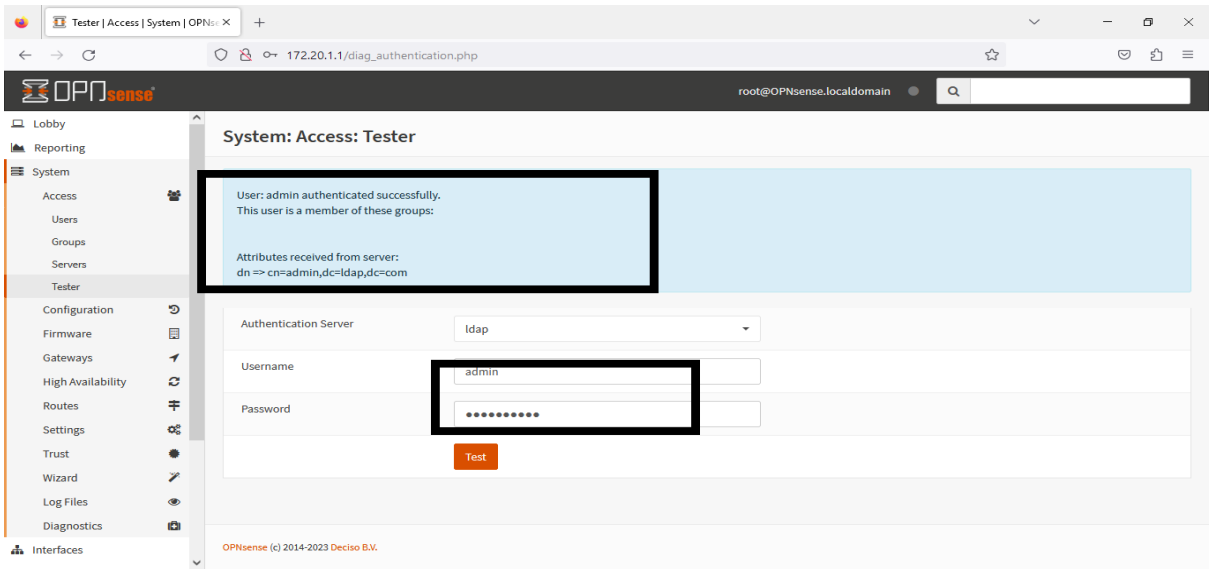

Figure 3. 12 : Vérification de la liaison

L'authentification a été un succès, le serveur et le pare-feu sont bien liés.

Maintenant les utilisateurs internes qui veulent partir sur internet sont obligés de s'authentifier avec notre serveur openldap alors on doit configurer le portail captif (une fonctionnalité d'OPNsense) qui permet de leur rediriger vers une page d'authentification à chaque fois qu'ils veulent partir sur internet.

3.4.3 Configuration du portail captif

On va dans service>captive portal>administration (figure 3.13).

- ➢ On active le portail captif.
- ➢ On choisit l'interface LAN (l'interface qui doit être authentifiée).
- ➢ On choisit le serveur qui va assurer l'authentification dans notre cas c'est openldap.

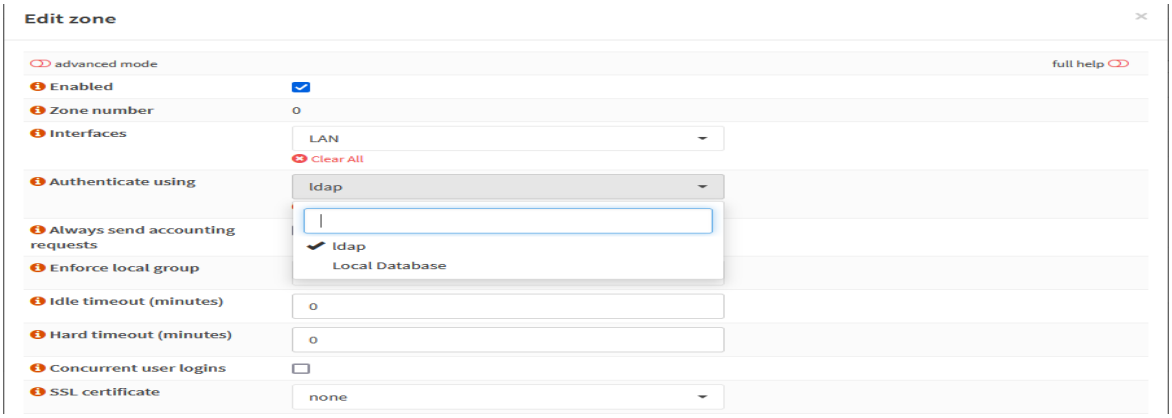

Figure 3. 13 : Configuration du portail captif

- ➢ Mettre en place les règles qui autorisent le portail captif (figure 3.14).

Puis on sauvegarde la configuration et on l'applique.

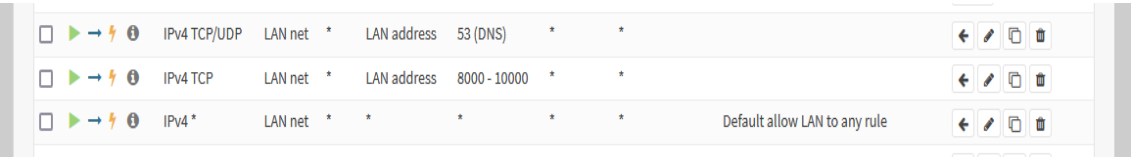

Figure 3. 14 : Les règles du portail captif

3.4.4 Test

On va faire le test pour voir si ça marche (figure 3.15).

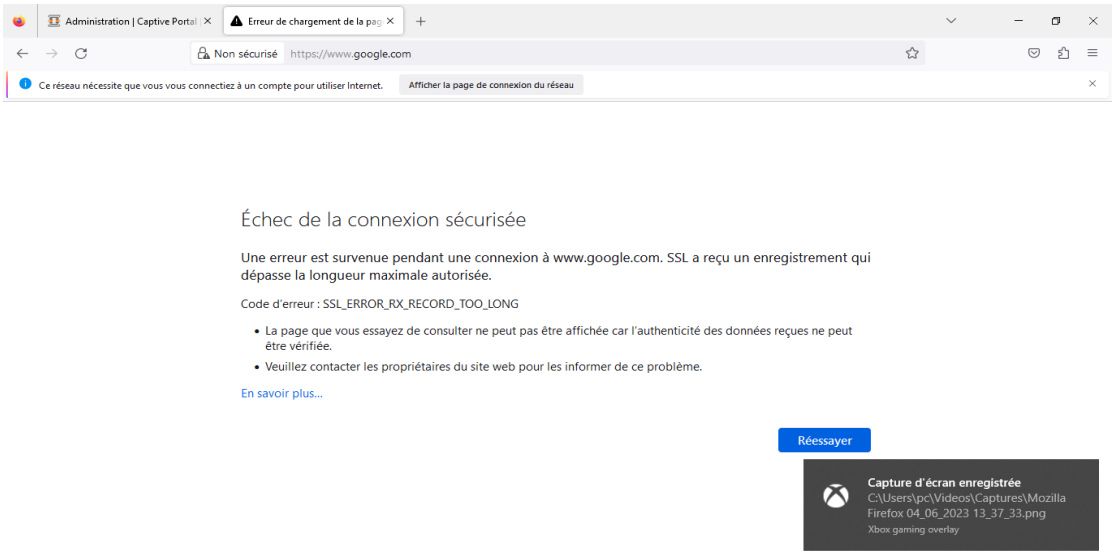

Figure 3. 15 : Test du portail captif

Dans l'image ci- dessus, le pare-feu a bloqué notre requête donc on n'a pas accès à google.com mais est apparu une phrase en bas : "ce réseau nécessite que vous vous connectiez à un compte utilisateur pour utiliser internet. Afficher la page de connexion du réseau". On appuie sur la dernière phrase puis on verra la page de connexion dans la figure en bas (figure 3.16).

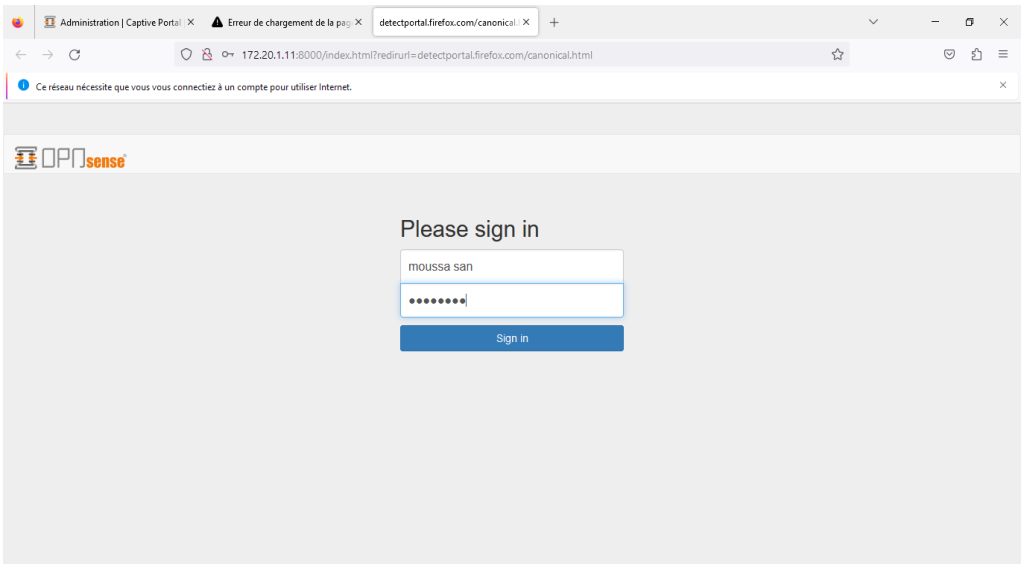

Figure 3. 16 : La page du portail captif

On doit se connecter avec les identifiants d'un compte qu'on a créé dans notre serveur OpenLDAP (dans ce cas on se connecte comme moussa san).

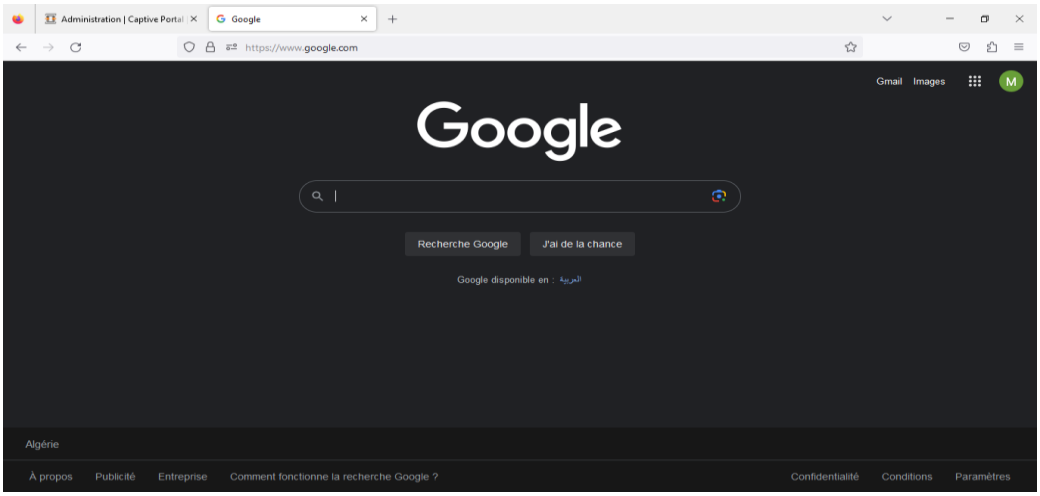

Figure 3. 17 : Accès internet

Après l'authentification, on a maintenant accès à l'internet (figure 3.17).

On peut contrôler les utilisateurs connectés, vérifier la date, l'heure et la date de la connexion.

3.5 Installation et configuration de notre serveur DNS

Alors pour le DNS, on a utilisé une autre distribution de Linux, il s'agit de CentOS.

On installe et on configure le système d'exploitation CentOS puis on le met à jour.

On télécharge (figure 3.18) les paquets bind qui permettent d'installer le DNS en tapant la commande "yum install bind bind-utils -y"

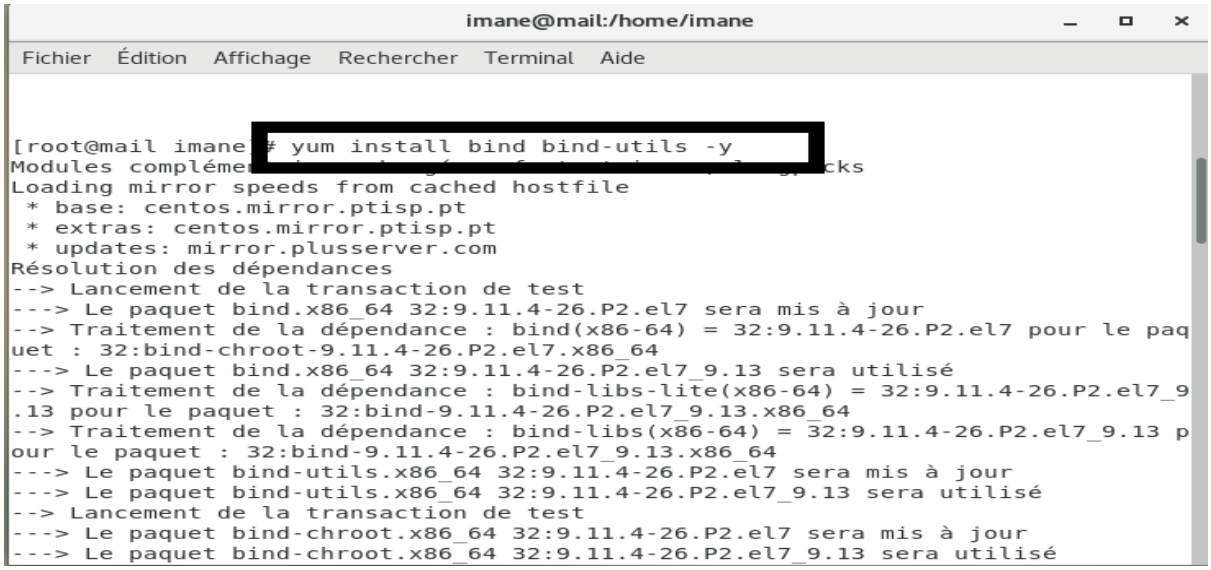

Figure 3. 18 : Installation des paquets bind

Après le téléchargement et l'installation des paquets bind, on va maintenant modifier quelques fichiers.

➢ Le fichier hosts : dans le fichier hosts, on met le nom de notre serveur(mail) devant le localhost ipv4 puis en bas on ajoute une autre ligne dans lequel on met l'adresse du serveur DNS suivi du nom de domaine complet (mail.imane.com) suivi du nom mail (figure 3.19).

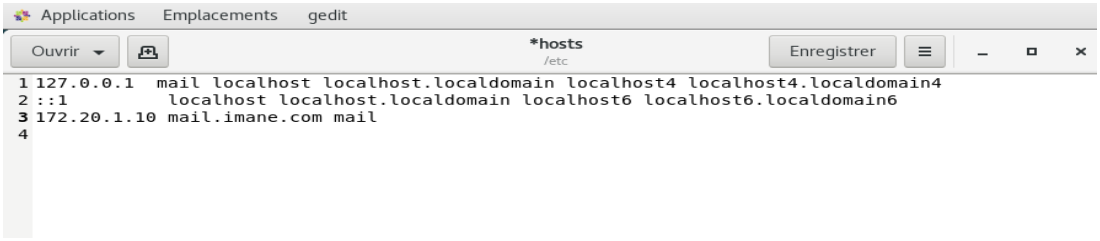

Figure 3. 19 : Configuration du fichier host

La commande pour cette modification est "gedit /etc/hosts".

➢ Le fichier resolv.conf en tapant "gedit /etc/resolv.conf" : C'est le fichier qui permet de traduire l'adresse ip en nom de domaine. Dans ce fichier on crée deux lignes avec l'adresse IP de notre serveur ainsi que le nom de domaine (figure 3.20).

Figure 3. 20 : Configuration du fichier resolv.conf

➢ Le fichier named.conf en tapant "gedit /etc/named.conf" : dans ce fichier, on va insérer l'adresse ip ainsi que l'adresse réseau du serveur DNS, créer deux zones (une zone directe et une zone inverse) comme vous pouvez le voir dans les lignes 58 et 62 puis on sauvegarde les modifications(figure 3.21 ;figure 3.22). :

Applications Emplacements gedit

Ouvrir *named.conf /etc Enregistrer

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
        listen-on port 53 { 127.0.0.1; 172.20.1.10; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost; 172.20.0.0/16; };

```

Figure 3. 21 : Configuration du fichier named.conf

```
        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};
zone "imane.com" IN {
        type master;
        file "direct";
};
zone "1.20.172.in-addr.apra" IN {
        type master;
        file "inverse";
};
```

Figure 3. 22 : Définition des zones

3.6 Configuration de la zone directe et inverse

3.6.1 Zone directe

La zone directe DNS est la zone qui permet de résoudre un FQDN (nom de domaine complet) à une adresse IP, c'est la plus utilisée couramment. Chaque fois qu'on va sur un navigateur et qu'on tape par exemple google.com, eh bien c'est cette zone qui est utilisée (figure 3.23).

imane@mail:/var/named

Fichier Édition Affichage Rechercher Terminal Aide

```
[root@mail imane]# cd /var/named/
[root@mail named]# ls
chroot  dynamic     named.ca      named.localhost  slaves
data    dyndb-ldap  named.empty   named.loopback
[root@mail named]# cp named.localhost direct
[root@mail named]# gedit direct
```

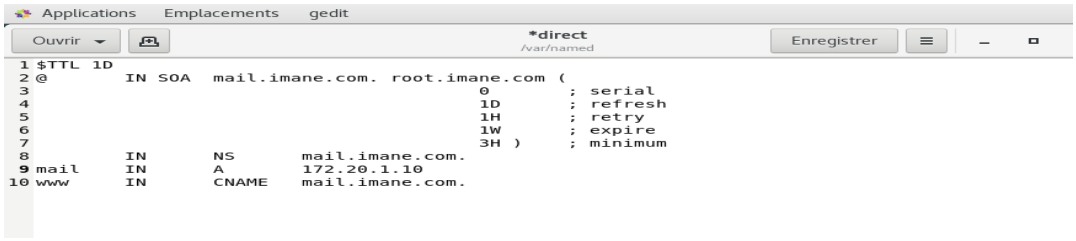

Figure 3. 23 : Configuration de la zone directe

3.6.2 Zone inverse

C'est la zone qui fait l'exact opposé de la zone directe c'est-à-dire fournir un nom de domaine à une adresse ip donnée (figure 3.24).

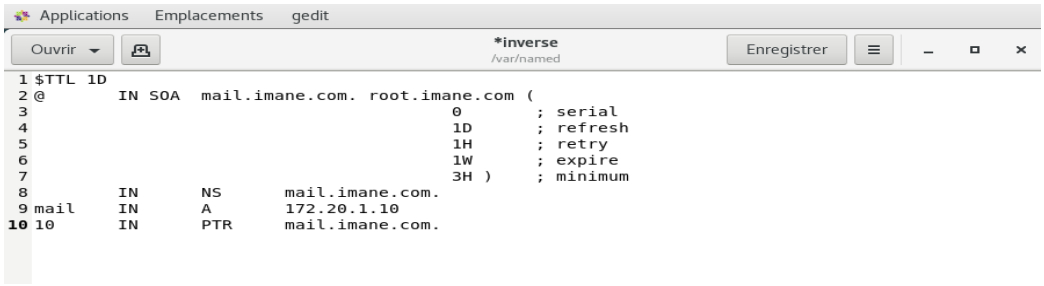

Figure 3. 24 : Configuration de la zone inverse

Maintenant on octroie les privilèges DNS, redémarrer le service named, redémarrer le réseau et nôtre DNS est opérationnel.

Pour vérifier, il suffit de taper dans le terminal la commande suivante "nslookup www".

Dans l'image ci-dessous (figure 3.25), on voit bien que le DNS est bien configuré, notre nom de domaine complet est le "mail.imane.com avec l'adresse 172.20.1.10" et le port du DNS est le 53. Par la suite on va mettre en place un serveur de messagerie raison pour laquelle on a mis en place un serveur DNS. Les deux travaillent de pair.

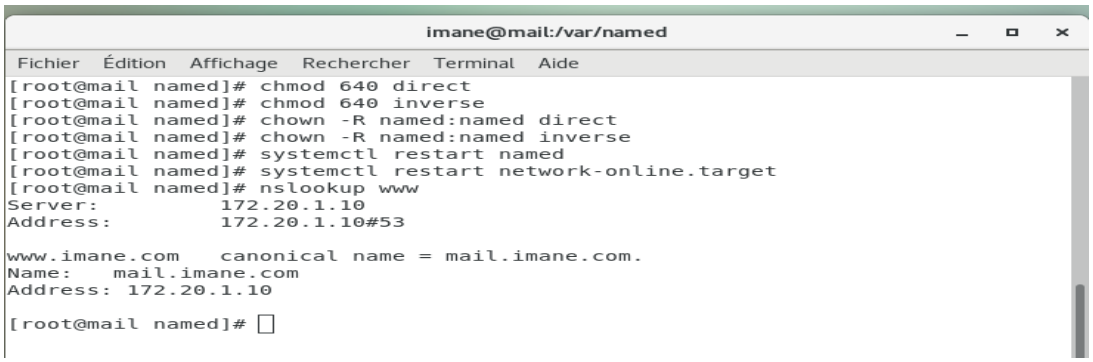

Figure 3. 25 : Attribution des droits et test du DNS

3.7 Installation et configuration du serveur de messagerie

Comme évoqué dans les lignes précédentes, le serveur de messagerie nécessite obligatoirement les services d'un serveur DNS, dans ce travail, le serveur de messagerie qu'on va mettre en place est zimbra.

3.7.1 Définition du serveur de messagerie Zimbra

Zimbra est un serveur de messagerie avec des fonctionnalités de travail collaboratif. Elle gère les e-mails, les contacts et les calendriers, les documents, le partage de fichiers, les tâches, les médias sociaux, plus la synchronisation vers d'autres ordinateurs de bureau et périphériques.

On utilisera le même pc de DNS pour la mise en place de zimbra donc l'adresse ip restera la même le "172.20.1.10".

3.7.2 Installation

Avant de commencer l'installation, on doit désactiver le pare-feu ainsi que le service postfix (figure 3.26). Postfix est un serveur de messagerie intégré dans plusieurs distributions Linux et comme deux serveurs de messagerie ne peuvent pas coexister sur le même périphérique, raison pour laquelle on le désactive (figure 3.26).

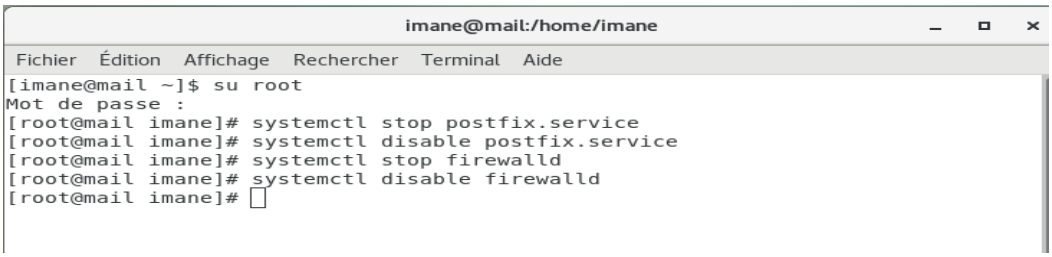

Figure 3. 26 : L'arrêt des services indésirables

On installe certains paquets pré requis pour l'installation de zimbra (figure 3.27).

```
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 38.517/39.939/40.804/0.710 ms
[imane@mail ~]$ clear
[imane@mail ~]$ su root
Mot de passe :
[root@mail imane]# yum install unzip net-tools systat openssh-clients perl-core libaio
 nmap-ncat libstdc++.so.6 wget -y
Loading mirror speeds from cached hostfile
 * base: centos.mirror.ptisp.pt
 * extras: centos.mirror.ptisp.pt
 * updates: mirror.plusserver.com
Le paquet net-tools-2.0-0.25.20131004git.el7.x86_64 est déjà installé dans sa dernière
 version
Aucun paquet systat disponible.
```

Figure 3. 27 : Les paquages prérequis de zimbra

Maintenant on télécharge(figure 3.28) les paquets zimbra avec la commande "wget https://files.zimbra.com/downloads/8.8.15_GA/zcs-8.8.15_GA_3869.RHEL7_64.20190918004220.tgz".

```
(gedit:15666): dconf-WARNING **: 12:00:48.409: failed to commit changes to dconf: La connex
ion est fermée
[root@mail imane]# cd zimbra
[root@mail zimbra]# wget https://files.zimbra.com/downloads/8.8.15_GA/zcs-8.8.15_GA_3869.RH
EL7_64.20190918004220.tgz
EL7_64.20190918004220.tgz
Résolution de files.zimbra.com (files.zimbra.com)... 13.33.234.36
Connexion vers files.zimbra.com (files.zimbra.com)|13.33.234.36|:443...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 255802491 (244M) [binary/octet-stream]
Sauvegarde en : «zcs-8.8.15_GA_3869.RHEL7_64.20190918004220.tgz»

12% [=====>                                                ] 32 709 629  11,0MB/s
```

Figure 3. 28 : Téléchargement de zimbra

On l'extrait (figure 3.29) avec la commande "tar xvf zcs-8.8.15_GA_3869.RHEL7_64.20190918004220.tgz".

```
imane@mail:/home/imane/zimbra
Fichier  Édition  Affichage  Rechercher  Terminal  Aide

[root@mail zimbra]# tar xvf zcs-8.8.15_GA_3869.RHEL7_64.20190918004220.tgz
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/bin/
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/bin/checkLicense.pl
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/bin/checkService.pl
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/bin/get_plat_tag.sh
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/bin/zmValidateLdap.pl
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/bin/zmdbintegrityreport
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/data/
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/data/versions-init.sql
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/admin.pdf
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/Fedora Server Config.pdf
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/Import_Wizard_Outlook.pdf
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/Migration_Exch_Admin.pdf
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/MigrationWizard_Domino.pdf
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/MigrationWizard.pdf
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/OSmultiserverinstall.pdf
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/quick_start.pdf
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/RNZCSO_2005Beta.pdf
zcs-8.8.15_GA_3869.RHEL7_64.20190918004220/docs/en_US/User Instructions for ZCS Import Wiza
rd.pdf
```

Figure 3. 29 : Extraction des fichiers zimbra

Installation des packages zimbra (figure 3.30).

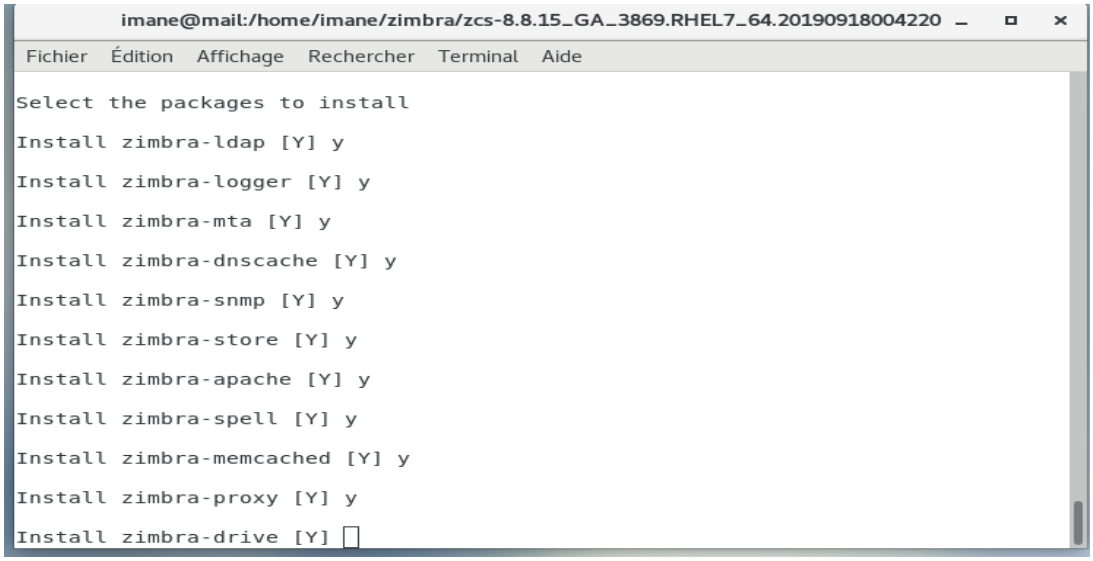

Figure 3. 30 : Installation de zimbra

Ainsi après l'installation, on voit la liste des menus principaux de zimbra (figure 3.31)

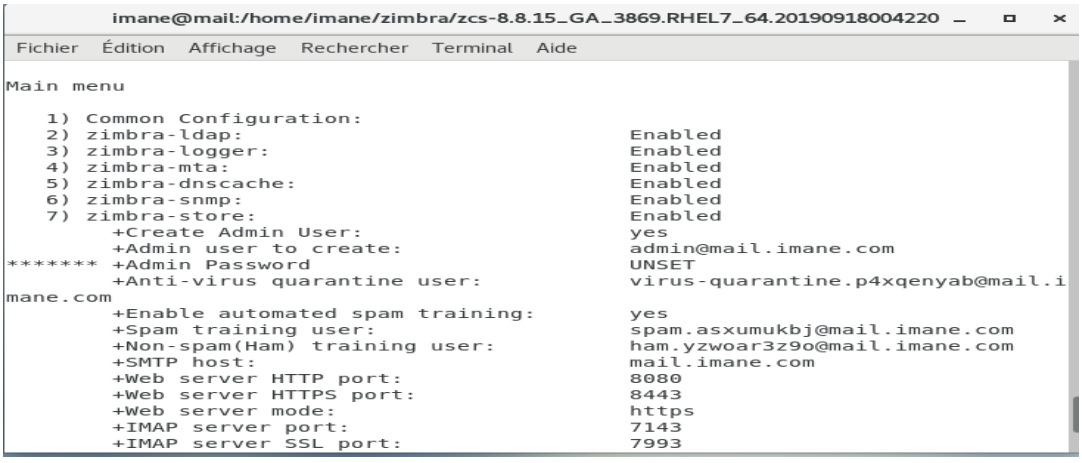

Figure 3. 31 : Les menus disponibles dans zimbra

On va maintenant créer le compte administrateur avec son mot de passe(figure 3.32). Les identifiants du compte administrateur sont "moussa@imane.com" et le mot de passe est "0123456"

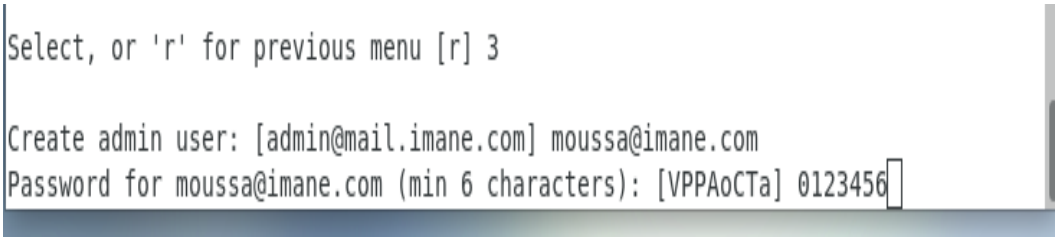

Figure 3. 32 : Création du compte administrateur

Après les configurations basiques, on va vérifier si tous les services de notre serveur fonctionnent correctement avec la commande "zmcontrol status". Le résultat nous montre que tous les services fonctionnent correctement (figure 3.33).

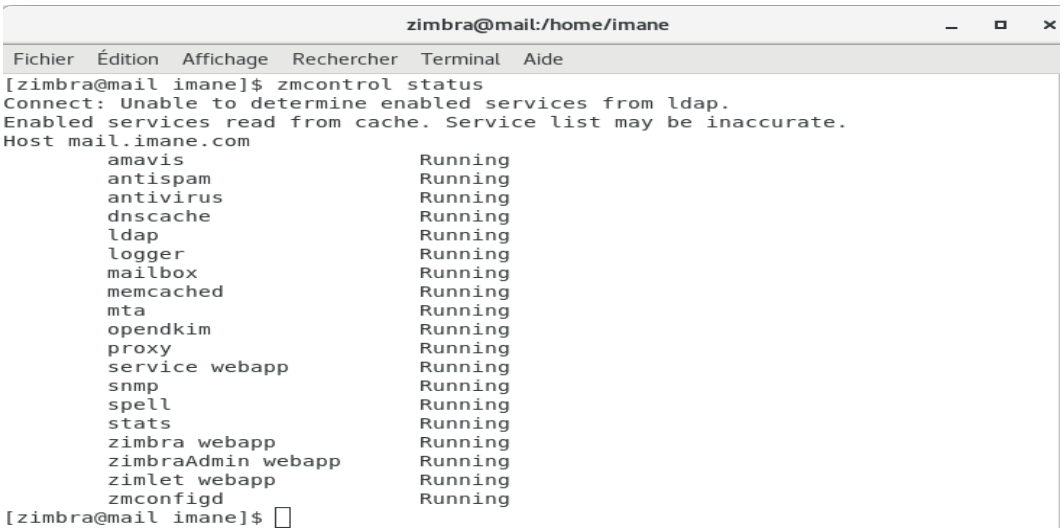

Figure 3. 33 : Vérification des services de zimbra

Le serveur de messagerie zimbra est maintenant bien configuré et prêt à l'utilisation.

Pour accéder à notre serveur zimbra(figure 3.34, figure 3.35), il suffit de taper l'url suivante : https://mail.imane.com:7071 ou https://172.20.1.10:7071

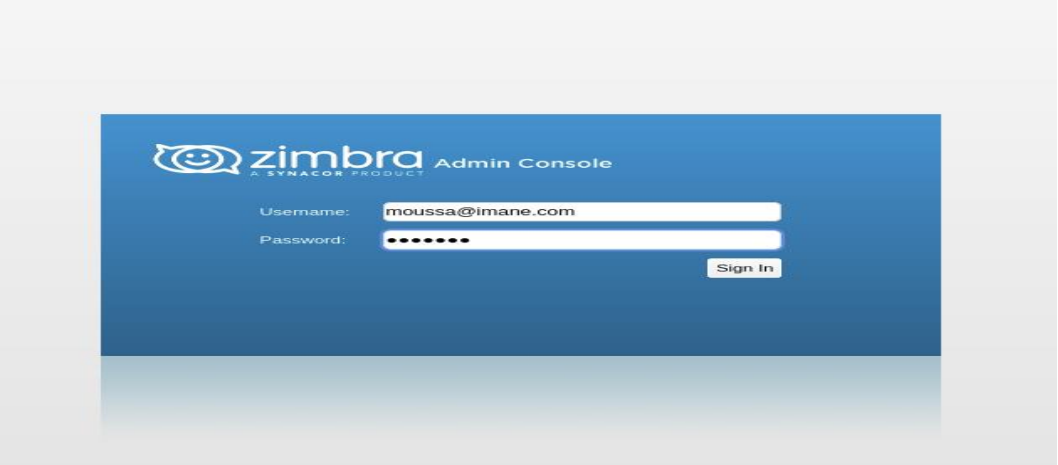

Figure 3. 34 : Connection en tant qu'administrateur du serveur zimbra

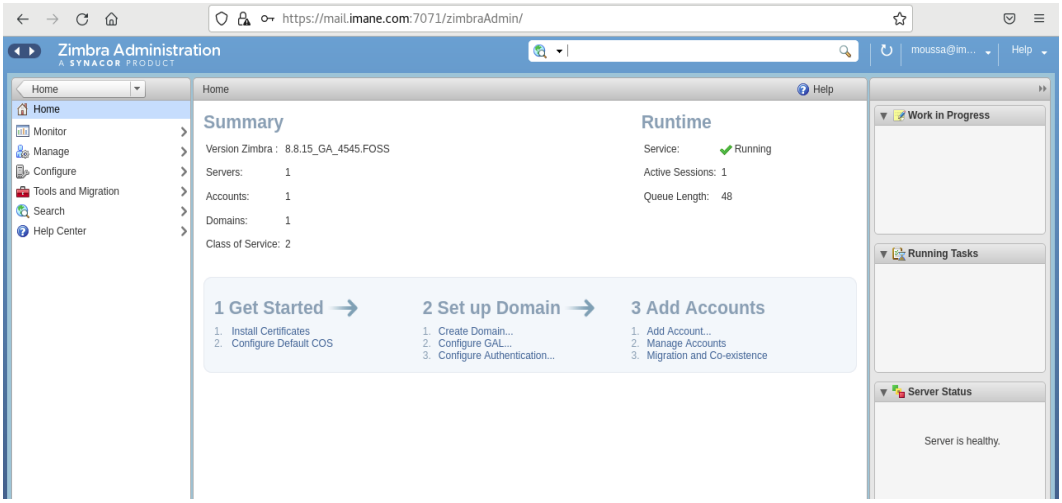

Figure 3. 35 : L'interface graphique de zimbra

3.7.3 Création des comptes utilisateurs

On va créer deux comptes utilisateurs (mehdi et aïcha) pour faire le test. La figure ci-dessous (figure 3.36) représente la création du compte de mehdi.

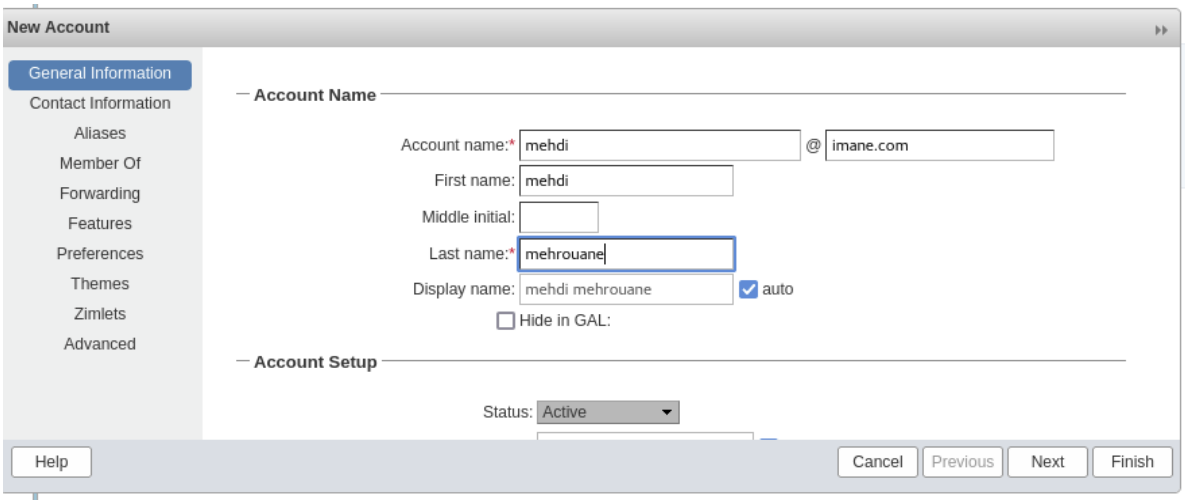

Figure 3. 36 : Création du compte utilisateur mehdi

Maintenant on va créer le compte de aïcha (figure 3.37).

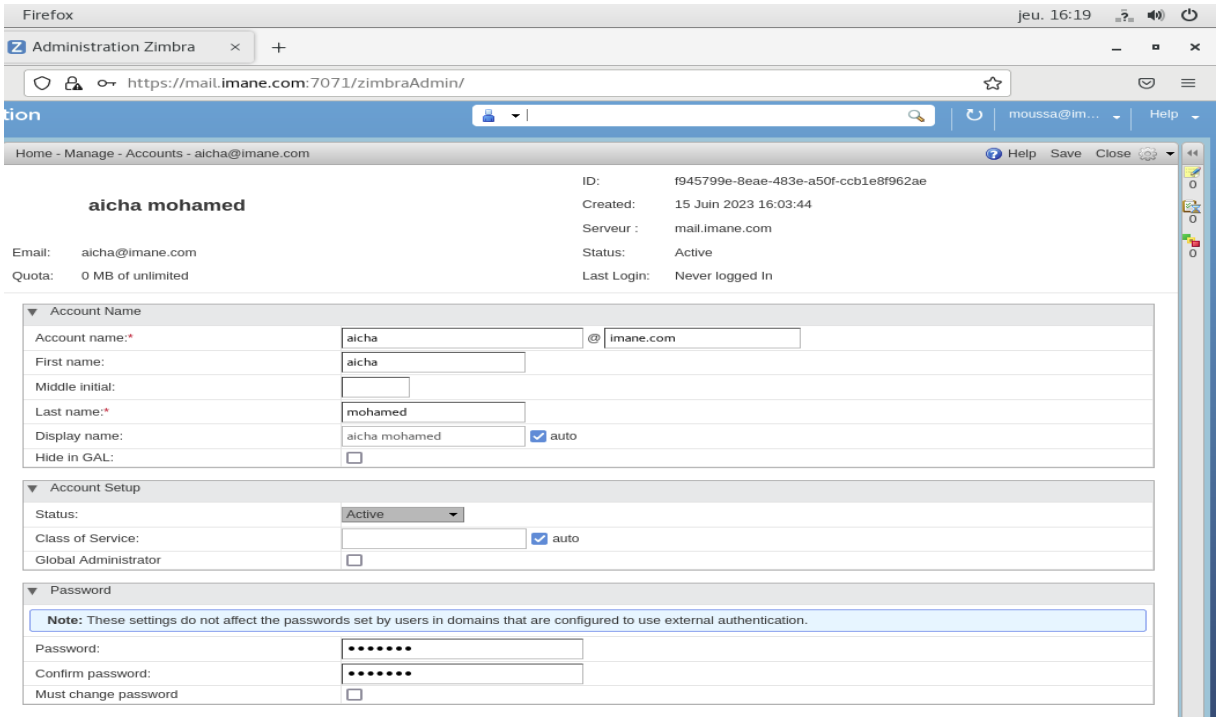

Figure 3. 37 : Création du compte utilisateur aicha

On peut facilement visionner les 2 comptes dans la figure en bas (figure 3.38).

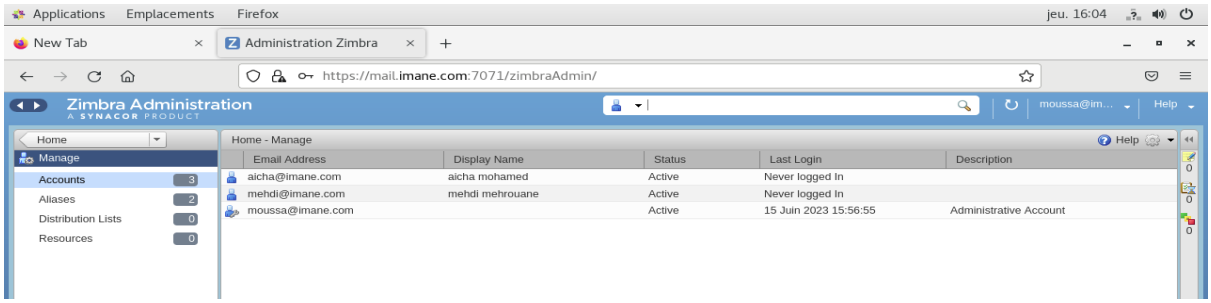

Figure 3. 38 : Gestion des différents comptes

3.7.4 Test

On va tester si notre serveur de messagerie fonctionne bien. Pour cela, les 2 utilisateurs vont s'envoyer des mails. Bien avant de converser, ils doivent d'abord se connecter en tant que client de notre serveur avec leurs identifiants.

Voir les figure 3.39 figure 3.40.

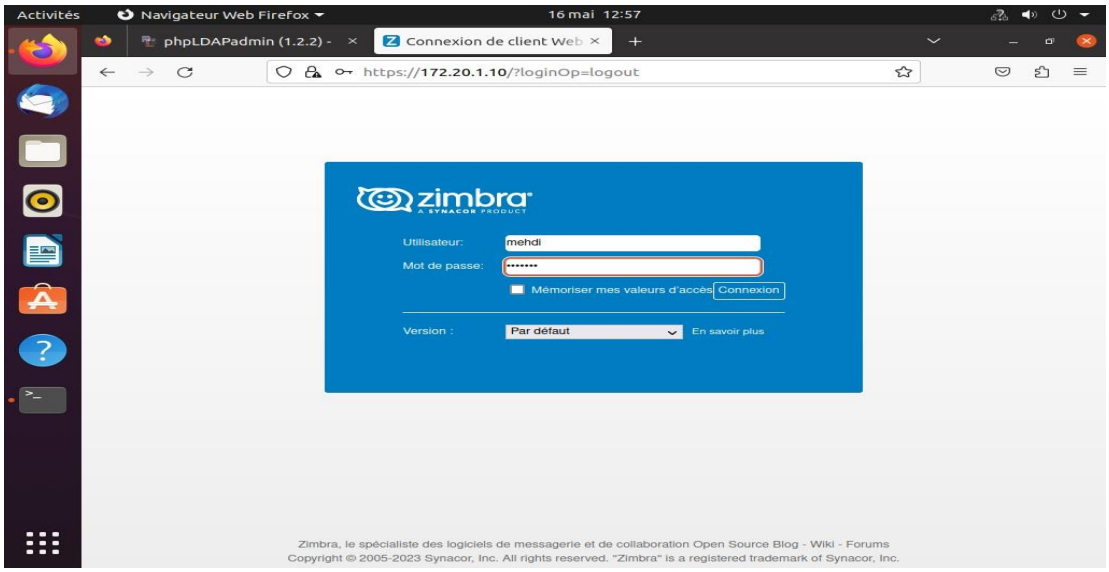

Figure 3. 39 : Connection en tant que client zimbra

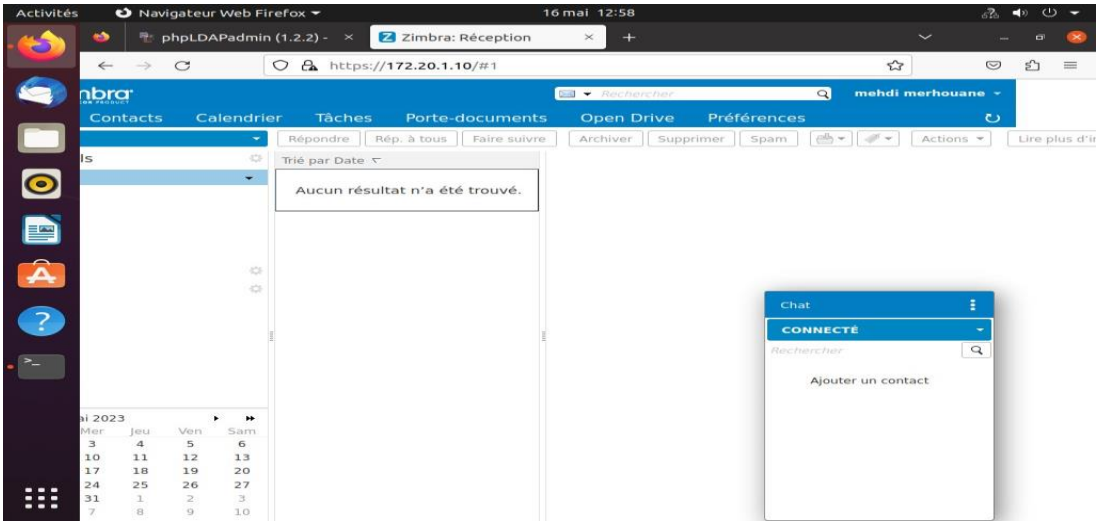

Figure 3. 40 : Boîte de réception de mehdi

Nous pouvons voir que la boîte de réception de mehdi est vide pour le moment (figure 3.40).

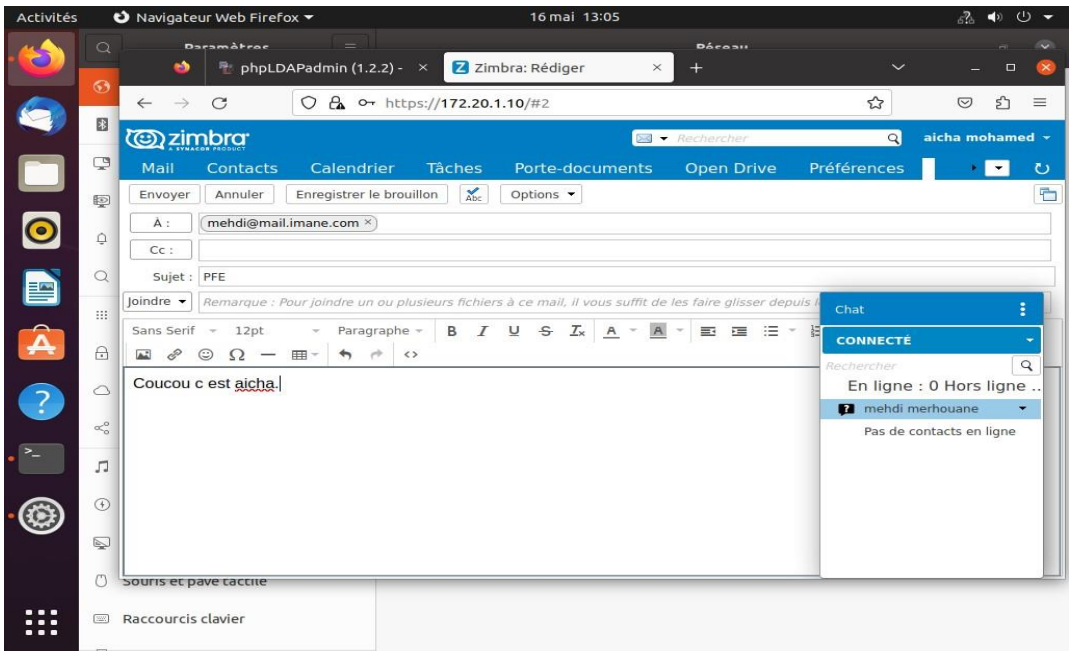

Figure 3. 41 : Envoi d'un mail à mehdi

Alors dans l'image ci-dessus (figure 3.41) nous sommes dans la boîte d'envoi d'aïcha qui envoie un message à mehdi. Dans la prochaine image ((figure 3.42), nous verrons que le message a été envoyé.

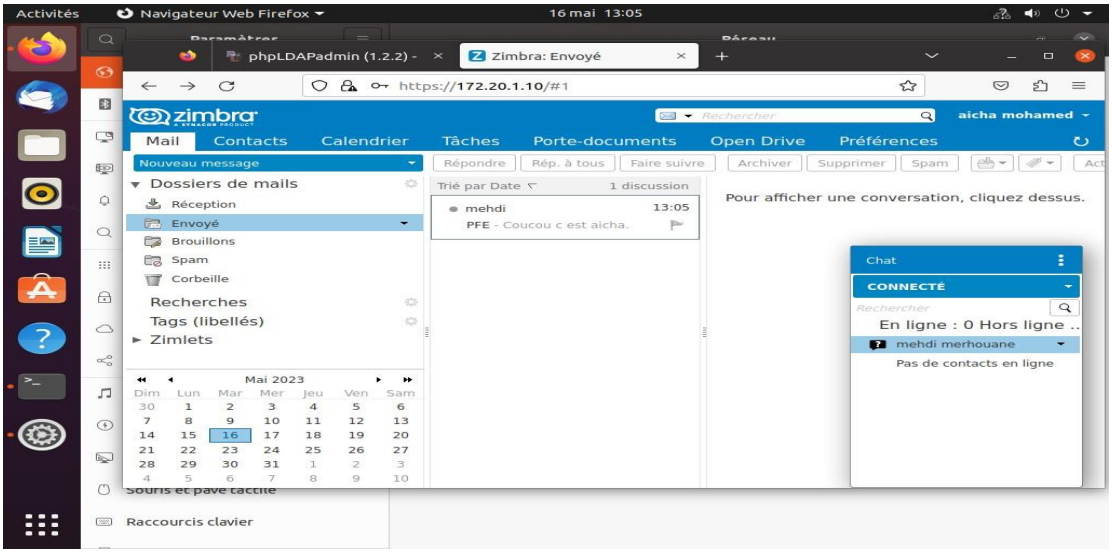

Figure 3. 42 : Envoi d'un mail à mehdi

Les prochaines images (figure 3.43, figure 3.44) nous montrent que mehdi a reçu le message d'aicha et il l'a ouvert.

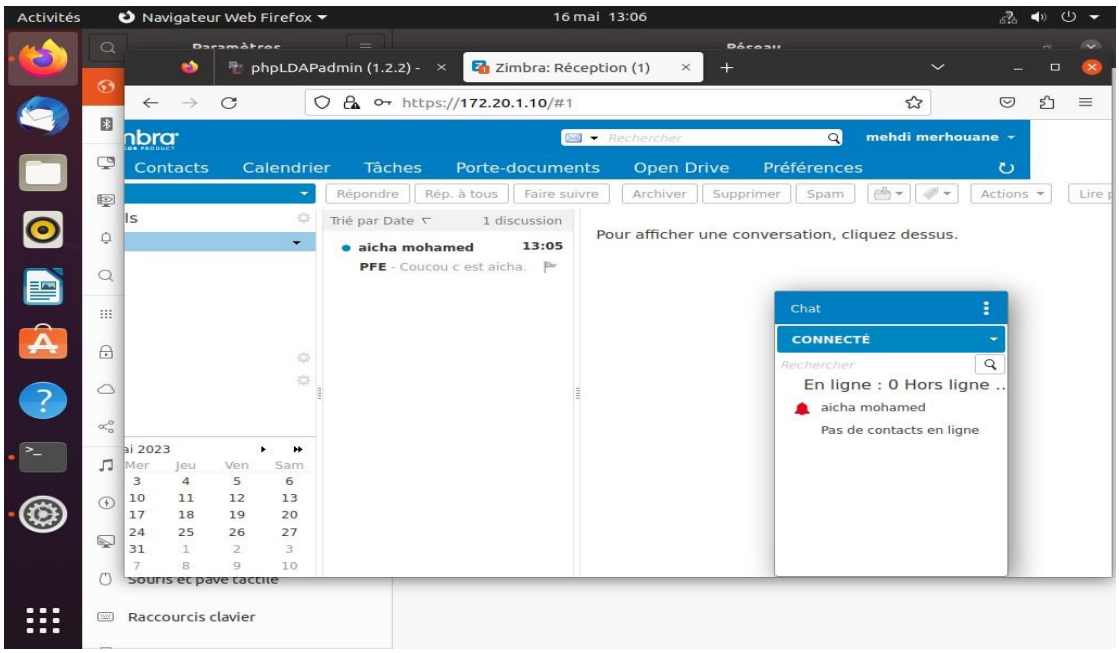

Figure 3. 43 : Réception du mail de aïcha

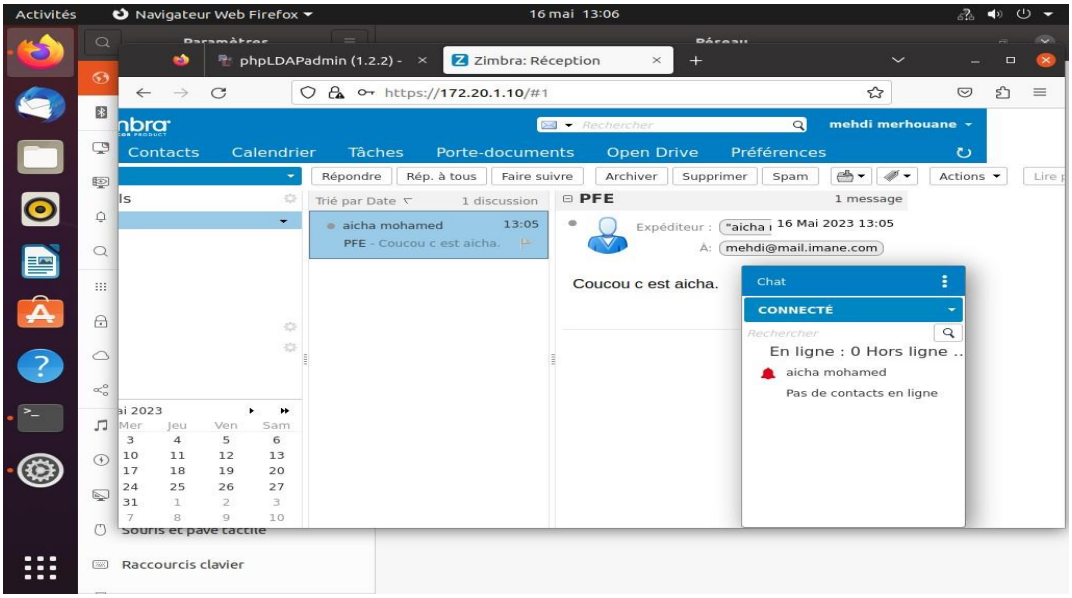

Figure 3. 44 : Lecture du mail de aïcha

Ainsi, notre serveur de messagerie fonctionne bien.

3.8 Déploiements courants

OPNsense est très puissant et polyvalent et peut être utilisé de plusieurs façons comme :

3.8.1 Routeur du réseau

Nous pouvons utiliser OPNsense comme routeur du réseau (figure 3.45). Il a même une option pour désactiver complètement le filtrage de paquets, ce qui améliore considérablement le débit du réseau, devenant simplement un routeur réseau sans pare-feu ni fonction NAT. Sans plugins supplémentaires, les capacités de routage sont minimales, simples et conviennent bien aux petits réseaux [4].

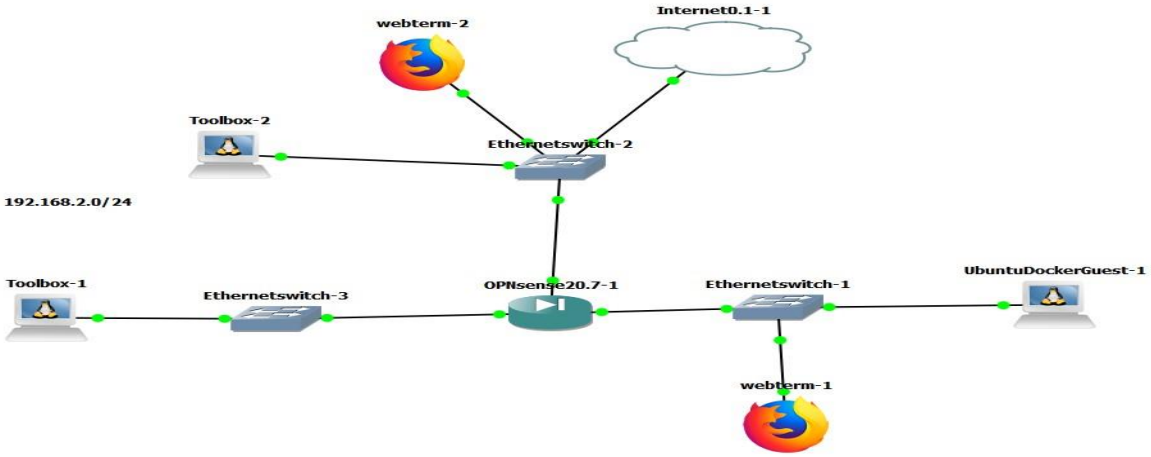

Figure 3. 45 : Architecture réseau[4]

3.8.2 IDPS

Combiné ou non à la fonction de pare-feu, OPNsense peut être utilisé comme un excellent IDS ou IPS, en alertant et en bloquant (lorsque l'IPS est activé) les paquets provenant du réseau surveillé. L'implémentation de suricata dans OPNsense est très bien conçue, et avec un matériel approprié, vous pouvez atteindre un débit de quelques gigabits par seconde [4].

3.8.3 Passerelle sans fil pour réseau d'invités (un réseau d'invités)

Avec un portail captif activé, vous avez beaucoup de contrôle sur le réseau des visiteurs. Vous pouvez combiner un pare-feu, un basculement WAN, un IPS et un proxy web avec le portail captif pour construire une solution robuste [4].

3.8.4 Pare-feu avec basculement WAN

Il s'agit de l'un des déploiements les plus courants, OPNsense étant utilisé comme pare-feu périmétrique ou interne, voir figure 3.46. Vous pouvez même l'utiliser comme pare-feu dans le nuage, en le combinant avec certains plugins tels que le ZeroTier VPN. Dans ce scénario, il sera probablement utilisé pour bloquer les paquets provenant d'un réseau externe. Il peut également être utilisé pour la redirection de ports (NAT et PAT) et pour bloquer les paquets sortants qui ne sont pas autorisés à quitter le réseau local. Lorsque plusieurs réseaux étendus sont disponibles, il est possible d'activer le basculement et l'équilibrage de la charge sortante pour garantir une bonne disponibilité de l'accès à l'internet [4].

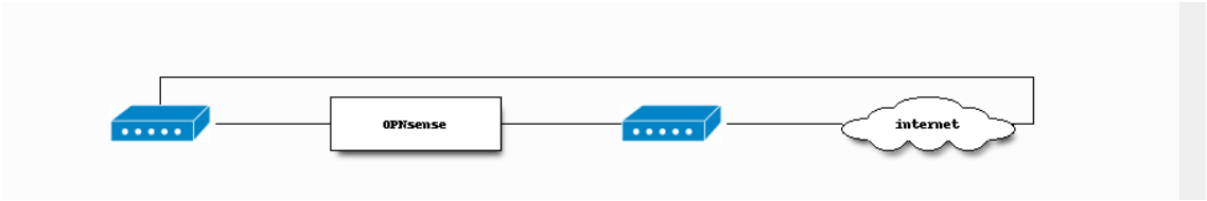

Figure 3. 46 : Pare-feu avec basculement WAN[4]

3.8.5 Serveur VPN

OPNsense dispose d'un excellent support pour les autorités de certification (CA) et les certificats, les utilisateurs et la gestion des groupes, localement et en externe. Vous pouvez, par exemple, l'utiliser comme une solution robuste de serveur OpenVPN pour des centaines, voire des milliers d'utilisateurs simultanés, en utilisant le matériel adéquat [4].

3.9 Configuration du pare-feu

Dans cette partie de notre travail, on va configurer des restrictions pour notre réseau local, l'utiliser aussi comme un système de détection et de prévention d'intrusion.

3.9.1 IDPS

Contrairement à PFsense qui nécessite d'installer snort(un système de prévention d'intrusion), le pare-feu OPNsense est natif des services IDPS, il suffit juste de l'activer.
Voir la figure ci-dessous (figure 3.47).

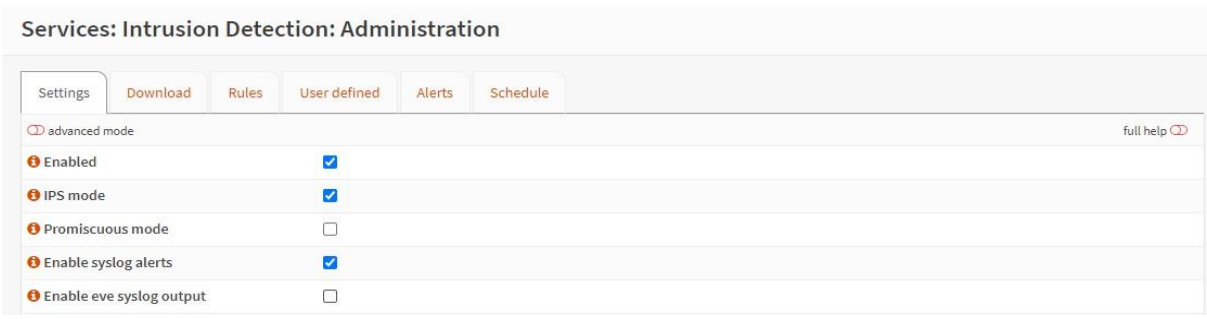

Figure 3. 47 : Configuration d'IDPS dans OPNsense

3.9.2 Les restrictions

Heureusement encore avec zenarmor, il est très simple de faire des restrictions avec OPNsense. On n'a pas besoin de mettre en place des règles pour interdire l'accès aux sites web dangereux, voir figure 3.48.

On se rend dans zenarmor>policies>security :
Par défaut, tout est désactivé, on active toutes les options (figure 3.48) de notre choix, dans ce travail on les a toutes activées. Le pare-feu bloque toutes ces options activées.

Figure 3. 48 : Activation des services de protection offerts par zenarmor

En plus de tout ça, on a ajusté le niveau de sécurité à "contrôle élevé", ce qui fait une restriction beaucoup minutieuse (figure 3.49).

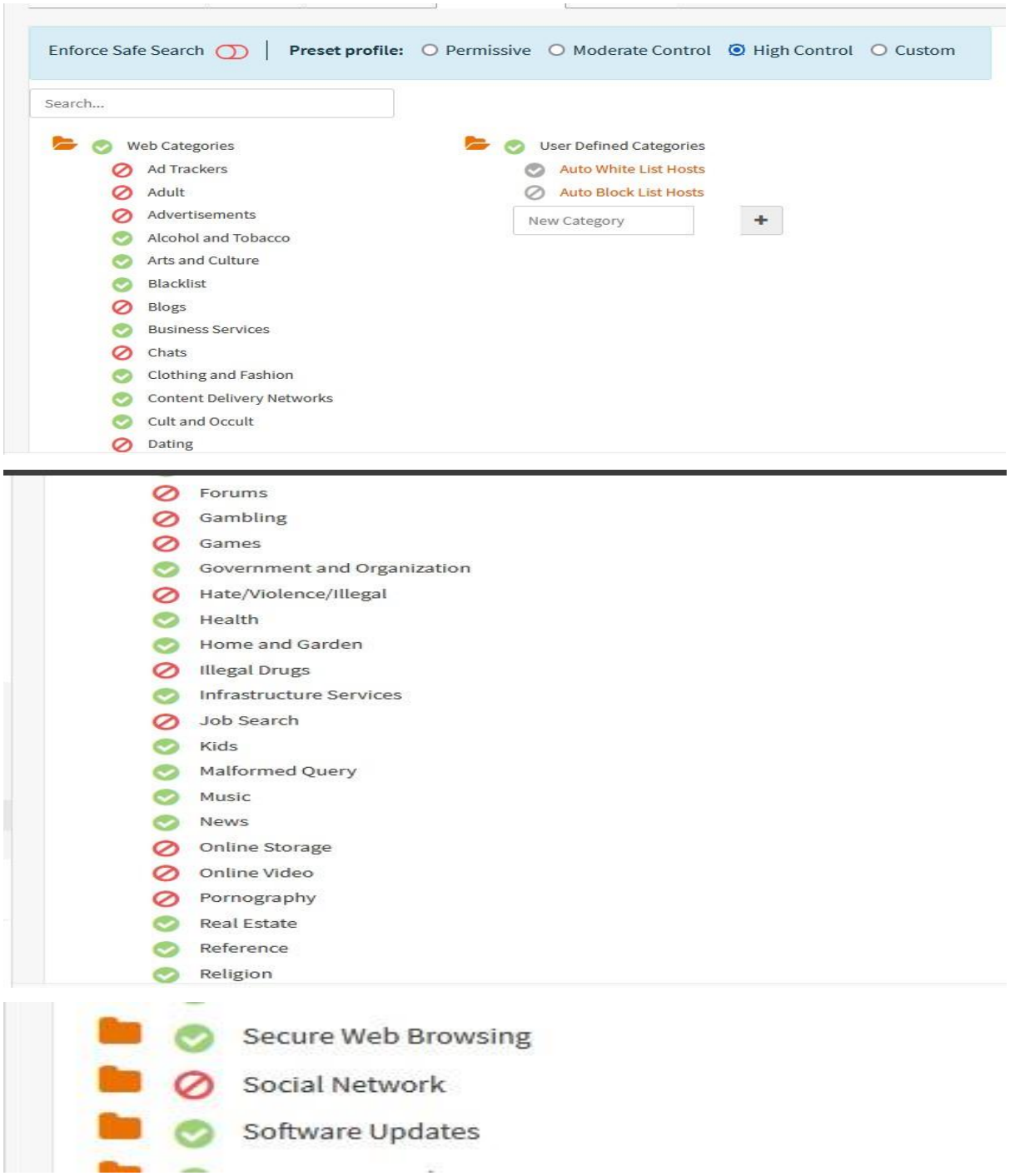

Figure 3. 49 : Mise en place des restrictions

Les utilisateurs de notre réseau local n'ont plus accès aux sites suivants :

- Les sites des réseaux sociaux (Instagram, Facebook, Snapchat, etc…) ;
- Les sites d'achats en ligne ;
- Les sites de jeu ;
- Les sites de forum ;

➢ Les sites pour contenu adulte ;

➢ Les sites de publicité.

3.9.3 Test

On va essayer de se rendre sur quelques-uns de ces sites pour voir si la configuration est bien faite.

- **Réseaux sociaux**

Facebook.com (figure 3.50)

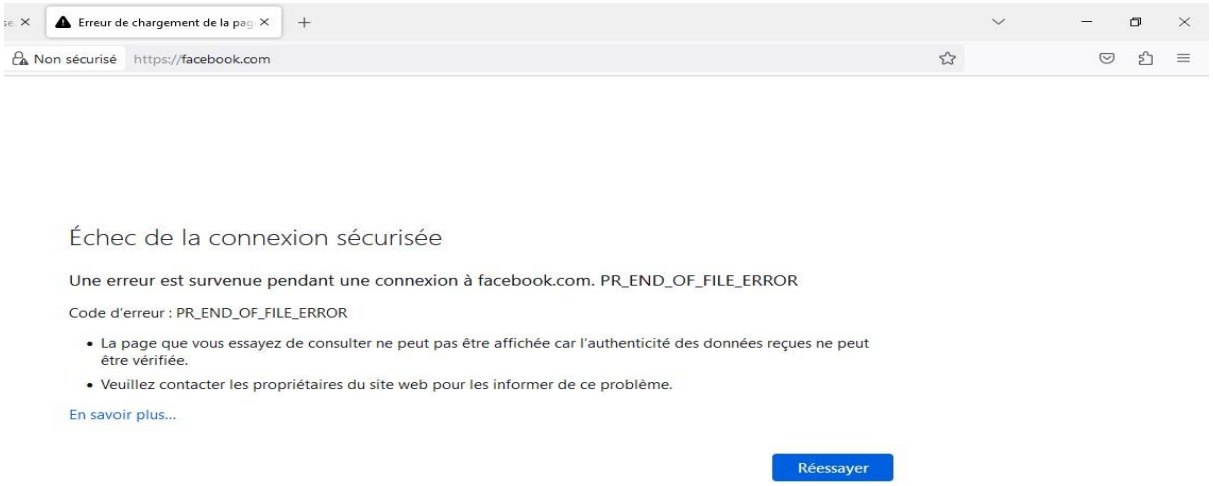

Figure 3. 50 : Test pour facebook.com

Instagram.com (figure 3.51)

Figure 3. 51 : Test pour instagram.com

On voit bien que l'accès aux réseaux sociaux est bloqué avec succès.

- **Site de jeu** (figure 3.52)

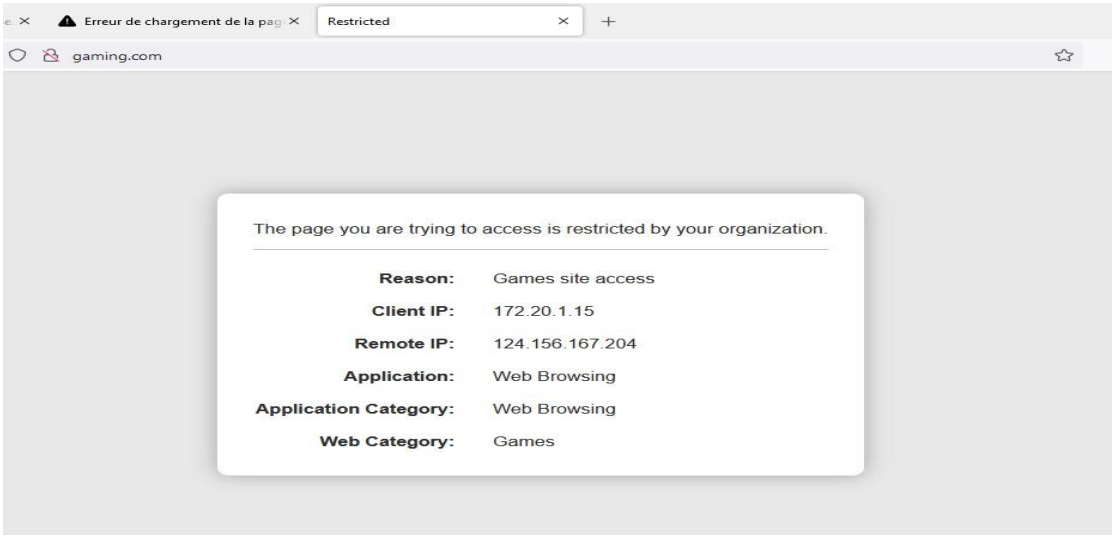

Figure 3. 52 : Test pour gaming.com

- **Site forum** (figure 3.53)

Figure 3. 53 : Test pour forumfr.com

3.10 Mise en place des règles

3.10.1 Création d'un alias

On a créé un alias du nom de serveur qui regroupent les adresses ip de nos différents serveurs. Ceci permet de facilement créer des règles qui concernent nos serveurs. C'est cet alias qu'on va utiliser pour toute règle concernant nos serveurs.

Voir figure ci-dessous (figure 3.54).

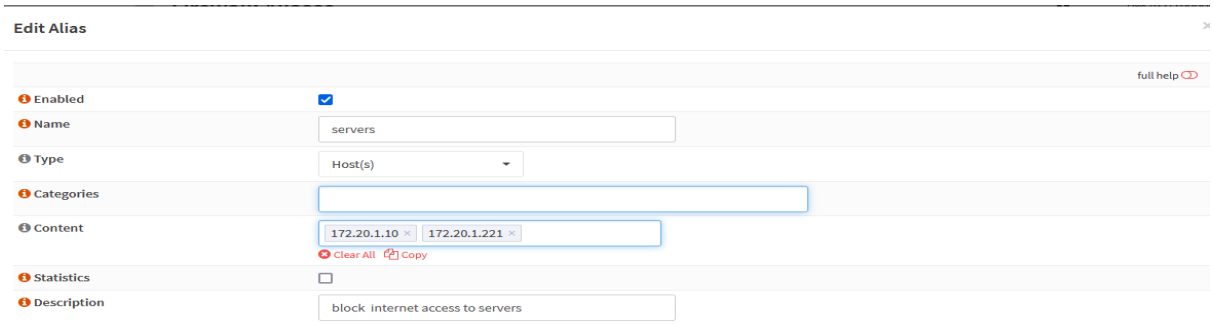

Figure 3. 54 : Configuration de l'alias

Ainsi, après la création de l'alias, on a mis en place 2 règles comme vous pouvez les voir dans la figure suivante (figure 3.55).

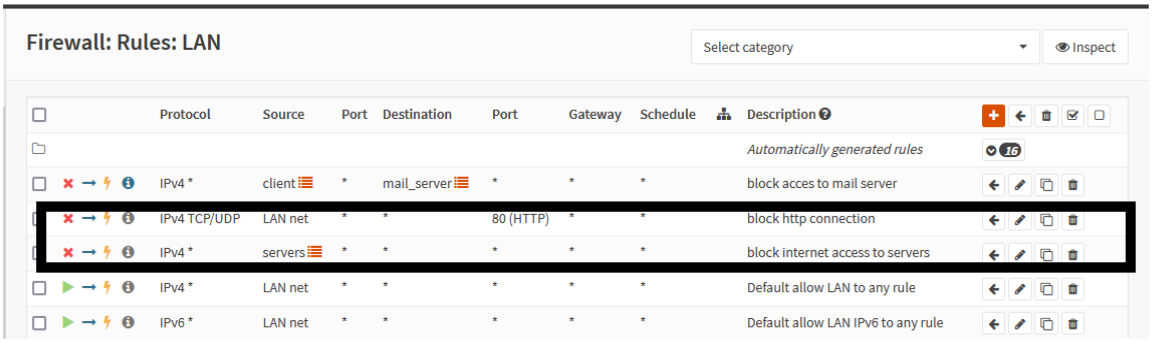

Figure 3. 55 : Définition des règles

- La première règle consiste à bloquer toute connexion de notre réseau local vers les sites http. Ainsi le risque d'exposition aux menaces diminue.
- La seconde règle consiste à interdire l'accès internet aux serveurs du réseau local pour question de sécurité aussi. Une fois que les serveurs du réseau local sont en pannes, le réseau devient inopérationnel.

3.10.2 Test des règles

On tente d'accéder à un site non sécurisé, c'est-à-dire les sites commençant par http. Dans la figure suivante (figure 3.56), le pare-feu a bloqué l'accès au site http://www.baidu.com .

Figure 3. 56 : Résultat du test des règles sur le LAN

Après on essaie d'accéder à internet à travers notre serveur d'authentification et l'accès aussi a été bloqué (figure 3.57).

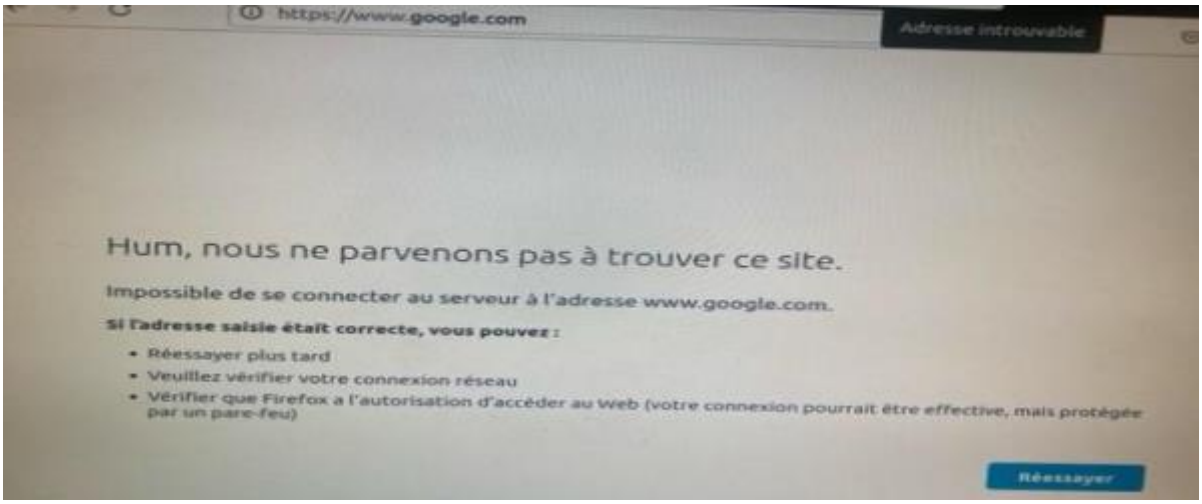

Figure 3. 57 : Résultat du test des règles sur les serveurs

Les règles mises en place fonctionnent très bien.

3.11 Conclusion

Nous pouvons constater que ce chapitre est purement pratique, car il a été focalisé sur l'essentiel même de notre projet. A travers ce chapitre on a non seulement fait des configurations en quantité et en qualité, mais aussi ça nous a permis de toucher le matériel, ce qui a une importance inestimable dans notre domaine car cela amène de la familiarité dans le milieu. L'assimilation de toutes ces connaissances nous aidera fortement dans nos prochaines formations professionnelles.

Conclusion générale

Le pare-feu est jusqu'à ces dernières années considéré comme une des pierres angulaires de la sécurité d'un réseau informatique. Il permet d'appliquer une politique d'accès aux ressources réseau. Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante). Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège.
On a vu les différents aspects de la sécurité réseau en mettant l'accent sur l'utilisation du pare-feu, ainsi que la mise en œuvre d'autres éléments essentiels tels que le serveur DNS, messagerie et authentification.

Nous avons utilisé le par feu OPNsense en explorant les principes fondamentaux de la sécurité d'une structure réseau et des serveurs, et on a survit les étapes suivantes :

- Installation du par feu.
- Mise en place d'un système d'authentification.
- Mise en place d'un système de messagerie et de DNS derrière le pare-feu.

Cependant, il est essentiel pour les organisations de continuer à se tenir au courant des dernières tendances en matière de sécurité réseau, et investir dans des solutions de sécurité robustes et de mettre en place des politiques et des procédures appropriées pour prévenir et atténuer les risques potentiels. Nous espérons que les informations et les recommandations fournies dans ce mémoire seront utiles aux professionnels de la sécurité réseau et contribueront à renforcer la sécurité des réseaux des organisations.
Ainsi, le travail que nous avons réalisé pourrait être complété sous divers aspects tels que :

➢ La mise en place d'une zone DMZ permettant la mise en place de diverses règles.

➢ Remplacer l'ipv4 par l'ipv6(qui est un protocole sécurisé).

➢ Mettre en place un système de surveillance permettant la localisation rapide des failles.

Références

[1] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf.

[2] https://www.kwtrain.com/blog/network-security-zones.

[3] Huawei Certification ICT Associate-Security.

[4] Building Internet Firewalls Internet and Web security Elizabeth D. Zwicky, Simon Cooper etc.) (Z-Library).

[5] Davis Chapman, <<Firewalls-LasécuritésurInternet>>, editionO'Reilly,1997.

[6]AKKOUCHE Hassiba MAHSASNesrine,<<cconception d'une passerelle internet sécurisée >>, mémoire de fin d'étude UABBT, 2020/2021.

[7] BENDAHMANE Ahmed, « Installation et configuration d'un firewall », Mémoire de fin d'études, UABBT, 2010/2011.

[8]https://www.fredzone.org/top-20-des-meilleurs-pare-feux-pour-la-securite-numerique-380452 .

[9] https://htpratique.com/pare-feu-gratuits/.

[10] https://www.opnsense.org (consulté en Avril 2023).

[11]https://www.pedagogie.ac-aix-marseille.fr/upload/docs/application/pdf/2012-07/formation_reseau.pdf.

[12] https://www.techno-science.net/glossaire-definition/Address-Resolution-Protocol.html.

[13] Jean-François Pilou et Jean-Philippe Bay. Sécurité informatique.4ième édition,Dunod.

[14]http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/Vasseur-Marcq/Attaques/Types_attaques.htm.

[15] Www.journaldunet.fr (consulté en Juin 2023).

[16] https://www.centos.org (consulté en Juin 2023).

[17] https://www.cisco.com (consulté en Mai 2023).