



# *Remerciements*

*Nous remercions Dieu le tout puissant, de nous avoir donné le courage, la patience et la volonté afin d'aboutir à l'accomplissement de ce travail.*

*Nous désirions exprimer ma gratitude à mon encadreur*

*Mme SAAD, pour le temps précieux qu'elle nous a consacrées, pour son orientation et encadrement.*

*Nous tenons à remercier Mr HERROUG chef de département informatique à Bejaia Logistique pour la qualité de son encadrement tout au long du déroulement de notre stage, pour sa disponibilité, sa rigueur et son partage d'expertise.*

*Nous tenons à remercier les membres de jury qui ont accepté de juger notre travail.*

*Nos remerciements les plus sincères à l'ensemble des enseignants du département informatique qui ont contribué à notre formation, et tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.*



## Dédicace

*je dédie ce modeste travail*

*Tout d'abord, je tiens à exprimer ma reconnaissance à **Dieu** le tout puissant, source de toute inspiration et de chaque opportunité qui s'est présentée à moi  
A mes chers **parents** , pour tous leurs sacrifices, leur amour, leur tendresse,  
leur soutien et leurs prières tout au long de mes études,*

*A mes chers **frères** , pour leur appui et leur encouragement, et leur soutien  
moral,*

*A mon cher **fiancé** , qui a toujours été à mes côtés , son soutien indéfectible ,  
ses encouragements, son respect et son amour sont une source d'inspiration  
pour moi.*

*A toute ma famille pour leur soutien tout au long de mon parcours universitaire,  
Mes chers amis **Ryma Lynda, et Myriam** qui ont été mes piliers  
émotionnels. Leur soutien inébranlable, leur écoute attentive et leurs  
encouragements*

*A ma chère binôme **Fatima** , avec qui j'ai partagé cette aventure. Notre  
collaboration, notre entraide et notre esprit d'équipe ont été une source de  
motivation constante.*

**Thiziri**



## Dédicace

*Je dédie ce modeste travail à :*

*À la mémoire de mes grands-parents maternel et paternel*

*À mon cher papa bien-aimé **Nadir** , ma source de courage, mon guide et mon soutien indéfectible.*

*À ma merveilleuse maman **Chahrazed** , ma source inépuisable de douceur, de tendresse et de force.*

*À mon cher frère Kaci, et à ma chère sœur Nedjma, pour leur soutien et leur présence à mes côtés.*

*À mon cher mari **Samy**, En signe de profond amour et de gratitude pour son soutien et son amour inconditionnel*

*À ma chère binôme **Thiziri**, pour tous les moments qu'on a passés ensemble. À tous ceux qui ont été à mes côtés durant la réalisation de ce travail*

**Fatima**

**Résumé** L'évolution technologique et la nécessité de protéger les données personnelles ont conduit à l'importance croissante des serveurs mandataires pour sécuriser le trafic sur Internet. Dans le cadre de notre étude, nous avons mis en place un serveur proxy squid sur la plateforme pfSense, en utilisant l'authentification LDAP.

Cette configuration nous a permis de bloquer sélectivement l'accès à Internet pour certains utilisateurs, ainsi que de filtrer les sites jugés dangereux ou inappropriés. En utilisant l'annuaire réseau LDAP, nous avons également mis en place un système d'authentification amélioré, offrant un meilleur contrôle et une gestion plus efficace des utilisateurs.

Cette expérience nous a permis de découvrir de nouveaux outils et systèmes pour améliorer les conditions de navigation sur Internet et renforcer la sécurité des réseaux. Nous avons ainsi acquis une expertise précieuse dans la configuration d'un proxy sécurisé avec l'authentification LDAP sur pfSense, offrant des avantages considérables en termes de contrôle et de gestion des utilisateurs.

**Mots-clés**— LDAP,PARE-FEU ,PROXY.

**Abstract** The technological evolution and the need to protect personal data have led to the increasing importance of proxy servers in securing Internet traffic. As part of our study, we have implemented a Squid proxy server on the pfSense platform, using LDAP authentication.

This configuration has allowed us to selectively block Internet access for certain users, as well as filter out websites deemed dangerous or inappropriate. By utilizing the LDAP directory service, we have also established an enhanced authentication system, providing better control and more efficient user management. This experience has enabled us to discover new tools and systems to enhance the browsing conditions on the Internet and strengthen network security. We have gained valuable expertise in configuring a secure proxy with LDAP authentication on pfSense, offering significant advantages in terms of user control and management

**Key-words**— LDAP,PARE-FEU ,PROXY

# Table de matière

Table des matières	iv
Table des figures	vii
Liste abréviation	ix
Introduction générale .....	1
<b>1. Etude de l'existant</b> .....	<b>2</b>
1.1.Introduction.....	2
1.2.Présentation de l'organisme d'accueil .....	2
1.2.1. Présentation de l'entreprise Bejaia Logistique.....	2
1.2.2. Historique de Bejaia Logistique.....	3
1.2.3. Les activités de Bejaia Logistique .....	4
1.3.Structure de Bejaia Logistique.....	4
1.3.1. Organigramme générale .....	4
1.3.2. La structure organisationnelle .....	5
1.4.Architecture de réseaux de BL.....	7
1.5.Infrastructure informatique de Bejaia logistique .....	7
1.6.Problématique .....	8
1.7.Solution proposée.....	8
1.8.Conclusion .....	9
<b>2. Généralités sur la sécurité</b> .....	<b>10</b>
2.1.Introduction.....	10
2.2.Définition de la sécurité informatique .....	10
2.3.Menaces .....	11
2.3.1. Les types de menaces .....	11
2.3.1.1.Les menaces accidentelles .....	11
2.3.1.2.Les menaces intentionnelles .....	11
2.4.Vulnérabilité .....	12
2.5.Attaques .....	12

2.5.1. Les différents types d'attaque .....	12
2.5.1.1.Ver .....	12
2.5.1.2.Virus Les menaces accidentelles .....	12
2.5.1.3.Déni de service (Dos) .....	13
2.5.1.4.L'homme du milieu (MITM) .....	13
2.6.Les intrusions .....	13
2.7.La politique de sécurité informatique .....	13
2.8.Les méthodes de protection .....	13
2.8.1. Les logiciels anti-virus .....	13
2.8.2. Chiffrement .....	14
2.8.2.1.Le chiffrement symétrique .....	14
2.8.2.2.Le chiffrement asymétrique .....	15
2.8.3. Pare-feu (Firewall) .....	16
2.8.4. Proxy .....	16
2.8.5. L'authentification .....	17
2.8.5.1.Les mots de passe .....	17
2.8.5.2.Les certificats numériques .....	17
2.9.Les protocoles de sécurité .....	18
2.9.1. Le protocole SSL .....	18
2.9.2. Le protocole SSH .....	18
2.9.3. IP sec (IP Secure) .....	18
2.10. Les annuaires réseaux .....	19
2.11. Définition .....	19
2.11.1. Les types d'annuaires .....	19
2.11.2. Les types d'annuaires .....	20
2.11.3. Le protocole LDAP .....	20
2.12. Conclusion.....	20
<b>3. Solution proposée .....</b>	<b>22</b>
3.1.Introduction.....	22
3.2.Solution proposée .....	22
3.3.Objectifs.....	23
3.4.Fonctionnement de pare-feu .....	23
3.5.Fonctionnement de l'Authentification LDAP (Lightweight Directory Access Protocol) .....	25
3.6.Fonctionnement d'un serveur proxy .....	27
3.7.Réseau étudié .....	28
3.8.Processus d'authentification LDAP .....	29
3.9.Le choix de protocole.....	30
3.10. Conclusion.....	31
<b>4. La mise en place et résultats .....</b>	<b>33</b>
4.1.Introduction .....	33

4.2.Installation et configuration des outils utilisés .....	33
4.2.1. VMware Workstation Pro 16.2.4 .....	33
4.2.2. Installation de pfSense .....	34
4.2.3. Installation de Microsoft Windows server 2019 .....	36
4.3.Configuration .....	40
4.3.1. Configuration pfSense .....	40
4.3.2. Installer Squid sur pfSense .....	44
4.3.3. Configurer Squid (Proxy) sur pfSense .....	45
4.3.4. Configurer les ACLs sur pfSense .....	49
4.3.5. Tester le proxy Squid .....	50
4.3.6. Configurer Squid en HTTPS (SSL Inspection) .....	52
4.3.7. Tester l'accès à Internet .....	53
4.3.8. Configurer l'authentification en Squid .....	54
4.3.9. Configurer la bande passante .....	55
4.4.Rapports d'accès Web Lightsquid .....	60
4.5.Conclusion .....	61
 Conclusion générale.....	 62
Bibliographie.....	63



# Table de figures

Figure 1– Logo de Bejaia Logistique	3
Figure 2 – organigramme générale de l’entreprise BL	4
Figure 3 – Architecture de réseaux de BL	7
Figure 4– Chiffrementsymétrique.	15
Figure 5 – Chiffrement asymétrique.	15
Figure 6 – Le principe de fonctionnement d’un Pare-feu (Firewall)	16
Figure 7 – Le principe de fonctionnement d’un serveur proxy	17
Figure 8 – Fonctionnement de pare-feu	24
Figure 9 – Fonctionnement de de l’Authentification	25
Figure 10 – Fonctionnement de proxy.	27
Figure 11– schéma global du réseau étudié	29
Figure 12 – Interface de menu du logiciel VMWare.	33
Figure 13 – Montage de l’image dans le lecteur CD de la machine virtuelle.	34
Figure 14 – Début de l’installation de pfSense.	35
Figure 15 – Progression de l’installation de pfSense.	35
Figure 16 – Fin d’installation de pfSense.	36
Figure 17 – choix du langage Windows Server.	37
Figure 18 – Fenêtre de début d’installation.	37
Figure 19 – Fenêtre de choix de la version.	38
Figure 20 – Choix de type d’installation.	38
Figure 21 – Choix de disque d’installation.	39
Figure 22 – Début d’installation de Windows Server.	39
Figure 23 – Vérification de l’adresse IP Windows Server.	40
Figure 24 – Vérification des adresses pare-feu.	41
Figure 25 – Configuration de l’adresse de machine Windows server 2019.	42
Figure 26 – Résultat du Ping de la machine Windows server.	42
Figure 27 – Résultat du Ping de la machine pare-feu.	43
Figure 28 – Accéder a` l’interface Web de pfSense.	43
Figure 29 – L’interface Web de pfSense.	44
Figure 30 – recherche du package Squid.	44
Figure 31– Installation du proxy Squid.	45
Figure 32- Configuration du cache dans le proxy Squid.	47
Figure 33– Configuration du proxy Squid.	48
Figure 34 - Configuration du proxy Squid (suite).	49
Figure 35- Configuration des ACLs proxy Squid.	50
Figure 36 – Configuration manuellement du proxy Squid.	50
Figure 37 – Résultat d’accès à yahoo.com	51
Figure 38 – Affichage des logs en temps réel coté Squid.	51

Figure 39 – Création du certificat. _____	52
Figure 40 – Activation la résolution DNS. _____	53
Figure 41 – Activation de l’option Enable SSL filtering. _____	53
Figure 42 – Teste d’accéder à la page facebook.com _____	54
Figure 43 – Configuration de l’authentification. _____	54
Figure 44 – Création des utilisateurs. _____	55
Figure 45– fenêtre d’authentification _____	55
Figure 46 – Création de limiteur Upload. _____	56
Figure 47 – Création d’une queue pour Upload. _____	57
Figure 48 – Création d’un limiteur Download _____	58
Figure 49 – Création d’une queue pour Download. _____	58
Figure 50 – Les limiteurs créés. _____	59
Figure 51 – Configuration des limiteurs dans les règles de pare-feu. _____	59
Figure 52 – Paquet LightSquid. _____	60
Figure 53– Configuration du paquet LightSquid. _____	60
Figure 54 – Rapport Squid. _____	61

# Liste abrégiation

API	Interface de programmation d'application
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name System)
DoS	Denial of Service
DSA	Directory System Agent
DUA	Directory User Agent
HTTP	HyperText Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IP sec	IP Secure
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAN	Metropolitan Area Network
MITM	Man-in-the-Middle
OSI	Open Systems Interconnection
RDN	Relative Distinguished Name
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

# Introduction générale

Les réseaux informatiques sont devenus un élément essentiel de notre vie quotidienne et professionnelle. Ils sont utilisés pour la communication, le partage de données et l'accès à Internet. Cependant, les réseaux informatiques sont également vulnérables aux menaces de sécurité telles que les attaques par déni, les virus, les logiciels malveillants et les attaques. Pour protéger les réseaux informatiques contre ces menaces, il est important de mettre en place des mesures de sécurité adéquates.

Le but de ce mémoire est de présenter les résultats d'une étude portant sur la mise en place d'un proxy sécurisé avec l'authentification LDAP. Ce proxy permet d'assurer la sécurité du réseau en filtrant le trafic entrant et en bloquant les accès non autorisés. L'authentification LDAP assure également la sécurité des données en permettant l'identification des utilisateurs et la gestion des accès.

Ce mémoire est divisé en quatre chapitres. Le premier chapitre présente une étude de l'existant, en décrivant les concepts de base des réseaux informatiques, les protocoles utilisés et les problèmes de sécurité courants. Le deuxième chapitre présente des généralités sur la sécurité des réseaux informatiques, en présentant les menaces de sécurité courantes et les mesures de sécurité à mettre en place. Le troisième chapitre se concentre sur la solution proposée, en présentant les objectifs de notre projet. Le quatrième et dernier chapitre décrit la mise en place du proxy sécurisé avec l'authentification LDAP, en expliquant les étapes à suivre pour sa réalisation.

En conclusion, ce mémoire offre une vue d'ensemble des réseaux informatiques, de leur sécurité et de la mise en place d'un proxy sécurisé avec l'authentification LDAP pour améliorer la sécurité du réseau.

# **Chapitre 1**

## **Etude de l'existant**

### **1.1. Introduction**

Dans ce chapitre, nous allons nous pencher sur la SARL Bejaia Logistique, en commençant par une présentation et l'historique de l'entreprise, depuis sa création jusqu'à ses activités actuelles. Nous étudierons également la situation informatique de l'entreprise, en examinant les outils et les technologies utilisés pour optimiser ses opérations logistiques. Enfin, nous poserons la problématique de l'entreprise et nous proposerons une solution.

### **1.2. Présentation de l'organisme d'accueil**

#### **1.2.1. Présentation de l'entreprise Bejaia Logistique**

La SARL Bejaia Logistique a été fondée en 2008 et est reconnue comme l'une des principales entreprises algériennes spécialisées dans le transport routier. Sa réputation de qualité et sa notoriété nationale sont le fruit de son important parc de transport, ainsi que de ses offres de location d'engins et de matériel pour les travaux publics, la manutention, la location de véhicules avec ou sans chauffeur, et le transport de produits pétroliers. Elle est enregistrée auprès du registre de commerce sous le numéro 07B0185663.

Bejaia Logistique est implantée dans la zone industrielle AHRIK, IGHZER AMOKRAN, située dans la commune d'Ouzellaguen, dans la wilaya de Bejaia, au nord-est de l'Algérie. Elle possède un capital de 95 400 000 DA et a réalisé un chiffre d'affaires de 1 940 619 000 DA en 2017. L'entreprise se concentre sur la fourniture de solutions logistiques dans divers domaines, ce qui explique la multiplication de ses clients internes et externes.

### 1.2.2. Historique de Bejaia Logistique

Au départ, avant d'obtenir son statut juridique de SARL, BL (Bejaia Logistique) était un service de parc et de transport dans l'entreprise de production d'eau minérale et de boissons diverses appelée SARL Ibrahim et Fils "Ifri". La création de ce service remonte à 2002, avec pour mission de transporter les marchandises produites par l'entreprise dans tout le pays.

Au fil des années, la production d'Ifri a augmenté, mais son système de distribution a été confronté à de nombreux problèmes. Les coûts de maintenance de ses moyens de transport étaient également très élevés, en particulier pendant la période hivernale. Pour alléger cette charge et éviter les coûts associés à l'utilisation de ses propres véhicules, Ifri a décidé de décentraliser son service de parc et de transport. Cette entreprise a été nommée Bejaia Logistique (BL) et a été créée en octobre 2008.

Au début, BL n'était qu'une petite entreprise chargée uniquement du transport des marchandises de sa société mère. Cependant, au fil des ans, elle a connu un grand succès et a vu son activité évoluer au fur et à mesure de sa performance. Grâce à une excellente gestion, elle est devenue une entreprise indépendante qui agit et pense par elle-même. Elle est passée d'une petite entreprise en 2008 à une moyenne entreprise, puis à une grande entreprise en seulement 10 ans.



*Figure 1– Logo de Bejaia Logistique. [1]*

### 1.2.3. Les activités de Bejaia Logistique

- La Sarl BL offre un large éventail de services, notamment le transport public de marchandises, la location d'engins et de véhicules avec ou sans chauffeur, ainsi que la location de matériel pour les bâtiments et les travaux publics. Au quotidien, BL se fixe de nombreuses missions liées à ses activités, telles que :
  - Garantir la satisfaction des clients.
  - Assurer la sécurité des personnes et des biens en relation avec les activités de transport.
  - Gérer la conduite, l'exploitation et la maintenance de ses réseaux d'activités, et étendre ses activités dans des zones inexplorées hors du pays.

## 1.3. Structure de Bejaia Logistique

### 1.3.1. Organigramme générale

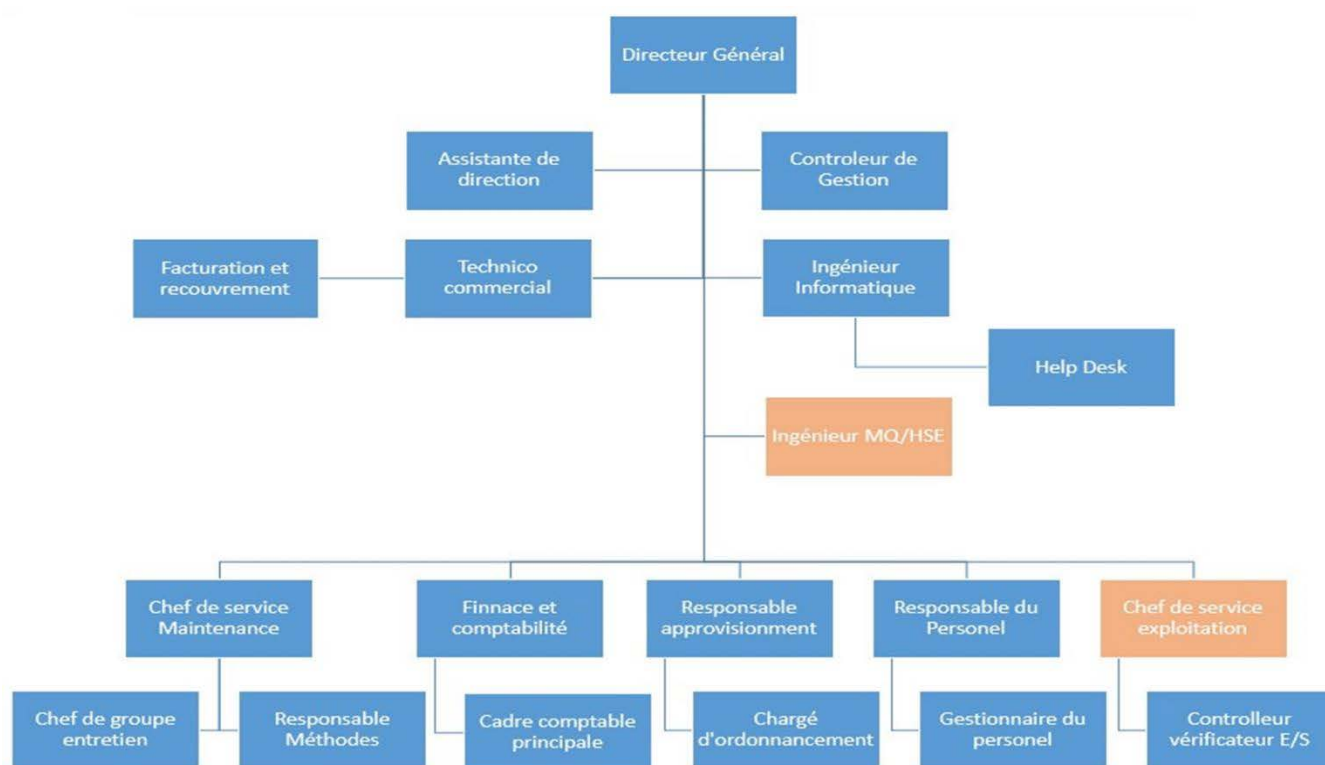


Figure 2 – Organigramme générale de l'entreprise BL.

### 1.3.2. La structure organisationnelle

#### ➤ **La direction générale**

Elle veille sur le bon déroulement des différentes tâches avec les meilleures conditions de travail et elle assure la conformité des informations entre les services, elle englobe les services contrôle de gestion, informatique MQ/HSE, RH, comptabilité, approvisionnement.

#### ➤ **Département secrétariat de direction**

Comprends deux postes, une secrétaire assistante et une standardiste, ses principales missions sont l'assistanat et d'assurer l'accueil physique, de répondre aux appels, aux courriers et aux e-mails.

#### ➤ **Département informatique**

Le département informatique a pour objectif d'assurer le développement de l'entreprise et de sélectionner les logiciels pour la gestion de l'entreprise. Il est également chargé d'établir la politique informatique et de garantir la sécurité et la disponibilité des données de l'entreprise.

#### ➤ **Département RH**

Le service RH a pour objectif d'apporter à l'entreprise le personnel nécessaire à son bon fonctionnement. Il se compose d'un chef ou d'un responsable de service, d'un chargé social, d'un chargé de formation, d'un suivi de paye et d'un suivi de carrière.

#### ➤ **Département facturation et comptabilité**

Le département de facturation et de comptabilité compte deux personnes qui se chargent respectivement de la facturation et des tâches comptables et financières. Leur rôle principal est d'assurer la conformité des opérations comptables, d'établir les factures et d'enregistrer les paiements des clients, tout en s'occupant des achats de fournitures nécessaires.



➤ **Département commercial**

Le département commercial est crucial pour le succès de l'entreprise. Il est chargé de la collaboration entre différents départements et de la réalisation des objectifs de l'entreprise.

➤ **Département d'exploitation**

Le département d'exploitation chez BL comprend un Responsable Exploitation TRM, un Chargé de suivi sinistre, un Chargé des dossiers d'exploitation et un Coordinateur TRM. Chacun de ces postes joue un rôle spécifique dans la gestion des opérations et la coordination des activités liées au transport routier de marchandises. [2]

## 1.4. Architecture de réseaux de BL

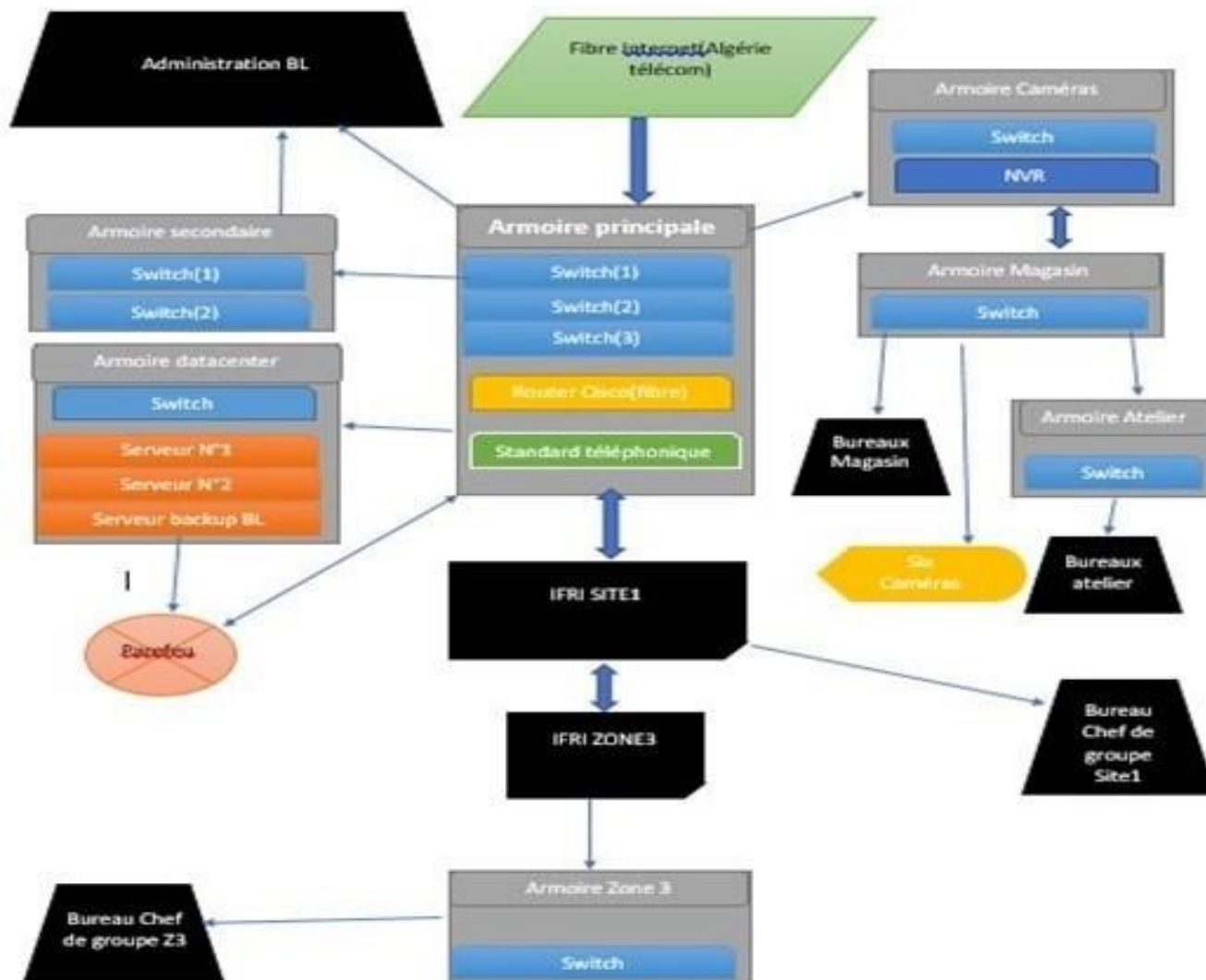


Figure 3 – Architecture de réseaux de BL. [3]

## 1.5. Infrastructure informatique de Bejaia logistique

L'entreprise d'accueil dispose d'un ensemble complet d'infrastructures informatiques pour soutenir ses activités. Au total, nous avons 103 ordinateurs, repartis dans différents départements et services. Ces ordinateurs sont soigneusement sélectionnés pour répondre aux besoins spécifiques de chaque équipe.

En ce qui concerne les logiciels, l'entreprise utilise au total 18 applications et programmes informatiques pour faciliter ses opérations. Parmi ces logiciels, 3 ont été développés en interne, spécialement conçus pour répondre aux exigences particulières de l'entreprise.

En ce qui concerne l'infrastructure matérielle, l'entreprise dispose de 37 imprimantes pour répondre aux besoins d'impression de ses employés. Ces imprimantes sont stratégiquement réparties dans les différents bureaux et départements pour garantir une accessibilité facile à tous.

Pour assurer une connectivité réseau fiable, l'entreprise possède 58 équipements réseau, tels que des routeurs, des commutateurs et des points d'accès sans fil. Ces équipements assurent une communication fluide entre les ordinateurs et les autres périphériques connectés au réseau.

En ce qui concerne la sécurité, l'entreprise dispose de 7 caméras de surveillance qui sont installées à des endroits clés de l'entreprise pour assurer la sécurité des locaux et des biens.

### **1.6. Problématique**

Bejaia Logistique (BL) est une entreprise de transports routiers qui bénéficie d'une réputation solide en Algérie. Toutefois, pour assurer une protection adéquate des informations sensibles, il est essentiel que les entreprises s'assurent que les données sont sécurisées contre les accès internet non autorisés. En outre, pour des raisons de sécurité, de conformité et de gestion de la bande passante, il est souvent nécessaire de contrôler l'accès à des ressources en ligne spécifiques. Pour garantir que seuls les utilisateurs autorisés peuvent accéder aux ressources en ligne, il est également important de fournir une méthode d'authentification fiable pour les utilisateurs. Cependant, la gestion de nombreux utilisateurs avec différents niveaux d'accès peut être difficile, ce qui rend la gestion des autorisations d'accès un défi important à relever pour les entreprises telles que BL.

### **1.7. Solution proposée**

En tant que stagiaires chez Bejaia Logistique, nous avons étudié différents scénarios et analysons les besoins de l'entreprise pour améliorer la sécurité des données et le contrôle d'accès aux ressources en ligne. Après notre analyse, nous avons proposé la mise en place d'un proxy sécurisé avec l'authentification LDAP comme solution adaptée à ces besoins.

Cette solution permet à Bejaia Logistique de garantir la confidentialité de ses données sensibles, en empêchant les accès non autorisés et en cryptant les échanges de données. Elle

permet également à l'entreprise de contrôler l'accès à ses ressources en ligne en fonction des besoins de chaque utilisateur et de limiter l'utilisation de la bande passante.

Grâce l'authentification LDAP, Bejaia Logistique pourrait gérer efficacement les comptes de ses utilisateurs et mettre à jour leurs informations d'identification en temps réel. Les administrateurs de l'entreprise auront également pu définir des règles pour permettre ou bloquer l'accès à des sites spécifiques en fonction des besoins de l'entreprise.

### **1.8. Conclusion**

En conclusion, la situation informatique actuelle de BL requiert une attention particulière pour répondre aux exigences de son évolution et pour s'assurer de bien sécuriser les accès au réseau, de limiter les risques d'attaques externes et internes et de renforcer la protection des données sensibles de BL. En optant pour la mise en place d'un proxy sécurisé avec l'authentification LDAP, l'entreprise pourra améliorer sa sécurité informatique et offrir à ses employés et à ses clients un environnement de travail plus sûr.

# Chapitre 2

## Généralités sur la sécurité

### 2.1. Introduction

Dans ce chapitre nous allons présenter un sujet essentiel qui est la sécurité informatique. Ce dernier est un enjeu crucial pour toutes les organisations. Nous allons examiner les menaces informatiques les plus courantes, les attaques et les méthodes de protection utilisées pour prévenir ces attaques malveillantes. Nous allons discuter également des normes et des standards en matière de sécurité informatique, afin de sensibiliser le lecteur aux enjeux de la sécurité des systèmes d'information.

Ce chapitre permettra aux lecteurs de comprendre les enjeux de la sécurité informatique.

Cette compréhension sera précieuse pour efficacement les systèmes et les données contre les menaces.

### 2.2. Définition de la sécurité informatique

La sécurité des réseaux consiste à prendre des mesures préventives pour protéger l'infrastructure réseau sous-jacente contre tout accès non autorisé, toute utilisation abusive, tout dysfonctionnement, toute modification, toute destruction ou toute divulgation inappropriée. La mise en œuvre de ces mesures permet aux ordinateurs, aux utilisateurs et aux programmes d'exécuter leurs fonctions critiques autorisées dans un environnement sécurisé. [4] La sécurité informatique vise généralement cinq principaux objectifs :

- ✓ L'intégrité : garantir que les données sont bien celles que l'on croit être
- ✓ La disponibilité : maintenir le bon fonctionnement du système d'information
- ✓ La confidentialité : rendre l'information inintelligible à d'autres personnes que les seuls acteurs d'une transaction.
- ✓ La non-répudiation : garantir qu'une transaction ne peut être niée
- ✓ L'authentification : assurer que seules les personnes autorisées aient accès aux ressources.

[5]

## 2.3. Menaces

Une menace est un danger qui existe dans l'environnement d'un système indépendamment de celui-ci. Il représente l'ensemble des actions de l'environnement d'un système pouvant entraîner des pertes financières. [6]

### 2.3.1. Les types de menaces

#### 2.3.1.1. Les menaces accidentelles

Ce sont :

- Pannes/dysfonctionnement du matériel.
- Pannes/dysfonctionnement du logiciel de base.
- Erreurs d'exploitation : oubli de sauvegardes, écrasement de fichiers.
- Erreurs de manipulation des informations : erreurs de saisie, erreurs de transmission, erreurs d'utilisation.
- Erreurs de conception des applications

#### 2.3.1.2. Les menaces intentionnelles

C'est l'ensemble des actions malveillantes qui constituent la plus grosse partie du risque, Parmi elles, on compte les menaces passives et les menaces actives

##### Les menaces passives

- Les menaces passives sont les détournements de logiciels : les copies illicites par exemple.

##### Les menaces actives

- Les menaces actives sont les modifications des informations : la fraude financière informatique,
- Les modifications des logiciels. [7]

### 2.4. Vulnérabilité

Une vulnérabilité est une faille de sécurité. Elle provient dans la majorité des cas d'une faiblesse dans la conception d'un système d'information (SI), d'un composant matériel ou d'un logiciel. [8]

### 2.5. Attaques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque, ce dernier est l'exploitation d'une faille d'un système informatique qui a pour conséquence d'utiliser le système d'une façon qui n'a pas été prévue par ses concepteurs [6]

- Pour accumuler des informations qui ne sont pas censées être publique.
- Pour effectuer des actions auxquelles l'on n'est normalement pas autorisé.
- Pour empêcher le système de fonctionner.

#### 2.5.1. Les différents types d'attaque

##### 2.5.1.1. Ver

Un ver informatique est un type de logiciel malveillant qui possède la faculté de se reproduire pour se propager, et ce, sans intervention humaine. Il exploite les failles connues d'un réseau pour s'introduire dans un système et se diffuser, notamment en utilisant la bande passante.

Il peut causer des dégâts considérables sur un appareil. S'il n'est pas nécessairement associé à des actions malveillantes telles que le vol d'informations ou d'argent, ce type de programme n'en est pas moins dangereux. Généralement, les vers provoquent un ralentissement brutal de la machine ciblée jusqu'à la rendre inutilisable. [9]

##### 2.5.1.2. Virus

Un virus est un logiciel capable de s'installer sur un ordinateur à l'insu de son utilisateur légitime. [10]

### 2.5.1.3. Déni de service (Dos)

Il s'agit d'attaques visant à perturber le bon fonctionnement d'un service, On distingue habituellement les types de déni de service suivant :

Exploitation de faiblesse des protocoles TCP/IP

Exploitation de vulnérabilité des logiciels serveurs. [11]

### 2.5.1.4. L'homme du milieu (MITM)

L'attaque de l'homme du milieu (HDM) ou man in the middle attack (MITM) en cryptographie est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. L'attaque "homme du milieu" est particulièrement applicable dans le protocole original d'échange de clés Diffie-Hellman, quand il est utilisé sans authentification. [12]

## 2.6. Les intrusions

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Le principal moyen pour prévenir les intrusions est le pare-feu. [6]

## 2.7. La politique de sécurité informatique

La Politique de sécurité du Système d'Information définit l'intégralité de la stratégie de sécurité informatique de l'entreprise. Elle se traduit par la réalisation d'un document qui regroupe l'ensemble des règles de sécurité à adopter ainsi que le plan d'action ayant pour objectif de maintenir le niveau de sécurité de l'information dans l'organisme. [13]

## 2.8. Les méthodes de protection

### 2.8.1. Les logiciels anti-virus

L'antivirus est un programme qui a pour but principal de détecter, neutraliser ou éradiquer les logiciels malveillants des ordinateurs et autres appareils informatiques qui sont infectés. Il joue



également un rôle préventif en empêchant les virus d'infecter les systèmes informatiques et de leur nuire. [14]

Les Antivirus ont différents modes de fonctionnement :

- La recherche par signature ou l'antivirus analyse le disque dur à la recherche d'une signature virus (un code de virus qui permet de l'identifier). L'antivirus compare son analyse du disque dur avec sa base de données pour détecter les virus (celle-ci doit être mise à jour régulièrement)
- L'analyse heuristique ou l'antivirus simule le comportement des logiciels pour voir s'ils ont un comportement agressif
- L'analyse du comportement ou l'antivirus surveille en permanence le comportement des logiciels actifs ainsi que les fichiers créés ou modifiés.

Ce type de fonctionnement est recommandé pour tout ordinateur connecté à internet.

Un antivirus va en réalité combiner ces trois méthodes puis lorsqu'il a détecté un virus, il va soit le réparer, le supprimer ou le mettre en "quarantaine" [15].

### 2.8.2. Chiffrement

Le chiffrement est utilisé pour assurer la confidentialité des données. Il est assuré par un système de clé appliquée au message envoyé. Ce dernier est d'encrypté par une clé unique [6] correspondant au cryptage.

Il existe deux types de chiffrement :

#### 2.8.2.1. Le chiffrement symétrique

La cryptographie symétrique (ou le cryptage des clés symétriques) est une classe d'algorithmes de cryptographie qui utilisent les mêmes clés cryptographiques pour le cryptage du texte clair et le décryptage du texte chiffré. [16]

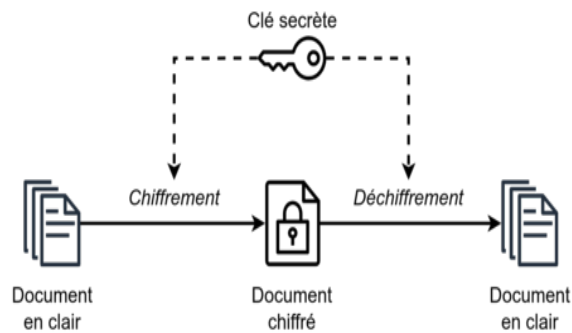


Figure 4– Chiffrement symétrique. [17]

### 2.8.2.2. Le chiffrement asymétrique

La cryptographie à clé publique (PKC), également appelée cryptographie asymétrique, se réfère à un algorithme cryptographique qui nécessite deux clés distinctes, dont l'une est secrète (ou privée) et l'autre public. Bien que différentes, les deux parties de cette paire de clés sont liées mathématiquement. [14]

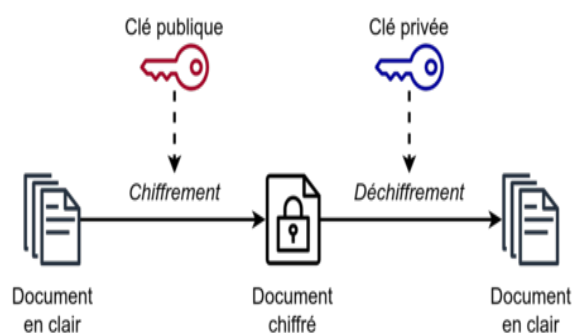
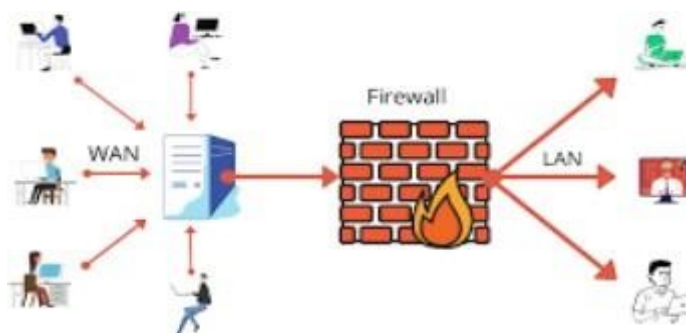


Figure 5 – Chiffrement asymétrique. [18]

### 2.8.3. Pare-feu (Firewall)

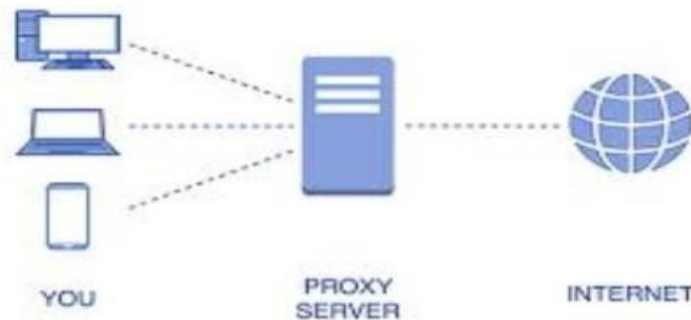
Un pare-feu est un système de sécurité qui surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de données en fonction d'un ensemble de règles de sécurité. Son objectif est de créer une barrière entre votre réseau interne et le trafic provenant de sources externes (telles que Internet) afin de bloquer le trafic malveillant tel que les virus et les pirates. [19]



*Figure 6 – Le principe de fonctionnement d'un Pare-feu (Firewall). [20]*

### 2.8.4. Proxy

Un serveur proxy est un ordinateur ou un système qui fonctionne comme une passerelle entre un dispositif terminal (navigateur Web ou ordinateur) et un serveur de destination (adresse Web) qui fournit un service demandé. [21]



*Figure 7 – Le principe de fonctionnement d’un serveur proxy. [22]*

### 2.8.5. L’authentification

C’est la vérification d’informations relatives à une personne ou à un processus informatique. L’authentification permet de prouver une identité déclarée. Dans un serveur, un processus de contrôle valide l’identité et après authentification, donne l’accès aux données, applications, bases de données, fichiers ou sites Internet. [6]

#### 2.8.5.1. Les mots de passe

Pour s’assurer que seules les personnes autorisées peuvent accéder à certaines parties du réseau, la méthode la plus simple et la plus courante consiste à protéger ces zones par un mot de passe.

#### 2.8.5.2. Les certificats numériques

Un certificat numérique authentifie les informations d’identification Web de l’expéditeur et permet au destinataire d’un message chiffré de savoir que les données proviennent d’une source fiable. [23]

## 2.9. Les protocoles de sécurité

### 2.9.1. Le protocole SSL

C'est un protocole destiné à assurer la sécurisation des échanges de données sur Internet. Il est indépendant du protocole de niveau applicatif. Ce qui signifie qu'il permet de chiffrer et d'authentifier différents types de protocoles. Le plus connu d'entre eux est évidemment http qui devient HTTPS une fois sécurisé par SSL. [24]

### 2.9.2. Le protocole SSH

Le protocole SSH (Secure Shell) est un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée. [6]

Les données circulantes entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (Spoofing).

### 2.9.3. IP sec (IP Secure)

C'est un protocole de la couche réseau. Il est issu de la suite protocolaire IPv6. Il s'agit de l'une des nombreuses options possibles. IP Sec va assurer à ses utilisateurs, tout à la fois : confidentialité, intégrité et authentification ainsi que la gestion des clés. [24]

#### IP sec repose sur deux mécanismes

- L'Authentication Header (AH) qui assure l'intégrité et l'authenticité des paquets IP.

- L'Encapsulating Security Payload (ESP) qui permet le chiffrement des informations en plus de l'authentification.

Bien que ces deux mécanismes soient indépendants, ils sont souvent utilisés ensemble. IP sec propose également des mécanismes de sécurisation des échanges entre les utilisateurs des VPN. En utilisant des algorithmes et des mécanismes de chiffrement, IP sec garantit l'authenticité des extrémités, la confidentialité et l'intégrité des échanges de données.

## 2.10. Les annuaires réseaux

### 2.11. Définition

Un annuaire réseau est un service ou une base de données qui stocke et organise des informations sur les ressources d'un réseau informatique, telles que des utilisateurs, des groupes, des ordinateurs et d'autres entités. Il permet de gérer les identités et les autorisations au sein d'un réseau en fournissant un moyen centralisé d'accès et de recherche d'informations. [6]

#### 2.11.1. Les types d'annuaires

La forme des annuaires électronique a beaucoup changé depuis leur apparition au début de l'ère informatique. Voici quelques-uns :

- Unix : /etc/password (années 70 – 80). Ce type d'annuaire qui est local à une machine, permet de gérer les différents utilisateurs pouvant être autorisés à se connecter à cette dernière.
- NIS (yellow pages; Network Information Service). Annuaire dont les données sont réparties sur l'ensemble des machines composant le réseau de l'entreprise, une machine au moins doit jouer le rôle de serveur.
- DNS (Domain Name System). Cet annuaire repartit au complet sur l'ensemble du réseau a comme rôle de traduire les noms de machines en adresses réseaux. X.500 (1988, 1993, 1997). Annuaire global de type pages blanches et pages jaunes.

- LDAP (Lightweight Directory Access Protocol), une version allégée des annuaires types X.500. [6]

### 2.11.2. Annuaires LDAP

Les annuaires LDAP (Lightweight Directory Access Protocol) sont des annuaires réseau basés sur le protocole LDAP, sont conçus pour être légers et efficaces.

### 2.11.3. Le protocole LDAP

Le protocole LDAP (Lightweight Directory Access Protocol) permet d'accéder à des bases d'informations sur les utilisateurs d'un réseau, via l'interrogation d'annuaires. [25]

LDAP emploie une approche client/serveur «en mode connecté avec le protocole TCP sur le port 389 par défaut. [26]

On retrouve dans le marché plusieurs annuaires LDAP, voici les plus connus :

- Apache Directory Server : <http://directory.apache.org>
- OpenLDAP : <http://www.openldap.org>
- 389 Directory Server.
- Microsoft Active Directory : <http://www.microsoft.com>
- Apple Open Directory.

## 2.12. Conclusion

En conclusion, la sécurité informatique est un aspect essentiel de notre vie moderne, étant donné notre dépendance croissante à l'égard des technologies de l'information. Au cours de ce chapitre, nous avons exploré les divers aspects de la sécurité informatique, notamment les menaces, les vulnérabilités, les attaques, les méthodes de protection et les protocoles de sécurité, ainsi que les annuaires réseau. Il est devenu évident que le paysage de la sécurité informatique est en constante évolution, avec des

menaces de plus en plus sophistiquées et des vulnérabilités à surveiller. La mise en place de méthodes de protection et de protocoles de sécurité appropriés est impérative pour garantir l'intégrité, la confidentialité et la disponibilité des données.

De plus, les annuaires réseau jouent un rôle crucial dans la gestion des ressources informatiques au sein d'une organisation. Il est essentiel de rester informé et d'adopter des pratiques de sécurité rigoureuses pour contrer les menaces et préserver la stabilité de nos système informatique.



# Chapitre 3

## Solution proposée

### 3.1. Introduction

Ce chapitre décrit les objectifs de notre projet, le fonctionnement de Pare-feu, ainsi que le fonctionnement de LDAP et le fonctionnement de proxy plus des schémas qui décrivent chaque fonctionnement, enfin l'architecture de notre réseau étudié et schéma qui le décrit. Dans ce chapitre, nous allons explorer les objectifs de notre projet, ainsi que le fonctionnement du pare-feu, de l'authentification LDAP et du proxy. Nous commencerons par d'écrire les objectifs que nous souhaitons atteindre, notamment l'optimisation des téléchargements, les analyses antivirus, la génération de statistiques détaillées, la gestion de la bande passante et la tolérance aux pannes grâce au load balancing. Ensuite, nous examinerons en détail le fonctionnement du pare-feu, du protocole LDAP et du serveur proxy, en fournissant des schémas explicatifs pour illustrer chaque processus, Enfin, nous présenterons l'architecture de notre réseau étudié, en fournissant un schéma qui décrit comment tous ces composants interagissent pour créer un environnement réseau robuste et sécurisé.

### 3.2. Solution proposée

En tant que stagiaires chez Bejaia Logistique, nous avons étudié différents scénarios et analysé les besoins de l'entreprise pour améliorer la sécurité des données et le contrôle d'accès aux ressources en ligne. Après notre analyse, nous avons proposé la mise en place d'un proxy sécurisé avec l'authentification LDAP comme solution adaptée à ces besoins.

Cette solution permet à Bejaia Logistique de garantir la confidentialité de ses données sensibles, en empêchant les accès non autorisés et en cryptant les échanges de données.

Elle permet également l'entreprise de contrôler l'accès à ses ressources en ligne en fonction des besoins de chaque utilisateur et de limiter l'utilisation de la bande passante.

Grâce à l'authentification LDAP, Bejaia Logistique pourrait gérer efficacement les comptes de ses utilisateurs et mettre à jour leurs informations d'identification en temps réel. Les administrateurs de l'entreprise auront également pu définir des règles pour permettre ou bloquer l'accès à des sites spécifiques en fonction des besoins de l'entreprise.

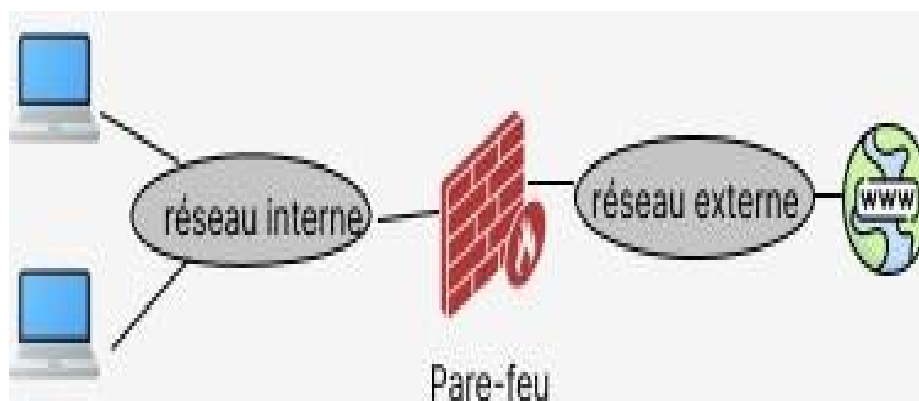
### 3.3. Objectifs

Les objectifs de notre projet de mise en place d'un proxy sécurisé avec l'authentification LDAP sont les suivants :

- **Optimisation des téléchargements** : Réduire le temps de téléchargement en mettant en cache les fichiers fréquemment demandés, améliorant ainsi l'efficacité et la productivité des utilisateurs.
- **Analyses antivirus** : Assurer une protection renforcée contre les logiciels malveillants en analysant chaque fichier téléchargé avant sa remise à l'utilisateur.
- **Génération de statistiques détaillées** : Collecter des informations sur l'utilisation du réseau, telles que les sites Web les plus visités, la bande passante utilisée par utilisateur, afin de mieux comprendre les tendances et d'optimiser la gestion du réseau.
- **Gestion de la bande passante** : Mettre en place des politiques de gestion de la bande passante pour garantir une utilisation équitable et prioriser certains types de trafic selon les besoins de l'entreprise.
- **Tolérance aux pannes avec le load balancing** : Assurer la continuité du service en répartissant la charge sur plusieurs connexions Internet ou serveurs proxy, minimisant ainsi les interruptions en cas de défaillance d'un équipement.

### 3.4. Fonctionnement de pare-feu

Un pare-feu est un système de protection du réseau qui surveille le trafic entrant et sortant, et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies. [27]



*Figure 8 – Fonctionnement de pare-feu. [28]*

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow).
- De bloquer la connexion (deny).
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées.
- Soit d'empêcher les échanges qui ont été explicitement interdits. [29]

### 3.5. Fonctionnement de l'Authentification LDAP (Lightweight Directory Access Protocol) :



*Figure 9 – Fonctionnement de l'Authentification LDAP. [28]*

- **Le protocole LDAP (Lightweight Directory Access Protocol) :** Est utilisé pour accéder et manipuler des services d'annuaires, tels que les serveurs LDAP. Voici quelques-uns de ses principaux services :
  - Recherche d'informations : LDAP permet de rechercher des informations spécifiques dans un annuaire en fonction de critères tels que des attributs particuliers, des noms d'utilisateurs ou d'autres informations liées à des objets stockés dans l'annuaire.
  - Interrogation et filtration : LDAP fournit des mécanismes pour interroger les annuaires en utilisant des filtres pour sélectionner des enregistrements particuliers en fonction de critères prédéfinis, ce qui facilite la récupération d'informations précises.

- Ajout, modification et suppression d'entrées : LDAP permet d'ajouter de nouvelles entrées dans l'annuaire, de modifier les attributs existants ou de supprimer des entrées, ce qui est essentiel pour la gestion des données dans l'annuaire.
- Authentification et autorisation : LDAP est couramment utilisé pour l'authentification des utilisateurs et la vérification de leurs informations d'identification.
- Il permet également de gérer les droits d'accès en autorisant ou en refusant l'accès à certaines parties de l'annuaire en fonction des rôles ou des groupes d'utilisateurs.
- Gestion des groupes et des utilisateurs : Les serveurs LDAP sont fréquemment utilisés pour gérer les informations relatives aux utilisateurs et aux groupes au sein d'une organisation. Ils permettent la création de profils d'utilisateurs, la gestion des rôles et des permissions, ainsi que la définition de relations hiérarchiques entre les utilisateurs et les groupes.
- Centralisation des informations : LDAP offre un moyen efficace de centraliser et de partager des informations importantes au sein d'une organisation. Il peut être utilisé pour stocker divers types d'informations, comme les adresses e-mail, les numéros de téléphone, les certificats de sécurité, etc.

Dans un scénario client- serveur LDAP typique, le client envoie des requêtes au serveur LDAP et reçoit des réponses en retour. Voici comment fonctionne le processus de base :

Pour son fonctionnement, LDAP définit deux méthodes de communication pour deux fonctions différentes. Le type de communication client/serveur permet au client d'accéder aux informations contenues sur le serveur. La communication de type serveur/serveur permet au serveur de répliquer ou de synchroniser ses informations sur d'autres serveurs.

❖ **Les opérations de base** : Définies par le protocole LDAP sont :

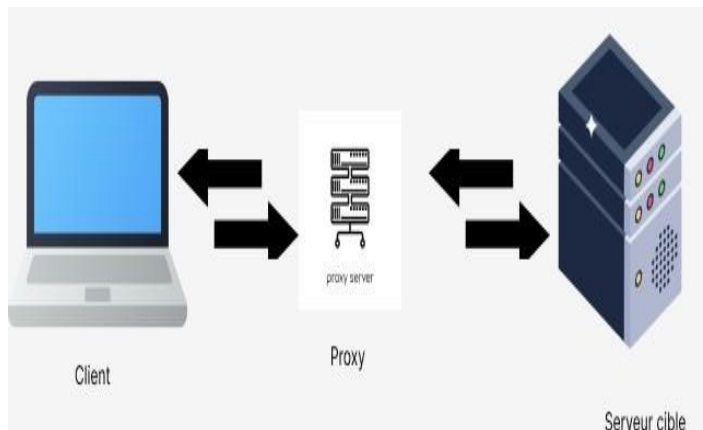
- ✓ **Requête** : Search, compare
- ✓ **Mise à jour** : Add, delete, modify
- ✓ **Connexion** : Bind, unbind, abandon

Le protocole LDAP utilise cinq modèles pour définir ses opérations à différents niveaux. Les 5 modèles sont :

- ✓ *Un modèle d'information* : Qui définit le type de données dans l'annuaire.
- ✓ *Un modèle de nommage* : Qui indique comment les données sont organisées.
- ✓ *Un modèle de fonction* : Qui indique comment accéder aux données.
- ✓ *Un modèle de sécurité* : Qui indique comment protéger l'accès aux données.
- ✓ *Un modèle de duplication* : Pour indiquer comment répartir les données entre les serveurs. [31]

### 3.6. Fonctionnement d'un serveur proxy

Un proxy agit comme un intermédiaire entre le client et le serveur, traitant les demandes et les réponses, contrôlant l'accès, améliorant les performances et fournissant des fonctionnalités de filtrage et de mise en cache. [32]



*Figure 10 – Fonctionnement de proxy. [33]*

Sur Internet, chaque ordinateur doit avoir une adresse IP (Internet Protocol) unique. On peut voir l'adresse IP. Un serveur proxy est connecté à Internet et dont notre ordinateur connaît l'adresse IP unique. Lorsqu'on envoie une requête Web, celle-ci est d'abord dirigée vers le serveur proxy. Celui-ci émet ensuite une requête en notre nom, récupère la réponse du serveur Web et nous transmet les données de la page Web afin que vous puissiez l'afficher dans votre navigateur. Lorsque le serveur proxy transmet les requêtes Web. Un serveur proxy peut modifier notre adresse IP,

Ce qui fait que le serveur Web ne sait pas exactement où nous nous trouvons. Il peut chiffrer nos données, ce qui les rend illisibles pendant leur transit. Et enfin, un serveur proxy peut bloquer l'accès à certaines pages Web, en se basant sur leur adresse IP.

### 3.7. Réseau étudié

Dans notre architecture, nous utilisons les composants suivants : pare-feu, proxy, et serveur LDAP, ces composants interagissent de la manière suivante :

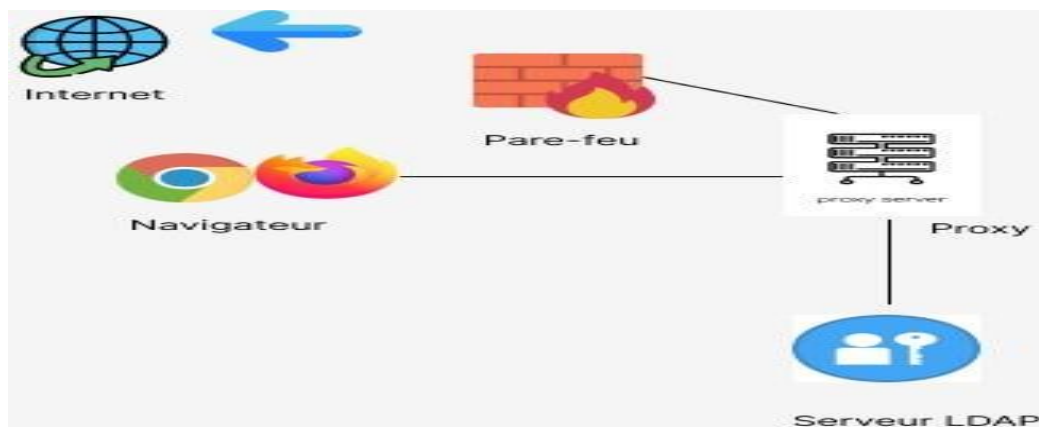
- **Le pare-feu utilise le protocole TCP/IP pour acheminer le trafic réseau :** Le pare-feu utilise le protocole TCP/IP pour acheminer le trafic réseau : Il examine les paquets de données entrants et sortants en fonction des règles de sécurité prédéfinies.

Pour la communication avec les utilisateurs, le pare-feu utilise le protocole TCP/IP pour établir des connexions et transférer les paquets de données entre les utilisateurs du réseau interne et Internet. Il peut également utiliser le protocole ICMP (Internet Control Message Protocol) pour envoyer des messages d'erreur ou des informations de contrôle liées au routage des paquets.

- **Le proxy utilise le protocole HTTP (Hypertext Transfer Protocol) :** Pour communiquer avec les clients et les serveurs Web. Lorsqu'un utilisateur envoie une requête Web, elle est d'abord dirigée vers le serveur proxy.

Le serveur proxy émet ensuite une requête HTTP vers le serveur Web correspondant pour récupérer la réponse. Il utilise également le protocole HTTP pour renvoyer les réponses aux utilisateurs. Il utilise le port 80 par défaut pour le trafic HTTP et le port 443 pour le trafic HTTPS.

- **Le serveur LDAP utilise le protocole LDAP (Lightweight Directory Access Protocol)** pour l'authentification des utilisateurs et la gestion des annuaires. Lorsqu'un utilisateur tente d'accéder à Internet, le proxy interroge le serveur LDAP en utilisant le protocole LDAP pour vérifier les informations d'identification de l'utilisateur, telles que le nom d'utilisateur et le mot de passe. Le serveur LDAP répond ensuite avec une réponse indiquant si l'authentification a réussi ou échoué, ce qui permet au proxy de prendre des décisions sur l'accès aux ressources. Le port standard utilisé par LDAP est le port 389, et pour des connexions sécurisées, le protocole LDAP peut également être utilisé avec SSL/TLS, dans ce cas le port 636 est utilisé.



*Figure 11– Schéma global du réseau étudié.*

### 3.8. Processus d'authentification LDAP

Le processus d'authentification LDAP suit un modèle client-serveur avec les éléments suivants :

- **DSA (Directory System Agent) :** serveur qui exécute le protocole LDAP sur le réseau.
- **DUA (Directory User Agent) :** utilisateur qui accède aux DSA en tant que client (par exemple, l'ordinateur portable d'un utilisateur).



- **DN (Distinguished Name)** : nom distinctif qui contient un chemin parcourant l'arbre DIT (Directory Information Tree) pour que le protocole LDAP puisse y accéder (par exemple : cn=Susanne, ou=utilisateurs, o=Entreprise).
- **RDN (Relative Distinguished Name)** : nom distinct relatif composé de chaque élément du chemin dans le DN (par exemple : cn=Susanne).
- **API** : Interface de programmation d'applications qui permet à un produit ou service de communiquer avec d'autres produits et services sans connaître les détails de leur mise en œuvre.

Voici les **étapes du processus d'authentification LDAP** :

- 1 . L'utilisateur lance un programme client LDAP (DUA) sur son ordinateur.
- 2 . Le DUA envoie une demande d'authentification contenant le DN de l'utilisateur au serveur LDAP (DSA) via le protocole LDAP.
- 3 . Le serveur LDAP utilise le DN pour rechercher les objets correspondants dans sa base de données.
- 4 . Les RDN contenus dans le DN sont utilisés pour trouver la personne concernée dans l'annuaire.
- 5 . L'objet correspondant au compte de l'utilisateur doit avoir les mêmes informations stockées dans l'annuaire (comme le nom d'utilisateur et le mot de passe) pour être validé.
- 6 . Une fois l'authentification réussie ou échouée, la connexion entre le client et le serveur LDAP est terminée.
- 7 . Les utilisateurs authentifiés peuvent accéder aux services et aux données d'application via l'API, en fonction des autorisations accordées par l'administrateur système.

Cela permet aux utilisateurs d'accéder aux fichiers, aux informations sur les utilisateurs et à d'autres données nécessaires via l'API et les services du réseau. [34]

### 3.9. Le choix de protocole

Le protocole LDAP présente plusieurs avantages pour la gestion des utilisateurs et l'authentification dans un réseau d'entreprise. Voici quelques raisons de choisir le protocole LDAP.

- **Simplification de la gestion** : Avec le protocole LDAP, les administrateurs réseaux peuvent gérer efficacement un grand nombre d'utilisateurs en attribuant des contrôles et des politiques d'accès en fonction de leur rôle et de leur niveau d'accès aux fichiers. Cela permet de simplifier le processus de gestion des utilisateurs et d'économiser du temps pour les administrateurs.
- **Centralisation de l'authentification** : Le protocole LDAP centralise le processus d'authentification, ce qui signifie que les utilisateurs peuvent utiliser les mêmes identifiants pour accéder à différents services et ressources du réseau. Cela simplifie l'expérience des utilisateurs et réduit la charge de gestion des mots de passe pour les administrateurs.
- **Accès quotidien aux données** : Si vos utilisateurs ont besoin d'accéder régulièrement à certaines données critiques, telles que l'intranet de l'entreprise, une application de messagerie ou d'autres services, le protocole LDAP est particulièrement adapté.
- **La recherche rapide et efficace des informations nécessaires** : ce qui facilite l'accès aux données fréquemment utilisées.

Avant de choisir d'implémenter le protocole LDAP, il est important de prendre en compte la capacité de stockage nécessaire pour gérer toutes les données des utilisateurs. De plus, il convient de considérer la fréquence d'accès aux données et services par les utilisateurs afin de déterminer si le protocole LDAP répondra efficacement à ces besoins. [35]

### 3.10. Conclusion

En conclusion, nous avons exploré les objectifs de notre projet de mise en place d'un proxy sécurisé avec l'authentification LDAP, ainsi que le fonctionnement du pare-feu, de l'authentification LDAP et du proxy. Chaque composant joue un rôle essentiel dans la création d'un environnement réseau robuste et sécurisé. Le pare-feu assure une protection en filtrant le trafic et en contrôlant l'accès, l'authentification LDAP vérifie l'identité des utilisateurs et applique les règles d'accès, tandis

que le proxy agit comme un intermédiaire pour optimiser les performances. Les schémas présentés ont permis de visualiser clairement le fonctionnement de chaque composant et leur interaction au sein de l'architecture du réseau étudié. Dans l'ensemble, notre projet vise à améliorer la productivité, la sécurité et la gestion de notre réseau, en offrant un environnement fiable et performant pour les utilisateurs.

Dans le chapitre suivant on va entamer la réalisation et la mise en place de notre solution de proxy sécurisé avec authentification LDAP. Nous allons décrire les différentes étapes de la mise en place et expliquer comment nous avons mis en place les différentes fonctionnalités de sécurité.

# Chapitre 4

## La mise en place et résultats

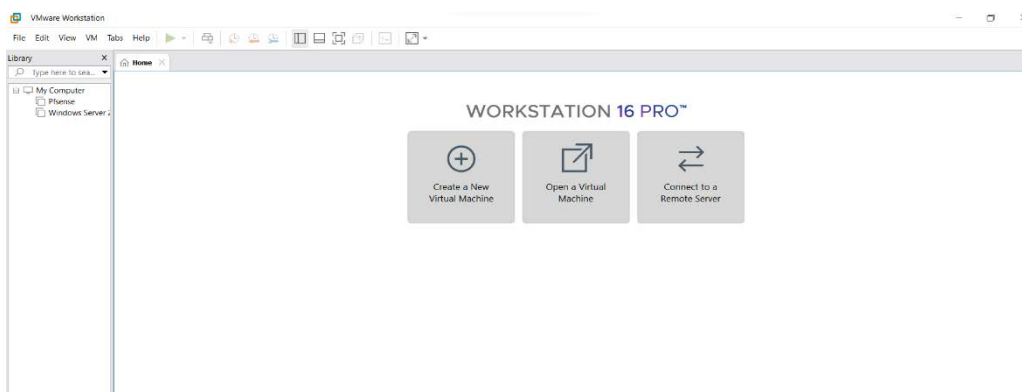
### 4.1. Introduction

Dans ce chapitre, nous allons aborder la mise en place d'un proxy **Squid** avec authentification **LDAP** par pfSense. Ce projet vise à améliorer la gestion du trafic réseau en utilisant un proxy Squid, qui agit comme un intermédiaire entre les utilisateurs et les serveurs, tout en renforçant la sécurité grâce à l'authentification LDAP. Nous explorerons les étapes clés de cette configuration, de l'installation des outils nécessaires à la configuration du proxy Squid et à l'activation de l'authentification des utilisateurs, Nous allons examiner également la gestion de la bande passante par utilisateur et l'utilisation du package LightSquid pour générer des rapports d'accès Web. Cette solution offre ainsi une visibilité accrue sur l'utilisation du réseau par les utilisateurs.

### 4.2. Installation et configuration des outils utilisés

#### 4.2.1. VMware Workstation Pro 16.2.4

**VMware Workstation** est un outil de virtualisation à destination des professionnels qui permet d'exécuter plusieurs systèmes d'exploitation en tant que machines virtuelles sur un PC Linux ou Windows. [35]

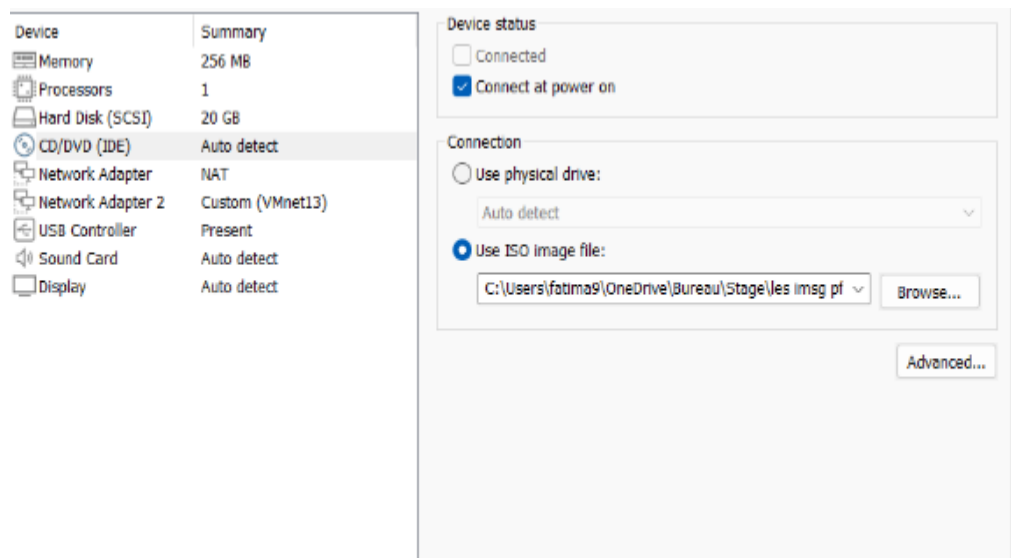


*Figure 12 – Interface de menu du logiciel VMware.*

### 4.2.2. Installation de pfSense

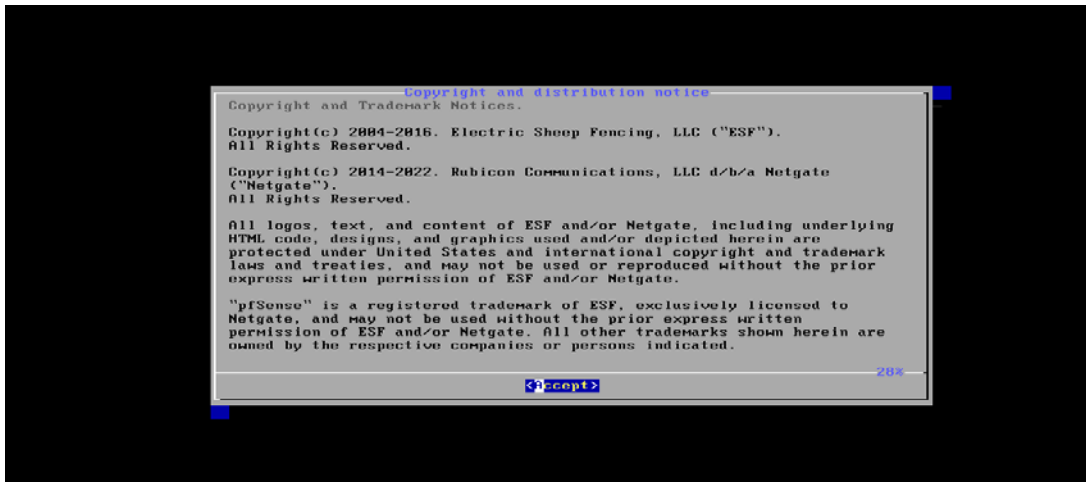
pfSense est un routeur/pare-feu open source basé sur FreeBSD. Il peut être installé sur un simple ordinateur personnel comme sur un serveur.

- Téléchargement de l'image ISO sur le site officiel de pfSense (<https://www.pfsense.org/>).
- Nous démarrons la machine après avoir inséré le périphérique nécessaire pour booter.
- Nous montons l'image dans le lecteur CD de la machine virtuelle.



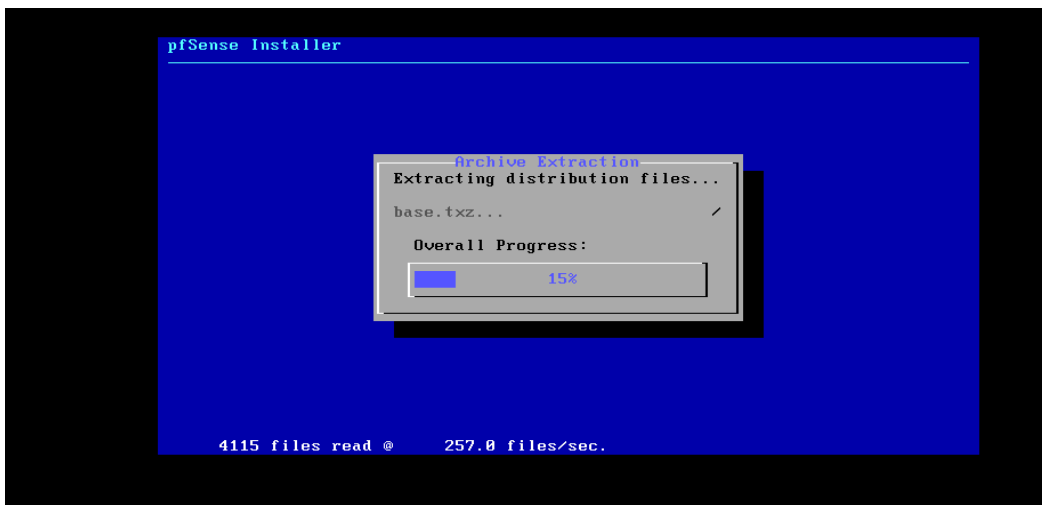
*Figure 13 – Montage de l'image dans le lecteur CD de la machine virtuelle.*

- Nous cliquons sur la case **accept** pour commencer l'installation.



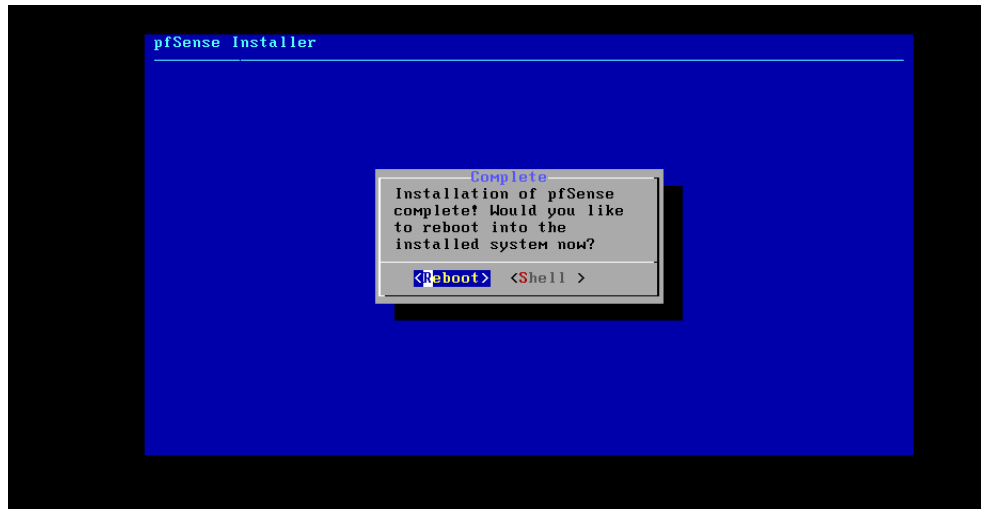
*Figure 14 – Début de l'installation de pfSense.*

- Nous allons suivre la procédure d'installation jusqu'à la fin de cette dernière.



*Figure 15 – Progression de l'installation de pfSense.*

- Le redémarrage de l'ordinateur est nécessaire afin d'utiliser la nouvelle installation.

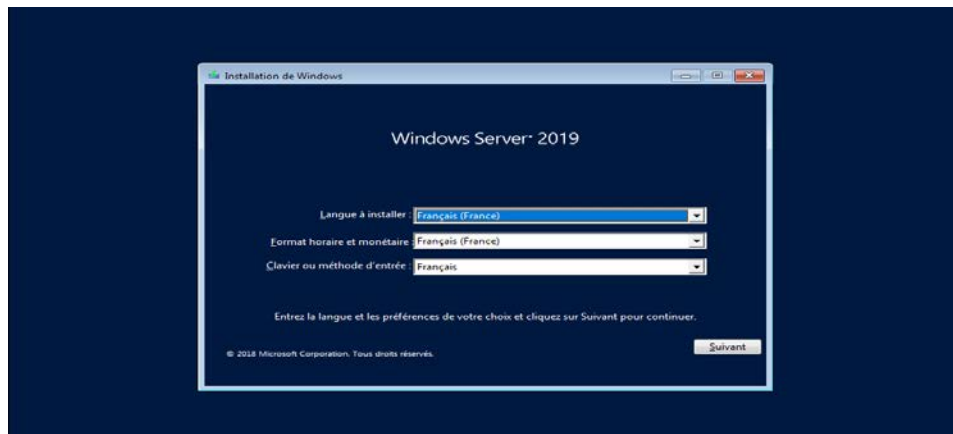


*Figure 16 – Fin d'installation de pfSense.*

#### 4.2.3. Installation de Microsoft Windows server 2019

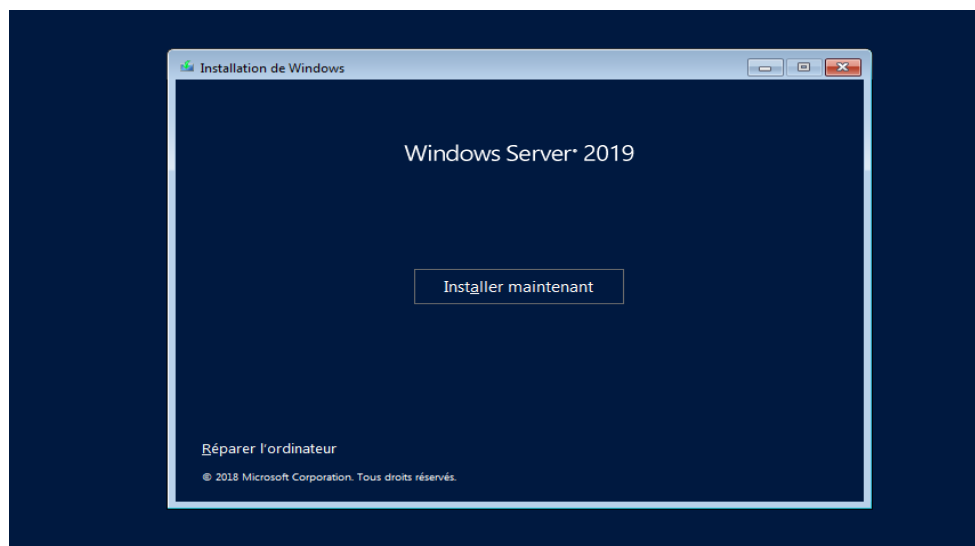
Microsoft Windows Server 2019 est un système d'exploitation de Microsoft orienté serveur. Nous avons utilisé Windows Server 2019 en tant que machine cliente. Windows Server 2019, la dernière version du système d'exploitation serveur de Microsoft, offre une plateforme robuste et fiable pour nos activités. Nous avons configuré Windows Server 2019 avec les paramètres nécessaires pour se connecter au réseau pfSense et bénéficier des fonctionnalités de sécurité avancées offertes par notre architecture.

- Nous téléchargeons le fichier d'installation (.iso) de Windows Server 2019 disponible sur le site officiel ( <https://www.microsoft.com/en-us/downloads/> )
- Nous démarrons la machine après avoir inséré le périphérique nécessaire pour booter.
- Dans la première fenêtre qui apparaît on choisit la langue souhaitée pour l'installation et nous appuyons sur **Next**.



*Figure 17 – choix du langage Windows Server.*

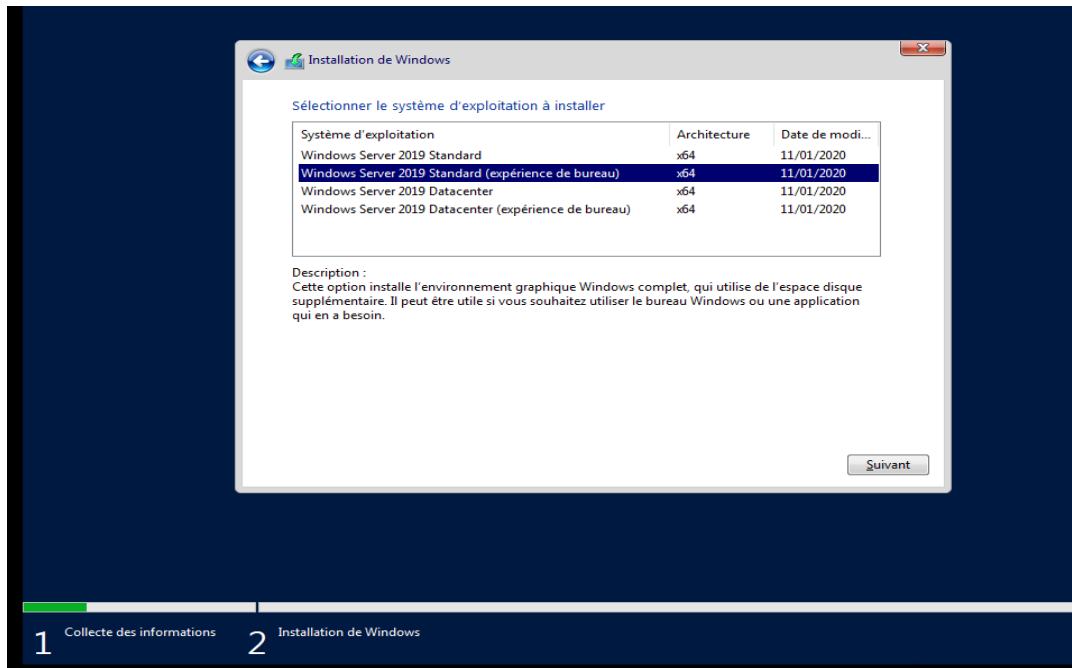
- Dans la deuxième fenêtre nous appuyions sur installer maintenant :



*Figure 18 – Fenêtre de début d'installation.*

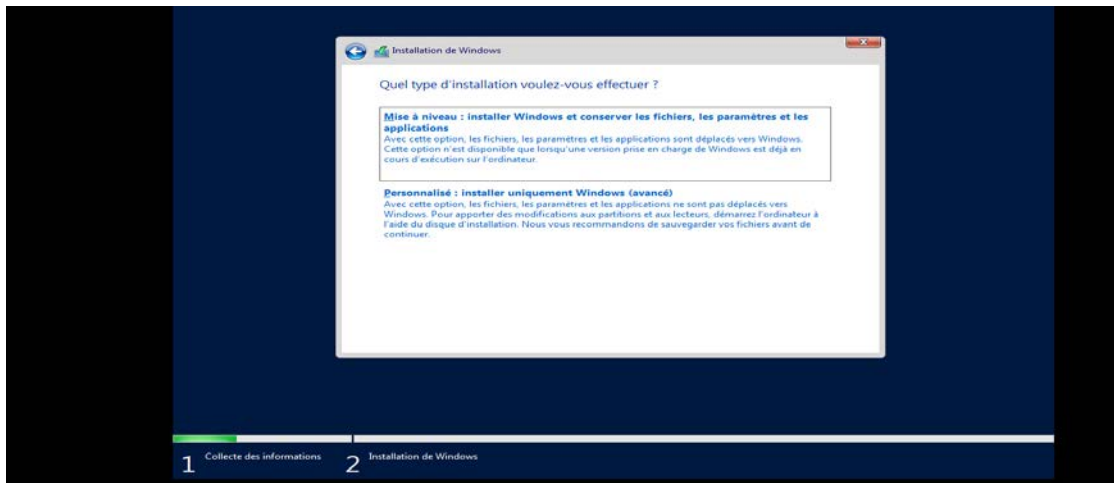
- Ensuite nous allons sélectionner l'Édition que nous souhaitons installer, qui est l'Édition Standard dans notre cas. Nous Cochons la case "Windows Server 2019 standard (expérience de bureau) " et nous cliquons sur **Suivant**.





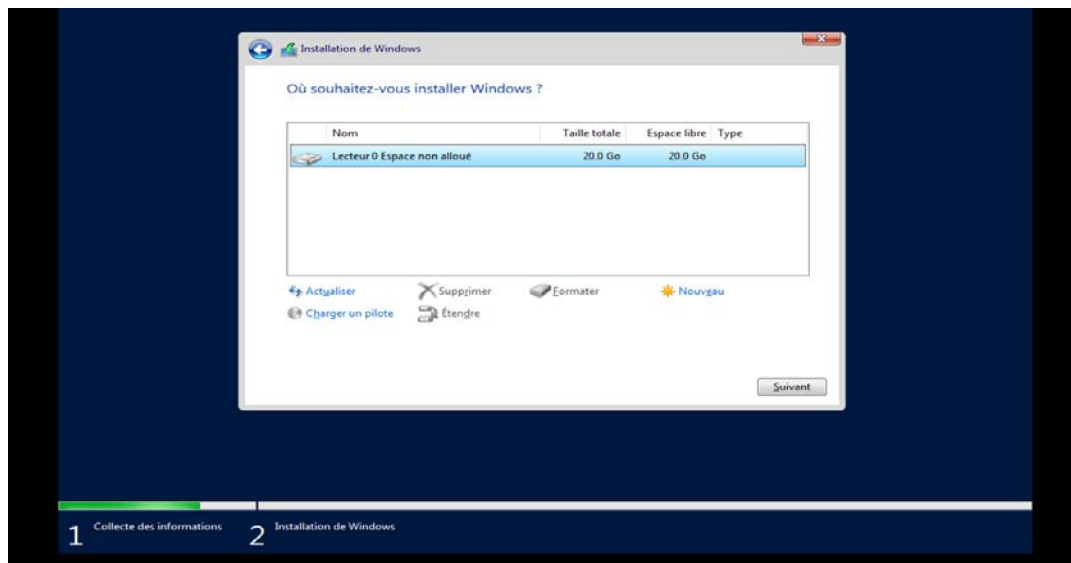
*Figure 19 – Fenêtre de choix de la version.*

- Ensuite nous sélectionnons le type d'installation **Personnalisé (avancé)** :

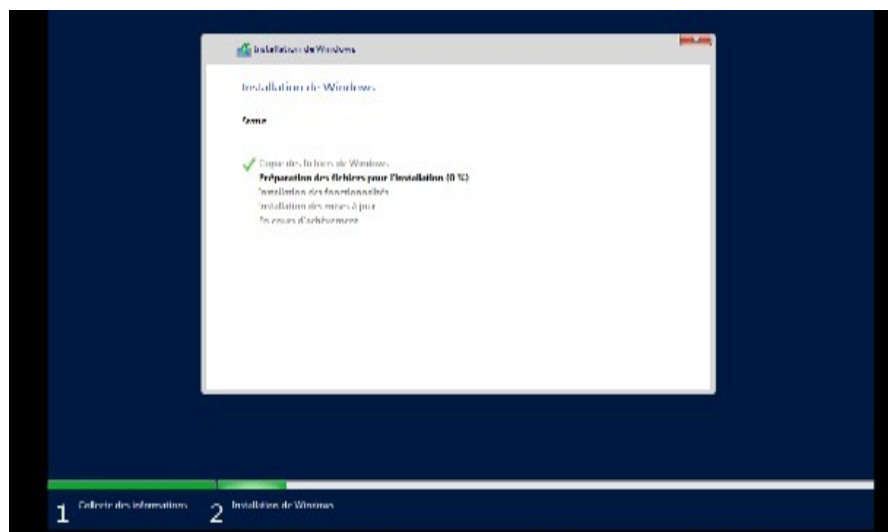


*Figure 20 – Choix de type d'installation.*

- Nous choisissons le disque sur lequel on veut installer notre Windows et nous cliquons enfin sur Suivant pour commencer l'installation de Windows Server 2019.



*Figure 21 – Choix de disque d'installation.*

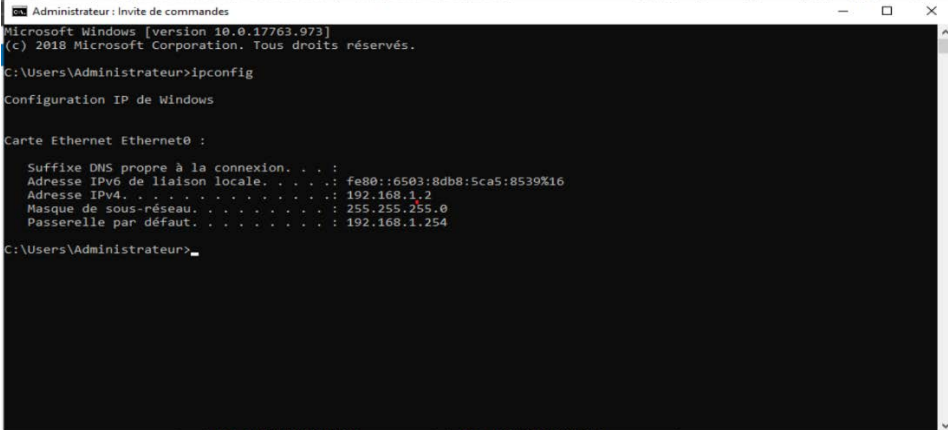


*Figure 22 – Début d'installation de Windows Server.*

## 4.3. Configuration

### 4.3.1. Configuration pfSense

- Au tout début, il est essentiel de vérifier les paramètres réseau des deux machines, à savoir celles du pfSense et du Windows Server 2019, afin d'obtenir leurs adresses IP respectives.
- Pour accéder à l'invite de commandes sur notre machine Windows Server 2019, nous devons commencer en appuyant sur le bouton "**Démarrer**". Ensuite, nous recherchons "cmd" dans la barre de recherche. Une fois que nous avons ouvert l'invite de commandes, nous tapons la commande "**ipconfig**" et appuyons sur la touche Entrée.



```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.17763.973]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . : fe80::6503:8db8:5ca5:8539%16
    Adresse IPv4. . . . . : 192.168.1.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.254

C:\Users\Administrateur>
```

*Figure 23 – Vérification de l'adresse IP Windows Server.*

L'adresse IP de cette machine est 192.168.1.2.

- Dans pfSense, nous pouvons observer deux interfaces réseau distinctes : **LAN** et **WAN**

```
Starting /usr/local/etc/rc.d/lighttpd_ls.sh...done.
Starting /usr/local/etc/rc.d/sq_monitor.sh...done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
ootup complete

FreeBSD/amd64 (pfsense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: fbc73f28e68e44963d00

** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfsense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.164.128/24
LAN (lan)      -> em1          -> v4: 192.168.1.254/24

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

Enter an option: █
```

*Figure 24 – Vérification des adresses pare-feu.*

- L'interface LAN est dédiée à la connectivité avec notre réseau local. Elle nous permet de communiquer avec les appareils présents sur notre réseau local.
- En revanche, l'interface WAN est utilisée pour établir une connexion avec des réseaux externes, tels que l'Internet.
- L'adresse IP 192.168.1.254, qui correspond à l'interface LAN du pfSense, sera utilisée comme adresse passerelle dans la machine Windows Server et aussi, cette adresse sera plus tard utilisée pour identifier le serveur Proxy.
- En utilisant l'adresse IP 192.168.1.254 comme adresse passerelle dans la machine Windows Server 2019, nous établissons une communication efficace entre cette machine et le pfSense, permettant ainsi la connectivité entre le réseau local et les réseaux externes.

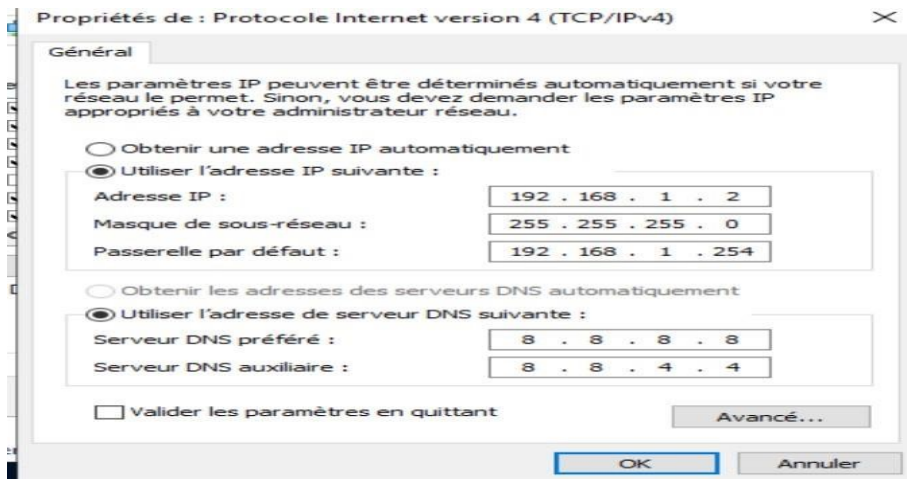


Figure 25 – Configuration de l'adresse de machine Windows server 2019.

- Nous testons la connectivité entre les deux machines :

### Connectivité vers le Windows Server

```

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.164.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.254/24

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

Enter an option: 8

[2.6.0-RELEASE][root@pfsense.home.arpa]/root: ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=128 time=0.434 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=0.503 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=0.543 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=0.504 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=128 time=0.555 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=128 time=0.446 ms

```

Figure 26 – Résultat du Ping de la machine Windows server.

## Connectivité vers la machine pfSense

```
C:\Users\Administrateur>ping 192.168.1.254

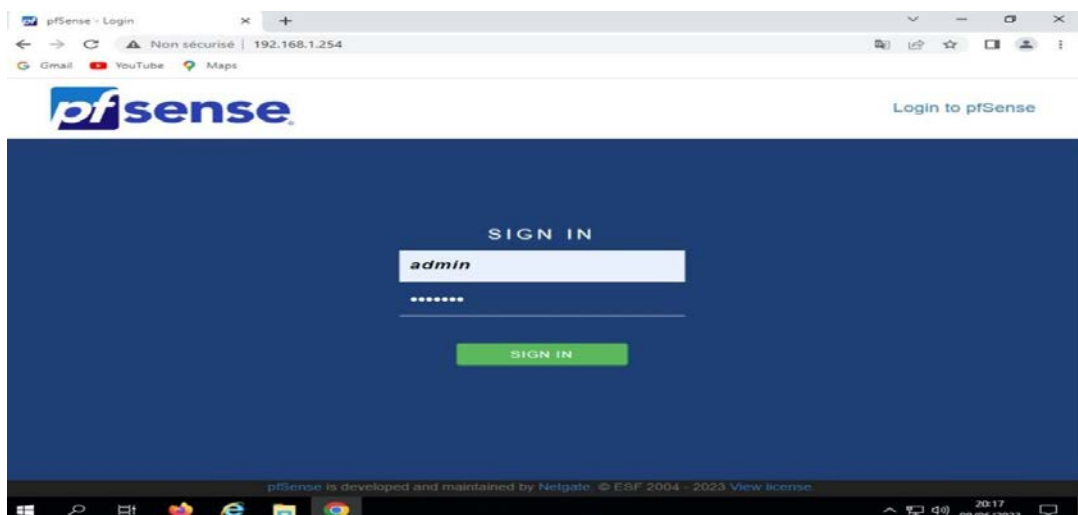
Envoi d'une requête 'Ping' 192.168.1.254 avec 32 octets de données :
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>
```

*Figure 27 – Résultat du Ping de la machine pare-feu.*

- Une fois que la connectivité est établie et vérifiée, nous devons effectuer l'installation des paquets sur la machine pfSense pour mettre en place Squid et configurer l'authentification de manière à sécuriser l'accès au proxy.
- Sur la machine Windows Server 2019, nous pouvons accéder à l'interface Web de pfSense en ouvrant votre navigateur et en entrant l'adresse IP LAN de pfSense dans la barre d'adresse, nous serons dirigés vers l'interface Web de pfSense. A partir de là, nous pourrions nous connecter et accéder aux fonctionnalités de configuration et d'administration de pfSense.



*Figure 28 – Accéder à l'interface Web de pfSense.*

- En utilisant les identifiants par défaut (Utilisateur : admin, mot de passe : pfSense), nous pouvons accéder à la page Web de pfSense. En saisissant ces informations dans la page de connexion, nous serons en mesure de nous connecter et d'accéder à l'interface Web de pfSense pour effectuer la configuration et l'administration.

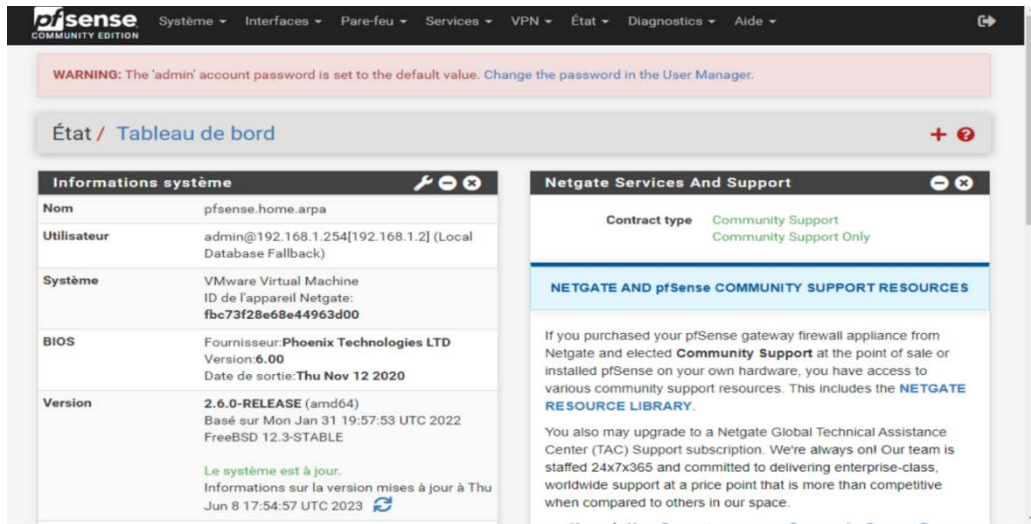


Figure 29 – L'interface Web de pfSense.

### 4.3.2. Installer Squid sur pfSense

Sur l'interface d'administration de pfSense, sous "System", on clique sur "Package Manager" et ensuite sur l'onglet " Available Packages "

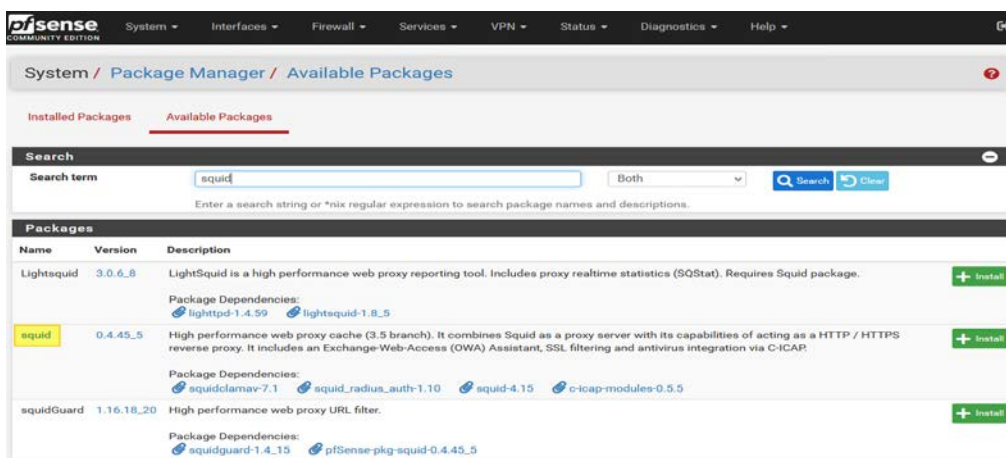
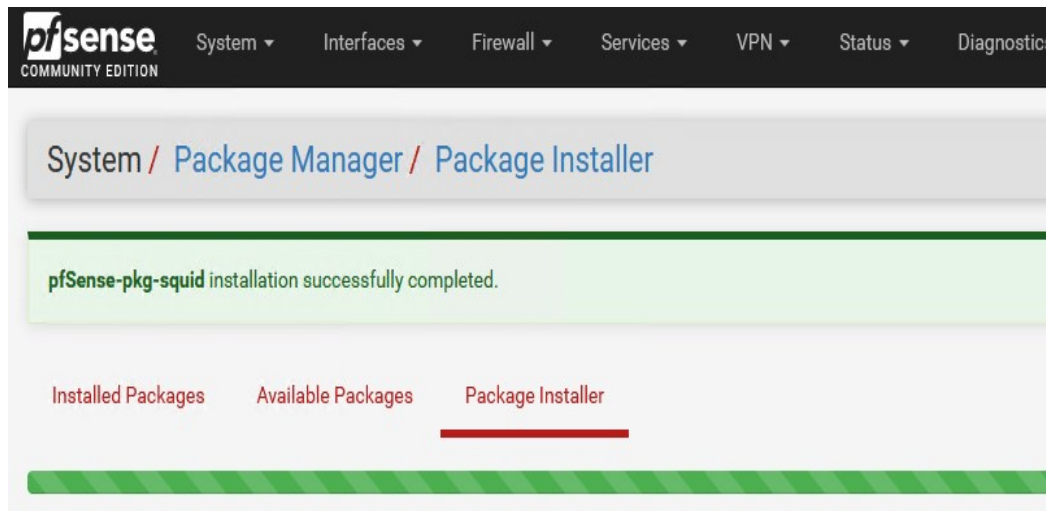


Figure 30 – recherche du package Squid.

A la fin de l'installation, le message (pfSense-pkg-squid installation successfully completed) s'affiche :



*Figure 31– Installation du proxy Squid.*

### 4.3.3. Configurer Squid (Proxy) sur pfSense

La configuration de Squid s'effectue via le menu "Services" puis "Proxy Server". Afin de pouvoir activer Squid, il faut configurer le cache local sinon le démarrage du processus Squid échouera.

Nous cliquons sur l'onglet "Local Cache".

- Hard Disk Cache Size : Sur "750" pour 750 Mo, cette valeur correspond à la taille maximale du cache sur l'espace disque. Nous pouvons augmenter cette valeur à 1024 Mo pour avoir 1 Go de cache.
- Hard Disk Cache Location : L'emplacement du cache, à savoir par défaut "/var/squid/cache".



Paquet / Proxy Server: Cache Management / Local Cache

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

### Squid Cache General Settings

**Disable Caching**  Disable caching completely.  
This may be required if Squid is only used as a proxy to audit website access.

**Cache Replacement Policy** Heap LFUDA  
The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. Default: heap LFUDA ⓘ

**Low-Water Mark in %** 90  
The low-water mark for AUFS/DFS/diskd cache object eviction by the cache\_replacement\_policy algorithm. ⓘ

**High-Water Mark in %** 95  
The high-water mark for AUFS/DFS/diskd cache object eviction by the cache\_replacement\_policy algorithm. ⓘ

**Do Not Cache**

### Squid Hard Disk Cache Settings

**Hard Disk Cache Size** 750  
Amount of disk space (in megabytes) to use for cached objects.

**Hard Disk Cache System** ufs  
This specifies the kind of storage system to use. ⓘ

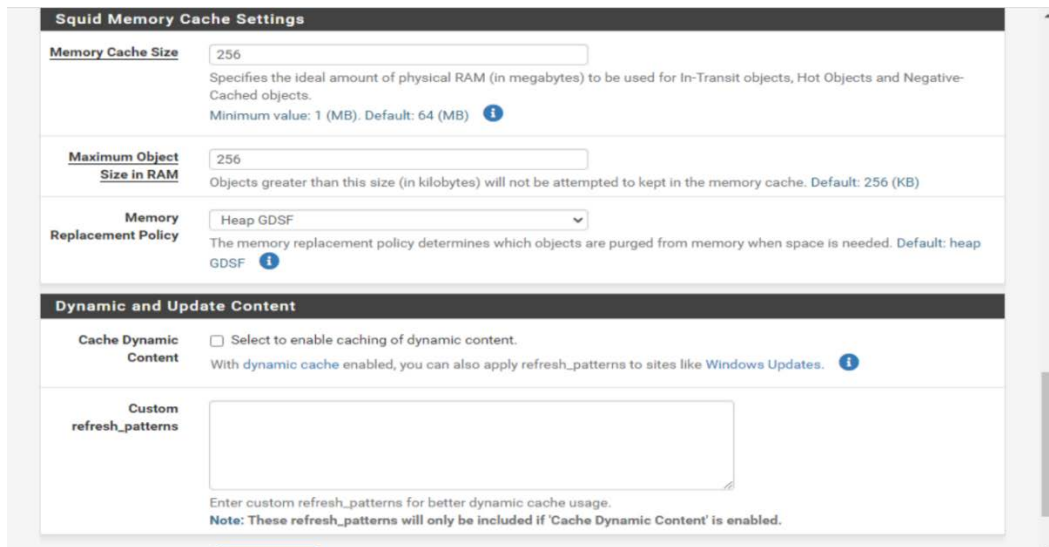
**Clear Disk Cache NOW**  
Hard Disk Cache is automatically managed by swapstate\_check.php script which is scheduled to run daily via cron. ⓘ  
If you wish to clear cache **immediately**, click this button **once**: [Clear Disk Cache NOW](#)

**Level 1 Directories** 16  
Specifies the number of Level 1 directories for the hard disk cache. ⓘ

**Hard Disk Cache Location** /var/squid/cache  
This is the directory where the cache will be stored. Default: /var/squid/cache ⓘ

**Minimum Object Size** 0  
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)

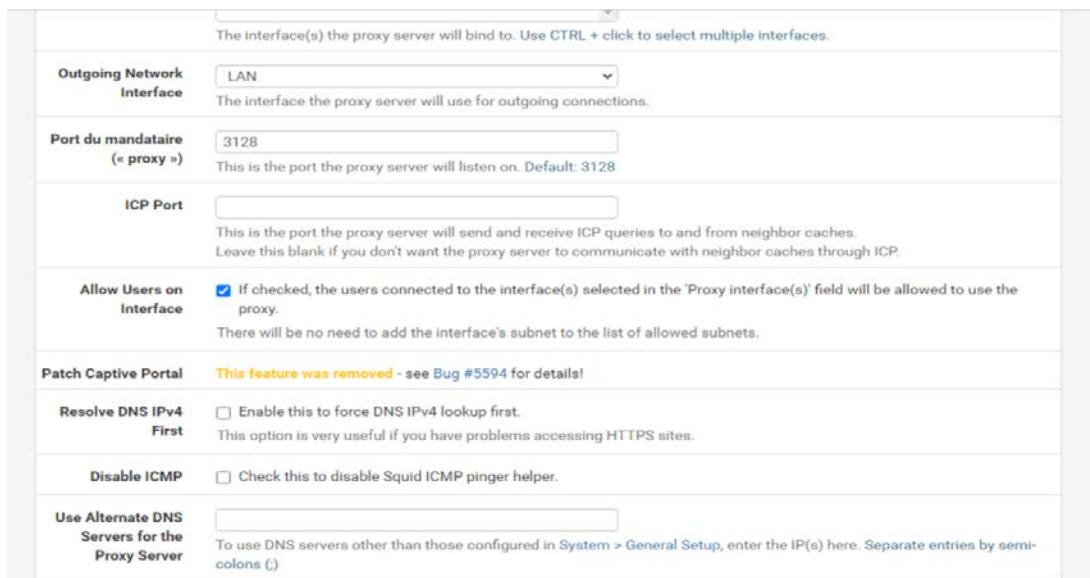
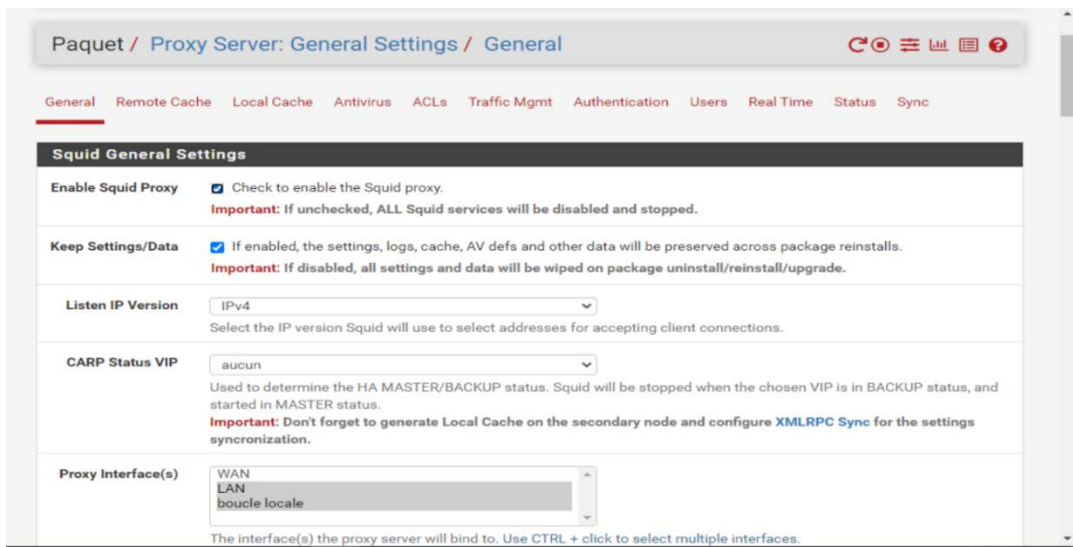
**Maximum Object Size** 10  
Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB) ⓘ



*Figure 32- Configuration du cache dans le proxy Squid.*

Ensuite, cliquez sur l'onglet "General".

- **Enable Squid Proxy** : nous cochons la case pour activer Squid sur le pare-feu, ce qui signifie qu'il va démarrer.
- **Proxy interface(s)** : Sur quelle interface nous souhaitons activer le proxy.
- **Proxy Port** : nous laissons le port par défaut, 3128.
- **AllowUsers on interface** : Cochez cette case pour autoriser implicitement les utilisateurs connectés sur le réseau "LAN" à utiliser le proxy.



*Figure 33– Configuration du proxy Squid.*

Nous continuons de descendre dans la page pour activez les journaux comme ceci :

- **Enable Access Logging** : nous allons cocher l’option pour activer les journaux, ce qui va permettre de savoir qui fait quoi sur Internet.
- **Rotate Logs** : Pendant combien de jours souhaitons-nous conserver les logs.

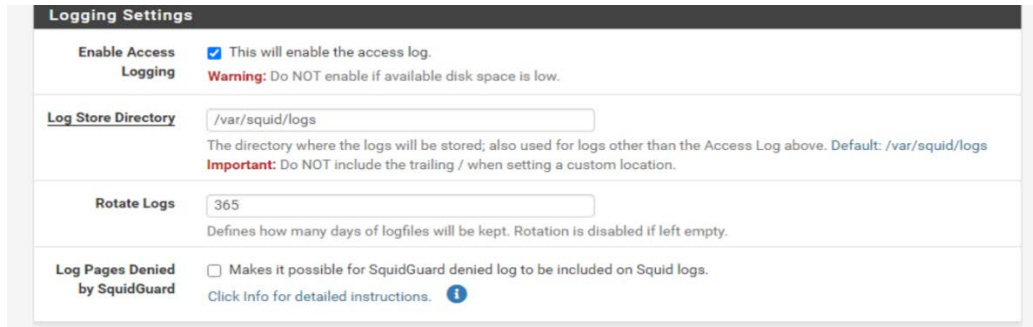
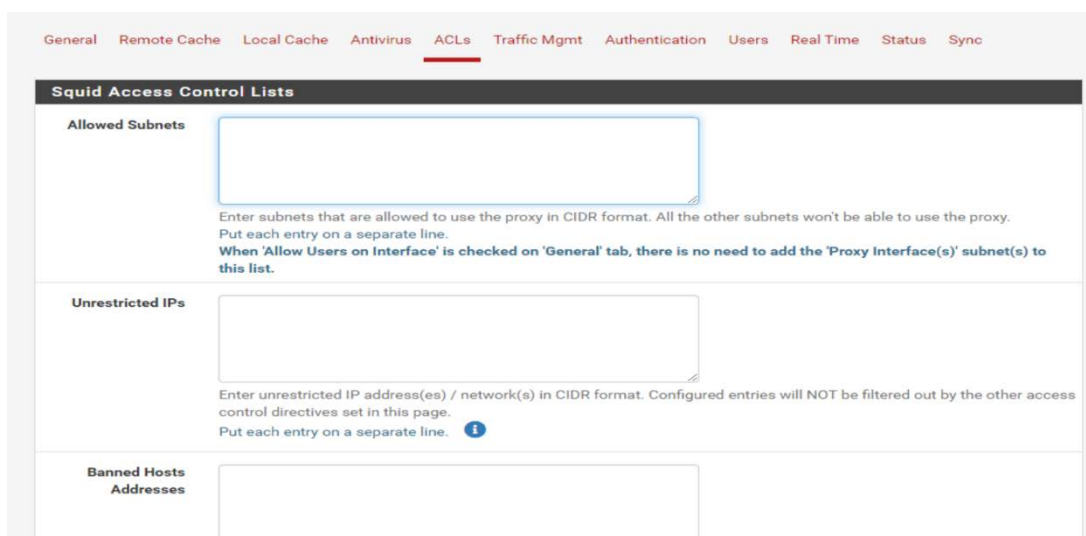


Figure 34 - Configuration du proxy Squid (suite).

Voilà, nous avons arrivé au bout de la page de configuration, nous cliquons sur **”Save”** pour appliquer cette nouvelle configuration.

#### 4.3.4. Configurer les ACLs sur pfSense

Nous cliquons sur l’onglet **”ACLs”**, toujours dans la configuration de Squid. C’est ici que nous pouvons déclarer les sous-réseaux autorisés à utiliser le proxy (**AllowedSubnets**), ce qui intéressant pour ce test, c’est l’option **”Blacklist”** puisqu’elle permet d’indiquer un ou plusieurs domaines à bloquer. Pour ce test, il nous faut un site en HTTP.



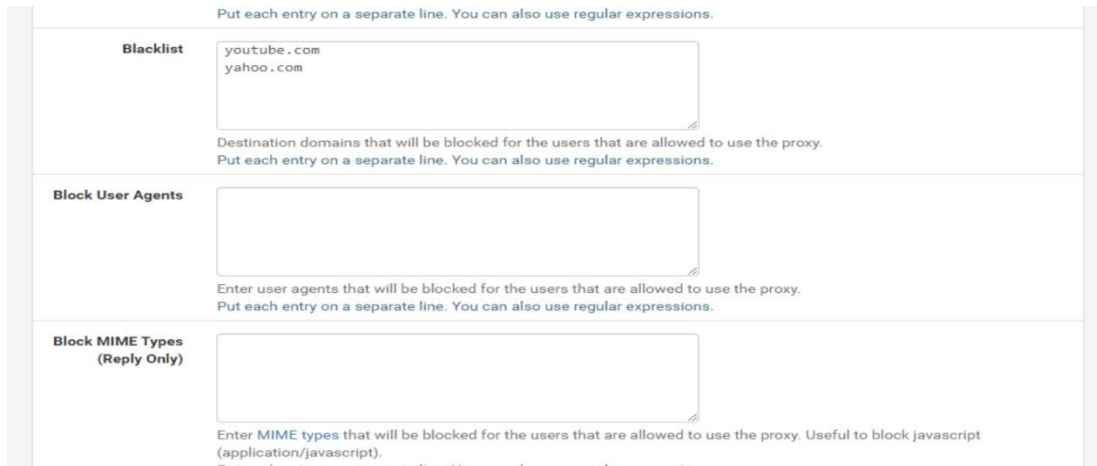


Figure 35- Configuration des ACLs proxy Squid.

### 4.3.5. Tester le proxy Squid

Tout d’abord nous devons activer le proxy manuellement dans le navigateur :

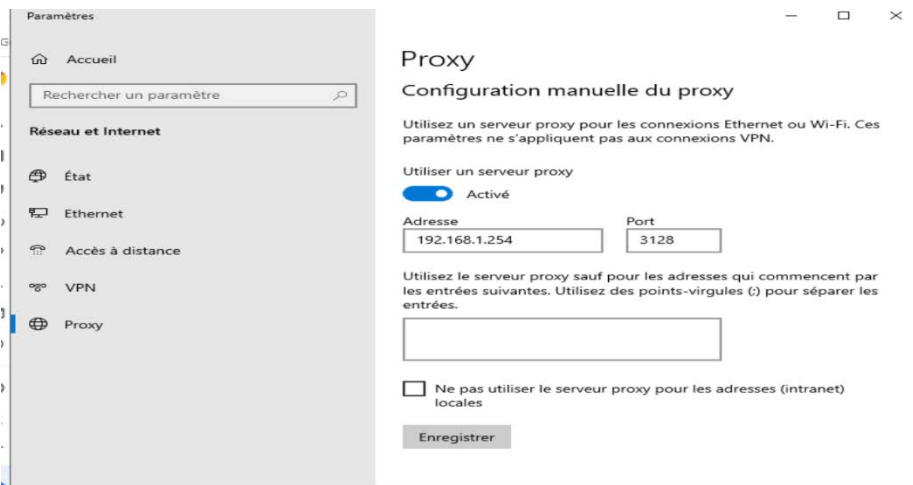
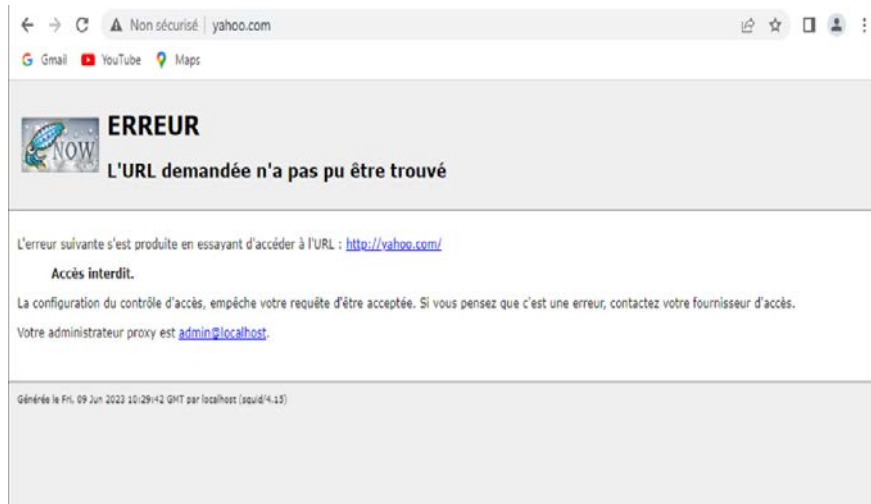


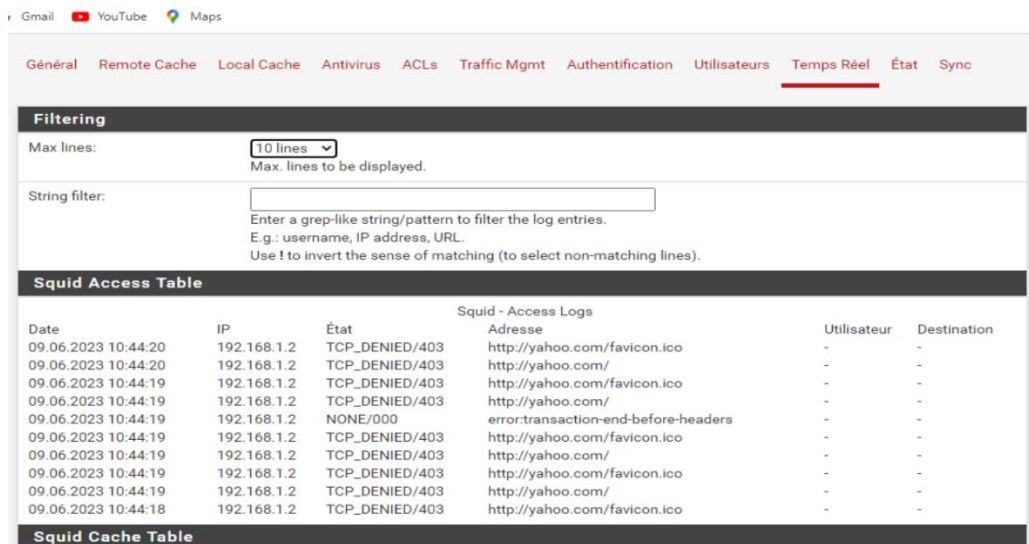
Figure 36 – Configuration manuellement du proxy Squid.

- Ensuite, à partir d’un poste de travail situé sur le réseau local, on tente d’accéder au site : **Yahoo.com**. Et là, on peut voir que ça ne fonctionne pas ! On peut voir qu’une page **”Accès interdit”** renvoyée par Squid s’affiche.



**Figure 37 – Résultat d'accès à yahoo.com.**

Nous pouvons aussi suivre les logs en temps réel côté Squid, via l'onglet "Real Time". Nous voyions très bien nos requêtes à destination du site "Yahoo.com" depuis l'hôte 192.168.1.2 : c'est la preuve irréfutable que notre PC passe bien par le proxy :



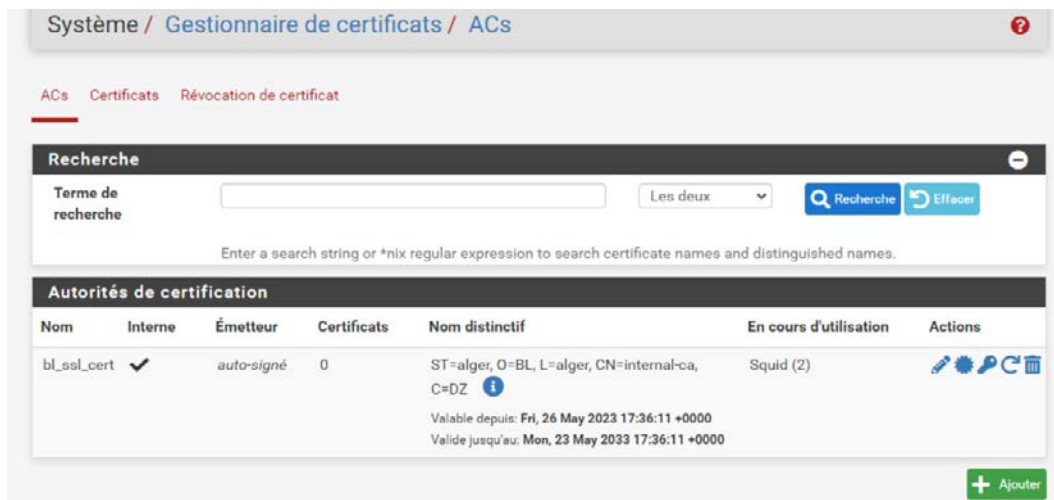
**Figure 38 – Affichage des logs en temps réel coté Squid.**

### 4.3.6. Configurer Squid en HTTPS (SSL Inspection)

Notre configuration proxy fonctionne seulement sur le protocole HTTP, il faut faire ce que l'on appelle :

**SSL Inspection.** Puisqu'un flux HTTPS est chiffré, le proxy ne peut pas seulement regarder les trames passer. En effet, pour chaque connexion, il doit déchiffrer le flux, l'inspecter puis le chiffrer à nouveau afin de l'acheminer.

- D'abord on doit Créer l'autorité de certification pfSense
- Dans **System** puis **"Cert. Manager"** et dans l'onglet **"CAs"**. On clique sur **"Add"**



*Figure 39 – Création du certificat.*

- Puis **SSL Inspection avec Squid** : Dans la configuration de Squid, via le menu **"Services"**. Nous cochons l'option **"Resolve DNS IPv4 First"** pour activer la résolution DNS du filtrage, ce qui est recommandé lorsque l'on filtre le HTTPS.

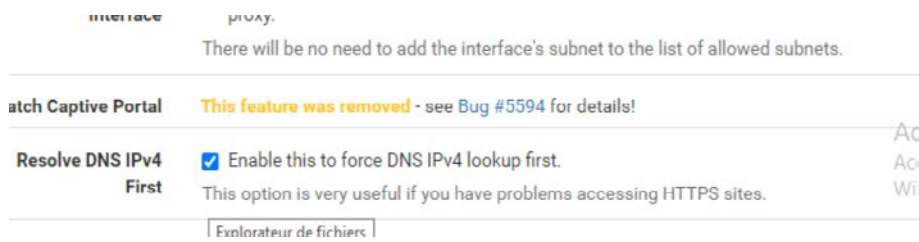


Figure 40 – Activation la résolution DNS.

- Ensuite, nous allons activer l’option ”**Enable SSL filtering**”. Pour le mode **SSL/MITM Mode**”, choisissez le mode **Splice All**.

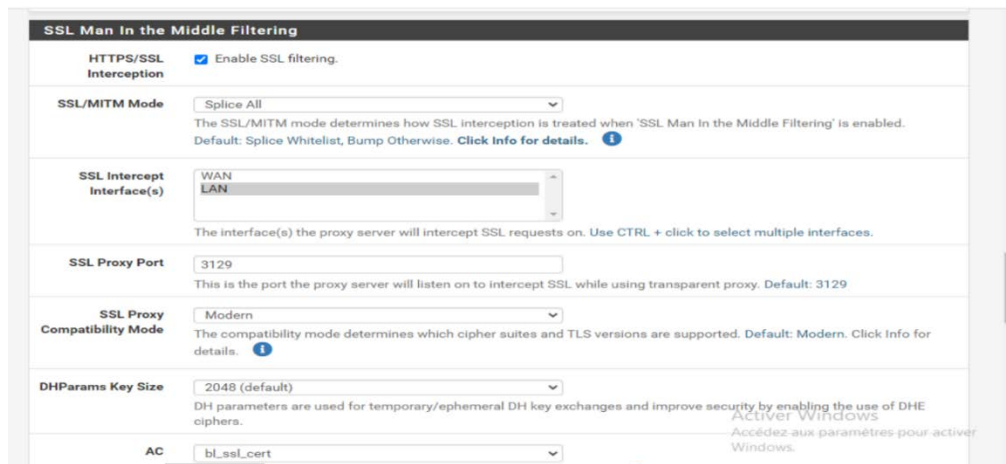


Figure 41 – Activation de l’option Enable SSL filtering.

#### 4.3.7. Tester l’accès à Internet

On tente de naviguer sur un site en HTTPS : Bloquer un site HTTPS dans Squid par exemple : **Facebook.com**.



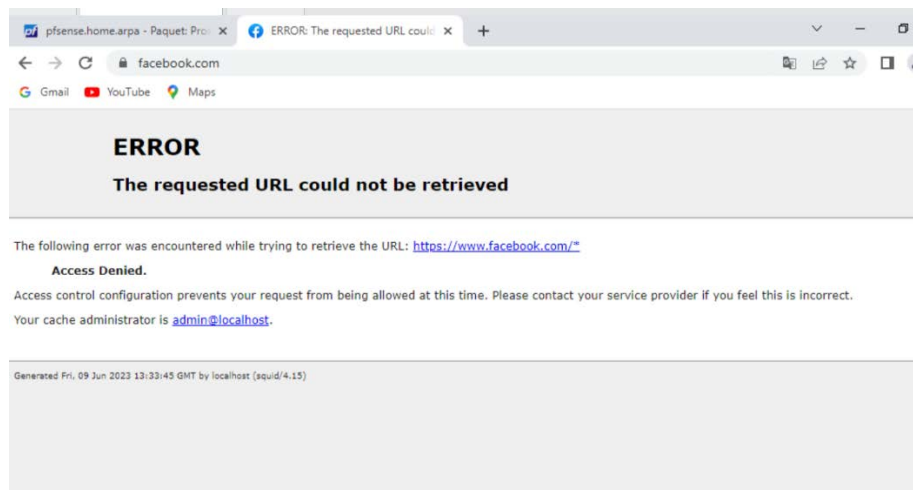


Figure 42 – Teste d’accéder à la page facebook.com

### 4.3.8. Configurer l’authentification en Squid

- **Authentification locale**

Dans la configuration de Squid sur l’onglet **Authentification**. Nous allons choisir la méthode d’authentification Local.

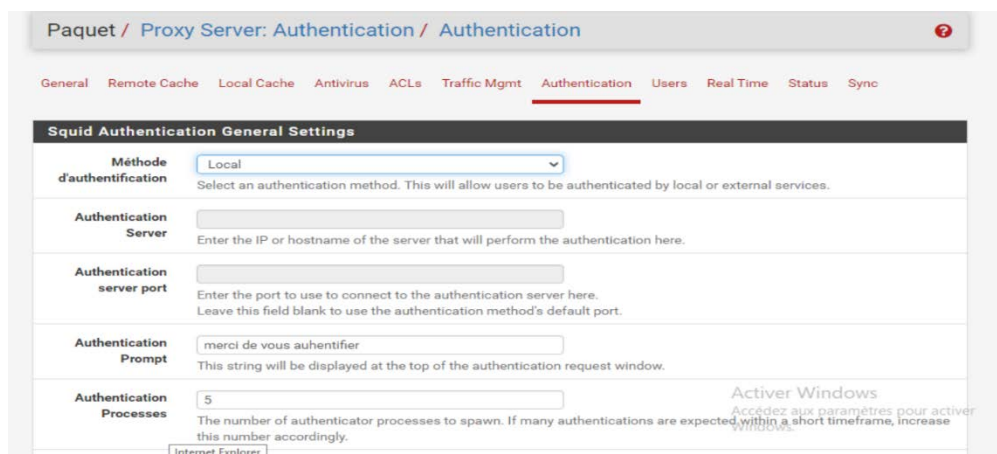


Figure 43 – Configuration de l’authentification.

- **Création des utilisateurs dans l'onglet Users**

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication **Users** Real Time Status Sync

**Squid Local Users**

**Nom d'utilisateur**   
Enter the username here.

**Mot de passe**   
Enter the password here.

**Description**   
You may enter a description here for your reference (not parsed).

Activer Windows  
Accédez aux paramètres pour active

*Figure 44 – Création des utilisateurs.*

- **Tester la connexion**

**Se connecter**

Le proxy http://192.168.1.254:3128 nécessite un nom d'utilisateur et un mot de passe.  
Votre connexion à ce site n'est pas privée

Nom d'utilisateur

Mot de passe

*Figure 45– Fenêtre d'authentification*

#### 4.3.9. Configurer la bande passante

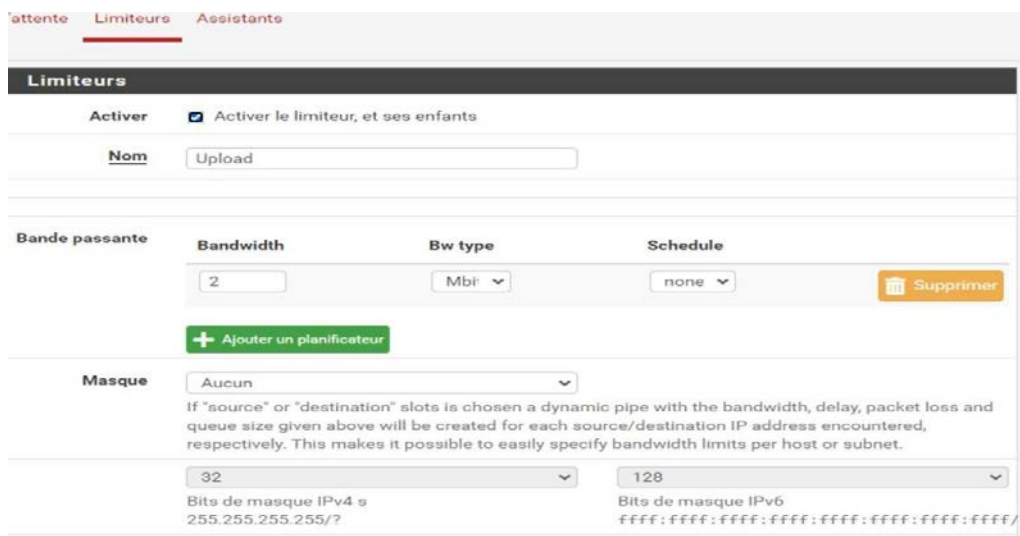
Nous Utilisons des limites pour contrôler la bande-passante par utilisateur.

- **Limitersroot (création de limiteur)**

Nous allons créer 2 **limitersroot** : un pour l'**Upload** et un pour le **Download**. La création s'effectue depuis le menu **Firewall >Traffic Shaper**.

Nous cliquons sur l'onglet **Limiters**, puis sur le bouton + **New Limiter**

- **Enable** : case à cocher pour activer le limiter root et ses queues
- **Name** : le nom de votre limiter root (caractères alphanumériques, tiret et Underscore uniquement). Dans notre cas, nous l'appellerons "Upload".
- **Bandwidth** : la bande-passante de votre limiter root. Il est à noter que l'on peut définir une bande-passante en fonction d'un calendrier (option "Schedule"). Dans notre cas, nous choisissons "2 Mbps".
- **Mask** : ce paramètre permet de définir comment la limitation va s'appliquer sur le trafic.
- Nous cliquons sur le bouton "**Save**" pour sauvegarder notre configuration.



*Figure 46 – Création de limiteur Upload.*

En bas de la page du Limiter que nous venons de créer, nous cliquons sur le bouton ”+ Add new Queue”

The screenshot shows the Mikrotik configuration interface for creating a queue limiter. The form is titled "Limiteurs" and contains the following fields and options:

- Activer:** A checkbox labeled "Activer cette file d'attente" which is checked.
- Nom:** A text input field containing "Lan\_upload".
- Masque:** A dropdown menu set to "Adresses Source". Below it is a note: "If 'source' or 'destination' slots is chosen a dynamic queue with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet, usually capped by the bandwidth of the parent limiter."
- Bits de masque IPv4 s:** A dropdown menu set to "32". Below it is the text "255.255.255.255/?".
- Bits de masque IPv6:** A dropdown menu set to "128". Below it is the text "ffff:ffff:ffff:ffff:ffff:ffff:ffff/".
- Description:** A text input field containing "queue par utilisateur". Below it is the text "Une description peut être saisie ici à des fins de référence administrative (non analysée)."

*Figure 47 – Création d’une queue pour Upload.*

Nos limiters (limiter root et queue) sont prêts pour le trafic sortant (Upload). Il nous reste à faire la même configuration pour le trafic entrant (Download).

- **Création du limiter pour le Download**

Nous allons faire la même configuration pour le trafic entrant (Download).

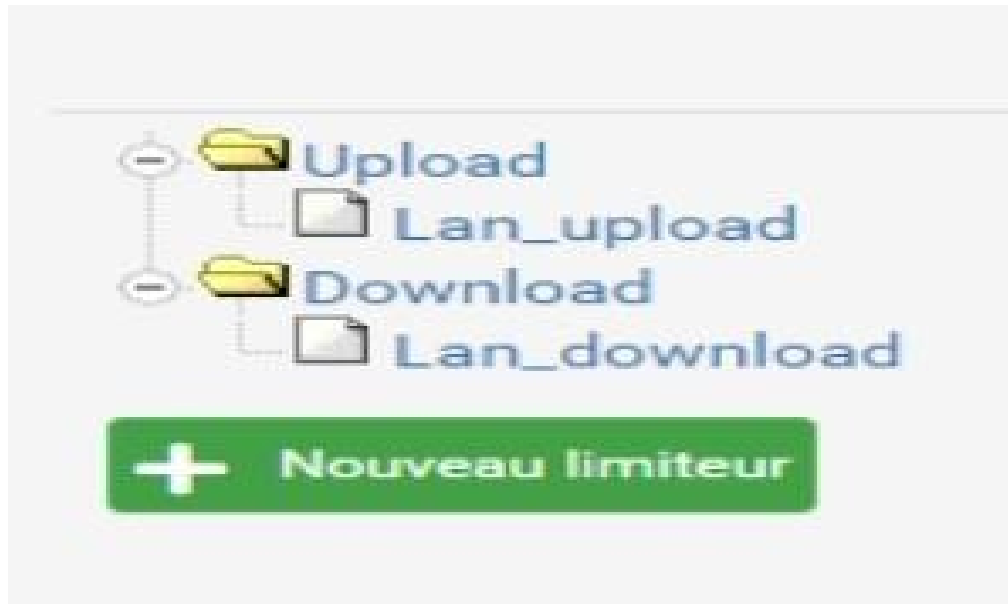
The screenshot shows the 'Limiteurs' configuration interface. At the top, there is a section for 'Activer' with a checked checkbox 'Activer le limiteur, et ses enfants'. Below this is a text input field for 'Nom' containing the value 'Download'. The main configuration area is titled 'Bande passante' and includes three sub-sections: 'Bandwidth' with a value of '20', 'Bw type' set to 'Mbit', and 'Schedule' set to 'none'. There is a 'Supprimer' button and a '+ Ajouter un planificateur' button. The 'Masque' section has a dropdown menu set to 'Aucun'. Below this is explanatory text: 'If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet.' There are two more dropdown menus for 'Masque' with values '32' and '128', corresponding to 'Bits de masque IPv4 s' (255.255.255.255/?) and 'Bits de masque IPv6' (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/). A 'Description' field is empty, with a note below it: 'Une description peut être saisie ici à des fins de référence administrative (non analysée).'

*Figure 48 – Création d'un limiteur Download*

The screenshot shows the 'Limiteurs' configuration interface for a queue. The 'Activer' section has a checked checkbox 'Activer cette file d'attente'. The 'Nom' field contains 'Lan\_download'. The 'Masque' dropdown is set to 'Adresse de destination'. Below this is explanatory text: 'If "source" or "destination" slots is chosen a dynamic queue with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet, usually capped by the bandwidth of the parent limiter.' There are two dropdown menus for 'Masque' with values '32' and '128', corresponding to 'Bits de masque IPv4 s' (255.255.255.255/?) and 'Bits de masque IPv6' (ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/). The 'Description' field contains 'queue par utilisateur', with a note below it: 'Une description peut être saisie ici à des fins de référence administrative (non analysée).'

*Figure 49 – Création d'une queue pour Download.*

• **Nos Limiters sont créés**

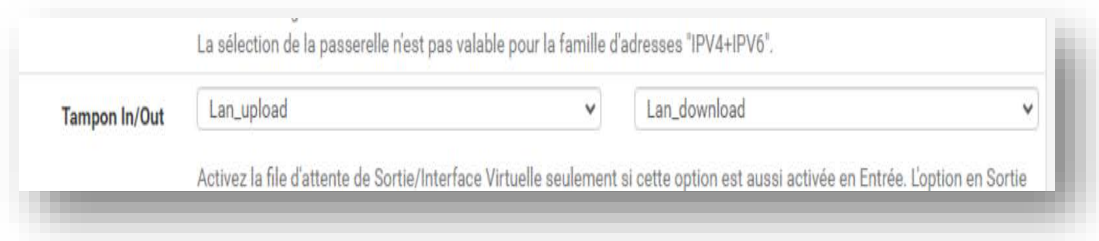


*Figure 50 – Les limiteurs créés.*

Il ne nous reste plus qu'à adapter nos règles de filtrage pour les mettre en application Cette configuration se fait depuis le menu **Firewall >Rules**.

Choisir l'onglet **LAN** et éditer les règles de filtrage :

En bas de page, pour l'option "In / Out ", choisir "**LAN Upload**" pour la première liste déroulante et "**LAN Download**" pour la seconde, Sur chaque règle :



*Figure 51 – Configuration des limiteurs dans les règles de pare-feu.*

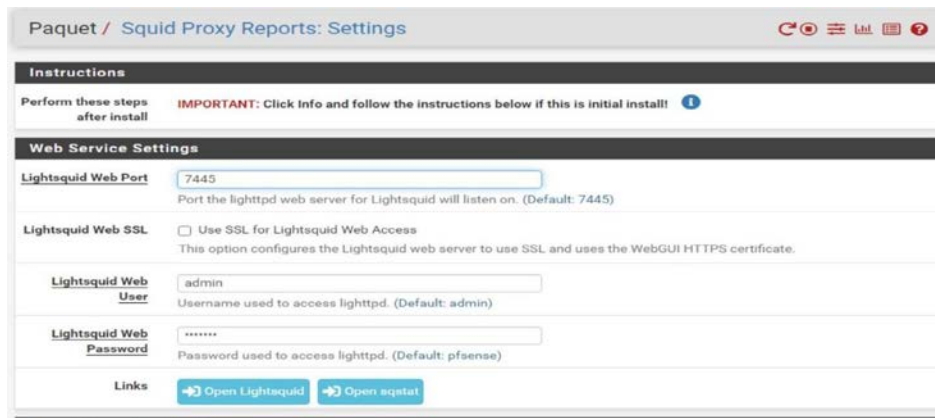
## 4.4. Rapports d'accès Web LightSquid

LightSquid est utilisé pour créer des rapports qui détaillent l'historique Web des ordinateurs qui ont accédé à des sites via le proxy.

Une fois le package LightSquid installé, les paramètres de rapport se trouvent sous Status>Squid Proxy Reports.

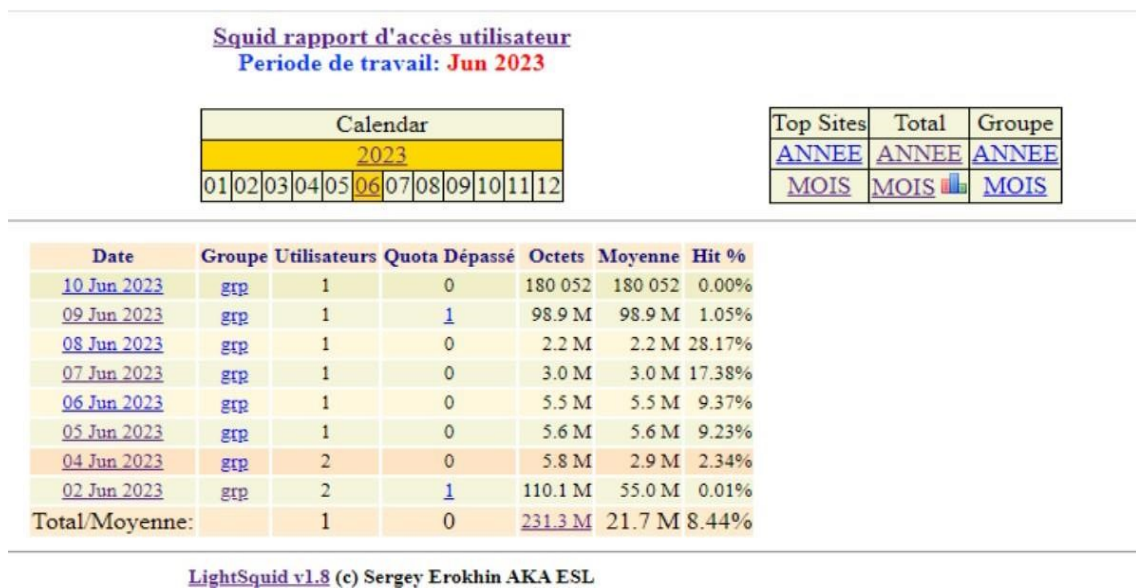


*Figure 52 – Paquet LightSquid.*



*Figure 53– Configuration du paquet LightSquid.*

- Ouvrir LightSquid pour afficher le rapport :



*Figure 54 – Rapport Squid.*

## 4.5. Conclusion

Dans ce chapitre réservé à la partie mise en place d'un proxy sécurisé avec l'authentification LDAP par pare-feu, nous avons commencé par la présentation des outils de la mise en place que nous avons utilisée. Nous avons présenté quelques interfaces pour montrer les résultats de notre travail.



## Conclusion générale

En conclusion, ce mémoire met en lumière l'importance croissante des réseaux informatiques dans notre vie quotidienne et professionnelle, ainsi que les menaces de sécurité auxquelles ils sont confrontés. Les réseaux informatiques jouent un rôle essentiel dans la communication, le partage de données et l'accès à Internet, mais ils demeurent vulnérables aux attaques malveillantes, telles que les attaques par déni de service, les virus et les logiciels malveillants.

Pour protéger efficacement ces réseaux contre de telles menaces, il est impératif de mettre en place des mesures de sécurité adéquates. Dans ce mémoire, nous avons examiné la mise en place d'un proxy sécurisé avec l'authentification LDAP comme moyen de renforcer la sécurité du réseau. Ce proxy permet de filtrer le trafic entrant et de bloquer les accès non autorisés, tandis que l'authentification LDAP garantit la sécurité des données en permettant l'identification des utilisateurs et la gestion des accès.

Au cours de cette étude, nous avons également exploré en détail les menaces de sécurité courantes auxquelles les réseaux informatiques sont exposés, ainsi que les mesures de sécurité recommandées pour les contrer.

La mise en place d'un proxy sécurisé avec l'authentification LDAP requiert des étapes précises et une compréhension approfondie des technologies et des protocoles impliqués. Ce mémoire a fourni une vue d'ensemble des étapes à suivre pour réaliser cette mise en place.

En résumé, ce mémoire a souligné l'importance cruciale de la sécurité des réseaux informatiques et a présenté une approche spécifique pour renforcer cette sécurité. La mise en place d'un proxy sécurisé avec l'authentification LDAP constitue une mesure efficace pour protéger les réseaux contre les menaces de sécurité.

En fin de compte, la sécurisation des réseaux informatiques représente un défi permanent qui nécessite une combinaison de technologies, de bonnes pratiques et de sensibilisation des utilisateurs. En adoptant des mesures de sécurité appropriées, nous pouvons améliorer la sécurité des réseaux informatiques et préserver la confidentialité, l'intégrité et la disponibilité des données.

# Bibliographie

- [1] <https://www.clusterboisson.com/.logo de Bejaia logistique>. Consulté le 18/06/2023.
- [2] TAGGUEB, A et IKKEN, Y. (2022). Conception et réalisation d'une application web pour la gestion des réservations des biens mobiles et immobiliers. Mémoire de fin de formation, Institut national spécialisé en formation professionnelle d'Akbou Centre de Formation Professionnel et de l'Apprentissage d'Akbou – LALA FATMA N'SOUMER. Consulté le 16/01/2023.
- [3] BERRI, Z. (2021). Refonte du réseau informatique du groupe IFRI. Mémoire de fin de formation, HIGHER INTERNATIONAL MANAGEMENT INSTIUT, Groupe INSIM. Consulté le 20/01/2023.
- [4] <https://developpementinformatique.com/definition-de-la-securite-informatique/>. Définition de la sécurité informatique. Consulté le 25/08/2023.
- [5] <https://wooxo.fr/Conseils-Cybersecurite/Principes-securite-informatique/>. Principes de la sécurité informatique. Consulté le 26/08/2023.
- [6] TOUHANT, F et FICHOUCHE, I. (2020). Mise en place d'un proxy sécurisé avec l'authentification LDAP. Mémoire de Master, Université SAAD DAHLAB DE BLIDA. <https://di.univ-blida.dz/xmlui/handle/123456789/13760/>
- [7] [https://www.memoireonline.com/12/09/3035/m\\_Audit-et-definition-de-la-politique-de-securite-du-reseau-informatique-de-la-fi4.html](https://www.memoireonline.com/12/09/3035/m_Audit-et-definition-de-la-politique-de-securite-du-reseau-informatique-de-la-fi4.html) /. Définition de la politique de sécurité du réseau informatique. Consulté le 02/07/2023.
- [8] <https://www.orange cyberdefense.com/fr/insights/blog/gestion-des-vulnerabilites/Vulnerabilites-de-quoi-parle-t-on/> /. Gestion des vulnérabilités. Consulté le 28/04/2023.
- [9] <https://nordvpn.com/fr/blog/ver-informatique/>. Verinformatique. Consulté le 25/05/2023.
- [10] Bloch et Wolfhugel, C. (2009). Sécurité informatique principes et méthode. EDITIONS : EYROLLES. Consulté le 25/09/2023.
- [11] Bay, J-ph et Pillou, J-F. (2016). Tout sur la sécurité informatique. Edition : Dunod. Consulté le 26/09/2023.
- [12] <https://www.techno-science.net/glossaire-definition/Attaque-de-l-homme-du-milieu.html> /. Définition de l'attaque de l'homme de milieu. Consulté le 02/08/2023.

- [13] <https://gplexpert.com/securite-informatique/mise-oeuvre-politique-securite-informatique-psi/>. Mise en œuvre d'une politique de sécurité informatique. Consulté le 06/07/2023.
- [14] <https://www.netexplorer.fr/blog/a-quoi-sert-antivirus-comment-utiliser/>. Définition d'un antivirus. Consulté le 15/08/2023.
- [15] <http://www.icour.fr/isn/fichiers/files/Les-methodes-de-protection.html/>. Les méthodes de protection. Consulté le 02/08/2023.
- [16] Ferrag, M-A. (2018). Sécurité informatique. Guelma. Récupéré de [http://www.researchgate.net/profile/Mohamed-Amine-Ferrag/publication/Securite\\_Informatique\\_-\\_Cours\\_et\\_TD/Securite-Informatique-Cours-et-TD.pdf](http://www.researchgate.net/profile/Mohamed-Amine-Ferrag/publication/Securite_Informatique_-_Cours_et_TD/Securite-Informatique-Cours-et-TD.pdf). Consulté le 02/08/2023.
- [17] [https://fr.wikipedia.org/wiki/Cryptographie\\_symetrique/](https://fr.wikipedia.org/wiki/Cryptographie_symetrique/). Cryptographie symétrique. Consulté le 13/05/2023.
- [18] [http://fr.wikipedia.org/wiki/cryptographie\\_asymetrique/](http://fr.wikipedia.org/wiki/cryptographie_asymetrique/). cryptographie asymétrique. Consulté le 10/04/2023.
- [19] <https://www.sekoia.io/fr/glossaire/firewall/>. Définition d'un pare-feu. Consulté le 15/05/2023.
- [20] <https://geekflare.com/fr/firewall-introduction/>. Le principe de fonctionnement d'un pare-feu. Consulté le 15/05/2023.
- [21] <https://nordvpn.com/fr/blog/serveur-proxy/>. Définition d'un Proxy. Consulté le 15/05/2023.
- [22] <https://fr.linkedin.com/pulse/le-serveur-harouna-moumouni-komoye>. Le principe de fonctionnement d'un serveur proxy. Consulté le 15/05/2023.
- [23] <https://fr.theastrologypage.com/digital-certificate>. Définition d'un certificat numérique. Consulté le 15/05/2023.
- [24] <https://s7deff5c7b202eed.jimcontent.com/download/version/158737764/mo2-543657/Name/protocole-securises.pdf/>. Définition du protocole SSL. Consulté le 20/05/2023.
- [25] <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203397-ldap-lightweight-directory-access-protocol-definition-traduction/>. Définition du protocole LDAP. Consulté le 20/05/2023.

- [26] Colombani,D .(2006).LDAP Maîtrise du protocole exploitation d'un service d'annuaire (Open LDAP, Active Directory). EDITIONS : ENI. Consulté le 28/09/2023.
- [27] <https://web.maths.unsw.edu.au/~lafaye/CCM/protect/firewall.html/>.Fonctionnement du par feu. Consulté le 15/09/2023.
- [28] <https://sebsauvage.net/comprendre/firewall/>. Fonctionnement d'un pare feu. Consulté le 15/09/2023.
- [29] <http://tvaira.free.fr/bts-sn/reseaux/cours/cours-reseaux-firewall.pdf> /. Les systèmes pare-feu(firewall). Consulté le 25/09/2023.
- [30] [https://igm.univmlv.fr/~dr/XPOSE2009/ldap/content/ldap\\_organization.html/](https://igm.univmlv.fr/~dr/XPOSE2009/ldap/content/ldap_organization.html/). Fonctionnement de LDAP. Consulté le 15/09/2023.
- [31] [https://igm.univ-mlv.fr/~dr/XPOSE2009/ldap/content/ldap\\_model.html](https://igm.univ-mlv.fr/~dr/XPOSE2009/ldap/content/ldap_model.html) /. Les modèles de protocole LDAP. Consulté le 15/09/2023.
- [32] <https://www.varonis.com/fr/blog/serveur-proxy/> . Fonctionnement d'un serveur proxy. Consulté le 15/09/2023.
- [33] <https://desgeeksetdeslettres.com/serveur-proxy-definition-fonctionnement/>. Définition et fonctionnement du serveur proxy. Consulté le 01/09/2023.
- [34] <https://jumpcloud.com/fr/blog/what-is-ldap-authentication/>. Processus d'authentification LDAP. Consulté le 01/09/2023.
- [35] <https://www.blogdumoderateur.com/tools/vmware-workstation-pro/>. Définition de VMware Workstation. Consulté le 12/08/2023 .

**Résumé** L'évolution technologique et la nécessité de protéger les données personnelles ont conduit à l'importance croissante des serveurs mandataires pour sécuriser le trafic sur Internet. Dans le cadre de notre étude, nous avons mis en place un serveur proxy squid sur la plateforme pfSense, en utilisant l'authentification LDAP.

Cette configuration nous a permis de bloquer sélectivement l'accès à Internet pour certains utilisateurs, ainsi que de filtrer les sites jugés dangereux ou inappropriés. En utilisant l'annuaire réseau LDAP, nous avons également mis en place un système d'authentification amélioré, offrant un meilleur contrôle et une gestion plus efficace des utilisateurs.

Cette expérience nous a permis de découvrir de nouveaux outils et systèmes pour améliorer les conditions de navigation sur Internet et renforcer la sécurité des réseaux. Nous avons ainsi acquis une expertise précieuse dans la configuration d'un proxy sécurisé avec l'authentification LDAP sur pfSense, offrant des avantages considérables en termes de contrôle et de gestion des utilisateurs.

**Mots-clés**— LDAP,PARE-FEU ,PROXY.

**Abstract** The technological evolution and the need to protect personal data have led to the increasing importance of proxy servers in securing Internet traffic. As part of our study, we have implemented a Squid proxy server on the pfSense platform, using LDAP authentication.

This configuration has allowed us to selectively block Internet access for certain users, as well as filter out websites deemed dangerous or inappropriate. By utilizing the LDAP directory service, we have also established an enhanced authentication system, providing better control and more efficient user management. This experience has enabled us to discover new tools and systems to enhance the browsing conditions on the Internet and strengthen network security. We have gained valuable expertise in configuring a secure proxy with LDAP authentication on pfSense, offering significant advantages in terms of user control and management

**Key-words**— LDAP,PARE-FEU ,PROXY