



République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediene

**Faculté d'Informatique
Département des Systèmes Informatiques**

Mémoire de Licence

Filière: Informatique

Spécialité: GTR

Thème

Étude et déploiement d'un firewall au sein d'une entreprise

Sujet Proposé par :
Mr. Bouchemla Chakib

Présenté par :
Sichaib Yasmine
Ali-khodja Myriam Erin Johanna Nefissa

Devant le jury composé de:

Présidente : Mme Bouziane Nabila
Membre : Mr Zeraoulia Khaled

Binôme n° : 10 / 2022

Remerciements

Au moment où s'achève la réalisation de notre projet et la rédaction de ce mémoire, nous remercions notre promoteur au sein de la société Algérie Télécom Monsieur Bouchemla Chakib pour avoir accepté de nous encadrer. Nous tenons à témoigner notre gratitude à Mme. Bouziane Nabila de nous avoir apporter son aide, sa patience et ses remarques constructives, qui ont été déterminants dans la réalisation de ce travail, ainsi que sa supervision et ses conseils qui nous ont permis de prendre les bonnes décisions malgré tous les obstacles rencontrés. Sans oublier tous les professeurs du département informatique et de l'USTHB qui ont contribué grandement à notre formation.

Nous sommes également reconnaissantes aux membres du jury pour l'intérêt qu'ils ont porté à notre humble travail en acceptant de l'examiner et de l'enrichir par leurs propositions.

Et sans oublier bien sûr, un grand merci à nos familles et nos amis ayant contribués, de près ou de loin au bon déroulement de ce projet, on vous remercie pour le soutien inconditionnel dont vous avez fait preuve. Votre présence et vos encouragements furent sans aucun doute, notre plus grande source de motivation.

Table des matières

Table des figures	v
Liste des tableaux	vii
Introduction générale	1
1 Généralités sur la cybersécurité	3
1.1 Introduction	3
1.2 Définition de la cybersécurité	3
1.3 La triade CID	3
1.3.1 La confidentialité	3
1.3.2 L'intégrité	4
1.3.3 La disponibilité	4
1.4 Définition d'une cyberattaque	4
1.4.1 Les différents types de virus	4
1.4.2 Les différents types d'attaque	5
1.4.3 Les étapes de la chaîne d'attaque (cyberkillchain)	6
1.5 Les enjeux de la cybersécurité	6
1.6 Politiques de sécurité d'une entreprise	7
1.6.1 Les équipements à implémenter	7
1.6.2 La sauvegarde des données	7
1.6.3 L'authentification, l'autorisation et la gestion des comptes	8
1.6.4 Mise à niveau, mise à jour et correctif	8
1.6.5 Test d'intrusion (Pentesting)	8
1.7 Conclusion	8
2 Notions théoriques sur les réseaux et la cybersécurité	9
2.1 Introduction	9
2.2 Les réseaux locaux virtuels (VLAN)	9
2.2.1 Définition	9
2.2.2 Les types de VLAN	10
2.2.3 Types de configuration des ports switch	10
2.2.4 Routage inter-VLAN	10
2.3 Les listes de contrôles d'accès (ACL)	10
2.3.1 Définition d'une ACL	10
2.3.2 Principe de fonctionnement des ACL	11
2.3.3 Les types d'ACL	11
2.4 Le pare-feu	11
2.4.1 Fonctionnement d'un pare-feu	11

2.4.2	Les différents types de pare-feu	12
2.5	La zone démilitarisée (DMZ)	13
2.6	Le NAT	13
2.7	Les VPN	14
2.8	Étude comparative des solutions de sécurité basées sur un pare-feu	14
2.9	Comparaison des différentes solutions pare-feu	16
2.9.1	Pfsense [46]	16
2.9.2	IPFire [47]	16
2.9.3	Cisco Firepower [48]	16
2.9.4	FortiGate NGFW [49]	17
2.9.5	OPNsense [50]	17
2.10	Tableau comparatif des caractéristiques des pare-feux	17
2.11	Conclusion	18
3	Conception et implémentation de la solution	19
3.1	Introduction	19
3.2	Spécifications des besoins réseaux et sécurité	19
3.3	Conception du réseau et de la sécurité de l'entreprise	19
3.3.1	Plan d'adressage et segmentation du réseau de la direction régionale	20
3.3.2	Définition des politiques de sécurité	20
3.4	Outils d'étude	21
3.4.1	Simulateurs Réseaux et sécurité	21
3.4.2	Logiciels de virtualisation et plateforme cloud	21
3.4.3	Pare-feu	21
3.4.4	Les ressources utilisées	22
3.4.5	Les équipements utilisés	22
3.5	Chronologie de la réalisation du projet	22
3.6	Implémentation du pare-feu	23
3.6.1	Configurations des adresses IP sur le pare-feu	23
3.6.2	Configuration de la passerelle	24
3.6.3	Installation de Odoo	25
3.6.4	Configuration du DHCP sur OPNsense	26
3.6.5	Création des VLAN	27
3.6.6	Configuration du port forwarding	27
3.6.7	Configuration du VPN	29
3.7	Ajout du module NGFW Zenarmor	31
3.8	Conclusion	33
Conclusion générale	34	
Annexes	35	
A	Architecture du réseau sur Packet Tracer	35
A.1	Création des VLAN et configuration du DHCP	36
A.2	Création des ACL	43

B Présentation de l'organisme d'accueil	45
B.1 Présentation d'Algérie Télécom	45
B.2 Missions et objectifs de l'entreprise	45
B.3 Présentation de la structure d'accueil	46
B.4 Organigramme général de l'entreprise	47
B.5 Organigramme de la division des systèmes d'information	48
B.6 Situation Actuelle	48
B.7 Notre Solution	48
Références	50

Table des figures

2.1	Organigramme de l'algorithme de fonctionnement des ACL	11
2.2	Représentation d'un réseau utilisant un tunnel VPN	14
3.1	Conception et planification de la mise en place du réseau.	20
3.2	Configuration des adaptateurs réseaux d'OPNsense.	23
3.3	Allocation de l'adresse IP pour l'interface LAN de OPNsense.	24
3.4	Interface graphique d'OPNsense aperçue grâce à l'adresse LAN.	24
3.5	Configuration de la passerelle du WAN.	24
3.6	Confirmation de l'accès à internet grâce à la passerelle.	25
3.7	Installation et vérification de l'adresse IP de OODOO.	25
3.8	Interface graphique de Odoo.	26
3.9	Configuration du DHCP sur OPNsense.(1)	26
3.10	Configuration du DHCP sur OPNsense.(2)	26
3.11	Création du VLAN et configuration de son interface.	27
3.12	Configuration du DHCP pour la DMZ.	27
3.13	Assignation d'un port spécifique à l'interface WAN du pare-feu.	28
3.14	Confirmation de la redirection de l'interface WAN de l'accès du pare-feu vers le port 9999.	28
3.15	Confirmation de la redirection de l'interface LAN de l'accès du pare-feu vers le port 2828.	29
3.16	Création de l'autorité de certification interne à OPNsense.	29
3.17	Autorisation du trafic VPN sur le WAN.	30
3.18	Configuration de OpenVPN.	30
3.19	Création de l'autorité de certification interne à OPNsense.	31
3.20	Ajout du module Zenarmor sur OPNsense.	32
3.21	Ajout du module Zenarmor sur OPNsense.	32
A.1	Architecture de la direction régionale.	36
A.2	Création des VLAN depuis le Switch niveau 3.	36
A.3	Allocation d'une adresse IP statique au serveur DHCP.	37
A.4	Ajout de la plage d'adresse pour le vlan 2 RH.	37
A.5	Ajout de toutes les plages associées aux VLAN.	38
A.6	Activation du mode trunk depuis le Switch niveau 3.	38
A.7	Création des VLAN sur le Switch niveau 2.	39
A.8	Association des interfaces à leurs VLAN.	40
A.9	Liste des VLAN associés à leurs interfaces.	40
A.10	Configuration de l'adresse d'assistance pour chaque VLAN.	41
A.11	Configuration du routage entre les différents VLAN depuis le Switch niveau 3.	41
A.12	Activation du DHCP sur le PC1 VLAN 6 du département sécurité.	41

A.13 Ping du PC Juridique vers PC1 Sécurité.	42
A.14 Ping du PC juridique vers le serveur DHCP avant l'ACL.	43
A.15 ACL étendue pour le VLAN 4 représentant le département juridique.	43
A.16 Liste des ACL étendues.	44
A.17 Ping du PC juridique vers le serveur DHCP après l'ACL.	44
B.1 Organigramme d'Algérie Télécom.	47
B.2 Organigramme de la division des systèmes d'information.	48

Liste des tableaux

2.1	Tableau comparatif des caractéristiques des pare-feux	18
3.1	Plan d'adressage IP et VLAN de la direction régionale de M'Sila.	20
A.1	Association des VLAN à des ports spécifiques	39
A.2	Règles des ACL appliquées aux VLAN.	43

Liste des symboles

ACL Access Control List

DDoS Distributed Denial of Service

DHCP Dynamic Host Configuration Protocol

DMZ Demilitarized Zone

DoS Denial of Service

ERP Enterprise Ressource Planning

FTP File Transfer Protocol

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IDS Intrusion Detection System

IP Internet Protocol

IPS Intrusion Prevention Systems

ISO International Organization for Standardization

LAN Local Area Network

MAC Media Access Control

NAT – T Network Address Translation Traversal

NAT Network Address Translation

NGFW Next Generation Firewall

NGIPS Next Generation Intrusion Prevention System

OSI Open Systems Interconnection

PAT Port Address Translation

PC Personal Computer

QoS Quality of Service

RDP Remote Desktop Protocol

SGBD Système de gestion de base de données

SLA Service Level Agreement

SSH Secure Shell

SSL Secure Socket Layer

SVI Switch Virtual Interface

TCP Transmission Control Protocol

UDP User Datagram Protocol

VLAN Virtual Local Area Network

VM Virtual Machine

VoIP Voice Over Internet Protocol

VPN Virtual Private Network

WAN Wide Area Network

WIFI Wireless Fidelity

Introduction générale

Mise en contexte

La sécurité à travers le temps a toujours occupé une place importante dans les entreprises. Les attaques qui autrefois étaient physiques, sont devenues aujourd’hui numériques, et ce depuis l’apparition et l’expansion d’internet. Le monde connecté quelque soit ses avantages, comprend d’importants risques, qui peuvent se traduire par des pertes financières, des perturbations des opérations, des chaînes d’approvisionnement, et peut également atteindre la réputation des clients et des investisseurs touchés.

La réponse à ces nombreuses attaques a été le développement d’équipements physiques ou logiques capables de répondre aux menaces, de les contourner, voire même de les prédire depuis quelques temps. Parmi les équipements de défense les plus connus, le pare-feu.

Problématique posée

Algérie Télécom est une société par actions à capitaux publics opérant sur le marché des réseaux et services de communications électroniques. Elle est présente sur tout le territoire national, la sécurité de ces clients, nous citoyens, en devient un devoir et une obligation. De ce fait, lorsqu’une nouvelle infrastructure voit le jour, elle représente un point d’entrée et une faiblesse pour l’entreprise. Une mise en place rapide des mesures de sécurité informatique doivent être implémentées. Quelles sont donc toutes les procédures techniques par lesquelles un ingénieur en sécurité réseau passe afin de sécuriser efficacement le réseau de l’entreprise lorsque celle-ci ouvre une nouvelle direction régionale ?

Objectif du projet

Notre projet vise à l’élaboration d’une solution basée sur un pare-feu, afin de sécuriser une nouvelle infrastructure ouverte au niveau de la wilaya de M’sila. Il est divisé en deux principaux axes : La spécification des besoins réseaux et sécurité émis par Algérie Télécom et leur traduction. La conception et l’implémentation des équipements nécessaires à la sécurisation de la direction régionale.

Plan de travail

Nous nous sommes organisés comme suit afin de répondre à la problématique posée :

1- État de l’art

Les deux premiers chapitres de notre mémoire représentent l’acquisition et la recherche des concepts et aspects qui nous étaient inconnus. Ils nous ont permis de nous approfondir, de découvrir certaines technologies et de concevoir un plan de travail efficace.

2- Étude comparative des solutions

Notre chapitre 3 est consacré à l'étude des différentes solutions qui s'offrent à nous. Ce dernier nous a permis de découvrir les différents équipements de sécurité présents sur le marché, de les différencier et d'évaluer leurs caractéristiques selon nos besoins et nos moyens.

3- Conception et implémentation

Le dernier chapitre de notre rapport regroupe toutes les attentes exprimées par l'entreprise. Nous avons regroupé les différentes spécifications et les avons traduites afin de concevoir une architecture sécurisée. Une fois celle-ci mise en place, nous avons pu passer à la réalisation de notre projet en implémentant notre solution dans un environnement domestique.

Chapitre 1

Généralités sur la cybersécurité

1.1 Introduction

En raison du progrès rapide des technologies et objets connectés, une entreprise peut désormais vérifier l'état d'avancement de n'importe quel projet en cours dans le monde, voire même consulter l'activité de ses employés. La technologie, formidable invention est elle aussi exposée à des risques et des menaces. Plus elle se développe, plus les acteurs malveillants et les risques augmentent. Dans ce chapitre, nous analysons les concepts de base de la cybersécurité, les différentes menaces auxquelles sont exposées les réseaux informatiques, et pour finir sur les enjeux de la cybersécurité dans notre société actuelle et les principaux moyens de se défendre.

1.2 Définition de la cybersécurité

La cybersécurité consiste à protéger les systèmes, les réseaux et les programmes contre les attaques numériques. À la différence de la sécurité, qui elle se concentre spécifiquement sur la protection du contenu et des données numériques comme les vidéos et les feuilles de calcul [?][1].

1.3 La triade CID

La triade CID (Confidentialité, Intégrité, Disponibilité) est l'essence même de la sécurité de l'information. C'est un modèle de sécurité composé de trois principes indispensables à la protection de l'information : confidentialité, intégrité et disponibilité. Les entreprises la sollicitent dans le but de mettre en place des contrôles et des politiques de sécurité efficaces [2].

Cela leur permet d'acquérir des moyens de défense contre les multiples menaces comme le vol d'informations, la perte et la manipulation de données induites par exemple par l'envoi d'un virus qui reformate le disque dur d'un ordinateur, l'usurpation d'identité, ou encore l'interruption de services [3].

1.3.1 La confidentialité

Garantit que seuls les utilisateurs disposant des autorisations requises peuvent accéder ou utiliser les informations et qu'elles ne soient pas détournées [4]. Comme par exemple Log4Shell, une bibliothèque utilisée par le langage de programmation Java, baptisée « Log4j » elle peut être détournée pour faire fonctionner du code non autorisé sur un serveur [5].

1.3.2 L'intégrité

Assure que les données ne soient pas altérées de manière non autorisée durant leur transmission. Par exemple, un ransomware peut chiffrer les données d'un disque dur sans pour autant les divulguer [6].

1.3.3 La disponibilité

Représente le fait qu'un service, une application ou un réseau soit toujours disponible pour les utilisateurs autorisés en tout temps afin de garantir le bon fonctionnement du système d'information. Un exemple concret qui touche à la disponibilité du système sont les attaques DoS (Attaque par déni de service) ou DDoS (Attaque par Déni de service distribués).

1.4 Définition d'une cyberattaque

Une cyberattaque est un acte offensif qui cible les Systèmes d'Information (SI) ou les entreprises dépendantes de technologies et de réseaux afin de voler, modifier ou détruire un système sensible [7].

1.4.1 Les différents types de virus

Voici une liste des différents types de virus les plus connus actuellement :

- Virus (Virus) : Est un code exécutable malveillant attaché à un autre programme, il doit être exécuté par l'utilisateur pour être activé. Ils se diffusent via des supports amovibles, téléchargements effectués sur Internet et pièces jointes dans un e-mail. Lorsqu'il contient une charge utile, il peut après une certaine période, effacer tout élément enregistré sur le disque dur [8].
- Vers (Worms) : Les vers informatiques reproduisent des copies fonctionnelles d'eux-mêmes et peuvent engendrer le même type de dommages que les virus. Ce sont des logiciels autonomes et ne requièrent pas de programme d'accueil ou d'intervention humaine pour se propager, ils utilisent les fonctionnalités du système pour voyager sans assistance à travers le réseau [9].
- Rançongiciel (Ransomware) : Bloque l'accès à un système informatique, ou les données qu'il héberge en les chiffrant à l'aide d'une clé inconnue de l'utilisateur. Ce dernier doit alors verser une rançon aux criminels pour obtenir à nouveau l'accès [10].
- Cheval de Troie (Trojan Horse) : Est un programme d'apparence légitime, mais qui contient un logiciel malveillant installé par l'utilisateur lui-même, ignorant cela, il permet aux pirates de contrôler les ordinateurs à distance et de perturber son fonctionnement à l'aide de portes dérobées [11].
- Logiciel espion (Spyware) : est un type particulier de malware qui se dissimule et enregistre secrètement des informations et suit des activités en ligne sur des appareils électroniques. Il peut surveiller et copier tout ce qui est saisi, chargé, téléchargé et stocké. Dans certains cas, il peut en outre activer les caméras et les micros sans être détecté [12].
- Virus polymorphes : Les virus polymorphes s'exécutent tous de la même façon, ils font partie de la famille des malware, l'une de leur particularité est d'avoir trouvés des mécanismes afin d'échapper aux logiciels anti-virus, et à l'analyse classique basée sur les signatures en modifiant

le contenu de leurs fichiers [13].

— Logiciels publicitaires (Adware) : Il est conçu pour afficher des publicités dans un navigateur web. En général, il est apte à collecter des informations sur les habitudes de l'internaute qui servent soit à afficher des réclames correspondant aux centres d'intérêt de celui-ci, soit à alimenter des bases de données commerciales. Bien que n'étant pas dangereux pour l'ordinateur, il est considéré comme un logiciel malveillant [14].

— Rootkits : Un rootkit est un malware élaboré afin d'infecter un PC, non détecté par les logiciels anti-virus et autres outils de sécurité et permet au pirate d'installer une série d'outils qui lui offre la possibilité d'accéder à distance à un ordinateur tels qu'un programme de capture de mots de passe, un module pour voler les informations de cartes et de comptes bancaires en ligne, un robot afin de mener des attaques DDoS ou possédant des fonctionnalités capables de désactiver les logiciels de sécurité [15].

1.4.2 Les différents types d'attaque

Une cyberattaque peut engendrer des coûts importants pour les entreprises. Parmi les attaques les plus répandues, on peut citer les suivantes :

— DoS : Les attaques DoS empêchent l'utilisation d'un service par les personnes autorisées en épuisant les ressources du système. Elles sont un risque majeur car elles interrompent la disponibilité, facteur important de la triade CID et provoquent une perte de temps et d'argent importante [16].

— DDoS : Un DDoS est similaire à une attaque DoS, mais il provient de sources multiples et coordonnées [16].

— L'homme du milieu (MitM : Man in the middle) : L'homme du milieu est une attaque dans laquelle deux parties qui croient communiquer directement l'une avec l'autre voient leur communication interceptée et relayée secrètement. L'attaque est une forme d'écoute clandestine dans laquelle l'attaquant lit et modifie les communications en temps réel [17].

— Hameçonnage (Phishing) : Les campagnes de Phishing ne visent pas une personne en particulier, mais des centaines, voire des milliers de destinataires. Le cybercriminel envoie un mail et se fait passer pour un organisme connu (banque, service des impôts), en utilisant le logo et le nom de cet organisme en demandant de "mettre à jour" ou de "confirmer des informations suite à un incident technique" [18].

— Harponnage (Spear Phishing) : Contrairement au hameçonnage classique, le spear phishing est une attaque très ciblée, qui ne vise qu'une seule personne. Les hackers se font passer pour un individu que vous connaissez [19].

— Téléchargement furtif (Drive-by download) : Ces malwares sont traditionnellement transmis au travers des vulnérabilités des navigateurs web ou des mauvais paramétrages de sécurité de l'ordinateur. Concrètement, il s'agit d'un programme frauduleux qui s'installe discrètement sur un ordinateur et il est téléchargé sans le consentement ou la connaissance de l'utilisateur : ce dernier n'a même pas à cliquer sur un lien corrompu pour être infecté, il est automatique [20].

- Injection SQL (Structured Query Language) : est un langage qui nous permet d’interagir avec des bases de données : L’injection SQL, est une forme de cyberattaque sur une application web dans laquelle le pirate injecte des requêtes SQL malveillantes pour manipuler la base de données [21].
- Script inter-sites (XSS : Cross-site scripting) : Un script malveillant est envoyé à un serveur Web via le chargement d’une adresse URL manipulée par exemple. Ce serveur Web retourne par la suite ce script au client sans vérification, le code malveillant n’est pas enregistré sur le serveur et existe seulement de manière temporaire lors du chargement de la page Web via le client. Il pourra par la suite récupérer des données qui lui serviront à se faire passer pour un utilisateur authentifié ou introduire un code malveillant que le navigateur exécutera ensuite [22].

1.4.3 Les étapes de la chaîne d’attaque (cyberkillchain)

La chaîne d’attaque décrit les phases qu’un cyber attaquant effectue avant de lancer une quelconque attaque, de la reconnaissance à l’exfiltration de données. Ce modèle peut aussi être utilisé comme outil de gestion, afin d’améliorer en permanence la défense du réseau [23].

— Reconnaissance : La mission de recueil d’informations est la phase préliminaire d’une cyberattaque. Pendant la reconnaissance, le cybercriminel recherche les indices susceptibles de révéler les vulnérabilités et les points faibles du système. Les pare-feux, les périmètres de sécurité, les dispositifs de prévention des intrusions et même les réseaux sociaux suscitent l’intérêt et sont donc examinés.

— Intrusion : Après avoir obtenu les renseignements, le hacker tente de s’infiltre. L’intrusion représente le moment où la charge utile est livrée afin de créer un point d’entrée. Les malwares peuvent être envoyés vers le système pour forcer l’entrée, s’il réussit l’intrusion il y aura une exploitation.

— Exploitation : Le hacker tire profit des failles du système, il peut désormais entrer dans le système, installer des outils supplémentaires, modifier les certificats de sécurité et créer de nouveaux scripts à des fins nuisibles.

— Escalade de priviléges : Les cybercriminels exploitent l’escalade de priviléges pour obtenir des autorisations élevées d’accès aux ressources. Ils modifient les paramètres de sécurité des objets de stratégie de groupe, les permissions, les fichiers de configuration et essaient d’en tirer profit afin de récolter des informations d’identification.

— Mouvement latéral : Afin d’acquérir d’autres accès, et d’obtenir plus de ressources, les cyberattaquants se déplacent de système en système, de manière latérale et recherchent des informations sensibles, des accès administrateur, des données critiques et des serveurs de messagerie. Ils se positionnent de manière à causer le plus de dégâts possibles et peuvent par exemple s’attaquer à l’ADDS (Active Directory Domain Services) ou au DNS (système de noms de domaine, Domain Name System) [24].

1.5 Les enjeux de la cybersécurité

Il appert que la cybersécurité représente ces dernières années avec la COVID-19 et la politique du BYOD - Bring your own device - une obligation et une nécessité pour toutes les entreprises voulant assurer une forte sécurité de l’information, des données et des appareils. Ces avantages sont multiples et peuvent se présenter comme suit :

- Dans les rares cas où la sécurité n'empêche pas une attaque ou une violation d'avoir lieu, elle réduit la surface des dégâts et implique un temps inférieur pour la restauration des systèmes/données [25].
- Permet la vérification redondante du réseau, afin de tester, d'analyser quotidiennement l'efficacité et de hiérarchiser ces faiblesses pour améliorer sa défense [26].
- Protège la réputation de l'entreprise car les dommages causés par une cyberattaque peuvent être difficile à réparer et rompre la confiance qu'accorde les clients à l'entreprise de cybersécurité. Avec une mise en place robuste nous protégeons à la fois l'entreprise, les clients mais aussi la crédibilité et la réputation de l'entreprise [26].

1.6 Politiques de sécurité d'une entreprise

Pour atténuer les attaques sur le réseau, il faut tout d'abord sécuriser les équipements (les routeurs, les commutateurs, les serveurs et surtout les hôtes, principal point d'entrée des cyberattaques). La plupart des organisations utilisent une approche de défense en profondeur (également connue comme étant l'approche par couches, ou en anglais multilayer) de la sécurité. Pour cela, divers appareils réseau et services doivent fonctionner en même temps.

1.6.1 Les équipements à implémenter

- VPN - Réseau privé virtuel - : est un support d'accès à distance qui crée un tunnel crypté sécurisé permettant de lier les utilisateurs afin d'accéder aux ressources de l'entreprise.
- Pare-feu : Équipement physique ou virtuel (logiciel) de protection du réseau permettant de surveiller le trafic et s'appuie sur une certaine politique de sécurité afin d'autoriser ou de bloquer ce trafic.
- IPS système de prévention des intrusions : permet de détecter et prévenir des menaces identifiées en surveillant le trafic entrant et sortant à la recherche de logiciels ou actes malveillants, de signatures d'attaques réseau. Si une menace est détectée, il peut sur-le-champ l'arrêter.
- IDS Système de détection des intrusions : Outils permettant d'analyser et de surveiller le trafic réseau périodiquement afin de vérifier l'intégrité des systèmes. Il s'appuie sur une base de données de règles ou de signatures d'attaques, en cas de correspondance, une alerte sera envoyée à un administrateur réseau.
- Serveur AAA Authentification Autorisation Traçabilité : contient une base de données sécurisée avec une liste des personnes autorisées à accéder et à gérer les périphériques du réseau. Grâce à cette base de données, les périphériques réseau sont aptes à authentifier les utilisateurs administratifs [27].

1.6.2 La sauvegarde des données

Est l'une des méthodes de protection les plus efficaces contre la perte des données, elle doit être effectuée régulièrement conformément à la politique de sécurité sur un disque amovible conservé en lieu sûr hors site et protégé à l'aide de mots de passe forts .

1.6.3 L'authentification, l'autorisation et la gestion des comptes

Tous les périphériques se doivent d'être administrés ou configurés de manière à ne fournir l'accès qu'aux personnes autorisées, de définir quelles sont les actions qu'elles effectuent lors de l'accès au réseau, et d'enregistrer ce qui a été fait pendant son séjour.

1.6.4 Mise à niveau, mise à jour et correctif

S'informer en continu sur les dernières attaques est obligatoire de nos jours ainsi, les entreprises doivent acquérir la version la plus récente de leur logiciel antivirus. La façon la plus adéquate de prévenir des risques est de :

- Télécharger les mises à jour de sécurité du fournisseur du système d'exploitation.
- Appliquer des correctifs sur tous les systèmes vulnérables.
- S'assurer que tous les terminaux prévoient les mises à jour de manière automatique [28].

1.6.5 Test d'intrusion (Pentesting)

Le test d'intrusion ou “pentesting” est une méthode de piratage éthique qui évalue la vulnérabilité d'un système informatique, d'une application ou d'un site web en détectant les failles susceptibles d'être exploitées par un hacker ou un logiciel malveillant. Ce test consiste à simuler et lancer des cyberattaques, notamment le fait d'essayer de cracker les mots de passe, vérifier la sensibilité des employés au phishing et bien d'autres encore. À la fin le pentester fournit un rapport à l'entreprise qui s'appuie sur des référentiels prévus pour ce genre d'activité (audit sécurité) expliquant quelles sont les vulnérabilités du système et comment il a pu les exploiter [29].

1.7 Conclusion

Il est important en cybersécurité de cerner les enjeux, et les responsabilités conséquentes que porte un ingénieur sur ces épaules. Il est également important de définir les différents aspects qui la régissent, et de se familiariser avec les attentes de ce secteur. Ce chapitre nous a permis de répertorier de manière claire et concise les attentes qu'ont les entreprises concernant la protection de leur système d'information.

Chapitre 2

Notions théoriques sur les réseaux et la cybersécurité

2.1 Introduction

Les réseaux commençant à grandir et le développement technologique devenant plus important, il est devenu primordial de contrôler le flux de trafic réseau. Une fuite et/ou une perte d'informations et/ou de données induiraient des conséquences non négligeables notamment monétaire. Ce besoin s'est traduit par la mise en place de différentes méthodes, techniques et protocoles afin de permettre l'optimisation du transfert d'informations et sa sécurité. Étudier ces principes permet alors leurs utilisations dans les scénarios adéquats.

2.2 Les réseaux locaux virtuels (VLAN)

Les réseaux locaux virtuels sont très présents dans les entreprises en raison de leurs nombreux avantages. Dans cette partie, une présentation de la technologie VLAN est abordée couplé aux types de configuration des ports switch et leurs routages.

2.2.1 Définition

Les réseaux locaux virtuels communément appelés VLAN créent plusieurs domaines logiques et indépendants de diffusion sur un commutateur ou un réseau physique. Les VLAN permettent un large éventail d'avantages tels que [30] :

- Réduire la taille des domaines de diffusion : l'utilisation de routeur pour la segmentation induisent à la création de nouveaux segments de réseaux distincts, et donc à d'autres domaines de diffusion. Les VLAN induisent à la segmentation du réseau sans nécessiter l'utilisation de routeurs ou d'équipements spécifiques, elle s'appuie sur les commutateurs de niveau 2 ou 3 afin d'acheminer l'information.
- La segmentation du trafic permet d'augmenter la sécurité en diminuant l'accès aux données sensibles par des utilisateurs non privilégiés.
- Réduire les coûts grâce à l'utilisation plus efficace de la bande passante en séparant les flux.
- Faciliter l'administration et la gestion notamment de la QoS, et du routage en regroupant les utilisateurs ayant des besoins réseau similaires dans un même VLAN par exemple : Services VoIP, et autres.

2.2.2 Les types de VLAN

Il existe différents types de VLAN classés selon le type de trafic ou selon le type de fonction qu'ils occupent. Il est possible de les citer comme suit [31] :

- VLAN par défaut : Il est affecté aux ports et aux trames, lorsqu'aucune configuration préalable n'est définie, par défaut sur les équipements CISCO il s'agit du VLAN 1.
- VLAN de données : Gère le trafic utilisateur, ce dernier permet de séparer un réseau en groupe d'utilisateurs ou de périphériques.
- VLAN natif : Par défaut il s'agit du VLAN 1, s'occupe de la transmission du trafic associé à plusieurs VLAN et permet d'affecter un trafic non étiqueté sur un port trunk 802.1Q.
- VLAN management : Est utilisé dans un but de gestion des fonctionnalités d'un commutateur, on attribue à ce type de VLAN une interface virtuelle de routage nommée SVI, qui connecte un VLAN à un équipement de couche 3. Les périphériques qui ne sont pas sur le même VLAN ne peuvent communiquer entre eux sans une certaine technique de routage, ceci entraîne donc à implémenter le concept de routage inter-VLAN. La SVI permet donc d'acheminer le trafic entre deux équipements de couche 3 sans pour autant utiliser un routeur. Les avantages de cette dernière sont : le routage entre VLAN, et une administration à distance via Telnet ou SSH.

2.2.3 Types de configuration des ports switch

Un administrateur réseau configure les ports un à un, notamment ces deux modes :

- Mode Access : Brancher un équipement à un port mode Access, lui permet de communiquer avec d'autres périphériques appartenant au même VLAN.
- Mode Trunk : À la différence du mode Access, la configuration du mode Trunk sur une interface permet la réception et l'envoi de trames appartenant même à des VLAN différents, on retrouve ce type de lien entre deux commutateurs ou un commutateur et un routeur en général [32].

2.2.4 Routage inter-VLAN

Chaque VLAN est un segment de réseau de niveau 2 isolé différent, les commutateurs de couche 3 se doivent donc d'être configurés de manière à permettre la communication entre VLAN. Le processus consiste en l'attribution d'une interface SVI de niveau 3 virtuelle, qui signifie également que les clients connectés à ce VLAN utiliseront cette interface comme passerelle par défaut.

2.3 Les listes de contrôles d'accès (ACL)

2.3.1 Définition d'une ACL

Une ACL nommée Liste de Contrôle d'Accès est un groupe de règles qui définissent si les paquets sont acceptés ou rejetés au niveau des interfaces d'entrée ou de sortie d'un routeur ou d'une interface virtuelle d'un VLAN.

Elle consiste à filtrer certains hôtes ou un groupe d'hôtes possédant une même plage d'adresses pour leur refuser ou leur accorder l'accès à une section du réseau ou à un certains types de services afin de fournir un niveau de sécurité d'accès au réseau. Le routeur examine chaque paquet dans le but de déterminer s'il doit le transmettre ou le rejeter en fonction des conditions précisées dans la liste de contrôle d'accès ACL. Les ACL appliquées à une interface d'entrée filtre

les paquets avant les décisions de routage contrairement aux ACL appliquées à une interface de sortie qui filtre les paquets après les décisions de routage [33].

2.3.2 Principe de fonctionnement des ACL

Il est possible de représenter le principe de fonctionnement d'une ACL grâce à cet organigramme :

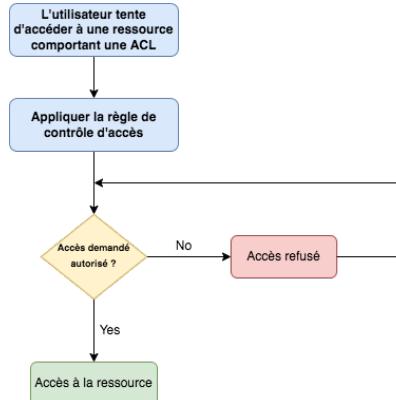


FIGURE 2.1 – Organigramme de l'algorithme de fonctionnement des ACL

2.3.3 Les types d'ACL

Elles sont divisées selon leurs types, notamment :

- ACL standard : Elle se base au niveau de la couche 3 en analysant le trafic uniquement sur les adresses IP sources. Elles sont numérotées entre 1-99 ou 1300-1999.
- ACL étendue : Elle s'appuie sur les adresses IP sources et destinations du paquet, les types de protocoles et les numéros de ports. Elles sont numérotées entre 100-199 ou 2000-2699 [33].

2.4 Le pare-feu

Un pare-feu est un équipement du réseau informatique, il peut être un matériel autonome qui protège tout un réseau d'ordinateurs et d'appareils, ou un logiciel installé sur un ordinateur, ou bien les deux. Son rôle est de sécuriser le réseau en surveillant le trafic, et en définissant les communications autorisées ou interdites entrantes et sortantes selon des règles de sécurité. Il permet d'interconnecter deux réseaux ou plus de niveaux de sécurité différents [34].

2.4.1 Fonctionnement d'un pare-feu

Le fonctionnement d'un pare-feu dépend des politiques de sécurité mise en place permettant de [35] :

- Autoriser les communications qui ont été explicitement autorisées.
- Bloquer les communications qui ont été explicitement interdites.

Une méthode de filtrage peut être déterminée selon les règles prédéfinies à l'intérieur du pare-feu citées ci-dessous :

- Autoriser la connexion (Allow).
- Bloquer la connexion tout en prévenant l'émetteur (Deny).
- Rejet de la connexion sans informer l'émetteur (Drop).

2.4.2 Les différents types de pare-feu

Depuis la naissance des pare-feux, ces derniers ont connu énormément d'amélioration, leur évolution se traduit comme suit [36] :

- Pare-feu de première génération : Les pare-feux de première génération appelés également pare-feux de filtrage de paquets ou encore Pare-Feux sans état (Stateless Firewalls), représentent les pare-feux les plus basiques. Ces derniers examinent tous les paquets entrants indépendamment des autres, seuls les paquets répondant aux critères de sécurité implantés ont le droit de passer. Ils s'appuient sur la taille du paquet, le protocole utilisé (IP ou TCP/UDP), l'adresse IP source et destination, le port source et destination, ce qui implique qu'ils fonctionnent au niveau de la couche 3 et 4 du modèle OSI. Toutefois, cette méthode de filtrage n'est pas optimale, car tant que le paquet répond aux conditions imposées par la politique de sécurité, celui-ci est considéré comme fiable. Si un acteur malveillant envoie une quantité importante de paquets, donc qu'une adresse IP source envoie une quantité assez grande dans une petite période de temps (Attaque DoS), cette attaque ne sera pas détectée. Ceci résulte du fait que l'adresse IP source est autorisée et que ce pare-feu ne prend pas en compte l'état de la communication. Une nouvelle réflexion vu le jour, et les pare-feux de seconde génération sont nés.
- Pare-feu de seconde génération : Les pare-feux de seconde génération autrement appelés pare-feux avec état (Stateful Firewalls) ont été créés afin de pallier aux problèmes du pare-feu de première génération. À la différence de son prédécesseur, celui-ci prendra en compte les paquets précédents, il n'autorisera ou ne bloquera pas uniquement selon le paquet actuel, mais aussi selon les paquets précédents et examinera continuellement les conversations IP entre les points terminaux. Ce qui implique que le pare-feu est conscient du contexte dans lequel l'envoi s'effectue. Mais encore une fois, un autre problème survient, plusieurs applications utilisent par exemple le protocole HTTP, et de ce fait, puisqu'ils utilisent tous le même port, le pare-feu n'est pas apte à les différencier. Afin de différencier entre ces paquets, il est nécessaire de s'approfondir et ainsi d'examiner la charge utile du paquet, payload.
- Pare-feu de troisième génération : Ces pare-feux utilisent ce qu'on appelle " le filtrage applicatif ", ils comprennent les niveaux les plus hauts, couche 7 du niveau OSI : protocoles, applications, contrôlent leurs différentes utilisations en les comparant à des utilisations simples de ces mêmes protocoles. Ils peuvent ainsi comprendre les protocoles tels que HTTP, FTP ou encore DNS, ceci répond à la problématique énoncée plus tôt, différencier entre le trafic d'un site web et le trafic d'un partage de fichier. Ces pare-feux jouent aussi le rôle de proxy Applicatif : il fait l'intermédiaire en invoquant le service demandé par l'utilisateur en masquant les adresses, il contacte le serveur externe avec sa propre adresse et non celle de l'utilisateur. Le Proxy cache donc toute l'infrastructure interne et joue le rôle de passerelle applicative.
- Les pare-feux de nouvelle génération ou NGFW pour Next Generation Firewall : Gartner le définit comme étant : " pare-feu d'inspection des paquets profonds qui va au-delà de l'inspection et du blocage des ports et des protocoles pour ajouter l'inspection au niveau de l'application, la prévention des intrusions et l'apport de renseignements de l'extérieur du pare-feu " [37]. Les NGFW ont la particularité de s'appuyer sur différentes méthodes pour assurer la

sécurité dans les entreprises. En effet, en plus des particularités des trois premiers décrits, ils ont la capacité de contrôler les applications cela en les classant ou en se basant sur les utilisateurs. Ils peuvent également adopter des politiques séparatistes variées, selon les utilisateurs, les appareils ou encore les applications ce qui permet de supprimer les points d'entrée des cyber attaquants. L'inspection haute performance comprend les applications, les ressources de calcul, l'analyse, et le stockage des données sur plusieurs réseaux privés et publics cloud.

2.5 La zone démilitarisée (DMZ)

Une zone démilitarisée est une aire réseau de demi-confiance en dehors de la zone de confiance du réseau contenant les ressources publiques accessibles, telles que serveur web, proxy. Elle est utilisée afin de relier les ressources internes d'une entreprise avec des ressources externes, venant par exemple d'internet [38].

Il existe différents niveaux de zone démilitarisée, leur description est la suivante [38] :

- Niveau 1 : Il s'agit du modèle le moins coûteux en termes d'équipements, mais représente aussi le premier niveau de sécurité, un segment séparé accessible depuis un port depuis le pare-feu de frontière, créant ainsi un point de filtrage et de protection.
- Niveau 2 : Ce modèle se concentre sur de multiples DMZ elles mêmes reliées à plusieurs port du pare-feu. Il existe toujours un seul point de sécurité et de filtrage le pare-feu, toutefois il faudra segmenter le réseau, donc attribuer des règles afin que les données échangées soient acheminées dans la bonne direction. De ce fait on divise les ressources et on augmente la sécurité car il y augmentation de la complexité du réseau.
- Niveau 3 : On remarque que celui-ci compte plusieurs pare-feux, ce qui crée différentes DMZ. Avoir différents pare-feux externes permet donc de cibler une sécurité plus élevée. On garde ainsi un trafic public entre les pare-feux, tout en autorisant les utilisateurs à avoir accès en interne aux ressources externes.
- Niveau 4 : Il s'agit là du modèle le plus coûteux, il emploie le couplage des pare-feux afin de créer les DMZ. Les ressources sont réparties par paire de pare-feux, ainsi on peut séparer les ressources selon le contrat SLA par exemple. Le seul inconvénient qu'on peut noter pour cette architecture et celle de niveau 3 est qu'au fur et à mesure que la sécurité augmente, également le nombre d'équipements s'accroît lui aussi. Pour chaque amélioration on paye un prix, notamment au niveau de la qualité de service, puisque les paquets doivent faire de plus longs chemins.

2.6 Le NAT

Le NAT permet de traduire une ou des adresses sources privées sortantes d'un réseau LAN en une ou plusieurs adresses externes dites publiques afin de leur permettre de communiquer avec l'extérieur en toute sécurité. Cette fonction est réalisée par un pare-feu ou un routeur jouant le rôle d'une passerelle, la trace des connexions est gardée dans une table appelée table NAT [39]. Il existe trois types de traduction d'adresse [39] :

- NAT statique (NAT 1 pour 1) : Chaque adresse interne lui correspond une adresse publique prédefinie fixe.
- NAT dynamique : Chaque machine du réseau LAN se voit assigner une adresse IP publique disponible non fixe parmi une plage d'adresses publiques.

- PAT (NAT n pour 1) : Toutes les adresses internes d'un même réseau LAN sont translatées vers une seule adresse IP globale publique. Chaque adresse IP bénéficie d'un numéro de port différent pour être différenciée des autres.

2.7 Les VPN

Certains utilisateurs se doivent d'accéder à un réseau interne (celui d'une entreprise par exemple) tout en restant éloignés géographiquement de ce réseau. Les Virtual Private Network représentent une des solutions les plus optimales et économiques pour une entreprise, si l'on considère l'utilisation de connexions VPN IPsec [40]. Ce type de connexion en particulier, permet assurément de transmettre les données à travers un réseau “non fiable” tel qu'Internet. Un VPN est un type de réseau informatique qui permet la création de liens directs entre des ordinateurs distants. Le réseau privé virtuel est utilisé également pour [41] :

- Chiffrer son adresse IP afin de renforcer l'anonymat d'un utilisateur ainsi que ses informations en ligne.
- Protocoles de chiffrement comme par exemple empêcher la fuite d'informations personnelles en chiffrant les cookies et l'historique de recherche.
- Lève les restrictions géographiques de certains site web en se connectant sur d'autres serveurs.
- Authentification à deux facteurs. Il est possible d'illustrer une connexion VPN entre deux réseaux par exemple grâce à une figure comme ceci :

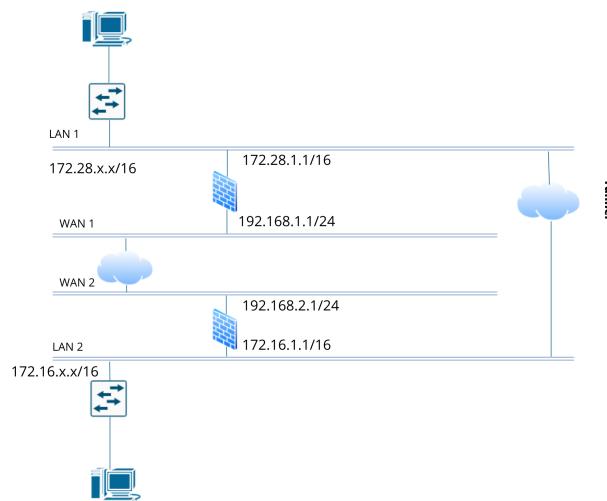


FIGURE 2.2 – Représentation d'un réseau utilisant un tunnel VPN

2.8 Étude comparative des solutions de sécurité basées sur un pare-feu

Plusieurs solutions de sécurité multicouches ont vu le jour ces dernières années pouvant être autant physiques que virtuelles. Afin de choisir la solution la plus optimale, il est nécessaire pour une entreprise de faire une étude comparative des différentes possibilités qui s'offrent à elle. En premier lieu, ce chapitre traite des différents types de pare-feux matériels et logiciels afin de relever leurs avantages et inconvénients, en second lieu, les différentes solutions propriétaires

et open source seront comparées afin de définir laquelle sera exploitée dans la conception et la réalisation du projet.

Pare-feu matériel

Un pare-feu matériel ou appelé également “pare-feu de périmètre”, est un périphérique physique conçu pour surveiller le trafic entrant ou sortant dans un réseau , il est utilisé par les grandes entreprises ayant un problème de sécurité important concernant la protection des données, comme par exemple les banques.

Avantages d'un pare-feu matériel

Les avantages qu'il est possible d'énumérer sont :

- Stabilité des performances : ce pare-feu n'est pas logiciel, il ne fonctionne donc pas sur le système, cela le rend plus difficile à déjouer.
- Rapide et peut s'intégrer facilement à d'autres systèmes de sécurité tels que l'équilibrage de charge (Load Balancing) [42].

Inconvénients d'un pare-feu matériel

Même si les avantages précédemment énumérés font du pare-feu matériel un choix sécurisé et assez recommandé, certains inconvénients peuvent laisser une entreprise refuser un tel investissement, notamment :

- Son prix, très coûteux, il s'agit d'un investissement assez conséquent pour une entreprise.
- Les installations de ce type de pare-feu demandent une certaine maintenance quotidienne et donc très souvent des ingénieurs afin de garantir une bonne configuration en tout temps [43].

Pare-feu logiciel

Le pare-feu logiciel est une solution logicielle exploitée par les petites entreprises ou particuliers grâce aux ordinateurs personnels ou aux machines virtuelles.

Avantages d'un pare-feu logiciel

Les avantages qu'ont les pare-feux logiciels peuvent être répertoriés comme ceci :

- Facilité d'administration : Il est très facile de configurer un pare-feu logiciel, souvent utilisé par les utilisateurs terminaux très peu expérimentés [44].
- Le prix : Il est possible de trouver de très bon pare-feu logiciel gratuit [45].

Inconvénients d'un pare-feu logiciel

Les inconvénients d'un pare-feu logiciel sont assez simples à mettre en lumière :

- La consommation des ressources physiques : Certes, nul besoin d'un matériel spécifique, toutefois quel qu'il soit, l'entreprise fera faire à une consommation de ressources. Mémoire ou encore espace disque seront forcément occupé par ce pare-feu, à la différence d'un pare-feu matériel qui utilise ses propres ressources.
- Son étude peut mener à trouver des failles de sécurité : en général ce genre de pare-feux lorsqu'ils sont open source et gratuit, ont une communauté assez importante, ce risque est donc présent, mais faible.

2.9 Comparaison des différentes solutions pare-feu

2.9.1 Pfsense [46]

Le projet PFsense est une distribution gratuite parue en 2004 basée sur le système d'exploitation FreeBSD tel que son précurseur m0n0wall¹. Il s'agit d'un routeur/pare-feu Open Source comprenant une interface web pour la configuration de tous les composants inclus, ainsi il n'y a pas besoin de réel connaissance UNIX, ou d'utiliser des commandes, en comparaison à d'autres solutions, il est important de noter que le projet pfSense n'est que la partie logicielle du pare-feu et que cela implique la possibilité de personnaliser le matériel que l'on désire choisir afin de répondre au mieux aux besoins spécifiques de l'environnement à sécuriser.

2.9.2 IPFire [47]

Représente un système d'exploitation open source dédié basé sur Linux renforcé et optimisé pour être utilisé en tant que pare-feu sur n'importe quel réseau, qu'il soit complexe niveau data center ou domestique. IPFire est un pare-feu à état qui utilise l'inspection des paquets avec état basé sur Netfilter un framework de Linux, il peut également fonctionner en tant que gateway VPN, analyser les payloads dans les paquets grâce à son IPS, ainsi que ces fonctionnalités apportées grâce aux modules complémentaires dont il est doté. Parmi les fonctionnalités mentionnées plus tôt on peut noter :

- La qualité de Service : Une allocation adéquate de la bande passante pour les applications critiques telles que les appels en VoIP afin de pallier aux problèmes de mauvaise qualité d'appels ou d'hébergement de site web lent.
- Système de prévention des intrusions : Permet une inspection approfondie des paquets, grâce à la comparaison avec une base de données des signatures pour les logiciels malveillants, détecte les comportements suspects afin de prévoir des attaques sophistiquées.
- Le proxy web : Est l'une des fonctionnalités les plus intéressantes car il permet de mettre en cache des mises à jour entières pour les systèmes d'exploitation ce qui permet d'économiser de la bande passante.

2.9.3 Cisco Firepower [48]

Cisco Firepower est le pare-feu nouvelle génération de Cisco, il est doté de plusieurs fonctionnalités complémentaires, et s'axe principalement sur une gestion complète et unifiée des politiques des fonctions de pare-feu, de la prévention des menaces et de la protection du réseau. Il intègre le pare-feu « stateful » le plus déployé au monde et offre un contrôle sur environ 4 000 applications et comprend :

- Une visibilité et un contrôle sur les applications.
- Un système de prévention des intrusions nouvelles générations NGIPS².
- Une protection avancée contre les malwares.
- Un filtrage des URL.

1. M0n0wall est une distribution FreeBSD dont le but est de fournir dans un système embarqué les services d'un pare-feu.

2. À la différence d'un IPS qui inspecte le trafic sur un réseau à la recherche de signature d'attaques connues et répond en conséquences, un Next Generation IPS inclura des fonctionnalités plus avancées. Ces derniers identifient un plus large éventail d'attaques grâce à différentes caractéristiques telles que : la contextualisation du réseau, l'identification des utilisateurs et des applications, et un traitement des menaces avancés en identifiant les charges suspectes et en les isolant dans un environnement mis en quarantaine.

2.9.4 FortiGate NGFW [49]

Fortigate est le pare-feu de nouvelle génération de la marque Fortinet, disponible en appliance virtuelle et en pare-feu matériel. Son système d'exploitation est notamment connu pour sa réduction de complexité des réseaux grâce à une vue de bout-en-bout. Cette visibilité englobe tous les appareils FortiGate sur le réseau et tous les appareils connectés aux FortiGate.

2.9.5 OPNsense [50]

OPNsense est un routeur/pare-feu open source issu de m0n0wall et Pfsense apparut pour la première fois en 2015. Basé sur FreeBSD, il inclut toutes les fonctionnalités qu'il est possible de retrouver sur des pare-feux coûteux notamment IPS, IDS, Filtrage web, et bien d'autres. L'environnement offre aux utilisateurs un espace agréable et facile à utiliser.

Cette solution offre différentes fonctionnalités, et est à la pointe de l'actualité en termes de sécurité notamment grâce à :

- Des mises à jour hebdomadaires.
- Environ deux sorties annuelles.
- Une documentation claire et un support gratuit.

Ces caractéristiques techniques sont nombreuses telles que :

- L'équilibrage des charges.
- IPS/IDS intégrés combinés à Nmap.³
- Filtrage de trafic (entrant et sortant) quelque soit le type de traffic IP ainsi que le protocole.
- Génération de certificat gratuit via Let's Encrypt, une autorité de certification automatisée, gratuite et ouverte.
- Accélération du traitement des paquets.

2.10 Tableau comparatif des caractéristiques des pare-feux

Après avoir étudié les pare-feux les plus utilisés actuellement sur le marché, il est important de réaliser un tableau récapitulatif afin de constater de manière globale la différence entre ces derniers et nous permettre de choisir la solution adaptée à nos besoins et moyens :

³. Nmap est un scanner de ports libre conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant

Caractéristique\Pare-feux	IPFire	OPNsense	PFsense	FirePower	FortiGate
Interface graphique	✓	✓	✓	✓	✓
Web Proxy	✓	✓	✓	✓	✓
IDS	✓	✓	✓	✓	✓
IPS	✓	✓	✓	✓	✓
NGIPS	✗	✗	✗	✓	✓
SSH	✓	✓	✓	✓	✓
Web Filtering	✓	✓	✓	✓	✓
NAT	✓	✓	✓	✓	✓
PAT	✓	✓	✓	✓	✓
IPSec	✓	✓	✓	✓	✓
Open VPN	✓	✓	✓	✗	✗
Multi-WAN	✗	✓	✓	✓	✓
Back up	✓	✓	✓	✓	✓
QoS	✓	✓	✓	✓	✓
Two factor authentication	✗	✓	✓	✓	✓
Ajout de fonctionnalités	✓	✓	✓	✗	✗

TABLE 2.1 – Tableau comparatif des caractéristiques des pare-feux

2.11 Conclusion

Dans ce chapitre, nous nous sommes familiarisés avec les aspects théoriques nécessaires à la réalisation de l’implémentation d’un pare-feu et sa configuration selon les attentes d’une entreprise. Nous avons ainsi pu nous approfondir et découvrir les différents moyens d’assurer la sécurité d’un réseau à travers une solution pare-feu. Nous avons plus tard exposé toutes les solutions propriétaires et open source qui s’offrent à nous. Par la suite, nous avons étudié les différentes caractéristiques de chaque pare-feu afin de faire le meilleur choix lors de notre implémentation. Les pages suivantes seront dédiées à la conception de notre solution, étape primordiale dans la réalisation d’un projet. Cette dernière sera suivie de la réalisation de l’architecture et sa sécurisation.

Chapitre 3

Conception et implémentation de la solution

3.1 Introduction

Le but de notre projet était l'étude d'une solution basée sur un pare-feu afin de sécuriser le réseau d'une nouvelle direction régionale d'Algérie Télécom prévue pour la wilaya de M'sila (28). Pour ce faire, nous avons évalué différentes solutions propriétaires et Open Source afin de réaliser un modèle d'implémentation réaliste et peu coûteux. Ce chapitre englobera l'ensemble des choix effectués afin de simplifier la tâche des ingénieurs, notamment grâce à la simulation de l'architecture avant et après implémentation du pare-feu. Lors de sa lecture, deux grands axes seront abordés, tout d'abord les besoins de l'entreprise exigés à travers un cahier des charges, pour finir sur une réalisation à la fois sur Packet Tracer et sur un logiciel de virtualisation.

3.2 Spécifications des besoins réseaux et sécurité

Il est crucial de regrouper tous les besoins énoncés par l'entreprise, et d'expliciter également toutes les spécificités fonctionnelles demandées. Pour cela, nous nous intéressons aux besoins réseaux puis aux besoins en termes de sécurité exigés par Algérie Télécom. Voici une partie du cahier des charges d'Algérie Télécom :

- Proposition d'un plan d'adressage optimal pour l'adresse réseau suivante : 172.28.0.0/16. Le 28 représentera la wilaya de la direction régionale de M'sila, et le 3ème octet représentera le VLAN concerné.
- Segmentation du réseau en VLAN selon les différents départements en prenant en compte une potentielle augmentation d'employés.
- Attribution d'une politique de sécurité vigoureuse selon les différents départements.
- Mise en place d'un serveur DHCP prenant en considération les différents VLAN et les serveurs utilisés.
- Création des DMZ.
- Mise en place d'un NAT pour augmenter la sécurité.
- Mise en place d'un VPN pour l'accès à distance.

3.3 Conception du réseau et de la sécurité de l'entreprise

Cette partie concerne la conception de l'architecture réseau et de la sécurité de la direction régionale. Elle s'articule sur la segmentation du réseau et la définition des politiques de sécurité.

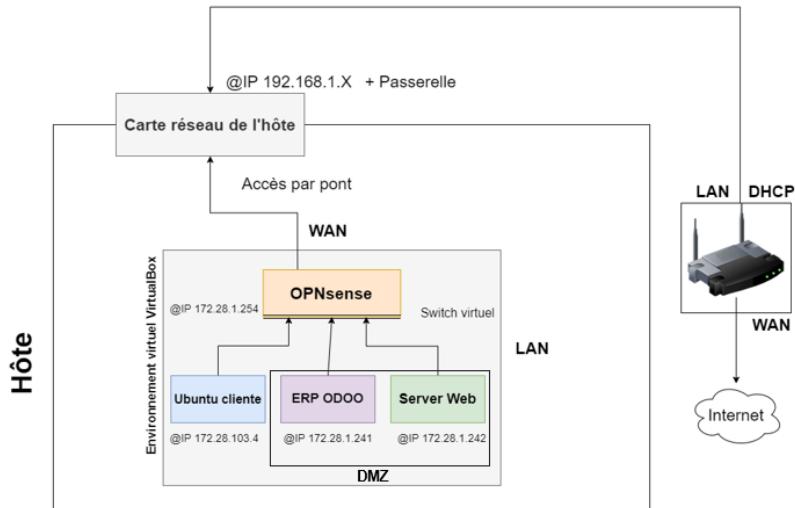


FIGURE 3.1 – Conception et planification de la mise en place du réseau.

3.3.1 Plan d'adressage et segmentation du réseau de la direction régionale

Voici le plan d'adressage conçu et la segmentation en VLAN proposée selon les attentes de l'entreprise :

Service	N°VLAN	Adresse réseau	Masque	Première adresse	Dernière adresse	Adresse de diffusion
RH	2	172.28.102.0	255.255.255.0	172.28.102.1	172.28.102.254	172.28.102.255
Finance et Comptabilité	3	172.28.103.0	255.255.255.0	172.28.103.1	172.28.103.254	172.28.103.255
Juridique	4	172.28.104.0	255.255.255.0	172.28.104.1	172.28.104.254	172.28.104.255
Communication et Marketing	5	172.28.105.0	255.255.255.0	172.28.105.1	172.28.105.254	172.28.105.255
Sécurité	6	172.28.106.0	255.255.255.0	172.28.106.1	172.28.106.254	172.28.106.255
Réseau	7	172.28.107.0	255.255.255.0	172.28.107.1	172.28.107.254	172.28.107.255
Hosting	8	172.28.108.0	255.255.255.0	172.28.108.1	172.28.108.254	172.28.108.255
Développement web et application	9	172.28.109.0	255.255.255.0	172.28.109.1	172.28.109.254	172.28.109.255
HelpDesk	10	172.28.110.0	255.255.255.0	172.28.110.1	172.28.110.254	172.28.110.255
Wifi	101	172.28.101.0	255.255.255.0	172.28.101.1	172.28.101.254	172.28.101.255
Directeur	204	172.28.204.0	255.255.255.0	172.28.204.1	172.28.204.254	172.28.204.255

TABLE 3.1 – Plan d'adressage IP et VLAN de la direction régionale de M'Sila.

Le plan d'adressage prend en considération l'augmentation d'employés que peut connaître la direction régionale comme voulu.

3.3.2 Définition des politiques de sécurité

Les objectifs de sécurité énoncés par Algérie Télécom étaient les suivants :

- Tous les départements hors du département système informatique ne peuvent accéder au serveur DHCP.
- Les serveurs se doivent d'avoir une identité statique, donc des adresses IP statiques.
- Les ports ne doivent pas être des ports par défaut, et ne doivent correspondre à aucune logique.
- Un accès VPN sans authentification d'utilisateur.

- L’allocation des adresses par le serveur DHCP ne doit pas prendre en compte la plage des serveurs.

3.4 Outils d’étude

Pour cette étude, nous avons eu à expérimenter différents outils, et différentes méthodes, toutefois certaines, faute de ressources, n’ont pu aboutir à une réalisation. De ce fait nous exposerons tous les outils que nous avons eu à découvrir ou tester et la solution finale que nous avons implémenter.

3.4.1 Simulateurs Réseaux et sécurité

Voici les différents simulateurs dont nous avons pris connaissance :

- EVE-NG : est un logiciel d’émulation de réseau multifournisseur sans client qui permet de simuler des réseaux et leur sécurité. En général, les entreprises l’utilisent dans le but de créer des preuves virtuelles de concepts, des solutions et des environnements de formation [51].
- GNS3 : est un logiciel multiplateforme utilisé par les ingénieurs réseau pour émuler, configurer, tester des réseaux virtuels et réels. Il permet d’exécuter une petite topologie composée de quelques appareils sur un ordinateur portable grâce à son interface graphique Drag and Drop [52].
- Packet Tracer : est le simulateur de matériel réseau Cisco fourni gratuitement par l’entreprise dans le but de se familiariser avec les configurations de base de leurs technologies, ou encore afin de simuler certaines architectures simples [53].

3.4.2 Logiciels de virtualisation et plateforme cloud

Plusieurs possibilités se sont ouvertes à nous lors de l’implémentation de notre solution, en particulier :

Oracle VM VirtualBox : est une application multi plateforme de virtualisation qui offre l’opportunité d’exécuter différents systèmes d’exploitation grâce à différentes machines virtuelles [54].

VMWare Workstation : est une solution logicielle multi plateforme permettant la virtualisation de différents systèmes d’exploitation ou applications sur un même ordinateur. Les limites de virtualisation de VMWare Workstation dépendent de la capacité de l’ordinateur hôte [55].

Azure : La plateforme cloud Azure compte plusieurs produits et services cloud conçus afin d’aider au développement de nouvelles solutions, et de faciliter aux entreprises et particuliers certaines tâches de gestion ou d’administration. Les machines virtuelles Azure sont des instances de service d’images qui fournissent des ressources informatiques à la demande [56].

Hyper-V : est un système de virtualisation créé par Microsoft basé sur un hyperviseur 64 bits de la version de Windows Server 2008. Ce dernier ouvre la possibilité de créer des environnements informatiques virtuels, d’exécuter et de gérer différents systèmes d’exploitation sur un seul et même hôte physique [57].

3.4.3 Pare-feu

Pour la réalisation de notre solution de sécurité, nous avons choisi le pare-feu OPNsense. Ce choix est dû à de multiples facteurs, notamment :

- L’outils choisi est Open Source, un certain niveau de liberté est ainsi permis en comparaison à certaines solutions certes sécurisées mais standardisées. Il est possible de créer ces propres scripts donc de répondre d’une manière plus centralisée et efficace aux besoins de l’entreprise.
- Il est envisageable de modifier le code source comme l’entreprise le souhaite, et d’ajouter

ou de supprimer des modules déjà existants. Dans le cas d'Algérie Télécom, certains services plus sophistiqués se devaient d'être présents tels que : la détection par intelligence artificielle d'un futur état de congestion. Ce travail nécessite un pare-feu qu'il est possible d'améliorer de manière libre.

- L'un des atouts majeurs d'OPNsense est son prix. En effet, il est gratuit ce qui implique la possibilité d'avoir un pare-feu à la fois gratuit, centré sur les objectifs de sécurité de l'entreprise, mais aussi étudié et mis à jour par une communauté très active.
- Très connu pour son ergonomie, il permet une expérience utilisateur plus agréable et rend le travail beaucoup plus simple, qu'il s'agisse de son interface graphique sur ordinateur, ou sur mobile.

3.4.4 Les ressources utilisées

Voici un récapitulatif de toutes les ressources mises en oeuvre afin de simuler notre architecture :

- Bitnami : est une bibliothèque d'installateur ou de package pour les applications et machines virtuelles, elle fournit des images prête à l'emploi pour la configuration automatisée des logiciels de serveur populaires sur les différentes plateformes. Chaque programme contient donc tous les logiciels nécessaires dès leur installation notamment le système d'exploitation, l'environnement du serveur web, SGBD. Il n'y a donc pas besoin de télécharger à nouveau d'autres fichiers, base de données complémentaires. Une fois installée, celui-ci n'interférera en aucun cas avec le système ou les logiciels déployés sur l'hôte [58].
- Odoo : Ce package est disponible sur Bitnami et représente un progiciel de gestion intégrée ERP extrêmement maléable et adapté à différents secteurs d'activités. Il est utilisé à la fois dans les cabinets dentaires, la logistique, la relation client [59]. Dans notre cas, il sera utilisé pour son module de finance, et représentera notre ERP pour le département Finance et comptabilité.
- Ubuntu : une machine virtuelle Ubuntu est nécessaire afin de simuler une machine cliente et vérifier les configurations apportées grâce au pare-feu.

3.4.5 Les équipements utilisés

Cette partie concerne tous les équipements que nous avons utilisé lors de la réalisation du projet :

- Image ISO de OPNSense : OPNsense-22.1.2-OpenSSL-dvd-amd64 (Dernière version).
- Image ISO de Ubuntu : ubuntu-budgie-20.10-desktop-amd64
- Image ISO de bitnami : bitnami-odoo-15.0.20220510-3-r01-linux-debian-10-x86_64-nami

3.5 Chronologie de la réalisation du projet

Il était convenu que nous réalisions au départ, une simulation grâce aux deux simulateurs GNS3 ou EVE-NG. Toutefois, en raison des ressources manquantes, nous n'avons malheureusement pas pu utiliser ces logiciels. Après plusieurs essais, nous avons décidé de nous tourner vers le cloud en utilisant Azure, et avons créé notre propre machine virtuelle dans le but d'installer une nouvelle fois les logiciels prévus à l'origine EVE-NG ou GNS3. Une fois installée la machine ne tolérait pas de virtualiser à nouveau à travers VirtualBox ou encore VMWare. Nous avons résolu ce problème grâce à Hyper-V, mais avons remarqué qu'il n'était pas configuré pour activer le contrôle des ressources du processeur et ne permettait donc pas de configurer les deux logiciels. Notre travail a donc été divisé en deux parties afin de répondre à la problématique pleinement :

D'une part, nous réaliserons la partie réseau sur le logiciel Packet Tracer qui se trouve en annexe A, en utilisant les équipements utilisés par l'entreprise, d'une autre part, nous configurerons le pare-feu sur notre propre machine hôte via VirtualBox.

3.6 Implémentation du pare-feu

Nous expliciterons dans cette section, toutes les étapes mises en places afin d'implémenter notre pare-feu. En premier lieu, nous avons installé ce dernier grâce à son image ISO. En second lieu, nous avons appliqué les configurations réseaux suivantes sur VirtualBox : un adaptateur en réseau interne qui représentera le LAN afin d'interconnecter les machines clientes et les serveurs de la DMZ, et un adaptateur en pont afin d'accéder au routeur ADSL domestique tel que notre PC hôte représentera le réseau WAN.

Pour ce faire, nous avons effectué ces modifications sur VirtualBox :

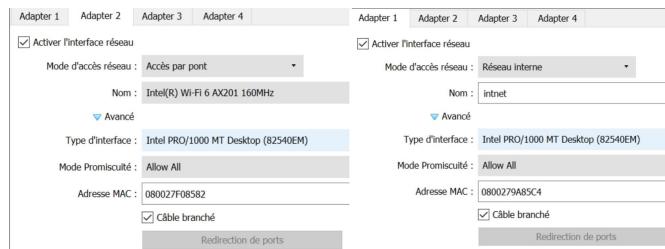


FIGURE 3.2 – Configuration des adaptateurs réseaux d'OPNsense.

Nous avons opté plus tard, pour une machine Ubuntu peu coûteuse en termes de ressources afin de représenter le réseau local de l'entreprise. Configurée en réseau interne elle nous habilitera à confirmer les résultats.

3.6.1 Configurations des adresses IP sur le pare-feu

Afin de configurer les adresses IP du LAN et notre WAN représenté par notre réseau local domestique, nous suivons les étapes suivantes :

Pour des raisons pratiques, nous activons le DHCP sur l'interface WAN. Néanmoins, la configuration de cette interface est également réalisable manuellement. En transcrivant l'adresse IP de l'interface LAN grâce à la machine Ubuntu ou WAN sur le navigateur de l'hôte, on obtient le résultat suivant :

```

Configure IPv4 address LAN interface via DHCP? [y/N] n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.28.1.254

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

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

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

Configure IPv6 address LAN interface via DHCP6? [y/N] ■

```

FIGURE 3.3 – Allocation de l’adresse IP pour l’interface LAN de OPNsense.

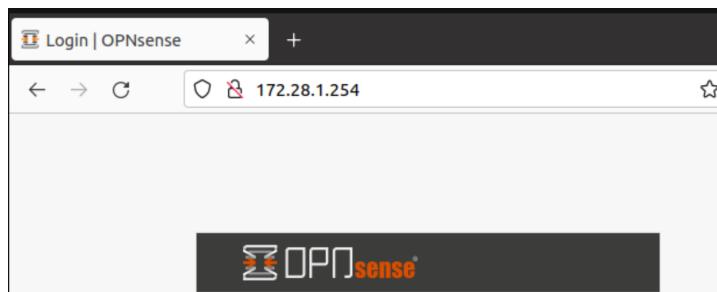


FIGURE 3.4 – Interface graphique d’OPNsense aperçue grâce à l’adresse LAN.

3.6.2 Configuration de la passerelle

Une fois que l’accès au pare-feu est établi, nous ajoutons la passerelle notre routeur, avec pour finalité l’accès à internet :

Edit gateway		full help ⓘ
<input checked="" type="checkbox"/>	Disabled	
<input type="checkbox"/>	Name	WAN_GW
<input type="checkbox"/>	Description	Vers ADSL
<input type="checkbox"/>	Interface	WAN
<input type="checkbox"/>	Address Family	IPv4
<input type="checkbox"/>	IP address	192.168.1.1
<input checked="" type="checkbox"/>	Upstream Gateway	
<input type="checkbox"/>	Far Gateway	
<input checked="" type="checkbox"/>	Disable Gateway Monitoring	
<input type="checkbox"/>	Monitor IP	8.8.8.8
<input type="checkbox"/>	Mark Gateway as Down	
<input type="checkbox"/>	Priority	255
<input type="checkbox"/>		Advanced - Show advanced option

FIGURE 3.5 – Configuration de la passerelle du WAN.

Nous constatons que la passerelle fonctionne à l'aide d'un ping vers les serveurs publics DNS Google réussi.

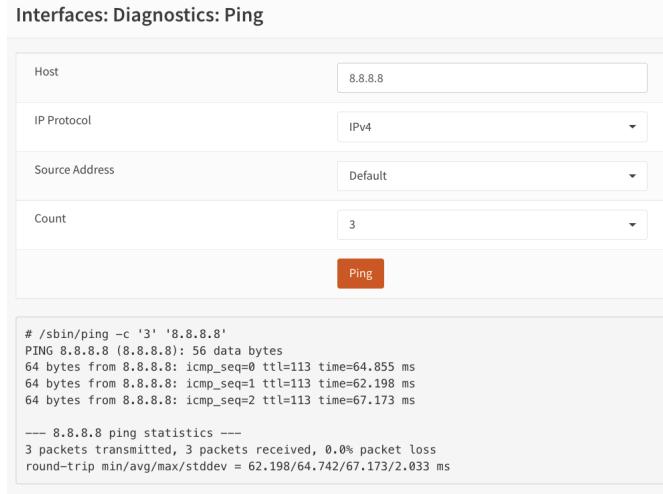


FIGURE 3.6 – Confirmation de l'accès à internet grâce à la passerelle.

3.6.3 Installation de Odoo

Une fois les configurations de base terminées, nous installons notre ressource. Pour ce faire, nous créons une machine virtuelle grâce à l'image ISO de Bitnami, et vérifions son adresse IP et son adresse MAC :

```
*** Welcome to the Odoo packaged by Bitnami 14.0.20220510-3 ***
*** Documentation: https://docs.bitnami.com/virtual-machine/apps/odoo/
*** https://docs.bitnami.com/virtual-machine/
*** Bitnami Forums: https://community.bitnami.com/
bitnami@debian:~$ sudo ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 172.28.1.241 netmask 255.255.0.0 broadcast 172.28.255.255
        inet6 fe80::a00:27ff:fe26:96ce prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:26:96:ce txqueuelen 1000 (Ethernet)
```

FIGURE 3.7 – Installation et vérification de l'adresse IP de OODOO.

Lorsque nous inscrivons l'adresse IP mentionnée nous accédons à l'interface graphique de l'ERP Odoo :

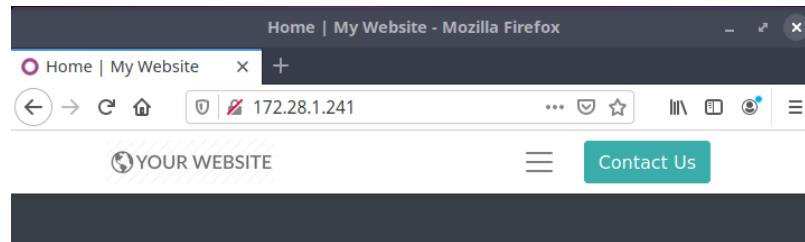


FIGURE 3.8 – Interface graphique de Odoo.

3.6.4 Configuration du DHCP sur OPNsense

Si nous voulons avoir accès à nos ressources, nous devons d'abord leur attribuer une adresse IP. Nous effectuons la configuration du serveur DHCP sur notre pare-feu, selon les caractéristiques présentes :

Première plage : 172.28.0.1 à 172.28.0.254/16

Seconde plage : 172.28.11.1 à 172.28.255.254/16

Dans le dessein de reconnaître les ressources d'une entreprise, on attribue une adresse fixe aux serveurs, dans notre cas nous utilisons le DHCP statique qui aide à attribuer une adresse IP fixe selon l'adresse mac telle que :

Serveur ERP a pour adresse IP : 172.28.1.241/16 et pour adresse MAC : 08 :00 :27 :26 :96 :ce

FIGURE 3.9 – Configuration du DHCP sur OPNsense.(1)

DHCP Static Mappings for this interface.				
Static ARP	MAC address	IP address	Hostname	Description
	08:00:27:26:96:ce	172.28.1.241	ERP_ODOO	

FIGURE 3.10 – Configuration du DHCP sur OPNsense.(2)

3.6.5 Création des VLAN

D'après le tableau 4.1, chaque service reçoit une plage précise d'adresse IP. Cette partie traite de la configuration des VLAN plus précisément le VLAN associé aux serveurs. La création de ces derniers nous permet d'appliquer des politiques de sécurité spécifiques afin de garantir la sécurité exigée.

The figure consists of two screenshots of a network configuration interface. The top screenshot, titled 'Interface VLAN Edit', shows fields for 'Parent interface' (em0), 'VLAN tag' (102), 'VLAN priority' (Critical Applications (3)), and 'Description' (DMZ). It includes 'Save' and 'Cancel' buttons. The bottom screenshot, titled 'Static IPv4 configuration', shows 'IPv4 address' (172.28.1.1) and 'IPv4 Upstream Gateway' (Auto-detect). Both screenshots include a small 'Info' icon next to each field.

FIGURE 3.11 – Crédit du VLAN et configuration de son interface.

Nous pouvons préciser via le pare-feu que les machines présentent au niveau de ce VLAN sont des serveurs et donc leur ajouter un DHCP différents, avec la plage qui correspond. Cela nous évite d'entrer manuellement toutes les adresses IP ou de fusionner les serveurs et les machines clientes.

The screenshot shows the 'DHCP' configuration page. It includes fields for 'Enable' (checked), 'Enable DHCP server on the DMZ interface' (checked), 'Deny unknown clients' (unchecked), 'Ignore Client UIDs' (unchecked), 'Subnet' (172.28.1.0), 'Subnet mask' (255.255.255.0), 'Available range' (172.28.1.1 - 172.28.1.254), and 'Range' (from 172.28.1.1 to 172.28.1.254). There are also '+' and '-' buttons for subnet management.

FIGURE 3.12 – Configuration du DHCP pour la DMZ.

Il est donc actuellement plus aisément de formuler des restrictions sur les serveurs grâce à la DMZ.

3.6.6 Configuration du port forwarding

La communication se fait en général grâce à l'assignation de ports spécifiques selon les protocoles. Elle permet donc à une personne scannant les ports de découvrir quels sont les types

de serveurs, les applications utilisés voire plus dans un réseau. Il est très courant d'attribuer d'autres ports non standards ou par défaut aux applications et services afin d'augmenter la sécurité du réseau et brouiller les pistes d'éventuels pirates informatiques.

Dans cette partie, nous allons présenter les différents ports que nous avons assigné à nos ressources sur le réseau :

— Accessibilité du pare-feu :

Afin d'accéder à OPNsense en dehors de son réseau local, c'est à dire depuis le réseau WAN, nous avons configurer un accès avec le port 9999.

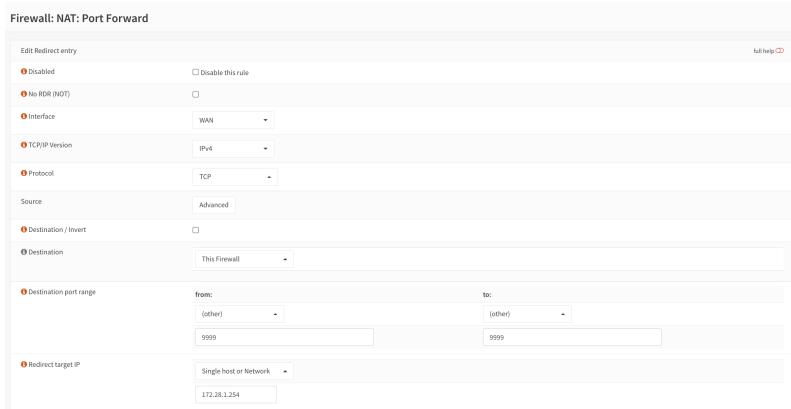


FIGURE 3.13 – Assignation d'un port spécifique à l'interface WAN du pare-feu.

Nous avons également assigné un port spécifique à l'interface LAN du pare-feu, que nous avons configuré avec le port 2828.

Pour confirmer que la connexion fonctionne effectivement lorsque l'on attribue les ports, nous inscrivons dans la barre de recherche l'adresse IP et le port correspondant :

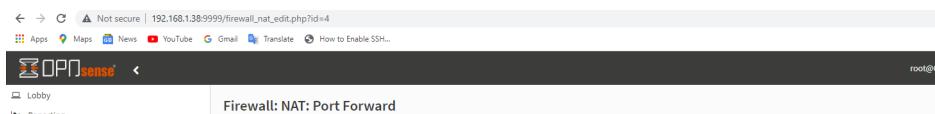


FIGURE 3.14 – Confirmation de la redirection de l'interface WAN de l'accès du pare-feu vers le port 9999.

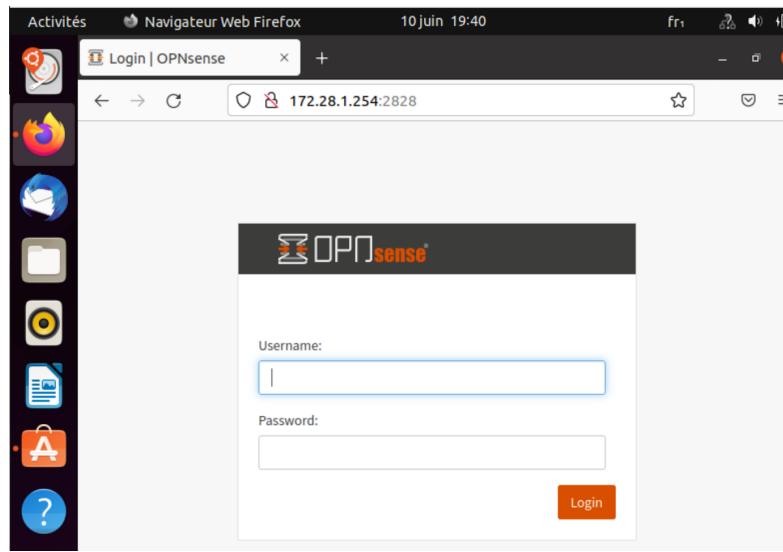


FIGURE 3.15 – Confirmation de la redirection de l'interface LAN de l'accès du pare-feu vers le port 2828.

— Accessibilité d'Odoo :

Le port 7777 de la même manière est attribué à Odoo, les ressources demandées par la mise en place de trois machines virtuelles étant trop importantes nous ne pourrons pas vérifier les résultats de la redirection de port.

3.6.7 Configuration du VPN

Nous avons tel que demandé par l'entreprise implémenté un VPN grâce à OpenVPN. Pour cela nous avons suivi les étapes suivantes :

— Crédation d'une autorité de certification : Il est obligatoire de créer une autorité de certification à travers OPNsense car nous ne nous referons à aucune autre autorité.

FIGURE 3.16 – Crédation de l'autorité de certification interne à OPNsense.

- Création d'un utilisateur : Notre client sera nommé "JOJO" et aura automatiquement un certificat lors de sa création.
- Autorisation du trafic VPN sur le WAN : Cette étape est primordiale, sans elle, le trafic VPN ne sera pas autorisée.



FIGURE 3.17 – Autorisation du trafic VPN sur le WAN.

- Configuration de OpenVPN : Nous avons ajouté le certificat serveur à OpenVPN sur OPNsense et défini les paramètres complémentaires à la création d'un serveur VPN.

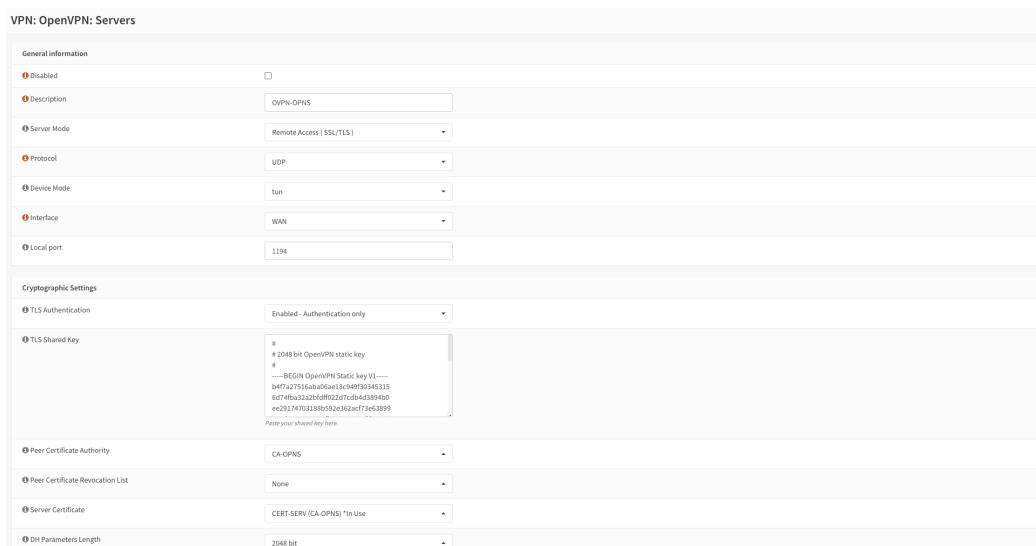


FIGURE 3.18 – Configuration de OpenVPN.

- Du côté client : Nous exportons le fichier sur l'application OpenVPN, puis nous transcrivons l'adresse IP du pare-feu sur le réseau local. Ainsi, nous nous trouvons à l'intérieur du réseau local, en étant dans un tout autre réseau.

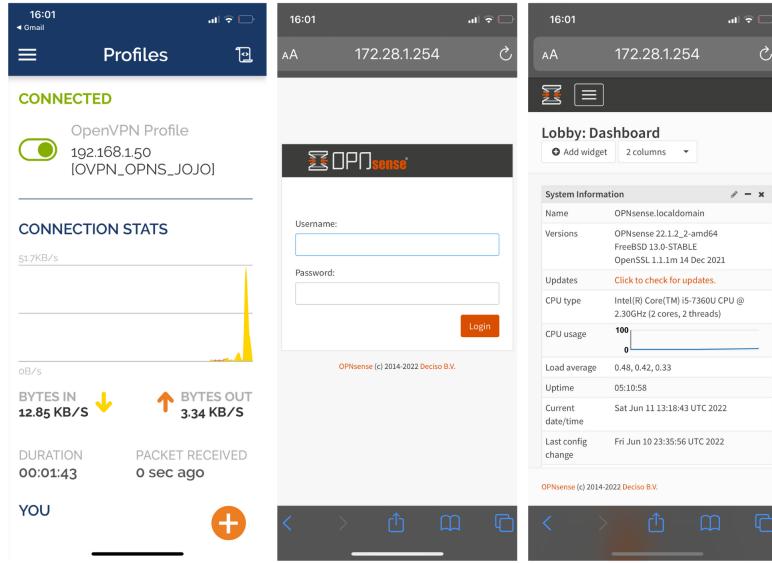


FIGURE 3.19 – Création de l'autorité de certification interne à OPNsense.

3.7 Ajout du module NGFW Zenarmor

Zenarmor (Sensei) est un pare-feu instantané entièrement logiciel qui peut être déployé pratiquement n'importe où.

Il peut être facilement implanté sur n'importe quelle plate-forme avec une connectivité réseau grâce à sa conception sans appareil, tout-en-un, entièrement logicielle, légère et simple. Pour les pare-feux open source, cette technologie offre des fonctionnalités de pointe de nouvelle génération qui ne sont pas actuellement disponibles dans des produits tels que OPNsense [60].

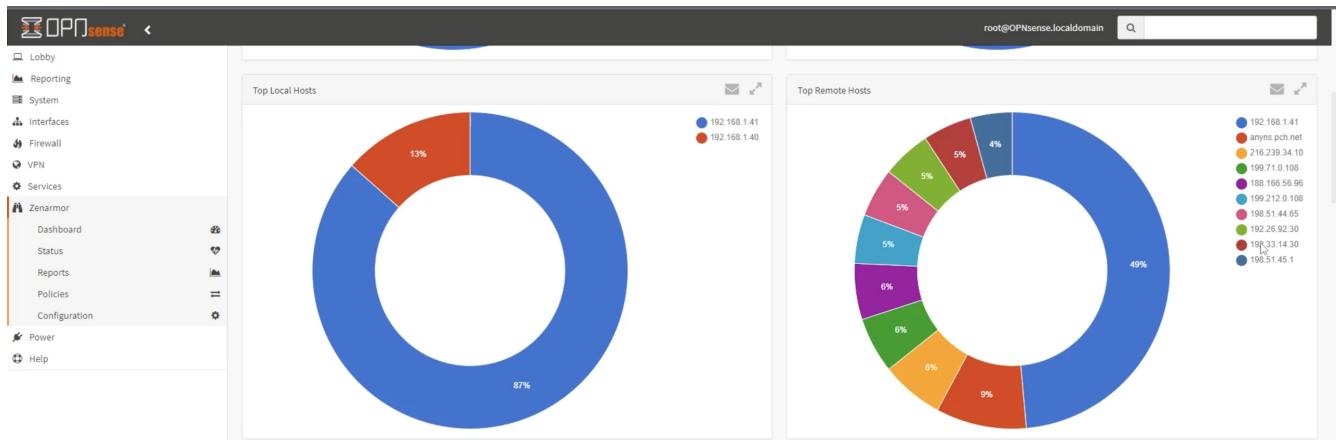


FIGURE 3.20 – Ajout du module Zenarmor sur OPNsense.

Il est ainsi possible grâce à la dashboard personnalisable de catégoriser les applications, les interfaces et bien d'autres paramètres selon les nécessités des administrateurs. Il est également possible d'avoir des rapports détaillés tels que le montre la figure 3.21 :

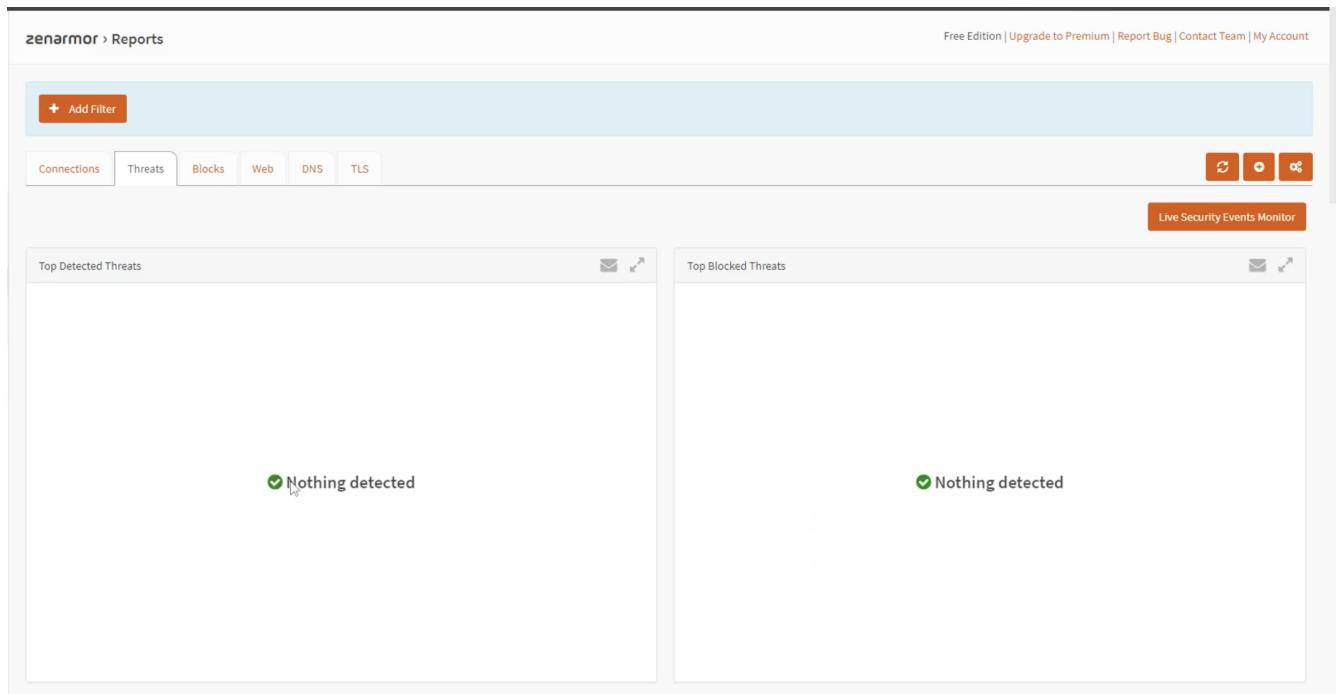


FIGURE 3.21 – Ajout du module Zenarmor sur OPNsense.

Le rapport de la détection des menaces est actuellement vide, synonyme de l'absence de menaces.

3.8 Conclusion

En conclusion, ce chapitre regroupe les différentes manipulations que nous avons réalisées afin d'implémenter notre pare-feu. Tout d'abord, nous avons mis en lumière les différentes technologies que nous devions utilisées, puis la solution finale à laquelle nous avons abouti. Faute de moyens, notre solution a été divisée en deux parties, sur deux technologies différentes, toutefois l'implémentation du pare-feu s'est faite à la fois sur un réseau local virtuel, mais aussi sur notre réseau local domestique. Ceci nous a notamment permis de découvrir l'environnement du pare-feu OPNsense, et de l'ERP Odoo.

Conclusion générale

Les pare-feux représentent des lignes de défense importantes pour les infrastructures réseaux, devenues primordiales, tous les secteurs se protègent mais d'une manière dissemblable.

Notre projet vise à implémenter une solution de sécurité basée sur le pare-feu OPNsense au sein d'une nouvelle direction régionale située à M'Sila de manière à pouvoir mettre en place une politique de sécurité efficace du réseau informatique.

La problématique exposée le long du rapport était l'étude de faisabilité du projet demandé avec des ressources limitées, et la capacité à interpréter des besoins fonctionnels d'après un cahier des charges en besoins techniques.

Pour ce faire, nous avons en premier lieu, étudier les différents aspects de la cybersécurité, les types d'attaques, la procédure à suivre lors de la mise en place d'une cyberattaque, puis les enjeux actuels en termes de cybersécurité. Ceci nous a permis de contextualiser notre étude, de visualiser l'ampleur et l'importance de cette dernière dans une entreprise. En second lieu, nous nous sommes intéressées aux aspects théoriques qui permettaient la mise en place d'un réseau sécurisé, cela nous a aidé à définir des politiques de sécurité rigoureuses, à déterminer les besoins d'une entreprise et à traduire des spécifications administratives en spécifications informatiques. De plus, nous avons réalisé une étude comparative des différentes solutions proposées actuellement sur le marché, ce qui a donné lieu à la possibilité de mettre en avant les caractéristiques propres à chaque technologie. Pour finir, nous avons découvert différents environnements, installé différents services et configuré ces derniers de manière à répondre à l'objectif du projet. Cette implémentation est fractionnée en plusieurs axes : l'installation du pare-feu, la configuration du DHCP et du DHCP statique, la configuration de la redirection des ports, l'installation de l'ERP Odoo, la possibilité d'accéder à internet depuis un réseau local, l'établissement d'un réseau privé virtuel, et la création de réseau locaux virtuels.

À travers cette étude, nous avons été amenées à manipuler des services connus en entreprise, qui permettent la gestion des ressources humaines, la maintenance des services informatiques, et la gestion de la comptabilité et des finances. Ces services étant tous centralisés sur un unique package qu'il est également possible d'administrer et de sécuriser grâce à des politiques de sécurité. Il est tout à fait envisageable qu'Algérie Télécom migrent vers les services que proposent Odoo, en raison de son large éventail. De même pour OPNsense, les configurations effectuées pourraient être plus centralisées sur les besoins de l'entreprise que certaines technologies conditionnées et standardisées.

Annexe A

Architecture du réseau sur Packet Tracer

Afin de simuler le réseau de notre direction régionale, nous aurons besoin de plusieurs équipements à implémenter :

- Serveur DHCP : alloue une adresse IP à chaque poste de travail dans la plage d'adresse du VLAN où il est situé. Le déploiement d'un serveur DHCP pour chaque sous-réseau peut revenir très coûteux. C'est pour cela qu'on a opté pour un seul serveur DHCP qui permettra de servir les clients provenant de VLAN différents. Afin que la diffusion des requêtes DHCP des clients soit possible, on a configuré une adresse d'assistance IP (qui est l'adresse IP du serveur DHCP) sur le Switch niveau 3.
- Cisco Catalyst Switch 3560-24PS Layer 3 : est un switch de niveau 3. Il est nécessaire dans une architecture composée de VLAN afin de permettre le routage et l'échange des données entre ces différents VLAN.
- Cisco Catalyst Switch 2960-24TT Layer 2 : est un switch de niveau 2. Il permet de gérer et d'acheminer uniquement les adresses MAC et ne permet pas le routage inter-vlan.

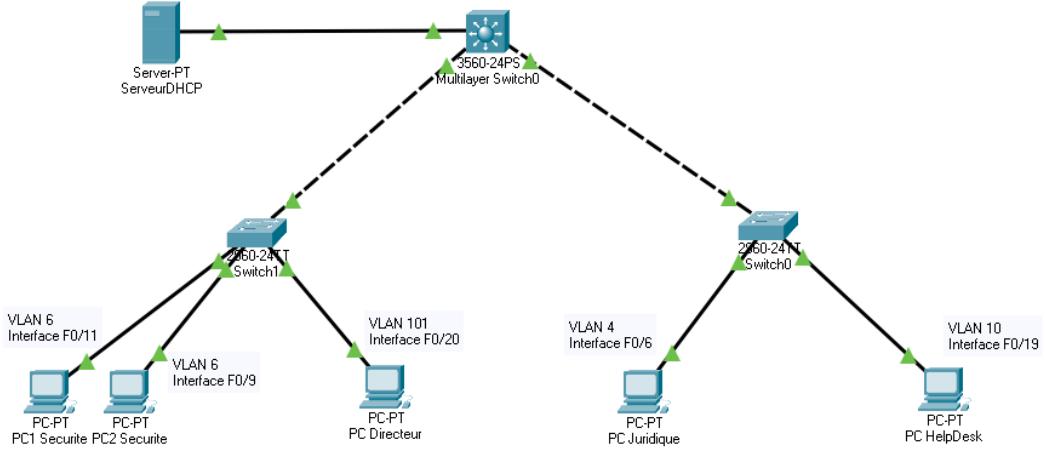


FIGURE A.1 – Architecture de la direction régionale.

A.1 Création des VLAN et configuration du DHCP

- Dans la figure ci-dessous, on a procédé à la création des VLAN dans le Switch niveau 3 en ligne de commande et on a affecté à chaque VLAN la première adresse de son sous-réseau. Le VLAN 1 a été configuré spécialement pour le serveur DHCP.

```

Switch(config-vlan)#int vlan 1
Switch(config-if)#ip add 172.28.100.1 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
*LINK-5-CHANGED: Interface Vlan1, changed state to up

*LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#vlan 2
Switch(config-vlan)#name RH
Switch(config-vlan)#int vlan 2
Switch(config-if)#
*LINK-5-CHANGED: Interface Vlan2, changed state to up

Switch(config-if)#ip add 172.28.102.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name FinanceEtComptabilite
Switch(config-vlan)#int vlan 3
Switch(config-if)#
*LINK-5-CHANGED: Interface Vlan3, changed state to up

Switch(config-if)#ip add 172.28.103.1 255.255.255.0
Switch(config-if)#exit

```

FIGURE A.2 – Création des VLAN depuis le Switch niveau 3.

Dans le serveur DHCP, en allant vers Desktop puis dans IP Configuration, on attribue à notre DHCP une adresse IP statique dans la plage du VLAN 1.

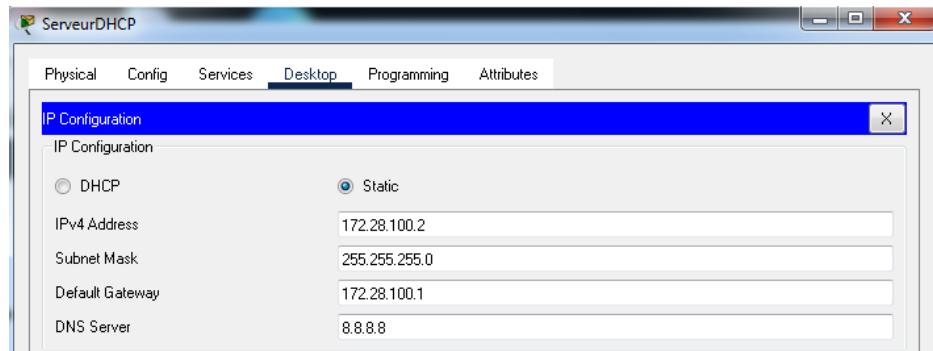


FIGURE A.3 – Allocation d'une adresse IP statique au serveur DHCP.

Dans Services, on active le service DHCP et on ajoute les plages d'adresse pour les 12 VLAN puis on reconfigure la plage par défaut du serveur et on l'associe au VLAN 1.

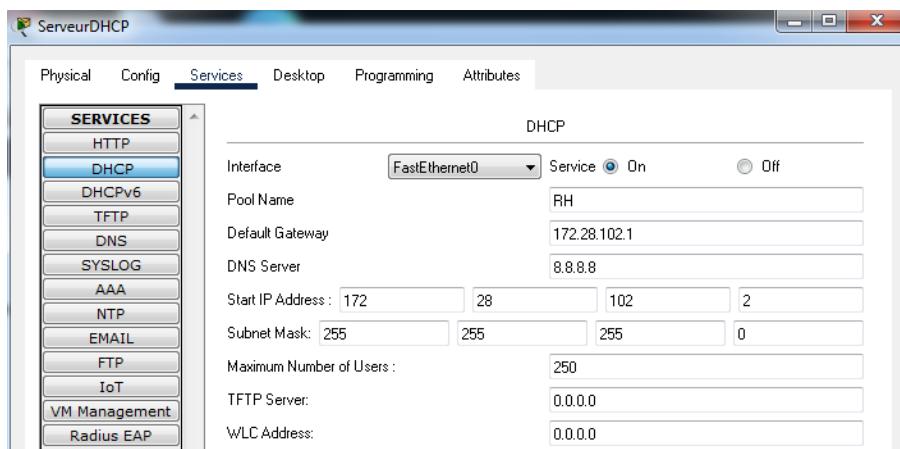


FIGURE A.4 – Ajout de la plage d'adresse pour le vlan 2 RH.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	172.28.100.1	8.8.8.8	172.28.100.3	255.255.255.0	250	0.0.0.0	0.0.0.0
Directeur	172.28.204.1	8.8.8.8	172.28.204.2	255.255.255.0	250	0.0.0.0	0.0.0.0
Wifi	172.28.101.1	8.8.8.8	172.28.101.2	255.255.255.0	250	0.0.0.0	0.0.0.0
HelpDesk	172.28.110.1	8.8.8.8	172.28.110.2	255.255.255.0	250	0.0.0.0	0.0.0.0
DeveloppementWebEtl	172.28.109.1	8.8.8.8	172.28.109.2	255.255.255.0	250	0.0.0.0	0.0.0.0
Hosting	172.28.108.1	8.8.8.8	172.28.108.2	255.255.255.0	250	0.0.0.0	0.0.0.0
Reseau	172.28.107.1	8.8.8.8	172.28.107.2	255.255.255.0	250	0.0.0.0	0.0.0.0

FIGURE A.5 – Ajout de toutes les plages associées aux VLAN.

Dans le switch niveau 3, on configure les deux interfaces G0/1 et G0/2 reliées aux switch niveau 2 en mode trunk, afin de permettre les trames non taguées provenant des différents VLAN de communiquer (Le dot1Q permet d'insérer un tag dans l'en-tête d'une trame ethernet).

```

Switch(config)#int g0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up

```

FIGURE A.6 – Activation du mode trunk depuis le Switch niveau 3.

On crée tous les VLAN et on les renomme selon chaque service dans les deux switchs de niveau 2, comme suit :

```

Switch(config)#vlan 2
Switch(config-vlan)#name RH
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name FinanceEtComptabilite
Switch(config-vlan)#vlan 4
Switch(config-vlan)#name Juridique
Switch(config-vlan)#vlan 5
Switch(config-vlan)#name CommunicationEtMarketing
Switch(config-vlan)#vlan 6
Switch(config-vlan)#name Securite
Switch(config-vlan)#vlan 7
Switch(config-vlan)#name Reseau
Switch(config-vlan)#vlan 8
Switch(config-vlan)#name Hosting
Switch(config-vlan)#vlan 9
Switch(config-vlan)#name DeveloppementWebEtApplication
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name HelpDesk
Switch(config-vlan)#vlan 101
Switch(config-vlan)#name Wifi
Switch(config-vlan)#vlan 204
Switch(config-vlan)#name Directeur

```

FIGURE A.7 – Création des VLAN sur le Switch niveau 2.

Après avoir créé les VLAN, on va associer chaque interface à son VLAN et ceci sur les deux switch de niveau 2.

N° VLAN	Attribution des ports sur les switchs de niveau 2
2	Interface F0/1 - F0/2
3	Interface F0/3 - F0/5
4	Interface F0/6 - F0/7
5	Interface F0/8
6	Interface F0/9 - F0/11
7	Interface F0/12 - F0/14
8	Interface F0/15 - F0/16
9	Interface F0/17
10	Interface F0/18 - F0/19
101	Interface F0/20
204	Interface F0/21

TABLE A.1 – Association des VLAN à des ports spécifiques

```

Switch(config)#int range f0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#int range f0/3-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 3
Switch(config-if-range)#exit
Switch(config)#int range f0/6-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 4
Switch(config-if-range)#exit
Switch(config)#int f0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 5
Switch(config-if)#exit
Switch(config)#int range f0/9-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 6
Switch(config-if-range)#exit

```

FIGURE A.8 – Association des interfaces à leurs VLAN.

```

Switch(config)#do sh vlan brief
-----+-----+-----+
VLAN Name          Status   Ports
-----+-----+-----+
1   default        active   Fa0/22, Fa0/23, Fa0/24, Gig0/2
2   RH             active   Fa0/1, Fa0/2
3   FinanceEtComptabilite active   Fa0/3, Fa0/4, Fa0/5
4   Juridique      active   Fa0/6, Fa0/7
5   CommunicationEtMarketing active   Fa0/8
6   Securite       active   Fa0/9, Fa0/10, Fa0/11
7   Reseau          active   Fa0/12, Fa0/13, Fa0/14
8   Hosting         active   Fa0/15, Fa0/16
9   DeveloppementWebEtApplication active   Fa0/17
10  HelpDesk        active   Fa0/18, Fa0/19
101 Wifi            active   Fa0/20
204 Directeur      active   Fa0/21
1002 fddi-default   active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default   active
Switch(config)#

```

FIGURE A.9 – Liste des VLAN associés à leurs interfaces.

Après avoir configuré et créé tous nos VLAN, nous passons à la configuration de l'adresse d'assistance pour chaque VLAN depuis le switch niveau 3 afin de permettre aux clients de recevoir une adresse IP dynamique.

```

Switch(config-if)#int vlan 1
Switch(config-if)#ip helper-add 172.28.100.2
Switch(config-if)#
Switch(config-if)#int vlan 2
Switch(config-if)#ip helper-add 172.28.100.2
Switch(config-if)#
Switch(config-if)#int vlan 3
Switch(config-if)#ip helper-add 172.28.100.2
Switch(config-if)#
Switch(config-if)#int vlan 4
Switch(config-if)#ip helper-add 172.28.100.2
Switch(config-if)#
Switch(config-if)#int vlan 5
Switch(config-if)#ip helper-add 172.28.100.2

```

FIGURE A.10 – Configuration de l'adresse d'assistance pour chaque VLAN.

Les requêtes de diffusion des clients DHCP seront transmises au serveur lui-même.

```

Switch(config)#ip routing
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr
Building configuration...
[OK]
Switch#

```

FIGURE A.11 – Configuration du routage entre les différents VLAN depuis le Switch niveau 3.

Après activation du DHCP sur les postes de travail, nous remarquons qu'ils ont reçu une adresse IP dynamique provenant de la plage de leur sous-réseau.

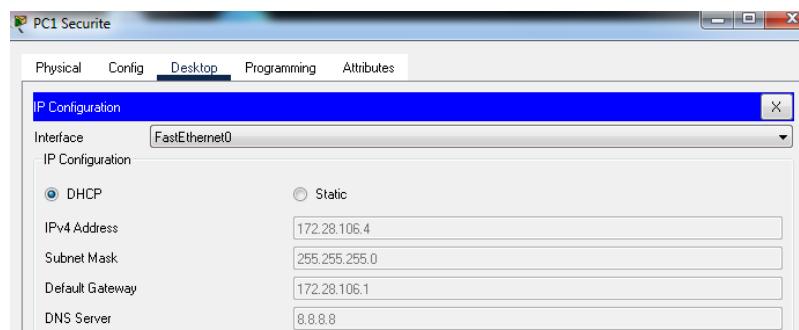


FIGURE A.12 – Activation du DHCP sur le PC1 VLAN 6 du département sécurité.

Dans le PC de la direction juridique, on accède à l'invite de commande via le Desktop puis nous effectuons un ping vers PC1 sécurité. Le ping s'est déroulé avec succès, les deux PC peuvent désormais s'échanger du trafic.

```
C:\>ping 172.28.106.4

Pinging 172.28.106.4 with 32 bytes of data:

Reply from 172.28.106.4: bytes=32 time<1ms TTL=127
Reply from 172.28.106.4: bytes=32 time=23ms TTL=127
Reply from 172.28.106.4: bytes=32 time=1ms TTL=127
Reply from 172.28.106.4: bytes=32 time=17ms TTL=127

Ping statistics for 172.28.106.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 23ms, Average = 10ms
```

FIGURE A.13 – Ping du PC Juridique vers PC1 Sécurité.

A.2 Création des ACL

Tous les départements hors du département système informatique ne peuvent accéder au serveur DHCP. Pour cela nous devons utiliser des ACL étendues pour préciser l'adresse de destination.

N°VLAN	Services	Source	Access Control List	Destination (Serveur DHCP)
2	RH	172.28.102.0	Rejeté	172.28.100.2
3	Finance et Comptabilité	172.28.103.0	Rejeté	172.28.100.2
4	Juridique	172.28.104.0	Rejeté	172.28.100.2
5	Communication et Marketing	172.28.105.0	Rejeté	172.28.100.2

TABLE A.2 – Règles des ACL appliquées aux VLAN.

Avant d'appliquer l'ACL, on effectue un ping depuis le PC juridique vers le serveur DHCP.

```
C:\>ping 172.28.100.2

Pinging 172.28.100.2 with 32 bytes of data:

Reply from 172.28.100.2: bytes=32 time=19ms TTL=127
Reply from 172.28.100.2: bytes=32 time=1ms TTL=127
Reply from 172.28.100.2: bytes=32 time<1ms TTL=127
Reply from 172.28.100.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.28.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 5ms
```

FIGURE A.14 – Ping du PC juridique vers le serveur DHCP avant l'ACL.

On crée une ACL étendue pour chacun des VLAN 2, 3, 4 et 5 en précisant le protocole, l'adresse IP source et destination sur l'interface entrante du Switch niveau 3.

```
Switch(config)#ip access-list extended Juridique-ACL
Switch(config-ext-nacl)#deny ip 172.28.104.0 0.0.0.255 host 172.28.100.2
Switch(config-ext-nacl)#permit ip any any
Switch(config-ext-nacl)#exit

Switch(config)#int vlan 4
Switch(config-if)#ip access-group Juridique-ACL in
Switch(config-if)#exit
```

FIGURE A.15 – ACL étendue pour le VLAN 4 représentant le département juridique.

En tapant la commande "sh access-lists" sur le Switch niveau 3, on voit s'afficher toutes les ACL que nous avons configurées.

```
Switch#sh access-lists
Extended IP access list Juridique-ACL
  10 deny ip 172.28.104.0 0.0.0.255 host 172.28.100.2 (4 match(es))
  20 permit ip any any
Extended IP access list RH-ACL
  10 deny ip 172.28.102.0 0.0.0.255 host 172.28.100.2
  20 permit ip any any
Extended IP access list FC-ACL
  10 deny ip 172.28.103.0 0.0.0.255 host 172.28.100.2
  20 permit ip any any
Extended IP access list CM-ACL
  10 deny ip 172.28.105.0 0.0.0.255 host 172.28.100.2
  20 permit ip any any
```

FIGURE A.16 – Liste des ACL étendues.

Afin de s'assurer que les ACL ont bien été appliquées, nous exécutons un ping depuis l'invite de commande du PC département juridique vers notre serveur. On constate que le PC n'a plus accès à celui-ci.

```
C:\>ping 172.28.100.2

Pinging 172.28.100.2 with 32 bytes of data:

Reply from 172.28.104.1: Destination host unreachable.

Ping statistics for 172.28.100.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

FIGURE A.17 – Ping du PC juridique vers le serveur DHCP après l'ACL.

Annexe B

Présentation de l'organisme d'accueil

B.1 Présentation d'Algérie Télécom

Algérie Télécom est leader sur le marché Algérien des télécommunications qui connaît une forte croissance. Offrant une gamme complète de services de voix et de données aux clients résidentiels et professionnels.

Algérie Télécom, est une société par actions à capitaux publics opérant sur le marché des réseaux et services de communications électroniques. Sa naissance a été consacrée par la loi 2000/03 du 5 août 2000, fixant les règles générales relatives à la poste et aux télécommunications ainsi que les résolutions du conseil national aux participations de l'Etats (CNPE) du 1er Mars 2001 portant création d'une Entreprise Publique Economique dénommée « Algérie Télécom ».

Algérie Télécom est donc régie par cette loi qui lui confère le statut d'une entreprise publique économique sous la forme juridique d'une société par actions SPA au capital social de 50.000.000.000 Dinars et inscrite au centre du registre de commerce le 11 mai 2002. Entrée officiellement en activité à partir du 1er janvier 2003, elle s'engage dans le monde des Technologies de l'Information et de la Communication avec trois objectifs :

- Rentabilité.
- Efficacité.
- Qualité de service.

Son ambition est d'avoir un niveau élevé de performance technique, économique, et sociale pour se maintenir durablement leader dans son domaine, dans un environnement devenu concurrentiel. Son souci consiste, aussi, à préserver et développer sa dimension internationale et participer à la promotion de la société de l'information en Algérie.

B.2 Missions et objectifs de l'entreprise

L'ambition d'Algérie Télécom est d'avoir un niveau élevé de performances techniques, économiques et sociales pour se maintenir durablement comme leader dans son domaine, dans un environnement devenu concurrentiel. Son souci consiste, aussi, à préserver et développer sa dimension internationale et participer à la promotion de la société de l'information en Algérie. L'activité majeure d'Algérie Télécom est de :

- Fournir des services de télécommunications permettant le transport et l'échange de la voix, de messages écrits, de données numériques, d'informations audiovisuelles, et autres.

- Développer, exploiter et gérer les réseaux publics et privés de télécommunications.
- Etablir, exploiter et gérer les interconnexions avec tous les opérateurs des réseaux.

Algérie Télécom est engagée dans le monde des technologies de l'information et de la communication avec les objectifs suivants :

- Accroître l'offre de services téléphoniques et faciliter l'accès aux services de télécommunications au plus grand nombre d'usagers, en particulier en zones rurales.
- Accroître la qualité de services offerts et la gamme de prestations rendues et rendre plus compétitifs les services de télécommunications.
- Développer un réseau national de télécommunications fiable et connecté aux autoroutes de l'information.

Les responsabilités d'Algérie Télécom s'exercent dans les trois domaines suivants :

- Les actionnaires : AT doit mériter leurs soutiens en valorisant leurs patrimoines.
- Les clients : AT doit anticiper leurs besoins en leur fournissant des produits et des services de qualité afin de gagner et de conserver leurs confiances.
- Le personnel : AT doit satisfaire ses attentes en organisant les conditions de l'épanouissement professionnel de chacun car la réussite d'AT dépend de l'engagement de tous.

B.3 Présentation de la structure d'accueil

La Division des Systèmes d'Information (DSI) d'Algérie Télécom est une division de services informatiques, qui a pour mission de fournir à l'entreprise des systèmes d'information de pointes, couvrant l'ensemble de ses activités.

La Division des Systèmes d'Information a pour missions principales :

- Faire évaluer et évoluer l'infrastructure informatique interne de l'entreprise.
- Veiller à la pérennité des applications de gestion et à leur intégration dans le système d'information global de l'entreprise.
- Assurer le support aux utilisateurs des systèmes d'information de l'entreprise et du matériel informatique utilisé (Dans tout le territoire national).
- Gérer et maintenir le tissu informationnel de l'entreprise, en mettant à disposition l'information nécessaire sous tous ses aspects (Archivage, Data base, portails, ainsi que les documents techniques), aux différents acteurs de l'organisation.
- Proposer des solutions et services, dans le domaine des systèmes d'information, pour les clients internes.
- Mettre en place un pôle de compétence, dans les systèmes d'information.

B.4 Organigramme général de l'entreprise

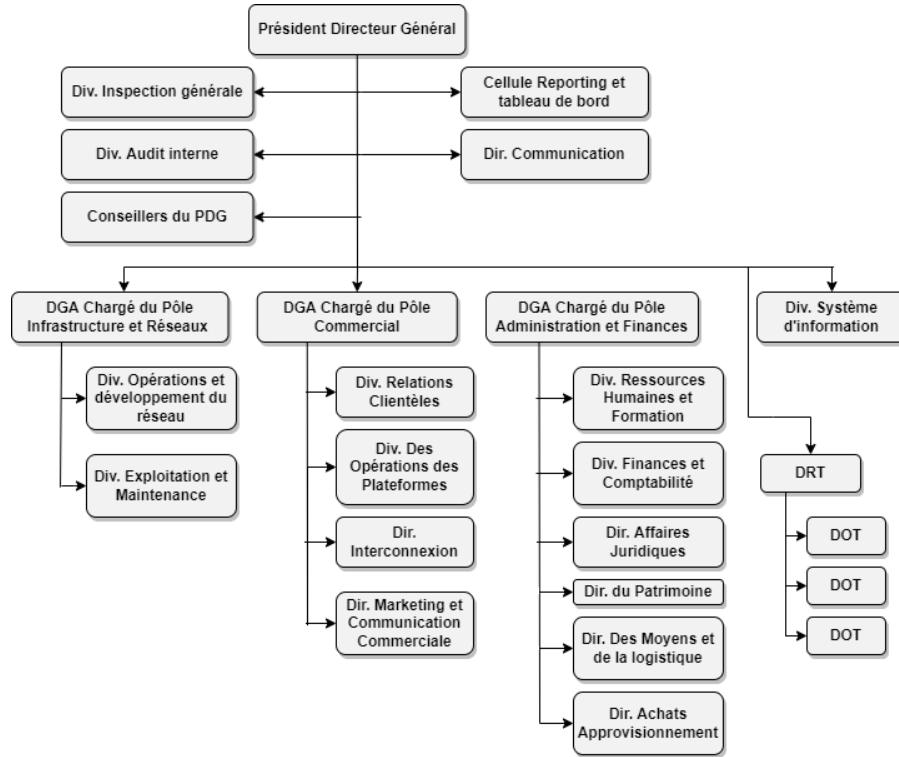


FIGURE B.1 – Organigramme d'Algérie Télécom.

PDG : Président Directeur Général.

DGA : Directeur Général Adjoint.

Div : Division.

Dir : Direction.

DRT : Délégation Régionale des Télécommunications.

DOT : Direction Opérationnelle des Télécommunications.

B.5 Organigramme de la division des systèmes d'information

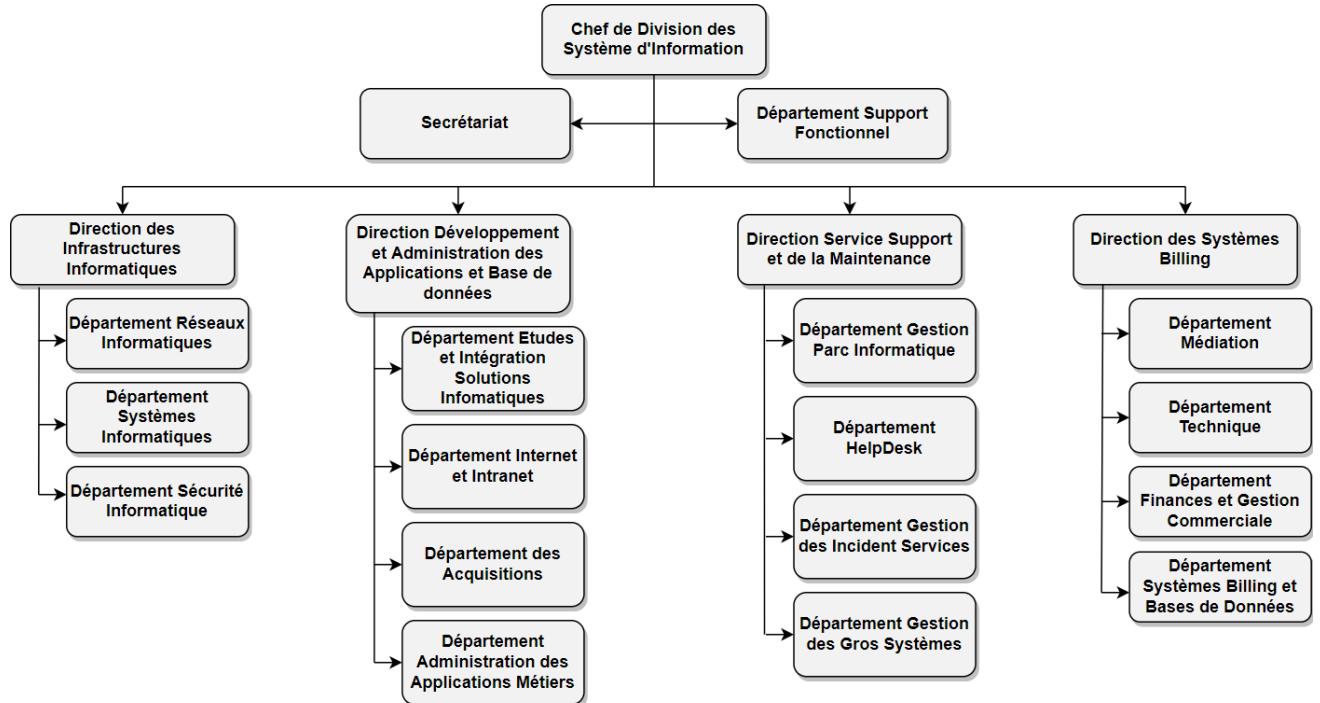


FIGURE B.2 – Organigramme de la division des systèmes d'information.

B.6 Situation Actuelle

Étant le leader des télécommunications en Algérie, Algérie Télécom a l'obligation d'être proche de ses clients et de leur assurer une totale sécurité de leurs informations personnelles (échange de messages, historique de navigation, et autres).

En vue du développement croissant des technologies, les cyberattaques ont elles aussi évoluées, ce qui s'est traduit également par le développement du service de réseau et sécurité d'Algérie Télécom. C'est pour cela, qu'actuellement, l'entreprise occupe toujours la première place et que les clients utilisent leurs services de manière sécurisée.

La direction régionale de M'Sila, n'a pas encore été inaugurée, de ce fait nous simulons actuellement l'implémentation d'une solution de sécurité basée sur un pare-feu.

B.7 Notre Solution

La solution que nous avons envisagée consiste à déployer un pare-feu au niveau de la nouvelle direction régionale de M'Sila d'Algérie Télécom. Dans le cadre de la mise en œuvre de cette solution, nous avons choisi d'utiliser OPNsense comme pare-feu et Odoo en tant qu'ERP.

Les deux sont des solutions open source et gratuites, faciles à trouver sur internet.

Algérie Télécom bénéficiera grâce à ces technologies les avantages suivants :

- La possibilité d'introduire de nouveaux modules correspondants à leurs besoins.
- Un accès à distance grâce à l'outil OpenVPN non disponible sur les technologies propriétaires avec lesquelles ils sont partenaires (Cisco, Fortinet) avec une double authentification.
- La possibilité d'ajouter n'importe quel équipement puisque OPNsense est une solution logicielle qui consomme très peu de ressources.
- La possibilité d'ajouter des paramètres de gestion de la qualité de service tels que le lissage et le marquage du trafic afin de réguler et de contrôler le volume du flux sur un réseau informatique.
- L'équilibrage de charge grâce à sa caractéristique multi-wan.

Résumé

Algérie Télécom, entreprise publique algérienne de télécommunications à caractère commercial, est à la recherche d'une stratégie de sécurité à mettre en oeuvre afin d'élargir son secteur petit à petit sur le territoire algérien de façon à ce que tout citoyen algérien puisse bénéficier des services suggérés par l'entreprise.

Notre projet a pour but, d'étudier les concepts fondamentaux de la cybersécurité notamment les pare-feux dans l'optique de sécuriser la nouvelle direction régionale de M'Sila. Pour ce faire, notre étude se basera sur la mise en place d'un pare-feu et d'un VPN pour la communication inter-sites avec un budget limité.

Après une étude comparative des différentes solutions propriétaires et open source existantes sur le marché, notre travail fût de segmenter les départements de notre direction régionale en plusieurs sous-réseaux, et de limiter l'accès aux ressources à certains employés non privilégiés. De plus, afin de garantir une sécurité supplémentaire, et de permettre aux utilisateurs externes d'accéder à certaines ressources de l'entreprise, nous avons mis en place une DMZ.

Mots clés : VLAN, ACL, pare-feu, open source, VPN, DMZ.

Références

- [1] <https://www.journaldunet.com/solutions/dsi/1508277-la-difference-entre-cybersecurite-et-securite-de-l-information/> Consulté le 19 Avril 2022
- [2] <https://www.jedha.co/blog/cybersecurite-quest-ce-que-la-triade-cia> Consulté le 19 Avril 2022
- [3] <https://thomasjzquel.wordpress.com/2016/12/16/synthese-a-lintention-des-utilisateurs-de-loid-sur-la-securite-dune-sta-de-type-pc/> Consulté le 19 Avril 2022
- [4] <https://www.matrox.com/fr/video/media/guides-articles/top-ip-kvm-security-elements>
Consulté le 19 Avril 2022
- [5] https://www.lemonde.fr/pixels/article/2021/12/13/log4shell-la-faille-de-securite-qui-seme-la-panique-sur-internet_6105907_4408996.html Consulté le 19 Avril 2022
- [6] <https://www.oracle.com/fr/cloud/cyberattaque-securite-reseau-informatique.html>
Consulté le 22 Avril 2022
- [7] <https://www.oracle.com/fr/cloud/cyberattaque-securite-reseau-informatique.html>
Consulté le 22 Avril 2022
- [8] <https://www.kaspersky.fr/resource-center/threats/viruses-worms> Consulté le 19 Avril 2022
- [9] <https://www.avast.com/fr-fr/c-computer-worm> Consulté le 19 Avril 2022
- [10] <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/ransomwares> Consulté le 20 Avril 2022
- [11] <https://ismvsectioninfo.wordpress.com/2018/11/04/le-cheval-de-troie/> Consulté le 20 Avril 2022
- [12] <https://www.avast.com/fr-fr/c-spyware> Consulté le 20 Avril 2022
- [13] <http://tecfetu.unige.ch/staf/staf-j/diego/staf14/ex8/virus.html> Consulté le 20 Avril 2022
- [14] <https://www.futura-sciences.com/tech/definitions/internet-adware-1857/> Consulté le 20 Avril 2022
- [15] <https://www.kaspersky.fr/blog/quest-ce-quun-rootkit/750/> Consulté le 21 Avril 2022

[16] <https://www.techno-science.net/glossaire-definition/Attaque-par-deni-de-service.html>
Consulté le 21 Avril 2022

[17] <https://actualiteinformatique.fr/cybersecurite/definition-dun-attaque-man-in-the-middle>
Consulté le 21 Avril 2022

[18] <https://www.cnil.fr/fr/cnil-direct/question/le-phishing-cest-quoi> Consulté le 24 Avril 2022

[19] <https://www.vadesecure.com/fr/blog/quelle-est-la-difference-entre-le-phishing-et-le-spear-phishing> Consulté le 24 Avril 2022

[20] <https://www.panoptinet.com/cybersecurite-decryptee/cest-quoi-un-drive-by-download.html> Consulté le 24 Avril 2022

[21] <https://www.kaspersky.fr/resource-center/definitions/sql-injection> Consulté le 24 Avril 2022

[22] <https://www.ionos.fr/digitalguide/sites-internet/developpement-web/quest-ce-que-le-xss-cross-site-scripting/> Consulté le 24 Avril 2022

[23] <https://www.manika-consulting.com/infographie-la-cyber-kill-chain-en-7-etapes/>
Consulté le 30 Avril 2022

[24] <https://www.varonis.com/fr/blog/la-chaine-cybercriminelle-en-8-etapes> Consulté le 30 Avril 2022

[25] <https://www.logpoint.com/fr/blog/solution-cybersecurite-definition-importance-avantages> Consulté le 30 Avril 2022

[26] <https://laptop28.com/fr/les-7-principaux-avantages-de-la-cybersecurite-dont-vous-devez-etre-conscient> Consulté le 30 Avril 2022

[27] Saadat Malik. (2002, 15 novembre). Network Security Principles and Practices. Cisco Press.
Consulté le 2 Mai 2022

[28] https://www.cisco.com/c/dam/global/en_ca/solutions/strategy/docs/sbaGov_securityG.pdf Consulté le 2 Mai 2022

[29] <https://www.login-securite.com/2019/02/22/le-pentest-de-a-a-z-methodologie-et-bonnes-pratiques-pour-securiser-son-si/> Consulté le 7 Mai 2022

[30] François-Emmanuel Goffinet. (2020a). Cisco CCNA guide de préparation à l'examen de certification CCNA 200-301 (Vol. 1). Leanpub. Consulté le 7 Mai 2022

[31] <http://cisco.ofppt.info/ccna2/course/module3/3.1.1.3/3.1.1.3.html> Consulté le 7 Mai 2022

[32] <https://www.ciscomadesimple.be/2010/07/08/configuration-dun-trunk-entre-deux-switch/> Consulté le 7 Mai 2022

- [33] <http://www.ismag.ma/wp-content/uploads/2020/03/ACL.pdf> Consulté le 7 Mai 2022
- [34] <https://fr.acervolima.com/difference-entre-le-pare-feu-materiel-et-le-pare-feu-logiciel/> Consulté le 7 Mai 2022
- [35] <https://wikimemoires.net/2012/08/quest-ce-quun-firewall-fonctionnement-et-types-de-firewall/> Consulté le 28 Mai 2022
- [36] <http://tvaira.free.fr/bts-sn/reseaux/cours/cours-reseaux-firewall.pdf> Consulté le 8 Mai 2022
- [37] <https://www.archivesfactory.com/quest-ce-quun-pare-feu-de-nouvelle-generation-renseignez-vous-sur-les-differences-entre-le-ngfw-et-les-pares-feu-traditionnels/> Consulté le 8 Mai 2022
- [38] https://infosecwriters.com/Papers/jwebb_network_demilitarized_zone.pdf Consulté le 8 Mai 2022
- [39] François-Emmanuel Goffinet. (2020a). Cisco CCNA guide de préparation à l'examen de certification CCNA 200–301 (Vol. 1). Leanpub. Consulté le 8 Mai 2022
- [40] Andrew Tanenbaum, David Wetherall. (2014). Réseaux. Dans Réseaux (5ème édition, p. 878-879). Nouveaux Horizons. Consulté le 8 Mai 2022
- [41] <https://www.kaspersky.fr/resource-center/definitions/what-is-a-vpn> Consulté le 8 Mai 2022
- [42] <https://www.ionos.fr/digitalguide/serveur/securite/le-pare-feu-materiel-le-pare-feu-le-plus-robuste/?fbclid=IwAR2Q6Sql90tNrec64B1HHurvdo0HkAb8AoXv4mmaHovp5Z0vGnmpHWUoVzo#:~:text=Un%20pare%2Dfeu%20externe%20est,aussi%20de%20pare%2Dfeu%20mat%C3%A9riel> Consulté le 16 Mai 2022
- [43] <https://geekflare.com/fr/hardware-vs-software-cloud-firewall/> Consulté le 16 Mai 2022
- [44] https://www.ionos.fr/digitalguide/serveur/securite/le-pare-feu-materiel-le-pare-feu-le-plus-robuste/?fbclid=IwAR0Vy4Rm_zCjs3LtcDL8-OcGaAs0uVJJ-EYcHQAfGIFrvjM8sxOoFh5H5ew#:~:text=Un%20pare%2Dfeu%20externe%20est,aussi%20de%20pare%2Dfeu%20mat%C3%A9riel Consulté le 16 Mai 2022
- [45] <https://jo-informatic.bzh/quest-ce-quun-pare-feu/#:~:text=Du%20c%C3%B4t%C3%A9%20des%20inconv%C3%A9nients%2C%20le,un%20professionnel%20en%20la%C3%A9mati%C3%A8re.> Consulté le 16 Mai 2022
- [46] <https://docs.netgate.com/pfsense/en/latest/index.html?fbclid=IwAR3yXRpFTKOh4-FMDwaDmPCPBC5bYNGixu16fALK7aMW81sBmSq73kT97qc> Consulté le 16 Mai 2022
- [47] <https://wiki.ipfire.org/configuration/firewall?fbclid=IwAR01TU4DUN3Wz1eIzdvAlaV5gYIyRpxHFvF4UAVTuvHh1ukYnlR4vaolUAs> Consulté le 18 Mai 2022

- [48] https://www.cisco.com/c/dam/global/fr_fr/assets/pdfs/c45-736624-00_cisco_firepower_next-generation_firewall_aag_v4a_fr_fr.pdf Consulté le 16 Mai 2022
- [49] <https://docs.fortinet.com/product/fortigate/7.2> Consulté le 16 Mai 2022
- [50] https://docs.opnsense.org/?fbclid=IwAR3LKTD1-EfmvH2HssBO2gAHj2VU5BzTdcqzCBAUN8oBWW6d_zG9iVuBjuA Consulté le 18 Mai 2022
- [51] <https://www.eve-ng.net/> Consulté le 23 Mai 2022
- [52] <https://www.gns3.com/software> Consulté le 23 Mai 2022
- [53] <https://www.netacad.com/fr/courses/packet-tracer> Consulté le 23 Mai 2022
- [54] <https://www.virtualbox.org/> Consulté le 23 Mai 2022
- [55] <https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html>
Consulté le 23 Mai 2022
- [56] <https://azure.microsoft.com/fr-fr/> Consulté le 23 Mai 2022
- [57] <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview> Consulté le 23 Mai 2022
- [58] <https://bitnami.com/> Consulté le 25 Mai 2022
- [59] https://www.odoo.com/fr_FR Consulté le 25 Mai 2022
- [60] <https://www.sunnyvalley.io/docs/opnsense> Consulté le 25 Mai 2022