République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté de la Technologie

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Thème

Etude et mise en place d'une nouvelle infrastructure réseau sécurisée

Préparé par :

- BEDACHE Celia
- DAHMANE Chahrazed

Dirigé par :

M. BESSAAD Omar

Examiné par :

M.ATMANI(P)

M.DIBOUNE

Année universitaire : **2023/2024**

Dédicace

C'est avec une profonde gratitude que je dédie ce travail :
À mes chers parents, pour leur amour inconditionnel, leur soutien constant, et leur confiance qui ont éclairé mon chemin tout au long de mes études.
À mes frères Hani, Fares, et Yacine, dont la présence et l'affection inébranlables ont été une source d'inspiration et de force quotidienne. À mes sœurs Nouria et Samira, pour leur amour, leurs encouragements, et les moments de joie partagés qui ont illuminé mon parcours. À ma cousine Chaima, pour ses conseils avisés, son soutien constant, et son amitié précieuse, qui m'ont guidé à chaque étape de ce projet. À tous mes amis, pour leur amitié sincère et leur soutien indéfectible, rendant ce voyage académique plus agréable et enrichissant.
Et tout particulièrement, à ma binôme Chahrazed, pour son dévouement, sa collaboration, et son soutien tout au long de ce travail. Sa persévérance et son esprit d'équipe ont été essentiels à la réussite de ce projet.

Celia

Dédicace

je dédie ce modeste travail à mes parents, dont le soutien inconditionnel et les encouragements constants ont été ma principale source de motivation.
A mes chers frères Yahia, Fodil, Alilo, et Rayan, ainsi qu'à mes chères sœurs Fahima, Fadila, Nacira, Siham, Warda, et Kafo. Votre soutien indéfectible, vos encouragements constants et votre amour m'ont donné la force de persévérer. Un hommage exceptionnel est adressé à Syrine, Dania, et Yasser.
Et tout particulièrement, à mes amis Rania, Rima, Dabi, et Melkhir qui ont partagé ce parcours avec moi, et également a ma binôme Celia.

Chahrazed

Remerciements

Nous souhaitons avant tout exprimer notre profonde gratitude à Dieu le Tout-Puissant pour nous avoir accordé la force, la volonté et la connaissance nécessaires à l'accomplissement de ce travail.

Nous adressons nos remerciements les plus sincères à notre encadrant, M. O. Bessaad, pour ses précieux conseils et ses encouragements constants tout au long de notre projet. Son soutien et son expertise ont été essentiels à la réalisation de ce travail.

Nous tenons également à remercier chaleureusement les membres du jury pour avoir accepté d'évaluer notre projet. Nous leur témoignons toute notre reconnaissance et notre respect profond.

Nos remerciements vont également à notre encadrant de stage, M. Y. Djebbari, pour son accueil chaleureux, son suivi rigoureux et ses conseils avisés durant toute notre période de stage pratique.

Nous exprimons notre gratitude infinie à nos familles, en particulier à nos parents, frères et sœurs, pour leur soutien inébranlable, leurs encouragements et leur aide précieuse tout au long de ce travail.

Nous souhaitons également remercier tous nos amis et collègues qui nous ont soutenus, en particulier ceux qui ont été présents à chaque étape de notre projet.

Enfin, nous tenons à exprimer notre profonde reconnaissance à toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ce projet. Leurs conseils, leur soutien et leurs encouragements ont été d'une valeur inestimable tout au long de notre parcours.

Table des matières

Table des figures

Liste des Abréviations

ACL : Access Control List

DDoS : Déni de Service Distribué

DoS : Déni de Service

VPN : Réseau Privé Virtuel (Virtual Private Network)

IDS : Système de Détection d'Intrusion (Intrusion Detection System)

IPS : Système de Prévention d'Intrusion (Intrusion Prevention System)

SSL : Secure Sockets Layer

TLS : Transport Layer Security

IPSec : Internet Protocol Security

IAM : Identity and Access Management

WAF : Web Application Firewall

API : Application Programming Interface

DNSSEC : Domain Name System Security Extensions

AES : Advanced Encryption System

DevOps : Development and Operations

GNS3 : Graphical Network Simulator

LAN : Local Area Network

WAN : Wide Area Network

HTTP : Hypertext Transfer Protocol

HTTPS : Hypertext Transfer Protocol Secure

SQL : Structured Query Language

API : Application Programming Interface

WAF : Web Application Firewall

DHCP : Dynamic Host Configuration Protocol

PC : Personal Computer

LAN : Local Area Network

WAN : Wide Area Network

TCP/IP : Transmission Control Protocol/Internet Protocol

OSI : Open Systems Interconnection

RIP : Routing Information Protocol

BGP : Border Gateway Protocol

OSPF : Open Shortest Path First

DSL : Digital Subscriber Line

MAC : Media Access Control

DNS : Domain Name System

ICMP : Internet Control Message Protocol

TCP/IP : Transmission Control Protocol/Internet Protocol

HTTP : HyperText Transfer Protocol

SMTP : Simple Mail Transfer Protocol

UDP : User Datagram Protocol

IP : Internet Protocol

ARP : Address Resolution Protocol

UDP : User Datagram Protocol

IGP : Interior Gateway Protocol

Introduction Générale

Dans le paysage technologique en constante évolution d'aujourd'hui, la sécurité des réseaux informatiques est devenue une préoccupation majeure pour les organisations du monde entier. Avec la prolifération des cybermenaces sophistiquées et la valeur croissante des données numériques, la nécessité de concevoir et de mettre en place des infrastructures réseau sécurisées est plus critique que jamais.Dans le contexte actuel où les cyberattaques sont de plus en plus fréquentes ce travail explore l'actualité brûlante de la sécurité réseau, en proposant des solutions pour faire face aux défis contemporains de la cybersécurité et à la mise en oeuvre de stratégies efficaces.

Ce mémoire se concentre sur l'étude et la mise en place d'une nouvelle infrastructure réseau sécurisée pour répondre aux besoins spécifiques d'une organisation donnée. Comment peut-on concevoir une infrastructure réseau sécurisée qui minimise les points de défaillance critiques, améliore la performance, réduit les failles de sécurité et assure une gestion efficace des accès et des segments de réseau ?

Au cœur de ce projet se trouve la compréhension des principes de base de la sécurité des réseaux, des menaces potentielles auxquelles les systèmes sont confrontés et des meilleures pratiques pour les contrer. En intégrant des mécanismes de défense en profondeur, des politiques de sécurité robustes et des technologies de pointe telles que les pare-feu, les VPN et les protocoles de sécurité réseau, nous visons à créer un environnement réseau sûr et fiable.

En outre, ce mémoire examinera les défis spécifiques rencontrés lors de la mise en œuvre d'une nouvelle infrastructure réseau sécurisée, y compris la gestion des ressources, la formation du personnel et l'adaptation aux exigences réglementaires et de conformité.

Ce mémoire propose une analyse et une approche pratique pour créer des infrastructures réseau sécurisées adaptées aux besoins des organisations modernes, afin qu'elles puissent évoluer en toute confiance dans un environnement numérique en constante évolution.

Chapitre 1

Concepts de base sur les réseaux informatiques

1.1 Introduction

Dans un monde de plus en plus connecté les réseaux informatiques jouent un rôle vital en facilitant la communication et l'échange d'information à travers le monde depuis leurs débuts modestes jusqu'à leur omniprésence dans tout les aspects de notre vie quotidienne, les réseaux informatique ont transformé la manière dont nous interagissons avec la technologie et entre nous. dans cette introduction, nous explorerons les concepts de base des réseaux informatiques, allant de la structure fondamentale des réseaux à leur fonctionnement interne en passant par les technologies et protocoles qui les sous-tendent, en comprenant ces concepts nous pourrons mieux appréhender l'importance et l'impact des réseaux informatiques dans notre société moderne.

1.2 Les réseaux informatiques

1.2.1 Définition d'un réseau informatique

Un réseau est un moyen de communication qui permet à des individus ou à des groupes de partager des informations et des services. La technologie des réseaux informatiques constitue l'ensemble des outils qui permettent à des ordinateurs, des serveurs et des équipements réseaux de partager des informations et des ressources, ces appareils sont reliés par des câbles physiques, des connexions sans fil ou une combinaison des deux et utilisent des protocoles de communication standardisés pour échanger des données de manière efficace et sécurisée. Les réseaux informatique peuvent être de différentes tailles, allant des réseaux locaux(LAN) aux réseaux étendus(WAN) qui couvrent de vaste régions géographiques.

1.2.2 Importances des réseaux dans les communications modernes

Les réseaux informatiques sont d'une importance capitale dans les communications modernes offrant une connectivité mondiale inégalée grâce à des infrastructures comme Internet. Cette connectivité permet aux individus, aux entreprises et aux organisations de communiquer et de partager des informations en temps réel quel que soit leur emplacement géographique favorisant ainsi la collaboration à distance et la gestion de projet à l'échelle mondiale, de plus les réseaux offrent un accès instantané à une vaste quantité d'informations et de ressources en

ligne, soutenant l'apprentissage continu, la résolution de problèmes et le maintien d'une veille informationnelle. en facilitant le commerce électronique, la transmission de média variés et l'innovation technologique et transforme ainsi la façon dont nous interagissons, travaillons et vivons dans le monde numérique d'aujourd'hui.[27]

1.3 Topologies de réseau

Plusieurs types de topologies peuvent exister dans l'entreprise en fonction des contraintes géographiques ou liées au débit et à la sécurité, chacune ayant ses propres caractéristiques, avantages et inconvénients, ces topologies incluent notamment :

1.3.1 La topologie en étoile

Dans les réseaux informatiques, la topologie en étoile est couramment utilisée, où tous les appareils sont connectés à un nœud central, souvent un commutateur. Ce commutateur achemine les données vers leur destination, soit en les diffusant à tous les autres ports(dans le cas d'un hub), soit en les transmettant uniquement au destinataire spécifique(dans le cas d'un switch). Les câbles utilisés pour connecter les appareils au commutateur sont des paires torsadées, comportant généralement 4 paires de fils, et munis de connecteurs RJ45 à leurs extrémités.[28]

FIGURE 1.1 – Topologie en étoile
[28]

Les avantages :

- Ajout facile des postes.
- Localisation facile des pannes.
- Débranchement d'une connexion ne paralyse pas le reste du réseau.
- Simplicité éventuelle des équipements au niveau des nœuds.
- C'est le concentrateur qui est intelligent.
- Évolution hiérarchisée du matériel possible, on peut facilement déplacer un appareil sur le réseau.[28]

Les inconvénients :

- Si le concentrateur est défectueux, tout le réseau est en panne.
- Utilisation de routeur ou switch afin de pouvoir communiquer entre différents réseaux ou ordinateur.[28]

1.3.2 La topologie en bus

La topologie en bus est une architecture de réseau où les appareils sont connectés à un seul câble partagé. Bien qu'elle soit simple et peu coûteuse, elle peut poser des problèmes de collision de données lorsque plusieurs appareils tentent de transmettre simultanément. Elle utilise CSMA/CD (Carrier Sense Multiple Access with Collision Detection) pour gérer l'accès au réseau. Bien qu'elle ait été largement utilisée pour sa simplicité et son faible coût, elle est moins adaptée aux réseaux importants d'aujourd'hui et est généralement utilisée pour connecter un petit nombre d'appareils dans des environnements domestiques ou de petite échelle.[28]

FIGURE 1.2 – Topologie en bus
[28]

Les avantages :

- Facile à mettre en œuvre.
- Utilisable pour des réseaux temporaires.
- Présente l'un des coûts de mise en réseau le plus bas.[28]

Les inconvénients :

- Longueur du câble et nombre de stations limités.
- Un câble coupé peut interrompre le réseau.
- Les coûts de maintenance peuvent être importants à long terme.
- Les performances se dégradent avec l'ajout de stations.
- Faible sécurité des données transitant sur le réseau (toutes les stations connectées au bus peuvent lire toutes les données transmises sur le bus).[28]

1.3.3 La topologie en anneau

Cette topologie est principalement utilisée par les réseaux Token Ring qui utilise la technique d'accès par jeton.

La topologie en anneau implique que toutes les machines sont connectées dans une boucle fermée. Les données circulent dans une seule direction, chaque ordinateur communiquant à tour de rôle. Le jeton détermine quelle machine peut émettre à un moment donné, transféré à chaque machine successivement. Cette topologie est active car chaque machine régénère le signal électrique, assurant ainsi la continuité de la communication dans l'anneau.[28]

FIGURE 1.3 – La topologie en anneau
[28]

Les avantages :

- La quantité de câble nécessaire est réduite.
- Le protocole est simple, il évite la gestion des collisions.
- Taux d'utilisation de la bande passante optimum.
- Fonctionne mieux qu'une topologie de bus sous une lourde charge de réseau
- Il est assez facile à installer et à reconfigurer, car ajouter ou retirer un matériel nécessite de déplacer seulement deux connexions.[28]

Les inconvénients :

- Le déplacement, l'ajout et la modification machines connectées peuvent affecter le réseau. [28]

1.3.4 La topologie maillé

Le réseau maillé est une topologie où tous les hôtes sont connectés directement les uns aux autres, formant un réseau en forme de filet. Chaque nœud doit recevoir, envoyer et relayer les données, ce qui évite les points sensibles et assure la connectivité même en cas de panne d'un nœud. Les réseaux maillés utilisent plusieurs chemins de transfert entre les nœuds pour garantir la disponibilité des données en cas de défaillance d'un nœud. Elle utilise le temps de rétention(THT) garantir une qualité de service élevée et assurer une communication fiable. Cette architecture est largement utilisée dans Internet, notamment dans les réseaux étendus (WAN), assurant ainsi la stabilité en cas de panne d'un nœud.

Le réseau Internet est basé sur une topologie maillée (sur le réseau étendu « WAN », elle garantit la stabilité en cas de panne d'un nœud).[28]

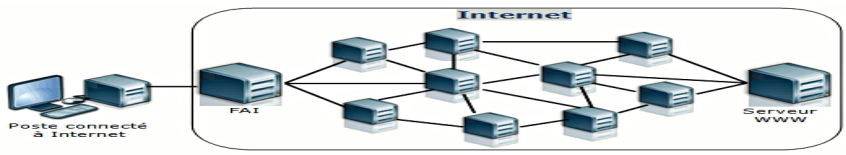


FIGURE 1.4 – La topologie maillé
[28]

Les avantages :

- Garantie d'une meilleure stabilité du réseau en cas d'une panne du nœud.
- Offre une sécurité des plus fiable et une performance inégalée.

- Une panne au niveau d'un poste en particulier n'empêche pas les autres stations de communiquer entre eux.[28]

Les Inconvénients :

- Les ressources nécessaires sont énormes que ce soit en matière d'équipement de connexion ou de câblage.[28]

1.4 Composants d'un réseau

1.4.1 Matériel réseau

Le matériel réseau constitue l'infrastructure fondamentale qui soutient les communications modernes, tant sur les réseaux locaux que sur internet comprend des équipements tels que les routeurs, les commutateurs, les pare-feu, les concentrateurs et les câbles utilisés pour connecter et interconnecter des appareils dans un réseau informatique, ils jouent un rôle crucial dans la communication en facilitant le transfert de données entre les appareils connectés. Ces dispositifs permettent le routage efficace des données, la gestion du trafic, la sécurisation des réseaux ainsi une communication fluide et fiable entre les utilisateurs on trouves notamment : [27]

Les câbles

Les câbles réseau constituent le support physique qui permet aux appareils de communiquer au sein d'un réseau informatique ils transportent des signaux électrique ou optiques qui permettent la transmission des données entre les appareils Il existe plusieurs types standard des câbles de réseau, câble coaxial, câble à paire torsadée, câble USB, câble croisé, câble de raccordement, câble à fibre optique, etc. Ces câbles sont disponible dans différentes catégories et qui offrant des vitesses et des performances variées.[13]

Les routeurs

Les routeurs contribuent à transmettre des paquets vers leurs destinations en traçant un chemin dans l'océan des équipements réseau interconnecter, à l'aide de différentes topologies de réseau, les routeurs sont des appareils universels qui interconnecter deux ou plusieurs réseaux hétérogènes ils constituant la colonne vertébrale des grands réseaux informatiques comme Internet ils sont votre première ligne de défense et doivent être configurés de manière à ne transmettre que le trafic autorisé par les administrateurs réseau. Les routages eux-mêmes peuvent être configurés comme statiques ou dynamiques ils communiquent généralement les informations de routage et autres en utilisant l'un des trois protocoles standard : le protocole d'informations de routage(RIP), le protocole de passerelle frontière(BGP) ou le chemin le plus court ouvert en premier(OSPF).[13]

Les commutateurs(Switch)

Un commutateur est un dispositif multiport qui améliore l'efficacité du réseau, il gère des informations de routage limitées sur les nœuds du réseau interne et permet des connexions à des systèmes tels que les concentrateurs ou les routeurs, l'utilisation de commutateurs améliore

l'efficacité du réseau par rapport aux concentrateurs ou aux routeurs, en raison de leur capacité à créer des circuits virtuels par conséquence ils améliorent également la sécurité du réseau, un commutateur peut opérer soit sur la couche liaison de données, soit sur la couche Réseau du modèle OSI.

Un commutateur multicouche est un commutateur qui peut fonctionner sur les deux couches, ce qui signifie qu'il peut servir à la fois de commutateur et de routeur. Il est un équipement hautes performances prenant en charge les mêmes protocoles de routage que les routeurs.[13]

Le concentrateur(hub)

Le concentrateur est le plus simple de la famille des équipements de connexion réseau, car il connecte des composants LAN ayant des protocoles identiques ils ne remplissent pas de fonctions de filtrage ou d'adressage de paquets, ils envoient simplement des paquets de données à tous les appareils connectés. Les concentrateurs opèrent au niveau de la couche Physique du modèle OSI. Il existe deux types de concentrateurs : à port simple et multiport.[13]

Les serveurs

Un serveur est une machine physique qui est connectée à un réseau et qui stocke des données et effectue diverses opérations en réponse à une requête qui offre des services à différents clients. Les services les plus courants sont :

> Le partage de fichier.

> L'accès aux informations du World Wide Web.

> Le courrier électronique.

> Le commerce électronique.

> Le stockage en base de données.

> Le jeu et la mise à disposition des logiciels applicatifs sur le réseau, il existe plusieurs serveurs spécifiques on trouve le serveur DNS, le serveur Web, le serveur DHCP... etc. [27]

Les modems

Les modems(modulateurs-démodulateurs) servent à transmettre des signaux numériques via des lignes téléphoniques analogiques. Les signaux numériques sont donc convertis par le modem en signaux analogiques de différentes fréquences et transmis à un autre modem au lieu de réception. Le modem récepteur effectue la transformation inverse et fournit une sortie numérique au dispositif qui y est connecté, généralement un ordinateur. Les données numériques sont habituellement transférées depuis le modem via une liaison série et une interface standard RS-232. De nombreuses compagnies téléphoniques offrent des services DSL et de nombreux câblo-opérateurs utilisent des modems comme terminaux finaux pour l'identification et la reconnaissance des utilisateurs individuels. Les modems opèrent à la fois sur la couche physique et liaison de donnée.[13]

1.4.2 Logiciel réseau

Les logiciels réseaux sont un ensemble diversifié d'outils logiciels conçus pour répondre aux besoins variés des réseaux informatiques modernes, cela comprend les protocoles de communication qui définissent les règles et les formats pour l'échange d'information ainsi que les systèmes d'exploitation réseau qui fournissent des fonctionnalités spécifiques pour la gestion et

le contrôle des ressources réseaux ainsi que des pare-feu pour la sécurité, des serveurs de messagerie pour la communication, des outils de surveillance réseau pour la gestion des performances et bien d'autres encore.[27]

Les protocoles

Afin d'échanger des données de manière structurée au sein d'un réseau, il faut avoir recours à des règles qui commandent le déroulement des communications : les protocoles, on distingue généralement deux grands types de protocoles : les protocoles routables et les protocoles non routables. Un protocole routable, comme le protocole IP, peut acheminer ses paquets de données vers un routeur. Plusieurs autres protocoles fonctionnent sur IP pour faciliter la communication et le transfert de données sur Internet, on trouve les protocoles de transport qui sont le protocole TCP qui garantit la livraison des données dans l'ordre et sans erreurs et le protocole UDP qui permet l'envoi de datagramme sans garantie de livraison ou l'ordre. Les protocoles d'adressage comme le protocole ARP qui est utilisé pour mapper une adresse ip à une adresse MAC et les protocoles de routages comme RIP, OSPF, BGP et d'autre protocoles comme ICMP, DHCP, DNS ...ect, et des protocoles non routable, il est encore le protocole par défaut des réseaux Microsoft sous Windows 95 et 98.[14]

Passerelle(gateway)

Les passerelles assurent la connexion entre deux ou plusieurs réseaux autonomes, chacun ayant ses propres algorithmes de routage, protocoles, topologies, services de noms de domaine, procédures et politiques d'administration réseau. La passerelle sert de point d'entrée et de sortie entre deux réseaux distincts, elle traduit les protocoles de communication d'un réseau pour qu'ils soient compréhensibles par un autre réseau.[13]

Les systèmes d'exploitation réseau

Sont des systèmes conçus spécifiquement pour gérer les fonctions et les ressources d'un réseau informatique ils offrent des fonctionnalités telle que la gestion des connexions réseaux et d'autre services liés à la connectivité et à la communication entre les ordinateurs et les périphériques du réseau, certains exemples de systèmes d'exploitation réseau comprennent Windows Servsr, Linux(avec des distributions comme Ubuntu server ou CentOS), macOS Server, des solutions spécialisées comme Cisco IOS pour les équipements réseau Cisco.[27]

Les Pare-feu

Un pare-feu(firewall), est un système permettant de protéger un ordinateur, ou un réseau d'ordinateurs, des intrusions provenant d'un réseau tiers (notamment Internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau.[1]

1.5 Modèles de référence

1.5.1 Modèle OSI

Le modèle OSI, développé par l'ISO décrit une architecture en sept couches pour l'interconnexion des systèmes ouverts. Chaque couche a des fonctions spécifiques et communique avec les autres couches selon des relations verticales et horizontales. L'organisation en couches permet une modularité et une indépendance des différentes parties du système, favorisant ainsi la flexibilité et la maintenance des réseaux. Chaque couche offre des services à la couche supérieure en utilisant les services de la couche inférieure, assurant ainsi une interopérabilité entre les composants du réseau. De plus, le modèle OSI a joué un rôle important dans la standardisation des protocoles de communication, facilitant ainsi l'interopérabilité entre les équipements réseau. Il offre également une abstraction des détails l'implémentassions et facilite le débogage et la maintenance en permettant l'isolation des problèmes à une couche spécifique sans perturber le fonctionnement des autres couches.

La communication entre couches adjacentes utilise la notion d'encapsulation des données où chaque couche ajoute un en-tête à l'émission qui sera retiré à la réception (extraction de la donnée), la couche N utilise la couche N-1 et fournit des services à la couche N+1.[5]

7	Couche Application
6	Couche Présentation
5	Couche Session
4	Couche Transport
3	Couche Réseau
2	Couche Liaison de données
1	Couche Physique

FIGURE 1.5 – Modèle OSI
[28]

1.5.2 Modèle TCP/IP

TCP/IP(Transmission Control Protocol/Internet Protocol) désigne communément une architecture réseau qui s'est imposée comme modèle de référence en lieu et place du modèle OSI. Cela tient tout simplement à son histoire. En effet, contrairement au modèle OSI, le modèle TCP/IP est né d'une implantation, la normalisation est venue ensuite, cet historique fait toute la particularité de ce modèle, ses avantages et ses inconvénients. Par conséquent, la segmentation en couches indépendantes d'OSI n'est pas présente de façon aussi stricte dans TCP/IP. Le modèle TCP/IP permet simplement de positionner les protocoles existants et futurs dans un cadre théorique, le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentassions la plus courante, ces couches sont représenté dans la figure suivante :[5]

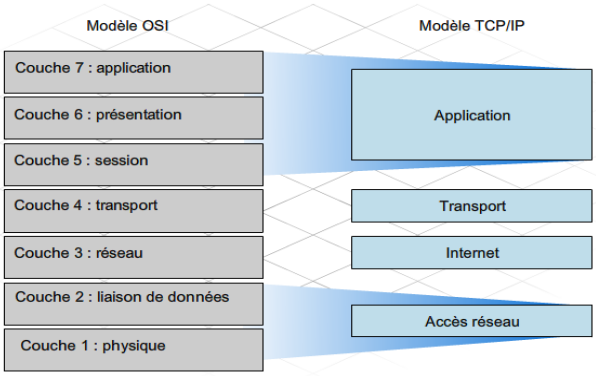


FIGURE 1.6 – Le modèle TCP/IP vs Le modèle OSI
[11]

1.6 Protocole réseau

1.6.1 Protocole de transport(TCP, UDP)

Le protocole TCP

Le protocole TCP(Transmission Control Protocol) est un des principaux protocoles de la couche transport du modèle TCP/IP, il permet au niveau des applications de gérer les données en provenance(ou à destination) de la couche inférieure du modèle(c'est-à-dire le protocole IP) lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP en fixant le champ protocole à 6(pour savoir que le protocole en amont est TCP) TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission.

Les caractéristiques principales du protocole TCP sont les suivantes :

- TCP permet de remettre en ordre les datagrammes en provenance du protocole IP.
- TCP permet de vérifier le flot de données afin d'éviter une saturation du réseau.
- TCP permet de formater les données en segments de longueur variable afin de les remettre au protocole IP.
- TCP permet de multiplexer les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources(application par exemple) distinctes sur une même ligne.
- TCP permet enfin l'initialisation et la fin d'une communication. [29]

Le protocole UDP

Le protocole UDP est basé en couche 4 du modèle OSI, il n'ouvre pas de session et n'effectue pas de contrôle d'erreur il est alors appelé mode non connecté il est peu fiable, cependant il permet aux applications d'accéder directement à un service de transmission de datagrammes rapide, UDP est utilisé pour transmettre de fiables quantités de données ou le coût de la création de connexions et du maintien de transmissions fiables s'avèrent supérieur aux données à émettre.[29]

1.6.2 Protocoles d'adressage(IP, ARP)

Le protocole IP

Internet Protocole IP est un protocole de communication de réseau informatique par commutation de paquets, IP est un protocole de niveau 3 du modèle OSI et du modèle TCP/IP permettant un service d'adressage unique pour l'ensemble des terminaux connectés, les adresses IP existent en deux versions principales : IPv4 et IPv6. Le protocole IP utilise des routeurs pour transmettre les paquets de données entre différents réseaux.

IP est considéré comme étant un protocole non-fiable car il n'offre aucune garantie pour les paquets envoyés pour aucun des points suivants :

- Corruption de donnée.
- Ordre d'arrivée des paquets (un paquet A peut être envoyé avant un paquet B, mais le paquet B peut arriver avant le paquet A).
- Perte ou destruction de paquet.
- Ré-émission des paquets en cas de non-réception.

En terme de fiabilité, le seul service offert par IP est de s'assurer que les en-tête des paquets transmis ne comportent pas d'erreurs grâce à l'utilisation de somme de contrôle (cheksum) si l'en-tête d'un paquet comprend une erreur, son ckecksum ne sera pas valide et le paquet sera détruit sans être transmis, en cas de destruction de paquets aucune notification n'est renvoyée à l'expéditeur.

La raison principale de cette absence de gestion de la fiabilité au niveau IP est la volonté de réduire le niveau de complexité des routeurs et ainsi de leur permettre de disposer d'une plus grande rapidité, l'intelligence est alors dépotée vers les points d'extrémités su réseau.[29]

Le protocole ARP

Le protocole ARP fonctionne à la couche 3 du modèle OSI, mais il est souvent considéré comme un protocole de "couche 2 et demi" en raison de son rôle de liaison entre les adresses IP et les adresses MAC. Il permet de faire correspondre une adresse IP à une adresse MAC, ce qui est essentiel pour la communication sur un réseau Ethernet.

Lorsqu'un appareil souhaite communiquer avec un autre sur un réseau Ethernet, il envoie une requête ARP pour demander la correspondance entre l'adresse IP du destinataire et son adresse MAC. Cette requête ARP est diffusée à tous les appareils du réseau et celui qui possède l'adresse IP demandée répond avec son adresse MAC.

La table ARP, également appelée cache ARP, est un élément crucial du fonctionnement du protocole ARP. Elle stocke les correspondances entre adresses MAC et adresses IP vues sur le réseau ou résolues via des requêtes ARP. Cela permet d'accélérer les échanges futurs en évitant de reproduire une requête ARP à chaque fois. Cependant, la table ARP est sujette à des attaques de type ARP spoofing, où des appareils malveillants tentent de falsifier les entrées de la table pour détourner le trafic réseau. Pour se protéger contre de telles attaques, diverses techniques de sécurisation ARP sont utilisées, telles que la surveillance constante de la table ARP et l'utilisation de la validation des entrées ARP.[30]

1.6.3 Protocole de routage

Le protocole RIP

Le protocole RIP (Routing Information Protocol) est conçu pour faciliter la gestion des informations de routage au sein des réseaux autonomes, qu'il s'agisse de réseaux locaux (LAN) ou de réseaux étendus d'entreprise (WAN). En utilisant RIP, les routeurs échangent régulièrement leurs tables de routage avec leurs voisins, assurant ainsi une mise à jour constante du réseau.

La simplicité de RIP en fait un choix attractif pour les petits réseaux, mais sa cadence de mise à jour, toutes les 30 secondes, peut engendrer une charge de trafic significative. De plus, sa limitation à 15 sauts en fait un protocole moins adapté pour les réseaux de grande envergure.

Il existe deux versions du protocole RIP pour le routage IPv4 : RIP v1 et RIP v2. Tandis que RIP v1 utilise la diffusion UDP pour transmettre les mises à jour des tables de routage, RIP v2 adopte la multidiffusion pour une distribution plus efficace des informations de routage.[27]

Le protocole OSPF

Le protocole OSPF (Open Shortest Path First) a été conçu par l'IETF pour répondre au besoin d'un protocole de routage intérieur (IGP) dans la pile des protocoles TCP/IP. Contrairement à RIP, OSPF est non-propriétaire et offre des fonctionnalités avancées.Il permet à chaque routeur de connaître l'ensemble des réseaux au sein d'une zone, ce qui élimine le besoin de limiter le nombre de sauts.

OSPF utilise le multicast pour envoyer ses mises à jour d'état de lien, réduisant ainsi la bande passante utilisée. Ces mises à jour ne sont envoyées qu'en cas de changement de topologie, ce qui économise encore plus de bande passante. De plus, OSPF offre une convergence plus rapide que RIP car les changements de routage sont propagés instantanément et de manière incrémentielle grâce aux relations de voisinage entre les routeurs.[15]

Le protocole BGP

Le Border Gateway Protocol(BGP) joue un rôle crucial dans la stabilisation du réseau Internet en facilitant l'échange d'informations sur les chemins de routage disponibles ou défaillants. Agissant à la fois en tant que protocole de passerelle extérieur(eBGP) et de passerelle intérieur(iBGP), il confère une stabilité accrue aux réseaux en permettant aux routeurs de s'adapter de manière flexible en cas de panne et de sélectionner d'autres chemins de routage logiques disponibles via BGP.

BGP est essentiel pour router et gérer les échanges de données entre les systèmes autonomes. Cependant, cette importance s'accompagne de vulnérabilités. De plus, les routeurs BGP peuvent rencontrer des problèmes de service ou des erreurs BGP, notamment en raison d'informations incorrectes ou incomplètes, de limitations de mémoire, ou de mises à jour trop lentes. Ces vulnérabilités exigent une vigilance particulière en matière de sécurité réseau pour garantir le bon fonctionnement du BGP et la stabilité du réseau Internet.[27]

1.7 Classes d'adresses IP

Pour acheminer les paquets, les routeurs doivent déterminer où envoyer chaque paquet reçu. Plus spécifiquement, les routeurs doivent déterminer pour chaque paquet reçu, l'adresse du prochain routeur et le port de sortie par lequel sera réexpédié le paquet. Ces deux informations

sont appelées « informations de routage » Le routeur prend l'adresses IP de destination d'un paquet et cherche dans sa table de routage les informations de routage, cette opération s'appelle consultation d'adresse IP(address lookup).

Une adresse IP(Internet Protocol) est une étiquette numérique attribuée à un appareil connecté à un réseau informatique, permettant son identification et sa communication avec d'autres appareils sur le réseau. Chaque adresse IP est composée de quatre octets, soit 32 bits, séparés par des points, et peut être représentée en notation décimale pointée (par exemple, 192.168.1.1).

Il existe deux types d'adresses IP :

- Adresse IP publique : Identifie un appareil sur Internet, permettant aux informations de circuler entre cet appareil et d'autres appareils connectés à Internet. Ces adresses sont uniques et attribuées par les fournisseurs d'accès à Internet(FAI).

- Adresse IP privée : Utilisée à l'intérieur d'un réseau privé pour établir des connexions sécurisées entre les appareils du réseau. Ces adresses ne sont pas routables sur Internet et sont souvent utilisées dans les réseaux domestiques et d'entreprise. Une adresse IP est divisée en deux parties :

Préfixe : Aussi appelé adresse réseau, il identifie le réseau physique auquel l'ordinateur est connecté. Il détermine la portion du réseau à laquelle appartient l'adresse IP.

Suffixe : Aussi appelé adresse d'hôte, il identifie l'ordinateur individuel sur le réseau. Il détermine la partie spécifique de l'adresse attribuée à chaque appareil sur le réseau.

L'adressage IP comprend cinq classes : A, B, C, D et E. Les classes A, B et C sont utilisées pour attribuer des adresses à des réseaux de différentes tailles, tandis que la classe D est réservée pour le multicast(communication de groupe) et la classe E est réservée à des fins expérimentales.[16]

FIGURE 1.7 – Classes d'adresses IP
[16]

1.7.1 Notion de sous-réseaux et de masque de sous-réseau

Le sous-réseau

Un sous-réseau est un espace d'adresses IP qui est divisé en espaces d'adresses plus petits. Le sous-réseau devient ainsi une partie d'un réseau dans lequel toutes les adresses IP utilisent la même adresse réseau, si tous les sous-réseaux sont connectés à un routeur, un grand réseau général peut être créé.

Les sous-réseaux sont utilisés lorsque la charge du réseau doit être réduite et mieux distribuée, dans ce cas, plusieurs adresses IP sont regroupées au sein d'un sous-réseau, les paquets de données ne doivent pas traverser plusieurs stations jusqu'à ce que l'adresse souhaitée soit atteinte, tout ce dont vous avez besoin, c'est de l'adresse réseau, par conséquent, les sous-réseaux sont utilisés chaque fois que plusieurs hôtes ou périphériques doivent être connectés à un réseau élargi.[27]

Le masque de sous-réseau

Un masque de sous-réseau est un nombre de 32 bits qui se présente sous la forme de uns et de zéros et s'écrit de la même manière qu'une adresse IP, les routeurs utilisent des masques réseau pour acheminer les paquets de données au bon endroit.[27]

1.8 Technologie réseau

1.8.1 Ethernet

Ethernet est défini comme une technologie de mise en réseau qui inclut le protocole, le port, le câble et la puce informatique nécessaires pour connecter un ordinateur de bureau ou un ordinateur portable à un réseau local(LAN) pour une transmission rapide des données via des câbles coaxiaux ou à fibre optique.[17]

Son fonctionnement

Le protocole Ethernet utilise une topologie en étoile ou bus linéaire, qui constitue la base de la norme IEEE 802.3. Dans la structure du réseau OSI, ce protocole fonctionne à la fois sur la couche physique et sur la couche liaison de données. Ethernet divise la couche de connexion de données en deux couches distinctes : le niveau de contrôle de liaison logique et également le niveau de contrôle d'accès au support(MAC). Ethernet utilise un mécanisme d'accès connu sous le nom de CSMA/CD(Carrier Sense Multiple Access/Collision Detection) pour permettre à chaque ordinateur d'écouter la connexion avant de transmettre des données sur le réseau.

Une connexion Ethernet englobe les éléments suivants :

1- Le protocole Ethernet : Il s'agit d'une série de normes qui régissent la manière dont les données sont envoyées.

2-Le port Ethernet : Les ports Ethernet(communément appelés jacks ou sockets) sont des ouvertures sur l'infrastructure réseau informatique dans les quelles on peut brancher des câbles Ethernet. Il prend en charge les câbles dotés de connecteurs RJ-45. Le connecteur Ethernet présent sur la majorité des ordinateurs sert à connecter l'équipement à une connexion filaire. Le port Ethernet d'un ordinateur est lié à un adaptateur réseau Ethernet, également appelé carte Ethernet, monté sur la carte mère. Un routeur peut contenir de nombreux ports Ethernet pour prendre en charge divers périphériques réseaux câblés.

3- Adaptateur réseau Ethernet : Un adaptateur Ethernet est une puce ou une carte qui s'insère dans un emplacement de la carte mère et permet à un ordinateur de se connecter à un réseau local(LAN). Dans le passé, ceux-ci étaient toujours utilisés avec des ordinateurs de bureau. Ethernet est désormais intégré aux chipsets des cartes mères d'ordinateurs portables et de bureau.

4-Un câble Ethernet : Un câble Ethernet, souvent appelé câble réseau, relie votre ordinateur à un modem, un routeur ou un commutateur réseau. Le câble Ethernet se compose de la connexion RJ45, du câblage interne et d'une gaine en plastique.[17]

Ces Normes

Les premières normes Ethernet définies prennent en charge un débit de données de 10 mégabits par seconde(Mbps). Ajours'hui, de nombreuses variantes du 802.3 sont utilisées.

3 - 10BASE5 : Câble coaxial à fils épais avec une longueur de câble maximale de 500 mètres. Ceci est basé sur le processus CSMA/CD.

3a - 10BASE2 : Câble coaxial à fil fin utilisant des connecteurs à baïonnette Neill-Concelman(BNC), avec une longueur de câble maximale de 185 mètres.

3i - 10BASE-F : Câbles Ethernet à fibre optique.

3i - 10BASE-T : Fil téléphonique à paire torsadée ordinaire qui utilise des câbles à paire torsadée non blindée (UTP) comme couche physique et des câbles à fibre optique comme support de transmission. Des variantes supplémentaires incluent IEEE 802.3u et 100BASE-TX.

3b - 10BROAD36 : Câble coaxial multicanal haut débit avec une longueur de segment maximale de 3 600 mètres.

3x - Full-Duplex : fournit un contrôle de flux et inclut le cadrage DIX. Le « 10 » dans la désignation du type de support fait référence à la vitesse de transmission de 10 Mbps.

Le «BASE» fait référence à la signalisation en bande de base, ce qui signifie que seuls les signaux Ethernet sont transportés sur le support(ou, avec 10BROAD36, sur un seul canal dans un câble partagé). [18]

1.8.2 NAT avec le PAT

également connu sous le nom de NAT surchargé (NAT Overload), est une extension du NAT qui utilise non seulement les adresses IP mais aussi les numéros de port Il permet à plusieurs appareils sur un réseau local d'utiliser une seule adresse IP publique, tout en gardant des connexions distinctes en utilisant des ports différents. Chaque connexion sortante est identifiée de manière unique par une combinaison d'adresse IP et de numéro de port.[27]

1.9 Services réseau

1.9.1 DNS(Domain Name System)

Le système DNS(Domain Name Service) est un protocole essentiel du réseau, associé au protocole TCP/IP standard. Il permet la résolution des noms d'ordinateurs en adresses IP et vice versa. Le DNS est un rôle serveur installable via le Gestionnaire de serveur ou PowerShell. Il est automatiquement configuré avec Active Directory pour localiser les contrôleurs de domaine. Le service client DNS est inclus dans toutes les versions de Windows et interroge les serveurs DNS pour localiser les contrôleurs de domaine et résoudre les noms d'ordinateurs. Le protocole DNS est intégré à la suite de protocoles TCP/IP, occupant une place cruciale dans la couche d'application du modèle de référence TCP/IP.[20]

Types de services DNS :

Un DNS officiel est le principal gestionnaire d'un domaine, responsable de la mise à jour des noms publics dans le DNS. Il répond aux serveurs DNS récursifs en fournissant les adresses IP correspondantes aux noms demandés.[19]

Un service DNS récursif agit comme un intermédiaire entre les clients et les serveurs DNS officiels. Il ne possède pas ses propres enregistrements DNS mais peut obtenir les informations pour les clients. Il répond aux requêtes en consultant sa propre cache ou en les transmettant aux serveurs DNS officiels pour obtenir les informations nécessaires.[19]

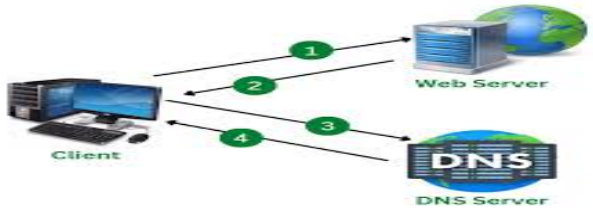


FIGURE 1.8 – Fonctionnement de serveur DNS
[24]

1.9.2 Protocole DHCP(Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol(DHCP) est un protocole client/serveur qui fournit automatiquement à un hôte sur un réseau TCP/IP son adresse IP et d'autres informations de configuration associées telles que le masque de sous-réseau et la passerelle par défaut.

Un serveur DHCP gère la distribution des adresses IP et des configurations associées. Sans DHCP, la configuration manuelle des adresses IP est fastidieuse et sujette aux erreurs. DHCP simplifie ce processus en attribuant dynamiquement les adresses IP aux clients lors de leur connexion au réseau, ces avantages incluent une configuration sans erreur, une administration réseau réduite et une gestion efficace des changements d'adresse IP pour les appareils mobiles. Les adresses qui ne sont plus utilisées sont automatiquement renvoyées au pool pour ré-allocation.[20]

1.10 Administration et gestion des réseau

1.10.1 Configuration et maintenance des équipements réseaux

configuration des équipements réseaux : Cela implique la mise en place initiale des équipements, tels que les routeurs, commutateurs, pare-feu..etc pour assurer qu'il fonctionnent correctement selon les besoins du réseau, cela comprend la configuration des adresses IP, des protocoles de routage, des listes de contrôle d'accès(ACL) des VLAN...etc. Elle implique d'abord d"accéder à l'interface de configuration que ce soit par une connexion directe ou distante pour configurer le nom les adresses IP manuellement ou bien avec le service DHCP, les masques de sous-réseau les VLANs, les protocoles de routage pour les routeurs...etc.

la configuration des services réseau tels que le NAT(Network address translation) pour permettre à plusieurs hôtes d'accéder à internet.

il est important de noter que la configuration des équipements réseaux peut varier en fonction du type d'équipements et des besoins spécifiques du réseau. [27]

Maintenance des équipements réseau : La maintenance d'un réseau informatique garantit la bonne installation et l'efficacité de fonctionnement du réseau informatique, en optimisant sa durée, et en réduisant les pannes et les risques de rupture de façon préventive. En fait, en cas de panne brusque, le réseau informatique sera restauré sans perdre de données, elle assure le suivi des évolutions du réseau pour permettre son ajustement, ainsi la maintenance doit faire la mise à jour de ses paramètres relatifs aux derniers changements, en fonction des utilisations, des applications et des matériels, ainsi que de ses besoins en serveurs.[27]

1.11 Application des réseaux

1.11.1 Internet et ses services

Internet est un réseau planétaire qui rassemble tous les réseaux(publics ou privés, de recherche ou commerciaux ...) fonctionnant sous le modèle de référence TCP/IP, et développé initialement pour les échanges entre scientifiques, plusieurs outils sont disponibles pour permettre la recherche(localisation) et la diffusion de documents sur le réseau Internet, ils peuvent être classés en différentes catégories selon leur objectif :

X.500 Son utilisation dans des applications courantes est très souvent limitée à des fonctions d'annuaire de type Pages Blanches (annuaires classés par pays). On peut y accéder facilement par le client WWW, Mosaic.

Les" News" sont un forum d'échanges d'informations sur des sujets divers diffusés à tous les abonnés, fonnant ainsi un réseau nommé USENET. Mais elles n'ont pas une durée de vie infmie.

Le service FTP anonyme est l'un des services proposé sur Internet il permet de transférer des fichiers entre deux stations.

WAIS est un ensemble de logiciels du domaine public qui permettent d'interroger des bases de données (ou sources d'information) et de retrouver ainsi des documents et des informations spécialisées (listing des sites ftp, bases de données du génome, ...) localisés sur des serveurs distants.

Gopher est un outil d'exploration, de recherche et de récupération de documents disponibles sur Internet.

World Wide Web est encore appelé WWW ou W3. W3 destiné à aider les utilisateurs à s'orienter dans Internet. il utilise des liens entre des documents qui peuvent être n'importe où sur Interne, Les documents référencés peuvent être accessibles par différents protocoles (HTTP, FTP, GOPHER ...). Ainsi ce service peut être utilisé si le domaine de recherche n'est pas vraiment délimité car il inclut tous les précédents. [22]

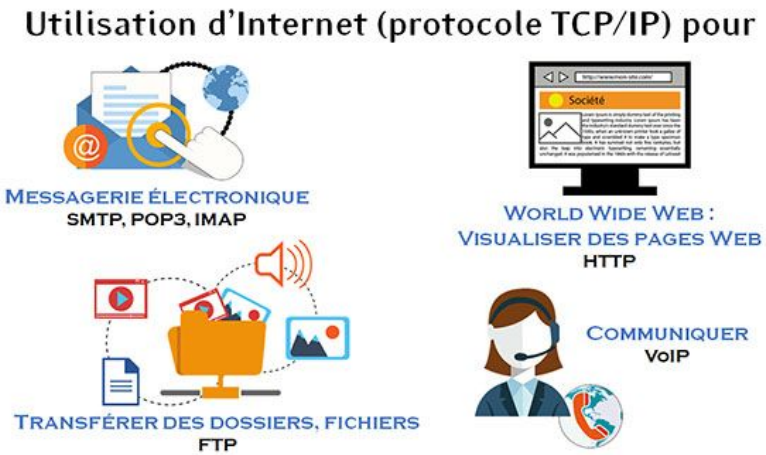


FIGURE 1.9 – Utilisation d'Internet
[23]

1.11.2 Internet et Extranet

L'intranet et l'extranet sont des réseaux http qui utilisent la même technologie mais ont des finalités distinctes,comme un site web standard un intranet ou un extranet reposent généralement sur une architecture sur 3 niveaux composée :

De clients(navigateur internet généralement).

D'un ou plusieurs serveurs d'application(middleware).

D'un serveur de bases de données(MySQL ou autre).

L'intranet est un réseau à usage privé d'un groupe par exemple, les employés d'une entreprise, le codage du réseau permet qu'il ne soit pas accessible par Internet afin de protéger les données de la communauté utilisatrice, par contre L'extranet est un réseau qui rend accessible le système d'information d'une entreprise à ses collaborateurs lorsqu'ils sont en dehors de l'entreprise. L'accès à l'extranet se fait par une authentification, l'extranet est accessible via le réseau public Internet dans les deux cas on peut développer l'intranet et l'extranet avec des technologies OpenSource (CMS ou frameworks PHP Symfony, Laravel) ou avec des outils propriétaires comme Sharepoint de Microsoft.[26]

1.12 Évolutions et Tendances

1.12.1 Réseau définis par logiciel(SDN)

Les solutions de réseaux définis par logiciel SDN gèrent dynamiquement le trafic réseau. Elles utilisent l'intelligence pour optimiser les performances. Par conséquent, elles réduisent considérablement les coûts, il est important de comprendre que cette approche simplifie la gestion du réseau. Elle facilite la mise à jour, le test ou même la surveillance de la sécurité de votre réseau, quel que soit le matériel sous-jacent, il existe 4 architectures SDN chacune fonctionne différemment et offre des avantages différents.

Open SDN : Le SDN ouvert utilise des protocoles logiciels libres tels que OpenFlow pour contrôler et acheminer le trafic réseau.

API SDN : permettant une gestion et un contrôle centralisés du réseau à travers des interfaces standardisées et programmables.

Modèle de superposition SDN : Modèle de superposition Le SDN crée des tunnels pour faire fonctionner plusieurs réseaux distincts au-dessus du réseau existant.

Modèle hybride SDN : Un modèle hybride Le SDN combine le SDN et les réseaux traditionnels comme une étape vers le SDN, ce qui signifie qu'il permet une transition graduelle.

Les fonctionnalités des réseaux définis par logiciel SDN permettent aux ingénieurs de réacheminer instantanément les réseaux en cas de panne, une fois qu'une anomalie a été détectée, les SDN agissent rapidement pour détourner le trafic réseau suspect vers les pare-feu et les systèmes de détection des intrusions et ils garantissent la fiabilité tout en réduisant les coûts de matériel.[25]

1.12.2 Service-Oriented Architecture(SOA)

SOA (Service-Oriented Architecture) est une méthode de conception informatique où les applications sont construites comme des services distincts et autonomes, disponibles via des interfaces standardisées. Chaque service effectue une fonction spécifique et peut être utilisé et réutilisé dans différents contextes métier, favorisant ainsi l'interopérabilité et la réduction des

redondances. SOA encourage la modularité en décomposant les fonctionnalités complexes en services plus simples, facilitant ainsi la gestion et la maintenance des systèmes. Elle repose sur des principes de flexibilité, d'agilité et de réduction des coûts en permettant une réponse rapide aux changements commerciaux et une intégration harmonieuse des systèmes hétérogènes à travers l'utilisation de protocoles de communication standard comme HTTP, XML, et SOAP.[27]

1.12.3 Internet des objets(IoT)

L'Internet des Objets, ou IoT, implique la connexion d'objets physiques à Internet, ainsi que la mise en réseau de ces objets. En substance, l'IoT permet à pratiquement tout élément capable de transmettre des données sur un réseau de se connecter entre eux.

Les objets connectés à l'IoT peuvent recueillir des données sur leur environnement grâce à des capteurs, les traiter via des processeurs intégrés, puis les transmettre à des destinataires via leur propre matériel de communication. Ces données sont souvent partagées à travers une passerelle IoT, facilitant la communication entre les appareils ou entre ces appareils et le cloud.

Quelques exemples d'IoT qui transforment notre quotidien comprennent les maisons intelligentes équipées de thermostats et de chaudières connectées, de systèmes d'éclairage intelligents et d'appareils électroniques contrôlables à distance via des appareils mobiles ou des ordinateurs. De même, les voitures connectées améliorent le confort et la sécurité des conducteurs grâce à des fonctionnalités telles que la climatisation, le contrôle de vitesse, la surveillance de la batterie et de la pression des pneus, le suivi de l'emplacement du véhicule, ainsi que l'automatisation de l'ouverture des portes de garage ou des portails.[27]

1.13 Conclusion

Les concepts de base des réseaux informatique constituent les fondations essentielles pour comprendre le fonctionnement et la gestion de ces systèmes interconnecter qui jouent un rôle crucial dans notre monde modernes, en explorant des éléments tels que les topologies réseaux les protocoles de communication, les adresses IP le modèle OSI, nous avons acquis une compréhension approfondie des principes fondamentaux qui sous-tendent la connectivité et l'échange d'informations à l'échelle mondiale.

Chapitre 2

La sécurité des réseaux informatiques

2.1 Introduction

Dans ce chapitre nous allons introduire la sécurité des réseaux informatiques, nous explorerons les principaux concepts, défis et solutions liés à la protection des réseaux informatiques. ainsi que les meilleures pratiques pour concevoir et mettre en œuvre des stratégies de sécurité efficaces.

2.2 La sécurité des réseaux

2.2.1 Définition

La sécurité informatique englobe les stratégies et technologies(des mesures de prévention, de détection et de réponse aux incidents de sécurité) qui protègent les systèmes, réseaux et données contre les menaces potentielles. Elle vise à assurer la confidentialité, l'intégrité et la disponibilité des informations en prévenant les accès non autorisés, les altérations et les pertes de données. [7]

2.2.2 Importance de la sécurité des réseaux dans les environnements informatiques actuels

La sécurité des réseaux revêt une importance cruciale dans les environnements informatiques actuels pour plusieurs raisons :

Protection des données sensibles :

Les réseaux informatiques transportent et stockent souvent des données sensibles, telles que des informations personnelles, des données financières ou des secrets commerciaux. La sécurité des réseaux est essentielle pour protéger ces données contre les accès non autorisés, les fuites ou les manipulations.[7]

Prévention des cyberattaques :

Les réseaux sont des cibles de choix pour les cyberattaques, telles que les attaques par déni de service(DDoS), les intrusions malveillantes ou les ransomwares. Une sécurité réseau

robuste permet de détecter et de contrer ces attaques, réduisant ainsi les risques d'interruption des services ou de compromission des données.[7]

Garantie de la continuité des opérations :

Dans un monde où la connectivité est essentielle pour les entreprises, la sécurité des réseaux est cruciale pour maintenir la disponibilité et la fiabilité des systèmes informatiques. En protégeant les réseaux contre les interruptions et les dommages, la continuité des opérations commerciales est assurée.[7]

Conformité réglementaire :

De nombreuses réglementations et normes en matière de protection des données exigent des entreprises qu'elles mettent en place des mesures de sécurité appropriées pour protéger les informations personnelles et sensibles. Une sécurité réseau efficace permet de se conformer à ces exigences légales et réglementaires.[7]

Protection de la réputation et de la confiance des clients :

Les incidents de sécurité, tels que les violations de données, peuvent entraîner une perte de confiance des clients et nuire à la réputation d'une entreprise. En investissant dans la sécurité des réseaux, les organisations démontrent leur engagement envers la protection de la confidentialité et de la sécurité des données de leurs clients.[7]

2.3 Menaces et attaques réseau

2.3.1 Malware

Un malware, ou logiciel malveillant, est un programme informatique conçu pour s'introduire dans un système sans autorisation et causer des dommages en volant des données, perturbant le fonctionnement normal de l'ordinateur ou du réseau. Les malwares peuvent prendre diverses formes telles que des virus, des chevaux de Troie, des spywares et des vers. Leur objectif peut être le vol de données sensibles, le chiffrement de fichiers pour demander une rançon(ransomware) ou le sabotage. Pour se protéger contre les malwares, il est essentiel d'adopter des pratiques de sécurité solides, d'utiliser des solutions de sécurité avancées telles que les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS), et de rester vigilants face aux menaces en ligne.[9]

2.3.2 Ingénierie sociale :

Techniques exploitant des erreurs humaines pour accéder à des informations ou services. Cela inclut le phishing (par e-mail) et le smishing (via SMS), représentant une part significative des brèches de sécurité dans divers secteurs comme la finance et la technologie.[10]

2.3.3 DDOS

Une attaque par déni de service (DoS, Denial of Service) vise à rendre les services ou ressources d'une organisation indisponibles pour une durée indéterminée. Généralement dirigées

contre les serveurs d'une entreprise, ces attaques empêchent leur utilisation et leur consultation. Lorsqu'un déni de service implique plusieurs machines, on parle de déni de service distribué (DDoS, Distributed Denial of Service). Les attaques DDoS les plus connues incluent Tribal Flood Network (TFN) et Trinoo.[1]

2.3.4 IP spoofing

L'usurpation d'adresse IP (également appelé mystification ou spoofing IP) est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis. La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu).[1]

2.3.5 Injection SQL

Les attaques par injection de commandes SQL sont des attaques visant les sites web s'appuyant sur des bases de données relationnelles. Dans ce type de sites, des paramètres sont passés à la base de données sous forme d'une requête SQL. Ainsi, si le concepteur n'effectue aucun contrôle sur les paramètres passés dans la requête SQL, il est possible à un pirate de modifier la requête afin d'accéder à l'ensemble de la base de données, voire d'en modifier le contenu. En effet, certains caractères permettent d'enchaîner plusieurs requêtes SQL ou bien ignorer la suite de la requête. Ainsi, en insérant ce type de caractères dans la requête, un pirate peut potentiellement exécuter la requête de son choix.[1]

2.4 Principes de base de la sécurité réseau

2.4.1 Confidentialité

La confidentialité se réfère à la pratique de protéger les informations sensibles et privées contre l'accès ou la divulgation non autorisés. Les entités peuvent être des sites, organisations, personnes, . . . etc[2]

2.4.2 Intégrité :

Assurer que les informations n'ont pas été modifiées (ou altérées) par des entités non autorisées ou inconnues. Généralement, l'intégrité est appliquée sur des données en transmission.[2]

2.4.3 Disponibilité :

S'assurer que les ressources informatiques et les données sont accessibles lorsque nécessaire et que les services restent opérationnels, même face à des incidents ou des attaques. La disponibilité garantit que les utilisateurs peuvent accéder aux systèmes et aux informations sans interruption indue.[2]

2.4.4 non-répudiation :

Est un principe de sécurité informatique assurant qu'une personne ou une entité ne peut pas nier l'origine ou l'envoi d'une communication ou d'une action, ni contester l'exactitude des informations échangées. Cela est crucial dans les environnements nécessitant une preuve fiable de l'authenticité et de l'intégrité des transactions.[2]

2.4.5 Modéle de défense en profondeur

Le modèle de défense en profondeur est une stratégie de sécurité informatique qui vise à protéger les réseaux et les systèmes informatiques en superposant plusieurs couches de sécurité. Cette approche permet de compenser les failles de chaque couche individuelle et de ralentir les attaquants, ce qui leur rend plus difficile d'atteindre leurs objectifs.[7]

Contrôle d'accès

Le contrôle d'accès permet de restreindre l'accès aux ressources du réseau en fonction de l'identité et des droits des utilisateurs. Cela peut être réalisé par le biais de solutions telles que les mots de passe, les certificats numériques, les listes de contrôle d'accès (ACL) et les firewalls.[7]

Protection du périmètre

La protection du périmètre vise à protéger le réseau contre les intrusions externes. On implémentant des solutions telles que les firewalls, les systèmes de détection d'intrusion(IDS) et les systèmes de prévention d'intrusion(IPS).[7]

Segmentation du réseau

consiste à diviser le réseau en plusieurs segments afin de limiter l'impact d'une attaque. Cela permet de confiner une attaque à un seul segment et d'empêcher sa propagation à l'ensemble du réseau.[7]

Sécurité des terminaux

La sécurité des terminaux vise à protéger les ordinateurs portables, les tablettes et les smartphones contre les malwares et les autres menaces. Cela peut être réalisé par le biais de solutions telles que les antivirus, les anti-spywares et les solutions de gestion des terminaux mobiles(MDM).[7]

Surveillance et détection

La surveillance et la détection permettent de détecter les intrusions et les attaques en temps réel. Cela peut être réalisé par les systèmes de détection d'intrusion (IDS), les systèmes de prévention d'intrusion(IPS) et les solutions de surveillance du réseau.[7]

Réponse aux incidents

C'est le processus qui permet de répondre à une attaque et de minimiser ses dommages. Cela inclut des mesures telles que la restauration des données, la correction des vulnérabilités et la poursuite des auteurs.[7]

2.5 Technologies de sécurité réseau

2.5.1 Pare-feu

Définition

Un pare-feu (firewall), est un système permettant de protéger un ordinateur, ou un réseau d'ordinateurs, des intrusions provenant d'un réseau tiers (notamment Internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit

ainsi d'une passerelle filtrante comportant au minimum les inter- faces réseau suivantes :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.

Le système pare-feu est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. [1]

Zone démilitarisée (DMZ)

Les systèmes pare-feu (firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entre- prises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de cloisonnement des réseaux. Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, serveur de messagerie, serveur Astirisk public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de zone démilitarisée pour désigner cette zone isolée hébergeant des applications mises à disposition du public.[1]

LAN (Réseau Local) :

Le pare-feu contrôle et sécurise les communications internes au sein du LAN, garantissant que seules les communications autorisées et sécurisées peuvent avoir lieu entre les différents appareils et serveurs.[27]

WAN (Réseau Étendu) :

En se plaçant entre le LAN et le WAN, le pare-feu surveille et filtre le trafic entrant et sortant du réseau local vers l'Internet, assurant que seuls les paquets autorisés par la politique de sécurité peuvent passer.[27]

2.5.2 VPN

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet. Cette technologie, de plus en plus utilisée dans les entreprises, permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente pour les utilisateurs concernés. Les données envoyées

au travers de ces liaisons virtuelles sont chiffrées, ceci garantit aux utilisateurs d'un VPN qu'en cas d'interception malveillante, les données soient illisibles.[3]

Intérêt

L'utilisation des VPN offre de nombreux avantages aux entreprises, parmi eux :

- Ils rendent notre connexion Internet privée, anonyme et protégée. Ils permettent aussi de masquer notre adresse IP sur internet .
- Ils laissent la possibilité de construire des réseaux overlay (ou réseaux superposés,réseau informatique bâti sur un autre réseau) .
- Le faible coût de l'accès à Internet, que ce soit à haut débit ou via une ligne téléphonique. [3]

Protocoles de sécurité réseau

SSL/TLS

SSL(Secure Sockets Layer) et TLS(Transport Layer Security) sont deux protocoles de sécurité qui chiffrent les communications sur Internet pour assurer la confidentialité, l'authentification et l'intégrité des données échangées entre deux parties. TLS est une version améliorée et plus sécurisée de SSL, mais les deux sont largement utilisés pour sécuriser les transactions en ligne et les échanges de données sensibles.[7]

IPsec

IPSec est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI. Il assure la confidentialité (grâce au cryptage), l'authentification (qui permet d'être certain de l'identité de l'émetteur) et l'intégrité des données permettant de s'assurer que per sonne n'a pu avoir accès aux informations.

IPSec permet de protéger les données et également l'en-tête d'une trame, en masquant le plan d'adressage grâce à l'ajout d'un en-tête IPSec à chaque datagramme IP. IPSec de par sa position, agit sur chaque datagramme IP et permet ainsi d'offrir une protection unique pour toutes les applications. [7]

Protocoles associés

- **ISAKMP**(Internet Security Association and Key Management Protocol) consiste à définir des procédures et des formats de paquets pour établir, négocier, modifier et supprimer des associations de sécurité entre deux extrémités IPsec.

  Une association de sécurité est une relation entre deux entités de réseau qui garantit les ser vices de sécurité pour le trafic généré. Elle définit l'ensemble des opérations IPSec devant être appliquées aux paquets.
- **IKE**(Internet Key Exchange) est un protocole non connecté opérant sur UDP (port500), au niveau de la couche Application. Il est chargé de négocier la connexion en se basant sur le protocole ISAKMP. Avant qu'une transmission IPsec puisse être possible, IKE est utilisé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clés partagées.

- **AH**(Authentication Header) fournit l'intégrité et l'authentification. Il authentifie les paquets en les signant, ce qui assure l'intégrité de l'information. Une signature unique est créée pour chaque paquet envoyé et empêche que l'information soit modifiée3.
- **Le protocole ESP (Encapsulating Security Payload)** il assure la confidentialité, l'intégrité et l'authentification des données en les encapsulant dans un en-tête de sécurité. Il chiffre les données en utilisant un cryptage asymétrique, avec des algorithme de chiffrement comme AES (Advanced Encryption Standard) ou 3DES(Triple Data Encryption Standard). AES est particulièrement populaire en raison de sa robustesse et de sa vitesse, tandis que 3DES est moins utilisé en raison de sa lenteur relative. Pour garantir l'intégrité des données, on utilise SHA (Secure Hash Algorithm) pour créer un HMAC (Hash-based Message Authentication Code), ce HMAC est ensuite ajouté aux paquets IP encapsulés pour assurer leur intégrité lors de la transmission à travers le tunnel sécurisé d'IPsec.[8]

2.5.3 Les mécanismes de prévention et détection d'attaques

IDS(Intrusion Detection System)

est un système qui détecte les attaques sur un client ou sur un réseau le plus tôt possible. Si l'IDS rencontre un trafic de données inhabituel pendant son analyse, il envoie un avertissement à l'administrateur.[7]

IPS(Intrusion Prevention System)

désigne un système qui a pour rôle de non seulement détecter et signaler les attaques potentielles, mais aussi les neutraliser par des contre-mesures actives. IPS utilise également des capteurs hôtes et réseau pour évaluer les données système et les paquets réseau.[7]

2.6 Sécurisation des périphériques réseau

2.6.1 Configuration sécurisée des périphériques réseau

Assurer une configuration sécurisée des périphériques réseau est une étape essentielle pour réduire les risques liés aux attaques et garantir l'intégrité du réseau. Voici quelques mesures et des exemples pour chaque point :[7]

Modifier les mots de passe par défaut

Les mots de passe par défaut des périphériques réseau sont souvent bien connus des pirates informatiques, ce qui les rend vulnérables aux attaques. Il est crucial de les modifier dès la mise en service du périphérique et d'utiliser des mots de passe forts et uniques. Par exemple, utiliser des combinaisons de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.[7]

Activer le chiffrement des données

Le chiffrement des données garantit que les informations transitant sur le réseau sont illisibles pour toute personne non autorisée. Par exemple, utiliser des protocoles comme WPA2 ou WPA3

pour sécuriser les réseaux sans fil, et le chiffrement SSL/TLS pour sécuriser les communications sur Internet.[7]

Mettre en place un pare-feu

Un pare-feu permet de filtrer le trafic réseau en autorisant uniquement le flux de données légitime. Il peut être matériel ou logiciel, et configuré pour bloquer le trafic malveillant.[7]

Désactiver les services non utilisés :

Les services inutilisés peuvent représenter des vulnérabilités potentielles et augmenter la surface d'attaque du réseau. Par exemple, désactiver les ports et les protocoles qui ne sont pas nécessaires à l'activité réseau normale.[7]

Mettre à jour le firmware

Les fabricants publient régulièrement des mises à jour du firmware pour corriger les failles de sécurité et améliorer les performances des périphériques réseau. Il est important de maintenir ces périphériques à jour en installant les dernières versions du firmware dès leur disponibilité on vérifie régulièrement les sites web des fabricants pour les annonces de mises à jour du firmware et les appliquer dès que possible.[7]

2.6.2 Mise à jour régulière des logiciels et des correctifs de sécurité

Les logiciels et les systèmes d'exploitation sont régulièrement mis à jour pour corriger les vulnérabilités découvertes et améliorer la sécurité globale. Voici quelques exemples supplémentaires :

Installer les mises à jour automatiques

Configurer les périphériques pour qu'ils installent automatiquement les mises à jour de sécurité dès leur publication, afin de garantir une protection constante contre les menaces émergentes.[7]

Scanner régulièrement les périphériques

Utiliser des outils de gestion de vulnérabilités pour scanner régulièrement les périphériques réseau à la recherche de failles de sécurité et appliquer les correctifs nécessaires.[7]

Gérer les correctifs de manière proactive :

Identifier et prioriser les correctifs en fonction de leur criticité et de leur impact sur la sécurité du réseau, en se concentrant sur les vulnérabilités les plus critiques en premier lieu.[7]

2.7 Politique de sécurité réseau

2.7.1 Définition

Est un document officiel qui définit les règles et les procédures à suivre pour protéger les systèmes d'information d'une organisation. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques.doit être adaptée aux besoins spécifiques de chaque organisation, en tenant compte de sa taille, de son activité, des risques auxquels elle est exposée et des ressources dont elle dispose.[7]

2.7.2 Gestion des identités et des accés

La gestion des identités et des accès (IAM - Identity and Access Management) est une composante essentielle de la politique de sécurité réseau d'une organisation. Elle vise à garantir que seules les personnes autorisées ont accès aux ressources et aux informations pertinentes, tout en empêchant les accès non autorisés.
Voici quelques éléments clés de la gestion des identités et des accès dans une politique de sécurité réseau :[7]

Identification et authentification des utilisateurs :

- L'identification consiste à attribuer une identité unique à chaque utilisateur, souvent sous forme de nom d'utilisateur.
- L'authentification est le processus par lequel l'utilisateur prouve son identité, généralement en fournissant un mot de passe, une carte à puce, une empreinte digitale ou d'autres facteurs d'authentification.[7]

Gestion des privilèges

- Les privilèges d'accès définissent ce que les utilisateurs sont autorisés à faire une fois qu'ils sont authentifiés.
- Elle implique de définir des rôles et des niveaux d'accès appropriés pour chaque utilisateur en fonction de ses responsabilités et de ses besoins.[7]

2.7.3 Sécurité des services cloud

La sécurité du cloud repose sur un modèle de responsabilité partagée entre les fournisseurs de services cloud et leurs clients. La responsabilité varie en fonction du type de services proposés. Quel que soit le type d'environnement ou la combinaison d'environnements utilisés par une organisation, la sécurité du cloud vise à protéger les réseaux physiques, y compris les routeurs et les systèmes électriques, ainsi que les données, le stockage des données, les serveurs de données, les applications, les logiciels, les systèmes d'exploitation et le matériel.[13]
les principaux piliers de la sécurité du cloud sont les suivants :

- **Limitation des accès :** dans la mesure où le cloud permet d'accéder à tout par Internet, il est extrêmement important de veiller à ce que seules les bonnes personnes aient accès aux bons outils au bon moment.[13]

- **Protection des données :** les organisations doivent savoir où se trouvent leurs données et mettre en place les contrôles appropriés pour protéger à la fois les données proprement dites et l'infrastructure où elles sont hébergées.[13]
- **Récupération des données :** une bonne solution de sauvegarde et un bon plan de récupération des données sont essentiels en cas de violation de la sécurité.[13]
- **Plan de réponse :** lorsqu'une organisation est attaquée, il lui faut un plan pour réduire l'impact de l'attaque et empêcher que d'autres systèmes ne soient compromis.[13]
- **Intégration précoce de la sécurité (Shift Left) :** les équipes chargées de la sécurité et du développement travaillent ensemble pour incorporer la sécurité dans le code lui-même, afin que les applications natives cloud démarrent et s'exécutent en toute sécurité.[13]
- **Unification de la visibilité de la posture de sécurité du DevOps :** réduisez les angles morts en rassemblant dans un seul affichage les informations relatives à la sécurité sur différentes plateformes DevOps.[13]
- **Surveillance étroite des menaces émergentes par les équipes de sécurité :** renforcez les configurations de ressources cloud dans le code pour réduire les problèmes de sécurité qui touchent les environnements de production.[13]
- **automatiser le réseau avec SDN :** pour gérer les charges de travail temporaires et les services virtualisés créés de manière dynamique pour répondre aux demandes à court terme. Dans un SDN, les charges de travail et les services sont créés avec des stratégies d'appartenance réseau, d'accessibilité et de sécurité attribuées et appliquées automatiquement pour simplifier les opérations et améliorer la sécurité.[26]

2.8 Conclusion

Ce chapitre a exploré la sécurité des réseaux informatiques en mettant en lumière ses concepts fondamentaux, ses défis et ses solutions. Il a également présenté les meilleures pratiques pour élaborer et mettre en œuvre des stratégies de sécurité efficaces. Comprendre et appliquer ces principes est essentiel pour garantir l'intégrité, la confidentialité et la disponibilité des données, ainsi que pour prévenir les cyberattaques et maintenir la confiance des utilisateurs dans un environnement numérique en constante évolution.

Chapitre 3

Présentations de l'organisme d'accueil

3.1 Introduction

Ce chapitre sera réservé à la présentation du l'entreprise COLLABLE où nous effectuons notre stage. Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecture réseau de cette entreprise et ses composantes afin de pouvoir suggérer d'éventuelles améliorations.

3.1.1 Création et évolution

NTS est une entreprise axée sur la recherche, la conception et la mise en œuvre de solutions, d'intégration de systèmes de sécurité, d'importation et de la distribution d'équipements et de matériels de sécurité des réseaux et des télécommunications, de la formation et le conseil. Elle a été crée en 2020 à Bejaia par Yassine Djebbari, qui a de nombreuses années d'expérience et a réalisé d'importants projets dans différents secteurs et régions du pays. Notre stage s'est déroulé chez un client de NTS, qui est un centre téléphonique nommé «COLLABLE».

3.1.2 La localisation de l'entreprise client

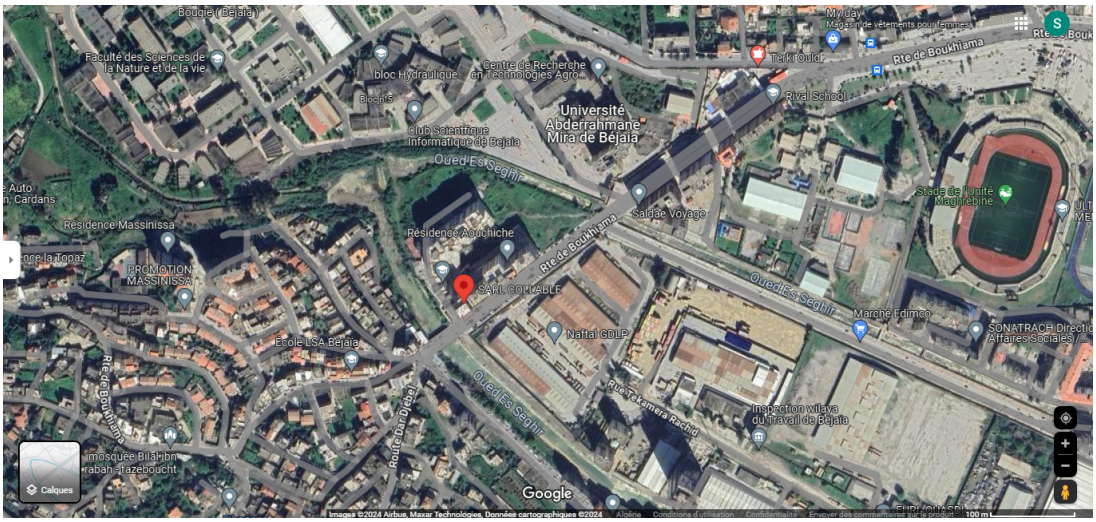


FIGURE 3.1 – Localisation de l'entreprise Collable.

3.1.3 Fiche technique

Le tableau 1 ci-dessous représente quelques informations relatives à l'entreprise Collable.

Dénomination	collable
Logo	
Siège	Promotion Immobilière AOUCHICHE Rachid, Route de Tazeboudjt, Béjaïa 06000
Secteurs d'activités	Couvre les secteurs service client, de la technologie, des services financiers, de la vente, du télémarketing et des ressources humaines.
Numéros de Téléphone	+213 552 478722
Email	contact@groupecollable.com
Site Internet	`https://groupecollable.com/`

Tableau 1 : Identification entreprise collable.

Organigramme général de l'organisme d'accueil

Les centres d'appels jouent un rôle essentiel en facilitant l'interaction efficace des entreprises avec leurs clients. Collable, un centre d'appels moderne, fournit une plateforme centralisée pour gérer les demandes d'assistance, offrir un support technique, et résoudre les problèmes relatifs aux services financiers et aux ressources humaines. Cette présentation offre un aperçu complet des services proposés par Collable.
Nous allons nous contenter de présenter ci- dessous la description de l'organigramme du l'entreprise COLLABLE(voir la figure 3.2).

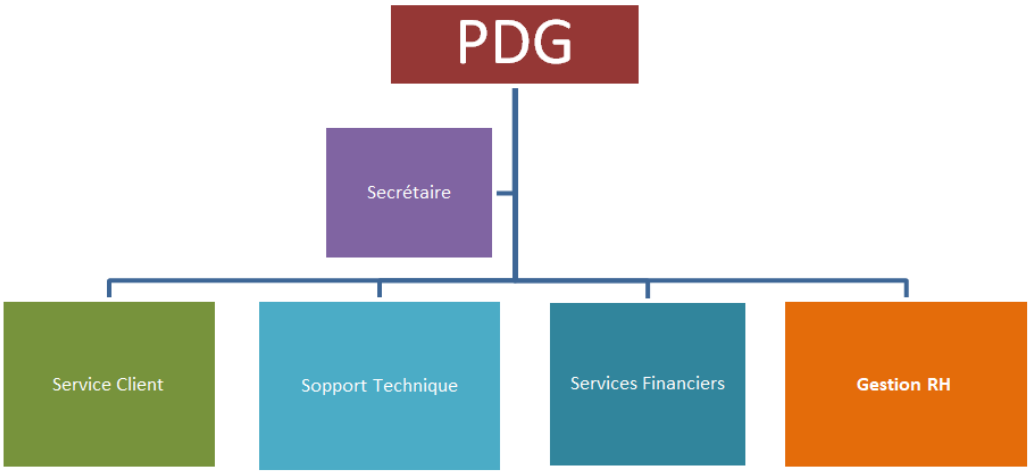


FIGURE 3.2 – L'organigramme de l'entreprise COLLABLE

Service Client

Le service client est au cœur des activités de Collable. Les agents de service client répondent aux questions des clients, résolvent leurs problèmes et veillent à ce qu'ils vivent une expérience positive avec l'entreprise. Ils doivent faire preuve de patience, de compréhension et de compétences en communication pour offrir un service de qualité.

- Répondre aux questions concernant les produits et services.
- Gérer les plaintes et les retours des clients.
- Résoudre les problèmes de facturation et de paiements.
- Offrir une assistance pour les commandes et les retours.
- Collecter les commentaires des clients pour améliorer les produits et services.

Support Technique

Le support technique est crucial pour les entreprises qui vendent des produits technologiques ou offrent des services en ligne. Les techniciens de Collable doivent avoir une connaissance approfondie des produits et services pour diagnostiquer et résoudre rapidement les problèmes. Ils doivent également communiquer efficacement avec les clients, même ceux sans connaissances techniques.

- Diagnostiquer et résoudre les problèmes techniques liés aux produits et services.
- Fournir des instructions et des conseils de dépannage.

- Offrir une assistance pour l'installation et la configuration des produits.
- Informer les clients sur les correctifs logiciels et les mises à jour de sécurité.
- Collaborer avec les équipes techniques pour résoudre des problèmes complexes.

Gestion RH

Collable peut jouer un rôle important dans la gestion des ressources humaines en offrant un point de contact centralisé pour répondre aux questions des employés et résoudre leurs problèmes, permettant ainsi aux professionnels des RH de se concentrer sur des tâches plus stratégiques.

- Répondre aux questions concernant les politiques et procédures RH.
- Gérer les demandes de congés et les absences.
- Aider les employés à s'inscrire aux programmes de formation et de développement.

Services Financiers

Collable peut offrir une gamme de services financiers aux clients, répondant à leurs questions sur les comptes, effectuant des transactions et offrant des conseils financiers, ce qui améliore la satisfaction et la fidélisation des clients.

- Répondre aux questions concernant les comptes bancaires et les investissements.
- Résoudre les problèmes liés aux cartes de crédit et de débit.
- Fournir des conseils financiers aux clients.

3.2 Présentation de l'architecture réseau existant dans COLLABLE

COLLABLE construit un réseau en choisissant une topologie arborescente pour connecter ses différents appareils, comme illustré dans la figure suivante :

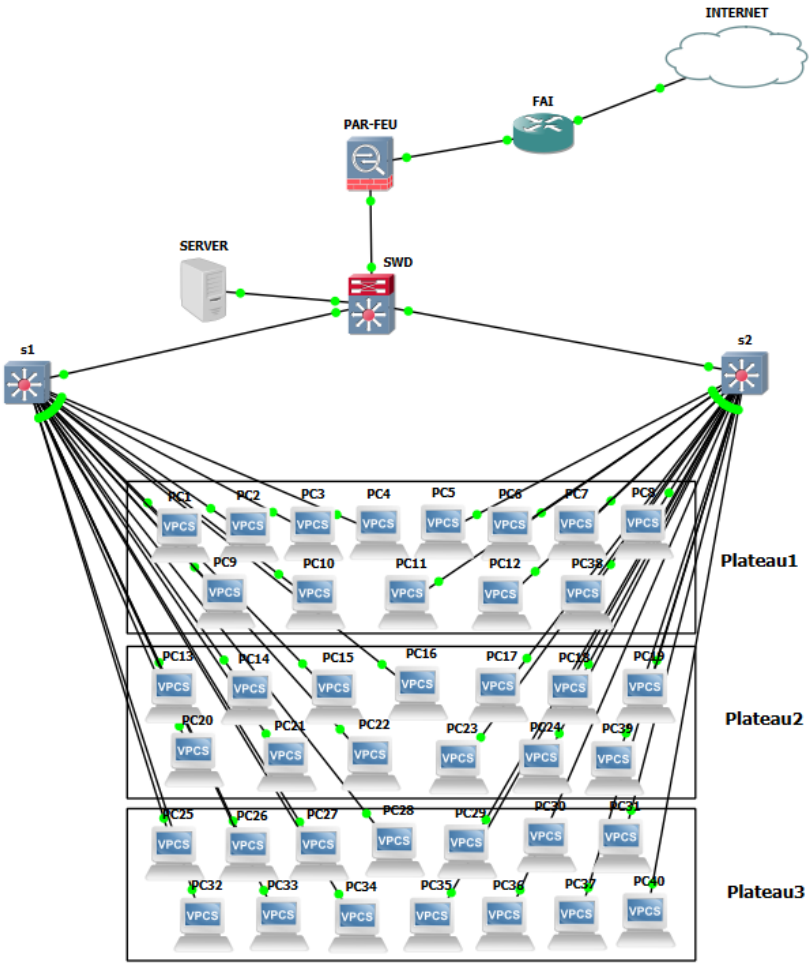


FIGURE 3.3 – Architecture de réseau (COLLABLE).

3.3 Analyse du parc informatique

3.3.1 Présentation d'environnement hard et soft

Nom de l'équipement	Hardware (hard)	Software (soft)
Routeur	ISR 4331	IOS (internetworking operating system)
Pare-feu	Pfsense	FreeBSD
Serveur	HP ProLiant DL380P génération 10	Windows server 2012
Switch	Switch Cisco Catalyst 3750-24PS	Switch Cisco Catalyst 3750-24PS IOS (internetworking operating system)
PC portable	Dell i5 VP inside	windows 10

TABLE 3.1 – L'environnement hardware et software

3.3.2 Les caractéristiques des équipements

Nom de l'équipement	Modèle	Caractéristique
Armoire de brassage  **prix :** 70000 DA **nombre :** 01	TOTEN RACK	Capacité 42U(racks) 700mm × 1100mm × 2000mm Porte devant et arrière perforée avec poignets rétractables contenant des serrures. Panneaux latéraux amovibles.Plaque de fond et de toiture avec des trous de ventilation + Kit de 4 ventilateurs de toit. Rail kit + étagère coulissante + deux étagères fixes. Bandeau d'alimentation.Entrée de câble sur le dessus et le dessous. 4 pieds ajustables + 4 roulettes.
Switch  **prix :** 150000 DA **nombre :**01	hpe officeconnect 1820 series switch j9983A	Ports : 24 ports Mémoire Flash : 16 Mo Mémoire RAM : 128 Mo Capacité de commutation : 32 Gbit/s

Serveur  **prix :** 800000 DA **nombre :** 01	HP ProLiant DL380P génération 10 (garantie de 5ans)	Processeur Intel Xeon Silver 4110 (Octo-Core 2.1 GHz / 3.0 GHz Turbo-16 Threads-cache 11 Mo) 16 Go DDR4 RDIMM (1x 16 Go - 12 slots)
PC portable  **prix :** 90000 DA **nombre :** 54	Dell i5 VP Inside	AMD core : i5 8th génération RAM : 8GO Disque :256GO Ecran : UHD Graphies
Router  **prix :** 250000 DA **nombre :** 01	ISR 4331	RAM : 4 G0 (installé)/16 GO (maximum) Mémoire Flash :4000 MO Débit :100 Mb/s Protocole de liaison de données : Ethernet, fast Ethernet et gigabit-ethernet.
Pare-feu  **prix :** 70000 DA **nombre :** 01	PFSENSE	Débit : 4000 Mbit/s Débit IPS : 2700Mbit/s Débit VPN IP sec : 560 Mbit/s

TABLE 3.2 – Détails des ressources disponibles de COLLABLE

3.4 Objectif du stage

Notre stage au sein du Groupe COLLABLE avait pour objectif la conception et la mise en place d'une nouvelle infrastructure réseau sécurisée.

3.5 L'étude de cas existant

Lors de notre stage au centre d'appel COLLABLE nous avons constaté qu'il dispose d'un réseau local de trois plat-forme, Nous avons identifié plusieurs points critiques :

- **Un seul serveur physique :** Un serveur physique unique héberge tous les services critiques de l'entreprise, y compris Asterisk, le serveur , sql , web et le serveur de messagerie.
- **Commutateur réseau(Distrubution) :** Un commutateur réseau relie tous les périphériques du réseau local.
- **Ports physiques non sécurisés :** Les ports physiques des équipements (serveur, switchs) réseau ne sont pas sécurisés, ce qui facilite l'accès non autorisé au réseau.

- **Configuration VLAN :** Les ports du commutateur sont configurés sur le VLAN par défaut (VLAN 1), ce qui signifie que tous les périphériques connectés au commutateur partagent le même espace de diffusion.
- **Adresses IP publiques :** Les appareils du réseau utilisent des adresses IP publiques, ce qui les rend accessibles depuis Internet.
- **Interconnexion non sécurisée :** L'interconnexion entre les sites distants n'est pas sécurisée, ce qui expose les données à des interceptions et des accès non autorisés.
- **Gestion des comptes non centralisée :** Il n'y a pas de solution centralisée pour gérer les comptes et les accès des utilisateurs, ce qui rend difficile le contrôle des accès et augmente le risque d'intrusions.
- **Accès à distance non sécurisé :** L'accès à distance aux équipements réseau n'est pas sécurisé, ce qui expose le réseau à des attaques et des intrusions.
- **Armoire non sécurisée :** L'armoire contenant les équipements réseau n'est pas sécurisée. Elle est accessible à tout le personnel sans aucun contrôle, exposant les équipements à des manipulations non autorisées.

3.6 Critiques détaillées pour chaque étape de l'étude de cas existant

- **Single Point of Failure (SPOF) :** Le serveur unique représente un point de défaillance critique. Une panne de serveur peut entraîner une interruption totale des services critiques de l'entreprise.
- **Problèmes de performance et de scalabilité :**L'hébergement de plusieurs services sur un seul serveur peut entraîner des goulots d'étranglement en cas de pics de charge ou d'augmentation imprévue de la demande.
- **Failles de sécurité :** La concentration de services sur un seul serveur augmente la surface d'attaque et le risque d'exploitation de vulnérabilités pour compromettre l'ensemble du système.
- **Diffusion sur le réseau et tempêtes de diffusion :** L'utilisation d'un seul VLAN par défaut peut causer des problèmes de diffusion et saturer le réseau, affectant sa performance.
- **Manque de segmentation du réseau :** L'absence de micro-segmentation limite la visibilité et le contrôle sur le trafic réseau, compliquant la gestion et la sécurité du réseau.
- **Exposition des adresses IP publiques :** Les adresses IP publiques des appareils sont vulnérables aux attaques et aux intrusions externes.
- **Interconnexion non sécurisée entre les sites :** L'absence de sécurisation des liaisons entre les sites distants expose les données à des interceptions et des accès non autorisés.
- **Gestion des comptes et des accès non centralisée :** L'absence d'une solution centralisée pour gérer les comptes et les accès augmente le risque d'erreurs de configuration et d'accès non autorisés.
- **Accès à distance non sécurisé :** Le manque de sécurisation de l'accès à distance aux équipements réseau expose le réseau à des attaques et des intrusions.
- **Ports physiques non sécurisés :** L'accès ouvert aux ports physiques facilite l'intrusion non autorisée dans le réseau.

3.7 Solution proposée (1)

Niveau 01 (physique) :

- Mise en place de contrôles d'accès physiques simples pour l'armoire, tels que des serrures à code ou des badges d'accès.
- Installation de caméras de surveillance visibles pour dissuader les intrusions.

Niveau 02(liaison de données) :

- Mise en place du filtrage par adresse MAC via la technique de Port Security pour limiter l'accès aux périphériques autorisés uniquement.
- Configuration des VLANs pour segmenter le trafic.

Niveau 03 (Réseau) :

- Configuration du routage inter-VLAN pour permettre la communication entre les VLANs.
- Mise en place d'un pare-feu matériel de base pour protéger le réseau contre les attaques externes.

Niveau 04 (Transport) :

- Mise en place d'un VPN de base pour sécuriser les accès à distance.

Niveau (05-06-07) (Application) :

- Mise en place des solutions logicielles de sécurité gratuites ou open source comme KeePass pour la gestion des mots de passe et ClamAV pour la protection contre les logiciels malveillants.

Avantages :

- Coût moins élevé pour l'achat et la mise en œuvre des technologies.
- Simplicité de la gestion et de la maintenance du réseau.

Inconvénients :

- Niveau de sécurité moins élevé par rapport aux solutions plus onéreuses.
- Fonctionnalités limitées de segmentation du réseau et de protection contre les menaces avancées.
- Nécessite une expertise plus poussée pour la configuration et la gestion des solutions open-source.

3.8 Solution proposée (2)

Niveau 01 (physique) :

- Mise en place d'une salle technique pour les armoires où sont regroupés les dispositifs de connexion réseau et de télécommunication dans le but de restreindre l'accès au réseau uniquement aux personnes autorisées, éliminant ainsi tout accès non autorisé.
- caméras de surveillance.

Niveau 02 (liaison de données) :

- Mise en place du filtrage par adresse MAC en utilisant la technique ports Security en restreignant l'accès uniquement aux périphériques approuvés.
- L'agrégation des liens LACP regroupe plusieurs connexions physiques entre deux équipements réseau pour garantir une tolérance aux pannes en cas de défaillance d'une

connexion, tout en offrant une bande passante combinée pour une performance accrue.
- la configuration de vtp pour facilité la gestion des VLANs.
- Mise en place des VLANs pour améliorer la sécurité du réseau et réduire les tempêtes de diffusion ARP.

Niveau 03 (Réseau) :
- La configuration de routage inter-VLAN pour faciliter la communication entre des réseaux virtuels distincts au sein d'une même infrastructure physique, permettant ainsi aux dispositifs situés dans des VLANs différents de se connecter tout en maintenant une segmentation logique du réseau.
- Mise en place des ACL(Access lists) pour sécuriser les routeurs, les commutateurs et les pare-feux en définissant des règles qui déterminent quel trafic est autorisé à traverser un périphérique réseau et lequel est bloqué.
- Nous allons déployer une zone démilitarisée(DMZ) afin de renforcer la sécurité du réseau interne contre d'éventuelles attaques, en isolant les serveurs accessibles au public dans une zone tampon. Dans cette section, nous allons configurer les PVLANs(private VLANs). L'objectif est d'avoir un VLAN dans lequel les utilisateurs ne peuvent pas communiquer entre eux.
- Mise en place d'un Canal sécurisé de bout en bout entre le site de Bejaia et celui de Alger en utilisant le protocole IPSec(IP securisé) pour avoir la confidentialité, l'intégrité et l'authentification des données circulant sur le réseau internet.

Niveau 04 (Transport) :
- Configuration d'un firewall existant pour contrôler, gérer et sécuriser les ports logiques ouverts sur le réseau externe.

Niveau (05-06-07) (Application) :
- Mise en place du protocole TLS et SSL pour sécuriser les accès à distance aux équipements d'interconnexion depuis l'intranet et l'extranet.
- Déploiement d'un serveur Active Directory pour centraliser la gestion des identités et des accès, renforcer la sécurité des communications et des sessions, et améliorer la gestion des utilisateurs et des ressources du réseau.

Avantages :

- Sécurité renforcée.
- Résilience et fiabilité.
- Gestion centralisée.
- Performance améliorée.

Inconvénients :

- Coûts un peu plus élevés.
- Risques de configuration incorrecte.

3.9 Solution proposée (3)

Pour répondre à cet objectif, nous avons proposé une série de solutions basées sur le modèle de référence OSI :

Niveau 01 (physique) :

- Mise en place d'une salle technique pour les armoires où sont regroupés les dispositifs de connexion réseau et de télécommunication.
- Mise en place d'un système de détection d'intrusions physique (IDS physique) : Ce système utilise des capteurs et des caméras pour détecter les intrusions non autorisées dans la salle technique, comme les tentatives d'effraction ou de manipulation des équipements.
- Mise en place d'un système de contrôle d'accès biométrique : Ce système utilise des empreintes digitales ou d'autres données biométriques pour identifier les personnes autorisées à accéder à la salle technique, augmentant la sécurité et réduisant le risque d'erreurs humaines.
- câblage blindé et encastré.
- détection d'incendie permettant une intervention rapide pour minimiser les dégâts et assurer la sécurité des personnes et des biens.

Niveau 02 (liaison de données) :

- Déploiement d'une solution de commutation SDN (Software Defined Networking) : SDN permet une gestion centralisée et programmable du réseau, offrant une flexibilité et une automatisation accrues.

Niveau 03 (Réseau) :

- Mise en place d'une solution de segmentation réseau basée sur la micro- segmentation : La micro-segmentation permet de créer des segments de réseau encore plus fins, offrant un contrôle granulaire du trafic et une protection renforcée contre les attaques latérales.

Niveau 04 (Transport) :

- Déploiement d'une solution de détection et de réponse aux intrusions (IDS/IPS) : IDS/IPS surveille le trafic réseau pour détecter et bloquer les attaques en temps réel.
- Mise en place d'un pare-feu nouvelle génération (NGFW) : NGFW offre des fonctionnalités avancées de sécurité, telles que le filtrage du contenu web, la protection contre les ransomwares et la prévention des intrusions basées sur les applications.

Niveau 05-06-07 (Application) :

- Déploiement d'une solution de gestion des accès à privilèges (PAM) : PAM centralise la gestion des accès aux comptes privilégiés, réduisant le risque de compromission des comptes et d'attaques par élévation de privilèges.

Avantages :

- Sécurité renforcée contre les intrusions physiques, les attaques réseau et les menaces applicatives.
- Flexibilité et automatisation accrues grâce à SDN.
- Protection granulaire du trafic réseau avec la micro-segmentation.
- Détection et réponse en temps réel aux intrusions avec IDS/IPS.

- Fonctionnalités avancées de sécurité avec NGFW.
- Gestion centralisée des accès à privilèges avec PAM.

Inconvénients :

- Coût plus élevé pour l'achat et la mise en œuvre des technologies.
- Complexité accrue de la gestion et de la maintenance du réseau.

Tableau Comparatif des Solutions Ajustées

Critère	**Solution 1**	**Solution 2**	**Solution 3**
Niveau 01 (Physique)			
Contrôles d'accès	Serrures à code, Badges	Système de contrôle d'accès avancé	Système de contrôle d'accès biométrique
Prix (DZD)	20 000	60 000	120 000
Surveillance	Caméras visibles	Caméras visibles	IDS physique avec caméras
Prix (DZD)	50 000	100 000	300 000
Détection d'incendie	Simple	Avancée	Avancée
Prix (DZD)	50 000	200 000	200 000
Câblage	Standard	Blindé et encastré	Blindé et encastré
Prix (DZD)	50 000	100 000	100 000
Niveau 02 (Liaison de Données)			
Filtrage MAC	Port Security	Oui	Oui
Prix (DZD)	30 000	50 000	50 000
Agrégation de liens	Non	LACP	SDN
Prix (DZD)	0	80 000	500 000
Gestion VLAN	Non	VTP	SDN
Prix (DZD)	0	50 000	500 000
Niveau 03 (Réseau)			
Sécurité	Pare-feu matériel de base	DMZ (+ 4 serveurs + 1 switch)	NGFW + DMZ + Micro-segmentation
Prix (DZD)	100 000	1 200 000	2 000 000
Routage	Non	Inter-VLAN	Inter-VLAN
Prix (DZD)	0	0	0
IPSec	Non	Oui	Oui
Prix (DZD)	0	200 000	200 000
Niveau 04 (Transport)			
VPN	Basique	SSL VPN	SSL VPN + PAM
Prix (DZD)	50 000	100 000	200 000
Niveau 05-06-07 (Application)			
Sécurité Applicative	Open-source	SSH + SSL VPN + Serveur AD	PAM
Prix (DZD)	0	240 000	500 000
Total des Coûts (DZD)			
Total (DZD)	**250 000**	**1 920 000**	**4 570 000**

TABLE 3.3 – Comparaison des coûts des solutions proposées avec correctifs

3.9.1 Recommandations

- **Solution 1 :** Convient pour des petites entreprises ou des organisations avec des budgets limités. Elle offre une sécurité de base avec des coûts et une gestion simplifiés.
- **Solution 2 :** Idéale pour des entreprises moyennes(comme collable) qui ont besoin d'une sécurité plus robuste et de fonctionnalités de gestion améliorées tout en restant raisonnables en termes de coûts.
- **Solution 3 :** Recommandée pour des grandes entreprises ou des environnements critiques nécessitant une sécurité avancée et des fonctionnalités sophistiquées malgré des coûts et une complexité plus élevés.

3.9.2 Les équipements ajoutés pour la solution 2, comprenant les caractéristiques et les prix des matériels ajoutés

Nom de l'équipement	**Modèle**	**Caractéristique**
Serveur **prix :** 200 000 DA **nombre :** 04	Dell PowerEdge R740	Processeur : Intel Xeon Silver 4214 (12 core, 2.2 GHz) Mémoire : 64 GB DDR4 Stockage : 2 x 1TB 7.2K SATA 6G LFF Réseau : 2 x 1GbE ports
Switch **prix :** 200 000 DA **nombre :**01	Cisco Catalyst 9300	Ports : 24 x 1GbE ports, 4 x 10GbE SFP+ uplinks Capacité de commutation : 480 Gbps Mémoire : 8 GB
Serveur Active Directory **prix :** 200 000 DA **nombre :**01	Dell PowerEdge R740	Processeur : Intel Xeon Silver 4214 (12 core, 2.2 GHz) Mémoire : 64 GB DDR4 Stockage : 2 x 1TB 7.2K SATA 6G LFF Réseau : 2 x 1GbE ports

TABLE 3.4 – Les Outils Ajoutés

3.10 Conclusion

Dans ce chapitre, nous avons débuté en présentant une vue d'ensemble de l'entreprise du campus NTS, mettant en lumière son partenariat avec COLLABLE, une entreprise cliente. Nous avons ensuite scruté l'état actuel du centre d'appels COLLABLE, identifiant les lacunes en matière de sécurité réseau. En réponse à ces défis, nous avons élaboré des solutions visant à renforcer la sécurité de son infrastructure. Dans le prochain chapitre, nous aborderons la mise en œuvre pratique de ces solutions, démontrant ainsi notre engagement à fournir à COLLABLE les outils nécessaires pour garantir la protection et la fiabilité de son réseau.

Chapitre 4

Implémentation et réalisation

4.1 Introduction

Dans ce chapitre, nous présentons les solutions pratiques mises en œuvre au centre d'appel Collable pour améliorer la sécurité et la gestion du réseau. En suivant le modèle de référence OSI, nous avons proposé des mesures à différents niveaux, allant de l'installation de salles techniques sécurisées et de systèmes de détection d'incendie à la configuration de VLANs et de pare-feux. Chaque solution vise à renforcer la protection, la performance, et la fiabilité de l'infrastructure réseau, assurant ainsi un environnement de travail plus sûr et plus efficace.

4.2 Présentation de l'environnement de travail :

4.2.1 Installation de GNS3 sous Windows :

GNS3(Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques. Pour installer GNS3, il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes d'installation jusqu'à la fin puis cliquer sur le bouton "Finish". La figure suivante représente le logo de GNS3.

FIGURE 4.1 – GNS3

4.2.2 Installation de VMware Workstation Pro

VMware Workstation est un outil de virtualisation il permet de créer de nouvelles machines virtuelles, transformer un PC en une machine virtuelle et effectuer un déploiement en masse. Afin de créer les machines utilisateurs virtuelles au sein du même pc, nous sommes appelés à installer VMware Workstation en suivant les étapes d'installations jusqu'à la fin puis cliquer sur le bouton "terminer". La figure suivante représente le logo de VMware.

FIGURE 4.2 – VMware

4.2.3 Wireshark

Wireshark est un analyseur de protocole réseau gratuit et open source qui permet aux utilisateurs de parcourir de manière interactive le trafic de données sur un réseau informatique. La figure suivante représente le logo de Wireshark.

FIGURE 4.3 – Wireshark

4.2.4 Les machines virtuelles :

Le PfSense

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter ainsi que des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. PfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

Windows serveur 2022

Windows Server 2022 est l'actuel système d'exploitation commercialisé par Microsoft et destiné aux serveurs. Le système offre une sécurité multicouche avancée, des fonctionnalités hybrides avec Azure et une plateforme d'application flexible.

Windows 10

Windows 10 est un système d'exploitation de la famille Windows NT développé par la société américaine Microsoft.

4.3 Architecture proposes

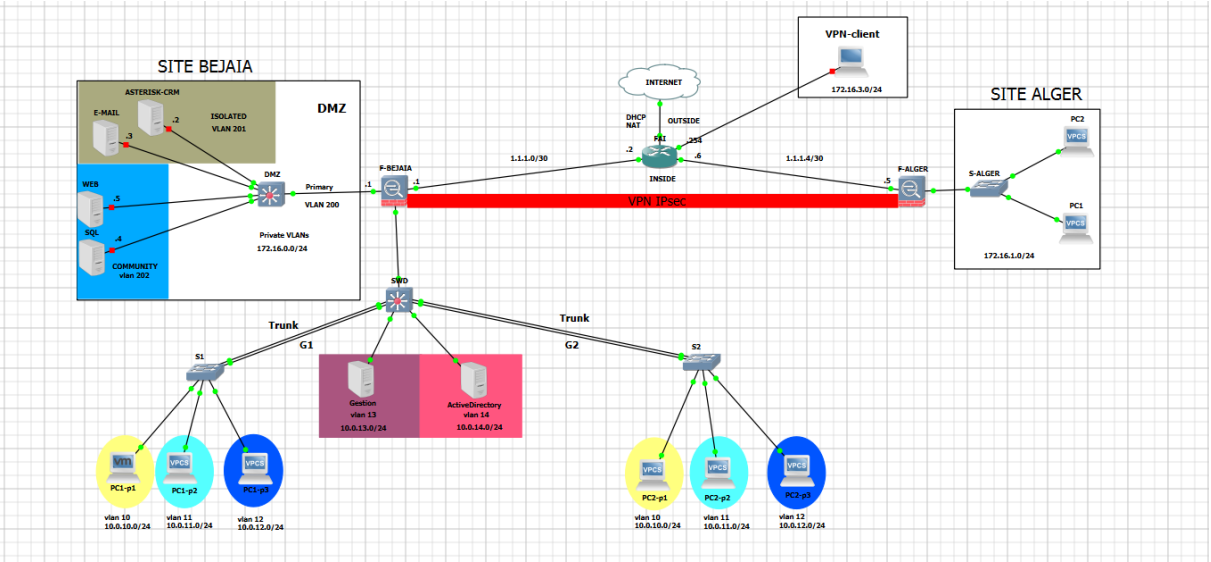


FIGURE 4.4 – Architecture de réseau proposée

- La figure 4.4 représente l'architecture sécurisée proposée pour COLLABLE. Il est important de noter que le site d'Alger est actuellement en cours de construction et a été ajouté uniquement dans le but de réaliser des tests entre les 2 sites.

4.4 Configuration de base

4.4.1 Plan d'adressage

Équipements

Dispositif	Interface	Adresse IP	Description	Passerelle
R-Fournisseur d'accès internet	E0/0	DHCP	Connecté sur internet	-
	E0/1	1.1.1.2/30	Connecté au F-Bejaia	-
	E0/2	1.1.1.6/30	Connecté au F-Alger	-
	E0/3	172.16.1.254/24	Connecté au VPN-Client	-
SWD (Switch Distribution)	E1/0	En mode trunk	Connecté au pfsense Bejaia	10.0.0.254
	E0/0	En mode trunk	Connecté au SWA1	10.0.0.254
	E0/1	En mode trunk	Connecté au SWA1	10.0.0.254
	E3/3	VLAN 13	Connecté au S-GESTION	10.0.0.254
	E0/2	En mode trunk	Connecté au SWA2	10.0.0.254
	E0/3	En mode trunk	Connecté au SWA2	10.0.0.254
	E3/2	VLAN 14	Connecté au S-ActiveDerictory	10.0.0.254
SWA1 (Switch accès 1)	E0/0	En mode trunk	Connecté au SWD	-
	E0/1	En mode trunk	Connecté au SWD	-
	E3/3	En mode acces	Connecté au VP1	-
	E3/2	En mode accès	Connecté au VP2	-
	E3/1	En mode accès	Connecté au VP3	-
SWA2 (Switch accès 2)	E0/0	En mode trunk	Connecté au SWD	-
	E0/2	En mode trunk	Connecté au SWD	-
	E3/3	En mode acces	Connecté au VP1	-
	E3/2	En mode accès	Connecté au VP2	-
	E3/1	En mode accès	Connecté au VP3	-
Switch DMZ	E1/0	En mode trunk	Connecté au Pfsense Bejaia	-
	E0/0	Vlan 201	Connecté au ASTERISK-CRM	-
	E0/1	Vlan 201	Connecté au E-MAIL	-
	E0/2	Vlan 202	Connecté au WEB	-
	E0/3	Vlan 202	Connecté au SQL	-
Switch Alger	E0/0	172.16.1.254	Connecté au Pfsense Alger	-
	E3/3	En mode accès	Connecté au Pc1	-
	E3/2	En mode accès	Connecté au Pc2	-

pfsense Alger	Em2	172.16.1.254	Connecté à S-Alger	-
	Em0	1.1.1.5/30	Connecté au fourniseure d'accés internet	
pfsense Bejaia	Em0	1.1.1.1/30	Connecté à fourniseure d'accés internet	-
	Em3	10.0.254.0/24	Connecté au SWD	172.16.0.1
	Em2	172.16.0.1/24	Connecté au DMZ	172.16.0.1
Client-vpn	E0	172.16.3.0/24	Connecté à fourniseure d'accés internet	-
ASTERISK-CRM	E0	172.16.0.2/24	Connecté au DMZ	172.16.0.1
E-MAIL	E0	172.16.0.3/24	Connecté au DMZ	172.16.0.1
SQL	E0	172.16.0.4/24	Connecté au DMZ	172.16.0.1
WEB	E0	172.16.0.5/24	Connecté au DMZ	172.16.0.1
GESTION	E0	10.0.13.0/24	Connecté au vlan 13	10.0.13.254
Active Directory	E0	10.0.14.0/24	Connecté au vlan 14	10.0.14.254

TABLE 4.1 – Tableau d'adressage des dispositifs réseau

VLANs

Nom Vlans	**IP Vlans**	**Réseau/Préfixe**
VP1	10	10.0.10.0/24
VP2	11	10.0.11.0/24
VP3	12	10.0.12.0/24
V gestion	13	10.0.13.0/24
V serveur	14	10.0.14.0/24
Vlan Native	99	//////////////////

TABLE 4.2 – La table des Vlans

Routage Inter Vlan

équipements	Vlans	Interface	Adresse IP /préfixe
pfsense (F-Bejaia)	vlan 10	Em3	10.0.10.254/24
pfsense (F-Bejaia)	vlan 11	Em3	10.0.11.254/24
pfsense (F-Bejaia)	vlan 12	Em3	10.0.12.254/24
pfsense (F-Bejaia)	vlan 13	Em3	10.0.13.254/24
pfsense (F-Bejaia)	vlan 14	Em3	10.0.14.254/24

TABLE 4.3 – La table de Routage Inter Vlan

4.4.2 La configuration de VTP

Le VTP (VLAN Trunking Protocol) simplifie la gestion des VLAN en permettant la transmission automatique des configurations entre les commutateurs réseau.

- **Mode Server** : est capable de créer, modifier et supprimer des VLANs. Les modifications effectuées sur un commutateur en mode serveur sont propagées à tous les autres commutateurs dans le même domaine VTP.

- **Mode Client** : Le mode client ne peut pas créer, modifier ou supprimer des VLANs. Il synchronise ses informations VLAN avec celles du serveur VTP dans le même domaine VTP.

  — Configuration de VTP mode Server sur le switch SWD.
  — Configuration de VTP mode Client sur les deux switch S1 et S2[voir l'annexe C.1].

4.4.3 La configuration des VLANs

La configuration de trunk

Le "mode trunk" dans les réseaux informatiques permet de transporter plusieurs VLAN sur un seul lien physique, simplifiant ainsi la gestion des réseaux et optimisant l'utilisation de la bande passante.

— Configuration des Interfaces en Mode Trunk sur le Commutateur SWD Reliées à S1 et S2[voire l'annexe C.2.1].

La création des VLANs

- Nous avons créé cinq VLANs pour segmenter les réseau : VP1, VP2 et VP3 pour les trois pelotons respectivement, un VLAN pour Active Directory et un autre pour la gestion.[Voir l'annexe C.2.2]
- Affectation des ports aux VLANs.[Voir l'annexe C.2.3]configuration de VLAN native.[Voir l'annexe C.2.4].

4.4.4 La configuration des liens d'agrégation (LACP)

LACP (Link Aggregation Control Protocol) est un protocole réseau qui permet de combiner plusieurs liaisons physiques en une seule liaison logique, améliorant ainsi la bande passante et la fiabilité en coordonnant la formation et la maintenance de ces agrégations de liens. Nous allons utiliser LACP avec deux groupes (G1 et G2) parce qu'il s'agit de connexions point à point.

- Configuration de LACP sur le commutateur SWD.[Voir l'annexe C.3]

4.4.5 Le port sécurité

Le port sécurité est une fonctionnalité des commutateurs Ethernet qui restreint l'accès aux ports en surveillant et limitant le nombre d'adresses MAC autorisées à transmettre des données. Cela empêche les appareils non autorisés d'accéder au réseau, renforçant ainsi la sécurité.

- La configuration du port sécurité sur le commutateur S1 au niveau de PC1-P1[Voir l'annexe C.4]

4.4.6 Configuration des deux Pare-feu

Nous avons ajouté une machine virtuelle dédiée à l'administration pour effectuer les configurations nécessaires sur les deux pare-feu et un commutateur pour connecter les deux pare-feu au PC admine.

Configurations des interfaces des deux Pare-feu

- **Au niveau de Pare-feu Bejaia :** L'interface em2 sera réservée à la DMZ, tandis que l'interface em3 sera utilisée pour le routage inter-VLAN. [Voir L'annexe C.5.1]
- **Au niveau de pare-feu d'Alger** Nous allons configurer l'interface em2 pour le LAN à Alger. [Voir L'annexe C.5.1]

4.4.7 Le routage inter-VLAN

Création des VLANs sous l'interface em3 sur le pare-feu de Bejaia

Nous avons créé cinq VLANs, à savoir VLAN 10, 11, 12, 13 et 14 sur l'interface du pare-feu qui est configurée pour le routage inter-VLAN. Cette configuration permettra au pare-feu de router efficacement le trafic entre les différents réseaux virtuels. [Voir l'annexe C.6.1]

L'assignation des interfaces aux VLANs

Nous avons créé cinq sous-interfaces et assigné chaque sous-interface à un VLAN. [voir l'annexe C.6.2]

4.4.8 Configuration des Listes de Contrôle d'Accès (ACL)

Elle est utilisée pour filtrer le trafic réseau en fonction de divers critères tels que les adresses IP source et de destination, les ports, les protocoles, etc, que les administrateurs réseau peuvent

restreindre l'accès aux ressources sensibles, limiter les attaques potentielles et optimiser les performances du réseau.

Au niveau des VLANs, nous mettrons en place une autorisation globale pour tous les protocoles ainsi que pour toutes les adresses sources et destinations.[Voir l'annexe C.7]

4.4.9 Configuration des services DHCP

Au niveau des VLANs, nous avons autorisé le service DHCP à leur attribuer des adresses IP. Nous attribuons également une adresse DNS à chacun de ces VLANs.[Voir l'annexe C.8]

4.4.10 La configuration de la DMZ(zone démilitarisée)

Dans le but de renforcer la sécurité de notre réseau, nous proposons d'adopter la technique de la DMZ. Cette approche permettra d'héberger nos serveurs tels que ASTERISK-CRM, Web, SQL et de messagerie électronique (E-MAIL), tout en maintenant une séparation sécurisée entre ces serveurs et le réseau interne. Cela nous permettra de fournir des services accessibles depuis Internet tout en protégeant nos ressources internes sensibles.

Configuration de VTP

Pour éviter que les changements de VLAN soient propagés automatiquement à travers le réseau via le protocole VTP (VLAN Trunking Protocol), vous pouvez désactiver le VTP ou le configurer en mode transparent. [Voir l'annexe C.9.1]

Configuration de Private VLANs(PVLAN)

Dans le cas de notre DMZ, nous avons besoin de connecter 4 serveurs au réseau, mais ils ne doivent pas pouvoir communiquer entre eux. Créer un VLAN distinct pour chaque serveur pourrait entraîner la création de nombreux sous-réseaux et un gaspillage d'adresses IP.

Une meilleure solution serait d'avoir un seul VLAN (et donc un seul sous-réseau) où les serveurs sont isolés les uns des autres, mais peuvent toujours se connecter au réseau principal. Les PVLAN permettent exactement cela.
PVLAN se compose d'une association de VLAN :

- Un VLAN Primary
- Un ou plusieurs VLAN Secondary

Le VLAN Secondary peut être de deux types :

- **Isolated :**les membres de ce VLAN ne peuvent pas communiquer etre eux.
- **Community :**les membres de ce VLAN peuvent communiquer entre eux.

En fin le port d'un switch peut fonctionner dans l'un des deux modes suivants :

- **Host :**Le port à un comportement qui découle du type de PVLAN auquel il est associé (isolated ou community).
- **Promiscuous :**le port peut communiquer avec les ports membres du même VLAN.[Voir l'annexe C.9.2]

Attribution d'adresses aux différents serveurs

[Voir l'annexe C.9.3]

4.4.11 Configuration de FAI

- Configuration des interfaces. [Voir l'annexe C.10.1]
- Configuration du NAT avec le PAT :
  Dans cette section, nous allons explorer l'utilisation du NAT avec PAT (Port Address Translation) pour traduire les adresses IP d'un réseau à un autre. Le NAT avec PAT est principalement déployé pour permettre à plusieurs dispositifs d'un réseau privé d'accéder à Internet tout en partageant une seule adresse IP publique. Cette méthode aide à renforcer la sécurité du réseau en masquant les adresses IP privées derrière une seule adresse IP publique, tout en utilisant différents numéros de port pour identifier chaque connexion.[Voir l'annexe C.10.2]

4.5 Configuration VPN

4.5.1 Configuration VPN site to site

Dans cette étape, nous avons examiné la proposition de mettre en place un tunnel VPN reliant deux sites, l'un à Béjaïa et l'autre à Alger, en utilisant le protocole IPsec. Ce protocole serait configuré dans les deux pare-feu pour sécuriser le trafic traversant ce tunnel.

Création de la premier phase

La création de la première phase, qui repose sur l'échange des clés via le protocole IKE.[Voir l'annexe D.1.1]

Création de la deuxième phase

La création de la deuxième phase, centrée sur la négociation du tunnel et la transmission des données via le protocole ESP.[Voir l'annexe D.1.2]

Connexion des deux phases

Pour que notre tunnel fonctionne, il est nécessaire de connecter les deux phases que nous avons créées.[Voir l'annex D.1.3]

4.5.2 Configuration du Client VPN

Nous allons configurer un VPN client-to-site Bejaia pour permettre aux employés de se connecter de manière sécurisée au réseau de l'entreprise depuis des emplacements distants. Nous allons utiliser les assistants de configuration (wizards) pour configurer notre client VPN de manière optimale et efficace.

Création d'un certificat d'autorité (CA) pour les connexions VPN

Nous avons créé une autorité de certification (CA) pour les connexions VPN. À partir de ce certificat d'autorité, nous allons générer des certificats pour les serveurs et les clients.[Voir l'annexe D.2.1]

Création d'un certificat d'autorité (CA) pour le serveur

On va créer un certificat pour le serveur en utilisant le certificat d'autorité VPN.[Voir l'annexe D.2.2]

Configuration du serveur

dans cette partie vous devrez configurer les paramètres du serveur. Cela inclut généralement la configuration des ports et des protocoles Par défaut, OpenVPN utilise souvent le port UDP 1194, ainsi que la définition des adresses IP et des sous-réseaux autorisés à se connecter au serveur.[Voir l'annexe D.2.3]

Ensuite, nous allons créer deux règles de filtrage : une pour les communications entre le client et le serveur, et l'autre pour les connexions des clients.[Voir l'annexe D.2.4]

Configuration des clients

1. Création des Utilisateurs. [Voir l'annexe D.2.5]
2. Téléchargement et installation du package OpenVPN. [Voir l'annexe D.2.5]
3. Installation du logiciel client VPN sur les appareils des utilisateurs : nous allons installer les deux pacages d'utilisateurs sur le PC VPN. [Voir l'annexe D.2.5]
4. Connecter au serveur : vous devrez saisir le nom d'utilisateur et le mot de passe pour vous connecter. [Voir l'annexe D.2.5]

Visualisation des utilisateurs connectés au client VPN

Nous pouvons contrôler les utilisateurs qui se connectent au client VPN. Il est possible de les bloquer ou de les supprimer selon les besoins.[Voir l'annexe D.2.6]

4.6 Configuration de l'Active Directory

Le service de domaine Active Directory (AD DS) stocke des informations sur les utilisateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations de manière sécurisée et facilitent le partage des ressources ainsi que la collaboration entre les utilisateurs. Le service AD DS nécessite également qu'un serveur DNS soit installé.

- Installation du service AD DS au niveau de serveur active directory. [Voir l'annexe E.1]

4.6.1 Configuration du Contrôleur de Domaine

La création d'une forêt Active Directory

nous avons configuré un nouveau contrôleur de domaine avec une nouvelle forêt Active Directory nommée 'collable.local'.[Voir l'annexe E.2.1]

La création une Unité d'organisation (OU)

la création d'un groupe et des utilisateurs dans une unité d'organisation (OU) du domaine 'collable.local'.[voir l'annexe E.2.2]

4.6.2 Procédure de Connexion au Domaine Active Directory

Nous allons accéder au domaine Active Directory en tant qu'administrateur pour gérer et contrôler tous les accès au domaine 'collable.local'. [Voir l'annexe E.3]

4.7 Tests de Configuration et Vérification

Nous avons effectué différents tests sur les techniques de sécurité que nous avons mises en place afin de vérifier leur validation et leur configuration correcte. Ces tests nous permettent de garantir que nos techniques de sécurité sont validées et assurant ainsi une protection optimale contre les menaces potentielles.[voir l'annexe F]

4.8 Conclusion

En conclusion, cette partie pratique a permis de valider la faisabilité de la conception et de l'implémentation d'une infrastructure réseau sécurisée pour une entreprise. Les objectifs ont été atteints avec succès, offrant une base solide pour des améliorations futures et pour de nouvelles recherches dans le domaine de la sécurité des réseaux. Cette expérience enrichissante servira de référence pour les futurs projets similaires et contribuera à l'avancement des pratiques en matière de sécurité des réseaux.

Conclusion Générale

La mise en place d'une nouvelle infrastructure sécurisée revêt une importance primordiale dans l'environnement technologique contemporain, marqué par l'évolution constante des menaces cybernétiques. Ce mémoire s'est ainsi penché sur les éléments clés liés à la conception et à la réalisation d'une telle infrastructure, en mettant particulièrement l'accent sur la sécurisation des réseaux d'entreprise.

Nous avons exploré les fondements théoriques, identifiant les topologies réseau, les équipements matériels et logiciels, ainsi que les protocoles de communication indispensables à la construction d'une infrastructure réseau solide. Parallèlement, nous avons analysé les défis sécuritaires auxquels font face les entreprises, en mettant en lumière les menaces potentielles et les meilleures pratiques pour y faire face.

L'étude de cas de l'entreprise Collable a mis en lumière les défis auxquels sont confrontées les organisations dans la sécurisation de leurs réseaux. En proposant une solution intégrée qui repose sur le concept de sécurité par couches, avec des mesures spécifiques pour chaque niveau. Cette stratégie offre une protection globale, couvrant tous les aspects du réseau, et garantit une défense solide contre les menaces cybernétiques, de la périphérie jusqu'au cœur du système.

Les tests réalisés ont validé l'efficacité de notre solution, tout en nous permettant d'approfondir notre compréhension des protocoles de sécurité et des technologies de communication. Cette expérience a également contribué à renforcer notre expertise dans ce domaine, et a ouvert de nouvelles perspectives pour des recherches futures dans le domaine de la sécurisation des infrastructures réseau.

Pour renforcer la sécurité des infrastructures réseau chez Collable à l'avenir, nous prévoyons d'intégrer des technologies avancées comme l'intelligence artificielle et le machine learning pour détecter proactivement les anomalies et les attaques. Nous améliorerons également l'audit et l'analyse des logs pour une surveillance accrue des activités réseau.

En conclusion, ce projet a apporté une contribution significative à la compréhension et à la mise en œuvre d'infrastructures réseau sécurisées chez Collable. En fournissant une méthodologie détaillée et une étude de cas pratique. Il offre un cadre solide pour protéger l'infrastructure numérique dans un contexte de menaces croissantes.

Annexe A

Environnement de travaille

A.1 Installation de VMware Workstation Pro

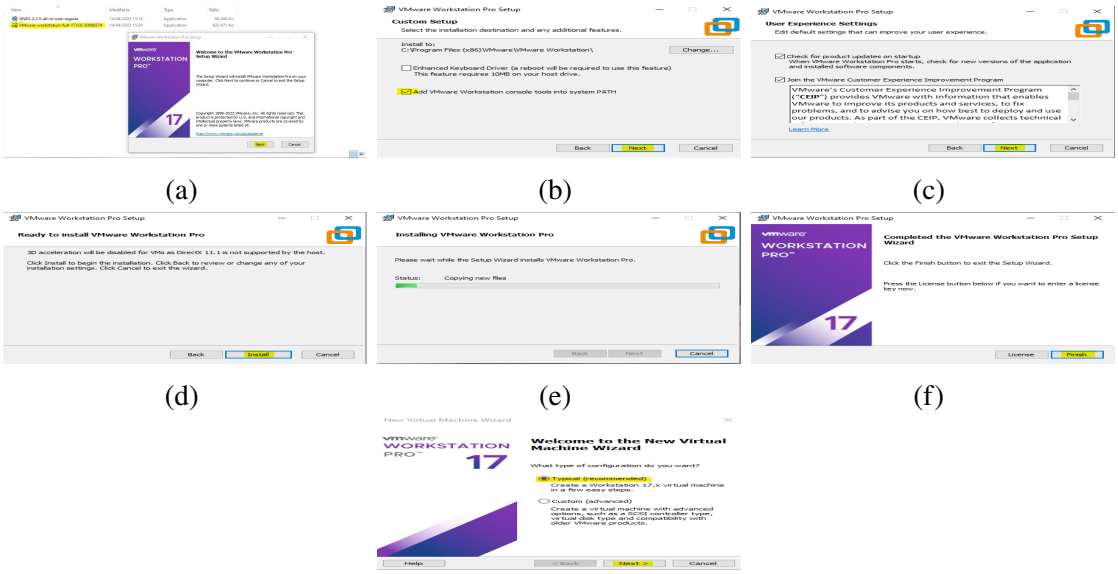
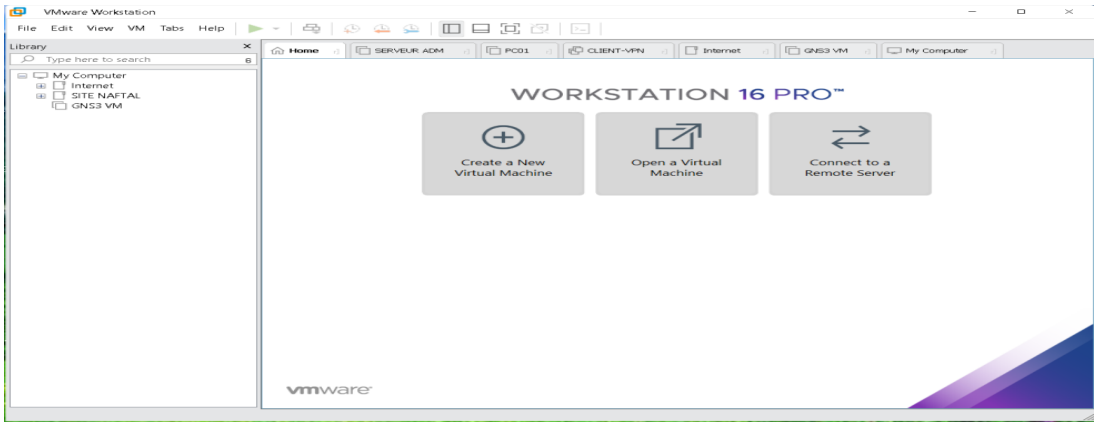


FIGURE A.1 – Étapes d'installation de VMware Workstation Pro

A la fin de l'installation, l'interface de VMware s'affiche comme suit :



A.2 Installation de GNS3

Vous pouvez télécharger GNS3 gratuitement sur le site www.gns3.com

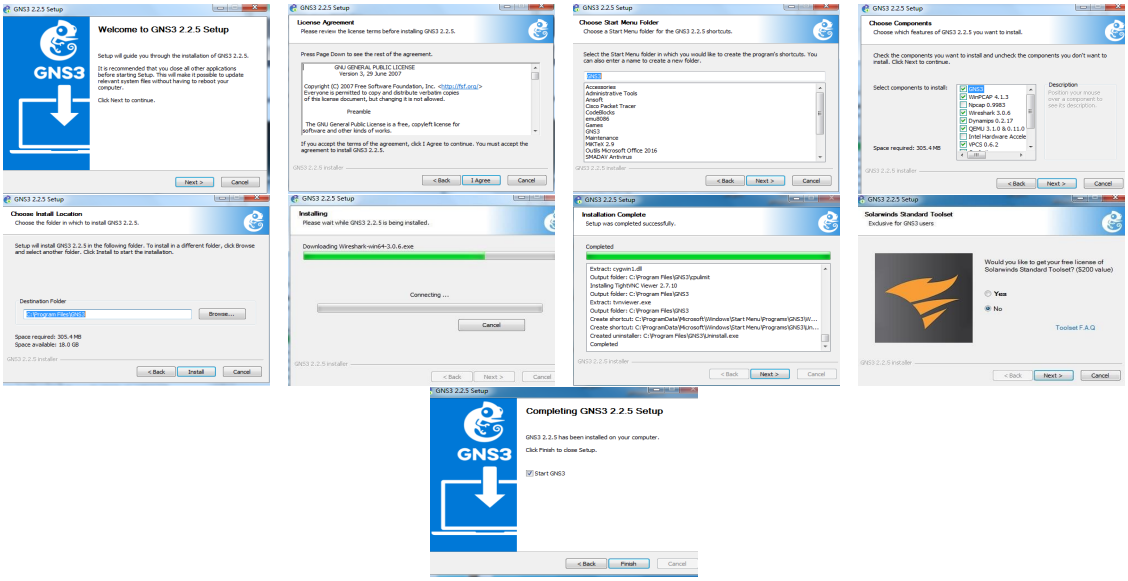
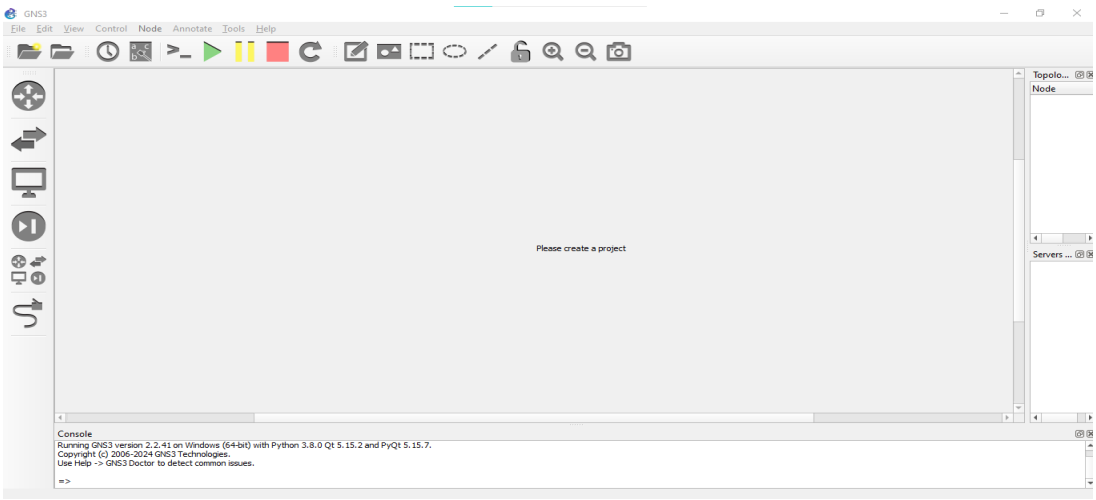


FIGURE A.2 – Étapes d'installation de GNS3

A la fin de l'installation, l'interface de Gns3 s'affiche comme suit :

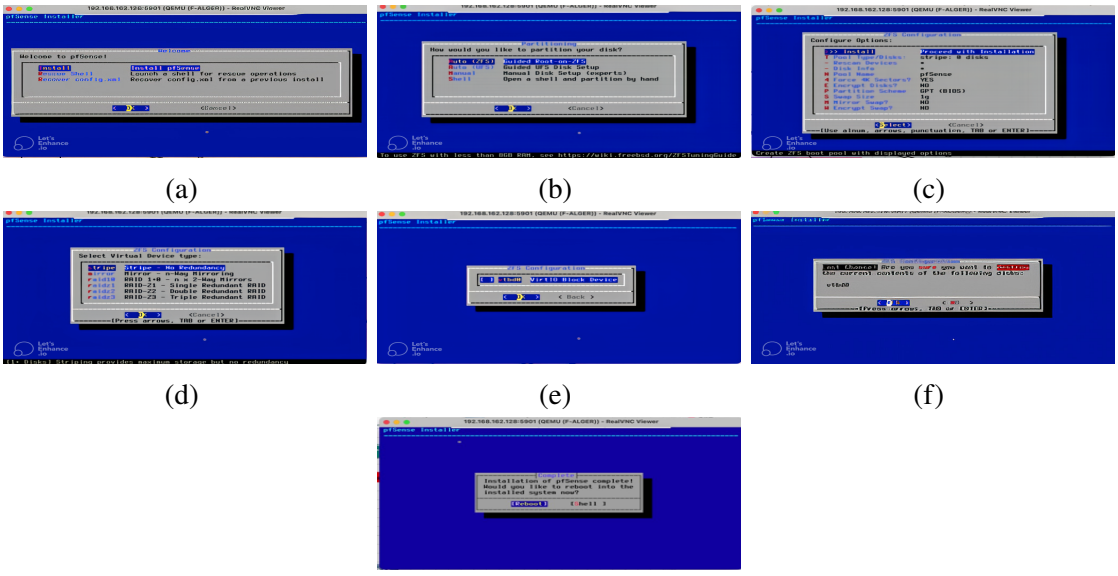


Annexe B

Installation des systémes

B.1 Installation de firewalls (Pfsense)

Pour installer le pare-feu pfSense, commencez par télécharger son image à partir de Google Chrome et décompressez-la en un fichier ISO.



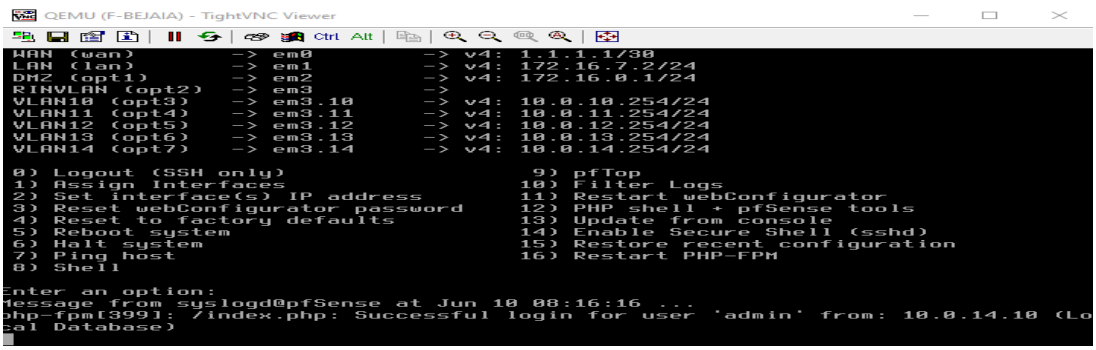
(a) (b) (c)

(d) (e) (f)

(g)

FIGURE B.1 – Étapes d'installation de Pare-feu Pfsense

A la fin de l'installation, l'interface de Pfsense s'affiche comme suit :



B.2 Installation des machines virtuelles

B.2.1 Installation de serveur

Accédez aux paramètres du serveur Active Directory, puis suivez ces étapes :

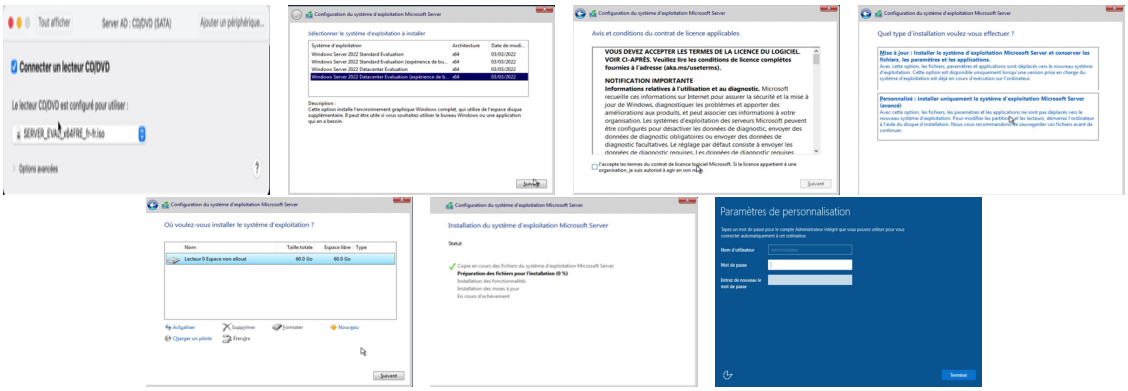
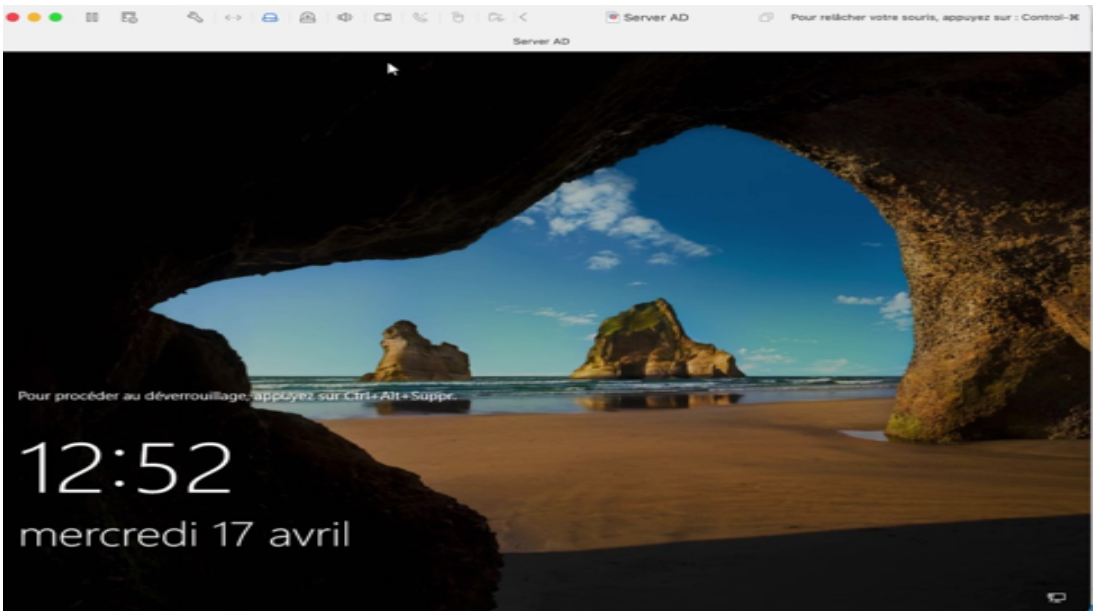


FIGURE B.2 – Étapes d'installation de Serveur AD

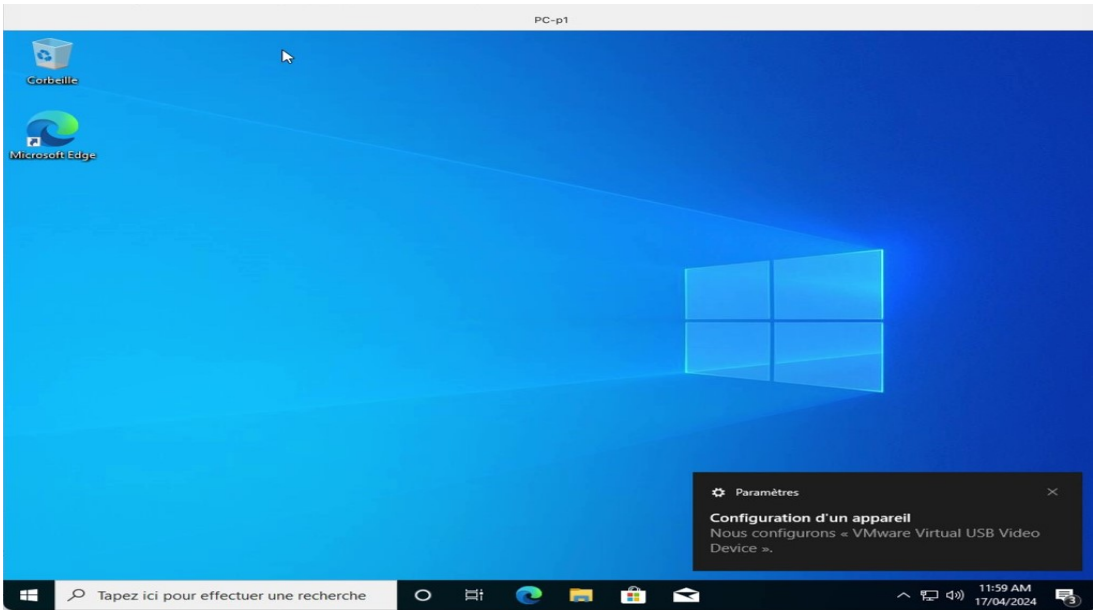
Le mot de passe à utiliser est "Rt2024PFE". A la fin de l'installation, l'interface de Serveur s'affiche comme suit :



B.2.2 Installation de PC1-P1

FIGURE B.3 – Étapes d'installation de PC1-P1

A la fin de l'installation, l'interface de PC s'affiche comme suit :



Nous avons dupliqué entièrement la machine virtuelle existante, préservant ainsi son système d'exploitation, ses logiciels et ses configurations, afin de créer des postes pour le réseau local de Bejaia et pour les clients VPN.

Une fois l'installation terminée, vous devez installer VMware sur les deux machines virtuelles. Pour ce faire, accédez à la machine virtuelle, sélectionnez l'option d'installation de VMware, puis cliquez sur "Installer". Ensuite, suivez simplement les étapes d'installation. Voici la même procédure à suivre pour le serveur AD, comme pour Pc1-P1.

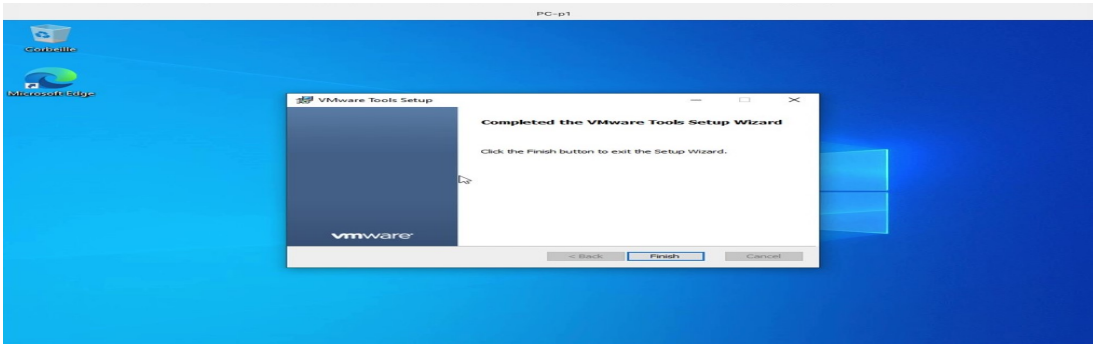


FIGURE B.4 – Installation de VMware sur PC1-P1

Annexe C

Configuration de base

C.1 Configuration VTP

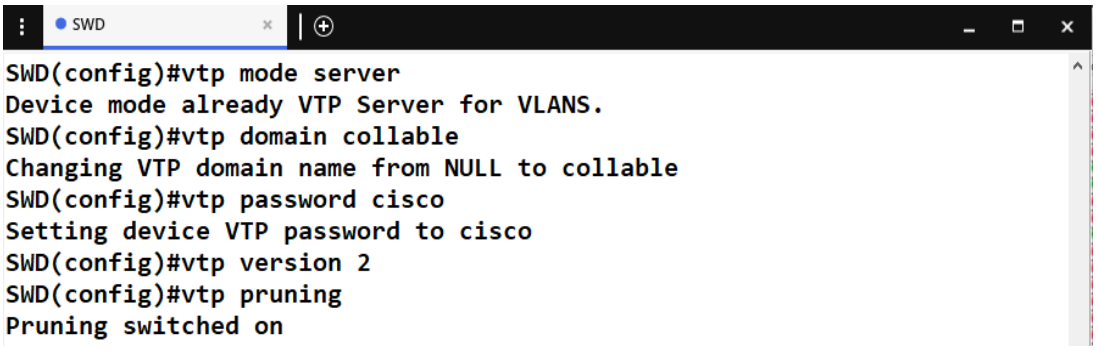


FIGURE C.1 – Configuration de VTP mode Server

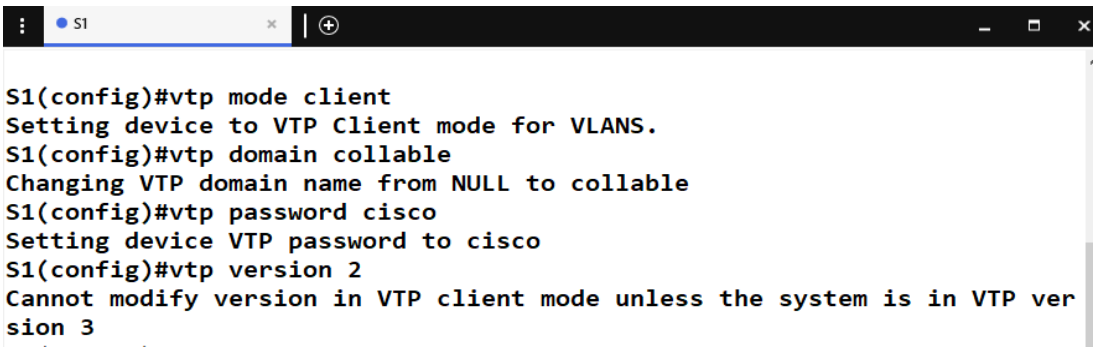


FIGURE C.2 – Configuration de VTP mode Client sur le commutateur S1

On applique les mêmes commandes au niveau du commutateur S2.

C.2 Configuration des VLANs

C.2.1 Configuration des interfaces en mode trunk

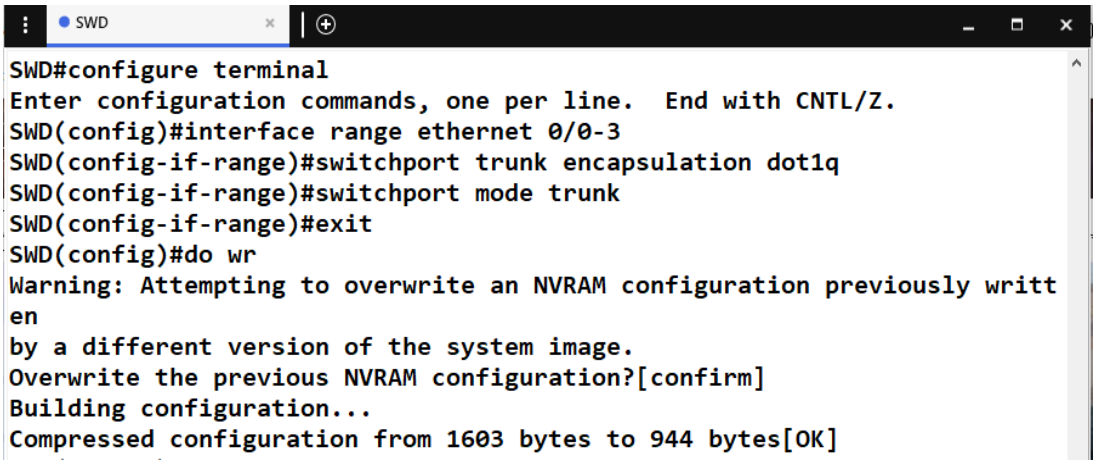


FIGURE C.3 – Configurations de trunk sur SWD

C.2.2 La création des VLANs

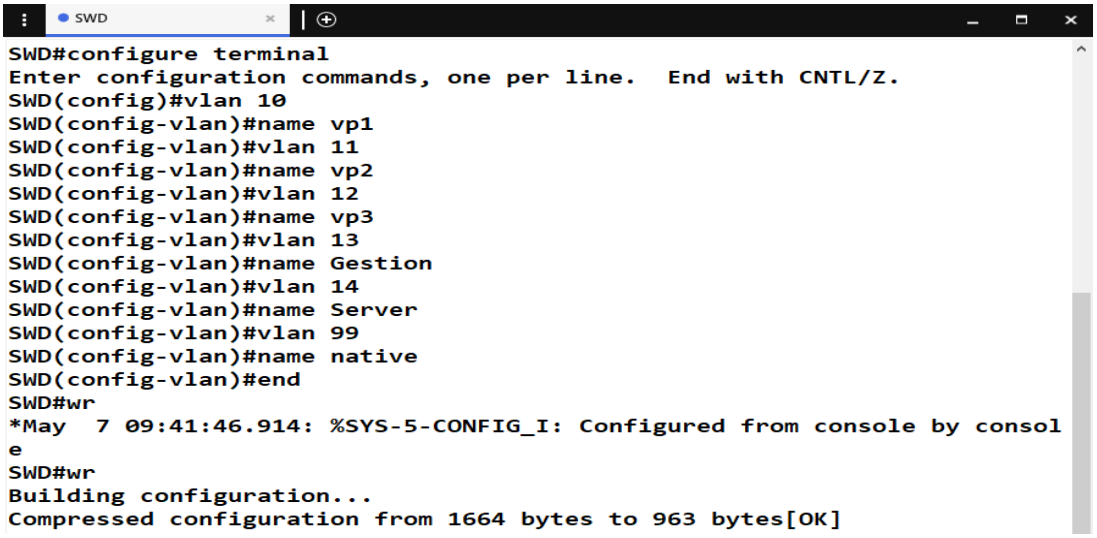


FIGURE C.4 – La création des VLANs sur le commutateur SWD

C.2.3 Affectation des ports aux VLANs

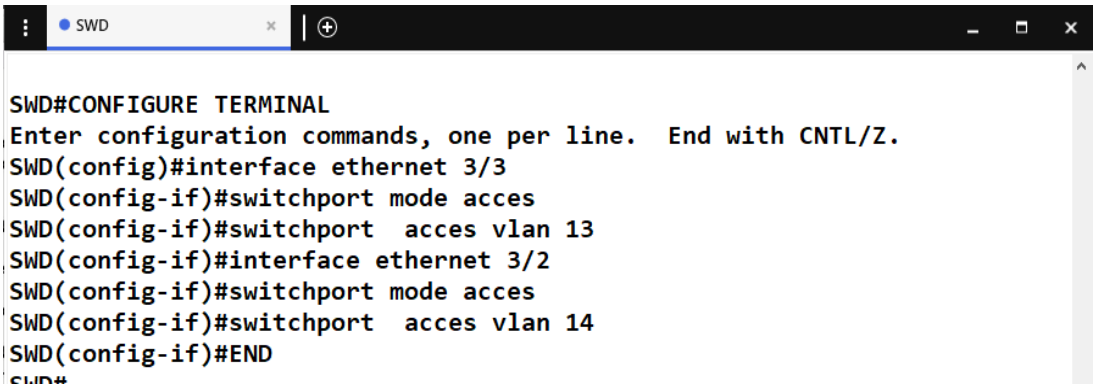


FIGURE C.5 – Affectation des ports de commutateur SWD aux VLANs

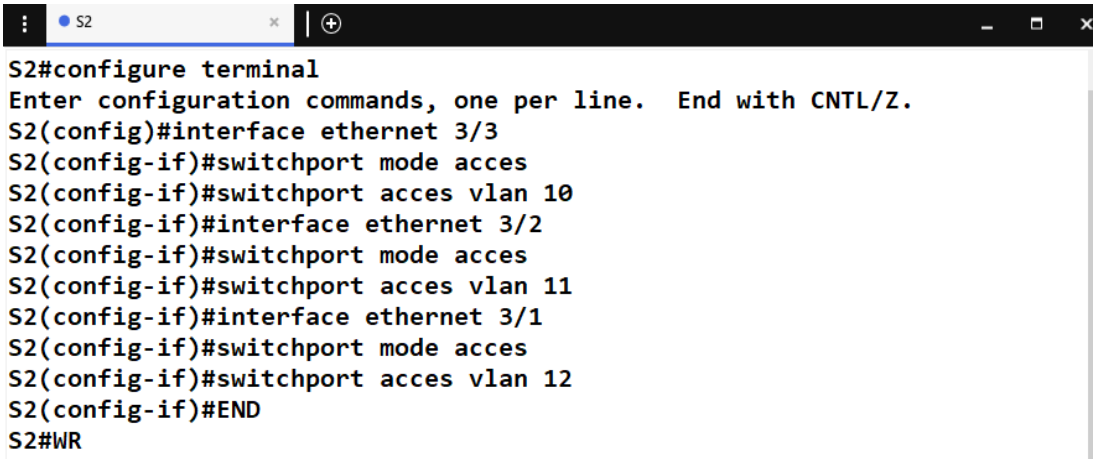
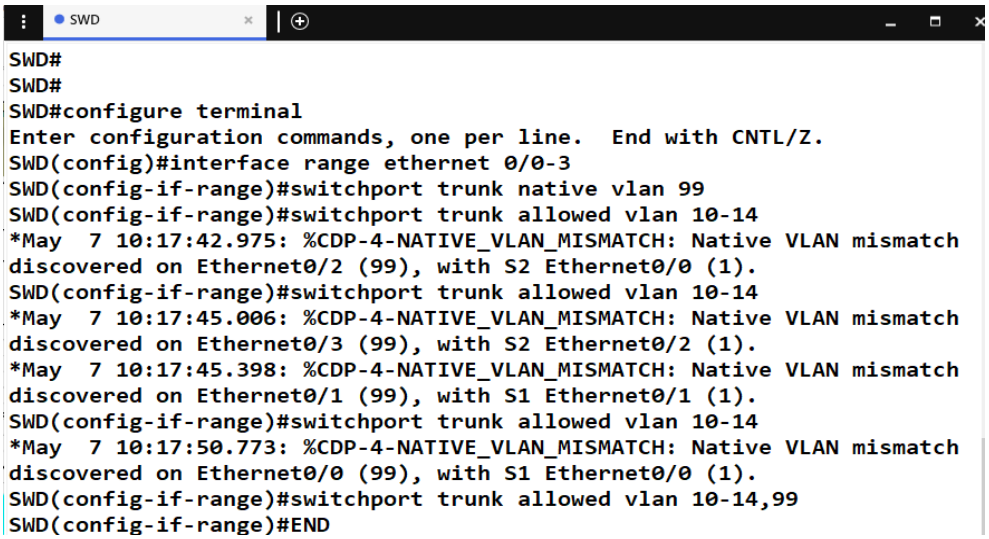


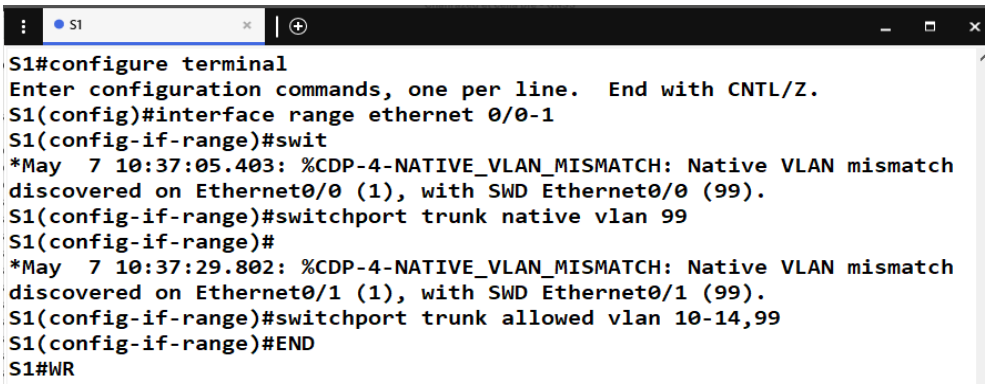
FIGURE C.6 – Affectation des ports de commutateur S2 aux VLANs

La même démarche est appliquée sur le commutateur S1.

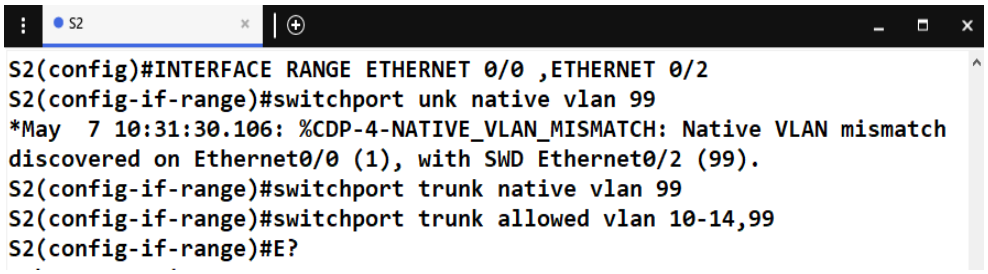
C.2.4 La configuration de VLAN native



(a) La configuration de VLAN native sur le commutateur SWD



(b) La configuration de VLAN native sur le commutateur S1



(c) La configuration de VLAN native sur le commutateur S2

FIGURE C.7 – Configuration de VLAN native sur les commutateurs SWD, S1, et S2

C.3 La configuration des liens d'agrégation LACP

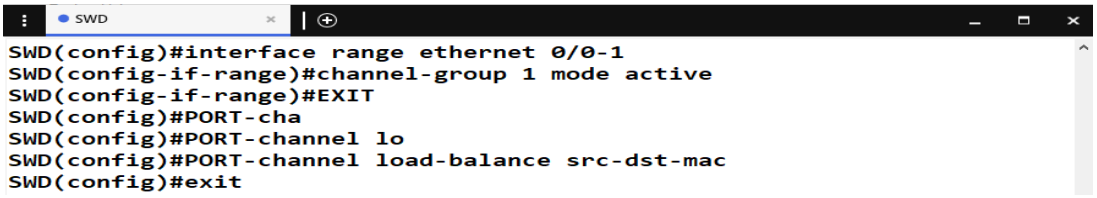


FIGURE C.8 – Configuration de LACP sur le commutateur SWD

C.3.1 Configuration de LACP sur l'autre coté (S1)

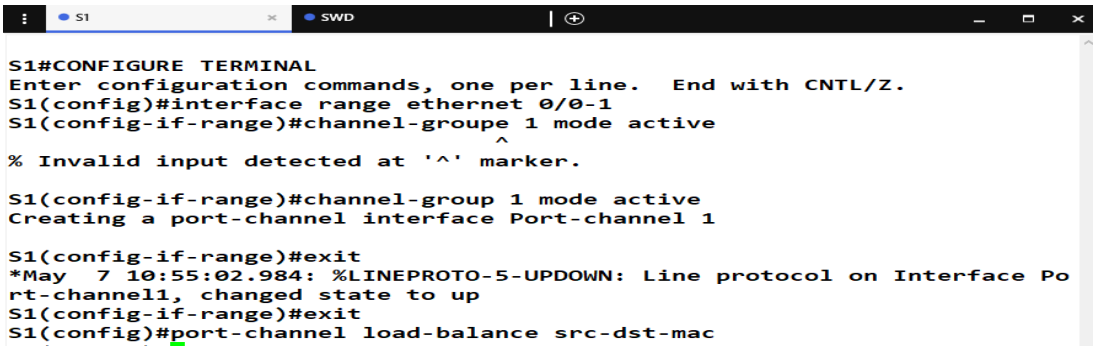


FIGURE C.9 – Configuration de LACP sur le commutateur S1

Nous procédons de la même manière qu'auparavant, mais cette fois-ci, nous assignons les interfaces (E0/2 et E0/3) reliant le commutateur SWD à S2, ainsi que les interfaces (E0/0 et E0/2) reliant S2 à SWD, au groupe 2 (G2).

C.4 Le port sécurité

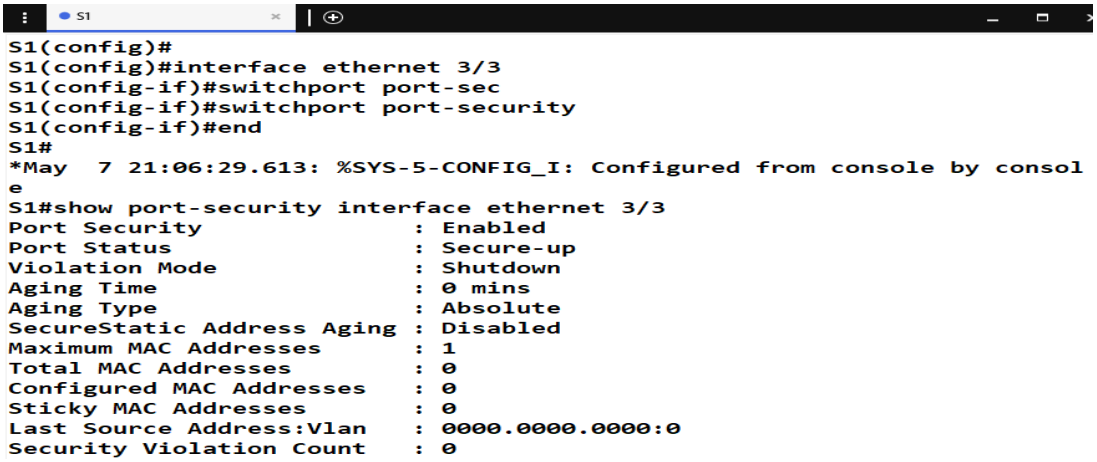


FIGURE C.10 – Activation de port sécurité pour l'interface E3/3 sur le commutateur S1

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface ethernet 3/3
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security maximum 1
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#end
S1#
*May  7 21:10:37.170: %SYS-5-CONFIG_I: Configured from console by consol
e
S1#wr
Building configuration...
Compressed configuration from 2106 bytes to 1172 bytes[OK]
```

FIGURE C.11 – La configuration du port sécurité sur le commutateur S1

C.5 Configuration des deux pare-feu

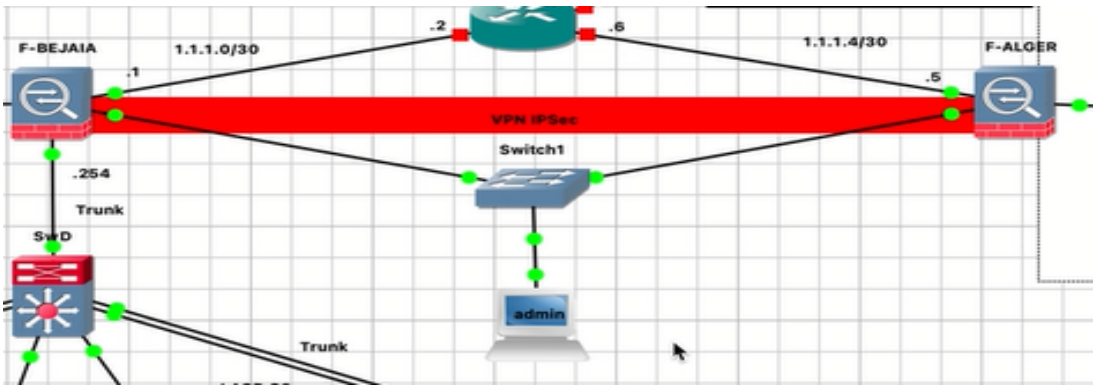


FIGURE C.12 – Emplacement du commutateur et du PC administratif ajoutés

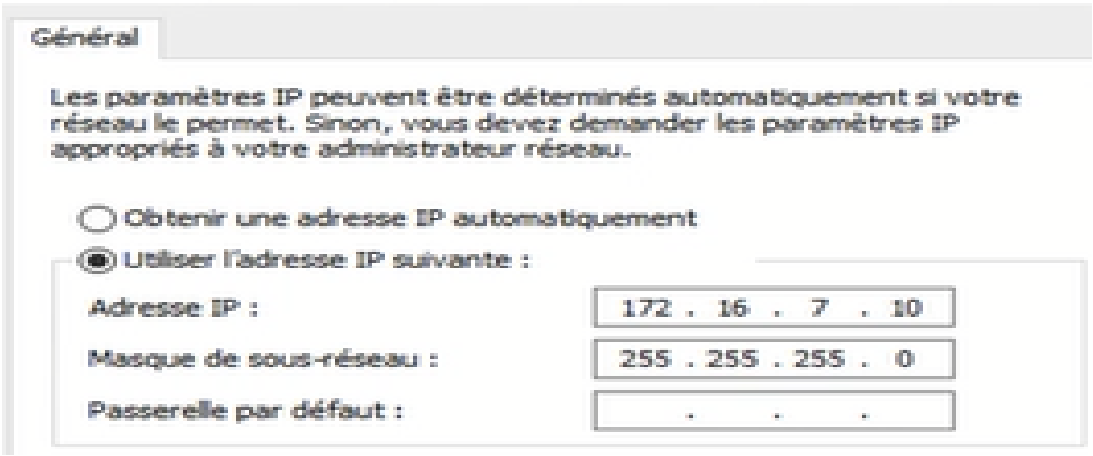


FIGURE C.13 – Attribution d'une adresse IP au PC Admin

FIGURE C.14 – Configuration des Paramètres de Base de pfSense de Bejaia

Nous avons suivi une procédure similaire pour celui d'Alger, mais cette fois-ci, nous lui avons attribué l'adresse 172.16.7.3.
Nous allons accéder au pare-feu de Bejaia à partir du PC administrateur en saisissant l'adresse IP de pfSense dans le navigateur. Utilisez le nom d'utilisateur 'admin' et le mot de passe 'pfsense' pour vous accéder et effectuer les configurations nécessaires. Lorsque vous accédez au pfSense, vous devez changer son mot de passe. Cliquez sur 'Change the password in the User Manager', puis changez le mot de passe en 'Admin123'. Ensuite, enregistrez les modifications en cliquant sur le bouton 'Save' au-dessus. Répétez la même procédure pour le pare-feu de Alger.

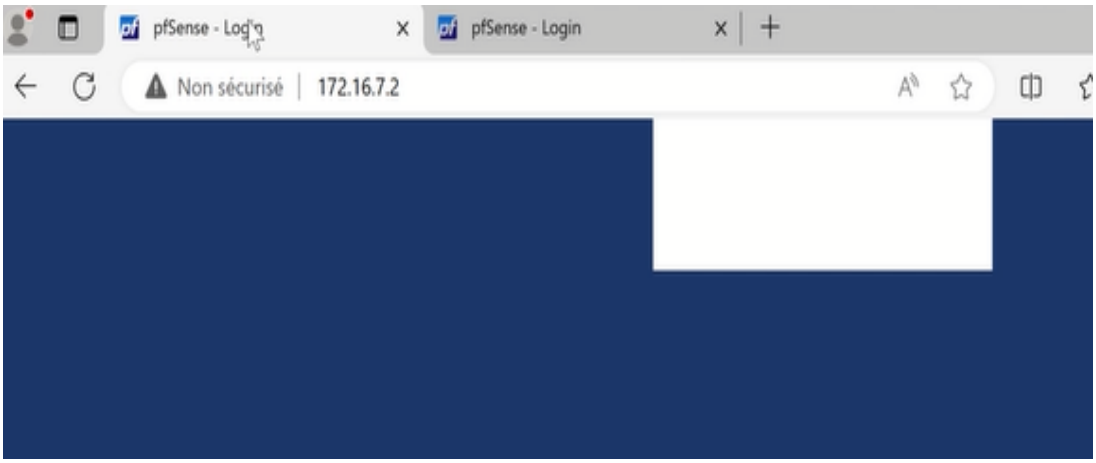


FIGURE C.15 – Accès au Pare-feu depuis le PC Admin

C.5.1 Configurations des interfaces des deux Pare-feu

Au niveau de pare-feu Bejaia

Pour configurer les interfaces réseau, nous avons deux interfaces existantes dans cette configuration : em0 et em1, dédiées respectivement aux connexions WAN et LAN. Nous allons ajouter deux interfaces supplémentaires, em2 et em3, en suivant les étapes suivant : tout d'abord, nous accédons à la section "Interfaces" et sélectionnons "Assignments". Ensuite, nous cliquons sur "Add" pour créer ces interfaces, en cliquant sur le bouton 'Save' pour chaque interface nouvellement créée.

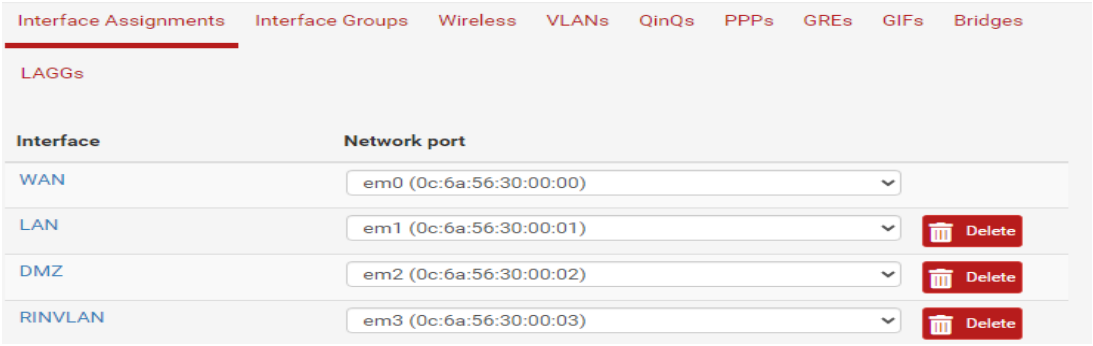
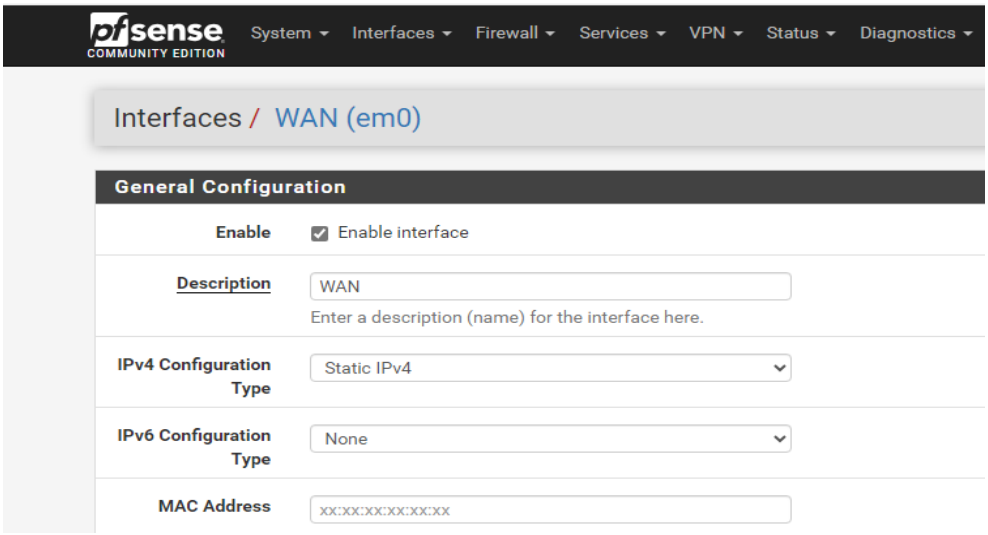
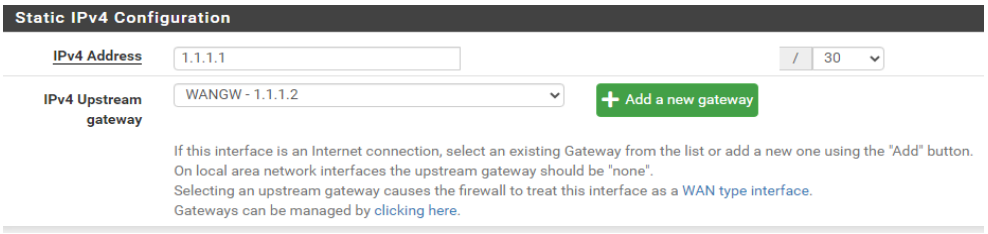


FIGURE C.16 – Création des Interfaces Réseau

Configuration de l'Interface WAN



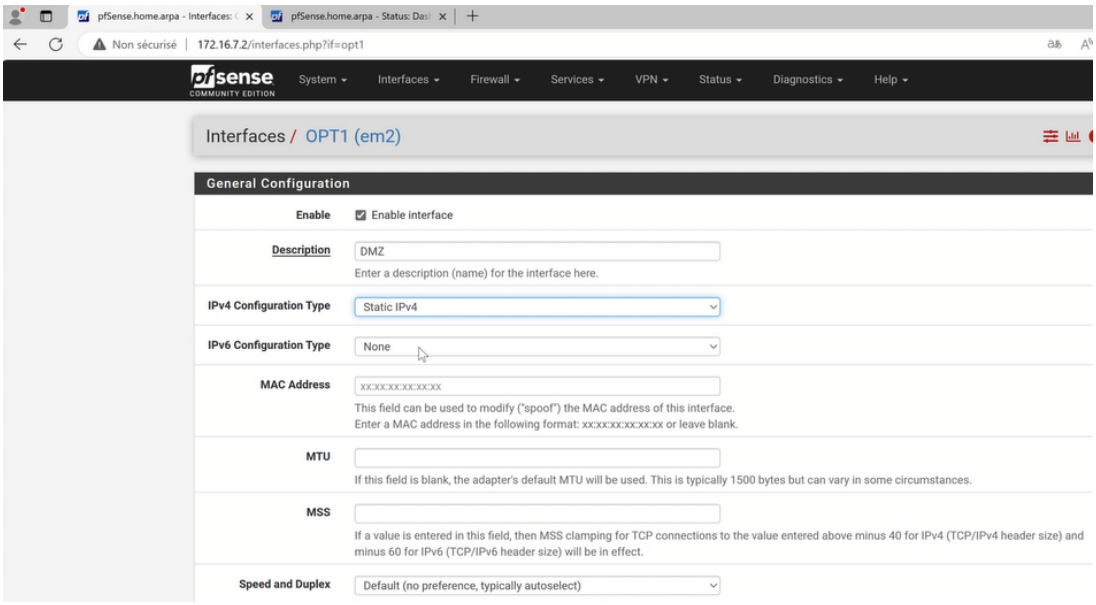
(a) L'interface WAN



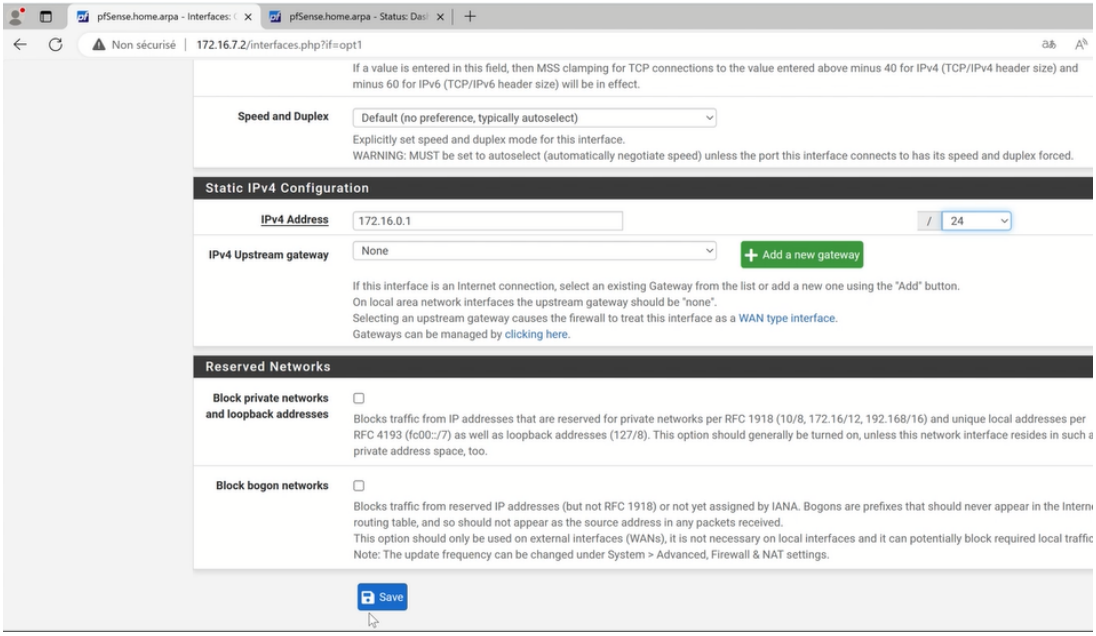
(b) Attribution d'Adresse au Interface WAN

FIGURE C.17 – Configuration de l'interface WAN

configuration de l'interface em2



(a) Activer l'interface em2 pour la DMZ



(b) Donner une adresse pour la DMZ et enregistrer

FIGURE C.18 – Configuration de l'interface de la DMZ

Au niveau de pare-feu Alger

La même procédure doit être suivie pour la configuration des interfaces au niveau du pare-feu à Alger.

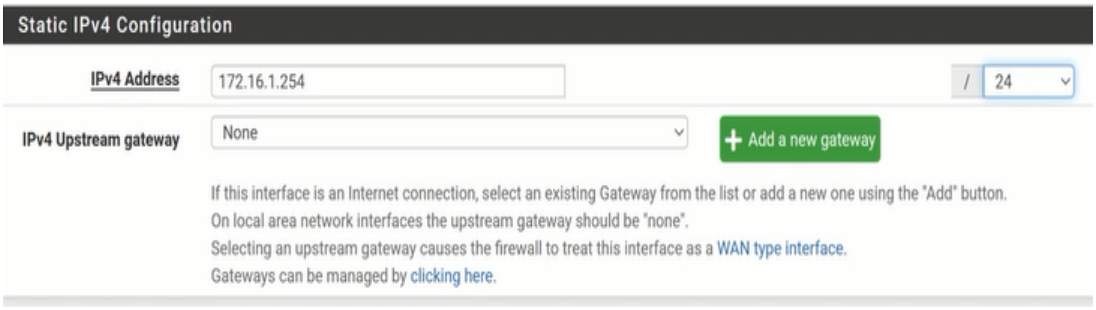
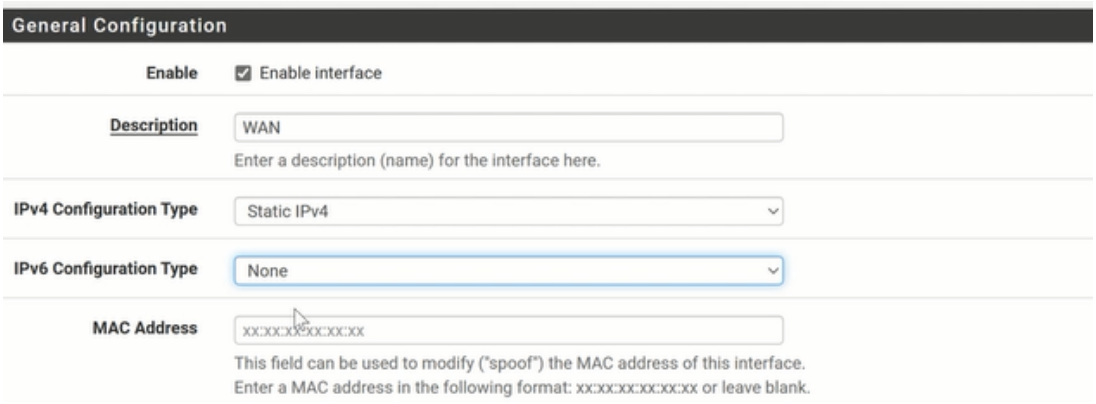
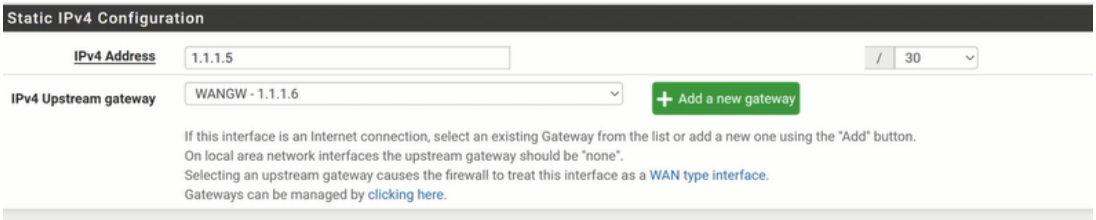


FIGURE C.19 – Attribution d'adresse au LAN à Alger



(a) Activation de l'interface WAN de pfSense Alger



(b) Attribution d'adresse à l'interface WAN de pfSense Alger

FIGURE C.20 – Configuration de l'interface WAN de pfSense Alger

C.6 Le routage inter-VLAN

C.6.1 Création des VLANs sous l'interface em3 sur le pare-feu de Bejaia

Pour créer des VLAN, vous accédez à "Interface Assignments", puis vous sélectionnez la catégorie "VLANs" et cliquez sur "Add". Ensuite, vous choisissez l'interface "em3" dans la case "Parent Interface", vous saisissez son numéro dans la case "VLAN Tag", et vous ajoutez son nom dans la case "Description". tel que VLAN 10 nommé VP1, VLAN 11 nommé VP2, VLAN 13 nommé VP3, VLAN 14 nommé gestion, et VLAN 15 nommé server. Enfin, n'oubliez pas d'enregistrer chaque configuration en cliquant sur le bouton 'Save'. Répétez cette étape pour chacun des cinq VLAN requis.

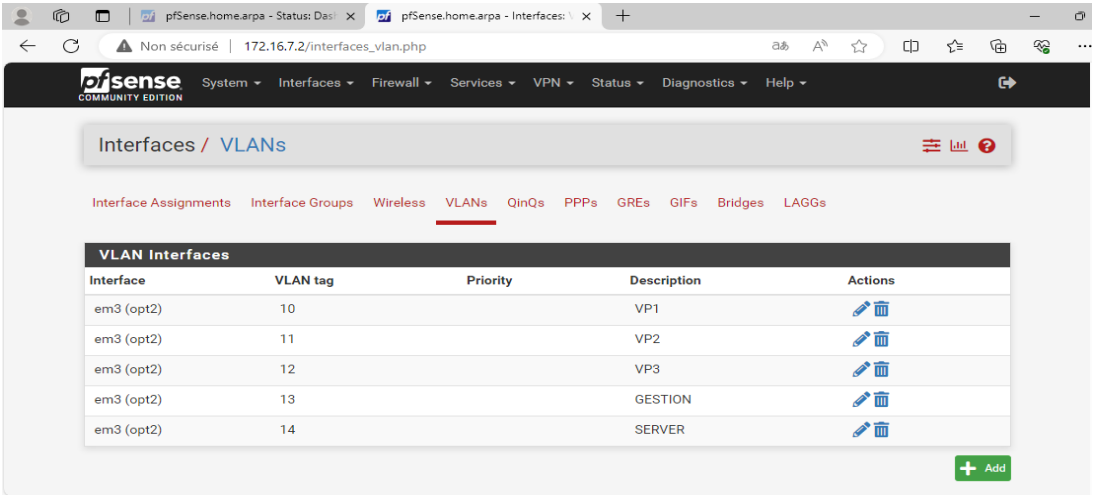


FIGURE C.21 – Création des VLANs sur Pfsense Bejaia

C.6.2 L'assignation des interfaces aux VLANs

Vous accédez aux paramètres d'interface dans la section 'Interfaces' de pfSense. Une fois dans les paramètres, vous créez des sous-interfaces sous em3, vous choisissez l'interface à ajouter, cochez la case "Enable Interface" pour l'activer, puis entrez son nom dans la case "Description", tel que VLAN 10, VLAN 11, VLAN 12, VLAN 13 et VLAN 14. Vous donner une adresse IP à chacune de ces interfaces. Une fois les modifications effectuées, en cliquant sur le bouton 'Save' pour les enregistrer.

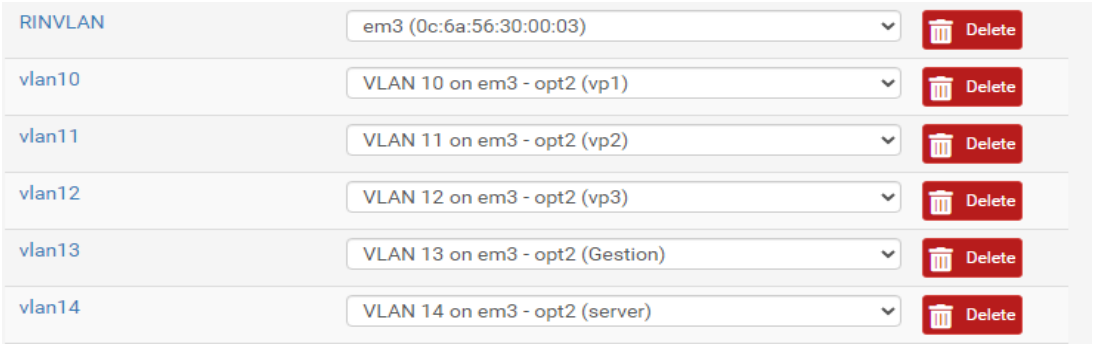


FIGURE C.22 – Les sous-interfaces créées dans l'interface em3

C.7 Configuration des Listes de Contrôle d'Accès (ACL)

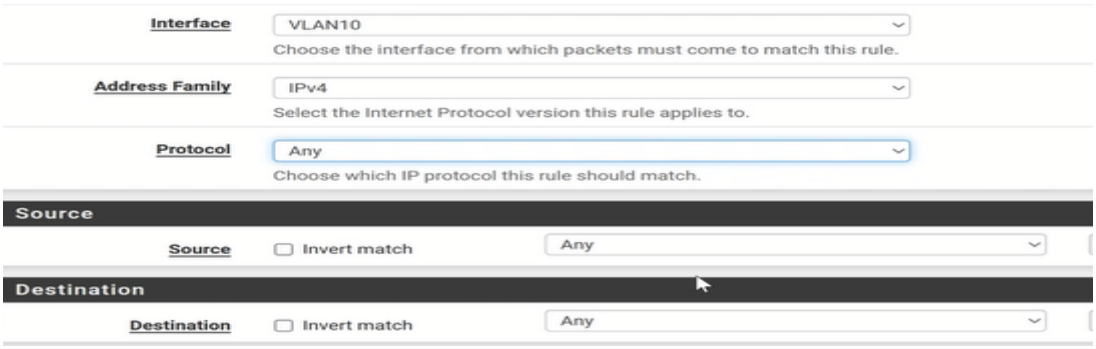


FIGURE C.23 – configuration des ACL au Niveau des VLANs

C.8 Configuration des services DHCP

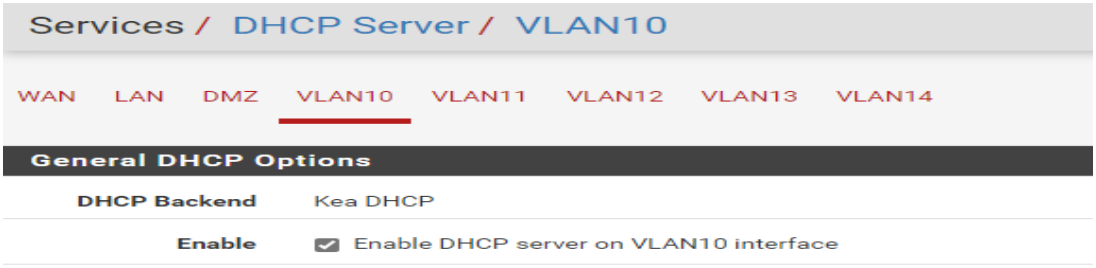


FIGURE C.24 – Autorisation des Services DHCP au Niveau des VLANs

Nous allons définir le pool d'adressage pour chacun de ces VLANs.

(a) Pool d'adressage du VLAN 10

(b) Pool d'adressage du VLAN 11

(c) Pool d'adressage du VLAN 12

(a) Pool d'adressage du VLAN 13

(b) Pool d'adressage du VLAN 14

FIGURE C.26 – Configuration du DHCP au Niveau des VLANs

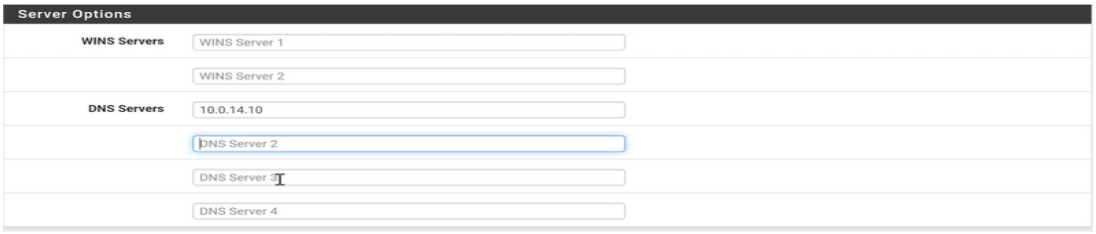


FIGURE C.27 – DNS de vlan 1O

Nous utiliserons la même adresse DNS pour tous les VLANs.

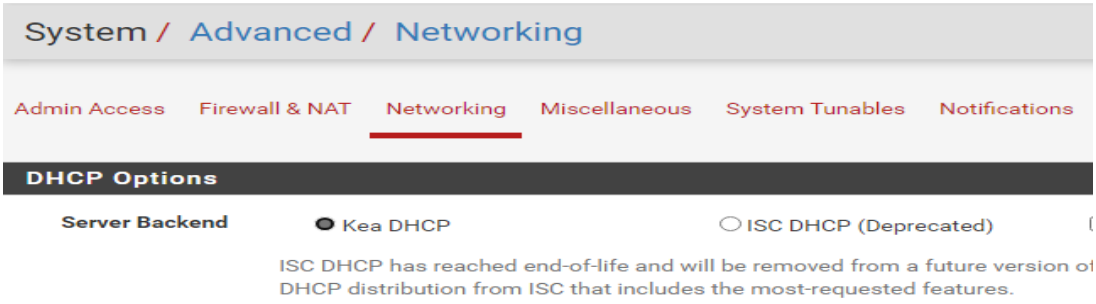


FIGURE C.28 – Activation du Service DHCP

Avec la commande "ip dhcp", le service DHCP attribuera automatiquement une adresse IP à chaque PC connecté.

```
PC1-p1>
PC1-p1> ip dhcp
DORA IP 10.0.10.10/24 GW 10.0.10.254

PC1-p1>
```

FIGURE C.29 – Attribution d'adresse au PC1-P1

C.9 La configuration de la DMZ(zone démilitarisée)

C.9.1 Configuration de VTP

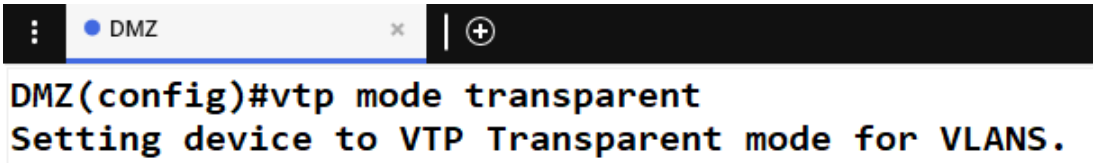


FIGURE C.30 – Configuration de VTP

C.9.2 Configuration de Private VLAN

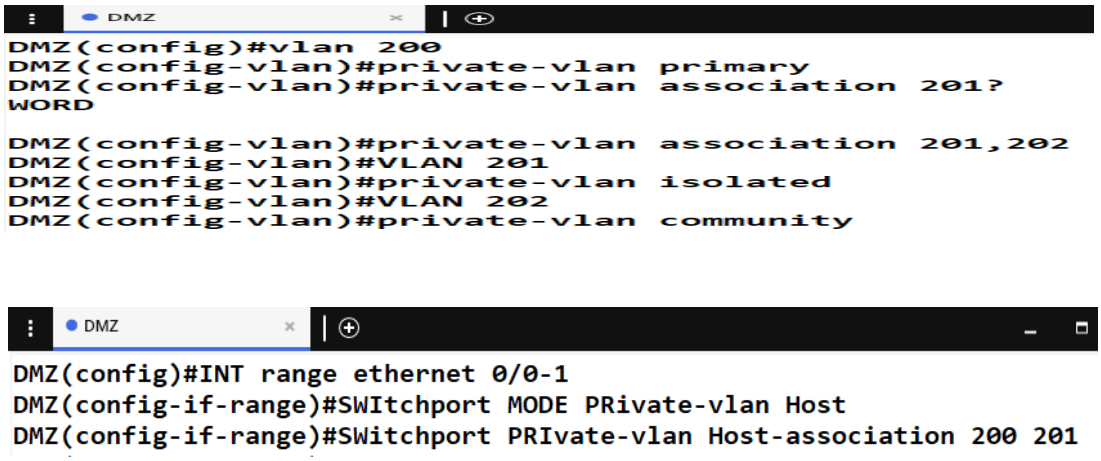


FIGURE C.31 – Configuration des interfaces E0/0-1 en mode host et lui associer au VLAN Isolated

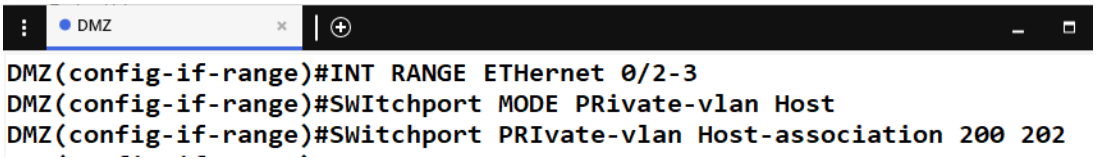


FIGURE C.32 – Configuration des interfaces E0/2-3 en mode host et lui associer au VLAN community

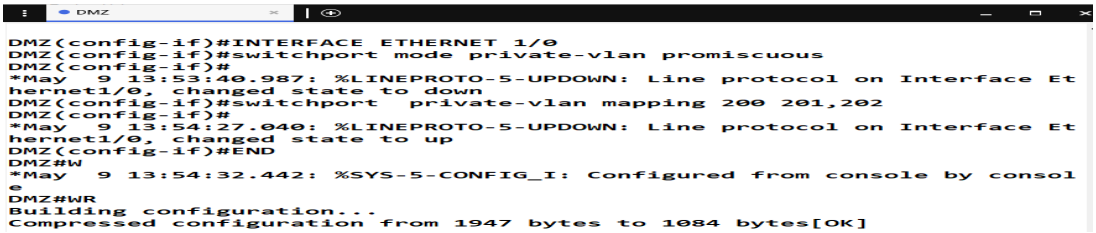
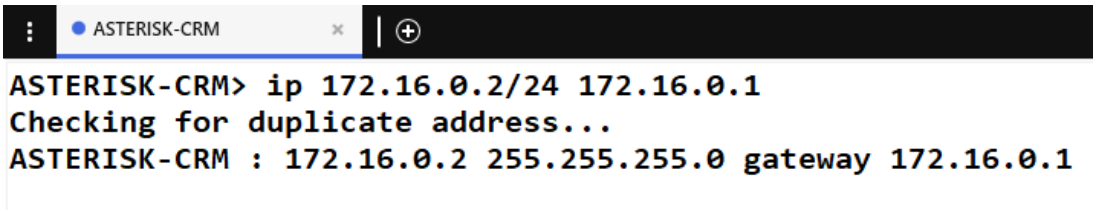
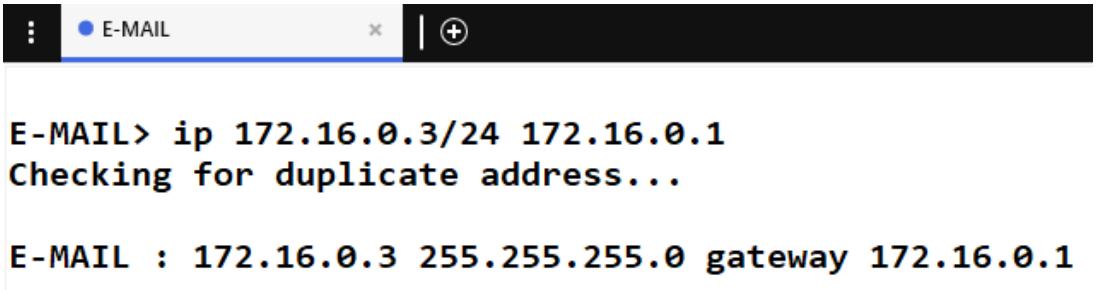


FIGURE C.33 – Configuration de l'interface E1/0 en mode promiscuous

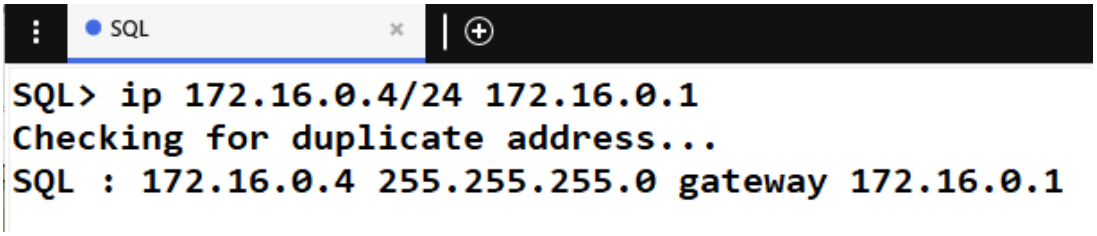
C.9.3 Attribution d'adresses aux différents serveurs



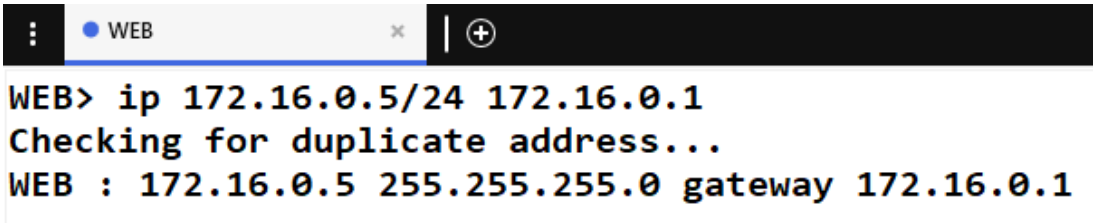
(a) Adresse du serveur ASTERISK-CRM



(b) Adresse du serveur E-MAIL



(c) Adresse du serveur SQL

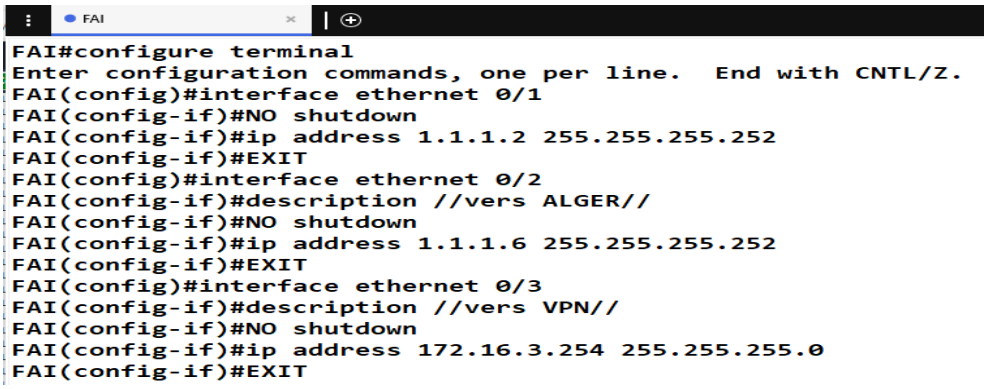


(d) Adresse du serveur WEB

FIGURE C.34 – Les adresses des différents serveurs

C.10 Configuration de FAI

C.10.1 Configuration des interfaces

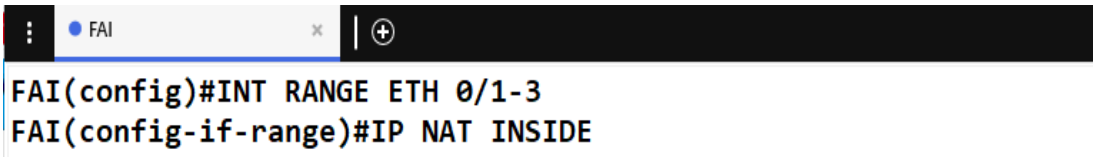


(a) Configuration des interfaces

(a) Configuration de l'interface internet

FIGURE C.36 – Configuration des interfaces de FAI

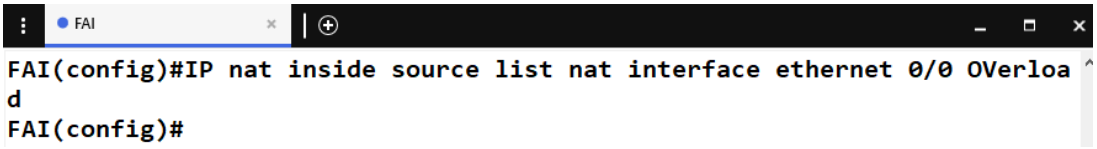
C.10.2 Configuration de NAT avec le PAT



(a) Configuration des interfaces E0/1, E0/2 et E0/3 en tant des interfaces NAT interne

(b) Configuration de l'interface E0/0 en tant qu'interface NAT externe

(a) Configuration de la liste d'accès standard pour le NAT



(b) Configuration du NAT avec surcharge (PAT) sur l'interface E0/0

FIGURE C.38 – Configuration du NAT avec le PAT

Annexe D

Configuration VPN

D.1 Configuration VPN site to site

Tout d'abord, nous allons attribuer une adresse IP aux VPCs situés dans le LAN d'Alger.

```
PC2> ip 172.16.1.12/24 172.16.1.254
Checking for duplicate address...
PC2 : 172.16.1.12 255.255.255.0 gateway 172.16.1.254
```

FIGURE D.1 – Configuration d'adresses IP pour le PC2 du LAN d'Alger

D.1.1 Création de la premier phase

Pour configurer IPsec, commencez par accéder aux pare-feu pfSense de Béjaïa et d'Alger depuis le PC admin. Ensuite, dirigez-vous vers l'onglet VPN et sélectionnez IPsec.

Pour créer la première phase, dans la section des tunnels, cliquez sur "Add P1". Dans la description, précisez la direction du tunnel, soit de Béjaïa vers Alger, soit d'Alger vers Béjaïa. Ensuite, spécifiez la version de l'échange des clés en choisissant IKEv2 des deux côtés. Définissez la passerelle (gateway) et la clé pré-partagée, que nous identifierons comme "collable123". Configurez également l'algorithme de chiffrement en veillant à ce qu'il soit le même des deux côtés.

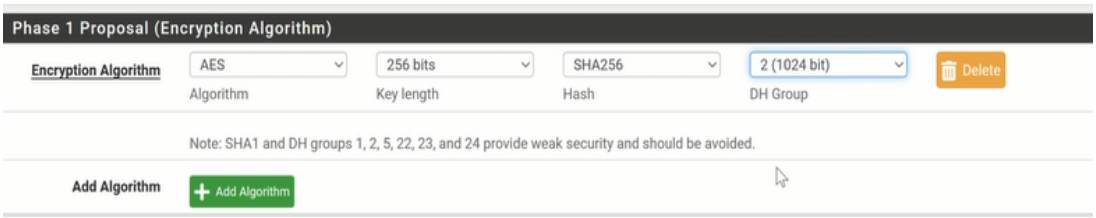
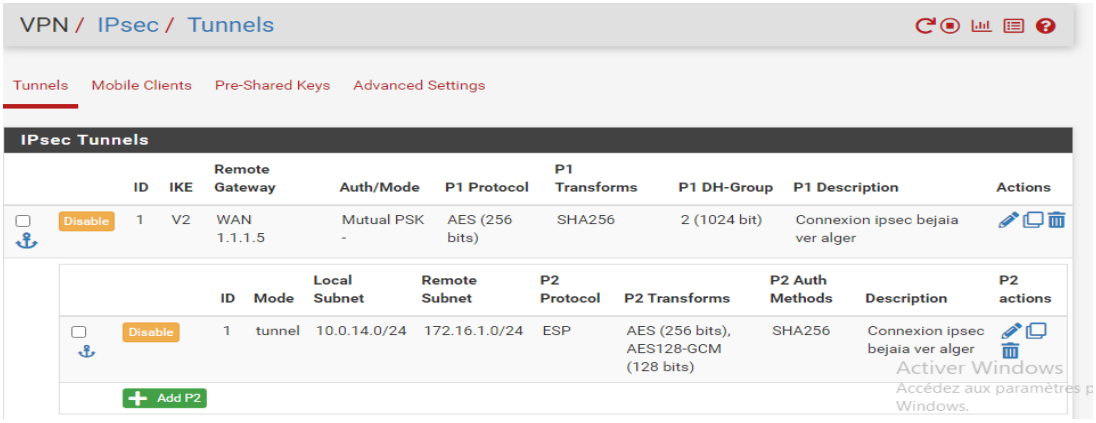


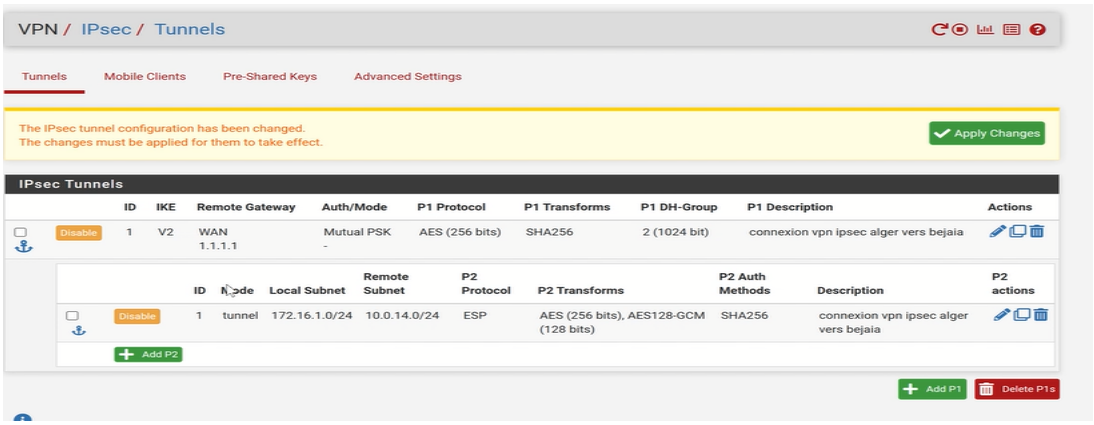
FIGURE D.2 – Algorithme de chiffrement

D.1.2 Création de la deuxième phase

Vous cliquez sur "Add P2". Sous l'onglet "Réseau", vous définissez le "sous-réseau local", qui correspond au réseau accessible depuis ce tunnel IPsec du côté où vous configurez la connexion. De même, vous spécifiez le "sous-réseau distant", qui représente le réseau situé de l'autre côté du tunnel IPsec. Il est important de noter que ces deux paramètres varient en fonction du côté où vous configurez la connexion IPsec. Dans la phase de proposition, vous configurez le protocole ESP (Encapsulating Security Payload) ainsi que les algorithmes de chiffrement, en veillant à ce qu'ils correspondent à ceux définis précédemment. Une fois ces configurations effectuées, vous les enregistrez. Vous répétez la même procédure de l'autre côté, d'Alger vers Béjaïa.



(a) Configuration d'IPsec sur pfSense de Béjaïa vers Alger

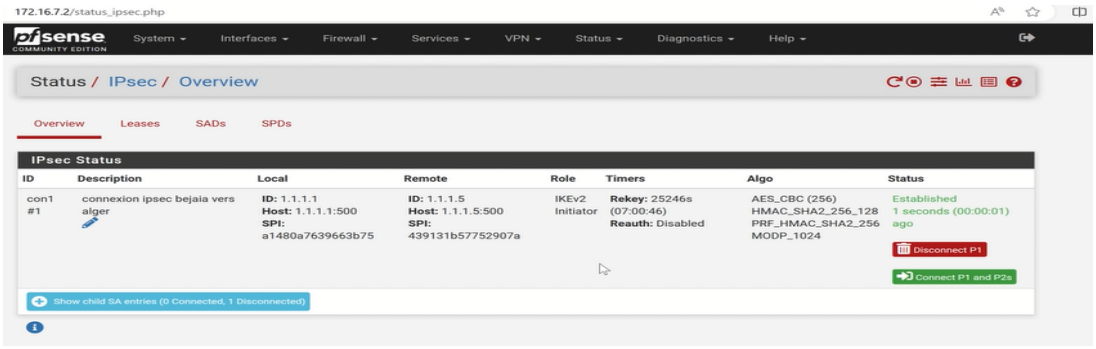


(b) Configuration d'IPsec sur pfSense de Alger vers Bejaia

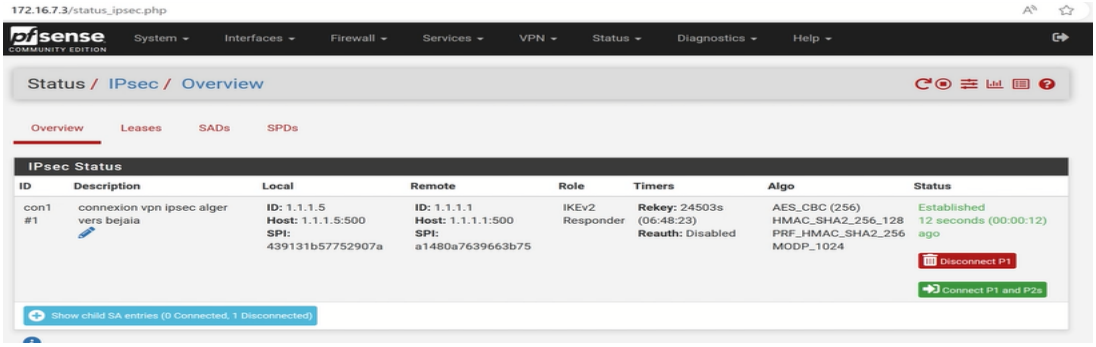
FIGURE D.3 – Configuration de tunnel VPN

D.1.3 Connexion des deux phases

En cliquant sur "Connect P1 and P2".



(a) Connexion des Phases 1 et 2 d'IPsec sur pfSense de Béjaïa



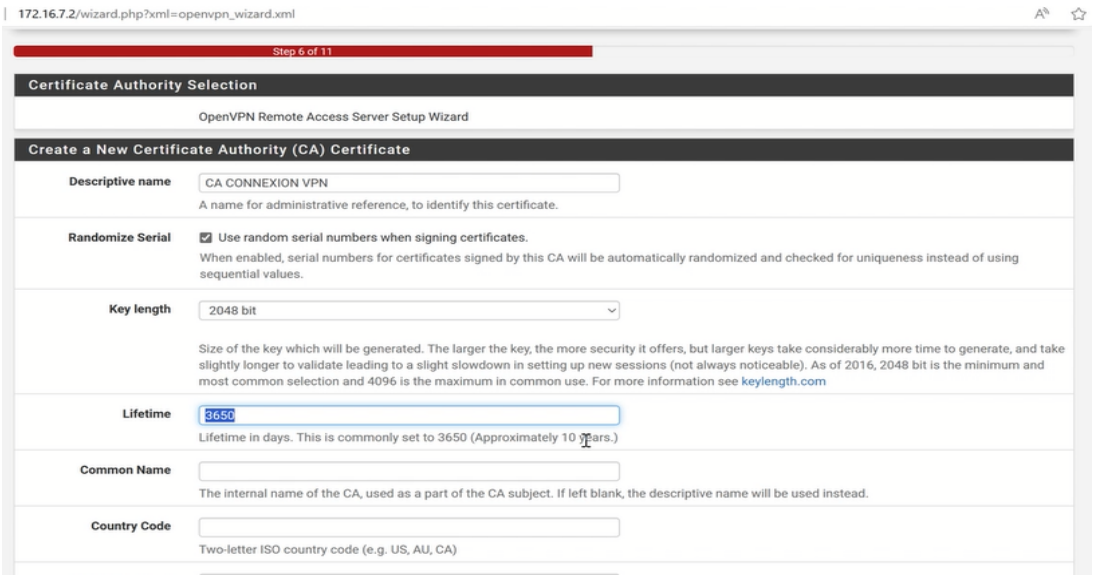
(b) Connexion des Phases 1 et 2 d'IPsec sur pfSense de Alger

FIGURE D.4 – Connexion des Phases IPsec

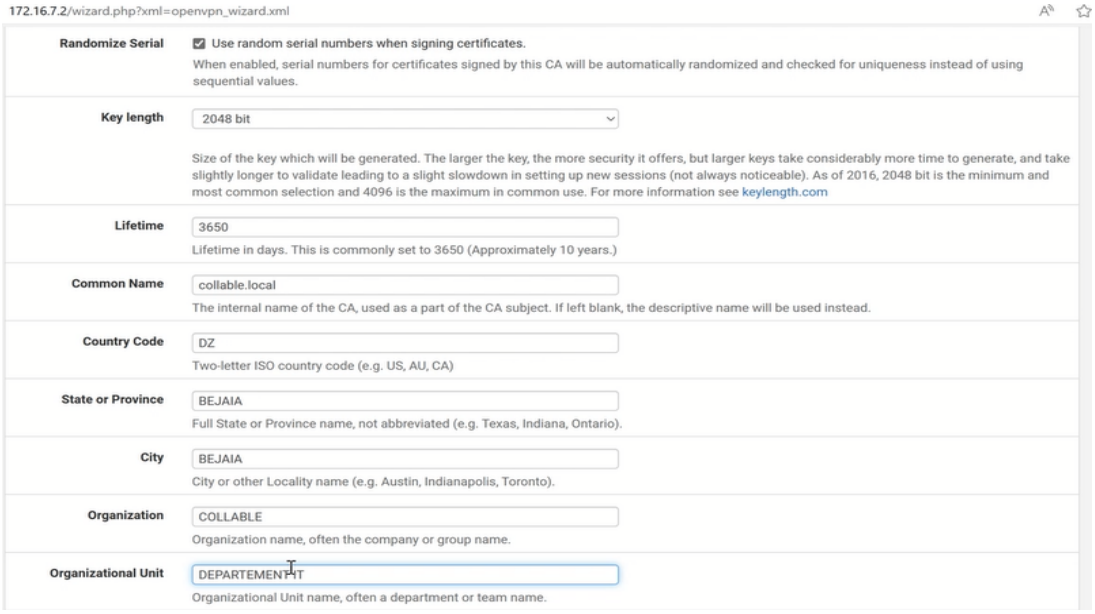
D.2 Configuration du Client VPN

D.2.1 Création d'un certificat d'autorité (CA) pour les connexions VPN

Au niveau de pfSense Bejaia, pour accéder au VPN, vous sélectionnez OpenVPN et vous allez dans la catégorie "Wizards".Vous sélectionnez "Local User Access" comme type de serveur, puis vous cliquez sur "Next" pour générer un certificat pour le VPN.



(a) Attribution d'une description au certificat



(b) Attribution des paramètres de localisation au certificat

FIGURE D.5 – Création d'un certificat pour le VPN

D.2.2 Création d'un certificat d'autorité (CA) pour le serveur

Vous cliquez sur 'Add a new CA', puis sur 'Add a new certificate' pour ajouter un certificat au serveur.

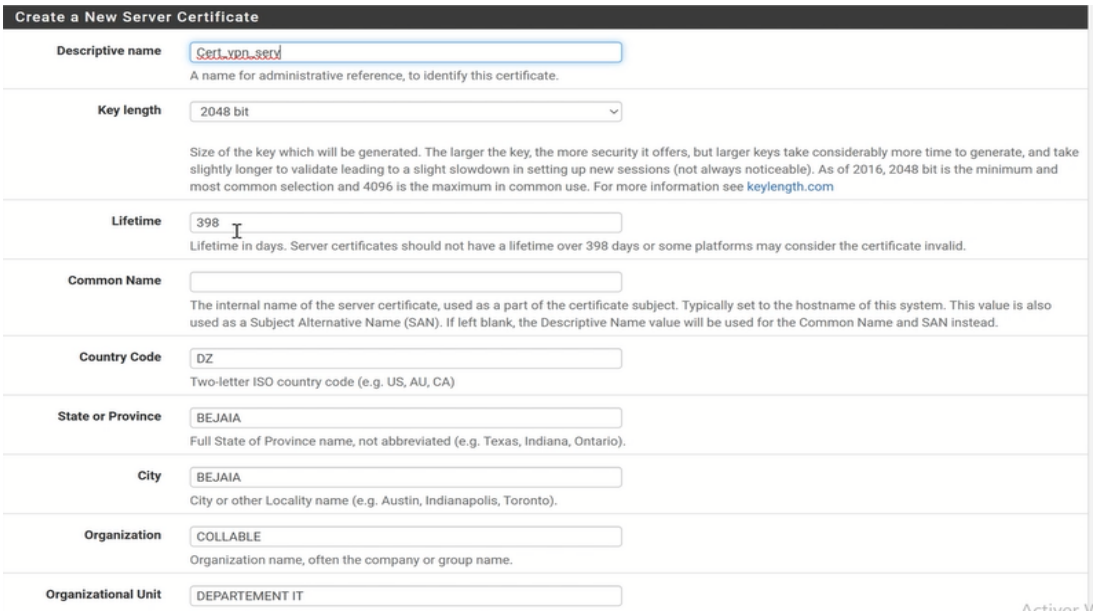
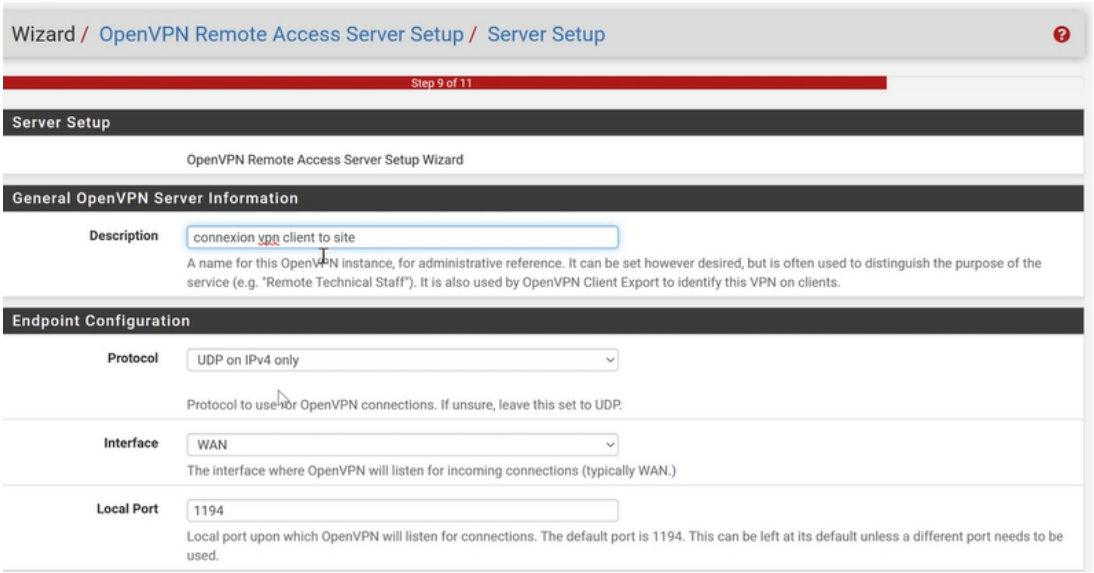


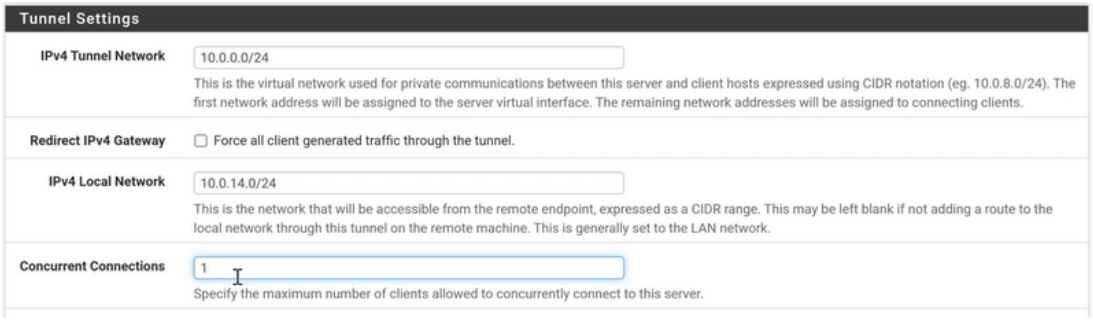
FIGURE D.6 – création de certificat au serveur

D.2.3 Configuration du serveur

cliquez sur "Create new certificate" Pour commencer la configuration du serveur.

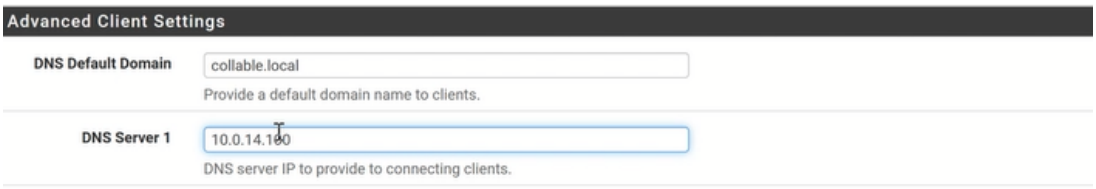


(a) configuration des ports et des protocoles



(a) Attribution des paramètres de localisation au certificat

FIGURE D.8 – Configuration de la plage d'adresses IP autorisées à se connecter au serveur



(a) Configuration des Paramètres DNS

FIGURE D.9 – Configuration des Paramètres du serveur

D.2.4 Règles de filtrage

en cochant ces deux cases. Ensuite, appuyez sur "Next" puis sur "Finish" pour terminer la configuration.

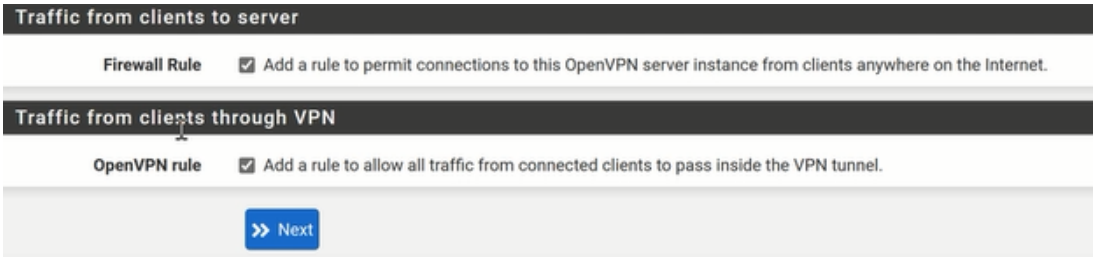


FIGURE D.10 – Génération de deux règles de filtrage au serveur

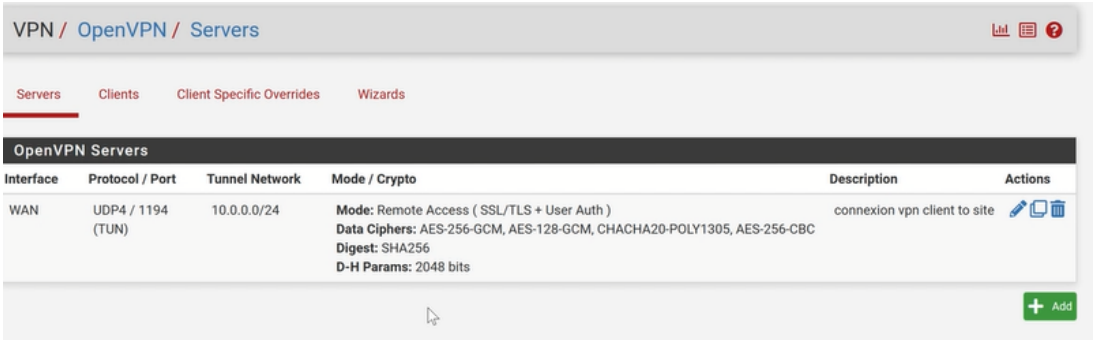


FIGURE D.11 – Configuration de serveur

D.2.5 Configuration des clients

Vous devrez télécharger le package Windows 10 pour les deux utilisateurs.

Création des Utilisateurs

Pour créer des utilisateurs, accédez à "Système", sélectionnez "User Manager", puis appuyez sur "Add". Entrez le nom d'utilisateur et le mot de passe, puis attribuez-lui un certificat.

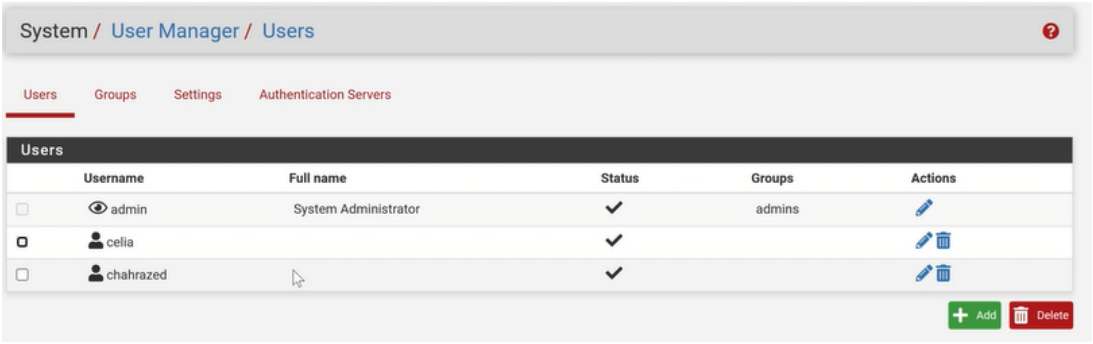


FIGURE D.12 – Création des Utilisateurs

Téléchargement et installation du package OpenVPN

Pour télécharger le package OpenVPN, accédez à "Système", puis sélectionnez "Package manager". Dans la barre de recherche, saisissez "OpenVPN" et cliquez sur "Installer".

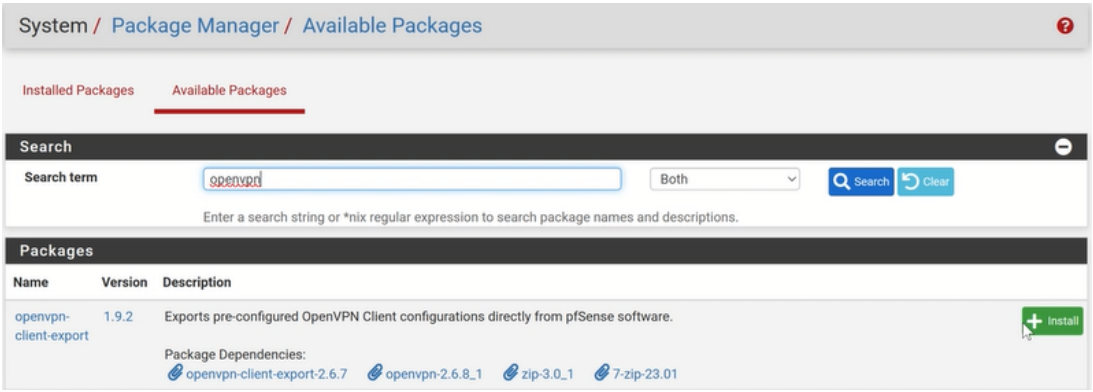


FIGURE D.13 – Téléchargement et installation du package OpenVPN

Téléchargement du package windows 10

Une fois le package installé, accédez à la section "VPN", puis sélectionnez "OpenVPN". Vous verrez qu'une nouvelle catégorie, "Client Export", a été ajoutée. Accédez à cette catégorie et téléchargez le package Windows 10 pour les deux utilisateurs.

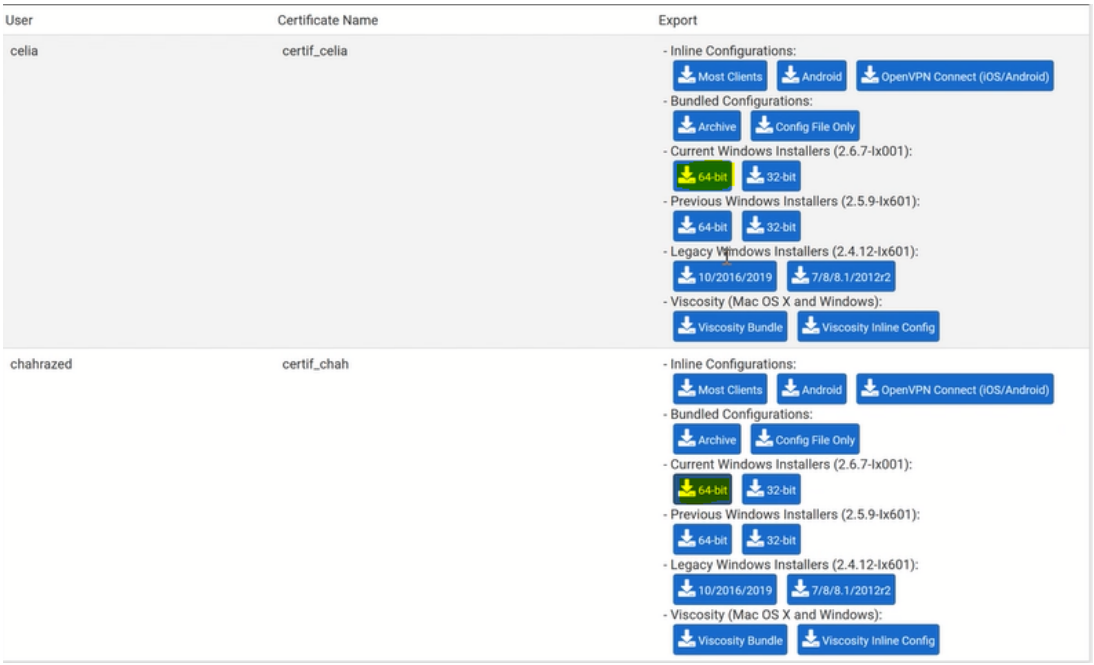


FIGURE D.14 – Téléchargement du package windows 10 pour les utilisateurs

On va accéder au PC VPN depuis VMware et lui attribuer une adresse IP.

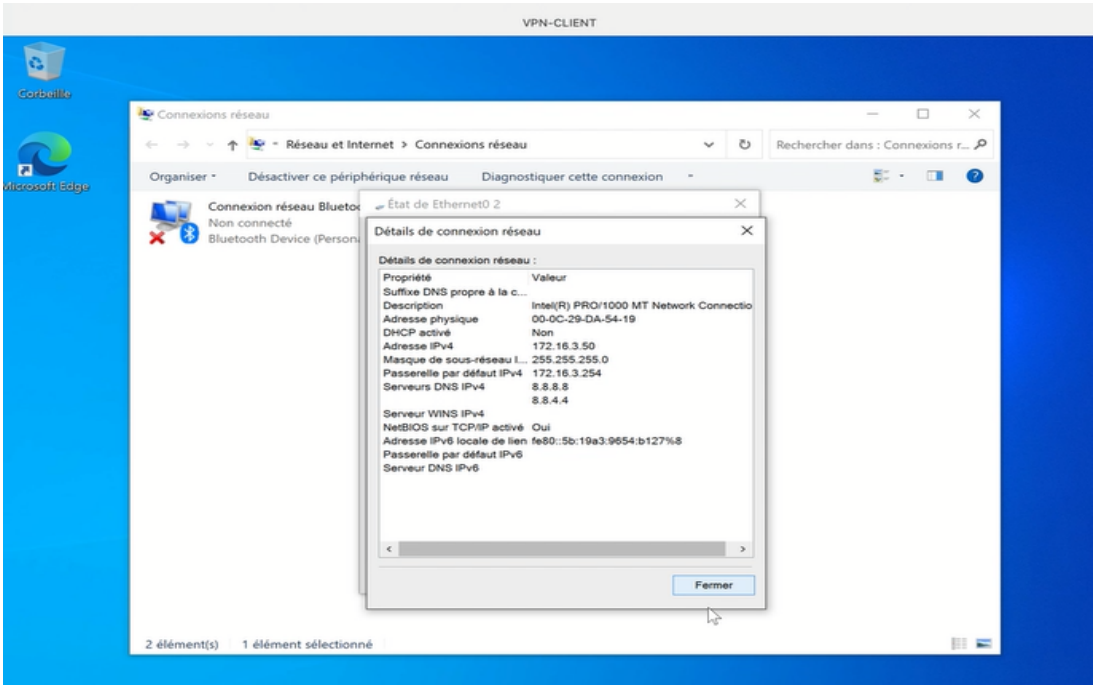
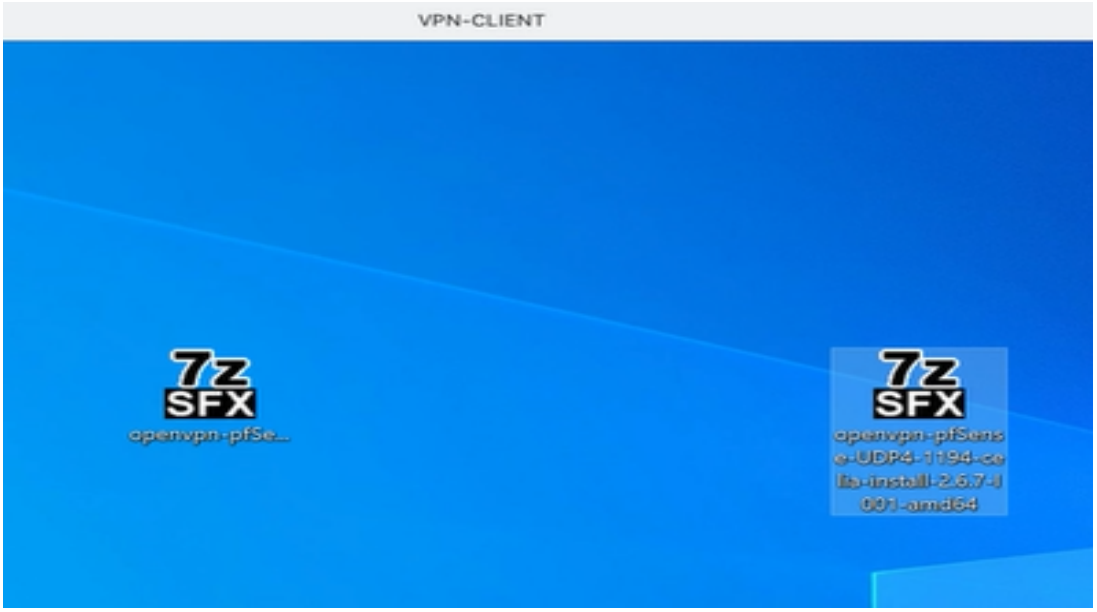


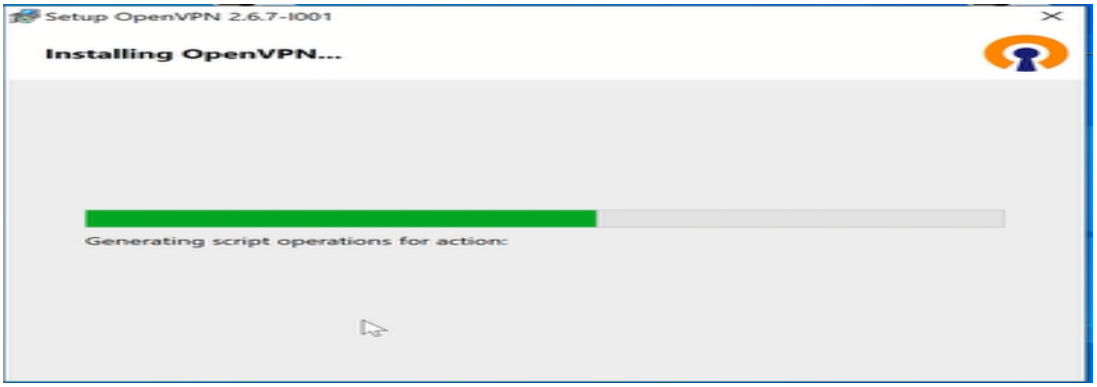
FIGURE D.15 – Attribution d'adresse IP au PC VPN.

Installation du logiciel client VPN sur les appareils des utilisateurs

Nous allons installer les deux pacages d'utilisateurs sur le PC VPN.



(a) Téléchargement des deux pacages utilisateurs sur le PC VPN



(b) Installation du logiciel OpenVPN sur le PC VPN

FIGURE D.16 – Installation du logiciel client VPN sur le PC VPN

Connecter au serveur

Vous devrez saisir le nom d'utilisateur et le mot de passe pour vous connecter.

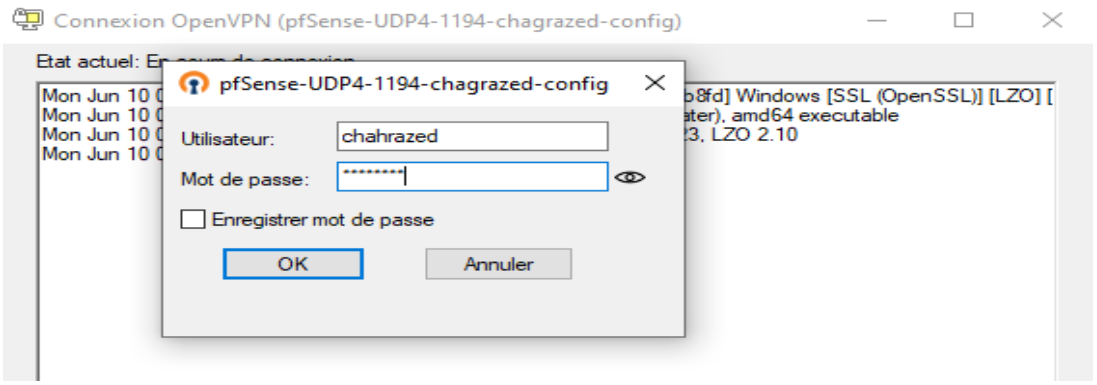


FIGURE D.17 – Connexion de l'utilisateur "Chahrazed"

D.2.6 Visualisation des utilisateurs connectés au client VPN

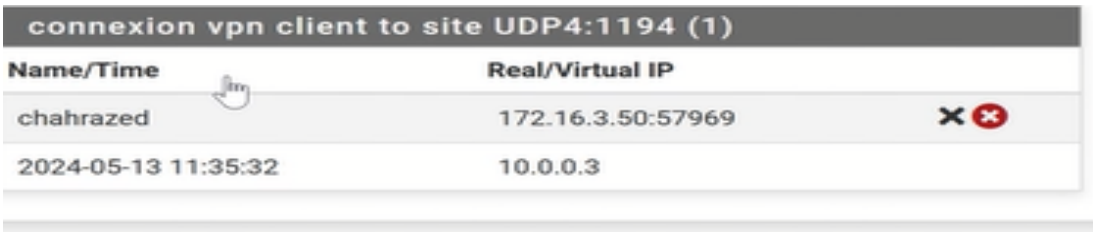
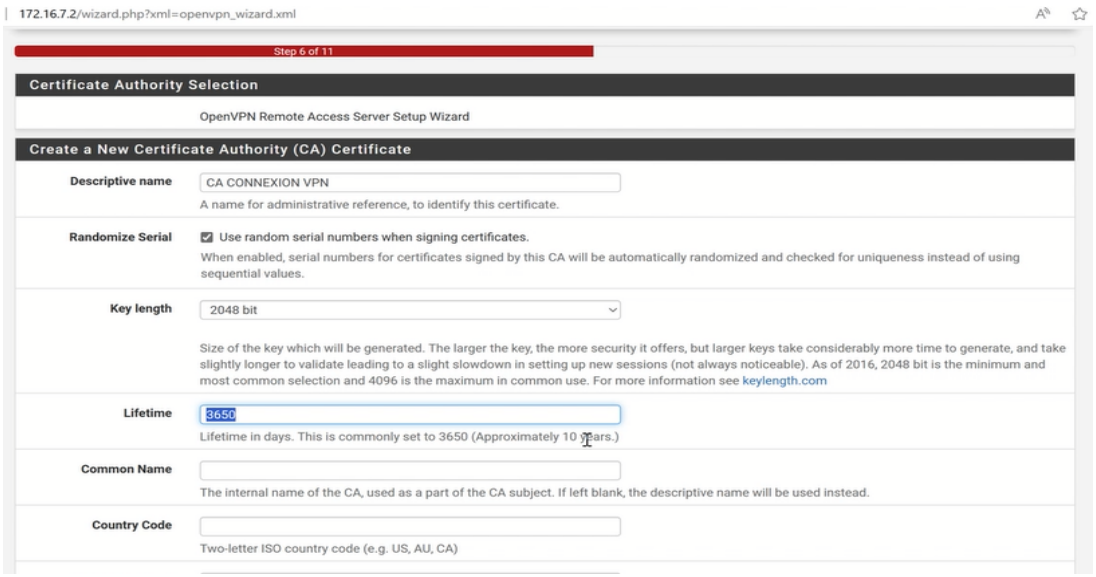
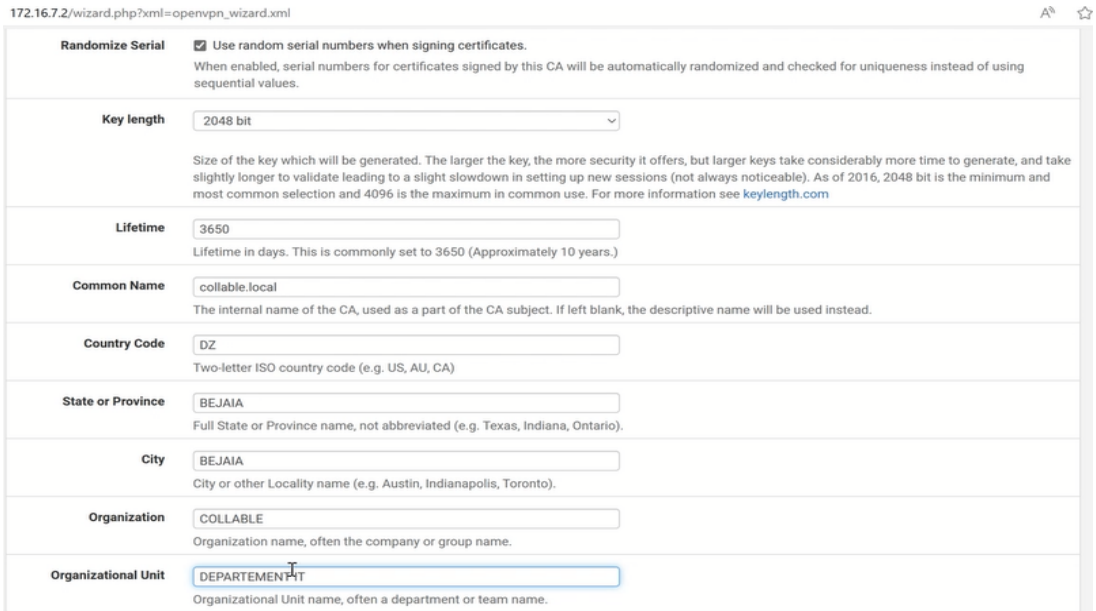


FIGURE D.18 – L'utilisateur Chahrazed est connecté



(a) Attribution d'une description au certificat



(b) Attribution des paramètres de localisation au certificat

FIGURE D.19 – Création d'un certificat pour le VPN

Annexe E

Configuration AD

E.1 Installation du AD DS

Lors de l'installation, accédez au serveur et cliquez sur "Ajouter des rôles et des fonctionnalités". Laissez tous les paramètres par défaut, mais assurez-vous de sélectionner le rôle de service "AD DS".

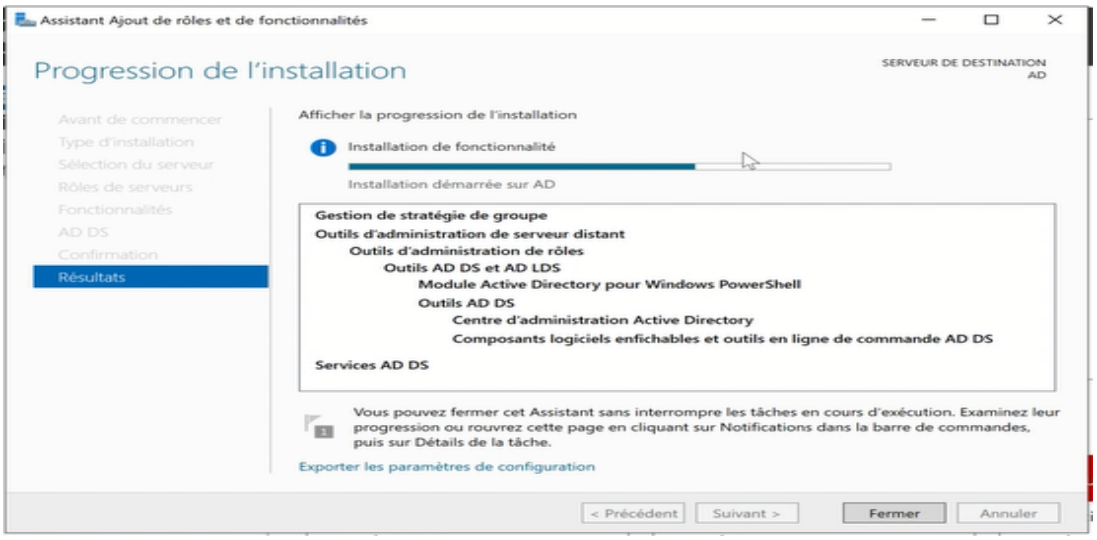
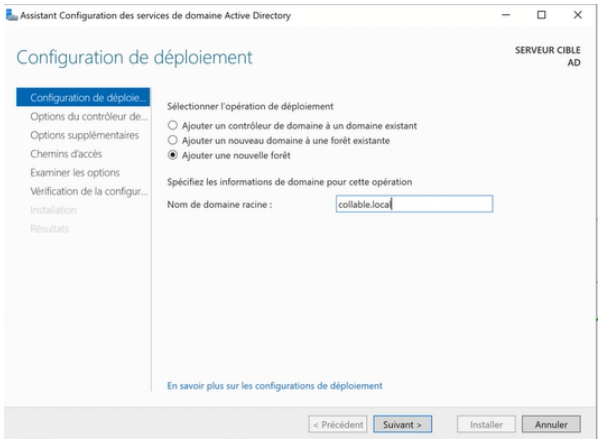


FIGURE E.1 – Installation de serveur AD DS

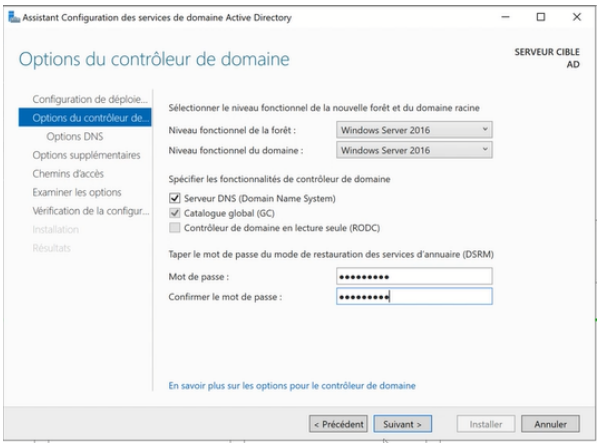
E.2 Configuration du Contrôleur de Domaine

E.2.1 La création d'une forêt Active Directory

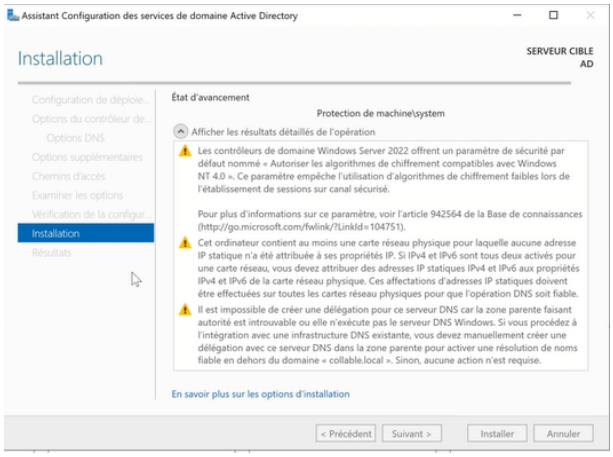
Pour créer une nouvelle forêt Active Directory, accédez à l'option "Promouvoir ce serveur en contrôleur de domaine". Sélectionnez ensuite "Ajouter une nouvelle forêt" et attribuez un nom de domaine, qui sera ‘collable.local‘ dans notre cas. Cochez l'option pour autoriser le serveur DNS et définissez le mot de passe pour le mode de restauration des services AD DS, ici ‘Rt2024PFE‘. Le nom NetBIOS sera automatiquement généré et sera ‘collable‘. Continuez les étapes de création en suivant les instructions à l'écran, puis cliquez sur le bouton "Installer" pour finaliser le processus.



(a) Attribution du Nom de Domaine



(b) Configuration du Serveur DNS et du Mot de Passe de Restauration

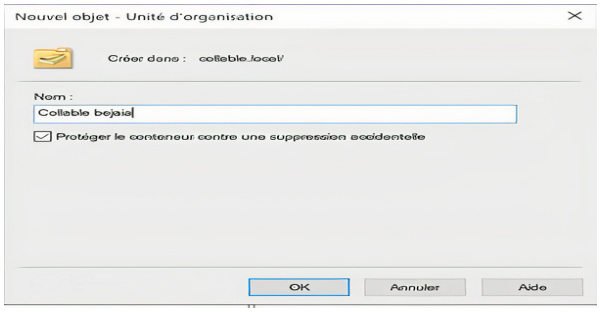


(c) Installation finale

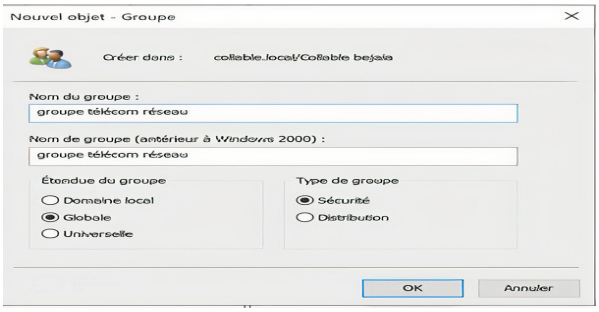
FIGURE E.2 – La création d'une forêt Active Directory

E.2.2 La création une Unité d'Organisation (OU)

Ouvrez "Utilisateurs et ordinateurs Active Directory", naviguez vers 'collable.local', faites un clic droit, sélectionnez "Nouveau" puis "Unité d'organisation", nommez-la et cliquez sur "OK". Ensuite, faites un clic droit sur l'OU, sélectionnez "Nouveau" puis "Groupe", nommez-le "groupe télécom réseau" et validez. Enfin, faites un clic droit sur le groupe, sélectionnez "Nouveau" puis "Utilisateur", remplissez les informations nécessaires et définissez un mot de passe.

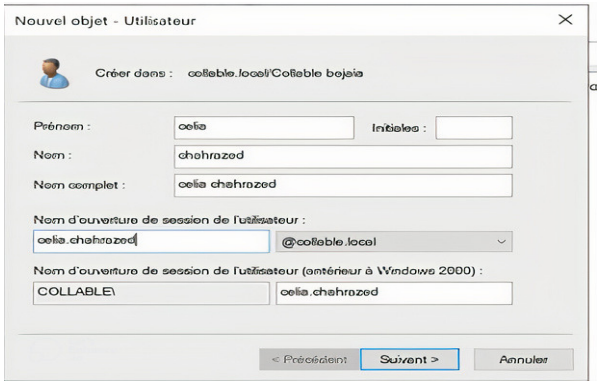


(a) Création d'une unité d'organisation

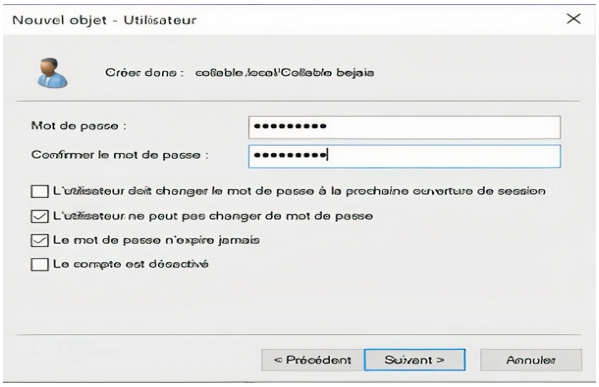


(b) Création de groupe télécom réseau

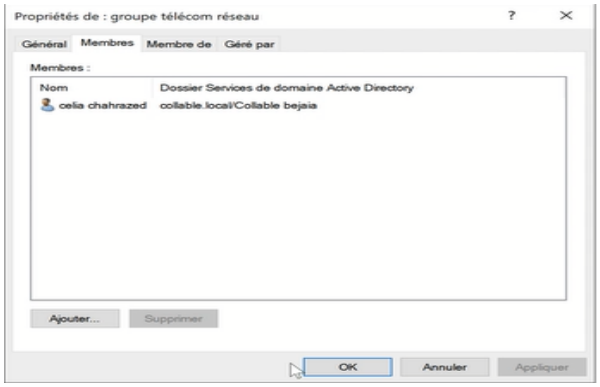
FIGURE E.3 – Création d'une unité d'organisation et d'un groupe télécom réseau



(a) Création d'un utilisateur



(b) Attribution d'un mot de passe au compte utilisateur

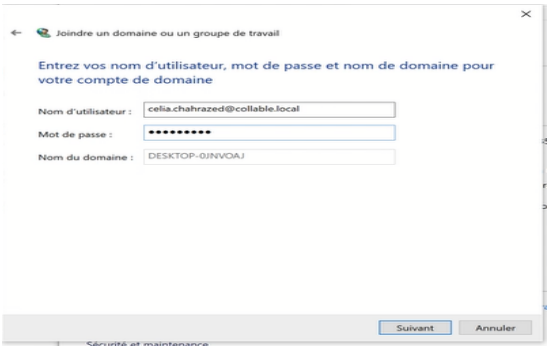


(c) Ajouter l'utilisateur créé au groupe télécom réseau

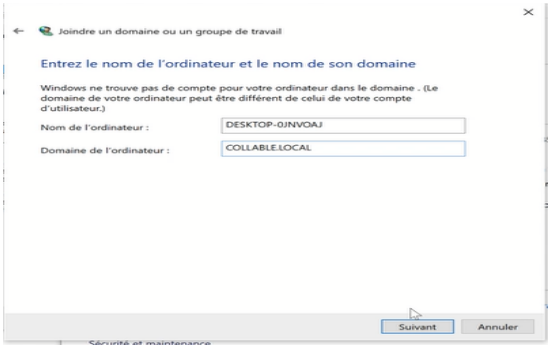
FIGURE E.4 – Création d'un utilisateur

E.3 Procédure de Connexion au Domaine Active Directory

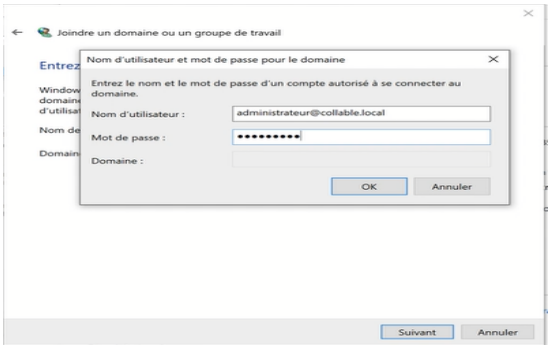
Sur le PC utilisateur, accédez aux "Propriétés système" via un clic droit sur "Ce PC" et sélectionnez "Propriétés". Cliquez sur "Modifier les paramètres"et vous suivre les étapes suivants :



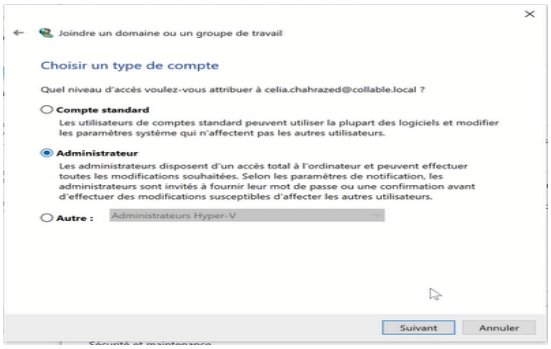
(a) Configuration des Identifiants Utilisateur



(b) Configuration du Nom d'ordinateur et son Domaine



(c) Connexion en Tant qu'Administrateur



(d) Connexion en Tant qu'Administrateur

FIGURE E.5 – Connexion au Domaine collable.local

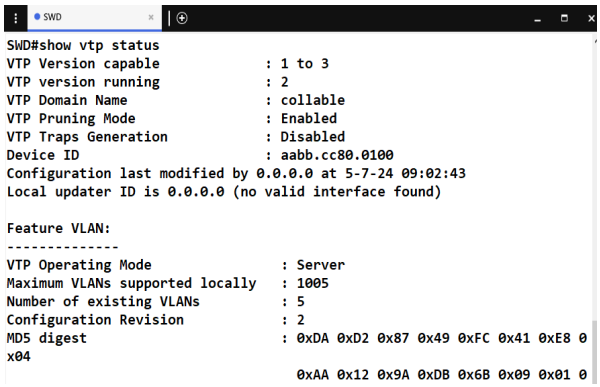
FIGURE E.6 – Accès Réussi au Domaine collable.local

Annexe F

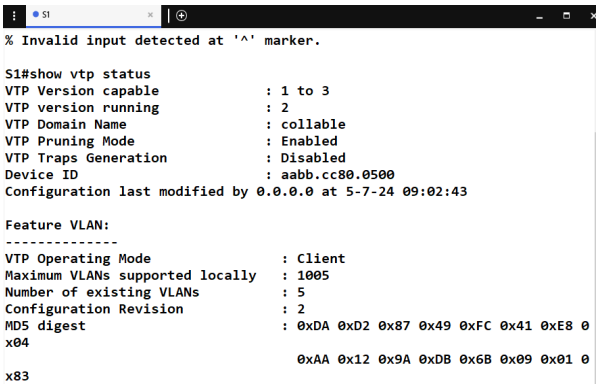
Test

F.1 Affichage des Paramètres VTP

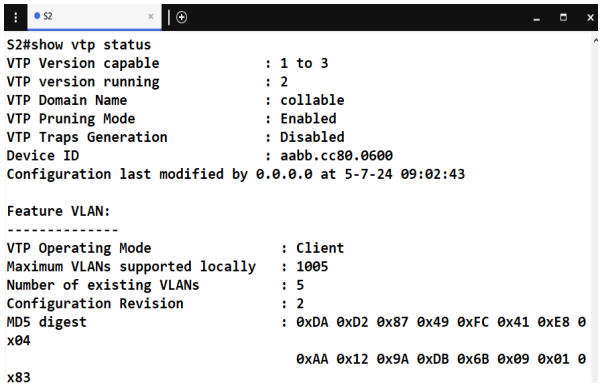
Pour vérifier la configuration des paramètres VTP, nous avons effectué l'affichage des paramètres VTP sur les trois commutateurs, à savoir SWD, S1, et S2.



(a) Affichage des paramètres VTP sur le commutateur SWD



(b) Affichage des paramètres VTP sur le commutateur S1

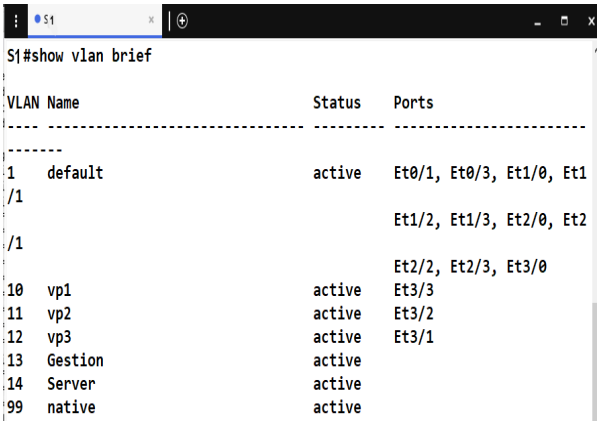


(c) Affichage des paramètres VTP sur le commutateur S2

FIGURE F.1 – Affichage des paramètres VTP sur les trois commutateurs

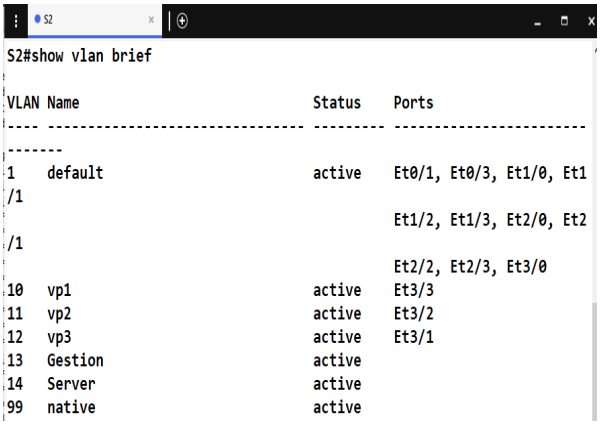
F.2 Validation des Configurations de VLAN

Les figures suivantes illustrent la vérification de notre configuration des VLANs, confirmant ainsi que les paramètres de configuration ont été correctement appliqués.



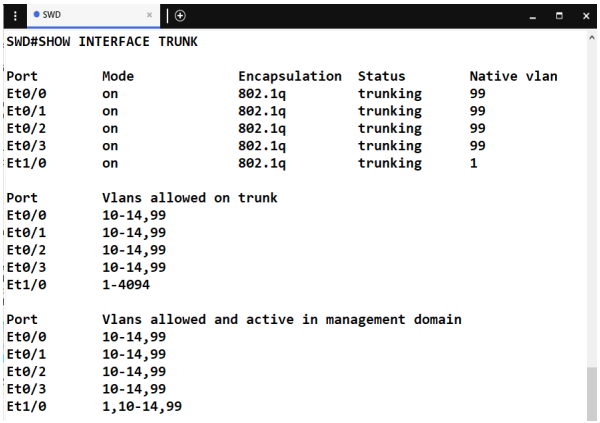
```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
-------
1    default                           active    Et0/1, Et0/3, Et1/0, Et1
/1
                                                 Et1/2, Et1/3, Et2/0, Et2
/1
                                                 Et2/2, Et2/3, Et3/0
10   vp1                               active    Et3/3
11   vp2                               active    Et3/2
12   vp3                               active    Et3/1
13   Gestion                           active
14   Server                            active
99   native                            active
```

(a) Interfaces Affectées aux VLANs sur S1



```
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
-------
1    default                           active    Et0/1, Et0/3, Et1/0, Et1
/1
                                                 Et1/2, Et1/3, Et2/0, Et2
/1
                                                 Et2/2, Et2/3, Et3/0
10   vp1                               active    Et3/3
11   vp2                               active    Et3/2
12   vp3                               active    Et3/1
13   Gestion                           active
14   Server                            active
99   native                            active
```

(b) Interfaces Affectées aux VLANs sur S1



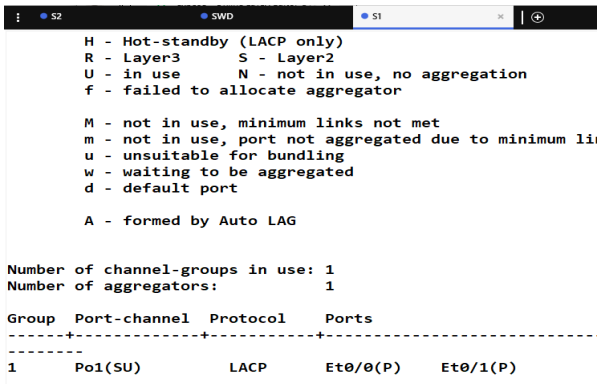
```
SWD#SHOW INTERFACE TRUNK

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      99
Et0/1       on               802.1q         trunking      99
Et0/2       on               802.1q         trunking      99
Et0/3       on               802.1q         trunking      99
Et1/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       10-14,99
Et0/1       10-14,99
Et0/2       10-14,99
Et0/3       10-14,99
Et1/0       1-4094

Port        Vlans allowed and active in management domain
Et0/0       10-14,99
Et0/1       10-14,99
Et0/2       10-14,99
Et0/3       10-14,99
Et1/0       1,10-14,99
```

(c) Affichage du VLAN Natif sur les Interfaces Configurées

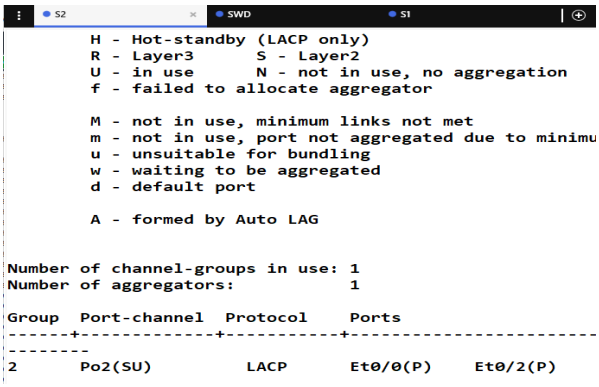
FIGURE F.2 – Affectation des Interfaces et Affichage de VLAN Native

F.3 Affichage des Paramètres LACP

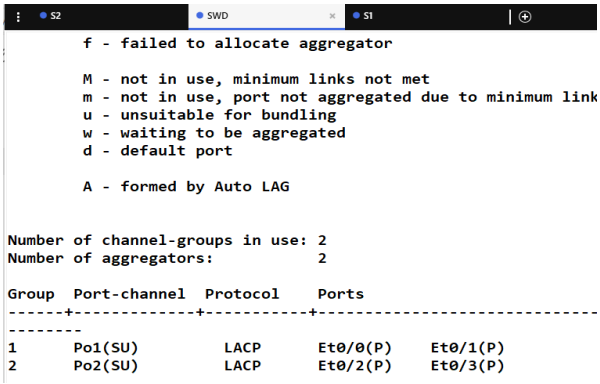
Pour s'assurer que les configurations de LACP sont correctement appliquées, nous avons procédé à l'affichage des paramètres LACP sur les trois commutateurs, SWD, S1, et S2.



(a) Affichage de l'agrégation Ethernet sur le commutateur S1



(b) Affichage de l'agrégation Ethernet sur le commutateur S2



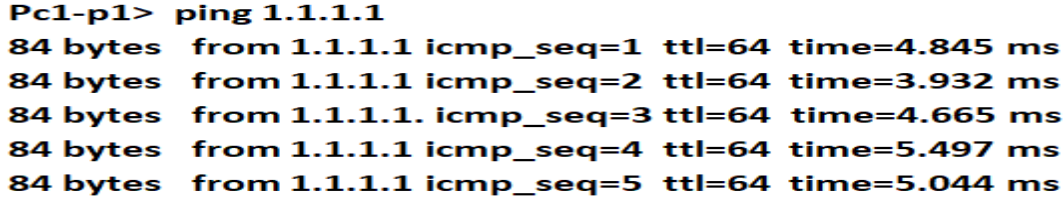
(c) Affichage de l'agrégation Ethernet des deux groupes sur le commutateur SWD

FIGURE F.3 – Affichage des Paramètres LACP sur les Commutateurs SWD, S1, et S2

F.4 Vérification de la Configuration de Port sécurité

F.4.1 Détection d'adresse MAC

Nous avons exécuté un ping depuis le PC configuré avec un port sécurisé sur le commutateur S1 afin de vérifier la détection de son adresse MAC à partir de ce dernier.



(a) Test de ping depuis PC1-P1 vers internet

PC1-P1 | S1

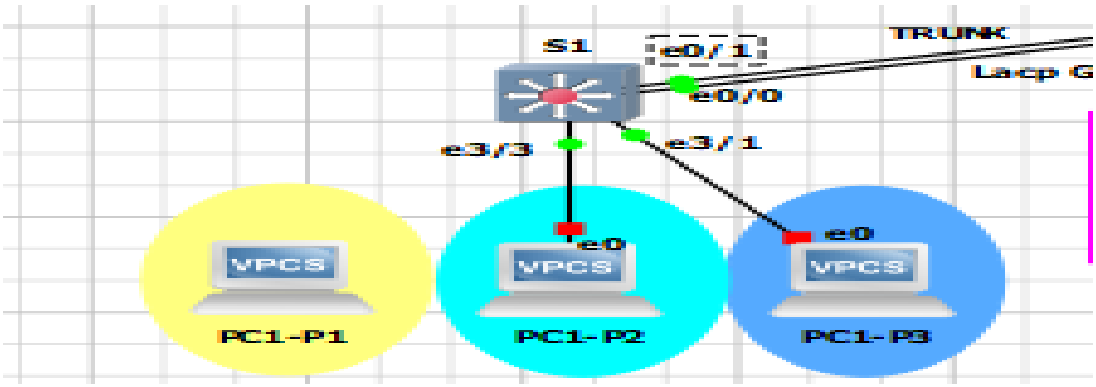
```
S1#show port-security interface ethernet 3/3
Port Security                   : Enabled
Port Status                     : Secure-up
Violation Mode                  : Shutdown
Aging Time                      : 0 mins
Aging Type                      : Absolute
SecureStatic Address Aging      : Disabled
Maximum MAC Addresses           : 1
Total MAC Addresses             : 1
Configured MAC Addresses        : 0
Sticky MAC Addresses            : 1
Last Source Address:Vlan        : 0050.7966.6800:10
Security Violation Count        : 0
```

(b) Détection d'adresse MAC de PC1-P1 depuis le commutateur S1

FIGURE F.4 – Test de ping et détection d'adresse MAC depuis PC1-P1

F.4.2 Validation de l'Interface Sécurisée lors du Changement d'Adresse MAC

On libère l'interface qui relie le commutateur S1 avec le PC1-P1 et on le reliait avec le PC1-P2 et pour vérifier la validation de cette configuration.



(a) Affectation d'interface E3/3 au PC1-P2

```
Pc1-p2> ping 1.1.1.1
1.1.1.1 icmp_seq=1 timeout
1.1.1.1 icmp_seq=2 timeout
1.1.1.1 icmp_seq=3 timeout
1.1.1.1 icmp_seq=4 timeout
1.1.1.1 icmp_seq=5 timeout
```

(b) Test de ping depuis PC1-P2 vers internet

FIGURE F.5 – Affectation et test de ping depuis PC1-P2

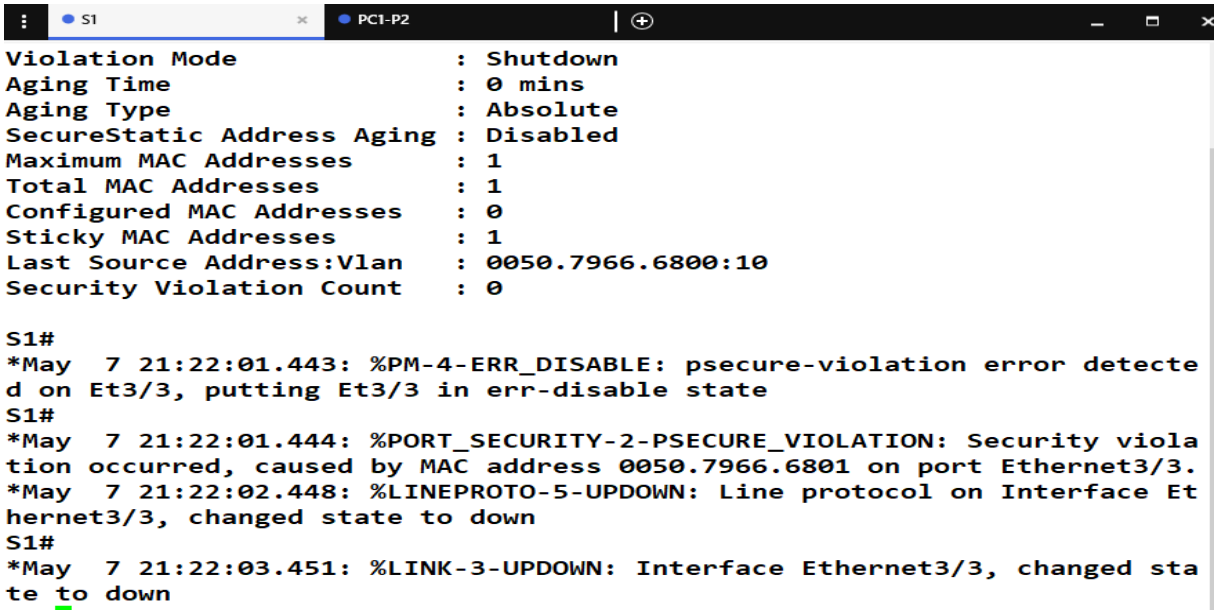
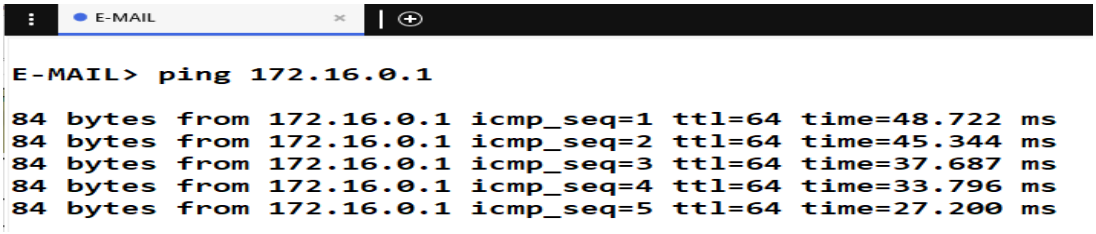


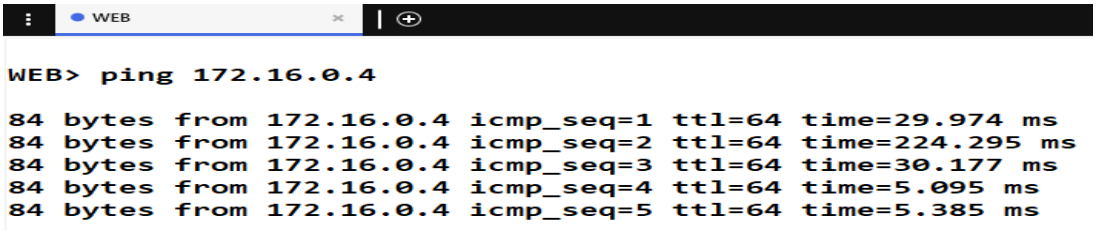
FIGURE F.6 – Affichage de l'état de l'interface E3/3

F.5 Vérification de l'isolation des PVLAN dans la DMZ

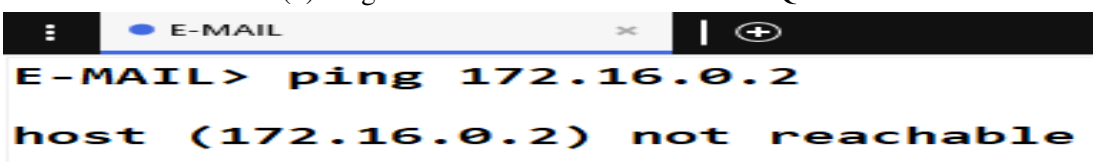
Nous allons exécuter un test entre les différents serveurs situés dans notre DMZ pour vérifier la validation de notre configuration des PVLAN. Ce test vise à assurer que chaque serveur est correctement isolé au sein du réseau, conformément à nos paramètres de sécurité.



(a) Un ping depuis le serveur de messagerie vers la passerelle



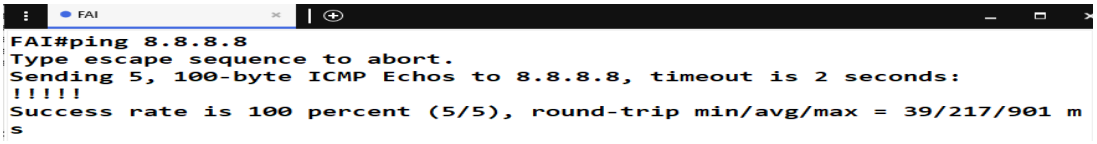
(b) Ping du serveur WEB vers le serveur SQL



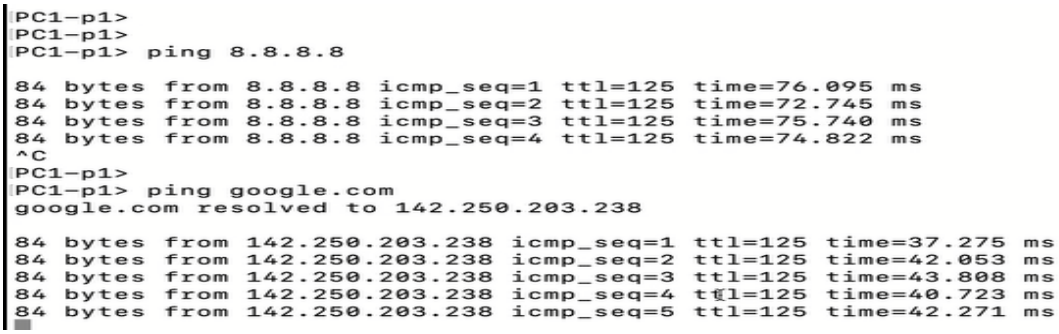
(c) Ping du serveur de messagerie vers le serveur ASTERISK-CRM

FIGURE F.7 – Test de connectivité

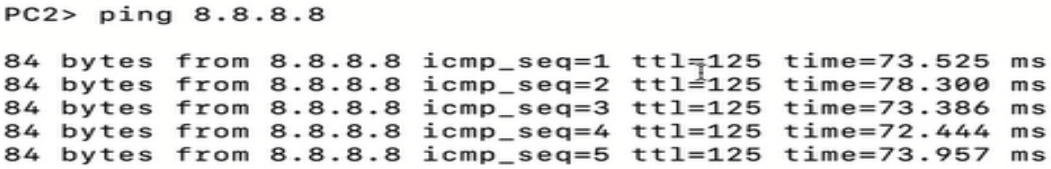
F.6 Vérification de la connectivité Internet après Configuration de NAT avec PAT



(a) Ping depuis FAI vers internet



(b) Ping depuis le PC1-P1 vers le serveurs vers google.com

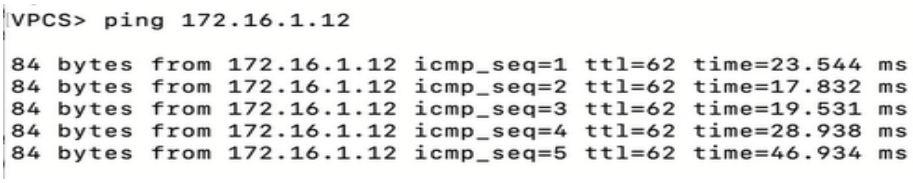


(c) Ping depuis le LAN Alger vers Internet

FIGURE F.8 – Test de connectivité

F.7 Test de connectivité VPN Site to Site par Pings entre les deux sites

Nous allons tester si notre tunnel fonctionne en effectuant des Pings d'un site vers l'autre.

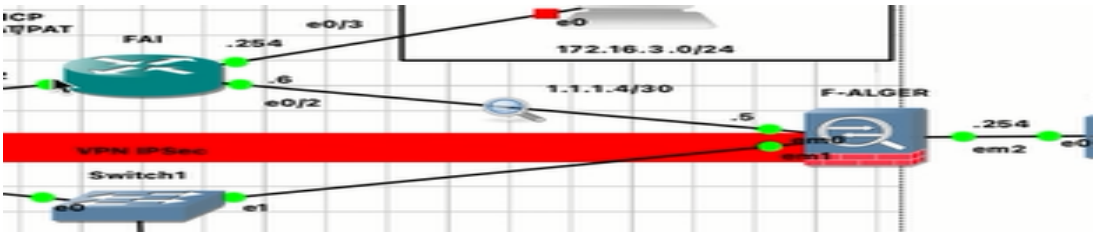


(a) Test de ping depuis le VLAN 14 vers le LAN Alger

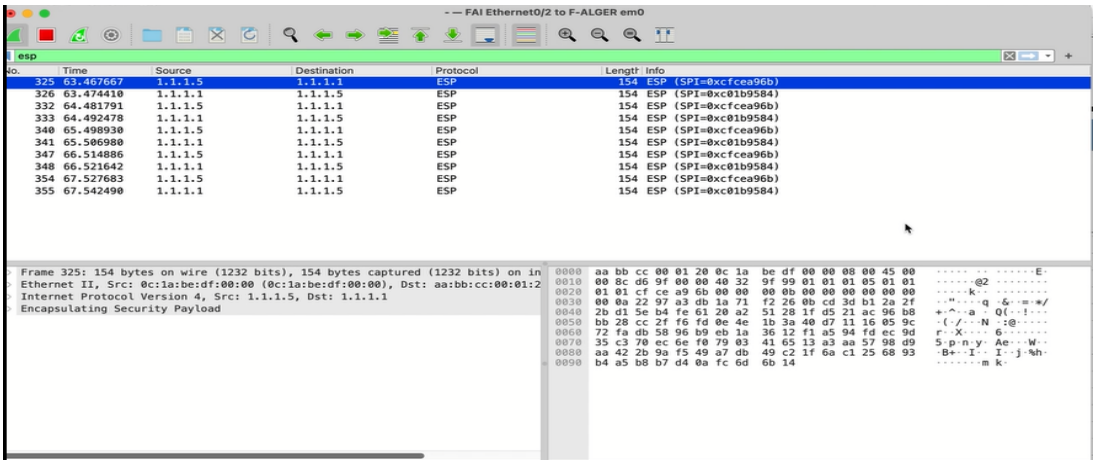
(b) Test de ping depuis le LAN Alger vers le VLAN 14

FIGURE F.9 – Tests de connectivité à travers le tunnel IPsec

Lorsque nous avons initié des pings depuis un site vers l'autre, cela a déclenché l'activation du protocole ESP.



(a) Activation du Protocole ESP dans la Topologie Réseau



(b) Déclenchement du Protocole ESP

FIGURE F.10 – Activation du Protocole ESP

F.8 Test de Connexion VPN Client vers le Réseau Local

Une fois que tout est configuré, nous effectuons des tests pour vous assurer que le PC VPN fonctionne correctement.

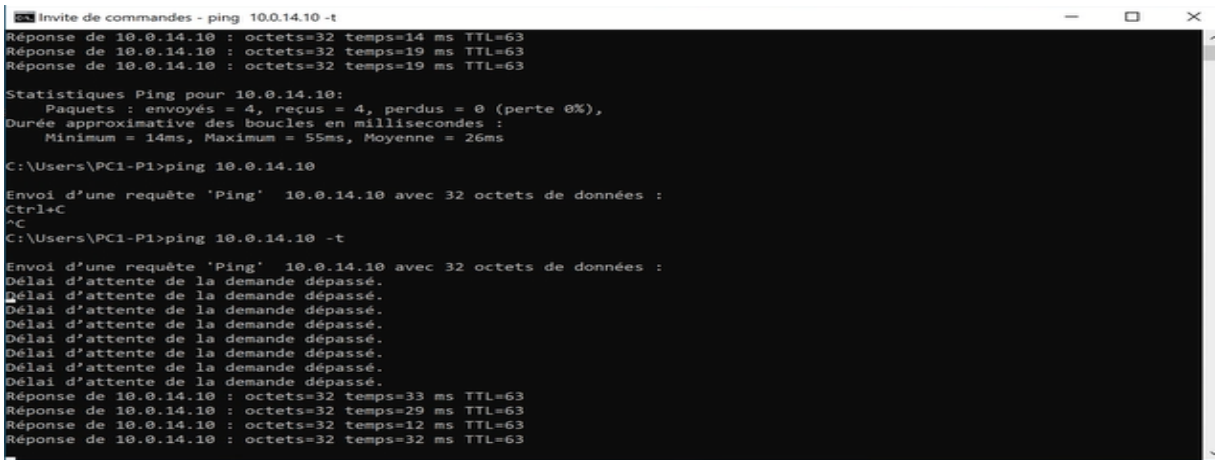


FIGURE F.11 – Test de ping depuis le PC VPN vers le serveur Active Directory

F.9 Validation de la Configuration Active Directory

Lorsque nous avons configuré Active Directory sur le serveur et qu'un PC utilisateur s'est connecté au domaine que nous avons créé, nous avons pu détecter ce PC dans le serveur Active Directory.

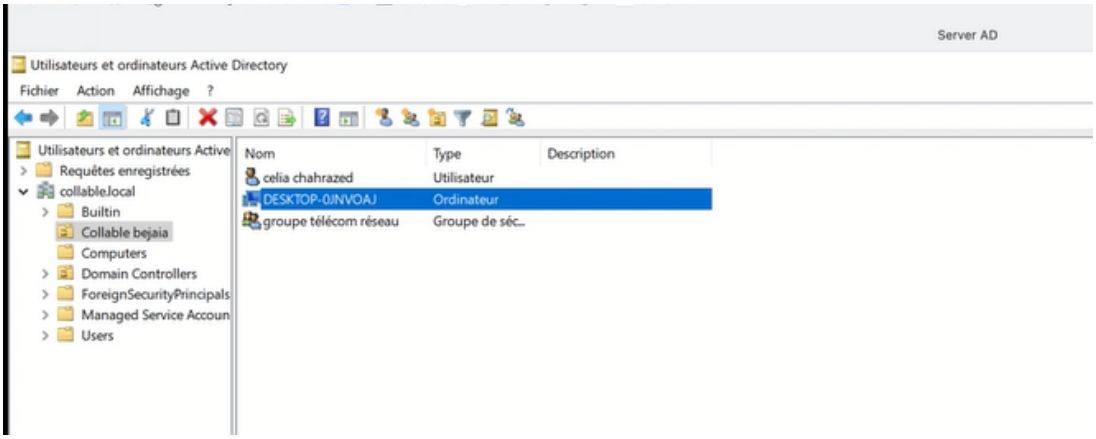


FIGURE F.12 – Affichage de pc utilisateur sur server AD

Bibliographie

[1] Jean-François pillou Jean-philippe, *Tout sur la sécurité informatique* , Édition 4, 2016.

[2] Support de cours Dr. FARAH Zoubeyr, Maître de conférences à l'université de Bejaia.

[3] J. Archier, *Les VPN : fonctionnement, mise en œuvre et maintenance des réseaux privés virtuels*, Edition ENI, 2010.

[4] Davis Chapman, *Firewalls - La sécurité sur Internet*, édition O'Reilly, 1997.

[5] Support de cours M. khirdin *Réseau de terrain*, chapitres 1 et 2.

[6] Support de cours M. Bessad, *Protocol multimédia*.

[7] Eric BAHATI - SHABANI , MISE EN PLACE D'UN RESEAU VPN AU SEIN D'UNE EN TREPRISE, Institut supérieur de commerce Kinshasa , Mémoire de Licence en Informatique de Gestion, 2011.

[8] ipsec(internet protocole security) , Centre Universitaire Nour Bachir , 2020.

Webographie

[9] Le Big Data, *Malware : qu'est-ce qu'un logiciel malveillant et comment s'en débarrasser ?*, 2024. Disponible en ligne : https://www.lebigdata.fr/malware-definition [Consulté le 20 mars 2024].

[10] Jaume Duch Guillot, *Cybersécurité : les menaces principales et émergentes*, 21-03-2023. Disponible en ligne : https://www.europarl.europa.eu/topics/fr/article/20220120STO21428/cybersecurite-les-menaces-principales-et-emergentes [Consulté le 9 juillet 2024].

[11] Cloudflare, Inc., *What is Web Application Security ?*, 2024. Disponible en ligne : https://www.cloudflare.com/fr-fr/learning/security/what-is-web-application-security [Consulté le 23 mars 2024].

[12] Microsoft, *What is Cloud Security ?*, 2024. Disponible en ligne : https://www.microsoft.com/fr-fr/security/business/security-101/what-is-cloud-security [Consulté le 12 mars 2024].

[13] Damien Ecrohart, *Tout ce qu'il faut savoir sur les équipements réseau*, 2019. Disponible en ligne : https://blog.netwrix.fr/2019/07/24/tout-ce-quil-faut-savoir-sur-les-equipements-reseau/ [Mis à jour le 17 octobre 2022].

[14] INF1160 - Protocoles Réseaux, 2013. Disponible en ligne : https://spip.teluq.ca/inf1160/IMG/pdf/inf1160-protocolesreseaux.pdf [Consulté le 17 février 2024].

[15] Cisco, *Introduction au protocole de routage dynamique OSPF*, 2020. Disponible en ligne : https://cisco.goffinet.org/ccna/ospf/introduction-au-protocole-routage-dynamique-ospf/ [Consulté le 9 mars 2024].

[16] Laurent Williams, *IP Address Classes*, 2023. Disponible en ligne : https://www.guru99.com/fr/ip-address-classes.html [Consulté le 17 avril 2024].

[17] Chiradeep BasuMallick, *What is Ethernet ?*, 2023. Disponible en ligne : https://www.spiceworks.com/tech/networking/articles/what-is-ethernet/ [Consulté le 13 avril 2024].

[18] Katie Terrell Hanna, *802.3*, 2024. Disponible en ligne : https://www.techtarget.com/searchnetworking/definition/8023 [Consulté le 12 février 2024].

[19] Amazon Web Services, *What is DNS ?*, 2023. Disponible en ligne : https://aws.amazon.com/fr/route53/what-is-dns/ [Consulté le 15 avril 2024].

[20] Microsoft, *Article*, 2023. Disponible en ligne : https://learn.microsoft.com/fr-fr [Consulté le 27 février 2024].

[21] SJVINIANT Mariane, *Resource Center*, 1994. Disponible en ligne : https://horizon.documentation.ird.fr/exl-doc/pleins-textes [Consulté le 1 mai 2024].

[22] *Qu'est-ce qu'un site Internet ?*, 2024. Disponible en ligne : https://www.imedias.pro/cours-en-ligne/web-internet/site-internet-site-web/qu-est-ce-qu-un-site-internet/ [Consulté le 14 mars 2024].

[23] *SMTP Extensions : STARTTLS and DANE*, 2024. Disponible en ligne : https://www.geeksforgeeks.org/smtp-extensions-starttls-and-dane/ [Consulté le 15 mars 2024].

[24] Dale Ford, *Software-Defined Networking*, 2024. Disponible en ligne : https://fr.digi.com/blog/post/software-defined-networking [Consulté le 21 avril 2024].

[25] Pulsar Agency, *Website*, 2024. Disponible en ligne : https://www.pulsar-agency.com [Consulté le 13 mai 2024].

[26] juniper network, *Qu'est-ce qu'un SDN ?*, https://www.juniper.net/fr/fr/research-topics/what-is-sdn.html , [consulté le 09/07/2024].

[27] *ChatGPT*, 2024. Disponible en ligne : https://chatgpt.com/ [Consulté le 11 juillet 2024].

[28] *Les couches du modèle OSI*, 2024. Disponible en ligne : https://jeretiens.net/couches-du-modele-osi [Consulté le 5 avril 2024].

[29] Mickael Dorigny, *Qu'est-ce que l'ARP ?*, 2024. Disponible en ligne : https://www.it-connect.fr//quest-ce-que-larp [Consulté le 12 mars 2024].

[30] *Exposés RIO 2002*, 2002. Disponible en ligne : http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/parexposesrio2002 [Consulté le 17 mars 2024].

Résumé

La sécurisation d'une infrastructure réseau est essentielle pour protéger les données sensibles et garantir la continuité des communications dans un environnement de menaces numériques croissantes. Ce mémoire décrit la mise en place d'une solution de sécurité complète pour l'infrastructure réseau de l'entreprise Collable. Nous avons créé une salle technique sécurisée avec un câblage blindé pour protéger les équipements contre les accès non autorisés et les interférences. Le filtrage par adresse MAC et l'agrégation de liens LACP ont été mis en œuvre pour contrôler les périphériques connectés et améliorer la tolérance aux pannes du réseau. La création de VLANs permet de segmenter le réseau et de limiter les impacts des incidents internes. Un canal sécurisé IPSec assure la confidentialité et l'intégrité des données échangées entre les sites de Bejaia et d'Alger, protégeant les communications sensibles. Le routage inter-VLAN et les listes de contrôle d'accès (ACLs) facilitent la gestion du trafic entre les segments tout en renforçant la sécurité du réseau. Pour renforcer la défense contre les attaques externes, une zone démilitarisée (DMZ) a été instaurée pour isoler les serveurs publics, avec des VLANs privés (PVLANs) qui empêchent la communication directe entre utilisateurs au sein de la DMZ, augmentant ainsi la sécurité interne. Les protocoles SSH et VPN SSL assurent la sécurité des accès distants, tandis qu'un serveur Active Directory centralise la gestion des identités et des accès, simplifiant l'administration et améliorant la sécurité des interactions réseau. Ces mesures ont réduit les incidents de sécurité et amélioré la disponibilité des services réseau pour Collable, assurant une infrastructure stable, résiliente et sécurisée.
Mots clés : Sécurité réseau, Infrastructure réseau, Collable, DMZ, VLAN, LACP, IPSec, SSH, VPN SSL, Active Directory.

Abstract

Securing a network infrastructure is essential to protect sensitive data and ensure communication continuity in an environment of increasing digital threats. This thesis describes the implementation of a comprehensive security solution for Collable's network infrastructure. We established a secured technical room with shielded cabling to protect equipment from unauthorized access and interference. MAC address filtering and LACP link aggregation were implemented to control connected devices and enhance network fault tolerance. VLAN creation enables network segmentation, limiting the impact of internal incidents. An IPSec secured channel ensures the confidentiality and integrity of data exchanged between the Bejaia and Algiers sites, protecting sensitive communications. Inter-VLAN routing and access control lists (ACLs) facilitate traffic management between segments while enhancing network security. To strengthen defenses against external attacks, a demilitarized zone (DMZ) with private VLANs (PVLANs) was established to isolate public servers, preventing direct communication between users within the DMZ and thereby increasing internal security. SSH and VPN SSL protocols secure remote access, while an Active Directory server centralizes identity and access management, simplifying administration and improving the security of network interactions. These measures have reduced security incidents and improved the availability of network services for Collable, ensuring a stable, resilient, and secure infrastructure.
Keywords : Network Security, Network Infrastructure, Collable, DMZ, VLAN, LACP, IPSec, SSH, VPN SSL, Active Directory.