

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abdelhamid MEHRI - Constantine 2



Faculté des Nouvelles Technologies de l'Information et de la Communication
Département de l'Informatique Fondamentale et ses Applications

Projet de fin d'études pour l'obtention du diplôme de

Licence en Informatique

Option : Science de l'informatique

Thème :

**Mise en œuvre d'une architecture réseau sécurisée à
haute disponibilité pour une clinique médicale**

Responsable d'atelier :

Dr R.SALIM BANAYOUNE

Réalisé par :

Ledra Marwa

Kerrouche Aymen

Session Juin 2021

Dédicace

Au nom de dieu le miséricordieux

Je dédie ce travail à :

Mes chers parents : Mon cher père Mohamed et ma tendre

Maman Chahrazed qui m'ont soutenu et encouragé durant toute la

Période de mes études et à qui je souhaite une longue et heureuse vie. A mes

frères Yasser, Ahmed et Issam

A toute ma famille

A mon binôme Aymen

A tous mes amis

A toute personne qui me connais.

Marwa

Dédicace

Au nom de dieu le miséricordieux

Je dédie ce travail à :

Mes chers parents : Mon cher père Ali et ma tendre

Maman Sina qui m'ont soutenu et encouragé durant toute la

Période de mes études et à qui je souhaite une longue et heureuse vie. A mon

frère Noufel et ma sœur Douaa

A toute ma famille

A mon binôme Marwa

A tous mes amis

A toute personne qui me connais.

Aymen

REMERCIEMENTS

Nos premiers remerciements s'adressent à Dieu le tout puissant qui par sa bonté et sa miséricorde nous a permis d'avoir le courage, la foi et la volonté de mener à bien ce travail.

Nous tenons aussi à remercier notre On précise d'abord à remercier notre encadreur Dr. Salim Benayoune pour leurs conseils Valeureux, leurs professionnalismes et leurs encouragements. -pour avoir dirigé ce travail, pour son assistance et ses conseils qui ont étayé notre conduite Dans la réalisation de ce mémoire

Nous remercions également tous les professeurs qui ont contribués de près ou de loin à notre formation universitaire, sans oublier toute personne qui nous a aidés à mener à terme notre projet.

Merci à tous.

SIGLES ET ABREVIATIONS

ACL: Access Control List.

DHCP: Dynamics Host Configuration Protocol.

Http/s: Hyper Text Transfer Protocol/Secure.

IP: Internet Protocol.

NAS: Network Attached Storage.

DMZ: Zone DéMilitarisée.

Wi-Fi: Wireless Fidelity.

DNS: Domain Name System.

NAT: Network Address Translation.

FTP: File Transfer Protocol.

LAN: Local Area Network.

VLAN: Virtual LAN ou Virtual Local Area Network.

STP: Protocole Spanning Tree.

VTP: Vlan Trunking Protocol.

VPN: Virtual Private Network.

LACP: Link Aggregation Control Protocol.

DTP: Dynamic Trunking Protocol.

RSTP: Rapid Spaning Tree Protocol.

MSTP: Multiple Spanning Tree.

PAgP: Port Aggregation Protocol.

RPS: Redundant Power System .

WRED: Weighted Random Early Detection .

LDAP: Lightweight Directory Access Protocol.

PSSI : Politique de Sécurité du Système d'Information.

VOIP : la VOix sur IP.

IDS : Système de Détection d'Intrusion.

IPS : Système de Prévention d'Intrusion

QoS : Quality Of Service.

HSRP: Hot Standby Routing Protocol.

CBWFQ: Class-Based Weighted Fair Queuing.

CF : Filtrage Contenu.

AS : Anti-Spam.

AV : Anti-Virus.

PCA : Planification de la Continuité des Activités.

AMP: Advance Malware Protection.

SSID: Service Set Identifier.

VLSM: Variable Length Subnet Mask.

CLI: Command-Line Interface.

WPA2: Wi-fi Protected Access.

WCCP : Web Cache Communication Protocol.

HTCP: Hyper Text Caching Protocol.

SNMP: Simple Network Management Protocol.

SMB: Server Message Block.

SSH: Secure Shell.

DOS: Denial Of Service.

USB: Universal Serial Bus.

WAN: Wide Area Network.

TCP: Transmission Control Protocol.

UDP: User Datagram Protocol.

EIGRP: Enhanced Interior Gateway Routing Protocol.

DCI : Data Center Interconnect.

GHz : GigaHertz.

Mbps : Mégabit Par Seconde.

Gbit /s : Gigabit Par Seconde.

AP : Access Point.

Liste des figures :

Figure N°	TITRE	PAGE
01	Réseau DMZ simple	07
02	Passerelle sécurisée vers internet	08
03	Pare-feu (firewall)	09
04	Un serveur proxy	10
05	Un serveur DNS	12
06	Proxy inverse (reverse proxy)	13
07	NAT (network address translation)	14
08	Modèle de conception de réseau à trois niveaux	16
09	Modèle de conception de réseau à deux niveaux	17
10	Réseau local	19
11	Passerelle sécurisée	20
12	Architecture de réseau interne de l'hôpital	22
13	Commutateur distribution1	24
14	Commutateur distribution2	25
15	Configuration de serveur DHCP	26
16	Configuration de serveur LDAP	27
17	Configuration de serveur WEB	28
18	VPN actif	31
19	DNS actif	36
20	Proxy actif	38
21	Pare-feu 01 actif	40
22	Pare-feu 02 actif	41
23	Reverse proxy actif	45
24	Un commutateur	63
25	Serveur NAS	64
26	Serveur DHCP	65
27	Serveur WEB	66
28	Serveur LDAP	67
29	Serveur VPN	67

Liste des tableaux :

Figure N°	Titre	Page
01	Segmentation de réseau interne	21
02	Table d'adressage	23
03	Tableau des (nom utilisateur, mot de passe, enable secret)	29
04	Devis du matériel	50

Table des matières :

<i>Dédicace</i>	
<i>Dédicace</i>	
REMERCIEMENTS	
SIGLES ET ABREVIATIONS	
Liste des tableaux :	
1. Introduction générale :	1
1.1. Contexte de projet :	1
1.2. Analyse du besoin contraintes :	2
1.3. Résumé des chapitres :	2
Chapitre 01 :Conception de L'architecture	
1. Introduction :	5
2. Passerelle sécurisée vers internet :	7
2.1. Définition :	7
2.2. Pare-feu (firewall) :	9
2.2.1. Définition :	9
2.3. Proxy :	10
2.3.1. Définition :	10
2.4. Serveur DNS :	11
2.4.1. Définition :	11
2.5. Proxy inverse :	12
2.5.1. Définition :	12
2.6. La NAT :	13
2.6.1. Définition :	13
2.7. IDS/IPS :	14
2.7.1. Définition :	14
2.7.2. IDS (Système de Détection d'Intrusion) :	14
2.7.3. IPS (Systèmes de Prévention des Intrusions) :	14
2.7.4 Distinction entre pare-feu et IDS/IPS :	15
3. Couches de réseau de campus :	15
3.1. Modèle de conception hiérarchique:	15
3.1.1. Modèle à trois niveaux :	16
3.1.2. Modèle à deux niveaux :	17
3.1.2.1. Définition de la couche d'accès :	17

3.1.2.2. Mécanismes de la couche d'accès :	18
3.1.2.3. Définition de la couche de distribution :	18
3.1.2.4. Mécanismes de la couche de distribution :	18
4. Architecture détaillée :	19
4.1. Introduction :	19
4.2. Présentation du réseau intranet :	19
4.2.1. Passerelle sécurisée :	20
4.2.2. Réseau interne :	20
4.2.2.1. Adressage IP :	22
4.2.2.2. Routage :	23
4.2.2.3. Serveur DHCP :	25
4.2.2.4. Serveur LDAP :	26
4.2.2.5. Serveur Web :	27
4.3. Sécurité de réseau :	28
4.3.1. Authentification :	29
4.3.2. Sécurité sur les ponts :	29
4.3.3. DHCP snooping :	30
4.3.4. Inspection dynamique de l'ARP:	30
4.3.5. Liste de contrôle d'accès :	30
4.3.6. SSH :	30
4.3.6. VPN :	30
4.3.7. Protocoles de sécurité sans fil :	32
Chapitre 02 :Réalisation et Choix Technique	
1. Introduction :	34
2. L'implémentation de la passerelle sécurisée :	34
2.1. BIND:	34
2.1.1. Définition :	34
2.1.2. Comment installer BIND :	35
2.1.3. Caractéristiques :	35
2.2. SQUID :	36
2.2.1. Définition :	36
2.2.2. Processus étape par étape pour configurer serveur proxy l'aide de SQUID Proxy: ...	36
2.2.3. SQUID Proxy Port :	37
2.2.4. Caractéristiques:	37
2.3. IPTABLES :	38

2.3.1. Définition :	38
2.3.2. Comment installer et utiliser le pare-feu Linux IPTABLES :	39
2.3.3. Caractéristiques:	39
2.4. SNORT :	41
2.4.1. Définition :	41
2.4.2. Comment installer SNORT :	41
2.4.3. Caractéristiques :	42
2.5. Fail2ban :	42
2.5.1. Définition:	42
2.5.2. Comment Installer fail2ban :	42
2.5.3. Caractéristiques :	43
2.6. Nginx :	43
2.6.1. Définition :	43
2.6.2. Comment Installer nginx :	44
2.6.3. Caractéristiques :	44
3. Choix techniques et chiffage d la proposition :	45
4. PSSI (Politique sécurité système information) :	50
4.1. Introduction :	50
4.2. Objectif :	51
4.3. Principes Organisationnels :	51
4.3.1. Politique de sécurité et politiques à thèmes :	51
4.3.1.1. Politique de sauvegarde :	51
4.3.1.2. Politique de protection contre les logiciels malveillants :	51
4.3.1.3. Politique de contrôle d'accès:	52
4.3.1.4. Adoption d'une échelle de besoins :	53
4.4. Principes de mise en œuvre :	53
4.4.1. Planification de la continuité des activités :	53
4.4.1.1. Définition du périmètre du plan de continuité :	53
4.4.1.2. Elaboration d'un plan de reprise :	53
4.4.1.3. Positionnement des applications dans le plan de continuité :	54
4.4.1.4. Mises-en place de procédures de sauvegarde et de restauration	54
4.4.1.5. Tests réguliers des plans :	54
Chapitre 03 :Bilan Personnel et Professionnel	
Bilan personnel :	57

Bilan professionnel :	58
Conclusion générale :	59
Bibliographie :	60
Annexes	62
Annexe 01 : 1. Réseau Local :	63
1.1. Introduction :	63
1.2. Le commutateur :	63
1.3. VLAN (Virtual Local Area Network):	64
1.4. Serveur NAS :	64
1.5. Serveur DHCP :	65
1.6. Serveur Web :	65
1.7. Serveur LDAP :	66
1.8. VPN (Virtual Private Network):	67
1.9. SSH (Secure Socket Shell):	68
1.10. Porte sécurité :	68
1.11. DHCP snooping :	68
1.12. ARP inspection :	68
1.13. NTP : (network time Protocol) :	69
1.14. Point d'Accès :	69

1. Introduction générale :

1.1. Contexte de projet :

Dans un hôpital, le réseau constitue un socle pour l'exécution des applications, dont la plupart sont liées à des fonctions fondamentales de l'hôpital. Les médecins ont besoin d'accéder aux informations sur leurs appareils mobiles personnels (smartphones, tablettes, etc.). Quant aux patients et aux visiteurs, ils veulent avoir accès à l'Internet pour se connecter à leurs réseaux sociaux et pour se divertir. Un grand nombre d'hôpitaux utilise une infrastructure de réseau distincte pour chaque département afin d'apporter sécurité et performance. Chaque infrastructure de réseau distincte comprend un équipement de mise en réseau et de gestion, le tout connecté à des serveurs, à des passerelles et à d'autres plateformes [1]

Aujourd'hui on ne peut pas imaginer notre quotidien et le monde du travail actuel sans l'existence des réseaux, La fonction principale d'un réseau est de fournir aux participants une plateforme pour l'échange de données et l'utilisation commune des ressources. Cette fonction revêt une importance cruciale [2].et Pour mener à bien notre projet qui est de proposer des solutions de sécurité pour le réseau local, nous devons commencer par expliquer le fonctionnement des réseaux informatiques, et définir certains concepts de la sécurité informatique.

D'une manière générale, un réseau n'est rien d'autre qu'un ensemble d'objets ou de personnes connectés ou maintenus en liaisons dont le but est d'échanger des informations ou des biens matériels [3]

Le rôle des réseaux a donc sensiblement évolué ces dernières années, la croissance phénoménale des établissements et entreprises au niveau architectural et financier a mené ces derniers à développer de nouveaux besoins pour la gestion et la coordination, et surtout la communication, la nécessité d'utiliser les réseaux et Internet était devenu plus qu'indispensable

La sécurité des réseaux est donc devenue un des éléments-clés de la continuité des systèmes d'informations de l'entreprise quelle que soit son activité, sa taille et sa répartition géographique, ainsi cette architecture réseau ne fait pas exception à cette règle. En effet la

nécessite de protéger les données sur les patients et les services disponibles, et la fragilité du réseau actuel aux différentes attaques internes et externes, nous ont poussé à réfléchir à comment sécuriser le réseau informatique de l'hôpital en question [4].

Pour répondre à l'appel du groupe « chifa » de faire un réseau sécurisé a une clinique on donne une proposition qui sera le thème de notre projet et elle sera bien détaillée dans les chapitres dans les chapitres suivant.

1.2. Analyse du besoin contraintes :

Pour faire ce travail on a besoin de réaliser deux parties essentielles :

- La première partie : le réseau et système

En créant d'abord une architecture réseau de notre hôpital par un choix précis d'équipement réseau tel que (les switches, les routeurs, les serveurs..), plans d'adressage et le routage.

Ensuite, l'installation et la configuration des services de l'infrastructure réseau : DNS, DHCP, LDAP, NAS, serveur WEB de prise de rendez-vous.

- La deuxième partie :

Assurer la sécurité de ce que on a parler en premier par offrir la sécurité de l'accès aux équipements réseau , segmenter notre architecture à deux zones passerelles sécurisée et réseau interne que ce dernier est segmenté aussi grâce à vlans , la configuration des pare-feux et des proxy , donner une solution VPN , et une gestion des accès distant et chiffrement des données clients , la création des vlans.

1.3. Résumé des chapitres :

Dans le présent mémoire, nous présenterons en détail les étapes que nous avons suivies pour réaliser notre projet, illustrées en trois chapitres organisés comme suit :

Le premier chapitre s'intitule « la conception de l'architecture » on définirons en premier lieu ce qu'est la sécurité , la haute disponibilité, les politiques de sécurité d'un système informatique , ensuite nous parlerons de la passerelle sécurisée vers l'internet , son fonctionnement et de ses objectifs , aussi des couches réseau de campus (modèle de conception hiérarchique, la couche d'accès et son mécanisme , la couche distribution et son mécanisme) , nous finirons par parler de notre architecture en détailles .

Dans le deuxième chapitre titré « réalisation et choix techniques » où nous présenterons l'implémentation de la passerelle sécurisée, les choix qu'on fait sur les équipements réseaux et chiffage de la proposition, et les Politique de sécurité du système d'information (PSSI).

Le troisième chapitre nommé « bilan personnel et professionnel » :

Bilan personnel : où nous parlerons des compétences acquises et la façon de durée le temps

Bilan professionnel : nous indiqueront tous ce qu'on a facilité le développement de travail et aussi les difficultés affronter

Enfin , dans la conclusion générale, nous ferons une récapitulation du travail effectué ainsi que l'expérience acquise durant ce projet

Chapitre 01 :

Conception de L'architecture

1. Introduction :

Le travail de conception consiste à déterminer les solutions théoriques qui permettent de satisfaire les besoins des contraintes. Dans cette phase, on donne les définitions des méthodes et des outils utilisés pour concevoir l'architecture d'un réseau sécurisé.

La sécurité c'est les processus et les méthodologies conçus et mis en œuvre pour protéger les informations ou données électroniques ou toute autre forme confidentielles, privées et sensibles contre tout accès, utilisation, abus, divulgation, destruction, modification ou perturbation non autorisés.

Les principes fondamentaux (principes) de la sécurité de l'information sont la confidentialité, l'intégrité et la disponibilité. Chaque élément d'un programme de sécurité de l'information (et chaque contrôle de sécurité mis en place par une entité) doit être conçu pour atteindre un ou plusieurs de ces principes

La confidentialité : signifie que les données, les objets et les ressources sont protégés contre les visualisations et autres accès non autorisés.

L'intégrité : signifie que les données sont protégées contre les modifications non autorisées afin de garantir leur fiabilité et leur exactitude.

La disponibilité : est une caractéristique d'un système qui vise à assurer un niveau convenu de performance opérationnelle

La modernisation a entraîné une dépendance accrue à l'égard de ces systèmes. Par exemple, les hôpitaux et les centres de données nécessitent une haute disponibilité de leurs systèmes pour effectuer les activités quotidiennes de routine. La disponibilité fait référence à la capacité de la communauté d'utilisateurs à obtenir un service ou un bien, à accéder au système, que ce soit pour soumettre un nouveau travail, mettre à jour ou modifier un travail existant, ou collecter les résultats de travaux antérieurs.

Les objectifs principaux de la sécurité de l'information sont d'empêcher la perte de disponibilité, la perte d'intégrité et la perte de confidentialité des systèmes et des données. La plupart des pratiques et des contrôles de sécurité remontent à la prévention des pertes dans un ou plusieurs de ces domaines.

Cette dernière garantit une bonne gestion des données. Cela implique l'utilisation de technologies, de protocoles, de systèmes et de mesures administratives pour protéger la confidentialité, l'intégrité et la disponibilité des informations.

Les outils de sécurité réseau peuvent être logiciels ou matériels et aident les équipes de sécurité à protéger les réseaux, l'infrastructure critique et les données sensibles de leur organisation contre les attaques. ... Ceux-ci incluent des outils tels que des pare-feu, des systèmes de détection d'intrusion et des programmes antivirus basés sur le réseau.

Et pour maximiser la sécurité informatique on a besoin des politiques de sécurité qui fait référence à des plans, règles et pratiques clairs, complets et bien définis qui régissent l'accès au système d'une organisation et aux informations qu'il contient. Une bonne politique protège non seulement les informations et les systèmes, mais également les employés individuels et l'organisation dans son ensemble. Il existe 2 types de politiques de sécurité : les politiques de sécurité technique et les politiques de sécurité administratives. Les politiques de sécurité technique décrivent la configuration de la technologie pour une utilisation pratique ; les politiques de sécurité du corps traitent de la manière dont toutes les personnes devraient se comporter. Tous les travailleurs doivent se conformer et signer chacune des politiques, En résumé, est une déclaration de ce qui est et de ce qui n'est pas autorisé.

L'objectif des politiques de sécurité informatique est de faire face aux menaces de sécurité et de mettre en œuvre des stratégies pour atténuer les vulnérabilités de sécurité informatique, ainsi que de définir comment récupérer lorsqu'une intrusion réseau se produit. De plus, les politiques fournissent des directives aux employés sur ce qu'il faut faire et ne pas faire.

Les étapes de l'élaboration des politiques sont l'élaboration, la formulation, l'adoption, la mise en œuvre, l'évaluation et la résiliation du programme.

2. Passerelle sécurisée vers internet :

2.1. Définition :

Les pare-feu ont souvent ce qu'on appelle communément une DMZ. DMZ signifie zone démilitarisée, ce qui n'a bien sûr rien à voir avec l'informatique. Il s'agit d'un terme militaire/politique faisant référence à une zone créée entre des forces opposées dans laquelle aucune activité militaire n'est autorisée. Par exemple, une zone démilitarisée a été créée entre la Corée du Nord et la Corée du Sud.

Dans le domaine de la sécurité du réseau, une DMZ est un réseau qui n'est ni à l'intérieur ni à l'extérieur du pare-feu. L'idée est que ce troisième réseau est accessible depuis l'intérieur (et probablement l'extérieur) du pare-feu, mais les règles de sécurité interdisent aux appareils de la DMZ de se connecter à des appareils à l'intérieur. Une DMZ est moins sécurisée que le réseau interne, mais plus sécurisée que le réseau externe.

Un scénario DMZ courant est illustré à la Figure 01. Internet est situé sur l'interface externe. Les utilisateurs sont sur l'interface interne. Tous les serveurs qui doivent être accessibles depuis Internet sont situés dans le réseau DMZ.

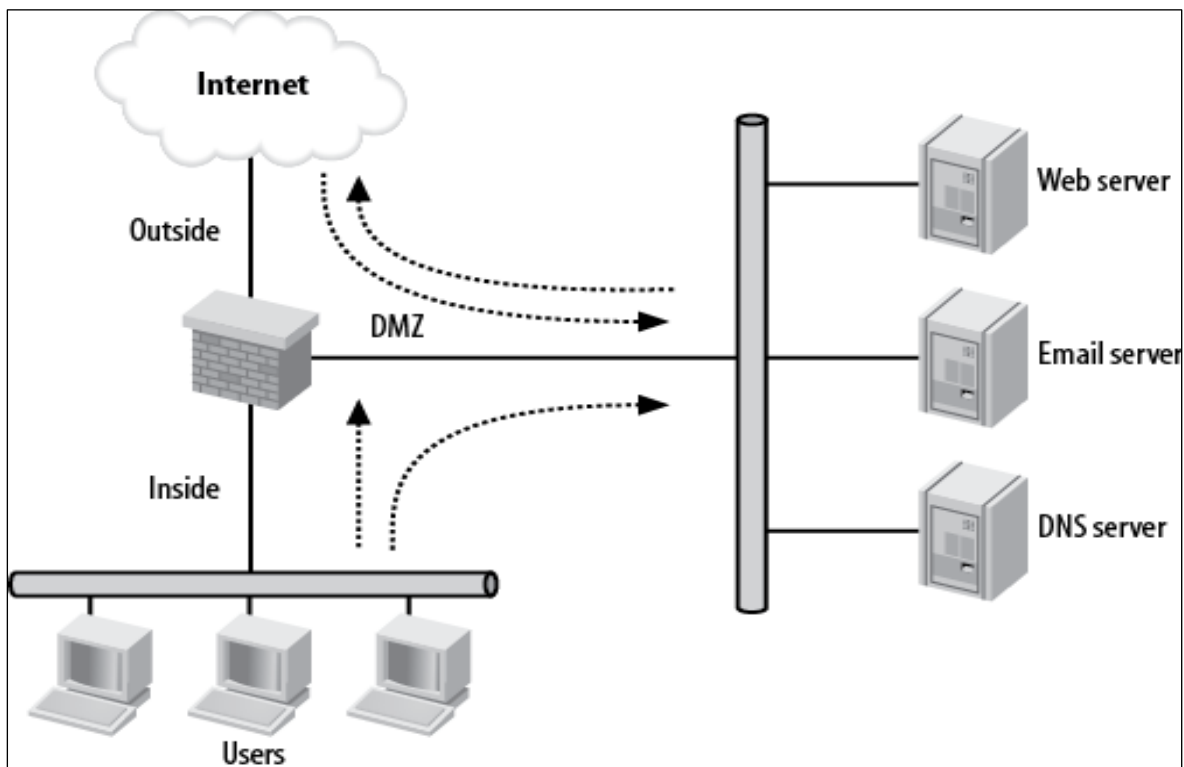


Figure 01 : Réseau DMZ simple.

Dans ce réseau, le pare-feu doit être configuré comme suit:

- **Réseau intérieur :**

Le réseau interne peut initier des connexions à n'importe quel autre réseau, mais aucun autre réseau ne peut initier de connexions avec lui.

- **Réseau extérieur :**

Le réseau extérieur ne peut pas initier des connexions au réseau intérieur.

Une ou plusieurs « DMZ » forme une passerelle d'interconnexion sécurisée.

Les « DMZ » doivent être des zones neutres, perdables et protégées par des pare-feux, ils servent à la rupture protocolaire et à l'analyse du trafic échangé entre un réseau public et le SI interne de l'entité [5].

L'objectif d'une DMZ est d'ajouter une couche de sécurité supplémentaire au réseau local d'une organisation. Un nœud de réseau protégé et surveillé qui fait face à l'extérieur du réseau interne peut accéder à ce qui est exposé dans la DMZ, tandis que le reste du réseau de l'organisation est en sécurité derrière un pare-feu.

Tout service fourni aux utilisateurs sur l'Internet public doit être placé dans le réseau DMZ. Certains des services les plus courants incluent les serveurs Web et les serveurs proxy, ainsi que les serveurs de messagerie, le système de noms de domaine (DNS), le protocole de transfert de fichiers (FTP) et la voix sur IP (VoIP).

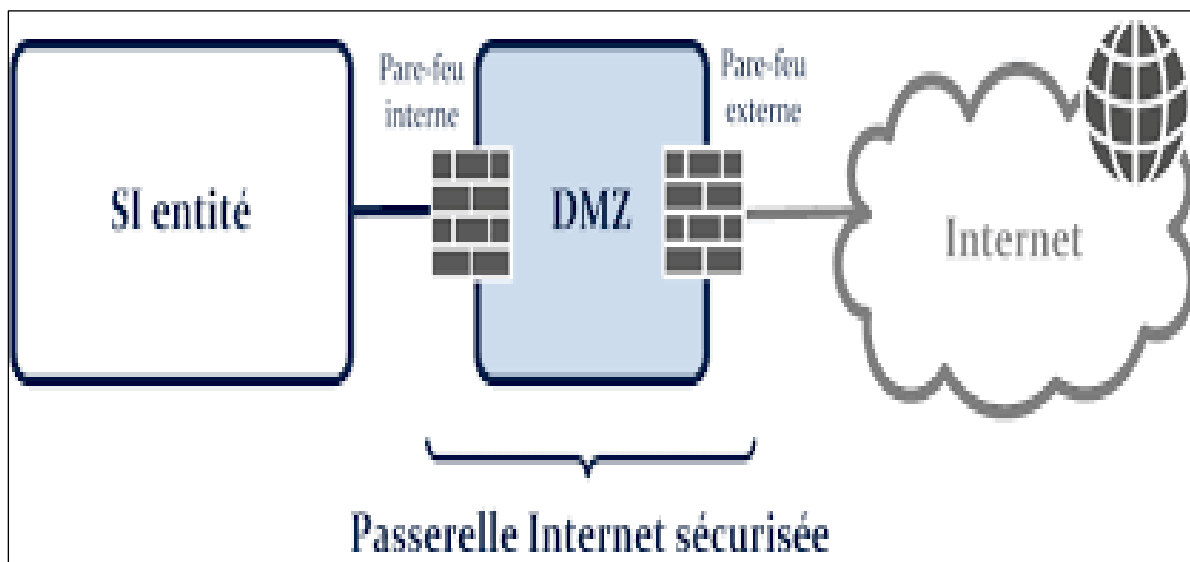


Figure 02: Passerelle sécurisée vers internet.

Dans notre architecture on a utilisé une seule « DMZ » où on a met 2 pare-feu, un serveur proxy, serveur DNS, serveur proxy inverse, NAT et IDS/IPS, leurs définitions sont comme suit :

2.2. Pare-feu (firewall) :

2.2.1. Définition :

Un pare-feu est un dispositif de sécurité réseau qui surveille le trafic réseau entrant et sortant et décide d'autoriser ou de bloquer un trafic spécifique en fonction d'un ensemble défini de règles de sécurité.

Les pare-feu constituent la première ligne de défense des réseaux depuis plus de 25 ans. Ils établissent une barrière entre les réseaux internes sécurisés et contrôlés qui sont dignes de confiance et les réseaux externes non fiables tels qu'Internet.

Un pare-feu peut être un équipement physique, un logiciel ou une combinaison des deux [6].

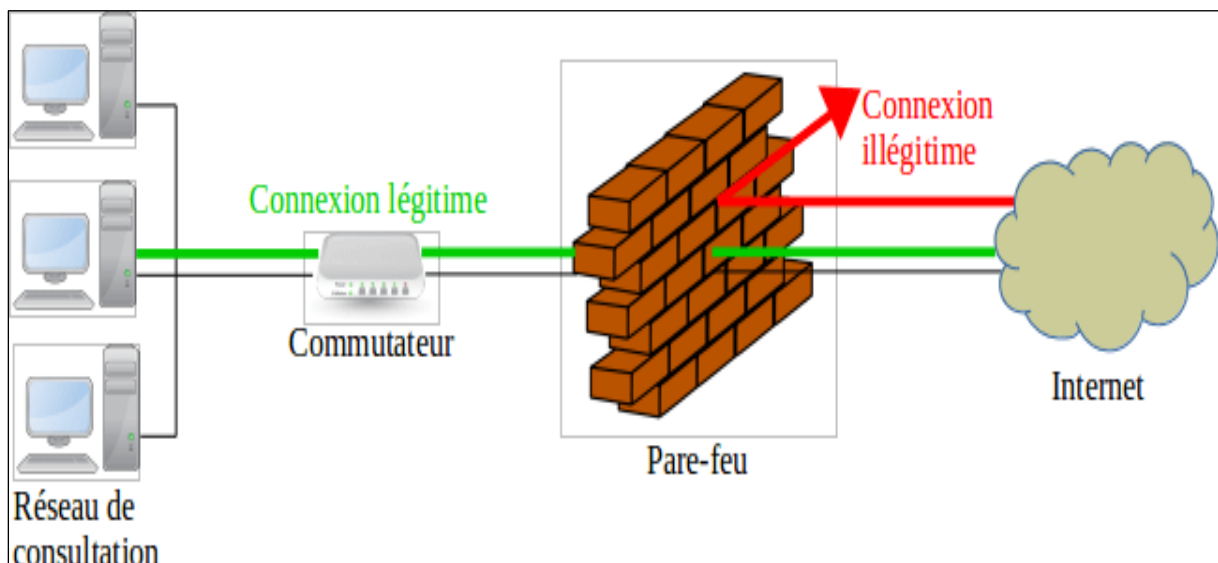


Figure 03: Pare-feu (firewall)

2.3. Proxy :

2.3.1. Définition :

Un serveur proxy fournit une passerelle entre les utilisateurs et Internet. Il s'agit d'un serveur, appelé « intermédiaire » car il relie les utilisateurs finaux aux pages Web qu'ils visitent en ligne. Lorsqu'un ordinateur se connecte à Internet, il utilise une adresse IP.

Les serveurs proxy agissent comme un pare-feu et un filtre Web, fournissent des connexions réseau partagées et mettent en cache les données pour accélérer les requêtes courantes. Un bon serveur proxy protège les utilisateurs et le réseau interne des mauvaises choses qui vivent sur Internet. Enfin, les serveurs proxy peuvent offrir un niveau élevé de confidentialité.

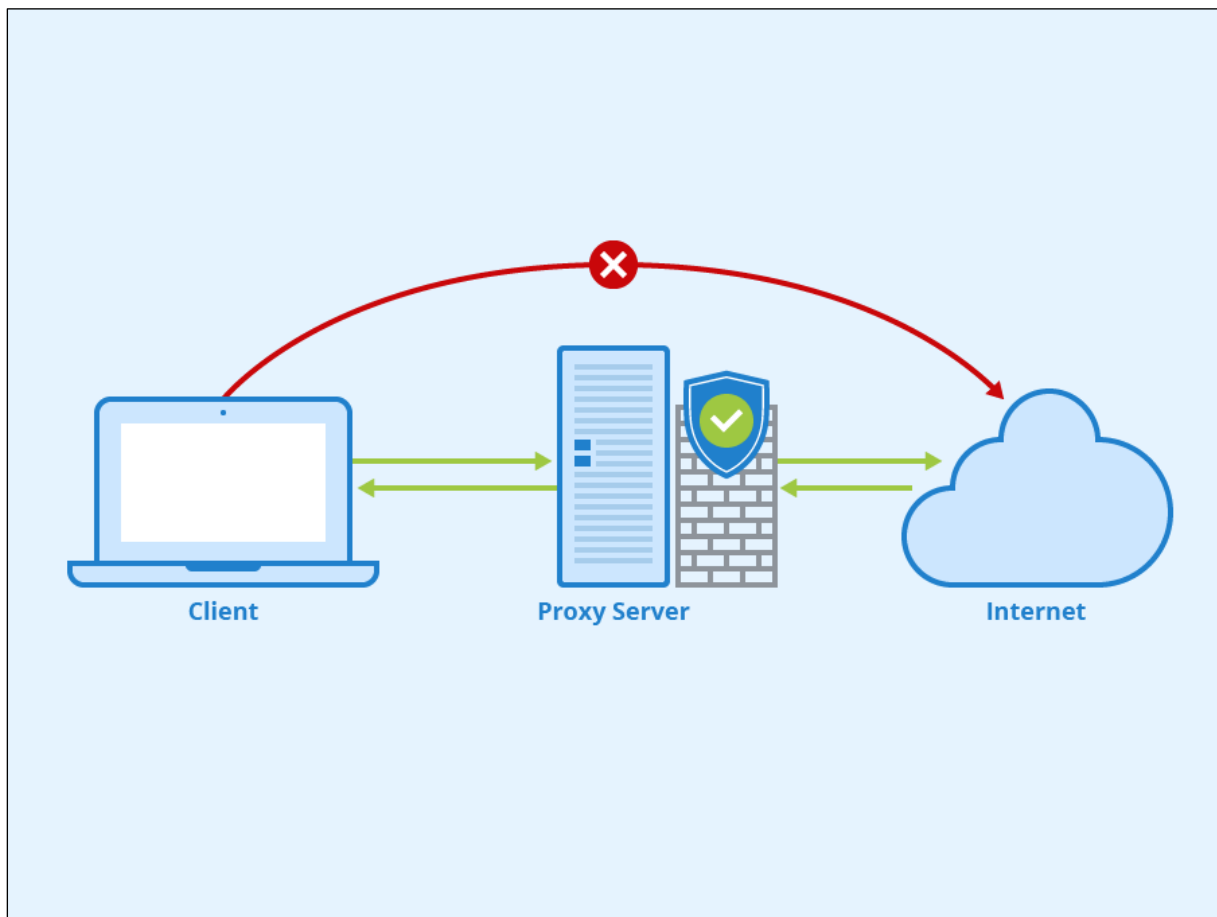


Figure 04 : Un serveur proxy.

2.4. Serveur DNS :

2.4.1. Définition :

Un serveur DNS est un serveur informatique qui contient une base de données d'adresses IP publiques et leurs noms d'hôtes associés, et sert dans la plupart des cas à résoudre ou traduire ces noms en adresses IP comme demandé. Les serveurs DNS exécutent un logiciel spécial et communiquent entre eux à l'aide de protocoles spéciaux.

La fonction la plus basique d'un serveur DNS est de traduire un nom de domaine en son adresse IP respective.

On cite par la suite les 3 types de serveur DNS :

Serveur maître (master) : le serveur maître fait autorité sur la zone DNS qu'il héberge. Les changements sont faits sur ce serveur, puis sont renvoyés (copiés) vers les serveurs secondaires (esclave) via le mécanisme de réplication.

Serveur esclave (slave) : le serveur esclave réplique les zones gérées par le serveur maître (master) en fonction de type de réplication mise en place. Ils font également autorité sur la zone qui héberge le serveur maître. Il peut assurer la disponibilité du service en cas de panne du serveur maître.

Serveur de cache : ce serveur garde en cache les requêtes DNS afin de répondre rapidement à la prochaine requête (identique). C'est ce qui permet d'améliorer les performances (limiter l'utilisation de la bande passante, réduire le temps de latence...). Cependant, les données sont vite obsolètes et il faut donc vider le cache DNS [7].

Dans l'architecture que nous avons proposée, nous n'avons utilisé que le serveur DNS maître.

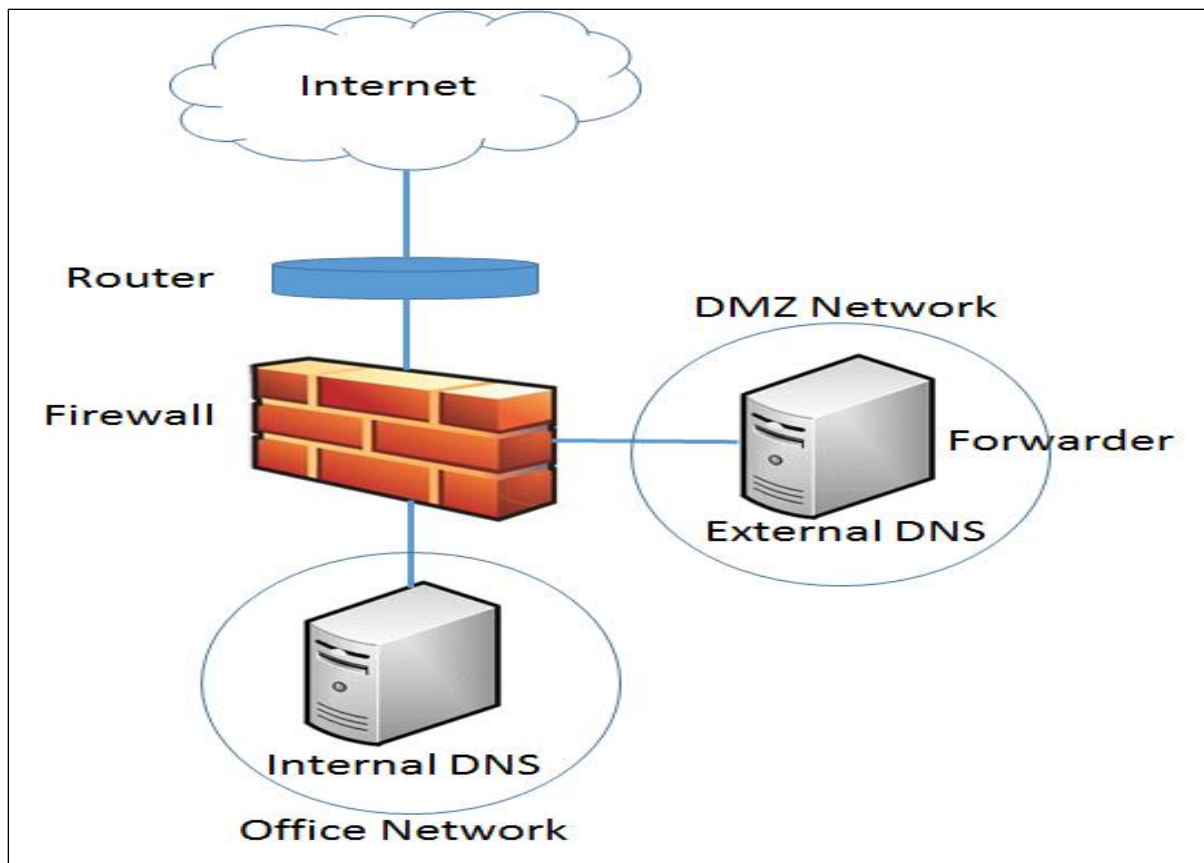


Figure 05 : Un serveur DNS.

2.5. Proxy inverse :

2.5.1. Définition :

Un serveur proxy inverse est un type de serveur proxy qui se trouve généralement derrière le pare-feu dans un réseau privé et dirige les demandes des clients vers le serveur principal approprié. Un proxy inverse fournit un niveau supplémentaire d'abstraction et de contrôle pour assurer la fluidité du trafic réseau entre les clients et les serveurs [8].

Un proxy inverse accepte une demande d'un client, la transmet à un serveur qui peut la satisfaire et renvoie la réponse du serveur au client. Un équilibreur de charge répartit les demandes client entrantes parmi un groupe de serveurs, renvoyant dans chaque cas la réponse du serveur sélectionné au client approprié.

Il offre également des avantages supplémentaires, notamment le masquage des serveurs Web et l'amélioration des performances

Comme son nom l'indique, un proxy inverse fait exactement le contraire de ce que fait un proxy direct. Alors qu'un proxy direct agit au nom des clients (ou des hôtes demandeurs), un proxy inverse agit au nom des serveurs. ... Dans la plupart des cas, les serveurs proxy inverses agissent également comme des équilibreurs de charge pour les serveurs derrière eux.

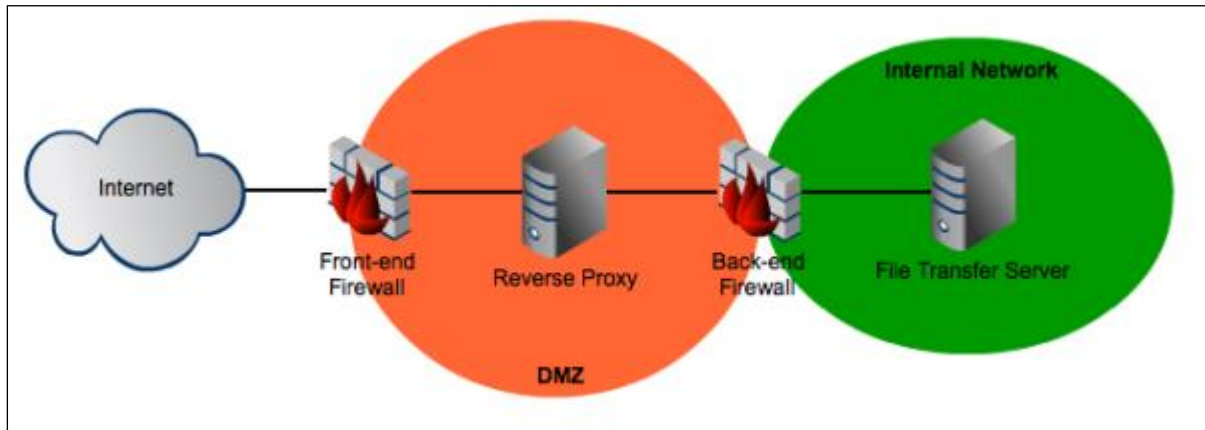


Figure 06: Proxy inverse (Reverse proxy).

2.6. La NAT :

2.6.1. Définition :

Est conçu pour la conservation des adresses IP. Il permet aux réseaux IP privés qui utilisent des adresses IP non enregistrées de se connecter à Internet [9].

Le NAT est un aspect très important de la sécurité du pare-feu. Il conserve le nombre d'adresses publiques utilisées au sein d'une organisation et permet un contrôle plus strict de l'accès aux ressources des deux côtés du pare-feu [10].

Il permet un certain type de sécurité, en ce sens que les personnes extérieures à votre réseau ne peuvent pas initier de connexions à l'intérieur de votre réseau. Cela réduit les vers et autres classes de logiciels malveillants.

Il existe deux types de NAT différents, la NAT dynamique et la NAT statique.

La NAT dynamique : associe n adresses privées à une seule adresse publique. Ainsi, on peut connecter n machines en n'utilisant qu'une seule adresse publique (one to many).

La NAT statique : on fixe une adresse publique pour chaque adresse privée (one to one) [11].

On a utilisé la NAT dynamique car celle-ci permet de répondre à la pénurie d'adresse IP.

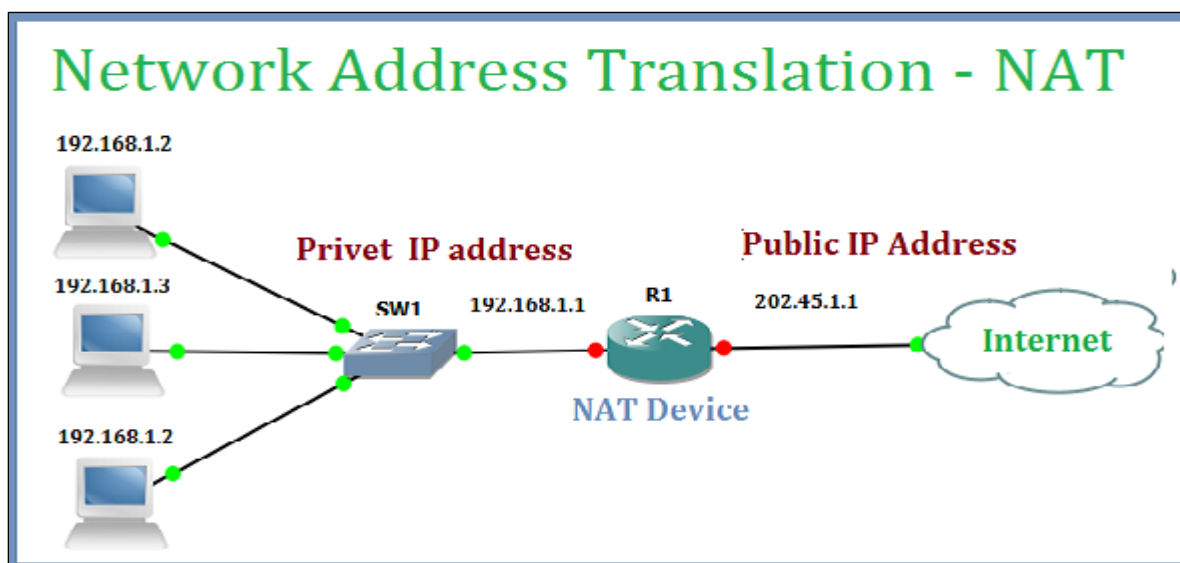


Figure 07 : NAT (Network Address Translation).

2.7. IDS/IPS :

2.7.1. Définition :

IDS et IPS sont des objets connexes aux pare-feu dans le rôle de filtrage de sécurité des réseaux. Ils sont le résultat d'une évolution technologique. Un IDS détecte des intrusions et il devient IPS quand il est capable d'y réagir automatiquement.

2.7.2. IDS (Système de Détection d'Intrusion) :

Un système de détection d'intrusion (IDS) est un dispositif ou une application logicielle qui surveille un réseau ou des systèmes pour déceler toute activité malveillante ou toute violation de politique de sécurité. Toute activité malveillante ou violation est généralement signalée à un administrateur ou est recueillie de façon centralisée au moyen d'un système de gestion des informations et des événements de sécurité (SIEM). Un système SIEM combine des sorties provenant de sources multiples et utilise des techniques de filtrage des alarmes pour distinguer les activités malveillantes des fausses alarmes.

2.7.3. IPS (Systèmes de Prévention des Intrusions) :

Les systèmes de prévention des intrusions (IPS), également connus sous le nom de systèmes de détection et de prévention des intrusions (IDPS), sont des dispositifs ou une

application logicielle de sécurité réseau qui surveille les activités du réseau ou du système pour détecter toute activité malveillante. Les principales fonctions des systèmes de prévention des intrusions sont d'identifier les activités malveillantes, d'enregistrer des informations sur ces activités, de les signaler et de tenter de les bloquer ou de les arrêter.

2.7.4 Distinction entre pare-feu et IDS/IPS :

Bien qu'ils soient tous deux liés à la sécurité du réseau, un IDS se distingue d'un pare-feu en ce sens qu'un pare-feu surveille les intrusions vers l'extérieur afin de les empêcher de se produire. Les pare-feu limitent l'accès entre les réseaux pour prévenir les intrusions et ne signalent pas une attaque de l'intérieur du réseau. Un IDS décrit une intrusion suspectée une fois qu'elle a eu lieu et signale une alarme. Un IDS surveille également les attaques provenant de l'intérieur d'un système. On y parvient traditionnellement en examinant les communications réseau, en identifiant les heuristiques et les modèles (souvent connus sous le nom de signatures) des attaques informatiques courantes et en prenant des mesures pour alerter les opérateurs. Un système qui termine les connexions s'appelle un système de prévention des intrusions et effectue le contrôle d'accès comme un pare-feu de couche d'application. [12].

3. Couches de réseau de campus :

3.1. Modèle de conception hiérarchique:

Le modèle de conception de réseau hiérarchique divise le réseau plat complexe en plusieurs réseaux plus petits et plus gérables. Chaque niveau de la hiérarchie se concentre sur un ensemble spécifique de rôles. Cette approche de conception offre aux concepteurs de réseaux un degré élevé de flexibilité pour optimiser et sélectionner le matériel, les logiciels et les fonctionnalités réseau appropriés pour remplir des rôles spécifiques pour les différentes couches réseau.

Une conception de réseau de campus d'entreprise hiérarchique typique comprend les trois couches suivantes :

- **Couche principale :** fournit un transport optimal entre les sites et un routage à haute performances.

En raison de la criticité de la couche centrale, les principes de conception du cœur doivent fournir un niveau de résilience approprié qui offre la possibilité de récupérer rapidement et en douceur après tout événement de défaillance du réseau avec le bloc central.

- **Couche de distribution** : Fournit une connectivité basée sur des politiques et un contrôle des limites entre les couches d'accès et de base.
- **Couche d'accès** : Fournit l'accès du groupe de travail/utilisateur au réseau.

Les deux architectures de conception hiérarchique principales et communes des réseaux de campus d'entreprise sont les modèles de couches à trois et deux niveaux [10].

3.1.1. Modèle à trois niveaux :

Ce modèle de conception, illustré à la Figure 08, est généralement utilisé dans les grands réseaux de campus d'entreprise, qui sont constitués de plusieurs blocs de couche de distribution fonctionnelle.

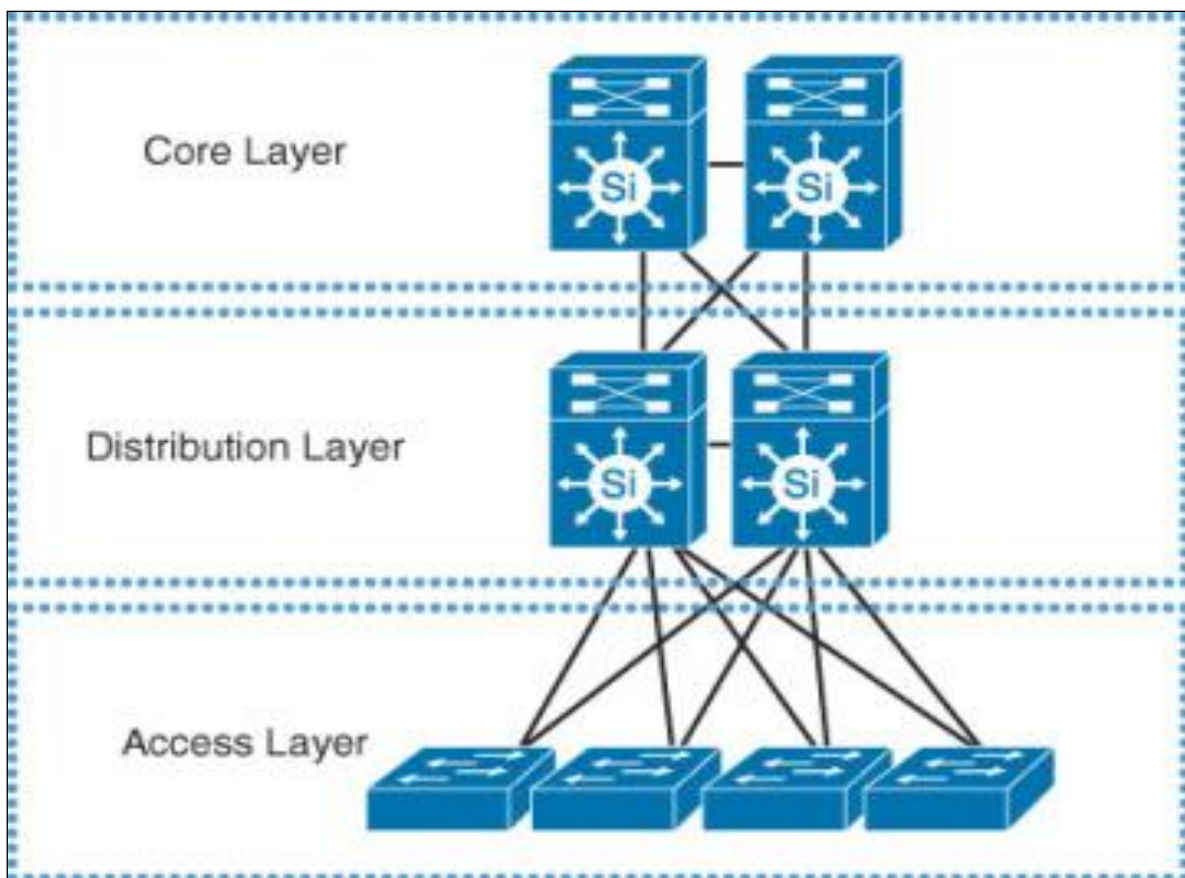


Figure 08 : Modèle de conception de réseau à trois niveaux.

3.1.2. Modèle à deux niveaux :

Ce modèle de conception, illustré à la Figure 09, est plus adapté aux réseaux de campus de petite et moyenne taille (idéalement pas plus de trois blocs fonctionnels à interconnecter), où les fonctions centrales et de distribution peuvent être combinées en une seule couche, également connue sous le nom d'architecture de distribution principale effondrée [5].

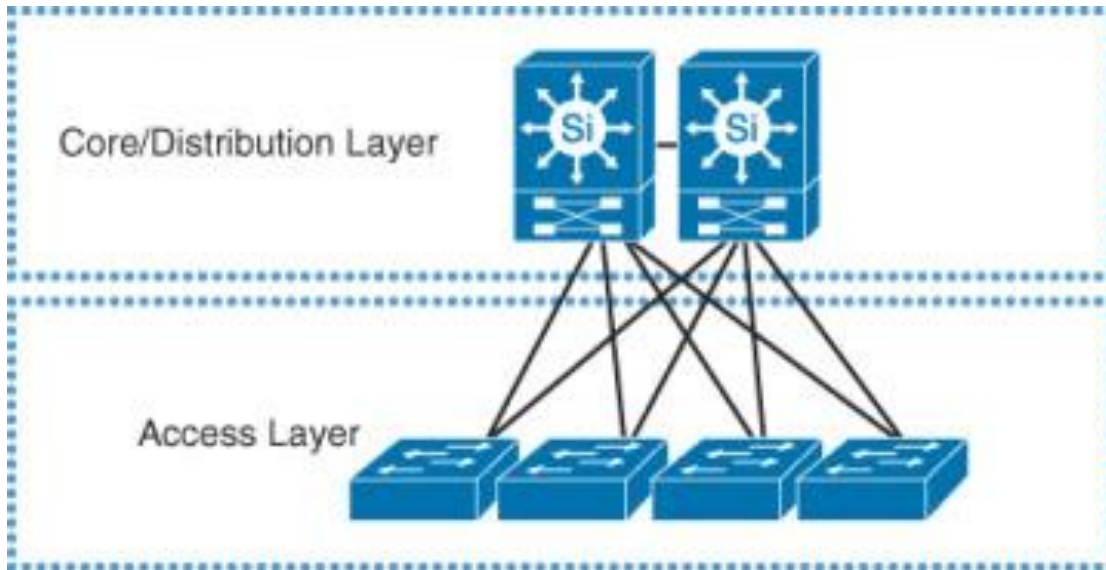


Figure 09 : Modèle de conception de réseau à deux niveaux.

Remarque : Le terme bloc de distribution fonctionnel fait référence à tout bloc du réseau du campus qui possède sa propre couche de distribution, tel qu'un bloc d'accès utilisateur, un bloc WAN ou un bloc de centre de données.

Dans notre architecture on a utilisé le modèle à deux niveaux car notre réseau de campus est de taille moyenne, par suite on va définir encore, ses couches avec leur mécanismes [13].

3.1.2.1. Définition de la couche d'accès :

Regroupement des postes des utilisateurs finals, des téléphones IP et des serveurs
Connexion aux commutateurs de la couche de distribution
Toutes les liaisons ascendantes acheminent activement le trafic (distribution de couche 3)
Dispositif de couche 2—Avec l'intelligence de couche 3 (sécurité, QoS, IP Multicast, etc.)
Utilisation d'Intelligent Network Services pour l'établissement de la frontière de confiance (Trust Boundary)

Commutation de couche 2 au niveau de l'armoire de câblage (peut être sensible à la couche 3)
Frontière de politique (policy boundary)

3.1.2.2. Mécanismes de la couche d'accès :

- Protocoles de niveau 2 (spanning tree protocol) : IEEE 802.1D, Rapid Spanning Tree Protocol (802.1w), Multiple Spanning Tree (802.1s).
- Caractéristiques STP : UplinkFast, CrossStack UplinkFast, Portfast, LoopGuard, BPDUGuard.
- Services réseau intelligents : Qualité de service, classification et contrôle du trafic, contrôle des accès, alimentation en ligne, VLAN voix , suppression de diffusion, agrégation de liens (trunking).
- VLAN privés.

3.1.2.3. Définition de la couche de distribution :

- Agrégation des armoires de câblage (couche d'accès) et liaison montante (uplink) au réseau d'infrastructure
- Protection du noyau contre l'interconnexion égale à égale à densité élevée
- Disponibilité, équilibre de charge et qualité de service sont les points importants à considérer au niveau de cette couche Utilisation de la commutation de couche 3 au niveau de la couche de distribution Suivi HSRP (tracking) et redondance de premier bond.

Commutation de niveau 3 Utilisation de protocoles de routage pour assurer des avantages comme l'équilibre de charge, la convergence rapide et l'évolutivité Procure une redondance/résilience de premier bond Regroupe les éléments de la couche d'accès.

3.1.2.4. Mécanismes de la couche de distribution :

- Caractéristiques de STP : Configuration de "STP Root" Protection avec "Root Guard".
- Routage de couche 3 :

Pèse les routes: Assure une symétrie

Sommaire de routes: Vers le noya

- HSRP :

Hot Standby Routing Protocol (HSRP): redondance premier bond

HSRP Timers: Reduit temps de panne

HSRP Track : Routage optimal

4. Architecture détaillée :

4.1. Introduction :

Dans ce titre nous commencerons par une présentation générale du réseau Intranet de l'hôpital, nous expliqueront comment se fait le routage inter-Vlan, ensuite nous essayerons de réduire le risque en voyant les vulnérabilités du réseau et donnerons des suggestions pour améliorer sa sécurité parce que l'hôpital data est sensible et tout échec de l'homme fait ou accidentel coûtera énormes pertes et impact social.

4.2. Présentation du réseau intranet :

Le réseau informatique de CHIFA hôpital est segmenté à deux zones : passerelle sécurisée et réseau interne, chaque zone contient plusieurs équipements informatiques et différents mécanismes appliqués pour sécuriser elle.

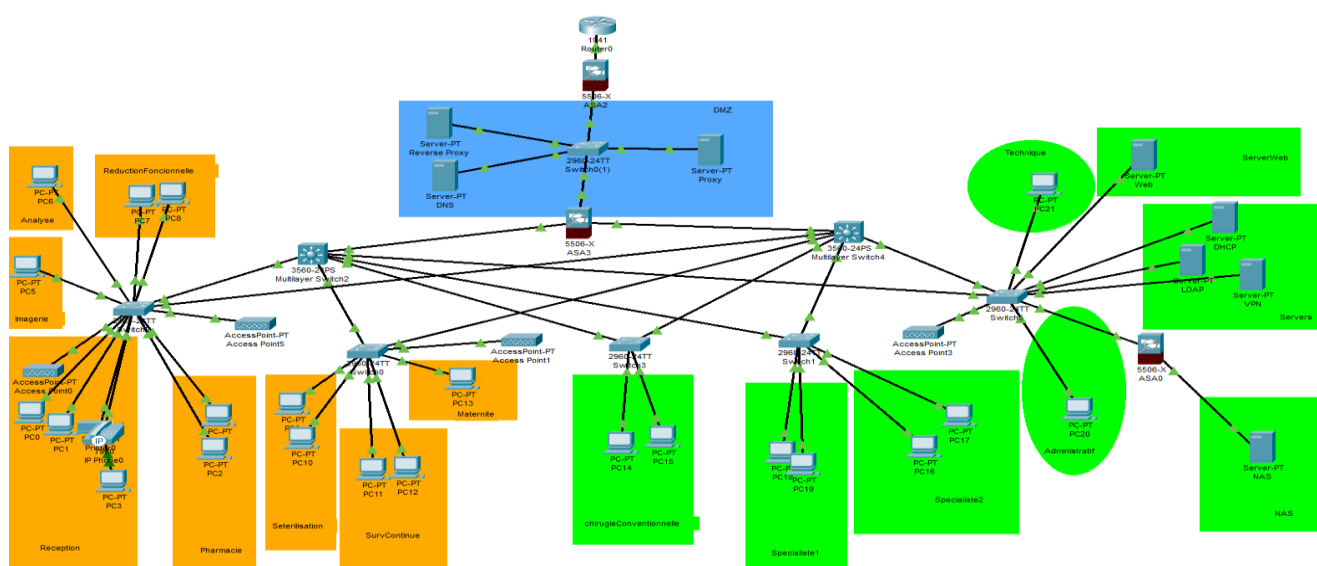


Figure 10 : Réseau locale.

4.2.1. Passerelle sécurisée :

Dans la passerelle sécurisée de notre architecture ou ce qu'on appelle ça DMZ nous mettons les services accessibles par internet nous listons serveur Dns, proxy, reverse proxy, connecté par câble a un commutateur. Nous avons utilisé 2 pare-feu : pare-feu interne et pare-feu externe, nous avons attribué ces services (pas des pare-feu) a vlan 79 de nom DMZ (Figure 11).

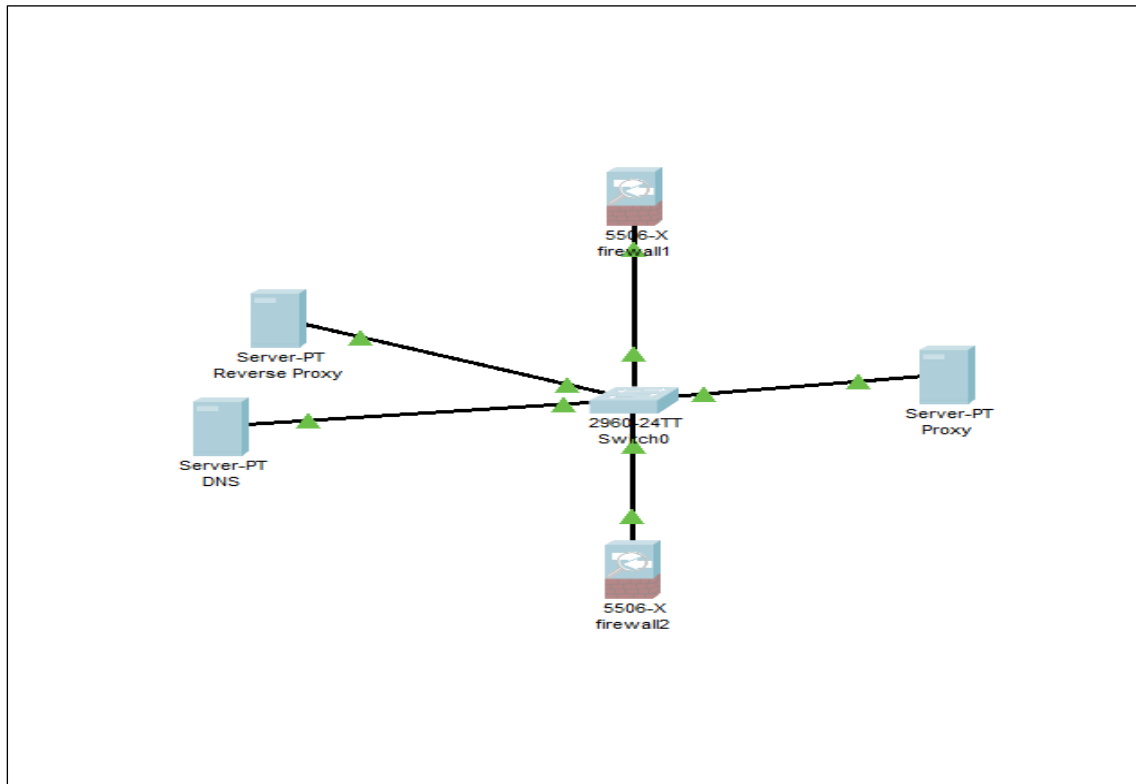


Figure 11 : Passerelle sécurisée.

4.2.2. Réseau interne :

La couche de réseau de campus utiliser dans l'hôpital est le modèle à deux niveaux parce que CHIFA hôpital consiste d'un seul bâtiment et d'autre objectif est pour minimiser le cout de l'architecture, dans la couche de distribution on a utilisé deux commutateur multicouche, la raison pour laquelle nous avons utilisé deux est d'atteindre la redondance , la haute disponibilité et d'assuré que le système est toujours en marche, au cas où l'un d'eux est en panne, l'autre fera tout le travail et maintiendra le système en marche. Dans la couche accès on a utilisé cinq commutateur chaque commutateur est connecté avec la couche distribution à l'aide de deux câbles torsadés, cela nous permettra de transmettre des données

de plus de 100 mégabits par seconde (fast Ethernet Lan), on a placé ici tous les services qui ne sont pas accessible par l'internet (NAS, serveur VPN, DHCP...). Notre réseau est segmenté logiquement a des sous-réseaux utilisant des vlan que nous avons créé pour chaque service hospitalier, pour chaque vlan nous avons assigné suffisamment de port de commutateur, tous les vlan seront listés ci-dessous :

Tableau 01 : Segmentation de réseau interne.

VLAN	NOM
10	Reception
11	Seterilisation
15	SurvContinue
19	Maternite
20	Urgence
23	chirurgieConventionnelle
24	chirurgieAmbulatoire
30	Imagerie
40	Analyse
50	Pharma
51	specialiste2
55	specialiste1
60	ReeductionFonc
61	Administratif
62	ServerWeb
66	Servers
69	Technique
70	Specialiste3
71	Specialiste4
73	NAS
79	DMZ
80	Wireless

Nous avons ajouté une connexion sans fil au réseau filaire de l'hôpital, en mettant dans chaque étage 2 point d'accès sauf le dernier étage on n'en met qu'un, nous avons configuré les

points d'accès pour utiliser le même SSID et le même mot de passe, Ainsi, lorsque quelqu'un se promène dans l'hôpital, son appareil passera d'AP à AP sans qu'il s'en remarque. Nous avons créé des vlans de vlan 10 à vlan 73 pour segmenter notre réseau sans fil.

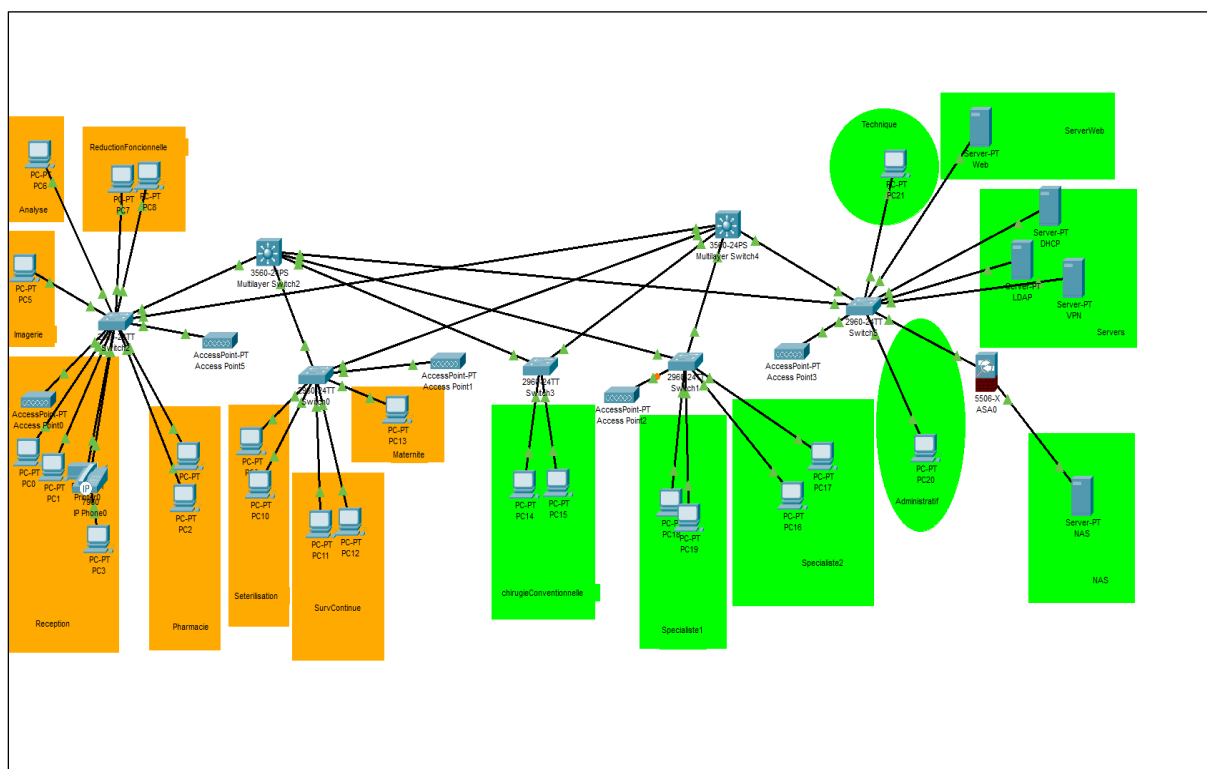


Figure 12 : Architecture de réseau interne de l'hôpital.

4.2.2.1. Adressage IP :

Nous adressons notre réseau avec l'adresse IP classe c 192.168.1.0 – 192.168.2.255 nous avons utilisé VLSM pour le sous-réseau, nous avons utilisé le serveur DHCP(192.168.2.115) pour attribuer des adresses IP à nos appareils, nous listons les adresses IP comme le montre le tableau :

Tableau 02 : Table d'adressage.

VLAN	ADRESSE IP
Reception	192.168.1.16/28
Seterilisation	192.168.1.112/28
SurvContinue	192.168.1.128/28
Maternite	192.168.1.144/28
Urgence	192.168.1. 32/28
chirurgieConventionnelle	192.168.1.160/27
chirurgieAmbulatoire	192.168.1.192/27
Imagerie	192.168.1.48/28
Analyse	192.168.1.64/28
Pharma	192.168.1.80/28
specialiste2	192.168.1.224/27
specialiste1	192.168.2.0/27
ReeductionFonc	192.168.1.96/28
Administratif	192.168.2.96/29
ServerWeb	192.168.2.104/29
Servers	192.168.2.112/29
Technique	192.168.2.120/29
Specialiste3	192.168.2.32/27
Specialiste4	192.168.2.64/27
NAS	192.168.2.128/29
DMZ	192.168.2.136/29

4.2.2.2. Routage :

Tant que votre réseau est segmenté, nous devons implémenter le routage afin que le trafic réseau soit transmis entre les vlans, Nous avons utilisé Multilayer Switch Inter-vlan (SVI) pour y parvenir. Nous avons mis d'abord les ports qui connectent les commutateurs d'accès aux commutateurs de distribution en mode trunk, et nous avons créé les mêmes vlans de la couche d'accès sur les commutateurs de couche distribution, alors nous serons prêts à

transférer le trafic, et notre commutateurs multicouche lorsque nous exécutons la commande « show ip route » affichera :

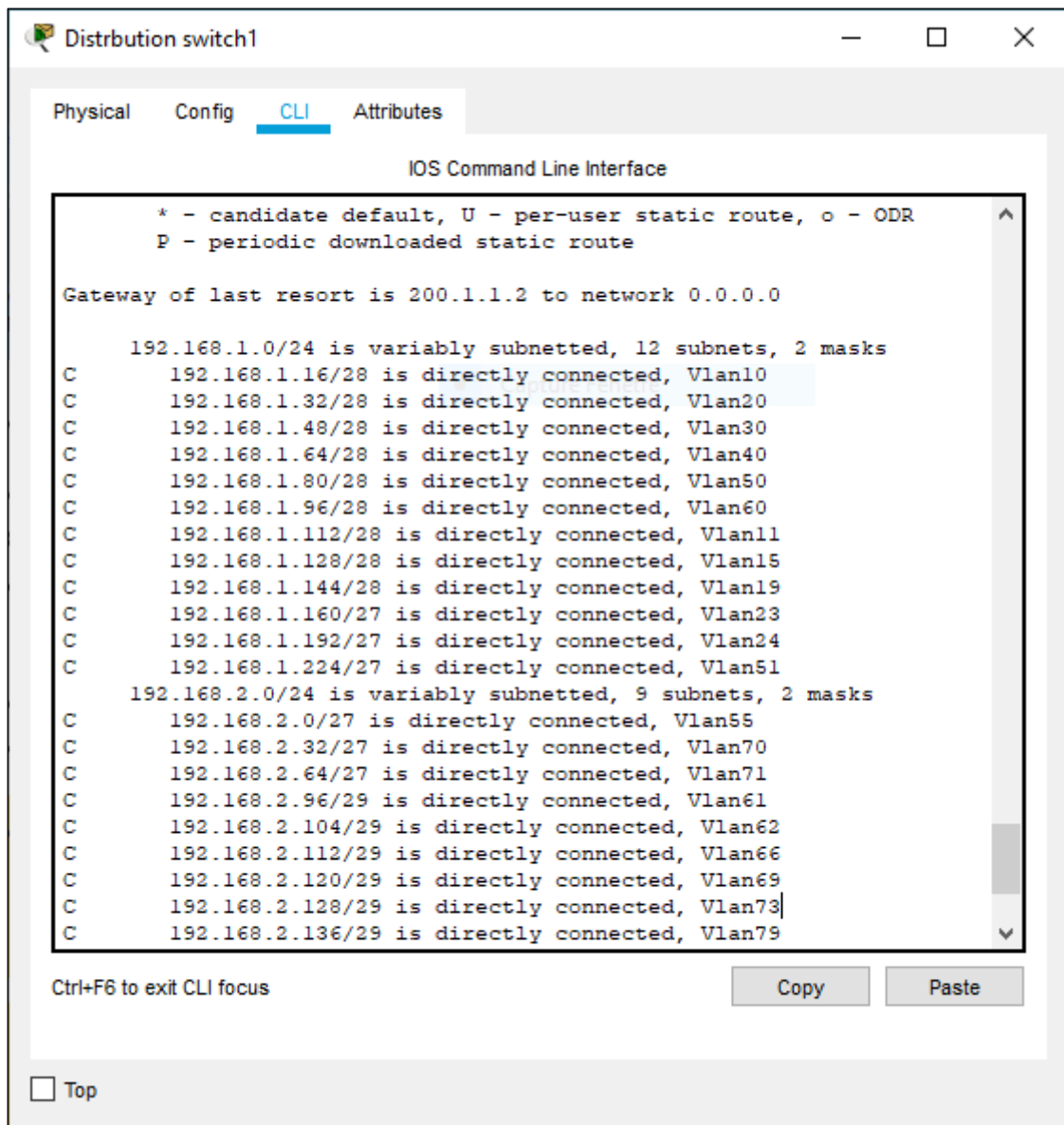


Figure 13: Commutateur Distribution1.

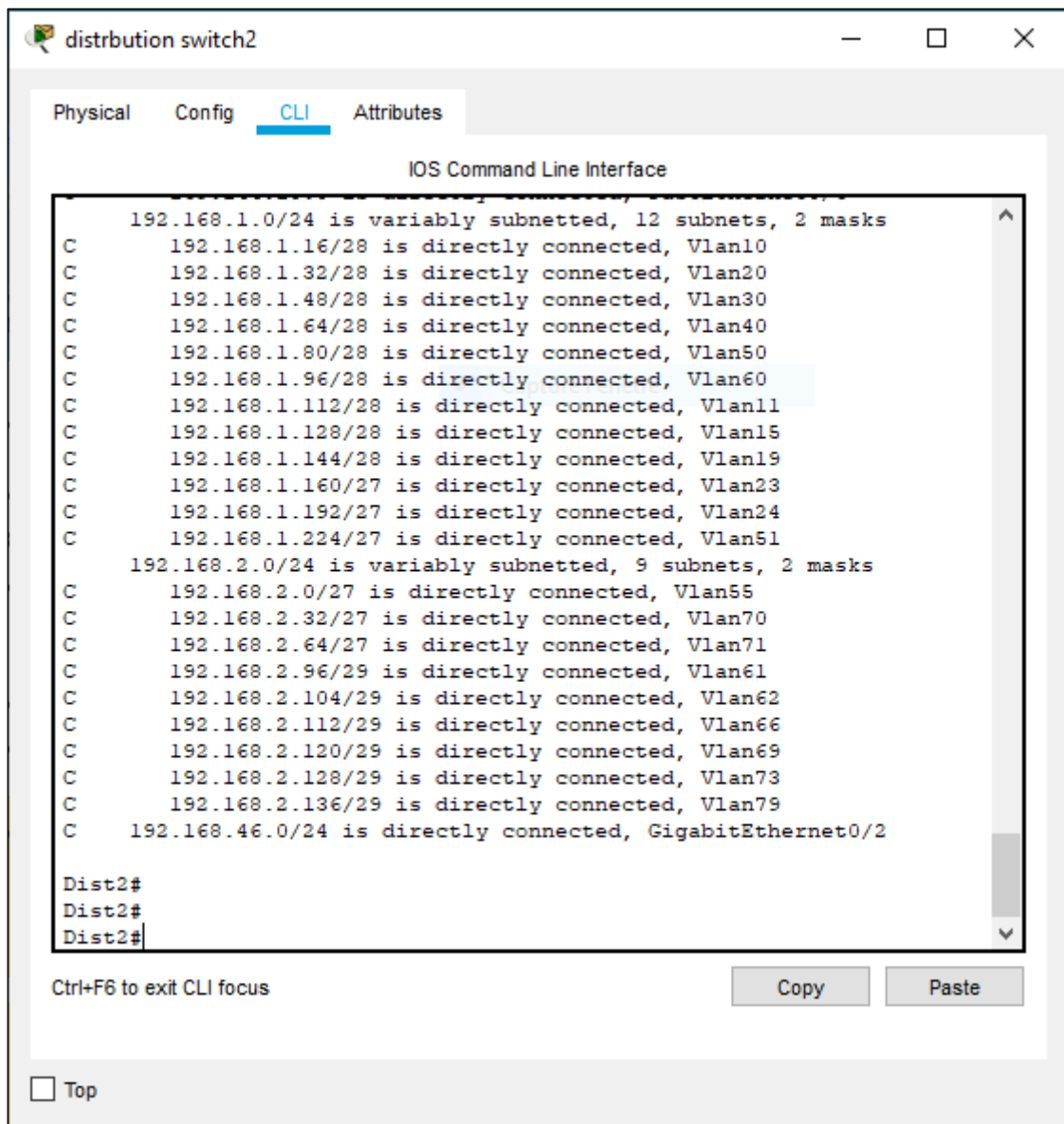


Figure 14 : Commutateur Distribution2.

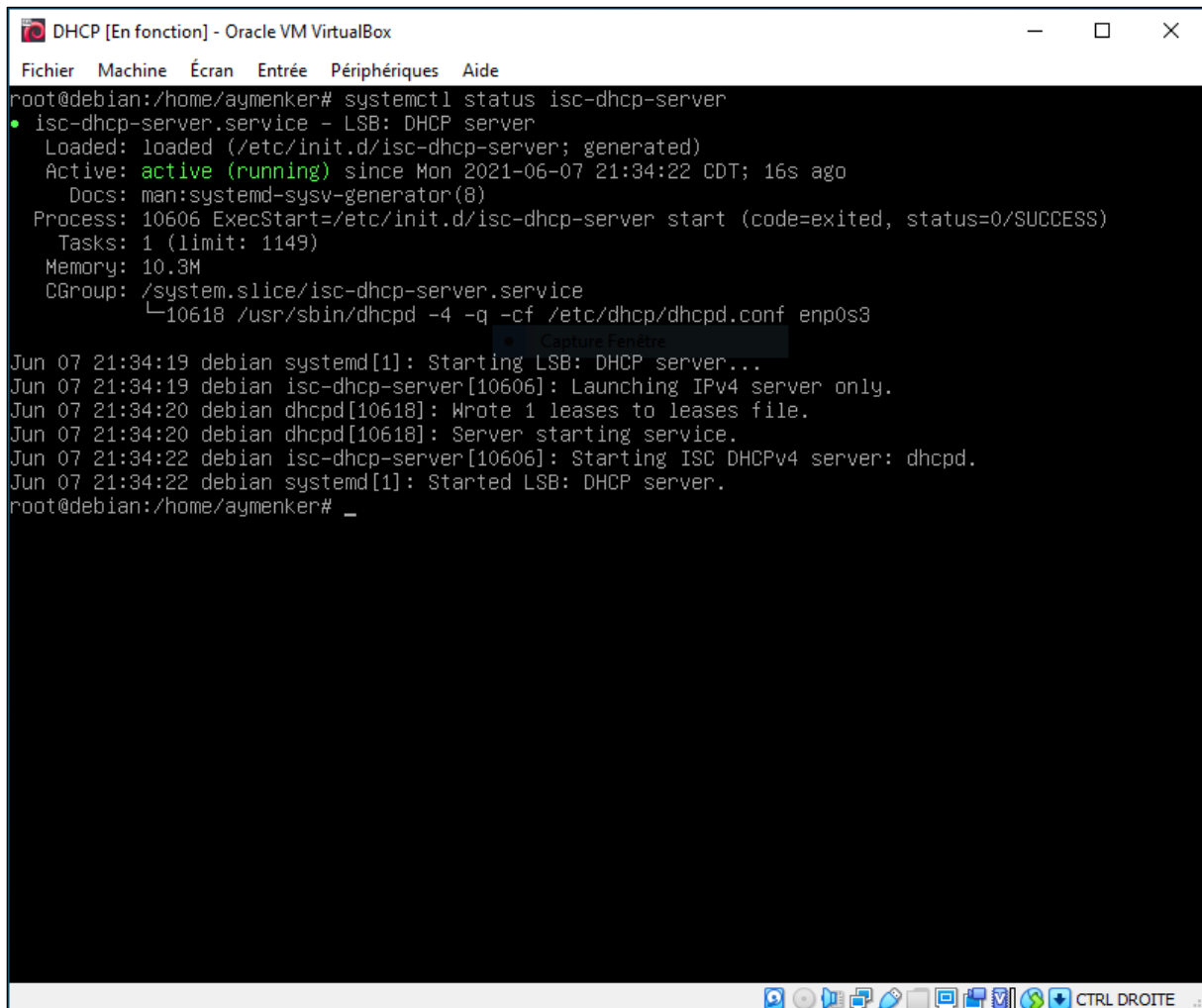
4.2.2.3. Serveur DHCP :

Quand on configure un réseau local, un client a besoin de certaines informations comme l'adresse IP. Avec le DHCP les ordinateurs font cela tout seul, à votre place. Ceci est particulièrement pratique pour connecter les ordinateurs portables au réseau.

Pour bénéficier de ces services nous avons installé le software isc-dhcp-server on serveur DHCP utilisant la commande « apt-get install isc-dhcp-server ».

Le serveur DHCP est configuré et fonctionne parfaitement comme la montre la figure :

La commande « `systemctl status isc-dhcp-server` ».



```
root@debian:/home/aymenker# systemctl status isc-dhcp-server
• isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: active (running) since Mon 2021-06-07 21:34:22 CDT; 16s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 10606 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 1149)
   Memory: 10.3M
    CGroup: /system.slice/isc-dhcp-server.service
            └─10618 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf enp0s3

Jun 07 21:34:19 debian systemd[1]: Starting LSB: DHCP server...
Jun 07 21:34:19 debian isc-dhcp-server[10606]: Launching IPv4 server only.
Jun 07 21:34:20 debian dhcpd[10618]: Wrote 1 leases to leases file.
Jun 07 21:34:20 debian dhcpd[10618]: Server starting service.
Jun 07 21:34:22 debian isc-dhcp-server[10606]: Starting ISC DHCPv4 server: dhcpd.
Jun 07 21:34:22 debian systemd[1]: Started LSB: DHCP server.
root@debian:/home/aymenker#
```

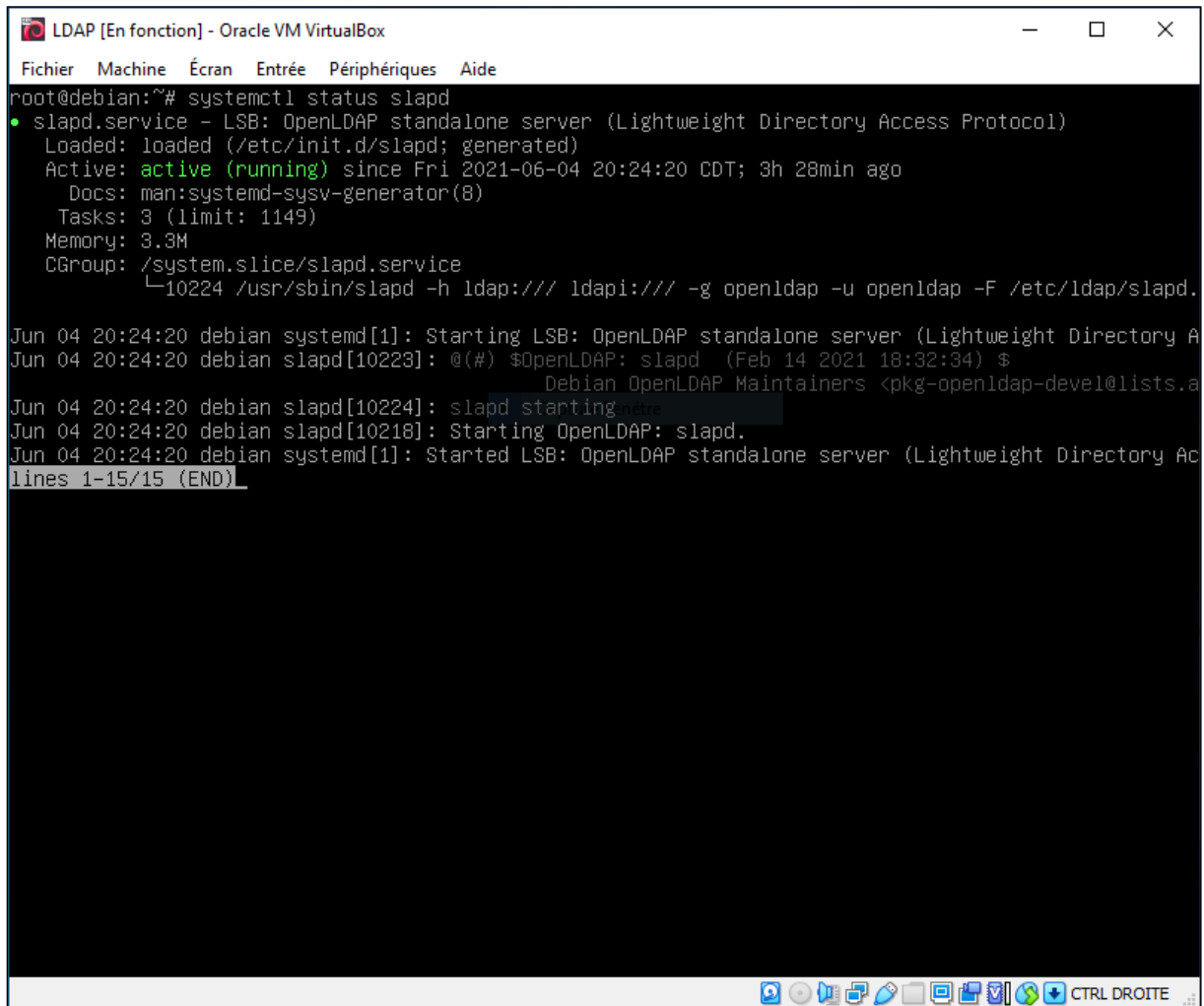
Figure 15 : Configuration de Serveur DHCP.

4.2.2.4. Serveur LDAP :

Les annuaires LDAP (Lightweight Directory Access Protocol) se situent au cœur des fonctions de communication et de collaboration de l'entreprise à travers son Intranet car ils en simplifient la gestion et l'administration. Nous avons installé l'open source OpenLdap utilisons le commande : « `apt-get install slapd ldap-utils` ». (slapd : serveur OpenLdap) (ldap-utils : outils pour interagir avec, interroger et modifier les entrées dans les serveurs LDAP locaux ou distants).

Le serveur LDAP est configuré et fonctionne parfaitement comme la montre la figure :

La commande « systemctl status slapd »



```
LDAP [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
root@debian:~# systemctl status slapd
• slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Active: active (running) since Fri 2021-06-04 20:24:20 CDT; 3h 28min ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 3 (limit: 1149)
   Memory: 3.3M
    CGroup: /system.slice/slapd.service
            └─10224 /usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap -F /etc/ldap/slapd.

Jun 04 20:24:20 debian systemd[1]: Starting LSB: OpenLDAP standalone server (Lightweight Directory A
Jun 04 20:24:20 debian slapd[10223]: @(#) $OpenLDAP: slapd (Feb 14 2021 18:32:34) $
                                Debian OpenLDAP Maintainers <pkg-openldap-devel@lists.a
Jun 04 20:24:20 debian slapd[10224]: slapd starting
Jun 04 20:24:20 debian slapd[10218]: Starting OpenLDAP: slapd.
Jun 04 20:24:20 debian systemd[1]: Started LSB: OpenLDAP standalone server (Lightweight Directory Ac
lines 1-15/15 (END)
```

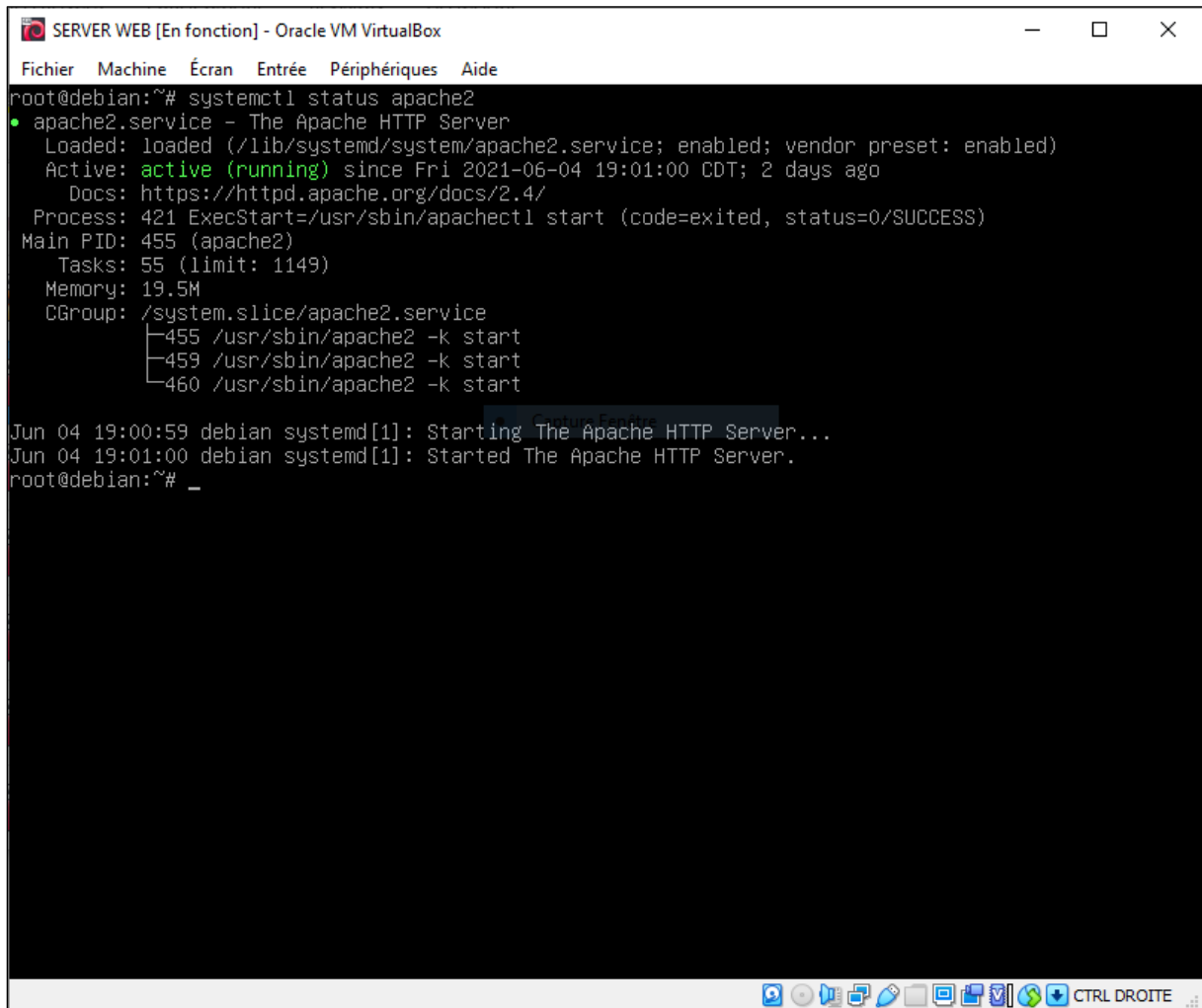
Figure 16: Configuration de serveur LDAP.

4.2.2.5. Serveur Web :

Un serveur HTTP permet à un site web de communiquer avec un navigateur en utilisant le protocole HTTP(S) et ses extensions (WebDAV, etc.). Apache est probablement le serveur HTTP le plus populaire. C'est donc lui qui met à disposition la plupart des sites Web. Pour installer le serveur apache2 utilise la commande : « apt-get install apache2 »

Le serveur Web est configuré et fonctionne parfaitement comme la montre la figure :

La commande « systemctl status apache2 »



```
SERVER WEB [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
root@debian:~# systemctl status apache2
• apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2021-06-04 19:01:00 CDT; 2 days ago
  Docs: https://httpd.apache.org/docs/2.4/
  Process: 421 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 455 (apache2)
  Tasks: 55 (limit: 1149)
  Memory: 19.5M
  CGroup: /system.slice/apache2.service
          └─455 /usr/sbin/apache2 -k start
            └─459 /usr/sbin/apache2 -k start
              └─460 /usr/sbin/apache2 -k start

Jun 04 19:00:59 debian systemd[1]: Starting The Apache HTTP Server...
Jun 04 19:01:00 debian systemd[1]: Started The Apache HTTP Server.
root@debian:~# _
```

Figure 17: Configuration de Serveur WEB.

4.3. Sécurité de réseau :

Maintenant nous discutons la partie la plus importante de notre projet, les techniques et méthodes utilisées pour sécuriser notre réseau, nous avons utilisé authentification, sécurité sur les ponts, DHCP snooping, dynamic ARP inspection, liste de contrôle d'accès, SSH, VPN, protocoles de sécurité sans fil. Avec toutes ces fonctionnalités de sécurité sera inutile si la sécurité physique n'a pas été correctement mise en œuvre.

4.3.1. Authentification :

D'abord, nous ne pouvons laisser aucun personne soit un patient ou un employé de l'hôpital de brancher un câble aux équipements réseaux et apporter des modifications à la configuration ou renifler nos précieuses données, nous avons donc mis l'authentification sur chaque équipement Nom d'utilisateur and mot passe , et nous avons attribué des mots de passe différents pour le même Nom d'utilisateur , parce que si quelqu'un était assez intelligent et chanceux pour cracker notre mot de passe, il n'aura pas accès à d'autres équipements, et pour y ajouter une couche de sécurité, nous avons attribué des niveaux de privilège et nous définissons un enable secret pour accéder au mode privilégié du CLI. Nous avons désactivé la récupération du mot de passe du commutateur. Et on règle l'heure de l'équipement de réseau donc quand nous garderons des journaux, nous aurons l'heure exacte.

Ce tableau contient les (nom utilisateur n, mot de passe, enable secret) des équipement réseau :

Tableau 03: Tableau des (nom utilisateur n, mot de passe, enable secret).

Equipement	Nom utilisateur	Mot de passe	Enable secret
Distribution switch 1	Aymen	chifa22\$	aymen99;
Distribution switch 2	Aymen	chifa23\$	aymen99;
Switch1	Aymen	chifa16\$	aymen99;
Switch2	Aymen	chifa17\$	aymen99;
Switch3	Aymen	chifa18\$	aymen99;
Switch4	Aymen	chifa20\$	aymen99;
Switch5	Aymen	chifa21\$	aymen99;
DMZ switch	Aymen	chifa19\$	aymen99;

4.3.2. Sécurité sur les ponts :

Nous avons utilisé sécurité sur les ponts collant « port security sticky » pour contrôler les adresses mac autorisées des équipements connectés et pour éviter les attaques inondation d'adresse mac « mac-address flooding », les adresse mac sont apprises dynamiquement à

partir des appareils connectés au port de commutation, nous avons limité le nombre des adresses mac apprises sur une interface à une et fermera le port si non autorisé adresse mac « violation » essayez de l'utiliser.

4.3.3. DHCP snooping :

Nous avons configuré dhcp-snooping pour exclure les serveurs DHCP malveillants et supprimer le trafic DHCP malveillant ou mal formé en faisant confiance uniquement à notre serveur dhcp (192.168.2.115), les Cyberattaques évitées grâce au DHCP Snooping est « dhcp spoofing », « dhcp stravation ».

4.3.4. Inspection dynamique de l'ARP:

Inspection dynamique de ARP « Dynamic arp inspection » est utilisé pour garantir que seules les demandes et réponses ARP valides sont relayées, DAI prévenir notre réseau de Attaques d'empoisonnement ARP « ARP poisoning attacks », en interceptant toutes les demandes et réponses ARP, Chacun de ces paquets interceptés est vérifié pour des liaisons adresse MAC à adresse IP valides avant la mise à jour du cache ARP local ou le paquet est transmis à la destination appropriée. Les paquets ARP non valides sont supprimés.

4.3.5. Liste de contrôle d'accès :

Nous avons utilisé un pare-feu configuré pour bloquer tout le trafic destiné au serveur NAS et n'acceptez que ce qui figure sur la liste blanche (le principe de moindre privilège), qui gardera notre serveur NAS hors des mains non autorisées, ainsi les données des patients avec qui ils nous ont fait confiance seront en sécurité, et le système sera toujours opérationnel.

4.3.6. SSH :

Les données de l'hôpital sont les plus importantes, nous nous sommes assurés que les personnes non autorisées ne : lire les données qui circulent sur notre réseau grâce à SSH qui partage et envoie les informations sous forme cryptée donc si quelqu'un intercepte les données qui circulent, il ne pourra pas les lire.

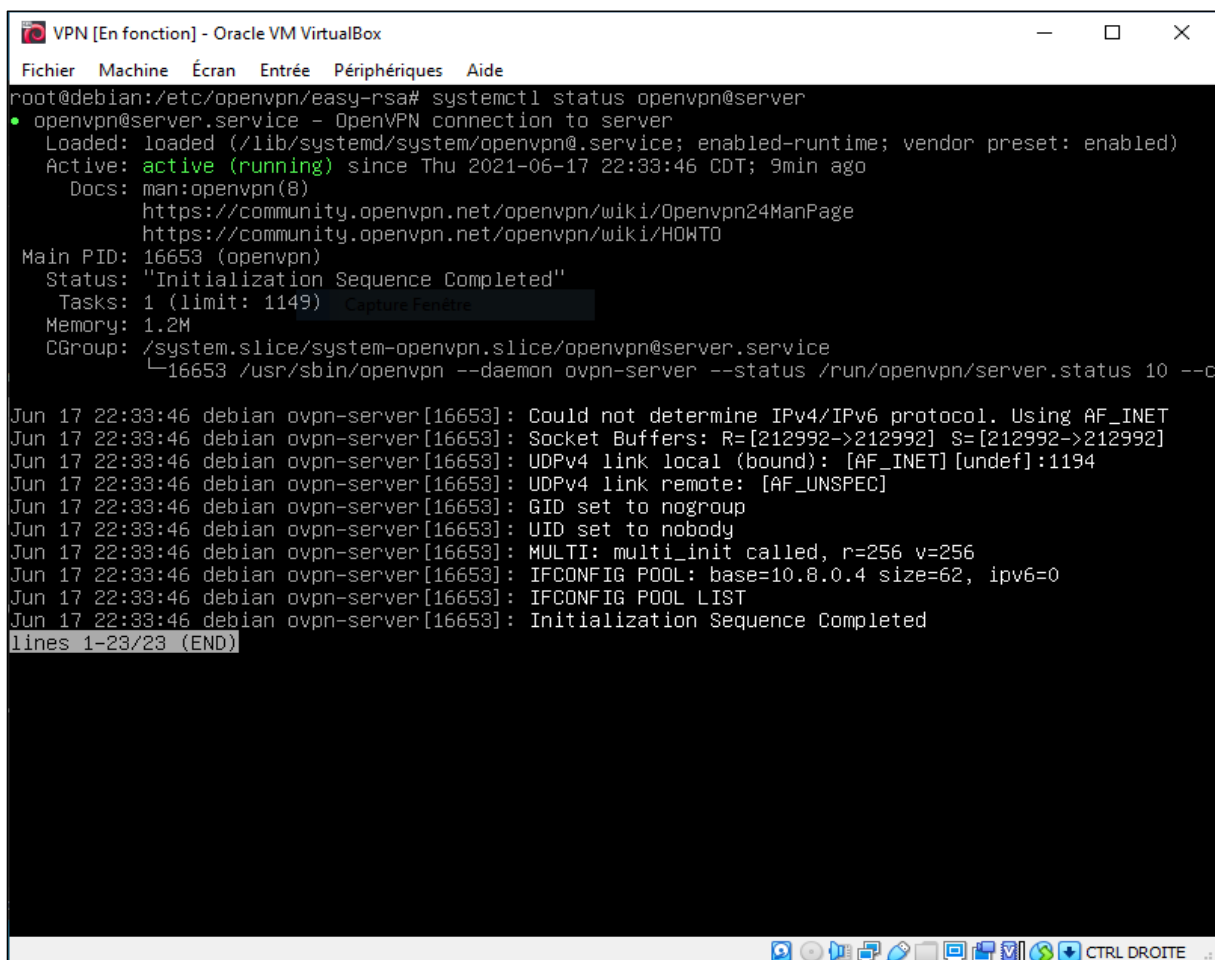
4.3.6. VPN :

Un VPN est un réseau privé virtuel Il offre la possibilité de se connecter en toute sécurité d'un ordinateur à un autre, ou d'un réseau à un autre réseau en passant par internet

réseau lui par défaut non-sécurisé. Un système très utile si vous souhaitez protéger au maximum vos données personnelles. Nous avons installé le serveur Openvpn pour crypte les données que vous transmettez d'un ordinateur à un autre, ce sera Impossible pour quelqu'un qui n'est pas sur votre réseau VPN de les lire, et si un employé de l'hôpital voulez accéder au réseau local de notre hôpital à travers une connexion sécurisée, et Openvpn Fournit un réseau privé virtuel de couche 3 utilisant le protocole OpenVPN. Le protocole OpenVPN utilise SSL/TLS avec des certificats client et serveur pour effectuer l'échange de clés et l'authentification mutuelle. OpenVPN est compatible avec les pare-feu et les proxys Web car le trafic crypté est tunnelé via UDP ou TCP. Et nous avons également utilisé ipsec vpn pour créer un tunnel point à point.

Le serveur VPN est configuré et fonctionne parfaitement comme la montre la figure :

La commande « systemctl status openvpn »



```
root@debian:/etc/openvpn/easy-rsa# systemctl status openvpn@server
• openvpn@server.service - OpenVPN connection to server
   Loaded: loaded (/lib/systemd/system/openvpn@.service; enabled-runtime; vendor preset: enabled)
   Active: active (running) since Thu 2021-06-17 22:33:46 CDT; 9min ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 16653 (openvpn)
   Status: "Initialization Sequence Completed"
     Tasks: 1 (limit: 1149)
    Memory: 1.2M
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─16653 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/server.status 10 --c

Jun 17 22:33:46 debian ovpn-server[16653]: Could not determine IPv4/IPv6 protocol. Using AF_INET
Jun 17 22:33:46 debian ovpn-server[16653]: Socket Buffers: R=[212992->212992] S=[212992->212992]
Jun 17 22:33:46 debian ovpn-server[16653]: UDPv4 link local (bound): [AF_INET][undef]:1194
Jun 17 22:33:46 debian ovpn-server[16653]: UDPv4 link remote: [AF_UNSPEC]
Jun 17 22:33:46 debian ovpn-server[16653]: GID set to nogroup
Jun 17 22:33:46 debian ovpn-server[16653]: UID set to nobody
Jun 17 22:33:46 debian ovpn-server[16653]: MULTI: multi_init called, r=256 v=256
Jun 17 22:33:46 debian ovpn-server[16653]: IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
Jun 17 22:33:46 debian ovpn-server[16653]: IFCONFIG POOL LIST
Jun 17 22:33:46 debian ovpn-server[16653]: Initialization Sequence Completed
lines 1-23/23 (END)
```

Figure 18 : VPN actif.

4.3.7. Protocoles de sécurité sans fil :

Le réseau sans fil permet d'utiliser un appareil mobile ou une tablette de n'importe où dans l'hôpital, Malheureusement, sans la sécurité appropriée, les réseaux sans fil peuvent être vulnérable aux attaques de pirates qui veulent voler les données de l'hôpital donc nous avons utilisé nous avons donc utilisé le protocole WPA2 entreprise et nous séparons le réseau sans fil des utilisateurs internes et invités, nous avons limité la force du signal wifi, et utilisé Rogue Access Point Détection.

Chapitre 02 :

Réalisation et Choix

Technique

1. Introduction :

L'étape de la réalisation est parmi les étapes les plus importantes dans la mise en œuvre de projet, ainsi que pour l'utilisateur simple qui comprend réellement le fonctionnement de cette projet et aussi elle est complémentaire de la phase conception qui a une relation avec elle. Après avoir terminé la phase de conception, dans une première partie, nous allons faire le choix du matérielles et logicielles qu'on a préféré pour l'implémentation et la réalisation de l'architecture réseau sécurisée.

2. L'implémentation de la passerelle sécurisée :

Comme nous avons parlé plus tôt dans le chapitre de la conception d'architecture ; on a met un ensemble de serveurs et deux pare- feu dans la DMZ qui doivent être configuré par des logiciels convenablement choisis.

Ces logiciels sont :

- Le logiciel bind9 pour le serveur DNS.
- Le logiciel SQUID pour le serveur Proxy.
- Le logiciel IPTABLES pour les pare-feu qui le laisse filtrer le trafic au niveau transport, on leur ajoute les logiciels SNORT (IDS) et Fail2ban(IPS) pour qui 'ils filtrent jusqu'au niveau application.

Pour réussir cela on a utilisé oracle VM virtualBox et système d'exploitation debian.

Les définitions et les caractères de ces logiciels pour les quels on les a choisi sont ci-dessous :

2.1. BIND:

2.1.1. Définition :

BIND (Berkeley Internet Name Domain) est une collection de logiciels d'outils comprenant le logiciel de serveur DNS (Domain Name System) le plus utilisé au monde. Cette implémentation complète du service et des outils DNS vise à être 100 % conforme aux normes et est ; destiné à servir d'architecture de référence pour les logiciels DNS. Pour les réseaux petits ou simples, BIND en lui-même est bien adapté pour fournir toutes les fonctions

de service liées au DNS. Avec BIND, vous pouvez exécuter des serveurs DNS de mise en cache, des serveurs faisant autorité ou même les deux ensembles.

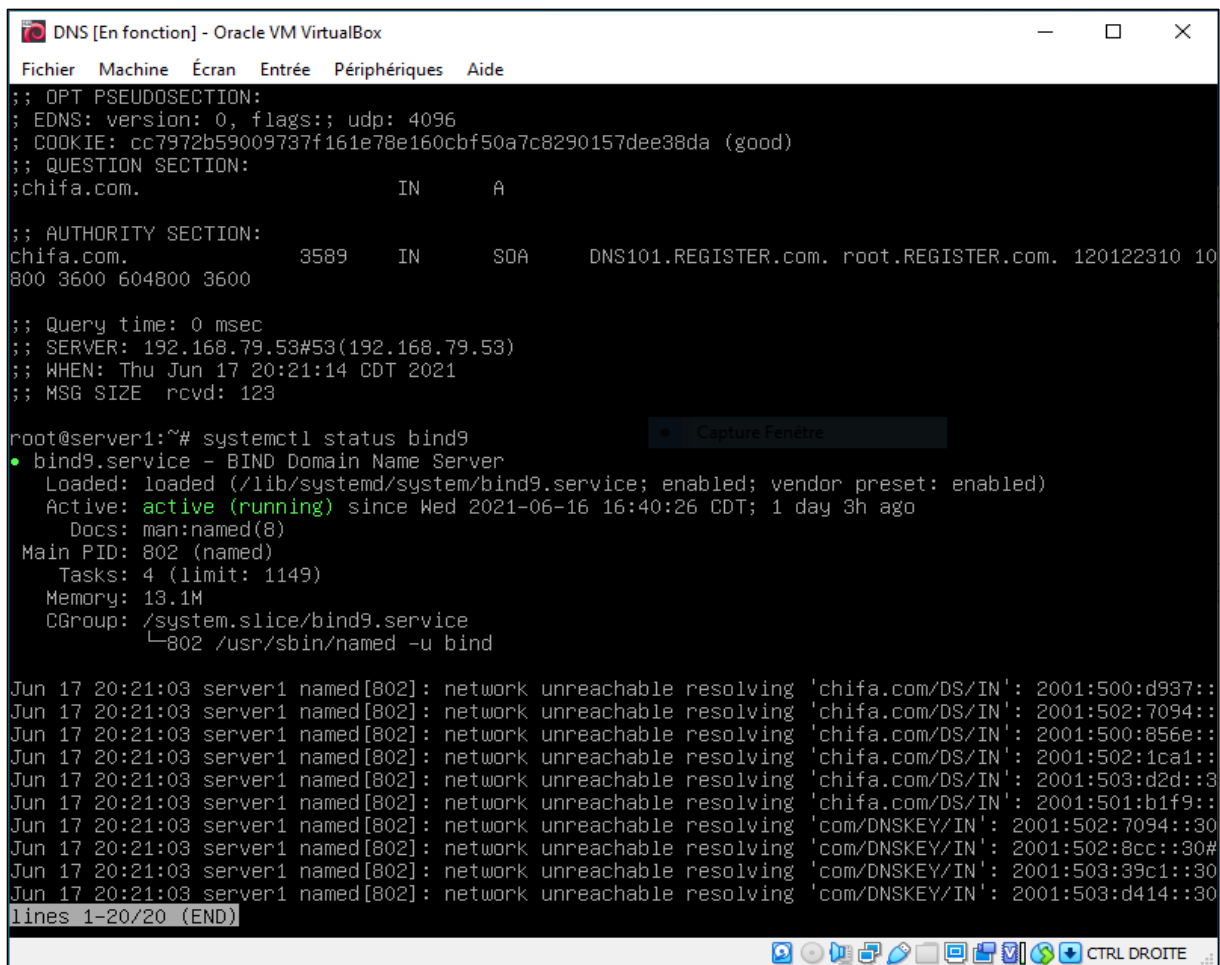
2.1.2. Comment installer BIND :

Installez bind9 avec apt.

```
sudo apt-get install -y bind9
```

2.1.3. Caractéristiques :

- BIND est personnalisable. Si vous pouvez coder en Perl, Python, BASH ou Powershell, vous pouvez créer n'importe quel outil personnalisé dont vous avez besoin pour vous-même et votre réseau.
- BIND est gratuit à l'avance. Contrairement aux solutions DNS commerciales (comme BlueCat, Microsoft ou Infoblox), BIND ne coûte rien pour commencer à utiliser. La plupart des distributions Linux/UNIX ont un package BIND préconstruit dans leurs référentiels.
- BIND a une grande communauté de soutien. La base de connaissances et la communauté pour l'utilisation et le dépannage de BIND sont vastes et mondiales.
- BIND est un outil incroyable pour commencer. La plupart des implémentations commerciales de DNS que vous rencontrerez au cours de votre carrière sont basées sur BIND. Avoir les connaissances de base nécessaires pour configurer un serveur BIND sera utile.



```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 4096
; COOKIE: cc7972b59009737f161e78e160cbf50a7c8290157dee38da (good)
;; QUESTION SECTION:
;chifa.com.                IN      A

;; AUTHORITY SECTION:
chifa.com.                 3589    IN      SOA      DNS101.REGISTER.com. root.REGISTER.com. 120122310 10
800 3600 604800 3600

;; Query time: 0 msec
;; SERVER: 192.168.79.53#53(192.168.79.53)
;; WHEN: Thu Jun 17 20:21:14 CDT 2021
;; MSG SIZE rcvd: 123

root@server1:~# systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2021-06-16 16:40:26 CDT; 1 day 3h ago
     Docs: man:named(8)
   Main PID: 802 (named)
      Tasks: 4 (limit: 1149)
     Memory: 13.1M
    CGroup: /system.slice/bind9.service
            └─802 /usr/sbin/named -u bind

Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'chifa.com/DS/IN': 2001:500:d937::
Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'chifa.com/DS/IN': 2001:502:7094::
Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'chifa.com/DS/IN': 2001:502:856e::
Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'chifa.com/DS/IN': 2001:502:1ca1::
Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'chifa.com/DS/IN': 2001:503:d2d::3
Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'chifa.com/DS/IN': 2001:501:b1f9::
Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'com/DNSKEY/IN': 2001:502:7094::30
Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'com/DNSKEY/IN': 2001:502:8cc::30#
Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'com/DNSKEY/IN': 2001:503:39c1::30
Jun 17 20:21:03 server1 named[802]: network unreachable resolving 'com/DNSKEY/IN': 2001:503:d414::30
lines 1-20/20 (END)
```

Figure 19 : DNS actif.

2.2. SQUID :

2.2.1. Définition :

SQUID est un serveur proxy basé sur Unix qui met en cache le contenu Internet plus près d'un demandeur que son point d'origine. SQUID prend en charge la mise en cache de nombreux types d'objets Web, y compris ceux accessibles via HTTP et FTP. La mise en cache des pages Web, des fichiers multimédias et d'autres contenus fréquemment demandés accélère le temps de réponse et réduit l'encombrement de la bande passante [14].

2.2.2. Processus étape par étape pour configurer un serveur proxy à l'aide de SQUID Proxy :

Un serveur proxy a de nombreux cas d'utilisation cela peut aller de l'accès Internet personnel à la restriction des systèmes/serveurs d'organisation pour accéder au monde externe ou à la limitation de l'accès Internet externe pour un ensemble de serveurs sur le cloud.

La meilleure façon de configurer un serveur proxy est d'utiliser le proxy Squid. C'est un serveur proxy largement utilisé.

Suivez les étapes ci-dessous pour un serveur proxy fonctionnel :

Étape 1 : Connectez-vous au serveur et mettez à jour la liste des packages.

```
sudo apt update -y
```

Étape 2 : Installez le serveur proxy Squid.

```
sudo apt -y install squid
```

Étape 3 : Démarrez et activez le service squid pour qu'il démarre au démarrage du système.

```
sudo systemctl start squid
```

```
sudo systemctl enable squid
```

Étape 4 : Vérifiez l'état du service de squid. Vous devriez voir le statut "actif".

```
sudo systemctl status squid
```

2.2.3. SQUID Proxy Port :

Par défaut, squid s'exécute sur le port 3128

Vous pouvez le vérifier en utilisant la commande suivante :

```
netstat -tnlp
```

2.2.4. Caractéristiques:[39] [15]

- Mandataire et cache des protocoles HTTP, HTTPS, Gopher, FTP.
- Hiérarchisation du cache.
- ICP, HTCP, CARP, Cache Digests.
- Processus de cache transparent.
- WCCP (SQUID v2.3 et supérieur).

- Contrôle des accès étendu.
- SNMP.
- Cache les requêtes DNS.
- Mandataire inverse (reverse proxy).
- logiciel libre.

```

root@debian:~# systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-06-04 19:03:48 CDT; 2 days ago
     Docs: man:squid(8)
   Process: 392 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
   Process: 464 ExecStart=/usr/sbin/squid -sYC (code=exited, status=0/SUCCESS)
  Main PID: 465 (squid)
    Tasks: 4 (limit: 1149)
   Memory: 32.5M
   CGroup: /system.slice/squid.service
           └─465 /usr/sbin/squid -sYC
             └─467 (squid-1) --kid squid-1 -sYC
               └─469 (logfile-daemon) /var/log/squid/access.log
                 └─470 (pinger)

Jun 06 18:12:21 debian squid[467]: NETDB state saved; 0 entries, 0 msec
Jun 06 18:52:28 debian squid[467]: Logfile: opening log stdio:/var/spool/squid/netdb.state
Jun 06 18:52:28 debian squid[467]: Logfile: closing log stdio:/var/spool/squid/netdb.state
Jun 06 18:52:28 debian squid[467]: NETDB state saved; 0 entries, 0 msec
Jun 06 19:49:23 debian squid[467]: Logfile: opening log stdio:/var/spool/squid/netdb.state
Jun 06 19:49:23 debian squid[467]: Logfile: closing log stdio:/var/spool/squid/netdb.state
Jun 06 19:49:23 debian squid[467]: NETDB state saved; 0 entries, 0 msec
Jun 06 20:57:12 debian squid[467]: Logfile: opening log stdio:/var/spool/squid/netdb.state
Jun 06 20:57:12 debian squid[467]: Logfile: closing log stdio:/var/spool/squid/netdb.state
Jun 06 20:57:12 debian squid[467]: NETDB state saved; 0 entries, 8 msec
root@debian:~# _

```

Figure 20 : Proxy actif.

2.3. IPTABLES :

2.3.1. Définition :

En termes simples, IPTABLES est un programme de pare-feu pour Linux. Il surveillera le trafic depuis et vers votre serveur à l'aide de tables. Ces tables contiennent des ensembles de règles, appelées chaînes, qui filtreront les paquets de données entrants et sortants.

Lorsqu'un paquet correspond à une règle, une cible lui est attribuée, qui peut être une autre chaîne ou l'une de ces valeurs spéciales :

ACCEPTER – permettra au paquet de passer.

DROP – ne laissera pas passer le paquet.

RETURN – empêche le paquet de traverser une chaîne et lui dit de revenir à la chaîne précédente.

2.3.2. Comment installer et utiliser le pare-feu Linux IPTABLES :

Nous allons diviser ce tutoriel IPTABLES en trois étapes :

Étape 1 - Installation d'IPTABLES

Étape 2 - Définir les règles de la chaîne

Activation du trafic sur Localhost.

Activation des connexions sur les ports HTTP, SSH et SSL.

Filtrage des paquets en fonction de la source.

Suppression de tout autre trafic.

Supprimer des règles:

Pour supprimer toutes les règles ou juste une règle spécifique.

Étape 3 - Changements persistants

IPTABLES est un puissant programme de pare-feu que vous pouvez utiliser pour sécuriser votre serveur Linux ou VPS. Ce qui est génial, c'est que vous pouvez définir différentes règles en fonction de vos préférences [16].

2.3.3. Caractéristiques: [17]

- IPTABLES est et permet le niveau d'accès le plus proche et le plus bas au pare-feu du noyau Linux qu'un utilisateur peut obtenir (vers). Pour info, le pare-feu Linux s'appelle IPTABLES, en premier lieu. C'est donc le pare-feu logiciel le plus robuste et le plus fiable que l'on puisse avoir.
- C'est un outil de contrôleur très polyvalent pour la ligne de commande.

- Si vous ne pouvez pas modifier un aspect du pare-feu Linux avec, alors cela n'existe pas, Vous le pouvez.
- Le concept de base du pare-feu IPTABLES et de l'outil est assez simple et agréable.
- Il existe une documentation complète (et disponible gratuitement) sur IPTABLES que vous pouvez étudier, directement à partir de la source.

```

Firewall1 [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
8  ACCEPT  all  --  192.168.79.80  anywhere
9  ACCEPT  tcp  --  anywhere  anywhere  tcp dpt:domain
10 DROP  all  --  anywhere  anywhere
root@debian:/home/aymenker# iptables -A FORWARD -j DROP
root@debian:/home/aymenker# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT all -- anywhere 192.168.79.85
2 ACCEPT tcp -- anywhere anywhere tcp dpt:smtp
3 ACCEPT icmp -- anywhere anywhere
4 ACCEPT tcp -- anywhere anywhere tcp dpt:ssh
5 ACCEPT tcp -- anywhere anywhere tcp dpt:https
6 ACCEPT tcp -- anywhere anywhere tcp dpt:http
7 ACCEPT udp -- anywhere anywhere udp dpt:domain
8 ACCEPT tcp -- anywhere anywhere tcp dpt:domain
9 DROP all -- anywhere anywhere

Chain FORWARD (policy ACCEPT)
num target prot opt source destination
1 ACCEPT udp -- anywhere anywhere udp dpt:openvpn
2 ACCEPT all -- 192.168.46.66 anywhere
3 ACCEPT icmp -- anywhere anywhere
4 DROP all -- anywhere anywhere

Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT tcp -- anywhere anywhere tcp dpt:smtp
2 ACCEPT tcp -- anywhere anywhere tcp dpt:https
3 ACCEPT tcp -- anywhere anywhere tcp dpt:http
4 ACCEPT tcp -- anywhere anywhere tcp dpt:ssh
5 ACCEPT udp -- anywhere anywhere udp dpt:domain
6 ACCEPT icmp -- anywhere anywhere
7 ACCEPT all -- 192.168.79.53 anywhere
8 ACCEPT all -- 192.168.79.80 anywhere
9 ACCEPT tcp -- anywhere anywhere tcp dpt:domain
10 DROP all -- anywhere anywhere
root@debian:/home/aymenker#
  
```

Figure 21 : Pare-feu 01 actif.

```

root@debian:/home/aymenker# /usr/sbin/iptables -L --line-
Chain INPUT (policy ACCEPT)
num target      prot opt source                destination            tcp dpt:domain
1  ACCEPT        tcp  --  anywhere               anywhere               udp dpt:domain
2  ACCEPT        udp  --  anywhere               anywhere
3  ACCEPT        icmp --  anywhere               anywhere
4  ACCEPT        tcp  --  anywhere               anywhere               tcp dpt:ssh
5  ACCEPT        tcp  --  anywhere               anywhere               tcp dpt:http
6  ACCEPT        tcp  --  anywhere               anywhere               tcp dpt:https
7  ACCEPT        tcp  --  anywhere               anywhere               tcp dpt:smtp
8  DROP          all  --  anywhere               anywhere

Chain FORWARD (policy ACCEPT)
num target      prot opt source                destination            udp dpt:openvpn
1  ACCEPT        all  --  192.168.46.66          anywhere
2  ACCEPT        udp  --  anywhere               anywhere
3  ACCEPT        icmp --  192.168.46.3           anywhere
4  ACCEPT        icmp --  192.168.46.80          anywhere
5  DROP          icmp --  192.168.46.30          anywhere
6  DROP          all  --  anywhere               anywhere

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination            udp dpt:domain
1  ACCEPT        udp  --  anywhere               anywhere               tcp dpt:domain
2  ACCEPT        tcp  --  anywhere               anywhere
3  ACCEPT        icmp --  anywhere               anywhere
4  DROP          all  --  192.168.46.30          anywhere
5  ACCEPT        all  --  192.168.46.80          anywhere
6  ACCEPT        all  --  192.168.46.3           anywhere
7  ACCEPT        tcp  --  anywhere               anywhere               tcp dpt:https
8  ACCEPT        tcp  --  anywhere               anywhere               tcp dpt:http
9  ACCEPT        tcp  --  anywhere               anywhere               tcp dpt:ssh
10 ACCEPT        tcp  --  anywhere               anywhere               tcp dpt:smtp
11 DROP          all  --  anywhere               anywhere
root@debian:/home/aymenker#

```

Figure 22 : Pare-feu 02 actif.

2.4. SNORT :

2.4.1. Définition :

SNORT est un système de détection d'intrusion réseau (IDS) et un système de prévention d'intrusion (IPS) gratuits et open source. Utilisé pour la détection des tentatives illégales et malveillantes dans le réseau. SNORT est maintenant développé par Cisco, En 2009, SNORT est entré dans l'Open Source Hall of Fame d'InfoWorld comme l'un des "plus grands logiciels open source de tous les temps [18].

SNORT peut être utilisé comme système de prévention des intrusions avec le pare-feu IPTABLES/pf.

2.4.2. Comment installer SNORT :

- Dans notre projet on a utilisé SNORT avec le pare-feu IPTABLES.

- Préparation de votre serveur.
- Installer SNORT à partir de la source.
- Configurer SNORT pour qu'il s'exécute en mode NIDS.
- Configuration du nom d'utilisateur et de la structure des dossiers.
- Configuration du réseau et des ensembles de règles.
- Validation des paramètres.
- Tester la configuration.
- Exécution de SNORT en arrière-plan.

2.4.3. Caractéristiques :

Les avantages de SNORT sont nombreux :

- A la capacité d'effectuer une analyse du trafic en temps réel et une journalisation des paquets sur les réseaux IP (Internet Protocol).
- Il peut effectuer une analyse de protocole.
- Une recherche/correspondance de contenu.
- Gratuits et open source.
- Peut être utilisé pour détecter une variété d'attaques et de sondes, telles que le débordement de la mémoire tampon, les analyses de ports furtifs, les attaques CGI, les sondes SMB, les attaques d'URL sémantiques , les tentatives d'empreintes digitales du système d'exploitation , les sondes de blocs de messages de serveur et bien plus encore.

2.5. Fail2ban :

2.5.1. Définition:

Fail2ban est un logiciel de prévention contre les intrusions qui se charge d'analyser les logs de divers services installés sur la machine, pour bannir automatiquement un hôte via IPTABLES pour une durée déterminée, en cas d'échec après X tentatives.

C'est un élément essentiel pour sécuriser son système, et éviter des intrusions via brute-force.

2.5.2. Comment Installer fail2ban :

Pour installer fail2ban, installer le paquet fail2ban.

Debian :

- Assurez-vous que votre système est à jour :

```
apt-get update && apt-get upgrade -y
```

- Installez Fail2ban :

```
apt-get install fail2ban
```

Le service démarre automatiquement.

- Facultatif) Si vous souhaitez une assistance par e-mail, installez Sendmail :

```
apt-get install sendmail-bin sendmail
```

2.5.3. Caractéristiques : [19]

- Fail2ban bloque les adresses IP appartenant à des hôtes qui tentent de casser la sécurité du système, pendant une période configurable (mise en quarantaine).
- Il lit les logs de divers services (SSH, Apache, FTP...) à la recherche d'erreurs d'authentification répétées et ajoute une règle IPTABLES pour bannir l'adresse IP de la source.
- Il permet de ralentir les attaques par force brute, ainsi que les attaques par déni de service.
- Fail2ban est aussi capable de bloquer les attaques distribuées.
- Déploie un service de surveillance fail2ban et de prévention des dénis de service (DoS), avec une configuration exposée pour aider à prévenir les attaques SSH DoS.
- Le service fail2ban analyse les fichiers journaux et bannit les adresses IP qui ont trop d'échecs de mot de passe. Le nombre d'échecs et le temps d'interdiction sont configurables.

2.6. Nginx :

2.6.1. Définition :

Un proxy inverse Nginx est un service proxy intermédiaire qui prend une demande client, la transmet à un ou plusieurs serveurs, puis renvoie la réponse du serveur au client. ... En utilisant un proxy inverse Nginx, toutes les applications peuvent bénéficier de ces fonctionnalités.

Est un logiciel gratuit, open-source et performant, C'est un excellent outil pour un environnement à plusieurs serveurs, créant une expérience client unifiée. Il peut également être utile pour des tâches plus simples comme garder un seul serveur anonyme.

2.6.2. Comment Installer nginx :

```
apt-get install nginx
```

```
apt-get install php5-fpm
```

```
systemctl enable nginx.service
```

2.6.3. Caractéristiques :

La configuration d'un proxy inverse Nginx HTTPS présente des avantages importants :

- Équilibrage de charge : un proxy inverse Nginx peut effectuer un équilibrage de charge qui permet de répartir les demandes des clients de manière uniforme sur les serveurs principaux. Cela améliore également la redondance car si un serveur tombe en panne, le proxy inverse redirigera simplement les demandes vers un serveur différent en fonction de la politique de routage.
- Sécurité accrue : un proxy inverse Nginx agit également comme une ligne de défense pour vos serveurs principaux. La configuration d'un proxy inverse garantit que l'identité de vos serveurs principaux reste inconnue.
- Meilleures performances : Nginx est connu pour ses meilleures performances dans la livraison de fichiers de contenu statique et l'analyse des URL
- Journalisation et audit faciles : comme il n'y a qu'un seul point d'accès lorsqu'un proxy inverse Nginx est implémenté, cela rend la journalisation et l'audit beaucoup plus simples.
- Connexion cryptée En cryptant la connexion entre le client et le proxy inverse Nginx avec TLS, les utilisateurs bénéficient d'une connexion HTTPS cryptée et sécurisée, protégeant leurs données [20].


```
REVERSE PROXY [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
root@debian:~# systemctl status nginx
• nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-06-07 20:35:46 CDT; 24h ago
     Docs: man:nginx(8)
   Process: 999 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, sta
   Process: 1000 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SU
   Main PID: 1001 (nginx)
      Tasks: 2 (limit: 1149)
     Memory: 2.7M
    CGroup: /system.slice/nginx.service
            └─1001 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
               └─1002 nginx: worker process

Jun 07 20:35:46 debian systemd[1]: Starting A high performance web server and a reverse proxy server
Jun 07 20:35:46 debian systemd[1]: nginx.service: Failed to parse PID from file /run/nginx.pid: Inva
Jun 07 20:35:46 debian systemd[1]: Started A high performance web server and a reverse proxy server.
lines 1-16/16 (END)
```

Figure 23 : Reverse proxy actif.

3. Choix techniques et chiffage d la proposition :

Pour terminer ce travaille on doit choisir les marques du matériels utilisé avec des bonnes caractéristiques et des prix raisonnables afin d’arriver à un devis acceptable

Tout cela est cité ci-dessous :

- **Switch :** **CISCO Catalyst 2960-24TC-S Switch**
Switch CISCO c2960-24-tc-s 24 ports 10/100+2g sfp
Marque : CISCO

Caractéristiques :

- Broadcast Storm Control, DHCP support, DiffServ support, Dynamic Trunking Protocol (DTP) support, IGMP snooping, Link Aggregation Control Protocol (LACP), MAC Address Notification, Multicast Storm Control, Multiple Spanning Tree

Protocol (MSTP) support, Port Aggregation Protocol (PAgP) support, Port Security, Quality of Service (QoS), Rapid Spanning Tree Protocol (RSTP) support, Syslog support, Unicast Storm Control, VLAN support, auto-negotiation, auto-sensing per device, auto-uplink (auto MDI/MDI-X), layer 2 switching

- Redundant Power System (RPS) connector

Prix : 67000 DA

- **Routeur : ROUTEUR CISCO isr 4321**

Référence : Cisco ISR 4321/k9

Marque : CISCO

Caractéristiques :

- Prise en charge VPN, prise en charge du réseau local (LAN) virtuel, prise en charge de Syslog, prise en charge d'IPv6, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), montage mural possible, assistance Access Control List (ACL), qualité de service (QDS), support RADIUS, NetFlow, IPFIX.
- Routeur CISCO serie 4000 Référence 4321 ISR , Les routeurs de services intégrés (ISR) de la gamme Cisco 4000 sont des routeurs modulaires offrant une connectivité LAN et WAN. Ils prennent en charge plusieurs modules d'interface, notamment les modules de service amélioré Cisco (SM-X) et les modules d'interface réseau de Cisco (NIM).

Prix : 188000 DA

- **Switch multilayer : Switch Catalyst WS-C3560G-24PS-E**

Cisco Catalyst switch 3560 24 ports 10/100/1000 T PoE + 4 SFP IPS Image

Marque : cisco

Caractéristiques :

- Cisco Catalyst 3560-24PS-S.
- Type de commutateur: Géré.
- Banc de commutateurs: L2+.

- Quantité de ports Ethernet RJ-45 de commutation de base: 28, 24, 28, Technologie de câblage Ethernet cuivre: 100Base-TX, 10Base-T.
- Standards réseau: IEEE 802.1D, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ad, IEEE 802.
- Répertoire MAC: 12000 entrées.
- Débit de transfert de données: 10/100 Mbps.
- Capacité de commutation: 32 Gbit/s.
- Protocoles de gestion: IGMP, RMON, SNMP, Telnet.
- Protocole de commutation: EIGRP, IPv6, DTP, PAgP, DHCP, HSRP, TCP, UDP Configuration fixe 1RU, commutateur multicouche.
- Services intelligents de classe entreprise fournis à la périphérie du réseau.
- Image logicielle multicouche améliorée (EMI) installée.
- Routage IP avancé.

Prix : 195000 DA

- **Point d'accès : Cisco Aironet 1832I-E AccessPoint**

Cisco Aironet 1832I-e Access Point. (AIR-AP1832I-E-K9C)

Marque: CISCO

Caractéristiques :

- Idéal pour les petites et moyennes entreprises, le point d'accès Cisco Aironet 1832I-e-k9c offre une connexion sans fil dual-band rapide et sûre. Disposant des derniers standards en matière de Wi-Fi (802.11ac Wave 2), ce point d'accès permet aux utilisateurs d'étendre la zone du sans-fil.
- Design fin et compact avec antennes internes, pour un faible encombrement.
- Technologie Wi-Fi N MIMO (3x3) avec vitesse maximale de 1000 Mbps (867 Mbps sur la 5 GHz et 300 Mbps sur 2.4 GHz)).

Prix : 75000 DA

Serveur NAS : SERVEUR NAS 6 BAIES SYNOLOGY DS1621+

Catégorie : Stockage externe

Caractéristiques :

- Emplacements disques : 6 baies
- Modes Raids : Synology Hybrid RAID,0,1,1+0 (10),5,6,JBOD
- Norme mécanique : SATA
- Type de RAID : RAID matériel

Prix: 220000 DA

Serveur Proxy: ASA 5500 UC Proxy 24 Session License

Référence: L-ASA-UC-24=

Marque : CISCO

Caractéristiques :

- License
- 24 sessions
- For ASA 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40

Prix : 265156,85 DA

Serveur : Supermicro SuperServer SYS-E300-9A w/ 2x SFP+, 2x 10GBase-T, 4x GbE LAN

Brand: Supermicro

Caractéristiques :

- Intel Atom C3858 12-Core Processeur.
- Prend en charge jusqu'à 256 Go de mémoire RDIMM ECC.
- Prend en charge jusqu'à 2 disques 2,5" et SSD M.2.
- Emplacement PCIe 3.0 x4 à profil bas.
- 2 ports 10GBase-T, 2 ports SFP+ et 4 ports LAN GbE.

Prix : 147101,15 DA

Pare-feu 01 : Fortinet Fortigate 60E-BDL

Le FortiGate 60E est une excellente solution de sécurité pour votre réseau. Avec son format compact et sans ventilateur, il sera parfait pour les moyennes entreprises en quête d'une sécurité optimale. Ce firewall vous protégera contre les cybermenaces avec un SD-WAN sûre et simple à déployer [21].

Marque : Fortinet

Caractéristiques :

- Pare-feu VPN jusqu'à 60 équipements, 7 ports 10/100/1000 Mbps + suite de sécurité FortiGuard UTM.
- 7 x Gigabit Ethernet - RJ45 Femelle.
- 3 x WAN - Gigabit Ethernet - RJ45.
- 1 x LAN ou DMZ - Gigabit - RJ45.

Prix : 129700,65 DA

Pare-feu 2 : ZyXEL USG 60W Pack UTM avec licences de service

Pare-feu VPN 40 tunnels 4 ports 10/100/1000 Mbps + 2 ports WAN Wi-Fi double radio + Licences (CF, AS, AV et IDP).

Marque : ZyXEL.

Caractéristiques : [22]

- Les passerelles de sécurité unifiée (USG) ZyXEL de dernière génération permettent d'effectuer des scans anti-virus et de bloquer des attaques sans ralentir la bande passante. Grâce à leur design tout-en-un avec un contrôleur Wi-Fi intégré, les nouveaux modèles réduisent les efforts de gestion.
- Pack UTM : filtrage de contenu (CF), anti-spam (AS), anti-virus (AV) et détection et prévention d'intrusion (IDP) d'une durée d'1 an
- 4 ports 10/100/1000 Mbps
- 2 ports WAN
- 2 ports USB
- Wi-Fi 802.11 a/b/g/n Double Radio 2.4 & 5 GHz
- Antenne : 3 dBi
- Unified Security Policy alliant les profils de pare-feu et UTM
- Contrôleur Wi-Fi intégré
- Détection et prévention d'intrusion (IDP)
- Filtrage de contenu pour une protection efficace

Prix : 111764,75 DA

Câble : Câble Cat. 6 FTP (500 mètres)

Câble Catégorie 6 FTP. Le touret de 500 mètres.

FTP : câble à paires torsadées avec blindage aluminium autour des paires.

Prix : 46980,70 DA.

Voici Le devis total du matériel utilisé :

Tableau 04 : devis du matériel.

Produit	Nombre	Prix
Switch	6	402 000 DA
Switch multilayer	2	390 000 DA
Routeur	1	188 000 DA
Point d'accès	5	375 000 DA
Serveur nas	2	440 000 DA
Serveur proxy	1	265 156,85 DA
Serveur	5	147 101,15 DA
Pare-feu 1	1	129 700,65 DA
Pare-feu 2	1	11 1764,75 DA
Cable	1	469 80,70 DA
		Devis total = 2495 704,1 DA

Le devis n'est pas vraiment exacte ; le chiffrage est approximative, Aussi on a juste citer le matériels nécessaire.

4. PSSI (Politique sécurité système information) :

4.1. Introduction :

La politique de sécurité du système d'information (PSSI) est un plan d'action visant à atteindre et maintenir en état de bon fonctionnement l'ensemble du Système d'information en définissant notamment les règles de sécurité informatique, le but de PSSI est définir et expliquer la vision stratégique de la DSI en termes de sécurité du SI. Elle informe l'ensemble des acteurs des enjeux, des choix face à la gestion des risques.

4.2. Objectif :

L'objectif de ce guide est de fournir un document au responsable de SSI Offre une vision stratégique de la gestion des risques globaux. Elle suscite la confiance dans le système d'information. Ce guide présente une stratégie et un ensemble de principes de sécurité et de références expliquer les mesures de sécurité de l'hôpital pour être toujours prêt à toute intrusion.

4.3. Principes Organisationnels :

4.3.1. Politique de sécurité et politiques à thèmes :

4.3.1.1. Politique de sauvegarde :

Faire des sauvegardes régulières et complètes des données est la seule bonne assurance contre une infection ou une attaque qui corromprait les données de production ou les rendrait inaccessibles. Les sauvegardes régulières consistent à faire une copie de toutes les données importantes sur un support (non) physique, qui est différent de celui sur lequel les données ont été générées. Expliquer pour les utilisateurs où les données critiques doivent être stockées. Définissez la fréquence des sauvegardes pour chaque type de données, le support sur lequel elles doivent être stockées et la durée de conservation de la sauvegarde [23] nous listons :

- Les informations sensibles et critiques doivent être sauvegardées selon une périodicité compatible avec leur importance pour les activités du l'hôpital.
- La sauvegarde de données peut également servir en cas d'erreur humaine afin de repartir d'une situation antérieure fiable.

4.3.1.2. Politique de protection contre les logiciels malveillants :

Un « programme malveillant » est un logiciel conçu par des pirates informatiques pour avoir accès à votre système d'information (virus, ransomware, fileless). Heureusement, il existe des moyens de bloquer ces logiciels malveillants avant leur propagation au sein de votre parc informatique Découvrez les bonnes pratiques à mettre en place [24] :

- Utilisez un bon antivirus pour protéger vos ordinateurs et serveurs contre les programmes malveillants.
- Utiliser une protection avancée contre les logiciels malveillants(AMP) pour empêcher les attaques de 0 jour.
- N'essayez pas de désinstaller ou de désactiver un logiciel antivirus. Tout message suggérant que la protection antivirus a été désactivée doit être examiné immédiatement.
- Télécharger uniquement des applications auprès des sites dignes de confiance.
- Les utilisateurs doivent être empêchés d'accéder à des sites Web malveillants connus soit par des logiciels de protection ou via une fonction de filtrage de contenu.
- Examinez les autorisations qui vous sont demandées par une application ou un logiciel.
- Les pièces jointes des e-mails doivent être analysées par un produit antivirus avant la livraison.
- N'ouvrez pas les pièces jointes suspectes et ne cliquez pas sur des liens dangereux.
- Ne connectez jamais de clés USB ou d'autres supports de stockage à votre ordinateur si vous ne savez pas d'où elles viennent.
- Mettre régulièrement à jour votre système d'exploitation, software, pour bénéficier des dernières mises à jour de sécurité du système.
- Former vos employés à acquérir les connaissances sur le domaine du cyber sécurité.

4.3.1.3. Politique de contrôle d'accès :

Le contrôle d'accès désigne les différentes solutions techniques qui permettent de sécuriser et gérer les accès physiques ou les accès logiques [25]. Les accès non autorisés aux systèmes et aux applications doivent être empêchés. Il est nécessaire de sécuriser les connexions et mettre si possible des procédures de contrôle. La gestion du contrôle d'accès passe par l'identification et l'authentification des utilisateurs pour un accès autorisé aux ressources réseau. De plus, il est important de cartographier, d'identifier les ressources qui peuvent être accéder par les utilisateurs sur le réseau. L'évolution possible du nombre d'utilisateurs est importante à prendre en compte :

- Seuls les médecins peuvent apporter des modifications aux données des patients.
- Les médecins n'ont pas le droit de d'effacer des diagnostics déjà établis.

- Seul l'administrateur réseau peut accéder à la pièce où se trouve l'équipement réseau.
- La création du droit d'accès est techniquement mise en œuvre par le responsable de la sécurité.

4.3.1.4. Adoption d'une échelle de besoins :

Une échelle de besoins selon différents critères de sécurité (disponibilité, intégrité, confidentialité...) permettra de faciliter la classification objective des éléments essentiels de l'hôpital. Notre situation privilégie la confidentialité pour cela nous avons plusieurs politiques pour protéger les données de nos patients : crypter toutes les données afin que personne ne puisse les lire, sauf les personnes autorisées.

4.4. Principes de mise en œuvre :

4.4.1. Planification de la continuité des activités :

4.4.1.1. Définition du périmètre du plan de continuité :

Il convient de définir précisément l'ensemble du cadre du plan de continuité (ressources, responsabilités, périodicité des tests...) pour chacun des aspects suivants : les installations, matériels et réseaux informatiques. Les programmes et données informatiques. Les utilisateurs du système d'information [26]. Nous avons assuré la continuité :

- Redondance des éléments totale ou partielle, adaptée en fonction de leur niveau de criticité en termes de disponibilité.
- Nous avons un serveur de sauvegarde pour les données critiques.
- Répartition des services pour diminuer les impacts du catastrophé (un feu, ...).

4.4.1.2. Elaboration d'un plan de reprise :

Un plan de reprise informatique (ou plan de reprise d'activité) est nécessaire

Pour protéger les tâches opérationnelles critiques du système d'information face aux défaillances majeures, aux erreurs humaines, aux catastrophes naturelles ou aux attaques délibérées [26] .Le plan de reprise d'activité impose la prise en compte de toutes les exigences opérationnelles du système d'information pour assurer un retour à un fonctionnement normal :

- Restaurer uniquement les services et les configurations qui permettent au système de fonctionner (permanente).
- Consacrer tous les efforts et le temps pour trouver une solution et réparer le système le plus bref délai.
- Former le personnel aux procédures d'urgence.
- Remettre le système dans son travail quotidien et restaurer toutes les données restantes.

4.4.1.3. Positionnement des applications dans le plan de continuité :

En fonction de l'analyse de risques de l'organisme, chaque application doit faire l'objet d'une notation en terme de priorité de reprise. Cette notation correspond à une mesure de l'impact qu'aurait l'indisponibilité de l'application sur l'activité de l'organisme [27]. nous classons les fonctionnalités hospitalières selon la gravité de la maladie.

4.4.1.4. Mises-en place de procédures de sauvegarde et de restauration :

En cas de perte d'informations sur le système, vous devez utiliser vos copies de sauvegarde de ces informations. Cet ensemble de rubriques vous aide à planifier votre stratégie et à effectuer les choix appropriés pour la configuration du système en termes de sauvegarde, de reprise et de disponibilité [27]. Nous appliquons une stratégie de sauvegarde moyenne dans un période de 4 à 6 heures par jour sans activité du système, respectons toujours le principe : plus le système est modifié, plus vous devez le sauvegarder souvent. Nous disposons des techniques suivantes, utilisables séparément ou de façon combinée :

- Sauvegarde des objets modifiés.
- Journalisation des objets et sauvegarde des récepteurs de journal.

4.4.1.5. Tests réguliers des plans :

Pour mériter un niveau de confiance élevé, le plan de continuité et les plans liés doivent être testés régulièrement. À la fin de chacun de ces exercices, il sera mis en place un groupe « retour d'expérience » qui mettra à jour les plans après analyse des dysfonctionnements ou lenteurs. Nous établissons une suite de tests et d'exercices :

- Tester techniquement tous les moyens de continuité prévus.
- Vérifier la restauration complète des données.
- Former tous les acteurs concernés par le PCA (Planification de la continuité des activités).

Réaliser un exercice d'intégration du PCA sur les activités les plus critiques d'une direction de l'hôpital.

Chapitre 03 :

Bilan Personnel et

Professionnel

Bilan personnel :

Ce travail de recherche étant terminé, je retire de nombreux apprentissages.

Cette recherche m'a permis de mieux maîtriser une méthodologie de projet et de comprendre en quoi la maîtrise et l'efficacité influencent les processus et les résultats.

Un tel travail s'inscrit dans la durée. J'ai dû me confronter à mes capacités organisationnelles et à ma façon de gérer le temps. Même si cela n'a pas toujours été facile, j'ai tout de même réussi à mener à bien cette recherche.

La difficulté principale que j'ai rencontrée reste le déroulement du travail.

Au terme de cette recherche, j'ai beaucoup appris sur la manière de développer un projet, et j'ai eu l'occasion de vivre durant quelques mois au sein d'une nouvelle expérience.

En effet, je confirme qu'il faut faire preuve de flexibilité d'esprit.

J'ai réalisé que le travail de recherche prend du temps et que sa bonne gestion est essentielle pour ne pas se laisser déborder.

Pour terminer, ce travail a été co-écrit avec un collègue. Le travail en duo m'a motivée, m'a amené à améliorer mes compétences de collaboration, Les nombreux échanges d'idées qu'il a donné ont enrichi notre projet.

Bilan professionnel :

Mon projet de licence consiste en la conception et la réalisation d'un réseau de campus et sa sécurité, afin d'avoir une expérience pratique dans ce domaine , ce qui ne permettra de créer une bonne base pour la vie professionnel .

A travers cette année, j'ai un peu développé ma professionnalité en m'appuyant sur les cours théoriques, des recherches sur internet, les séances d'ateliers présentiels expliqués par notre encadreur ainsi les vidéos qui nous ont été envoyées, durant une période limitée.

Malheureusement cette année on n'a pas eu la chance de faire un stage à cause de l'épidémie de covid-19 donc on n'a pas eu des rencontres avec les professionnels en réseau et sécurité qui représentent pour nous un pilier et nous accompagnent dans l'acquisition de nouvelles compétences ; ce qui a laissé une ambiguïté dans notre vue.

Malgré ces empêchements on est arrivé à acquérir des compétences et connaître les outils dans ce domaine et savoir les manipuler on cite :

Exemple dans la partie de conception on a appris à utiliser le logiciel packet tracer qui ne permet de concevoir l'architecture de ce réseau sécurisé afin de passer à la réalisation qui ne aidera à approfondir nos connaissances dans les domaines suivants :

- Comprendre les notions de virtualisation et d'émulation

- Administration des systèmes Linux

- Configuration et mises en place des équipements de sécurité

- Durcissement d'un système d'exploitation

- Configuration et audit des serveurs

- Mises-en place de la QoS (Quality of Service)

Enfin, je peux dire que durant cette formation je me suis sentie réellement à ma place au sein d'un thème que j'ai choisi et qui m'a intéressée.

Conclusion générale :

L'objectif de notre projet de fin d'étude était de concevoir et réaliser un réseau sécurisé pour le groupe « chifa » ; (une clinique médicale).

Pour mener à bien notre mission, nous avons mis en œuvre toutes nos connaissances acquises durant notre parcours universitaire.

En outre, ce projet nous a offert la possibilité de revoir et de suivre avec beaucoup d'attention les méthodes fondamentales des deux concepts « réseau » et « sécurité », grâce auxquelles l'application a été mise au point.

Les fonctions principales fournies par notre proposition sont : rendre la clinique numérisée, faciliter la tâche du corps hospitalier et satisfaire les besoins du patient.

Nous avons par la suite entamé la phase de conception de l'architecture qui donne une vision générale de la structure de réseau et Ensuite, la phase de réalisation où on fait la configuration des équipements choisis pour leur bon fonctionnement.

Et on a terminé par le bilan personnel et professionnel qui parle des difficultés affronter, le déroulement de travail et des compétences acquises.

Nous sommes d'autant plus satisfaits que la réalisation de ce projet représente une opportunité pour nous découvrir le monde professionnel, ses réalités, ses difficultés et ses engagements imposés.

Enfin, nous espérons que ce modeste travail servira de référence et de base à tous ceux qui voudront s'engager dans un travail typique.

Bibliographie :

- [1] : <https://www.al-enterprise.com/-/media/assets/internet/documents/hospital-networking-guide-brochure-fr.pdf>
- [2] : <https://www.ionos.fr/digitalguide/serveur/know-how/reseau-informatique-definition/>
- [3] : [3] : JF.PILLOU, Fabrice LEMAINAQUE, Tout sur les réseaux et internet, 4eme édition dunod, 3 juin 2015.
- [4] : Mémoire de fin de Cycle, Université Abderrahmane Mira de Béjaïa, Département Informatique
THÈME : Proposition de solution de sécurité pour le Réseau local de l'hôpital d'Amizour
Réalisé par : Mr. Fares KHELOUFI, Mr. Yacine IKHLEF,
Encadrés par : Mme GHANEM Souhila Melle SADOU Malika
- [5] https://www.ssi.gouv.fr/uploads/2012/01/anssi-guide-passerelle_internet_securisee-v2.pdf
- [6] : https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html
- [7] : <https://ichi.pro/fr/proxy-inverse-apache-contenu-de-differents-sites-web-68731816878922>
<https://pixelabs.fr/serveur-dns-master-slave-debian-bind9/>
- [8] : https://www.cisco.com/c/fr_ca/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html
- [9] : <https://www.tech-faq.com/nat-network-address-translation.html>
- [10] : CCDE Study Guide , l'auteur : marwan al-shawi
<http://ptgmedia.pearsoncmg.com/images/9781587144615/samplepages/9781587144615.pdf>
- [11] : <https://sylvaindebeer.weebly.com/fonctionnement-de-la-nat.html>
- [12] : <https://cisco.goffinet.org/ccna/filtrage/concept-ids-ips/>
- [13] : 18_Reseau_Campus.PDF https://www.cisco.com/c/dam/global/fr_ca/training-events/pdfs/1-8_Deploiement_de_reseaux_Campus_multicouches.pdf
- [14] :
- [15] : <http://www.squid-cache.org/>
- [16] : <https://www.hostinger.com/tutorials/iptables-tutorial>
- [17] : <https://www.quora.com/What-are-the-advantages-and-disadvantages-of-Iptables-and-how-do-I-overcome-them>
- [18] : [https://en.wikipedia.org/wiki/Snort_\(software\)](https://en.wikipedia.org/wiki/Snort_(software))
- [19] : <https://fr.wikipedia.org/wiki/Fail2ban>
- [20] : <https://www.scaleway.com/en/docs/how-to-configure-nginx-reverse-proxy/>
- [21] : <https://www.ldlc-pro.com/fiche/PB00243500.html>
- [22] : <https://www.ldlc.com/fr-lu/fiche/PB00168292.html>
- [23] : <https://cyberguide.ccb.belgium.be/fr/politique-sauvegarde>
- [24] : <https://www.itaia.fr/logiciels-malveillants/>
- [25] : https://fr.wikipedia.org/wiki/Contr%C3%B4le_d'acc%C3%A8s
- [26] : <https://www.ssi.gouv.fr/uploads/IMG/pdf/pssi-section3-principes-2004-03-03.pdf>

- [27] : https://www.ibm.com/docs/fr/ssw_ibm_i_73/rzaj1/rzaj1pdf.pdf
- [28] : <https://searchnetworking.techtarget.com/definition/local-area-network-LAN>
- [29] : <https://www.networkworld.com/article/3584876/what-is-a-network-switch-and-how-does-it-work.html>
- [30] : <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203415-vlan-virtual-local-area-network-definition-traduction/>
- [31] : <https://www.futura-sciences.com/tech/definitions/informatique-nas-18209/>
- [32] : <https://culture-informatique.net/cest-quoi-un-serveur-dhcp-niv1/>
- [33] : <https://openclassrooms.com/fr/courses/1733551-gerez-votre-serveur-linux-et-ses-services/5236036-installez-un-anuaire-ldap>
- [34] : <https://www.lemagit.fr/definition/SSH-Secure-Shell>
- [35] : <https://www.it-connect.fr/securiser-son-switch-cisco-avec-port-security/>
- [36] : <https://community.fs.com/fr/blog/what-is-dhcp-snooping-and-how-it-works.html>
- [37] : <https://techterms.com/definition/ntp>
- [38] : <https://www.linksys.com/fr/r/ressource-center/qu'est-ce-qu'un-point-d'acc%C3%A8s/>
- [39] : [https://fr.wikipedia.org/wiki/Squid_\(logiciel\)](https://fr.wikipedia.org/wiki/Squid_(logiciel))

Annexes

Annexe 01 : 1. Réseau Local :

1.1. Introduction :

Un réseau local est un groupe d'ordinateurs et de périphériques qui partagent une ligne de communication commune ou une liaison sans fil avec un serveur dans une zone géographique distincte. Les administrateurs réseau configurent des réseaux locaux afin que les nœuds de réseau puissent communiquer et partager des ressources telles que des imprimantes ou un stockage réseau. La mise en réseau LAN nécessite des câbles Ethernet et des commutateurs de couche 2 ainsi que des périphériques pouvant se connecter et communiquer via Ethernet. Les plus grands réseaux locaux incluent souvent des commutateurs ou des routeurs de couche 3 pour rationaliser les flux de trafic [28].

1.2. Le commutateur :

Un commutateur est un périphérique réseau qui fonctionne au niveau de la couche de liaison de données du modèle OSI couche 2, Il reçoit les paquets envoyés par les appareils connectés à son port physique et les envoie à nouveau mais seulement à travers les ports qui conduisent aux appareils que les paquets sont destinés à atteindre, Le commutateur utilise l'adresse MAC pour identifier à partir de quel périphérique connecté les paquets sortants sont envoyés et où livrer les paquets entrants. Ils peuvent également fonctionner au niveau de la couche réseau couche 3 où le routage se produit [29].



Figure 23: Un commutateur.

1.3. VLAN (Virtual Local Area Network):

Un VLAN, pour Virtual Local Area Network, décrit un type de réseau local. On le traduit en français par réseau local virtuel. Le VLAN regroupe, de façon logique et indépendante, un ensemble de machines informatiques. On peut en retrouver plusieurs coexistant simultanément sur un même commutateur réseau. Le VLAN améliore la gestion du réseau en apportant plus de souplesse dans son administration. Les VLAN sont un groupe d'hôtes ou de ports qui peuvent être situés n'importe où dans un réseau mais qui communiquent comme s'ils se trouvaient sur le même segment physique [30].

1.4. Serveur NAS :

NAS est l'acronyme anglais de Network Attached Storage qui signifie serveur de stockage en réseau. Il se présente généralement sous la forme d'un boîtier connecté au réseau local ou à internet pouvant accueillir un ou plusieurs disques durs, dont le contenu est accessible à tout moment par une interface sécurisée, il s'agit d'un serveur de fichiers capable de fonctionner de façon autonome. On le résume parfois à un disque dur relié à un réseau (privé, professionnel) [31].



Figure 24: Serveur NAS.

1.5. Serveur DHCP :

Un serveur DHCP (ou service DHCP) est un serveur qui délivre des adresses IP aux équipements qui se connectent sur le réseau. En effet, la plupart du temps, les cartes réseaux de ces équipements sont en attente d'une adresse IP leur permettant de communiquer sur le réseau. En même temps qu'il envoie l'adresse, le service DHCP envoie quelques informations complémentaires concernant le réseau sur lequel est branché l'hôte qui reçoit cette adresse, Je vous rappelle que l'adresse IP doit être unique sur un réseau donc le serveur DHCP va gérer les adresses et n'attribuer que des adresses non utilisées à tout nouvel hôte qui en fait la demande, Vous l'avez compris, le serveur DHCP m'a donné une adresse IP, mais elle est limitée dans le temps (4h, 6h, ... cela dépend du réglage de l'administrateur du service) [32].

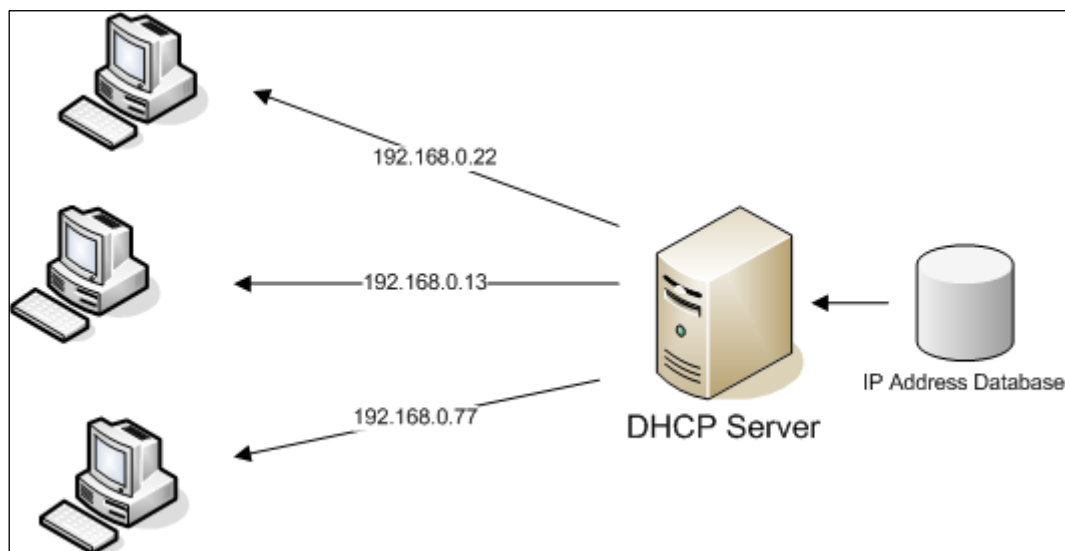


Figure 25 : Serveur DHCP.

1.6. Serveur Web :

Un serveur Web est un logiciel et un matériel qui utilise http et d'autres protocoles pour répondre aux demandes des clients faites sur le World Wide Web. Le travail principal d'un serveur Web est d'afficher le contenu du site Web en stockant, traitement et livraison des pages Web aux utilisateurs. Le matériel du serveur Web est connecté à Internet et permet l'échange de données avec d'autres appareils connectés, tandis que le logiciel de serveur Web contrôle la façon dont un utilisateur accède aux fichiers hébergés. Le processus de serveur

Web est un exemple du modèle client/serveur, Tous les ordinateurs qui hébergent des sites Web doivent avoir d'un logiciel de serveur Web.

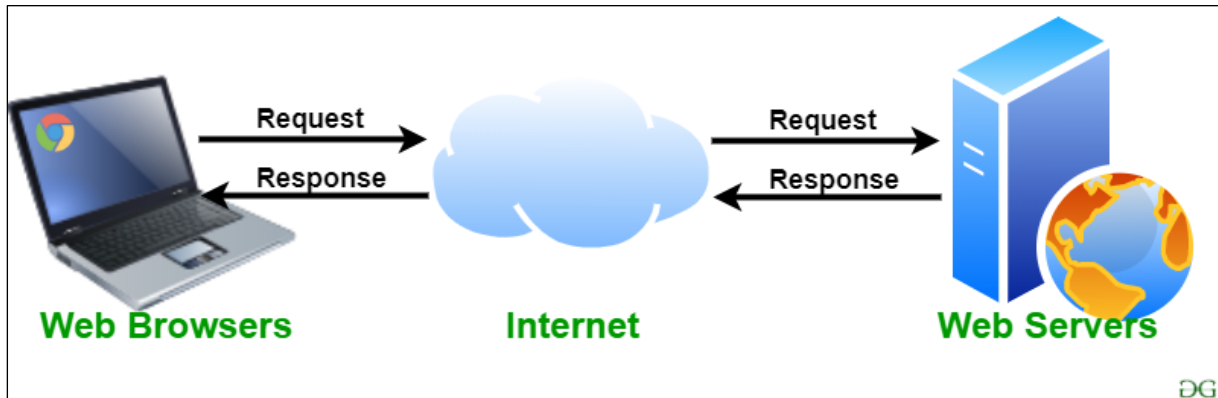


Figure 26 : Serveur Web.

1.7. Serveur LDAP :

LDAP signifie Lightweight Directory Access Protocol. C'est le standard de fait pour accéder à un annuaire. Un annuaire est une base de données qui va contenir des informations sur des personnes, des machines, des groupes ou toute autre catégorie que vous pourriez imaginer. Un annuaire se distingue d'une base de données relationnelle par le fait qu'il a une structure hiérarchique et qu'il est très rapide pour chercher et lire des éléments mais plus lent pour les modifier, les annuaires sont couramment employés pour stocker les données d'authentification ou pour obtenir des informations sur des personnes. un annuaire LDAP est une organisation hiérarchique d'entrées, cette organisation constitue un arbre appelé DIT (Directory Information Tree) dont une des entrées est la racine [33].

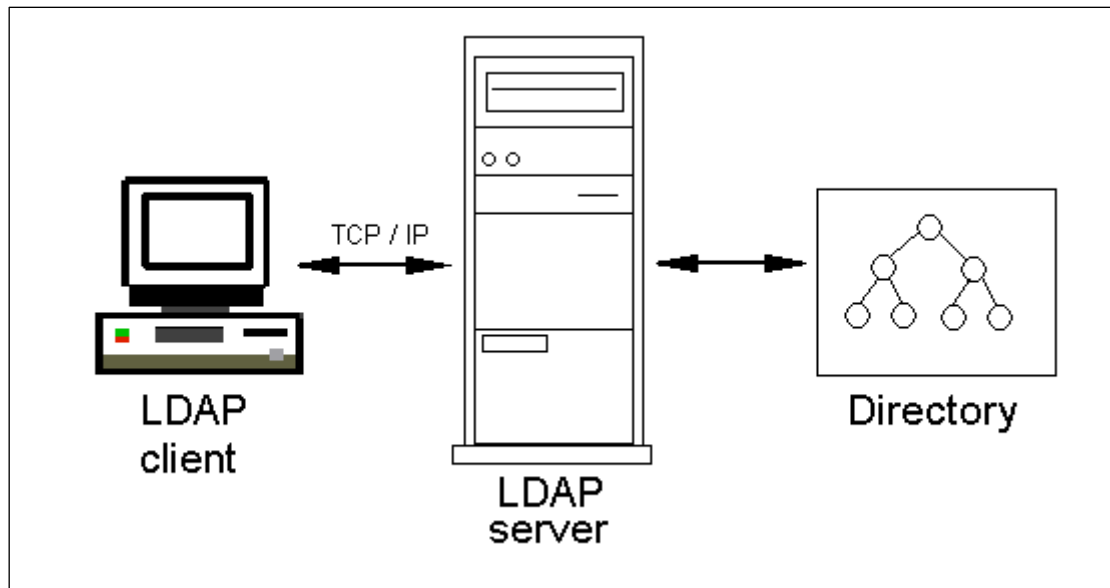


Figure 27: Le serveur LDAP.

1.8. VPN (Virtual Private Network):

VPN signifie Virtual Private Network, qui permet à un utilisateur de se connecter à un réseau privé sur Internet de manière sécurisée et privée, Le VPN crée une connexion cryptée appelée tunnel VPN, et tout le trafic Internet et les communications passent par ce tunnel sécurisé. Il existe 3 types standards d'utilisation des VPNs selon leur mode d'utilisation:

VPN d'accès (Host to Lan), l'intranet vpn (Lan to Lan), l'extranet vpn (host to host)

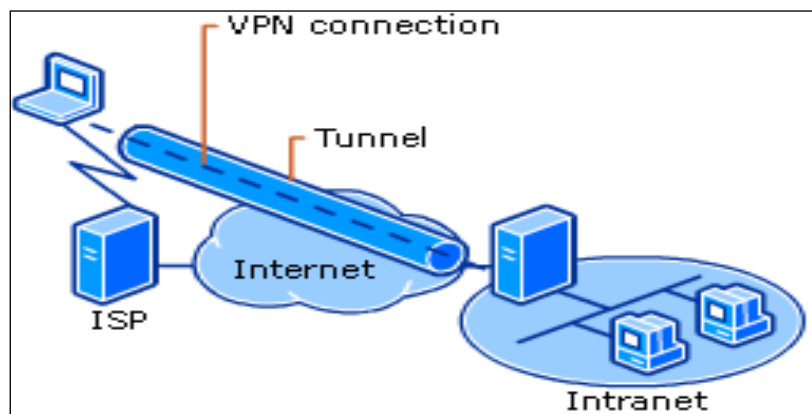


Figure 28: VPN.

1.9. SSH (Secure Socket Shell):

SSH, ou Secure Socket Shell, est un protocole réseau qui permet aux administrateurs d'accéder à distance à un ordinateur, en toute sécurité. SSH désigne également l'ensemble des utilitaires qui mettent en œuvre le protocole. Le protocole Secure Shell assure une authentification forte et des communications de données chiffrées sécurisées entre deux ordinateurs connectés sur un réseau peu sûr, tel qu'Internet. SSH est largement utilisé par les administrateurs réseau pour gérer à distance les systèmes et les applications, car il leur permet de se connecter à un autre ordinateur sur un réseau, d'exécuter des commandes et de déplacer des fichiers d'un ordinateur à un autre. SSH désigne à la fois le protocole de réseau cryptographique et les utilitaires qui mettent en œuvre ce protocole. SSH fonctionne selon le modèle client-serveur, en connectant une application client Secure Shell - là où s'affiche la session - à un serveur SSH - là où s'exécute la session [34].

1.10. Porte sécurité :

Avec les Switchs Cisco, il est possible de faire un contrôle sur les ports en limitant l'accès à certaines adresses MAC, cela permet de sécuriser l'accès. Pour cela, il faut utiliser l'option « Port-security ». Il y a deux méthodes, la première consiste à enregistrer manuellement l'adresse MAC autorisée et la seconde consiste à prendre comme adresse MAC autorisée celle de l'hôte qui va se connecter et envoyer une trame en premier à ce port du Switch Cisco [35].

1.11. DHCP snooping :

DHCP Snooping est une technologie de sécurité de couche 2 du modèle OSI intégrée dans le système d'exploitation d'un commutateur réseau capable qui connecte les clients aux serveurs DHCP et supprime le trafic DHCP jugé inacceptable. Il empêche les serveurs DHCP non autorisés qui offrent des adresses IP aux clients DHCP [36].

1.12. ARP inspection :

ARP inspection est une fonction de sécurité qui rejette les paquets ARP invalides et malveillants, la fonctionnalité empêche une classe d'attaques de l'homme du milieu, où une station hostile intercepte le trafic pour d'autres stations en empoisonnant les caches ARP de ses voisins sans méfiance, le mécréant envoie des demandes ou des réponses ARP mappant l'adresse IP d'une autre station à sa propre adresse MAC.

1.13. NTP : (network time Protocol) :

NTP est un protocole utilisé pour synchroniser les horloges des ordinateurs sur plusieurs systèmes. Il prend en charge la synchronisation sur les réseaux locaux et Internet. Faire correspondre les horodatages de deux ou plusieurs systèmes peut sembler une tâche simple, mais cela implique plusieurs étapes. Étant donné que tous les réseaux ont une certaine latence, le délai entre la demande et la réponse doit être pris en compte. NTP utilise le modèle client-serveur et calcule le délai d'aller-retour [37].

1.14. Point d'Accès :

Un point d'accès est un appareil qui crée un réseau local sans fil, ou WLAN, habituellement dans un bureau ou dans un grand bâtiment. Un point d'accès se connecte à un routeur filaire, hub ou commutateur par câble Ethernet et délivre un signal Wi-Fi à une zone dédiée. Si vous souhaitez par exemple activer le Wi-Fi dans le hall de réception de votre entreprise, mais vous ne disposez pas d'un routeur à portée de main, vous pouvez alors installer un point d'accès près de la réception en acheminant un câble Ethernet à travers le plafond vers la salle des serveurs [38].