N° Ordre...../F.S.S.A/UAMOB/2020

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE AKLI MOHAND OULHADJ-BOUIRA

Faculté des Sciences et des Sciences Appliquées

Département Génie Électrique

Mémoire de fin d'étude

Présenté par :

BOULILA Nedjma

BOULILA Ranida

En vue de l'obtention du diplôme de **Master en :**

Filière : Télécommunication

Option : Système de Télécommunication

Thème

Mise en réseau d'une Infrastructure Hyper-Convergée via deux WANs en redondance (ADSL et MPLS)

Soutenue le : 19/01/2021.

Devant le jury composé de :

CHELBI Salim	MCB	UAMOB	Président
SAOUD Bilal	MCA	UAMOB	Encadreur
NOURINE Mourad	MCA	UAMOB	Examinateur

Année Universitaire 2019/2020

Résumé

Les nouvelles technologies des réseaux informatiques, notamment « les réseaux contrôlés par logiciel », viens changer la face du réseau (sur le déploiement et gestion), et permettent de résoudre de nombreux problèmes et contraintes liés à l'activité des entreprises. Notre projet a été réalisé au niveau de l'Etablissement Publique- Algérienne Des Eaux (EP-A.D.E), qui vise à revoir la manière dont cet établissement exploite les ressources de l'infrastructure du DataCenter à sa disposition, et assurer un accès fluide, sécurisé et ajusté aux besoins de l'ensemble des utilisateurs, exerçant leurs taches dans des structure séparées géographiquement. Notre proposition est adaptée au besoin de l'EP-ADE et assujetti à une politique de sécurité, qui a pour condition d'assurer la confidentialité et l'intégrité des données. Les différentes taches englobées dans notre projet sont simulées et testées sur le simulateur GNS3 et réellement au niveau de EP-A.D.E.

Mots-clés: Réseaux informatiques, Entreprise, Datacenter, Sécurité, GNS3.

Abstract

New computer network technologies, in particular "Software-Defined Networks", are changing the face of the network (on deployment and management), and make it possible to solve many problems and constraints related to business activity. Our project was carried out at the level of the Algerian Public-Water Establishment (EP-A.D.E), which aims to review the way in which this establishment uses the resources of the DataCenter infrastructure at its disposal, and to ensure fluid, secure access adjusted to the needs of all users, carrying out their duties in geographically separate structures. Our proposal is adapted to the needs of the EP-ADE and subject to a security policy, which has the condition of ensuring the confidentiality and integrity of the data. The different tasks included in our project are simulated and tested on the GNS3 simulator and really at EP-A.D.E.

Keywords: Computer networks, Company, Datacenter, Security, GNS3.

ملخص

تعمل تقنيات شبكات الكمبيوتر الجديدة، ولا سيما "الشبكات التي يتحكم فيها البرنامج"، على تغيير وجه الشبكة (عند النشر والإدارة)، وتسمح بحل العديد من المشكلات والقيود المتعلقة بنشاط الأعمال. تم تنفيذ مشروعنا على مستوى المؤسسة العامة الجزائرية للمياه (EP-ADE)، والذي يهدف إلى مراجعة الطريقة التي تستخدم بها هذه المؤسسة موارد البنية التحتية لمركز البيانات الموجودة تحت تصرفها، ولضمان الوصول السلس والآمن لموارد مركز البيانات وذلك لتلبية احتياجات جميع المستخدمين، وتنفيذ واجباتهم في هياكل منفصلة جغرافيا. تم ضبط اقتراحنا مع احتياجات الجزائرية للمياه مع الخضوع لسياسة أمنية تشترط ضمان سرية وسلامة البيانات. تمت محاكاة المهام المختلفة المضمنة في مشروعنا واختبارها على برنامج GNS3 وعلى مستوى EP-A.D.E.

الكلمات الرئيسية: شبكات الكمبيوتر، الشركة، مركز البيانات، أمن البيانات.

Dédicace

Je dédie ce mémoire

À ma chère mère ;

À mon cher père ;

Qui n'ont jamais cessé, de formuler des prières à mon égard, de me soutenir et de m'épauler pour que je puisse atteindre mes objectifs.

À ma chère sœur, et frères

Pour leurs soutiens moral et leurs conseils précieux tout au long de mes études ;

À mon chère binôme, Nedjma

Pour sa entent et sa sympathie ;

À mon chère fiancé, Sofiane

Ainsi qu'à sa famille ;

Pour leur aide et support dans les moments difficiles ;

À toute ma famille ;

À tous mes autres amies, chaleureusement à Thilleli, Wissam, et Sabrina ;

À tous ceux que j'aime et ceux qui m'aiment.

Ranida

Dédicace

Avec un énorme plaisir, un cœur ouvert et une immense joie, que je dédie ce modeste travail :

À mes très chers parent, pour leurs patiences, leurs amour, leurs encouragements et leurs sacrifices tout au long de mon parcoure ;

À mon très cher mari SALIM Pour son aide précieuse et ses encouragements, ainsi qu'à toute sa famille ;

À mes frères et ma sœur ;

À mes oncles, mes tantes ;

À toute ma famille BOULILA ;

À mon cher binôme RANIDA ainsi qu'à sa famille ;

À tous mes amies ;

À mes enseignants et mes collèges d'études ;

ET à tous ceux qui m'ont aidé de près ou de loin dans l'élaboration de ce travail.

Nedjma

Remerciement

Tout d'abord, le grand et l'infini remerciement au bon dieu ALLAH, le tout puissant de nous avoir illuminé et ouvert les portes du savoir et nous avoir donné la volonté, la santé et le courage pour effectuer ce travail.

Nous souhaitons adresser nos remerciements aux personnes qui nous ont aidées dans la réalisation de notre mémoire de fin d'études. En premier lieu, nous remercions notre promoteur ***Mr SAOUD Bilal*** *d'avoir accepté de nous encadrer, orienté, pour notre projet, ainsi que pour sa confiance, ses encouragements, ses corrections et pour les conseils qu'il apporté. Nous tenons également à remercier l'ensemble des membres de jury de nous avoir honorés en acceptant d'évaluer notre travail, ainsi que pour d'éventuelles suggestions.*

Et de manière spéciale nous exprimons nos chaleureux remerciements pour notre encadreur de stage ***Mr KHELLAL Salim*** *qui nous a donné l'opportunité de nous familiariser avec le milieu de travail, nous avoir aidé avec toute sa patience et qui nous a ouvert les horizons par ses idées, ses propositions et ses ambitions et qui nous a soutenus jusqu'au bout.*

Nous présentons aussi nos remerciements à ***Mr MAKACI Anis*** *pour le temps qu'il nous a accordé et pour son aide précieuse durant la période de notre stage, Nos remerciements vont également à l'ensemble du personnel de L'Etablissement Publique Algériennes des Eaux (EP-ADE) de Bouira, et en particulier l'équipe informatique, pour tous les moyens qu'ils nous ont offert pour un stage de qualité.*

Nous tenons également à remercier toutes nos familles, nos ami(e), nos collègues étudiants et tous ceux qui ont participés de près ou de loin à la réalisation de ce travail

Nous profitons aussi cette occasion pour exprimer nos plus vifs remerciements envers tous les enseignants du département Génie Electrique, de la Faculté des Sciences et Sciences Appliquées, d'Université Akli Mohand Oulhadj de Bouira qui nous ont apportés du soutien durant nos études.

Sommaire

Liste des figures

Liste des tableaux

Liste des abréviations

ACL	*Access Control List*
ADE	*Algérienne Des Eaux*
ARP	*Address Resolution Protocol*
ATM	*Asynchrone Transfer Mode*
BAS	*Broadband Access Server*
BGP	*Broder Gateway Protocol*
CPU	*Central Procissing Unit*
DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
DSLAM	*Digital Subscriber Line Access Multiplexer*
EAP	*Extensible Authentication Protocol*
EGP	*Exterior Gateway Protocol*
EIGRP	*Enhanced Interior Gateway Routing Protocol*
EP-ADE	*Etablissement Publique – Algérienne Des Eaux*
ESX	*Elastic Sky X*
ESXi	*Elastic Sky X Integrated*
FAI	*Fournisseur d'Accès à Internet*
FTP	*File Transfer Protocol*
HCI	*Hyper-converged infrastructure*
HTTP	*Hyper Text Transfer Protocol*
ICMP	*Internet Control Message Protocol*
IEEE 802.1Q	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Enginering Task Force*
IGP	*Interior Gateway Protocol*
IOPS	*Input /Output Operation Per Second*
IOS	*Internetwork Operating System*
IP	*Internet Protocol*
IPSec	*Internet Protocol security*
IPv4	*Internet Protocol Version 4*
IPv6	*Internet Protocol Version 6*
IS-IS	*Intermidiat System to Intermidiat System*
KVM	*Keyboard Video Mouse Switch*
LAN	*Local Area Network*
LDAP	*Lightweipht Directory*
LDP	*Label Distribution Protocol*
LSR	*Label Switching Router*
LTE	*Long Terme Evaluation*

MAC	*Media Access Control*
MPLS	*MultiProtocol Label Switching*
NAS	*Network Attachement Storage*
NAT	*Network Address Translation*
NRA	*Noeud de Raccordement d'Abonnés*
OSI	*Open System Interconnect*
OSPF	*Open Shortest Path First*
PC	*Personal Computer*
PDA	*Personal Digital Assistant*
PGP	*Pretty Good Privacy*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
PSK	*Pre-Shared Key*
RSA	*Rivest –Shanir-Aldman*
RTC	*Réseau Téléphonique Commuté*
SAN	*Storage Area Network*
SATA	*Serial Advanced Technology Attachement*
SCSI	*Small Computer System Interface*
SDN	*Software Defined Network*
SD-WAN	*Software-Defined Wide Area Network*
SMTP	*Simple Mail Transfer Protocol*
SSH	*Secure Shell*
SSID	*Service Set IDentifier*
SSL	*Secure Sockets Layer*
SQL	*Structure Query Language*
TCP	*Transmission Control Protocol*
TCP / IP	*Transmission Control Protocol /Internet Protocol*
TKIP	*Temporal Key Integrity Protocol*
UDP	*User Datagram Protocol*
VCI	*Virtual Channel Identifier*
VLAN	*Virtual Local Area Network*
VM	*Virtual Machine*
VPI	*Virtual Path Identifier*
WAN	*Wide Area Protocol*
WEP	*Wired Equivalent Privacy*
WIFI	*WIreless FIdelity*
WPA	*Wi-Fi Protected Access*
xDSL	*Digital Subscriber Line*

Introduction Générale

La finalité d'une entreprise, dépend directement des moyens sociotechniques à sa disposition, en d'autres termes, la capacité et l'efficacité du système informatique à rependre aux besoins de ces utilisateurs, et à assurer un support technique adapté minutieusement a la nature de l'entreprise, et le type de son activité. Toutefois, le choix des différents outils pour la mise en œuvre d'un system d'information, comporte des compromis, et vise à rependre au mieux et à la fois aux exigences des utilisateurs, et ce à moindre coût.

La gestion des données et processus souvent sensibles, voire confidentiels, est un défi, qui consiste à la fois d'assurer la simplicité de la gestion, l'intégrité et la sécurité des données de l'entreprise.

L'établissement Public - Algérienne des Eaux (E.P-A.D.E), de son caractère industriel et commercial, a éprouvé le besoin d'intégrer une solution de centralisation, qui vise à revoir radicalement le support technique en place, en mettant en œuvre un nouveau système d'information, et donc une nouvelle infrastructure.

La solution consiste à mettre en place une infrastructure hyper-convergée, qui va permettre d'héberger une solution pour la gestion commerciale, aux premiers temps, (centralisation de base de données, relève avec PDA, calcul automatique de la facture, e-paiement,….), mais l'ambition de cette dernière va encore plus loin, et dans le collimateur, la comptabilité, l'hydraulique, et les autres services et départements.

Le choix de l'infrastructure hyper-convergée s'explique par sa facilité de déploiement et la possibilité d'intégrer des services tel que la téléphonie IP, la visioconférence, la virtualisation des systèmes d'exploitation, la surveillance à distance, …, ainsi qu'une gestion centralisée, mais encore un tableau de bords complet, qui offre une vision globale et statistique, des activités de l'EP-A.D.E, et ce a un coût très abordable, mais toutefois, cette infrastructure né pas accompagnée avec les solutions adéquates, pour son exploitation optimale, et un rendement à la hauteur d'un tel investissement.

Le projet en cours que mène l'équipe informatique de l'EP-A.D.E nous offre l'opportunité d'apporter notre contribution, afin d'exploiter au mieux l'infrastructure en place (Datacenter). Notre travail sera donc consacrer à étudier cette dernière, et à proposer les meilleurs solutions, en vue d'assurer et d'optimiser l'accès des différentes structures (géographiquement distinctes) du même établissement, via les lignes WAN à disposition, et ce d'une manière contrôlée et sécurisée (mise en œuvre d'une politique de sécurité), et offrir un accès aisé pour les utilisateurs de l'établissement, aux ressources du système d'information, tel que l'accès à internet, annuaires, messagerie, progiciels…, sur des PC et des appareil mobiles (téléphones et tablettes via le réseau wifi), tout en assurant la confidentialité et l'intégrité des données de l'établissement.

Notre travail sera rapporté selon la méthodologie en vigueur, sous forme d'un mémoire de fin d'étude, structuré comme suite :

Dans un premier chapitre nous présentons la structure hyper convergée (Datacenter), le deuxième chapitre se rapportera sur un rappelle a des notions sur les réseaux informatiques, et un troisième chapitre sera dédier a la sécurité informatique, et enfin le quatrième chapitre sera consacrer à l'étude de l'existant et la mise en œuvre de la mise en réseau de l'infrastructure de l'EP-A.D.E, et nous terminerons avec une conclusion.

CHAPITRE I

Présentation de L’infrastructure Hyper-Convergée

I.1 Introduction

Le terme «DataCenter» est en train de changer complètement de signification, car les entreprises recherchent des moyens pour gérer leurs charges de travail critiques, et pour déterminer ces moyens, il est à envisager de prendre en compte plusieurs aspects (le coût de l'investissement, la facilité du déploiement, et l'efficacité du support technique à rependre aux besoins de gestion).

Afin de simplifier l'architecture du Datacenter, les entreprises optent pour l'infrastructure hyper-convergée. Elle présente plusieurs avantages tel que l'homogénéité matérielle, qui grâce au billet de la virtualisation, permet d'exploiter au mieux les ressources physiques de cette dernière.

Dans ce chapitre; nous abordons des notions de base de l'infrastructure hyper-convergée.

I.2 **Historique**

Le modèle d'infrastructure traditionnel (Figure 1.1) repose sur des silos séparés et dédiés, (stockage, réseau, unité de calcul), et une couche logiciel propre à chaque silos, ce caractérise par la complexité et sa difficulté de déploiement et d'optimisation.

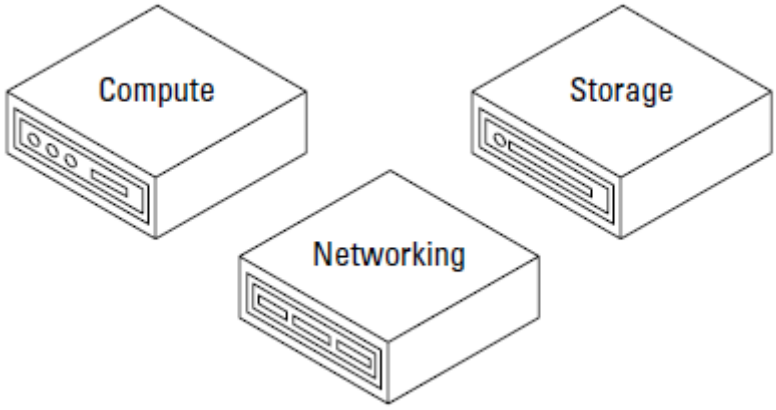


Figure I. 1 Infrastructure traditionnelle basée sur des silos [1].

L'infrastructure convergée améliore le modèle traditionnel, en convergeant les silos (calcule, stockage, la gestion et la mise en réseau) dans une seule baie [1].

L'assemblage de l'infrastructure peut se faire à partir des solutions proposées par des différents fournisseurs. Il est donc possible de choisir leurs serveurs de calcule, ceux du stockage et les équipements de la mise en réseau chez les différents fournisseurs, (l'approche Best of Breed), dans le but de choisir les meilleurs composants individuels mais absolument pas l'homogénéité de la solution par rapport à la gestion de l'ensemble de l'infrastructure [2], ainsi les limites physiques peuvent avoir été éliminés [1].

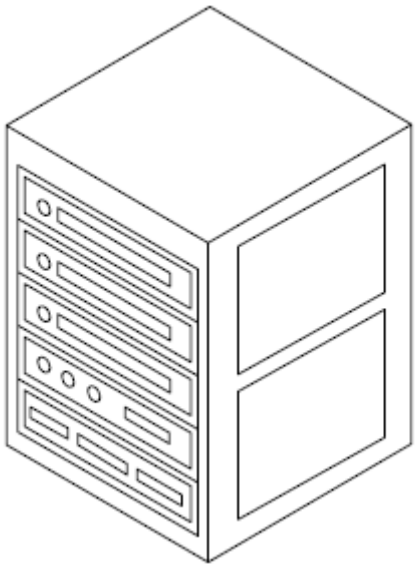


Figure I. 2 Infrastructure Convergée [1].

I.3 Le concept de l'Hyper-Convergence

L'hyper-convergence est venue du rapprochement du serveur de calcule et le serveur de stockage sous forme d'Appliance gérable via une solution logiciel unique, intégrant la virtualisation des ressources. Afin de pour supprimer les problèmes de gestion connus auparavant dans les infrastructures traditionnelles [3]. En outre, et à la différence de la convergence, l'hyper-convergence est une technologie définie par logiciel, qui dissocie les opérations d'infrastructure du matériel système et les fait converger au niveau de l'hyperviseur dans un bloc de construction unique (d'où le terme hyper-convergence), éliminant ainsi les inefficacités et accélérant les calculs, et encore la haute disponibilité et l'extensibilité.

I.3.1 Définition de l' l'Infrastructure Hyper-convergée

L'infrastructure hyper-convergée *(ou HCI pour Hyper-converged infrastructure en anglais)* est un type d'infrastructure informatique distribuée dans lequel le stockage partagé est délivré par une couche logicielle exploitant la capacité des disques durs installés dans les serveurs eux-mêmes [2]. Elle permet de piloter à la fois les fonctions de calcule et les fonctions de stockage, ainsi que les services additionnels éventuellement proposés dans l'infrastructure. Cette approche intégrée est un point qui rapproche les infrastructures hyper-convergées des infrastructures convergées [2].

Chaque serveur est à la fois un élément de « Compute » virtualisé et de stockage. En reliant ces serveurs via un réseau généralement en fibre optique, créant ainsi un système informatique distribué, dont la puissance et la capacité s'accroissent avec le nombre de nœuds (ajout de cartes de calcules ou des disques dures en extension). Le stockage partagé dans le cluster est le produit de l'agrégation par une couche logicielle plus ou moins propriétaire de la capacité de stockage des différents nœuds [2].

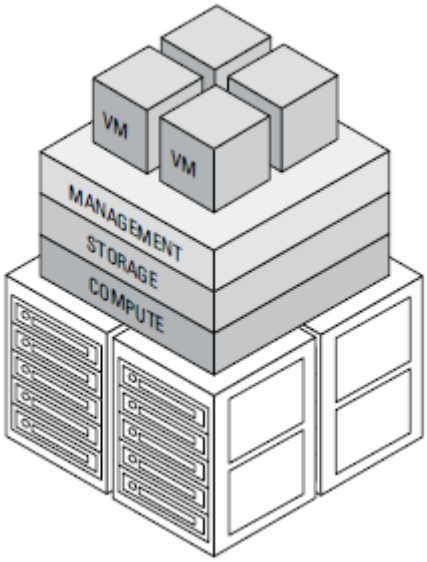


Figure I. 3 Infrastructure Hyper-Convergée [1].

I.3.2 Les composants essentiels de l'Infrastructure Hyper-Convergée

Quatre composants logiciels étroitement intégrés forment la plate-forme hyper-convergée :

- Virtualisation du stockage
- Virtualisation de l'unité de calcule.
- Virtualisation du réseau
- Fonctionnalités de gestion avancées.

I.3.3 Fonctionnement de l'Infrastructure Hyper-Convergée

Toutes les fonctions critiques du Data Center sont exécutées dans une couche logicielle étroitement intégrée plutôt que sur du matériel dédié. L'infrastructure hyper-convergée comprend trois composants : la virtualisation de l'environnement informatique, la virtualisation du stockage et la gestion. Le logiciel de virtualisation abstrait et regroupe les ressources sous-jacentes, puis les alloue dynamiquement aux applications exécutées dans des VM *(Machine Virtuelle)* ou des conteneurs [4].

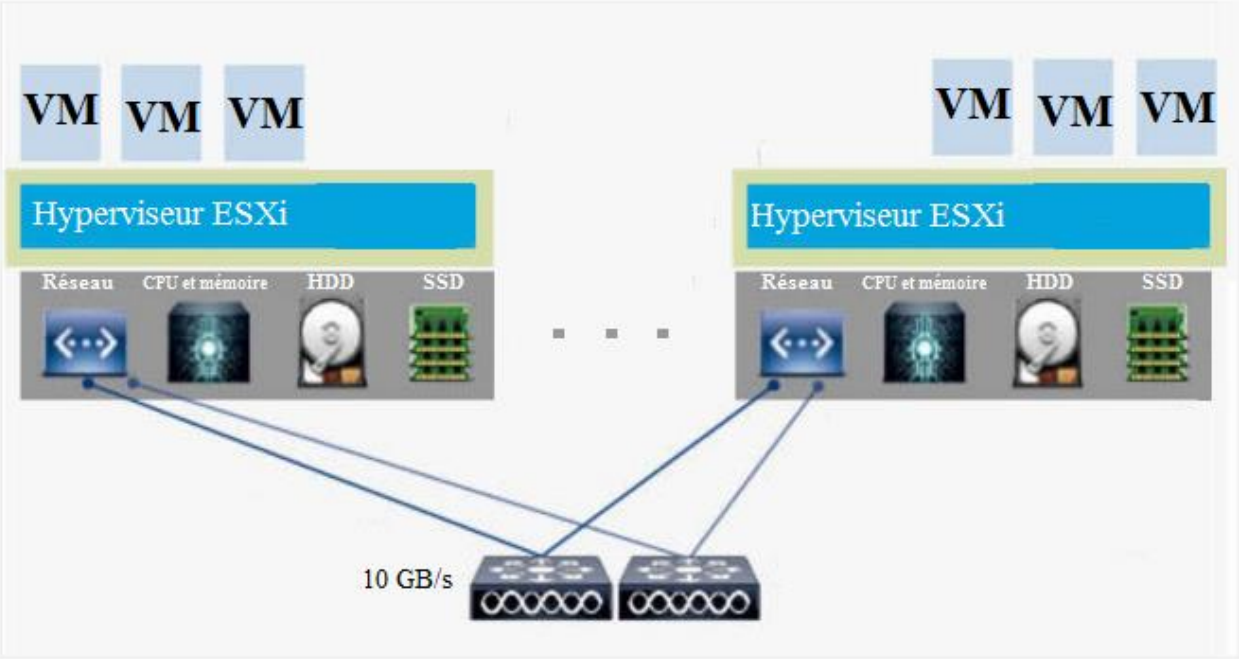


Figure I. 4 Fonctionnement de l'Infrastructure Hyper-Convergée.

I.3.4 Caractéristiques de l'Infrastructure Hyper-Convergée

I.3.4.1 Redondance matérielle (La haute disponibilité de l'infrastructure)

La redondance est une conception de systèmes dans laquelle les composants [5] primordiaux pour le fonctionnement du système (équipements, liaisons fibre optique, alimentation électrique,...) sont dupliqués, afin de garantir un certain niveau de haute disponibilité, pour accès ininterrompu aux bases de données et aux ressources du Datacenter.

I.3.4.2 Une technologie extensible «Scale Out »

Une technologie dans laquelle il est possible d'augmenter la quantité d'espace de stockage, et la puissance de calcul en ajoutant des unités à des baies reliées entre elles et dotées de leurs propres ressources [5]. L'architecture de l'infrastructure hyper-convergée permet l'ajout et la configuration de nouvelles unités de stockage ou de calcule au fur et à mesure suivant les besoins. Lorsque le système manque de performances ou atteint sa limite de stockage, il suffit d'ajouter de nouveaux disques ou/et plus volumineux pour le stockage et des unités de calcule. Grâce à ce type d'architecture, Cela permet à la fois d'accroître les performances aux besoins et d'éliminer des investissements inutiles [5].

I.3.4.3 L'Infrastructure Définie par Logiciel (SDI)

L'hyper-convergence étant basée sur une gestion centralisée par logiciels, assure la flexibilité nécessaire pour répondre aux besoins actuels et futurs de l'entreprise, sans devoir démonter et remplacer des composants de l'infrastructure. Encore mieux, à mesure que les fournisseurs développent de nouvelles caractéristiques dans les nouvelles versions de logiciels. Les clients profitent immédiatement des avantages de ces caractéristiques, sans devoir modifier l'infrastructure [6].

I.3.5 Mise en réseau d'une Infrastructure Hyper-Convergée

En examinant l'histoire de l'infrastructure hyper-convergée, il devient clair que les fondements de la technologie se concentrent carrément sur les parties de stockage et de calcul de la triade du Datacenter, laissant la partie réseau comme rien de plus qu'un élément de soutien. Le résultat a été une série de déploiements d'infrastructure hyper-convergée qui peuvent fonctionner sur des réseaux qui n'ont jamais vraiment été conçus avec les besoins uniques de l'hyper-convergence à l'esprit [7].

Bien plus que les autres technologies de stockage, l'hyper-convergence repose sur le réseau en tant qu'élément fondamental de ses capacités. Considère ceci: dans tout système de stockage qui utilise plusieurs copies de données dans le cadre du mécanisme global de protection des données, les données doivent être écrites dans deux ou plusieurs Emplacements. Lorsque le système de stockage est autonome, comme c'est le cas avec des périphériques SAN et NAS plus traditionnels, ces opérations d'écriture peuvent se dérouler parfois, dans les limites d'un seul châssis ou à travers un tissu de stockage dédié.

En revanche, la plupart des solutions d'infrastructure hyper-convergées reposent sur Ethernet comme liaison entre les nœuds les uns aux autres [7].

I.3.6 Enjeu économique

Les frais d'établissement des systèmes hyper-convergés sont faibles. Étant donné que l'on peut ajuster l'infrastructure aux besoins de l'entreprise au premiers temps, et faire des extensions au besoin (évolutivité centré sur logiciel). Ce qui permet de minimiser le budget de la mise en œuvre, et adopter une politique d'investissement de long terme.

I.3.7 Les avantages d'une Infrastructure Hyper-Convergée

L'infrastructure hyper-convergée offre plusieurs avantages. Parmi ces avantages on trouve :

- Gérer de manière fluide une infrastructure complexe.
- Accélère les charges de travail virtualisées.
- Améliore l'efficacité opérationnelle et de réduire les coûts.
- Offre la fiabilité, la disponibilité, la performance.
- Augmente la capacité dont les utilisateurs ont besoin tout en préparant votre infrastructure informatique pour l'avenir et en réduisant le coût total de possession.
- Permet une gestion centralisée d'environnements virtuels via une seule et même interface, ce qui réduit le nombre d'activités nécessitant beaucoup de ressources humaines.
- Offre une acquisition, un déploiement, une assistance et une gestion simplifiés.
- Fournit une approche évolutive en blocs de construction facilement extensibles.
- Réduit les besoins de stockage, de largeur de bande et d'opérations d'entrée-sortie par seconde (IOPS).
- Facilite l'évolution/réduction de ressources en fonction des demandes de l'entreprise [7].
- Centralise la charge de travail : avec l'infrastructure hyper-convergée, l'attention est portée sur la charge de travail, avec tous les systèmes associés orientés sur les applications.
- Assure la restauration de données en cas de perte ou de corruption qui représente une exigence fondamentale en informatique.
- Mobilité entre machines virtuelles : l'infrastructure hyper-convergée facilite encore davantage la mobilité entre les applications/charges de travail.
- Permet des niveaux plus élevés de disponibilité des données qu'avec les systèmes traditionnels.
- Offre un modèle économique durable par étapes qui élimine le gaspillage en informatique [6].

I.4 Virtualisation en Infrastructure Hyper-Convergée

I.4.1 Concept

C'est un processus informatique qui consiste à ajouter une couche d'abstraction entre les ressources physiques et la représentation logique d'un système ou d'un réseau informatique sous-jacent de manière à simplifier les interactions entre cette ressource et d'autres systèmes, d'autres applications et les utilisateurs. Elle permet ainsi de regrouper plusieurs entités physiques en une seule entité logique et vice versa [8].

Grâce à la virtualisation : toutes les machines virtuelles et les systèmes d'exploitation cohabites ensemble et en temps réel, partageant ainsi les même ressources (espace de stockage, internet...).

Il existe plusieurs domaines de virtualisation. On trouve : la virtualisation d'applications, la virtualisation de réseaux, la virtualisation de stockage et la virtualisation des unités de calcul.

I.4.2 Virtualisation des machines

Les approches basées sur la virtualisation des machines consistent à isoler les ressources informatiques de façon à pouvoir exécuter plusieurs instances de réseaux virtuels par un moyen de groupes de machines virtuelles interconnectées (VMs). Ces machines sont utilisées pour créer des routeurs et des liens virtuels pour servir de liaison. Cette technique est relativement utile. Dans ce qui suit nous allons présenter en détail les techniques basées sur la virtualisation de machines [9].

I.4.2.1 Cloisonnement

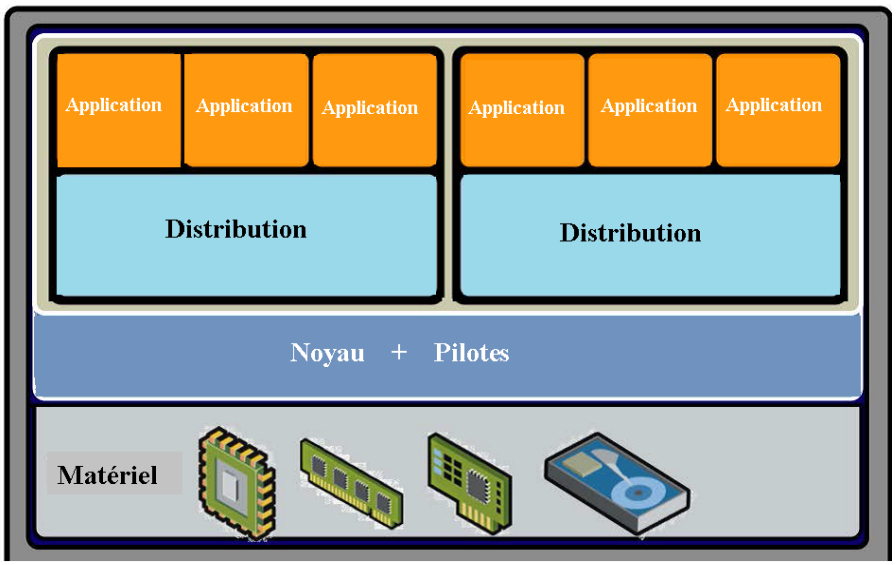


Figure I. 5 La technique du cloisonnement

Le cloisonnement est une technique de virtualisation très légère, se déploie au sein d'un même système d'exploitation. Pour cela on le divise en plusieurs espaces ou environnements, géré par le système d'exploitation hôte comme un processus isolé dans un conteneur partageant le même noyau. Il permet aux programmes de chaque contexte de communiquer seulement avec les processus et les ressources qui leur sont alloués. L'espace noyau fournit la virtualisation, l'isolement et la gestion des ressources. Ce partage du noyau limite cette technique aux environnements de mêmes types [9].

I.4.2.2 Virtualisation complète

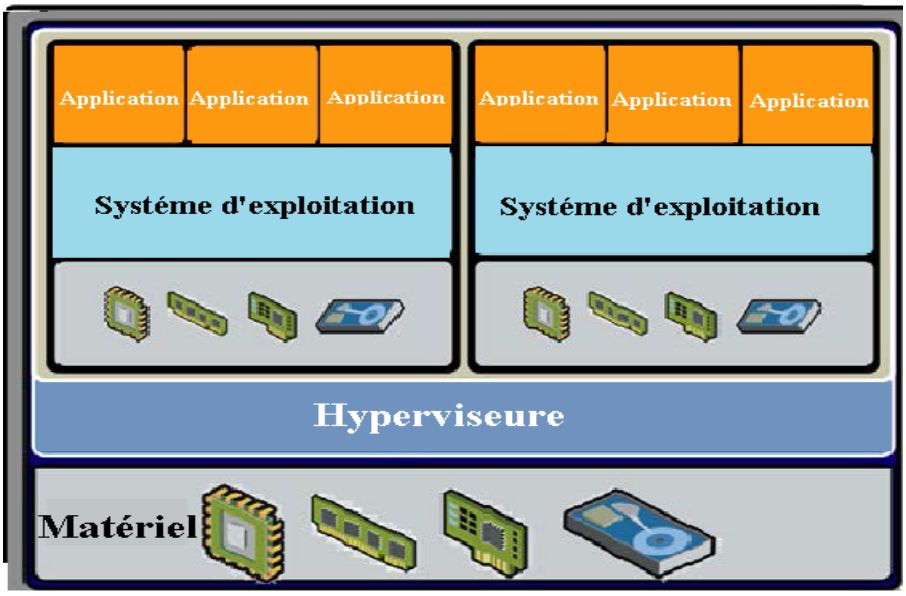


Figure I. 6 Schématisation de la virtualisation complète.

C'est une technique de virtualisation qui offre une réplique virtuelle du matériel du système de sorte que les systèmes d'exploitation et logiciels puissent fonctionner sur le matériel virtuel exactement comme sur le matériel d'origine, grâce à l'hyperviseur, au moment de l'exécution, les instructions du système d'exploitation invité ne donnent accès qu'au matériel virtuel présenté par ce dernier.

Afin d'offrir une meilleure isolation et plus de sécurité pour les machines virtuelles simplifiant ainsi la migration et la portabilité.

La figure I.6 illustre la création de deux machines virtuelles sur une seule machine physique tout en isolant les ressources. Les programmes qui s'exécutent sur l'espace utilisateur d'un système d'exploitation invité n'ont pas un accès direct au matériel, mais uniquement à la couche d'abstraction [9].

I.4.2.3 Para-Virtualisation

Semblable au concept de la virtualisation complète. Repose sur un hyperviseur pour gérer liaison avec les ressources physiques. A l'exception que la para-virtualisation permet une coopération entre l'hyperviseur et le système d'exploitation invité, lors de son exécution, l'hyperviseur capture les appels de ce dernier et les transmet au matériel.

L'hyperviseur gère l'interface qui va permettre à plusieurs systèmes d'exploitation invités d'accéder de manière concurrente aux ressources. Le système d'exploitation invité est conscient de l'exécution sur une machine virtuelle (VM). Cette opération nécessite des logicielles additionnel et pilotes non seulement au niveau du système d'exploitation hôte mais également au niveau du système d'exploitation invité [9].

La Figure I.7 schématise la technique de Para-virtualisation.

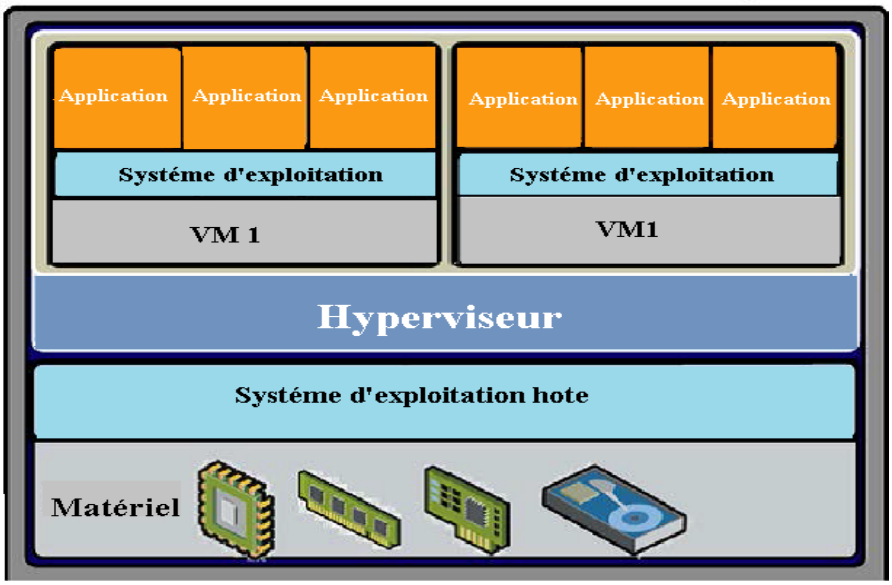


Figure I. 7 La technique de la para-virtualisation.

I.4.3 Virtualisation d'Application

C'est une technologie logicielle qui va permettre d'améliorer la portabilité et la compatibilité des applications en les isolants du système d'exploitation sur lequel elles sont exécutées [8].

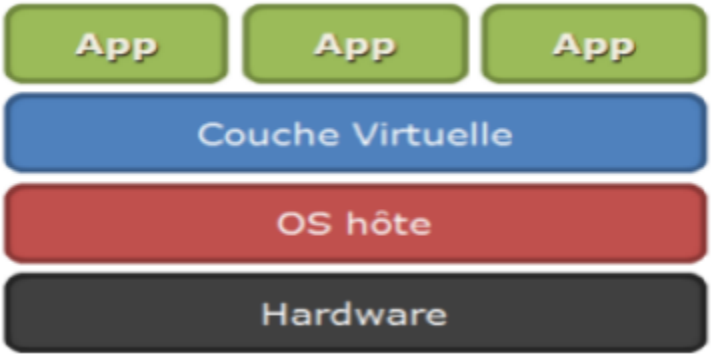


Figure I. 8 Virtualisation d'une application.

I.4.4 Virtualisation du Réseau

Elle consiste à partager une même infrastructure physique (débit des liens, interface physique) au profit de plusieurs entités logiques (VMs, routeur virtuels...) [8].

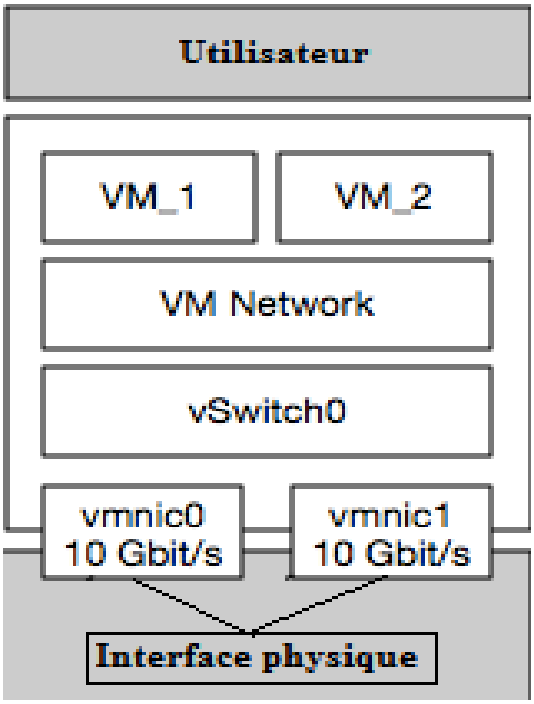


Figure I. 9 Virtualisation des réseaux

I.4.5 Virtualisation de Stockage

Son but est de faire abstraction des périphériques de stockage utilisés et des interfaces qui sont associés (SATA, SCSI,...) afin de limiter l'impact des modifications structurelles de l'architecture de stockage. Cette virtualisation nous permet d'avoir une flexibilité en termes de d'organisation logique (niveau applicatif) plutôt qu'une organisation physique [8].

I.4.6 Virtualisation des Unités de Calcul

Elle consiste à masquer les ressources du serveur, c'est à dire le nombre et les caractéristiques et la puissance des composants physiques (CPU, mémoire vive...). L'ensemble sera divisé en plusieurs environnements virtuels isolés les uns des autres pour faciliter la gestion [8].

I.4.7 Outils de Virtualisation: Les Hyperviseurs

L'hyperviseur, ou programme de contrôle, est un logiciel constitué de plusieurs fonctionnalités classés en deux types:

I.4.7.1 Hyperviseur type 1

C'est une couche qui s'interpose entre la couche matérielle et la couche logicielle (barre métal) et qui exploite directement les composants physiques de la machine, L'hyperviseur type 1 possède son propre noyau. Il pilote les systèmes d'exploitation à partir de la couche matérielle et

s'administre via une interface de gestion des machines virtuelles. Il s'exécute directement sur une plateforme matérielle donnée et implémente la plupart des services que fournissent les noyaux des systèmes d'exploitation comme le montre la figure I.9. Parmi ces hyperviseurs, on trouve VmWare vSphere (ESXi), Microsoft Hyper-V, XEN, KVM…. [8].

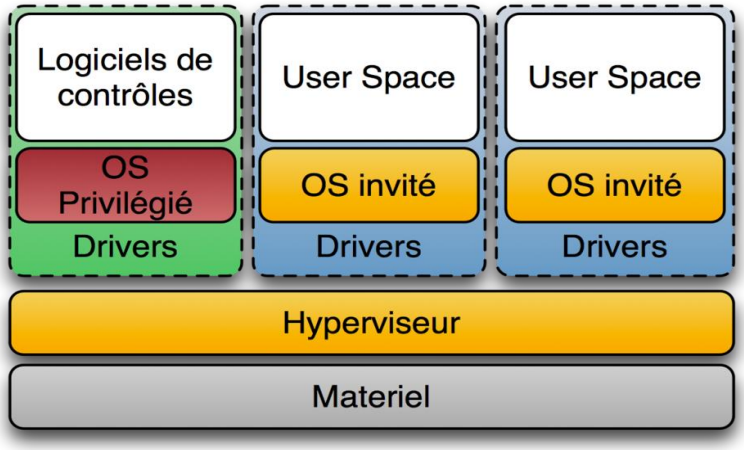


Figure I. 10 Hyperviseur type 1.

- VMware ESXi est un exemple d'hyperviseur de type 1, Ayant comme caractéristiques :

- Indépendant des systèmes d'exploitation.
- Repose lui-même sur le système d'exploitation VMkernel
- Assure l'interface avec les agents dont il soutient l'exécution.
- Est l'hyperviseur exclusif des licences VMware vSphere 5.x.
- Décrit le système ESXi comme similaire à un nœud informatique sans état.
- Système d'exploitation d'ESXi (VMkernel) assure directement l'interface avec les agents VMware et les modules tiers agréés.
- Les administrateurs chargés de la virtualisation peuvent configurer VMware ESXi via sa console ou le client VMware vSphere,
- La console permet de consulter la liste de compatibilité matérielle de VMware pour y trouver les équipements agréés et pris en charge sur lesquels installer ESXi [5].
- Successeur de la version VMware ESX.
- L'hyperviseur prend en charge la fonction de déploiement automatisé Auto Deploy, la création d'images personnalisées, ainsi que d'autres outils que n'intégrait pas ESX.
- Les détenteurs de licences ESX peuvent opter pour le déploiement d'ESXi au lieu d'ESX sur n'importe quel serveur [5].
- Une version gratuite allégée d'ESXi *(VMware vSphere Hypervisor)* prend en charge moins de fonctions.

I.4.7.2 Hyperviseur type 2

Comme représenté dans la figure I.11, c'est un logiciel qui s'exécute à l'intérieur d'un système d'exploitation, le système hôte. Les systèmes invités devront donc traverser deux couches logicielles avant d'accéder au matériel. Les performances s'en ressentent, mais la facilité d'installation et de configuration de ce type de système d virtualisation représente un grand avantage [8].

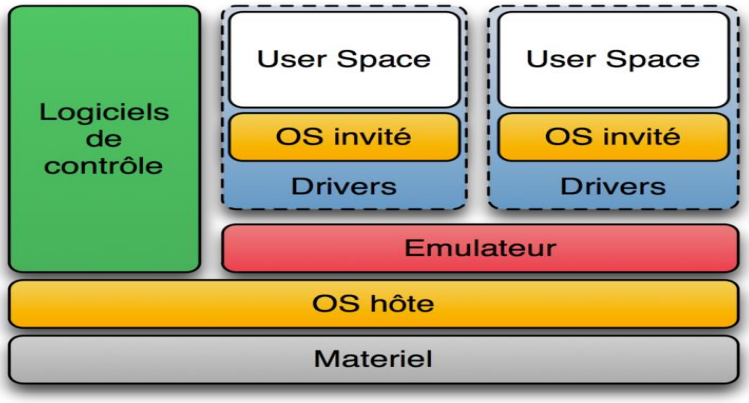


Figure I. 11 Hyperviseur type 2.

VmWare Workstation est un exemple d'hyperviseur de type2, Ayant comme caractéristique :

- Offre les avantages de plusieurs PC sans les coûts supplémentaires, la configuration physique et la maintenance.
- Exécute plusieurs systèmes d'exploitation et applications sur une machine virtuelle isolée et sécurisée.
- Un même PC peut alors héberger simultanément un grand nombre de machines virtuelles.
- Associe les ressources matérielles physiques aux ressources de la machine virtuelle. Ainsi, chaque machine virtuelle dispose d'un processeur, de mémoire, de disques, de périphériques d'E/S propres et autres.
- S'installe exactement comme un programme standard sur un PC Windows ou Linux.
- Accès en tout lieu et à tout moment à distance aux machines virtuelles exécutées sur la plate-forme VMware Workstation
- Partage des avantages de la virtualisation sous forme de serveur pour héberger des applications. Il s'agit du moyen le plus rapide pour héberger un serveur de fichiers ou d'impression existant ou partager une machine virtuelle avec un contrôle renforcé sur l'accès des utilisateurs.

- Réplication d'un environnement Web ou Cloud complet : VMware Workstation peut répliquer des clients, des navigateurs, des réseaux, des serveurs et des bases de données, le tout sur un seul PC.
- Mode de travail optimisé grâce à l'interface utilisateur ergonomique, remaniée avec des menus simplifiés.
- Intégration transparente des applications des machines virtuelles Windows et Linux donnant l'impression qu'elles s'exécutent sur le poste de travail natif [3].

I.5 Conclusion

Nous avons présenté, dans ce chapitre, les différents éléments de base d'une infrastructure hyper-convergée (infrastructure de Datacenter), et étudié chaque composant, afin de pouvoir déterminer l'ensemble des outils techniques permettant d'ajuster l'infrastructure au besoin spécifiques d'une entreprise. Ces notions nous permettent de trouver une solution à la fois simple, efficace, et moins couteuse qu'une infrastructure traditionnelle.

CHAPITRE II

Généralités sur les Réseaux Informatiques

II.1 **Introduction**

Il existe deux mondes coexistaient : Le monde des télécommunications, fermée, avec ses propres services et ses infrastructures, et le monde des informaticiens de l'internet, plus ouvert, avec une organisation décentralisée, mais souvent moins fiable. Aujourd'hui, devant la multitude des services (téléphonie IP, applications temps réel, visioconférence…) la tendance est à la convergence. Pour transporter des paquets d'un réseau à l'autre [10], mais surtout, assurer un débit plus important pour satisfaire l'expansion de ces applications réseau.

L'objectif de ce chapitre est de présenter quelques concepts de base sur les réseaux informatiques. Nous allons aussi illustrer quelques protocoles dans le cadre des réseaux informatiques. Ainsi, les nouveaux outils récemment développés, qui vise à promouvoir les infrastructures des systèmes informatiques, seront présentés.

II.2 **Le modèle OSI**

Le standard OSI *(Open Système Interconnect)* est le résultat du travail effectué au sein de l'Organisation internationale pour la normalisation (ISO). Le but d'OSI est de représenter en 7 couches abstraites [12], les différentes étapes par lesquelles les données doivent passer lorsqu'elles sont transportées d'un terminal à un autre dans un réseau [11]. Chaque couche regroupe un ensemble de protocoles de communication qui communiquent avec des couches inférieures et supérieures. De plus, les fonctionnalités de certaines couches sont liées dans le fonctionnement d'une couche inférieur à une couche supérieure à l'horizontale [12]. La figure suivante présente le modèle OSI en sept couches :

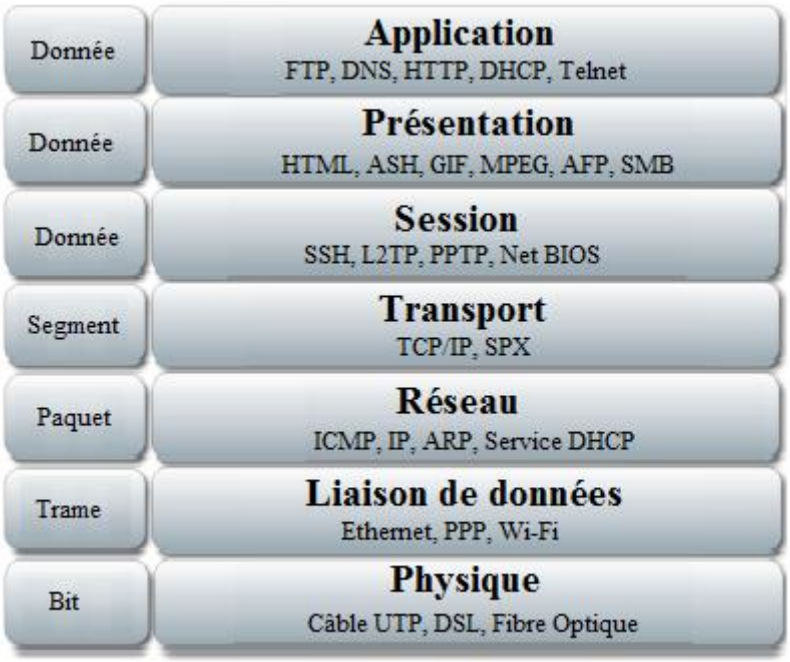


Figure II. 1 Le modèle OSI.

II.3 **Modèle TCP / IP**

Dans un effort pour standardiser l'ensemble des protocoles réseau, le TCP / IP *(Transmission Control Protocol/Internet Protocol)* a été développé. Il désigne communément une architecture réseau à quatre couches. Le modèle est créé en référence au modèle OSI à sept couches (figure II.9).La pile de protocoles est représentée en couches distinctes pour faciliter le remplacement d'un protocole par un autre. La suite de protocoles montre la manière dont les données sont manipulées au-dessus et en dessous de chaque protocole couche. Lors de la conception des protocoles, les spécifications définissent la maniéré avec laquelle l'information est traitée avec un protocole en couches au-dessus ou en dessous [13].

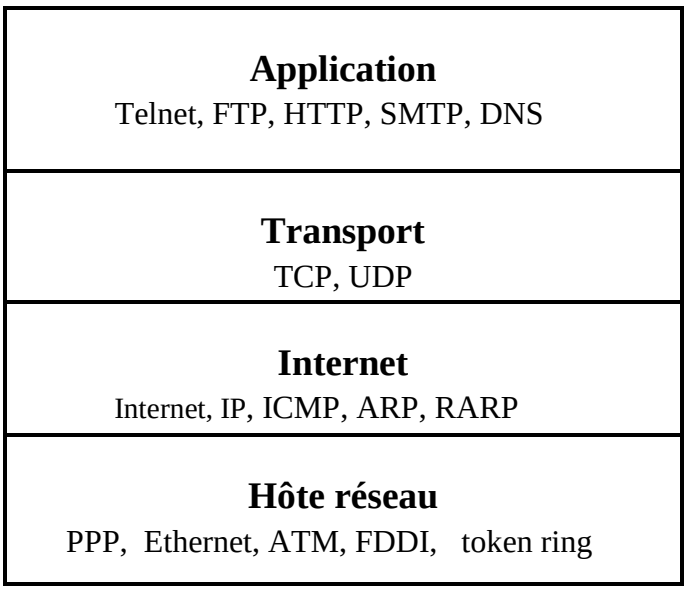


Figure II. 2 Suite de protocoles du modèle TCP/IP.

II.3.1 Hôte-réseau

Prend en charge la communication avec l'interface physique afin de transmettre ou de récupérer les paquets de données qui sont transmis de la couche internet. Le protocole est utilisé pour assurer cet interfaçage, n'est pas explicitement défini. Il dépend du réseau utilisé ainsi que du nœud (Ethernet en LAN, X25 en WAN, …).

II.3.2 Internet

S'occupe de l'acheminement, vers le hôte distant, des paquets de données indépendamment les uns des autres, soit de leur routage à travers les différents nœuds par rapport au trafic et à la congestion du réseau. Il n'est en revanche pas du ressort de cette couche de vérifier le bon routage.

Le protocole IP (Internet Protocol) assure intégralement les services de cette couche, et constitue donc l'un des points-clefs du modèle TCP/IP. Comme il définit les paramètres clef du paquet [15].

II.3.3 Transport

Gère le fractionnement et le réassemblage en paquets du flux de données à transmettre. Le routage ayant pour conséquence un arrivage des paquets non séquencés. Cette couche s'occupe aussi du réagencement ordonné de tous les paquets d'un même message.

Deux principaux protocoles pouvant assurer les services de cette couche :

- TCP *(Transmission Control Protocol)* : Est un protocole orienté connexion, fiable, assure une communication sans erreurs par un mécanisme question/réponse/confirmation/synchronisation.
- UDP *(User Datagram Protocol)* : Est un protocole sans connexion, non-fiable, assure

une communication rapide mais pouvant contenir des erreurs en utilisant un mécanisme question/réponse.

II.3.4 Application

Correspond aux différentes applications qui reposent sur les services réseaux pour communiquer à travers un réseau.

Un grand nombre de protocoles divers de haut niveau permettent d'assurer les services de cette couche :

- Telnet : Ouverture de session à distance ;
- FTP *(File Transfer Protocol)* : Protocole de transfert de fichiers;
- HTTP *(HyperText Transfer Protocol)* : Protocole de transfert de l'hypertexte ;
- SMTP *(Simple Mail Transfer Protocol)* : Protocole simple de transfert de courrier;
- DNS *(Domain Name System)* : Système de nom de domaine;

Le modèle TCP/IP correspond donc à une **pile de protocoles** représentés en différents niveaux, participant à l'établissement d'une communication via un réseau informatique.

II.4 Le protocole IP

Le protocole IP est un protocole réseau de niveau 3, ce protocole permet d'émettre (encapsuler) des paquets d'informations à travers le réseau, ainsi, il offre un service d'adressage (IPv4 et IPv6) unique pour l'ensemble des machines (terminaux), pour que ces dernières puissent dialoguer. Il n'est pas orienté connexion, c'est à dire qu'il n'est pas fiable [14].

II.5 Protocole MPLS

Le protocole *Multi Protocol Label Switching* (noté MPLS) a été développé par l'IETF pour rétablir une norme qui régit une manière de transporter des paquets IP sur des sous-réseaux fonctionnant en mode commuté. L'objectif est la mise en œuvre de la qualité de service dans le réseau à commutation de paquets.

MPLS se situe entre la couche de la liaison de données et la couche réseau du modèle OSI, d'où la nomination « multi-protocole » étant indépendant des protocoles de ces deux couches. La clé principale de l'MPLS est le découpage entre le routage (détermination des routes) et la propagation (détermination de la direction à suivre). MPLS change uniquement de la propagation. Le routage se fait par d'autres protocoles rependant à des contraintes spécifiques. Nous nous intéressons maintenant aux mécanismes nécessaires à la propagation. Nous supposons donc le chemin appelé LSPs dans le jargon MPLS et sur lesquels les données seront propagées et calculés [16].

L'établissement effectif de ces chemins est exécuté par des protocoles de distribution de labels. Au moment où les informations de routage sont exploitées. La propagation des données par MPLS sur ces LSPs est indépendante du routage. Dans cette section, nous présentons les deux principes clé sur lesquels se base MPLS qui sont la commutation des labels et les distributions de label [16].

II.5.1 Commutation de labels

L'MPLS remplace les mécanismes traditionnels de routage par des mécanismes plus rapide basés sur la commutation de label. En ce cas, les informations nécessaires pour acheminer une unité de donnes sont obtenues à l'aide d'une valeur dont l'application générique est étiquette ou label. Un contexte qui existe déjà dans les réseaux, où l'étiquette ou appelé *Data Link Connexion Identifier* (DLCI), dans les réseaux asynchrone, sous l'application *Virtual Path Identifier /Virtual Channel Identifier* (VPI/VCI). Il s'applique principalement au plan usage MPLS [16].

Le principe de base de l'MPLS est illustré sur la (figure II.3). Contrairement au routage IP qui est basé sur les adresses IP. En effet, tout paquet entrant dans le domaine MPLS via le routeur d'entré (Ingress router) se voit attribuer un label de taille fixe. A l'intérieur du domaine MPLS, un routeur MPLS, appelé *Label Switching Router* (noté LSR) examine de label entrant du paquet MPLS, examine la table de commutation MPLS et remplace ce label par label sortant .Quand le routeur quitte le domaine MPLS, le label est enlevé par le dernier routeur du domaine MPLS (*egress router*) .Les routeurs d'entée et de sortie dans un domaine MPLS portent le nom de Label Edge Router (noté LSR).

II.5.2 Distribution de labels

Afin d'utiliser les LSPs, les tables de commutation de chaque LSR doivent effectuer un lien du couple (interface d'entrée, label d'entée) vers le couple (interface de sortie, label de sortie) .Ce processus est appelé distribution de labels.

Le standard ne spécifie pas un protocole prévu pour la distribution des étiquettes entre LSRs. Au contraire, il recommande le recours à des protocoles de signalisation multiples. Cette propriété, conséquence directe de séparation du plan de contrôle et usager, est plutôt avantageuse. En outre, par rapport au plan usager, rien ne change si les tables de commutation ou été approvisionné manuellement ou résultante d'un établissement dynamique à l'aide des protocoles de signalisation conçus à cet objet.

Le protocole *Label Distribution Protocol* (noté LDP) est un protocole de signalisation (plus précisément de distribution de labels). C'est un protocole simple mais fortement limité, présente deux grandes limitations.

D'une part, le protocole n'a aucun moyen pour la spécification des paramètres de trafic permettant de formuler une demande de ressource à l'établissement d'une LSP. Aussi, les LSP établis en utilisant le protocole LDP sont contraints par le protocole de routage IGP.

Pour la réalisation d'une ingénierie de trafic efficace, l'architecture MPLS requière des protocoles de signalisation et de contrôle vérifiant un certain nombre de propriétés. Elles sont répertoriées comme suite [16] :

- établissement des LSPs sur une route explicite (liste de routeur à traverser), non contrainte par le protocole de routage .C'est à dire que les routes ne doivent pas forcement suivre le plus court chemin imposé par le protocole de routage suivant une métrique administrative.
- Possibilité d'une réservation de ressources au moyen d'objets d'informations capable de définir, au l'aide d'un nombre réduit de paramètres, les propriétés stochastiques du trafic.
- Prise en charge du mécanisme de restauration basée sur MPLS (*appelés en anglais MPLS based recovery*) avec une gestion de priorités à l'établissement et la modification des LSPs.

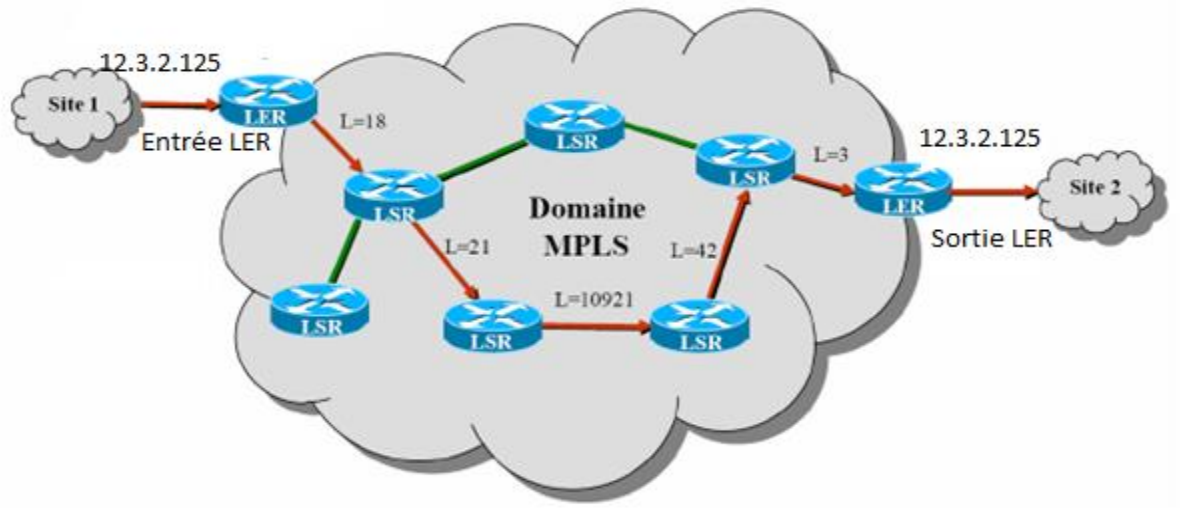


Figure II. 3 Exemple d'un réseau MPLS.

II.6 **Technologie xDSL**

La technologie xDSL vise à faire passer du haut débit sur la paire de cuivre utilisée pour les lignes RTC *(Réseau Téléphonique Commuté).* On distingue deux types de transmission xDSL. Un type à transmission symétrique et un autre a transmission asymétrique. Les types visent à exploiter les fréquences supra vocales qui ne sont pas utilisées par le téléphone. Cette technique requière l'installation d'équipements de communication spécifiques aux deux extrémités de la ligne RTC. Les trafics de l'ADSL et du téléphone passent par le même fil jusqu'à la centrale téléphonique, mais chaque trafic est indépendant de l'autre. Cette centrale, généralement appelée nœud de raccordement d'abonnés (NRA), filtre les basses fréquences, sur

lesquelles transite la voix, vers le RTC et les hautes fréquences, sur lesquelles transitent les données vers le réseau du FAI (Fournisseur d'Accès à Internet). Joue le rôle de répartiteur, qui tri les lignes des abonnés et les transfère vers les multiplexeurs d'accès DSL des FAIs correspondants à chaque ligne. Ce multiplexeur, appelé DSLAM (*Digital Subscriber Line Access Multiplexer*), L'équipement central auquel sont connectées les abonnés DSL. Il est composé d'un châssis sur lequel sont installées les cartes modem et les cartes filtres. Fait donc la liaison entre les lignes des abonnés et le réseau du FAI. Il gère les différents trafics. Ensuite, le DSLAM les envoie sur le réseau de fibre optique du fournisseur pour être acheminé vers son infrastructure. Le trafic de la voix est envoyé par la carte filtre vers le réseau commuté. Par contre celui de l'ADSL est envoyé vers la carte modem. Qui elle-même rassemble les flux numériques de chaque abonné et les fait converger par multiplexage temporel où les données sont enfin transportées en IP ou en ATM via une liaison haut débit vers le (BAS) Broadband Access Server (serveur d'authentification du client en charge de transmettre des paramètres IP). La figure II.4 illustre les différentes composantes et le fonctionnement de l'ADSL [9].

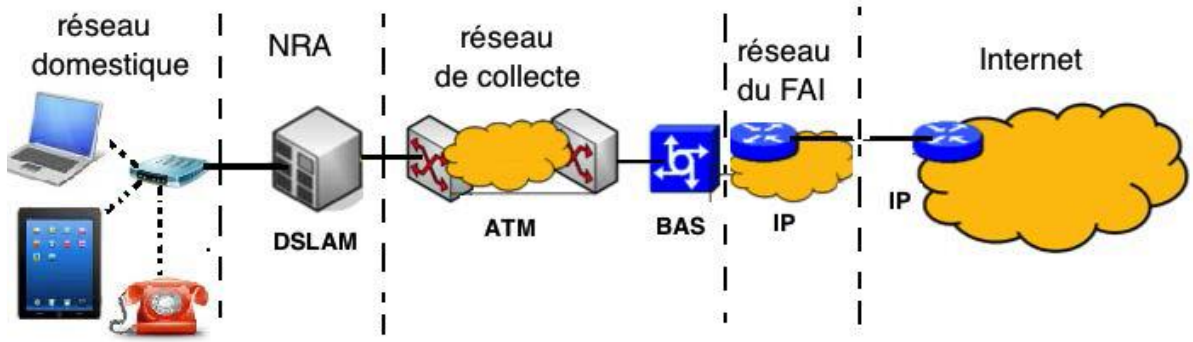


Figure II. 4 Fonctionnement de l'ADSL [9].

II.7 Les Réseaux Définie par Logiciel

Les réseaux Définie par Logiciel *(Software Defined Network SDN)* désignent un ensemble de techniques innovantes prévues pour contrôler et centraliser la gestion des ressources réseau, ainsi que la virtualisation de ces ressources. En les dissociant des éléments physiques du réseau, dans le but de simplifier et d'optimiser l'administration du réseau via la gestion centralisé par application, afin que la virtualisation est réalisé dans le domaine du réseau Ce qui signifie que les périphériques réseau (switch, routeur…) prennent leurs propres décisions pour trouver la meilleure façon d'orienter le trafic. S'appuyant sur les informations distribuées collectées par des protocoles de routage comme OSPF et BGP, mais ces protocoles reste peut flexibles. Pour fonctionner ensemble, tous les périphériques du réseau doivent suivre les règles régies par les standards [2].

Dans une architecture SDN, la séparation entre le plan de contrôle (qui définit comment un équipement achemine le trafic) et le plan de données (la partie des commutateurs et routeurs qui assure effectivement le mouvement des données) est claire. En outre, le plan de contrôle est placé dans un contrôleur centralisé qui a une visibilité sur l'ensemble des équipements connectés au réseau, y compris les machines (hôtes) ainsi que la visibilité sur la topologie de cet ensemble [2].

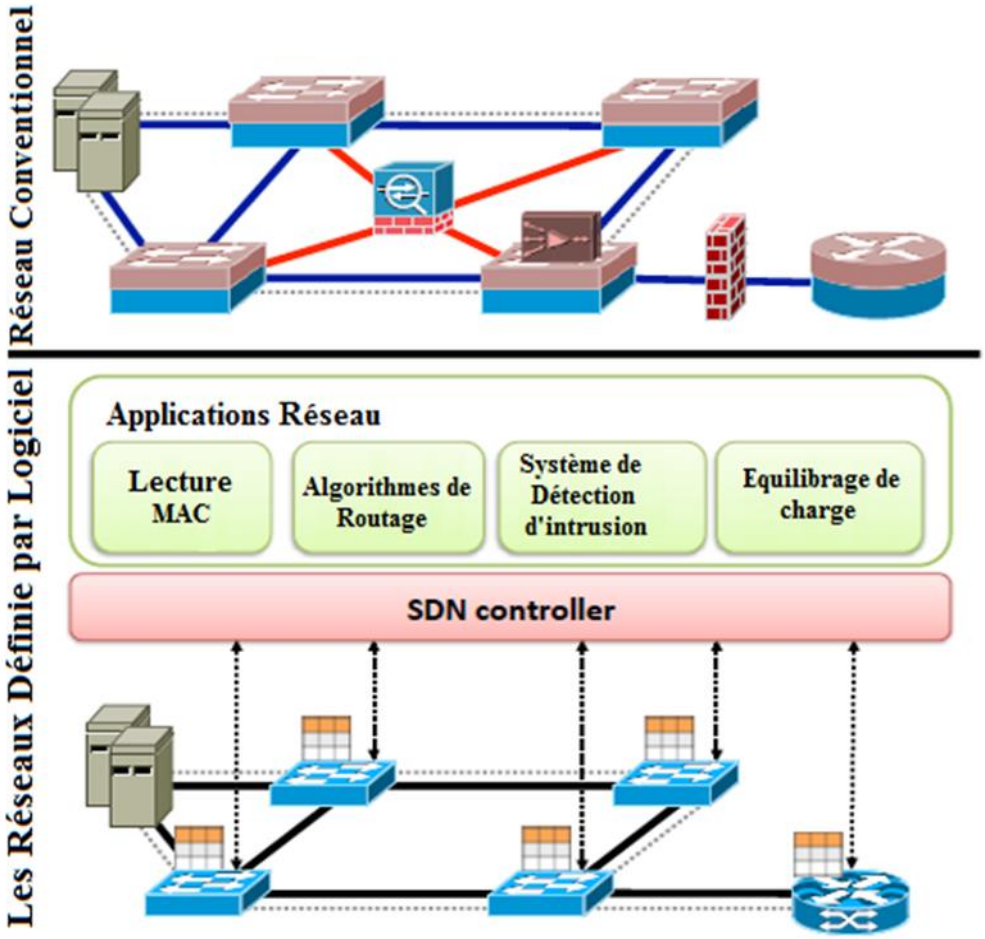


Figure II. 5 Mise en réseau traditionnelle et mise en réseau définie par logiciel (SDN) [18].

Cette approche a plusieurs avantages: Il devient plus facile à programmer les applications, à savoir, la possibilité de partager les ressources abstraite fournies par la plateforme de contrôle. Et donc, toutes les applications peuvent profiter du même réseau.

Ces applications peuvent prendre des décisions (c.-à-d., Reconfigurer des périphériques ou n'importe quelle partie du réseau). Là n'est donc pas nécessaire de concevoir une stratégie précise.

II.7.1 SD-WAN

Sert à répartir le trafic sur des réseaux étendus (WAN). S'appuyant sur les règles des réseaux contrôlés par logiciel (SDN), Consiste en une couche virtuelle indépendante de la couche transport vient en superposition : elle rend transparentes les connexions sous-jacentes du réseau étendu public ou privé, comme MPLS, ADSL, LTE,… Sans modifier les liaisons WAN existantes au sein de l'entreprise.

Le SD-WAN va utiliser les différentes liaisons, pour exploiter d'une manière optimale la bande passante de l'ensemble des accès WAN, en routant le trafic vers le meilleur itinéraire disponible entre le Datacenter et les différents sites distants ou vers internet.

Cette technologie SD-WAN centralise le contrôle du réseau et gère le trafic sur ces liaisons en temps réel et de façon flexible. Il est ainsi, pas nécessaire, voire inutile, de configurer manuellement des routeurs traditionnels sur les sites distants ayant la fonctionnalité SD-WAN configurée [2].

On distingue deux approches : Le réseau étendu programmable superposé ou le réseau à la demande. Avec une couche SD-WAN en superposition, Les constructeurs proposent des appareils dotés de logiciels nécessaires au fonctionnement de la technologie SD-WAN. Pour le déploiement, il ne reste plus au client qu'à connecter ses liaisons WAN à l'appareil, capable de lire la topologie du réseau et choisir les meilleurs paramètres [2].

Quand le SD-WAN prend la forme d'un réseau à la demande, le client a accès à ses propres réseaux privés via le FAI. Les fonctionnalités SD-WAN, telles que les méthodes de hiérarchisation du trafic ou d'optimisation du réseau étendu, sont intégrées au service.

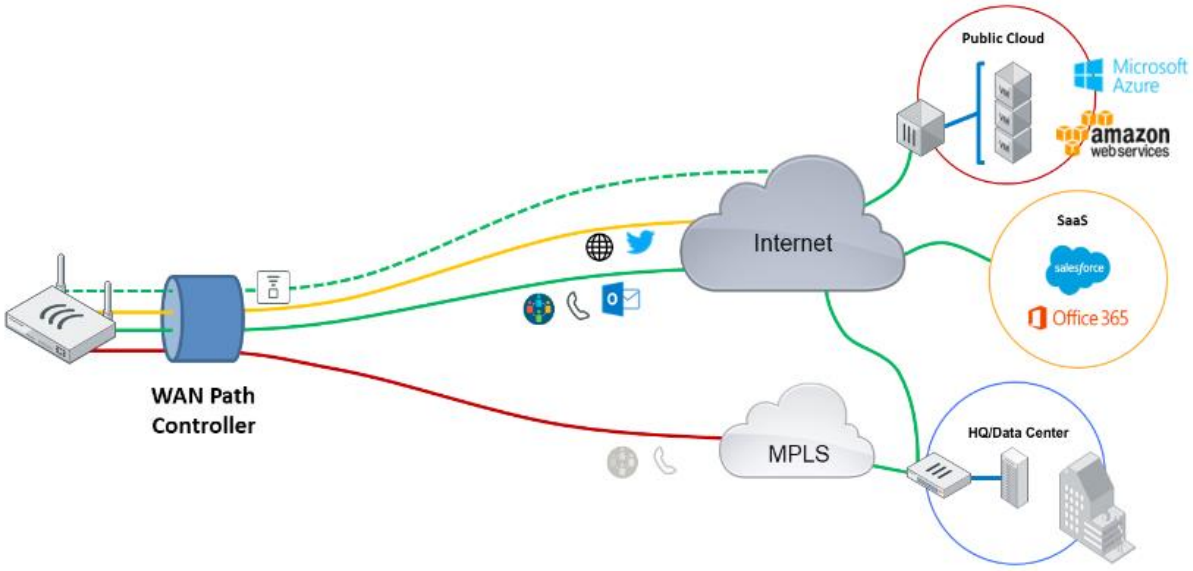


Figure II. 6 SD-WAN

II.7.1.1 Avantages du SD-WAN

Le SD-WAN bascule automatiquement le trafic vers une autre liaison en cas de défaillance ou de surcharge, d'où l'amélioration des performances des applications et la réduction de la latence [2]. Dans une architecture SD-WAN, les administrateurs peuvent réduire voire éliminer leur dépendance à la couteuse liaison spécialisée MPLS. A savoir, envoyer les données moins sensibles et de priorité plus faible sur des liaisons Internet publiques (ADSL) moins coûteuses, gardant ainsi les liaisons privées au trafic stratégique ou sensible à la latence comme la voix sur IP (VoIP).

SD-WAN étant une technologie flexible, permet de réduire le recours au sur provisioning et donc le coût global du réseau étendu.

En conclusion, le SD-WAN simplifie la gestion du réseau dont il automatise les déploiements et les configurations et optimise l'exploitation des ressources du réseau [2].

II.8 Les techniques de la Virtualisation des Réseaux

La virtualisation est une technique utilisée pour modifier les propriétés d'un service de réseau sans introduire de modifications au niveau matériel. Elle permet la coexistence de multiples réseaux hétérogènes dans une seule infrastructure.

Plusieurs techniques ont été utilisées pour créer des réseaux virtuels comme les VLANs *(Réseaux Locaux Virtuels)* et les VPNs *(Réseaux Privés Virtuels).* Récemment, les approches de virtualisation des serveurs ont été utilisées pour créer des routeurs et des liens virtuels sur des équipements physiques et des canaux de communication [9].

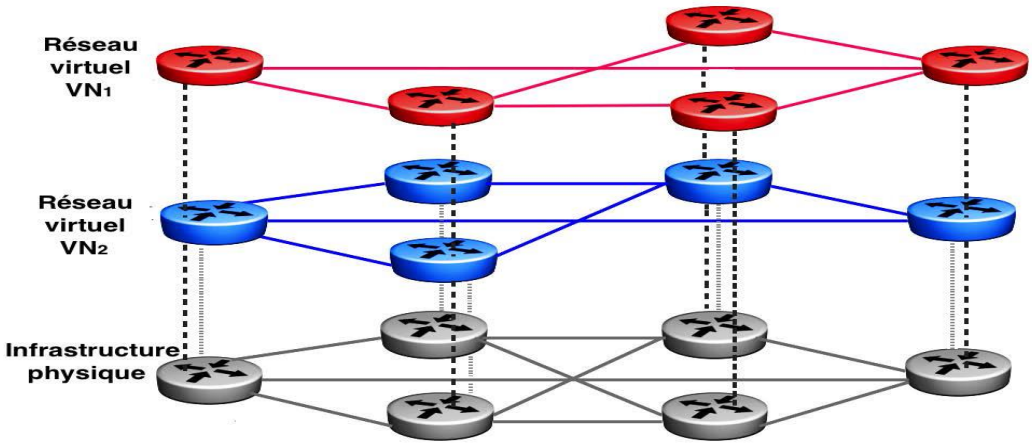


Figure II. 7 Schéma d'une architecture de réseau virtualisé [9].

II.8.1 Les Réseaux Locaux Virtuels

Un VLAN est l'interconnexion de plusieurs hôtes, de façon logique et non physique de leur connectivité physique. D'une maniéré à créer des domaines de diffusion gérés logiquement a l'instar de l'emplacement géographique de ses hôtes.

Plusieurs VLANs peuvent coexister sur un même switch réseau, et ils peuvent être locaux (sur un même switch) ou s'étendre sur un ensemble de switch interconnectés. L'objectif est de contourner les limitations de d'aspect physique. Ce qui améliore la gestion du réseau et d'optimise la bande passante en séparant le trafic de chaque groupe d'hôtes (machines).

Chaque trame possède un identifiant du VLAN dans l'en-tête de contrôle d'accès au support (*Media Access Control*, (MAC)). Les réseaux locaux virtuels fonctionnent au niveau des couches liaison de données du modèle OSI. Régit par la norme IEEE 802.1Q.

La figure II.8 illustre le regroupement de plusieurs hôtes connectés en VLANs indépendamment de leur connectivité physique [9].

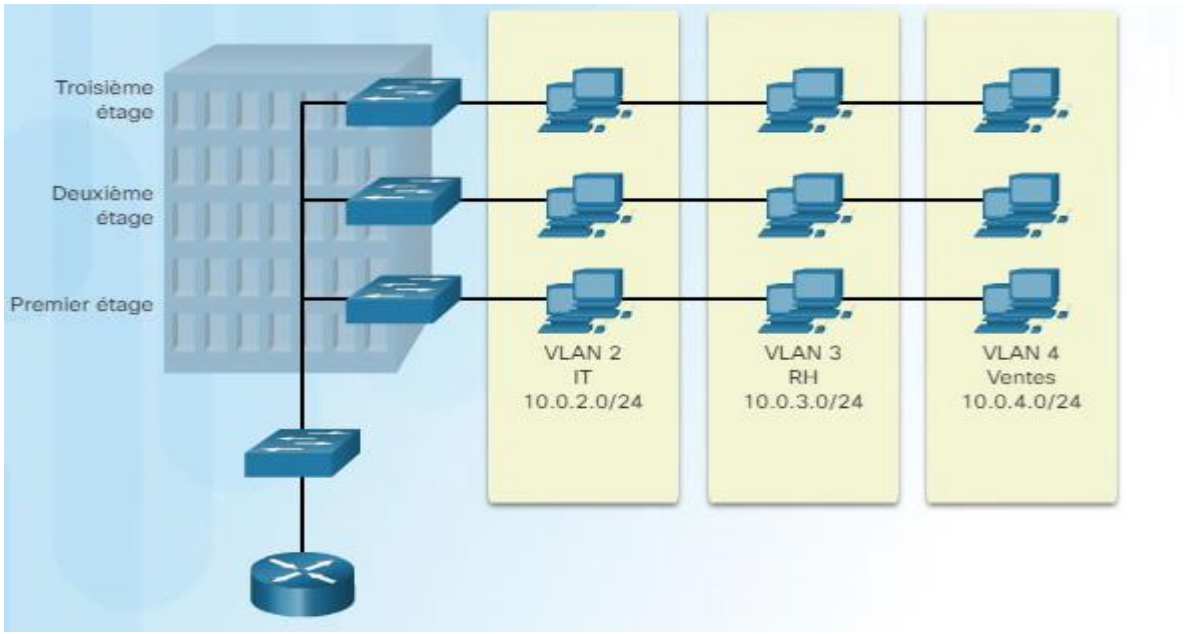


Figure II. 8 Regroupement des PCs en VLANs [9].

II.9 Conclusion

Dans ce chapitre nous avons présentés les notions et les concepts de base concernant les réseaux informatiques. Ces derniers évoluent constamment et prennent de plus en plus de place dans le milieu d'entreprise. Leur évolution les rend indispensable par le billet de nouvelles techniques telles que la virtualisation et les réseaux contrôlés par logiciels. Les entreprises adoptent ces nouvelles techniques dans un cadre de modernisation du system d'information.

CHAPITRE III

Sécurité des systèmes informatiques

III.1 Introduction

Tout système informatique présente des failles et des vulnérabilités, que certains utilisateurs mal intentionnés peuvent exploiter pour accéder à des informations, les lires, les modifier, voire même les détruire. Notamment, les systèmes informatiques d'entreprise dont les bases de données sont de différents niveaux de confidentialité et accessible pour des utilisateurs de différents niveaux d'habilité, utilisant pour la plupart des accès publics tels qu'internet, pour accéder aux ressources et bases de données, default du coût élevé des lignes spécialisées.

Dans ce chapitre, nous présentons le concept de la sécurité des systèmes informatiques, des exemples de menaces et de risques liés à ces derniers. La sélection de contre-mesures et des mécanismes de sécurité seront présentés.

III.2 **Définition**

La sécurité informatique est l'ensemble des moyens techniques déployés pour éliminer à l'aumône la vulnérabilité d'un système, pour faire face à des éventuelles menaces accidentelles ou intentionnelles. L'objectif de la sécurité informatique est donc, d'assurer que les ressources matérielles et/ou logicielles d'un parc informatique sont uniquement utilisées dans le cadre prévu et par des personnes autorisées [19].

III.3 **Les principes de la sécurité informatique**

Elle repose sur trois principes essentiels: la confidentialité, l'intégrité, disponibilité,… Certains principes sont plus importants que d'autre, selon le contexte d'utilisation. Par exemple, la confidentialité est la plus importante dans le cadre d'une transmission entre des organisations telles que les banques, vue la sensibilité des données échangées. Par contre, la disponibilité est la plus importante pour les sites e-commerce, ou les entreprises à caractère industriel et/ou commercial, ou l'interruption du service peuvent causer des pertes économiques importantes [20]. On donne quelques définitions :

- **La confidentialité:** La confidentialité consiste à préserver la divulgation sans autorisation d'informations sensibles. Une action qui pourrait être volontaire (attaque visant à exploiter une faille de sécurité, décryptage des données..), ou involontaire dû à l'incompétence des utilisateurs qui manient les informations.
- **L'intégrité :** L'intégrité consiste à garantir trois principaux buts :
  - Préserver la modification des informations par les utilisateurs non authentifiés.
  - Préserver la modification non autorisé ou involontaire d'informations par les utilisateurs authentifiés.
  - Préserver la cohérence des données
  - Faire en sorte qu'aucun utilisateur ne puisse empêcher une modification légitime apportée à l'information.
- **La disponibilité:** Garantie l'accès ininterrompu des utilisateurs authentifiés a l'information.
- **L'authentification :** L'authentification est le contrôle d'accès, qui détermine les utilisateurs autorisés à accéder aux informations, grâce à de simples moyens, basés sur les noms d'utilisateurs et les mots de passe lors du contrôle d'accès.
- **Le non répudiation :** Cette propriété garantie qu'un utilisateur ayant réalisé une action dans le système ne puisse nier l'avoir réalisée. Permet d'assurer que les extrémités d'une transmission (émetteur et récepteur) sont bien les seules personnes autorisées à envoyer ou réceptionner les informations sans aucune remise en cause, cette vérification s'effectue

grâce à un certificat numérique qui assure l'identité de l'émetteur et le récepteur. Les certificats eux-mêmes sont protégés par le moyen des signatures des utilisateurs. Dans certains cas la signature d'un utilisateur est son identité [20].

III.4 Menaces liés aux systèmes informatiques

Les systèmes informatiques sont confrontés à une multitude d'attaques, qui visent à modifier le comportement d'un SI. À travers diverses actions ou manipulations, des logiciels malicieux visant à compromettre le système. Une fois que l'intrus s'introduit dans ce dernier, il entreprend des actions, profitant des vulnérabilités, pour pérenniser son accès à l'insu des utilisateurs légitimes. Les vulnérabilités que nous allons évoquer, constituent une brèche favorisant l'accès illégitime aux informations [19].

III.4.1 Attaque de déni de service distribué (DDoS)

Le but de cette attaque est que la victime n'arrive pas à isoler les attaquants vu le nombre important des machines utilisées pour réaliser cette attaque. Pour réaliser cette attaque, il faut premièrement pénétrer par diverses méthodes des systèmes dits "zombies" que l'attaquant contrôle, qui eux même contrôlent un ensemble de systèmes agents. L'attaquant lance l'attaque en ordonnant les systèmes "zombies", qui eux-mêmes ordonnent les agents, d'envoyer des requêtes vers la machine victime, afin de mette cette dernière hors service Le schéma suivant illustre le fonctionnement de l'attaque DDoS (Voir Figure III.1) [21].

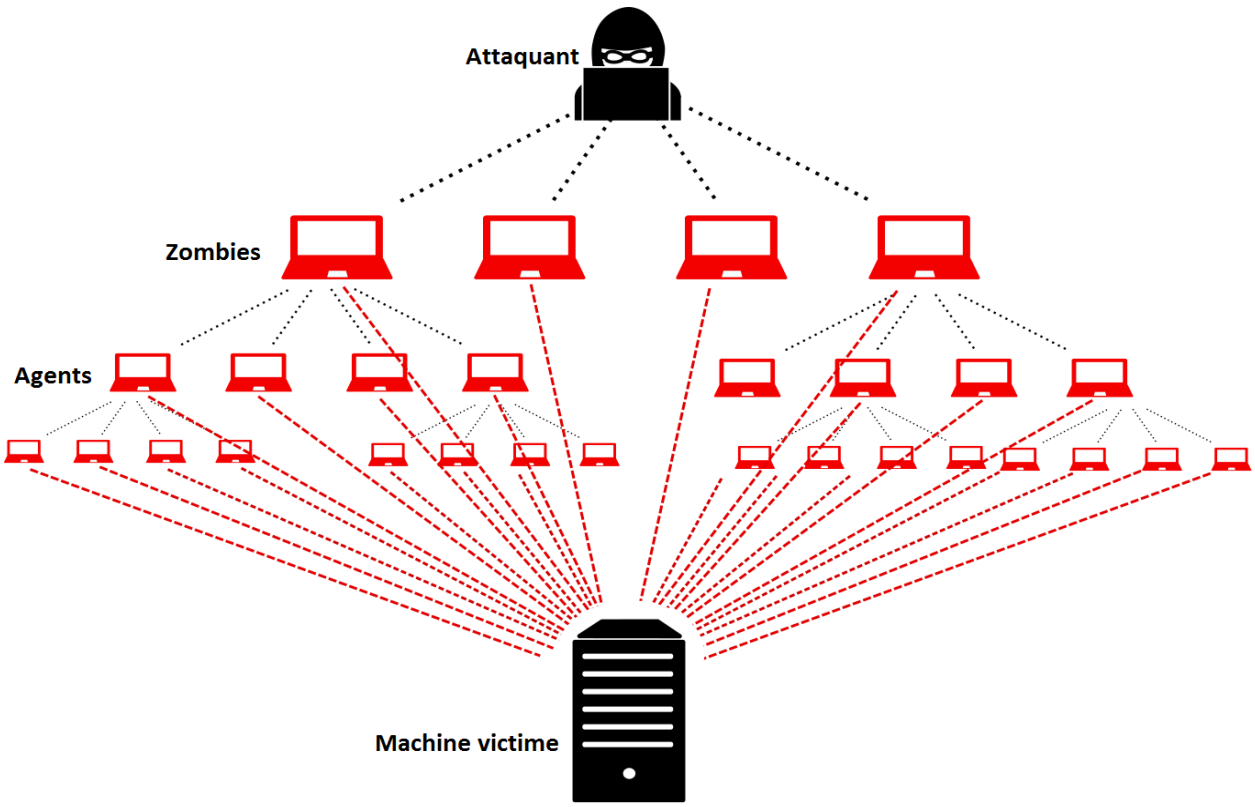


Figure III. 1 L'attaque DDoS.

III.4.2 Empoisonnement du cache ARP

La mystification ARP, particulièrement utilisable sur les réseaux Ethernet LAN, utilisant le protocole TCP/IP. Cette attaque est basée sur l'accouplement d'une adresse IP avec une adresse MAC non correspondante, pour que la victime soit redirigée vers une autre machine [22].

III.4.3 Injection SQL

Les injections SQL sont des vulnérabilités permettant d'exécuter des commandes non illégitimes. Cette attaque exploite une faille de sécurité d'une application web tous en injectant une requête SQL malicieuse pouvant compromettre sa sécurité [22].

III.4.4 Attaque de pirate au milieu

Plus connue sous le nom de « Man in the middle » cette attaque permet d'être une tierce partie entre deux stations communiquant dans le but de détourner le trafic réseau. Après le détournement, les données peuvent être modifiés, endommagées ou justement lises. Cette attaque même transparente pour les clients [22].

III.4.5 Attaque par logiciel malveillant

Parmi les multiples procédés d'attaque contre les systèmes informatiques, il convient de réserver une attention spéciale aux logiciels malveillants (programme développé dans le but de nuire à un système informatique) qui se répandent en général par le réseau, soit par accès direct à l'ordinateur attaqué, soit cachés dans un courriel ou un site Web [23].

De nos jours, le terme « virus » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les malicieux englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces. La catégorie des virus informatiques, qui a longtemps été la plus répandue, a cédé sa place aux chevaux de Troie en 2005 [19].

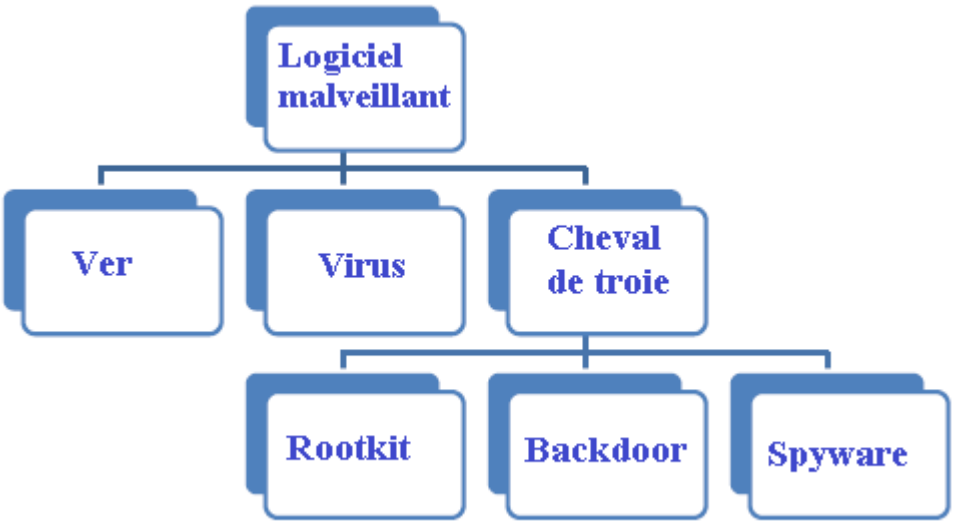


Figure III. 2 Logiciel malveillant.

III.4.5.1 virus

Un virus informatique est tout programme capable de s'auto-reproduire, c'est le type d'attaque le plus courant. Il peut prendre la forme d'une routine ou d'un programme une fois activé il utilise tous les moyens pour empoisonner le système. Plusieurs types de virus peuvent être cités [21]:

- Virus de secteur d'amorçage.
- Virus d'infection des fichiers (parasites).
- Virus non-résidents mémoire.
- Virus résidents mémoire.
- Virus polymorphes (mutants).
- Bombes logiques.

III.4.5.2 Ver

Un ver *(Worm)* est une variété de virus qui se propage par le réseau. Il peut s'agir d'un bot. Il y a cinq ou six ans les virus n'étaient pas des vers (ils ne se propageaient pas par le réseau) et les vers n'étaient pas des virus (ils ne se reproduisaient pas). Aujourd'hui la confusion entre les deux catégories est presque totale [23].

III.4.5.3 Le cheval de Troie (Trojan horse en anglais)

Est un type de logiciel malveillant, qui ne doit pas être confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient un programme malveillant. Son rôle est de faire entrer ce parasite sur l'ordinateur et de l'installer à l'insu de l'utilisateur [19].

Les ROOTKITS : Aussi appelé « *outil de dissimulation d'activité* », ou « *maliciel furtif* », Est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir un accès (généralement non autorisé) à un hôte, de la manière la plus discrète possible. Le terme peut désigner un ensemble particulier d'outils informatiques mettant en œuvre cette technique pour l'« *attaquant* », Soit de mettre à disposition des ressources système (processeur, connexions réseaux, etc.) sur une ou plusieurs machines, parfois en utilisant un « hôte cible » comme intermédiaire pour une autre attaque ; soit d'espionner, d'accéder aux données stockées ou en transitant sur la hôte cible. Les rootkits généralement classés parmi les logiciels malveillants, mais pas toujours ; ils peuvent utiliser des «*techniques virales* » pour se transmettre (par exemple, en utilisant un virus ou un cheval de Troie) [19].

III.5 La politique de sécurité

Une politique de sécurité fait référence à l'ensemble des outils et contre-mesures sélectionnées pour la mise en œuvre, afin de remédier à l'ensemble des menaces à lesquelles est exposé le système informatique, sans elle, la stratégie de sécurité est susceptible d'avoir un désordre de contre-mesures.

Une bonne politique est toujours adaptée aux menaces, car elle devrait préciser qui est responsable de quoi (mise en œuvre, exécution, vérification, examen), la nature de cette politique de sécurité du réseau et pourquoi elle est de cette nature. La réponse à ces questions est très importante parce qu'une politique claire, concise, cohérente et constante est plus susceptible d'être suivie. Décrit donc les besoins en outils à utiliser, et la maniéré de les déployer. Par exemple : Est-il nécessaire de mette en place un pare-feu ? Qu'elle est la configuration adéquate pour permettre l'accès de tel groupe d'utilisateurs à internet et interdire tel groupe?....Sans la politique de sécurité, il né pas possible de rependre systématiquement aux questions qui cerne le besoin en sécurité [20].

III.6 Outils de défense informatique

Afin de remédier, aux différentes attaques informatiques cité auparavant, ou au moins réduire leurs risque, différents moyens peuvent être utilisés, parmi ces systèmes on peut citer:

III.6.1 Pare-feu

Est un dispositif dont le rôle est de bloquer tout trafic non autorisé entre deux réseaux, un réseau de confiance tel que le réseau local, et un réseau public (suspect), tel qu'internet. Un firewall permet aussi, d'isoler des sous-réseaux internes nécessitant des critères de sécurité déférents comme, par exemple, un sous-réseau de développement, un sous-réseau de teste et le sous-réseau de production [24].

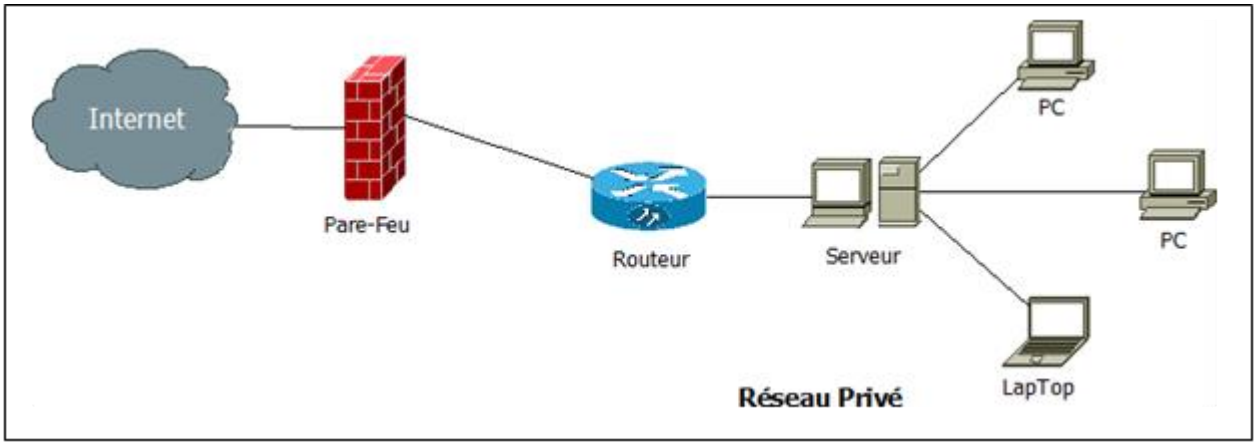


Figure III. 3 Exemple d'un pare-feu installé entre un réseau privé et Internet [25].

Selon le type de service de sécurité offert pour chaque service dans le modèle TCP/IP, les pare-feu peuvent être divisés en quatre types qui sont:

- Pare-feu de la couche application: offre des services tels que le cryptage, et la passerelle niveau application.
- Pare-feu de la couche transport : offre principalement la fonctionnalité de filtrage de paquets TCP, UDP (*User Datagram Protocol*), ICMP (*Internet Control Message Protocol*).
- Pare-feu de la couche réseau: Offre la fonctionnalité de filtrage NAT (*Network Adressa Translation*) et IP.
- Pare-feu de la couche liaison de données: offre la fonctionnalité de filtrage des adresses MAC (*Media Access Control*) [25].

III.3.4.2 Les Antivirus

L'antivirus sont des programmes prévus pour détecter la présence de virus sur un système d'exploitation, ainsi que de les mette en quarantaine « les isoler » ou les neutraliser, sans endommager les fichiers infectés. Mais parfois, ce nettoyage simple n'est pas possible [26].

Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement du système d'exploitation [19].

Il est intéressant de noter qu'une fois un fichier infecté, il ne l'est jamais deux fois. En effet, un virus est programmé de telle sorte qu'il signe le fichier dès qu'il est contaminé. On parle ainsi de signature de virus. Cette signature consiste en une suite de bits apposée au fichier. Cette suite, une fois décelée, permettra de reconnaitre le virus. Lorsque le virus est détecté par l'antivirus, plusieurs possibilités sont offertes pour l'éradiquer :

- Supprimer le fichier infecté ;
- Supprimer le code malicieux du fichier infecté ;
- Le placer en "quarantaine" pour un traitement futur [19].

III.6.2 VPN

Les VPN *(Virtual Private Network),* ou réseaux privés virtuels, peuvent être définis comme un ensemble de ressources susceptibles d'être partagées par des flots de paquets ou de trames provenant de machines autorisées. Les VPN peuvent utiliser des technologies et des protocoles quelconques. La gestion de ces ressources nécessite un haut niveau d'automatisation pour obtenir la dynamique nécessaire au fonctionnement d'un VPN. Pour obtenir cette dynamique, les ressources permettant d'acheminer les paquets au destinataire doivent être gérés avec efficacité, utilisant des outils d'authentification et des systèmes cryptographiques, afin d'acheminer des paquets d'informations, à savoir sensibles, via des réseaux généralement publiques [17].

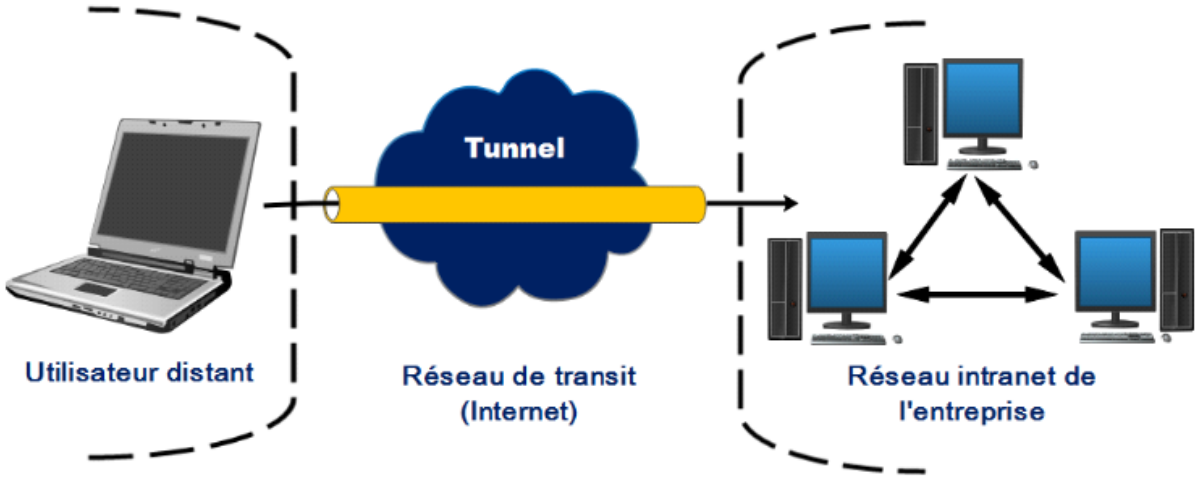


Figure III. 4 Exemple de VPN *(Ghost Warrior).*

III.7 Les techniques de sécurité

La mise en œuvre d'une politique de sécurité consiste à déployer un ensemble d'outils et de dispositifs, visant à sécuriser un système informatique, ainsi qu'à l'application des règles définis par une organisation quelconque. Ce qui signifie, faire le bon choix de l'ensemble des mécanismes et des techniques les plus simples a déployé, permettant de protéger et préserver les ressources du système informatique, de la manière la plus efficace, avec un faible coût. Il existe différentes techniques utilisées contre les attaques informatiques, ces techniques sont classées comme suite [21]:

III.7.1 La sécurisation des accès réseau

La protection des accès réseau consiste à maîtriser les flux réseau à l'aide des pare-feu et assurer un niveau de confidentialité des données grâce aux protocoles de cryptographie tel que l'IPSec.

III.7.1.1 Superviser les connexions réseau

La vérification du trafic réseau consiste à ne laisser passer que les connexions autorisées. L'objectif de ce contrôle est de créer un périmètre de sécurité, limiter le nombre de points d'accès pour faciliter la gestion de la sécurité, et disposer de trace des systèmes en cas d'incident de sécurité. Nous citons certains dispositifs de contrôle et de filtrage de connexion [20] :

- Le pare-feu : (voire **III.5.1**).
- Contrôle de l'accès réseau : un nouveau concept développé par Cisco, consiste à contrôler les accès les plus près à leurs sources, il permet de vérifier un système avant que celui-ci soit autorisé à se connecter au réseau local [20].

III.7.1.2 Assurer la confidentialité des connexions

La confidentialité des données au sein d'un réseau informatique est assurée par l'utilisation du cryptage des données, avant leur envoi et un décryptage à leur réception. Le schéma suivant montre où intervient le chiffrement dans une architecture de communication TCP/IP [21].

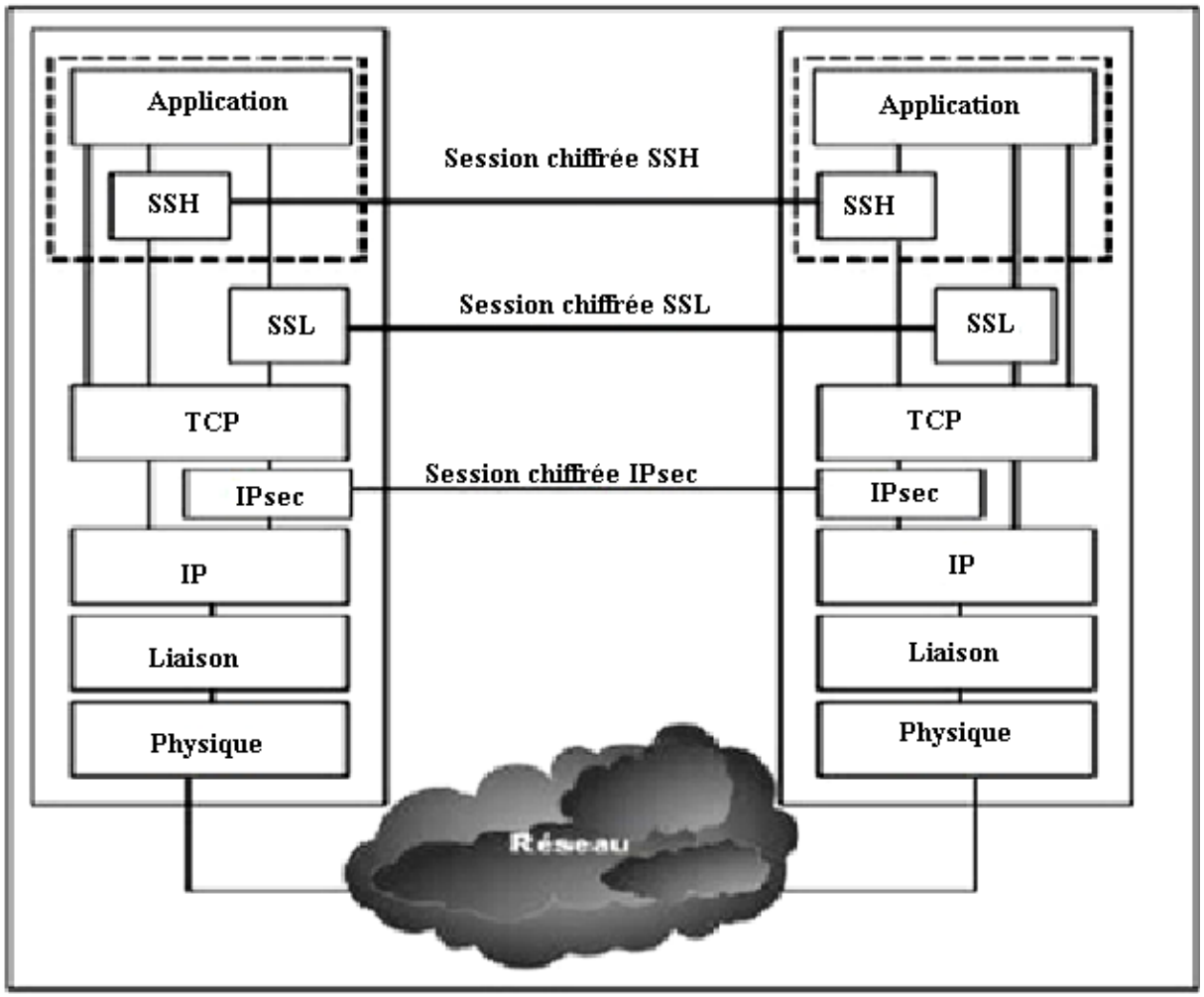


Figure III. 5 La représentation en couches des protocoles de sécurité.

- **Les algorithmes cryptographiques**

La cryptographie est l'une des disciplines de la cryptologie, qui consiste en la conception d'algorithmes, protocoles, et de systèmes pour la protection de l'information contre des menaces spécifiques. En effet, l'action de crypter une information signifie la modifier d'une telle manière à ce qu'elle ne soit comprise que par les personnes ayant en possession la clé du cryptage/dd̂écryptage [25].

- Les algorithmes cryptographiques à clé secrète ou symétrique qui se basent sur une même clé qui chiffre et déchiffre. Cette clé est partagée par les deux communicants.
- Les algorithmes cryptographiques à clé publique ou asymétrique qui se basent sur une clé publique de chiffrement et une clé secrète de déchiffrement.

Il existe aussi les algorithmes de hachage qui nous permettent d'obtenir une signature numérique à partir des données comme :

- IPSec : Créé pour corriger les problèmes d'authentification et de confidentialité du protocole IP. IPSec opère au niveau IP, son fonctionnement consiste en l'encapsulation des paquets des protocoles (TCP, UDP, ICMP, etc.). IPSec offre des services de contrôle d'accès, d'intégrité, d'authentification, de confidentialité, fait aussi face aux attaques de type paquets Relay.

- SSL *(Secure Sockets Layer)* : Opère au-dessus de la couche TCP interagis avec les navigateurs internet, en leur offrant la possibilité d'établir des sessions chiffrées et authentifiées. Le protocole SSL a été standardisé par le groupe de travail TLS (Transport Layer Security) formé au sein de l'IETF.

- SSH *(Secure Shell)* : Il opère au niveau application et permet d'obtenir un interprète des commandes (Shell) à distance sécurisés.

III.7.2 La protection des accès distants

L'accès distant au réseau d'une organisation offre plusieurs avantages, par ailleurs, le risque de pénétration est en ce cas optimal, et les failles des protocoles sont bien exploitées. Afin d'assurer la protection des accès distants, on doit assurer l'authentification des connexions distantes, le contrôle des accès physiques à un réseau local, le contrôle des accès distants classiques, le contrôle des accès distants WI-FI.

III.7.2.1 Assurer l'authentification des connexions distantes

L'authentification vise à garantir une protection contre toute sorte d'attaques, dont le but est l'usurpation d'identité d'un utilisateur légitime, tel que les attaques IP spoofing, les attaques visant à dérober les mots de passe, les attaques par cheval de Troie… etc. on distingue plusieurs outils qui offrent le service d'authentification, nous citons ici quelques-uns :

- **Le mot de passe :** Est un mot ou une série de caractères définis comme le moyen d'authentification le plus simple et le plus utilisé, pour prouver l'identité d'une personne légitime lorsque l'on désire accéder à une entité protégée, à une ressource ou à un service dont l'accès est limité [23]. Les faiblesses liées aux mots de passe viennent généralement des failles de protocoles d'accès, qui ne les chiffrent pas avant de les envoyer à travers le réseau, comme le Telnet. En second lieu, on trouve les faiblesses dues à la simplicité des mots de passe comme la suite simple 1234, les dates de naissance, les prénoms …etc, facile à deviner [20].
- **Le Token RSA** : Il se base sur la technologie des tickets ou des mots de passe a durée d'utilisation limitée (quelques dizaines de seconds). Au début l'utilisateur se sert d'un

authentifiant (le jeton ou carte à puce) plus un code PIN secret. L'authentifiant génère des codes d'identification aléatoires toutes les soixante secondes. L'identification de l'utilisateur est garantie par la combinaison du code PIN, l'authentifiant et le code aléatoire.

- **Le certificat électronique:** Il assure l'identité électronique d'un utilisateur ou d'un système. Il se base sur les infrastructures PKI *(Public Key Infrastructure).*
- **La paire de clés PGP *(Pretty Good Privacy):*** Elle offre des services de confidentialité et d'authentification pour la messagerie électronique et les supports de stockage des données. La certification des clés privées/publiques crées, sont pas standardisées. Contrairement à PKI chaque utilisateur possède une ou plusieurs paires de clés privées/publiques. Il communique les clés publiques aux personnes avec lesquelles il veut communiquer.

III.7.2.2 Assurer le contrôle des accès physiques à un réseau local

Le protocole IEEE 802.1X est un standard doté d'un mécanisme d'autorisation d'accès physique à un réseau local après authentification. Les dispositifs qui interviennent dans un tel mécanisme sont le système à authentifier, le point d'accès au réseau local (commutateur, routeur, etc.) et le serveur d'authentification [20].

III.7.2.3 Assurer le contrôle des accès WI-FI

La norme 802.11 a défini le protocole WEP *(Wired Equivalent Privacy)* pour assurer confidentialité et l'intégrité des données. Par contre, ce protocole possède des faiblesses de sécurité, la clé "maître" utilisée pour le chiffrement des données est trop petite pour assurer la complexité requise, la petite taille et la prédictibilité du vecteur d'initialisation. Pour remédier à ce problème, de nombreuses améliorations ont été proposées afin de renforcer la sécurité de ces accès, comme le WPA *(Wi-Fi Protected Access)* qui intègre des fonctionnalités comme :

- Le mécanisme de négociation d'authentification fondé sur EAP *(Extensible Authentiquassions Protocol)* ou PSK *(Pre-Shared Key).*
- Le mécanisme de gestion et de distribution des clés TKIP *(Temporal Key Integrity Protocol).*
- Le mécanisme d'intégrité des trames TKIP + algorithme Michael [20].

III.7.3 La protection des systèmes et des applications

Englobe les mesures et les dispositions suivantes :

III.7.3.1 Séparation des plates-formes

Elle consistant à déployer des services de nature différente sur des plates-formes séparées. Cette solution implique un coût élevé de déploiement et d'administration, mais avec un avantage de facilité de déploiement et de gestion, de plus, une grande résistance ne contre les attaques.

III.7.3.2 Protection des systèmes d'exploitation

La protection d'un système d'exploitation nécessite un déshabillage (strip-down) et un blindage (hardening) de ce dernier.

- **Le déshabillage :** Déshabiller un système d'exploitation fait référence à la désactivation des services réseau inutiles ou dangereux. L'importance de cette approche réside dans le fait qu'un système qui n'entend pas certaines requêtes est complètement immunisé contre les attaques ciblant ces services. Par exemple, les services tels que Berkeley (rsh, rexec, rlogin) et Telnet doivent être désactivés sur les systèmes Unix.
- **Le blindage :** Ça consiste à minimiser systématiquement les privilèges. Par exemple :
  - Rétrogradation ou redéfinition des privilèges sur les processus.
  - Synchronisation de l'horloge du système sur au moins deux sources fiables [20].
  - Installation d'un système de vérification de l'intégrité des répertoires et des fichiers stables.

III.7.3.3 Protection des droits d'accès

Elle consiste à authentifier les accès d'une maniéré individuelle, et chaque utilisateur doit respecter la règle du plus bas niveau des privilèges, où le niveau des privilèges monte sur une base temporaire pour effectuer une tâche bien déterminée, puis il regagne son niveau de privilège initial. Parmi les gestionnaires des droits d'accès, on peut citer :

- L'annuaire LDAP qui représente une structure centrale compatible avec tout type de table, y compris des tables d'authentification.
- Kerberos est un outil qui gère les droits d'accès des systèmes distribués. Il est basé sur le principe de tickets. Compatible sous Windows et Unix [20].

III.7.3.4 Protection du contrôle d'intégrité

L'objectif étant l'application de la politique de sécurité, le principal est donc l'intégrité. Pour une politique de sécurité quelconque, on doit vérifier l'intégrité de l'implémentation et celle de la configuration du système. Deux méthodes de vérification d'intégrité sont à citer :

- La copie et l'archivage de tous les fichiers système puis comparé la version actuelle avec la version archivée.
- La création et l'archivage d'une signature numérique puis comparer la signature numérique de la version actuelle avec la signature archivée [20].

III.7.4 La protection de la gestion du réseau

Cette gestion comprend la supervision du réseau, la gestion du routage, la gestion du service des noms de domaine, la gestion du service de mise à l'heure, et la gestion de la zone d'administration.

La gestion du routage réseau (IS-IS, OSPF, BGP, EIGRP… etc.) : Se résume en les pratiques suivantes [20]:

- La description des règles de configuration du protocole IGP et EGP permettant d'assurer le périmètre sécurité du processus de routage.
- Mise en œuvre d'un mécanisme de supervision des indicateurs des tables de routage.
- Description des procédures d'intervention pour le *trouble shooting* (diagnostique) et la résolution des problèmes de perturbation des connexions.

La gestion du service des noms de domaine (DNS) : Comporte les actions suivantes:

- Prévoir des serveurs dédiés à la résolution des noms de domaine (serveurs DNS).
- Se focaliser sur la sécurité systèmes d'exploitation des serveurs DNS.
- Localiser les serveurs DNS dans la zone d'administration.
- Suivre et appliquer tous les patchs de sécurité relatifs aux serveurs et aux services DNS.

La gestion de la zone d'administration : S'articule sur les pratiques suivantes:

- Spécifier une zone d'administration pour le réseau.
- Déterminer le périmètre de sécurité par un filtrage très strict.
- Mettre en œuvre des mécanismes d'authentification pour tous les accès à la zone d'administration.
- Générer et sauvegarder les traces des accès et les commandes effectuées, à des fins d'investigation de sécurité.
- Equiper la zone d'administration du réseau par des dispositifs de détection d'intrusion
- Etablir un plan d'adressage spécifique au réseau [20].

III.8 Conclusion

Ainsi, nous aurions fait le tour des plus importants axes de la sécurité des systèmes informatiques, dont lequel nous avons présenté une multitude de vulnérabilités, auxquelles il faut faire face, faisant appel aux différents mécanismes et techniques de sécurité informatiques, dignes de rivaliser avec la sophistication des outils d'attaques actuelles. Par conséquent, une bonne configuration, protection du réseau, systèmes et applications, suivant une politique de sécurité ajusté aux besoins de sécurité de l'entreprise en question, permet de prévenir d'éventuels dommages dus à des attaques, à savoir irréversibles, comme on dit : « il vaut mieux prévenir que guérir ».

CHAPITRE IV

Mise en réseau de l'infrastructure de L'EP-ADE

IV.1 **Introduction**

Dans ce chapitre, nous allons présenter l'Etablissement Publique Algérienne des Eaux (EP-ADE), une étude du réseau local et l'ensemble des moyens techniques existants, ainsi que notre travail qui consiste en l'interconnexion des différentes structures de l'EP-ADE de Bouira (nous prenons pour l'exemple l'agence commerciale « LAKHDARIA »), nous présentons aussi, un cas pratique d'une application d'une politique de sécurité (filtrage de sites web, sécurité wifi, sécurité du réseau ….etc.), une configuration adaptée aux besoins de l'EP-ADE, et nous achèverons la présentation avec une phase de tests de fonctionnement, pour les solutions apportées , en vue d'améliorer le fonctionnement du support technique de cet établissement.

IV.2 Présentation de l'organisme d'accueil

IV.2.1 L'EP-A.D.E

L'Algérienne des Eaux (ADE) est un établissement public national à caractère industriel et commercial doté de la personnalité morale et de l'autonomie financière. Il a été créé par le décret exécutif n° 01-101 DU 27 Moharrem 1422 correspondants au 21 Avril 2001. L'établissement est place sous la tutelle du ministre charge des ressources en eau, et son siège social est fixe à Alger.

IV.2.1.1 L'organigramme hiérarchique :

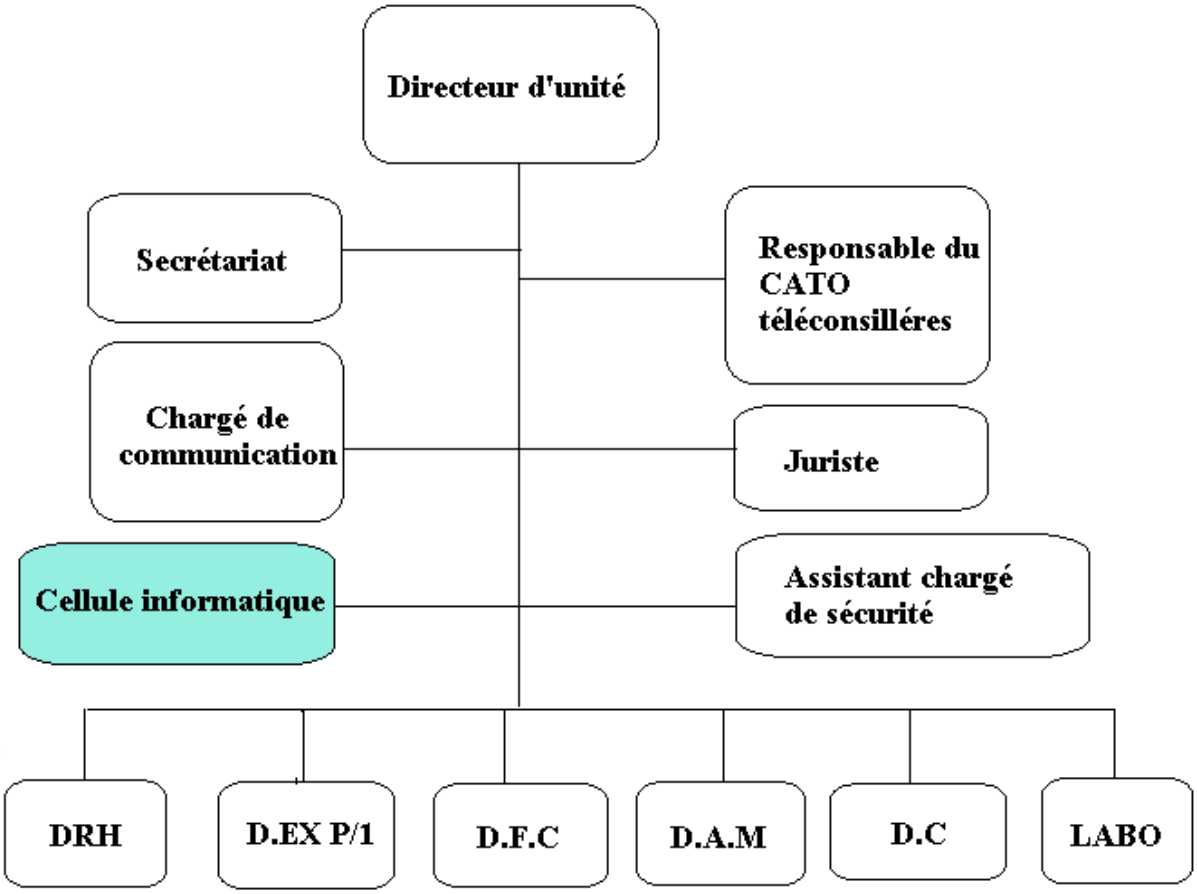


Figure IV. 1 L'organigramme hiérarchique de l'EP-ADE

IV.2.1.2 La cellule informatique

Dirigée par un chef de cellule informatique, un cadre chargé du réseau et un cadre chargé du développement logiciel (figure IV.2), sa mission est :

- D'élaborer et d'assurer la mise en œuvre et le suivi du schéma directeur d'informatisation.
- D'assister les différentes structures de l'EP-A.D.E, l'utilisation des technologies de l'information et de la communication.

- De concevoir et de développer des applications informatiques pour améliorer le support technique des utilisateurs.
- D'assurer la maintenance du parc informatique.
- De contribuer à la mise en œuvre de la stratégie de développement et de modernisation du système informatique de l'EP-A.D.E.

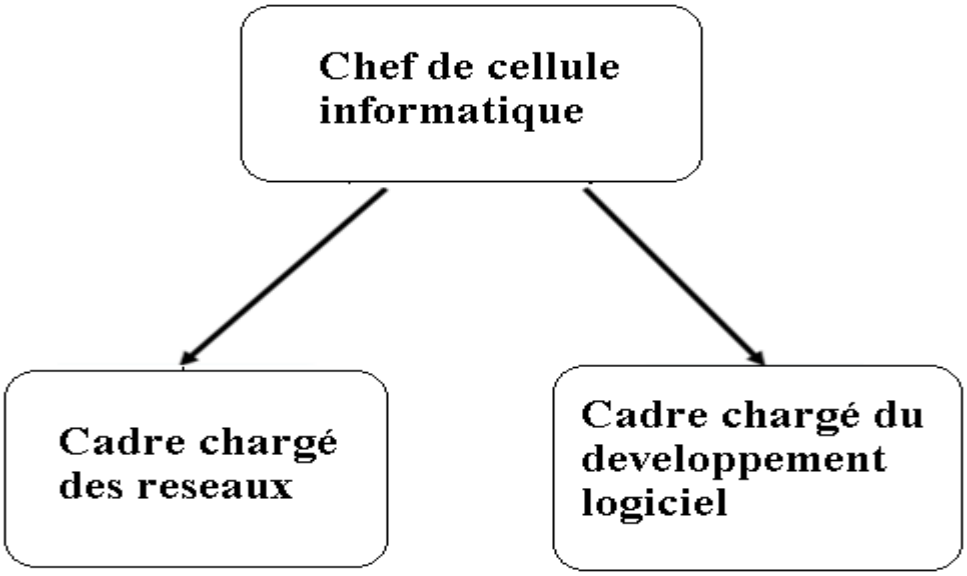


Figure IV. 2 Organigramme hiérarchique de la cellule informatique.

IV.2.1.3 Locaux techniques

IV.2.1.3.1 La salle technique (DataCenter) de l'EP-ADE

Equipée de :

- Un système de détection et d'extinction automatique d'incendies.
- Un système de détection de liquides.
- Une porte coupe-feu.
- Une vitre coupe-feu.
- Deux onduleurs 20 KVA configurés en redondance pour l'alimentation des équipements.
- Systèmes d'alarmes.
- Faux plafonds et faux planché en fibre de carbone.
- Systèmes de mesure de température et d'humidité

L'armoire technique

Equipé de :

- Un routeur Cisco 4200 configuré pour la liaison spécialisée Ls/Mpls (WAN1)
- Switch L3 cisco catalyst 3750 avec modules SFP/FO.
- Router ADSL (WAN2)

IV.2.1.3.2 Les armoires de brassage

Deux armoires de brassage connectées à l'armoire technique de la direction via des liaisons fibre optique (en redondance), chaque armoire dispose de deux switch L2 48 ports configurés en STACK, connectent l'ensemble des ordinateurs de bureau, les téléphones IP, les imprimantes de groupe etc.

IV.2.1.3.3 Les équipements à disposition

- Le pare-feu fortinet Fortigate 101E.
- Une infrastructure (CISCO HyperFlex)
- Le serveur de fichiers (NAS/SAN)
- Les bornes WIFI fortinet.

IV.2.1.4 Les access WAN

Le réseau de la direction de l'EP-ADE dispose de deux accès WAN :

- Une ligne spécialisé MPLS (Data/internet) routé directement à la direction générale (routage statique), avec un débit data de 100 Mo et un débit d'accès à internet de 12 Mo
- Une ligne ADSL d'un débit de 8 Mo, avec une adresse IP statique.

IV.2.2 Etude de l'existant

IV.2.2.1 Le réseau local de la direction de l'EP-ADE

La direction d'EP-ADE dispose d'un réseau local. Nous avons étudié la structure et l'architecteur de ce réseau. Ces principaux composants, que nous décrivons comme suite:

- L'ensemble des équipements (pc, téléphone IP, imprimantes, etc..) de la direction sont connectés via une liaison Ethernet aux switches L2 du réseau local.
- Des VLANs sont configurés d'une telle manière à isoler les différents services et département en sous réseaux différents.
- Les switch L2 sont configurés en STACK (empilement), connectés via la liaison fibre optique au switch L3, avec une redondance de lien.
- Les bases de données sont stockées sur le serveur de fichier (NAS), accessible pour les utilisateurs, une fois authentifiés par le contrôleur de domaine.
- Les VMs sont créés au niveau de hôte ESXI, gérées par l'administrateur, sur le serveur VSphere, accessibles aux utilisateurs, une fois authentifiés par le contrôleur de domaine.
- Les utilisateurs sont organisés en groupes de différents privilèges (autorisations) dans le contrôleur de domaine.

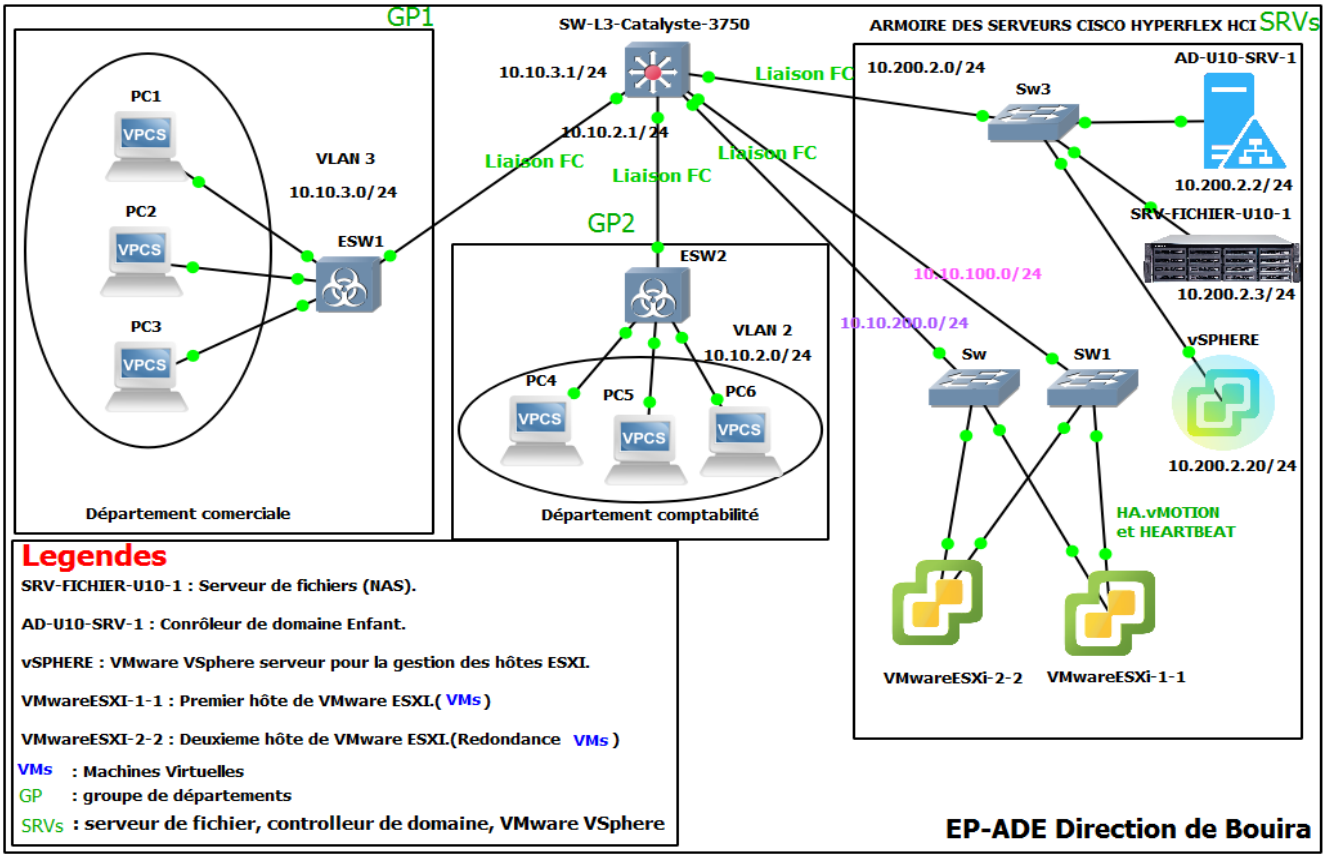


Figure IV. 3 L'architecture du réseau local de la direction de l'EP-ADE.

IV.2.2.1.1 Plan d'adressage

Le tableau suivant (IV.1) présente les adresses et le masque de sous réseaux pour le switch L3:

Dispositif	Interface	Adresse/masque	Liaison
Sw-L3-Catalyste-3750	G1/0	10.200.2.1/24	lien vers SRVs
	G2/0	10.10.100.1/24	lien vers hôtes ESXi
	Vlan3	10.10.3.1/24	Lien vers GP1
	Vlan2	10.10.2.1/24	Lien vers GP2
AD-U10-SRV	G0/0	10.200.2.2/24	Lien vers SW-L3-C3750
SRV-FICHIER-U10	G0/0	10.200.2.10/24	Lien vers SW-L3-C3750
VSphere-SRV	G0/0	10.200.2.20/24	Lien vers SW-L3-C3750
VMwareESXi-1-1	G0/0	10.10.100.2/24	Lien vers SW-L3-C3750 (acces VMs)
	G0/1	10.10.200.2/24	Lien vers SW-L3-C3750 (HA-Vmotion-Hartbeat)

VMwareESXi-2-2	G0/0	10.10.100.3/24	Lien vers SW-L3-C3750 (acces VMs)
	G0/1	10.10.200.3/24	Lien vers SW-L3-C3750 (HA-Vmotion-Hartbeat)

Tableau IV. 1 Le plan d'adressage du réseau local de l'EP-ADE.

IV.2.2.2 Politique de sécurité à mettre en œuvre

- **Interconnexion avec le réseau de la direction générale**

Toute interconnexion entre les réseaux locaux de la direction de Bouira et le réseau de la direction générale doit être réalisée via la liaison spécialisée.

- **Sécurisation des mécanismes de commutation et de routage**

Tout routage passant par la liaison ADSL doit s'accompagner d'une restriction d'accès par ACLs.

- **Mise en place d'un filtrage réseau pour les flux sortants et entrants**

L'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées et surveillé par un pare-feu.

- **Modification systématique des éléments d'authentification par défaut des équipements**

Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.

- **La configuration et l'usage des réseaux sans fil**

Les protections intrinsèques étant insuffisantes, des mesures complémentaires doivent être prises, dans le cadre de la défense en profondeur. Une segmentation du réseau (en VLAN) doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une éventuelle intrusion depuis la voie radio (WiFi).

IV.2.2.3 Le plan d'adressage à mettre en œuvre :

Dispositif	Interface	Adresse/masque	Liaison
SW-L3-C3750	G1/0	10.200.2.1/24	lien vers SRVs
	G2/0	10.10.100.1/24	lien vers hôtes ESXi
	Vlan3	10.10.3.1/24	Lien vers GP1
	Vlan2	10.10.2.1/24	Lien vers GP2

SW-L3-C3750	G5/0.10	10.10.17.1/24	Lien vers GP2
	G0/0	10.10.15.2/24	Lien vers FG-U10 port3
FG-U10	Port 1	222.222.222.222/24	Port de gestion
	Port 2	10.10.14.2/24	Lien vers Cisco-4200
	Port 3	10.10.15.1/24	Lien vers SW-L3-C3750
	Port 4	192.168.1.10/24	Lien vers R-ADSL
	Int virtuelle	192.168.0.1/24	Interface type WiFi SSID
Router Cisco-4200	G0/0	10.10.14.1/24	Lien vers FG-U10 port 2
	G1/0	20.20.20.2/24	FAI
R-ADSL	G0/0	192.168.1.1/24	Lien vers FG-U10 port 4
	PORT WAN PPPOE	40.40.40.200/24	FAI
AD-U10-SRV	G0/0	10.200.2.2/24	Lien vers SW-L3-C3750
SRV-FICHIER-U10	G0/0	10.200.2.10/24	Lien vers SW-L3-C3750
VSphere-SRV	G0/0	10.200.2.20/24	Lien vers SW-L3-C3750
VMwareESXi-1-1	G0/0	10.10.100.2/24	Lien vers SW-L3-C3750 (acces VMs)
	G0/1	10.10.200.2/24	Lien vers SW-L3-C3750 (HA-Vmotion-Hartbeat)
VMwareESXi-2-2	G0/0	10.10.100.3/24	Lien vers SW-L3-C3750 (acces VMs)
	G0/1	10.10.200.3/24	Lien vers SW-L3-C3750 (HA-Vmotion-Hartbeat)

Tableau IV. 2 Le plan d'adressage à mettre en œuvre

IV.2.2.4 Logiciels de simulation et de virtualisation

- **GNS3**

GNS3 *(Graphical Network Simulator)* est un simulateur graphique de réseaux qui permet de créer des topologies du réseau complexes et d'en établir des simulations. Ce logiciel est un excellent outil pour l'administration des réseaux Cisco. Il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco ou pour tester les configurations devant être déployées dans le futur sur des routeurs réels. Ce projet est évidemment Open Source et multi-plates-formes.

- **L'hyperviseur VMware Workstation :** voire **« I.3.7.2** Hyperviseur type 2 ».

IV.3 Mise en réseau de l'infrastructure de l'EP-ADE

Note : Toutes les configurations que nous allons effectuer, représentes des taches d'un projet de mise en œuvre d'un système d'information, soumis à un cahier des charges, détaillé sous formes d'articles, dont lesquelles la politique de sécurité et le plan d'adressage qui nous ont été adressés en font partie.

IV.3.1 Configurations de base

Avant toutes choses, il est nécessaire de configurer une interface de gestion, via laquelle on pourra accéder, avec le navigateur pour configurer le Pare-feu fortigate (adresse IP et autorisations pour les protocoles http et https), cette configuration se fera sur une ligne de commande comme suite :

```
Fotigate-101E# config system interface
Fotigate-101E (interface) # edit port1
Fotigate-101E (port1) # set alias Management
Fotigate-101E (port1) # set mode static
Fotigate-101E (port1) # set ip 222.222.222.222 255.255.255.0
Fotigate-101E (port1) # set allowaccess http https ping
Fotigate-101E (port1) # end
```

IV.3.1.1 Configuration du Pare-feu fortigate 101E

Une fois accédé à l'interface du Pare-feu via le navigateur, nous configurons le nom du pare-feu fortigate 101E «FG-U10 » en référence à « fortigate - Unité Bouira », ainsi que la session d'administration par default du Pare-feu, à savoir, changer le mot de passe de la session « administrateur local » étant exigé dans la politique de sécurité de l'EP-ADE.

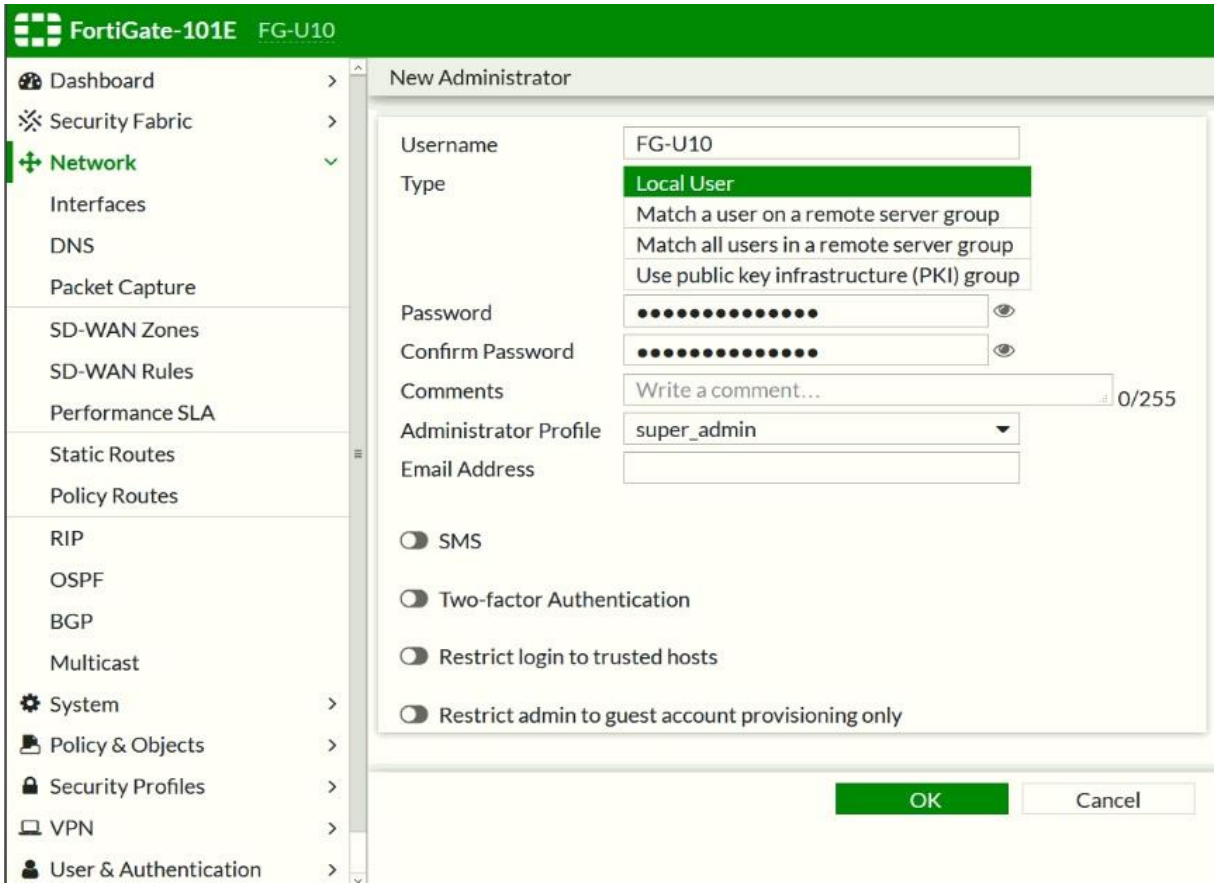


Figure IV. 4 Configuration de l'authentification a l'interface du Pare-feu (session administrateur)

IV.3.1.2 Interconnexion du pare-feu « FG-U10 » et le switch L3 « SW-L3-C3750 »

Nous commençons notre configuration du Pare-feu FG-U10**,** avec une interface de type LAN, qui sera dédier pour connecter le réseau local (la zone interne), avec une adresse IP fixe, le Pare-feu sera connecté directement au switch L3 du réseau local.

Configuration FG-U10 vers SW-L3-C3750

```
FG-U10 # config system interface
FG-U10 (interface) # edit port3
FG-U10 (port3) # set alias LOCAL-U10
FG-U10 (port3) # set mode static
FG-U10 (port3) # set ip 10.10.15.1 255.255.255.0
FG-U10 (port3) # set allowaccess https ping
FG-U10 (port3) # set role lan
FG-U10 (port3) # end
```

Nous configurons également l'interface G0/0 du switch L3 **C3750**, directement connectée à FG-U10.

- **Configuration SW-L3-C3750 vers FG-U10**

```
SW-L3-C3750#configure terminal.
SW-L3-C3750 (config) #interface g0/0
SW-L3-C3750 (config-if) #ip address 10.10.15.2 255.255.255.0
SW-L3-C3750 (config-if) #no shutdown
```

IV.3.1.3 Interconnexion de la direction de Bouira a la direction générale via la liaison spécialisée LS/MPLS

La liaison fibre optique LS/MPLS est directement connectée à la direction générale configurée en routage statique par le FAI. Notre configuration se résume à l'interface d'entré du routeur, afin de le connecter au Pare-feu en tant que WAN.

- **Configuration Cisco-4200 vers FG-U10**

```
Cisco-4200#configure terminal
Cisco-4200(config) #interface g0/0
Cisco-4200(config-if) #ip address 10.10.14.1 255.255.255.0
Cisco-4200(config-if) #no shutdown
Cisco-4200(config-if) #exit
```

Nous configurons également l'interface du Pare-feu directement connecté au routeur Cisco 4200 en mode WAN.

- **Configuration FG-U10 vers Cisco-4200**

```
FG-U10 # config system interface
FG-U10 (interface) # edit port2
FG-U10 (port2) # set alias WAN-LS.
FG-U10 (port2) # set role wan
FG-U10 (port2) # set mode static
FG-U10 (port2) # set ip 10.10.14.2/24
FG-U10 (port2) # set allowaccess https ping
FG-U10 (port2) # end
```

IV.3.1.4 Interconnexion de l'agence commerciale LAKHDARIA et la direction de Bouira via la liaison ADSL

Nous configurons l'interface d'entré du routeur ADSL pour le connecter directement au pare-feu en tant que WAN2 :

- **Configuration R-ADSL vers FG-U10**

```
R4#configure terminal
R4 (config) #hostname R-ADSL
R-ADSL (config) #interface g0/0
R-ADSL (config-if) #ip address 192.168.1.1 255.255.255.0
R-ADSL (config-if) #no shutdown
```

Nous configurons également l'interface du pare-feu directement connectée au routeur ADSL en mode WAN.

- **Configuration FG-U10 vers R-ADSL**

```
FG-U10 (interface) # edit port4
FG-U10 (port4) # set alias WAN-ADSL
FG-U10 (port4) # set role wan
FG-U10 (port4) # set mode static
FG-U10 (port4) # set ip 192.168.1.10/24
FG-U10 (port4) # set allowaccess https ping
FG-U10 (port4) # end
```

IV.3.2 Configurations avancées

IV.3.2.1 Configuration de l'SD-WAN sur FG-U10

Afin de mieux exploiter et optimiser l'utilisation du débit des deux accès WAN, et avoir une redondance de liens, (balancement du trafic en cas de panne de l'une des liaisons WAN) nous configurons la fonctionnalité SD-WAN du pare-feu FG-U10.

IV.3.2.1.1 Assignation des interfaces WANs pour le SD-WAN

- **Assignation de la liaison LS-MPLS**

Nous spécifions l'interface du Pare-feu connecté au routeur Cisco 4200 dédié pour le WAN, ainsi que l'adresse IP de l'interface d'entré du routeur de destination (passerelle par default), afin d'assigner le lien physique pour le lien virtuelle du SD-WAN.

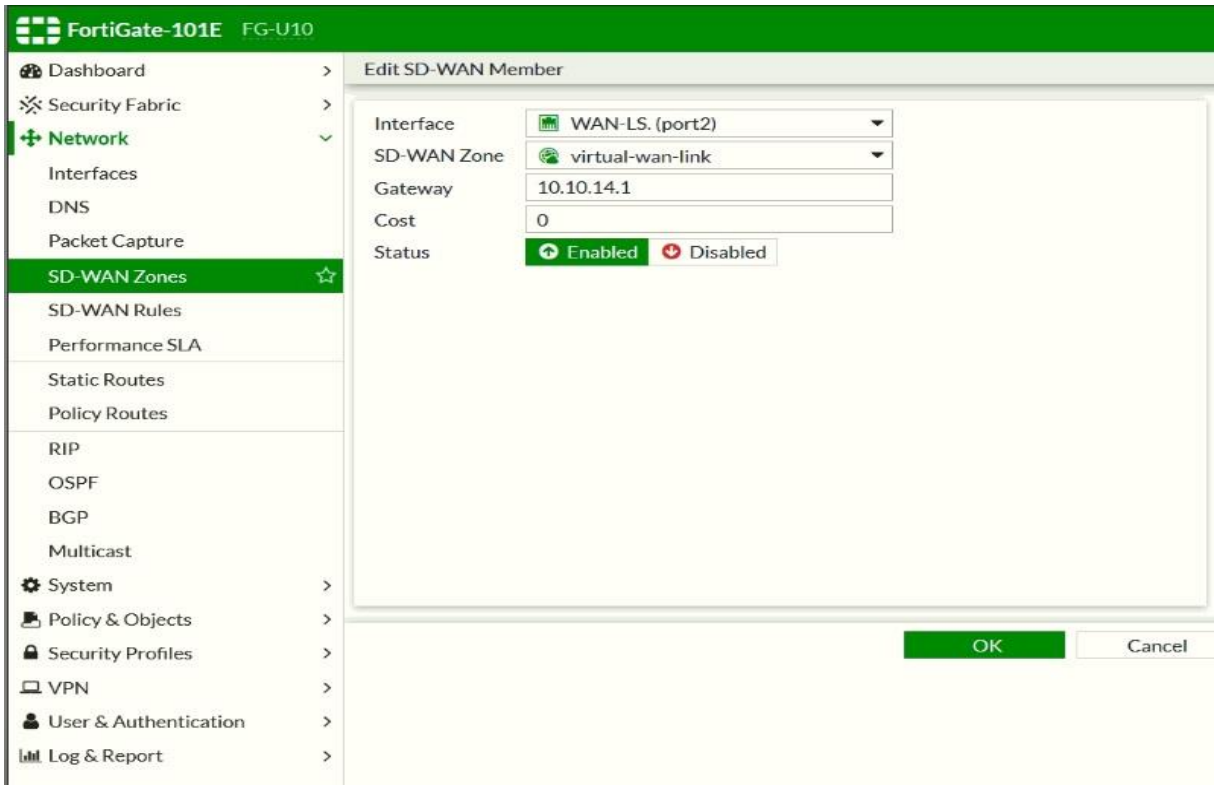


Figure IV. 5 Assignation de la liaison LS-MPLS

- **Assignation de la liaison ADSL**

Nous spécifions l'interface du pare-feu connecté au routeur R-ADSL dédié pour le WAN, ainsi que l'adresse IP de l'interface d'entré du routeur de destination (passerelle par default), afin d'assigner le lien physique pour le lien virtuelle du SD-WAN.

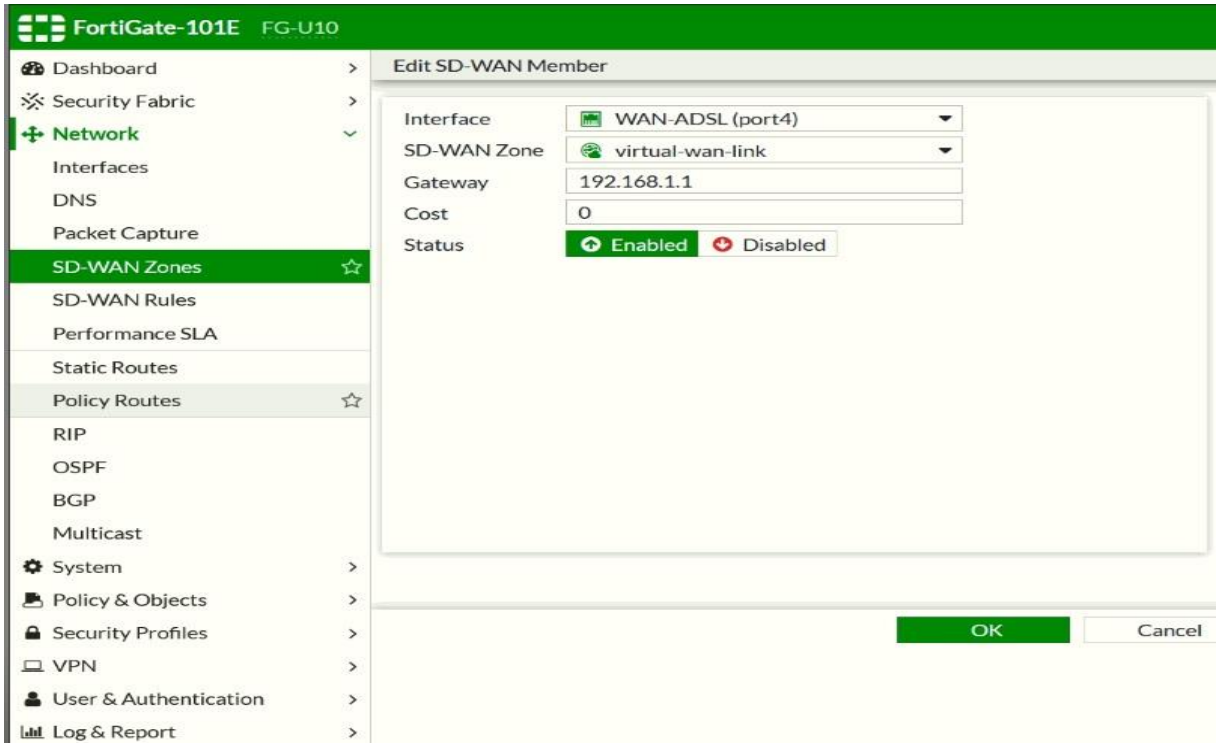


Figure IV. 6 Assignation de la liaison ADSL.

IV.3.2.1.2 Configuration du partage de charge pour l'accès à internet (Load Balancing)

Nous allons partager l'accès aux deux liaisons WAN par le volume du trafic sortant, afin de laisser l'algorithme gérer le partage automatiquement, la liaison LS-MPLS ayant 12Mo de débit d'accès à internet aura une part de 60% de l'ensemble du trafics, et l'ADSL ayant 8Mo, aura pour sa part 40%. Si toutefois l'une des liaisons est HS, la fonctionnalité 'Load Balancing' basculera la totalité du trafic vers la liaison en service.

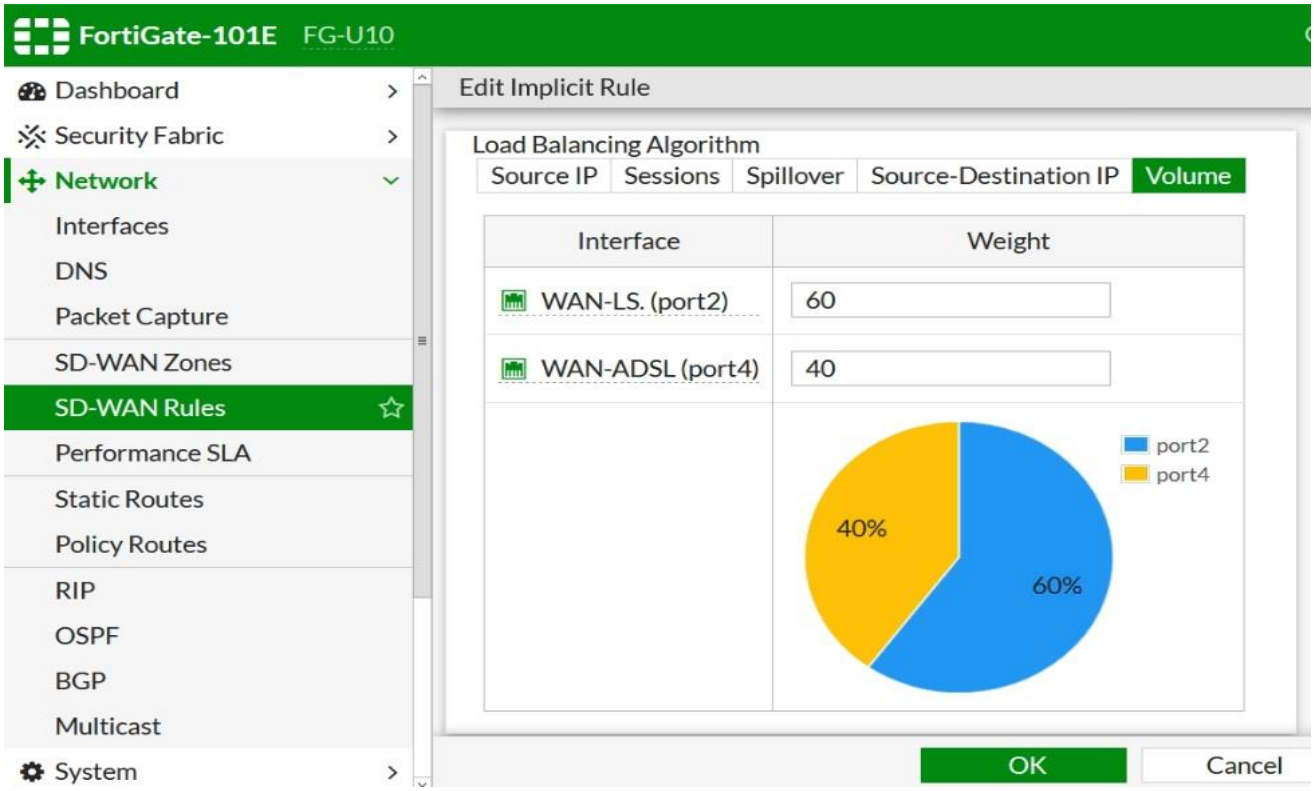


Figure IV. 7 Configuration du partage de charge pour l'accès à internet *(Load Balancing)*

IV.3.2.1.3 Spécification des adresses DNS du domaine de l'EP-ADE

Pour éviter que le traffic passe par le serveur DNS par default du constructeur du Pare-feu, et pour rependre à des spécifications mentionnées dans la politique de sécurité qui nous a été attribuée, nous allons spécifier pour la fonctionnalité SD-WAN, les adresses des serveurs DNS de l'EP-ADE.

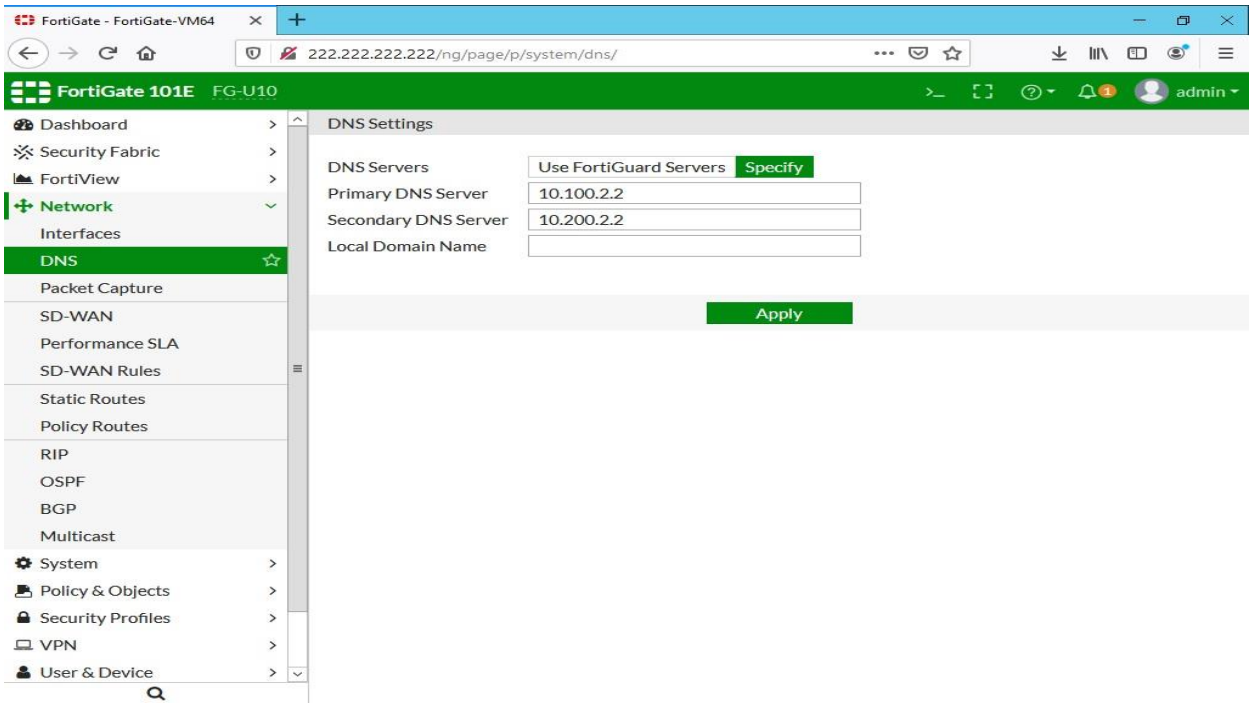


Figure IV. 8 Spécification des adresses DNS du domaine de l'EP-ADE.

IV.3.2.1.4 Définition des routes statiques vers les liaisons WAN (ADSL et MPLS) sur le pare-feu fortigate

Afin que le trafic vers internet soit routé vers l'ensemble des liaisons WAN (lien virtuel SD-WAN) nous configurons la route statique comme suite :

```
FG-U10 # config router static
FG-U10 (static) # edit 1
FG-U10 (1) # set distance 1
FG-U10 (1) # set sdwan enable
FG-U10 (1) # end
```

IV.3.2.2 Configuration du réseau WIFI pour le réseau local de la direction de Bouira

L'objectif de cette configuration est de permettre aux utilisateurs de la direction de Bouira d'accéder avec des appareils mobiles, aux ressources du Système d'Information (internet, messagerie, applications web…), via le réseau local. La première étape consiste en la configuration d'une sub-interface sur le switch L3, ainsi que la configuration d'un serveur DHCP dont nous spécifions les adresses DNS (serveur EP-A.D.E) pour la sub-interface.

- **Configuration du DHCP et la sub-interface sur SW-L3-C3750**

```
SW-L3-C3750 (config) #interface g5/0.10
SW-L3-C3750 (config-subif)#encapsulation dot1Q 10
SW-L3-C3750 (config-subif) #ip address 10.10.17.1 255.255.255.0
SW-L3-C3750 (config-subif) #exit
SW-L3-C3750 (config) #ip dhcp excluded-address 10.10.17.1
SW-L3-C3750 (config) #ip dhcp pool vlanAP
SW-L3-C3750 (dhcp-config) #network 10.10.17.0 255.255.255.0
SW-L3-C3750 (dhcp-config) #lease 15
SW-L3-C3750 (dhcp-config) #domain-name BOUIRA.ADE.DZ
SW-L3-C3750 (dhcp-config) #DNs-server 10.200.2.2 10.100.2.2
SW-L3-C3750 (dhcp-config) #DEFault-router 10.10.17.1
SW-L3-C3750 (dhcp-config) #END
```

- **Configuration du vlan sur ESW2**

Nous configurons le vlan10 pour connecter les bornes WiFi sur le switch L2 « ESW1 » du réseau local

```
ESW1#configuration terminal
ESW1 (config) #vlan 10
ESW1 (config-vlan) #name vlanAP
ESW1 (config-vlan) #exit
ESW1 (config) #interface f1/4
ESW1 (config-if) #switchport mode access
ESW1 (config-if) #switchport access vlan 10
ESW1 (config-if) #exit
```

- **Configuration du port 3 sur FG-U10**

Nous configurons l'interface du Pare-feu connecté au réseau local pour activer détection et l'identification des bornes WiFi « fortiAP »

```
FG-U10 # config system interface
FG-U10 (interface) # edit port3
FG-U10 (port3) # set allowaccess https ping fabric
FG-U10 (port3) # set device-identification enable
FG-U10 (port3) # set auto-auth-extension-device enable
FG-U10 (port3) # end
```

IV.3.2.3 Configuration des options de sécurité

Quel que soit la manière dont les utilisateurs de l'EP-A.D.E accèdent aux ressources du SI, il est primordial d'accompagner ses accès avec des solutions adéquates.

Le Pare-feu fortigate nous offre une multitude de solutions permettant de rependre à ce besoin, notamment le filtrage DNS et sites web, 'Portail Captif', ainsi que le serveur LDAP, grâce à lequel on peut profiter de la fiabilité du contrôleur de domaine 'Active Directory', en important les groupes d'utilisateurs, et les associer à la politique de sécurité du Pare-feu.

IV.3.2.3.1 Configuration du serveur LDAP

Le serveur LDAP permet d'importer des groupes d'utilisateurs, préalablement configurés dans l'annuaire 'Active directory', ainsi que l'ensemble des autorisations qui leurs ont été associées.

L'authentification du pare-feu lui-même se fera via un compte « fortiGate-U », aussi préalablement configuré dans l'annuaire, dédié pour l'authentification du pare-feu fortigate, a l'annuaire 'Active Directory' pour importer ses groupes d'utilisateurs.

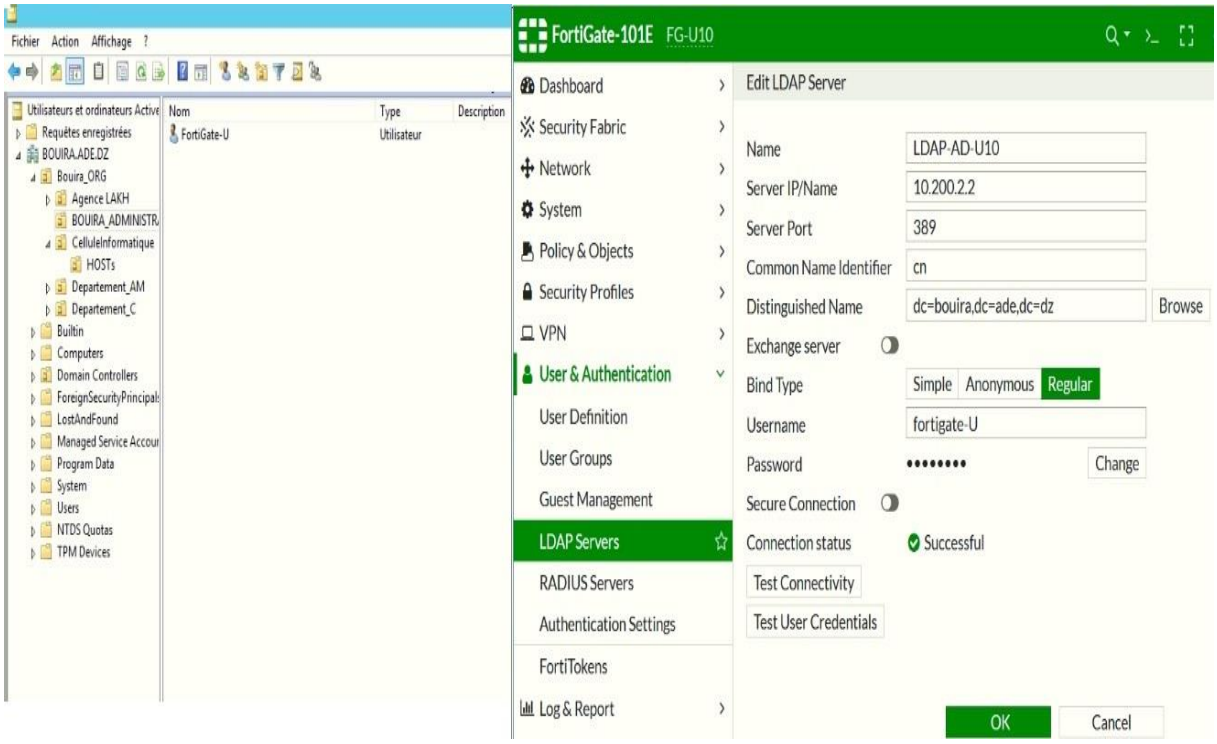


Figure IV. 9 Configuration du serveur LDAP.

- **Importation des groupes d'utilisateur depuis l'annuaire active directory**

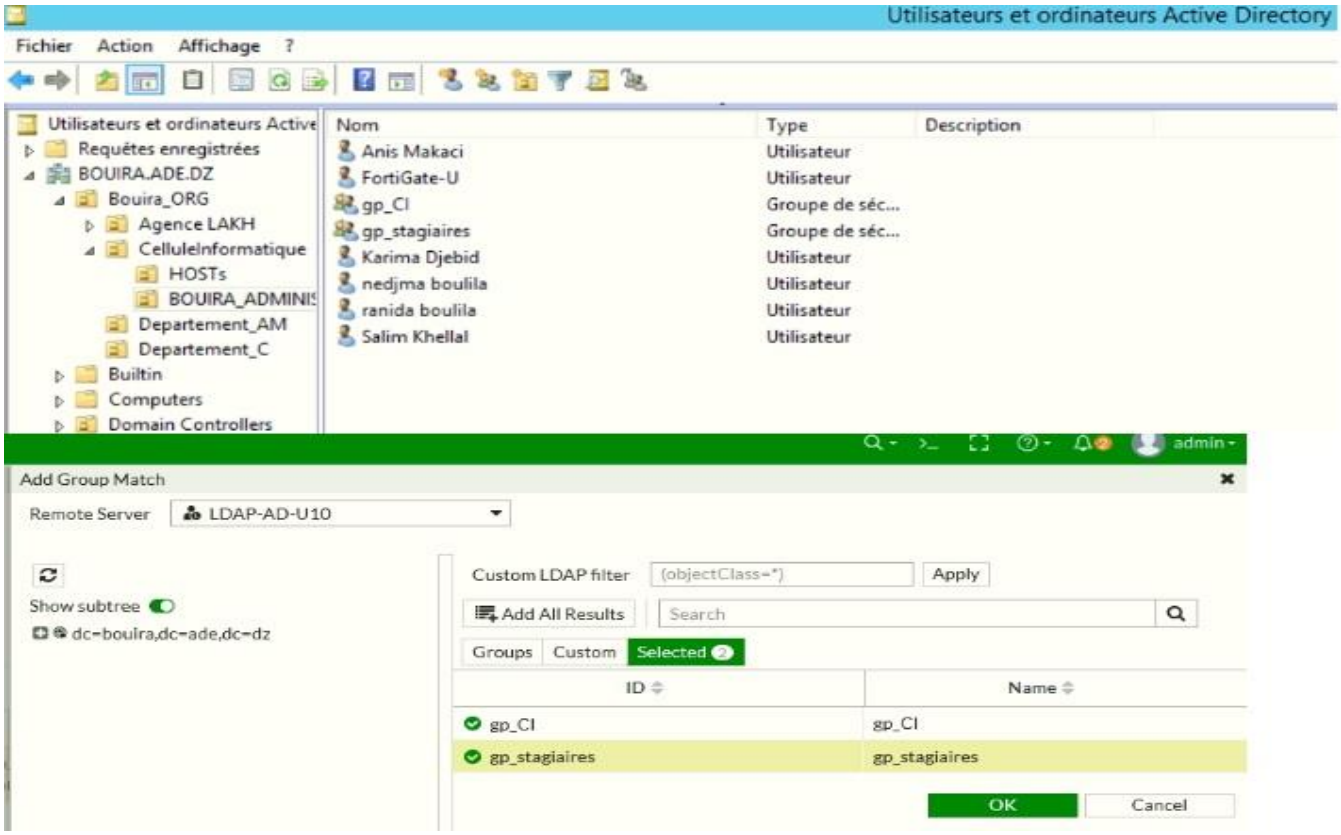


Figure IV. 10 Importation des groupes d'utilisateur depuis l'annuaire 'Active Directory'.

IV.3.2.3.2 Création des profils de filtrage de site web

- **Profile 1 : « only_search » :** Ce profile interdit tout accès à internet sauf pour les moteurs de recherche

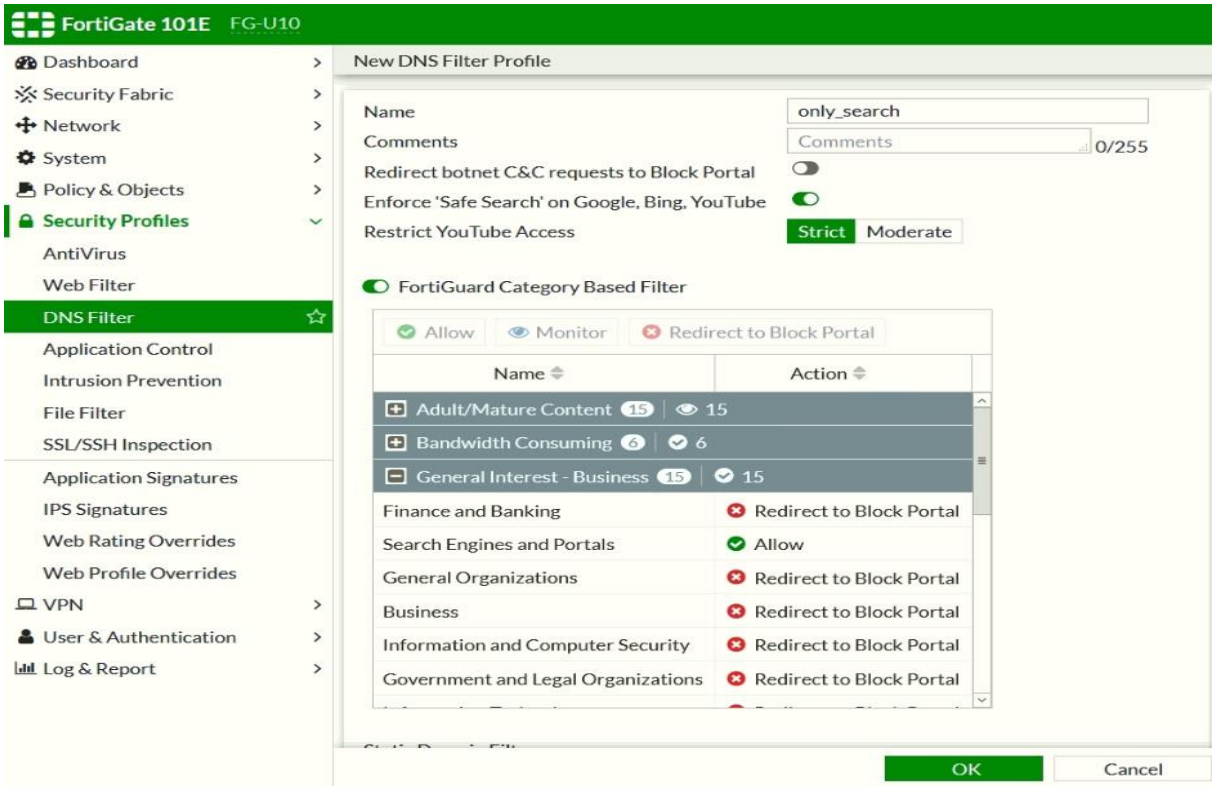


Figure IV. 11 Création de Profile 1 « only_search » de filtrage de site web

- **Profile 2** : « **only_search_email** » Ce profil consiste à restreindre l'accès à tous les sites sauf la messagerie électronique et les moteurs de recherche.

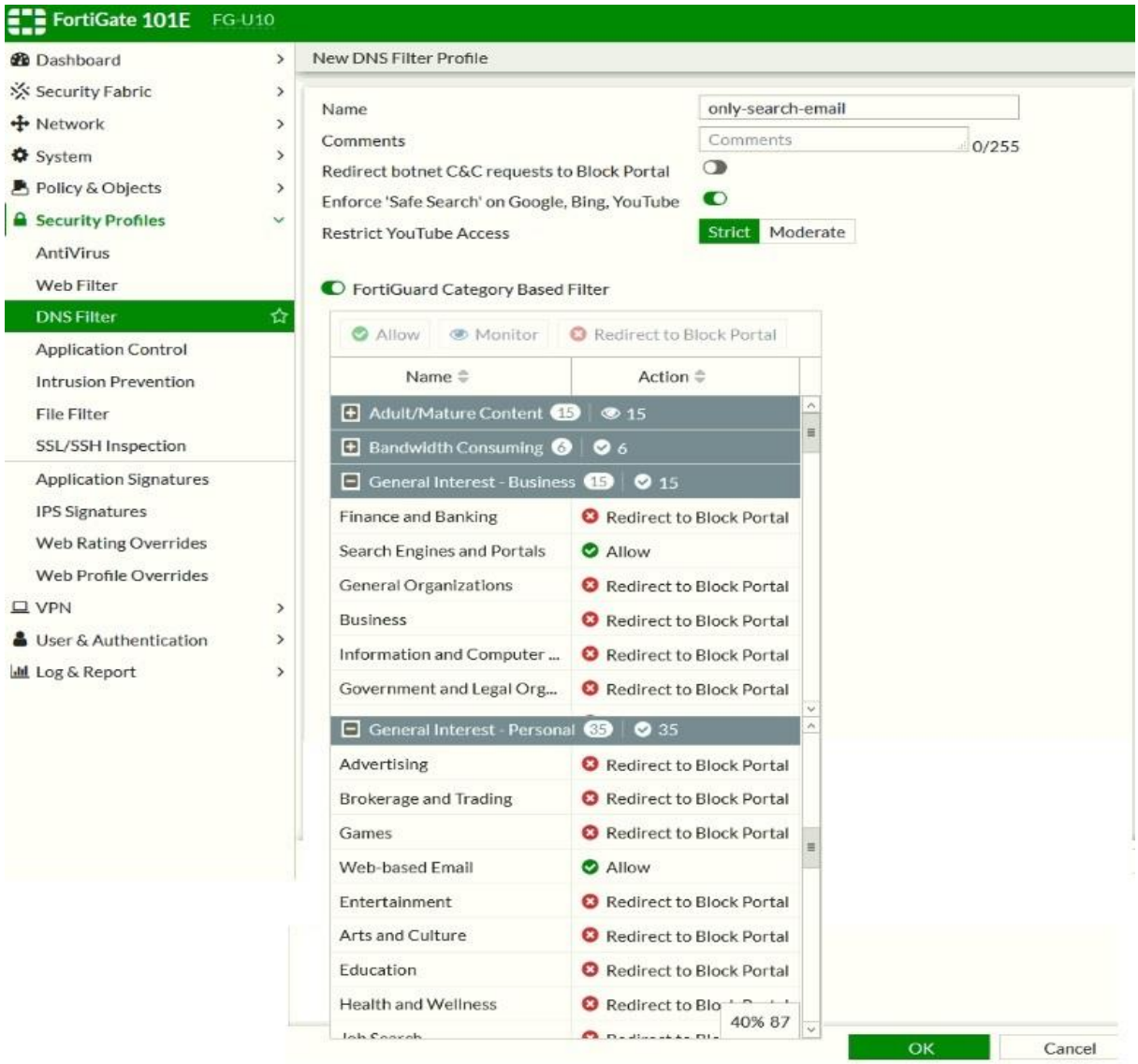


Figure IV. 12 Création Profile 2 « only_search_email » de filtrage de site web.

- **Profile 3 : « full_access » :** ce profil autorise l'accès aux moteurs de recherche, la messagerie électronique, les réseaux sociaux et le streaming vidéo.

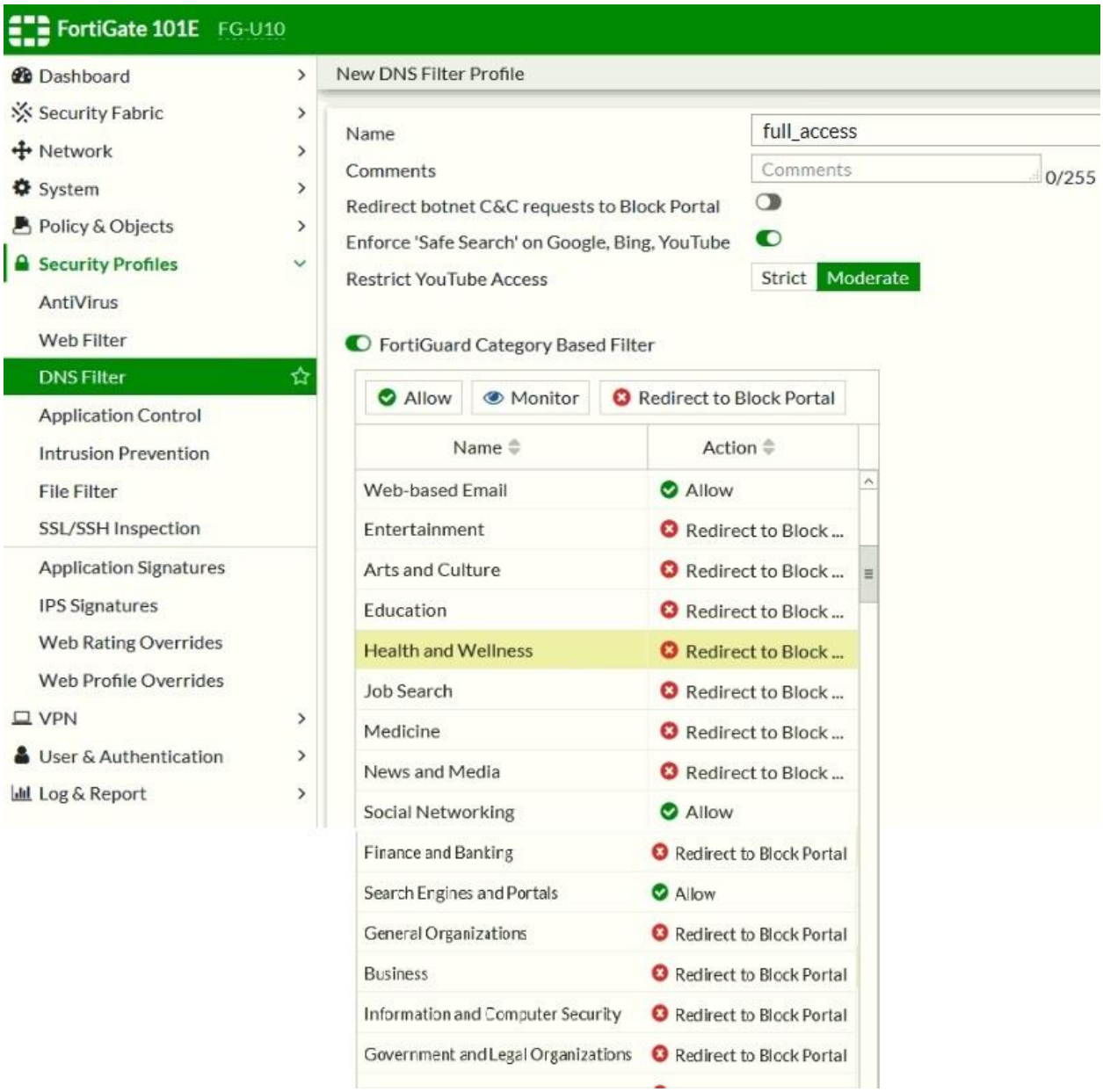


Figure IV. 13 Création Profile 3 « full_access» de filtrage de site web.

IV.3.2.3.3 Configuration de la politique de sécurité

Après avoir importé les groupes d'utilisateurs sur le serveur LDAP, et crée les profils de filtrage web nous affectons pour chaque profil de filtrage l'ensemble des utilisateurs, en fonction de la nature de ces dernier, nous prenons en exemple :

Le profil 1 « only_search » pour le groupe d'utilisateurs « gp_stagiaires »

Le profil 2 « only_search_email » pour le groupe « gp_DAM »

Le profil 3 « full_Access » pour Le groupe « gp_administrateur »

Exemple d'affectation d'un profil de filtrage web pour un groupe d'utilisateurs :

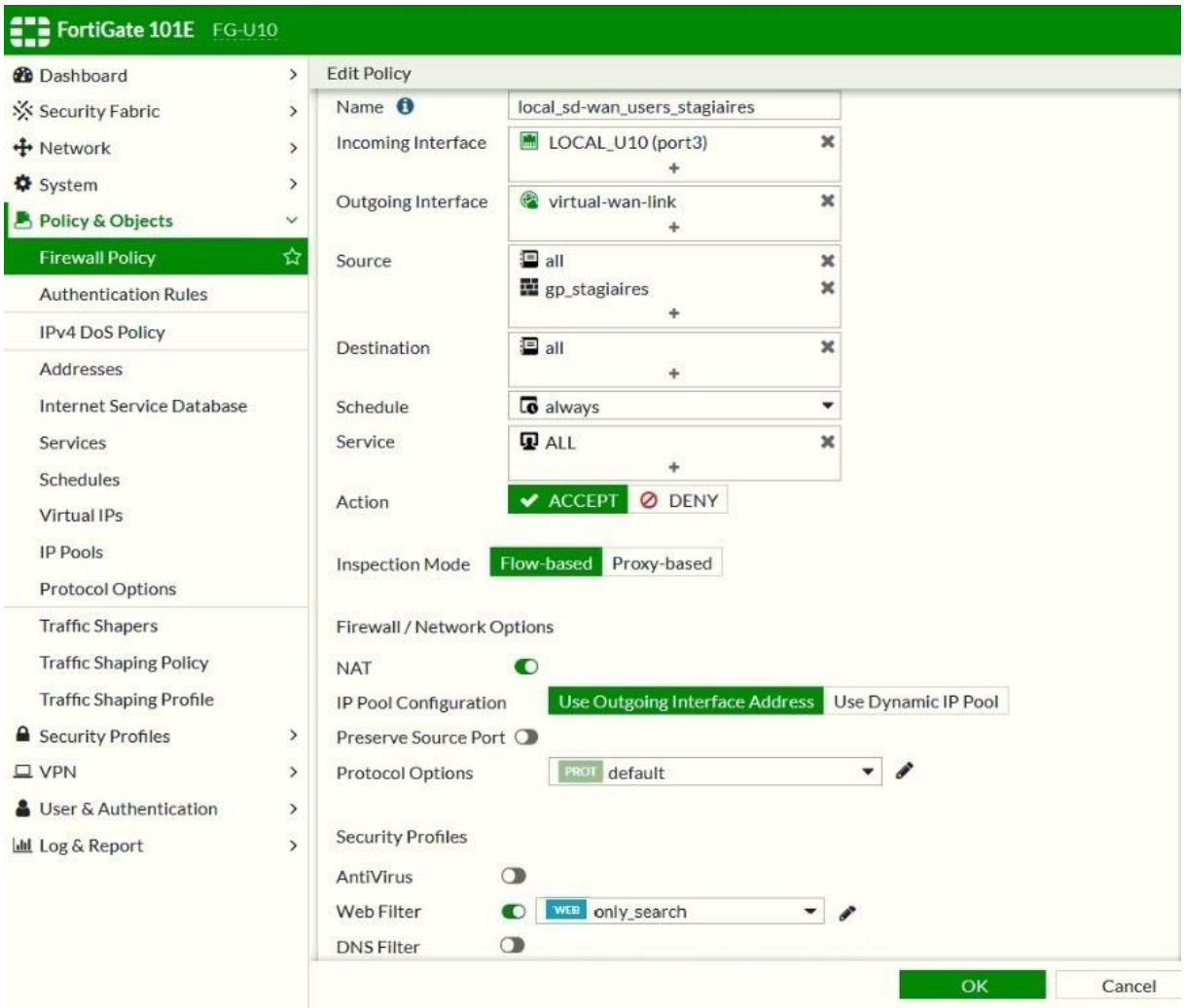


Figure IV. 14 Exemple d'affectation d'un profil de filtrage web pour un groupe d'utilisateurs.

IV.3.2.4 Configuration du portail captif pour l'accès WIFI

Cette étape consiste à configurer un 'Portail Captif', qui est une fonctionnalité du pare-feu fortigate 101E, qui intègre une authentification personnalisée pour sécuriser l'accès au réseau et aux ressources du Système d'Information de l'EP-ADE.

Configuration du port 3 sur FG-U10

```
FG-U10 # config system interface
FG-U10 (interface) # edit port3
FG-U10 (port3) # set security-mode captive-portal
FG-U10 (port3) # end
```

IV.3.2.4.1 Configuration d'une interface virtuelle de type « Wifi SSID »

Cette configuration consiste à créer une interface virtuelle (sub-interface) de type « wifi-SSID », pour le port3 du Pare-feu, et l'assigner pour les bornes wifi en mode tunnel, l'interface sur laquelle on va pouvoir configurer les paramètres de l'ensemble des bornes WiFi.

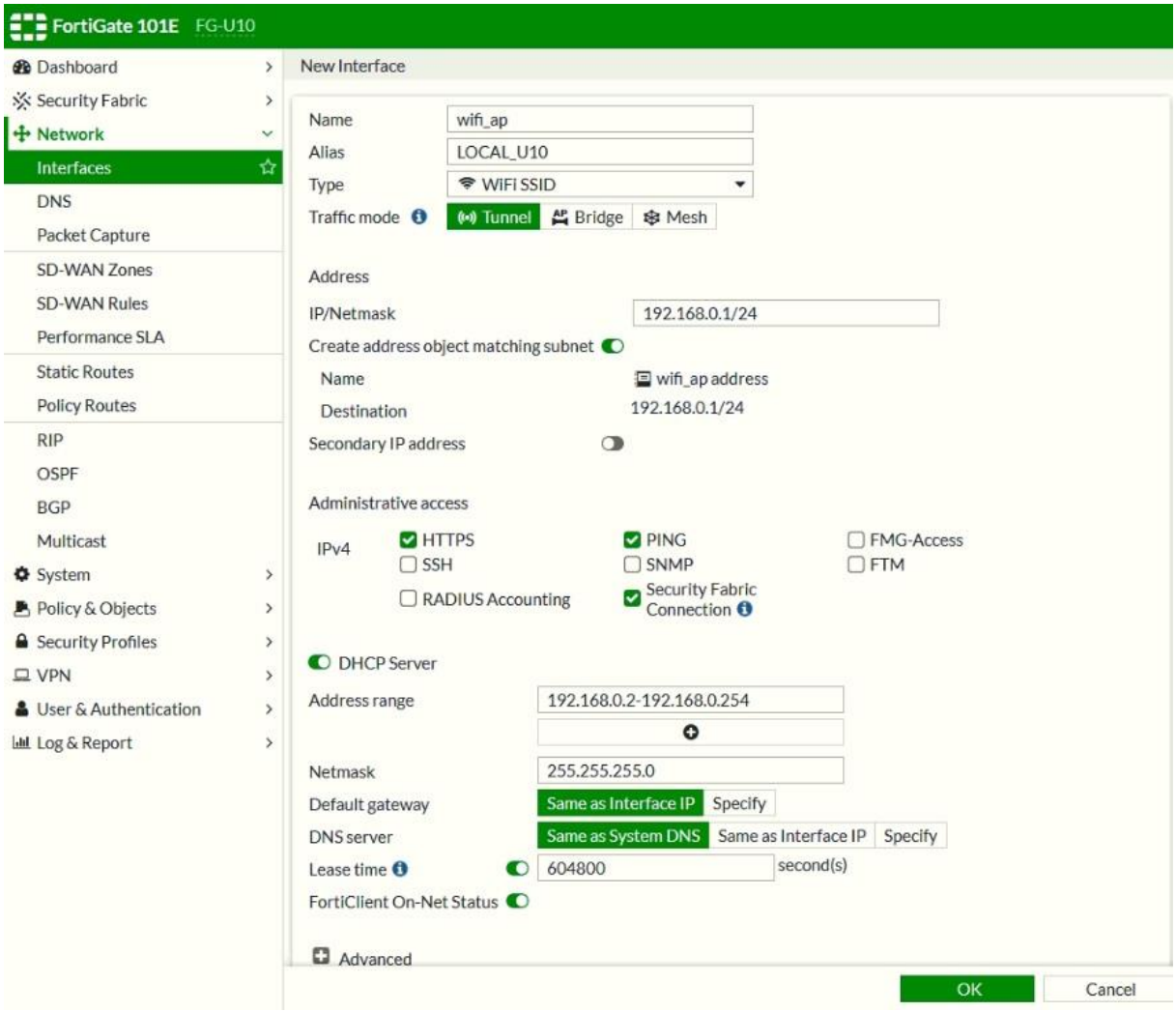


Figure IV. 15 Configuration d'une interface virtuelle de type « Wifi SSID ».

IV.3.2.4.2 Définition des groupes d'utilisateurs pour l'accès au réseau via le WiFi

Les utilisateurs autorisés à accéder par wifi sont importés via le serveur LDAP, depuis l'annuaire 'Active Directory'. Ce qui signifie que les utilisateurs doivent s'identifier avec le nom et le mot de passe du compte Windows.

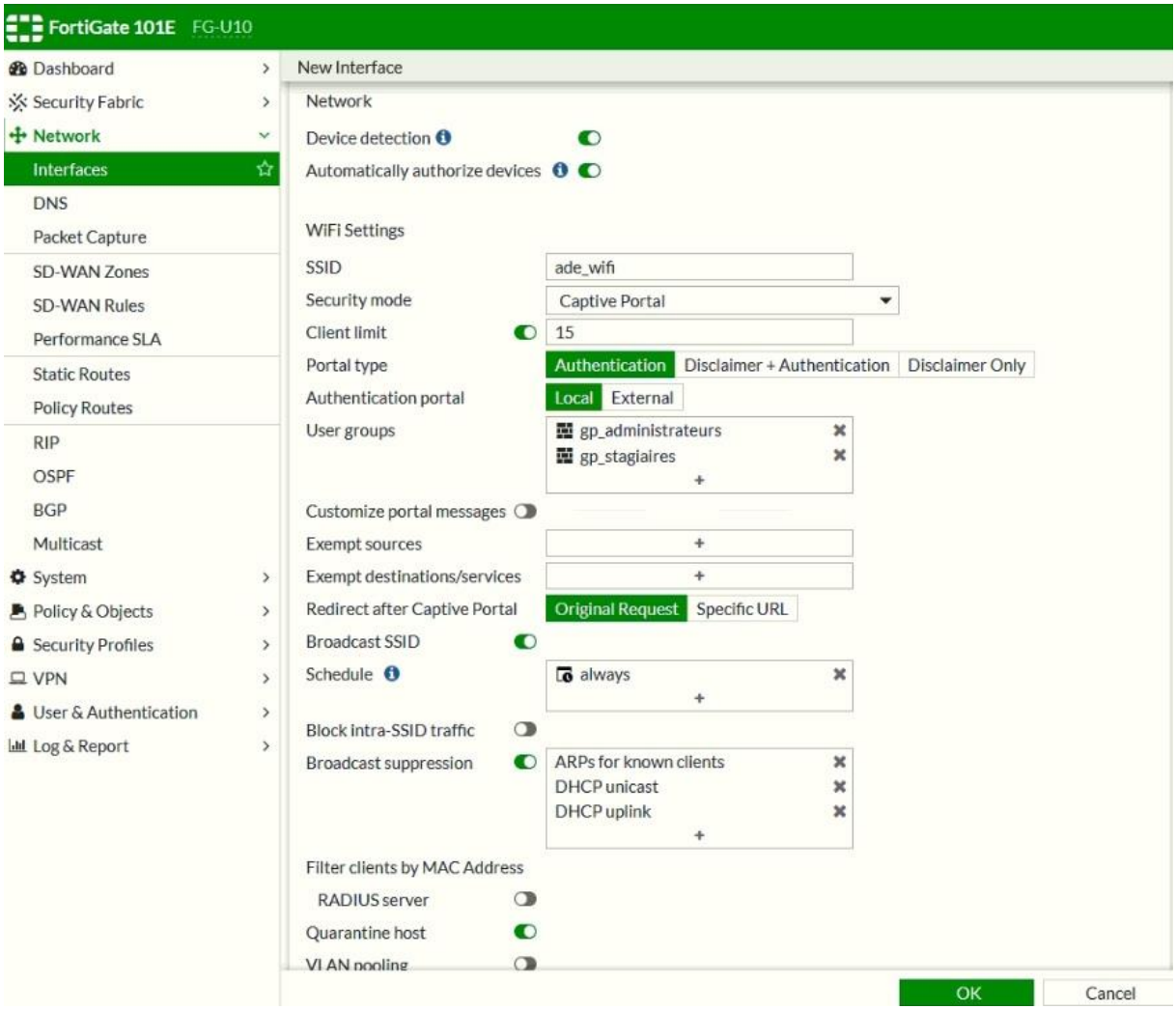


Figure IV. 16 Définition des groupes d'utilisateurs pour l'accès au réseau via le WiFi.

IV.3.2.4.3 Autorisation de l'accès à internet via la borne wifi

Afin que permettre le trafic vers l'ensemble des WANs (SD_WAN), depuis le wifi, nous configurons une politique de sécurité. Le filtrage des sites web n'est pas nécessaire, étant déjà configuré dans la fonctionnalité « filtrage web», il suffit juste de sélectionner le profil de filtrage précédemment crée.

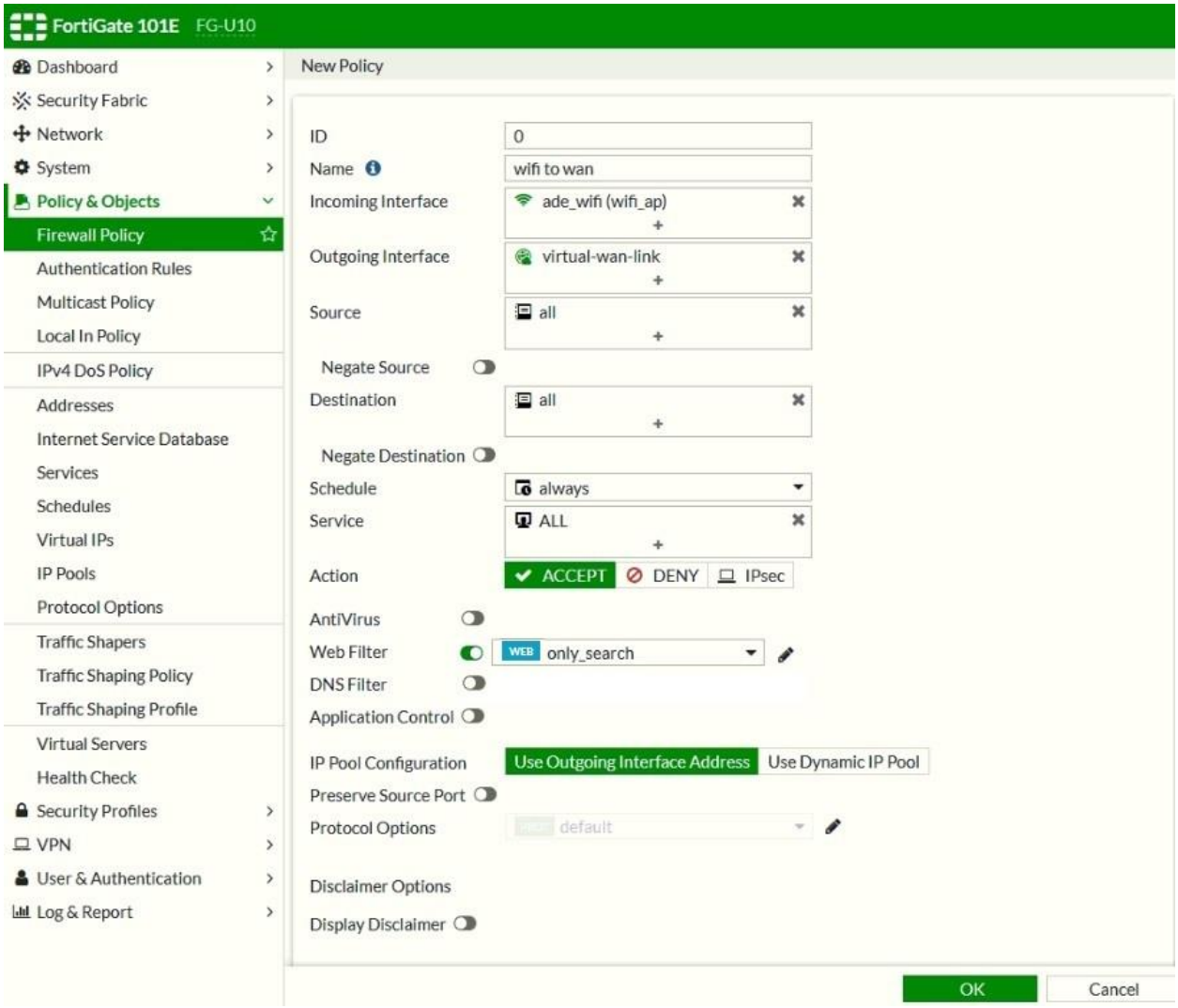


Figure IV. 17 Exemple d'autorisation de l'accès à internet via la borne wifi.

IV.4 **Testes de fonctionnement**

IV.4.1 Accès au réseau local via le Wifi *(authentification au Portail Captif)*

Nous pouvons tester le fonctionnement du wifi sur un Smartphone ou un Laptop, une fois accéder, le 'Portail Captif' apparait pour demander les informations d'authentification (compte Windows).

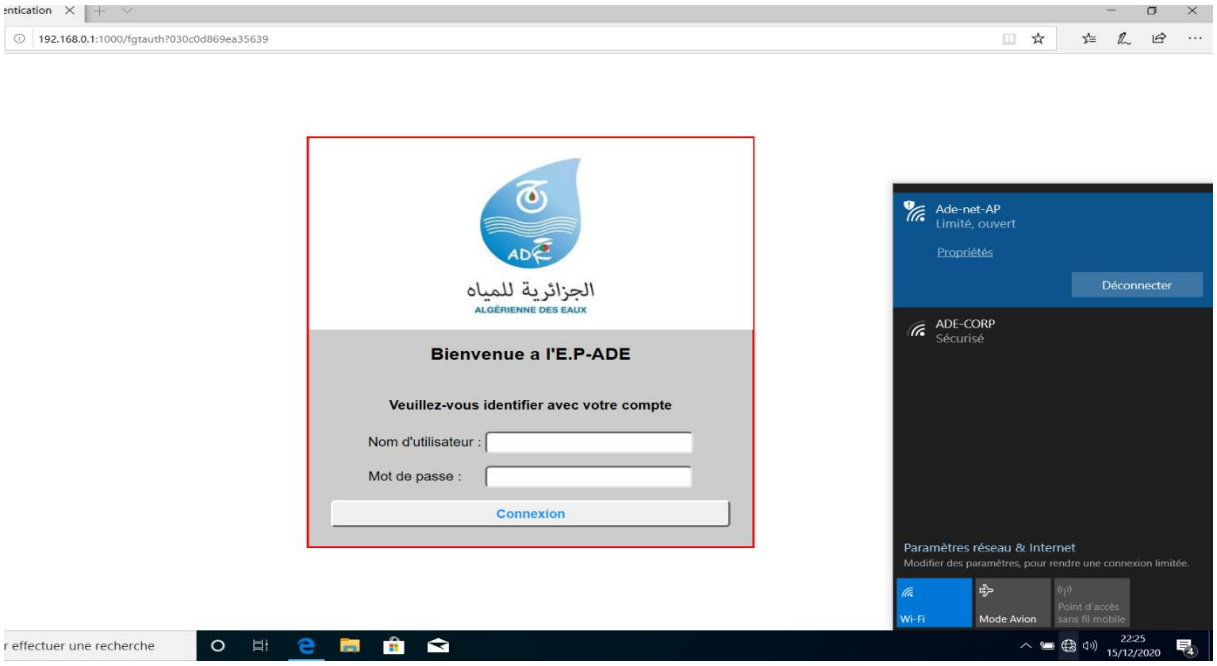


Figure IV. 18 Accès au réseau local via le Wifi (authentification au portail captif).

IV.4.2 Authentification au domaine

Une fois connecté au réseau local, que ça soit via le réseau filaire ou wifi (après authentification), ou depuis l'agence commerciale, l'utilisateur n'accède toujours pas aux ressources du SI, il faut joindre le domaine afin de pouvoir s'authentifier, et se connecter avec la session Windows.

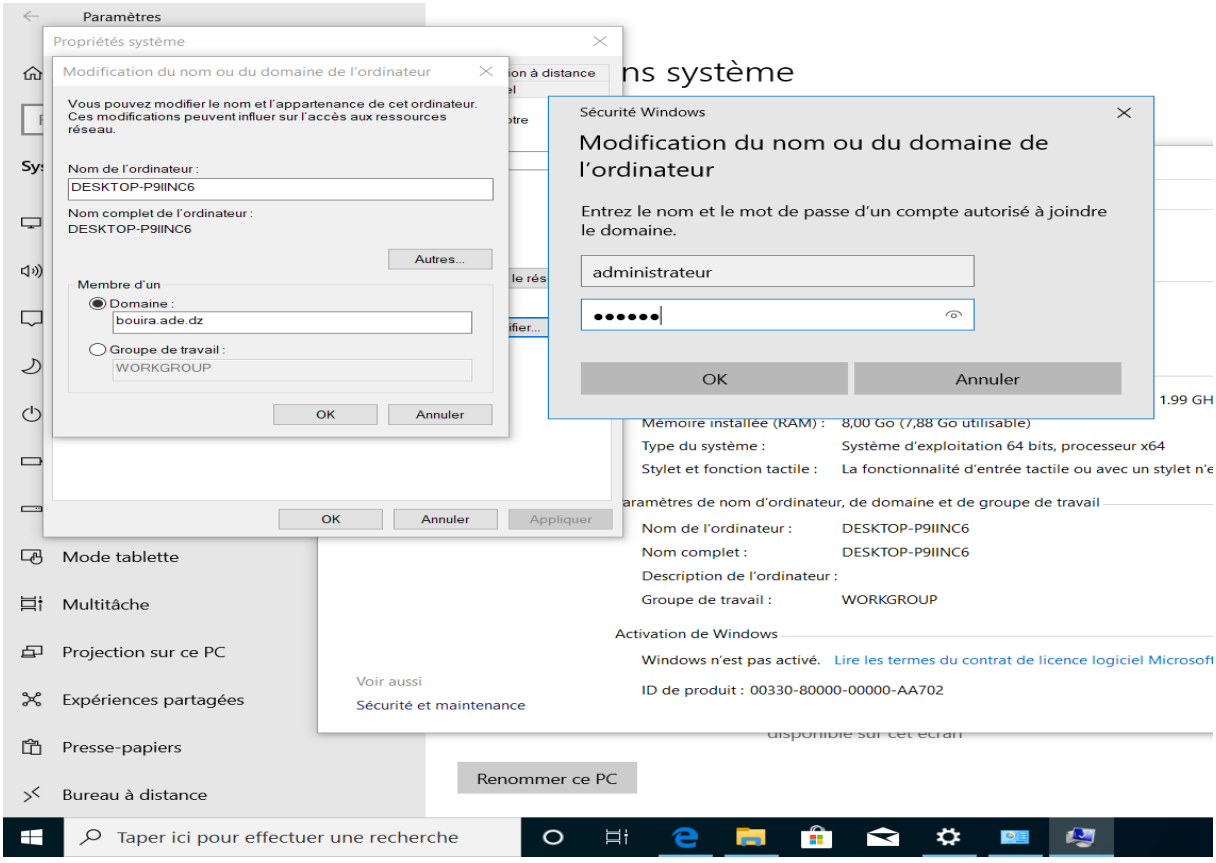


Figure IV. 19 Authentification au domaine.

Une fois authentifié au domaine, le contrôleur du domaine détermine les droits d'accès pour chaque utilisateur, et le pare-feu détermine les accès autorisé à internet pour l'utilisateur en question.

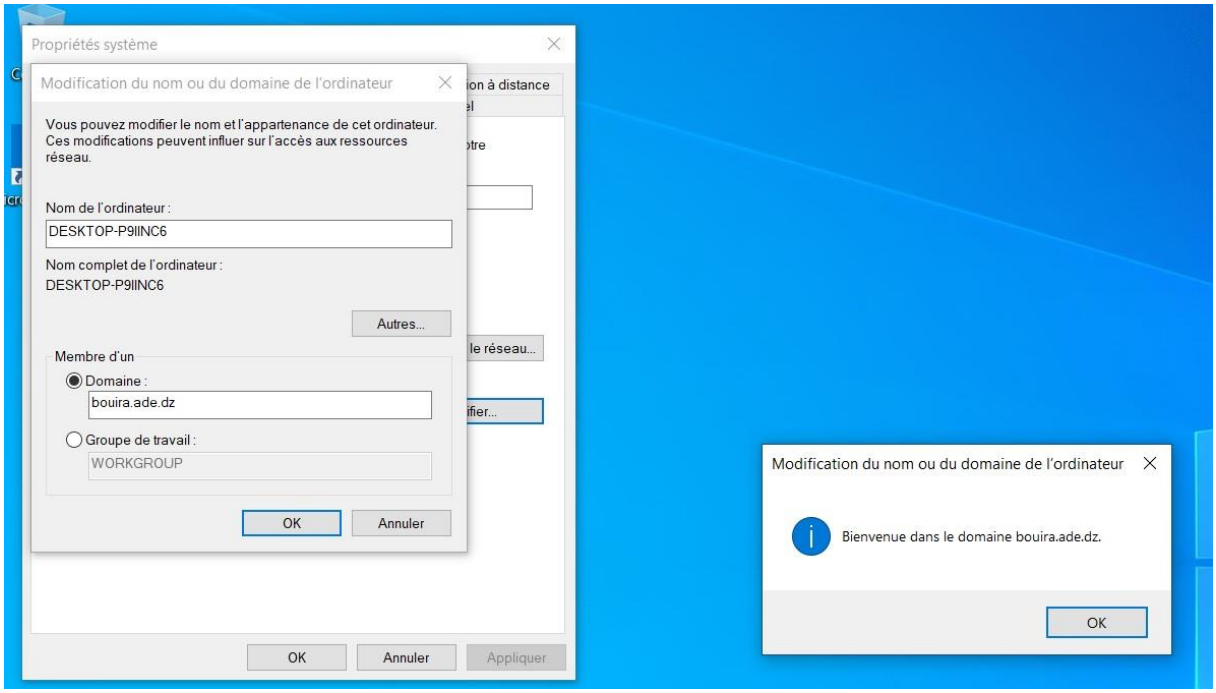


Figure IV. 20 Authentification au domaine réussie.

IV.4.3 Accès aux applications web

Nous testons l'accès à l'application « DEX Maintenance » depuis l'agence LAKHDARIA.

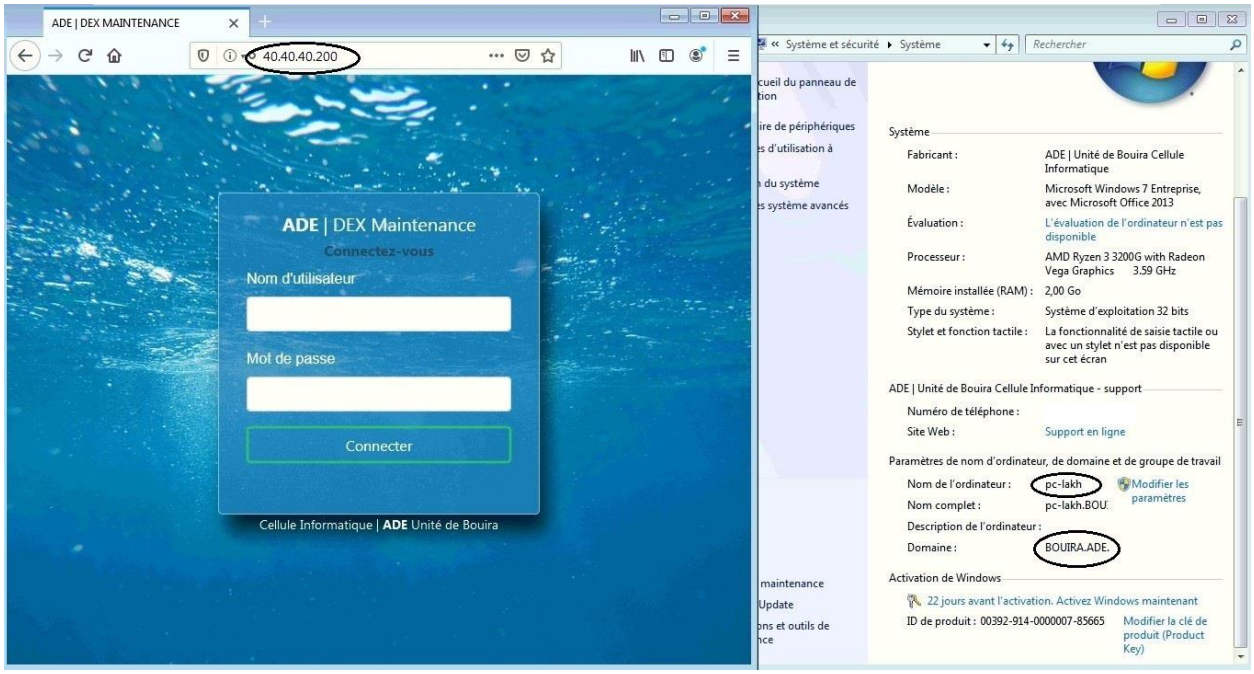


Figure IV. 21 Accès aux applications web.

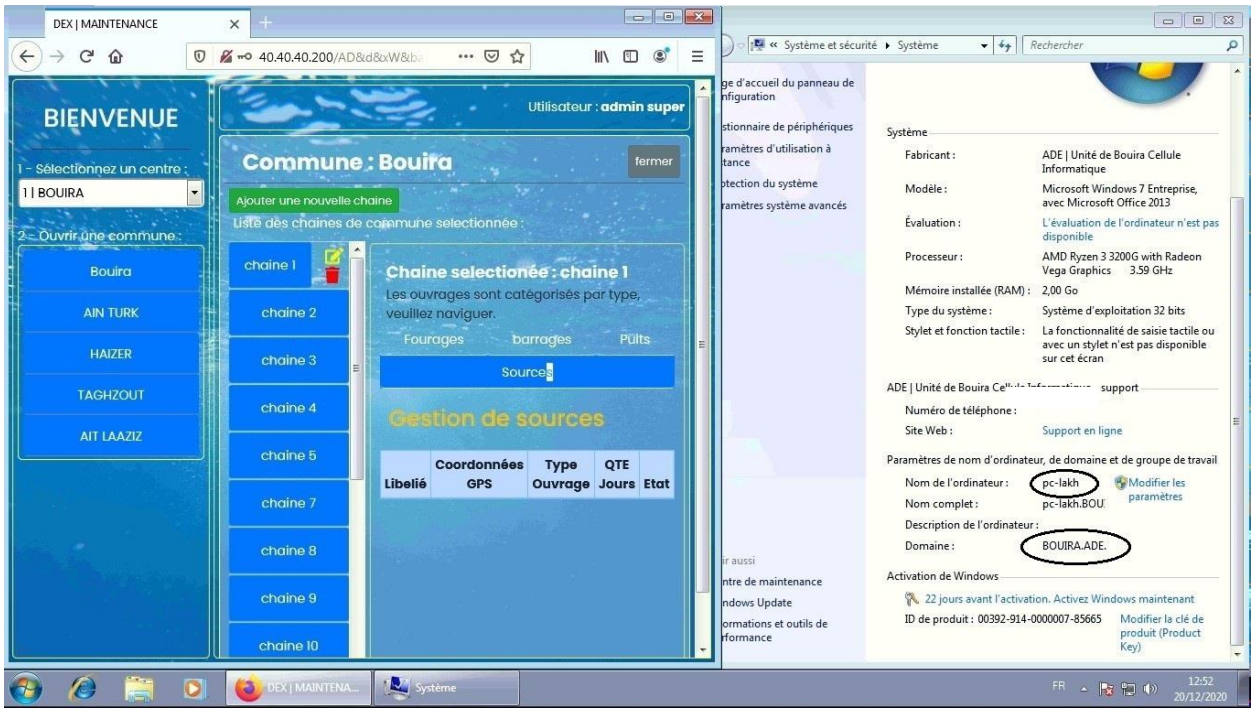


Figure IV. 22 Accès aux applications web.

IV.4.4 La synchronisation des bases de données des NAS (direction Bouira et direction générale)

Création d'un fichier pour le teste de la synchronisation sur le serveur de la direction de Bouira < SRV_FICHIER_U10 >

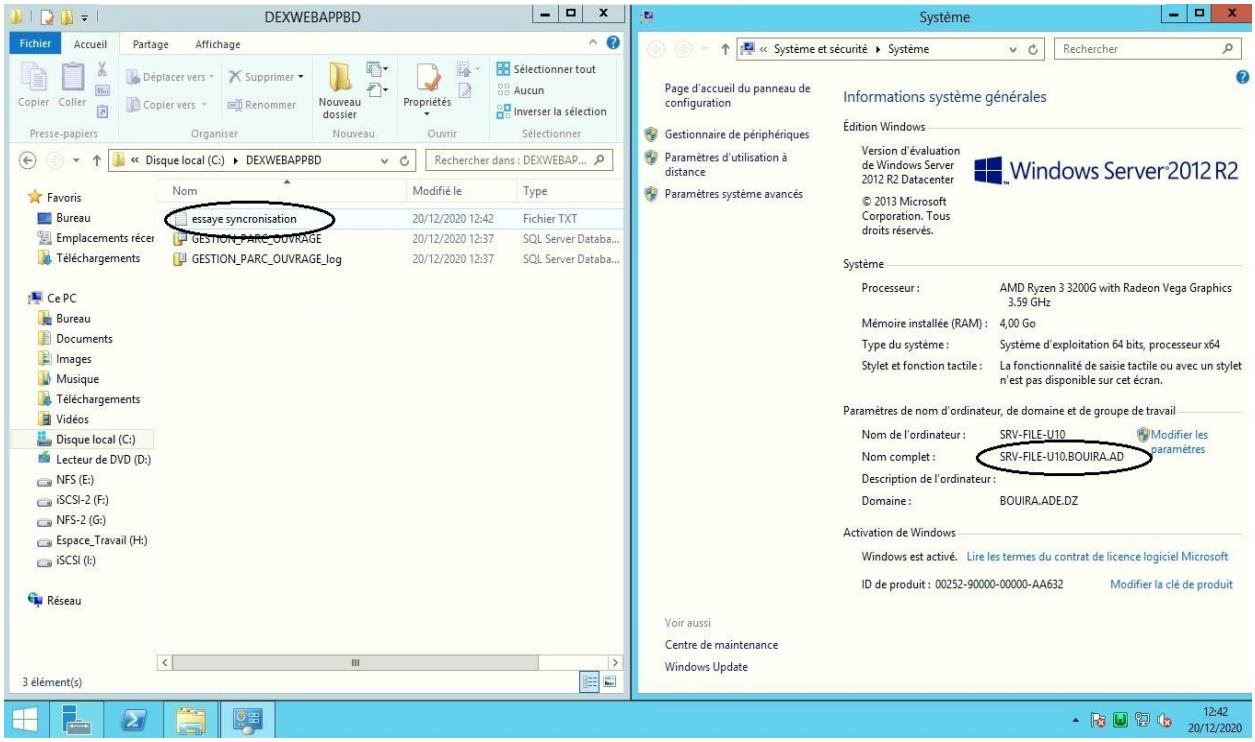


Figure IV. 23 Création d'un fichier.

Vérification de la réplication du fichier sur le serveur de stockage de la DG <SRV_FICHIER_DG > :

En cas de création d'un nouveau dossier ou fichier, la réplique se crée instantanément sur le NAS de la direction générale.

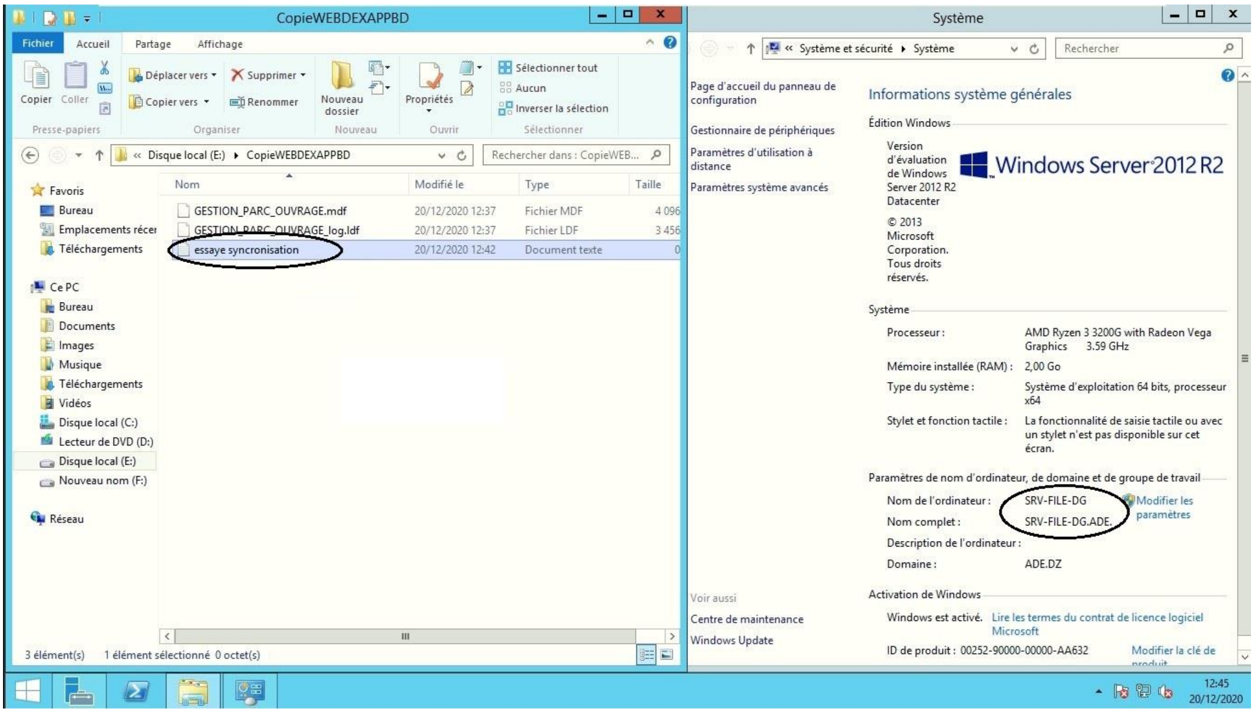
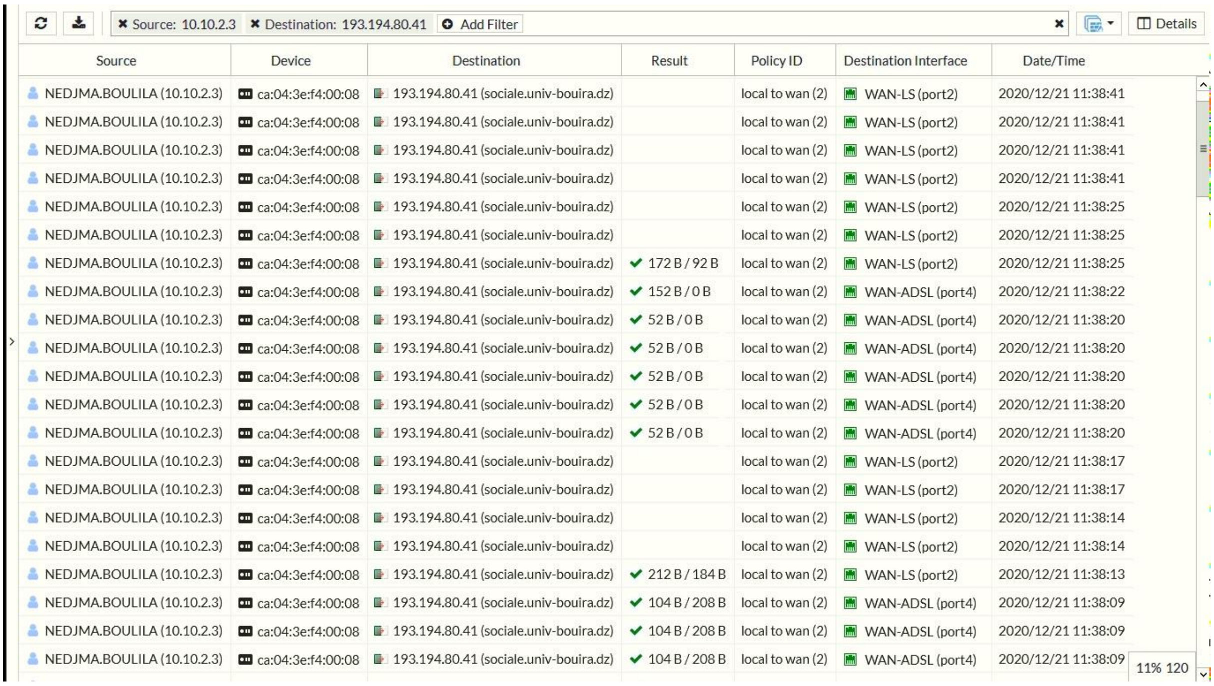


Figure IV. 24 Vérification de la réplication du fichier

IV.4.5 SD-WAN *(Répartition de charge du trafic et « Load Balancing »)*

Le SD-WAN partage le trafic en sessions, afin d'équilibrer la charge entre les deux WAN, si toutefois un lien est HS (Hors Service), l'application redirige tout le trafic sur le lien disponible.



Source: 10.10.2.3 | Destination: 193.194.80.41 | Add Filter | Details

Source	Device	Destination	Result	Policy ID	Destination Interface	Date/Time
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:41
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:41
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:41
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:41
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:25
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:25
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 172 B / 92 B	local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:25
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 152 B / 0 B	local to wan (2)	WAN-ADSL (port4)	2020/12/21 11:38:22
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 52 B / 0 B	local to wan (2)	WAN-ADSL (port4)	2020/12/21 11:38:20
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 52 B / 0 B	local to wan (2)	WAN-ADSL (port4)	2020/12/21 11:38:20
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 52 B / 0 B	local to wan (2)	WAN-ADSL (port4)	2020/12/21 11:38:20
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 52 B / 0 B	local to wan (2)	WAN-ADSL (port4)	2020/12/21 11:38:20
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 52 B / 0 B	local to wan (2)	WAN-ADSL (port4)	2020/12/21 11:38:20
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:17
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:17
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:14
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)		local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:14
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 212 B / 184 B	local to wan (2)	WAN-LS (port2)	2020/12/21 11:38:13
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 104 B / 208 B	local to wan (2)	WAN-ADSL (port4)	2020/12/21 11:38:09
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 104 B / 208 B	local to wan (2)	WAN-ADSL (port4)	2020/12/21 11:38:09
NEDJMA.BOULILA (10.10.2.3)	ca:04:3e:f4:00:08	193.194.80.41 (sociale.univ-bouira.dz)	✔ 104 B / 208 B	local to wan (2)	WAN-ADSL (port4)	2020/12/21 11:38:09

11% 120

Figure IV. 25 Le SD-WAN partage le trafic en sessions.

Le tableau de bord montre des statistiques des accès au WAN, le nombre élevé des accès vers WAN Ls/Mpls est dus au trafic généré à cause de la synchronisation des bases de données, étant donné que la synchronisation ne se fait que via Ls/Mpls.

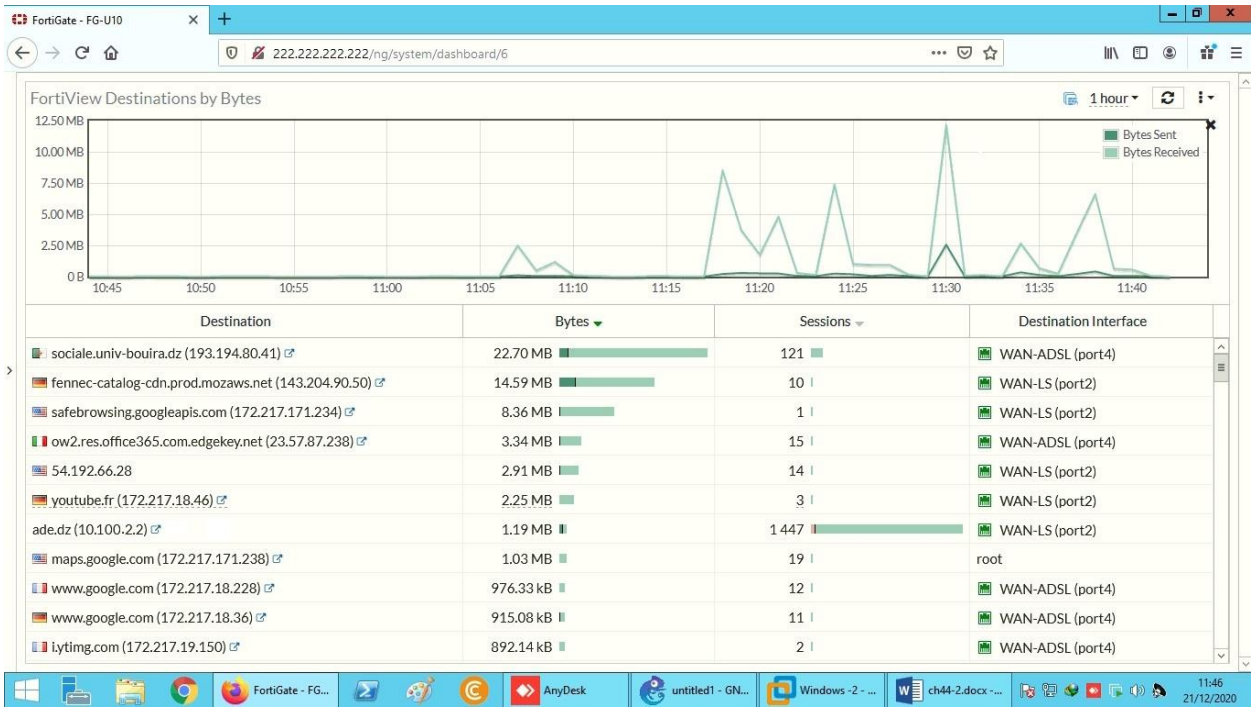


Figure IV. 26 Statistique de la fonctionnalité du partage de charge.

IV.4.6 Filtrage des sites web pour les groupes d'utilisateurs

Le groupe d'utilisateur gp-stagiaires est associé au profil de filtrage web « search-only » dans le lequel tous les sites sons bloqué sauf la catégorie « web search ».

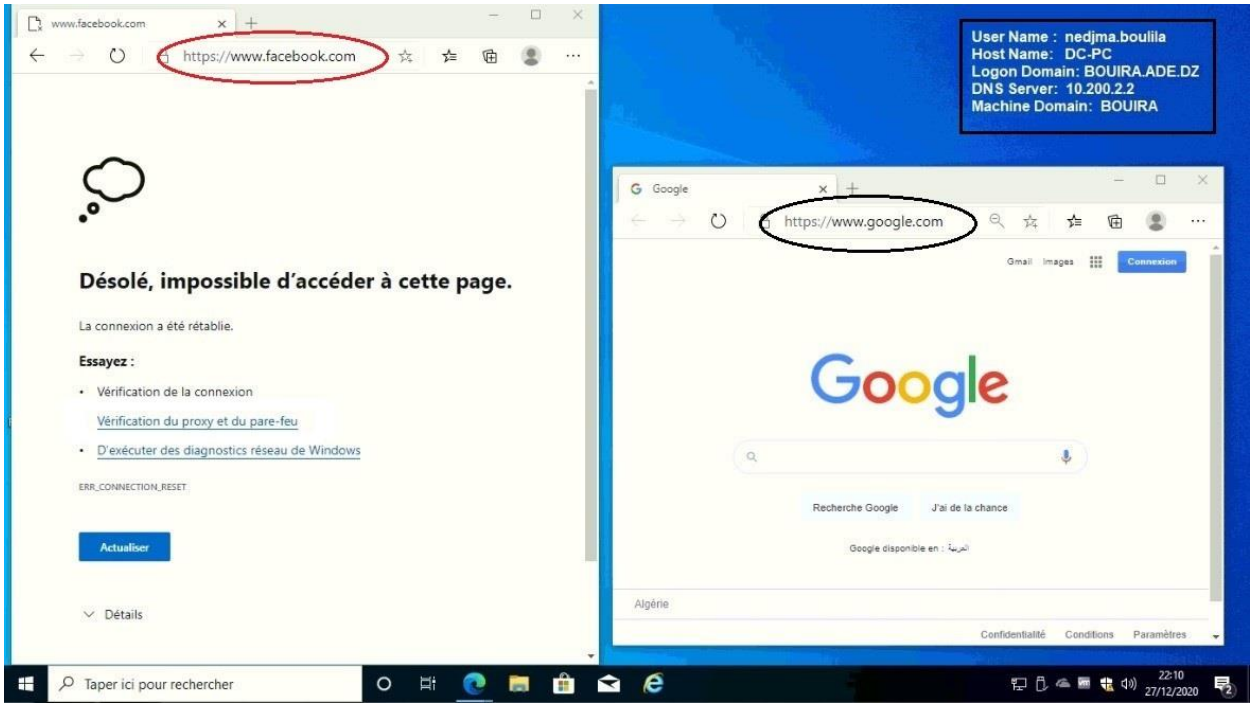
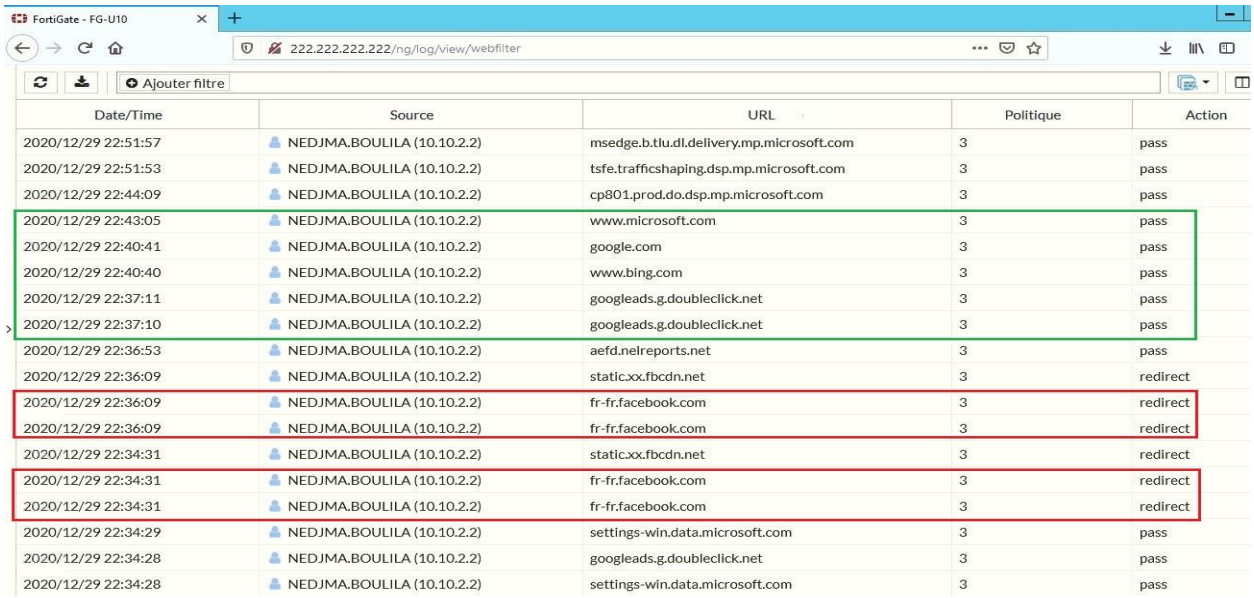


Figure IV. 27 Filtrage des sites web pour les groupes d'utilisateurs.

IV.4.7 Rapport de filtrage de sites web

Le rapport montre que les sites Google et bing étant dans la catégorie « web search » passent, contrairement aux autres sites.



Date/Time	Source	URL	Politique	Action
2020/12/29 22:51:57	NEDJMA.BOULILA (10.10.2.2)	msedge.b.tlu.dl.delivery.mp.microsoft.com	3	pass
2020/12/29 22:51:53	NEDJMA.BOULILA (10.10.2.2)	tsfe.trafficshaping.dsp.mp.microsoft.com	3	pass
2020/12/29 22:44:09	NEDJMA.BOULILA (10.10.2.2)	cp801.prod.do.dsp.mp.microsoft.com	3	pass
2020/12/29 22:43:05	NEDJMA.BOULILA (10.10.2.2)	www.microsoft.com	3	pass
2020/12/29 22:40:41	NEDJMA.BOULILA (10.10.2.2)	google.com	3	pass
2020/12/29 22:40:40	NEDJMA.BOULILA (10.10.2.2)	www.bing.com	3	pass
2020/12/29 22:37:11	NEDJMA.BOULILA (10.10.2.2)	googleads.g.doubleclick.net	3	pass
2020/12/29 22:37:10	NEDJMA.BOULILA (10.10.2.2)	googleads.g.doubleclick.net	3	pass
2020/12/29 22:36:53	NEDJMA.BOULILA (10.10.2.2)	aefd.nelreports.net	3	pass
2020/12/29 22:36:09	NEDJMA.BOULILA (10.10.2.2)	static.xx.fbcdn.net	3	redirect
2020/12/29 22:36:09	NEDJMA.BOULILA (10.10.2.2)	fr-fr.facebook.com	3	redirect
2020/12/29 22:36:09	NEDJMA.BOULILA (10.10.2.2)	fr-fr.facebook.com	3	redirect
2020/12/29 22:34:31	NEDJMA.BOULILA (10.10.2.2)	static.xx.fbcdn.net	3	redirect
2020/12/29 22:34:31	NEDJMA.BOULILA (10.10.2.2)	fr-fr.facebook.com	3	redirect
2020/12/29 22:34:31	NEDJMA.BOULILA (10.10.2.2)	fr-fr.facebook.com	3	redirect
2020/12/29 22:34:29	NEDJMA.BOULILA (10.10.2.2)	settings-win.data.microsoft.com	3	pass
2020/12/29 22:34:28	NEDJMA.BOULILA (10.10.2.2)	googleads.g.doubleclick.net	3	pass
2020/12/29 22:34:28	NEDJMA.BOULILA (10.10.2.2)	settings-win.data.microsoft.com	3	pass

Figure IV. 28 Rapport de filtrage de sites web

IV.5 Architecture actuelle du réseau de L'EP-ADE

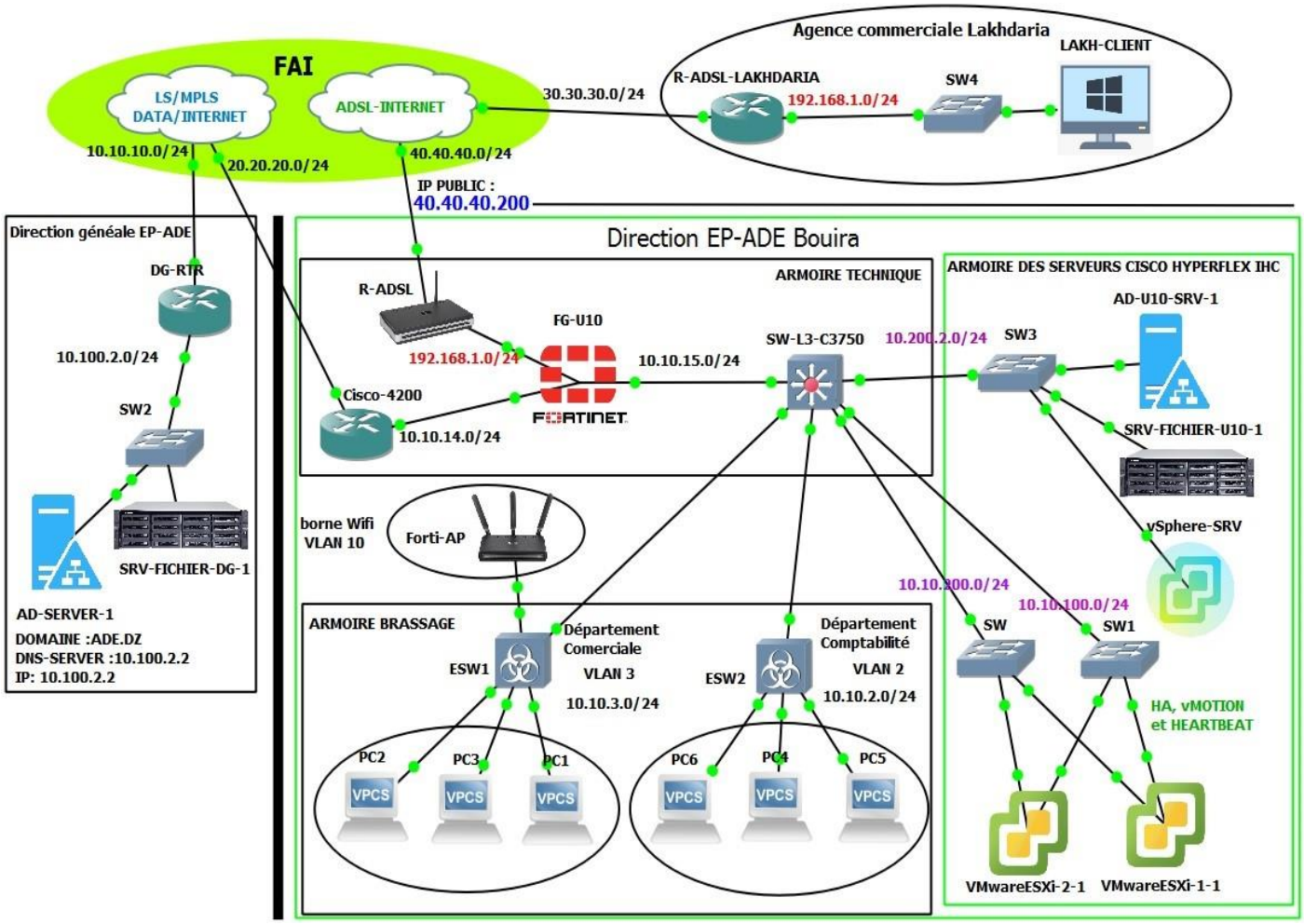


Figure IV. 29 Architecture actuelle du réseau local de L'EP-A.D.E.

- L'armoire technique d'après l'installation des équipements d'interconnexion (figure IV.30).

Figure IV. 30 Etat de l'armoire Technique.

IV.6 **Conclusion**

Ainsi, nous aurions présentés brièvement, les taches effectuées lors de la réalisation de nos objectifs tracés, ayant pour ambition de faciliter aux employés de l'EP-ADE, d'accéder aux ressources du SI, en effet, les tests de fonctionnement montre que les solutions apportés, repondent aux besoins des utilisateurs en terme de débit, accessibilité, disponibilité et d'organisation, accompagné d'une sécurité de données minutieusement ajustée.

Conclusion Générale

Nous aurions atteint nos objectifs tracés, et réalisés les solutions que nous avons préconisés, dans le cadre de l'amélioration de la manière dont l'EP-ADE, exploite les ressources de l'infrastructure de son SI.

Nos objectifs avaient pour ambition de diversifier et d'optimiser l'accès à l'infrastructure du Système d'Information de l'EP-ADE, (étant inaccessible pour les agences commerciales de l'établissement et via des appareils mobiles pour les utilisateurs de la direction de Bouira), en assurant la haute disponibilité et la sécurité des données, lors des échanges entre les sites de l'établissement. Par le billet des nouvelles applications du réseau informatique.

Nos solutions sont basées sur une étude théorique, des principaux composants de l'infrastructure hyper-convergée, du réseau informatique, des menaces et risques liés à ses réseaux, et les mécanismes de sécurités associés, et une étude des besoins spécifiques des utilisateurs de l'EP-ADE. En outre, les taches que nous avons effectuées étaient soumises à des articles, définissant la politique de sécurité, ainsi qu'un plan d'adressage à respecter.

Une phase de test de fonctionnement a été réalisée, et montre qu'en effets, grâce à la solution SD-WAN, qui a assuré la haute disponibilité et la rapidité de l'accès à l'infrastructure du (DataCenter) de la direction de Bouira, les utilisateurs de cet établissement peuvent profiter des multiples services offerts par l'infrastructure, tel que la centralisation des bases de données, la virtualisation des systèmes d'exploitation, la téléphonie IP, la visio-conférence, la messagerie…, et un accès redondant et surveillé à internet.

Grâce à la synchronisation, Les bases de données de l'établissement étant répliquées instantanément sur le NAS de la direction générale, est un atout majeur pour le développement de l'EP-ADE en toute quiétude.

L'ensemble des solutions apportées au support technique, ont fournis une valeur ajoutée à l'exploitation de l'infrastructure de l'EP-ADE, et améliore le quotidien des employés de cette entreprise, sans oublier l'impact positif sur les abonnées (clientèles) de ce dernier.

Notre stage à l'EP-ADE nous a permis d'avoir une formation sur plusieurs maitrises (firewalling, routing and switching, virtualisation, gestion de projet, …), de se familiariser avec l'environnement professionnel, d'élargir et de concrétiser nos connaissances théoriques, une expérience qui va nous servir d'avantage dans notre vie professionnelle.

Bibliographie

[1] M. Haag, « *QHyper-Converged Infrastructure for Dummies* », VMware 2nd special Edition, vol. 64, 2018.

[2] M. Rouse, www.lemagit .fr, mai 2015, consulter le 11/10/2020.

[3] Y. Grandmontagne, https://itsocial.fr, consulter le 12/ 10/2020.

[4] www.vmware.com/fr, consulter le 11/10/2020.

[5] whatis.techtarget.com/fr, Consulter le 29/10/2020.

[6] S. Lowe, « *L'infrastructure hyper-convergée pour les Nuls* », 2e édition spéciale de HPE SimpliVity, vol. 60, John Wiley & Sons, 2019.

[7] H. Ave, T. Franklin, «*Installation et configuration de vCenter Server* », support de cours, 2018.

[8] A. Haji, « *Architecture de Cloud Orientée Service* », Thèse de doctorat, L'Ecole Supérieure des Communications de Tunis, 2016.

[9] M. Seddiki, «*Allocation dynamique des ressources et gestion de la qualité de service dans la virtualisation des réseaux* », Thèse de doctorat, l'Université de Lorraine. France, 2015.

[10] S. Lohier, D. Présent, «*Réseaux et transmissions* », 7eme Edition, vol. 316, 2020.

[11] A. Maini, V. Agrawal, « *Satellite Technology: Principles and Applications*», 3 Edition, vol. 469, 2014.

[12] T. Jyrki, J. Penttinen, « *The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile and Satellite Systems* », 1eré edition, vol.99, 2015.

[13] M. Rhee**, «** *Wireless mobile internet Security* », 2eme Edition, vol. 481, 2013.

[14] Y. Nedjadi, N. Timeridjine, « *Etude et configuration de liaisons virtuelles (VLAN et VPN) au sein de l'entreprise portuaire de Bejaia "EPB"* », Mémoire de fin de cycle, université de Bejaïa. Algérie, 2016.

[15] M. Saidi, *« Méthodes de contrôle distribué du placement de LSP de secours pour la protection des communications unicast et multicast dans un réseau MPLS* », Thèse de doctorat, l'Université de Rennes 1. France, 2008.

[16] A. Kotti Abdmoulah, « *Evaluation, et amélioration des méthodes d'énergie de trafic : mise en œuvre d'une infrastructure d'établissement de LSPs supportant la différentions des services dans les réseaux IP/MPLS* », Thèse de doctorat, école supérieur des communications de Tunis, 2011.

[17] G. Pujolle, « *Les réseaux* », 5eme édition, vol. 1069, 2006.

[18] D. Kreutz, et al, « *Software-Defined Networking: A Comprehensive Survey, Proceedings of the IEEE* », Vol. 103, 2015.

[19] R. Yende, *« Cours de Sécurité Informatique & Crypto* », support de cours, Congo-Kinshasa., vol. 139, 2018.

[20] H. Ahmim, « *Système de détection d'intrusion adaptatif et distribué* », Thèse de doctorat, université Badji Mokhtar. Annaba, 2014.

[21] A. Lokbani, « *Le problème de sécurité par le Data Mining* », Thèse de doctorat, Université Djillali Liabes. Sidi Bel Abbes, 2017.

[22] M. Sidi Mohammed, A. Moulkhaloua, *« Système DE Détection D'intrusions Informatiques par Système Multi_Agents* », Mémoire de master, Universitaire Belhadj Bouchaib. Aïn-Témouchent, 2018.

[23] L. Bloch, C. Wolfhugel, « *Sécurité informatique principes et méthode* », 2eme édition, groupe eyrolles, vol. 292, 2009.

[24] J-F. Carpentier, « *La sécurité informatique dans la petite entreprise : état de l'art et bonnes pratique* », Edition ENI, vol. 265, 2009.

[25] M. Belaoued, « *Approches Collectives et Coopératives en Sécurité des Systèmes Informatiques* », Thèse de doctorat, Université 20 Août 1955. Skikda, 2016.

[26] G. Charpentier et al, « *VIRUS / ANTIVIRUS Nouvelles technologies Réseaux*», support de cours, enseignant : Etienne DURIS, vol. 49, 2004.