REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de Technologie

Département Ingénierie des Systèmes Electriques

Mémoire de Master

Présenté par

NINOUH Nabila BOUKHETAIA Miassa

Filière : Télécommunication

Spécialité : Réseau et télécommunication

Monitoring et supervision de réseau NESDA

Soutenu le 03 /07 /2024 devant le jury composé de:

MAHDI	Ismahan	MCB	Encadrante
KESSAISSIA	Karima	MAA	Présidente
HOCINE	Faiza	MCB	Examinatrice

Année Universitaire : 2023/20224

Remerciements

Tout d'abord, nous remercions ALLAH le tout puissant de nous avoir donné la santé, le courage et la volonté de réaliser ce présent travail.

Nous remercions sincèrement Madame Mahdi Ismahane, notre promotrice, pour son encadrement exceptionnel, ses conseils avisés et sa disponibilité tout au long de cette période. Son soutien constant et ses orientations pertinentes ont été essentiels pour mener à bien ce projet.

Nous souhaitons également exprimer notre gratitude à Monsieur Hebabcha Kamel, notre encadrant, pour son accompagnement, ses précieuses recommandations et son expertise. Sa rigueur et son implication nous ont permis d'avancer sereinement dans notre travail.

Nous tenons également à remercier Monsieur Lekrim Mohamed, pour sa présence indispensable et son aide précieuse lors des moments critiques. Son intervention a été d'un grand secours et a grandement contribué au bon déroulement de notre projet.

Nous souhaitons adresser un remerciement à Monsieur Ayoub Mohamed Dahman, pour son aide dans la résolution des problèmes d'intégration de FortiGate dans le FortiManager et le FortiAnalyzer. Son expertise a été déterminante pour le succès de cette tâche.

Nous remercions toute l'équipe de NESDA pour leur accueil chaleureux. Leur bienveillance ont rendu notre stage encore plus enrichissant.

Nous tenons à exprimer notre profonde gratitude à notre famille et à nos amis pour leur soutien et leurs précieuses contributions tout au long de notre parcours académique.

Nous exprimons notre profonde gratitude au jury de PFE. Votre conseils précieux et expertise et vos retours constructifs auront grandement enrichi notre travail et contribué à notre développement professionnel.

Enfin, nous tenons à remercier tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce projet. Leur aide et leurs encouragements nous ont été très précieux.

Merci à tous.

Dédicaces

Je dédie ce travail à mes chers parents qui m'ont toujours soutenu et motivé dans mes études et qui ne m'ont jamais oublié en priant pour ma réussite.

Sans eux, je ne serais certainement pas arrivé à ce point.

Par conséquent, tout ce travail a été le résultat de leurs encouragements tout au long des étapes d'études que j'ai traversées.

À mes frères Sami, Mohamed et Sid Ali, ainsi qu'à ma chère et unique sœur, merci de m'avoir soutenu pendant mes études et d'être toujours à mes côtés.

À l'âme de mes grands-parents, que je souhaitais être avec moi en ce jour important, leur amour et leurs prières ont été le moteur de ma réussite. Je n'ai jamais oublié, mon cher grand-père, ton désir de me voir devenir une belle diplômée. Même s'ils sont absents parmi nous aujourd'hui, ils sont toujours présents dans mon cœur.

À mes amis et à mes professeurs, ainsi qu'à tous ceux qui m'ont soutenu, encouragé et conseillé sans réserve, je tiens à exprimer ma sincère gratitude.

Miassa

Dédicaces

Je dédie ce projet de fin d'études à mes parents bien-aimés, dont les prières constantes et l'encouragement indéfectible m'ont porté tout au long de ce parcours. Votre soutien inébranlable a été une source de force et de motivation inestimable. Vous êtes tous ma source d'inspiration et je vous remercie du fond du cœur pour tout ce que vous avez fait pour moi.

À mes frères, Merouan et Nedjem Eddine, vos encouragements m'ont toujours poussé à aller plus loin et à me dépasser. À ma sœur unique, dont la présence chaleureuse et les mots réconfortants m'ont été d'un grand réconfort.

Et enfin, à notre chouchou de la famille, mon neveu Akçil, ta joie de vivre et ton sourire ont été une lumière dans les moments les plus difficiles

Tout au long de ma vie, j'ai toujours suivi l'idée que chacun a son horloge, et vous m'avez tous aidé à trouver et à suivre la mienne.

Avec tout mon amour et ma gratitude,

Nabila

Sommaire

Table des matières

Liste Des Abréviations

Liste Des Figures

Liste Des Tableaux

Résumé **1**

Introduction générale **3**

Chapitre I: Généralités sur l'administration des réseaux informatique

Introduction **6**

I. Réseau informatique **7**

I.1. Définition 7

I.2. Types de réseau informatique 7

I.2.1. Réseau filaire 7

I .2.2 réseaux sans fil 7

I.3. Classification D'un réseau informatique 8

I.3.1 selon la portée 8

I.3.2 selon la topologie 9

I.3.3. Selon l'architecture 11

II.1.OSI 13

II.2.TCP/IP 13

I.3. SDN 14

II.4. MPLS 15

II.5. IP/MPLS 16

III. les serveurs **17**

III.1 Types des serveurs 17

III.1.1 serveur de fichiers 17

III.1.2 serveur d'applications 17

III.1.3 serveur WEB 17

III.1.4 Les serveurs DNS 18

III.1.5 serveur de bases de données 18
III.1.6 Serveur Virtual 18
III.2 Rôle des serveurs 19
IV Réseaux virtuels **19**
IV.1 Principe de virtualisation 20
IV.2 Principaux logiciels de virtualisation 20
IV.2.1 VMware Workstation Pro : 20
IV.2.2 Oracle VM VirtualBox : 20
IV.2.3 Microsoft Hyper-V: 21
IV.2.4 Red Hat virtualisation 21
IV.3 Les avantages et les limites de la virtualisation 22
IV.4 La sécurité en virtualisation 23
Conclusion **24**

Chapitre II : Solutions de sécurité des réseaux

Introduction **25**
I. Sécurité réseau **25**
I .1Définition : 25
II.2 types des attaques informatiques 25
II .2.1 Attaques spoofing 25
II.2.2 Déni de service (DOS « Denial Of Service ») 26
II.2.3 Déni de service distribué (DDOS) 26
II.2.4 Sniffing (écoute du réseau) 27
II.3 Le système de détection d'intrusion IDS/IPS **28**
III. Protocoles de sécurité **30**
III.1 HTTPS 30
III.2 SSH 30
III.3 SSL 31
III.4 IPSec 32
III.5 PGP 33
III .6 VPN 33
IV. Mécanismes de sécurité **34**

IV.1 Crypto 34
IV.2 Antivirus 34
IV.3 Firewall 34
V. Les différents types de pare-feu matériels **35**
V.1 Les pare-feu matériels 35
- ✓ **Avantage** 35
- ✓ **Limites [35]** 36

V.2 Les pare-feu logiciel 36
- ➢ **Les pares-feux personnels** 36
- ➢ **Les pares-feux plus-sûr** 36

VI. Solutions de Pare feu logiciels **36**
Conclusion **37**

Chapitre III: Mise en place d'une solution d'administration et de sécurisation Firewall Fortinet

III.1 Présentation de l'organisme d'accueil **55**
III.1.1 Historique de l'entreprise 39
III.1.2 Taches de l'agence : 39
III.1.3 Organigramme de l'organisme d'accueil : 39
III.2 Etude de l'existant **41**
III.2.1 Problématique 41
III.2.2 Infrastructure réseau 41
III.2.3 Matériels et logiciels exploités 42
III.2.4 Principales composantes d'Active Directory 44
III.2.4.1 Les étapes d'organisation : 45
III.3 Failles de sécurités constatées : **48**
III.3 Implémentation de la solution de sécurité : **50**
III.3.1 La topologie de réseau à étudié 50
III.3.2 Installation et configuration des matériaux et logiciels utilisés : 50
III.3.2.1 Installation de le fortiGate 50
III.3.2.2 Configuration de Fortigate 52
III.3.2.3 Installations de FortiManger 60

III.3.2.4 Configuration de FortiManger 61
III.3.2.5 L'installation de FortiAnalyzer 64
III.3.2.6 La configuration de FortiAnalyzer 64
III.3.3 Configuration de la topologie via VPN IPsec 65
III.3.4 Integration des fortigates dans le fortimanager et fortianalyzer 69
III.3.4.1 Intégration de fortigate dans le fortimanager 69
III.3.4.2 Intégration de fortigate dans le fortianalyzer 72
III.4 Teste et simulation :..... 78
III.4.1 Exécution des codes CLI : 78
III.4.2 Les codes CLI exécutés pour chaque alertes 81
III.5 Conclusion générale..... 91
Bibliographie..... 92

Table des abbreviations

A

AVS Antivirus Software

AVS Advanced Visual Systems

APT Advanced Persistent Threat

AD Active Directory

AD DS Active Directory Domain Services

ANADE Agence Nationale d'appui et de Développement de l'Entreprenariat,

B

BTS Base Transceiver Station

BSD Berkeley Software Distribution

C

CD Compact Disc

Cisco ASA Adaptive Security Appliance

D

DNS Domain Name System

DVD Digital Versatile Disc

DOS Disk Operating System

DDOS Distributed Denial of Service

DHCP Dynamic Host Configuration Protocol

F

FSSO

H

HTML HyperText Markup Language

Hyper-V Hyper version

HTTPS HyperText Transfer Protocol Secure

I

IP Internet Protocol

IBM International Business Machines

IDS Intrusion Detection System

IPS Intrusion Prevention System

IPSec Internet Protocol Security

IIS Internet Information Services

IOS Indicateur d'Ordonnancement de Sécurité

L

LAN Local Area Network

LSP Label Switched Path

LER Label Edge Router

LSR Label Switching Router

LUN Logical Unit Number

LDAP Lightweight Directory Access Protocol)

M

MAN Metropolitan Area Network

MPLS	Multiprotocol Label Switching
MAC	Macintosh
MacOS	Macintosh Operating System
MySQL	My Structured Query Language,

N

NESDA	National Entrepreneurship Support and Developement Agency
NGFW	Next Generation Firewall
NAC	Network Access Control

O

OSI	Open Systems Interconnection
OU	Organizational Unit

P

PDA	Personal Digital Assistant
PAN	Persona Area Network
P2P	Peer to Peer
PRA	Plan de Reprise d'Activité
PFSense	Packet Filter Sense
PGP	Pretty Good Privacy
PHP	Hypertext Preprocessor

Q

Qos	Quality of Service

R

RSA	Rivest, Shami, Adlman

S

SDN	Software Defined Networking
SSL	Secure Sockets Layer
SSH	Secure Socket Shell

T

TCP	Transmission Control Protocol
TLS	Transport Layer Security

U

USB	Universal Serial Bus
UTM	Unified Threat Management

V

VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VXLAN	Virtual Extensible LAN

W

WAN	Wide Area Network
WIFI	wireless fidelity
Web PI	Web Platform Installer

Liste des figures

Chapitre I: Généralités sur l'administration des réseaux informatique

Figure I.1 : Réseau PAN 7
Figure I.2 :Réseau LAN..... 7
Figure I.2 :Réseau MAN..... 8
Figure I.2 :Réseau WAN..... 8
Figure I.5: La topologie en bus 9
Figure I.6:La topologie en étoile 9
Figure I.7: La topologie Arborescente 9
Figure I.8: La topologie Arborescente 10
Figure I.9: La topologie maillée 10
Figure I.10: Réseau Peer to peer vs client/serveur 11
Figure I.11: Architecture réseau Trois tiers 11
Figure I.12: OSI vs TCP/IP 12
Figure I.13: Openflow dans l'architecture SDN 13
Figure I.14: Implémentation d'un réseau MPLS 15
Figure I.15: Principe du réseaux IP/MPLS 15

Chapitre II : Solutions de sécurité des réseaux

Figure II.1: Attaque spoofing 26
Figure II.2: Attaque DOS 26
Figure II.3 : Attaque DDOS 27
Figure II.4: Attaque Sniffing 28
Figure II.5: Différence entre IDS et IPS 29
Figure II.6: Fonctionnement de Protocol de sécurité HTTPs 30
Figure II.7 : Fonctionnement de Protocol de sécurité SSH 31
Figure II.8: Fonctionnement de Protocol de sécurité SSL 32
Figure II.9 : Protocol de sécurité IPSec..... 32
Figure II.10: Protocol de sécurité PGP..... 33
Figure II.11: Protocol de sécurité VPN 34

Chapitre III : Mise en place d'une solution d'administration et de sécurisation Firewall Fortinet

Figure III.1 : Organigramme de l'organisme d'accueil 40
Figure III.2 : Architecture réseau de la NESDA 41
Figure III.3: Unité d'organisation dans un Domain AD 44
Figure III.4 : création d'unité d'organisation 45
Figure III.5 : création de group UMBB-GG 45
Figure III.6: création d'ordinateur UMBB_01 46
Figure III.7: Création d'un nouvel utilisateur 46
Figure III.8: insertion de mot de passe pour l'utilisateur 47
Figure III.9 : La topologie de réseau à étudié 49
Figure III.10: Création de la machine virtuel FG_01 50
Figure III.11: Configuration des cartes réseaux 50
Figure III.12: Configuration des cartes réseaux pour les adaptateurs 52
Figure III.13: L'interface web de fortigate 55
FigureIII.14: L'interface graphique de FortiGate 55
Figure III.15: L'affichage des interfaces de fortigate 56
Figure III.16 : Configuration de Gateway 57
Figure III.17: Configuration de politique de fortigate (pare-feu) 58
Figure III.18: L'authentification de l'utilisateur au niveau de serveur LDAP 59
Figure III.19: Configuration de FSSO 60
Figure III.20 : Instalation de fortimanager 61
Figure III.21 : L'interface web de FortiManager 63
Figure III.22: L'interface graphique de FortiManager 63
FigureIII.23 : L'interface web de FortiAnalyzer 65
FigureIII.24 : L'interface graphique de FortiAnalyzer 65
Figure III.25: Configuration de VPN 66
Figure III.26: Authentification de VPN pour l'interface de fortigate de la DG 66
Figure III.27Création automatique de politique de sécurité et de route statique 67
Figure III.28: Configurer FG de l'annexe de Boumerdes 67
Figure III.29: Authentification VPN pour l'interface de FG de l'annexe 68
Figure III.30: Configuration des tunnels Ipsec(l'état : Down) 68
Figure III.31: Vérification de l'état de tunnel (L'état : Up) 69
FigureIII.32 : Ajout de numéro de série de fortimanager au fortiagte 71
Figure III.33: Le fortigate avant l'autorisation 71
Figure III.34: L'autorisation de fortigate dans le fortimanager 71
Figure III.35: L'interface graphique de FortiGate depuis le FortiManager 72
Figure III.36 : Ajout de numéro de série de fortianalyzer dans le fortigate 74
Figure III.37 : Le fortigate avant l'autorisation 74
Figure III.38 : Autorisation de fortigate dans le fortianalyzer 75
FigureIII.39 : Confirmation d'intégration de fortigate dans le fortianalyzer 75

Figure III.40: Courbe graphique montrant le taux de fonctionnement de fortigate…… ….76

Figure III.41 : les deux fortigates sont integrés dans le fortimanager..... 76
Figure III.42: Les deux FortiGates sont intégrés dans le fortianalyzer..... 77
Figure III.43: Cordonnées géographique de fortigate de l'annexe de Boumerdes..... 77
Figure III.44: l'emplacement et le bon état des FortiGates gérés sur Google Maps 78
Figure III.45 : Une capture d'écran montre l'exécution de code de la règle d'alerte 79
Figure III.46 : Les dispositifs fortigates sélectionnés 79
Figure III.47 : Confirmation de l'exécution de script …...……...80

Figure III.48 : Les règles d'alerte exécutées au niveau de FortiManager..... 80
Figure III.49: L'exécution avec succès de script..... 81
Figure III.50 :Modifications apporté au fortigate de la DG après l'exécution de CLI ...…….81

Figure III.51 : Modifications apporté au fortigate de l'annexe après l'exécution de CLI 82
Figure III.52 : Log event reçu par le fortigate de l'annexe de Boumerdes après le teste d'alert.....84

Figure III.53 : Log event reçu par le fortigate de l'annexe de Boumerdes après le teste d'alerte…..84

Figure III.54 : Log reçu sur le fortimanager après la désactivation de la deuxième interface de l'annexe de Boumerdes…….86

Figure III.55 Réactivation de l'interface désactivée 86
Figure III.56 : Logs reçus d'après le FG au FA après la réactivation de l'interface bloqué…87

Figure III.57 : Log reçu sur le FA indiquant l'état de l'interface pendant la période où elle était désactivée……..87

Figure III.58 : Log reçu sur le FA indiquant la reprise de la connexion de l'interface…….....88

ملخص

مع تزايد انتشار الهجمات والتهديدات السيبرانية، لم يعد تأمين الشبكات خيارًا، بل أصبح ضرورة مطلقة للشركات التي تتطلع إلى حماية أعمالها على المدى الطويل وبناء ثقة العملاء. لقد أصبح تحديا حاسما للشركات من جميع الأحجام. ويكمن التحدي في المراقبة والإدارة المستمرة والحماية الكافية للشبكات. ولهذا السبب قمنا بتطوير حل مركزي ومراقبة الشبكة من قبل الشركة الأم فقط، وبالتالي التكيف مع قدرات الشركة ومهندسيها. يتميز مشروعنا بتبسيط تشغيل الشبكة دون إضاعة الوقت أو الجهد.

الكلمات المفتاحية: الحماية, جدار الحماية, VPN ,الهجمات السيبرانية fortimanger, fortigate, FortiAnalyzer

Résumé

Les cyberattaques et les menaces sont de plus en plus répandues, ce qui rend la sécurisation des réseaux indispensable pour les entreprises qui souhaitent préserver leur activité à long terme et renforcer la confiance de leurs clients. Les entreprises de toutes tailles font face à un défi crucial. Le défi consiste à surveiller, gérer de manière continue et assurer une protection adéquate des réseaux. C'est la raison pour laquelle nous avons mis en place une solution axée sur la centralisation et la surveillance du réseau par l'entreprise mère, en s'adaptant aux compétences de l'entreprise et de ses ingénieurs. Notre projet se démarque en rendant le réseau plus facile à utiliser sans perdre de temps ni d'efforts.

Mots Clés : Sécurité, FireWall, cyberattaques, VPN, Fortigate; Fortimanger

Abstract

Cyberattacks and threats are becoming increasingly prevalent, making network security essential for businesses looking to safeguard their long-term operations and enhance customer trust. Companies of all sizes are facing a critical challenge: monitoring, continuously managing, and ensuring adequate protection for their networks. This is why we have implemented a solution focused on centralizing network monitoring within the parent company, adapting to the skills of the business and its engineers. Our project stands out by making network operations more user-friendly without wasting time or effort.

Keywords : Security, FireWall, Attacks, VPN, Fortigate, FortiManger, FortiAnalyzer

Introduction Générale

Introduction générale

La gestion efficace des réseaux et la sécurité des données sont des éléments essentiels dans un environnement informatique en perpétuelle évolution afin de garantir la sécurité, la performance et la disponibilité des infrastructures de l'entreprise, surtout lorsque ces réseaux s'étendent sur plusieurs sites ou antennes.

Antérieurement, la gestion et l'analyse des alertes à distance dans les FortiGates des annexes depuis la Direction Générale (DG) étaient inefficaces. Chaque fois que les administrateurs réseaux de NESDA voulaient mettre en place une nouvelle règle d'alerte, ils devaient la proposer à chaque annexe. De plus, bien que les FortiGates des annexes puissent être configurés pour envoyer des alertes directement au FortiGate de la DG via syslog, cette approche présente des limitations significatives en termes de gestion et d'efficacité, rendant difficile l'analyse et la gestion centralisée des alertes.

Avant de proposer la solution pour centraliser la gestion et offrir une analyse approfondie des journaux de sécurité de la Nesda, il est primordial de bien appréhender les infrastructures réseaux actuelles.

Nous avons rassemblé quelques concepts sur l'administration des réseaux informatiques dans le premier chapitre intitulé "Notions et concepts sur l'administration des réseaux". Ce chapitre offre une vision détaillée des éléments essentiels sur les réseaux informatiques.

Dans le deuxième chapitre qui s'intitule "Solutions de sécurité des réseaux", nous avons examiné les problèmes majeurs tels que les attaques informatiques. Ensuite, nous avons examiné les solutions de sécurité des réseaux, un élément essentiel pour prévenir les attaques informatiques et assurer la confidentialité et l'intégrité des données.

Enfin, notre projet sera terminé par l'ajout d'un troisième chapitre, afin de passer des concepts théoriques à la mise en pratique concrète.
Tout d'abord, nous présenterons l'organisme d'accueil et son organigramme. Il est crucial de décrire les différentes étapes de mise en place de notre solution, car nous débuterons par décrire l'environnement de développement sur le système de virtualisation La VMware

Workstation, puis la mise en place de la solution des équipements Fortinet virtuels, les logiciels, les étapes d'installation, la configuration et les tests.

Nous terminons par une conclusion générale qui résume l’apport essentiel de notre travail.

Chapitre I :

Notions et concepts sur l’administration des réseaux informatique

Introduction

La gestion des réseaux informatiques implique de nombreuses tâches importantes pour assurer le bon fonctionnement, la sécurité et la maintenance d'un réseau d'entreprise. Les concepts clés de la gestion des réseaux informatiques comprennent la configuration, l'installation, la sécurité, la maintenance des réseaux, d'appareils et d'applications informatiques, qu'ils soient centralisés ou distribués. Dans ce chapitre ; nous allons présenter le réseau informatique et différents modèles et serveurs utilisés, couvrant des sujets allant des principes fondamentaux des réseaux informatiques aux nouvelles technologies de virtualisation.

I. Réseau informatique

I.1. Définition

Un réseau informatique est un ensemble d'appareils informatiques (ordinateurs et périphériques) connectés entre eux via un support de communication (tel qu'un câble : réseau câblé ou des ondes radio : réseau sans fil) qui permet la communication (transmission d'informations électroniques) et partage de ressources (matériel et logiciel) [1].

I.2. Types de réseau informatique

I.2.1. Réseau filaire

Un réseau filaire, comme son nom l'indique, est un réseau utilisé avec une connexion filaire. Ce réseau utilise des câbles Ethernet pour connecter les ordinateurs et les appareils via des routeurs ou des commutateurs [2].

I .2.2 réseaux sans fil

Un réseau sans fil est un réseau qui permet à au moins deux appareils de communiquer par ondes radio sans connexion par câble. Il connecte différents postes (Ordinateur, laptop, PDA, Caméra wifi, etc.) entre eux par ondes radio.

Un réseau sans fil se compose de stations de base cellulaires (BTS) avec une couverture point à point ou point-multipoint. Ce dernier type est utilisé dans la plupart des réseaux locaux et peut couvrir un groupe d'abonnés au sein d'une zone prédéfinie. La connexion sans fil du BTS à l'abonné est appelée canal descendant (downstream), et le canal montant(upstream) fait référence à la connexion de l'abonné au BTS [3].

I.3. Classification D'un réseau informatique

I.3.1 selon la portée

- **Réseau personnel PAN (Persona Area Network) :** Il s'agit de la portée minimale d'un réseau point à point de type, qui est un réseau sans fil à courte portée, de l'ordre de plusieurs dizaines de mètres. Ce type de réseau est généralement utilisé pour connecter appareils [1]**.**

Figure 1.1 : Réseau PAN [4]

- **Réseau local LAN (Local Area Network) :** Ce type de réseau est le plus répandu dans les entreprises et est plus grand qu'un PAN, permettant par exemple la connexion d'ordinateurs à proximité et de périphériques dans un même bâtiment. Il S'étendant sur des centaines de mètres [5].

Figure I.2: Réseau LAN [5]

- **Réseau métropolitain MAN (Metropolitan Area Network) :** C'est un réseau métropolitain, il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN, et il s'étend sur plusieurs kilomètres dans une ville [5].

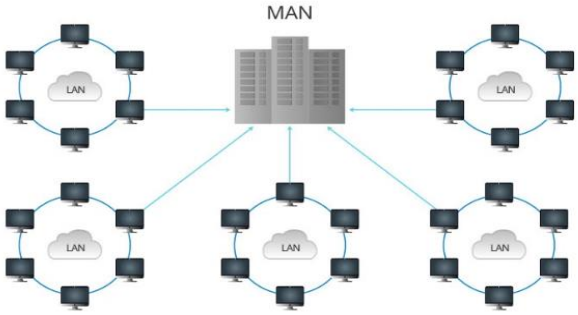


Figure I.3 : Réseau MAN [4]

- **Réseau étendu WAN (Wide Area Network):** Ce type de réseau est constitué de réseaux de type LAN, voir MAN, les réseaux étendues sont capables de transmettre les informations sur des centaines et milliers de kilomètres à l'échelle d'un pays ou à l'échelle mondiale. Ils fonctionnent grâce à des équipements réseau appelés routeurs [5].

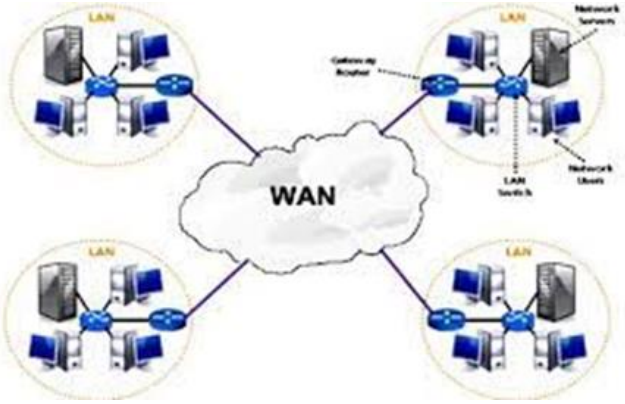


Figure I.4: Réseau WAN [7]

I.3.2 selon la topologie

- **Topologie en bus** : Le bus est le segment central par lequel les données sont transmises sur toute la longueur du réseau. Une seule station peut émettre à la fois, avec une « prise » au bout pour libérer le canal. Les bus offrent une tolérance aux pannes indépendante et sont faciles à déployer.

Cependant, il existe des inconvénients tels que l'indisponibilité du réseau lors des interruptions, les limitations de longueur de câble et l'incapacité de régénérer les signaux [7].

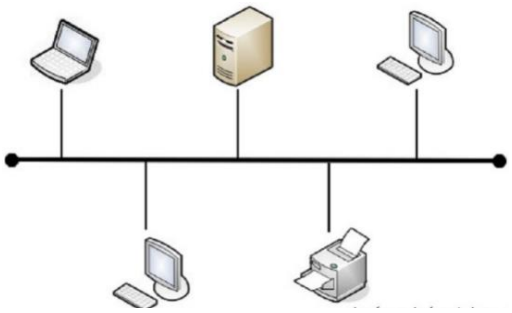


Figure I.5: La topologie en bus[w12]

- **Topologie en étoile :** La topologie en étoile est courante dans les réseaux Ethernet RJ45. Chaque station est reliée à un hub central. Ce type de réseau est facile à surveiller et la panne d'une station n'affecte pas l'ensemble du réseau. Cependant, cela nécessite davantage de câbles et une panne de hub entraîne l'arrêt de l'ensemble du réseau. De plus, le débit réel est souvent inférieur à celui des autres topologies **[7].**

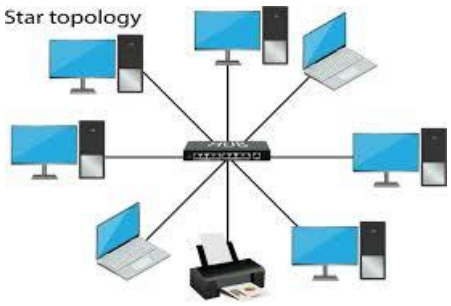


Figure I.6: La topologie en étoile [8]

- **Topologie en anneau :** Chaque équipement est relié à l'équipement voisin de telle sorte que l'ensemble forme une boucle fermée. Les nœuds sont actifs, ils reçoivent et régénèrent le message. Mais en cas de coupure de l'anneau, le réseau est interrompu, ce qui est le cas lors de l'installation d'une nouvelle station de travail **[5].**

Figure I.7: La topologie Arborescente [10]

- **Topologie Arborescente :** C'est une Structure arborescente hiérarchique. Un réseau arborescent se compose d'une série de réseaux en étoile connectés à un seul nœud

central par des hubs. Cette structure est couramment utilisée dans les réseaux locaux [9].

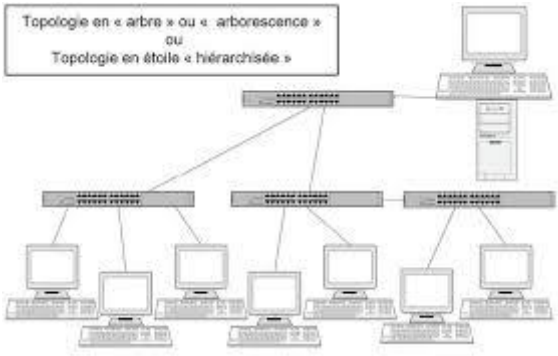


Figure I.8: La topologie Arborescente [10]

- **Topologie maillée :** Pour des raisons de défaillances, le réseau est maillé où chaque nœud est caractérisé par sa connectivité, c'est-à-dire que pour accéder à un même nœud, il existe plusieurs chemins, cette structure optimisé emploi des ressources en répartissant la charge entre les différentes voies [9].

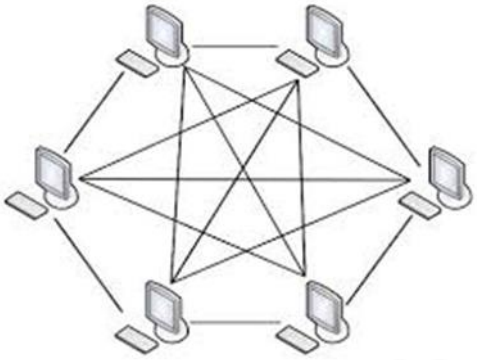


Figure I.9: La topologie maillée [8]

I.3.3. Selon l'architecture

- **Les réseaux Post à post (Peer to Peer= P2P):** Dans une architecture poste à poste, tous les ordinateurs sont identiques ; il n'y a pas de machine spécifique. Cela signifie que tous les ordinateurs du réseau peuvent partager librement cette ressource. Par conséquent, un ordinateur connecté à une imprimante peut partager cette imprimante, permettant ainsi à tous les autres ordinateurs d'y accéder via le réseau [11].

- **Architecture client/serveur:** De nombreuses applications fonctionnent dans un environnement client/serveur. Cela signifie que l'ordinateur client se connecte à un serveur (un ordinateur généralement très puissant en termes de capacités d'entrée/sortie

et qui fournit des services). Dans un environnement client/serveur pur, les ordinateurs du réseau (clients) ne peuvent voir que le serveur. C'est l'un des principaux avantages de ce modèle [11].

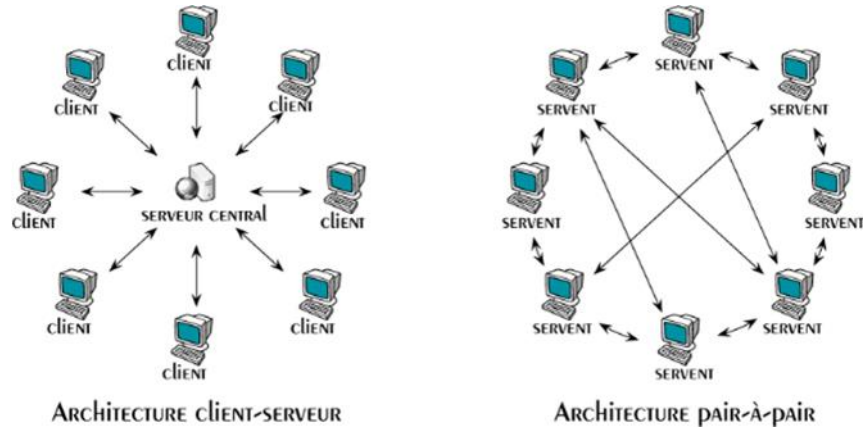


Figure I.10: Réseau Peer to peer vs client/serveur [10]

- **Architecture Trois tiers :** Dans l`architecture à 3 niveaux (appelées architecture 3-tier), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre : Le client, le demandeur de ressources. Le serveur d'application, le serveur chargé de fournir la ressource mais faisant appel à un autre serveur. Le serveur secondaire, fournissant un service au premier serveur [11].

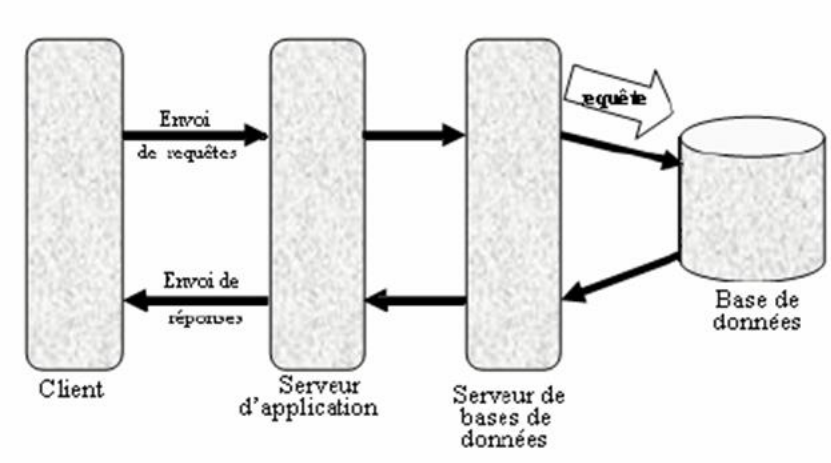


Figure I.11: Architecture réseau Trois tiers [12]

II. Modèles réseau

II.1.OSI

Le modèle OSI est une manière standardisée de diviser le processus de communication entre deux entités en plusieurs blocs. Chaque bloc issu de cette segmentation est appelé une couche. Une couche est un ensemble de services qui atteignent un objectif spécifique. L'avantage de cette segmentation est que chaque couche du modèle OSI communique avec les couches situées au-dessus et au-dessous d'elle (également appelées couches adjacentes). La couche ci-dessous fournit les services utilisés par le niveau actuel, et le niveau actuel fournit les services dont la couche supérieure a besoin pour remplir son rôle[w1].

II.2.TCP/IP

TCP/IP est une suite de protocoles. L'acronyme TCP/IP signifie « Transmission Control Protocol / Internet Protocol ». TCP/IP représente d'une certaine manière toutes les règles de communication sur internet et repose sur la notion d'adressage IP, c'est-à-dire la pratique consistant à fournir une adresse IP à chaque machine du réseau pour permettre le routage des paquets de données. Il est conçu pour répondre à certains critères, notamment :

- Division des messages en paquets
- Utilisation du système d'adressage
- Routage des données sur le réseau (routage)
- Vérification des erreurs de transmission des données.

Le protocole TCP/IP étant antérieur au modèle OSI, il ne suit pas réellement ce modèle. Cependant, on peut combiner approximativement les différents services utilisés et fournis par TCP/IP avec le modèle OSI et ainsi obtenir un modèle à 4 couches[w1].

Modèle OSI

Cette couche gère les formats de données entre les logiciels.	**Application** (data) 7
Met en forme les données pour permettre aux applications de les traiter (chiffrement/déchiffrement, compression/décompression…)	**Présentation** (data) 6
Organise et synchronise les échanges et les communications	**Session (data)** 5
Responsable du bon acheminement des messages entre les machines (vérifications des erreurs) et de l'optimisation des ressources réseaux.	**Transport** (segment) 4
La couche réseau s'occupe de déterminer le mode et la méthode d'acheminement entre plusieurs machines.	**Réseau** (paquet) 3
Permet de former des paquets parmi les signaux électriques, de vérifier les erreurs et de les fournir à la couche supérieure	**Liaison de données** (trames) 2
Transmission physique des bits d'une machine à une autre (transmission électrique au travers les connecteurs et câbles)	**Physique** (bits) 1

Modèle TCP / IP

4 **Application** (data)	On trouve ici les protocoles « de haut niveau » qui sont associés à un service final comme le web (http/https), la messagerie (SMTP/POP/IMAP), le stockage de fichier (FTP/TFTP/…) ou le chiffrement (SSL) par exemple.
3 **Transport** (segment)	Responsable du bon acheminement des messages entre les machines et de l'optimisation des ressources réseaux.
2 **Réseau** (paquet)	La couche réseau s'occupe de déterminer le mode et la méthode d'acheminement entre plusieurs machines.
1 **Accès au réseau** (bits, trames)	Permet à un hôte d'envoyer des informations à un autre hôte, elle est la combinaison de la couche 1 et 2 du modèle OSI

Figure I.12: OSI vs TCP/IP [w2]

I.3. SDN

SDN signifie littéralement Software Defined Networking. Il est donc facile de constater que ce sujet est vaste et il est difficile de trouver une définition uniforme. La définition académique a été de considérer le SDN comme une architecture qui sépare les fonctions de contrôle du réseau et de transfert de données, ce qui donne lieu à une infrastructure physique totalement exempte de services réseau. Dans ce modèle, le périphérique réseau implémente simplement les règles saisies par l'application pour gérer le flux de données. Cet appareil ne nécessite aucun protocole de routage [13].

Une entité intelligente appelée « contrôleur » voit l'ensemble du réseau et injecte des règles de traitement des données directement dans chaque appareil [13].

Ainsi, le SDN est actuellement considéré comme une architecture permettant d'ouvrir les réseaux aux applications. Cela regroupe deux aspects :

•Permet aux applications de programmer le réseau pour accélérer le déploiement.

•Permet au réseau de mieux identifier les applications transférées afin qu'elles puissent être mieux gérées (par exemple, qualité de service, sécurité, ingénierie du trafic) [w3]

SDN représente une architecture de réseau dans laquelle le plan de contrôle est complètement séparé du plan de données, comme le montre la Figure 13 [13] :

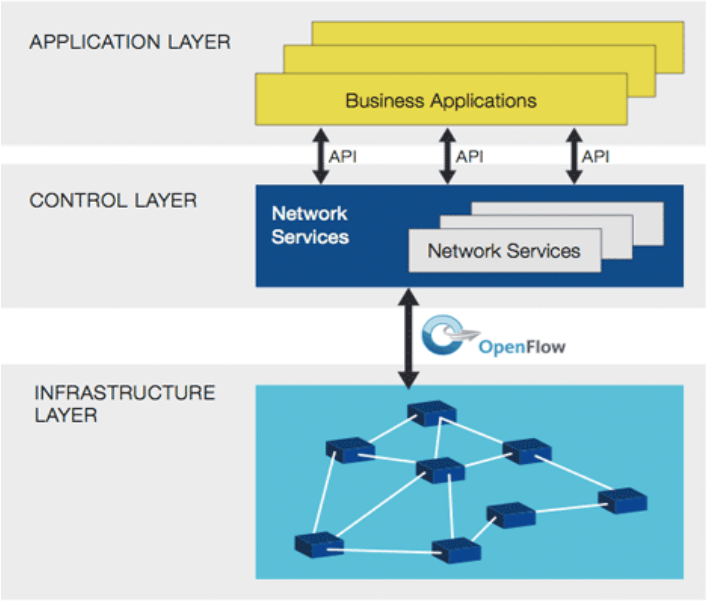


Figure I.13: Openflow dans l'architecture SDN [13]

La Figure 13 montre l'architecture SDN et l'emplacement du protocole OpenFlow. Ensuite, nous pouvons voir que le SDN se compose de trois couches [13] :

•La couche infrastructure contient des éléments de réseau responsables du transfert du trafic et ceux-ci prennent en charge le protocole OpenFlow qu'il partager avec le contrôleur.

•La couche de contrôle est un logiciel basé sur le contrôleur SDN qui offre une visibilité globale des équipements de réseau et d'infrastructure.

•La couche application permet l'automatisation des applications sur un réseau à l'aide d'interfaces programmables.

Par conséquent, grâce à l'approche SDN, la charge de calcul associée au contrôleur est largement supprimée du routeur. Le contrôleur est responsable du calcul et de la mise à jour de la table de routage.

II.4. MPLS

Multi Protocol Label Switching, en français « commutation par étiquette de multiple protocoles », est une technique de transmission de données destinée aux réseaux WAN à très hautes performances.

MPLS s'appuie sur des étiquettes pour transmettre des paquets d'un nœud à un autre au lieu d'utiliser les informations contenues dans les en-têtes de couche réseau et transport, évitant ainsi la complexité de la recherche d'itinéraire via les tables de routage et facilitant les décisions concernant la qualité du service. MPLS peut encapsuler de nombreux protocoles réseau, d'où le nom « multiprotocole » [w4].

Les « labels » ou « étiquettes » sont échangées entre les routeurs afin qu'ils puissent créer des mappages étiquette à étiquette, qui sont attachés aux paquets IP, permettant aux routeurs de transmettre des paquets en se référant uniquement à l'étiquette sans jamais voir l'adresse de destination de couche réseau contenue dans le paquet. C'est ce qu'on appelle « la commutation d'étiquettes » ou »la commutation par labels » au lieu du routage de la couche réseau [w4].

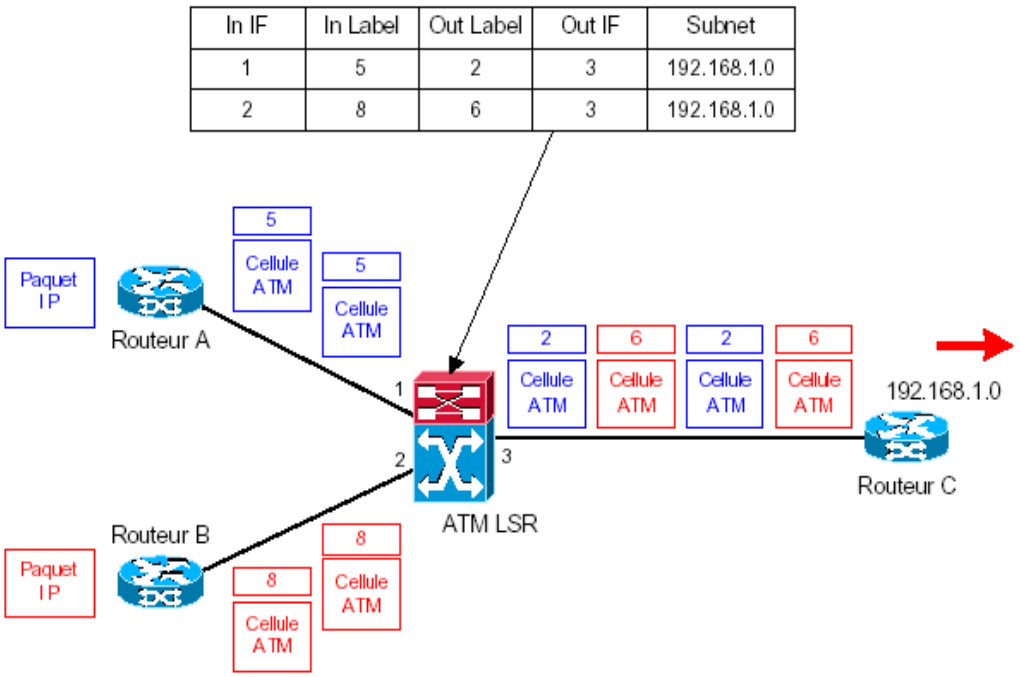


Figure I.14: Implémentation d'un réseau MPLS [w5]

II.5. IP/MPLS

Les réseaux IP/MPLS sont basés sur l'établissement d'un chemin entre deux machines (étiquetés chemins commutés ou LSP). La commutation des paquets envoyés le long de cette route s'effectue en analysant l'étiquette contenue dans l'en-tête MPLS ajouté entre la couche 2 et la couche IP [14].

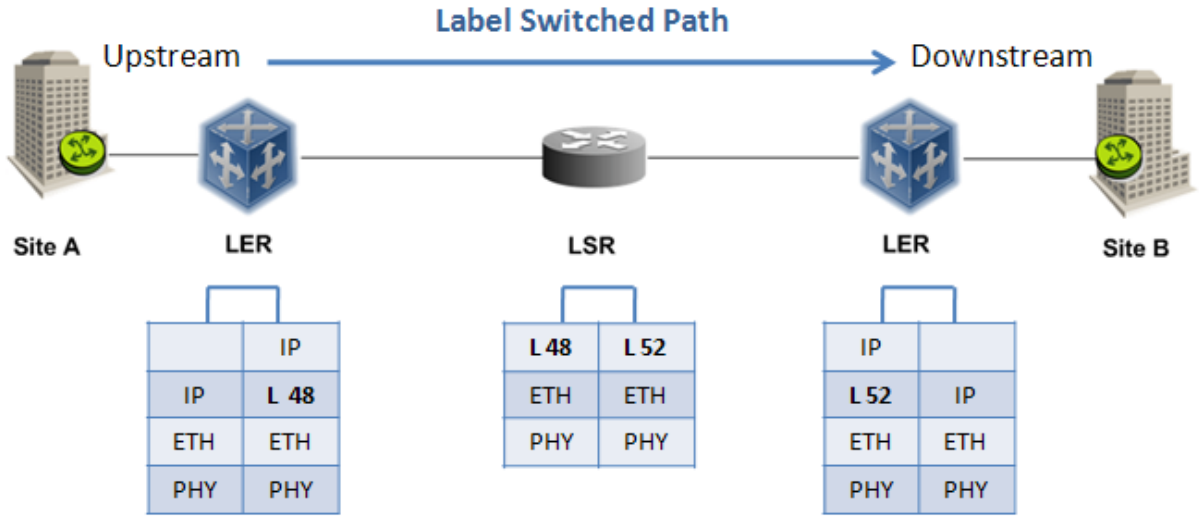


Figure I.15: Principe du réseaux IP/MPLS [15]

La figure II.4 résume le principe de la commutation d'étiquettes le long d'un chemin ou d'un chemin de commutation d'étiquettes. Lors de leur entrée dans le réseau MPLS, les paquets IP sont étiquetés avec l'étiquette « Ingress Label Edge Router » ou « Ingress LER » insérée par. Le LER est un routeur MPLS situé à la périphérie du réseau d'un opérateur. Les paquets

balisés sont transmis au cœur du réseau en fonction de leur numéro de balise. Routeurs MPLS dans le réseau central, commutation d'étiquettes routeurs, commutation des étiquettes vers le LER de sortie (egress LER). Le chemin préétabli qu'un paquet suit à travers le réseau est appelé chemin de commutation d'étiquettes (LSP) [14].

III. les serveurs

Un serveur, dans le contexte informatique, est un ordinateur ou un logiciel qui fournit des services, des données ou des ressources à d'autres ordinateurs, appelés clients, dans un réseau informatique. Les serveurs sont conçus pour répondre aux exigences des clients, effectuer des tâches spécifiques et permettre le partage de ressources [w6].

III.1 Types des serveurs

III.1.1 serveur de fichiers

Les serveurs de fichiers hébergent et diffusent des fichiers que peuvent partager une multitude de clients ou d'utilisateurs. Grâce au stockage central des fichiers, il est plus simple d'effectuer
des sauvegardes et de déployer des solutions de tolérance aux pannes que si on tentait d'assurer la sécurité et l'intégrité des fichiers sur chacun des appareils appartenant à une entreprise. La partie matérielle du serveur de fichiers est parfois conçue pour maximiser les vitesses de lecture et d'écriture afin d'optimiser les performances [w6].

III.1.2 serveur d'applications

Le serveur d'applications fournit l'environnement d'exécution aux clients, évitant ainsi le traitement local des applications. Il accueille habituellement des applications intensives en ressources utilisées par de nombreux utilisateurs. Cette approche dispense les clients d'avoir des capacités matérielles étendues pour leurs applications et de gérer des mises à jour logicielles sur plusieurs machines. En centralisant les applications sur le serveur, tous les utilisateurs peuvent en profiter sans nécessiter d'installation individuelle [w6].

III.1.3 serveur WEB

Un serveur Web est une plate-forme sur laquelle des logiciels utiles à l'entreprise peuvent être installés et exécutés sur des ordinateurs clients connectés via un réseau.

Ils prennent en charge les sites Web en fournissant du contenu HTML, des images et des vidéos, afin que, par exemple, vous puissiez visualiser une page Web tout en la lisant.

Il assure également la tâche d'alimenter l'intranet.

Les administrateurs peuvent accéder au serveur Web via des outils en ligne, apporter des modifications au serveur Web et approuver ou refuser l'accès [w7].

III.1.4 Les serveurs DNS

Un serveur DNS, pour Domain Name System, est un système d'application qui traduit le nom de domaine d'un site Web en une adresse IP compréhensible par l'ordinateur qui l'utilise.

Ce type de serveur agit comme un annuaire géant contenant les noms et adresses IP des sites Web connectés à d'autres serveurs DNS, permettant d'accéder à des informations supplémentaires **[w7].**

III.1.5 serveur de bases de données

Les serveurs de bases de données sont essentiels pour stocker les grandes quantités de données d'une entreprise et garantir que les employés peuvent accéder efficacement aux informations dont ils ont besoin.

Garantissez un accès continu aux fichiers et aux données sur les ordinateurs clients et automatisez les autorisations.

Il s'agit d'un élément important de la sécurité des données, en particulier lorsqu'il s'agit d'informations sensibles ou personnelles sur les clients**.**

Les serveurs de bases de données, souvent associés aux services de sécurité, sont essentiels pour prévenir les violations et les fuites de données [w7].

III.1.6 Serveur Virtual

Les serveurs virtuels conquièrent le monde informatique.

Contrairement aux serveurs traditionnels, dont le système d'exploitation est installé sur une machine physique, les serveurs virtuels ne peuvent fonctionner que sur un logiciel spécial appelé hyperviseur.

Chaque hyperviseur peut exécuter simultanément des centaines, voire des milliers de serveurs virtuels.

Les hyperviseurs présentent le matériel virtuel aux serveurs comme s'il s'agissait de matériel physique.

Les serveurs virtuels utilisent du matériel virtuel comme du matériel classique, et l'hyperviseur, commun à tous les autres serveurs virtuels, transfère les tâches de calcul et de stockage vers la machine sur laquelle le serveur virtuel est installé [w6].

III.2 Rôle des serveurs

Les serveurs jouent un rôle important dans les réseaux informatiques :

- **Partage de ressources**

Les serveurs permettent de partager des fichiers, des imprimantes, des bases de données et d'autres ressources entre plusieurs utilisateurs, réduisant ainsi les coûts et libérant l'utilisation des ressources.

- **Centralisation des données**

Le serveur centralise le stockage des données et facilite la sauvegarde, la gestion et la sécurité des données.

- **Gestion des accès**

Les serveurs contrôlent l'accès aux ressources et aux données pour garantir la sécurité et la confidentialité.

- **Améliorations des performances**

Les serveurs peuvent décharger les tâches des clients, améliorant ainsi les performances et la réactivité.

- **Disponibilité du service**

Les serveurs sont généralement disponibles 24 heures sur 24, 7 jours sur 7, garantissant un accès continu au service.

IV Réseaux virtuels

Un réseau virtuel est un réseau superposé mis en œuvre au-dessus d'un réseau physique existant. Les réseaux virtuels permettent une isolation des réseaux des locataires du centre de données. Généralement, les réseaux virtuels utilisent des services tels que des VLAN (LAN

virtuels) ou des VPN (réseaux privés virtuels) , ou de nouveaux services tels que des VxLAN (LAN virtuels extensibles) [14].

IV.1 Principe de virtualisation

Le principe de la virtualisation existe depuis de nombreuses années, à commencer par les ordinateurs IBM dans les années 70, et la première introduction de la virtualisation dans le monde des PC remonte aux années 80, notamment pour émuler des machines de types DOS/Windows sur des macs ou des machines UNIX, ou pour émuler des ordinateurs personnels sur des machines à caractère plus professionnel (PC). Actuellement on tend à intégrer de plus en plus des supports de virtualisation directement dans le matériel et installer une couche d'abstraction directement sur le matériel (hyperviseur) cette couche peut recevoir plusieurs systèmes d'exploitation virtualisés [15].

IV.2 Principaux logiciels de virtualisation

Un logiciel de virtualisation est un outil qui permet de créer un environnement virtuel sur un ordinateur physique. Cela nous permet d'augmenter notre matériel informatique, d'économiser de l'espace de stockage ou de partitionner notre machine physique**.** Voici quelques-uns des meilleurs logiciels de virtualisation en 2024 :

IV.2.1 VMware Workstation Pro :

Est un outil de virtualisation professionnel qui vous permet d'exécuter plusieurs systèmes d'exploitation en tant que machines virtuelles sur votre PC Linux ou Windows.Cet outil prend en charge plus de 200 systèmes d'exploitation (Linux, Windows et ses anciennes versions, BSD, etc.) .Cette solution permet de [16] :

- Créez une nouvelle machine virtuelle.
- Créez une grande machine virtuelle (32 processeurs, 128 Go de RAM).
- Convertissez votre PC en machine virtuelle.
- Offrez un déploiement massif de performances.

Fournit des fonctionnalités de sécurité supplémentaires telles que la création et la gestion d'instantanés pour les machines virtuelles chiffrées et les sauvegardes de données.

La version professionnelle dispose également de fonctionnalités avancées : personnalisation du réseau virtuel (NAT, renommage du réseau) et simulation (latence, bande passante).

IV.2.2 Oracle VM VirtualBox : Est le logiciel de virtualisation open source gratuit, multiplateforme et open source d`Oracle. Ce logiciel fonctionne sur une variété de systèmes

d'exploitation hôtes, notamment Windows, Linux, MacOs et Solaris, et prend en charge une variété de systèmes d'exploitation invités en tant que machines virtuelles, notamment Windows, Linux, Solaris, Mac et Unix.Cette solution apporte de nombreuses fonctionnalités telles que [16]:

- Importer ou exporter une machine virtuelle vers une solution cloud.
- Transférer des fichiers d'une machine hôte vers une machine virtuelle (Windows uniquement).
- Possibilité d'importer une machine virtuelle vers une solution cloud Contrôler l'accès à distance.
- Accès sécurisé via clé de cryptage (par 256 bits)

Le logiciel peut être utilisé sur n`importe quel support et s`adapte non seulement aux systèmes embarqués, mais également aux ordinateurs, aux datacenters et même aux environnements cloud.

IV.2.3 Microsoft Hyper-V:

Est un hyperviseur de type 1 intégré à Windows Server qui vous permet de créer et de gérer des machines virtuelles. Il est souvent utilisé par les entreprises pour consolider les charges de travail, améliorer l'utilisation des ressources et simplifier la gestion de l'infrastructure informatique. Cette solution apporte de nombreuses fonctionnalités telles que[17] :

- Intégration avec les systèmes d'exploitation Windows.
- Prise en charge des charges de travail critiques pour l'entreprise (bases de données, applications d'entreprise, environnements de bureau virtualisés).
- La version gratuite présente des limites (en termes de fonctionnalités) et nécessite des connaissances techniques supplémentaires.
- Des connaissances techniques plus avancées peuvent être requises et gérées.

IV.2.4 Red Hat virtualisation : est basée sur l'open source et vous permet de créer et de gérer des environnements virtualisés à grande échelle. Il prend en charge une large gamme de systèmes d'exploitation invités et offre des fonctionnalités avancées telles que la migration en direct, la haute disponibilité et une sécurité renforcée .Cette solution apporte de nombreuses fonctionnalités telles que [17] :

- Obtenir une haute disponibilité des machines virtuelles avec fonction de basculement automatique en cas de panne du serveur physique.

- Gestion centralisée des ressources pour simplifier la gestion des environnements virtualisés.
- Coûts de licence élevés pour les moyennes et grandes entreprises.

IV.3 Les avantages et les limites de la virtualisation

✓ Les avantages de virtualisation

Au fil des années, les performances des équipements informatiques n'ont cessé d'évoluer pour atteindre l'extraordinaire puissance dont ils disposent aujourd'hui. Les applications provisionnées aujourd'hui nécessitent beaucoup de ressources mais n'utilisent paradoxalement qu'une fraction du potentiel de certains serveurs. Selon Microsoft, il est généralement possible de regrouper jusqu'à plusieurs serveurs sur une seule machine sans sacrifier les performances. La virtualisation offre donc de nombreux avantages [w9] :

- En termes d'espace requis, un serveur a la capacité d'exécuter différents systèmes fonctionnant sur un Une seule machine réduite en moyenne de moitié la capacité des serveurs au sein de l'entreprise.
- Elle permet de réduire le nombre de machines physiques, conduisant à un retour sur investissement intéressant.
- En plus de réduire l'espace, la réduction du nombre de machines physiques entraîne une réduction de la consommation d'énergie.
- Enfin, moins de machines signifie moins de contrats de support matériel (souvent très coûteux sur les serveurs, où la maintenance doit être rapide en cas de panne matérielle).
- En plus de ces avantages, la virtualisation permet une gestion simple des pools de serveurs.
- Autrefois, les applications étaient étroitement couplées aux serveurs sur lesquels elles s'exécutaient.
- La technologie de virtualisation crée une couche d'abstraction entre le matériel physique et le logiciel, elle permet l'exécution et la coexistence de plusieurs serveurs très distincts sur une même machine.
- Par conséquent, les applications métier développées en interne qui s'exécutent uniquement sur les systèmes d'exploitation existants (tels que NT4) peuvent être conservées sans conserver les contraintes associées au serveur physique existant.

- La virtualisation réduit le temps et les coûts souvent coûteux d'administration du serveur . La gestion de la flotte est plus facile, ce qui aide à réduire la charge des administrateurs.
- Il simplifie le déploiement sur les plateformes de test ou de production en réduisant le temps requis pour provisionner les serveurs.
- Enfin, cela augmente la disponibilité des serveurs avec une récupération plus rapide que les machines physiques.

On peut ajouter à ces fonctionnalités un réseau plus sécurisé. En effet, l'attaquant ne peut pas voir la machine hébergeant les systèmes virtuels.

✓ Les limites de la virtualisation

Malgré tous ces avantages, ce n'est pas une bonne idée de se lancer dans la virtualisation sans réflexion, sans recherche et surtout sans plan de reprise d'activité (PRA) pouvant mettre en danger votre système d'information[w9] :

- La mise en œuvre de la virtualisation introduit une complexité de gestion et entraîne les risques inhérents au « tout virtuel ».
- Il s'agit d'une manière différente d'organiser votre équipement informatique et peut prendre du temps à s'adapter
- Un autre problème surgit : la gestion des données. Comment retrouver vos données lorsqu'elles sont partagées sur plusieurs disques physiques mais stockées sur des disques logiques ? Il est absolument nécessaire d'effectuer une cartographie détaillée à T de ses données. Le LUN (Logical Unit Number) doit être standardisé, avec un nom et un numéro.
- Enfin, si la machine hébergeant tous les systèmes d'exploitation s'arrête ou si la charge de l'application augmente sensiblement, la situation peut vite devenir un problème.
- Surtout parce que la virtualisation cache souvent la source des erreurs, notamment grâce à l'équilibrage de charge automatique, rendant l'erreur presque invisible, car le système continue de fonctionner quoi qu'il arrive. Mais si une erreur plus importante se produit, il sera très difficile pour les administrateurs de la localiser.

Pour une virtualisation redondante il est donc capital de dupliquer les machines virtuelles.
Dans tous les cas la virtualisation n'est pas à prendre à la légère et doit être mûrement réfléchie

IV.4 La sécurité en virtualisation

- L'hyperviseur est responsable de l'isolation des machines virtuelles.
- Une meilleure sécurité peut être assurée si les machines hôtes sont situées dans un cluster. Évitez les points de défaillance uniques.
- Redondance facile et réduisez les risques.
- Chaque machine virtuelle peut être spécialisée pour un service spécifique, permettant d'appliquer des politiques de sécurité spécifiques à chaque serveur virtuel [16].

Conclusion

Ce chapitre a présenté les éléments essentiels de la gestion des réseaux informatiques, offrant ainsi une base solide pour une compréhension et une gestion efficaces des réseaux. Explorant les différentes définitions, types et topologies des réseaux informatiques ainsi que des principaux modèles de réseau tels que l'OSI, le TCP/ IP, la SDN, le MPLS et l'IP/ MPLS.

Nous avons aussi pris en compte l'importance des serveurs dans les réseaux informatiques ainsi que les diverses catégories de serveurs disponibles.

En fin de compte, nous avons exploré le domaine des réseaux virtuels et analysé sa définition, les principes de la virtualisation, les logiciels de virtualisation les plus essentiels, ainsi que les bénéfices et les désavantages liés à cette industrie.

Chapitre II

Solutions de sécurité des réseaux

Introduction

À mesure que les cyberattaques deviennent plus diversifiées et complexes, assurer la sécurité du réseau devient de plus en plus important pour protéger les données sensibles et assurer la continuité des activités. La sécurité du réseau est un pilier clé pour sécuriser les systèmes informatiques modernes. L'objectif de ce chapitre est d'examiner divers aspects de la sécurité des réseaux, en commençant par une définition claire et concise de ce concept. Couvre également les mécanismes de sécurité clés tels que le cryptage, l'antivirus, le VPN et les pare-feu. Enfin, nous fournissons un tableau comparatif des solutions de pare-feu logiciels telles que Zone Alarm, pfSense, AVS Firewall…etc pour fournir un aperçu clair des options disponibles pour améliorer la sécurité de notre réseau.

I. Sécurité réseau

I .1Définition :

La sécurité des réseaux est une branche de l'informatique qui consiste à sécuriser tous les éléments d'un réseau informatique pour empêcher les accès non autorisés, le vol de données, l'utilisation abusive des connexions réseau et la modification des données. Par conséquent, son objectif est de fournir des méthodes et des mécanismes de défense proactifs pour protéger le réseau contre les menaces externes et internes [22] .

II. Attaques informatiques

Chaque ordinateur qui est connecté à un réseau informatique peut être exposé à une attaque. La majorité de ces attaques se font automatiquement à partir de machines infectées (virus, chevaux de Troie, vers, etc.), sans l'intervention de leur propriétaire. De manière plus rare, il s'agit de l'intervention de pirates informatiques [23].

II.2 types des attaques informatiques

Il existe plusieurs types d'attaques, parmi elle :

II .2.1 Attaques spoofing

L'attaque spoofing est une méthode de piratage informatique qui consiste à exploiter l'adresse IP d'une machine cible pour en prendre l'identité. Cette attaque vise à obtenir l'accès à des données en se faisant passer par la machine dont l'adresse est supprimée [24].

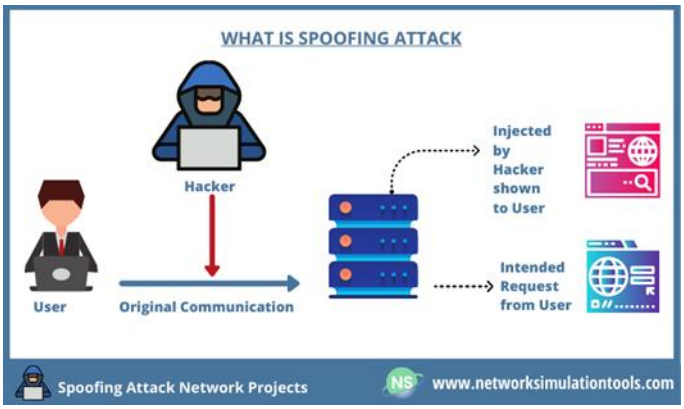


Figure II.1: Attaque spoofing [w13]

II.2.2 Déni de service (DOS « Denial Of Service »)

Une attaque DOS implique de surcharger les ressources d'un système afin de le perturber, en lui envoyant des milliers de paquets IP depuis la machine de l'hacker.En général, l'hacker ne pénètre pas dans les réseaux informatiques et n'a donc pas besoin de mots de passe ou d'autres moyens d'accès similaires, ce qui rend cette technique réalisable et facile à mettre en œuvre. Le système attaqué subit des conséquences désastreuses : instabilité, voire indisponibilité partielle ou totale du système [24].

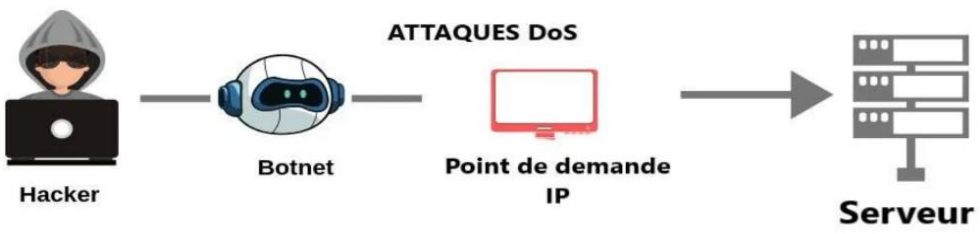


Figure II.2: Attaque DOS [37]

II.2.3 Déni de service distribué (DDOS)

Une attaque DDoS est une forme d'attaque DoS qui consiste à utiliser plusieurs machines compromises pour envoyer en même temps une multitude de requêtes à un système cible, ce qui peut entraîner son instabilité ou son indisponibilité complets. Souvent, des machines contrôlées et infectées par des Trojans sont responsables des attaques DDoS [24].

Figure II.3 : Attaque DDOS [37]

- **DOS vs DDOS**

Tableau II.1: DOS vs DDOS [37]

Critéres	DOS	DDOS
Source d'attaque	Utilise une seule machine et un seul réseau pour inonder un système ou une ressource ciblée	Utilise plusieurs machines et réseaux pour inonder un système ou une ressource ciblée
Niveau de menace	Niveau de menace faible	Niveau de menace moyen à élevé, car il peut être utilisé pour endommager gravement les réseaux et les systèmes
Implication de logiciels malveillants	Aucune implication de logiciels malveillants	Un botnet est généralement composé de milliers de PC infectés
Coût et gestion	Il est plus facile à utiliser et gérer	Il n'est pas facile à utiliser et à gérer
Protection	Le système peut être arrêté/protégé facilement	Système difficile à protéger

II.2.4 Sniffing (écoute du réseau)

Le sniffing est une méthode qui implique d'analyser le trafic réseau afin de collecter de manière illicite des informations confidentielles (par exemple, les mots de passe). Grâce à un logiciel connu sous le nom de sniffer, les pirates informatiques auront la capacité d'intercepter tous les paquets qui circulent sur un réseau, y compris ceux qui ne sont pas destinés [24].

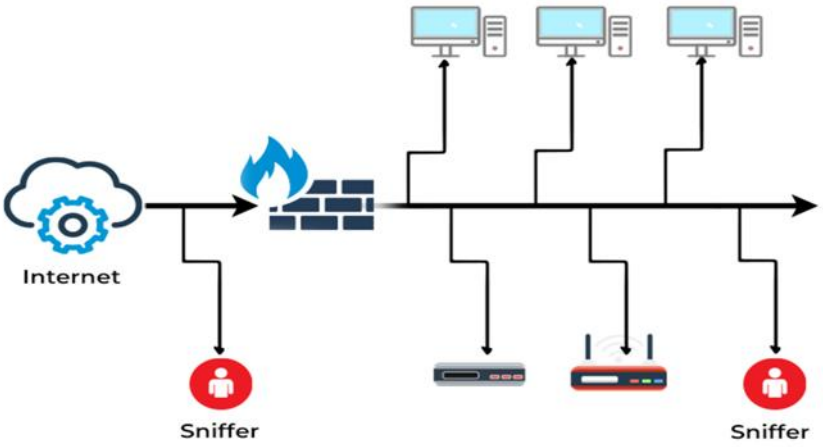


Figure II.4: Attaque Sniffing [38]

II.3 Le système de détection d'intrusion IDS/IPS

IDS ou (Intrusion Detection System) ou Intrusion Detection System est un logiciel ou un matériel qui automatise la surveillance et détecte les signes d'intrusion. Placé judicieusement dans un réseau ou un système. Automatisez la surveillance pour identifier les activités suspectes ou anormales sur cette cible et alerter les administrateurs de sécurité.

De cette façon, vous pouvez avoir un aperçu des tentatives réussies (ou infructueuses) d'attaque ou de pénétration de votre système [25].

IPS ou (Un système de prévention des intrusions) est un composant logiciel et/ou matériel dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système.IPS supprime de manière proactive les paquets réseau en fonction des profils de sécurité si les paquets représentent une menace connue. En fait, le concept IPS a été principalement conçu pour répondre aux limites de l'IDS du point de vue de la réponse passive aux attaques. Il ne s'agit plus seulement de détecter les attaques en cours, il s'agit en premier lieu de les empêcher de démarrer. Les systèmes IPS doivent donc être en ligne pour répondre aux attaques [25].

IDS et IPS lisent les paquets réseau et comparent leur contenu à une base de données de menaces connues. La principale différence entre les deux réside dans ce qui se passe ensuite [25].

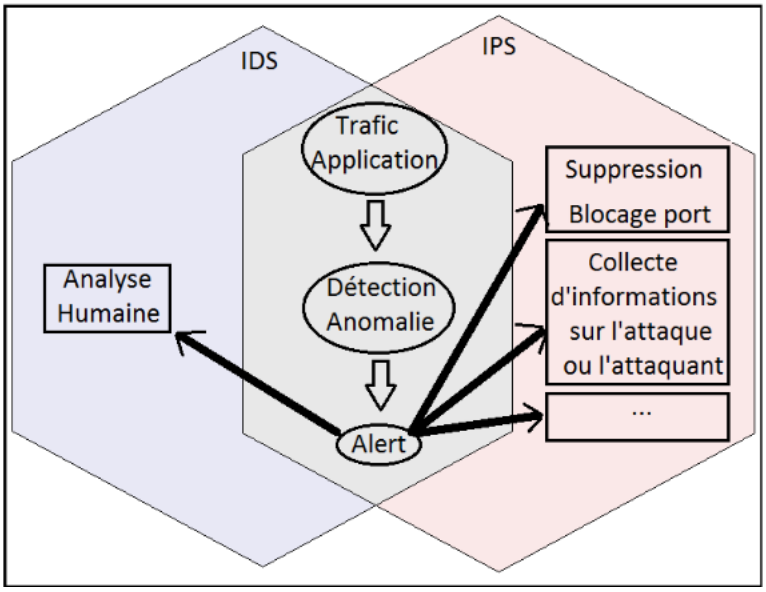


Figure II.5: Différence entre IDS et IPS [25]

Tableau II.2 : IPS vs IDS [25]

IDS	IPS
• IDS est un outil de découverte et de surveillance qui n'effectue aucune action par lui-même. • Un humain ou un autre système doit ensuite examiner les résultats et décider des mesures à prendre. Cela peut devenir un travail à temps plein en fonction de la quantité de trafic quotidien généré. • IDS ne modifie en aucun cas les paquets réseau.	• IPS représente un système de contrôle qui accepte ou rejette paquets sur la base d'un ensemble de règles. • L'IDS est un excellent outil à utiliser dans le cadre d'une enquête sur un incident de sécurité. • IPS empêche l'envoi de paquets en fonction de leur contenu, tout comme un pare-feu bloque le trafic en fonction de l'adresse IP .

De nombreux fournisseurs IDS/IPS ont intégré de nouveaux systèmes IPS avec des pare-feu, créant ainsi une technologie appelée gestion unifiée des menaces (UTM). Cette technologie combine les fonctionnalités de ces deux systèmes similaires en une seule unité. Certains systèmes combinent les fonctionnalités IDS et IPS dans la même unité [25].

III. Protocoles de sécurité

III.1 HTTPS

Https est utilisé dans le but de transmettre des données sur Internet. Les serveurs stockent les pages Web envoyées aux ordinateurs clients lorsque les utilisateurs les visitent.

Cette communication entre les serveurs et les clients crée un réseau connu sous le nom de World Wide Web (www).

Https dispose d'une couche SSL/TLS supplémentaire qui récupère les informations demandées du serveur Web et garantit que toutes les données transmises sont cryptées et sécurisées.

La sécurité fournie par HTTPS est très importante pour les sites Web qui transmettent des informations sensibles telles que des informations de carte de crédit ou des adresses de facturation[w14].

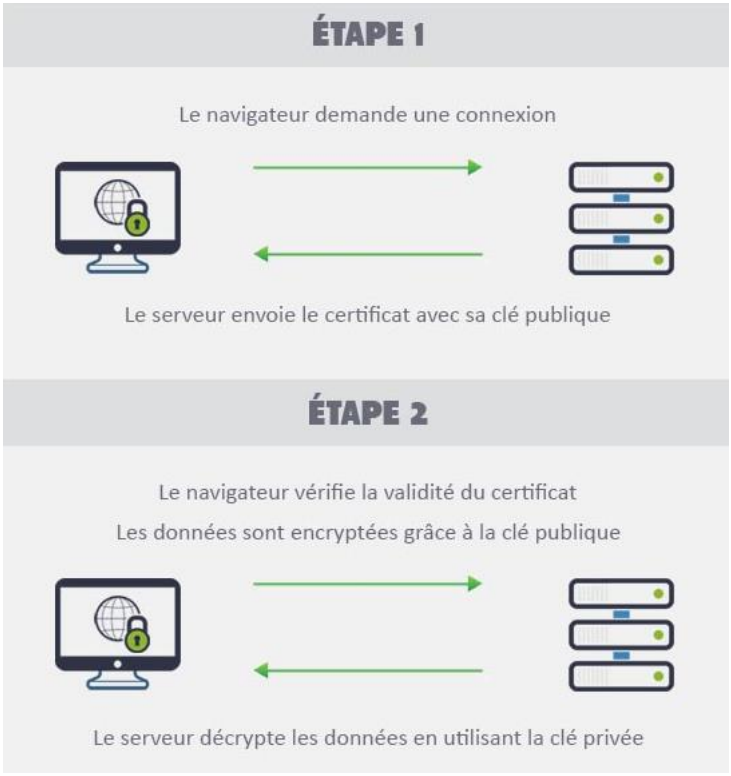


Figure II.6: Fonctionnement de Protocol de sécurité HTTPs [w18]

III.2 SSH

Le SSH (Secure Shell) permet de répondre à la principale problématique posée par la sécurité des informations, la confidentialité.il Permet le cryptage des communications entre deux machines, garantissant la confidentialité des données, l'authentification des utilisateurs et des serveurs et l'intégrité des données grâce aux signatures électroniques.

Le protocole SSH offre une sécurité robuste lors des connexions entre un client et un serveur. Une fois la connexion initiale établie, le client peut être certain de se connecter au bon serveur lors des sessions suivantes, ce qui évite les attaques de type "homme du milieu". De plus, les données d'authentification telles que le nom d'utilisateur et le mot de passe sont transmises de manière cryptée, empêchant leur interception par des tiers malveillants. Enfin, toutes les données échangées entre le client et le serveur sont chiffrées, garantissant une confidentialité totale et une protection contre les écoutes indiscrètes[1].

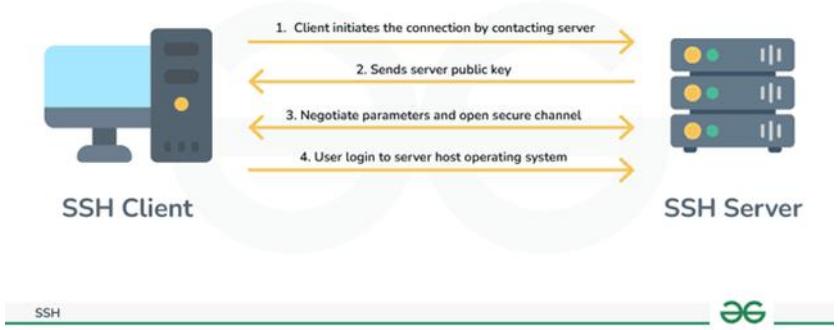


Figure II.7 : Fonctionnement de Protocol de sécurité SSH [w14]

Comme illustré dans l'image ci-dessus, un processus de connexion SSH est décrite, décrivant les différentes étapes nécessaires pour créer une connexion sécurisée entre un client SSH et un serveur SSH.

Le client SSH établit la connexion au serveur SSH, puis envoie la clé publique du serveur. Ensuite, Lorsque le client et le serveur discutent des paramètres de connexion, ils établissent un canal sécurisé. Et la prochaine étape est Le système d'exploitation de l'hôte du serveur est accessible à l'utilisateur.

III.3 SSL

SSL (Secure Sockets Layer) est un protocole assurant la sécurité des échanges indépendamment du protocole applicatif utilisé. Il permet de chiffrer les communications entre deux machines et d'assurer la confidentialité des données, l'authentification de l'utilisateur et du serveur, ainsi que l'intégrité des données par signature électronique [1]

Le principe d'une authentification du serveur avec SSL est le suivant :

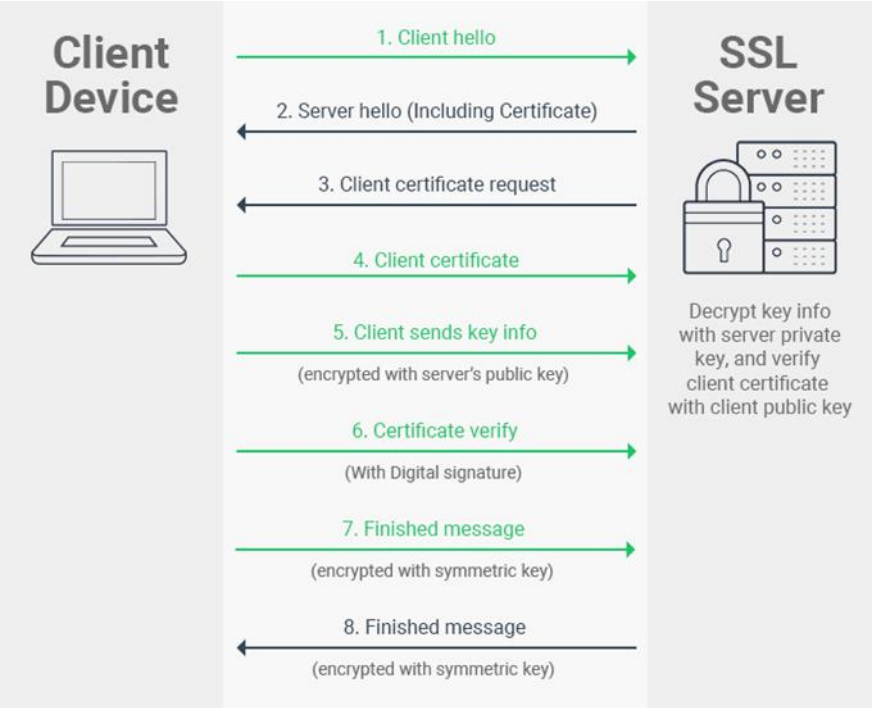


Figure II.8: Fonctionnement de Protocol de sécurité SSL [w14]

III.4 IPSec

IPSec (Internet Protocol Security) est un protocole de niveau 3.

Il est souvent utilisé pour créer des réseaux privés virtuels et sécuriser l'accès à distance aux intranets. Les services IPSec reposent sur des mécanismes cryptographiques offrant un haut niveau de sécurité.

La sécurité étant assurée au niveau IP, IPSec peut être implémenté sur n'importe quel périphérique réseau et offre une protection unique pour l'échange de données. IPSec s'intègre dans la pile de protocoles TCP/IP au niveau IP.Cela présente l'avantage d'être disponible à un niveau supérieur et d'offrir une protection unique pour toutes les applications [26].

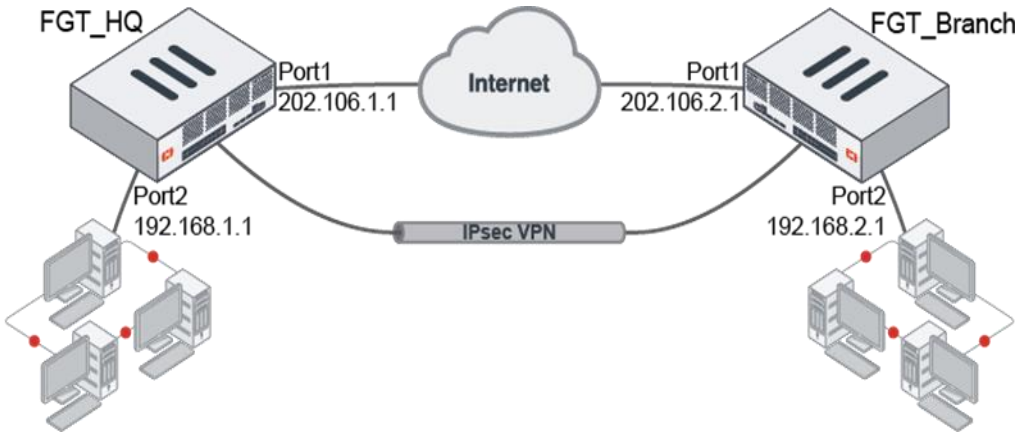


Figure II.9 : Protocol de sécurité IPSec [w15]

III.5 PGP

PGP (Pretty Good Privacy) est un protocole de sécurité de cryptage des données qui garantit la confidentialité et l'intégrité des communications électroniques. Le chiffrement de toutes les informations avec la clé publique nécessite beaucoup de temps de calcul, c'est pourquoi PGP utilise une technique plus rapide. Le document est compressé (évitant la redondance) et chiffré à l'aide uniquement d'une clé de session aléatoire (cryptage rapide) .La clé de session est chiffrée avec la clé publique du destinataire et ajoutée au document. Le destinataire peut utiliser sa clé privée pour déchiffrer la clé de session et décrypter et décompresser le document[27].

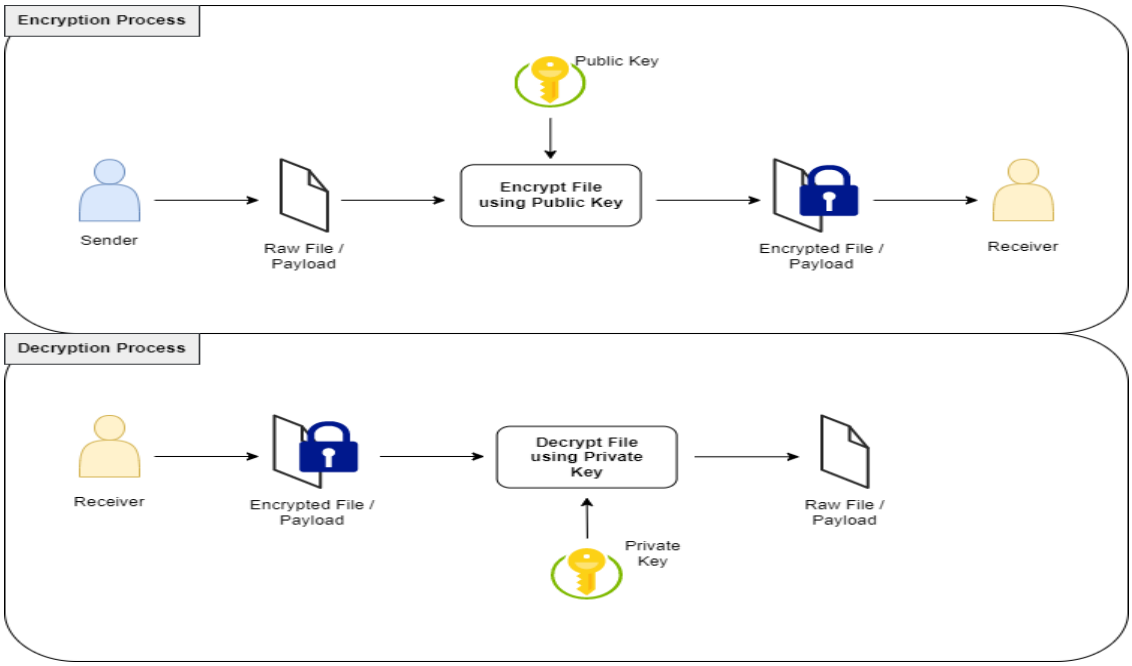


Figure II.10: Protocol de sécurité PGP [40]

III .6 VPN

Un VPN pour (réseau privé virtuel) ou VPN pour (réseau privé virtuel) est une ligne privée virtuelle spéciale installée sur un réseau qui utilise un VPN pour connecter deux emplacements distants (communication sécurisée et échange d'informations) et assurer la protection. et la confidentialité des données en circulation afin que les informations ne puissent pas être obtenues ou interceptées par des personnes malveillantes. Les VPN reposent principalement sur des lignes partagées non dédiées, et votre connexion Internet est plus lente qu'une connexion dédiée, ce qui a un impact direct sur les performances [28].

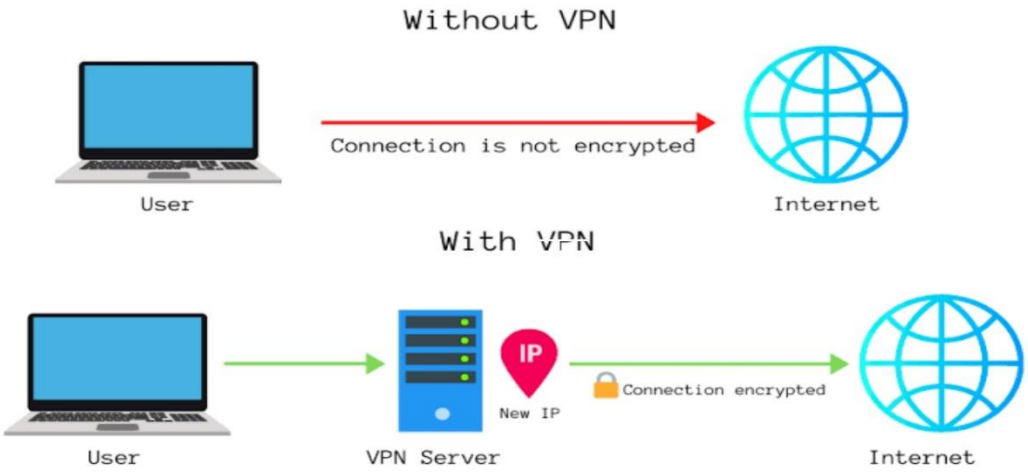


Figure II.11: Protocol de sécurité VPN [39]

IV. Mécanismes de sécurité

IV.1 Crypto

Le cryptage est un procédé cryptographique qui rend un document inintelligible à toute Personne ne disposant pas de la clé de cryptage (déchiffrement) . Ce principe est généralement associé au principe d'accès conditionnel. Le cryptage peut garder la signification d'un document privée, mais d'autres techniques cryptographiques sont nécessaires pour sécuriser la communication [29].

IV.2 Antivirus

Un programme antivirus est un logiciel conçu pour identifier, neutraliser et éliminer les logiciels malveillants.Ceux-ci peuvent être basés sur l'exploitation de failles de sécurité, mais il s'agit de programmes qui modifient ou suppriment des fichiers, tels que des documents appartenant aux utilisateurs de l'ordinateur infecté ou des fichiers nécessaires au bon fonctionnement de l'ordinateur[30].

Un antivirus vérifie les fichiers et courriers électroniques, les secteurs de boot (pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet), etc[31].

IV.3 Firewall

Un firewall, également appelé pare-feu ; est destiné à contrôler et filtrer les accès entre un réseau d'entreprise ou un ordinateur personnel et un autre réseau, en l'occurrence Internet.

Un pare-feu est soit un objet matériel, soit un programme qui s'exécute sur notre ordinateur[32].

Un pare-feu est un composant (logiciel, matériel ou les deux) intégré à un réseau informatique qui peut protéger le réseau en déterminant quelles communications sont autorisées ou interdites. Les pares-feux permettent de connecter deux (ou plusieurs) réseaux avec différents niveaux de sécurité, comme Internet et le réseau interne d'une entreprise. Cela facilite la catégorisation, l'examen et la réalisation des communications [33].

V. Les différents types de pare-feu matériels

V.1 Les pare-feu matériels

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en termes de configuration, ils sont aussi peu vulnérables aux attaques, car présent dans la « boite noire » qu'est le routeur. De plus, étant souvent très liés au matériel, l'accès à leur code est assez difficile, et le constructeur a eu toute latitude pour produire des systèmes de codes « signés » afin d'authentifier le logiciel (système RSA ou assimilés). Ce système n'est implanté que dans les firewalls haut de gamme, car cela évite un remplacement du logiciel par un autre non produit par le fabricant, ou toute modification de ce dernier, rendant ainsi le firewall très sûr. Son administration est souvent plus aisée que les firewalls bridges, les grandes marques de routeurs utilisant cet argument comme argument de vente. Leur niveau de sécurité est de plus très bon, sauf découverte de faille éventuelle comme tout firewall. Néanmoins, il faut savoir que l'on est totalement dépendant du constructeur du matériel pour cette mise à jour, ce qui peut être, dans certains cas, assez contraignant. Enfin, seules les spécificités prévues par le constructeur du matériel sont implémentées. Cette dépendance induit que si une possibilité nous intéresse sur un firewall d'une autre marque, son utilisation est impossible. Il faut donc bien déterminer à l'avance ses besoin et choisir le constructeur du routeur avec soin [34].

- ✓ **Avantage**
  - Intégré au matériel réseau
  - Administration relativement simple
  - Bon niveau de sécurité

✓ **Limites [35]**

- Dépendant du constructeur pour les mises à jour.
- Souvent peu flexibles.

V.2 Les pare-feu logiciel

Les pares-feux logiciels sont présents à la fois dans les serveurs et les routeurs, nous Pouvons les classer en deux catégories ; les pares-feux personnels et les pares-feux plus sûr [31].

➢ **Les pares-feux personnels**

Ceux-ci sont souvent de nature commerciale et visent à protéger des ordinateurs spécifiques plutôt que des groupes d'ordinateurs. Ils sont souvent payants, très restrictifs et parfois extrêmement dangereux.

En fait, nous visons la simplicité plutôt que l'exhaustivité pour le rendre plus accessible aux utilisateurs finaux [36].

Les pares-feux commerciaux offrent une sécurité en bout de chaîne au niveau de l'ordinateur client et sont personnalisables avec facilité. Cependant, ils peuvent être facilement contournés et il peut être difficile de choisir parmi leur nombre important de variantes disponibles [w16].

➢ **Les pares-feux plus-sûr**

Les pares-feux nommés plus-sûr tournent généralement sous linux, car ils offrent une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les pares-feux matériels des routeurs. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux. Toute fonctionnalité des firewalls de routeurs est potentiellement réalisable sur une telle plateforme [34].

VI. Solutions de Pare feu logiciels

TableauII.3 : Solutions de Pare feu logiciels[w17]

Caractéristiques	Type	Licence	Système d'exploitation supporté	Fonctionnalités principales
Zone Alarm	logiciel	Gratuit / Payant	Windows	Protection WIFI /Surveillance de trafic / Recherches sécurisés/Anti-phishing / Téléhargement sécurisé
pfSense	logiciel	Gratuit / Open Source	Multiplateforme	Filtrage de paquets, NAT, VPN, QoS, Proxy

AVS Firewall	logiciel	Payant	Windows	Bloquage d'annonces et bannières, Défense contre les logiciels espions, Contrôle des applications
Comodo Internet Security	logiciel	Gratuit / Payant	Windows	Modes de fonctionnement flexibles, Contrôle des connexions entrantes et sortantes, Auto-apprentissage
BullGuard	logiciel	Payant	Windows / Android / macOS	Contrôle des applications, Protection proactive, Contrôle des communications entrantes et sortantes
GlassWire	logiciel	Payant	Windows	Filtrage du trafic, Visualisation de l'activité réseau, Profilage
Cisco ASA	logiciel	Payant	/	Contrôle et filtrage du trafic réseau, Gestion de VPN, Prévention des intrusions
SonicWall	logiciel	Payant	/	Technologie de sécurité unifiée des menaces, Antivirus, Prévention des intrusions, Filtrage de contenu

Conclusion

Assurer la sécurité du réseau est essentiel pour maintenir la fiabilité et la fonctionnalité des systèmes informatiques modernes.

Dans ce chapitre, nous avons passé en illustré les concepts clés de la sécurité des réseaux, les différents types d'attaques et les protocoles de sécurité importants. Les mécanismes de sécurité tels que le cryptage, les programmes antivirus, les VPN et les pare-feu jouent un rôle important dans la défense contre les cybermenaces. La comparaison de plusieurs solutions de pare-feu logiciels révèle leurs fonctionnalités particulières et leur capacité à protéger notre infrastructure réseau. En fin de compte, une stratégie de sécurité réseau efficace nécessite une combinaison réfléchie de ces outils et pratiques pour fournir une protection solide contre les cyberattaques.

Chapitre III

Mise en place d'une solution d'administration et de sécurisation Firewall Fortinet

III.1 Présentation de l'organisme d'accueil

III.1.1 Historique de l’entreprise

L`Agence Nationale de Soutien et de Développement de l'Entreprenariat, connue sous l'abréviation « NESDA », est un type particulier d'agence gouvernementale dotée de la personnalité juridique et de l'indépendance financière. Ceci est placé sous la supervision du Ministre plénipotentiaire chargé des Petites et Moyennes Entreprises, qui représente le Premier Ministre. Cette agence aide les entrepreneurs à démarrer et à développer de petites entreprises qui produisent des biens et des services.

L’ANADE a pour objectifs :

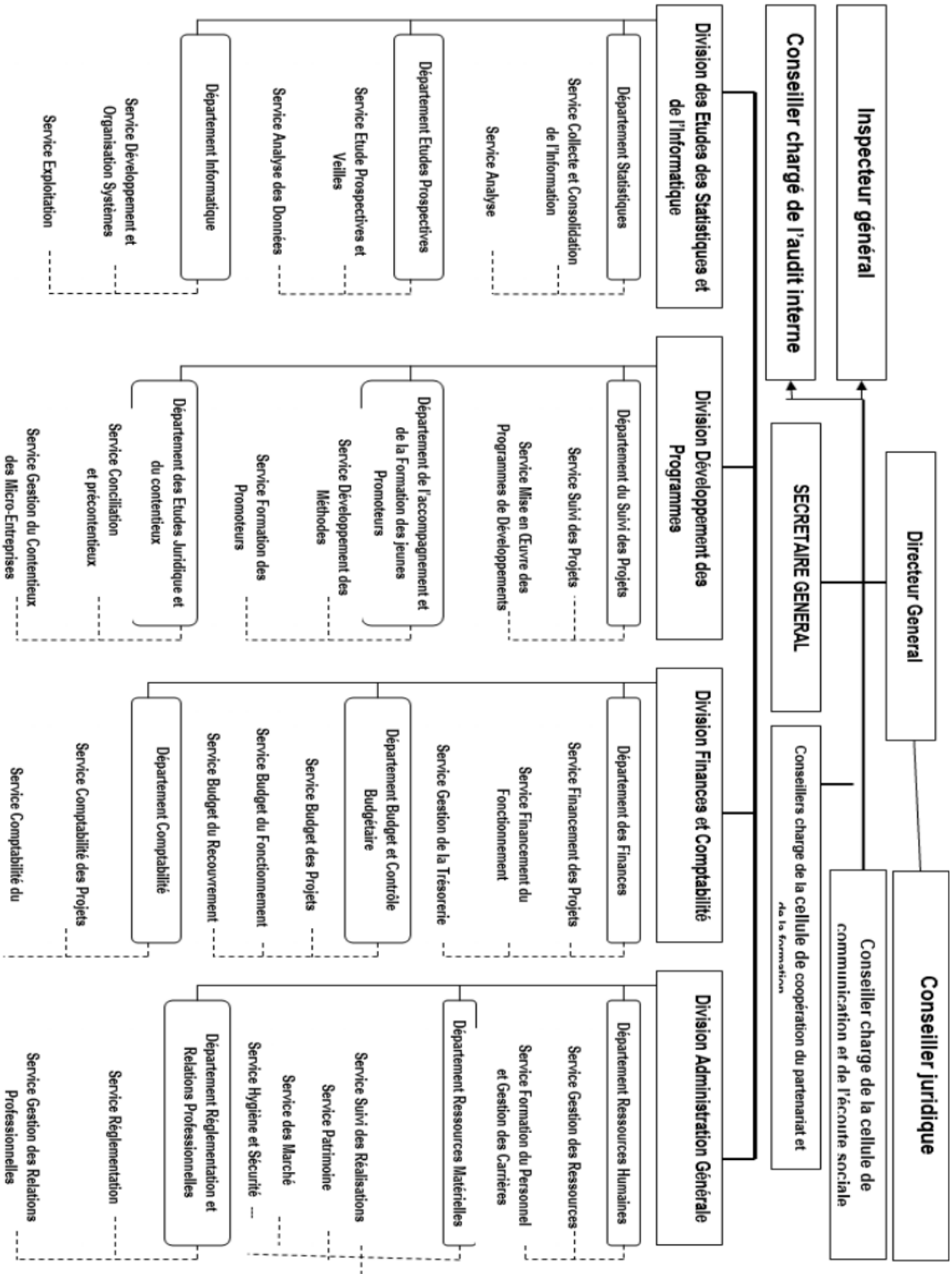
- ✓ Facilite la création et l'expansion d'activités de production de biens et de services par les entrepreneurs.
- ✓ Promotion de toutes formes d'actions et de mesures visant à promouvoir l'entrepreneuriat.

III.1.2 Taches de l’agence :

Les responsabilités de l'Agence Nationale d'Appui et de développement de l'entrepreneuriat comprennent :

- ➢ Fournir un soutien, des conseils et une assistance.
- ➢ Fournit toutes les informations économiques, techniques, législatives et réglementaires liées aux activités du chef de projet.
- ➢ Nouer des relations avec les partenaires et parties prenantes (banques, fisc, caisses de sécurité sociale).
- ➢ Construire des partenariats entre différents secteurs pour identifier les opportunités d'investissement.
- ➢ Formation de chefs de projets au Centre de développement de l'entrepreneuriat.
- ➢ Finance des projets jeunesse et informe sur les différentes subventions accordées.
- ➢ Accompagnement et suivi à distance des petites et moyennes entreprises fondées par des entrepreneurs.
- ➢ Promotion de toutes activités et mesures visant à favoriser le développement et l'expansion des activités

III.1.3 Organigramme de l’organisme d’accueil :



FigureIII.1 : Organigramme de l'organisme d'accueil

III.2 Etude de l'existant

III.2.1 Problématique

Avant, dans le cadre du projet de fin d'étude, nous avons effectué un stage pratique au sain de la direction général de NESDA. Cette dernière est structurée comme suit :

- **Direction générale :** hébergeant des ports clients et des serveurs, tels qu'Active directory, serveur fichier, serveur de messagerie…
- **Les annexes** : situées aux niveaux du différentes wilayas, chaque annexe comporte des antennes. Certaine annexe équipée d'un firewall fortigate.

Vu la complexité du réseau NESDA, et vu la charge et les problèmes de sécurité et de confidentialité, nous étions appelées à mettre en place une solution de supervision et de sécurité contre les attaques internes et externes, basés sur un firewall fortinet.

III.2.2 Infrastructure réseau

La cartographie ci-dessous montre l'architecture réseau de la NESDA

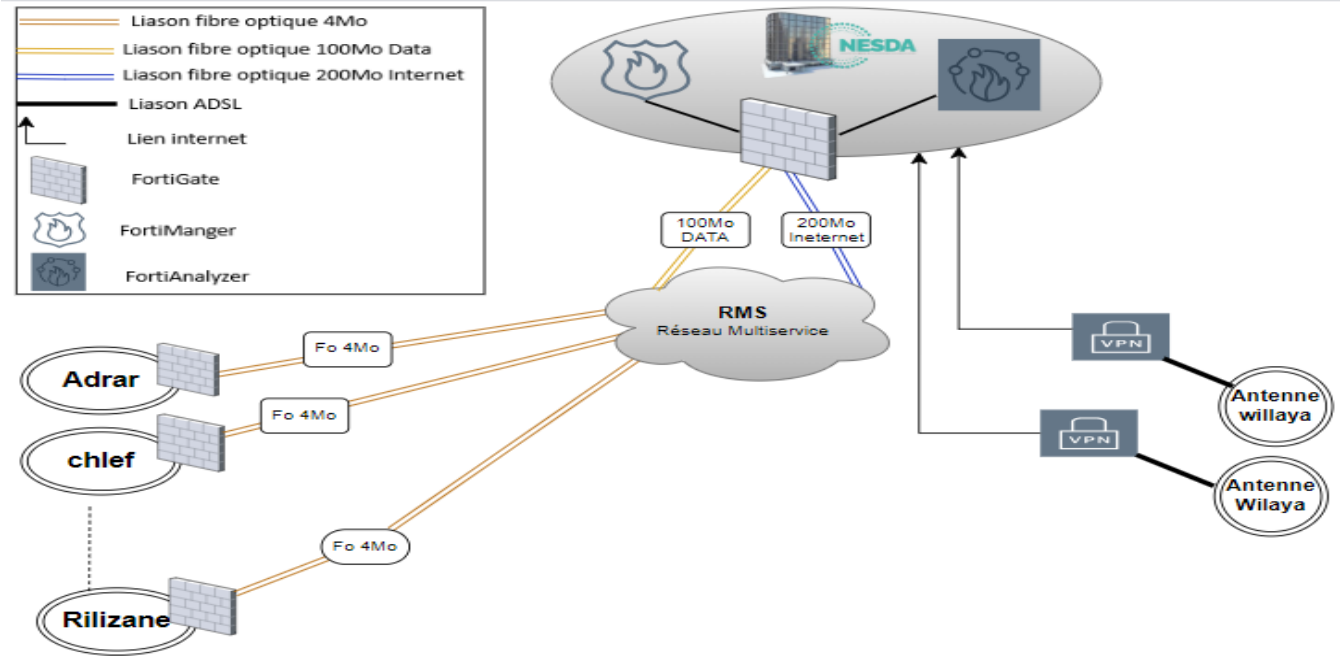


Figure III.2 : Architecture réseau de la NESDA

III.2.3 Matériels et logiciels exploités

La mise en œuvre de la solution de monitoring et de supervision pour notre projet nécessite l'utilisation de différents équipements et logiciels virtuels. Cette mise en œuvre vise à

instaurer un cadre sécurisé qui facilite la gestion centralisée des politiques de sécurité, la collecte et l'analyse des journaux de sécurité, ainsi que la sécurité du réseau contre les risques. Afin d'atteindre cette finalité, nous avons employé plusieurs Appliance de sécurité virtuelles de Fortinet qui sont installé sur la plateforme de virtualisation VMWre Workstation pro17

Tableau III.1 : Caractéristiques du matériel utilisé

Machine	Système d'exploitation	Processeur	RAM	Disque Dur
DELL	Windows 10 Professionnel 64 bits (10.0 ,Version19045)	Intel®Core™ i5-6300U CPU @2.40GHz(4CPUs),~(2.5GHz)	16384 MB	Disque SSD
Serveur ESXI02.ansej.lan	Modèle : PRIMERGY RX4770 M1	55.3 GHz	66 678 947,84 Mb	E7-4850

Tableau III.2 : Caractéristiques des logiciels utilisés

Logiciel	Caractéristiques	Rôle
Windows 10	VersionPro,64 bits de MicroSoft	Système d'exploitation utilisé pour les machines clientes
VMware Workstation	Version Pro 17 Type de fichier : Raccourci (.lnk) TAIL : 1,24 Ko (1 276 octets) Sur disque : 4,00 Ko (4 096 octets)	Solution utilisée dans la création d'une ou plusieurs machines virtuelles au sein du même système d'exploitation, situées sur le même ordinateur physique, mais connectées au réseau local via des adresses IP différentes. Pour notre cas nous allons l'utilisée pour la virtualisation des différents dispositifs de sécurité
Windows Server 2019	Version 2019, 64 bits de MicroSoft	Système d'exploitation utilisé pour les machines serveurs, ainsi que pour configurer et gérer Active Directory (AD) intégré dans notre solution de sécurité
Fortigate	Version :7 .0.15/ 7.4.2 /7.4.3 de FortiNet RAM : 2Go	Dispositif de sécurité Pare-Feu de nouvelle génération (NGFW) contre les attaques et les cybermenaces

	Adresse IP : 10.10.0.1 /24	
FortiManager	Version :7 .0.12 / 7.4.2 de FortiNet RAM : 8Go minimum Adresse IP(1ère utilisation) : 10.10.0.20 /24 Adresse IP(2ème utilisation) : 10.10.0.10 /24	Dispositif de sécurité et de protection basée sur une gestion centralisée du réseau. Il fournit les fonctionnalités suivantes : ✓ Gestion des micrologiciels ✓ Configuration des appareils à partir d'une seule console ✓ Gestion centralisée et suivi de la configuration du système ✓ Utilisation des Scripts (langage CLI) Génération des journaux de trafic des appareils connectés et prise en charge de la gestion des ressources
FortiAnalyser	Version :7 .0.12 / 7.4.2 de FortiNet RAM : 2 Go minimum Adresse IP(1ère utilisation) : 10.10.0.10 /24	Dispositif d'analyse et de traitement centralisée de données provenant de diverses sources sur le réseau. Il permet de générer des rapports et des journaux sur le trafic réseau fournissant les informations suivantes : ✓ Indicateurs automatisés de compromission (IOC), analyse des journaux de sécurité avec FortiGuard IOC Intelligence pour la détection APT ✓ Aperçu historique et en temps réel de l'activité du réseau Gestion simplifiée des événements

III.2.4 Principales composantes d'Active Directory

Tableau III.3 : Principales Composantes d'AD

Composantes	Rôle / Caractéristiques
Domaine	La base de données est responsable de rassembler les objets qui partagent un même espace de nom (un domaine doit nécessairement être basé sur un système DNS, qui peut être mis à jour en temps réel). [42] Dans notre cas, Nous avons créé une machine virtuel nommée client01 qui fonctionne sur Windows 10. Ensuite, nous l'avons intégrée dans notre domaine « **Nesda.lan** ».
Arbre	Il s'agit du rassemblement hiérarchique de divers domaines qui partagent un espace de nom. [42]
Forêt	Il s'agit d'une association de plusieurs arbres de domaine qui partagent un catalogue global et qui ne partagent pas nécessairement un espace de

	nom commun. [42]
Unité d'organisation	Une unité d'organisation (OU) est une partie d'un dossier ou d'un sous-conteneur dans un système d'exploitation où se trouvent des comptes d'utilisateurs, des ordinateurs, des groupes, etc. Seuls des administrateurs de domaine et des utilisateurs ayant des autorisations déléguées à une unité d'organisation peuvent gérer les unités d'organisation. [W25] Vu que notre entreprise propose de nombreux services et plusieurs appareils et utilisateurs, il est important de configurer Active Directory efficacement. Chaque service (Unité d'organisation) contient plusieurs ordinateurs et utilisateurs organisés.

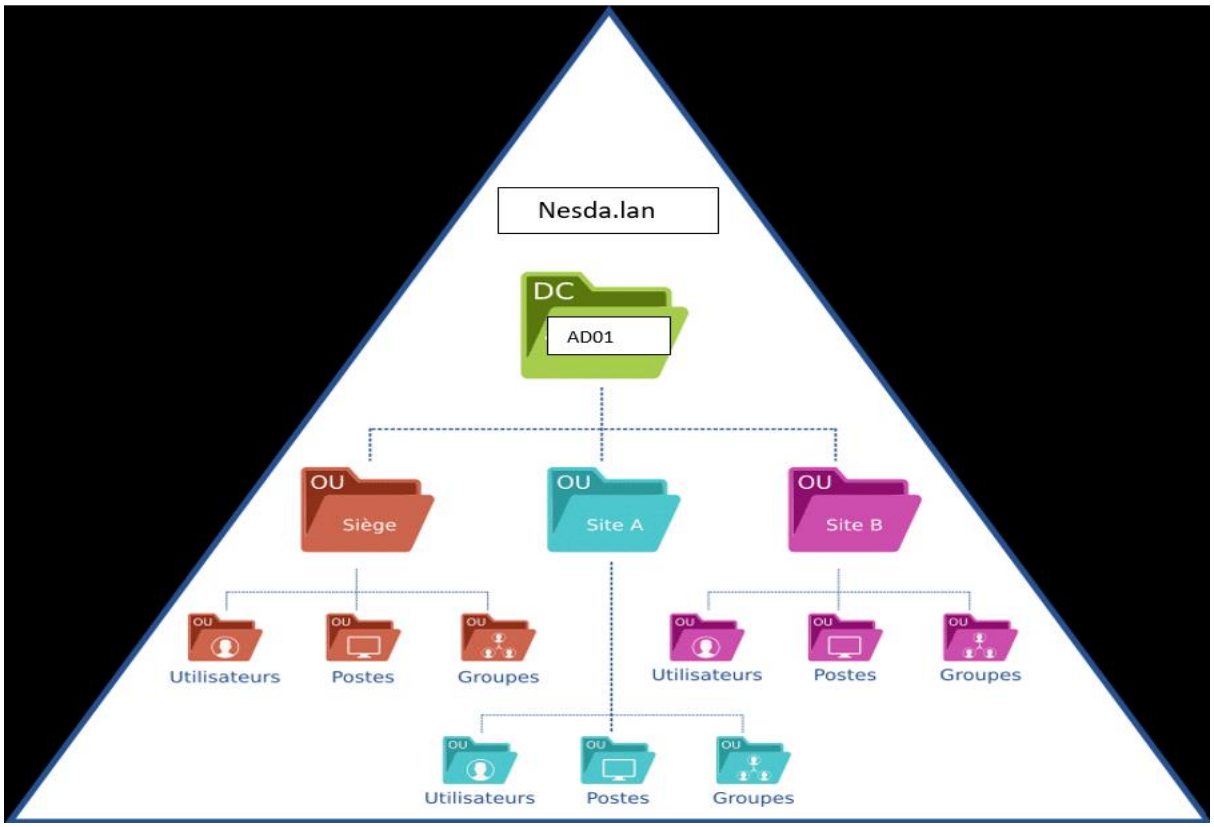


Figure III.3: Unité d'organisation dans un Domain AD [W26]

III.2.4.1 Les étapes d'organisation :

- **Création d'une unité d'organisation « UMBB »**

Dans la barre Outil, ouvrez la console « Utilisateurs et ordinateurs Active Directory ». Ensuite, cliquez droit sur le nom du domaine « Nesda.lan », puis sélectionnez « Nouveau » puis « Unité d'organisation ».

Ensuite, nous mentionnons le nom de l'unité d'organisation (nous avons opté pour « UMBB »)

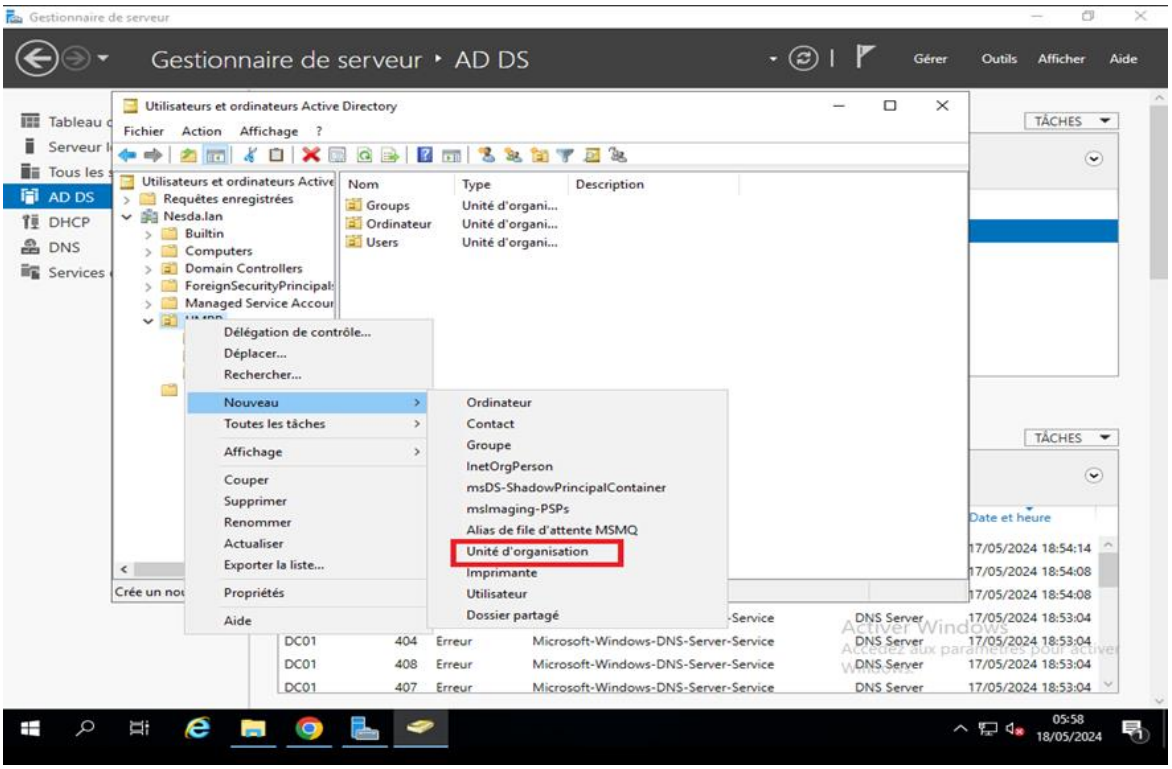


Figure III.4 : création d'unité d'organisation

- **Création d'un groupe « UMBB-GG »**

Nous faisons une clique droite sur l'unité d'organisation UMBB, puis nous sélectionnons « Nouveau » puis « Groupe » et puis nous sélections le nom de group « UMBB-GG »

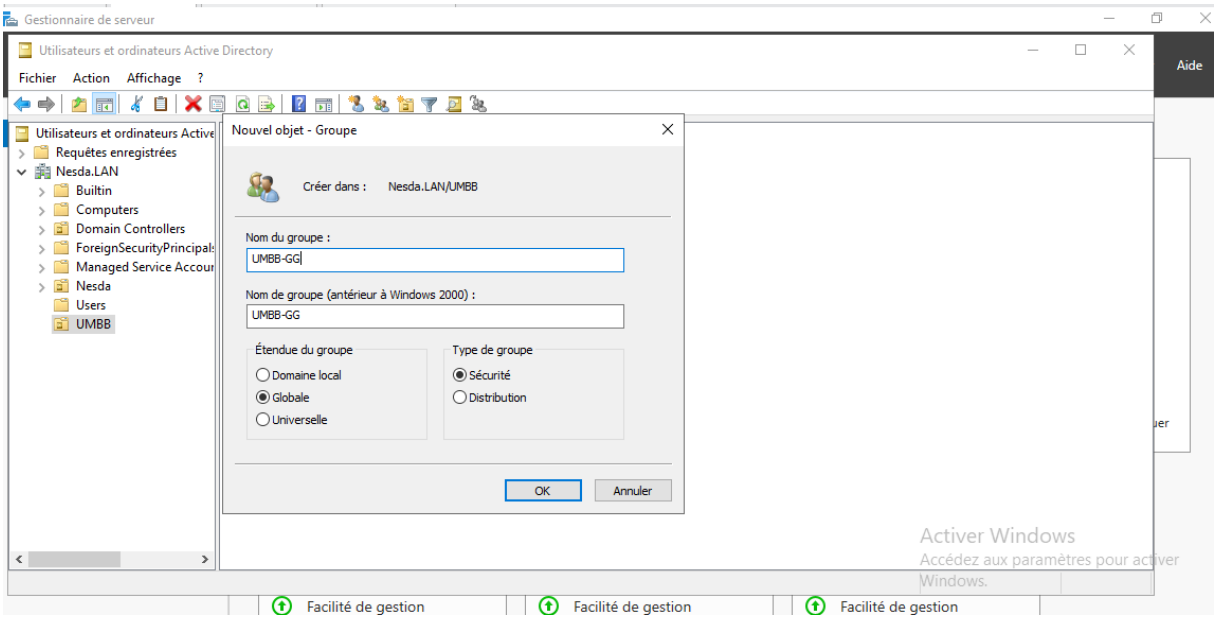


Figure III.5 : création de group UMBB-GG

- **Création d'ordinateur**

Nous faisons une clique droite sur l'unité d'organisation UMBB, puis nous sélectionnons « Nouveau » puis « Ordinateurs »

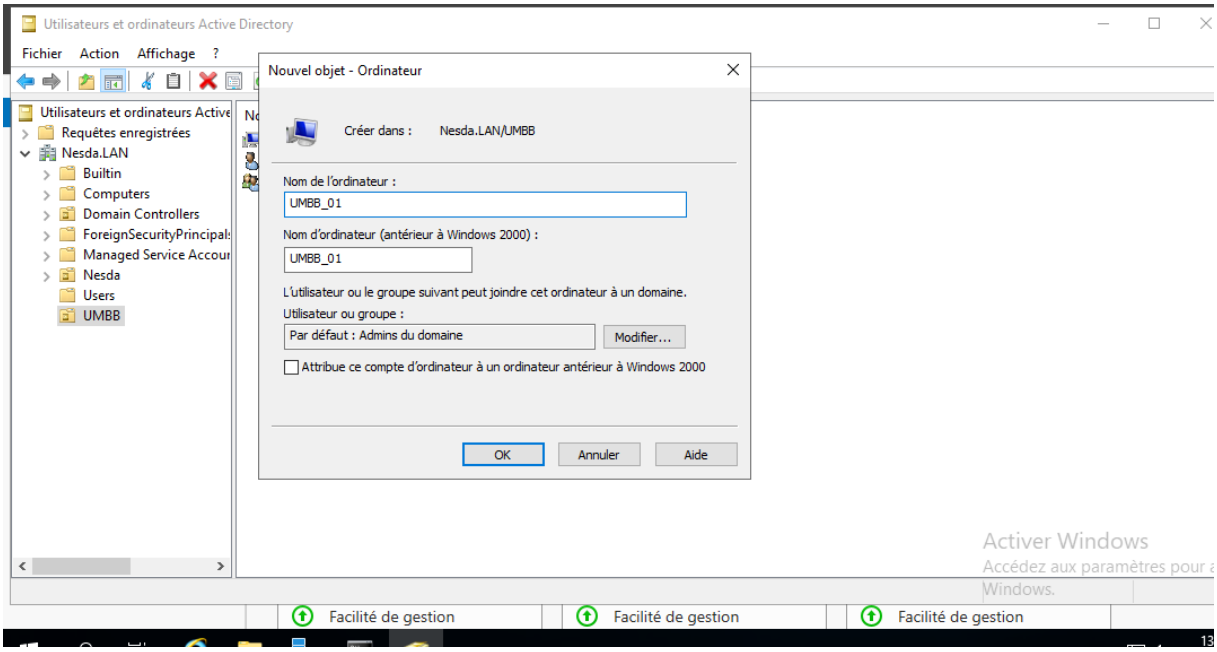


Figure III.6: création d'ordinateur UMBB_01

- **Création des utilisateurs**

Nous faisons une clique droite sur l'unité d'organisation UMBB, puis nous sélectionnons « Nouveau » puis « Utilisateur »

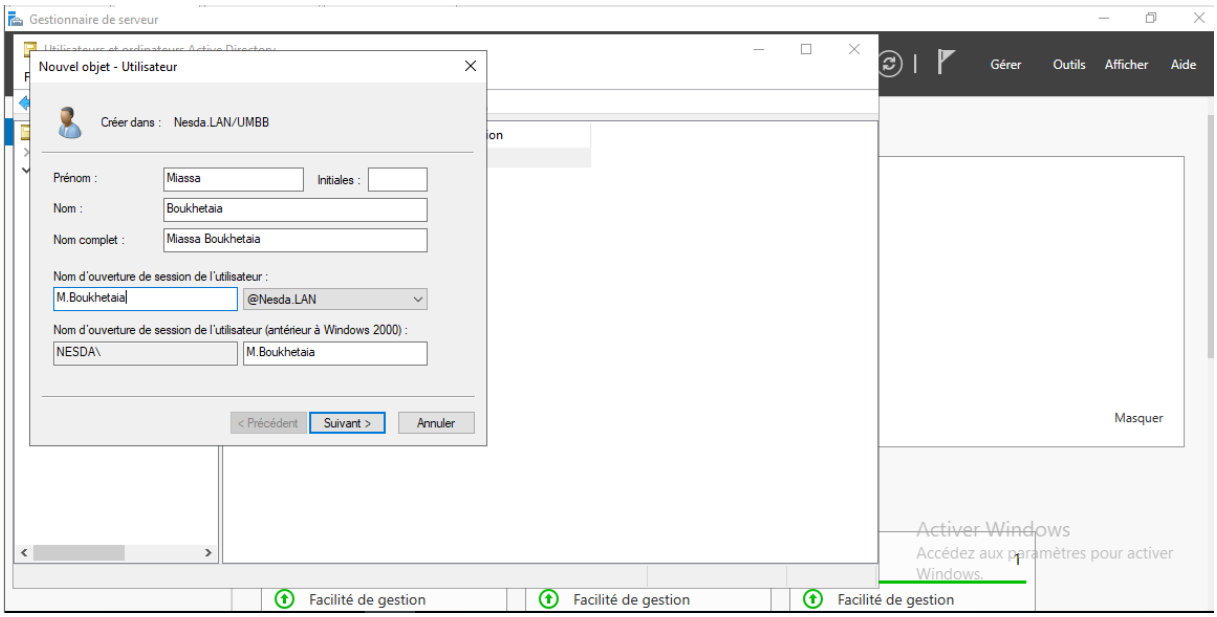


Figure III.7: Création d'un nouvel utilisateur

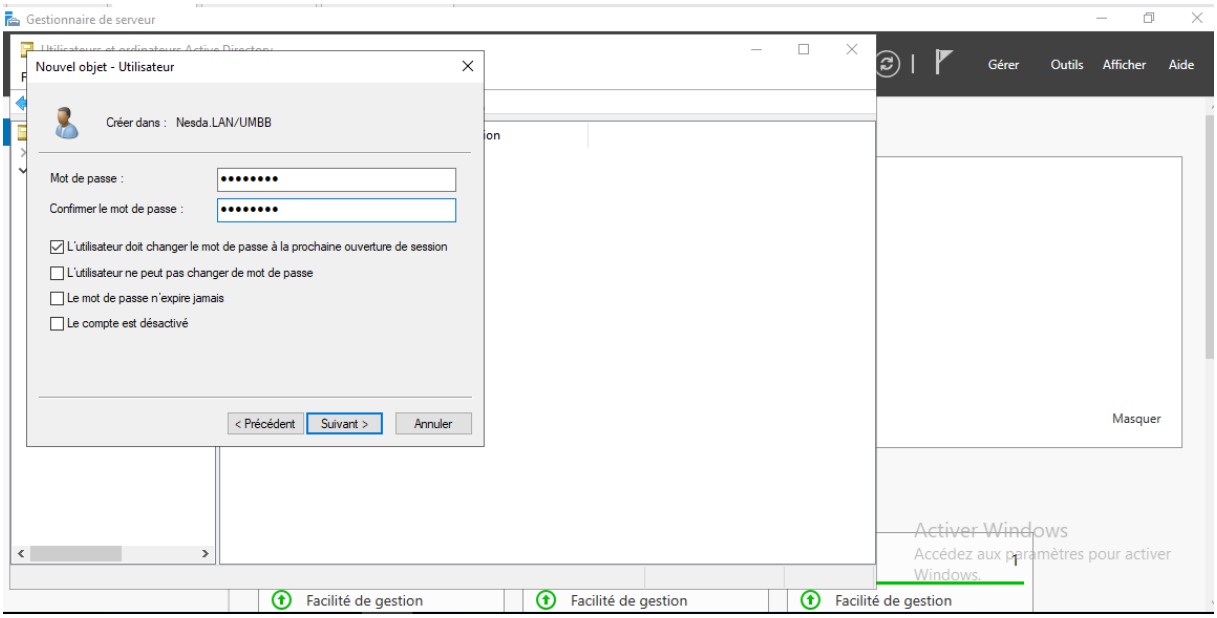


Figure III.8: insertion de mot de passe pour l'utilisateur

III.3 Failles de sécurités constatées :

Les failles de sécurité informatique sont la principale cause des cyberattaques. Une faille de sécurité c'est une vulnérabilité d'un système ou d'une application qui peut être exploitée par des cybercriminels pour accéder aux données ou contrôler le système. Il existe de nombreux types, chacune présentant des caractéristiques et des méthodes d'exploitation uniques. [W27]

Notre réseau peut être soumis à diverses alertes internes et externes. Nous allons Jeter un coup d'œil aux alertes les plus courantes détectées sur notre réseau :

Tentative d'authentification : Lorsqu'un utilisateur ou un appareil tente de se connecter à un réseau d'entreprise, il doit d'abord fournir une identité qui sera validé donc l'identifiant aura l'autorisation d'accéder à la ressource autorisé et vice versa selon la base de données de serveur d'authentification LDAP. Les tentatives d'authentification, qu'elles réussissent ou non, sont généralement enregistrées dans les journaux de sécurité à des fins de suivi et d'audit, ce qui permet aux administrateurs réseau de bien contrôler et gérer le réseau.

Panne de réseau (Network down) : Les événements « Panne de réseau » sont souvent considérés comme des alertes critiques pouvant compromettre le bon fonctionnement du réseau. La défaillance d'une interface réseau ou d'une connexion critique peut avoir de graves conséquences, notamment :

Perte de connectivité : les utilisateurs et les services peuvent ne pas pouvoir accéder aux ressources du réseau.

Perturbation de service : Les applications dépendantes du réseau peuvent ne pas fonctionner correctement.

Risque de sécurité : les pannes de réseau peuvent également être exploitées par des attaquants pour compromettre la sécurité.

Impact sur la productivité : Les utilisateurs peuvent ne pas être en mesure de terminer leurs tâches et la productivité globale peut être affectée.

Par conséquent, il est important de surveiller de près les événements de panne de réseau et de définir des alertes appropriées pour les résoudre rapidement.

Anomalie de la bande passante (Bandwidth anomaly) :

Les alertes d'anomalie de bande passante sont importantes pour détecter un comportement anormal du réseau tel que des pics soudains ou une utilisation excessive du trafic.

Ces anomalies peuvent être le signe d'une attaque DoS ou DDoS, où un attaquant inonde le réseau de trafic afin de le rendre inutilisable. Ces attaques constituent une menace sérieuse pour le réseaux d'entreprise, provoquant des interruptions de service, des pertes de revenus et des problèmes de réputation. En configurant des alertes pour ces anomalies, les organisations peuvent identifier rapidement ces menaces et prendre des mesures pour protéger leurs réseaux.

Licence expirée d'un fortigate : la licence FortiGate est importante pour activer et maintenir des fonctionnalités de sécurité avancées telles que les mises à jour antivirus, la prévention des intrusions, le filtrage Web et le contrôle des applications. L'lorsqu'une licence expire, ces mises à jour et fonctionnalités importantes sont désactivées, ce qui rend FortiGate moins efficace et vulnérable aux nouvelles cyberattaques. Cela peut également conduire au non-respect des règles de sécurité. Fortinet fournit des alertes proactives d'expiration de licence et crée des journaux d'expiration qui sont envoyés à FortiManager et FortiAnalyzer pour garantir une surveillance continue et une gestion efficace de la sécurité.

III.3 Implémentation de la solution de sécurité :

III.3.1 La topologie de réseau à étudié

Le réseau de l'entreprise NESDA est vaste, composé de la direction générale (DG) et de 58 annexes. Pour incarner notre étude au niveau de ce réseau, nous avons dû l'appliquer à une seule annexe et de poursuivre nos simulations à distance via VPN avec la machine de notre encadrant, en raison des problèmes et des obstacles de la durée de validité des licences, leurs compatibilités et de la sous-performance de notre machine physique, que nous avons rencontrés au cours de notre période de stage.

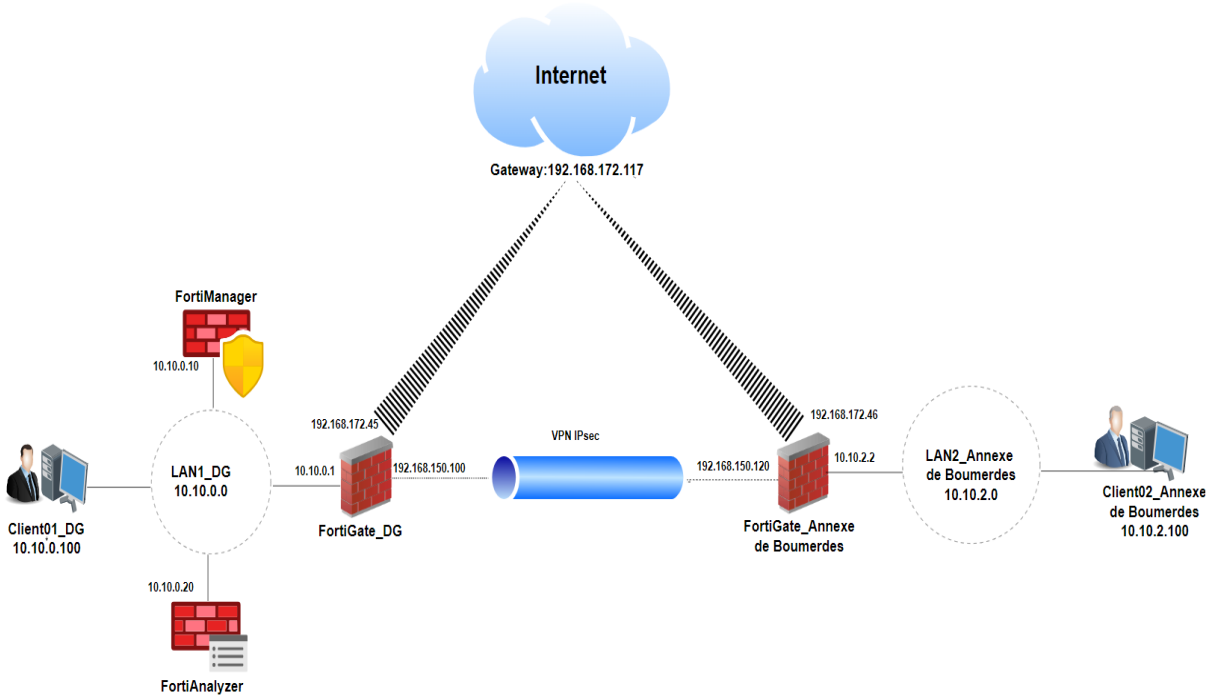


Figure III.9: La topologie de réseau à étudié

III.3.2 Installation et configuration des matériaux et logiciels utilisés :

III.3.2.1 Installation de le fortiGate

- **Téléchargement de L'image OVF de Fortigate**

D'abord pour installer le fortigate sur VMWare on doit télécharger le fichier de l'image « ovf » de fortigate depuis le site de Fortinet

- **Création de la nouvelle machine virtuelle FG_01**

Il vous suffit de sélectionner « file » puis « Open » sur l'interface de VMWare pour créer une nouvelle machine virtuelle FortiGate. Nous choisissons l'image OVF de notre Fortigate, puis nous lui donnons le nom « FG_01 ». Enfin, nous spécifions l'emplacement où nous souhaitons stocker la VM.

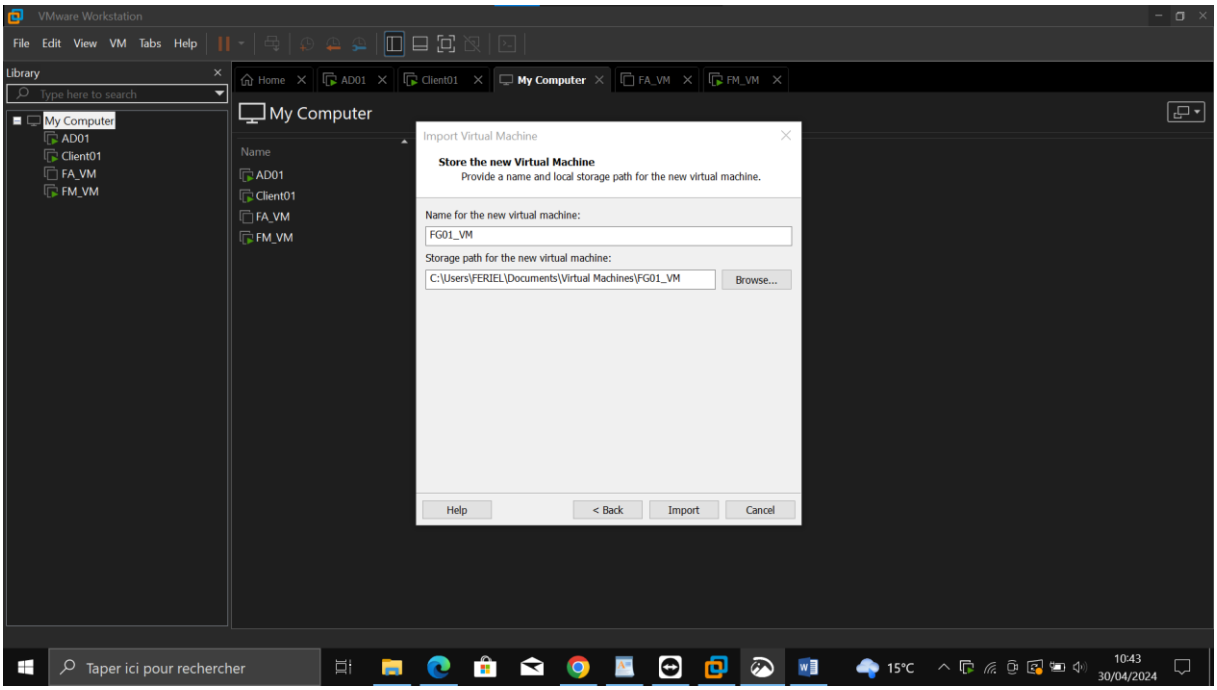


Figure III.10: Création de la machine virtuel FG_01

- **Configuration des cartes réseaux**

La premier carte est « Network adapter » on la configure « Bridged » et on va à « Edite » puis choisit « Virtual Network Editor» , après on clique sur « Change setting » on choisit « VMnet0 » et dans la barre Vmnet Information on sélectionne Bridged on choisit « Intel(R)Dual Band Wireless7265 »

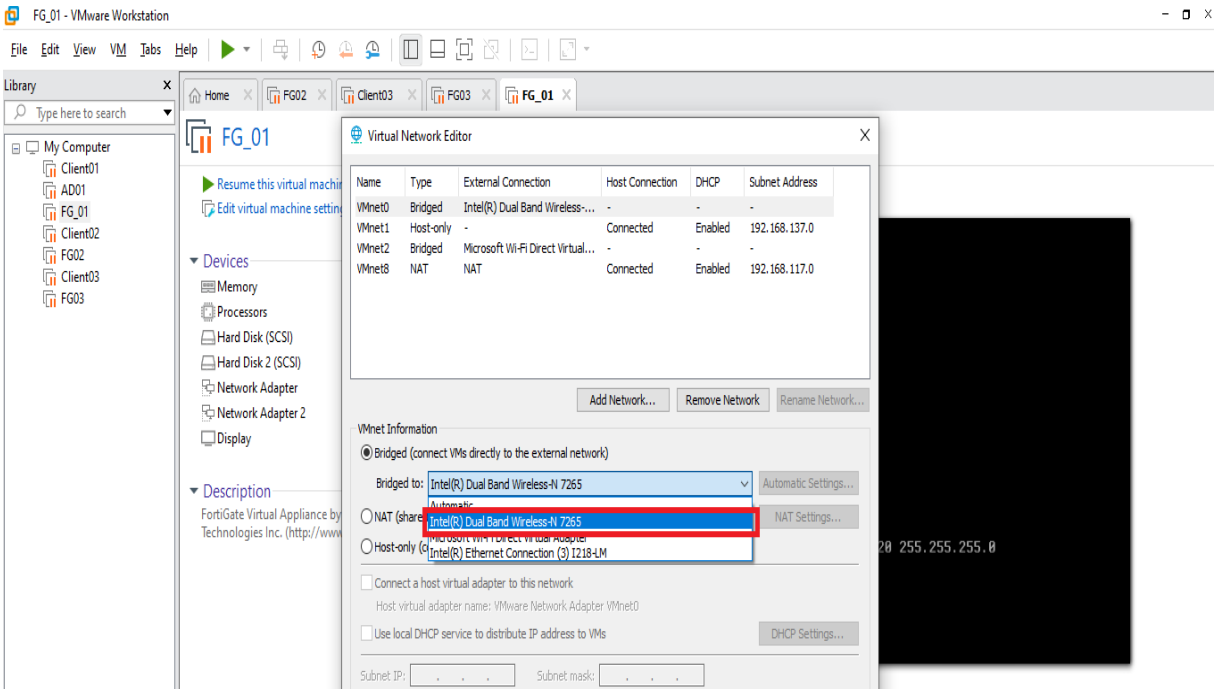


Figure III.11: Configuration des cartes réseaux

Et le deuxième carte « Network adapter1 » nous avons lui configurer en « LAN »

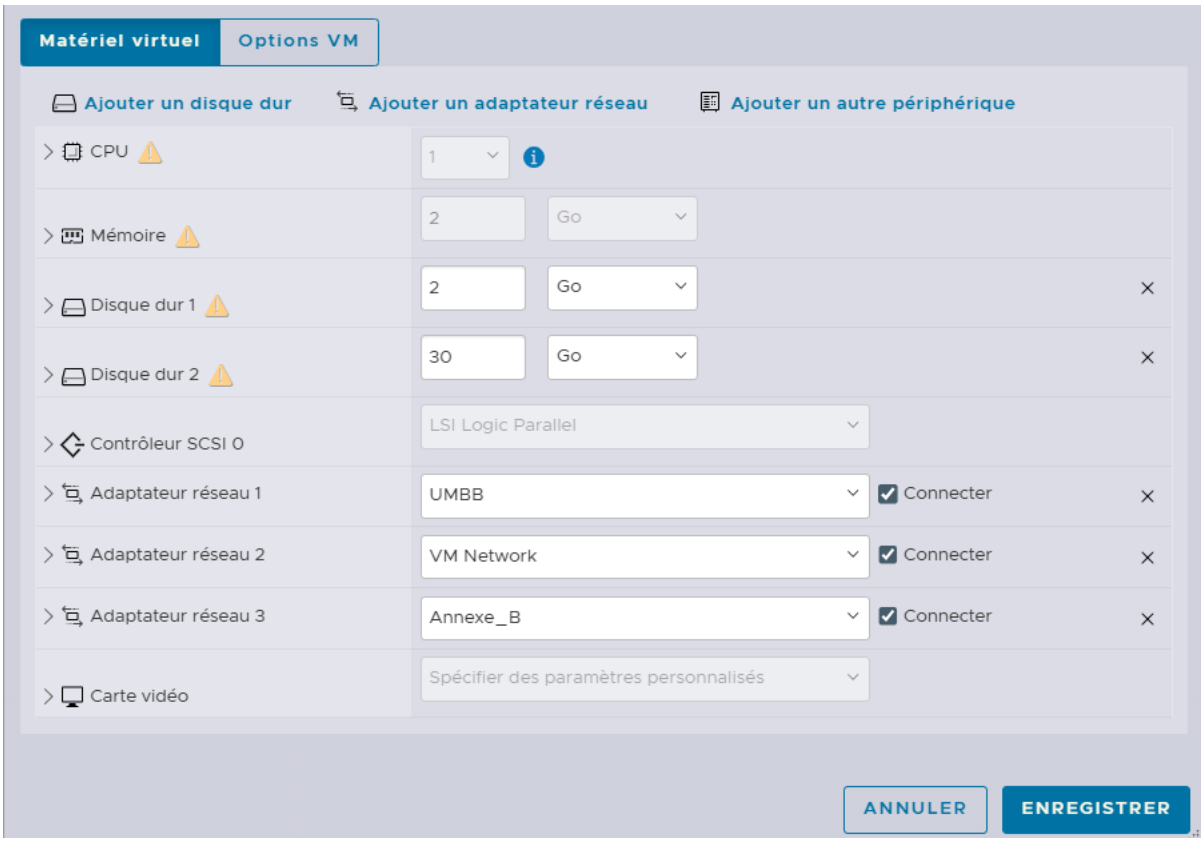


Figure III.12: Configuration des cartes réseaux pour les adaptateurs

III.3.2.2 Configuration de Fortigate

- **Accès au consol et configuration des adresses IP de gestion**

Après avoir démarré la machine virtuelle « **FG_01** » en cliquant sur « **Power on This Virtual Machine** » dans VMware, nous avons accédé à l'interface de connexion où nous avons saisi « **admin** » et appuyé sur « **Entrée** ».

Comme le mot de passe par défaut était vide, nous avons simplement appuyé à nouveau sur « **Entrée** » pour accéder au système.

Ensuite, nous avons été invités à changer notre mot de passe, que nous avons fait et confirmé.

```
Loading flatkc... ok
Loading /rootfs.gz...ok

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Serial number is FGVMEVFNESNWNJAD

FortiGate-VM64 login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
```

Après avoir été connectés, nous avons procédé à la configuration des interfaces réseau en utilisant la ligne de commande FortiGate (CLI). Ainsi, nous avons entré la commande « **configuration interface système** » afin d'accéder au mode de configuration des interfaces Système.

Ensuite, en optant pour la commande « **éditer port1** », nous avons choisi l'interface réseau 1, qui était l'interface Bridged utilisée pour la connexion à Internet dans notre cas.

La commande « **set mode DHCP** » a été utilisée pour configurer cette interface en mode DHCP, ce qui permet à l'interface port1 de recevoir automatiquement une adresse IP de notre serveur DHCP, qui est intégré à notre serveur AD.

```
FGVMEVJHVFOQVFE3 # config  system  interface

FGVMEVJHVFOQVFE3 (interface) # edit port1

FGVMEVJHVFOQVFE3 (port1) # set mode static

FGVMEVJHVFOQVFE3 (port1) # set ip 10.10.0.1 255.255.255.0

FGVMEVJHVFOQVFE3 (port1) # set allowaccess ping https http  ssh fgfm

FGVMEVJHVFOQVFE3 (port1) # next
FGVMEVJHVFOQVFE3 (interface) # edit port2

FGVMEVJHVFOQVFE3 (port2) # set mode static

FGVMEVJHVFOQVFE3 (port2) # set ip 192.168.172.45 255.255.255.0

FGVMEVJHVFOQVFE3 (port2) # set allowaccess ping https http  ssh fgfm

FGVMEVJHVFOQVFE3 (port2) # next

FGVMEVJHVFOQVFE3 (interface) # edit port3

FGVMEVJHVFOQVFE3 (port3) # set mode static

FGVMEVJHVFOQVFE3 (port3) # set ip 192.168.150.100 255.255.255.0

FGVMEVJHVFOQVFE3 (port3) # set allowaccess ping https http ssh fgfm
```

Nous avons utilisé la commande « **set allowaccess ping http https ssh fgfm** » pour autoriser les différentes formes d'accès sur cette interface. Cette commande donne accès aux éléments suivants :

- ✓ L'accès HTTP/HTTPS pour la gestion via une interface Web sécurisée.
- ✓ L'accès Ping pour tester la connectivité et diagnostiquer d'éventuels problèmes de réseau.
- ✓ L'accès SSH pour une connexion sécurisée à distance via Secure Shell.
- ✓ L'accès au FortiGate Fabric Management (fgfm) pour une gestion centralisée par FortiManager

La commande « **set mode static** » ont été utilisées pour configurer l'interface2 en mode statique, ainsi que l'adresse IP 10.10.0.1 et le masque de sous-réseau /24. En utilisant les commandes « **set ip 10.10.0.1** » Par la suite, nous avons permis l'accès requis à cette interface et quitté le mode de configuration en cliquant sur « **end** ». La commande « **get sys interface physical** » a été utilisée pour vérifier la configuration des interfaces physiques et obtenir toutes les informations sur les interfaces de notre FortiGate.

```
FGVMEVJHVFOQVFE3 # get system interface physical
== [onboard]
        ==[port1]
                mode: static
                ip: 10.10.0.1 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 10000Mbps (Duplex: full)
                FEC: none
                FEC_cap: none
        ==[port2]
                mode: static
                ip: 192.168.172.45 255.255.252.0
                ipv6: ::/0
                status: up
                speed: 10000Mbps (Duplex: full)
                FEC: none
                FEC_cap: none
        ==[port3]
                mode: static
                ip: 192.168.150.100 255.255.255.0
--More--
```

- ➢ **Vérification l'accès à l'internet**

Afin de vérifier si le fortigate est connecté à Internet, nous pouvons effectuer un ping sur le 8.8.8.8

```
FGVMEVJHVFOQVFE3 # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=114 time=27.4 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=25.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=25.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=25.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=26.1 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 25.3/25.9/27.4 ms
```

➢ Connexion à l'interface Web et graphique

Nous ouvrons le navigateur web sur le client et saisissons l'adresse http://10.10.0.1 La connexion n'étant pas sécurisée, nous recevons un avertissement. Nous cliquons sur « **Avancé** » pour continuer l'accès à notre FortiGate. Ensuite, nous saisissons le nom d'utilisateur et le mot de passe pour nous connecter.

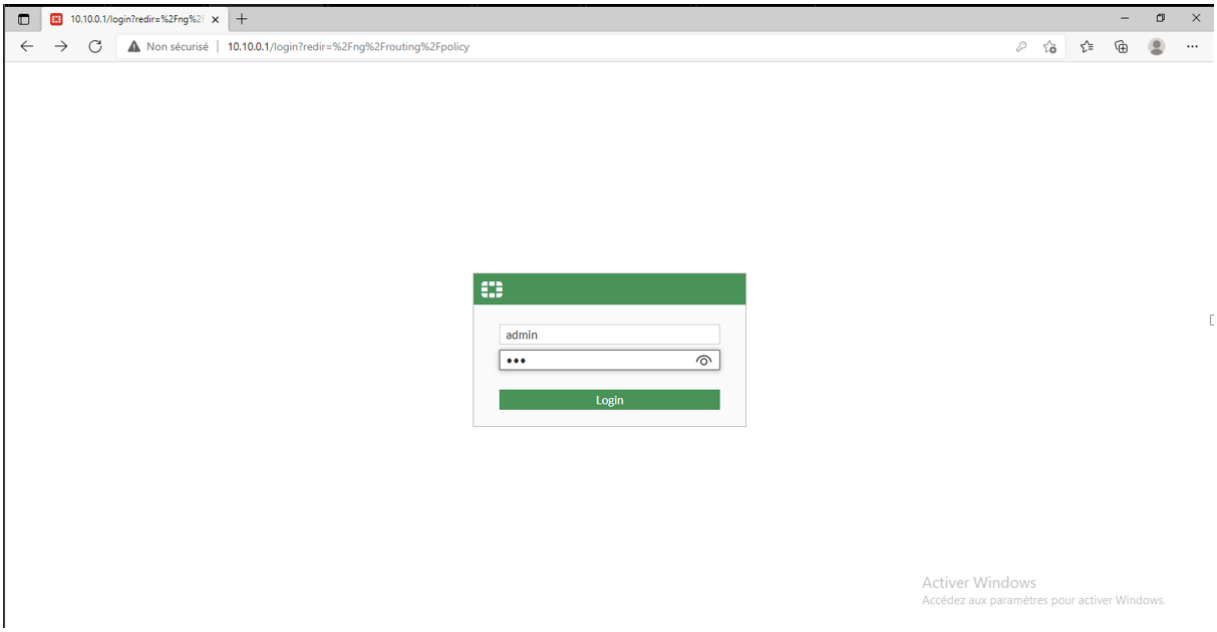
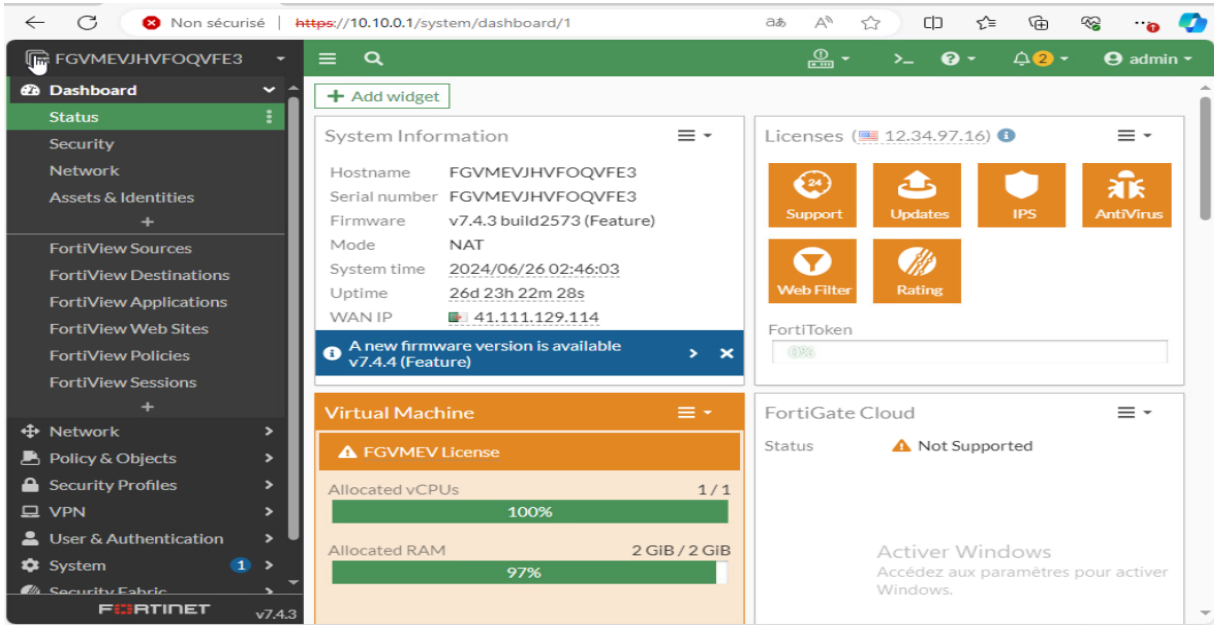


Figure III.13: L'interface web de fortigate

Nous cliquons sur « **Connexion** » pour accéder à l'interface graphique de notre FortiGate .



FigureIII.14 : L'interface graphique de FortiGate

- **Les interface (ports) de fortigate sur l'interfaces (ports) graphique**

Au sein de l'interface graphique de FortiGate, nous sélectionnons « **Network** » puis « **Interface** » afin de vérifier les ports de notre FortiGate.

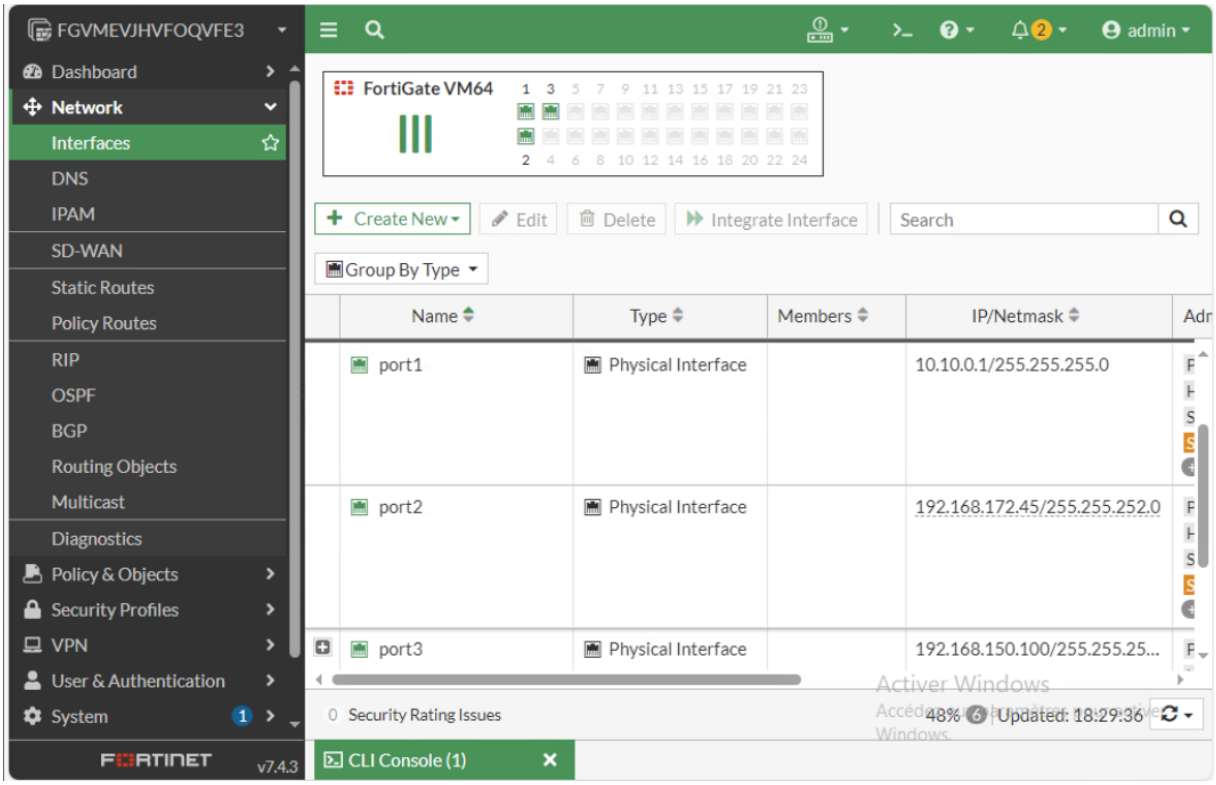


Figure III.15 : L'affichage des interfaces de fortigate

- **Configuration de Gateway**

Dans cette étape, nous devons configurer une passerelle (Gateway) pour le FortiGate. Pour cela, nous cliquons sur « **Network** », puis sur « **Static Route** », et ensuite sur « **Create New** ».

La destination est configurée par défaut en tant que route « **0.0.0.0/0.0.0.0** », ce qui implique que cette route sera utilisée pour tout le trafic qui ne correspond pas à des routes plus spécifiques déjà configurées sur le FortiGate.

Enfin, nous indiquons l'adresse IP de la passerelle par défaut, qui est l'adresse IP de la passerelle du réseau du fournisseur de services Internet.

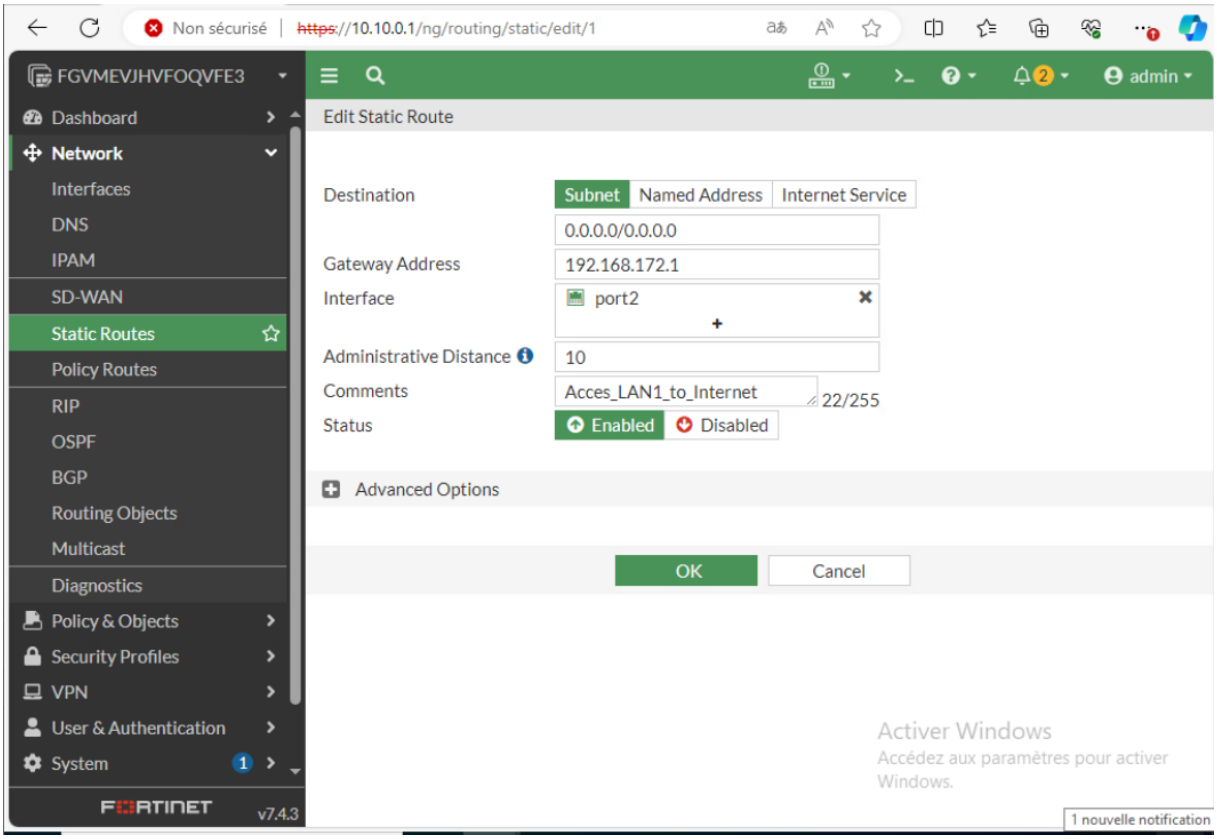


Figure III.16: Configuration de Gateway

- **Configuration de politique de fortigate (pare-feu)**

On va à « **Policy and Object** » sélectionné « firewall Policy », Nous avons créé une règle qui permet à tous les équipements réseau d'accéder à Internet et à tous les sites Web.

Dans notre FortiGate, la politique « **Internet Accès** » établit les réglages de connexion à Internet pour les appareils connectés au port2 (incoming) et au port1 (outgoing). Toutes les sources et destinations, peu importe le service utilisé, sont autorisées ou interdées par cette politique, avec une attitude d'acceptation ou de refusion constante.

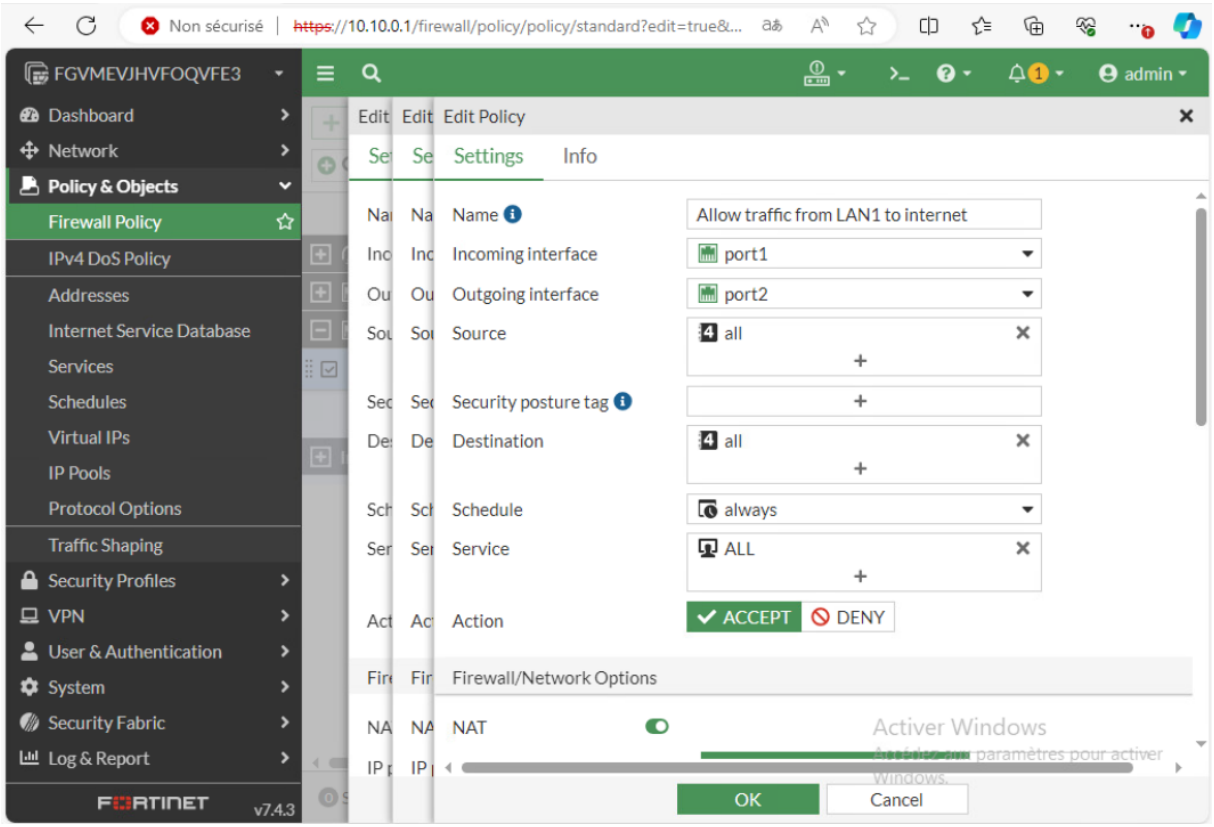


Figure III.17: Configuration de politique de fortigate (pare-feu)

➢ Création de LDAP server

Afin de centraliser et de gérer de manière efficace les informations d'identification et les autorisations au sein de notre réseau, nous avons mis en place un serveur LDAP dans notre fortigate. Ce serveur peut interroger et obtenir des informations sur les utilisateurs et les ordinateurs stockés dans le serveur Active Directory. Ceci rend l'authentification des utilisateurs plus facile et assure la sécurité. En utilisant les informations centralisées stockées dans AD, il est possible de gérer les politiques et l'accès au réseau.

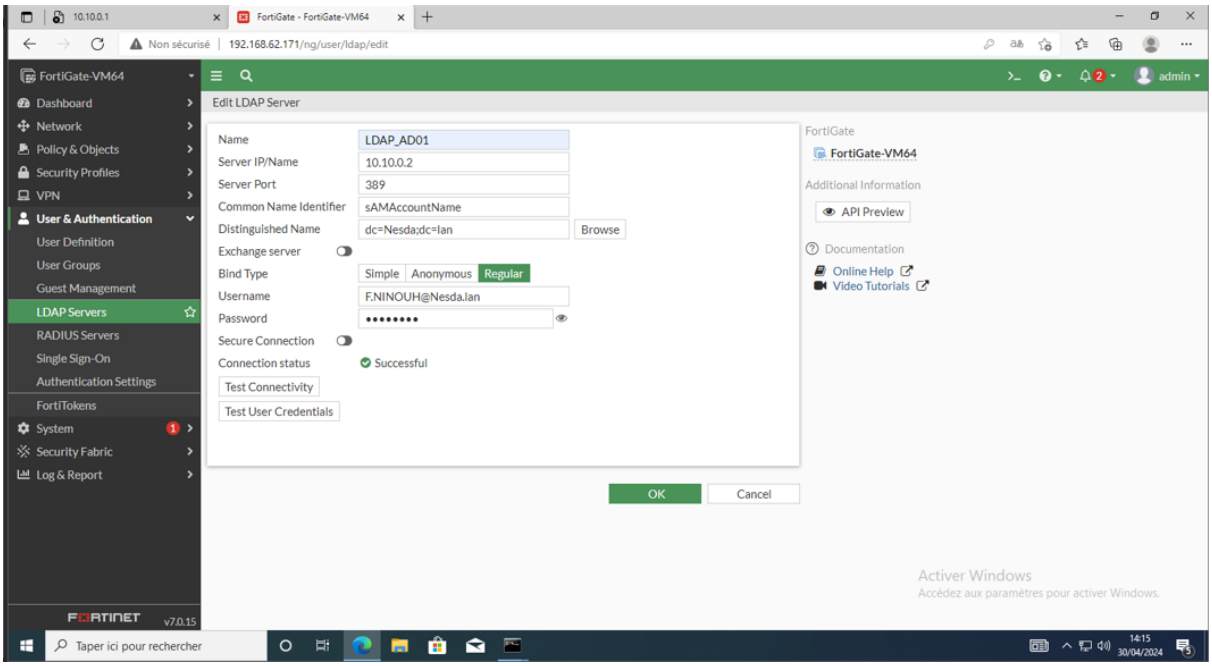


Figure III.18: L'authentification de l'utilisateur au niveau de serveur LDAP

Ainsi, un serveur LDAP a été installé sur notre FortiGate, que nous avons baptisé LDAP_AD01. L'adresse IP « **10.10.0.2** » du serveur LDAP est identique à celle d'AD et le port par défaut « **389** » est utilisé pour les communications. L'identifiant de nom commun « **sAMAccountName** »est utilisé pour identifier les utilisateurs, tandis que le nom distinctif est défini comme « **dc=nesda,dc=lan**» On a choisi le mode de connexion Normal, avec le nom d'utilisateur « **F.Ninouh@NESDA.lan** » et son mot de passe correspondant

- **Création de l'agent FSSO**

Quand nous ajoutons un utilisateur à Active Directory (AD) et que nous utilisons l'agent FSSO (Fortinet Single Sign-On) avec notre Fortigate, ces informations d'identification sont synchronisées avec le Fortigate par l'agent FSSO. Cela implique que chaque ajout ou modification d'un utilisateur dans AD est détectée par l'agent FSSO, qui met à jour les informations sur le Fortigate. De cette manière, le Fortigate conserve constamment les dernières informations d'authentification pour chaque utilisateur, assurant ainsi une gestion efficace des accès et une sécurité accrue sur le réseau. La synchronisation entre les utilisateurs du domaine AD et les règles de sécurité mises en place par le Fortigate est assurée grâce à ce processus automatisé, garantissant ainsi un environnement réseau cohérent et sécurisé.

Afin d'activer l'agent FSSO. Ainsi, nous avons suivi ces étapes.

Téléchargement de fichier d'installation FSSO via le site Fortinet « **support.fortinet.com** » ou n'importe quel site comme : https://infosecmonkey.com/installing-and-configuring-fsso/.

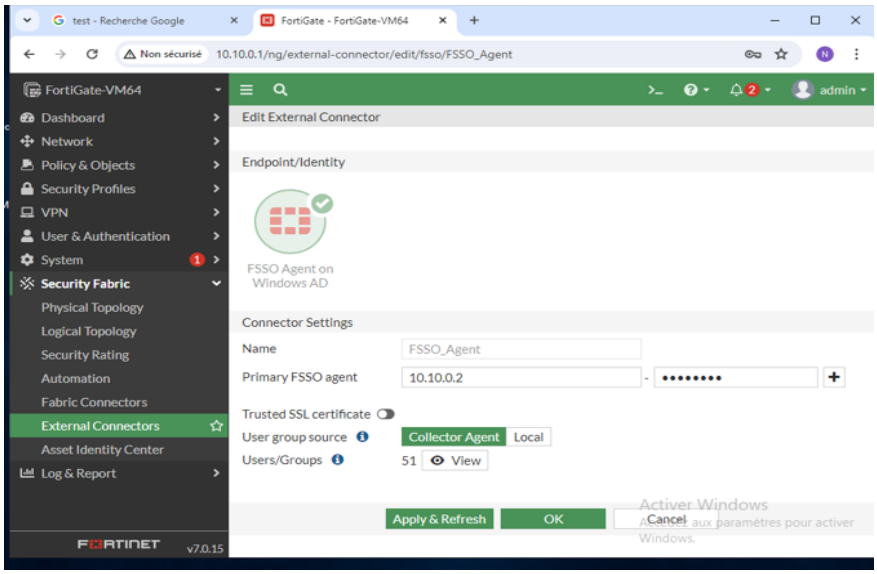


Figure III.19: Configuration de FSSO

III.3.2.3 Installations de FortiManger

Nous commençons par télécharger l'image OVF de FortiManager depuis le site web de Fortinet afin de procéder à l'installation.

Par la suite, dans VMware, nous nous rendons dans le menu « **File** » et choisissons « **Open** ».

Nous Nous sélectionnons le fichier « **fortimanager-vm64.ovf** » que nous avons déjà téléchargé.

Après avoir choisi le fichier, nous l'avons importé en cliquant sur « **Next** ». D'abord, acceptons les conditions de la licence, puis nommons la machine virtuelle FortiManager « **FM_VM** » et indiquons son emplacement de stockage sur notre système.

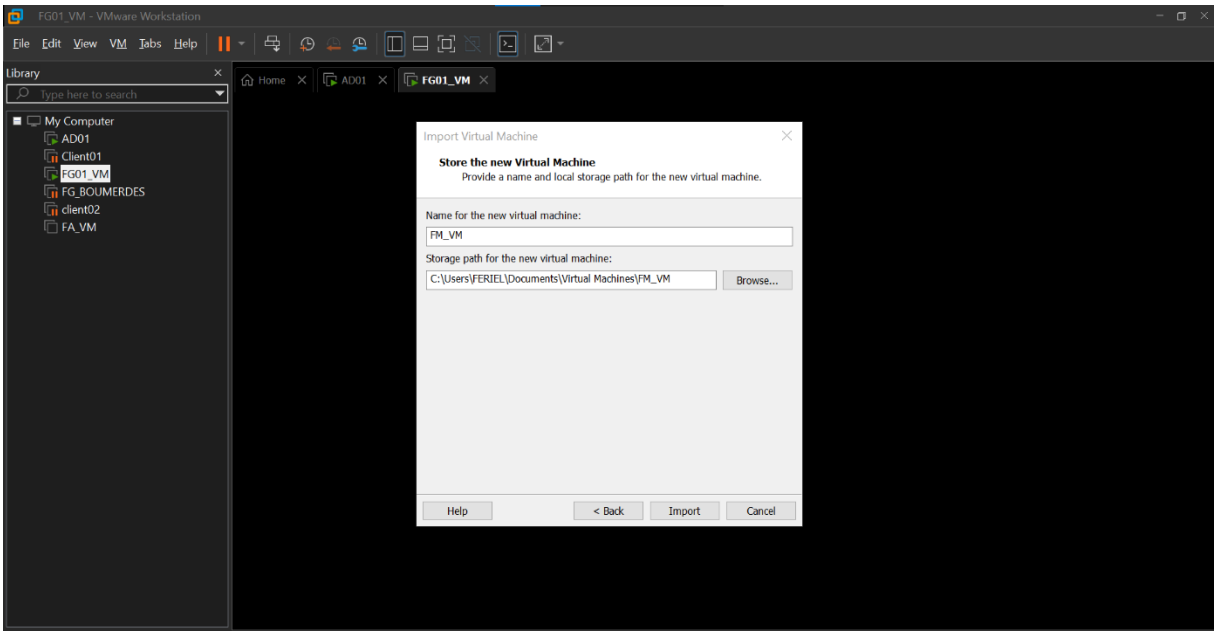


Figure III.20 : Instalation de fortimanager

L'unique carte réseau de notre FortiManager a été configurée en mode LAN.

III.3.2.4 Configuration de FortiManger

La configuration de l'interface de FortiManger présente une configuration similaire à celle du port Fortigate.

```
Serial number:FMG-VM0000000000

Total RAM 3G, CPU number 2, Set maximum concurrent Resync processes per CPU 4


FMG-VM64 login: admin
Password:
FMG-VM64 # config system interface

(interface)# edit port1

(port1)# set mode static

(port1)# set ip  10.10.0.10/24

(port1)# set allowaccess ping  http https  snmp ssh

(port1)# end

FMG-VM64 #
```

- **Configuration de serveur DNS**

Pour commencer, nous tapons la commande « **config system dns** » afin d'entrer en mode de configuration DNS. Ensuit il faut ajoute une nouvelle route via « **edit 1** ». Après on Effectue la configuration du serveur DNS principal avec l'adresse IP de serveur DNS principal « **set primery 10.10.0.2** » cela permet le FortiGate de résoudre les noms de domain et on ajout le serveur DNS secondaire avec l'adresse IP 8.8.8.8, qui est un serveur DNS public de Google avec la cammande «**set secondary 8.8.8.8** »

- **Configuration de la route par défaut**

Pour débuter, on utilise la commande « **config router static** » afin d'accéder au mode de configuration des routes. Par la suite, une nouvelle route est ajoutée en utilisant la commande « **edit 1** », puis on utilise la commande « **set gateway 10.10.0.1** » pour configurer la passerelle par défaut. Finalement, nous terminons avec l'option « **set device port1** » afin de préciser que l'interface de sortie pour cette route est porte1.

Il est essentiel de mettre en place ces configurations afin d'assurer une communication efficace de FortiManager sur le réseau, de résoudre les noms de domaine et de transmettre le trafic via la passerelle adéquate. Le script prépare FortiManager à gérer et contrôler les appareils FortiGate de manière centralisée et sécurisée en définissant ces paramètres de base.

```
FA_VM # config  system  route
(route)# edit 1
(1)# set gateway  10.10.0.1
(1)# set device port1
(1)# end
FA_VM # config  system  dns
(dns)# set primary 10.10.0.2
(dns)# set secondary 8.8.8.8
(dns)# end
```

- **Connexion à l'interfaceWeb et graphique**

On ouvrira le navigateur web dans le client SSH et on tape http://10.10.0.10 .Nous entrons le nom de l'admin et son mot de passe, puis nous cliquons sur « login »

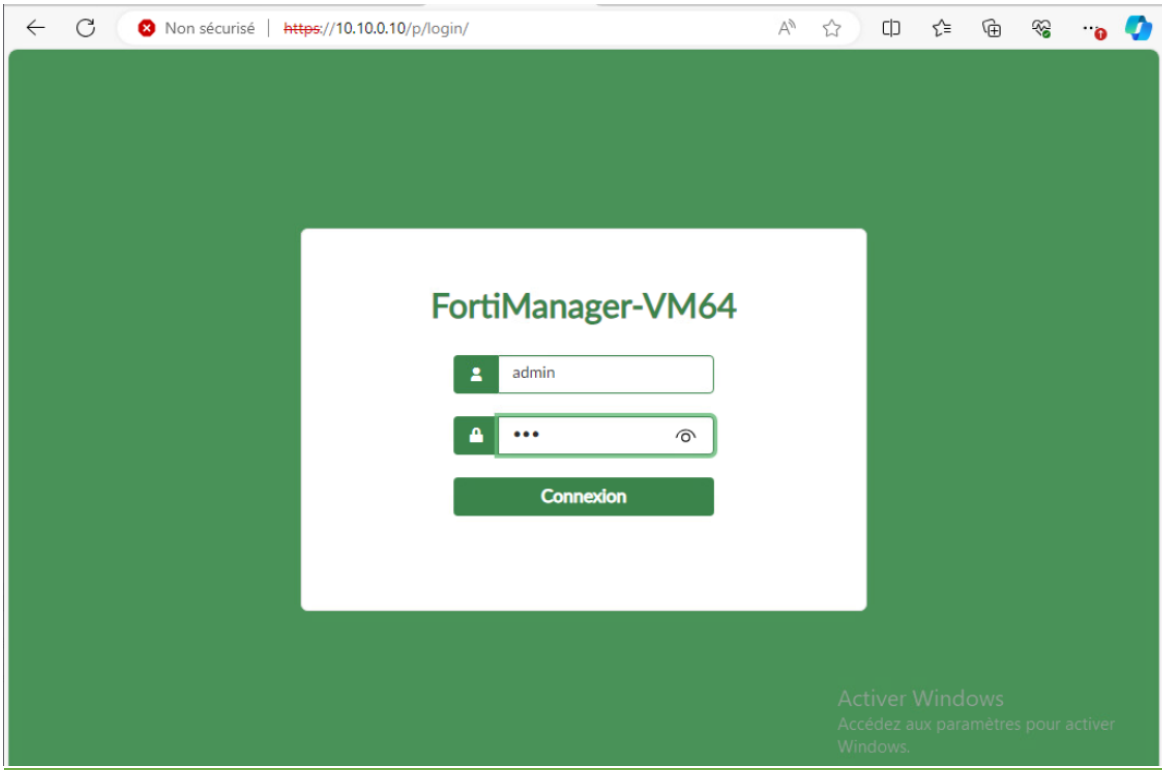


Figure III.21 : L'interface web de FortiManager

Nous cliquant sur « **Connexion** » pour accéder à l'interface graphique de notre FortiManager

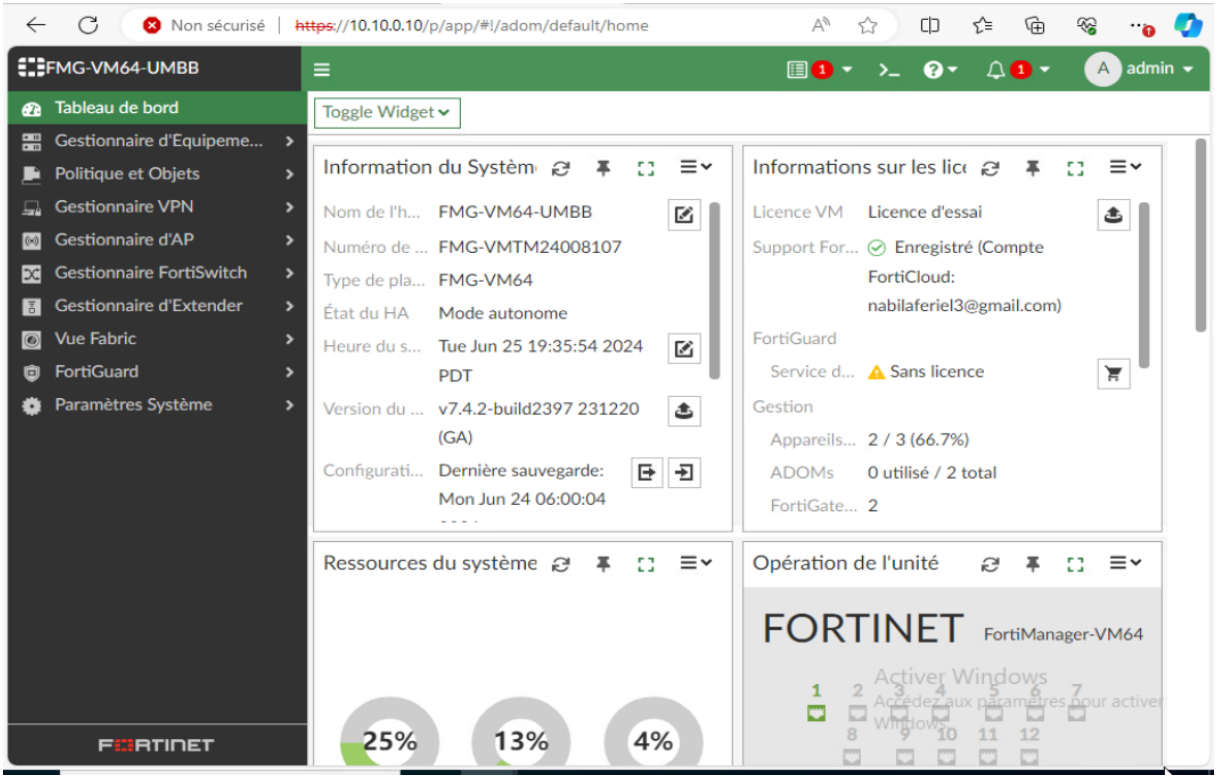


Figure III.22: L'interface graphique de FortiManager

III.3.2.5 L'installation de FortiAnalyzer :

Pour l'installation de FortiAnalyzer, nous suivons les mêmes étapes que pour l'installation de FortiManager. Tout d'abord, nous téléchargeons l'image OVF de FortiAnalyzer depuis le site web de Fortinet.

Ensuite, dans VMware, nous allons dans le menu « **File** » et sélectionnons « **Open** ». Cette fois-ci, nous choisissons le fichier « **FortiAnalyzer-vm64.ovf** » que nous avons déjà téléchargé. Après avoir sélectionné le fichier, nous l'importons en cliquant sur « **Next** ». Nous acceptons les conditions de la licence, puis nous nommons la machine virtuelle FortiAnalyzer « **FA_VM** » et indiquons son emplacement de stockage sur notre système. Les étapes suivantes de l'installation sont identiques à celles décrites précédemment pour FortiManager.

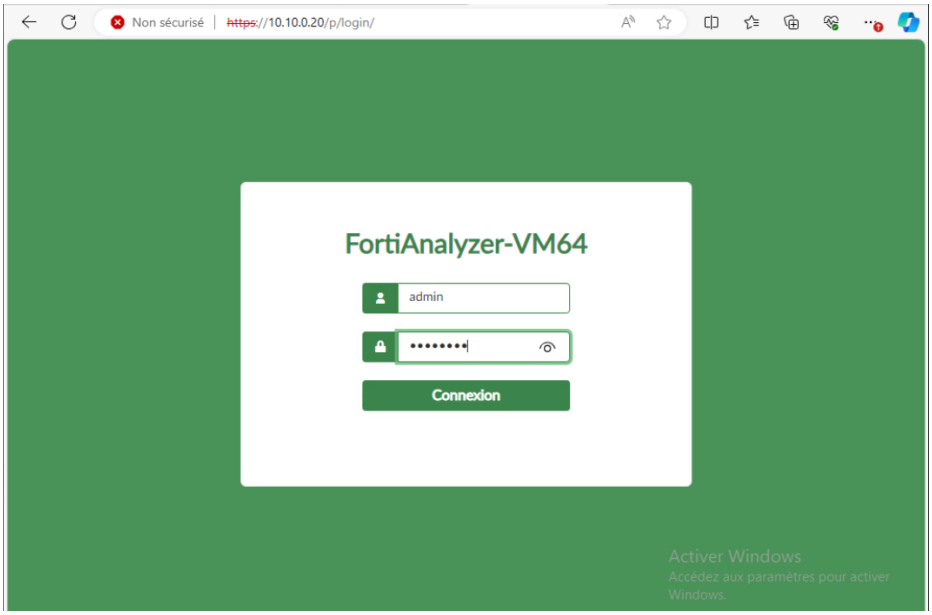
III.3.2.6 La configuration de FortiAnalyzer :

La configuration de l'interface de FortiAnalyzer est similaire que le FortiGate et FortiManager.

```
FA_VM login: admin
Password:
FA_VM # config  system  interface

(interface)# edit port1

(port1)# set ip  10.10.0.20 255.255.255.0

(port1)# set allowaccess ping  http https ssh

(port1)# end
```

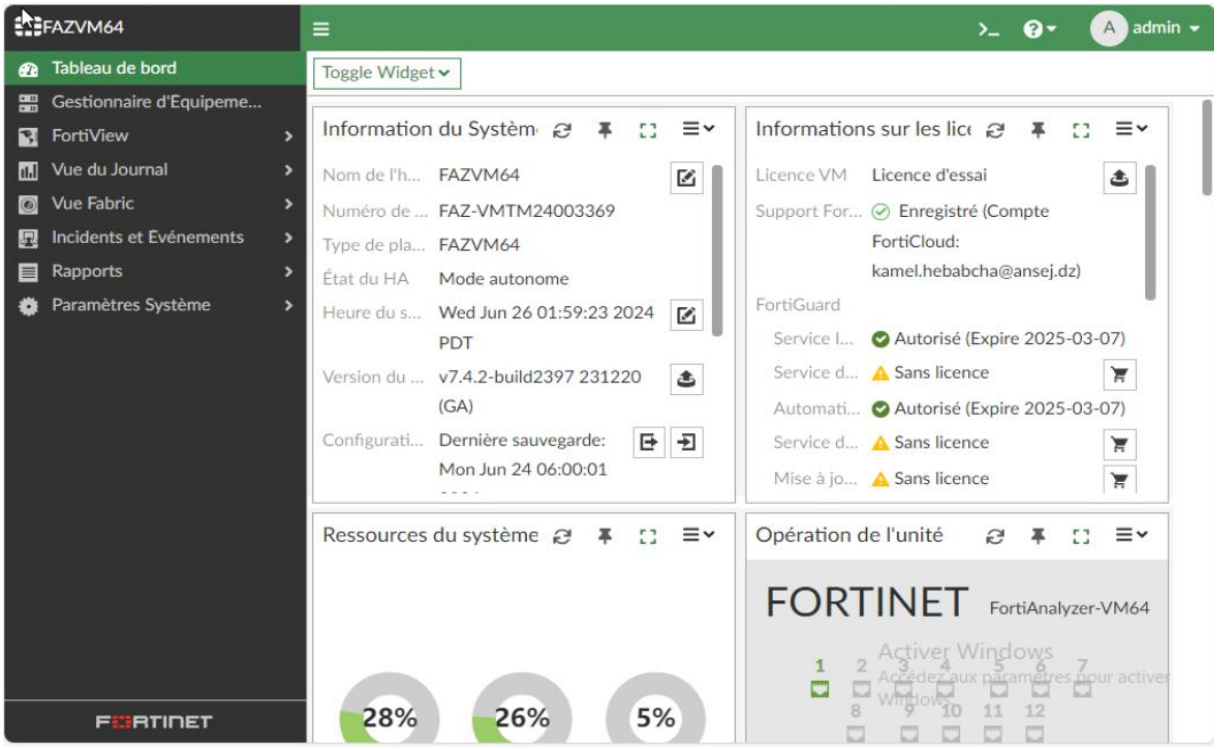
Connexion à l'interface graphique :

On ouvrira le navigateur web dans le client SSH et on tape https://10.10.0.20 ,nous entrons le nom de l'admin et son mot de passe, puis nous cliquons sur « **login** ».



FigureIII.23 : L'interface web de FortiAnalyzer

Nous cliquant sur « **Connexion** » pour accéder à l'interface graphique de notre FortiAnalyzer.



FigureIII.24 : L'interface graphique de FortiAnalyzer

III.3.3 Configuration de la topologie via VPN IPsec

Tout d'abord, nous allons configurer les deux fortigates via les assistants VPN IPsec, puis nous allons vérifier la connectivité réseau entre LAN1 et LAN2.

Sur le FG de la DG, nous accédons à « **VPN > IPsec Wizard** »et nous sélectionons sur **« Site à site** »– FortiGate

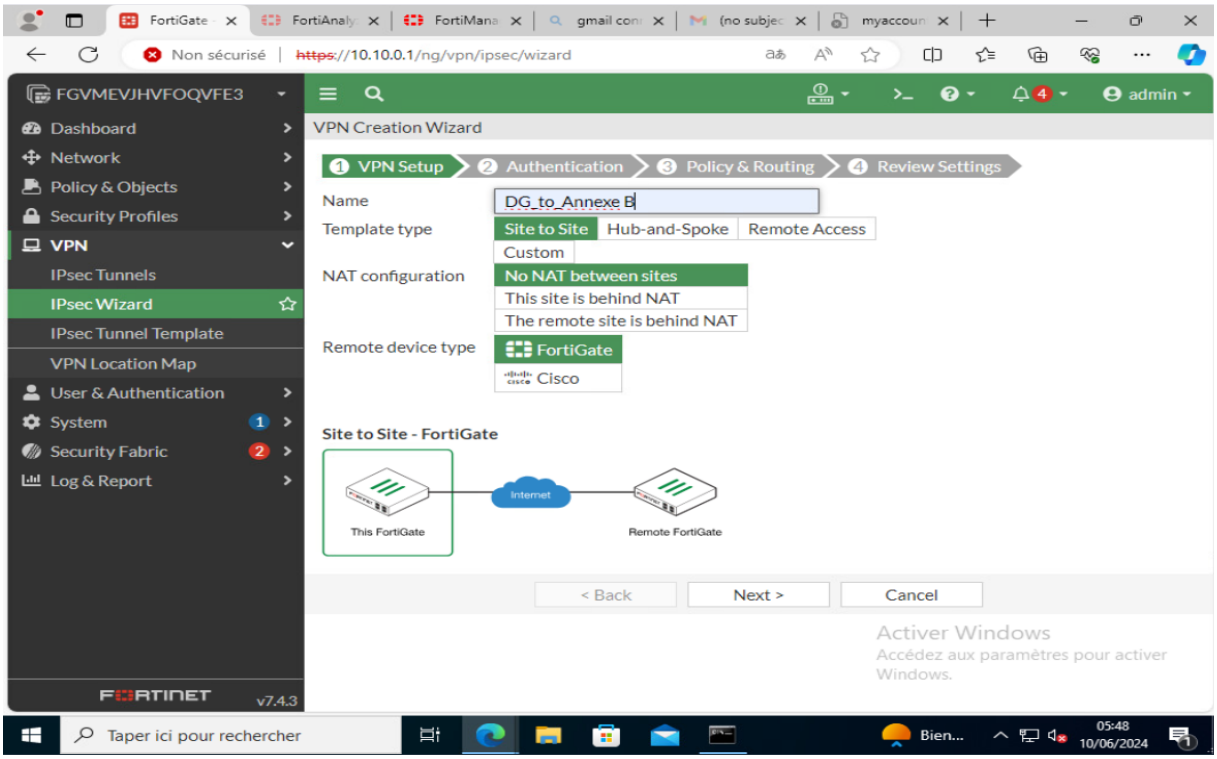


Figure III.25: Configuration de VPN

Sélectionnons « **Site to Site** » > « **No Nat** » > « **FortiGate** » **.** Entrons l'adresse IP distante : « **192.168.150.120/24** », interface sortante « **port**3 », et nous tapons une clé commune.

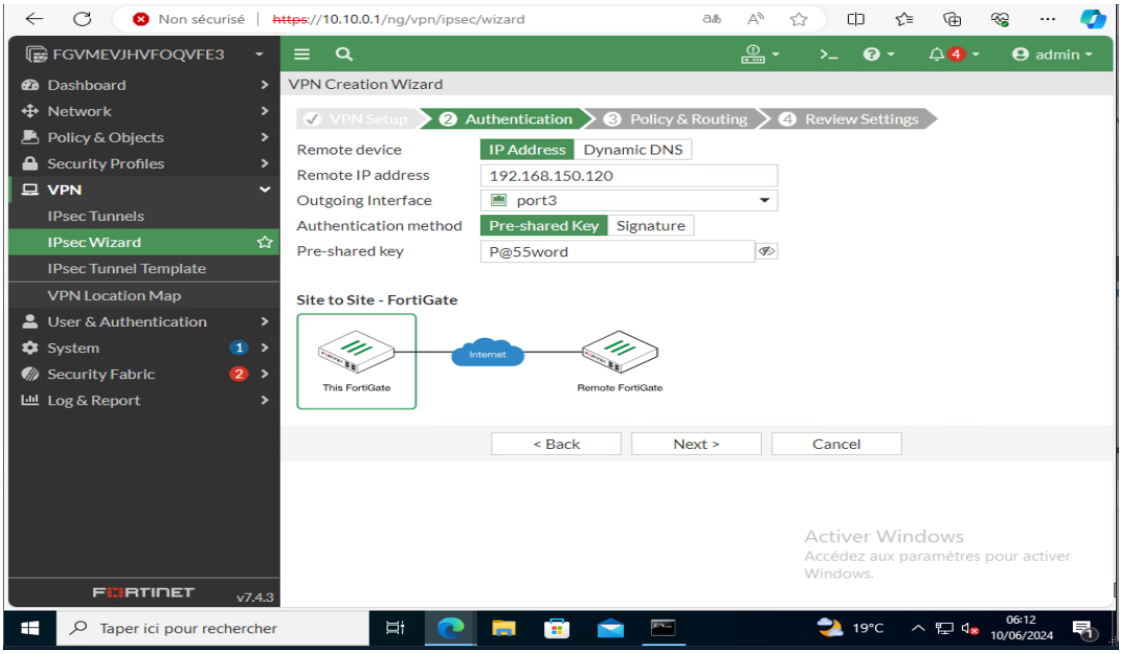


Figure III.26: Authentification de VPN pour l'interface de fortigate de la DG

Interface locale : port1, IP : **10.10.0.0/24**, sous-réseau distant : **10.10.2.0/24**. Cela crée deux politiques de sécurité et deux routes statiques dans les fortigate.

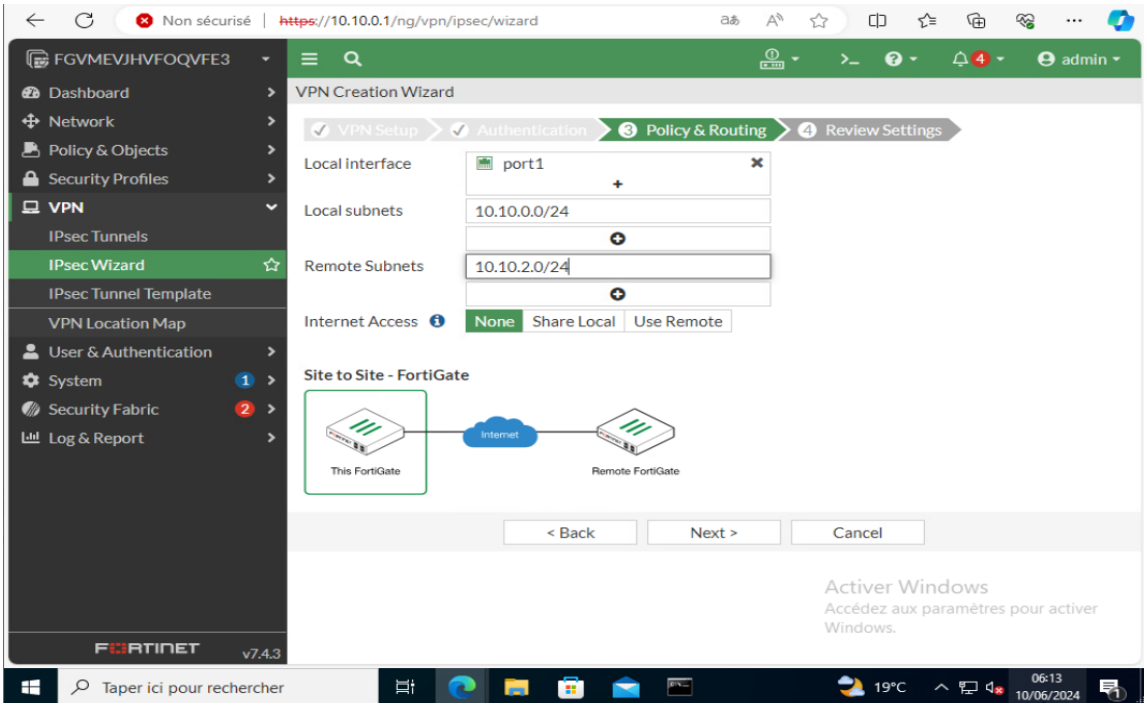


Figure III.27: Création automatique de politique de sécurité et de route statique

Sur le FG de l'annexe, nous accédons à « **VPN** » puis **« IPsec Wizard »** après nous sélectionnons « Site-to-Site « – FortiGate- No nat ».

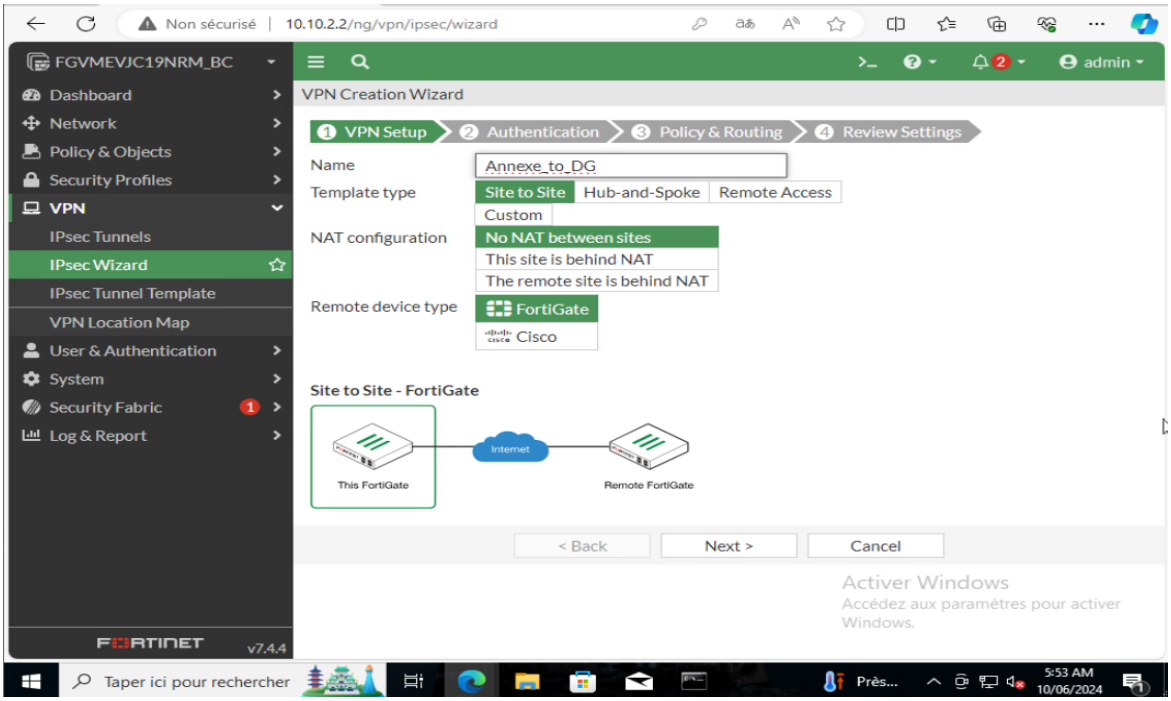


Figure III.28: Configurer FG de l'annexe de Boumerdes

Nous allons continuer la même configuration pour FG de notre annexe.

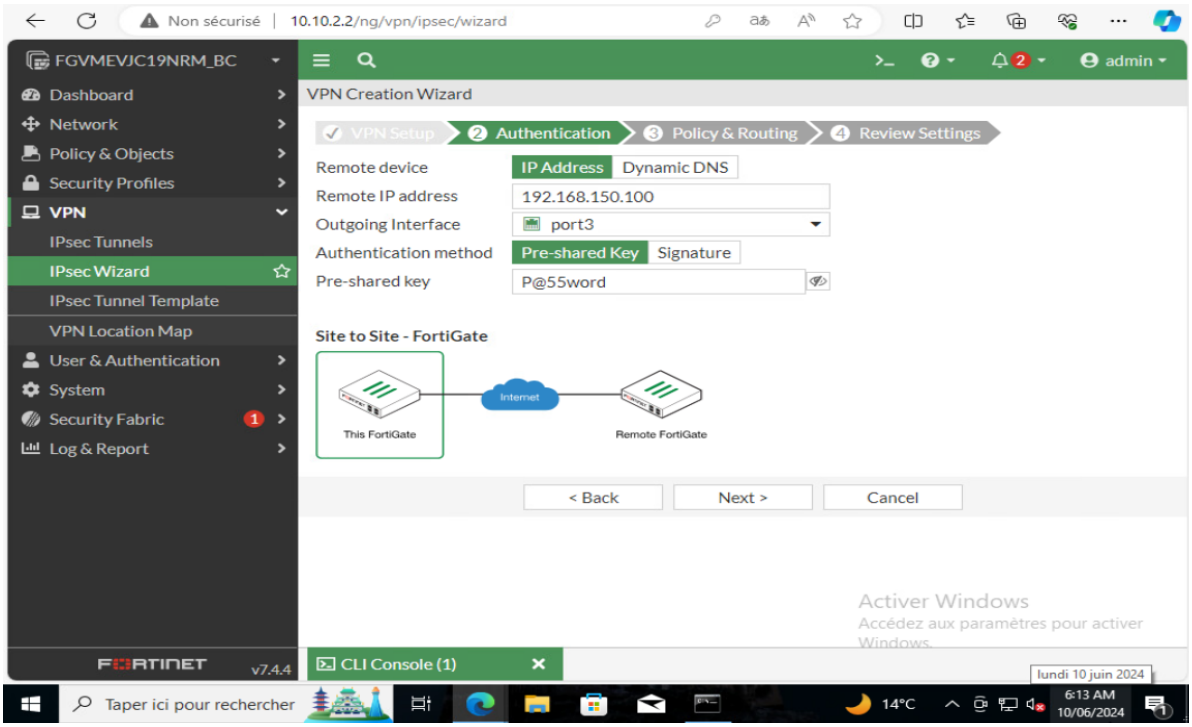


Figure III.29: Authentification VPN pour l'interface de FG de l'annexe

Quand on termine la configuration de FG de l'annexe, nous allons accéder dans IPsec tunnels et double-cliquons sur Inactif.Sur les fenêtres suivantes, faisons un clic droit sur le **tunnel** > **Bring UP** > **All Phase 2 selectors** . Ensuite, notre tunnel devrait être en place.

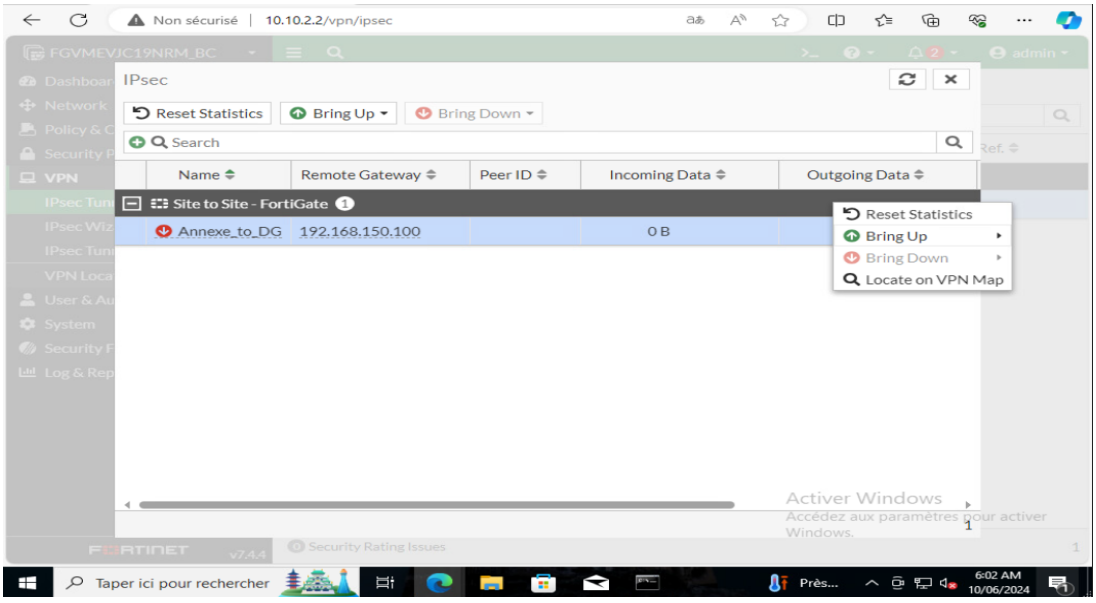


Figure III.30: Configuration des tunnels Ipsec(l'état : Down)

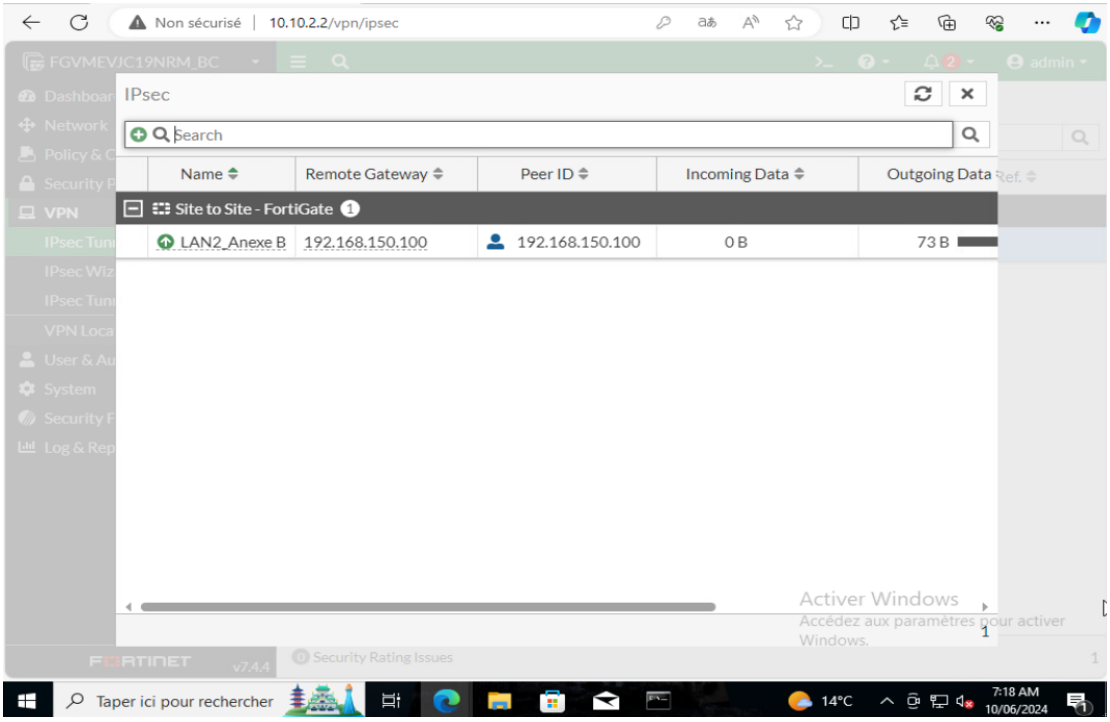


Figure III.31 : Vérification de l'état de tunnel (L'état : Up)

Et comme ça, nous avons établi la connectivité réseau entre LAN1 et LAN2 , nous pouvons confirmer cette connectivité utilisant le ping entre machines.

III.3.4 Integration des fortigates dans le fortimanager et fortianalyzer

III.3.4.1 Intégration de fortigate dans le fortimanager

Pour rétablir cette intégration il faut suivre ces étapes :

- **Vérification de la comptabilité entre les 2 OS**

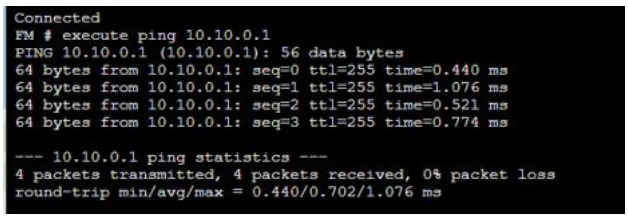
  Selon la documentation de fortinet les 2 OS sont compatibles (7.x .x).

- **Vérification de la connectivité réseau**

  Depuis le FortiGate au fortiManger

```
FGVMEVJHVFOQVFE3 # execute ping 10.10.0.10
PING 10.10.0.10 (10.10.0.10): 56 data bytes
64 bytes from 10.10.0.10: icmp_seq=0 ttl=64 time=0.6 ms
64 bytes from 10.10.0.10: icmp_seq=1 ttl=64 time=0.6 ms
64 bytes from 10.10.0.10: icmp_seq=2 ttl=64 time=0.6 ms
64 bytes from 10.10.0.10: icmp_seq=3 ttl=64 time=0.8 ms
64 bytes from 10.10.0.10: icmp_seq=4 ttl=64 time=0.6 ms

--- 10.10.0.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.6/0.6/0.8 ms
```

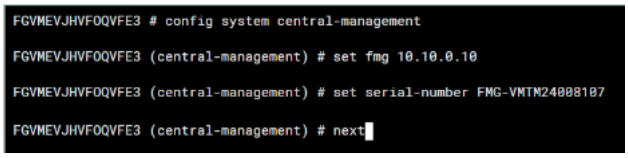
Depuis le FortiManager au FortiGate



- **Vérification de l'accès FMG sur FortiGate**

Nous assurons que l'interface réseau (port1) de notre fortigate permet l'accès de fortimanager

- **Forcer l'ajout du numéro de série du FortiManager dans la gestion centrale de l'unité via un script batch sur le FortiGate**



Nous pouvons réaliser cette étape à partir de l'interface graphique de fortigate :

- Nous accédons à « **Security Fabric** » puis « **Fabric Connectors** » et double-clique sur la carte « **FortiManager** ». Pour « **Statut** », cliquons sur **« Activer (Enabled)** ».
- Pour **« Type »,** nous cliquons sur « **Sur site (On-Premises)** » .
- Nous entrons l'adresse IP/le nom de domaine du FortiManager.
- Nous Cliquons sur « **OK** ».

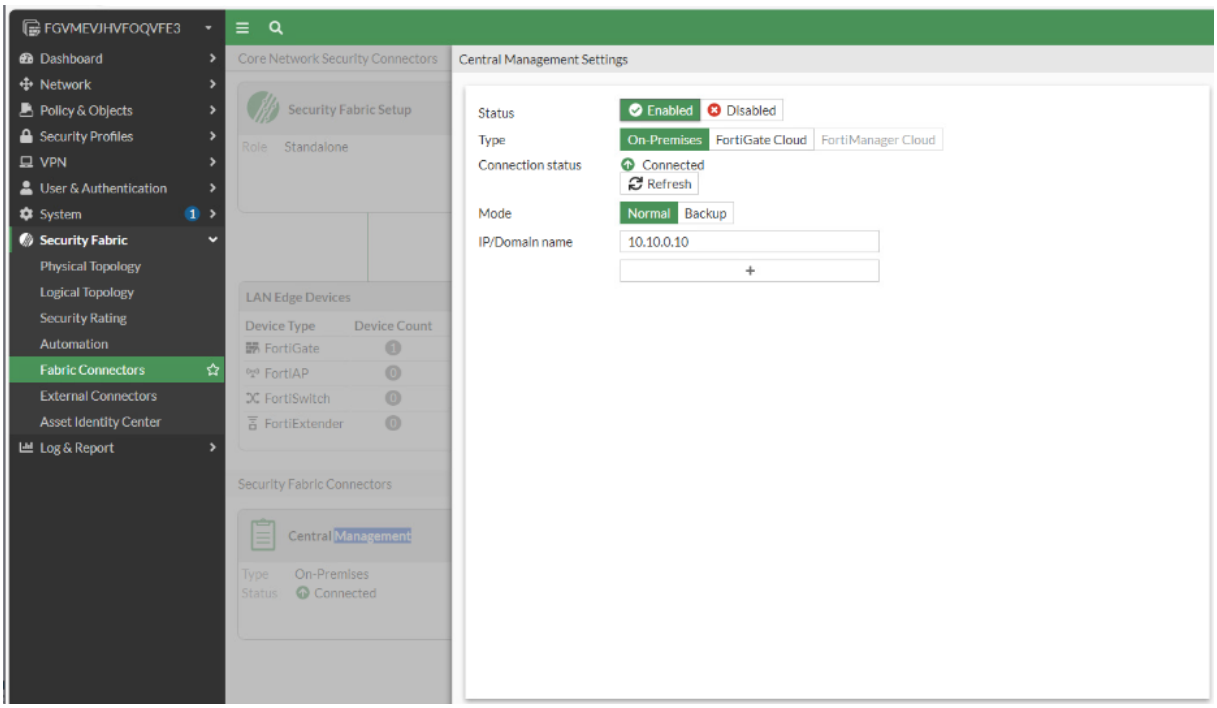


Figure III.32: Ajout de numéro de série de fortimanage au fortiagte

- Sur le FortiManager, nous accédons au « **Gestionnaire de périphériques** » et recherchons le FortiGate dans « **la liste des périphériques** » non autorisés.
- Sélectionnons-le ou les appareils FortiGate, puis nous cliquons sur « **Autoriser** » dans la barre d'outils.

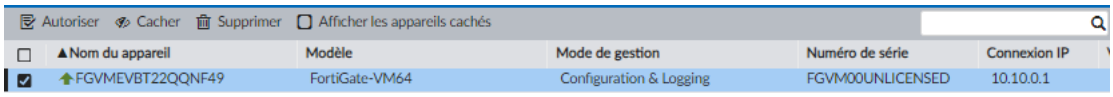


Figure III.33: Le fortigate avant l'autorisation

- Dans la fenêtre contextuelle « **Autoriser** » le périphérique, nous ajustons le nom *de* l'appareil, puis nous cliquons sur « **OK** ».

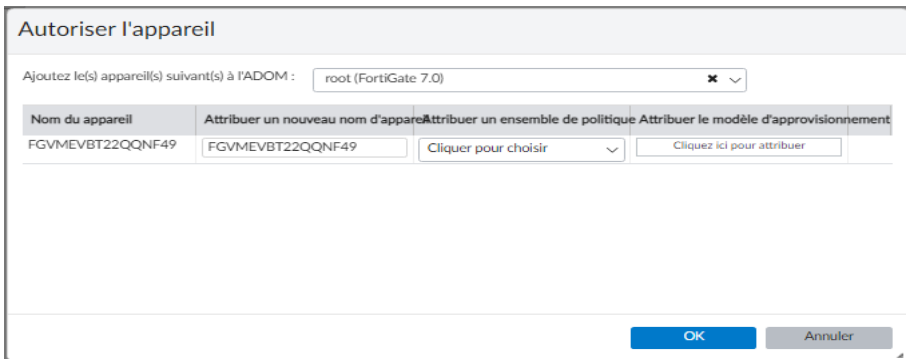


Figure III.34 : L'autorisation de fortigate dans le fortimanager

- Nous pouvons maintenant accéder à l'interface graphique de fortigate à travers le fortimanager.

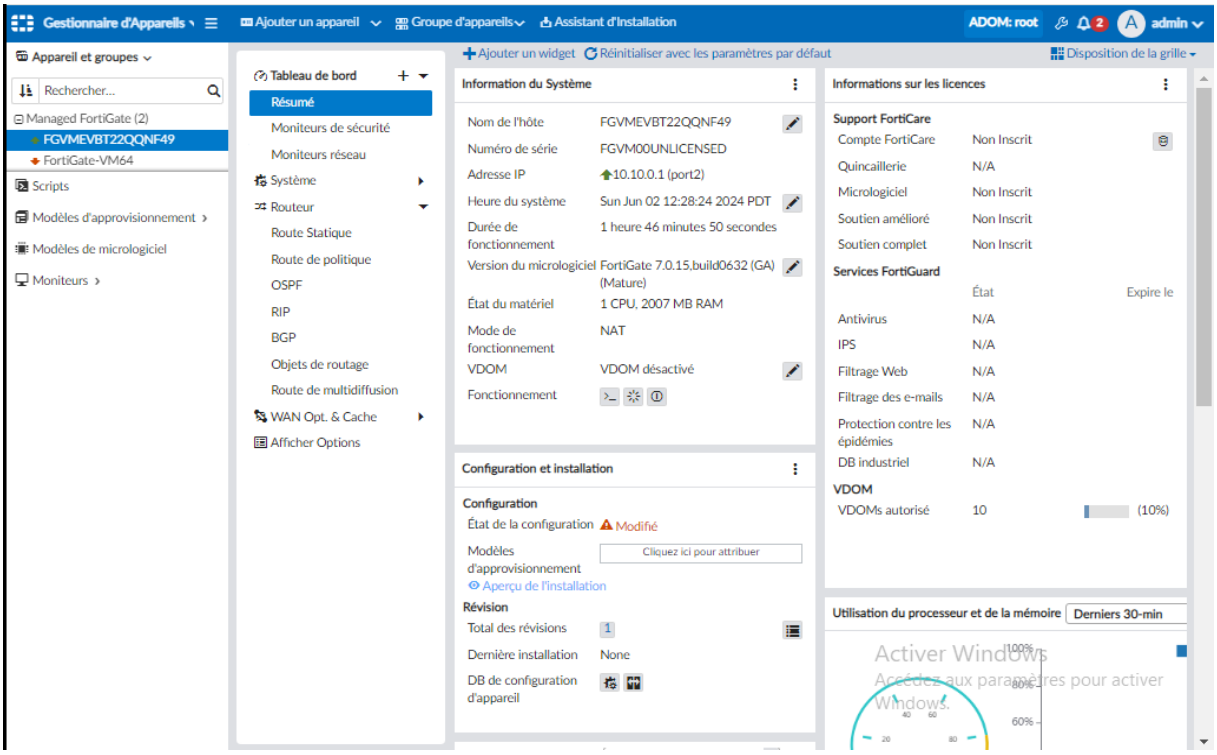


Figure III.35 : L'interface graphique de FortiGate depuis le FortiManager

NB : Nous repassons par les mêmes étapes que le premier fortigate pour l'integration de deuxième fortigate dans le fortmanager.

III.3.4.2 Intégration de fortigate dans le fortianalyzer

Dans notre cas, nous avons décidé d'ajouter le fortigate au fortianalyzer utilisant l'interface graphique (GUI) et la ligne des commandes (CLI) en même temps suivant ces étapes :

- **Vérification de la comptabilité entre les 2 OS : Selon la documentation de fortinet les 2 OS sont compatibles.**
- **Vérification de la connectivité réseau :**

  Depuis le fortigate au fortianalyzer

```
FGVMEVJHVFOQVFE3 # execute ping 10.10.0.20
PING 10.10.0.20 (10.10.0.20): 56 data bytes
64 bytes from 10.10.0.20: icmp_seq=0 ttl=64 time=0.5 ms
64 bytes from 10.10.0.20: icmp_seq=1 ttl=64 time=0.4 ms
64 bytes from 10.10.0.20: icmp_seq=2 ttl=64 time=0.7 ms
64 bytes from 10.10.0.20: icmp_seq=3 ttl=64 time=0.5 ms
64 bytes from 10.10.0.20: icmp_seq=4 ttl=64 time=0.7 ms

--- 10.10.0.20 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.7 ms
```

Depuis le fortianalyzer au fortigate

```
Connected
FA_VM # execute ping 10.10.0.1
PING 10.10.0.1 (10.10.0.1): 56 data bytes
64 bytes from 10.10.0.1: seq=0 ttl=255 time=2.228 ms
64 bytes from 10.10.0.1: seq=1 ttl=255 time=0.649 ms
64 bytes from 10.10.0.1: seq=2 ttl=255 time=0.435 ms
64 bytes from 10.10.0.1: seq=3 ttl=255 time=0.481 ms

--- 10.10.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.435/0.948/2.228 ms
```

- **Forcer l'ajout du numéro de série du FortiAnalyzer dans la gestion centrale de l'unité via un script batch sur le FortiGate :**

```
FGVMEVJHVFOQVFE3 # config  log  fortianalyzer setting

FGVMEVJHVFOQVFE3 (setting) # set status enable

FGVMEVJHVFOQVFE3 (setting) # set upload-option  realtime

FGVMEVJHVFOQVFE3 (setting) # set serial FAZ-VMTM24003369

FGVMEVJHVFOQVFE3 (setting) # set source-ip 10.10.0.20
```

-La commande « **config log fortianalyzer setting** » permet de configurer les paramètres de fortigate pour qu'il puisse envoyer les logs au Fortianalyzer.

-La commande « **set status enable** » active l'envoi des logs vers le Fortianalyzer.

-La commande « **set server 10.10.0.20** » spécifie l'adress IP du Fortianalyzer , ce qui permet au fortigate de lui envoyer ses logs.

-La commande « **set upload-option realtime** » signifie que les logs sont transmis immédiatement au fortianalyzer , ce qui lui permet de recevoir et d'analyser les événements en temps quasi réel. Ceci est essentiel pour détecter et répondre rapidement aux incidents de sécurité.

-La commande « **set source-ip** » spécifie l'adresse ip source d'où les logs seront prévenus.

-La commande « **set serial FAZ-VMTM24003369** » signifie le numéro de série de fortianalyzer, ce qui s'assure l'envoie des logs au bon fortianalyzer.

-Nous jeton un coup d'œil sur « **Fabric Connectors** » ,nous allons trouvé que le nombre de série de notre fortianalyzer est ajouté.

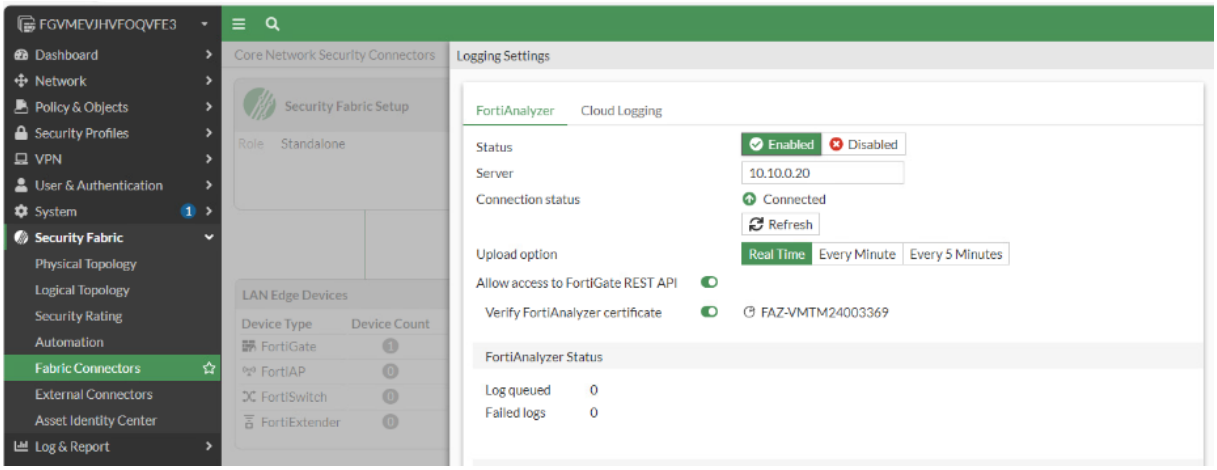
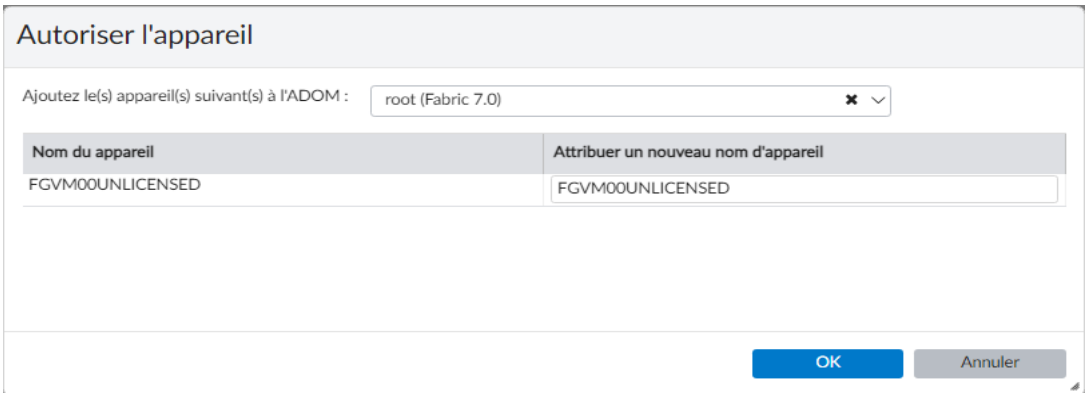


Figure III.36 : Ajout de numéro de série de fortianalyzer dans le fortigate

- Sur le Fortianalyzer, nous accédons au Gestionnaire de périphériques et nous allons trouver notre FortiGate dans la liste des périphériques non autorisés.
- Sélectionnons-le puis nous faisons un clic droit, puis nous cliquons sur Autoriser dans la barre d'outils.

Figure III.37 : Le fortigate avant l'autorisation

- Dans la fenêtre contextuelle Autoriser le périphérique, nous ajustons le nom *de* l'appareil, puis nous cliquons sur « **OK** ».



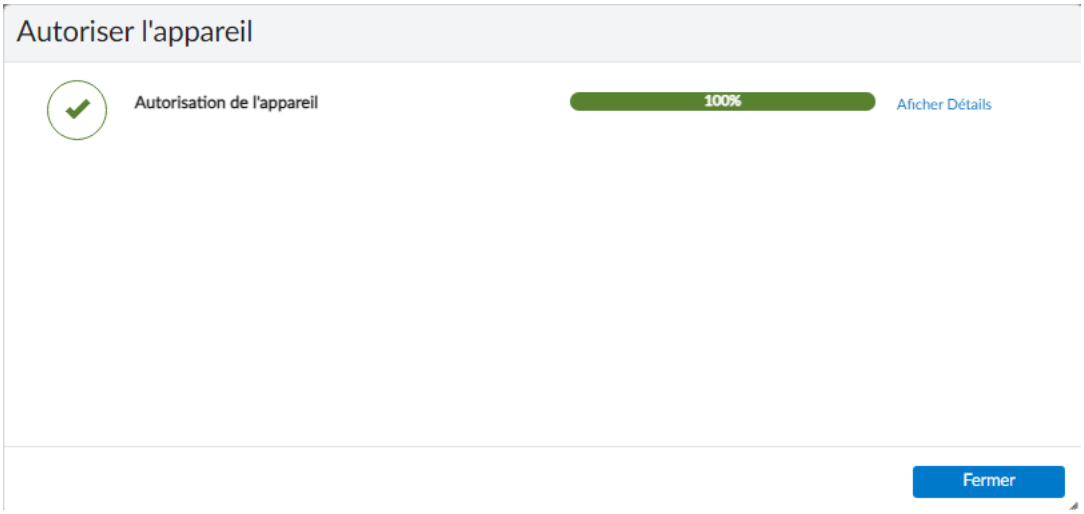


Figure III.38: Autorisation de fortigate dans le fortianalyzer

- Nous allons confirmer que notre fortigate est bien intégré dans le fortianalyzer

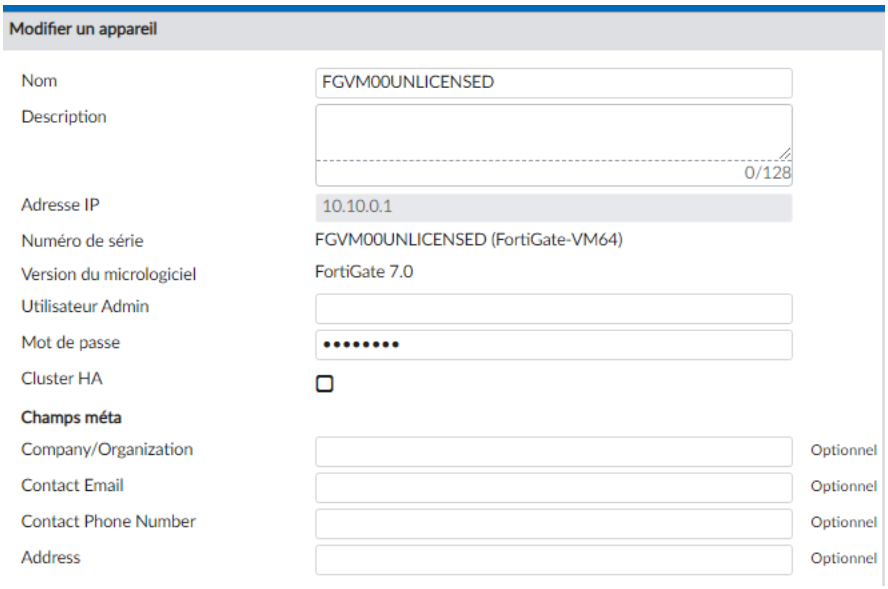


Figure III.49 : Confirmation d'intégration de fortigate dans le fortianalyzer

- Nous pouvons également suivre le taux de fonctionnement de notre appareil durant la journée de travail à l'aide de la courbe graphique ci-dessous.

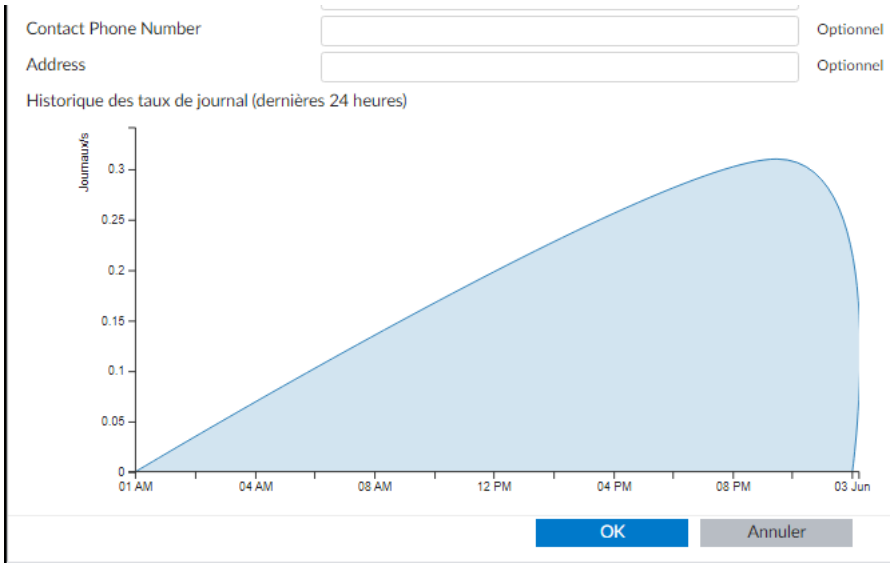


Figure III.40: Courbe graphique montrant le taux de fonctionnement de fortigate

NB : Nous repassons par les mêmes étapes que le premier fortigate pour l'intégration de deuxième fortigate dans le fortianalyzer.

Après avoir terminé ces opérations, nous pourrons maintenant accéder à n'importe lequel des fortigates via le fortimanager et le fortianalyzer

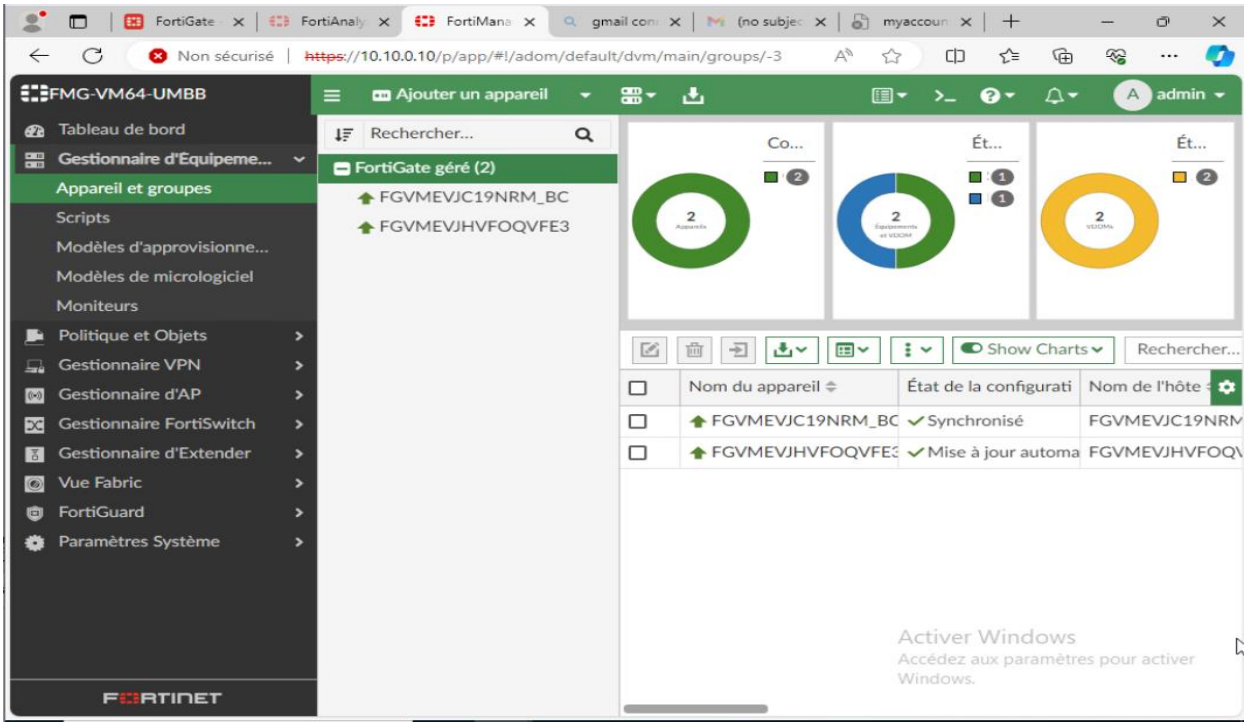


Figure III.41 : les deux fortigates sont integrés dans le fortimanager

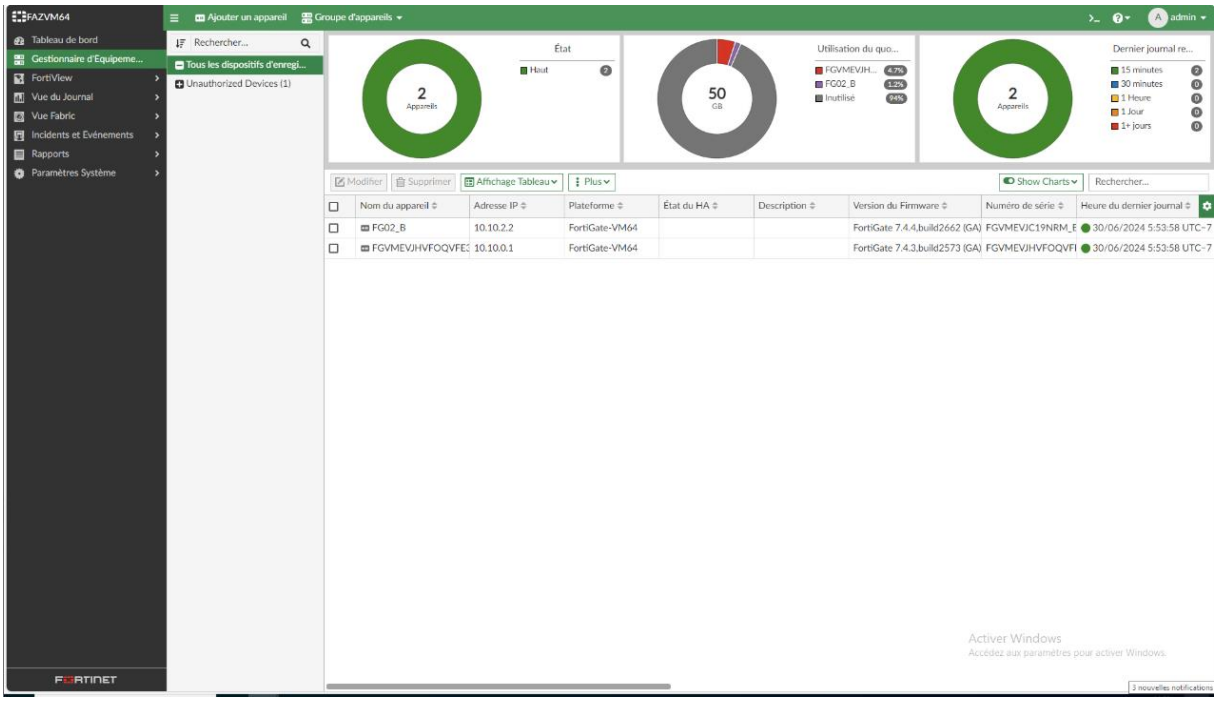


Figure III.42 : Les deux FortiGates sont intégrés dans le fortianalyzer

Nous pouvons surveiller et visualiser l'emplacement de ces dispositifs et leur état combiné dans les couleurs vert et rouge sur la Vue cartographique « Map View » dans la barre d'outils. En précisant l'emplacement de chaque FortiaGate.

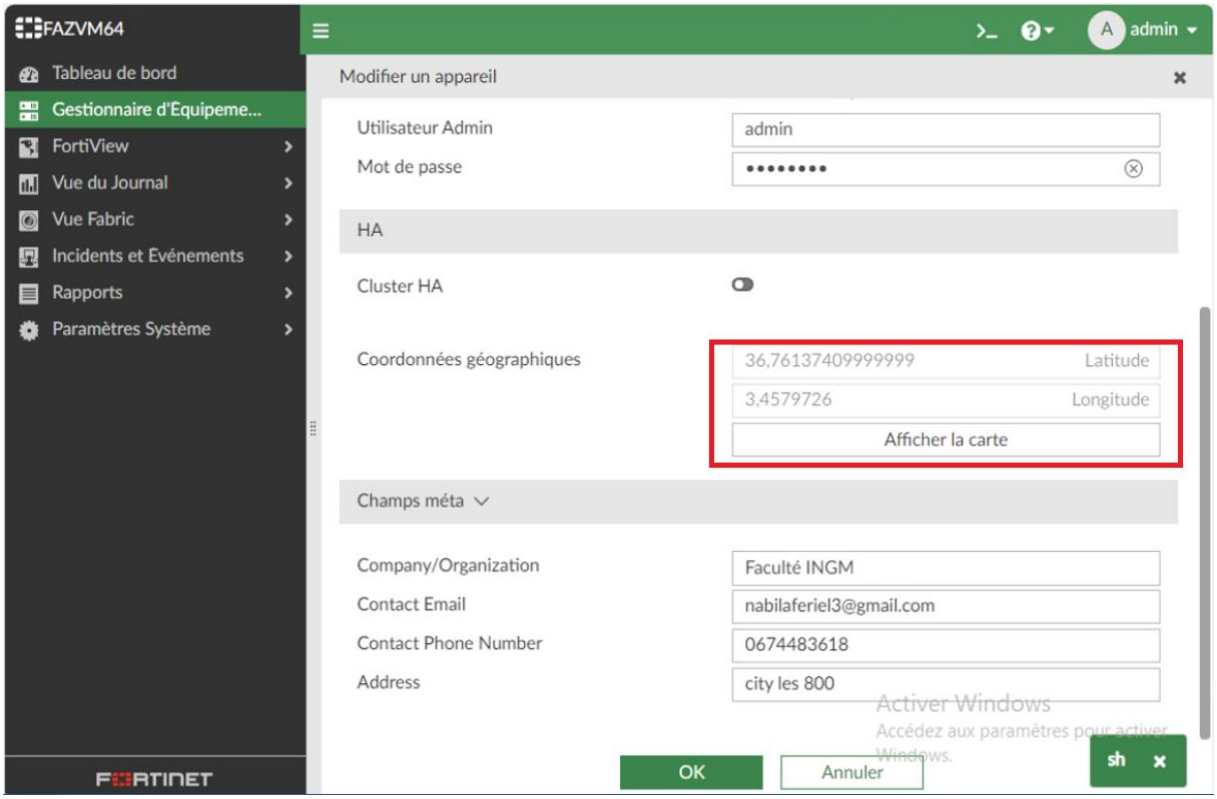


Figure III.43: Cordonnées géographique de fortigate de l'annexe de Boumerdes

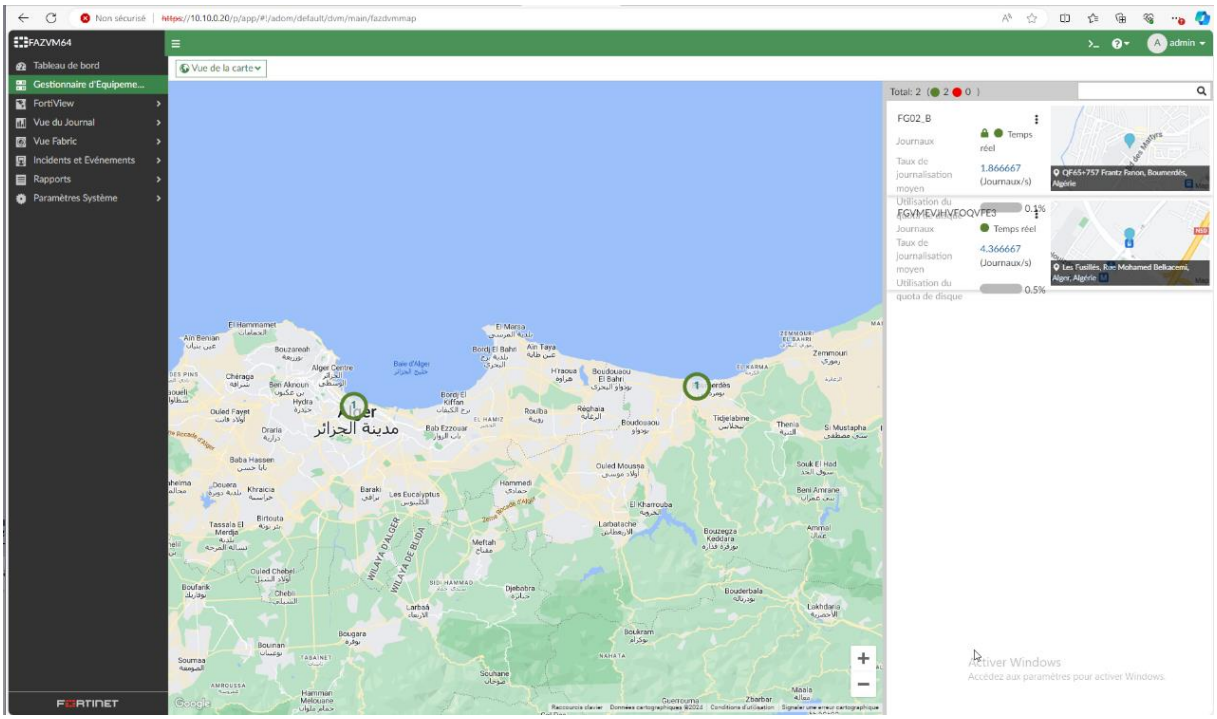


Figure III.44: l'emplacement et le bon état des FortiGates gérés sur Google Maps

- La clé des couleurs :
  Vert : Indique que les appareils sont en bon état.
  Rouge : Indique un état d'erreur.

III.4 Teste et simulation :

III.4.1 Exécution de code CLI :

L'exécution du code de l'interface de ligne de commande (CLI) sur FortiManager et son déploiement sur FortiGate est une méthode courante pour gérer et configurer de manière centralisée les appareils FortiGate. Pour déployé le code de la règle d'alerte « changement de configuration au niveau d'un fortigate » , nous allons suivre ces étapes

-Nous accédons à l'interface web de FortiManager (https://10.10.0.10) en utilisant les identifiants d'administrateur.

-Dans le tableau de bord de FortiManager, naviguons vers **Policy & Objects > Scripts.**

-Vous pouvez créer un nouveau script ou éditer un script existant. Pour créer un nouveau script, cliquez sur **Create New.**

-Nous allons donner un nom au script et sélectionnez le type de script **(CLI Script).**

-Dans l'éditeur de script, nous saisissons les commandes CLI que nous souhaitons exécuter sur le FortiGate.

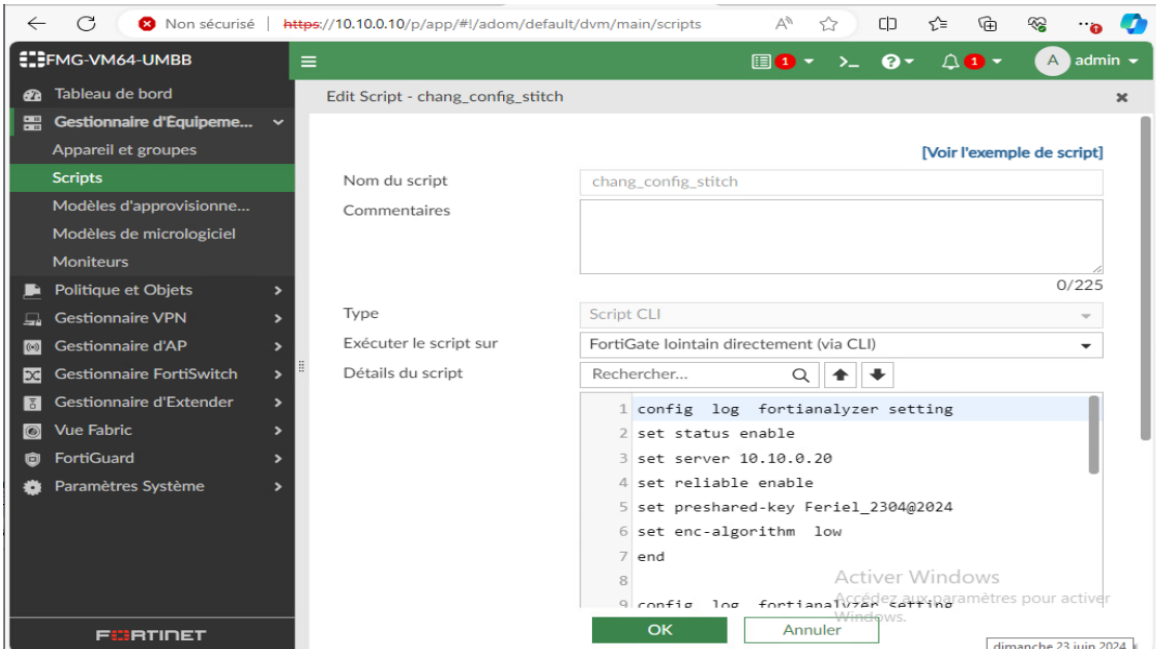


Figure III.45 : Une capture d'écran montre l'exécution de code de la règle d'alerte

-Nous enregistrons le script une fois la rédaction terminée, puis nous sélectionnons les dispositifs FortiGate sur lesquels nous souhaitons déployer le script.

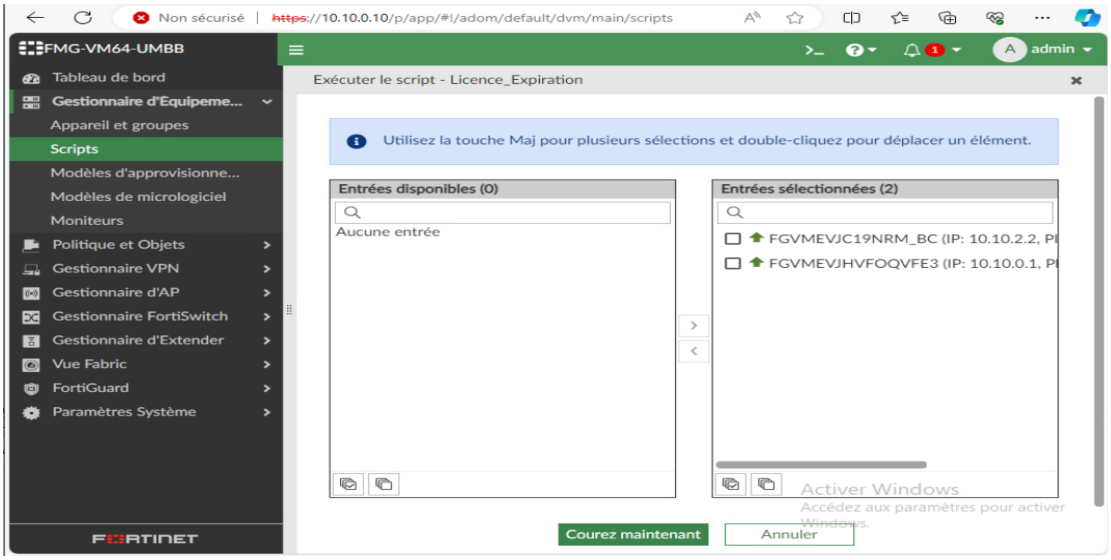


Figure III.46 : Les dispositifs fortigates sélectionnés

-Cliquons sur **Courez maintenant** pour exécuter le script sur les dispositifs sélectionnés.

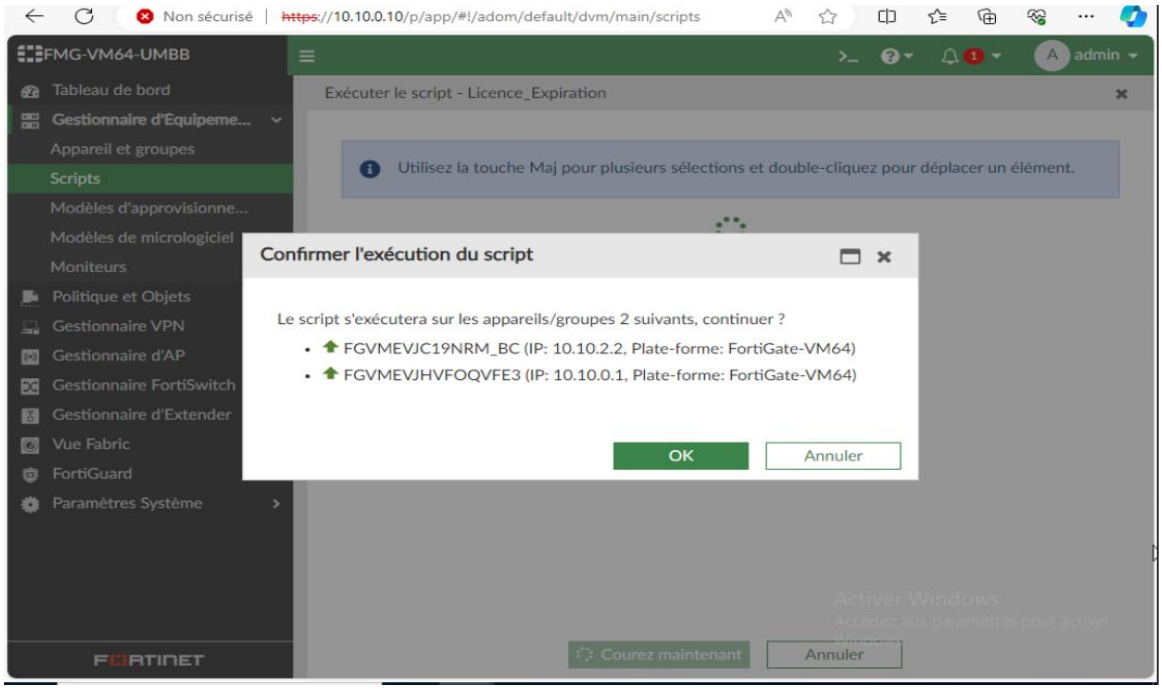


Figure III.47: Confirmation de l'exécution de script

-FortiManager enverra les commandes au FortiGates sélectionnés.

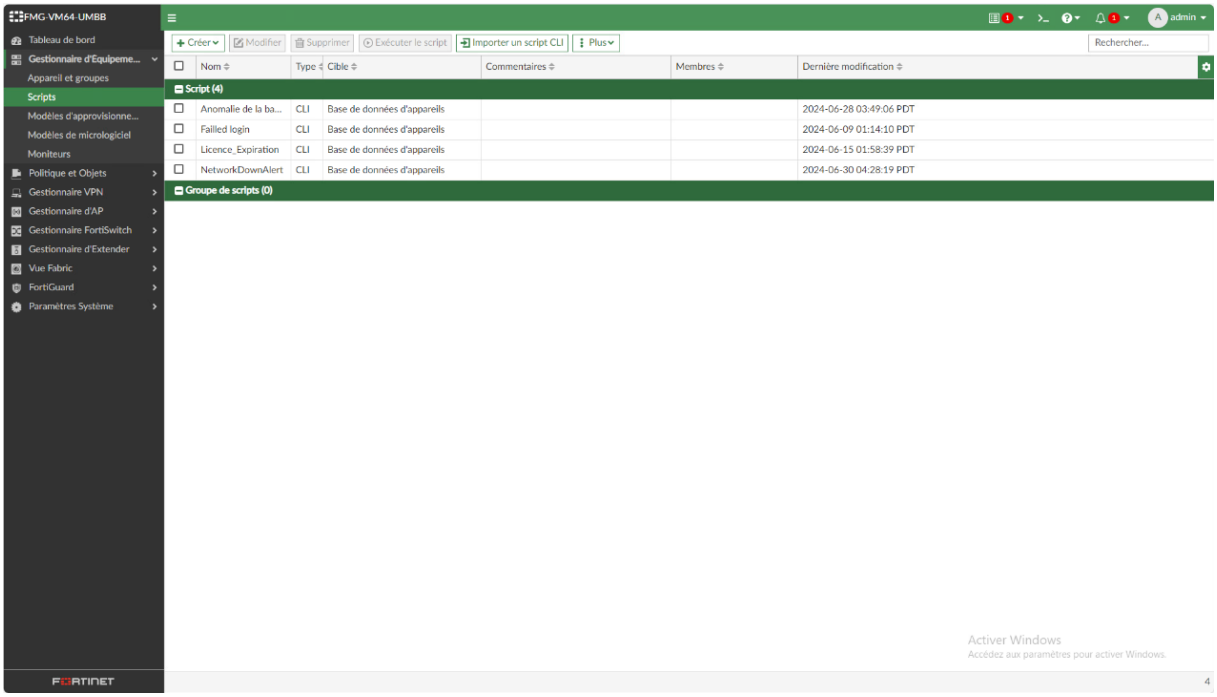


Figure III.48 : Les règles d'alerte exécutées au niveau de FortiManager

-Nous pouvons prévisualiser le script pour nous assurer qu'il est correct avant de le déployé. Nous sélectionnons sur le nom de CLI que nous voulons tester puis en sélectionne sur « **Exécuter le script ».**

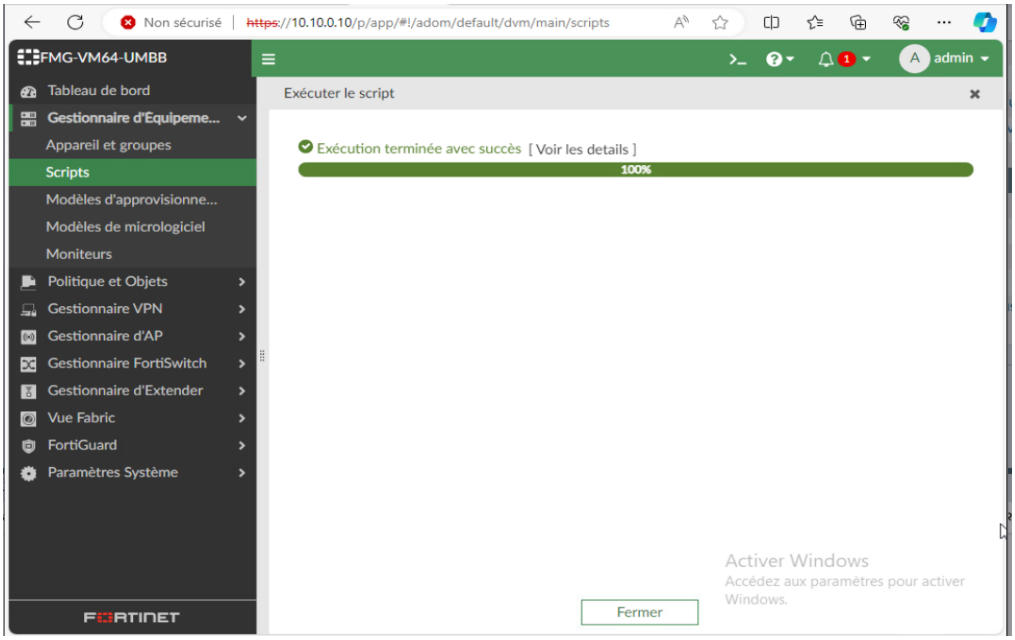


Figure III.49 : exécution avec succès de script

-Une fois le script exécuté, nous pouvons vérifier les modifications apportées sur les FortiGates via l'interface web.

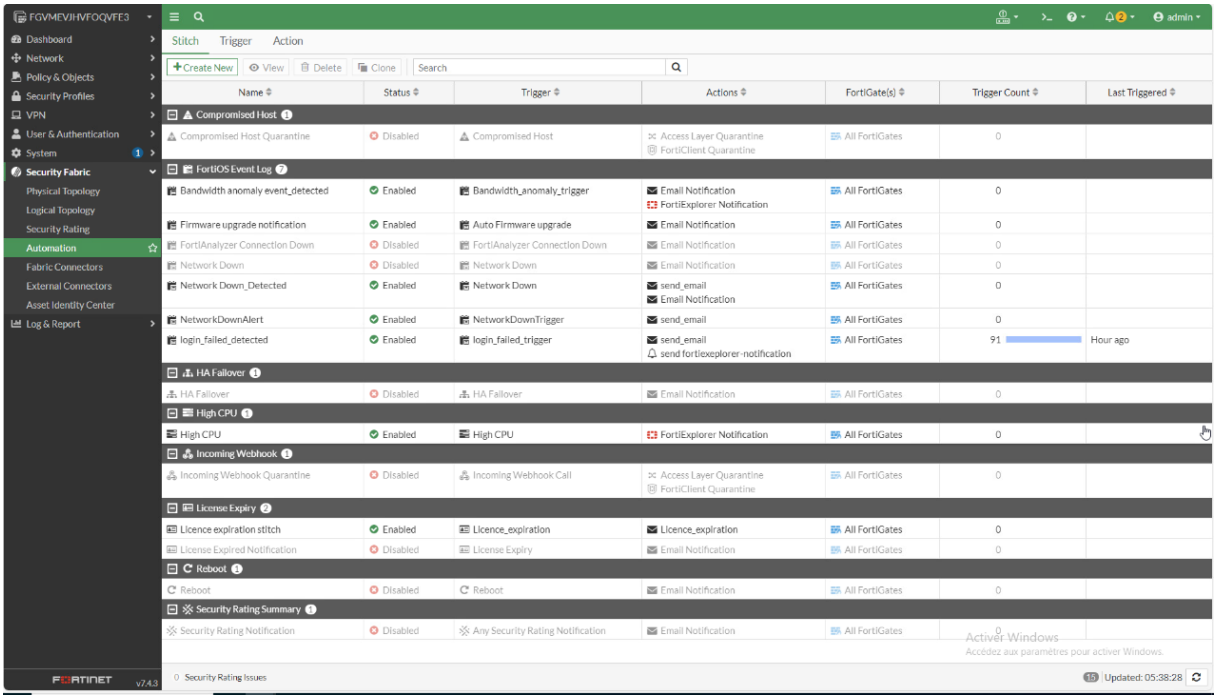


Figure III.50 : Modifications apporté au fortigate de la DG après l'exécution de CLI

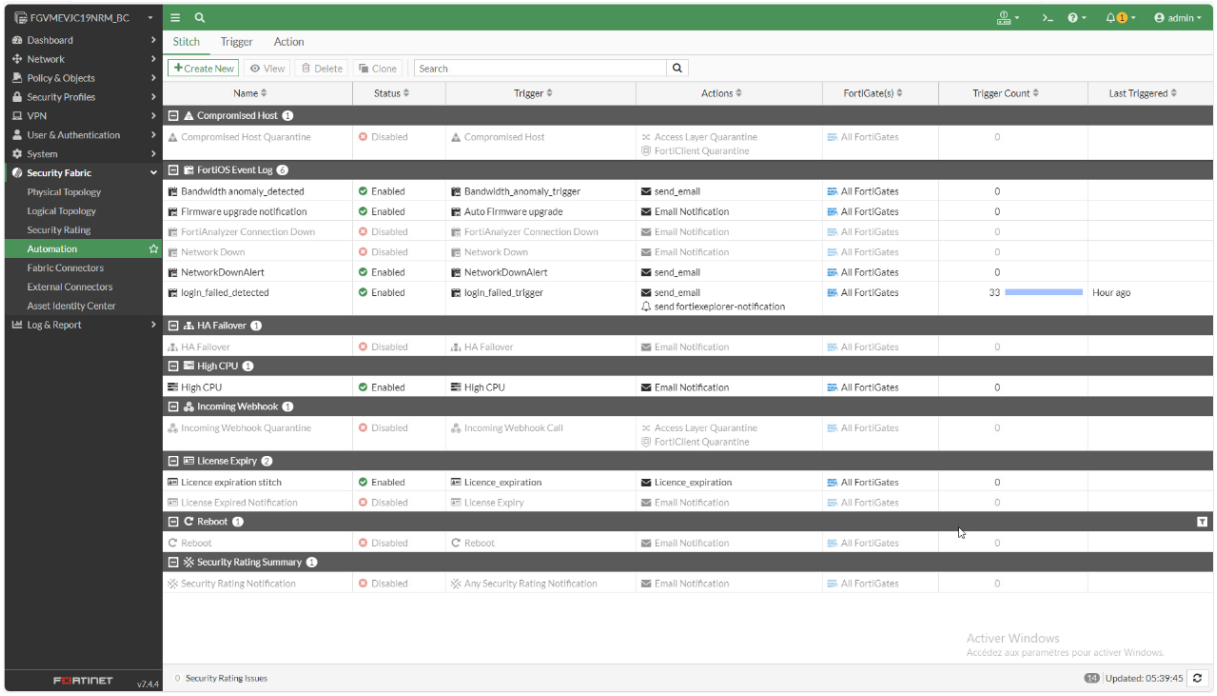
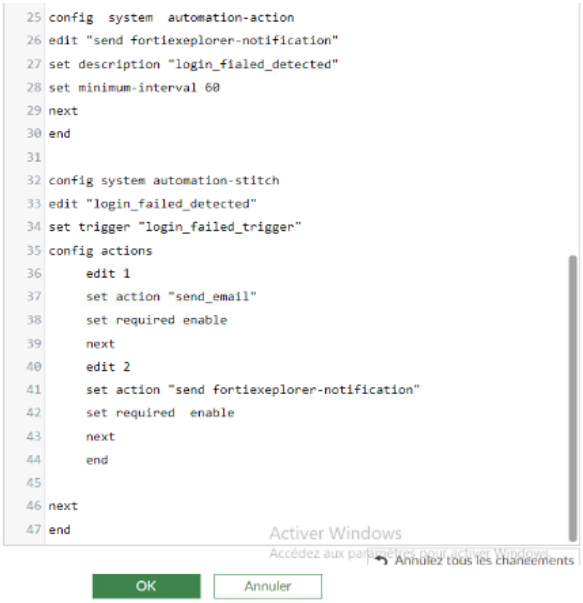


Figure III.51 : Modifications apporté au fortigate de la DG après l'exécution de CLI

Les codes CLI exécutées pour chaque règle d'alerte :

- **Code CLI de l'alerte « Tentative d'accès (failed login) » :**

```
config  log  fortianalyzer setting
set status enable
set server 10.10.0.20
set reliable  enable
set preshared-key "Feriel_2304@2024"
set enc-algorithm  low
end

config  system  automation-trigger
edit "login_failed_trigger"
set event-type event-log
set logid 32102
next
end

config  system automation-action
edit "send_email"
set action-type email
set email-to "ninouhnabila@gmail.com"
set email-subject "failed login"
set message "login failed detected"
next
end
```



Log event reçu au niveau de FortiAnalyzer : après avoir essayé d'entrer un nom d'utilisateur et un mot de passe erronés, la règle d'alerte au niveau de FortiGate de la direction général a déclenché et nous avons reçu un log d'après ce dernier au niveau de FortiAnalyzer comme le montre la figure précédente.Comme solutions ,l'administrateur réseaux peut désactiver temporairement ou bloquer le compte utilisateur correspondant à l'ID pour éviter d'autres tentatives d'accès et vérifie les logs pour toute activité anormale ou des tentatives d'accès supplémentaires liées à cet ID et à cette heure spécifique.

N.B : Malheureusement, nous ne pouvons pas recevoir de notifications par email car nous utilisons des licences d'essai.

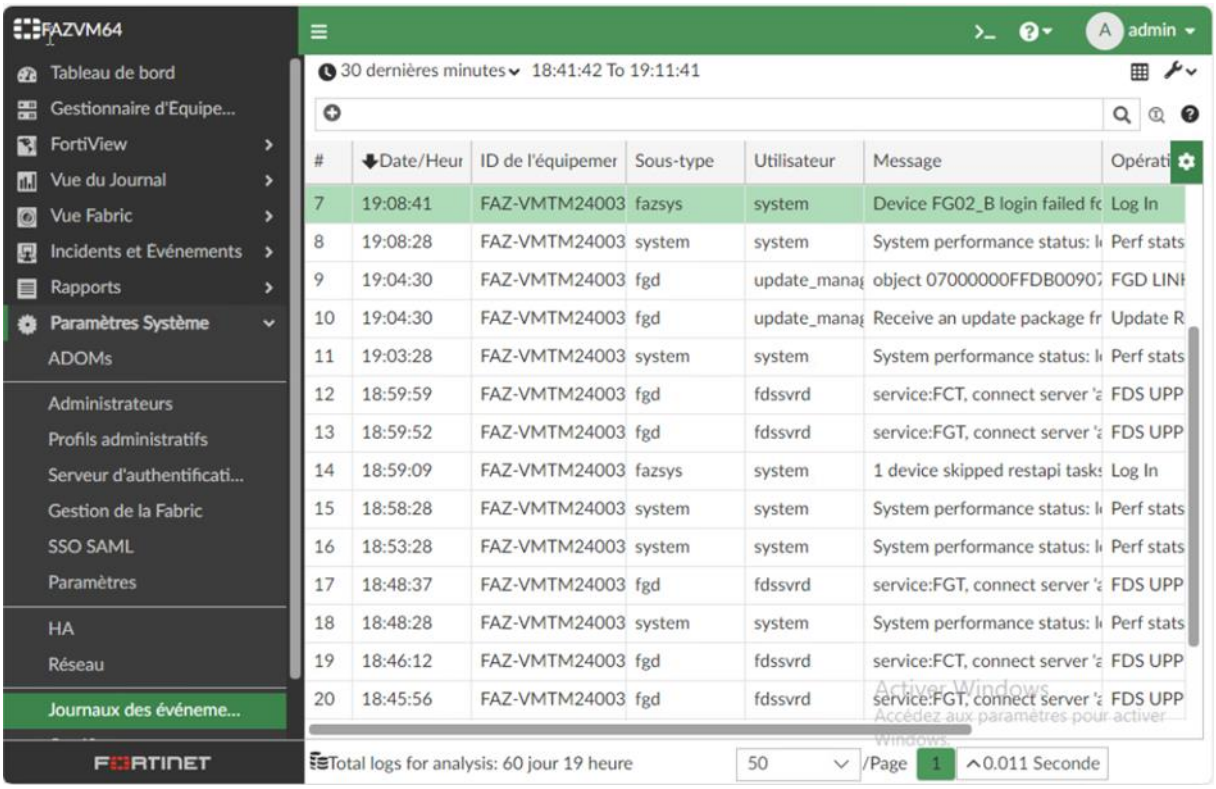


Figure III.52: Log event reçu par le fortigate de l'annexe de Boumerdes après le teste d'alerte

Pour une analyse approfondie de l'événement log recu ,nous pouvons télécharger le journal :

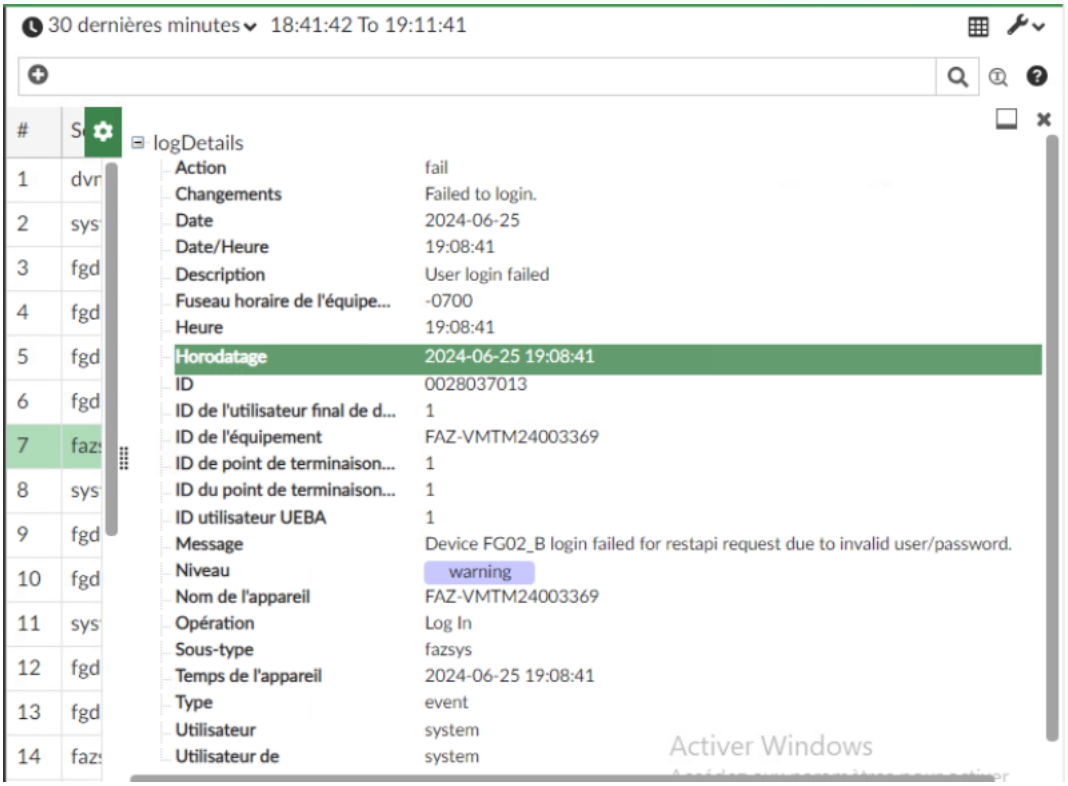
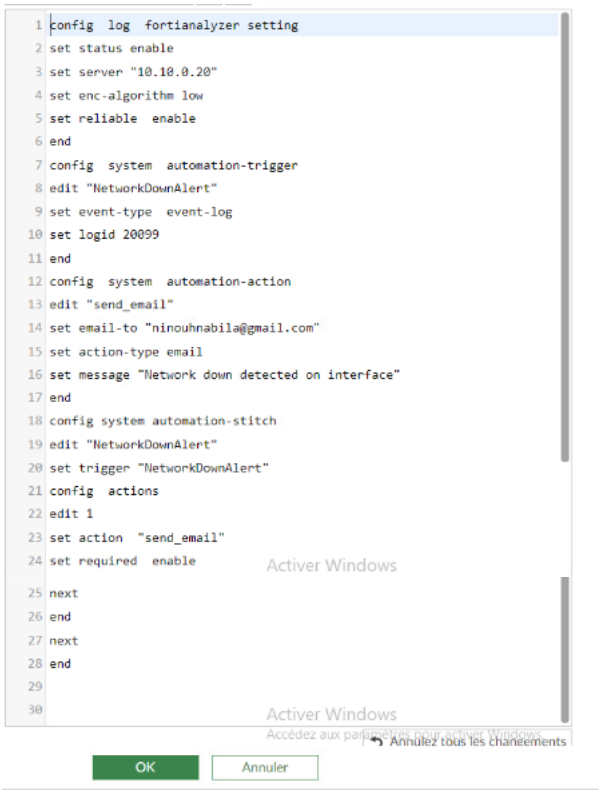


Figure III.53 : Log event reçu par le fortigate de l'annexe de Boumerdes après le teste d'alerte

- **Code CLI de l'alerte « Panne de réseau» :**



Log event reçu au niveau de FortiAnalyzer : Nous allons désactivé la deuxième interface de fortigate de l'annexe de Boumerdes .Dans ce cas, la direction générale a perdu l'accès avec l'annexe , l'appareil FG02_B envoie des rapports(log) de statut aux systèmes de gestion et d'analyse . Comme FortiManager est principalement utilisé pour la gestion et la configuration centralisée, il reçoit et enregistre immédiatement l'état de l'interface.Parcontre le FA ne reçoit pas immédiatement le log indiquant que le périphérique est "offline" (hors ligne) parce qu'il ne peut plus communiquer avec l'interface désactivée. Cette situation peut entraîner un délai ou une absence de certains logs jusqu'à ce que la communication soit rétablie.

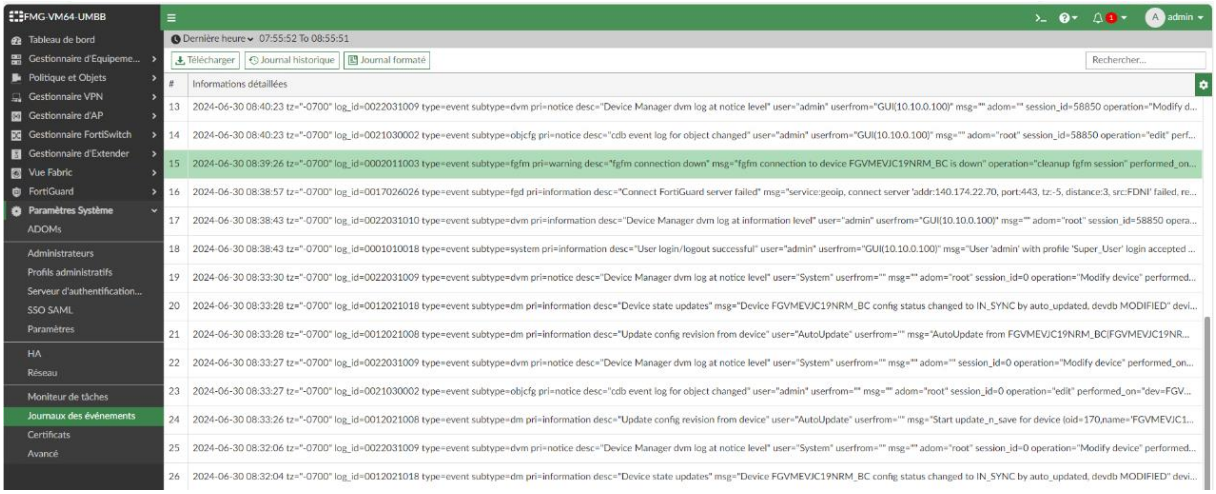


Figure III.54: Log reçu sur le fortimanager après la désactivation de la deuxième interface de fortigate de l'annexe de Boumerdes

Pour activer l'interface, nous allons accéder au FortiGate depuis le Fortimanger et nous réactivons l'interface désactivée.

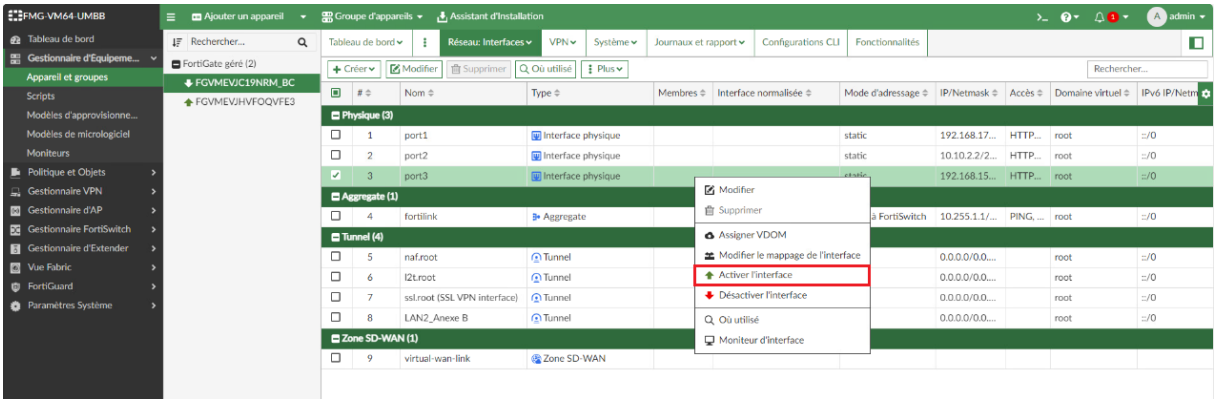


Figure III.55 : Réactivation de l'interface désactivée

Lorsque l'interface est réactivée, le FG envoie des logs indiquant que le périphérique est de nouveau "online" (en ligne).Le FA reçoit alors un log indiquant que l'appareil est de nouveau en ligne(2), ainsi qu'un log contenant les informations complètes sur la période pendant laquelle l'interface était désactivée (1).

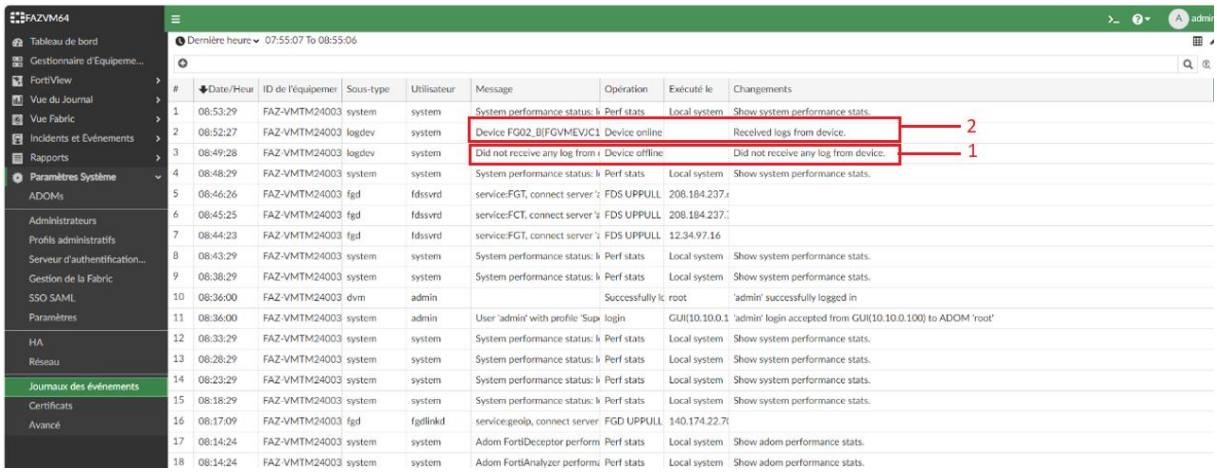


Figure III.56 : Logs reçus d'après le FG au FA après la réactivation de l'interface bloqué

Log event reçu au niveau de FortiAnalyzer : Une fois l'interface réactivée, FortiAnalyzer reçoit un log indiquant que le périphérique est de nouveau en ligne. Il reçoit également des informations rétrospectives sur l'état de l'interface pendant la période où elle était désactivée.

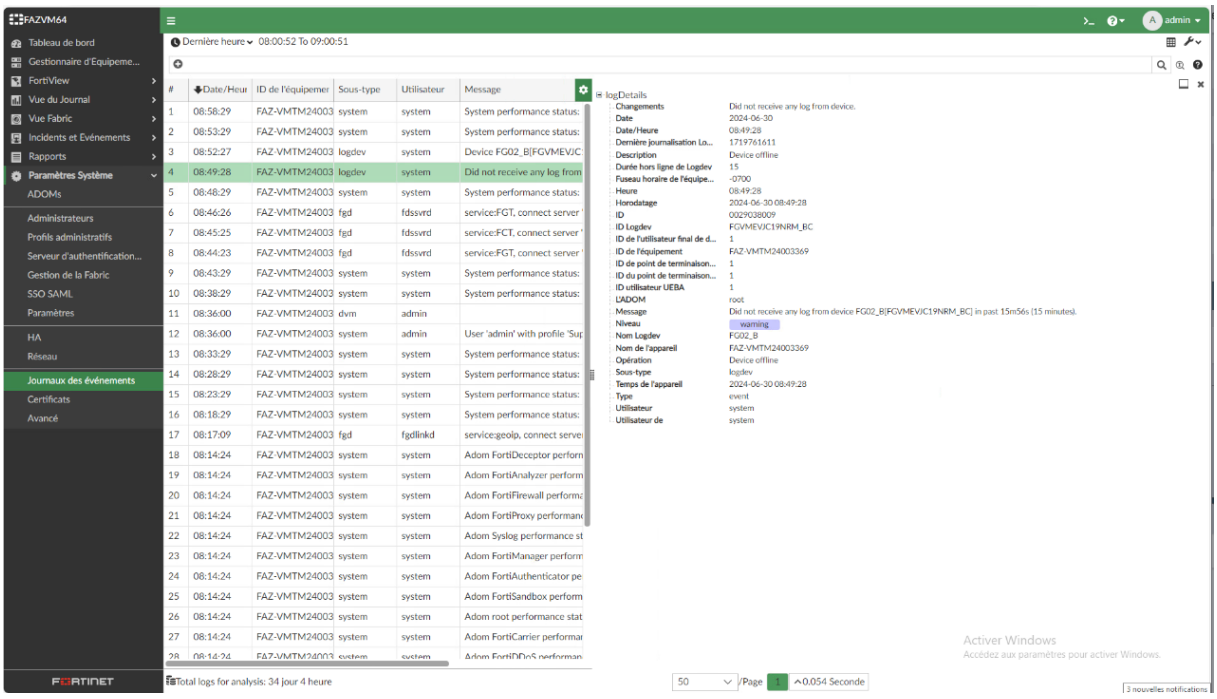


Figure III.57 : Log reçu sur le FA indiquant l'état de l'interface pendant la période où elle était désactivée.

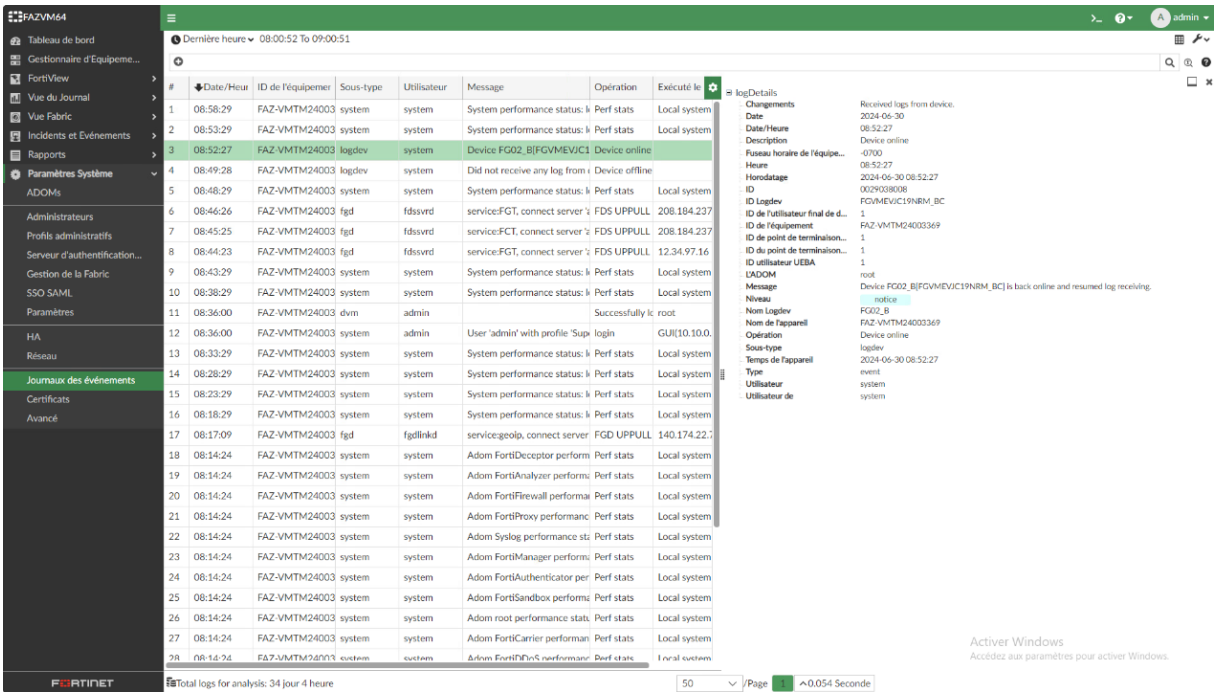


Figure III.58 : Log reçu sur le FA indiquant la reprise de la connexion de l'interface

➢ Code CLI de l'alerte « Anomalie de la bande passante» :

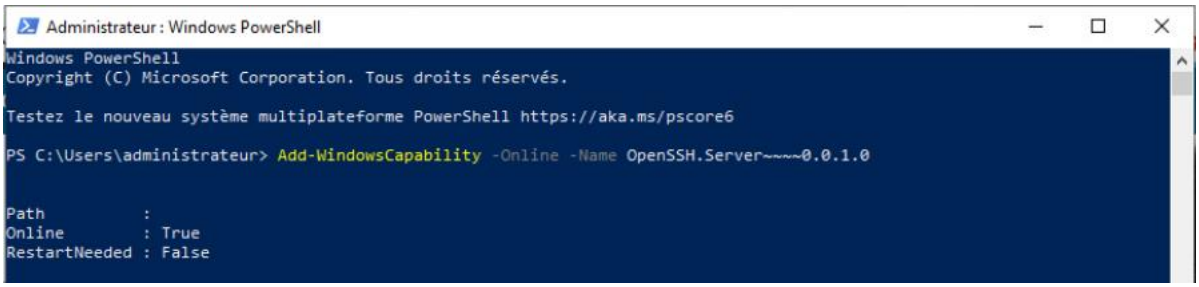
```
config firewall shaper traffic-shaper
edit "Bandwidth_limit_between_LANs"
set maximum-bandwidth 1
next
end

config  system  automation-trigger
edit "Bandwidth_anomaly_trigger"
set event-type event-log
set logid 20221 20220
next
end

config  system automation-action
edit "send_email"
set action-type email
set email-to "ninouhnabila@gmail.com"
set email-subject "Bandwidth anomaly_event"
set message "Bandwidth anomaly_event_detected"
next
end


config system automation-stitch
edit "Bandwidth anomaly_detected"
set trigger "Bandwidth_anomaly_trigger"
config actions
     edit 1
     set action "send_email"
     set required enable
     next
     end
next
end
```


Annulez tous les changements

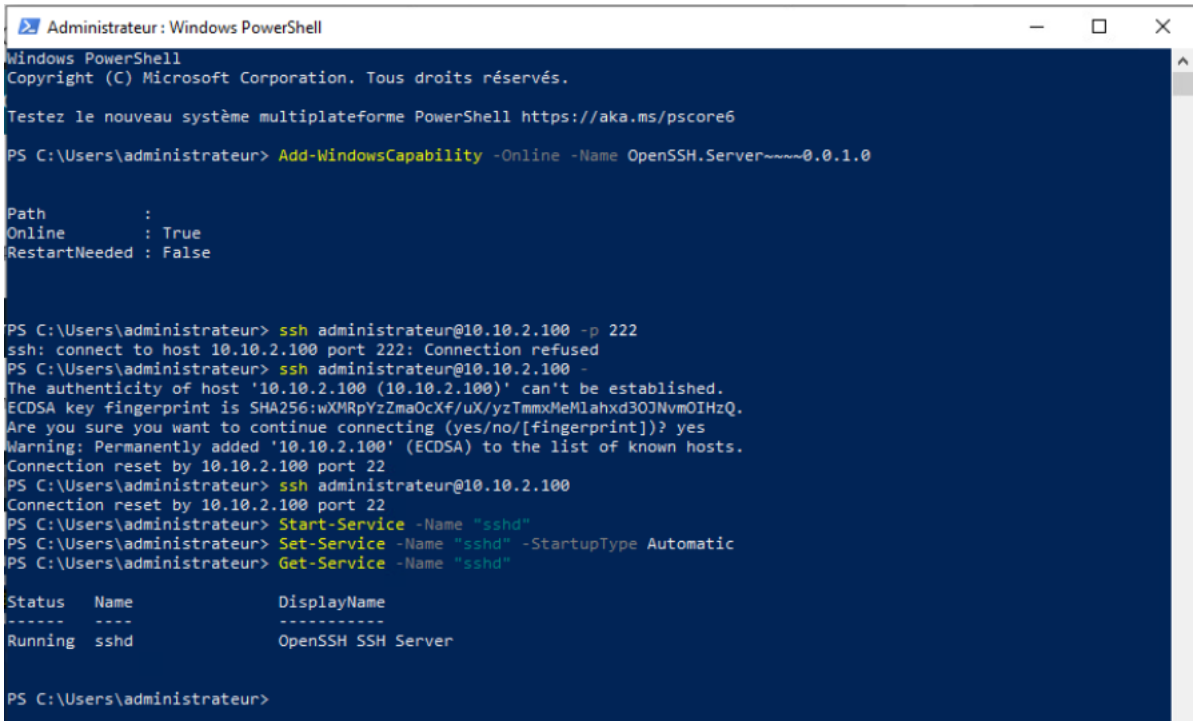
OK Annuler

Log event reçu au niveau de FortiAnalyzer : Nous ne pouvons pas tester et simuler cette alerte actuellement car notre FortiGate est limité à trois politiques au maximum en raison de la licence d'essai. Ces trois politiques sont déjà utilisées pour la configuration de notre topologie actuelle. Toutefois, si à l'avenir Fortinet ajoute une politique supplémentaire, nous testerons cette alerte en envoyant des fichiers de grande taille via OpenSSH en suivant ces étapes :

- Instalation de l'OpenSSH sur les machines sources et destinations utilisant la commande : «Add-WindowsCapability –Online –Name OpenSSH.Server~~~~~0.0.1.0 » sur le PowerShell tant qu'administrateur.



- Puis nous tapons ces étapes :



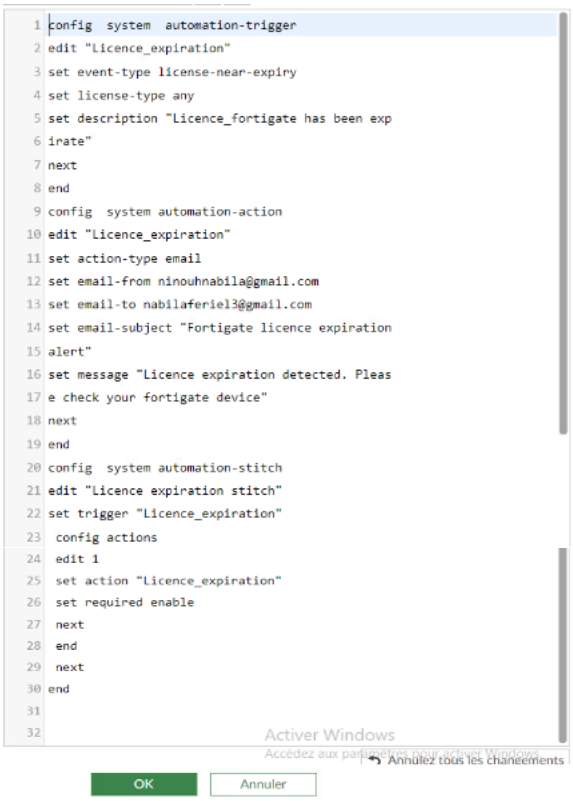
```
PS C:\Windows\system32> scp -r C:\Users\User\Downloads\testfile.dat NESDA\Administrateur@10.10.0.100:C:\Users\User\Downloads\
NESDA\Administrateur@10.10.0.100's password:
scp: C:/Users/User/Downloads/: No such file or directory
PS C:\Windows\system32> scp -r C:\Users\User\Downloads\testfile.dat NESDA\Administrateur@10.10.0.100:C:\uSERS\administrateur\
NESDA\Administrateur@10.10.0.100's password:
testfile.dat                                                  100%   20MB  11.7MB/s   00:01
PS C:\Windows\system32> scp -r C:\Users\User\Downloads\testfile.dat NESDA\Administrateur@10.10.0.100:C:\uSERS\administrateur\
NESDA\Administrateur@10.10.0.100's password:
testfile.dat                                                  100%   20MB  16.9MB/s   00:01
PS C:\Windows\system32> scp -r C:\Users\User\Downloads\testfile.dat NESDA\Administrateur@10.10.0.100:C:\uSERS\administrateur\
NESDA\Administrateur@10.10.0.100's password:
testfile.dat                                                  100%   20MB  15.0MB/s   00:01
PS C:\Windows\system32> scp -r C:\Users\User\Downloads\testfile.dat NESDA\Administrateur@10.10.0.100:C:\uSERS\administrateur\
NESDA\Administrateur@10.10.0.100's password:
testfile.dat                                                  100%   20MB  17.4MB/s   00:01
PS C:\Windows\system32> scp -r C:\Users\User\Downloads\testfile.dat NESDA\Administrateur@10.10.0.100:C:\uSERS\administrateur\
NESDA\Administrateur@10.10.0.100's password:
testfile.dat                                                  100%   20MB  16.1MB/s   00:01
PS C:\Windows\system32> scp -r C:\Users\User\Downloads\testfile.dat NESDA\Administrateur@10.10.0.100:C:\uSERS\administrateur\
NESDA\Administrateur@10.10.0.100's password:
testfile.dat                                                  100%   20MB  16.2MB/s   00:01
PS C:\Windows\system32> scp -r C:\Users\User\Downloads\testfile.dat NESDA\Administrateur@10.10.0.100:C:\uSERS\administrateur\
NESDA\Administrateur@10.10.0.100's password:
```

Sur le Powershell de la machine de destination « Client de la DG » , nous tapons la commande « ls » pour confirmer l'arrivage des fichiers :

```
PS C:\Users\administrateur> ls


    Répertoire : C:\Users\administrateur


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        29/06/2024     02:16                .ssh
da----        28/06/2024     20:18                10.10.2.100
d-r---        21/04/2024     11:15                3D Objects
d-r---        21/04/2024     11:15                Contacts
d-r---        28/06/2024     22:10                Desktop
d-r---        21/04/2024     11:15                Documents
d-r---        29/06/2024     19:28                Downloads
d-r---        21/04/2024     11:15                Favorites
d-r---        21/04/2024     11:15                Links
d-r---        21/04/2024     11:15                Music
d-r---        21/04/2024     11:17                OneDrive
d-r---        21/04/2024     11:15                Pictures
d-r---        21/04/2024     11:15                Saved Games
d-r---        21/04/2024     11:15                Searches
d-r---        27/04/2024     11:14                Videos
-a----        29/06/2024     17:29       20971520 fichier1.dat
-a----        29/06/2024     15:37     4420971520 fichier2.dat
-a----        29/06/2024     18:59     4420971520 fichier3.dat
-a----        29/06/2024     15:33       20971520 testfile.dat
```

Après l'envoi de ces fichiers de grande taille dans une courte période peut déclencher l'alerte d'anomalie de la bande passante par ce que cela a dépassé le seuil précisé dans le code CLI (1 Mbps) .Dans ce cas, l'administrateur peut vérifier les logs et isoler et limiter le trafic suspect, et mettre à jour les règles de sécurité pour bloquer les comportements malveillants. Des actions préventives telles que l'amélioration des politiques de QoS et la surveillance proactive peuvent également être mises en place pour éviter de futures anomalie.

- **Code CLI de l'alerte « La licence expirée» :**



Log event reçu au niveau de FortiAnalyzer : Nous ne pouvons pas tester l'avertissement d'expiration de la licence, car notre licence d'essai des machines n'expirent qu'en 2025.Cela signifie que d'ici là, nous ne pouvons pas simuler ou lancer une expiration de licence pour vérifier la fonctionnalité et l'efficacité de cet avertissement.

Conclusion générale

Notre projet de fin d'études visait principalement à satisfaire les exigences particulières de l'entreprise en ce qui concerne le monitoring et la supervision de réseau de l'entreprise NESDA.

Après avoir profondément compris la conception du réseau de NESDA, nous avons essayé de fournir une solution qui leur permet de surveiller et de gérer leur réseau de manière plus sophistiquée et plus efficace. Nous avons pu mettre en place une solution qui leur permet de mieux contrôler l'ensemble de leurs équipements de manière simple et sécurisée. Elle leur donne même une vue globale et unifiée de l'infrastructure réseau, identifie plus rapidement les problèmes et améliore la performance globale de leur réseau. Cela leur a également permis d'économiser beaucoup de temps, d'efforts et, surtout, de budget.

Ce projet est à la fois enrichissant et gratifiant car Grâce à cette tâche, nous avons pu développer une expertise approfondie dans la gestion et la supervision de réseaux d'entreprises à grande échelle. Dans le domaine de la sécurité des réseaux, nous avons également acquis diverses compétences en manipulant les concepts d'administration des réseaux informatiques et de sécurité que nous avons cités dans les chapitres précédents.
Nous avons effectué un travail de supervision et de suivi du réseau NESDA en deux parties distinctes :

- ✓ **Centraliser la gestion :** L'objectif de cette section est de rassembler et gérer de manière centralisée les configurations et les mises à jour d'équipements de sécurité réseau virtuel "fortigate".
- ✓ **L'analyse centralisée des données de sécurité :** offre une vision d'ensemble de la sécurité du réseau grâce à des analyses temporelles détectant les menaces, générant des rapports détaillés sur le trafic et les activités, et automatisant la réponse aux incidents pour renforcer la cyberdéfense et faciliter la conformité

Bibliographie

[1] M , Mihoubi ., N. Medjani . "Sécurisation d'une infrastructure LAN/WANA base d'équipement Cisco", Université Mouloud Mammeri de Tizi-ouzou, Faculté de génie éléctrique et d'informatique,2015.

[2] A , Djaouti ., H, Mechaour ." Conception et réalisation d'une centrale domotique", Université Mouloud Mammeri de Tizi-Ouzou, Faculté de génie éléctrique et d'informatique , Mémoire de master , 2014/2015.

[3] K, Hadiouche ., S, Guidoum ." Etude et implantation d'un réseau WIFI sécurise au sein de l'INPED", Université Mouloud Mammeri de Tizi-ouzou , Faculté de génie éléctrique et d'informatique, Mémoire de master , 2010-2011.

[4] B, Randi ." Etude et simulation d'un réseau IP-MPLS sous GNS3", Université Mouloud Mammeri, Faculté de génie éléctrique et d'informatique ,Mémoire de master ,2018.

[5] J. Dordoigne ."Réseaux Informatiques . Traité des noyions fondamentales " Série ressources informatiques ,France , 4éme édition, Edition ENI,ISBN:978-2-7460-6145-3, Février 2011.

[6] N,BELAID., CH,ARKOUB .« Services d'accélération des applications et optimisation des liens WAN (WAAS : Wide Area Application services) au niveau de la CNAS d'Alger », Université Mouloud Mammeri de Tizi-ouzou , Faculté de génie éléctrique et d'informatique, Mémoire de Master, 2010/2011.

[7] F , Slamani .,O , Yermeche. « Etude d'une liaison de transmission en fibre optique », Université Mouloud Mammeri de Tizi-Ouzou, Faculté de génie éléctrique et d'informatique, Mémoire de Master ,2017.

[8] M, Rekhis e ., A, Segueni." Migration de IPv4 vers IPv6". Doctorate Thesis,. Université Mouloud Mammeri, Faculté De Génie Electrique Et Informatique Département D'Électronique, Mémoire de master,2018.

[9] Jérôme Durand." Le SDN pour les nuls, Cisco Systems, 11 rue Camille Desmoulins, 92130 Issy-les-Moulineaux, 15 December 2015.

[10] H, Bouida ., " Etude et mise en oeuvre d'une solution SDN : Application de Gestion de VLANs", Mémoire de Master, Université Abou Bakr Belkaid , Tlemcen, Faculté des Sciences Département d'Informatique , 2017.

[11] S, Zidelmal . M. Toumi ., "Implémentation de MPLS sur le backbone d'un fournisseur de service",Mémire master, Université Mouloud Mammeri de Tizi-Ouzou, Faculté de Génie Electrique et d'Informatique Département d'informatique, 2017-2018.

[18] Traore Issa, Kouassi Brou Médard, Atta A. Ferdinand ," Etude du nomadisme dans un Cloud éducatif administré par la technologie SDN/OpenFlow", Doctorate Thesis, Institut de recherches mathématique Université Félix Houphouët-Boigny, Actes de la conférence WACREN 2016.

[19] L. CHERMAK , K. NAILI, "Implémentation d'un Service Cloud Privé pour ATM Mobilis", Université Mouloud Mammeri Tizi-Ouzou, Faculté De Génie Electrique Et Informatique Département D'Électronique, Mémoire de master, 2016.

[20] I . Dob,"Etude et Implémentation d'une solution de virtualisation pour les PME",Mémoire de master , Université Kasdi Merbah-Ouargla , Informatique Industrielle, 2014 .

[21] Arnaud A. A AMELINA,Alain Patrick AINA, Virtualisation & Partage de charge,AFNOG 2014.

[22] A. Sadiqui, "Sécurité des réseaux informatique",Collection Informatique,27-37 ST George's RoadLondon SW19 4EU,UK ISTE ,ISBN 978-1-78405-621-6(print),ISBN 978-1-78405-621-5(e-book), edition Ltd 2019.

[23] Benjamin Morin, Cédric Llorens, Laurent Levier, Denis Valois - Collection Blanche, "Tableaux de bord de la sécurité réseau", 3éme édition, Eyrolles,paris, parution le 26/08/2010.

[24]DJEMAH Massicilia ; « Test d'intrusion interne avec une mise en place d'une solution de sécurité » ; mémoires de master ; Université Mouloud Mammeri de Tizi-ouzou , Faculté de génie éléctrique et d'informatique; 2015.

[25] Selmani Elgharbi ," Mise en place d'un IDS pour sécuriser un réseau en utilisant Snort", Université Mouloud Mammeri de Tizi-ouzou , Faculté de génie éléctrique et d'informatique;2020

[26] Guy Pujolle, Les réseaux locaux, Eyrolles, ISBN13 : 978-2-212-11086-9 ; ISBN10 : 2-212-11086-3 ;Edition 2003.

[27] K.Meksem ; L.Menad, « Conception D'une Interface De Configuration D'un Serveur SSH Sous Windows XP », Mémoire De master, Université Mouloud Mammeri de Tizi-ouzou , Faculté de génie éléctrique et d'informatique ,2011.

[28] Dj.Mahrez ; A.Zerrouki ;" Pratique de solution tunnel VPN IPsec dans un environnement Virtuel et open source ", Mémoire de master Université Ibn Khaldoun – Tiaret, 2020.

[29] Rabehi Sidi Mohamed El Amine, « Mise en place d'un serveur radius sous linux pour la sécurisation d'un réseau 802.11 », Mémoire de Master, Université Abou Bakr Belkaid, Tlemcen-Algérie, 2011.

[30] Vincent Erceau & Romain Colombier, « GMSI Informatique », Projet SAS, 2011

[31] R.Atbane ; « Proposition et implémentation d'une solution sécurité pour un réseau LAN » ; Mémoire de master ; Université Mouloud Mammeri de Tizi-ouzou , Faculté de génie éléctrique et d'informatique ;2018.

[32] A. Maracon, B. Fabrejon, " Les Firewalls - La sécurité des réseaux ", Eyrol, 1999 .

[33] Y. Kherroubi ; K.Idir ; « Mise en œuvre d'une sécurité réseau basée sur l'utilisation du pare-feu PfSence Cas : Algérie Télécom de Tizi-Ouzou » ; Université Mouloud Mammeri de Tizi-ouzou , Faculté de génie éléctrique et d'informatique Mémoire de Master ; 2018.

[34] A.JAQUEMIN, A.MERCIER, Les firewalls.

[35] Belalia Mohamed Cherif ;Maache.kh ; « étude et conception d'un firewall » ;mémoire de master ; Univirsitée saad dahleb Blida. 2011.

[36] Davis Chapman ; « firewall – la sécurité sur internet » édition O'Reilly ;ISBN 978-2-84177-018-2 , parution le 02/01/1997.

[37] Z.Messaoudi , "une présentation de cyber security sur le déni de service", 28 févr. 2024.

[38] Chiradeep BasuMallick , "What Is Packet Sniffing? Meaning, Methods, Examples, and Prevention Best Practices for 2022" , Last Updated: May 10, 2022.

[39] C.Yodha ,"What is a virtual private network(VPN)?",February 06, 2023.

[40] Kamil Karwacki, "PGP (Pretty Good Privacy) in Mulesoft" ,first article, 21 juin 2022.

[41] ADJOUADI.O ; IKHLEF.Y ; « Configuration sécurisée d'un contrôleur de domaine pour une gestion centralisée des utilisateurs au sein d'une entreprise cas « Tchin-Lait» ; Mémoire de Master ; Université Abderrahmane Mira de Béjaia ; 2017

[42] Tamare NDJIE MENGBWA ; « Mise en place d'un contrôleur de domaine sous Windows serveur 2008 » ; Diplôme de technicien Supérieur (DTS) ; IAI-Cameroun ;2013

Webographie

[w1] https://www.paessler.com/fr/it-explained/server consulté le 01/ 05 /2024

[w2] https://www.codeur.com/blog/quels-sont-les-differents-types-de-serveurs/ Consulté le 01/ 05 /2024

[w3] https://www.blogdumoderateur.com/tools/tech/virtualisation/ Consulté le 01/05/2024.

[w4] https://www.blogdumoderateur.com/tools/tech/virtualisation/. Consulté le 01/05/2024.

[w5] https://www.axido.fr/quels-sont-les-logiciels-de-virtualisation/. Consulté le 01/05/2024.

[w6] https://www.linkedin.com/pulse/personal-area-network-mohammed-shafi-eu3kc Consulté le 01/05/2024.

[w7] https://brain-services.fr/audit_lan.html. Consulté le 01/05/2024.

[w8] https://www.clic-formation.net/seance-10-reseau/support.html. Consulté le 01/05/2024

[w9] http://www.it-connect.fr/les-modeles-osi-et-tcpip/ . Consulté le 01/05/2024

[w10] https://www.frameip.com/mpls-cisco/. Consulté le 07/05/2024

[w11] http://www.it-connect.fr/les-modeles-osi-et-tcpip/ Consulté le 07/05/2024.

[w12] https://zestedesavoir.com/tutoriels/2789/les-reseaux-de-zero/le-concept-et-les-bases/les-topologies/. Consulté le 05/05/2024.

[w13] https://networksimulationtools.com/spoofing-attack-network-projects/ Consulté le 09/05/2024.

[w14] https://www.fortinet.com/fr/resources/cyberglossary/what-is-https Consulté le 09/05/2024.

[w15] https://docs.fortinet.com/document/fortigate/7.0.0/new features/649094/dedicated-tunnel-id-for-ipsec-tunnels-7-0-1 Consulté le 09/05/2024.

[w16] https://www.frameip.com/firewall/ Consulté le 09/05/2024.

[w17] https://www.blogdumoderateur.com/tools/zonealarm-firewall/ Consulté le 10/05/2024.

[w18] https://wecomm.fr/connexion-https-securite/ Consulté le 10/05/2024

[W19] https://learn.microsoft.com/en-us/windows-server/ consulter le 17/05/2024

[W20] https://www.gladir.com/OS/WINDOWS2019SERVER/intro.htm consulter le 17/05/2024

[W21] https://www.enbitcon.fr/shop/fortinet/fortimanager/ consulter le 17/05/2024

[W22]https://www.nomios.fr/partenaires/fortinet/gestion-et-visibilite/fortianalyzer/ consulter le 17/05/2024

[W23] https://www.acipia.fr/infrastructure/securite/fortianalyzer/ consulter le 17/05/2024

[W24] https://activedirectorypro.com/what-is-active-directory/#lesson4 consulter le 17/05/2024

[W25] https://serverspace.io/fr/support/help/how-to-manage-ous-in-active-directory/ consulter le 18/05/2024

[W26]https://www.tranquil.it/gerer-identification-authentification-utilisateurs/ consulter le 18/05/2024

[W27]https://aris-informatique.fr/quelles-sont-les-principales-failles-de-securite-informatique/ Consulter le 01/06/2024