

République Islamique de Mauritanie
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Nouakchott Faculté des
Sciences et Techniques

Département Mathématiques et
Informatique



Mémoire de Fin d'Étude

En vue de l'obtention du

Diplôme de Master en :
Informatique, Science de données et Réseaux (Parcours Réseaux et Systèmes Communicants)

Analyse et Optimisation des Performances d'un Réseau Informatique d'Entreprise

Réalisé par :

Brahim Ahmed Mahmoud
Aichetou Med Lemaidel

Encadrer par :

Dr. Mamadou Tourad DIALLO
Ing. Mouhamed Mahmoud Taghi

Année Universitaire : 2023/2024

DÉDICACES

Nous dédions ce mémoire à nos familles, qui ont été des piliers inébranlables tout au long de ce parcours. Leur amour, leur soutien inconditionnel et leurs encouragements constants ont été notre source de force, de motivation et d'inspiration. Ils ont su nous guider et nous offrir l'énergie nécessaire pour surmonter les défis académiques et personnels rencontrés au fil des années. Leur foi en nos capacités et leur présence indéfectible ont été essentielles pour mener à bien ce projet.

À nos amis, qui ont toujours été là pour nous, dans les moments de doute comme dans les moments de réussite. Leur présence bienveillante, leur écoute attentive et leur soutien moral ont été des facteurs clés qui nous ont permis de continuer à avancer, même lorsque les obstacles semblaient insurmontables. Ils ont su rendre ce parcours plus léger, apportant de la joie et de la sérénité dans nos moments de tension.

À tous ceux qui croient en l'importance de la connaissance et de l'innovation, et qui œuvrent pour un avenir meilleur. Ce travail est un hommage à l'effort collectif de toutes les personnes qui contribuent à faire avancer la science, les technologies et l'éducation. Nous espérons que ce mémoire, fruit de nos efforts et de nos recherches, puisse participer à cet élan d'innovation et inspirer ceux qui, comme nous, ont la conviction que la quête de la connaissance et de l'amélioration continue est essentielle pour bâtir un avenir plus lumineux pour les générations futures.

Que ce mémoire soit le reflet de nos efforts communs, le témoignage de notre détermination, et qu'il marque le début de nouveaux horizons, tant sur le plan personnel que professionnel. Que ces quelques pages puissent inspirer et guider ceux qui se lancent, eux aussi, dans des projets de recherche et d'innovation.

REMERCIEMENTS

Nous tenons à exprimer notre profonde gratitude à notre encadrant, Dr. Mamadou Tourad DIALLO, pour sa guidance précieuse et ses conseils avisés tout au long de ce projet. Sa rigueur académique, son expertise dans le domaine et sa capacité à nous orienter vers des solutions pertinentes ont été des éléments essentiels dans la réalisation de ce mémoire. Nous lui sommes reconnaissants pour ses encouragements constants et pour la disponibilité qu'il a su maintenir malgré ses multiples engagements. Ses remarques constructives ont enrichi notre réflexion et contribué à affiner nos idées tout au long de ce parcours.

Nos remerciements vont également à Ing. Mouhamed Mahmoud Taghi, pour son expertise technique et ses suggestions pertinentes, qui ont grandement contribué à l'enrichissement de ce travail. Son accompagnement a permis d'approfondir nos connaissances pratiques et d'appliquer des concepts théoriques à des cas réels, renforçant ainsi la qualité de notre réflexion. Ses conseils pratiques et son implication ont joué un rôle clé dans le succès de ce projet.

Nous tenons à remercier nos collègues et amis pour leur soutien moral tout au long de cette aventure académique. Leurs discussions constructives, leur écoute attentive et leurs critiques bienveillantes ont permis de maintenir un environnement d'échanges productifs et d'améliorer la qualité de notre travail. Ils ont apporté une dimension humaine et enrichissante à ce parcours, nous permettant de mieux appréhender les défis du projet et d'en tirer le meilleur parti.

Enfin, nous adressons notre reconnaissance à tous les enseignants de l'Université de Nouakchott et à tout le personnel de la Faculté des Sciences et Techniques, pour les connaissances qu'ils nous ont transmises durant notre formation. Leurs enseignements théoriques et pratiques ont été essentiels dans l'acquisition des compétences nécessaires pour la réalisation de ce mémoire. Nous leur sommes profondément reconnaissants pour leur engagement et pour la qualité de l'enseignement dispensé, qui a largement contribué à la réussite de notre parcours académique.

Chacun d'entre eux a joué un rôle déterminant dans la réalisation de ce travail et dans notre épanouissement personnel et professionnel. À tous, nous exprimons nos sincères remerciements.

Résumé:

Ce mémoire porte sur l'analyse et l'optimisation des performances du réseau informatique de Mauritel, visant à garantir une infrastructure performante, sécurisée et évolutive. À l'aide d'outils comme GNS3, VMware, Zabbix et FortiGate, une méthodologie rigoureuse a été adoptée pour modéliser, superviser et sécuriser le réseau. Zabbix a permis une surveillance en temps réel des équipements critiques, tandis que FortiGate a assuré la segmentation et la protection des zones réseau (LAN, DMZ, WAN) contre les intrusions, ainsi que la mise en place de connexions sécurisées via VPN. Les résultats incluent une amélioration significative des performances réseau, une réduction des goulots d'étranglement, et une sécurisation renforcée des services critiques, offrant une base solide pour relever les futurs défis technologiques de Mauritel.

الملخص:

يركز هذا البحث على تحليل وتحسين أداء شبكة المعلومات الخاصة بشركة Mauritel، بهدف ضمان بنية تحتية عالية الأداء وأمنة وقابلة للتتوسيع. باستخدام أدوات مثل GNS3 و VMware و Zabbix و FortiGate، تم تبني منهجية دقيقة لنموذج الشبكة، مراقبتها وتأمينها. ساهم Zabbix في المراقبة الفورية للأجهزة الحرجة، بينما وفر FortiGate تقسيماً وحماية لمناطق الشبكة (LAN، DMZ، WAN) ضد التهديدات، بالإضافة إلى إنشاء اتصالات آمنة عبر شبكات VPN. تشمل النتائج تحسيناً كبيراً في أداء الشبكة، وتقليل نقاط الاختناق، وتعزيز أمان الخدمات الحيوية، مما يوفر أساساً قوياً لمواجهة التحديات التكنولوجية المستقبلية لشركة Mauritel.

Abstract:

This thesis focuses on the analysis and optimization of Mauritel's IT network performance, aiming to ensure a high-performing, secure, and scalable infrastructure. Using tools such as GNS3, VMware, Zabbix, and FortiGate, a rigorous methodology was adopted to model, monitor, and secure the network. Zabbix enabled real-time monitoring of critical equipment, while FortiGate ensured segmentation and protection of network zones (LAN, DMZ, WAN) against intrusions and established secure connections through VPNs. The results include significant network performance improvements, reduced bottlenecks, and enhanced security for critical services, providing a solid foundation to address Mauritel's future technological challenges.

Table des matières

Liste des Figures	1
Liste des Tableaux	1
Liste des abréviations.....	1
INTRODUCTION GÉNÉRALE.....	2
Chapitre 1 : Cadre Conceptuel du Projet	2
Partie 1 : Présentation de l'Entreprise Mauritel.....	3
I. Introduction.....	3
II. Présentation générale de Mauritel.....	3
III. Historique de Mauritel.....	4
IV. Les services offerts par Mauritel.....	4
V. Structure organisationnelle de l'entreprise	5
VI. Conclusion.....	5
Partie 2 : Cadre d'Analyse du Projet	6
I. Introduction.....	6
II. Étude de l'existence	6
III. Critique de l'existence	6
IV. Contexte et problématique.....	6
V. Objectifs du projet	6
VI. Structure du rapport.....	7
VII. Méthodologie.....	7
VIII. Organisation des Travaux	7
IX. Conclusion.....	8
Chapitre 2 : État de l'art et technologies utilisées	9
2.1 Introduction.....	10
2.2 Monitoring, surveillance réseau informatique	10
2.2.1 Les objectifs du monitoring	10
2.2.2 Outils de Monitoring	11
2.2.2.1 Les Plateformes Éditeurs	11
2.2.2.2 Les plateformes libres :	11
2.2.2.2.1 Nagios :	11
2.2.2.2.2 Zabbix.....	12
2.2.2.2.3 GLPI/OCS :	12
2.2.3 Etude comparatif.....	13
2.2.3.1 Diagramme radar	13
2.2.3.2 Tableau comparatif	13
2.2.4 Choix de Plateforme	14
2.2.4.1 Fonctionnement de Zabbix	14

2.2.4.2	Interactions entre les Composants	14
2.2.4.3	Gestion des flux.....	15
2.2.4.4	Checks actifs/passifs	16
2.2.4.5	Système d'alerte	16
2.2.4.6	Architecture	17
2.3	Les systèmes de sécurité des réseaux.....	19
2.3.1	IPFire.....	19
2.3.2	pfSense.....	20
2.3.3	FortiGate :	20
2.3.4	Tableau comparatif :	21
2.3.5	Choix préférentiel :.....	22
2.4	Surveillance des services critiques et optimisation réseau (QoS)	22
2.4.1	Supervision des Services Critiques	22
2.4.2	Mécanismes d'Optimisation comme la QoS	22
2.5	Approches de détection des intrusions et des menaces	23
2.5.1	Systèmes de Détection d'Intrusion (IDS) :	23
2.5.2	Systèmes de Prévention d'Intrusion (IPS) :	23
2.5.3	Gestion des événements de sécurité (SIEM).....	23
2.6	Technologies de pare-feu et VPN dans les réseaux d'entreprise	23
2.6.1	Pare-feu FortiGate.....	23
2.6.2	VPN FortiGate	24
2.7	Outils de simulation et virtualisation	24
2.7.1	Les outils de simulation :	24
2.7.2	Choix préférentiel :.....	25
2.7.3	Les outils de virtualisation :.....	25
2.7.4	Choix préférentiel :.....	26
2.8	Trello	26
2.9	Conclusion	27
Chapitre 3 : Mise en place du réseau et configuration des systèmes	28	
3.1	Introduction.....	29
3.2	Déploiement de l'infrastructure réseau	29
3.2.1	Installation et Configuration de VMware Workstation.....	29
3.2.2	Installation et configuration de GNS3	31
3.2.3	Installation et Configuration de Zabbix Serveur sur Ubuntu	38
3.2.4	Installation et configuration de l'agent Zabbix sur Windows	42
3.2.5	Installation de FortiGate.....	44
3.2.6	Ajout des Machines Virtuelles dans VMware et GNS3	46
3.2.6.1	Environnement Virtualisé.....	46
3.2.6.2	Création du projet GNS3.....	46

3.2.6.3	Topologie Réseau Simple	47
3.2.6.4	Topologie :	47
3.2.6.4.1	Zone LAN	48
3.2.6.4.2	Zone DMZ	48
3.2.6.4.3	Zone LAN	48
3.2.6.4.4	VPN à distance	48
3.2.7	Connexion au FortiGate et configuration	49
3.3	AD et LDAP avec FortiGate	54
3.3.1	Configuration du serveur (AD) :	54
3.3.2	Intégration LDAP avec FortiGate :	57
3.4	VPN pour accès sécurisé.....	58
3.4.1	Installation et Configuration du Client VPN	59
3.5	Conclusion	62
Chapitre 4 : Résultats et analyse	63
4.1	Introduction.....	64
4.2	Résultats de la supervision et incidents détectés	64
4.3	Analyse des performances réseau sous supervision	65
4.3.1	Services Critiques	65
4.3.2	Bande passante :	65
4.3.3	La latence :	66
4.3.4	Taux de perte de paquets	66
4.4	Services DMZ accessibles depuis le LAN.....	67
4.5	Résultats des simulations d'attaques et contre-mesures.....	68
4.5.1	DoS (Denial of Service)	68
4.5.2	Antivirus.....	69
4.5.3	Web Filtre	71
4.5.4	L'injection SQL (SQL Injection)	72
4.6	Conclusion	74
CONCLUSION GÉNÉRALE	76
Bibliographie	77

LISTE DES FIGURES

Figure 1: Logo Mauritel	3
Figure 2 : Organisme Mauritel	5
Figure 3 : Diagramme radar	13
Figure 4 : Architecture de Zabbix	15
Figure 5 : Les Protocoles et Ports dans l'Architecture Zabbix	15
Figure 6 : Échange de Données du Serveur Zabbix a l'Agent Zabbix.....	16
Figure 7 : Échange de Données de l'Agent au Serveur Zabbix	16
Figure 8 : Collecte des Données et Alertes	16
Figure 9 : Architecture mono-serveur	17
Figure 10 : Architecture Multi-serveur.....	17
Figure 11 : Architecture Multi-proxy	18
Figure 12 : Architecture Multi-serveur et Multi-proxy	18
Figure 13 : Logo d'IPFire	19
Figure 14 : Logo de pfSense.....	20
Figure 15 : Logo de FortiGate.....	20
Figure 16 : Logo de GNS3	25
Figure 17 : Logo de VMWare	26
Figure 18 : Logo de Trello	26
Figure 19 : Début de l'installation de VMWare.....	29
Figure 20 : Acceptation du contrat de licence	29
Figure 21 : Ajout à la variable PATH	30
Figure 22 : Installation en cours	30
Figure 23 : Interface de VMWare	30
Figure 24 : Création de compte GNS3	31
Figure 25 : Connexion au site GNS3.....	31
Figure 26 : Démarrage de l'installation.....	31
Figure 27 : Acceptation de la licence	32
Figure 28 : Sélection des composants	32
Figure 29 : Choix de VMware Workstation	32
Figure 30 : Téléchargement de la VM GNS3.....	33
Figure 31 : Chemin de la VM téléchargée.....	33
Figure 32 : Installation de WinPCAP	33
Figure 33 : Installation de Npcap	34
Figure 34 : Installation de Solar-Putty.....	34
Figure 35 : Configuration de Solar-Putty	34
Figure 36 : Fin de l'installation	35
Figure 37 : Décompression de la VM.....	35
Figure 38 : Importation de l'OVA dans VMware	35
Figure 39 : Nom et emplacement de la GNS3 VM	36
Figure 40 : Paramètres de la GNS3 VM dans VMware	36
Figure 41 : Préférences de GNS3	36
Figure 42 : Activation et configuration de la VM	37
Figure 43 : Lancement de la VM GNS3.....	37
Figure 44 : Vérification de l'état de la VM	37
Figure 45 : Téléchargement du paquet Zabbix	38
Figure 46 : Ajout du dépôt Zabbix	38
Figure 47 : Installation de Zabbix	38
Figure 48 : Installation de MySQL.....	38
Figure 49 : Création de la base de données	39
Figure 50 : Importation de la base de données	39

Liste des figures

Figure 51 : Redémarrage des services	39
Figure 52 : Accès à l'interface web	40
Figure 53 : Vérification des prérequis	40
Figure 54 : Configuration de la base de données	40
Figure 55 : Page login Zabbix	41
Figure 56 : Accès au Dashboard	41
Figure 57 : Configuration SMTP pour les notifications Zabbix	41
Figure 58 : Téléchargement de l'agent Zabbix	42
Figure 59 : Choix de la version de l'agent	42
Figure 60 : Fenêtre d'installation de l'agent	42
Figure 61 : Configuration de l'hôte et IP	43
Figure 62 : Finalisation de l'installation	43
Figure 63 : Téléchargement de l'image VM FortiGate	44
Figure 64 : Installation de FortiGate dans GNS3	44
Figure 65 : Importation de l'image dans GNS3	45
Figure 66 : Installation de FortiGate dans GNS3	45
Figure 67 : Environnement Virtualisé	46
Figure 68 : Création du projet GNS3	46
Figure 69 : Topologie Réseau Simple	47
Figure 70 : Topologie réseau	47
Figure 71 : Connexion à l'interface webGUI FortiGate	49
Figure 72 : Tableau de bord FortiGate	49
Figure 73 : Interfaces de FortiGate	49
Figure 74 : Configuration de l'interface LAN	50
Figure 75 : Configuration de l'interface LAN	50
Figure 76 : Politique de pare-feu	51
Figure 77 : Configuration SNMP	51
Figure 78 : Liste des utilisateurs	52
Figure 79 : Groupes d'utilisateurs	52
Figure 80 : Serveurs LDAP	52
Figure 81 : Traffic Shapers	52
Figure 82 : Politiques de gestion du trafic	53
Figure 83 : Login portail captif	53
Figure 84 : Test de bande passante après connexion	53
Figure 85 : Choix de la langue d'installation	54
Figure 86 : Lancement de l'installation	54
Figure 87 : Définition du mot de passe Administrateur	55
Figure 88 : Accès Windows avec Ctrl + Alt + Suppr	55
Figure 89 : Tableau de bord Server Manager	56
Figure 90 : Ajout d'ordinateurs dans AD	56
Figure 91 : Gestion des utilisateurs dans AD	56
Figure 92 : Connexion LDAP de FortiGate à AD	57
Figure 93 : Authentification des utilisateurs FortiGate via LDAP	57
Figure 94 : Configuration VPN sur FortiGate	58
Figure 95 : Création de la Politique d'Accès	58
Figure 96 : Configuration des Utilisateurs et Groupes	58
Figure 97 : Début de l'installation de FortiClient VPN	59
Figure 98 : Acceptation des Conditions d'Utilisation	59
Figure 99 : Accès à la Configuration VPN dans FortiClient	60
Figure 100 : Réglages VPN	60
Figure 101 : Réglages VPN	61
Figure 102 : Login de VPN	61
Figure 103 : Accès distant via VPN sur LAN	62

Liste des figures

Figure 104 : Surveillance des Équipements	64
Figure 105 : Suivi des Performances de l'Infrastructure	64
Figure 106 : Alertes par e-mail de Zabbix dans Gmail	65
Figure 107 : Supervision des Performances Réseau et Services Critiques.....	66
Figure 108 : Accès au serveur web depuis le LAN	67
Figure 109 : Envoi d'e-mail entre les clients	67
Figure 110 : Envoi d'e-mail entre les clients	67
Figure 111 : Application de DoS.....	68
Figure 112 : Limitation des paquets contre DoS	68
Figure 113 : Simulation d'une attaque ICMP Flood.....	69
Figure 114 : Détection et blocage d'une attaque ICMP Flood.....	69
Figure 115 : Fonctionnement de l'antivirus	70
Figure 116 : Blocage du fichier EICAR par FortiGate.....	70
Figure 117 : Blocage du fichier EICAR par FortiGate.....	70
Figure 118 : Blocage d'accès à un site web via FortiGate	71
Figure 119 : Blocage d'accès à Facebook par FortiGate	71
Figure 120 : IP Virtuelle pour l'Accès Web DMZ	72
Figure 121 : DVWA accessible via WAN	72
Figure 122 : Extraction de données DVWA.....	73
Figure 123 : Prévention des attaques Web	73
Figure 124 : Blocage d'accès via FortiGate	74
Figure 125 : Prévention des injections SQL.....	74

LISTE DES TABLEAUX

Tableau 1 : Planification	8
Tableau 2 : Tableau comparatif de supervision.....	14
Tableau 3 : Tableau comparatif des pare-feux	22

Liste des abréviations

LISTE DES ABRÉVIATIONS

IP/MPLS: Internet Protocol / Multi-Protocol Label Switching

LAN: Local Area Network

DMZ: Demilitarized Zone

WAN: Wide Area Network

BTS: Base Transceiver Station

QoS: Quality of Service

VMware: Virtual Machine Software

SMS: Short Message Service

GNS3: Graphical Network Simulator-3

GFU : Groupe Fermé d'Usagers

MS-SQL : Microsoft SQL Server

NPM: Network Performance Monitor

OT: Operational Technology

IoT: Internet of Things

SNMP: Simple Network Management Protocol

ICMP: Internet Control Message Protocol

TCP: Transmission Control Protocol

HTTP: HyperText Transfer Protocol

IPMI: Intelligent Platform Management Interface

JMX: Java Management Extensions

IGLP : Gestionnaire Libre de Parc Informatique

OCS: Open Computer and Software Inventory

PHP: HyperText Preprocessor

SPI: Stateful Packet Inspection

Liste des abréviations

VPN: Virtual Private Network

IPSec: Internet Protocol Security

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

DPI: Deep Packet Inspection

NGFW: Next-Generation Firewall

SSL: Secure Sockets Layer

SIEM: Security Information and Event Management

ASIC: Application-Specific Integrated Circuit

NAT: Network Address Translation

KVM: Kernel-based Virtual Machine

MySQL: MySQL Database Management System

vCPU: Virtual Central Processing Unit

OVA: Open Virtualization Archive

WINS: Windows Internet Name Service

ALDP: Lightweight Directory Access Protocol

AD: Active Directory

INTRODUCTION GÉNÉRALE

Dans un monde de plus en plus connecté, où la performance des réseaux informatiques est essentielle pour le bon fonctionnement des entreprises, l'optimisation des infrastructures réseau devient un enjeu crucial. Les réseaux, qui relient des systèmes informatiques variés, doivent être capables de gérer efficacement le trafic tout en garantissant la sécurité des données. La capacité à identifier les goulets d'étranglement et à résoudre les problèmes de latence est fondamentale pour maintenir une productivité élevée et une expérience utilisateur satisfaisante. Dans ce contexte, des solutions innovantes et des outils de surveillance avancés, tels que Zabbix et FortiGate, jouent un rôle déterminant pour assurer une gestion efficace des ressources réseau.

Dans cette optique, Mauritel, en tant que principal fournisseur de services de télécommunications en Mauritanie, a mis en place une infrastructure réseau complexe et étendue. Disposant de plusieurs Datacenters interconnectés à travers le pays via des réseaux LAN et WAN basés sur la technologie IPMPLS, l'entreprise offre une gamme de services variés, allant de l'hébergement de serveurs aux solutions de gestion de données. Les équipements utilisés, comprenant des Microsoft et Linux, des bases de données Oracle et MySQL, ainsi que des appliances de sécurité, sont intégrés de manière à optimiser les performances et la disponibilité des services. Dans ce cadre, une évaluation régulière des performances du réseau est nécessaire pour répondre aux exigences croissantes des clients et assurer la qualité de service.

Notre projet se concentre sur l'analyse et l'optimisation des performances du réseau informatique de Mauritel. À l'aide d'outils de simulation comme GNS3 et de solutions de virtualisation telles que VMware, nous avons créé une topologie réseau intégrant un pare-feu FortiGate pour gérer le trafic entre différentes zones, notamment le LAN, le WAN et la DMZ. Le FortiGate joue un rôle clé dans la sécurisation de l'infrastructure, en appliquant des politiques de sécurité rigoureuses pour contrôler l'accès aux ressources. Grâce à des politiques adaptées, nous avons pu permettre la communication entre le LAN et le WAN tout en limitant l'accès aux services sensibles hébergés dans la DMZ. Le FortiGate assure une protection contre les menaces externes tout en optimisant le flux de données à travers le réseau. Parallèlement, nous avons intégré Zabbix comme solution de surveillance réseau, permettant de suivre en temps réel les performances des équipements et d'identifier rapidement les problèmes potentiels. Zabbix collecte des données sur le trafic, la bande passante, et les temps de latence, fourni ainsi une visibilité complète sur l'état du réseau. Grâce à des déclencheurs configurés, il est possible de recevoir des alertes en cas de dysfonctionnements, ce qui permet une réaction rapide et appropriée pour minimiser les interruptions de service. Ce projet vise non seulement à identifier et résoudre les problèmes de performance, mais aussi à mettre en œuvre des solutions d'optimisation adaptées aux besoins de l'entreprise, grâce à une approche méthodique et intégrée de la surveillance et de la sécurité.

Ce rapport se compose de quatre chapitres :

Chapitre 1 : Présente l'entreprise Mauritel et le cadre conceptuel du projet.

Chapitre 2 : Aborde les technologies et outils utilisés.

Chapitre 3 : Décrit la mise en place de l'infrastructure réseau.

Chapitre 4 : Analyse les résultats obtenus et propose des optimisations.

Introduction Générale

1

Chapitre 1 : Cadre Conceptuel du Projet

Partie 1 : Présentation de l'Entreprise Mauritel

I. Introduction

Dans cette première partie, nous allons explorer l'entreprise Mauritel en présentant son rôle dans les télécommunications en Mauritanie, son historique, les services qu'elle offre, et sa structure organisationnelle. Cette analyse servira de base pour comprendre les enjeux liés à notre projet d'optimisation des performances d'un réseau informatique.

II. Présentation générale de Mauritel

Moov Mauritel est l'opérateur de télécommunications mobile et fixe le plus ancien et le plus établi en Mauritanie. Fondée en 1999, elle hérite de l'activité télécom de l'opérateur historique l'OPT (Office des Postes et Télécommunications), devenant ainsi un acteur central du développement économique et social du pays. Depuis sa création, Mauritel n'a cessé de jouer un rôle clé dans la transformation numérique de la Mauritanie, contribuant à son ouverture aux nouvelles technologies et au monde connecté.

Grace à son infrastructure réseau robuste et bien repartie, Mauritel assure la connectivité à travers tout le territoire national. La société exploite plusieurs Datacenters interconnectés, basés sur des technologies modernes telles que l'IPMPLS, qui facilitent le transport rapide et sécurisé des données. Ces centres de données hébergent une gamme variée de systèmes d'exploitation, allant des Microsoft et Linux aux plateformes de virtualisation avancées comme VMware et NUTANIX. Ce vaste écosystème permet à Mauritel de proposer des services performants, adaptés aux besoins variés de ses clients, qu'ils soient particuliers, professionnels ou entreprises.

Leader sur le marché des télécommunications en Mauritanie, Mauritel a constamment cherché à innover pour répondre aux attentes de ses clients et relever les défis technologiques. Toutefois, avec l'augmentation exponentielle de la demande en bande passante, l'adoption massive des services numériques, et l'évolution des habitudes de consommation de données, une optimisation continue de son infrastructure réseau est devenue cruciale. Cela permet à l'entreprise de maintenir sa position de leader, tout en garantissant une qualité de service irréprochable.

Ainsi, Mauritel s'engage à poursuivre son développement technologique et à renforcer sa capacité à offrir des solutions de télécommunications modernes, fiables et accessibles à l'ensemble de la population mauritanienne, tout en préparant son réseau à répondre aux défis futurs du secteur.



Figure 1: Logo Mauritel

III. Historique de Mauritel

Suite à un appel d'offres international lancé par le gouvernement mauritanien le 12 avril 2001, Maroc Télécom a acquis 54 % du capital de Mauritel SA. Cette acquisition a permis à Mauritel de devenir un opérateur global, bénéficiant ainsi de la synergie entre toutes ses activités : fixe, mobile et Internet.

➤ **Téléphonie Fixe, Data et Internet**

MAURITEL propose des services de téléphonie fixe (voix et données) ainsi qu'un accès à Internet, se positionnant comme le premier opérateur sur ce marché. Cependant, bien que le premier acteur n'ait jusqu'à présent développé ni réseaux ni offres fixes, le second fournit ses services fixes via son réseau CDMA. À la fin décembre 2011, Mauritel comptait 14 000 lignes fixes, enregistrant une hausse de 1,6 % et permettant d'offrir des services Internet haut débit à ses clients. Elle comptait près de 7 000 abonnés Internet, avec une croissance de 1,4 %.

➤ **Téléphonie Mobile**

L'activité mobile de MAURITEL propose des services prépayés et post-payés, ainsi que des offres de voix et de données, incluant notamment les SMS. L'entreprise assure également le roaming pour les abonnés mobiles à l'étranger, ainsi que pour les clients des opérateurs partenaires séjournant en Mauritanie. Pour fournir ces services, MAURITEL s'appuie sur un réseau de 623 stations de base (BTS) réparties sur l'ensemble du territoire mauritanien, permettant l'offre des services 2G et 3G, cette dernière ayant été lancée en 2009. En 2011, le parc mobile de Mauritel a enregistré une croissance soutenue de 10,9 %, atteignant 1,7 million de clients, malgré un taux de pénétration élevé de 93 % au 30 septembre 2011.

IV. Les services offerts par Mauritel

Trois types de services sont commercialisés par MAURITEL MOBILES :

- **Service Post-paye** : un service d'abonnement mobile avec facturation mensuelle.
- **Service Prépaye** : accès aux services mobiles via une carte à gratter prépayée.
- **GFU (Groupe Fermé d'Usagers)** : ce service permet aux utilisateurs d'un même réseau au sein d'un groupe de communiquer à des tarifs réduits, pouvant atteindre jusqu'à 75 %.

De plus, MAURITEL propose également des services à valeur ajoutée, tels que les messages courts (SMS), la messagerie vocale et le roaming.

V. Structure organisationnelle de l'entreprise

La structure organisationnelle de Mauritel se compose de plusieurs entités clés sous la direction du **Directeur Général**.

- **Services Ressources Humaines & Organisation** : Gère le personnel et l'organisation interne.
- **Secrétariat Général** : Assure la coordination administrative.
- **Service Contrôle Général** : Supervise les opérations et évalue les performances.
- **Service Qualité** : Garantit le respect des standards de qualité.
- **Direction Commerciale** : Développe les affaires et gère les relations clients.
- **Direction Réseaux** : S'occupe de la gestion des infrastructures réseau.
- **Direction Administrative & Financière** : Gère les aspects financiers et administratifs.

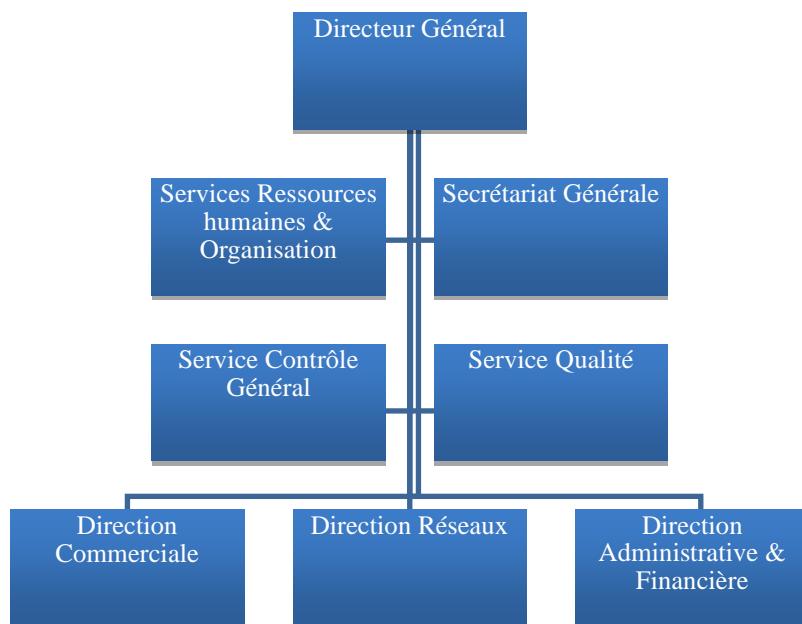


Figure 2 : Organisme Mauritel

VI. Conclusion

Cette première partie a examiné Mauritel, opérateur majeur des télécommunications en Mauritanie, depuis son acquisition par Maroc Télécom jusqu'à son rôle actuel. Nous avons abordé ses services en téléphonie fixe et mobile ainsi que l'accès à Internet, soulignant son importance pour la connectivité dans le pays. La structure organisationnelle de Mauritel a également été présentée, montrant comment elle s'organise pour répondre aux besoins des clients et relever les défis du secteur.

Partie 2 : Cadre d'Analyse du Projet

I. Introduction

Dans cette partie, nous analysons le cadre actuel du projet en examinant son contexte, ses objectifs, et les problématiques rencontrées. Cette analyse critique nous permettra de proposer une méthodologie structurée et d'élaborer une solution adaptée aux besoins identifiés.

II. Étude de l'existence

L'étude de l'existant consiste à analyser l'infrastructure actuelle de Mauritel. L'entreprise dispose de Datacenters interconnectés à travers le pays via des réseaux LAN et WAN de type IP/MPLS. Ces Datacenters abritent divers serveurs basés sur les technologies Microsoft, Linux, VMware, ainsi que des bases de données Oracle, MySQL et MS-SQL. Le réseau utilise une architecture Fortinet pour assurer la sécurité, avec des pare-feux, des switchs d'accès, et des solutions de supervision IP-Sensor. Cette analyse permet de comprendre les équipements, les technologies et les configurations en place, formant la base de notre projet d'optimisation.

III. Critique de l'existence

Après l'analyse de l'existant, plusieurs limitations ont été identifiées. Bien que l'infrastructure réseau actuelle permette une connectivité large, des problèmes de performance subsistent, notamment des goulots d'étranglement et des congestions. La gestion du trafic et la surveillance de sécurité peuvent être renforcées, et certains équipements pourraient être optimisés pour réduire la latence et améliorer la bande passante. Ces observations indiquent une opportunité d'amélioration dans la structure actuelle pour mieux répondre aux besoins de l'entreprise.

IV. Contexte et problématique

La croissance de l'activité de Mauritel et l'expansion de ses services imposent une exigence accrue en termes de performance et de sécurité réseau. La problématique principale réside dans l'optimisation des performances réseau pour garantir une connectivité fiable et rapide tout en répondant aux attentes croissantes des utilisateurs et des applications critiques. Face aux limitations de l'infrastructure actuelle, le défi est de trouver des solutions pour maximiser l'efficacité du réseau, assurer la sécurité, et offrir une expérience utilisateur optimale.

V. Objectifs du projet

Ce projet vise à améliorer les performances du réseau de Mauritel à travers une approche en plusieurs étapes. Les objectifs principaux sont :

1. Auditer l'infrastructure actuelle pour identifier les problèmes de performance.
2. Proposer des solutions pour éliminer les goulots d'étranglement et améliorer la qualité de service (QoS).
3. Recommander des solutions pour optimiser le réseau, comme l'ajout de bande passante ou des configurations plus efficaces
4. Évaluer l'impact des améliorations afin de garantir des performances optimales et un environnement sécurisé.

VI. Structure du rapport

Le rapport est structuré pour offrir une analyse claire et progressive de notre démarche. Après une présentation de l'infrastructure existante, nous abordons une critique de ses faiblesses, suivie du contexte et des objectifs du projet. Les étapes de la méthodologie appliquée sont ensuite détaillées, et le rapport conclut par une évaluation des résultats et des recommandations pour le futur.

VII. Méthodologie

La méthodologie adoptée repose sur une analyse approfondie et une approche pratique. En utilisant des outils comme GNS3, VMware et Zabbix, nous avons conçu une topologie réseau intégrant un FortiGate pour la sécurité et un serveur Zabbix pour la surveillance continue. La méthodologie inclut la configuration de politiques de sécurité et de surveillance, la collecte de données de performance réseau, et l'évaluation des effets des optimisations sur la connectivité et la sécurité. Cette approche permet de vérifier et de valider les changements en conditions réelles.

VIII. Organisation des Travaux

Phase	Activités Principales	Durée Estimée
1. Planification et Préparation	-Réalisation d'entretiens avec les responsables. - Étude des documents existants. - Définition des objectifs et contraintes.	2 semaines
2. Création de l'Environnement	-Installation de VMware et GNS3 - Crédit des VMs - Configuration réseau - Installation des OS - Configuration de base	2 semaines
3. Installation et Surveillance avec Zabbix	-Installation du serveur et des agents -Création de déclencheurs pour les alertes.	2 semaines
4. Configuration des Services Sécurisés	- Mise en place d'un serveur AD et intégration LDAP avec FortiGate - Configuration du VPN IPSec pour accès sécurisé - Activation des services DNS, Web, et messagerie dans la DMZ.	4 semaines
5. Sécurisation et Prévention	- Activation IPS/IDS (protection DoS, antivirus, SQL injection, filtrage Web) - Simulation d'intrusions - Analyse des logs et réaction aux incidents.	5 semaines
6. Analyse et Optimisation	- Collecte et analyse des données réseau - Identification des goulets d'étranglement	2 semaines

7. Documentation et Clôture	- Rédaction de la documentation finale. - Préparation de la présentation. - Clôture du projet.	2 semaines
------------------------------------	--	------------

Tableau 1 : Planification

IX. Conclusion

Le projet a permis de concevoir une architecture réseau plus performante et sécurisée pour Mauritel. En centralisant la surveillance des équipements et en optimisant la gestion du trafic à travers FortiGate et Zabbix, les objectifs de performance et de sécurité sont atteints. Cette configuration offre un cadre adapté aux besoins actuels de l'entreprise et pose des bases solides pour répondre à ses futures exigences de connectivité et de sécurité.

Chapitre 2 : État de l'art et technologies utilisées

2.1 Introduction

Dans ce chapitre, nous allons aborder l'importance et le rôle des différents outils et systèmes utilisés dans le domaine de l'informatique. Nous examinerons en détail les systèmes de supervision, les outils de sécurité, les outils de simulation, ainsi que les outils de virtualisation.

Chaque section permettra de mieux comprendre comment ces technologies contribuent à la gestion, à la sécurité, et à l'efficacité des infrastructures informatiques, tout en mettant en lumière leur impact sur la performance globale d'un réseau d'entreprise.

2.2 Monitoring, surveillance réseau informatique

Le monitoring ou supervision est une activité de suivi qui permet de surveiller, analyser, rapporter, et alerter sur les dysfonctionnements des systèmes informatiques. Il aide à diagnostiquer rapidement les pannes et à anticiper les plantages des serveurs, équipements réseau ou services logiciels.

2.2.1 Les objectifs du monitoring

- **Surveillance des performances** : Mesurer en temps réel les ressources (CPU, mémoire, disque, bande passante) pour identifier et corriger les goulets d'étranglement.
- **Détection et gestion des incidents** : Déetecter rapidement les anomalies ou pannes avant qu'elles n'affectent les utilisateurs.
- **Assurer la disponibilité** : Garantir que les services critiques (sites web, bases de données, serveurs de messagerie) sont toujours disponibles.
- **Optimisation des ressources** : Identifier les ressources sous ou sur-utilisées pour optimiser leur allocation et éviter les coûts inutiles.
- **Analyse des tendances et prédition** : Utiliser les données historiques pour analyser les tendances de performance à long terme.
- **Sécurité** : Déetecter les tentatives d'intrusion, comportements anormaux, et surveiller les logs pour prévenir les failles de sécurité.
- **Conséquences de l'absence de supervision**
 - Ne pas détecter les attaques (brute force, DoS, etc.).
 - Subir des interruptions de service prolongées.
 - Mauvaise gestion des ressources, entraînant une sous-utilisation ou surcharge.
 - Difficulté à identifier les causes des baisses de performance.
 - Incapacité à diagnostiquer les incidents en temps réel.
 - Non-respect des politiques de sécurité.
- **Importance de la configuration** : La simple installation de l'outil ne suffit pas. Il est essentiel de configurer le monitoring pour surveiller la disponibilité, la vitesse et l'utilisation des ressources réseau. La supervision fournit une vision claire des équipements et alerte l'administrateur avant que les problèmes n'impactent les utilisateurs, assurant une exploitation maximale des ressources à moindre coût et garantissant un service de qualité.

⊕ Domaines de surveillance :

- Surveillance des performances réseau : Bande passante, latence.
- Surveillance des serveurs : CPU, mémoire, disques.
- Surveillance des équipements réseau : Routeurs, commutateurs, pare-feu.
- Surveillance de la sécurité : Détection d'intrusions, analyse des journaux.
- Surveillance des logs : Événements et comportements anormaux.
- Surveillance des services et applications : Disponibilité, performances.
- Surveillance des utilisateurs : Activités suspectes.
- Surveillance des ressources système : Gestion et anticipation des besoins.

2.2.2 Outils de Monitoring

Les outils de supervision varient en fonction des besoins et de l'impact économique, avec des solutions gratuites et payantes.

2.2.2.1 Les Plateformes Éditeurs

- **SolarWinds (NPM)** : Surveille les performances réseau dans les environnements hybrides, détecte et résout les problèmes pour assurer un fonctionnement ininterrompu.
- **PRTG Network Monitor** : Supervision des réseaux pour infrastructures petites et moyennes, adapté aux environnements OT et IoT, évolutif sur serveurs Windows.

2.2.2.2 Les plateformes libres :

Il existe des solutions de supervision libres et professionnelles. L'avantage de ces logiciels libres réside dans leur gratuité, la disponibilité du code source, ainsi que la liberté d'étudier, de modifier le code selon nos besoins, et de le redistribuer.

De plus, une communauté d'utilisateurs et de développeurs très active contribue à l'amélioration continue de ces logiciels, offrant ainsi une assistance précieuse via des documentations en ligne et des forums d'entraide.

Parmi les outils les plus répandus et reconnus actuellement, nous pouvons citer Nagios, Zabbix et GLPI/OOC :

2.2.2.2.1 Nagios :

Outil de supervision open-source avec une vue complète de l'infrastructure IT. Il est flexible, extensible via des plugins, mais son interface est vieillissante et sa configuration complexe. (1)

Avantages:

- Surveille serveurs, services, applications avec alertes en temps réel.
- Extensible avec de nombreux plugins.

Inconvénients:

- Configuration complexe via fichiers texte.
- Interface obsolète et gestion fragmentée.

2.2.2.2 Zabbix

Zabbix est un logiciel de supervision informatique gratuit et open source, développé en 2001. Il repose sur une architecture monolithique, ce qui signifie que toutes ses fonctionnalités principales (collecte d'informations, traitement, stockage, etc.) sont intégrées dans une seule et même application cohérente. Grâce à cette conception, ses différents composants fonctionnent de manière fluide et harmonieuse via une interface unique qui centralise l'ensemble des données et processus.

Zabbix se distingue par sa capacité à effectuer une supervision élargie. En effet, il ne se limite pas uniquement à surveiller la disponibilité des services ou à déclencher des alertes en cas d'incident. Il est également fortement orienté vers la gestion des performances des systèmes et des réseaux, ce qui en fait un outil complet pour le monitoring et l'optimisation des infrastructures IT. (2)

Avantages :

- Personnalisation et flexibilité : Zabbix permet de créer des tableaux de bord et des configurations hautement personnalisables, adaptés aux besoins spécifiques des utilisateurs.
- Surveillance en temps réel : Les tableaux de bord offrent une visualisation en temps réel des métriques clés, facilitant le suivi des performances.
- Interface intuitive : Son interface moderne et simple d'utilisation rend la configuration et le déploiement de solutions de surveillance plus accessibles.
- Support professionnel : Zabbix propose des services de support (technique, formation, etc.) pour une prise en main rapide et efficace de l'outil.

Inconvénients :

- Complexité d'utilisation : Zabbix peut être difficile à configurer et à exploiter, surtout pour les utilisateurs novices.
- Documentation technique : Bien qu'elle soit étendue, la documentation peut être compliquée à comprendre.
- Performance : Dans les environnements très larges, une gestion précise des ressources est nécessaire pour maintenir des performances optimales.
- Absence de version entreprise : Contrairement à d'autres solutions, Zabbix ne propose pas de version entreprise spécifique.

2.2.2.3 GLPI/OCS :

GLPI gère les ressources IT et les tickets d'assistance, tandis qu'OCS Inventory effectue l'inventaire automatique des équipements.

Avantages :

- Gratuit, gestion centralisée, intégration avec OCS Inventory.

Inconvénients :

- Complexité d'installation et documentation parfois limitée.

2.2.3 Etude comparatif

La comparaison générale des outils de supervision open source précédemment cités a été réalisée en premier lieu à l'aide d'un diagramme radar, selon les critères suivants :

- Personnalisation.
- Facilité de configuration.
- Communauté/Soutien.
- Gestion des performances.
- Surveillance en temps réel.
- Gestion centralisée.

2.2.3.1 Diagramme radar

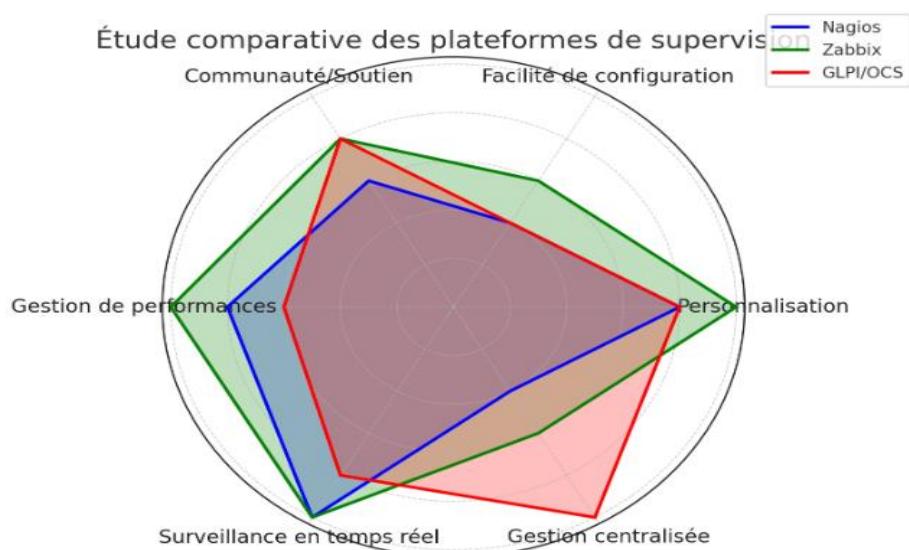


Figure 3 : Diagramme radar

2.2.3.2 Tableau comparatif

Critères	Nagios	Zabbix	GLPI/OCS
Fonctionnalités	Surveillance des hôtes, services, et applications avec alertes en temps réel. Extensible avec des plugins.	Supervision complète (serveurs, réseaux, applications) avec gestion avancée des performances.	Gestion de parc informatique (inventaire, tickets, interventions).
Support des protocoles	Supporte SNMP, ICMP, TCP, HTTP, et plus via plugins	Supporte SNMP, ICMP, TCP, HTTP, IPMI, JMX, et autres	Supporte SNMP, OCS Inventory pour gestion automatique des équipements

Chapitre 2 : État de l'art et technologies utilisées

Facilité d'installation	Installation et configuration complexes pour les débutants	Relativement complexe, surtout dans les grands environnements	Installation relativement simple, mais peut être complexe avec OCS Inventory
Coût	Gratuit (open source), sauf pour support commercial	Gratuit (open source), support professionnel payant disponible	Gratuit (open source), coûts pour support professionnel
Performances	Bonnes pour des infrastructures petites à moyennes.	Très performante pour la supervision en temps réel.	Limitée pour la supervision en temps réel.
Scalabilité	Scalabilité possible, mais nécessite des configurations avancées.	Très scalable avec proxies et gestion centralisée efficace.	Scalabilité limitée, surtout pour la surveillance réseau.
Intégrations	Large bibliothèque de plugins et intégrations avec d'autres outils (Centreon, Icinga)	Intégrations natives avec des solutions comme Grafana, Kubernetes, et autres	Intégration native avec OCS Inventory, plugins disponibles pour d'autres systèmes

Tableau 2 : Tableau comparatif de supervision

2.2.4 Choix de Plateforme

Raisons pour choisir Zabbix

- **Interface utilisateur moderne :** Facile à utiliser et personnalisable.
- **Autodécouverte :** Détecte automatiquement les nouveaux dispositifs.
- **Graphiques et tableaux de bord intégrés :** Outils de visualisation des données.
- **Évolutivité :** Adaptable aux réseaux de toutes tailles.
- **Open-source :** Gratuit et modifiable selon les besoins.
- **Communauté active :** Améliorations et extensions régulières.

2.2.4.1 Fonctionnement de Zabbix

Zabbix est une solution de supervision puissante et modulable, capable de surveiller des infrastructures complexes. Ses composants essentiels incluent :

- **Zabbix Server :** Gère la collecte et la gestion des données de supervision.
- **Zabbix Frontend :** Interface web en PHP pour la visualisation et la configuration.
- **Zabbix Proxy :** Réduit la charge du serveur principal, utile pour les sites distants.
- **Zabbix Agent :** Facultatif, améliore la supervision en collectant des données détaillées sur les hôtes.

2.2.4.2 Interactions entre les Composants

Zabbix est un système flexible et adaptable, facile à déployer dans différentes infrastructures, Zabbix permet ainsi une surveillance centralisée, adaptée aux environnements locaux et distants.

Les interactions entre ses composants sont essentielles pour bien comprendre son fonctionnement :

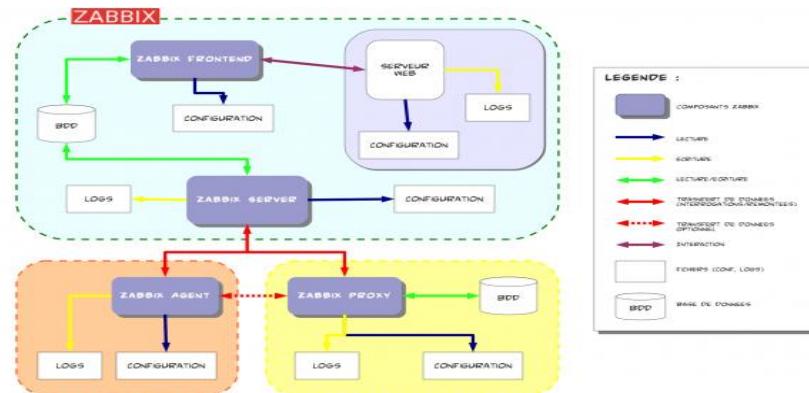


Figure 4 : Architecture de Zabbix

Les composants Zabbix sont organisés en trois parties distinctes :

- **Bloc Serveur Zabbix** : Comprend le Zabbix Server, qui collecte et gère les données de supervision, et le Frontend, une interface web pour la configuration et la visualisation en temps réel. Les informations sont stockées dans une base de données.
- **Bloc Agent** : Le Zabbix Agent, installé sur les hôtes supervisés, collecte des données locales (utilisation des ressources, état des services) et les transmet au serveur pour analyse.
- **Bloc Proxy** : Le Zabbix Proxy agit comme intermédiaire pour les réseaux distants, réduisant la charge du serveur principal en traitant les données localement avant de les envoyer.

2.2.4.3 Gestion des flux

Gestion des flux pour illustrer les protocoles et flux utilisés par les différents composants de la supervision Zabbix.

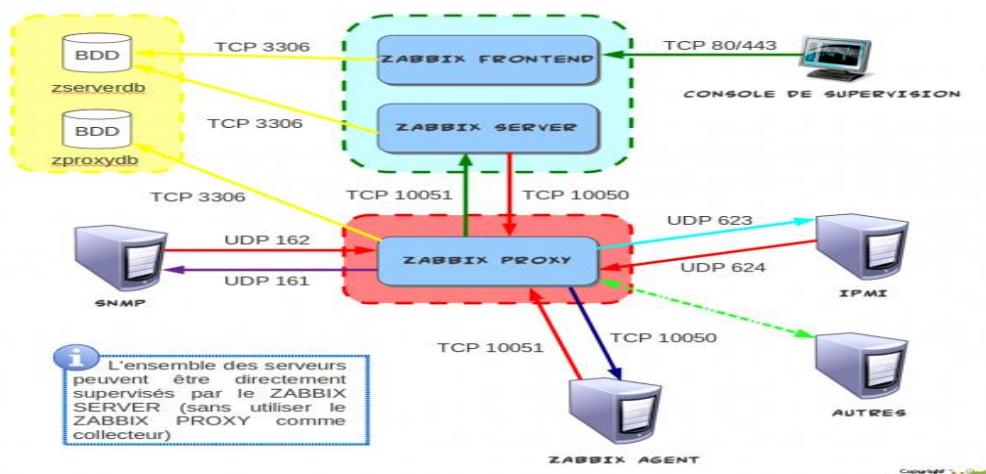


Figure 5 : Les Protocoles et Ports dans l'Architecture Zabbix

2.2.4.4 Checks actifs/passifs

- ❖ *Checks passifs*

Le serveur envoie une requête à l'agent pour collecter des données.

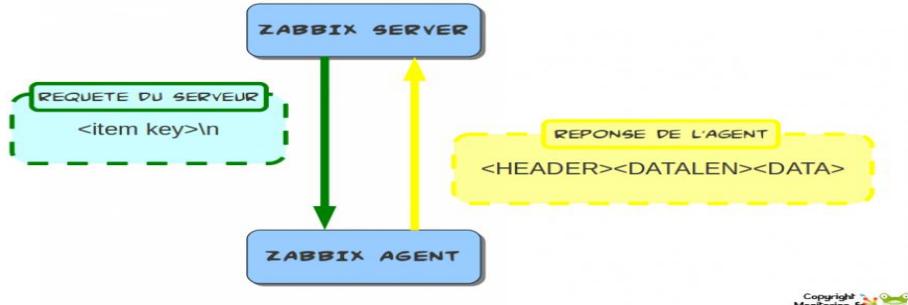


Figure 6 : Échange de Données du Serveur Zabbix à l'Agent Zabbix

- ❖ *Checks actifs*

L'agent envoie de manière périodique des données collectées au serveur.

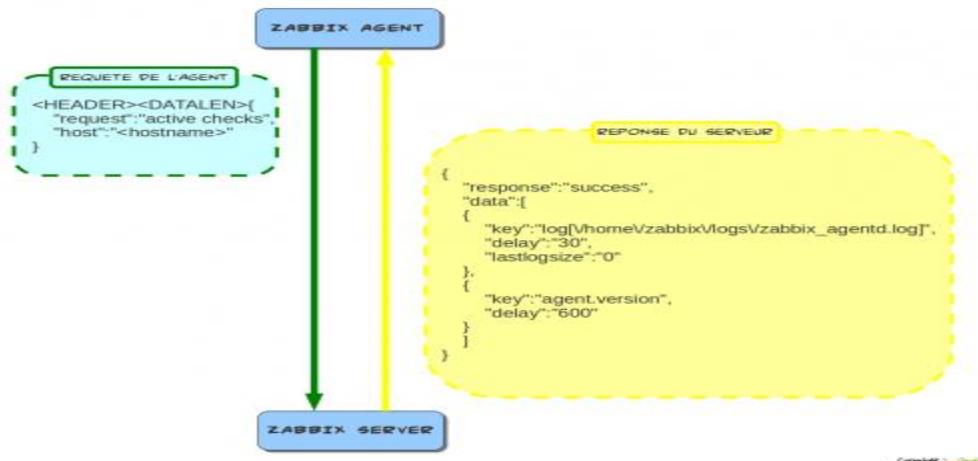


Figure 7 : Échange de Données de l'Agent au Serveur Zabbix

2.2.4.5 Système d'alerte

Zabbix génère des alertes en utilisant trois éléments essentiels :

- *Item* : Collecte des données spécifiques.
- *Trigger* : Réagit à certaines valeurs et génère des événements.
- *Action* : Envoie des notifications (email, SMS) selon des événements précis.

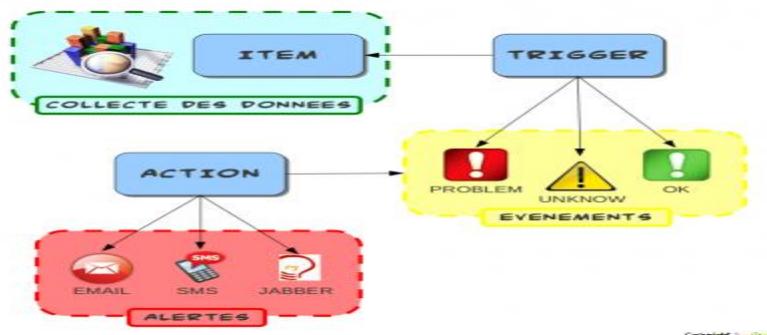


Figure 8 : Collecte des Données et Alertes

2.2.4.6 Architecture

- 1) **Mono-serveur** : Adapté aux petites entreprises, surveille des agents et équipements via un serveur unique.

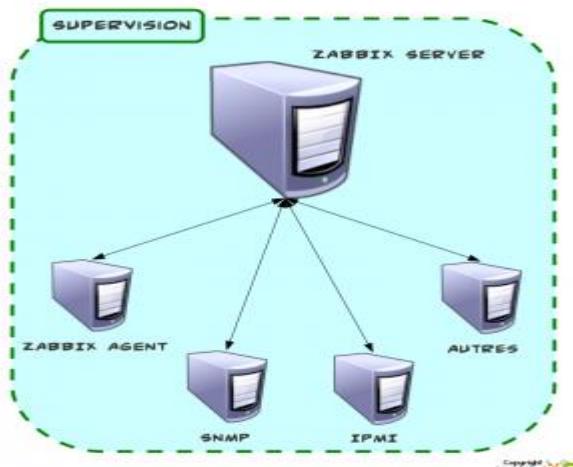


Figure 9 : Architecture mono-serveur

2) Distribuée

- **Multi-serveur** : Plusieurs serveurs dans différents sites pour une administration locale.

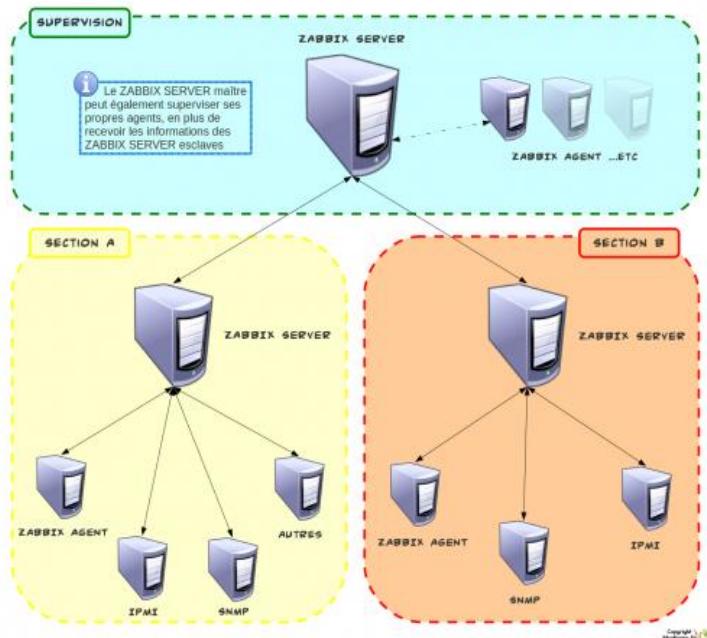


Figure 10 : Architecture Multi-serveur

Chapitre 2 : État de l'art et technologies utilisées

- *Multi-proxy* : Un seul serveur Zabbix avec plusieurs proxys pour la collecte de données de sites distants.

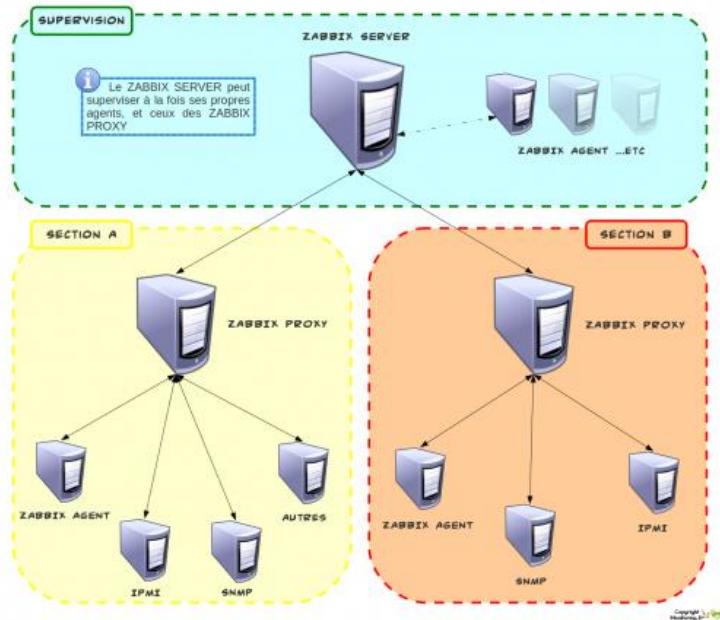


Figure 11 : Architecture Multi-proxy

- *Multi-serveur et Multi-proxy* : Combine serveurs et proxys pour une administration à la fois centralisée et décentralisée.

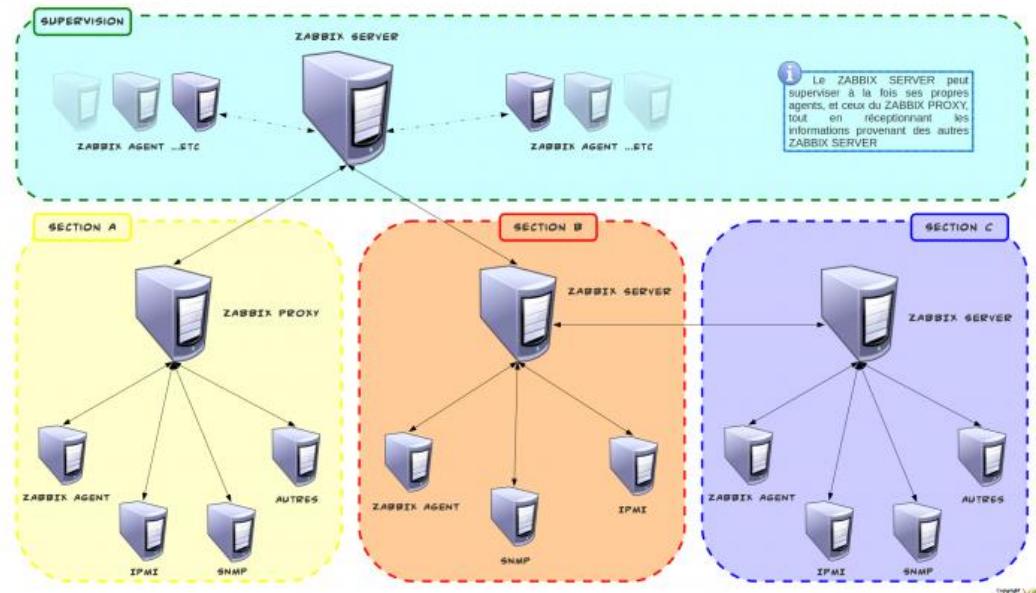


Figure 12 : Architecture Multi-serveur et Multi-proxy

2.3 Les systèmes de sécurité des réseaux

La sécurité des réseaux est un enjeu crucial à l'ère numérique. Cette section examine différentes solutions de supervision et de sécurité réseau, en mettant en avant les fonctionnalités, avantages et inconvénients des pare-feux et des systèmes de prévention des intrusions.

2.3.1 IPFire

IPFire est un système open-source basé sur Linux, conçu pour la sécurité réseau, agissant comme pare-feu, routeur, proxy et VPN.



Figure 13 : Logo d'IPFire

Fonctionnalités clés

- Pare-feu SPI pour un filtrage sécurisé.
- Réseaux segmentés avec des zones (Rouge, Vert, Bleu, Orange).
- Support de VPN (IPsec, OpenVPN).
- Proxy et cache intégrés.
- IDS pour détecter les intrusions.

Avantages

- Interface web intuitive.
- Modularité avec extensions.
- Sécurité renforcée grâce au pare-feu SPI.
- Faible consommation de ressources.

Inconvénients

- Complexité pour les novices.
- Performances dépendantes du matériel.
- Maintenance régulière nécessaire.

2.3.2 pfSense

pfSense est un système open-source basé sur FreeBSD, utilisé comme pare-feu et routeur, réputé pour sa fiabilité et ses fonctionnalités avancées.



Figure 14 : Logo de pfSense

Fonctionnalités clés

- Filtrage IP et port pour un contrôle granulaire.
- NAT pour la gestion du trafic réseau.
- VPN (IPsec, OpenVPN).
- QoS pour prioriser les flux critiques.
- Monitoring et statistiques via une interface graphique.

Avantages

- Flexibilité et nombreuses fonctionnalités.
- Interface web intuitive.
- Solution économique, gratuite.

Inconvénients

- Complexité pour les débutants
- Interface utilisateur dense en options.
- Maintenance et support communautaires peuvent être limités.

2.3.3 FortiGate :

FortiGate est un dispositif de sécurité réseau de la société Fortinet, utilisé pour superviser et sécuriser les infrastructures réseau. Il intègre plusieurs fonctions de sécurité pour protéger contre les cybermenaces et assurer la continuité des opérations. (3)



Figure 15 : Logo de FortiGate

Chapitre 2 : État de l'art et technologies utilisées

Contexte et Historique : Fondée en 2000, Fortinet s'est rapidement imposée comme un leader de la sécurité réseau grâce à ses solutions innovantes. Les pare-feux FortiGate ont été introduits pour répondre au besoin croissant de solutions de sécurité intégrées et robustes, capables de contrer les menaces évoluées. L'architecture unique de FortiGate repose sur des processeurs ASIC (Application-Specific Integrated Circuit) dédiés, conçus pour optimiser les performances de traitement des paquets et de la sécurité.

Fonctionnalités Clés

Les pare-feux FortiGate se distinguent par leurs fonctionnalités avancées :

- Pare-feu : FortiGate agit en tant que pare-feu de nouvelle génération, filtrant le trafic entrant et sortant pour prévenir les accès non autorisés.
- Système de prévention des intrusions (IPS) : Il détecte et empêche les activités malveillantes sur le réseau grâce à des signatures et des techniques de détection basées sur des anomalies.

Avantages

- Performance Élevée : FortiGate utilise des processeurs spécialisés en sécurité, comme le processeur NP7, pour une analyse rapide et efficace des paquets.
- Convergence Réseau : Les solutions FortiGate intègrent plusieurs fonctions de sécurité en un seul appareil, simplifiant la gestion et réduisant les coûts.
- Protection Avancée : Des fonctionnalités telles que l'inspection approfondie des paquets, le filtrage des applications et la prévention des intrusions offrent une sécurité robuste.
- Scalabilité : Les pare-feux FortiGate sont facilement extensibles pour répondre aux besoins croissants des entreprises.

Inconvénients

- Complexité de Configuration : La configuration initiale et la gestion des pare-feux FortiGate peuvent être complexes, nécessitant une expertise technique.
- Coût : Les solutions FortiGate peuvent être coûteuses, notamment pour les petites et moyennes entreprises.
- Maintenance : La maintenance et les mises à jour régulières des pare-feux exigent des ressources et du temps.

2.3.4 Tableau comparatif :

Critères	IPFire	pfSense	FortiGate
Type	Open-source (Linux)	Open-source (FreeBSD)	Propriétaire (NGFW)
Pare-feu	SPI	Filtrage IP/port	DPI
Zones de sécurité	Segmentées (Rouge, Vert...)	Manuelles	Avancées
VPN	IPsec, OpenVPN	IPsec, OpenVPN	IPsec, SSL, SD-WAN VPN
QoS	Non spécifié	Oui	Oui
IDS/IPS	IDS intégré	Via plugins	IPS intégré
Proxy	Oui, avec cache	Non	Non (contrôle applicatif)

Interface	Intuitive	Complexe	Avancée
Modularité	Extensions disponibles	Très modulaire	Solution tout-en-un
Performances	Faible conso. Ressources	Stabilité robuste	Haute performance (ASIC)
Scalabilité	Limité	Très flexible	Très scalable
Coût	Gratuit	Gratuit	Coût élevé
Maintenance	Fréquente, manuelle	Régulière, technique	Régulière, nécessite ressources
Support	Communautaire	Communautaire	Commercial

Tableau 3 : Tableau comparatif des pare-feux

2.3.5 Choix préférentiel :

Raisons pour choisir FortiGate

- **Performance élevée** grâce à des composants spécialisés.
- **Sécurité avancée** contre une variété de menaces informatiques.
- **Scalabilité** pour s'adapter aux besoins des réseaux de différentes tailles.
- **Facilité de gestion** avec une administration centralisée.
- **Intégration** avec d'autres solutions Fortinet pour une protection complète.

2.4 Surveillance des services critiques et optimisation réseau (QoS)

2.4.1 Supervision des Services Critiques

- Continuité des Activités : La supervision garantit la disponibilité des services critiques, même en cas de panne ou d'attaque, grâce à des outils de surveillance et des alertes en temps réel permettant de résoudre rapidement les problèmes.
- Sécurité des Données : Elle détecte proactivement les menaces sur les données sensibles et permet aux administrateurs de les contrer avant qu'elles ne causent des dommages.
- Performance et Fiabilité : La surveillance continue aide à identifier les problèmes de performance, à optimiser les ressources et à améliorer la fiabilité des services.

2.4.2 Mécanismes d'Optimisation comme la QoS

- Allocation des Ressources : La QoS priorise le trafic réseau pour assurer que les services critiques reçoivent les ressources nécessaires.
- Réduction de la Latence : Elle minimise les délais de transmission, essentiel pour les services en temps réel, comme dans les secteurs financiers ou de la santé.
- Amélioration de l'Expérience Utilisateur : La QoS réduit les interruptions et améliore la qualité des services pour une meilleure satisfaction des utilisateurs.
- Gestion de la Bande Passante : Elle contrôle l'utilisation de la bande passante pour éviter la congestion et assurer une performance stable pour tous les services.

2.5 Approches de détection des intrusions et des menaces

La détection des intrusions et des menaces dans les réseaux informatiques est cruciale pour protéger les données sensibles et garantir la sécurité des systèmes.

2.5.1 Systèmes de Détection d'Intrusion (IDS) :

- IDS basés sur les signatures : Ces systèmes comparent le trafic réseau à des signatures connues d'attaques pour détecter des menaces. Ils sont efficaces contre les attaques déjà répertoriées.
- IDS basés sur les anomalies : Ils surveillent les activités réseau pour identifier les comportements anormaux qui pourraient indiquer une intrusion. Ils sont utiles pour détecter des attaques nouvelles ou inconnues. (4)

2.5.2 Systèmes de Prévention d'Intrusion (IPS) :

Similaires aux IDS, mais avec la capacité d'intervenir activement pour bloquer les menaces détectées en temps réel. (5)

2.5.3 Gestion des événements de sécurité (SIEM)

Collectent et analysent les données de sécurité provenant de différentes sources pour fournir une vue d'ensemble et détecter des anomalies ou des intrusions.

2.6 Technologies de pare-feu et VPN dans les réseaux d'entreprise

Les technologies de pare-feu et VPN sont essentielles pour la protection des réseaux d'entreprise. FortiGate est une solution qui combine ces deux fonctionnalités, offrant une protection complète et sécurisée.

2.6.1 Pare-feu FortiGate

- Filtrage des paquets : FortiGate analyse chaque paquet de données entrant et sortant pour vérifier son intégrité et sa conformité avec les politiques de sécurité définies.
- Inspection approfondie des paquets (DPI) : Il va au-delà du simple filtrage pour inspecter les données à un niveau plus granulaire, détectant et bloquant les menaces cachées dans le trafic légitime.
- Contrôle des applications : FortiGate permet de gérer et de contrôler l'accès aux applications, empêchant l'utilisation de celles non autorisées et minimisant les risques associés.

2.6.2 VPN FortiGate

- VPN Site-à-Site : FortiGate établit des connexions sécurisées entre différents sites de l'entreprise, permettant une communication sécurisée et fiable.
- VPN SSL : Il fournit un accès distant sécurisé aux utilisateurs, leur permettant de se connecter au réseau de l'entreprise depuis n'importe où tout en garantissant la confidentialité des données transmises.
- VPN IPsec : FortiGate utilise des protocoles IPsec pour chiffrer le trafic réseau, assurant que les données restent confidentielles et protégées contre les interceptions.

Dans ce projet, FortiGate est utilisé pour mettre en place des pare-feux robustes et des VPN sécurisés, assurant la protection périphérique du réseau et la sécurisation des communications entre les différents sites et utilisateurs distants. Ces technologies contribuent à renforcer la résilience du réseau face aux menaces externes et internes.

2.7 Outils de simulation et virtualisation

La simulation et la virtualisation : Deux concepts essentiels dans le monde de l'informatique et des technologies modernes.

- **Simulation :** La simulation modélise des phénomènes réels dans un environnement virtuel, permettant de tester, comprendre ou prédir le comportement de systèmes sans avoir à les construire physiquement.
- **Virtualisation :** La virtualisation consiste à créer des versions virtuelles de serveurs ou systèmes, optimisant ainsi l'utilisation des ressources matérielles en faisant tourner plusieurs systèmes sur une seule machine. Elle offre efficacité, flexibilité, économies de coûts, et améliore la sécurité en isolant les environnements.

2.7.1 Les outils de simulation :

De nombreux outils de simulation existent, parmi lesquels on peut citer :

- Cisco Packet Tracer : Un outil gratuit spécifiquement conçu pour l'enseignement et l'apprentissage des réseaux Cisco.
- Cisco VIRL (Virtual Internet Routing Lab) : Proposé par Cisco, il permet de simuler des environnements réseau complexes.
- GNS3 (Graphical Network Simulator-3) : Un outil de simulation de réseau qui permet de créer et de tester des topologies réseau virtuelles. Il est largement utilisé pour l'apprentissage et le développement de compétences en réseau. (6)

Fonctionnalités principales de GNS3 :

- Simulation de réseaux : Permet de créer des topologies réseau avec des routeurs, des commutateurs et d'autres dispositifs réseau.
- Émulation de dispositifs Cisco : Utilise Dynamips pour émuler des routeurs Cisco, permettant de tester des configurations et des protocoles de routage.
- Intégration avec VMware et VirtualBox : Permet de connecter des machines virtuelles hébergées par VMware ou VirtualBox à des topologies réseau simulées dans GNS3.

Chapitre 2 : État de l'art et technologies utilisées

- Interface intuitive : Offre une interface graphique conviviale pour la conception et la gestion des réseaux.

Avantages de GNS3 :

- Simulation réseau : Idéal pour simuler des architectures réseau et des configurations de routeurs.
- Open source : Gratuit et open source, avec une communauté active.
- Compatibilité : Intégration avec des émulateurs comme Dynamips pour simuler du matériel Cisco.

Inconvénients de GNS3 :

- Limité à la simulation réseau : Il ne propose pas de fonctionnalités de virtualisation de serveurs.
- Interface complexe : Peut-être intimidant pour les débutants.

2.7.2 Choix préférentiel :

GNS3 est un outil de simulation réseau très polyvalent qui permet de simuler différents dispositifs réseau comme des routeurs et des commutateurs. Il est open source et gratuit, accessible à tous. Compatible avec Windows, macOS et Linux, il peut être utilisé avec VMware et VirtualBox. GNS3 bénéficie également d'une communauté active, offrant un support et des ressources abondantes.



Figure 16 : Logo de GNS3

2.7.3 Les outils de virtualisation :

Il existe de nombreux outils de virtualisation, parmi lesquels on peut citer :

- Oracle VM VirtualBox : Gratuit et open source, il supporte plusieurs systèmes d'exploitation.
- Microsoft Hyper-V : Gratuit avec Windows Server, il est intégré à l'écosystème Microsoft.
- VMware Workstation Pro : Un logiciel de virtualisation puissant qui permet d'exécuter plusieurs systèmes d'exploitation sur une seule machine physique. Il est largement utilisé par les développeurs, les professionnels de l'informatique et les entreprises pour tester, développer et déployer des logiciels sur différentes plateformes.

Fonctionnalités clés de VMware Workstation Pro :

- Exécution de multiples systèmes d'exploitation : Permet d'exécuter plusieurs systèmes d'exploitation simultanément sur le même PC.
- Support des dernières versions de Windows : Compatible avec les dernières versions de Windows, y compris Windows 11. (7)
- Mise à jour et installation à distance : Offre la possibilité de mettre à jour et d'installer des machines virtuelles (VMs) à distance.

Chapitre 2 : État de l'art et technologies utilisées

- Chiffrement des VMs : Propose des options de chiffrement pour sécuriser les VMs.
- Surveillance des VMs : Permet de surveiller les VMs pour détecter les problèmes et optimiser les performances.

Avantages de VMware Workstation Pro :

- Polyvalence : Supporte plusieurs systèmes d'exploitation (Windows, Linux, macOS).
- Performance : Haute performance avec des fonctionnalités avancées telles que vMotion et Live Migration.
- Sécurité : Offre des solutions robustes de sauvegarde et de récupération.
- Interface conviviale : L'interface utilisateur est intuitive et facile à utiliser.

Inconvénients de VMware Workstation Pro :

- Coût : Les licences peuvent être coûteuses.
- Complexité : Peut nécessiter une courbe d'apprentissage pour les utilisateurs novices.

2.7.4 Choix préférentiel :

VMware Workstation Pro se distingue par sa polyvalence, sa compatibilité avec divers systèmes d'exploitation (Windows, Linux, macOS), ses fonctionnalités avancées comme la gestion des instantanés et le support graphique, et par ses mesures de sécurité qui isolent les machines virtuelles. Enfin, sa compatibilité avec les processeurs Intel et AMD 64 bits en fait une solution flexible et robuste pour la virtualisation.



Figure 17 : Logo de VMWare

2.8 Trello

Trello est un outil de gestion de projet en ligne qui permet d'organiser des tâches à l'aide de tableaux, de listes et de cartes. Chaque carte représente une tâche ou un élément à accomplir, et peut être assignée à un utilisateur spécifique, tout en étant déplacée d'une liste à une autre pour indiquer son état d'avancement. Inspiré de la méthode Kanban, il facilite la collaboration et le suivi des projets en temps réel. (8)



Figure 18 : Logo de Trello

2.9 Conclusion

Ce chapitre a fourni un panorama exhaustif des systèmes et outils de supervision, des mécanismes de sécurité et des technologies de virtualisation et de simulation. Nous avons exploré les définitions et objectifs des systèmes de supervision, la présentation de divers outils comme Zabbix et Nagios, et les technologies de sécurité telles que SIEM, IDS, IPS et FortiGate. Nous avons également discuté de l'importance de la surveillance des services critiques et de l'optimisation réseau avec la qualité de service (QoS). Enfin, nous avons abordé les approches de détection des intrusions et des menaces, les technologies de pare-feu et VPN, ainsi que les outils de simulation et de virtualisation comme VMware et GNS3. Trello a également été évoqué comme un outil de gestion de projet permettant de suivre efficacement l'avancement des tâches au sein de ces processus. Ce socle théorique établit les fondations nécessaires pour une compréhension approfondie et une mise en œuvre efficace des solutions de supervision et de sécurité des réseaux dans un contexte d'entreprise.

Chapitre 3 : Mise en place du réseau et configuration des systèmes

3.1 Introduction

Dans ce chapitre, nous avons mis en place une infrastructure réseau virtualisée et sécurisée pour simuler un environnement d'entreprise, spécifiquement pour l'entreprise Mauritel. En utilisant VMware Workstation et GNS3, nous avons créé une topologie incluant des machines virtuelles sous Ubuntu et Windows, un serveur Zabbix pour la surveillance, et un pare-feu FortiGate pour sécuriser le réseau segmenté en trois zones : WAN, DMZ et LAN. Nous avons également intégré un serveur Active Directory pour la gestion centralisée des utilisateurs, configuré FortiGate pour l'authentification LDAP et déployé un VPN sécurisé par IPSec pour permettre un accès distant sécurisé aux ressources de l'entreprise Mauritel.

3.2 Déploiement de l'infrastructure réseau

Cette section décrit l'installation de VMware Workstation, GNS3, et la configuration de Zabbix et FortiGate pour créer une infrastructure réseau sécurisée, avec des machines virtuelles et un accès distant via VPN.

3.2.1 Installation et Configuration de VMware Workstation

Après avoir téléchargé l'installateur de VMware Workstation, exécutez-le et suivez les étapes simples pour finaliser l'installation.

- Cliquez sur **Next** pour commencer l'installation :



Figure 19 : Début de l'installation de VMWare

- Acceptez le contrat de licence et cliquez sur **Next**

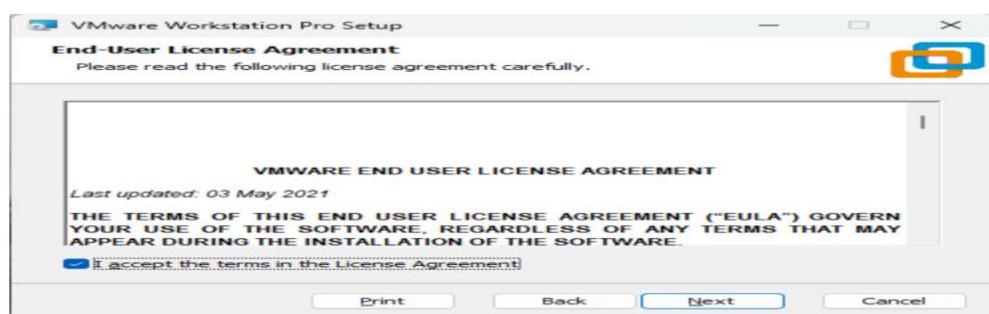


Figure 20 : Acceptation du contrat de licence

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- La seconde l'option ajoute VMware à la variable PATH, permettant d'utiliser vctl.exe en ligne de commande, cliquez sur **Next**

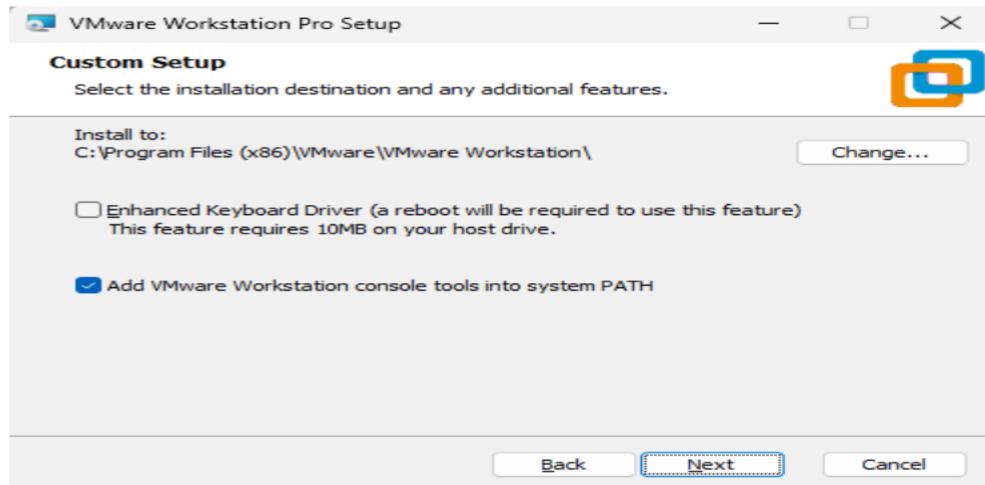


Figure 21 : Ajout à la variable PATH

- Poursuivez...

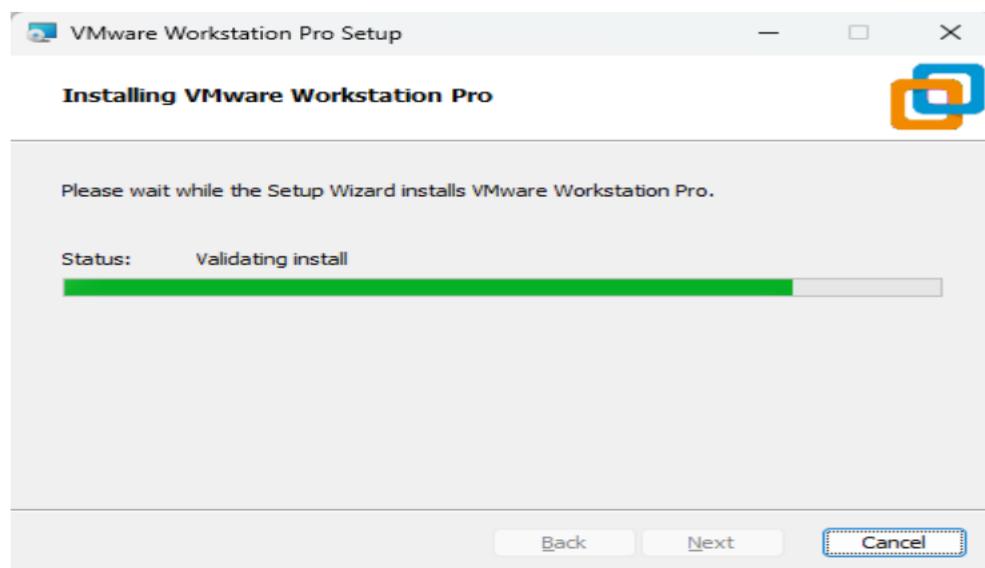


Figure 22 : Installation en cours

- Après l'installation, ouvrez la console de gestion de VMware Workstation

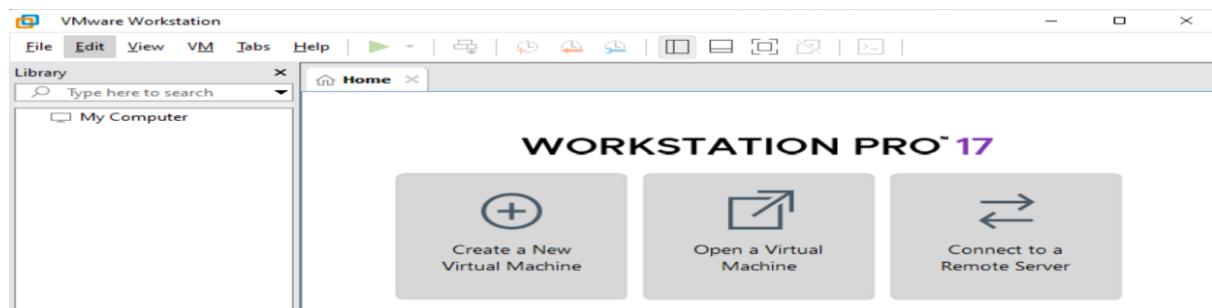


Figure 23 : Interface de VMware

3.2.2 Installation et configuration de GNS3

- L'installation de GNS3 nécessite la création d'un compte sur le site officiel. Une fois le compte créé, connectez-vous :

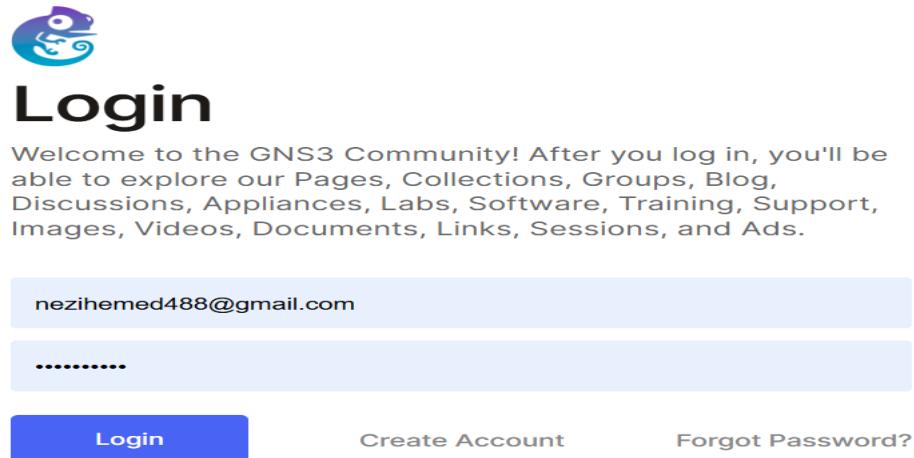


Figure 24 : Création de compte GNS3

- Une fois connecté, accédez aux liens de téléchargement pour Windows.



Figure 25 : Connexion au site GNS3

- La première boîte de dialogue recommande de fermer les applications ouvertes. Cliquez sur « Suivant » pour continuer.



Figure 26 : Démarrage de l'installation

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Acceptez la licence en cliquant sur « I Agree » pour continuer.

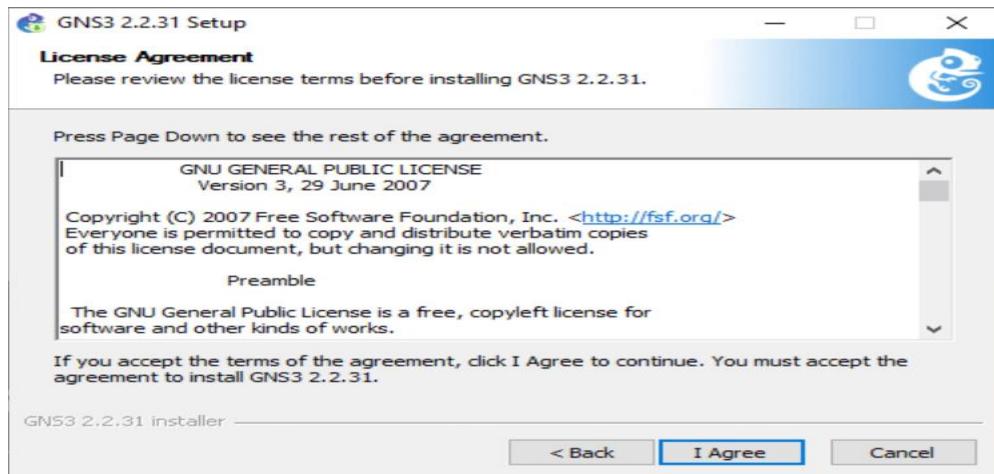


Figure 27 : Acceptation de la licence

- Sélectionnez les composants à installer : le client lourd, le client léger (web client) et la machine virtuelle.

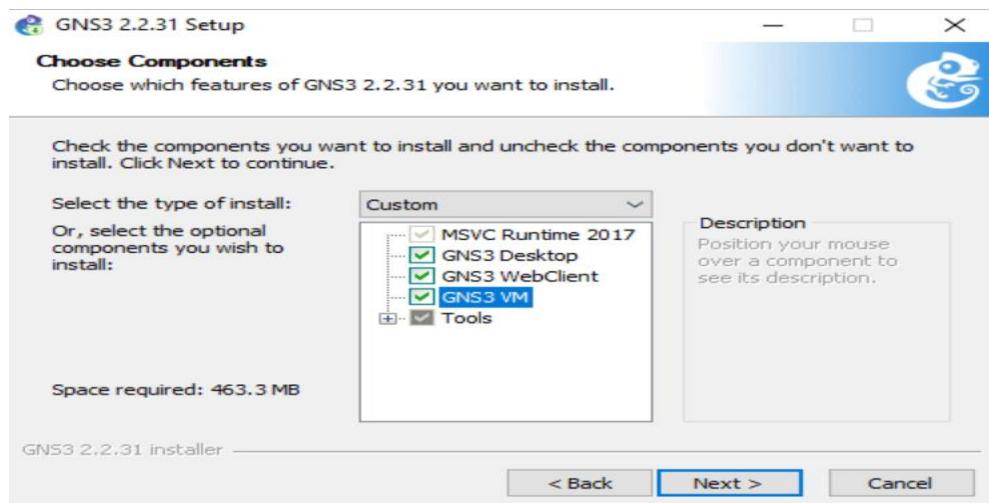


Figure 28 : Sélection des composants

- Sélectionnez « VMware Workstation » comme hyperviseur pour exécuter la GNS3 VM.

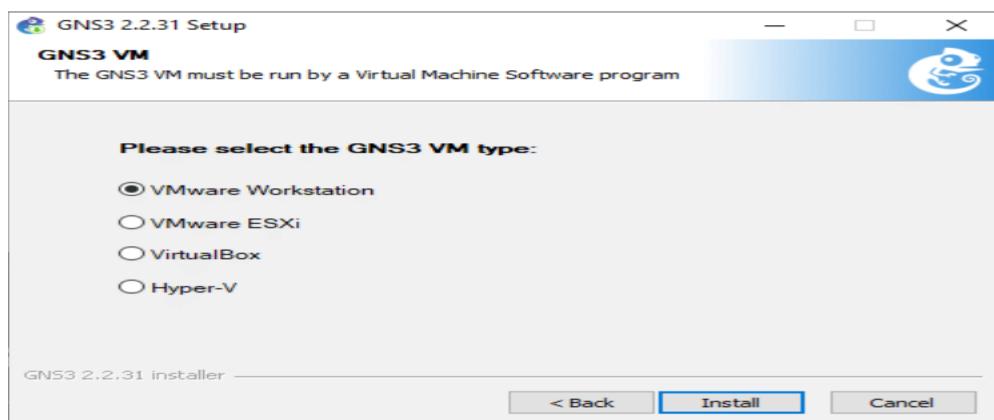


Figure 29 : Choix de VMware Workstation

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- L'installation commence avec le téléchargement de la machine virtuelle.

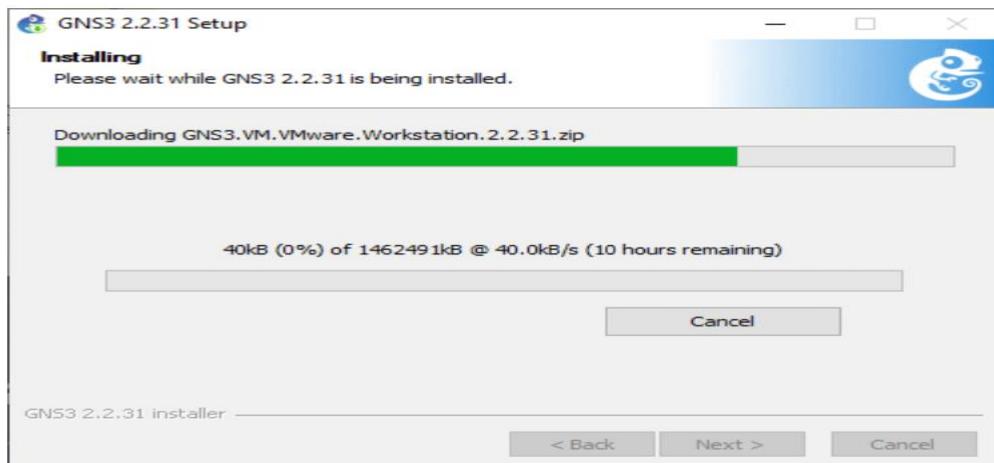


Figure 30 : Téléchargement de la VM GNS3

- À la fin du téléchargement, une boîte de dialogue vous indiquera le chemin du fichier.

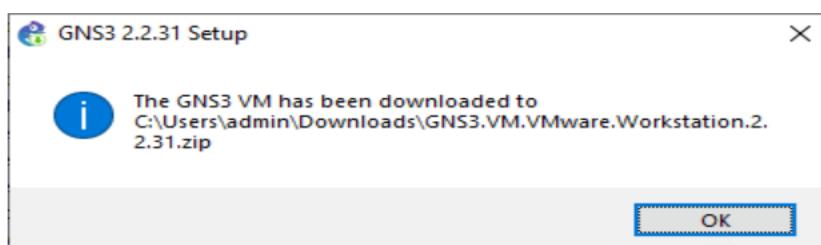


Figure 31 : Chemin de la VM téléchargée

- Installez WinPCAP pour ajouter une couche réseau de bas niveau, en laissant les valeurs par défaut.

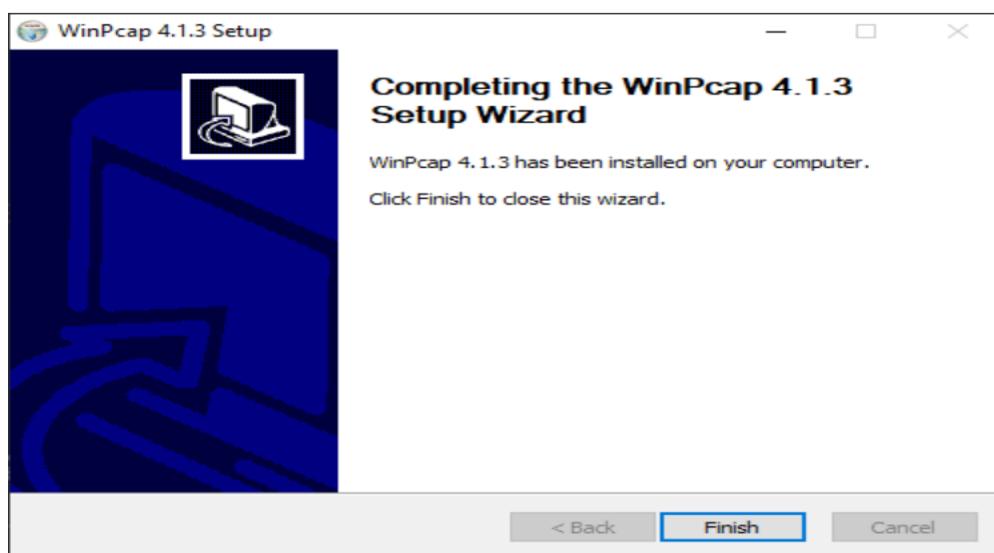


Figure 32 : Installation de WinPCAP

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Installez Npcap pour la capture de trames, en laissant les valeurs par défaut.

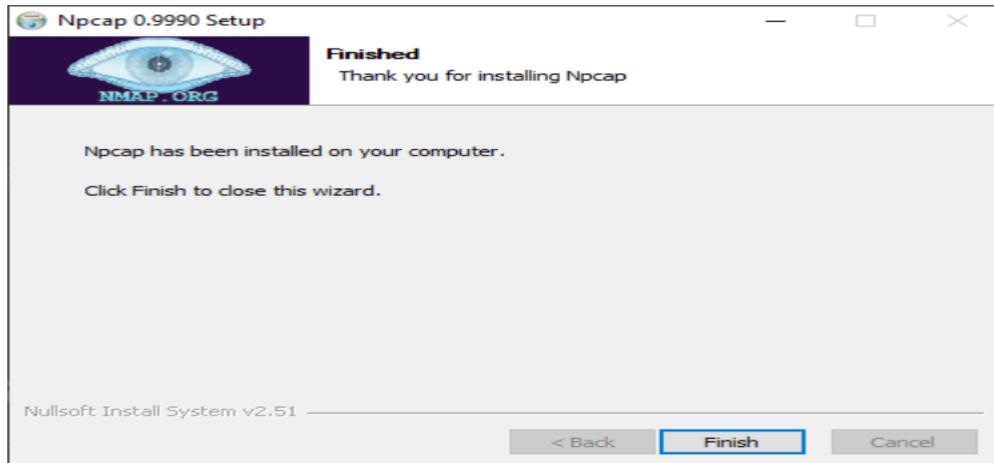


Figure 33 : Installation de Npcap

- Installez Solar-Putty pour paramétriser les équipements GNS3, puis acceptez les conditions et cliquez sur **Accept**

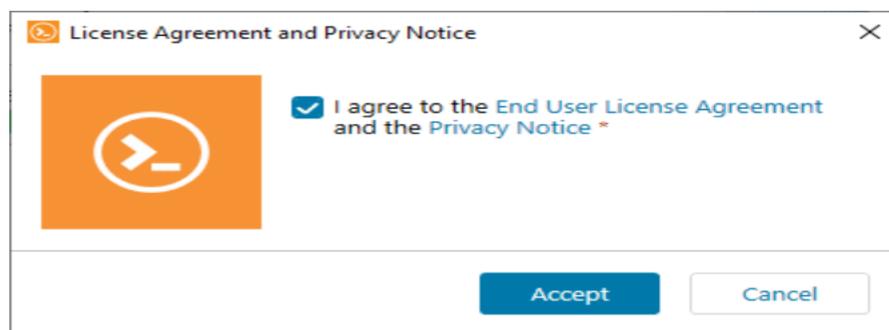


Figure 34 : Installation de Solar-Putty

- Après l'installation de Solar-Putty, cochez « No » pour l'outil supplémentaire et cliquez sur **Next**

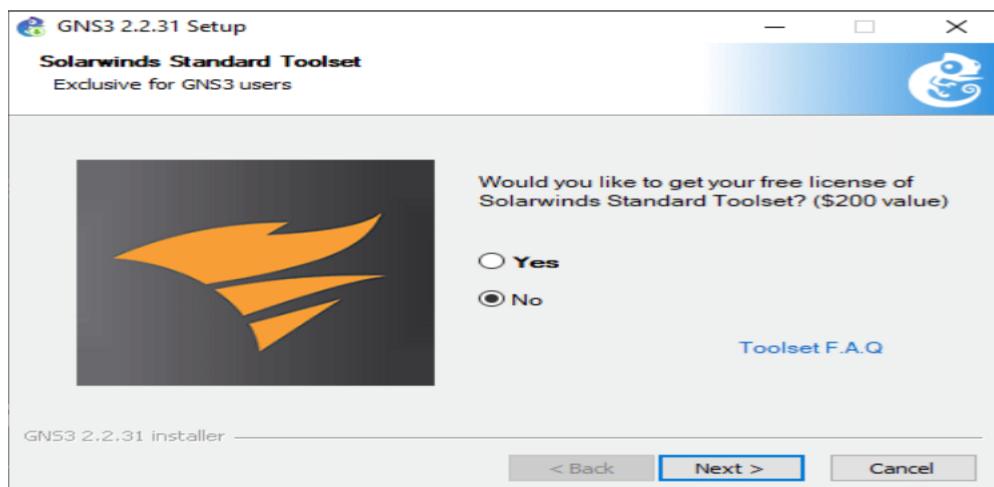


Figure 35 : Configuration de Solar-Putty

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Cliquez sur **Finish** pour terminer l'installation de GNS3.

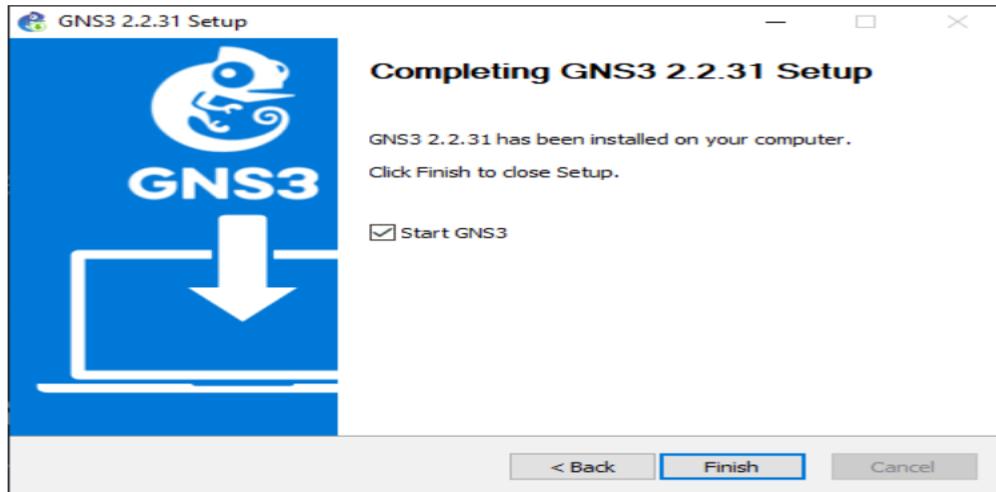


Figure 36 : Fin de l'installation

- Décompressez l'archive téléchargée pour importer la machine virtuelle dans VMware Workstation.

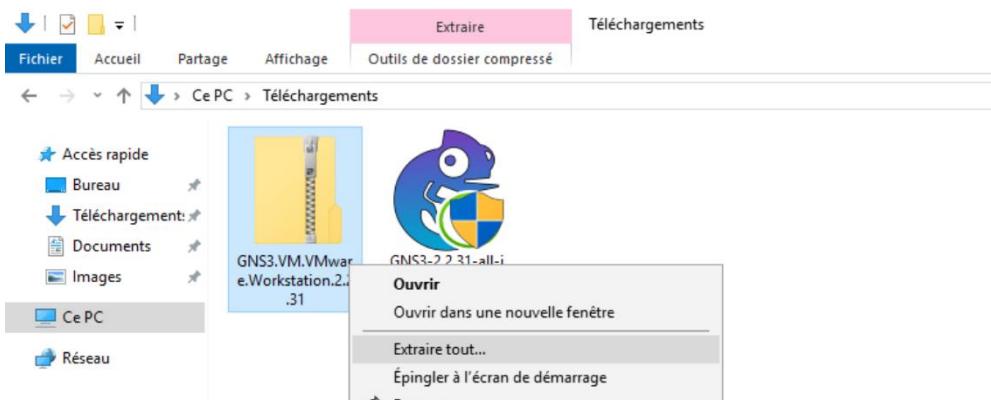


Figure 37 : Décompression de la VM

- Double-cliquez sur le fichier OVA pour importer l'appliance dans VMware Workstation

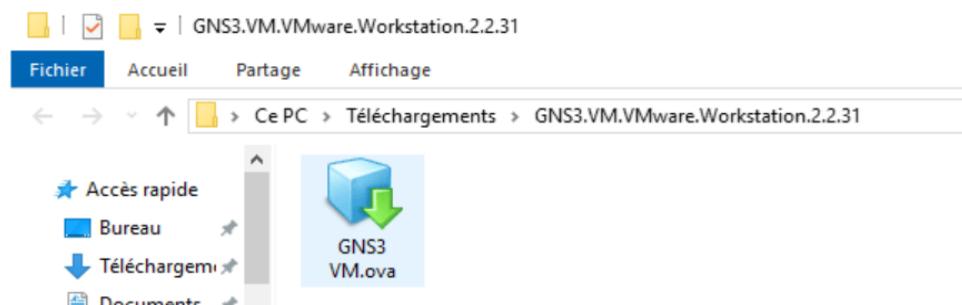


Figure 38 : Importation de l'OVA dans VMware

- Nommons la machine virtuelle et son emplacement, puis cliquons sur **Import**

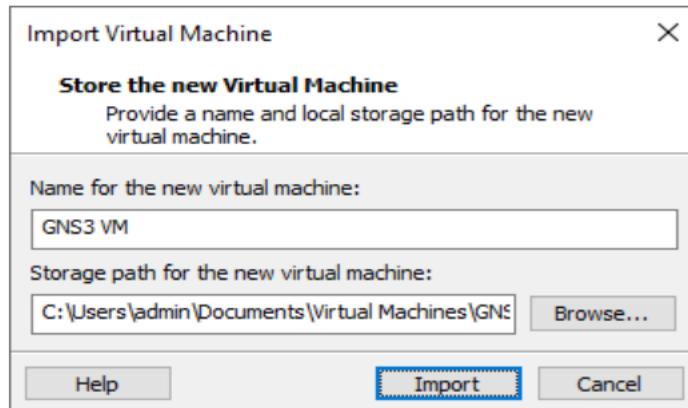


Figure 39 : Nom et emplacement de la GNS3 VM

- Après l'importation, accédez à la configuration via **Edit Virtual Machine Settings**

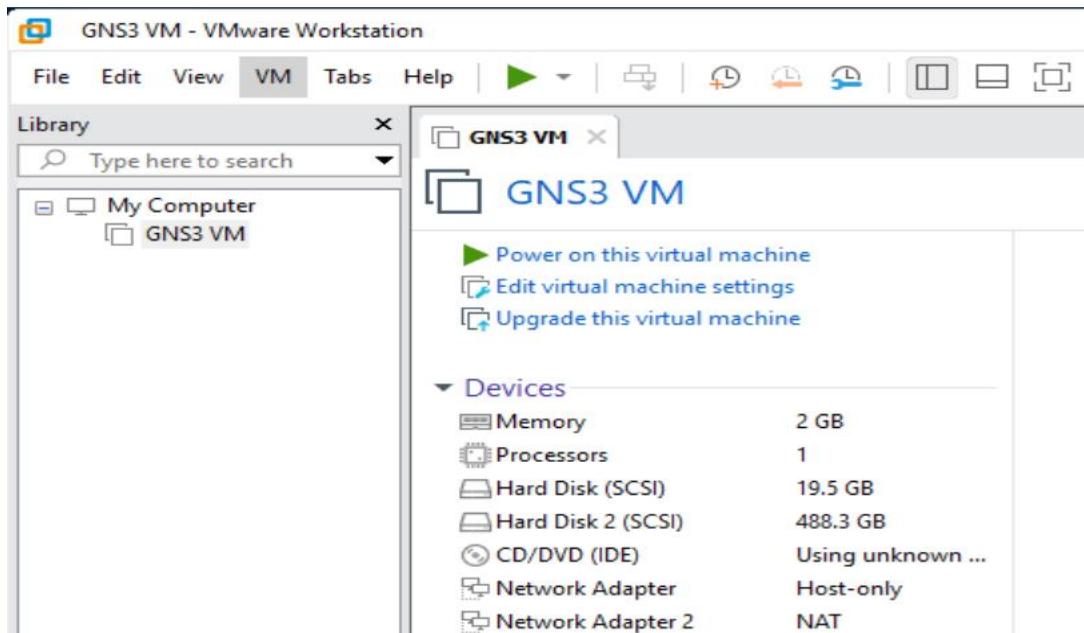


Figure 40 : Paramètres de la GNS3 VM dans VMware

- Une fois la VM prête, ouvrez **Edit** dans GNS3 et sélectionnez **Preferences...**

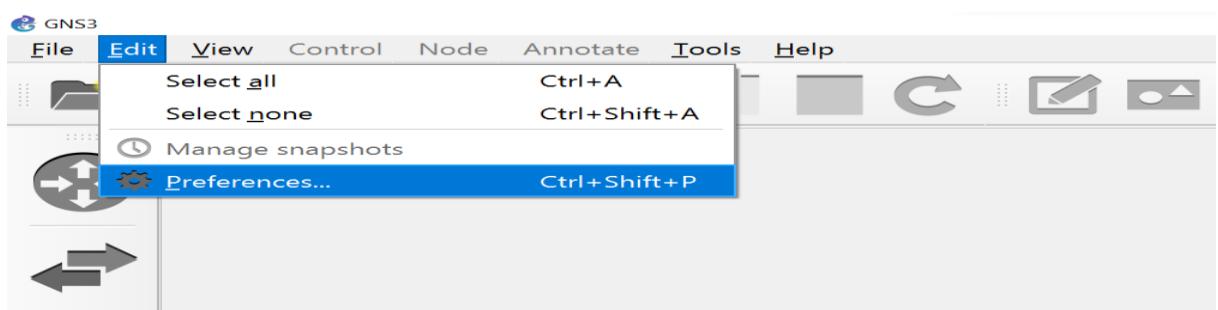


Figure 41 : Préférences de GNS3

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Dans le menu latéral, choisissez GNS3 VM, cochez **Enable the GNS3 VM**, sélectionnez l'appliance GNS3, configurez les vCPU et la RAM, puis cliquez sur **Apply** et **OK**

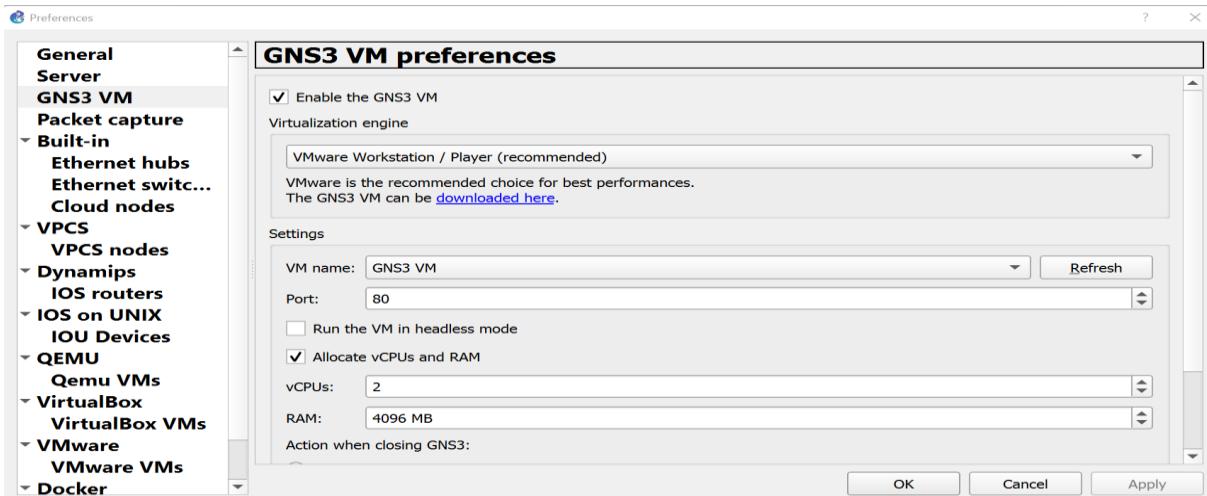


Figure 42 : Activation et configuration de la VM

- En cliquant sur **OK**, la VM GNS3 démarre.

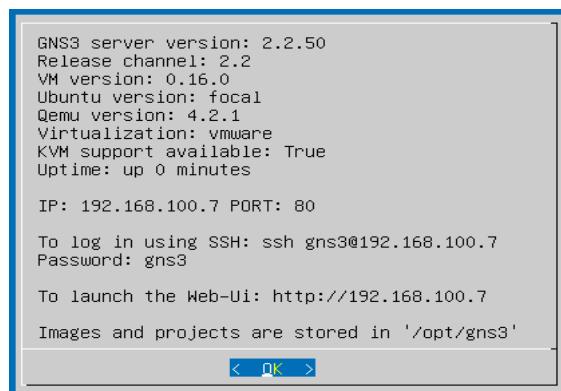


Figure 43 : Lancement de la VM GNS3

- Dans **Servers Summary** de GNS3, une icône verte à côté de GNS3 VM confirme que l'appliance fonctionne.

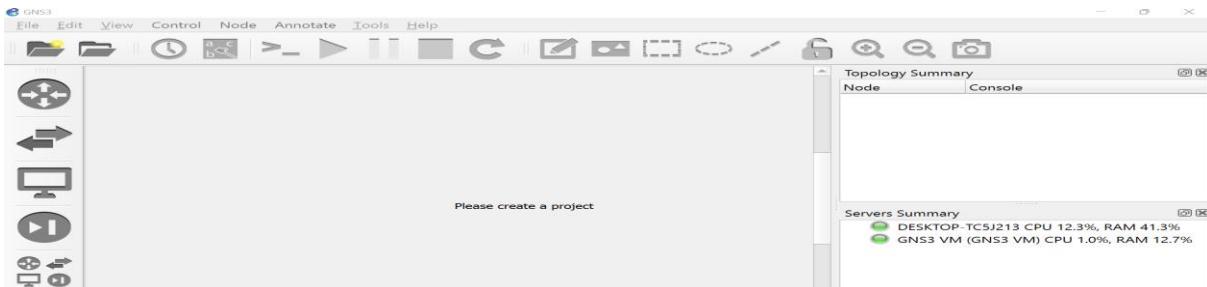


Figure 44 : Vérification de l'état de la VM

Après l'installation de GNS3, configurez VMware et créez un nouveau projet dans GNS3. Ajoutez des machines virtuelles et configurez le réseau avec des équipements comme des commutateurs et des pare-feu pour simuler un environnement complet.

3.2.3 Installation et Configuration de Zabbix Serveur sur Ubuntu

Pour installer Zabbix Serveur, commencez par télécharger le paquet d'installation. Ajoutez ensuite le dépôt Zabbix à votre système avec la commande wget. Installez les composants nécessaires (serveur, agent, frontend) et assurez-vous que MySQL est également installé pour que tout fonctionne correctement.

- Téléchargez le paquet d'installation de Zabbix.

```
zabbix-S:~$ sudo -s
root@zabbix-S:/home/zabbix# wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest+ubuntu22.04_all.deb
--2024-10-28 15:04:01-- https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest+ubuntu22.04_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8288 (8.1K) [application/octet-stream]
Saving to: 'zabbix-release_latest+ubuntu22.04_all.deb'

zabbix-release_latest+u 100%[=====] 8.09K ---KB/s   in 0s

2024-10-28 15:04:02 (29.2 MB/s) - 'zabbix-release_latest+ubuntu22.04_all.deb' saved [8288/8288]
```

Figure 45 : Téléchargement du paquet Zabbix

- Ajoutez le dépôt Zabbix à votre système

```
root@zabbix-S:/home/zabbix# dpkg -i zabbix-release_latest+ubuntu22.04_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 202702 files and directories currently installed.)
Preparing to unpack zabbix-release_latest+ubuntu22.04_all.deb ...
Unpacking zabbix-release (1:7.0-2+ubuntu22.04) ...
Setting up zabbix-release (1:7.0-2+ubuntu22.04) ...
root@zabbix-S:/home/zabbix# apt update
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:2 http://mir.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://mir.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
```

Figure 46 : Ajout du dépôt Zabbix

- Installez Zabbix Server, Agent et Frontend.

```
root@zabbix-S:/home/zabbix# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache
-conf zabbix-sql-scripts zabbix-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
 fonts-dejavu fonts-dejavu-extra fping libevent-core-2.1-7 libevent-pthreads-2.1-7
```

Figure 47 : Installation de Zabbix

- Installez MySQL pour la base de données de Zabbix.

```
root@zabbix-S:/home/zabbix# apt-get install mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
 libaio1 libcgi-fast-perl libcgi-pm-perl libfcgi-bin libfcgi-perl libfcgi0ldbl
 libhtml-template-perl libmecab2 libprotobuf-lite23 mecab-ipadic mecab-ipadic-utf8
 mecab-utils mysql-server-8.0 mysql-server-core-8.0
Suggested packages:
 libipc-sharedcache-perl mailx tinyca
The following NEW packages will be installed:
 libaio1 libcgi-fast-perl libcgi-pm-perl libfcgi-bin libfcgi-perl libfcgi0ldbl
```

Figure 48 : Installation de MySQL

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Créez la base de données Zabbix et un utilisateur pour la gérer.

```
root@zabbix-S:/home/zabbix# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.39-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0.00 sec)

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| zabbix |
+-----+
5 rows in set (0.00 sec)

mysql> create user zabbix@localhost identified by 'zabbix';
Query OK, 0 rows affected (0.03 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.01 sec)
```

Figure 49 : Création de la base de données

- Importe la base de données Zabbix et désactive la vérification des créateurs de fonctions dans MySQL.

```
root@zabbix-S:/home/zabbix# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --
default-character-set=utf8mb4 -uzabbix -p zabbix
Enter password:
root@zabbix-S:/home/zabbix# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 15
Server version: 8.0.39-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> set global log_bin_trust_function_creators = 0;
Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> quit;
Bye
root@zabbix-S:/home/zabbix# gedit /etc/zabbix/zabbix_server.conf
```

Figure 50 : Importation de la base de données

- Redémarrez les services Zabbix pour commencer à l'utiliser.

```
execute errto process - does launch (no such file or directory)
root@zabbix-S:/home/zabbix# systemctl restart zabbix-server zabbix-agent apache2
root@zabbix-S:/home/zabbix# systemctl enable zabbix-server zabbix-agent apache2
Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.service → /lib/systemd/system/zabbix-server.service.
```

Figure 51 : Redémarrage des services

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Accédez à l'interface web de Zabbix pour vérifier l'installation et configurez les paramètres nécessaires.



Figure 52 : Accès à l'interface web

- Vérifiez les conditions préalables et cliquez sur "Next step", puis entrez les informations de connexion à la base de données.

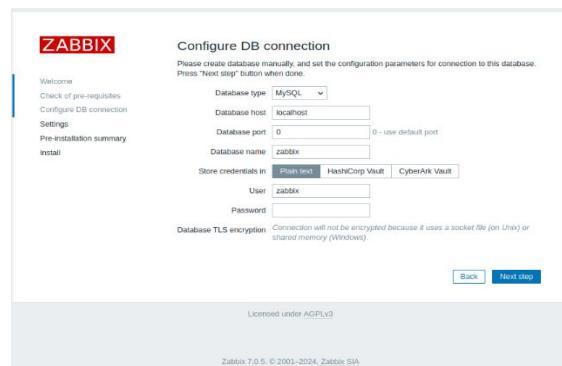


Figure 53 : Vérification des prérequis

- Le "Name" est facultatif, cliquez sur "Next step" pour continuer et vérifiez le résumé de pré-installation.

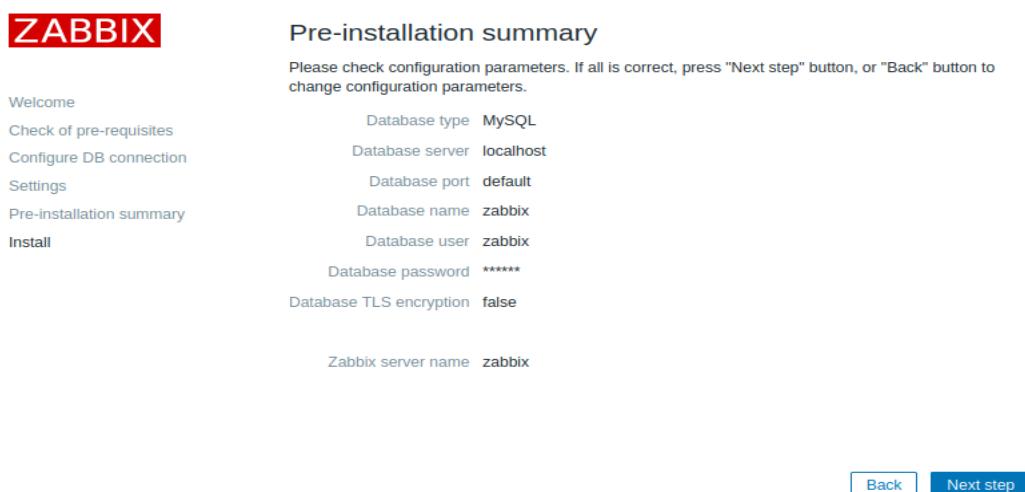


Figure 54 : Configuration de la base de données

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Accédez à l'interface web de Zabbix via <http://172.16.0.5/zabbix/>

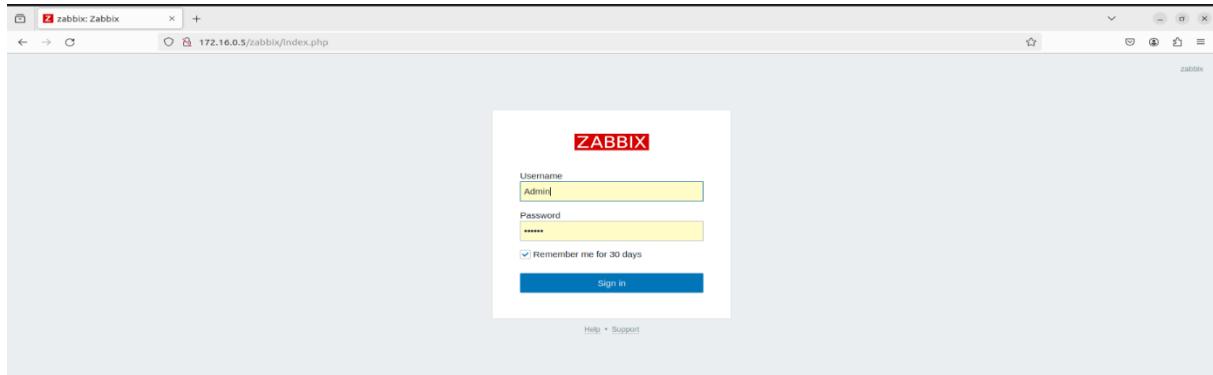


Figure 55 : Page login Zabbix

- Une fois connecté, cliquez sur "Dashboard"

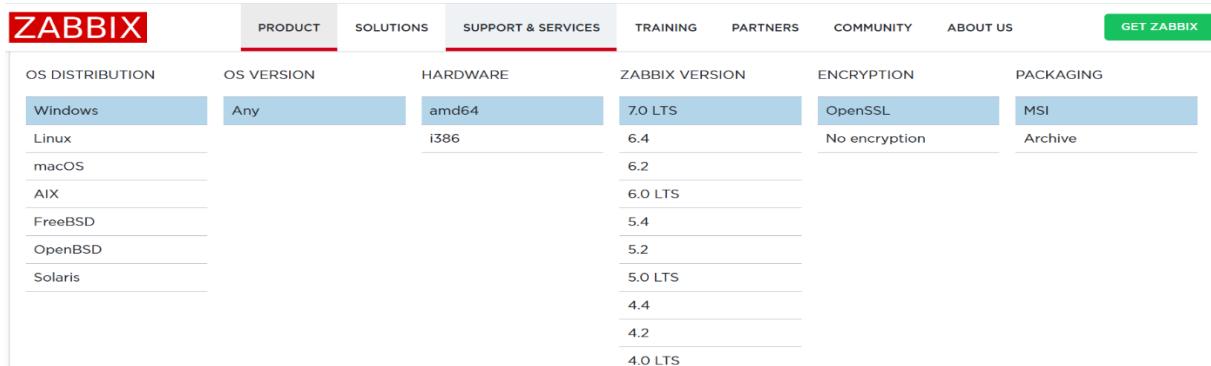
Figure 56 : Accès au Dashboard

Configurez les alertes par e-mail pour recevoir des notifications d'incidents réseau.

Figure 57 : Configuration SMTP pour les notifications Zabbix

3.2.4 Installation et configuration de l'agent Zabbix sur Windows

- Téléchargez l'agent Zabbix pour Windows depuis le site officiel.



The screenshot shows the Zabbix download page with the following table:

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	7.0 LTS	OpenSSL	MSI
Linux		i386	6.4	No encryption	Archive
macOS			6.2		
AIX			6.0 LTS		
FreeBSD			5.4		
OpenBSD			5.2		
Solaris			5.0 LTS		
			4.4		
			4.2		
			4.0 LTS		

Figure 58 : Téléchargement de l'agent Zabbix

- Choisissez la version de l'agent Zabbix compatible avec votre version de Windows sur la page de téléchargement.



Zabbix agent v7.0.5 Read manual

Packaging: MSI
 Encryption: OpenSSL
 Linkage: Dynamic
 Checksum:
 sha256: 1d5a1e93626091b89546b6cb00197fe0569ce77cc062691604d10d24203a2d30
 sha1: 238f36d2db2ccbec09f88273da2278a8783dc64
 md5: f3cac46e40150ac95e05e615f37a2db8

DOWNLOAD https://cdn.zabbix.com/zabbix/binaries/stable/7.0/7.0.5/zabbix_agent-7.0.5-windows-amd64-openssl.msi

Figure 59 : Choix de la version de l'agent

- Une fenêtre d'installation s'ouvrira avec plusieurs options.

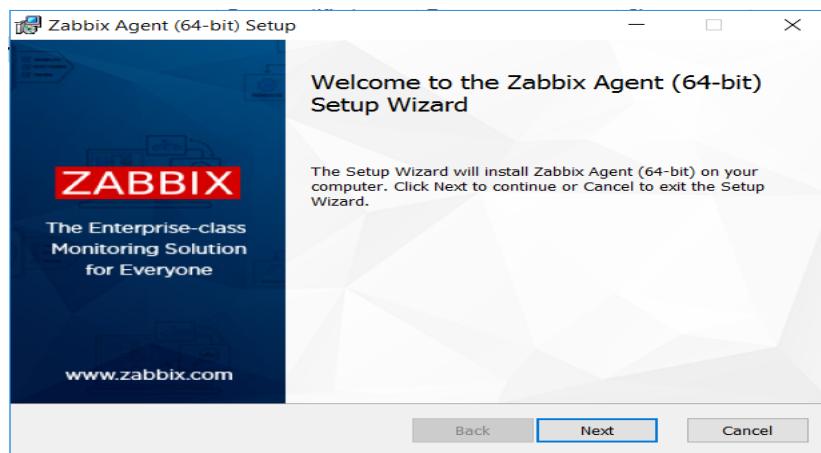


Figure 60 : Fenêtre d'installation de l'agent

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Ajoutez l'adresse IP du serveur Zabbix dans la configuration de l'agent pour permettre la communication entre les deux.

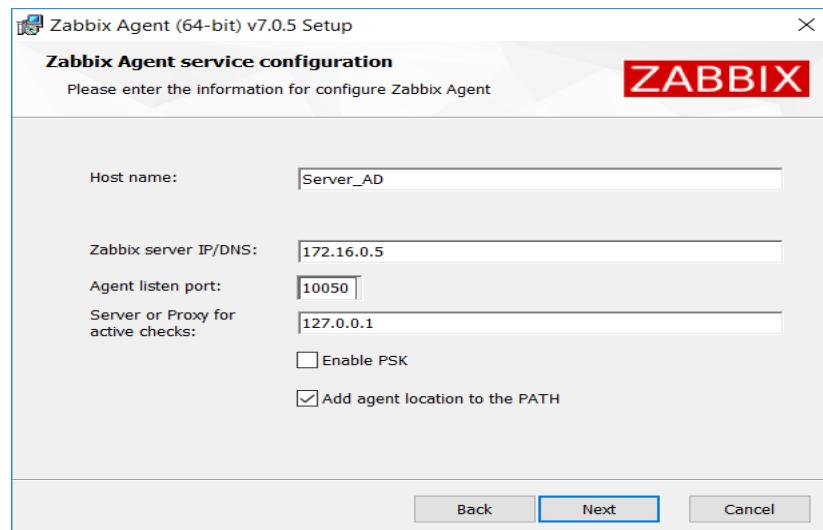


Figure 61 : Configuration de l'hôte et IP

- Terminez l'installation et vérifiez que l'agent fonctionne correctement.

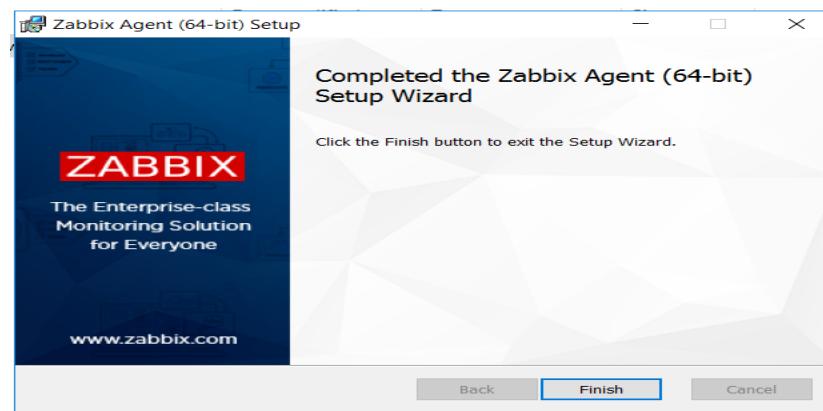


Figure 62 : Finalisation de l'installation

3.2.5 Installation de FortiGate

Pour télécharger un firmware Fortinet, créez un compte sur le site Fortinet, puis utilisez-le pour installer FortiGate

- Allez dans "Prise en charge" => "Images VM", sélectionnez KVM dans le menu déroulant, puis téléchargez l'image



Figure 63 : Téléchargement de l'image VM FortiGate

Une fois le firmware et le fichier qcow2 téléchargés, ouvrez GNS3 et attendez qu'elle se connecte à la VM GNS3.

- Pour ajouter le FortiGate dans GNS3, sélectionnez « Browse all appliances », puis « new template ». Choisissez Install an appliance from the GNS3 server et cliquez sur Next.

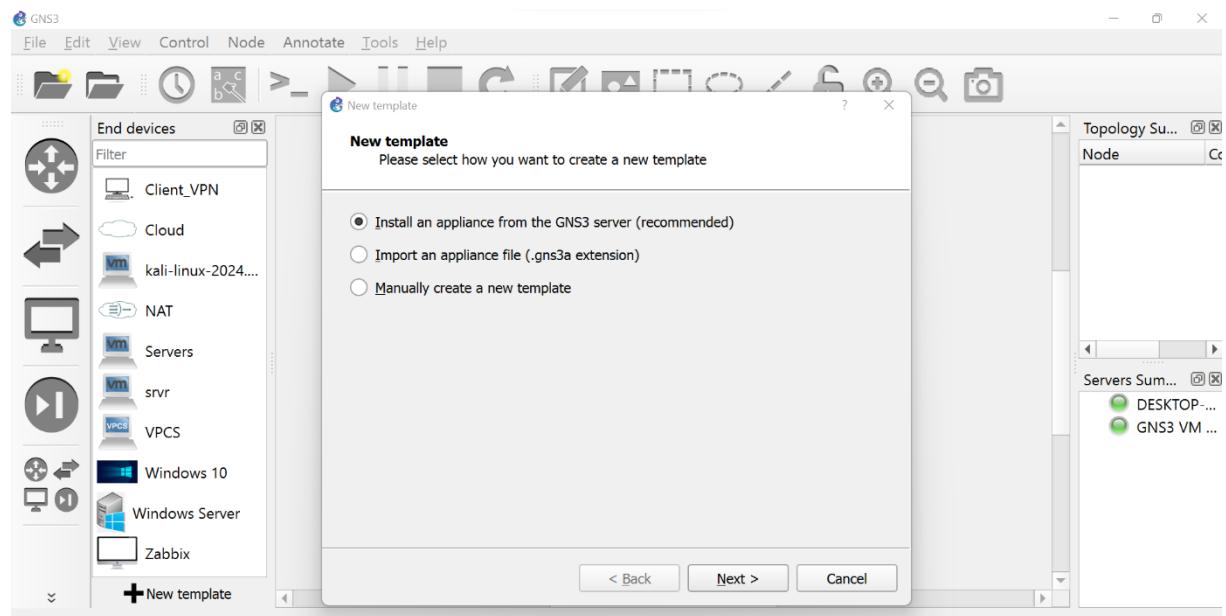


Figure 64 : Installation de FortiGate dans GNS3

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Sous « **Firewall** », sélectionnez FortiGate, puis installez. Si la version FortiOS souhaitée est absente, créez-la manuellement.

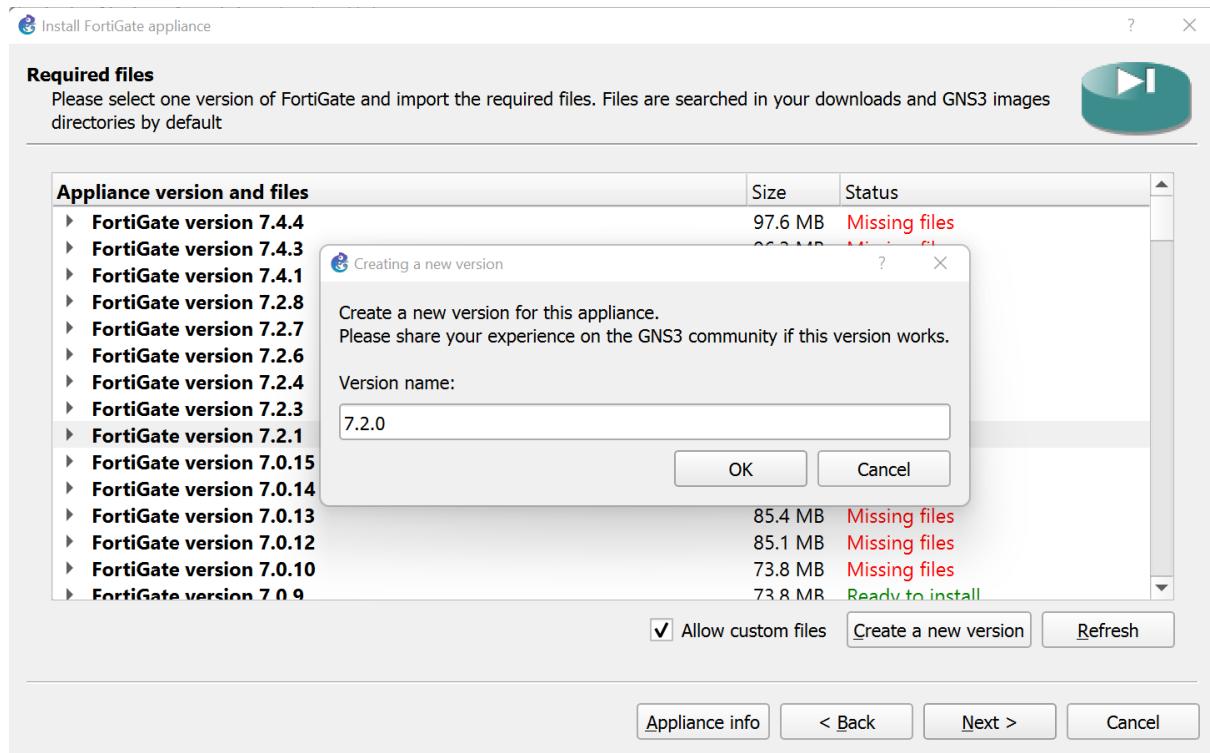


Figure 65 : Importation de l'image dans GNS3

- Après l'installation de l'image, elle s'affiche dans le panneau de gauche avec les autres appareils. Depuis l'accueil de GNS3, cliquez sur "Nouveau projet", nommez-le et cliquez sur "Créer".

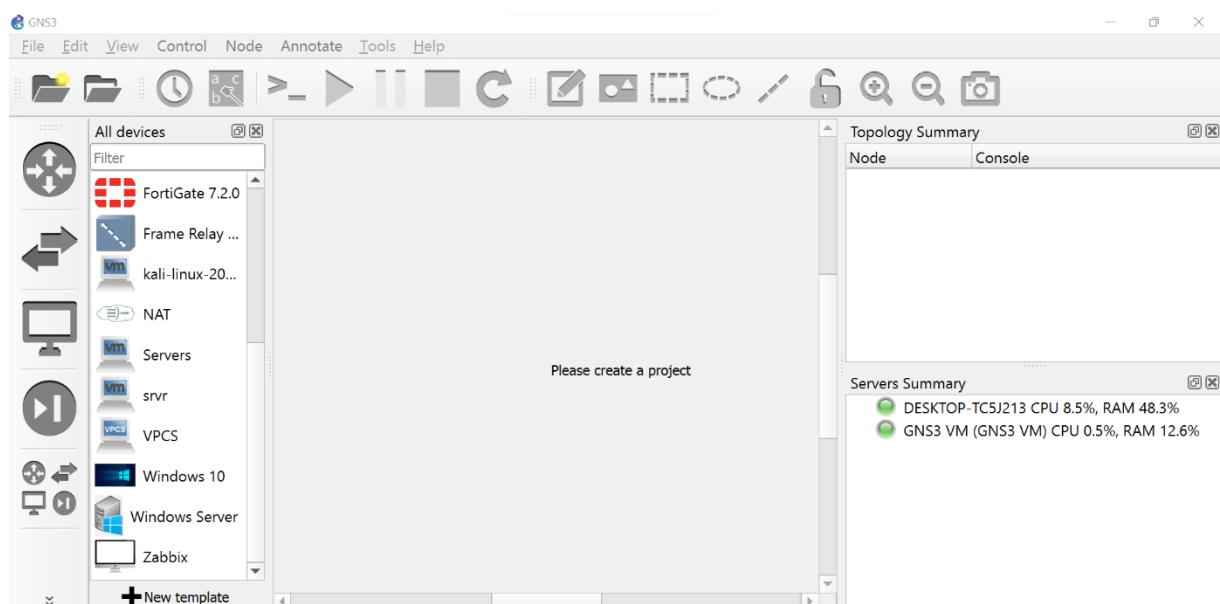


Figure 66 : Installation de FortiGate dans GNS3

3.2.6 Ajout des Machines Virtuelles dans VMware et GNS3

3.2.6.1 Environnement Virtualisé

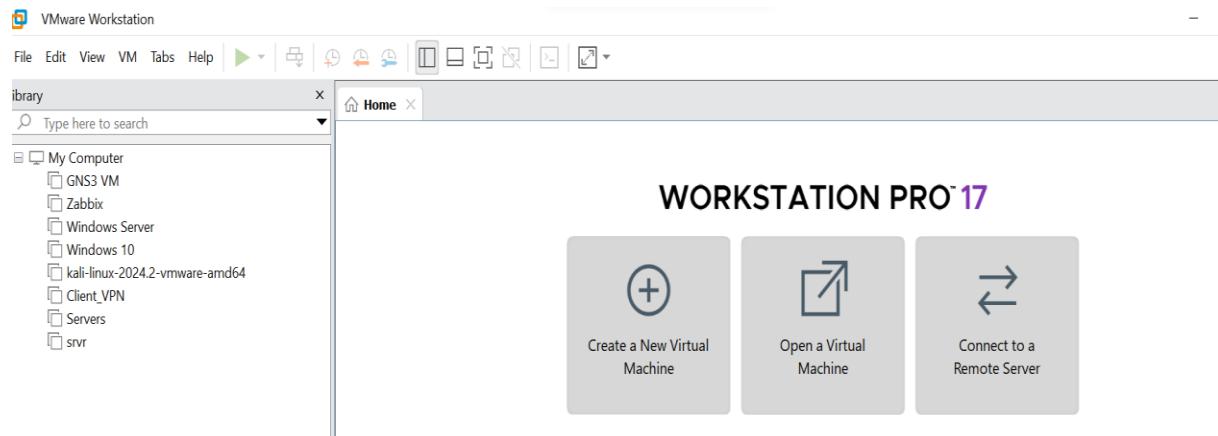


Figure 67 : Environnement Virtualisé

VMware Workstation Pro 17, associé à GNS3, permet de créer un environnement virtuel complet avec des machines comme Zabbix sur Ubuntu, Windows Server, Windows 10, Kali Linux pour la sécurité, un client VPN et des serveurs sur Ubuntu, parfait pour tester et simuler des réseaux.

3.2.6.2 Crédation du projet GNS3

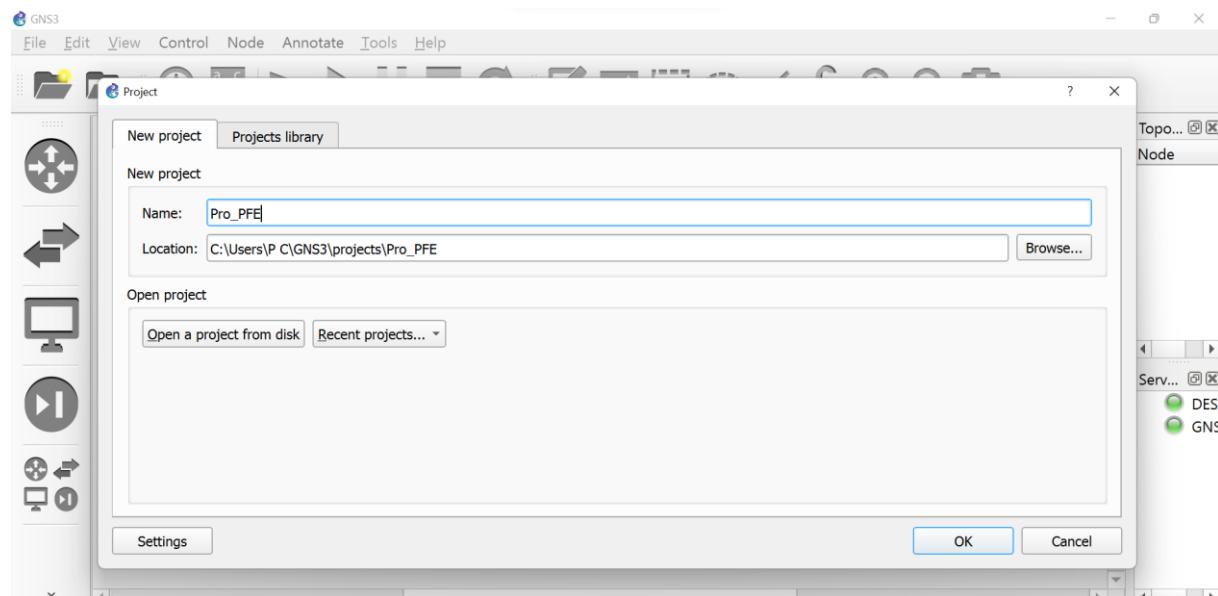


Figure 68 : Crédation du projet GNS3

3.2.6.3 Topologie Réseau Simple

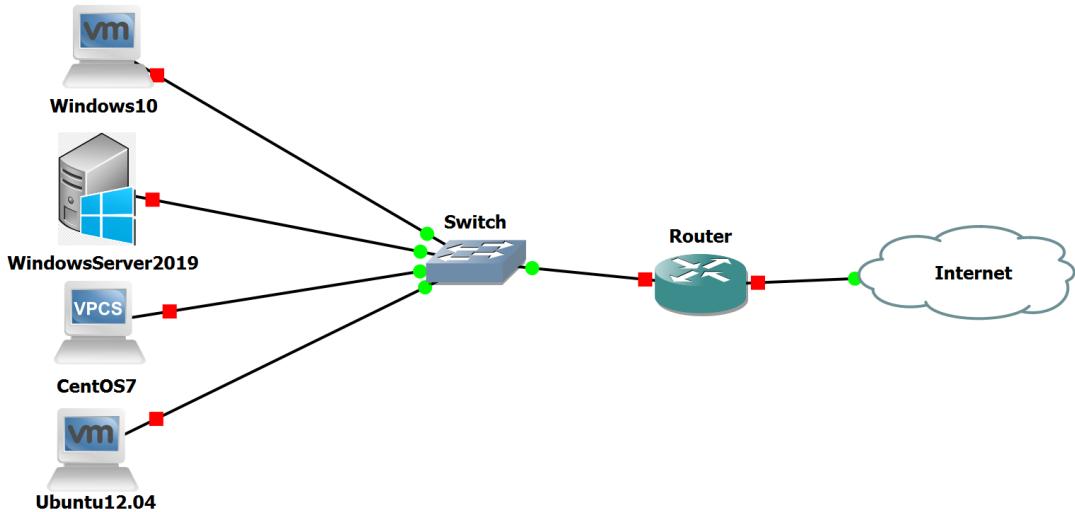


Figure 69 : Topologie Réseau Simple

Cette topologie représente un réseau d'entreprise simple avec des systèmes connectés via un commutateur et un routeur reliant l'Internet. Elle permet une communication libre entre les machines, sans sécurité ni supervision, servant à tester la connectivité de base entre différents systèmes d'exploitation.

3.2.6.4 Topologie :

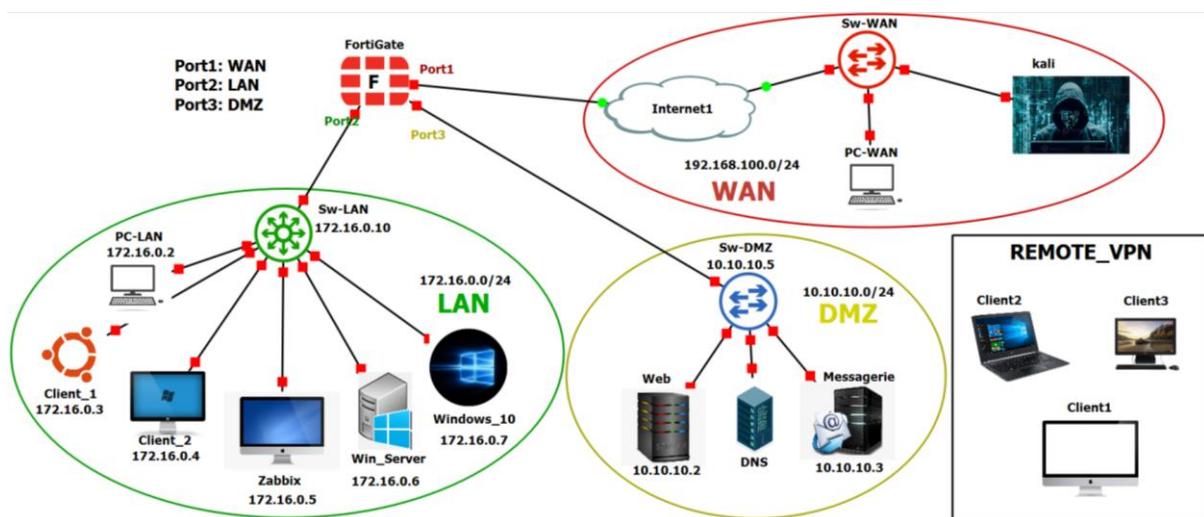


Figure 70 : Topologie réseau

Le schéma décrit un réseau d'entreprise sécurisé, segmenté en trois zones : WAN, DMZ et LAN, interconnectées par un pare-feu FortiGate. La zone WAN relie l'entreprise à Internet, la DMZ héberge les serveurs accessibles depuis l'extérieur, tandis que le LAN regroupe les postes de travail et serveurs internes. Le FortiGate assure la sécurité et la gestion du trafic entre ces zones, tandis que des switchs connectent les équipements au sein de chaque zone. Le réseau inclut également des clients VPN pour un accès sécurisé à distance et utilise Zabbix pour la surveillance de l'infrastructure.

3.2.6.4.1 Zone LAN

- ⊕ **Serveur Zabbix** : a été installé et configuré sur une machine Ubuntu 22.04 pour assurer la supervision de tous les éléments du réseau, y compris les machines du LAN, les serveurs situés en DMZ, et le pare-feu FortiGate.
- ⊕ **Serveur Windows** : a été configuré pour gérer les ressources réseau via Active Directory (AD), intégration LDAP avec FortiGate.
- ⊕ **Client Windows 10** : Connexion au domaine, agent Zabbix, tests d'accès aux services et emails via IredMail en DMZ.

3.2.6.4.2 Zone DMZ

❖ Présentation des services dans la DMZ

DMZ contient deux machines virtuelles Ubuntu 22.04, chacune hébergeant des services critiques pour le réseau. Ces services sont configurés pour être accessibles conformément aux politiques de sécurité définies sur le pare-feu FortiGate.

❖ Services configurés :

- **Serveur Web** avec Apache2, hébergement de pages Web simples (Dashboard, login, logout) et de l'application DVWA pour des tests de sécurité (SQL Injection). Accessible depuis les réseaux LAN et WAN via FortiGate.
- **Serveur DNS** avec BIND9 pour la résolution de nom du domaine.
- **Serveur de Messagerie** avec iRedMail, Deux utilisateurs ont été créés (nezihe@mauritel.mr et brahim@mauritel.mr) pour tester la communication via SOGo entre les utilisateurs du LAN.

3.2.6.4.3 Zone LAN

- ✓ **Kali Linux** : Utilisé pour effectuer des tests d'attaques externes.

3.2.6.4.4 VPN à distance

La configuration du VPN IPSec permet d'établir un tunnel sécurisé entre le site distant et le réseau local via FortiGate, garantissant ainsi une connexion privée et sécurisée pour les utilisateurs distants. Cela permet d'accéder aux services internes du réseau, tout en assurant la confidentialité et l'intégrité des données échangées, en protégeant le trafic contre les attaques externes et en maintenant un haut niveau de sécurité pour les communications.

3.2.7 Connexion au FortiGate et configuration

Pour administrer le FortiGate, vous avez deux options : utiliser l'interface webGUI ou vous connecter en ligne de commande. Nous utiliserons l'interface webGUI.

Connectez le port 1 du FortiGate à votre carte réseau : vous obtiendrez une adresse IP via son DHCP, configuré par défaut sur 192.168.100.0/24 avec le FortiGate à 192.168.100.40. Dans votre navigateur, entrez cette adresse IP pour afficher l'interface d'administration. Connectez-vous avec les identifiants par défaut, « admin » et un mot de passe vide. Un assistant vous proposera des options de préconfiguration avant d'atteindre le tableau de bord.



Figure 71 : Connexion à l'interface webGUI FortiGate

➤ L'interface de FortiGate

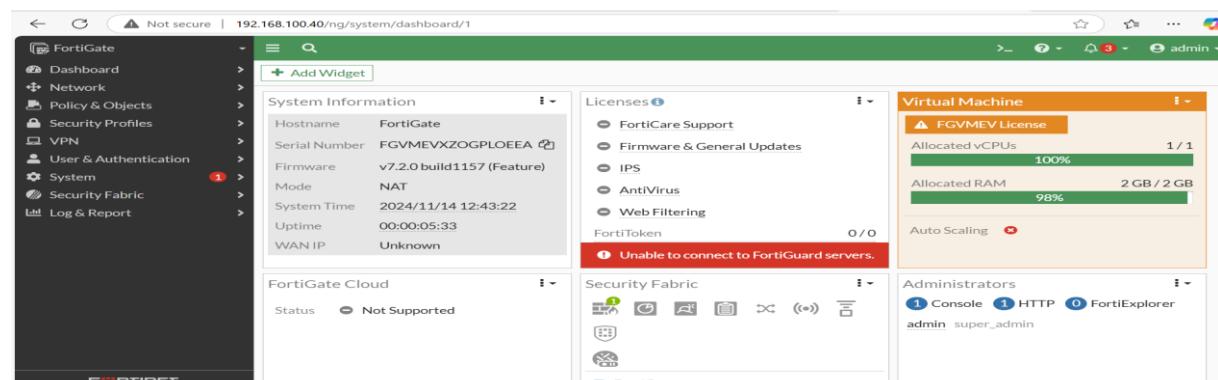


Figure 72 : Tableau de bord FortiGate

➤ Les interfaces réseau configurées pour relier les différentes zones LAN, WAN, et DMZ.

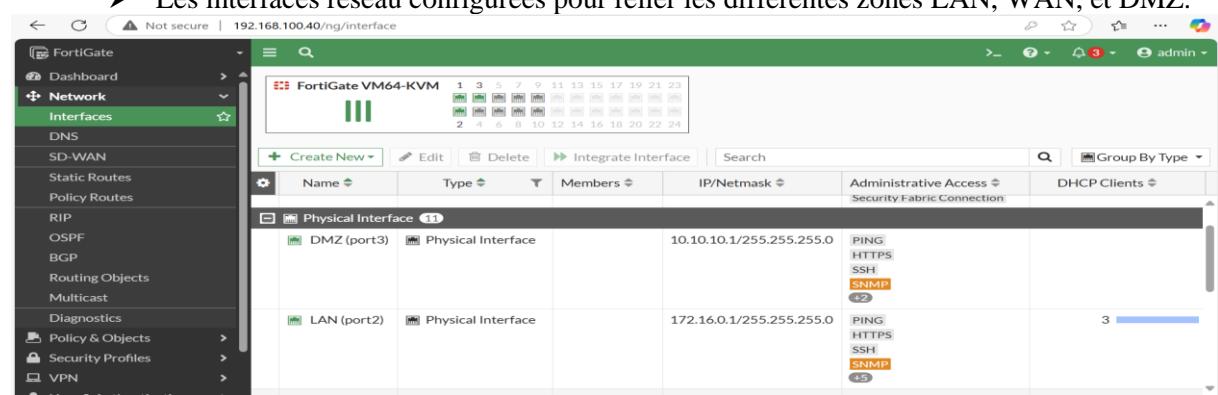


Figure 73 : Interfaces de FortiGate

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- **Configuration de l'interface LAN** : Détails des paramètres de l'interface LAN, incluant l'IP

Edit Interface

Name	LAN (port2)
Alias	LAN
Type	Physical Interface
VRF ID	0
Role	LAN

Address

Addressing mode	Manual	DHCP	Auto-managed by IPAM
IP/Netmask	172.16.0.1/255.255.255.0		
Create address object matching subnet	<input checked="" type="checkbox"/>		
Secondary IP address	<input checked="" type="checkbox"/>		

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input checked="" type="checkbox"/> FMG-Access
	<input checked="" type="checkbox"/> SSH	<input checked="" type="checkbox"/> SNMP	<input checked="" type="checkbox"/> FTM
	<input checked="" type="checkbox"/> RADIUS Accounting	<input checked="" type="checkbox"/> Security Fabric Connection <small>i</small>	<input checked="" type="checkbox"/> Speed Test

Figure 74 : Configuration de l'interface LAN

- **Les réglages DHCP**

Edit Interface

DHCP Server

DHCP status	<input checked="" type="button"/> Enabled	<input type="button"/> Disabled
Address range	172.16.0.2-172.16.0.254	
Netmask	255.255.255.0	
Default gateway	Same as Interface IP	Specify
DNS server	Same as System DNS	Same as Interface IP
Lease time <small>i</small>	604800	second(s)

Advanced

Network

Device detection <small>i</small>	<input checked="" type="checkbox"/>
Automatically authorize devices <small>i</small>	<input checked="" type="checkbox"/>
Security mode	<input checked="" type="checkbox"/>

Figure 75 : Configuration de l'interface LAN

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Les règles de pare-feu pour contrôler et sécuriser les échanges entre zones réseau.

The screenshot shows the FortiGate management interface for Firewall Policy. The left sidebar navigation includes Dashboard, Network, Policy & Objects (selected), Firewall Policy, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, and Traffic Shaping. The main content area displays a table of firewall rules:

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
DMZ (port3) → LAN (port2)	DMZ (port3)	LAN (port2)						
DMZ (port3) → WAN (port1)	DMZ (port3)	WAN (port1)						
LAN (port2) → DMZ (port3)	LAN (port2)	DMZ (port3)						
LAN (port2) → WAN (port1)	LAN (port2)	WAN (port1)						
RA_IPSEC → LAN (port2)	RA_IPSEC	LAN (port2)						
WAN (port1) → DMZ (port3)	WAN (port1)	DMZ (port3)						
Implicit								

Figure 76 : Politique de pare-feu

- **Configuration SNMP** : Paramètres SNMP pour la surveillance et la collecte de données réseau en temps réel

The screenshot shows the FortiGate management interface for System - SNMP. The left sidebar navigation includes Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, System (selected), Administrators, Admin Profiles, Fabric Management, Settings, HA, and SNMP (selected). The main content area displays the SNMP configuration:

SNMP Agent

Description	monitoring
Location	Nouakchott
Contact Info	nezihemed488@gmail.com

SNMP v1/v2c

Name	Queries	Traps	Hosts	Events	Status
IT	v1 Enable v2 Enable	v1 Enable v2 Enable	172.16.0.5/24	36	Enable

Additional Information: API Preview, Edit in CLI, Documentation, Online Help, Video Tutorials.

Figure 77 : Configuration SNMP

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- La Liste des utilisateurs créés avec leurs permissions d'accès

The screenshot shows a table of users in the FortiGate interface. The columns are Name, Type, Two-factor Authentication, Groups, Status, and Ref. The users listed are:

Name	Type	Two-factor Authentication	Groups	Status	Ref.
Client1	LOCAL	Disabled	VPN_GROUP	Enabled	1
DMZ	LOCAL	Disabled	VPN_GROUP	Enabled	0
Domain Controller	LOCAL	Disabled	LAN	Enabled	2
admin_zabbix	LOCAL	Disabled	LAN	Enabled	2
brahimelbou	LDAP	Disabled	LAN	Enabled	2
guest	LOCAL	Disabled	Guest-group	Enabled	1
nezihemed	LDAP	Disabled	LAN	Enabled	2

Figure 78 : Liste des utilisateurs

- Les groupes pour gérer les permissions d'accès des utilisateurs par rôle

The screenshot shows a table of user groups in the FortiGate interface. The columns are Group Name, Group Type, Members, and Ref. The groups listed are:

Group Name	Group Type	Members	Ref.
Guest-group	Firewall	guest	0
LAN	Firewall	admin_zabbix, brahimelbou, Domain Controller, nezihemed	0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)	guest	1
VPN_GROUP	Firewall	Client1	1
administrators	Firewall	admin_zabbix, Domain Controller	0
remote_group	Firewall	domail, nezihemed, brahimelbou	0

Figure 79 : Groupes d'utilisateurs

- Serveurs LDAP configurés pour centraliser l'authentification utilisateur

The screenshot shows a table of LDAP servers in the FortiGate interface. The columns are Name, Server, Port, Common Name Identifier, Distinguished Name, Exchange Server, and Ref. There is one entry:

Name	Server	Port	Common Name Identifier	Distinguished Name	Exchange Server	Ref.
domail	172.16.0.6	389	sAMAccountName	DC=mauritel,DC=mr		4

Figure 80 : Serveurs LDAP

- Traffic Shapers : Profils de limitation de bande passante pour gérer l'utilisation réseau

The screenshot shows a table of traffic shapers in the FortiGate interface. The columns are Name, Guaranteed Bandwidth, Max Bandwidth, Bandwidth Utilization, Dropped Bytes, and Priority. The profiles listed are:

Name	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization	Dropped Bytes	Priority
Bande Passante Administrateurs	1.00 Mbps	1.00 Mbps	0 bps		High
Bande Passante DMZ	1.00 Gbps	1.00 Gbps	0 bps		Medium
Bande Passante Utilisateurs	500.00 kbps	500.00 kbps	0 bps		Low
guarantee-100kbps	100.00 kbps	1.05 Gbps	0 bps		High
high-priority		1.05 Gbps	0 bps		High
low-priority		1.05 Gbps	0 bps		Low
medium-priority		1.05 Gbps	0 bps		Medium
shared-1M-pipe		1.02 Mbps	0 bps		High

Figure 81 : Traffic Shapers

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- **Politiques de gestion du trafic :** Règles de QoS pour prioriser certains types de trafic et garantir une qualité de service optimale

The screenshot shows the FortiGate management interface under the 'Traffic Shaping' tab. On the left is a sidebar with various policy and object categories. The main window is titled 'Traffic Shaping Policies' and displays three entries for 'IPv4'. Each entry has columns for Name, Source, Destination, To, Action, Shared Shaper, and Rule. The first rule is 'Bande Passante Administrateurs P' with source 'administrators' and destination 'all', mapped to 'WAN (port1)' and 'Apply Shaper'. The second rule is 'Bande Passante Utilisateurs p' with source 'Clients' and destination 'all', mapped to 'WAN (port1)' and 'Apply Shaper'. The third rule is 'Bande Passante DMZ' with source 'all' and destination 'all', mapped to 'LAN (port2)' and 'Apply Shaper'. There is also an 'Implicit' row.

Figure 82 : Politiques de gestion du trafic

- Un portail captif FortiGate limite la bande passante et contrôle l'accès réseau via des identifiants utilisateur

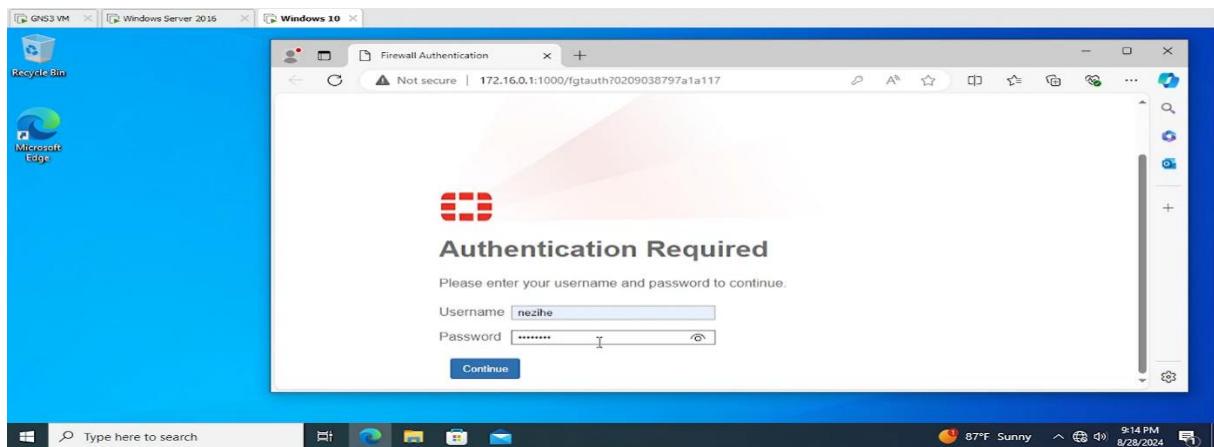


Figure 83 : Login portail captif

- Un portail captif sur FortiGate a été configuré avec une gestion QoS limitant la bande passante, et un test Speedtest a validé cette configuration avec des débits réduits conformément aux règles établies.

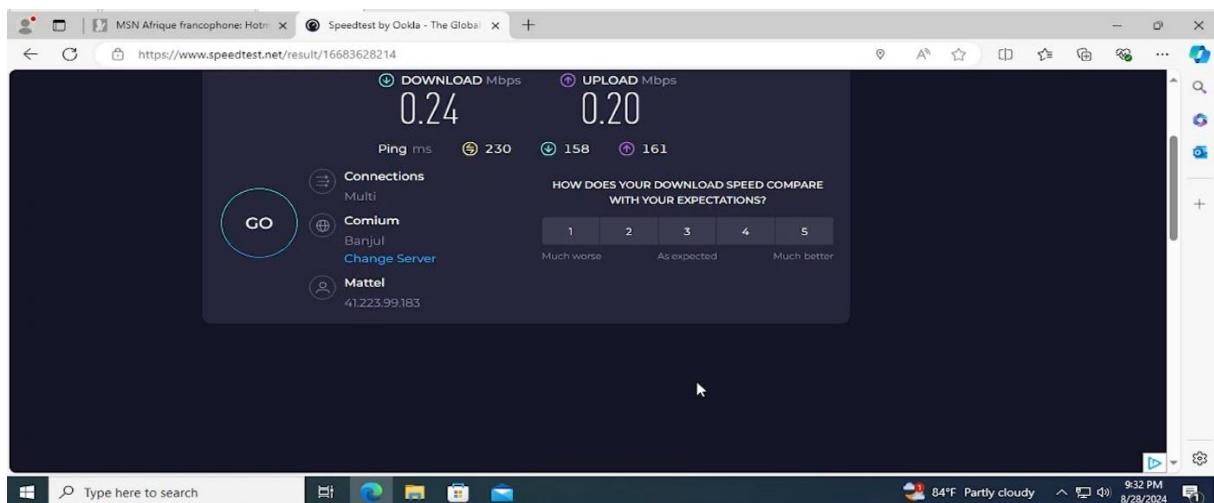


Figure 84 : Test de bande passante après connexion

3.3 AD et LDAP avec FortiGate

3.3.1 Configuration du serveur (AD) :

Tout d'abord, nous procédons à l'installation et à la configuration de Windows Server 2016 : pour agir en tant que contrôleur de domaine.

- Choisissez la langue d'installation et cliquez sur **Suivant**

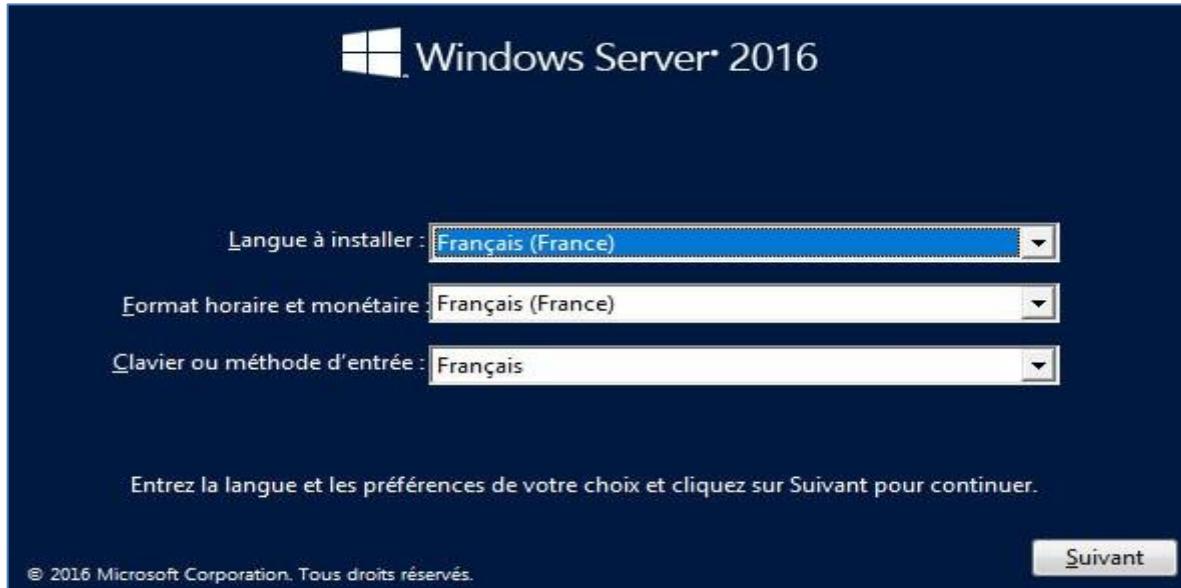


Figure 85 : Choix de la langue d'installation

- Cliquez sur **Installer Maintenant**



Figure 86 : Lancement de l'installation

- Personnalisation : Définissez le mot de passe Administrateur, puis cliquez sur **Terminer**.

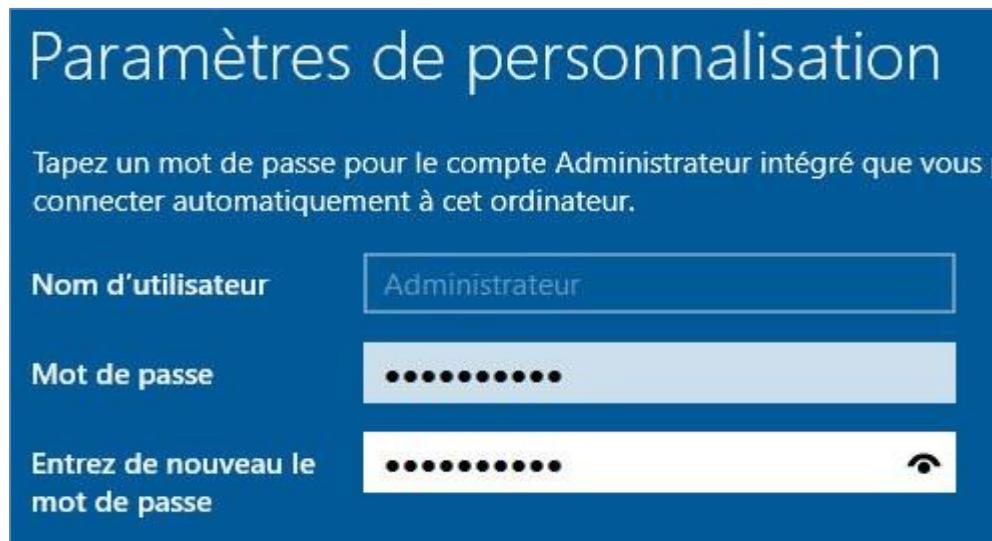


Figure 87 : Définition du mot de passe Administrateur

- Déverrouillage : Ctrl + Alt + Suppr, puis entrez le mot de passe Administrateur pour accéder à Windows



Figure 88 : Accès Windows avec Ctrl + Alt + Suppr

- Nous avons installé et configuré AD DS pour gérer les ressources du réseau et DNS pour la résolution des noms.

Chapitre 3 : Mise en place du réseau et configuration des systèmes

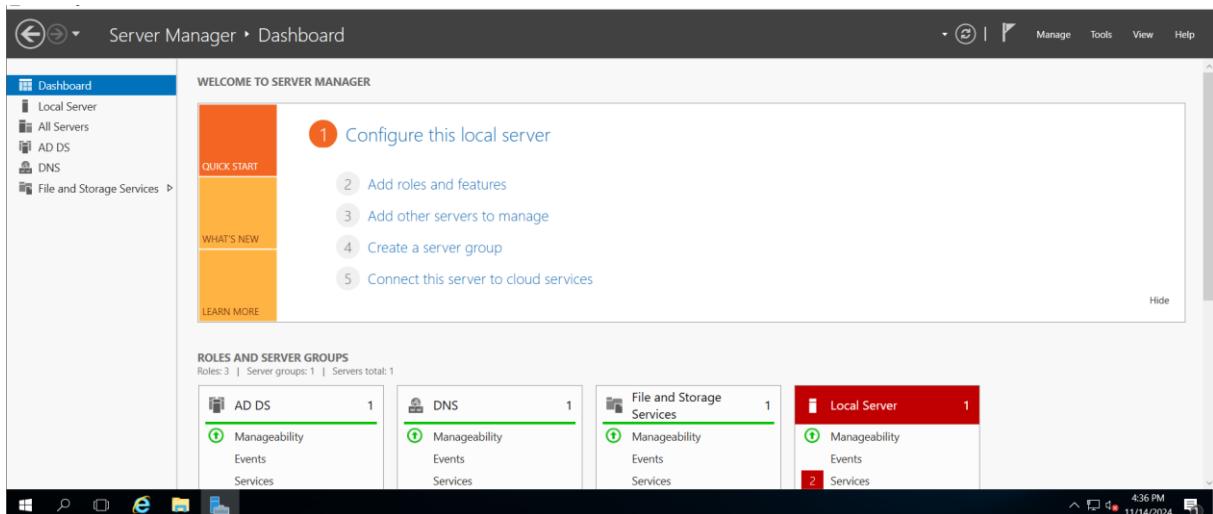


Figure 89 : Tableau de bord Server Manager

- Création et gestion des utilisateurs, des groupes et des unités organisationnelles (OU) dans Active Directory.

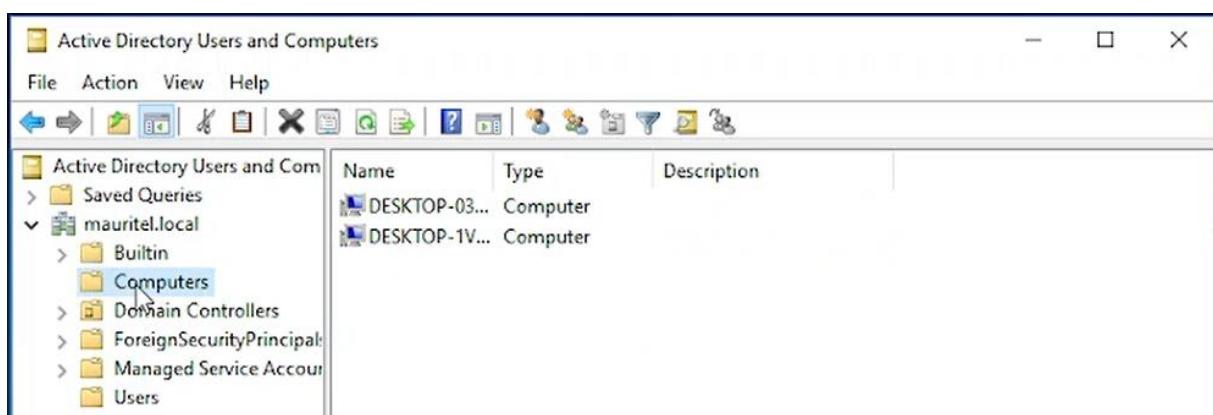


Figure 90 : Ajout d'ordinateurs dans AD

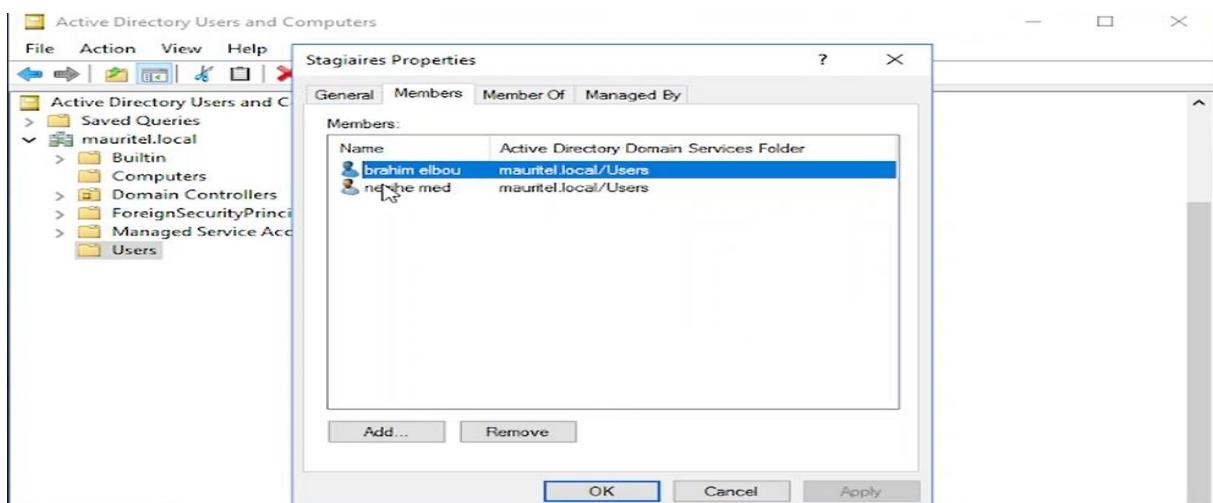


Figure 91 : Gestion des utilisateurs dans AD

3.3.2 Intégration LDAP avec FortiGate :

- Configuration de FortiGate pour se connecter à Active Directory via le protocole LDAP

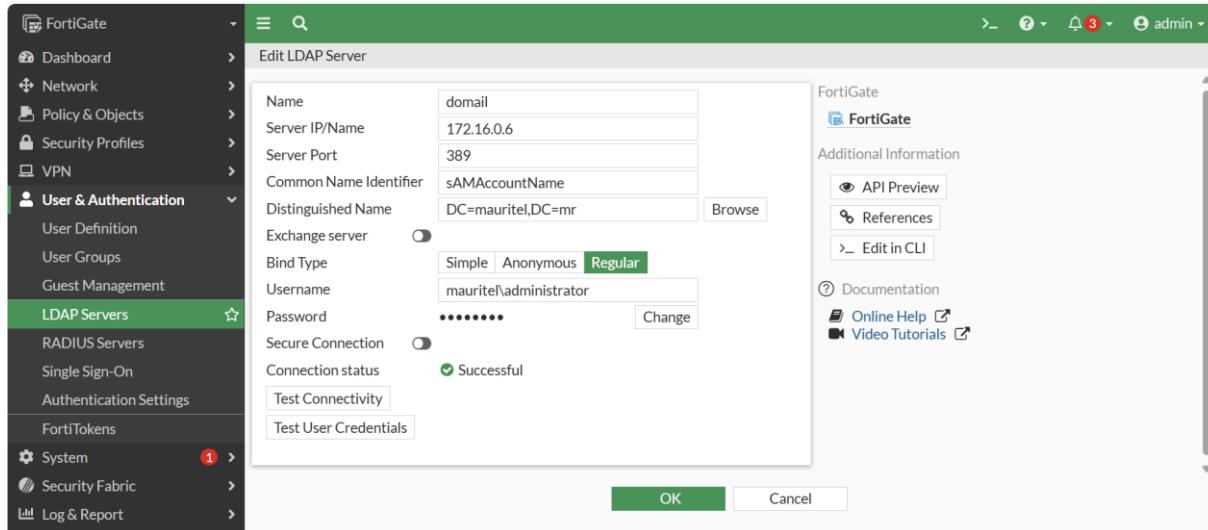


Figure 92 : Connexion LDAP de FortiGate à AD

- Paramétrage de FortiGate pour l'authentification des utilisateurs via l'annuaire AD

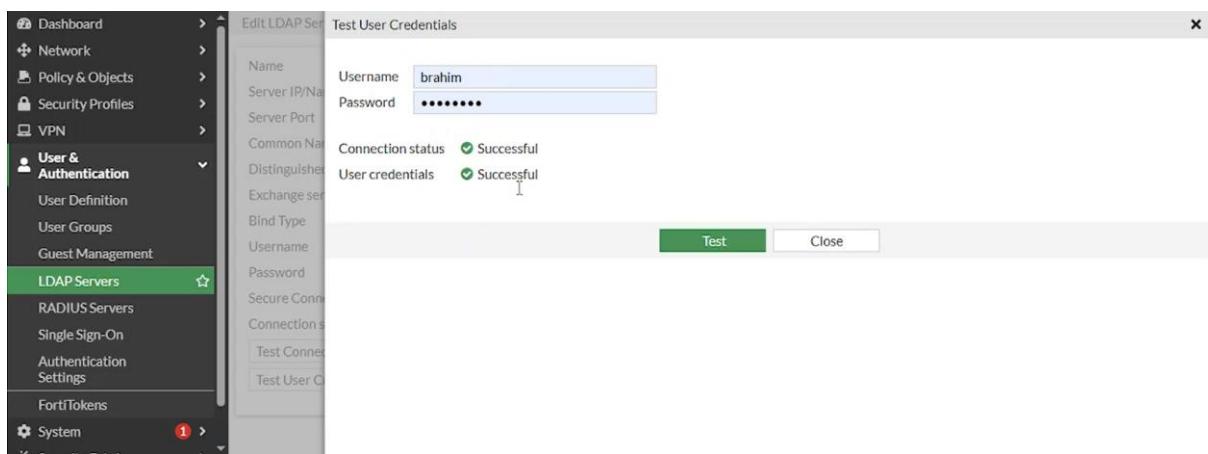


Figure 93 : Authentification des utilisateurs FortiGate via LDAP

3.4 VPN pour accès sécurisé

- Configuration du VPN sur FortiGate

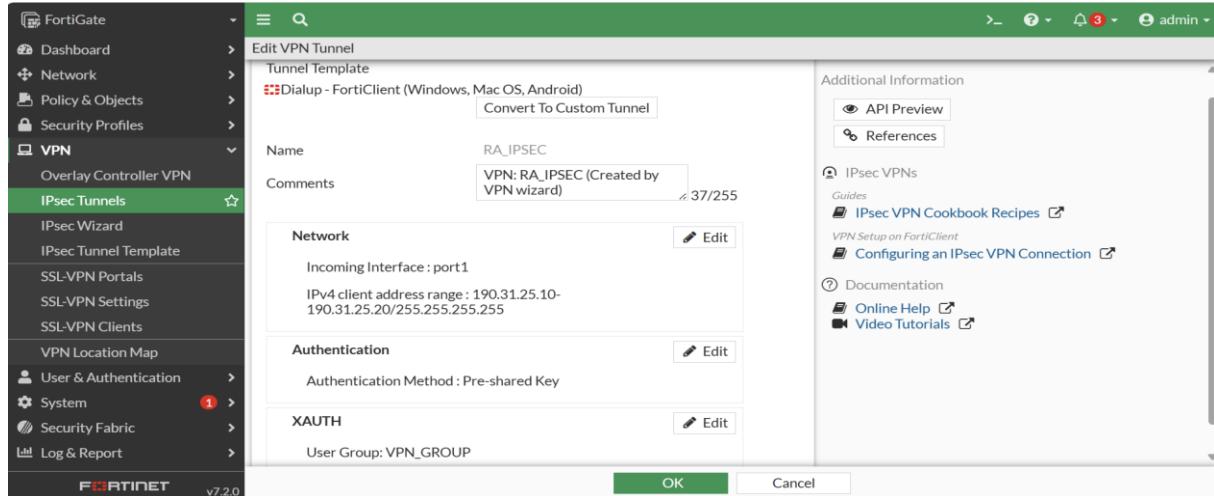


Figure 94 : Configuration VPN sur FortiGate

- Création d'une politique d'accès

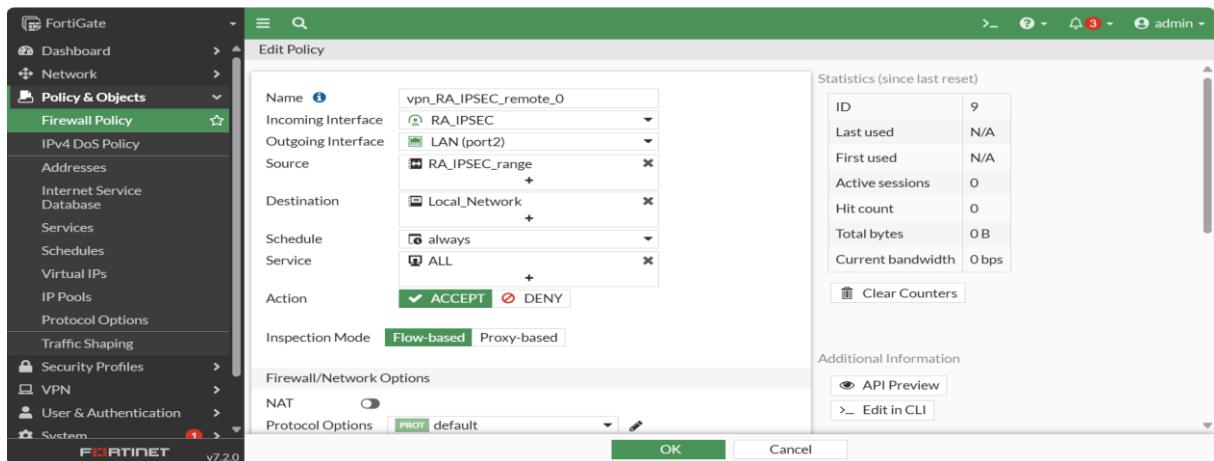


Figure 95 : Crédit de la Politique d'Accès

- Configuration des utilisateurs et des groupes
-

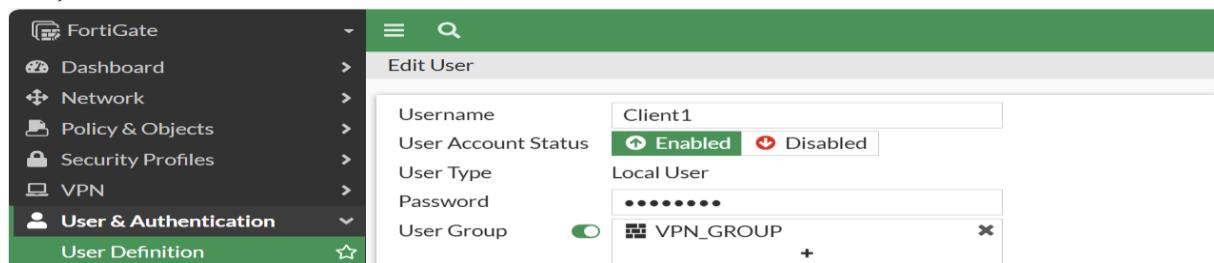


Figure 96 : Configuration des Utilisateurs et Groupes

3.4.1 Installation et Configuration du Client VPN

- Début de l'installation de FortiClient VPN en cliquant sur "Yes" pour confirmer.

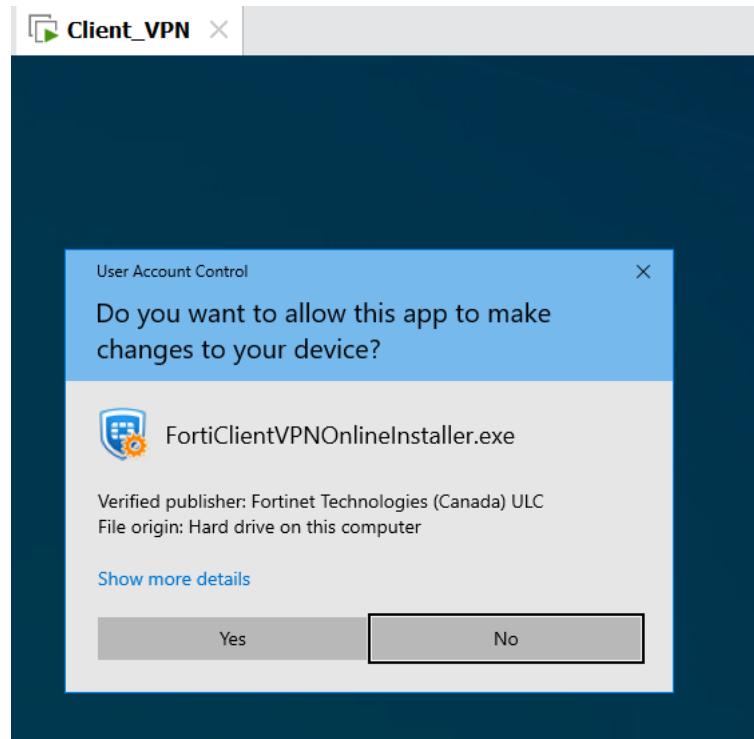


Figure 97 : Début de l'installation de FortiClient VPN

- Acceptez les conditions en cliquant sur **Accept**

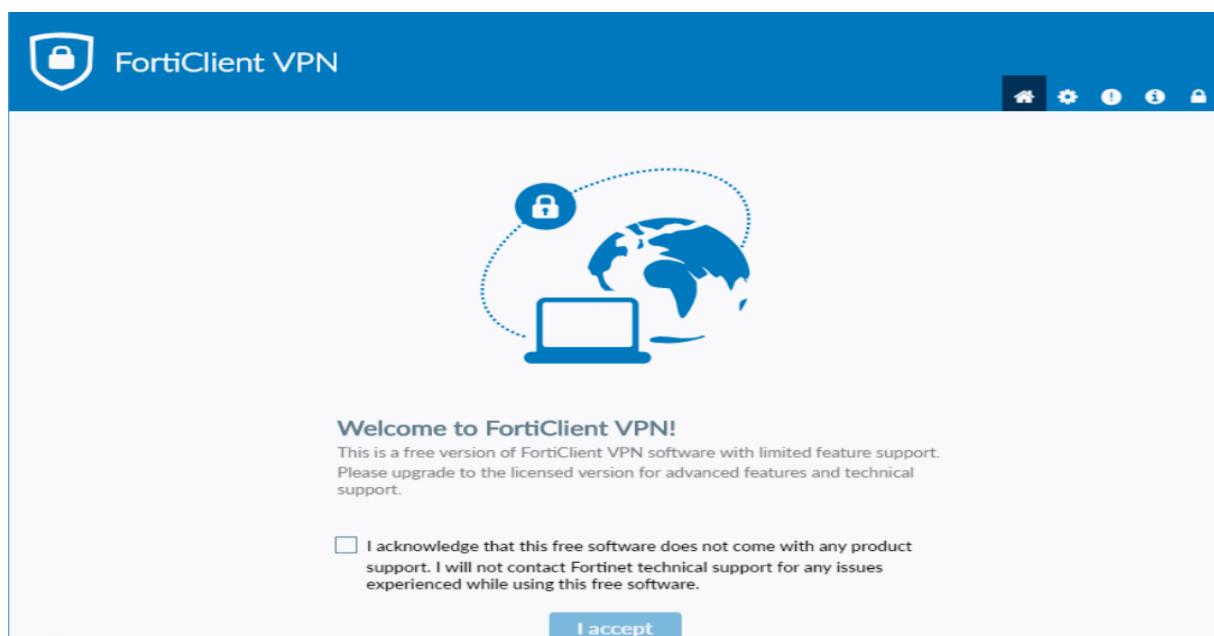


Figure 98 : Acceptation des Conditions d'Utilisation

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- "Configure VPN" dans FortiClient, permettant d'accéder aux paramètres VPN

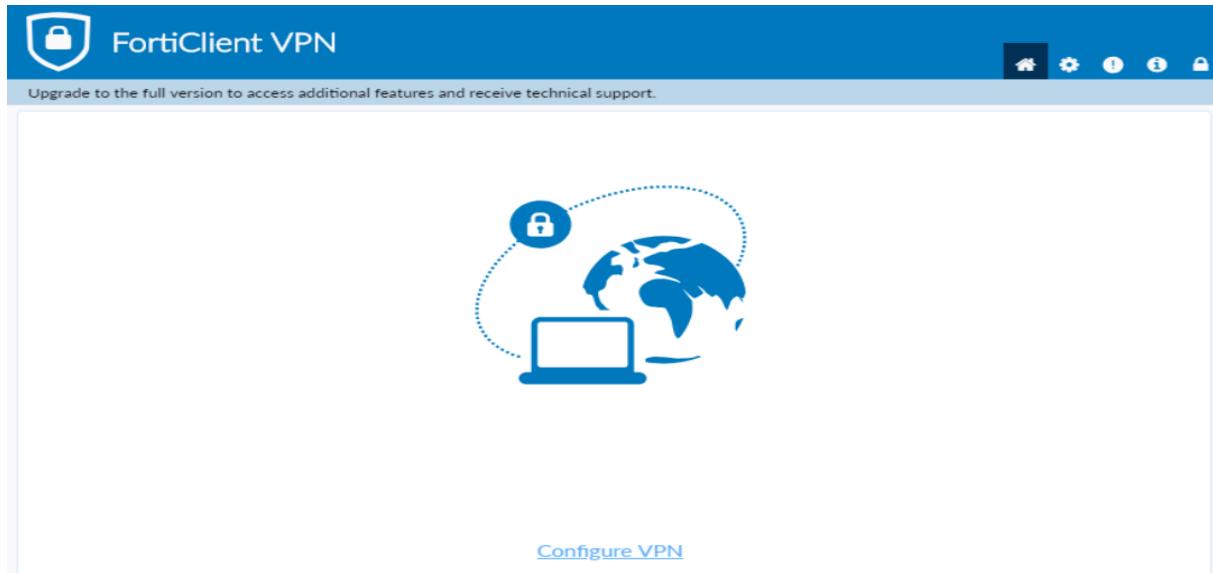


Figure 99 : Accès à la Configuration VPN dans FortiClient

- Paramétrage de la Connexion VPN dans FortiClient



Figure 100 : Réglages VPN

Chapitre 3 : Mise en place du réseau et configuration des systèmes

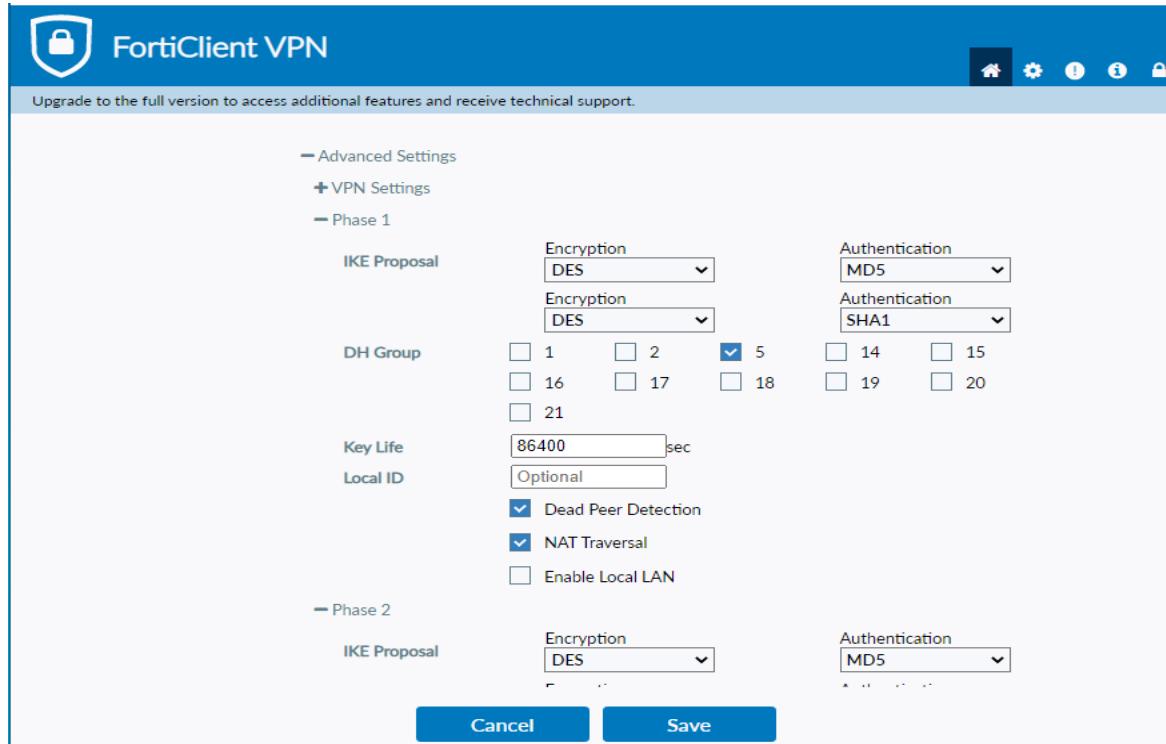


Figure 101 : Réglages VPN

- Saisie des Informations de Connexion VPN, puis clique sur "Connect" pour établir la connexion.

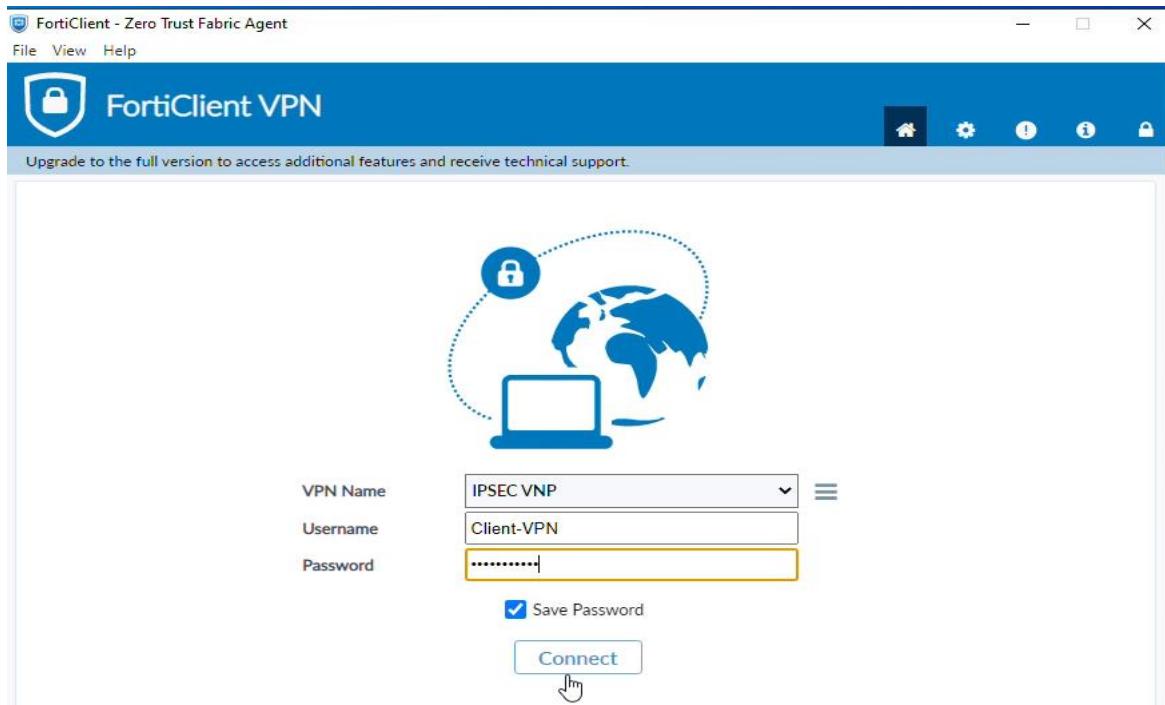


Figure 102 : Login de VPN

Chapitre 3 : Mise en place du réseau et configuration des systèmes

- Après la connexion, l'utilisateur peut accéder aux ressources du réseau local comme s'il était directement connecté au LAN

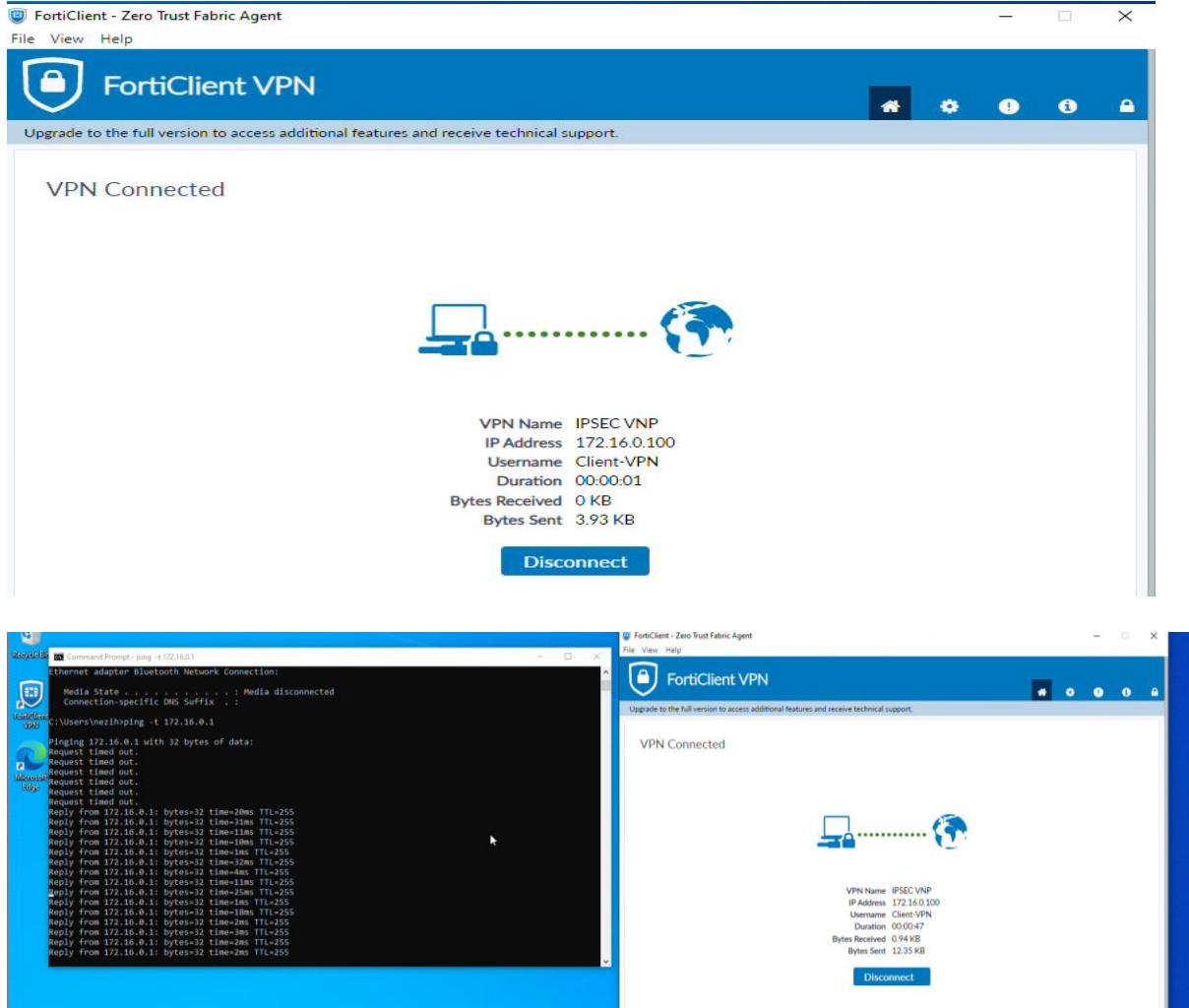


Figure 103 : Accès distant via VPN sur LAN

3.5 Conclusion

Ce chapitre a permis de déployer une infrastructure réseau sécurisée, surveillée et centralisée pour l'entreprise Mauritel. Grâce à VMware, GNS3, Zabbix, FortiGate et l'intégration d'Active Directory via LDAP, nous avons construit un réseau d'entreprise virtuel, segmenté et sécurisé. Le VPN sécurisé par IPSec offre un accès distant fiable et protégé, tandis que la gestion des utilisateurs via LDAP assure un contrôle centralisé des accès réseau. Cette solution complète répond aux besoins de sécurité, de gestion et de connectivité d'une entreprise moderne comme Mauritel, garantissant une infrastructure robuste et flexible.

Chapitre 4 : Résultats et analyse

Chapitre 4 : Résultats et analyse

4.1 Introduction

Dans ce chapitre, nous présentons les résultats de la supervision du réseau. Nous discutons des incidents détectés, comme les problèmes de trafic, les pannes de matériel et les tentatives d'intrusion. Ces incidents sont classés par type, gravité et heure d'occurrence, ce qui nous aide à identifier les vulnérabilités et les zones qui nécessitent une attention urgente.

4.2 Résultats de la supervision et incidents détectés

Dans cette section, nous analysons les données collectées par Zabbix, l'outil de supervision utilisé pour surveiller notre réseau. Les éléments suivis comprennent :

- Utilisation du processeur (CPU) : Indique le pourcentage d'utilisation du processeur sur chaque appareil.
- Utilisation de la mémoire (RAM) : Montre combien de mémoire est utilisée et combien est encore disponible.
- Espace disque : Surveille l'espace utilisé et disponible sur les disques des serveurs.

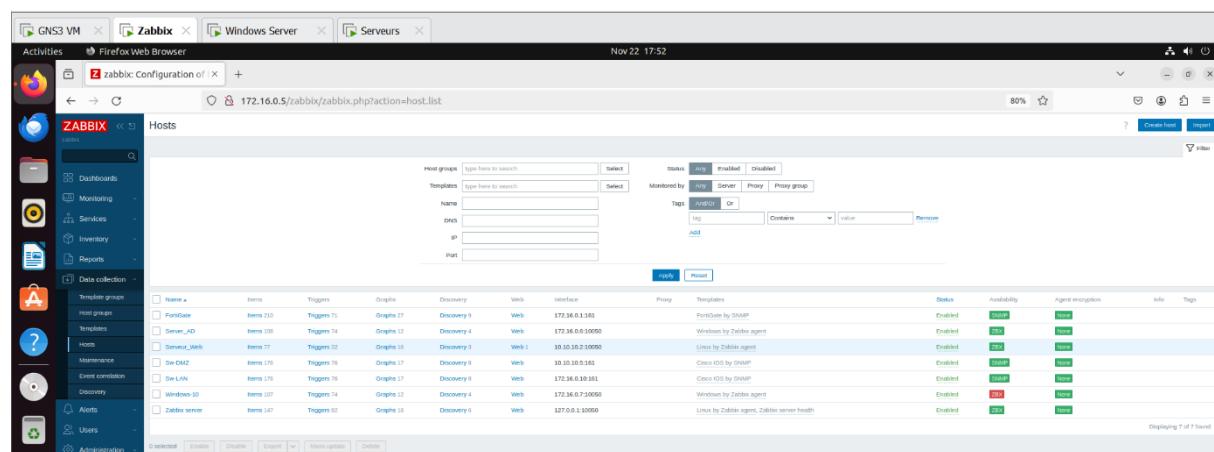


Figure 104 : Surveillance des Équipements

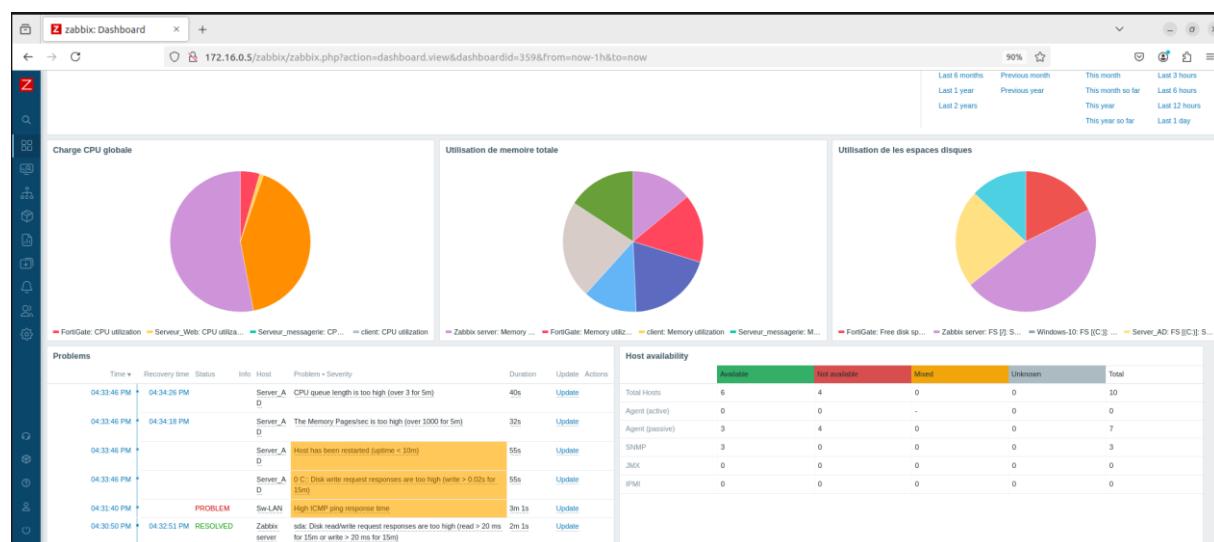


Figure 105 : Suivi des Performances de l'Infrastructure

Chapitre 4 : Résultats et analyse

Les alertes par e-mail envoyées par Zabbix nous informent de problèmes comme l'indisponibilité des agents Zabbix, des pannes de serveurs ou des redémarrages des machines. Chaque alerte précise le problème, l'heure à laquelle il s'est produit et l'action nécessaire pour le résoudre.

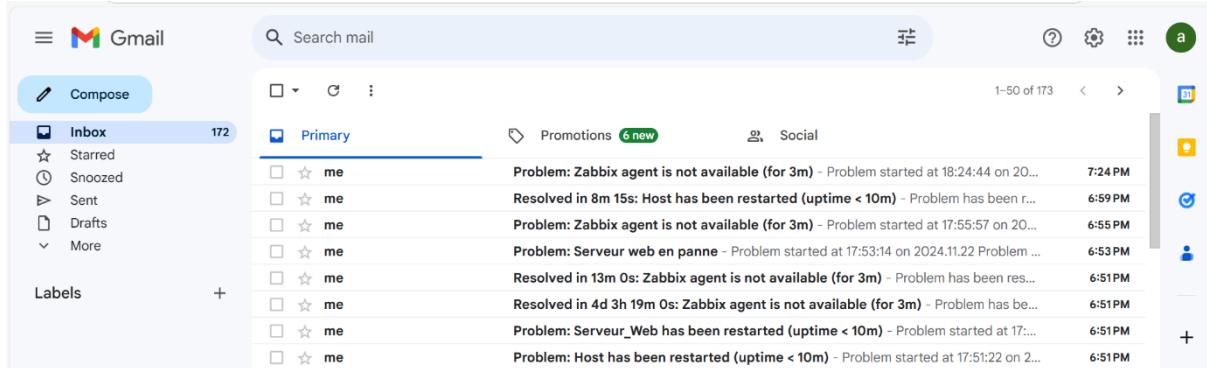


Figure 106 : Alertes par e-mail de Zabbix dans Gmail

4.3 Analyse des performances réseau sous supervision

Cette section analyse les performances du réseau, en utilisant des indicateurs comme la latence, la bande passante et la fiabilité du réseau. Nous avons utilisé des métriques telles que le temps de réponse, le taux de perte de paquets, et la stabilité des connexions pour évaluer l'efficacité du réseau.

4.3.1 Services Critiques

Nous avons vérifié le bon fonctionnement des services essentiels suivants :

- L'application web,
- Le serveur de messagerie,
- Les contrôleurs de domaine sous Windows Server.

Cela garantit leur disponibilité et leur performance continue, ce qui renforce la fiabilité du réseau.

4.3.2 Bande passante :

La bande passante mesure la quantité maximale de données qu'un réseau peut transférer à un moment donné. C'est un facteur important pour évaluer et améliorer les performances du réseau :

- Elle montre la capacité de transfert des données.
- Elle aide à identifier les goulots d'étranglement dans le réseau.
- Elle permet d'optimiser l'utilisation des ressources réseau pour assurer le bon fonctionnement des services critiques.

Chapitre 4 : Résultats et analyse

4.3.3 La latence :

La latence est le délai entre l'envoi d'une demande et la réception de la réponse. Cela affecte la rapidité des échanges sur le réseau :

- Mesure le délai de transmission des données.
- Évalue la réactivité du réseau.

4.3.4 Taux de perte de paquets

Le taux de perte de paquets correspond au pourcentage de paquets de données perdus ou non livrés lors du transit sur un réseau :

- Mesure l'efficacité du réseau à transmettre des données sans erreurs.
- Évalue les performances réseau.
- Un taux élevé peut nuire à l'expérience utilisateur, notamment pour les applications en temps réel.

Nous avons supervisé les services critiques dans Zabbix Server à l'aide des protocoles suivants :

- HTTP pour les serveurs web : Surveillance des performances et de la disponibilité des applications web via des requêtes HTTP pour garantir des temps de réponse rapides et des services accessibles.
- SNMP pour les serveurs de messagerie : Utilisation de SNMP pour vérifier la disponibilité et la performance des serveurs de messagerie, assurant ainsi une communication fluide.
- LDAP pour les contrôleurs de domaine : Surveillance des contrôleurs de domaine via le protocole LDAP afin d'assurer que les services d'authentification et de gestion des utilisateurs fonctionnent correctement.

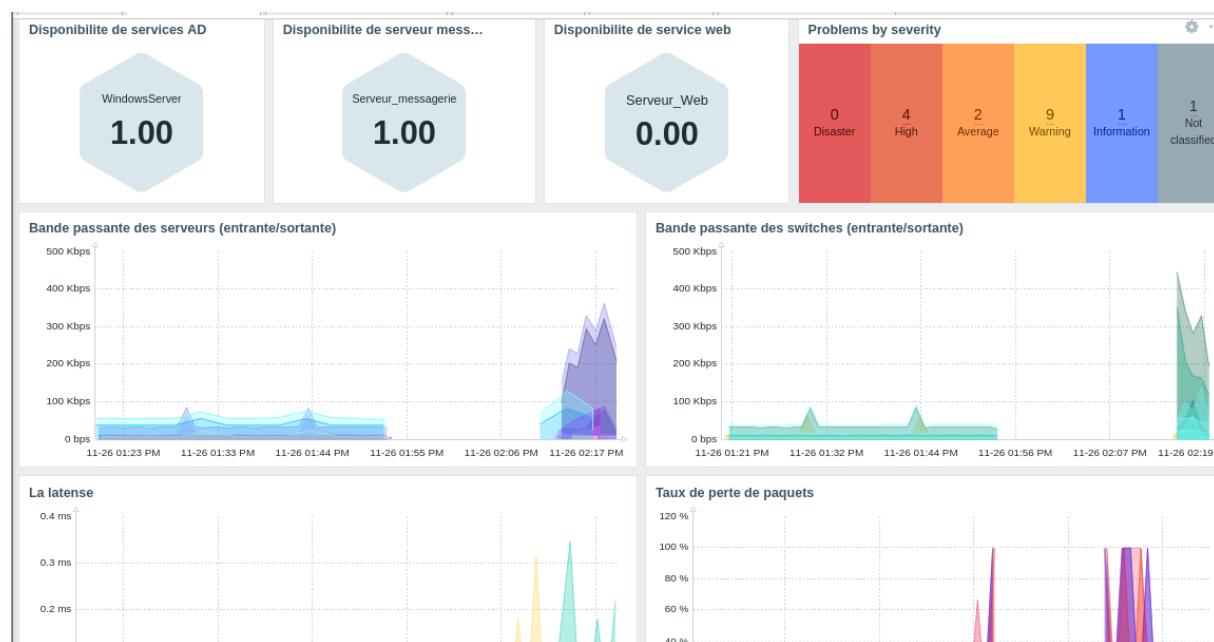


Figure 107 : Supervision des Performances Réseau et Services Critiques

4.4 Services DMZ accessibles depuis le LAN

Les services de la DMZ, comme le serveur web et le serveur de messagerie, offrent des fonctionnalités essentielles au LAN tout en garantissant une sécurité renforcée.

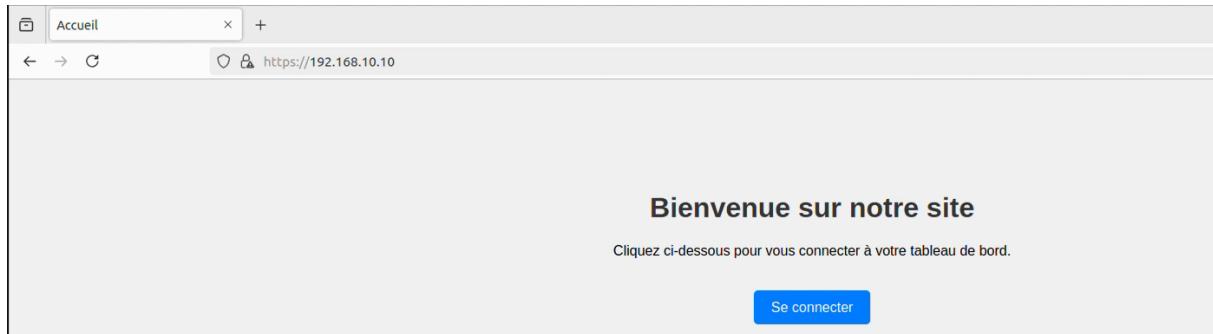


Figure 108 : Accès au serveur web depuis le LAN

L'interface de messagerie SOGo permet l'envoi d'e-mails entre les clients du LAN via un serveur de messagerie situé dans la DMZ. L'utilisateur "nezihe" prépare un message à destination de "brahim" avec le sujet "test_Demo".

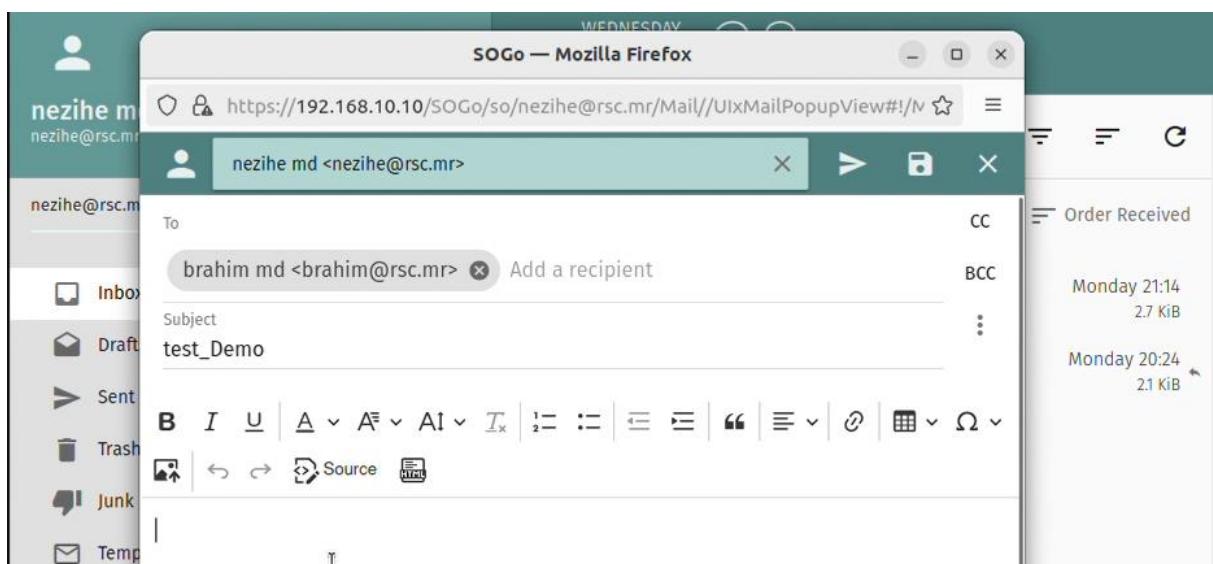


Figure 109 : Envoi d'e-mail entre les clients

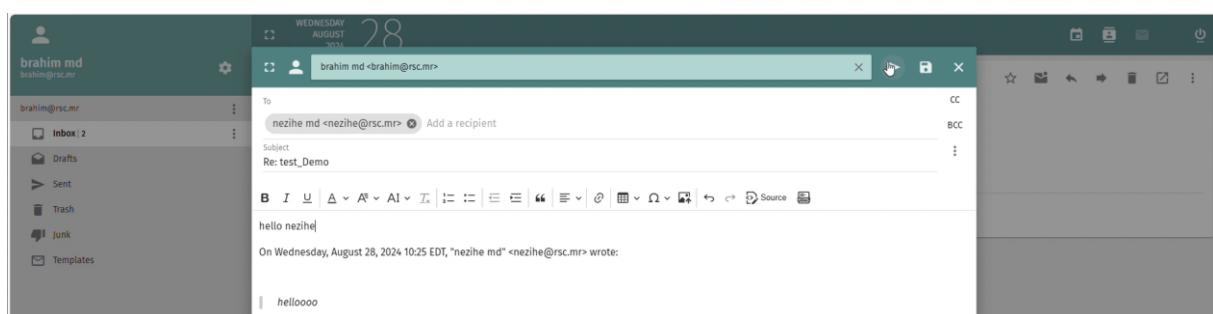


Figure 110 : Envoi d'e-mail entre les clients

4.5 Résultats des simulations d'attaques et contre-mesures

Dans cette section, nous détaillons les résultats des simulations d'attaques réalisées pour tester la résilience du réseau face à diverses menaces. Chaque simulation est décrite en termes de méthodologie, des types d'attaques simulées (par exemple, DDoS, phishing, malware), et des résultats obtenus. Nous expliquons également les contre-mesures appliquées et leur efficacité, offrant des recommandations basées sur ces résultats.

4.5.1 DoS (Denial of Service)

Une attaque par déni de service (DoS) vise à surcharger un serveur ou une ressource réseau pour rendre un service indisponible. Cela se fait en envoyant un grand nombre de requêtes ou de paquets de données, saturant ainsi le système.

Contre-mesures avec FortiGate :

- DoS Protection Policy : Configuration de politiques pour détecter et bloquer les anomalies de trafic, avec des seuils spécifiques pour des attaques comme SYN Flood, UDP Flood, ou ICMP Flood.
- Rate Limiting : Mise en place de limites de taux pour les requêtes afin de prévenir une surcharge excessive.

Politique limitant les paquets simultanés pour prévenir les attaques DoS/DDoS, comme les inondations TCP SYN et la détection de ports.

Name	<input type="text" value="DOS attack"/>
Incoming Interface	<input type="button" value="LAN (port2)"/>
Source Address	<input type="button" value="all"/> <input type="button" value="x"/>
Destination Address	<input type="button" value="all"/> <input type="button" value="x"/>
Service	<input type="button" value="ALL"/> <input type="button" value="x"/>

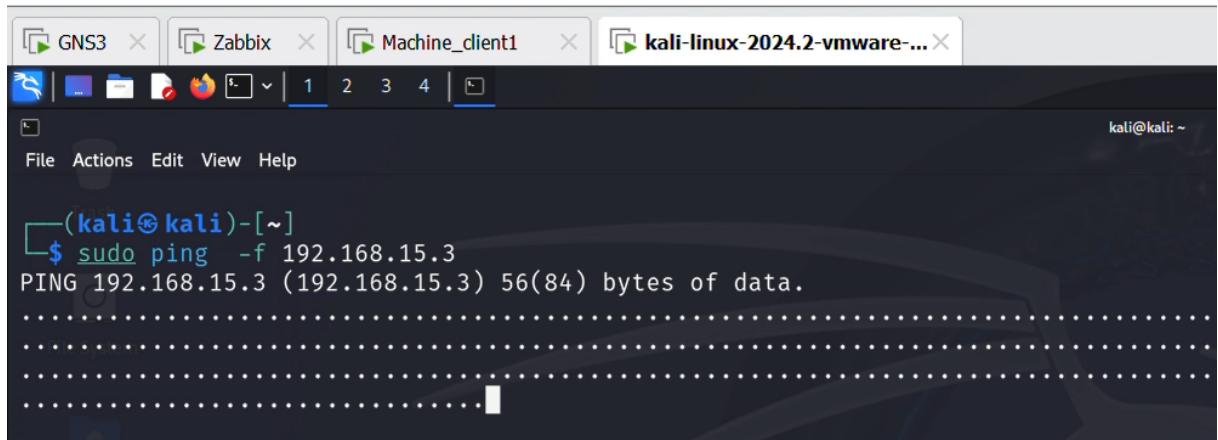
Figure 111 : Application de DoS

Name	Logging	Action			Threshold
		Disable	Block	Monitor	
tcp_syn_flood	<input checked="" type="checkbox"/>	<input type="button" value="Disable"/>	<input checked="" type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="text" value="20"/>
tcp_port_scan	<input checked="" type="checkbox"/>	<input type="button" value="Disable"/>	<input checked="" type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="text" value="20"/>
tcp_src_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="text" value="5000"/>
tcp_dst_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="text" value="5000"/>
udp_flood	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="text" value="2000"/>
udp_scan	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="text" value="2000"/>
udp_src_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="text" value="5000"/>
udp_dst_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="text" value="5000"/>
icmp_flood	<input checked="" type="checkbox"/>	<input type="button" value="Disable"/>	<input checked="" type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="text" value="20"/>

Figure 112 : Limitation des paquets contre DoS

Chapitre 4 : Résultats et analyse

L'attaque ICMP Flood inonde une cible de paquets ICMP pour surcharger ses ressources, simulant une attaque DoS dans un cadre de test contrôlé.

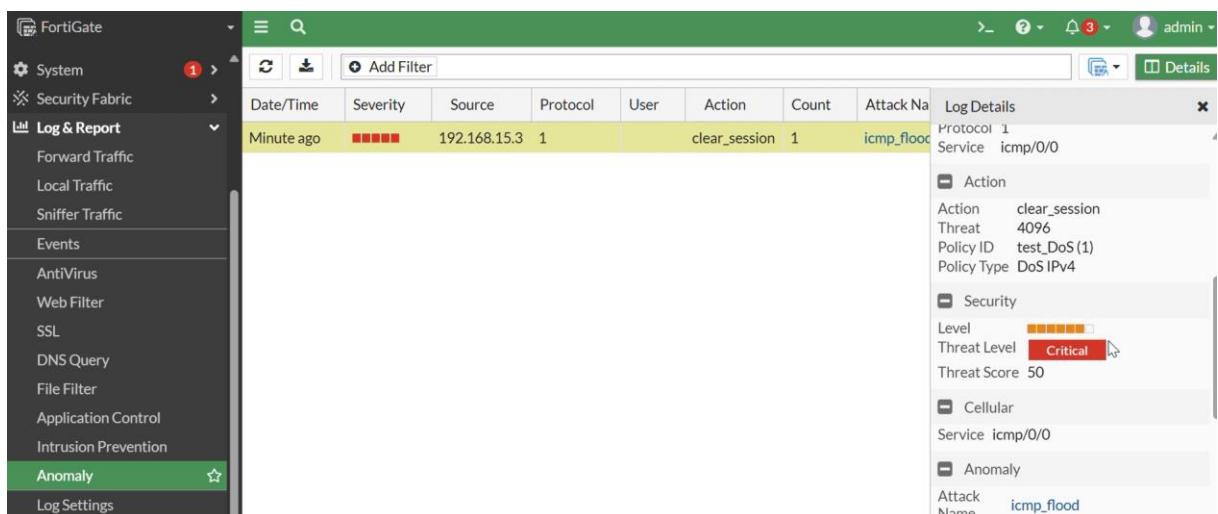


The screenshot shows a terminal window on a Kali Linux system. The command entered is `sudo ping -f 192.168.15.3`. The output shows the ping command running, with multiple dots indicating the continuous transmission of ICMP packets.

```
(kali㉿kali)-[~]
$ sudo ping -f 192.168.15.3
PING 192.168.15.3 (192.168.15.3) 56(84) bytes of data.
.
.
.
.
```

Figure 113 : Simulation d'une attaque ICMP Flood

FortiGate protège le réseau en détectant et bloquant les attaques comme l'ICMP Flood, rapidement générée grâce à sa politique DoS configurée.



The screenshot shows the FortiGate management interface under the 'Log & Report' section. A log entry is displayed for an ICMP flood attack. The log details are as follows:

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
Minute ago	██████	192.168.15.3	1		clear_session	1	icmp_flood

Log Details:

- Protocol: 1
- Service: icmp/0/0
- Action: clear_session
- Threat: 4096
- Policy ID: test_DoS (1)
- Policy Type: DoS IPv4
- Security Level: Critical
- Threat Score: 50
- Cellular Service: icmp/0/0
- Anomaly Attack Name: icmp_flood

Figure 114 : Détection et blocage d'une attaque ICMP Flood

4.5.2 Antivirus

Un antivirus est conçu pour détecter, prévenir, et éliminer les logiciels malveillants, tels que les virus, vers, chevaux de Troie, etc. (9)

Fonctionnement de l'antivirus :

- Détection : Analyse des fichiers et du trafic réseau pour repérer des signatures de logiciels malveillants connus.
- Prévention : Blocage ou isolation des menaces détectées avant qu'elles ne puissent infecter le système.

Chapitre 4 : Résultats et analyse

L'antivirus détecte, bloque et élimine les menaces comme virus et ransomwares.

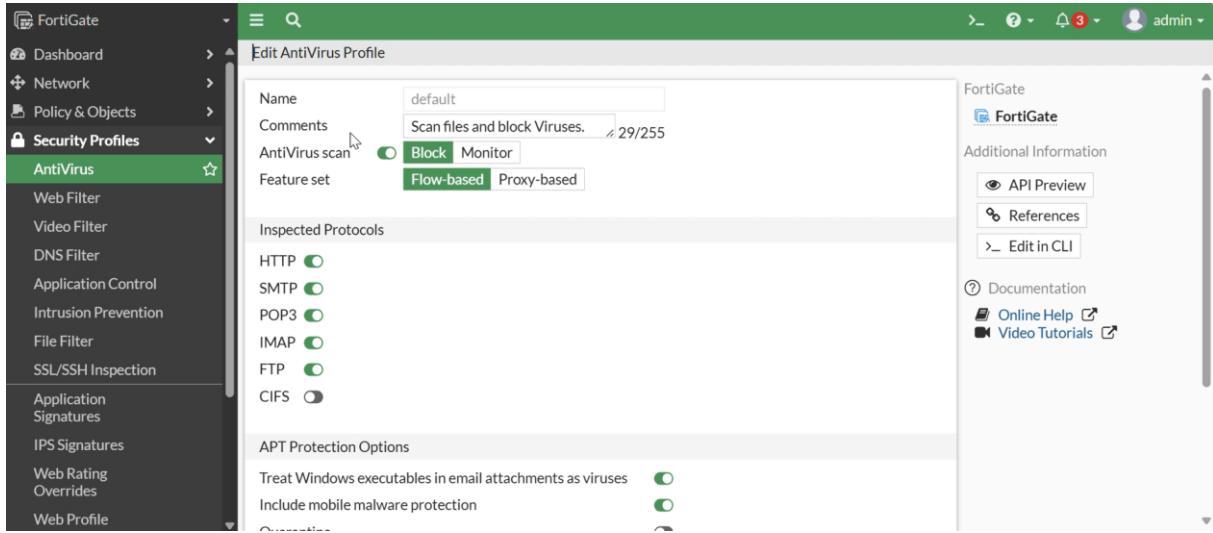


Figure 115 : Fonctionnement de l'antivirus

FortiGate bloque le téléchargement du fichier de test EICAR, démontrant ainsi l'efficacité de ses règles de filtrage pour prévenir l'accès aux fichiers malveillants dans le réseau.

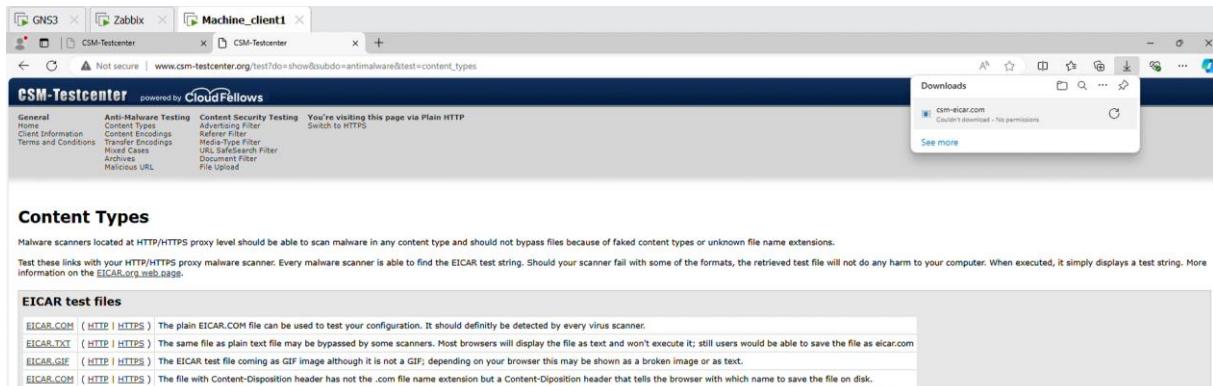


Figure 116 : Blocage du fichier EICAR par FortiGate

Date/Time	Source	File Name	Virus/Botnet	User	Details	Action
25 seconds ago	HTTP	192.168.15.3	csm-eicar.com	EICAR_TEST_FILE	URL: http://www.csm-testcenter.org/csm-...	blocked
30 seconds ago	HTTP	192.168.15.3	csm-eicar.com	EICAR_TEST_FILE	URL: http://www.csm-testcenter.org/csm-...	blocked
7 hours ago	HTTP	192.168.15.3	csm-eicar.com	EICAR_TEST_FILE	URL: http://www.csm-testcenter.org/csm-...	blocked
7 hours ago	HTTP	192.168.15.3	csm-eicar.com	EICAR_TEST_FILE	URL: http://www.csm-testcenter.org/csm-...	blocked
9 hours ago	HTTP	192.168.15.3	csm-eicar.com	EICAR_TEST_FILE	URL: http://www.csm-testcenter.org/csm-...	blocked

Figure 117 : Blocage du fichier EICAR par FortiGate

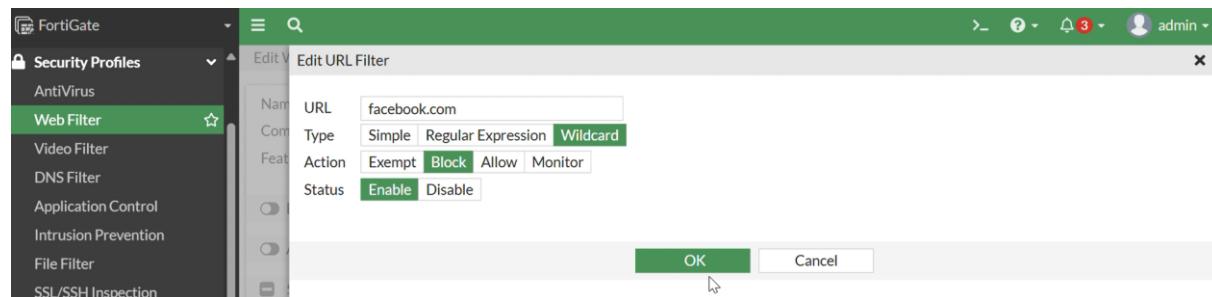
Chapitre 4 : Résultats et analyse

4.5.3 Web Filtre

Le filtrage web est une technologie qui contrôle l'accès des utilisateurs à des sites internet spécifiques pour renforcer la sécurité du réseau.

Fonctionnement du Web Filtre :

- Blocage** : Empêche l'accès à des sites non autorisés selon des politiques définies, comme les réseaux sociaux ou les contenus malveillants.
- Contrôle** : Réduit les risques liés à la navigation en ligne et garantit une utilisation conforme des ressources du réseau.



L'accès à "www.facebook.com" a été bloqué par une politique de sécurité FortiGate pour renforcer la sécurité du réseau.

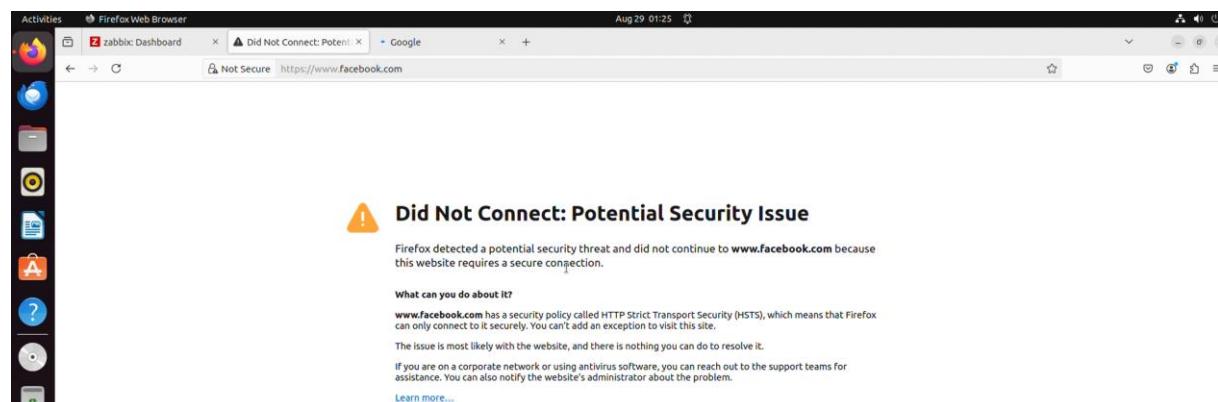


Figure 118 : Blocage d'accès à un site web via FortiGate

FortiGate bloque les tentatives d'accès à des sites indésirables, comme facebook.com, en appliquant des règles de filtrage d'URL, assurant ainsi la sécurité du réseau.

Date/Time	Source	Device	Destination	Application Name	Log Details
5 minutes ago	192.168.15.5	serveur-zabbix	192.168.10.10		
5 minutes ago	192.168.15.5	serveur-zabbix	34.107.243.93 (push.ser...		
5 minutes ago	192.168.15.5	serveur-zabbix	157.240.212.35 (fbsbx.c...		
5 minutes ago	192.168.15.5	serveur-zabbix	157.240.212.35 (fbsbx.c...		
5 minutes ago	192.168.15.5	serveur-zabbix	157.240.212.35 (fbsbx.c...		
6 minutes ago	192.168.15.5	serveur-zabbix	192.168.10.10		
6 minutes ago	192.168.15.5	serveur-zabbix	192.168.10.10		
7 minutes ago	192.168.15.5	serveur-zabbix	192.168.10.10		
7 minutes ago	192.168.15.5	serveur-zabbix	192.168.10.10		

Figure 119 : Blocage d'accès à Facebook par FortiGate

4.5.4 L'injection SQL (SQL Injection)

L'injection SQL est une technique d'injection de code malveillant dans des requêtes SQL via des entrées utilisateur, visant à accéder à des données sensibles ou à compromettre un serveur. (10)

Exemple d'injection SQL :

Supposons une requête SQL :

```
SELECT * FROM Users WHERE UserId = 'user_input';
```

Si un utilisateur saisit 105 OR 1=1, la requête devient :

```
SELECT * FROM Users WHERE UserId = '105 OR 1=1';
```

Cela permet de contourner les restrictions et d'accéder à toutes les données.

Prévention avec FortiGate :

- Signature d'intrusion : Utilisation de signatures d'intrusion pour détecter et bloquer les tentatives d'injection SQL en analysant les motifs de trafic réseau.

La configuration d'une IP virtuelle (VIP) sur FortiGate permet de rendre un serveur web dans la DMZ accessible depuis le WAN en utilisant le NAT statique.

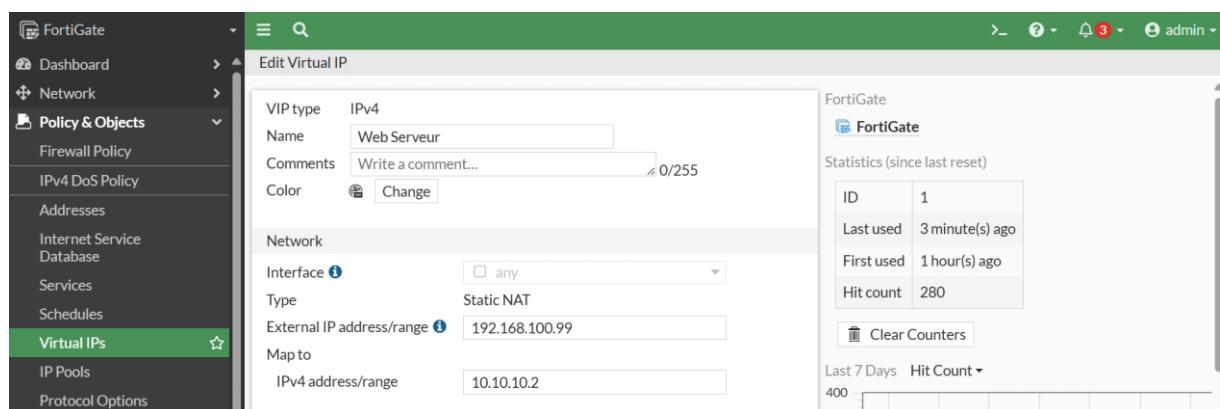


Figure 120 : IP Virtuelle pour l'Accès Web DMZ

L'injection SQL est une vulnérabilité exploitant des failles dans les requêtes aux bases de données, souvent présente dans des applications accessibles par WAN, permettant d'accéder ou de manipuler des données sensibles.

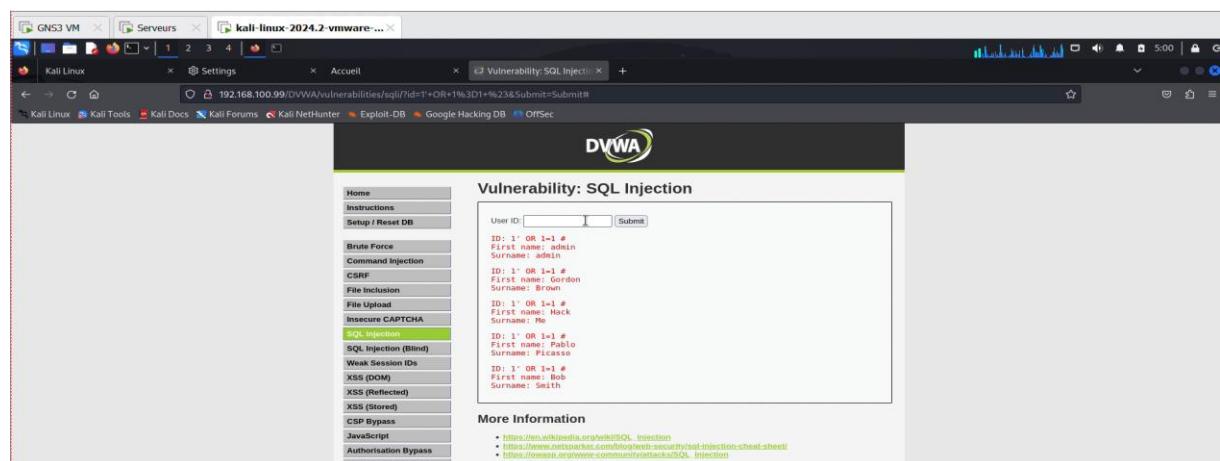


Figure 121 : DVWA accessible via WAN

Chapitre 4 : Résultats et analyse

Extraction de données depuis une base DVWA accessible via WAN grâce à une injection SQL.

```

kali@kali: ~/Downloads
[05:05:42] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[05:05:42] [INFO] resuming password 'abc123' for hash 'e99a18c428b28d5f26085367892e03'
[05:05:42] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fc69216b'
[05:05:42] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name | last_login | failed_login |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | /DVWA/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | admin | 2024-11-21 08:28:56 | 0 |
| 2 | gordonb | /DVWA/hackable/users/gordonb.jpg | e99a18c428b28d5f26085367892e03 (abc123) | Brown | Gordon | 2024-11-21 08:28:56 | 0 |
| 3 | i337 | /DVWA/hackable/users/i337.jpg | 8d3533d75ae2c3966d7e0d4fc69216b (charley) | Me | Hack | 2024-11-21 08:28:56 | 0 |
| 4 | pablo | /DVWA/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso | Pablo | 2024-11-21 08:28:56 | 0 |
| 5 | smithy | /DVWA/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob | 2024-11-21 08:28:56 | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
[05:05:42] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.100.99/dump/dvwa/users.csv'
[05:05:42] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[05:05:42] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[1 entry]
+-----+-----+
| comment_id | name | comment |
+-----+-----+
| 1 | test | This is a test comment. |
+-----+-----+
[05:05:42] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.100.99/dump/dvwa/guestbook.csv'
[05:05:42] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.100.99'

```

Figure 122 : Extraction de données DVWA

C'est une politique ou stratégie de sécurité utilisée pour prévenir les attaques des applications Web, notamment les injections SQL, vise à empêcher ces attaques, quelle que soit leur gravité.

The screenshot shows the Fortinet FortiGate interface under the 'Intrusion Prevention' tab. A modal window titled 'Add Signatures' is open, showing the configuration for a new signature:

- Type:** Block (radio button selected)
- Action:** Enable (radio button selected)
- Status:** Enable (radio button selected)
- Filter:** A dropdown menu showing several severity levels (SEV) with their corresponding color-coded icons.

Below the filter dropdown is a search bar and a table listing existing signatures:

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 5,864				Block	CVE-2005-0277
3Com.3CDaemon.FTPServer.Buffer.Overflow	██████	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTPServer.Information.Disclosure	███	Client	Windows	Pass	CVE-2005-0278

At the bottom right of the modal are 'OK' and 'Cancel' buttons.

Figure 123 : Prévention des attaques Web

Chapitre 4 : Résultats et analyse

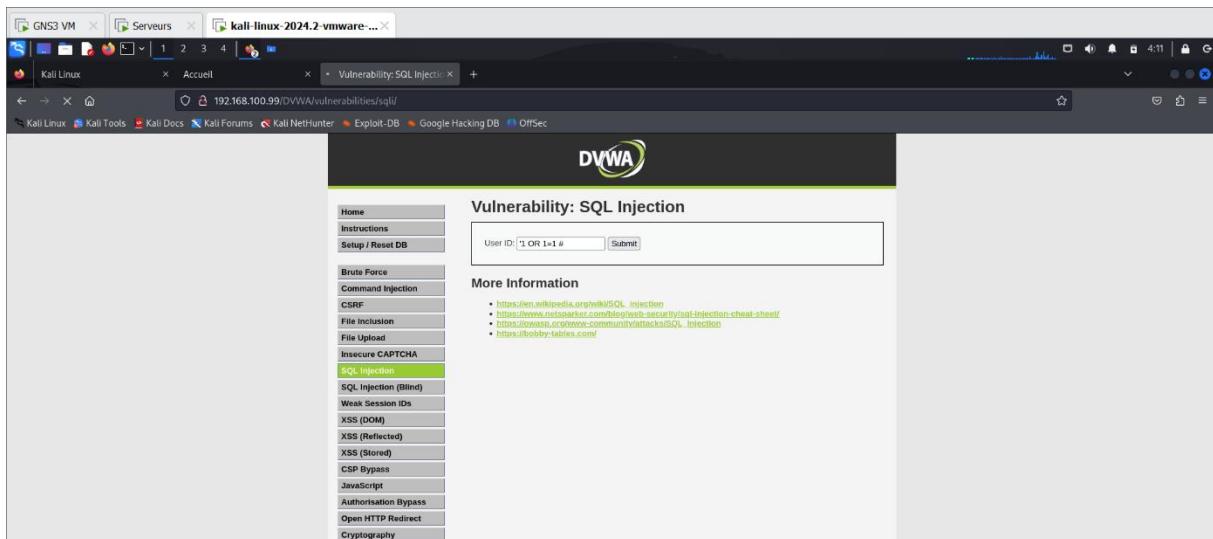


Figure 124 : Blocage d'accès via FortiGate

Le **journal de sécurité du FortiGate** suit les attaques bloquées, comme les tentatives d'injection SQL. Grâce à la **prévention avec FortiGate**, les **signatures d'intrusion** détectent et bloquent ces menaces en analysant le trafic réseau.

Intrusion Prevention								
Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name	
7 seconds ago	■■■■■	192.168.100.23	6		dropped		HTTP.URI.SQL.Injection	
23 seconds ago	■■■■■	192.168.100.23	6		dropped		HTTP.URI.SQL.Injection	
2 minutes ago	■■■■■	192.168.100.23	6		dropped		HTTP.URI.SQL.Injection	

Figure 125 : Prévention des injections SQL

4.6 Conclusion

Ce chapitre a mis en évidence l'efficacité des outils de supervision et des mesures de sécurité déployées dans l'environnement réseau. Grâce à l'analyse des performances et à la détection proactive des incidents, nous avons pu identifier des anomalies critiques, évaluer la fiabilité des services, et renforcer la résilience du réseau. Les simulations d'attaques ont permis de tester la robustesse des dispositifs de sécurité, notamment FortiGate, tout en proposant des contre-mesures adaptées. Les résultats obtenus soulignent l'importance d'une supervision continue pour optimiser les performances et garantir la disponibilité des services critiques. Cette approche contribue à réduire les risques et à maintenir un réseau sécurisé et performant.

Chapitre 4 : Résultats et analyse

CONCLUSION GÉNÉRALE

Le projet de fin d'étude intitulé "Analyse et optimisation de la performance du réseau de l'entreprise avec Zabbix et FortiGate" a permis de répondre efficacement aux besoins de performance, de sécurité et de connectivité de l'entreprise Mauritel. À travers une démarche rigoureuse et une méthodologie basée sur des outils modernes et éprouvés, nous avons pu concevoir et mettre en œuvre une infrastructure réseau optimisée et sécurisée.

Dans un premier temps, l'analyse approfondie de l'architecture existante a permis d'identifier les failles et limitations affectant les performances et la sécurité. Sur cette base, nous avons conçu une solution réseau adaptée aux besoins actuels et aux exigences futures de l'entreprise. L'intégration de Zabbix pour la supervision centralisée et de FortiGate pour la gestion avancée de la sécurité a joué un rôle déterminant dans l'amélioration de l'efficacité et de la robustesse du réseau.

Ensuite, l'étude des outils de virtualisation, de simulation, et des technologies de sécurité a offert un cadre théorique solide pour guider la mise en œuvre des solutions. Cette phase nous a permis de comparer plusieurs outils, de comprendre leurs spécificités, et de sélectionner ceux qui répondent le mieux aux besoins de l'entreprise. Des concepts clés comme les IDS/IPS, les VPN et la qualité de service (QoS) ont enrichi notre compréhension des enjeux de supervision et de sécurité dans un contexte d'entreprise.

Enfin, la mise en place d'une infrastructure réseau virtualisée et segmentée a permis d'intégrer des solutions avancées comme Active Directory via LDAP et un VPN sécurisé par IPSec. Les simulations et tests pratiques, notamment les scénarios d'attaques, ont validé l'efficacité des dispositifs déployés et la résilience de l'architecture face à des menaces potentielles.

En conclusion, ce projet a démontré que la combinaison d'outils comme Zabbix et FortiGate, soutenue par une méthodologie claire et des tests rigoureux, permet d'optimiser les performances, de renforcer la sécurité et de répondre aux besoins croissants en connectivité. Cette solution ne se limite pas à résoudre les problématiques actuelles de Mauritel, mais établit également des bases solides pour accompagner son évolution future dans un environnement technologique en constante mutation.

5 Bibliographie

- [1] 1. DataScientest. Nagios: Surveillance et Monitoring des Infrastructures IT. [En ligne] 2024. <https://datascientest.com/nagios-tout-savoir>.
- [2] 2. Zabbix LLC. Zabbix: The Enterprise-Class Monitoring Solution. *Zabbix*. [En ligne] Zabbix LLC, 2001-2024. <https://www.zabbix.com>.
- [3] 3. Fortinet, Inc.. FortiGate: Next-Generation Firewall Solutions. [En ligne] 2024. <https://www.fortinet.com>.
- [4] 4. IBM. Qu'est-ce qu'un IDS ? *IBM*. [En ligne] <https://www.ibm.com/fr-fr/topics/intrusion-detection-system>.
- [5] 5. —. Qu'est-ce qu'un IPS ? *IBM*. [En ligne] <https://www.ibm.com/fr-fr/topics/intrusion-prevention-system>.
- [6] 6. openclassrooms. *Simulez des architectures réseaux avec GNS3*. [En ligne] <https://openclassrooms.com/fr/courses/2581701-simulez-des-architectures-reseaux-avec-gns3>.
- [7] 7. blogs.vmware. vmware. *blogs.vmware*. [En ligne] <https://blogs.vmware.com/workstation/2024/05/vmware-workstation-pro-now-available-free-for-personal-use.html>.
- [8] 8. Wikimedia Foundation. Trello. *Wikipédia*. [En ligne] <https://fr.wikipedia.org/wiki/Trello>.
- [9] 9. Fortinet, Inc. Configuring an Antivirus Profile. *Fortinet Documentation*. [En ligne] <https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/922423/configuring-an-antivirus-profile>.
- [10] 10. —. SQL Injection. *Fortinet*. [En ligne] <https://www.fortinet.com/fr/resources/cyberglossary/sql-injection>.