République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de BEJAIA

Faculté des Sciences Exactes

Département d'informatique

Mémoire de fin de cycle

En vue de l'obtention du diplome de Master Professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Etude et mise en place d'une station de gestion et de surveillance à distance

Cas d'etude : "Entreprise Ngtmeziani" Campus NTS

Réalisé par :

M^{lle}. AMIROUCHE Damia et M^{lle}. ABDOUNE Katia

Devant le jury composé de :

Président	*M SALHI* Nadir	*U. A/Mira Bejaia.*
Examinateur	*M MOHAMMEDI* Mohamed	*U. A/Mira Bejaia.*
Encadrant	*M TOUAZI* Djoudi	*U. A/Mira Bejaia.*
Co-Encadrant	*M DJEBBARI* Yassine	*CAMPUS NTS*

Année Universitaire : 2022/2023

Remerciements

En premier lieu, nous souhaitons exprimer notre reconnaissance envers Dieu le Tout-Puissant pour nous avoir accordé la force, le courage et la patience nécessaire pour mener humblement à bien ce travail.

Nous tenons également à exprimer notre infinie gratitude et nos sincères remerciements à nos parents pour leurs sacrifices et leur soutien tout au long de nos études et de la réalisation de ce travail.

Nous remercions sincèrement notre encadrant, M^r TOUAZI Djoudi, pour ses précieux conseils, orientations, disponibilité, sympathie et le temps qu'il nous a accordé tout au long de notre projet.

Nos remerciements les plus chaleureux vont particulièrement à notre tuteur de stage, M^r Yassine DJEBBARI, pour son encadrement rigoureux et ses orientations tout au long de notre stage au sein du CAMPUS NTS.

Nous exprimons également notre reconnaissance envers chacun des membres du jury pour l'intérêt porté à notre travail en acceptant de l'examiner et de le compléter avec leurs propositions.

Nous tenons à remercier tous nos proches et amis qui nous ont soutenus et encouragés tout au long de notre parcours universitaire et de la réalisation de ce travail.

Enfin, nous souhaitons exprimer notre gratitude envers tous ceux qui ont contribué, directement ou indirectement, à l'élaboration de ce travail humble. Nous leur exprimons nos profondes gratitudes et notre respect.

DÉDICACE

À mes chers parents, mes éternels supporteurs et mes confidents dans cette vie,
Votre amour inconditionnel a été une source de force et de motivation tout au long de mon parcours. Je suis fiere d'être votre enfant et je vous remercie de m'avoir toujours soutenue pour donner le meilleur de moi-même et de m'avoir encouragée à réaliser mes rêves les plus ambitieux.

En ce jour de réussite où j'achève mes études, je vous dédie ce mémoire, symbole de mes efforts et de ma réussite. J'espère sincèrement que cela vous remplira de fierté et de bonheur, car cette réussite ne m'appartient pas seulement, elle est toute entière la vôtre.

À mes chers confidents, ma sœur et mon frère,
Votre rôle a été crucial dans ma réussite et cette victoire est également la vôtre. Votre présence a été un cadeau inestimable dans ma vie. Je vous remercie du fond du cœur pour votre amitié, votre soutien et votre amour.

À Katia ABDOUNE, ma binôme exceptionnelle et mon amie fidèle,
Notre réussite est le résultat de notre travail acharné et de notre dévouement. Je suis fiere de tout ce que nous avons accompli ensemble. Nous avons su relever des défis et surmonter des obstacles pour atteindre nos objectifs. Merci pour cette expérience inoubliable et je te souhaite le meilleur pour la suite de ta carrière.

À mes proches aimés et mes copines,
Merci d'avoir été là pour moi à chaque étape de ma vie. Votre amour, votre soutien et votre amitié ont été une source de réconfort et de joie pour moi, particulièrement dans les moments difficiles.

À mon encadrant M^r TOUAZI Djoudi et mon promoteur de stage M^r Yassine DJEBBARI, merci pour votre précieux soutien, vos conseils avisés et votre expertise. Votre contribution a été essentielle dans la réussite de ce projet.

Damia AMIROUCHE.

DÉDICACE

À mes chers parents, ma source d'amour et de soutien infinis,

Votre soutien inconditionnel et votre confiance en moi ont été les piliers de mon parcours. Cette dédicace de mémoire est un humble témoignage de ma gratitude éternelle envers vous. Que cette réussite soit également la vôtre.

À mes chères sœurs et cher frère, mes complices de vie,

Votre présence à mes côtés a rendu chaque étape de cette aventure plus douce et mémorable. Cette dédicace de mémoire vous est dédiée en reconnaissance de notre lien familial unique et précieux.

À ma binôme, Damia Amirouche, ma partenaire indissociable,

Cette dédicace de mémoire est une célébration de notre collaboration exceptionnelle. Notre entente, notre complémentarité et notre persévérance ont fait de chaque défi une opportunité de grandir et d'apprendre ensemble.

À ma chère copine, Hadil Boulaouad, ma fidele confidente,

Cette dédicace de mémoire est un hommage à notre amitié précieuse. Ta bienveillance, ta perspicacité et ta douceur m'ont permis de surmonter les défis avec confiance. Puissions-nous continuer à partager de nombreux moments merveilleux ensemble.

À mon encadrant Djoudi Touazi et mon promoteur de stage Yacine Djebbari, les guides éclairés.

Je tiens à exprimer ma profonde gratitude pour votre expertise, votre guidance et votre bienveillance tout au long de ce stage. Je vous remercie du fond du cœur pour votre précieuse contribution.

Katia ABDOUNE.

Table des matières

Liste des Figures

Liste des Tableaux

Liste des Abbreviations

API	Application Programming Interface.
AVG	Anti-Virus Guard.
AH	Authentication Header.
CI/CD	Continuous Integration/Continuous Delivery.
CCNA	Cisco Certified Network Associate.
CCNP	Cisco Certified Network Professional.
C	The C Programming Language.
C#	C Sharp.
CSS	Cascading Style Sheets.
COW	Copy On Write.
DMZ	Demilitarized Zone.
DDOS	Distributed Denial Of Service.
DNS	Domain Name System.
ESP	Encapsulating Security Payload.
FTP	File Transfer Protocol.
FTTH	Fiber to the Home.
FTTX	Fiber to the X.
FCAPS	Fault Configuration Accounting Performance and Security.
GNS3	Graphical Network Simulator-3.
HIPS	Host Intrusion Prevention System.
HIDS	Host-Based Intrusion Detection System.
HTML5	HyperText Markup Language 5.
HTTP	Hyper Text Transfer Protocol.
IP	Internet Protocol.
IOS	International Organization for Standardization.
ICMP	Internet Control Message Protocol.
IT	Information Technology.
IA	Artificial Intelligence.
IPS	Intrusion Prevention System.
IDS	Intrusion Detection System.
IKE	Internet Key Exchange.
IPSEC	Internet Protocol Security.
IEC	International Electrotechnical Commission.
ISMS	Information Security Management System.
LAN	Local Area Network.
LACP	Link Aggregation Control Protocol.
MIB	Management Information Base.
MACOS	Media Access Control Operating System.
ML	Meta Langage.

MAC	Media Access Control.
MAN	Metropolitan Area Network.
NIPS	Network Intrusion Prevention System.
NIDS	Network-Based Intrusion Detection System.
NBA	Network Behavior Analysis Program.
NTS	New Technology et Solutions.
NETOPS	Network Operations.
NFV	Network functions virtualization.
NAT	Network Address Translation.
OSI	Open Systems Interconnection.
OAUTH	Open Authorization.
POODLE	Padding Oracle On Downgraded Legacy Encryption.
PPP	Point-to-Point Protocol.
PHP	Hypertext Preprocessor.
GDPR	General Data Protection Regulation.
SSO	Single Sign-On.
SI	Information System.
SQL	Structured Query Language.
STP	Secure Tunneling Protocol.
SA	Security Association.
SYSLOG-NG	Next-generation System Log Manager.
SYSLOG	System Logging Protocol.
S&R	Synchronizing Resources.
SLA	Service Level Agreement.
SSL	Secure Socket Layer.
SMTP	Simple Mail Transfer Protocol.
SSH	Secure Shell.
SNMP	Simple Network Management Protocol.
SMS	Short Message System.
TCP/IP	Transmission Control Protocol/Internet Protocol.
TLS	Transport Layer Security.
UDP	User Datagram Protocol.
UTM	Unified Threat Management.
VLAN	Virtual Local Area Network.
VTP	VLAN Trunk Protocol.
VPN	Virtual Private Network.
WAN	Wide Area Network.
WIPS	Wireless Intrusion Prevention System.
YAML	Yet Another Markup Language.
2FA	TWO-FACTOR AUTHENTICATION.

Introduction générale

L'informatique est aujourd'hui un élément clé pour le fonctionnement des entreprises, les réseaux informatiques sont devenus indispensables pour permettre aux utilisateurs d'accéder aux services et aux données. Cependant, la sécurité des réseaux est devenue un enjeu majeur, avec l'augmentation des cyberattaques et des menaces externes.

Dans ce contexte, ce mémoire a pour objectif d'analyser les besoins de l'entreprise ngtmeziani en matière de gestion de réseau, ainsi que d'étudier une solution sur l'automatisation et la supervision de ses réseaux. Le mémoire se compose de quatre parties principales :

En premier, nous avons l'état de l'art sur les réseaux et la sécurité informatique : cette partie examine les différentes technologies et normes utilisées pour les réseaux informatiques, ainsi que les différentes menaces et vulnérabilités auxquelles les réseaux sont confrontés.

Deuxiement, étude et analyse des besoins : cette partie présente une analyse détaillée des besoins de l'entreprise ngtmeziani en matière de gestion de réseau. Nous examinons les équipements existants, les exigences de performance, les objectifs de sécurité, et les contraintes budgétaires.

Ensuite, l'automatisation et la supervision des réseaux : cette partie explore les différentes solutions d'automatisation et de supervision des réseaux, telles que Ansible, Puppet, Nagios et Zabbix. Nous examinons les avantages et les inconvénients de chaque solution, ainsi que leur pertinence pour répondre aux besoins de l'entreprise ngtmeziani.

Enfin, la mise en œuvre des solutions retenues : cette partie décrit la mise en œuvre des solutions retenues pour répondre aux besoins de l'entreprise ngtmeziani. Nous présentons les étapes de mise en œuvre, les problèmes rencontrés, et les résultats obtenus.

En somme, ce mémoire vise à fournir une analyse approfondie de la supervision et la gestion du réseau, ainsi que des solutions disponibles pour répondre aux besoins de l'entreprise ngtmeziani. La mise en œuvre de ces solutions contribuera à améliorer la fiabilité, la performance et la sécurité du réseau de l'entreprise.

Chapitre 1

Etats d’arts sur les réseaux et la sécurité informatique

1.1 Introduction

De nos jours, la communication et la technologie ont pris une place prépondérante dans la société, ce qui entraîne une croissance et un développement continus des réseaux informatiques pour l'avenir. Dans ce contexte, la sécurité informatique est devenue un enjeu majeur pour toute organisation qui utilise un réseau informatique, dans le but de protéger les données et les systèmes contre les menaces potentielles.

Dans cette optique, il est primordial de maîtriser les bases des réseaux et de la sécurité informatique, notamment les différentes topologies, les modèles OSI et TCP/IP, ainsi que les équipements d'interconnexion. Par ailleurs, il convient d'identifier les critères de sécurité et les meilleures pratiques pour les garantir. C'est précisément l'objet de ce chapitre.

1.2 Les réseaux informatiques

1.2.1 Définition

Un réseau informatique est composé d'une série de dispositifs électroniques connectés les uns aux autres, permettant ainsi le partage de ressources et de données. Ces réseaux peuvent faciliter la communication et la collaboration entre les utilisateurs, ainsi que l'accès à des services et des applications à distance.[1]

1.2.2 Intérêt des réseaux d'entreprise

- Les réseaux informatiques d'entreprise permettent le partage de données et de logiciels entre tous les membres d'une entreprise.[2]
- Ils simplifient également la gestion, la sauvegarde et le stockage des données, ainsi que la configuration des différents droits pour assurer la sécurité.[2]
- Sans le réseau informatique, il serait impossible de fonctionner de manière efficace.[2]
- Par conséquent, les professionnels spécialisés dans ce domaine sont d'une importance cruciale au sein des entreprises de toutes tailles.[2]

1.2.3 Classification des réseaux informatiques

Les réseaux informatiques peuvent être classifiés selon leur étendue géographique, leur topologie et leur méthode de transmission de données. En ce qui concerne l'étendue géographique :

LAN : Il s'agit d'un réseau local qui relie des équipements situés dans un même bâtiment ou campus, souvent utilisé par une entreprise ou une organisation.[1]

MAN : Le réseau étendu est similaire à un LAN en plus grand, et peut être public ou privé, couvrant un campus, une ville ou même une région géographique.[1]

WAN : Le réseau métropolitain permet de connecter des réseaux locaux sur de longues distances, souvent utilisé par des entreprises ayant des succursales situées dans différentes villes ou pays.[1]

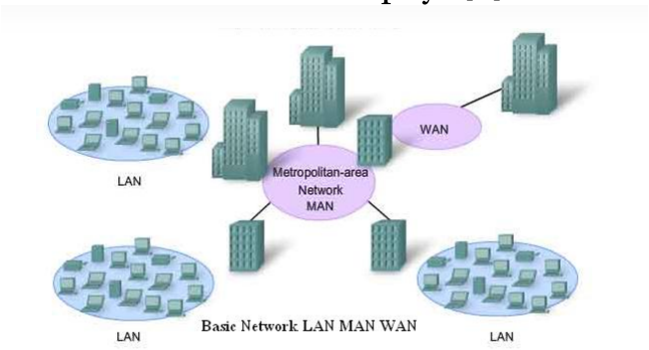


FIGURE 1.1 – Classification des réseaux informatiques.

1.2.4 Types de réseau

1. L'intranet est un réseau interne à l'organisation qui n'est accessible qu'aux employés de celle-ci.[2]
2. Internet est un réseau public et accessible à tous.[2]
3. L'extranet permet à des utilisateurs externes d'accéder de manière limitée et sécurisée à l'intranet, en utilisant Internet comme canal de communication.[2]

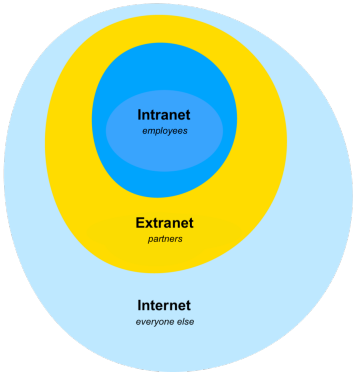


FIGURE 1.2 – Type de réseaux.

1.2.5 Les normes de communication réseau

A. Le modèle OSI (**O**pen **S**ystems **I**nterconnection) :

Le modèle OSI est une architecture de référence qui permet de décrire les communications dans les réseaux informatiques.[2]

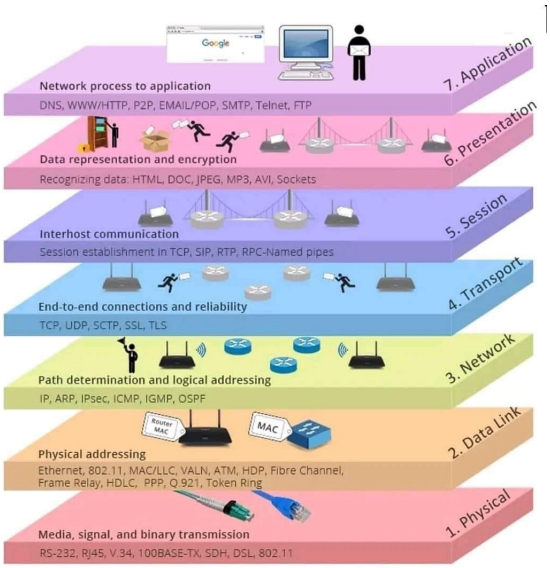


FIGURE 1.3 – Le modèle OSI.
[24]

Il définit 7 couches :

1. **La couche physique :** Elle gère les aspects matériels des connexions, tels que les câbles, les cartes réseau, etc.[1]
2. **La couche liaison :** Elle gère l'accès au support physique, en utilisant notamment les adresses MAC et en assurant la détection d'erreurs.[1]

3. **La couche réseau :** Elle gère l'adressage des machines en utilisant les adresses IP et assure l'acheminement des paquets de données.
4. **La couche transport :** Elle assure le contrôle de flux et la correction d'erreurs entre les applications réseau fonctionnant sur des hôtes distants.[2]
5. **La couche session :** Elle gère l'établissement, la gestion et la fin des sessions entre les applications.[2]
6. **La couche présentation :** Elle gère les formats de données, notamment la compression et le cryptage.[2]
7. **La couche application :** Elle définit les protocoles utilisés par les applications réseau, tels que HTTP, FTP, SMTP, etc.[2]

Le principal avantage du modèle OSI est de fournir un cadre de référence pour faciliter la conception et l'interopérabilité des réseaux informatiques.

B. Le modèle TCP/IP : (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol)
Le modèle TCP/IP est le modèle de référence utilisé par Internet ainsi que la plupart des réseaux informatiques actuels.[2]
Il comprend 4 couches principales :

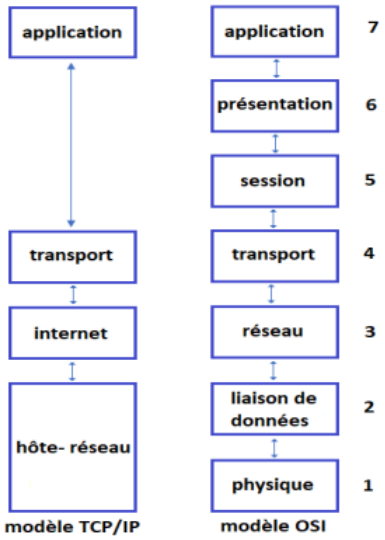


FIGURE 1.4 – Modèle TCP/IP comparé au modele OSI.

1. **La couche liaison :** Tout comme le modèle OSI, le modèle TCP/IP gère l'accès au support physique et les adresses MAC.
2. **La couche internet :** Le modèle TCP/IP gère l'adressage IP des machines, l'acheminement et le routage des paquets de données. Cette gestion correspond aux couches réseau et transport du modèle OSI.
3. **La couche transport :** Elle assure la fiabilité de la transmission des données entre les hôtes du réseau, en utilisant les protocoles TCP et UDP.
4. **La couche application :** Le modèle TCP/IP définit les protocoles utilisés par les applications réseau, tels que HTTP, FTP, SMTP, etc. Cette gestion correspond aux couches session, présentation et application du modèle OSI.

Le modèle TCP/IP est largement utilisé dans les réseaux informatiques, notamment sur Internet. Il est plus simple que le modèle OSI et est mieux adapté aux réseaux IP, ainsi, il est moins rigoureux en matière de normalisation et de définition des couches. Parmi les organisations utilisant TCP/IP :

— Les opérateurs de centres de données qui utilisent le modèle TCP/IP pour gérer et contrôler le trafic réseau au sein de leurs centres de données.

1.2.6 Architecture réseau

Il existe deux types de réseaux LAN :

1. Réseaux poste à poste.
2. Réseaux avec client/serveur.

   a)L'architecture poste à poste : C'est la plus simple, elle est constituée uniquement de clients (ordinateurs personnels) isolés les uns des autres, sans connexion réseau ni ressources partagées. Cette architecture convient aux petites structures ayant des besoins limités.[1]

b) L'architecture client/serveur : Elle implique la présence d'un serveur central auquel tous les clients (postes de travail) sont connectés via un réseau local. Le serveur centralise les ressources partagées telles que les fichiers, les imprimantes et les applications, et les rend accessibles aux clients.[2]
L'architecture client/serveur est beaucoup plus puissante que l'architecture poste à poste et convient mieux aux besoins des organisations modernes, au détriment d'une plus grande complexité. Elle nécessite la mise en place d'un serveur central et d'un réseau local.

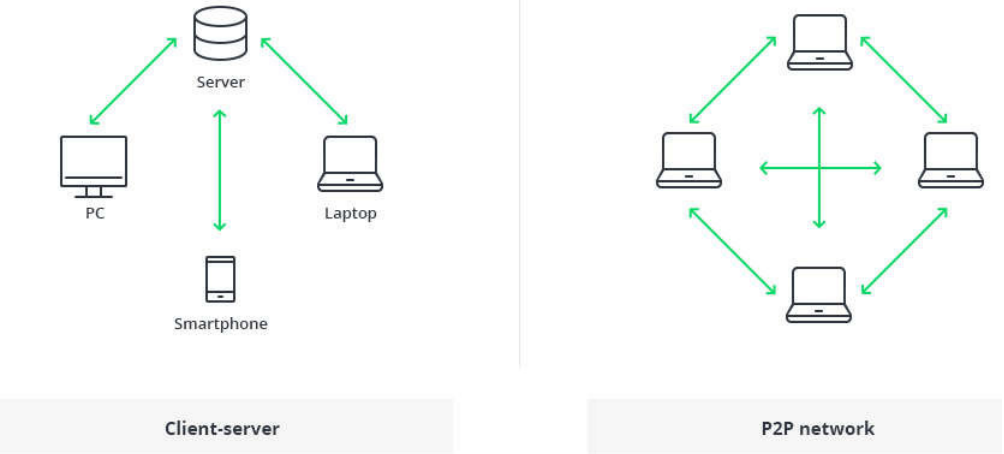


FIGURE 1.5 – Différence entre l'architecture client-serveur et poste à poste.

1.2.7 Alternative de raccordement

Equipements physique : Les équipements physiques requis pour créer un réseau informatique varient en fonction de la taille et de la complexité du réseau.

1. **Equipements d'interconnexion :**

   • **Les terminaux :** Les terminaux sont des périphériques ou des appareils qui sont effectivement connectés au réseau, et leur diversité ne cesse d'augmenter avec l'évolution des technologies. Cependant, leur rôle reste le même : permettre aux utilisateurs d'accéder aux ressources et aux services du réseau. Les terminaux mobiles tels que les smartphones et les tablettes représentent une part de plus en plus importante du trafic réseau, ce qui nécessite une réflexion sur la réarchitecture et la sécurité des réseaux.[1]

FIGURE 1.6 – Les terminaux.

• **Switch :** Il assure l'interconnexion des ordinateurs, des serveurs et des autres équipements du réseau local (LAN) en opérant au niveau de la couche liaison de données (couche 2). Il filtre et dirige le trafic réseau en fonction des adresses MAC.[1]

FIGURE 1.7 – Switch.

• **Router :** Il assure l'interconnexion de différents réseaux, qu'ils soient locaux ou étendus, en opérant au niveau de la couche réseau (couche 3). Il achemine les paquets IP en fonction des adresses IP, ce qui permet de relier des LAN distants.[1]

FIGURE 1.8 – Router.

2. **Topologie physique :** La topologie physique d'un réseau informatique décrit la manière dont les différents ordinateurs, serveurs et équipements sont connectés les uns aux autres physiquement.
   Les principales topologies physiques sont :
   • **Bus :** C'est une configuration de réseau très simple qui relie tous les appareils à un câble commun, permettant ainsi des liaisons de transmission et une seule liaison sur laquelle un seul ordinateur peut envoyer des données à la fois.[3]

• **Anneau :** Les équipements sont connectés les uns aux autres pour former un anneau dans cette topologie. Cette configuration est plus résiliente car elle permet de maintenir la connectivité du réseau même si un lien tombe en panne.[3]

• **Etoile :** Tous les équipements sont connectés à un point central, qui est généralement un commutateur ou un concentrateur. Cette topologie est actuellement la plus courante, en particulier dans les réseaux Ethernet.[3]

• **Arbre :** Il s'agit d'une topologie multi-niveaux, où les équipements sont connectés à différents niveaux. Cette configuration est souvent utilisée dans les grands réseaux d'entreprise.[3]

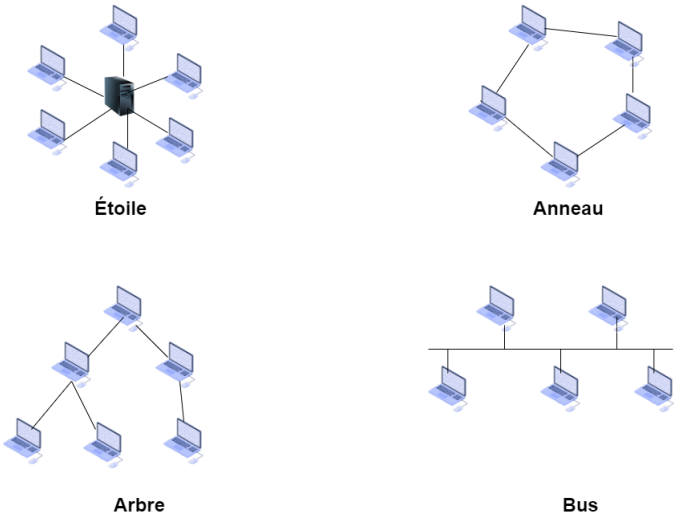


FIGURE 1.9 – Topologie physique.

1.3 La sécurité informatique

1.3.1 Définition

La sécurité informatique englobe toutes les mesures visant à protéger les systèmes d'information et les données contre les menaces et les attaques.[4]
Elle inclut :

- La protection des réseaux et des systèmes contre les intrusions.[4]
- La protection des données grâce à des techniques de chiffrement et des contrôles d'accès.[4]
- La sécurité des terminaux contre les virus et les logiciels malveillants.[4]
- La gestion des identités numériques et des accès.[4]
- La conformité aux réglementations de sécurité telles que le RGPD.[4]

1.3.2 Critères de la sécurité informatique

Les critères suivants sont utilisés pour mesurer la qualité et l'efficacité d'un système de sécurité informatique. Ils doivent être pris en compte tout au long du cycle de vie d'un système d'information, de sa conception à son exploitation.
Les principaux critères couramment utilisés pour évaluer la sécurité des systèmes informatiques sont :

FIGURE 1.10 – Critères de la sécurité informatique.

• **Confidentialité :** Elle vise à garantir que seules les personnes autorisées ont accès aux informations et aux systèmes en utilisant des mécanismes d'authentification et de chiffrement.[5]
• **L'intégrité :**Elle assure que les informations et les systèmes ne sont pas modifiés de manière inappropriée ou sans autorisation en utilisant des contrôles d'intégrité et des mécanismes de détection de modifications.[5]
• **La disponibilité :** Elle garantit que les utilisateurs autorisés ont accès aux informations et systèmes quand ils en ont besoin. Elle implique la mise en place de redondances, de plans de reprise après sinistre et d'une surveillance de la disponibilité des services.[5]
• **La traçabilité :** Elle permet de retracer les actions effectuées sur un système en identifiant qui a fait quoi, quand et comment. Elle utilise des journaux d'événements détaillés et des techniques d'authentification forte.[5]

1.3.3 Normes de sécurité

La norme ISO/CEI 27000, également appelée famille de normes ISMS ou ISO 27k, est un ensemble de normes internationales publiées conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) pour la gestion sécurisée de certains types d'informations.[5] Les normes ISO 27000 couvrent plusieurs aspects de la sécurité de l'information, notamment :

FIGURE 1.11 – Les standards de SMSI.

• **ISO/IEC 27001 :** La norme ISO 27001 est la norme phare de la série ISO 27000 et définit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI).[7]

• **ISO/IEC 27002 :** Auparavant connue sous le nom d'ISO 17799, la norme ISO 27002 propose des recommandations et des contrôles de sécurité à mettre en place dans le cadre d'un SMSI conforme à la norme ISO 27001.

• **ISO/IEC 27003 :** La norme ISO 27003 fournit des recommandations pour la mise en place d'un SMSI conforme à la norme ISO 27001.

• **ISO/IEC 27004 :** La norme ISO 27004 permet de mesurer l'efficacité d'un SMSI en fournissant des directives pour évaluer et améliorer en permanence un système de management de la sécurité.

• **ISO/IEC 27005 :** La norme ISO 27005 aide dans la gestion des risques en matière de sécurité de l'information, en fournissant un guide pour l'évaluation et le traitement des risques.[7]

• **ISO/IEC 27006 :** La norme ISO 27006 définit les exigences pour les organismes de certification et d'évaluation des SMSI.

• **ISO/IEC 27007 :**La norme ISO 27007 fournit des lignes directrices pour auditer la conformité d'un SMSI par rapport à la norme ISO 27001.[1]

1.3.4 Outils et systèmes d'authentification

Les systèmes et outils d'authentification sont des mécanismes qui permettent de vérifier l'identité des utilisateurs qui accèdent aux systèmes informatiques ou aux applications en ligne.
Les systèmes et outils d'authentification les plus fréquemment utilisés sont :

• **Nom d'utilisateur et mot de passe :** L'authentification par nom d'utilisateur et mot de passe est la méthode la plus courante. Elle nécessite que l'utilisateur entre son nom d'utilisateur et un mot de passe qu'il est le seul à connaître. Toutefois, les mots de passe présentent de nombreuses vulnérabilités.[7]

FIGURE 1.12 – Authentification avec nom d'utilisateur et mot de passe.

• **Authentification à deux facteurs (2FA) :** L'authentification à deux facteurs consiste à associer deux éléments parmi ce que vous possédez (mot de passe), ce que vous connaissez (PIN) et ce que vous êtes (biométrie). Cette méthode est considérée comme très sécurisée.[7]

FIGURE 1.13 – Authentification à deux facteurs.

• **Authentification biométrique :** L'authentification biométrique repose sur les caractéristiques physiques ou comportementales uniques de l'utilisateur, telles que l'empreinte digitale, la reconnaissance faciale, de l'iris ou vocale. Cette méthode est considérée comme l'une des plus sécurisées.[8]

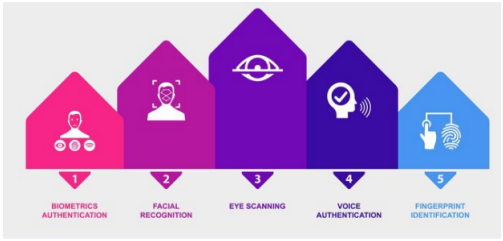


FIGURE 1.14 – Authentification biométrique.

• **Certificats numériques :** L'authentification par certificat numérique consiste à vérifier l'identité des utilisateurs à l'aide d'un certificat numérique délivré par une autorité de certification.[8]

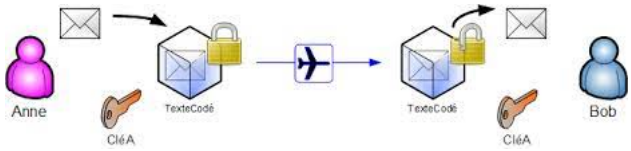


FIGURE 1.15 – Certificats numériques.

• **SSO (Single Sign-On) :** L'authentification unique (SSO) est une méthode qui permet à un utilisateur de s'authentifier une seule fois pour accéder à plusieurs systèmes ou applications en ligne.[8]

FIGURE 1.16 – SSO (Single Sign-On).

• **OAuth :** Open Authorization (autorisation ouverte) permet aux utilisateurs de se connecter à des services tiers, tels que Google ou Facebook, en utilisant les informations d'identification de leurs fournisseurs d'identité.[8]

FIGURE 1.17 – OAuth.

• **Kerberos :** Le système d'authentification Kerberos est largement utilisé dans les environnements de réseau Microsoft. Il utilise des tickets d'authentification pour vérifier l'identité des utilisateurs.[8]

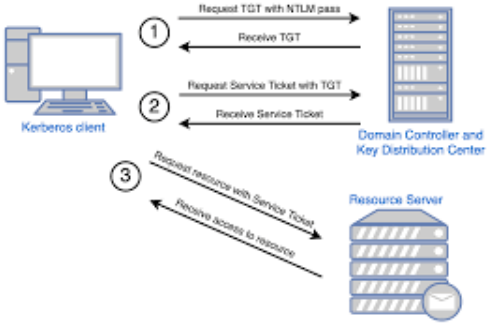


FIGURE 1.18 – Kerberos.

Il n'existe pas de méthode d'authentification parfaite et il est souvent nécessaire de combiner plusieurs méthodes pour garantir un niveau de sécurité élevé tout en offrant une expérience utilisateur agréable.

1.3.5 Les dimensions de la sécurité des systèmes d'information

1. **Dimension Technique :**
   La technologie de traitement électronique de l'information se réfère aux moyens techniques capables d'effectuer des tâches liées aux processus de collecte, stockage et traitement des informations. Elle est caractérisée par deux dimensions : sa fonction de base et ses performances en termes de capacité, qualité et coût.[9]

En outre, cette technologie est également définie par la compression du temps et de l'espace, l'expansion des capacités de stockage, la facilité d'utilisation et la connectivité.[9]

2. **Dimension Organisationnelle :**
   Les dimensions organisationnelles sont examinées sous deux angles : une perspective fonctionnelle et une perspective structurelle.

   • **SI et fonctionnement de l'organisation :** Le système d'information a pour objectif de répondre aux besoins particuliers de chaque processus fonctionnel ainsi qu'aux besoins de communication entre les différents processus.[9]

   • **SI et structure organisationnelle :** La mise en place du système d'information implique une sélection organisationnelle basée sur les caractéristiques de la structure organisationnelle, la pertinence pour chaque unité organisationnelle et la cohérence globale, ce qui soulève la question de l'appropriation du système par les acteurs de l'organisation.[9]

1.3.6 Vulnérabilités

Dans le domaine de la sécurité informatique, une vulnérabilité désigne une brèche ou une faiblesse présente dans un système, une application, un réseau ou un protocole, qui peut être exploitée par un attaquant pour compromettre la sécurité, accéder à des informations sensibles ou perturber le fonctionnement du système.[10]
Voici quelques exemples de vulnérabilités de sécurité informatiques spécifiques à certains produits et logiciels qui sont parmi les plus connues : [10]

• **Shellshock :** (aussi appelée « **Bashdoor** »), cette vulnérabilité touche les systèmes Linux, Unix et macOS, et permet à un attaquant de prendre le contrôle de la machine visée.[10]

• **Heartbleed :** Cette vulnérabilité provient d'une implémentation défectueuse du protocole TLS par la bibliothèque OpenSSL, permet à un attaquant de lire une partie de la mémoire du serveur, notamment les clés privées utilisées pour le cryptage des communications ou d'autres informations sensibles du serveur.[12]

• **Poodle : P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption, cette faille présente dans le protocole de chiffrement SSLv3, rend l'application vulnérable aux attaques de l'homme du milieu (MITM).[12]

• **Dirty COW :** (COW veut dire « copy-on-write »), cette vulnérabilité, présente dans Linux, peut être exploitée pour obtenir une élévation de privilèges.[10]

• **Spectre et Meltdownsont :** Il s'agit de vulnérabilités touchant les processeurs, qui permettent principalement à Intel de récupérer des informations depuis la mémoire.[10]

1.3.7 Attaque

Une attaque de sécurité informatique est une action malveillante visant à accéder à des informations sensibles, perturber le fonctionnement ou causer des dommages à un système d'information, une application, un réseau ou un dispositif de stockage.

Voici quelques exemples courants d'attaques de sécurité informatique :

a.A ttaques par déni de service (DDoS) : Cette attaque a pour objectif de rendre un serveur ou un réseau indisponible pour les utilisateurs légitimes en le submergeant de trafic inutile.[13]

b.P hishing : L'attaque de phishing utilise des e-mails ou des SMS frauduleux pour tromper les utilisateurs et les inciter à fournir des informations sensibles, telles que des noms d'utilisateur, des mots de passe ou des informations de carte de crédit.[13]

c.M alware : L'attaque de malware vise à infecter un système avec un logiciel malveillant, tel qu'un virus ou un cheval de Troie, dans le but d'accéder à des informations sensibles ou de prendre le contrôle du système.[13]

d. Attaques par force brute : L'attaque par force brute consiste à essayer toutes les combinaisons possibles de mots de passe pour accéder à un compte ou à un système, même sans connaître le mot de passe initial.[13]

e.I njection de code (injection SQL) : L'attaque par injection de code vise à exécuter du code malveillant sur un serveur en exploitant une vulnérabilité dans une application web.[13]

1.3.8 Mécanismes de défense

Les mécanismes de défense sont des mesures de sécurité qui peuvent aider à protéger les systèmes d'information, les applications, les réseaux et les dispositifs de stockage contre les attaques malveillantes.
Voici quelques exemples courants de mécanismes de défense :

1. **Protection réseau :**

   • **Firewall :** Le pare-feu est un dispositif matériel ou logiciel qui permet de contrôler le trafic réseau entrant et sortant d'un système ou d'un réseau informatique. Il peut aider à prévenir les attaques en bloquant le trafic malveillant et en vérifiant que les communications respectent les règles de sécurité définies.[13]

   • **DMZ :** Une zone démilitarisée est une zone de sécurité intermédiaire située entre un réseau privé interne et un réseau public externe, tel qu'Internet. Elle est spécialement conçue pour isoler les serveurs accessibles au public, de manière à protéger le réseau interne contre les attaques potentielles.[13]

   • **Segmentation VLAN :** Est une technique de séparation du trafic au niveau du commutateur, utilisant des structures logiques appelées VLAN (Virtual Local Area Network). Cette méthode est largement utilisée pour segmenter efficacement un réseau.[14]

   • **Redondance :** La conception redondante est une méthode qui consiste à ajouter des éléments supplémentaires pour garantir une disponibilité continue et minimiser les interruptions de service.[11]

2. **Chiffrement de flux et VPN :**
   Le chiffrement de flux est une méthode qui consiste à chiffrer les données en temps réel pendant leur transmission, afin de les protéger contre les interceptions malveillantes. Les réseaux privés virtuels (VPN) offrent une solution de sécurité pour les communications entre deux ordinateurs sur un réseau public, en utilisant le protocole de tunnelisation sécurisé (Secure Tunneling Protocol ou STP) ou le protocole PPP (Point-to-Point Protocol).[17]

- Il existe plusieurs techniques pour le chiffrement des flux de données, notamment :

  • **IPSec (Internet Protocol Security) :** IPSec est un protocole de sécurité réseau qui utilise des algorithmes de chiffrement pour protéger les données transmises sur le réseau. Il est couramment utilisé pour établir des connexions VPN entre deux ordinateurs ou deux réseaux. La suite IPSec est composée de plusieurs protocoles, tels que Authentication Header (**AH**), Encapsulating Security Payload (**ESP**), Internet Key Exchange (**IKE**) et Security Association (**SA**).[13]

  • **Tunnel SSH :** Le tunneling SSH, également appelé redirection de port SSH, est un protocole de communication sécurisé qui permet de transférer des données entre deux ordinateurs en utilisant une connexion SSH. Il est principalement utilisé pour sécuriser les connexions à distance et contourner les restrictions imposées par les pares-feux.[19]

3. **Détection d'intrusion :**
   Les systèmes de détection et de prévention des intrusions (IDS/IPS) sont des outils de surveillance des activités du réseau qui permettent de détecter les tentatives d'intrusion et de prévenir les attaques potentielles.[20]

   • **IDS (Intrusion Detection System) :** C'est un mécanisme conçu pour détecter des activités anormales ou suspectes sur la cible analysée, qu'il s'agisse d'un réseau ou d'un hôte. Il permet ainsi d'obtenir une vue d'ensemble sur les tentatives réussies ou échouées d'intrusion.[20]
   L'IDS est généralement divisé en trois catégories :

   - **N-IDS** (Network-Based Intrusion Detection System)
   - Les **H-IDS** (Host-Based Intrusion Detection System).
   - Les **IDS hybrides** qui utilisent à la fois des **NIDS** et des **HIDS** pour obtenir des alertes plus spécifiques et adaptées.

   • **IPS (Intrusion Prevention System) :** C'est une méthode de sécurité réseau qui a pour objectif de détecter et de prévenir les menaces identifiées en temps réel. Les systèmes de prévention des intrusions surveillent constamment votre réseau, recherchant tout acte de malveillance potentiel et collectant des informations à leur sujet.[20]

Il existe quatre types principaux de systèmes de prévention des intrusions :

- **NIPS** (Network Intrusion Prevention System).
- **WIPS** (Wireless Intrusion Prevention System).
- **HIPS** (Host Intrusion Prevention System).
- **NBA** (Network Behavior Analysis Program).

4. **Centralisation des traces :**
   La centralisation des traces est une méthode visant à rassembler et à stocker les Logs provenant de divers équipements réseau sur un serveur centralisé. Cette technique facilite la gestion des journaux et permet de détecter rapidement les problèmes de sécurité.[21]
   Plusieurs outils sont disponibles pour suivre de manière centralisée les journaux, notamment :
   • **Syslog (System Logging Protocol) :** Syslog est un protocole normalisé de journalisation des messages informatiques, qui permet de séparer la génération des messages de leur stockage et de leur analyse. Plusieurs implémentations et outils sont disponibles pour améliorer la collecte et la gestion des journaux Syslog, tels que **Syslog-ng** et **RSyslog**.[23]
5. **Antivirus :**
   Les antivirus sont des logiciels indispensables qui ont pour fonction de détecter et de supprimer les virus, les logiciels malveillants et autres menaces informatiques, tels que les chevaux de Troie et les vers.
   Il existe des programmes antivirus disponibles en version gratuite ou payante, tels que Avast, Bitdefender, Kaspersky, McAfee et AVG.[3]

1.4 Conclusion

Dans ce chapitre, nous avons abordé de manière générale les réseaux informatiques et avons introduit les concepts de sécurité des réseaux et des systèmes informatiques. Dans le prochain chapitre, nous allons présenter l'organisme d'accueil.

Chapitre 2

Etude et analyse des besoins

2.1 Introduction

Ce chapitre sera dédié à la présentation du Campus NTS (New Technology & Solutions), où nous avons effectué notre stage. Dans le but de mieux appréhender la structure et les objectifs de l'entreprise, nous commencerons par un bref aperçu de celle-ci. Ensuite, nous procéderons à l'analyse de son architecture réseau et ses composants individuels, en vue d'identifier des possibilités d'amélioration.

2.2 Partie 01 : Présentation de l'entreprise « Campus NTS »

2.2.1 Création et évolution

NTS est une entreprise émergente, se concentre sur la recherche, la conception et la mise en œuvre des solutions, l'intégration des systèmes de sécurité, l'importation et la distribution d'équipements et du matériels de sécurité des réseaux et des télécommunications, ainsi que la formation et le conseil. En 2020, à Bejaia, M^r Yassine DJEBBARI a fondé cette entreprise, bénéficiant de plusieurs années d'expérience et d'une solide réalisation de projets majeurs dans divers secteurs et régions du pays. A titre d'exemple, citons :

- Air Algérie.
- Retelem Alger.
- Poste d'Algérie.
- Adèle.
- RATP ALJAZAIR.
- La technologie.
- Géant de l'électronique BBR.
- Morsi.
- Université de Bejaïa.
- Cité universitaire à Bejaïa (targa ouzamour, 17 octobre...etc).
- SARL Alphas Bejaïa.
- Providentia Béjaïa.

2.2.2 La localisation de l'entreprise

L'entreprise se situe à Targa Ouzemour Bejaia,en face du campus Targa de l'Universite Abderahmane Mira.

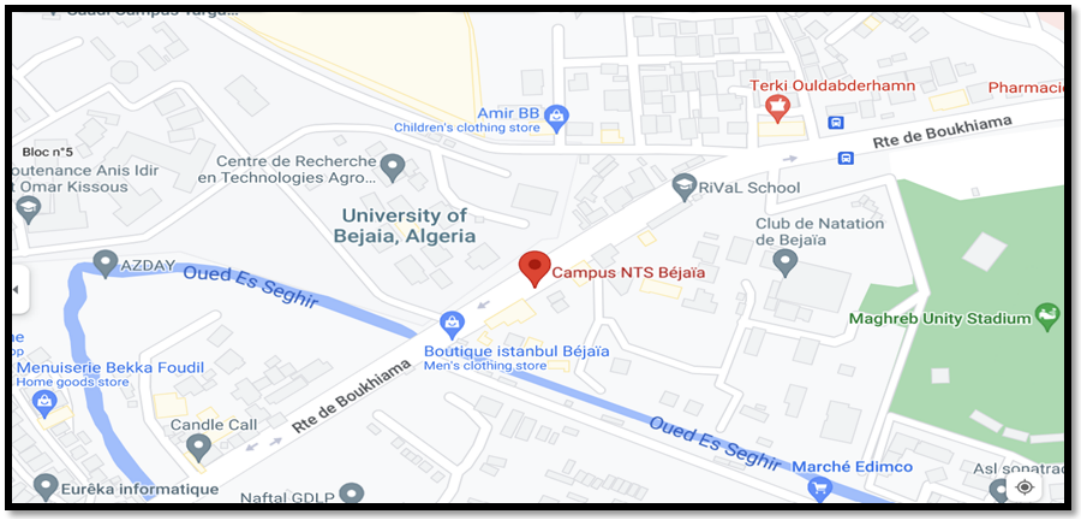


FIGURE 2.1 – Localisation de l'entreprise NTS.

2.2.3 Fiche technique

Le tableau ci-dessous présente quelques informations concernant l'entreprise dans laquelle nous avons effectué notre stage de fin de cycle.

Dénomination	Campus NTS
Logo	CAMPUS NTS INNOVATION TECHNOLOGY
Siège	Bâtiment A les beaux quartiers Targa Ouzemour, Béjaïa 06000
Secteurs d'activités	Informatique et télécommunication
Numéros de FAX	044 204 400
Numéros de Téléphone	0770446101
Email	contact@campus-nts.com
Site Internet	http ://www.campus-nts.com/

TABLE 2.1 – Identification sur campus NTS.

2.2.4 Objectifs, Missions et Activités de l'Entreprise « N.T.S »

Les objectifs, les missions et les activités sont représentées dans la figure ci-dessous :

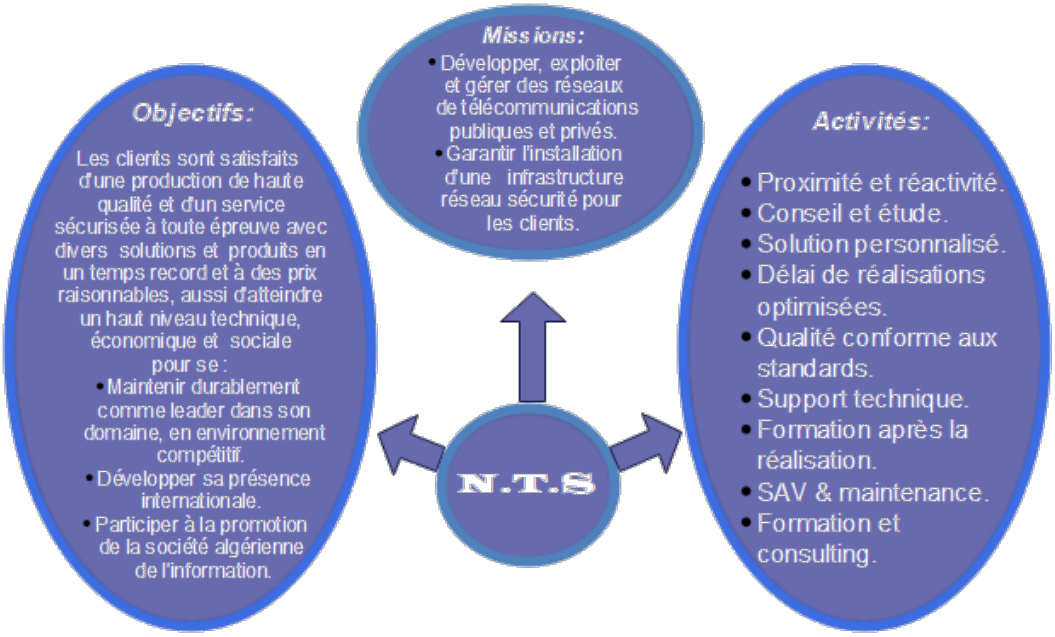


FIGURE 2.2 – Objectifs, Missions et Activités de NTS.

2.2.5 Organigramme général de l'organisme d'accueil

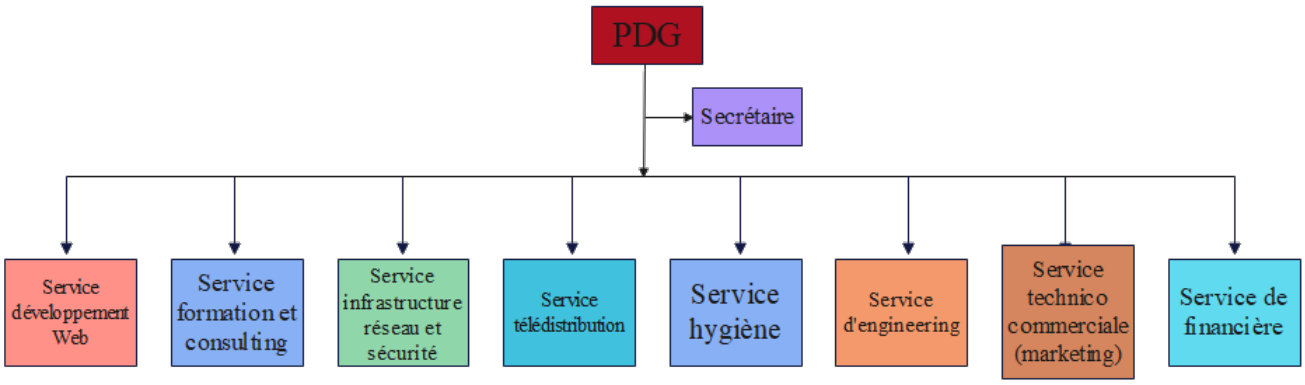


FIGURE 2.3 – L'organigramme de campus NTS.

Ci-dessous, nous présenterons la description de l'organigramme du Campus NTS (voir la figure 2.3), où cette apprentissage marque la fin du stage :

A. Service développement web :

Il est chargé de créer des sites web, des applications internet et mobiles, ainsi que des solutions logicielles personnalisées répondant aux besoins des clients, en utilisant des langages de programmation tels que HTML5, CSS, JavaScript et PHP. Dans l'ensemble, il gère toutes les étapes du développement du site web, y compris l'amélioration de son référencement sur les moteurs de recherche, en vue de son hébergement sur Internet.

B. Service formation et consulting :

Le campus NTS a créé ce secteur dans le but de proposer des stages et des formations professionnelles dans les domaines suivants :

- Installation et configuration des réseaux informatiques.
- Administration et sécurité des réseaux et système.
- Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto…).
- Installation et configuration des réseaux sans fil professionnel.
- Installation et configuration des caméras de surveillance analogique et numérique.
- Fibre optique les réseaux d'accès FTTH/FTTX.
- Création des sites web.
- Programmation (C, C++, C#, Java, Python ,etc.).
- Electricités Bâtiments et industriels.
- Formation Cisco CCNA, CCNP, S&R.
- Virtualisation.
- Microsoft server, SQL.
- Cyber sécurité.

Ces stages sont destinés aux étudiants, travailleurs, entreprises en fin de projet et à tous ceux qui souhaitent développer leurs compétences en sécurité, acquérir des qualifications supérieures et acquérir de l'expérience en entreprise.

Pour ce faire, NTS s'appuie sur la capacité de ses ressources et de ses structures pour fournir des services de qualité à ses clients et partenaires, tels qu'Alhua, Hikvision, Cisco, Legend, Mikrotik, Zkteco, Commax, D-link, Alcatel-Lucent, Synology, Microsoft, Apollo, Panasonic, Huawei.

C. Service d'accueil :

- Présentation de service infrastructure réseau et sécurité :

L'infrastructure réseau est essentielle aux opérations commerciales dans de nombreuses industries, étant donné que c'est le centre névralgique de toute l'organisation informatique, où les données sont centralisées, les échanges de données simplifiés et la communication entre les employés facilitée. De ce fait, elle est un outil critique pour le fonctionnement régulier de l'entreprise, et nécessite une surveillance constante en matière de sécurité, afin de prévenir les attaques externes et internes qui sont de plus en plus nombreuses et nuisibles.

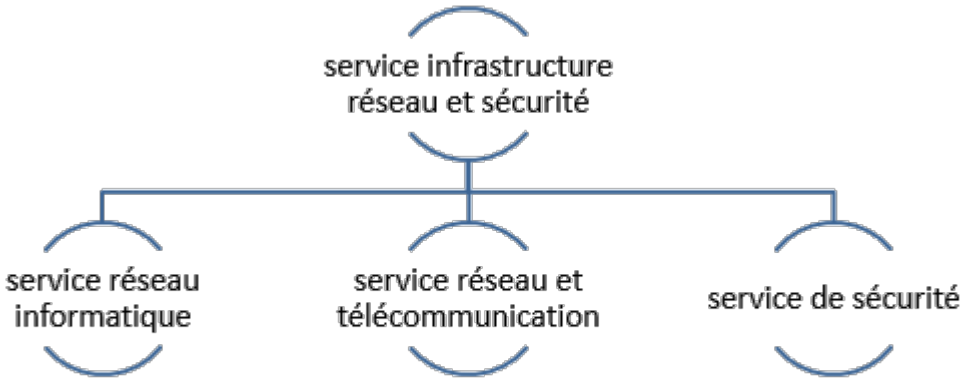


FIGURE 2.4 – Organigramme de service d'accueil.

1. **Service réseau informatique :**
   Ce service couvre l'ensemble des équipements et périphériques d'une entreprise qui sont interconnectés physiquement ou virtuellement via un réseau Wi-Fi professionnel ou d'autres méthodes, dans le but de partager des ressources ou des informations.

En effet, l'infrastructure réseau propose un large éventail de fonctionnalités pour les clients de services et les fournisseurs de services, notamment :

- Limitation de débit.
- analyse.
- vérification.
- surveillance.
- enregistrement et sécurisation du réseau de cette entreprise.

2. **Service réseau et Télécommunication :**
   Les services de télécommunications sont destinés à transmettre des informations en temps réel, en synchronisant les données sous forme analogique ou numérique, à l'exception de la radio et de la télévision. La plupart de ces services peuvent aider les clients à identifier leurs besoins en matière d'infrastructure de télécommunications. Voici quelques exemples de services d'infrastructure de télécommunications :
   - Pose de fibre optique.
   - Emplacement du site de la tour cellulaire.
   - Test d'antenne radio.
   - Installation d'équipements téléphoniques standards et réseau de données.
   - Téléphonie standard.

3. **Service de sécurité :**
   NTS est une entreprise qui propose des services de gardiennage ainsi que d'installation de systèmes de sécurité électroniques. Elle fournit également à ses clients des solutions complètes et fiables pour protéger leurs ressources. Cela comprend les services suivants :
   - Caméras de surveillance.
   - Alarme anti- intrusion.
   - Détection incendie.
   - Pointeuse et Contrôles d'accès.
   - Vidéophonie.

D. Service télédistribution :

Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou d'autres systèmes de distribution (paraboles collectives, télévision numérique terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit. En outre, les services de télédistribution sont devenus un acteur majeur dans l'émergence des nouveaux médias tels que :

- Rediffusion de programmation par satellite.
- Transmission de chaînes de télévision par abonnement.
- Services interactifs.
- Programmation locale.

E. Service d'engineering :

Il est composé d'une équipe d'experts multidisciplinaire dont la mission est de rechercher et d'analyser les besoins des clients afin de trouver la meilleure solution spécifique pour leur projet.

L'équipe du campus NTS n'hésite pas à se déplacer sur le terrain pour vérifier l'état d'avancement du projet et faire face à d'éventuelles difficultés qui auraient pu survenir.

Cette équipe est constituée de :

- D'ingénieurs en télécommunications.
- D'informaticiens en gestion et sécurité des réseaux.
- D'administrateurs de systèmes d'information.
- D'informaticiens en programmation.
- De techniciens fibre.
- De techniciens supérieurs en informatique.

Ils proposent des solutions de recherche en informatique et sécurité, avec une expertise particulière dans les réseaux et les systèmes de télécommunication.

F. Service technico commerciale (marketing) :

Leurs offres vont au-delà des simples fournitures standards, avec une équipe dédiée à répondre aux besoins et au confort de leurs précieux clients, dans le but de développer les services de l'entreprise. De plus, ce service commercialise également les services proposés par le campus NTS.

G. Service des finances :

Le service financier est situé au cœur de l'entreprise et regroupe l'ensemble des personnes chargées de la fonction comptable. Il intervient pour réaliser de bons investissements et prévenir les risques de perte potentiels. Ce service englobe un ensemble de tâches et de rôles au sein de la société NTS :

1. **Les tâches principales du Service des finances**

   • Assurer une gestion saine des ressources financières de l'entreprise, notamment par la planification.

   • La coordination et le contrôle de toutes les politiques et procédures nécessaires pour protéger les actifs.

   • Il est également responsable de produire des informations financières précises et pertinentes, afin de permettre aux gestionnaires de prendre des décisions éclairées.

2. **Le rôle du service financier**

   • La préparation et le suivi des budgets de fonctionnement et d'investissement.

   • La préparation des états financiers.

   • La gestion de la trésorerie et des encaissements.

   • La gestion de la paie des employés et des comptes fournisseurs.

   • L'acquisition de biens et services pour l'ensemble de l'entreprise, y compris les projets de recherche.

   • La réception des marchandises et du courrier.

H. Service hygiène :

La sécurité et la santé sont des aspects essentiels des conditions de travail. L'employeur est responsable de la santé et de la sécurité de ses salariés. Il coordonne ses équipes et leur fournit les moyens nécessaires tels que :

• Mettre en œuvre des mesures de prévention des risques professionnels et de la pénibilité au travail.

• Établir une organisation et fournir des moyens adaptés pour garantir la sécurité et la santé de ses employés.

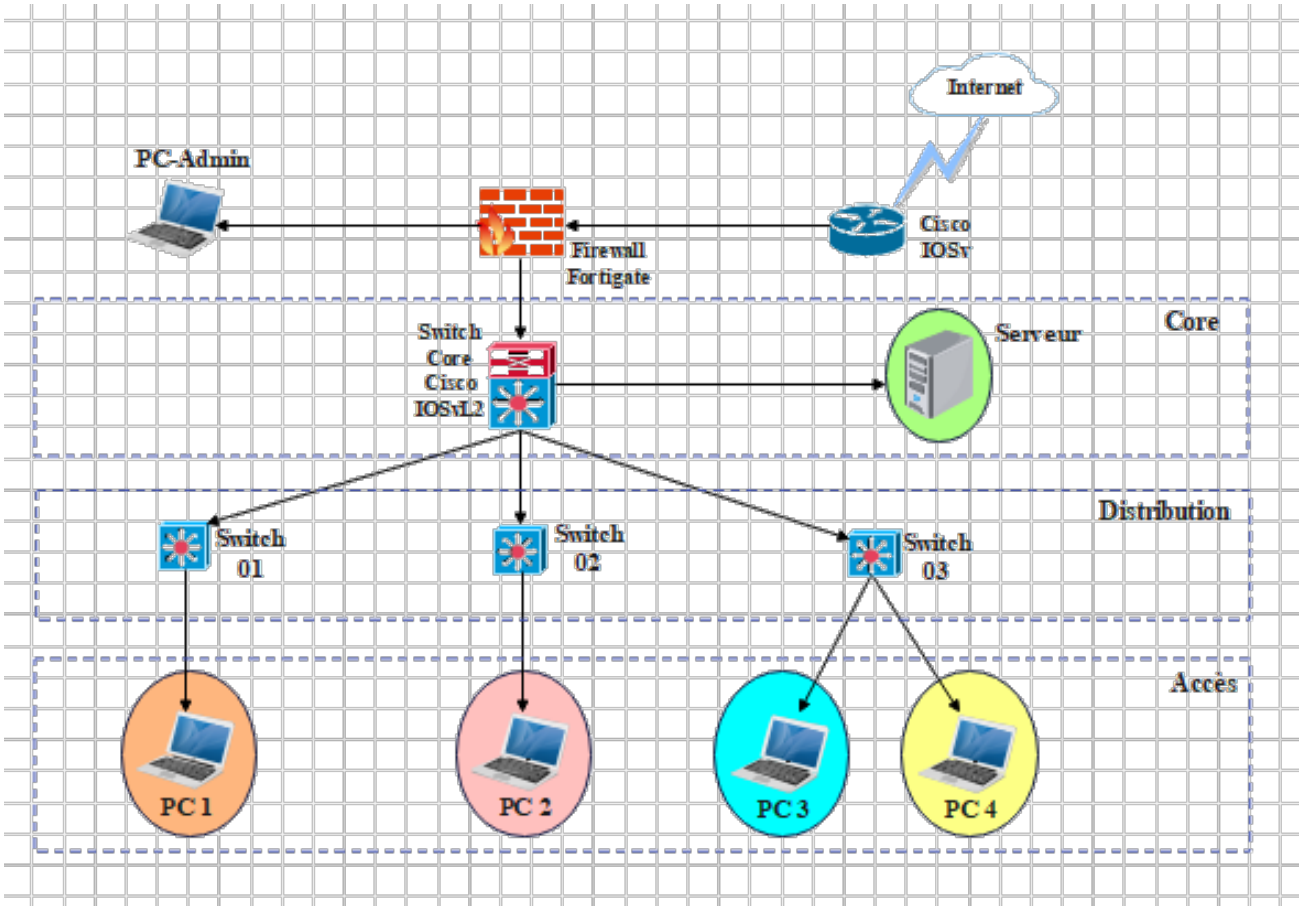
2.3 Partie 2 : Etude des lieux du client « ngtmeziani »

2.3.1 Présentation du réseau « ngtmeziani »

Afin de mieux comprendre les domaines dans lesquels un service informatique doit améliorer ses capacités, ainsi que les besoins et les contraintes d'information à respecter, il est essentiel d'examiner un ensemble de spécifications pour l'infrastructure informatique et technique dont le service a besoin. Cette section contient tous les détails sur l'infrastructure réseau et matérielle.

A. Présentation de l'architecture réseau « ngtmeziani »

Le service informatique « ngtmeziani » a opté pour une topologie arborescente pour connecter ses différents appareils, comme le montre la figure suivante :



5

FIGURE 2.5 – Architecture actuelle de réseau ngtmeziani.

B. Analyse du parc informatique

Les périphériques connectés sont : les ordinateurs, téléphones et les imprimantes. Le tableau suivant contient les statistiques des périphériques par service :

Services	Nombre d'hôtes	Type de connexion
Informatique	25	RJ45 ET WIFI
Maintenance ET SAV	08	RJ45 ET WIFI
Projets	10	RJ45 ET WIFI
Marketing	18	RJ45 ET WIFI
Comptabilité	12	RJ45 ET WIFI
Direction Générale	04	WIFI

TABLE 2.2 – Nombre de périphérique par service.

- **Matériel utilisé**

Le matériel utilisé dans le réseau sont :

- Firewall.
- Switches Multicouche.
- Switches d'accès.
- Les Points d'accès.
- Les ordinateurs et imprimantes.
- Serveurs.
- Prises RJ45.
- Câbles à paire torsadée.
- Câble à fibre optique pour les armoires.

La figure suivante contient précisément le type de chaque équipement utilisé dans le réseau ngtmeziani :

Nom de l'équipement	Le hardware (hard)	Software (soft)
Firewall 	FortiGate 1800F Series	FortiOS (Fortinet Operating System)
Switches Multicouche 	Cisco MDS 9000	IOS (Internetwork Operating System)
Switches d'accès Stackable (Empilable) 	Catalyst 9200 multigigabit 48 ports	IOS (Internetwork Operating System)
Les ordinateurs (Bureau et Portable) 	DELL PC Bureau : Optiplex 7080 MT PC Portable : DELL LATITUDE 5300	Windows 10 et 11
Serveurs 	Serveur HPE ProLiant DL380 Gen 10	ESXI Server Windows Server 2022 Linux Server

TABLE 2.3 – L'environnement hardware et le software.

2.4 Partie 3 : Problématiques et Solutions proposées

1. **Problématiques :**

Nous avons identifié plusieurs problemes liées à la sécurité et à la gestion du réseau de l'entreprise "ngtmeziani". Tout d'abord, nous avons constaté que les postes informatiques étaient connectés à un réseau local câblé et sans fil, ce qui implique la nécessité de mettre en place des mesures de sécurité pour protéger les données et les équipements contre les menaces externes.

De plus, nous avons remarqué que la gestion du réseau était complexe et nécessitait une intervention manuelle pour chaque modification ou mise à jour, ce qui peut entraîner des erreurs et des retards. Par conséquent, l'automatisation des tâches de gestion de réseau est une problématique importante à résoudre.

Enfin, nous avons noté un manque de supervision du réseau, ce qui peut entraîner des problèmes de performance et de disponibilité des équipements. La mise en place d'une solution de supervision est donc une autre problématique importante à considérer.

2. **Solutions :**
   Notre étude vise principalement à mettre en place une solution d'administration et d'authentification pour une meilleure gestion et sécurité de l'accès aux services réseaux de «ngtmeziani». Pour atteindre cet objectif, nous avons opté pour les solutions suivantes :

   Pour automatiser et superviser leur réseau, nous avons opté pour plusieurs solutions. Nous allons utiliser Ansible pour automatiser les tâches de gestion de réseau telles que le déploiement de configurations, la mise à jour des systèmes, et la gestion des équipements. Cela permettra de réduire les erreurs et les retards, et de garantir une gestion plus efficace et conforme du réseau.

   En ce qui concerne la supervision du réseau, nous allons mettre en place une solution de supervision telle que Zabbix pour surveiller les performances du réseau et détecter les problèmes à temps. Nous allons configurer des alertes pour être informés lorsque des seuils de performance sont dépassés ou lorsque des problèmes sont détectés, ce qui permettra aux administrateurs de réseau de réagir rapidement pour résoudre les problèmes.

De plus, nous allons utiliser des outils de collecte de données tels que SNMP pour collecter des informations sur les équipements réseau tels que les routeurs, les commutateurs, les serveurs, etc. Cette collecte de données permettra aux administrateurs de réseau de mieux comprendre l'état du réseau et d'identifier les problèmes potentiels avant qu'ils ne deviennent critiques.

En résumé, notre étude vise à mettre en place des solutions d'automatisation et de supervision pour améliorer la gestion et la sécurité du réseau de "ngtmeziani". Cela permettra aux administrateurs de réseau de mieux gérer le réseau, de réduire les erreurs et les temps d'arrêt, et d'améliorer la satisfaction des utilisateurs.

2.5 Conclusion

Ce chapitre a commencé par une vue d'ensemble de l'entreprise du campus NTS et de son client, « ngtmeziani ». Nous avons ensuite identifié un problème qui nous a conduit à rechercher une architecture qui assure la sécurité et la reactivité du réseau de l'entreprise . Le chapitre suivant sera consacré à l'application de la solution proposée.

Chapitre 3

Automatisation et supervision des réseaux

3.1 Introduction

Les systèmes informatiques sont aujourd'hui essentiels au bon fonctionnement des entreprises et des administrations. Tout dysfonctionnement ou panne survenant sur une partie de ce système pourrait avoir des conséquences lourdes, tant sur le plan financier qu'organisationnel.
Par conséquent, il est devenu impératif d'automatiser, surveiller et contrôler de tels systèmes. Dans ce chapitre, nous allons préciser les concepts d'automatisation et de surveillance.

3.2 Automatisation des réseaux

3.2.1 Définition

L'automatisation du réseau désigne le processus qui automatise les configurations, les gestion, les tests, le déploiement et le fonctionnement des périphériques physiques et virtuels dans un réseau. Cette technologie permet aux NetOps de configurer, de mettre à l'échelle, de sécuriser et d'intégrer le réseau et les services d'applications plus rapidement que les utilisateurs.[29]

3.2.2 Fonctionnement

Le fonctionnement de l'automatisation peut être décrit en plusieurs points :

- Planification et conception du réseau, y compris la planification des scénarios et la gestion des inventaires.
- Test des équipements et vérification de la configuration.
- Provisionnement des équipements et services physiques déployés, ainsi que provisionnement des équipements virtuels.
- Collecte des données en temps réel relatives aux équipements, systèmes, logiciels, topologies réseau, trafic et services.
- Analyse des données, y compris l'analyse prédictive basée sur l'IA et le ML, pour évaluer le comportement actuel et futur du réseau.
- Conformité de la configuration pour assurer le bon fonctionnement de tous les équipements et services réseau.
- Mise à jour des logiciels, y compris la restauration si nécessaire.

• Résolution en boucle fermée des incidents réseau, y compris des pannes et des défaillances masquées (« grises »).
• Production de données de rapports, tableaux de bord, alertes et alarmes.
• Application des règles de sécurité.
• Surveillance du réseau et de ses services pour garantir le respect des SLA et la satisfaction des clients.

3.2.3 Rôle de l'automatisation pour les entreprises

L'automatisation est devenue un élément crucial de la transformation numérique des entreprises, car elle leur permet de gagner en efficacité, en productivité et en agilité.
Voici quelques-uns des avantages clés de l'automatisation pour les entreprises :

a) Réduction des coûts de production : Grâce à l'automatisation, il est possible de réduire les coûts en éliminant les tâches manuelles répétitives, en améliorant la qualité et la précision des processus, et en limitant les erreurs humaines. Cette optimisation peut entraîner des économies considérables en termes de temps, de main-d'œuvre et de ressources pour l'entreprise.

b) Augmentation de la productivité : Grâce à l'automatisation, les employés peuvent être libérés des tâches répétitives et chronophages, et ainsi se concentrer sur des tâches à plus forte valeur ajoutée. Cette optimisation peut augmenter la productivité globale de l'entreprise, ainsi que la satisfaction et la motivation des employés.

c) Amélioration de la qualité : L'automatisation permet d'améliorer la qualité des processus en limitant les erreurs humaines et en assurant la cohérence et la précision des résultats. Cette optimisation peut améliorer la satisfaction des clients et renforcer la réputation de l'entreprise.

d) Accélération des délais : Grâce à l'automatisation, les délais de traitement peuvent être réduits en éliminant les tâches manuelles répétitives et en accélérant les processus. Cette optimisation peut améliorer la réactivité de l'entreprise et lui permettre de répondre plus rapidement aux demandes des clients.

e) Renforcement de l'agilité : L'automatisation permet de rendre les processus plus flexibles et adaptables aux changements, en permettant une modification facile et rapide des processus et des workflows. Cette optimisation peut aider les entreprises à s'adapter plus rapidement aux changements de marché et à maintenir leur compétitivité.

3.2.4 Outils de l'automatisation

Comme indiqué dans la Figure 3.1, il y a quatre domaines d'application dans le monde de l'automatisation, chacun utilisant ses propres outils mentionnés ci-dessous.

1. L'Orchestration :
   - BMC
   - Mcollective
   - Chef Metal
   - Ansible
2. Déploiement d'application :
   - Fabric
   - Capistrano
   - Nolio
   - Ansible

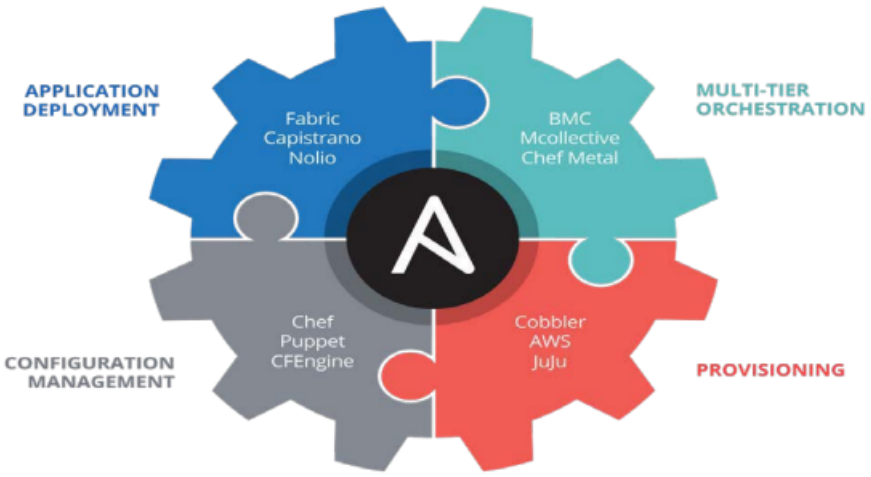


FIGURE 3.1 – Principe de supervision.

3. Provisionnement :
   • Cobbler
   • AWS
   • JuJu
   • Ansible
4. Gestion des configuration :
   • Puppet
   • Chef
   • CFengine
   • Ansible

Ansible est l'outil qui permet d'automatiser tous les domaines d'application, il est utilisé dans de nombreuses entreprises connues, telles que Udemy, Alibaba Travel, Tokopedia, etc.

a) Définition :

Ansible est un outil d'automatisation open source flexible et puissant qui simplifie la gestion de l'infrastructure IT et des applications d'une entreprise. Il améliore l'agilité, la fiabilité et la réactivité des environnements de production. Voici quelques-uns des principaux avantages qu'il offre :

• **Agentless :** Ansible ne nécessite pas l'installation d'un agent sur les serveurs gérés. Il utilise plutôt SSH (Secure Shell) pour se connecter et exécuter des commandes à distance.

• **Configuration en YAML :** (**Y**et **A**nother **M**arkup **L**anguage)Les playbooks Ansible sont rédigés en YAML, un format de données simple et facile à lire. Il est utilisé pour la partie déclarative, notamment pour les playbooks et l'inventaire.

• **Gestion de la configuration :** Ansible peut gérer efficacement la configuration de plusieurs serveurs pour garantir qu'ils respectent les bonnes pratiques et les politiques de l'entreprise.

• **Déploiement d'applications :** Ansible peut déployer et mettre à jour des applications sur plusieurs serveurs en synchronisant les fichiers et en exécutant les commandes nécessaires.

• **Polyvalent :** Ansible est compatible avec divers systèmes d'exploitation tels que Linux, Windows, macOS, Cisco IOS et bien d'autres encore.

• **Modules integrés :**De nombreux modules prêts à l'emploi, développés en Python, sont disponibles pour Ansible, et il est également facile de créer des modules personnalisés.

• **Contrôle d'accès fin :** Ansible offre un contrôle d'accès précis permettant de limiter l'accès en fonction des tâches à effectuer.

• **Intégration à CI/CD :** Il est facile d'intégrer Ansible aux pipelines CI/CD pour automatiser les déploiements d'applications.

b) Domaine d'application :

Ansible peut automatiser divers processus informatiques, tels que :

- La gestion des configurations :

Ansible permet de gérer à grande échelle la configuration des serveurs, des réseaux et des applications. Elle permet de définir des configurations standardisées pour l'ensemble des serveurs d'un parc informatique, assurant ainsi une cohérence et une sécurité améliorées.

- L'orchestration :

Ansible permet d'orchestrer des tâches complexes qui impliquent plusieurs serveurs. Elle peut être utilisée pour automatiser des tâches de sauvegarde, de mise à jour, de surveillance, et bien d'autres encore.

- Le déploiement d'application :

Ansible permet de déployer des applications sur des serveurs en automatisant toutes les tâches nécessaires à leur installation et à leur configuration. Cela peut inclure l'installation de dépendances, la configuration de bases de données, la mise en place de certificats SSL, et bien d'autres encore.

- Le provisionnement :

Ansible peut être utilisé pour provisionner et configurer des infrastructures à la demande, que ce soit sur site, dans le cloud ou dans des environnements hybrides. Il peut aider à créer et à gérer des serveurs, des réseaux, des services de stockage, ainsi que d'autres ressources d'infrastructure.

3.3 La supervision des réseaux

3.3.1 Le concept de supervision

La supervision de réseau, également appelée monitoring, regroupe un ensemble de technologies matériels et logiciels qui permettent de surveiller à distance l'activité d'un réseau informatique. Elle permet également de réaliser une cartographie du réseau. La supervision est particulièrement adaptée aux réseaux comportant plus de 50 équipements, ainsi qu'aux prestataires de services.[6][8]

• De manière générale, la supervision implique :

- L'installation d'agents ou de sondes sur les équipements à surveiller.
- Les informations collectées sont centralisées sur un ou plusieurs serveurs pour une présentation cohérente aux techniciens ou aux administrateurs.
- L'utilisation des technologies quasi temps réel pour la surveillance des équipements.
- La gestion de parc informatique utilise des technologies moins dynamiques, telles que la gestion des stocks et l'inventaire des machines.
- Il est important de faire la distinction entre la supervision et la gestion de parc informatique.[8]

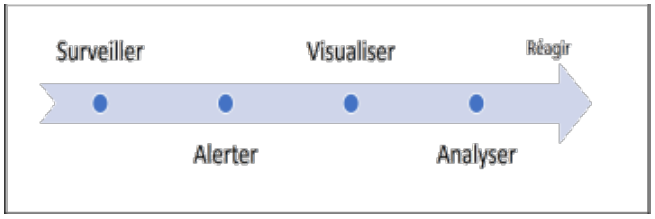


FIGURE 3.2 – Principe de supervision.

3.3.2 Type de surveillance et actions liées

Il existe divers types de surveillance réseau, chacun avec des objectifs et des méthodes spécifiques. Voici quelques exemples :

1. **Surveillance des performances :** Elle vise à mesurer les performances du réseau, telles que la latence, le débit et la disponibilité. Les outils utilisés peuvent identifier les goulots d'étranglement et les problèmes de connectivité.[9]

2. **Surveillance de la sécurité :** Elle vise à détecter les menaces de sécurité et les activités suspectes sur le réseau. Les outils de surveillance de la sécurité peuvent identifier les tentatives de piratage, les virus et les logiciels malveillants.[9]
3. **Surveillance du trafic :** Elle permet de suivre le trafic sur le réseau afin d'identifier les problèmes de congestion et d'optimiser la distribution des ressources. Les outils de surveillance du trafic peuvent également aider à détecter les activités malveillantes.[9]

Les actions liées à la surveillance réseau peuvent inclure :
- La configuration et l'installation d'outils de surveillance adaptés aux différents types de surveillance.
- La collecte et l'analyse des données de surveillance pour identifier les problèmes et les tendances.
- La mise en place de plans d'action pour résoudre les problèmes identifiés.
- La mise en place de politiques de sécurité et de sauvegarde pour protéger le réseau et les données qui y circulent.

3.3.3 Les protocoles de monitoring

Il existe plusieurs protocoles de monitoring, chacun ayant ses propres avantages et inconvénients en fonction de l'application ou du système surveillé.
Voici quelques-uns des protocoles de monitoring les plus courants :
• **SNMP** (Simple Network Management Protocol) : Il s'agit d'un protocole de gestion de réseau standard qui permet de superviser et de gérer des dispositifs réseau tels que des routeurs, des commutateurs, des pares-feux, etc.[10]
• **ICMP** (Internet Control Message Protocol) : Il s'agit d'un protocole de communication utilisé pour surveiller les connexions réseau et les erreurs de transmission.[10]
• **HTTP** (HyperText Transfer Protocol) : Il s'agit d'un protocole de communication utilisé pour surveiller les applications Web.[35]
• **SMTP** (Simple Mail Transfer Protocol) : Il s'agit d'un protocole de communication utilisé pour surveiller les serveurs de messagerie électronique.[10]
• **DNS** (Domain Name System) : Il s'agit d'un protocole de résolution de noms de domaine utilisé pour surveiller la disponibilité des serveurs DNS.[10]
• **SSH** (Secure Shell) : Il s'agit d'un protocole de communication sécurisé utilisé

pour surveiller les connexions à distance à un serveur.[12]

• **Telnet :** Il s'agit d'un protocole de communication utilisé pour surveiller les connexions à distance à un serveur.[10]

• **FTP** (File Transfer Protocol) : Il s'agit d'un protocole de transfert de fichiers utilisé pour surveiller les transferts de fichiers entre les serveurs.[10]

• **NetFlow :** Il s'agit d'un protocole de surveillance de flux réseau utilisé pour surveiller le trafic réseau.[12]

• **WMI** (Windows Management Instrumentation) : Il s'agit d'un protocole de gestion de Windows qui permet de surveiller les performances, les événements et les configurations système.[12]

3.3.4 Le protocole SNMP

SNMP (Simple Network Management Protocol) est un protocole de communication qui a été créé pour être une couche utilisant TCP/IP à un niveau supérieur. Il opère en accord avec UDP et IP, et permet de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseau et matériels à distance. C'est l'un des protocoles les plus utilisés pour la gestion (management, monitorage) des réseaux.[10]

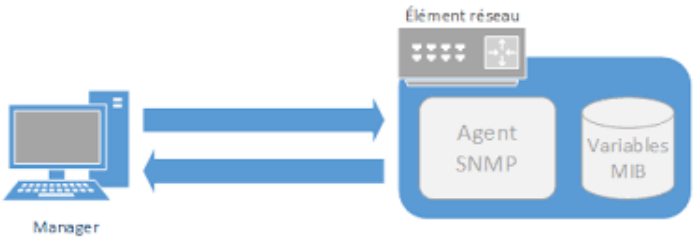


FIGURE 3.3 – Protocole SNMP.

SNMP est utilisé pour :[35]

• Administrer les équipements et échanger des éléments de configuration.

• Surveiller le comportement des équipements et les performances réseaux.

• Modifier le paramétrage de certains composants.

Comme son nom l'indique, il est relativement simple tout en étant très complet. En effet, sa simplicité ne lui empêche pas de pouvoir gérer des réseaux hétérogènes complexes.

Son utilisation est basée sur ces 3 éléments :[10]

• Les agents, placés sur les éléments actifs du réseau.

• Les managers.

• La MIB.

Toutefois, il y'a deux modes de fonctionnement :[10]

• **Le polling :** Dans lequel la station de supervision interroge les agents à tour de rôle.

• **Les traps SNMP :** Où l'équipement remonte lui-même une alarme afin de signaler une anomalie au superviseur.

3.3.5 Quelques outils de supervision

Les outils de supervision sont des logiciels conçus pour surveiller les performances et les activités d'un système informatique, notamment les réseaux, les serveurs, les applications et les dispositifs.

Voici quelques exemples d'outils de supervision couramment utilisés :

— **Nagios :** Un outil open source de surveillance réseau offrant des alertes en temps réel, des tableaux de bord personnalisables et des rapports détaillés.[14]

— **PRTG Network Monitor :** Un outil commercial de surveillance réseau offrant une interface graphique conviviale, des alertes personnalisables et des rapports détaillés.[15]

— **Centreon :** Un outil open source de supervision et de gestion des infrastructures informatiques offrant des fonctionnalités avancées de gestion des événements et de rapports.[13]

— **Zabbix :** Est une solution open-source de supervision et de surveillance des réseaux, des serveurs et des applications. Elle offre un large éventail de fonctionnalités pour collecter, analyser et présenter les données de performance, ainsi que pour générer des alertes en cas de problèmes.[14]

La solution Zabbix comprend plusieurs composants clés :

• **Serveur Zabbix :** C'est le composant central qui collecte, stocke et traite les données de performance provenant des agents Zabbix et d'autres sources.

• **Agents Zabbix :** Ce sont des agents légers qui sont installés sur les hôtes à surveiller. Les agents collectent les données de performance, telles que

l'utilisation du processeur, la consommation de mémoire, les statistiques réseau, etc., et les envoient au serveur Zabbix.

• **Base de données :** Zabbix utilise une base de données pour stocker les données collectées, les configurations et les paramètres du système.

• **Interface utilisateur :** Zabbix propose une interface web conviviale qui permet de visualiser les données de performance, de configurer des alertes, de créer des tableaux de bord personnalisés et de générer des rapports détaillés.

Le choix d'un système de suveillance et de gestion informatique est essentiel pour les entreprise modernes qui cherchent à maintenir leurs opérations en ligne et à assurer la disponibilité de leurs services.

Parmi les nombreuses solutions disponibles sur le marché, Zabbix se démarque comme une plateforme de surveillance open-source très populaire, offrant une large gamme de fonctionnalités et une flexibilité, ainsi des avantages distincts qui répondent aux exigences des entreprises modernes de toute taille.

Dans cette analyse comparative, nous examinerons les points forts de Zabbix par rapport aux autres solutions de surveillance disponibles, en mettant l'accent sur les principaux critères de sélection. Nous verrons comment Zabbix se distingue par sa facilité d'utilisation, sa capacité à surveiller de manière exhaustive les infrastructures complexes, son extensibilité, sa compatibilité avec différentes technologies et sa communauté active de développeurs. Nous aborderons également les coûts associés à l'implémentation et à la maintenance de Zabbix, ainsi que les avantages d'une solution open-source par rapport aux alternatives commerciales.

Grâce à cette analyse comparative approfondie, vous aurez une compréhension claire des avantages de Zabbix par rapport aux autres solutions de surveillance du marché. Cela vous permettra de prendre une décision éclairée pour choisir la solution qui correspond le mieux aux besoins spécifiques de votre entreprise, en assurant la stabilité de vos opérations et la disponibilité de vos services.

3.4 Conclusion

Dans ce chapitre, nous avons examiné les concepts d'automatisation et de supervision. Dans le chapitre suivant, nous aborderons les aspects pratiques de notre projet en détaillant les différentes étapes de préparation, de configuration et d'installation de notre application.

Chapitre 4

Mise en oeuvre des solutions retenus

4.1 Introduction

Ce chapitre constitue une partie essentielle du mémoire, car il présente les détails concrets de la réalisation de notre solution de supervision ainsi que la solution d'automatisation afin d'aboutir à des résultats satisfaisants.

4.2 Présentation de l'environnement de travail

En termes de logiciels, nous avons utilisé plusieurs systèmes d'exploitation, notamment Windows 10 et Ubuntu. Nous avons installé les outils nécessaires sur ces systèmes d'exploitation, tels que :

1. **GNS3 (Graphical Network Simulator) :** Il s'agit d'un logiciel libre qui permet de créer et de simuler notre architecture informatique.
2. **VMWARE :** VMware Workstation 17 est une solution logicielle professionnelle qui permet de créer un environnement de test de machines virtuelles.
3. **FortiGate :** C'est une solution de pare-feu nouvelle génération et une passerelle de sécurité unifiée (Unified Threat Management, UTM) développée par Fortinet. Elle comprend des fonctionnalités intégrées pour les plates-formes de data center et combine plusieurs fonctions de sécurité telles que l'antivirus, le VPN, l'IPS, l'Antispam, etc.
4. **Putty :** Il s'agit d'une application open-source d'émulation de terminal qui peut être utilisée en tant que client pour divers protocoles informatiques tels que SSH.
5. **Ansible :** Il s'agit d'un outil open-source d'automatisation qui permet aux utilisateurs d'automatiser des tâches informatiques telles que la gestion de configuration, le déploiement d'applications et l'automatisation de tâches.
6. **Zabbix :** Il s'agit d'une plateforme open-source de surveillance et de gestion de réseau qui permet aux utilisateurs de surveiller en temps réel les performances et la disponibilité des périphériques réseau, des serveurs, des applications et des services.

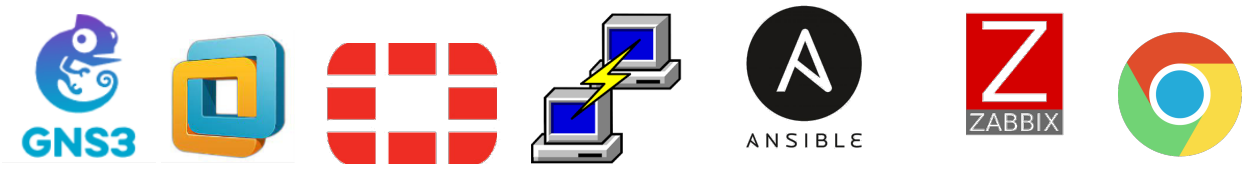


FIGURE 4.1 – Outils de travail.

4.3 L'architecture proposée

La figure ci-dessous représente l'architecture du réseau que nous avons créée pour virtualiser notre solution à l'aide du logiciel GNS3.

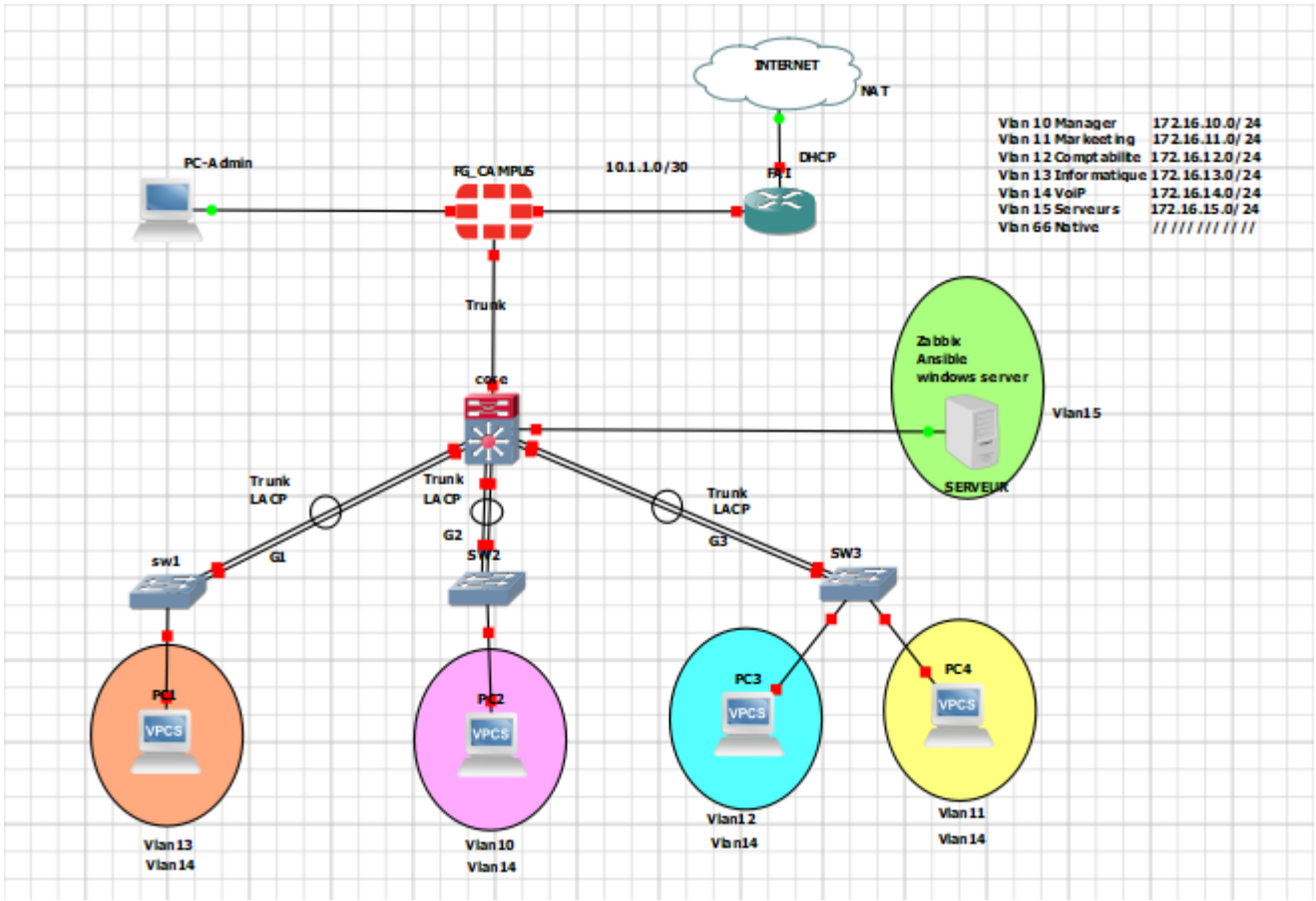


FIGURE 4.2 – Architecture proposée.

4.4 Méthodologie

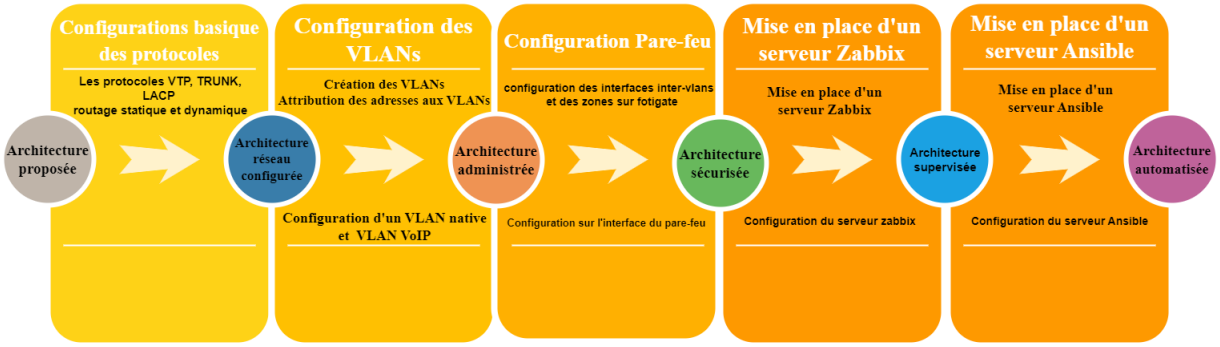


FIGURE 4.3 – Méthodologie.

4.5 Tableau d'adressage générale

Le nom d'équipement	Interface	Description	Adresse IP/masque	Gateway
Pare-feu Fortigate	Port 1	Wan	10.1.1.1/30	/
	Port 2	Lan	/	/
	Port 3	admin	192.168.199.1/24	/
Routeur FAI	Eth 0/1	Lan	10.1.1.2/30	/
	Eth 0/0	Wan	192.168.137.129/24	/
Switchcore	Eth 0/0	Vlan13	172.16.13.0/24	172.16.13.1
	Eth 0/2	Vlan10	172.16.10.0/24	172.16.10.1
	Eth 1/0	Vlan12,Vlan11	172.16.12.0/24	172.16.12.1
			172.16.11.0/24	172.16.11.1
Serveur Zabbix	inet	Vlan15	172.16.15.5	172.16.15.1
Serveur Ansible	ens33	Vlan15	172.16.15.9/24	172.16.15.1
Serveur Windows 2022	Ethernet 0	Vlan15	172.16.15.12/24	172.16.15.1

TABLE 4.1 – Tableau d'adressage générale.

4.6 Tableau d'adressage des Vlans

Le tableau ci-dessous présente les VLAN que nous avons proposés pour notre réseau, ainsi que les adresses IP correspondantes.

Vlan ID	Nom du Vlan	Adresse IP
VLAN 10	Manager	172.16.10.0/24
VLAN 11	Marketing	172.16.11.0/24
VLAN 12	Comptabilité	172.16.12.0/24
VLAN 13	Informatique	172.16.13.0/24
VLAN 14	VoIP	172.16.14.0/24
VLAN 15	Serveurs	172.16.15.0/24
VLAN 66	Native	172.16.66.0/24

TABLE 4.2 – Tableau d'adressage des VLANs.

4.7 Installation des systèmes et préparation du lab

1. Installation de GNS3 : Pour installer GNS3, il vous suffit de télécharger son fichier exécutable, de le lancer et de suivre les étapes d'installation présentées dans l'annexe jusqu'à la fin, pour obtenir l'interface illustrée dans la figure suivante.

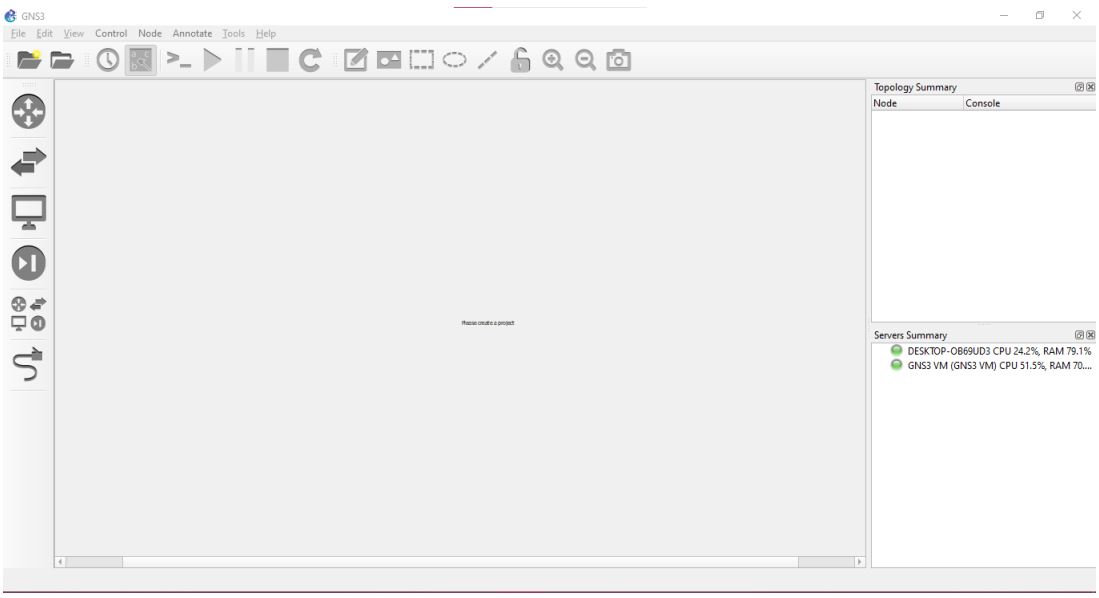


FIGURE 4.4 – Interface de GNS3.

2. Installation de VMware Workstation version 17 : Afin de créer plusieurs machines virtuelles pour nos serveurs sur un seul ordinateur, nous devons installer VMWare Workstation en suivant les étapes présentées dans l'annexe, pour obtenir à la fin l'interface illustrée dans la figure ci-dessous.

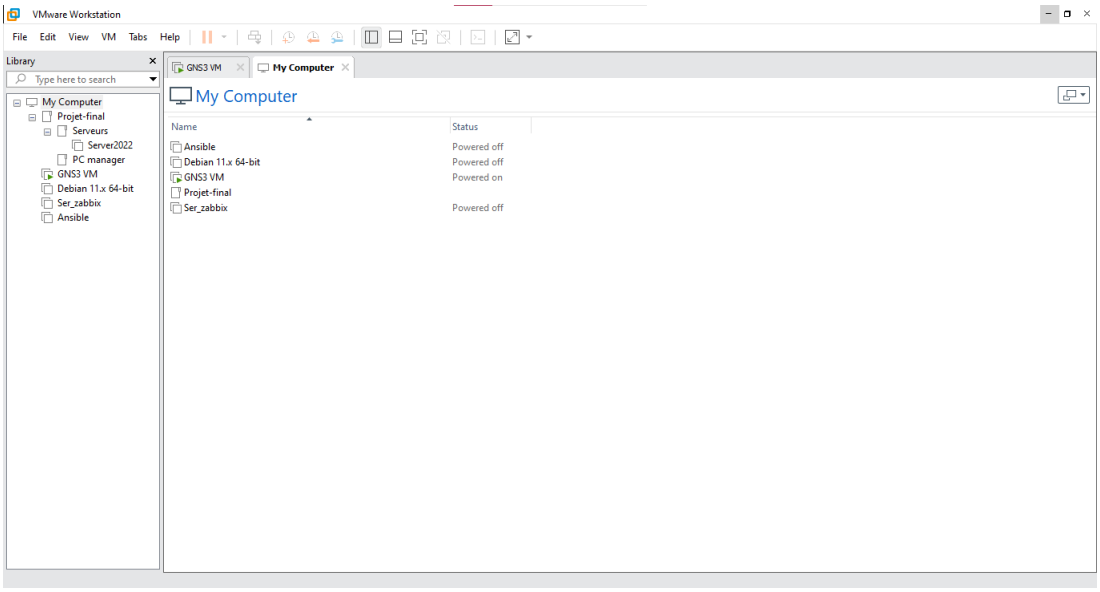


FIGURE 4.5 – Interface de VMWare Workstation version 17.

3. Installation de Windows Server 2022 : Pour installer Windows Server 2022, nous allons ajouter son image dans la machine virtuelle et suivre les étapes jusqu'à la fin, pour obtenir enfin l'interface visible dans la capture d'écran suivante.

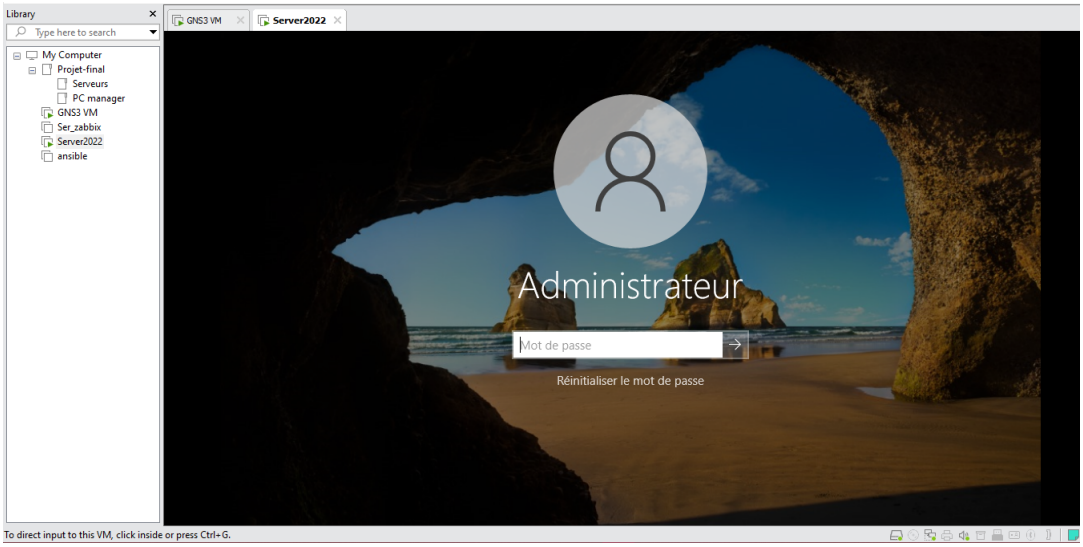


FIGURE 4.6 – Interface de Windows Server 2022.

• **Installation de l'active directory :** Il s'agit d'un service de gestion des identités et des accès qui joue un rôle crucial dans les environnements Windows, en permettant l'authentification unique et la gestion des stratégies de groupe. Nous avons configuré notre contrôleur de domaine CampusNts sur Windows Server 2022.

La figure suivante montre notre interface du gestionnaire de serveur et les fonctionnalités que nous avons configurées.

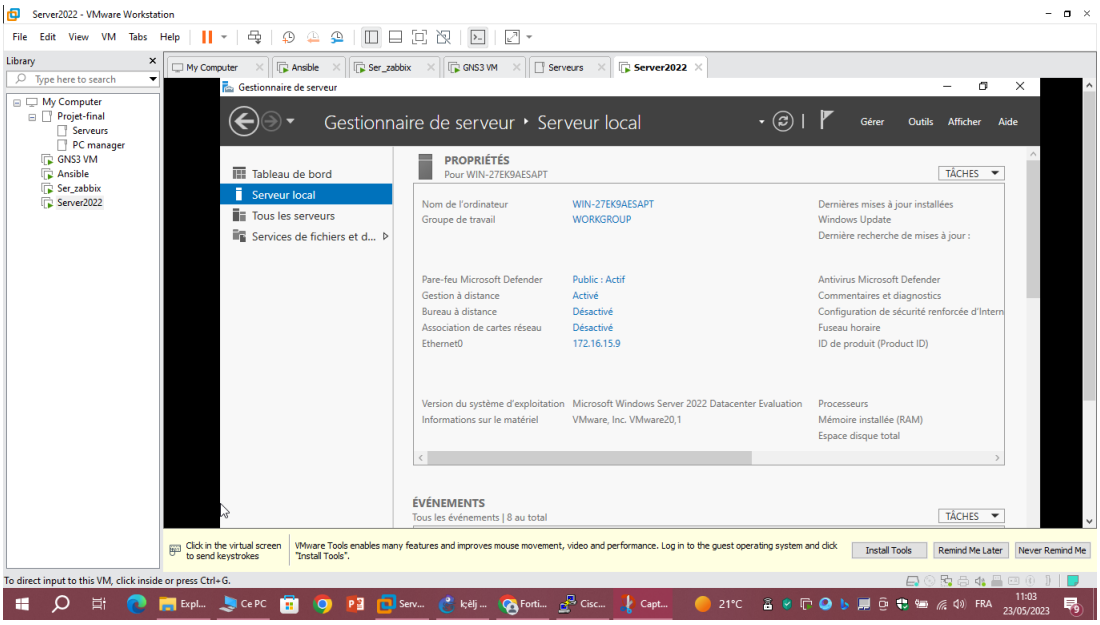


FIGURE 4.7 – Interface du gestionnaire de serveur.

4.8 Configuration des équipements

La première étape pour mettre en place l'architecture proposée consiste à configurer nos équipements respectifs au niveau des consoles, en utilisant des commandes spécifiques. Dans cette partie, nous allons fournir un exemple commenté des configurations essentielles nécessaires pour la mise en œuvre de notre architecture.

4.8.1 Configuration de base :

Cette configuration inclut l'attribution des adresses IP sur la console, ainsi que les fonctionnalités et les protocoles qui faciliteront la gestion de ce réseau.

1. **Configuration du hostname du switch core :**

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ho
Switch(config)#hostname Core1
Core1(config)#
Core1(config)#
Core1(config)#
Core1(config)#
Core1(config)#end
Core1#
Core1#
```

FIGURE 4.8 – Configuration du hostname au niveau du switch core.

2. **Configuration du protocole VTP :** Le protocole VTP permet une gestion centralisée des réseaux VLAN, ce qui facilite la propagation des modifications effectuées sur le serveur à tous les clients VTP. Nous utiliserons deux modes, à savoir le mode serveur et le mode client. Le Switch core sera configuré en mode serveur, tandis que le reste des Switchs d'accès seront configuré en mode client.

   • **Serveur VTP :** Nous désignons le switch core en tant que serveur VTP.

```
Core1(config)#vtp mo
Core1(config)#vtp mode se
Core1(config)#vtp mode server
Device mode already VTP Server for VLANS.
Core1(config)#vtp dom
Core1(config)#vtp domain campusnts.vtp
Changing VTP domain name from NULL to campusnts.vtp
Core1(config)#vtp
*Apr  5 13:20:51.388: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to campusnts.vtp.pass
Core1(config)#vtp password cisco
Setting device VTP password to cisco
Core1(config)#vtp ve
Core1(config)#vtp version 2
Core1(config)#vtp pru
Core1(config)#vtp pruning
Pruning switched on
Core1(config)#end
Core1#
```

FIGURE 4.9 – Configuration du VTP au niveau du switch core.

• **Client VTP :** Les switchs d'accès seront configurés en mode client.

```
Sw3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw3(config)#
Sw3(config)#vtp mo
Sw3(config)#vtp mode cli
Sw3(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
Sw3(config)#vtp pass
Sw3(config)#vtp password cisco
Setting device VTP password to cisco
Sw3(config)#vtp dom
Sw3(config)#vtp domain c
Sw3(config)#vtp domain campusnts.vtp
Changing VTP domain name from NULL to campusnts.vtp
Sw3(config)#vtp
Sw3(config)#vtp ve
Sw3(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
Sw3(config)#vtp
Sw3(config)#end
Sw3#
```

FIGURE 4.10 – Configuration du VTP au niveau du Switch 3 .

3. **Configuration des interfaces Trunk :** Le trunking permet de transporter plusieurs VLAN sur une seule liaison physique, ce qui facilite la connectivité entre les différents segments du réseau. Pour cela, il est important de configurer les trunks des deux côtés de la liaison (switch core et switch d'accès).

• **Sur le switch distribution :**

```
Core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core1(config)#in
Core1(config)#interface  ran
Core1(config)#interface  range gi
Core1(config)#interface  range gigabitEthernet 0/0-3, g
Core1(config)#interface  range gigabitEthernet 0/0-3, gigabitEthernet
*Apr  5 13:18:35.831: %PLATFORM-5-SIGNATURE_VERIFIED: Image 'flash0:/vios_l2-adventerprisek9-m' p
on1/0-1
Core1(config-if-range)#
Core1(config-if-range)#
Core1(config-if-range)#$range gigabitEthernet 0/0-3, gigabitEthernet 1/0-1
Core1(config-if-range)#
Core1(config-if-range)#
Core1(config-if-range)#
Core1(config-if-range)#sw
Core1(config-if-range)#switchport tr
Core1(config-if-range)#switchport trunk en
Core1(config-if-range)#switchport trunk encapsulation do
Core1(config-if-range)#switchport trunk encapsulation dot1q
Core1(config-if-range)#sw
Core1(config-if-range)#switchport mo
Core1(config-if-range)#switchport mode tr
Core1(config-if-range)#switchport mode trunk
```

FIGURE 4.11 – Configuration de l'interface Trunk au niveau du switch distribution.

- **Sur les switchs d'accès :**

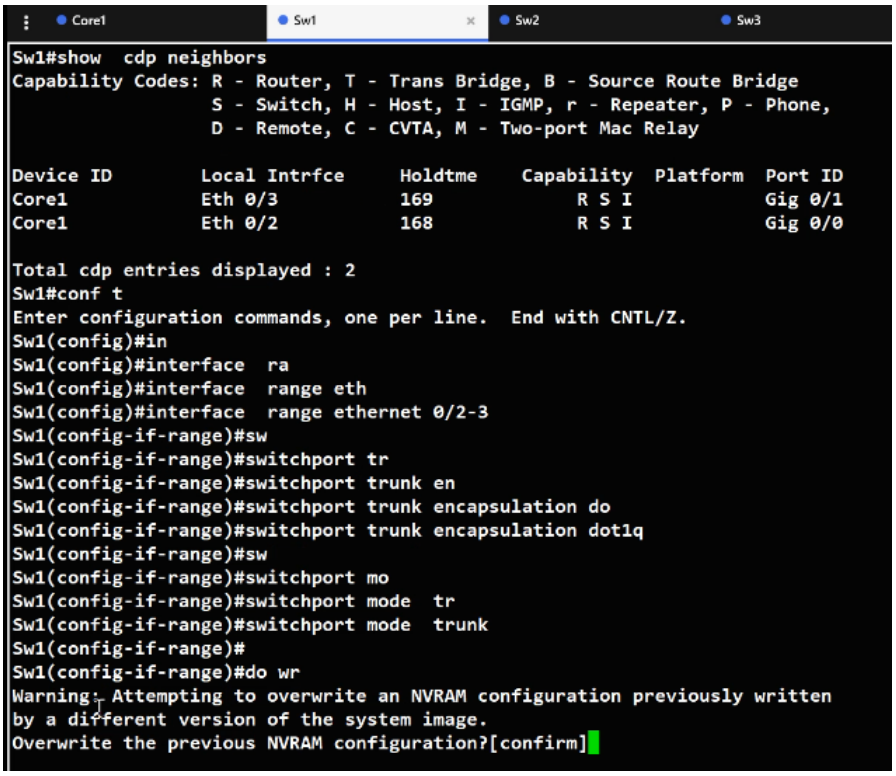


FIGURE 4.12 – Configuration de l'interface Trunk au niveau du Switch 1.

4. **Création des VLANs :** La configuration des VLAN permet d'optimiser les performances et d'offrir une flexibilité de gestion pour une meilleure organisation, et cela se fait au niveau du switch core.

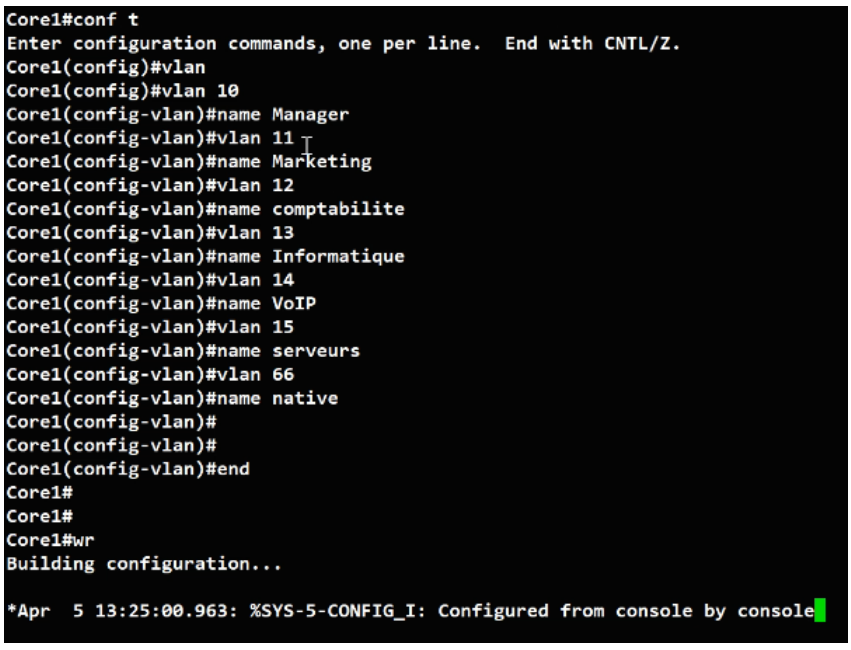


FIGURE 4.13 – Création des VLANs au niveau des switchs core.

5. **Configuration des interfaces Access :** Les interfaces VLAN sont configurées sur les switchs pour permettre la connectivité entre les périphériques finaux et le réseau local. Une interface de commutation est configurée pour un seul VLAN comme suit :

```
Sw2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw2(config)#in
Sw2(config)#interface  eth
Sw2(config)#interface  ethernet 0/0
Sw2(config-if)#sw
Sw2(config-if)#switchport mo
Sw2(config-if)#switchport mode  acc
Sw2(config-if)#switchport mode  access
Sw2(config-if)#
Sw2(config-if)#sw
Sw2(config-if)#switchport acc
Sw2(config-if)#switchport access vl
Sw2(config-if)#switchport access vlan  10
Sw2(config-if)#
Sw2(config-if)#sw
Sw2(config-if)#switchport voi
Sw2(config-if)#switchport voice vl
Sw2(config-if)#switchport voice vlan 14
Sw2(config-if)#
Sw2(config-if)#end
```

FIGURE 4.14 – Configuration d'une interface de commutation au niveau du Switch 1 pour le Vlan 10.

6. **Configuration du protocole LACP :** Le protocole de contrôle de liens LACP (Link Aggregation Control Protocol) est utilisé pour agréger plusieurs liens physiques en un seul lien logique, ce que nous allons configurer sur le switch core.

```
Core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core1(config)#interface range gigabitEthernet 0/0-1
Core1(config-if-range)#chann
Core1(config-if-range)#channel-g
Core1(config-if-range)#channel-group 1 mo
Core1(config-if-range)#channel-group 1 mode  ac
Core1(config-if-range)#channel-group 1 mode  active
Creating a port-channel interface Port-channel 1

Core1(config-if-range)#
Core1(config-if-range)#
Core1(config-if-range)#
Core1(config-if-range)#
*Apr  5 14:01:16.816: %EC-5-L3DONTBNDL2: Gi0/0 suspended: LACP currently not enabled on the remote port.
*Apr  5 14:01:17.313: %EC-5-L3DONTBNDL2: Gi0/1 suspended: LACP currently not enabled on the remote port.
*Apr  5 14:01:30.380: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
Core1(config-if-range)#
Core1(config-if-range)#
Core1(config-if-range)#
Core1(config-if-range)#end
```

FIGURE 4.15 – Configuration du protocole LACP sur le switch core.

4.8.2 Configuration du Pare-feu (Fortigate) :

Tout d'abord, nous allons configurer les interfaces du pare-feu au niveau de la console :

```
FG-CAMPUS # config system interface

FG-CAMPUS (interface) # edit port3

FG-CAMPUS (port3) # set mode static

FG-CAMPUS (port3) # set ip 192.168.19.1/24

FG-CAMPUS (port3) # end

FG-CAMPUS #
FG-CAMPUS #
FG-CAMPUS # config system interface

FG-CAMPUS (interface) # edit port3

FG-CAMPUS (port3) # set  allowaccess ping https http telnet ssh

FG-CAMPUS (port3) #
```

FIGURE 4.16 – Configuration des interfaces du pare-feu .

1. **Connexion à l'interface du pare-feu :** Une interface d'authentification sera affichée pour accéder et configurer le pare-feu, comme indiqué dans la figure ci-dessous :

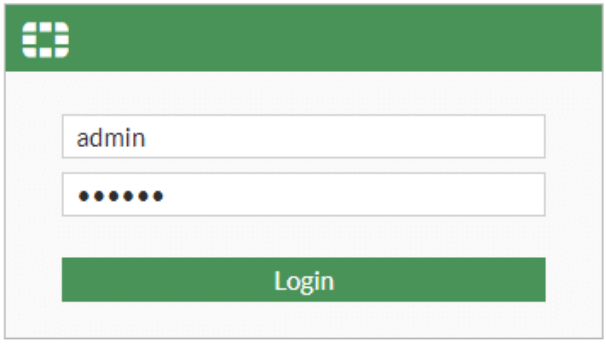


FIGURE 4.17 – Interface d'authentification du pare-feu.

Après avoir entré le nom d'utilisateur et le mot de passe, une page d'accueil apparaîtra comme illustré dans la figure suivante :

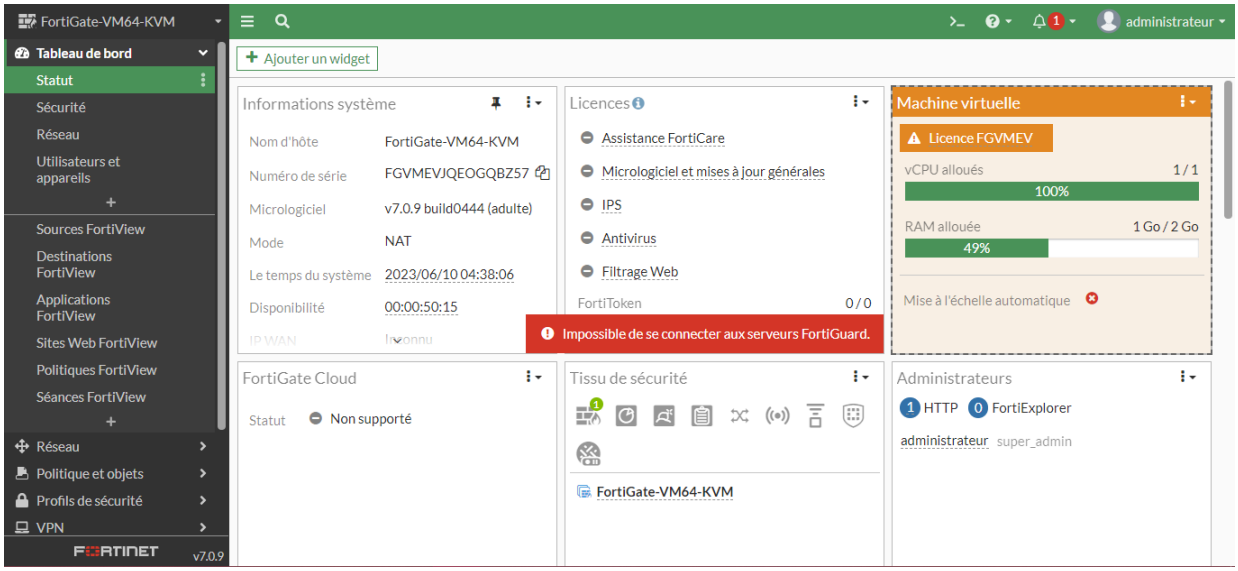


FIGURE 4.18 – Page d'acceuil de l'interface du pare-feu.

2. **Création des Vlans sur l'interface web du Fortigate :** Il suffit d'ajouter les VLAN sur l'interface inter-VLAN (port 2) et de configurer les paramètres spécifiques à l'interface, comme illustré ci-dessous :

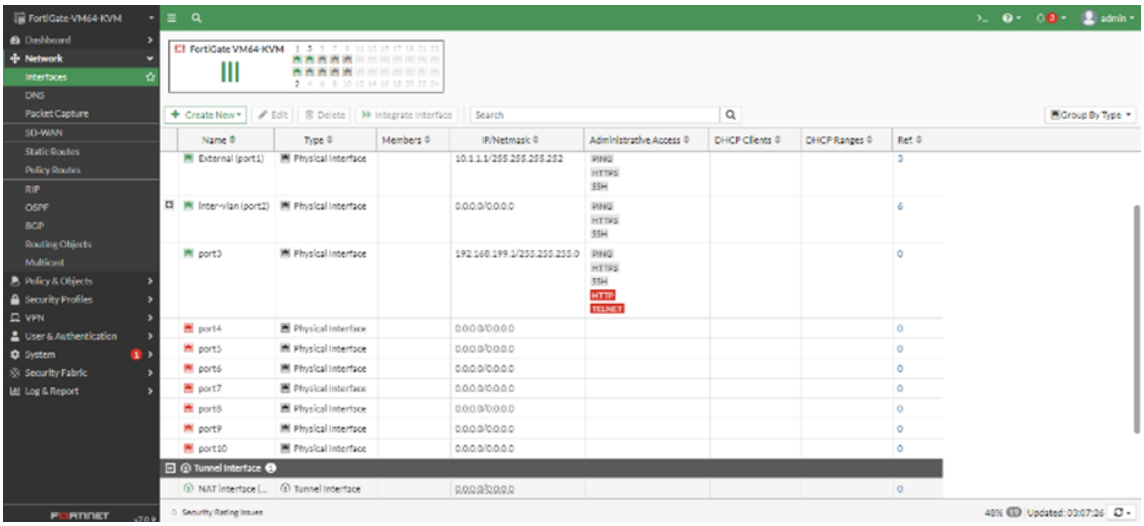


FIGURE 4.19 – Création des Vlans sur l'interface web du Fortigate.

3. **Création des zones :** Cette étape est importante car elle permet de regrouper des interfaces, de définir des règles de sécurité ou des paramètres de routage et de contrôle d'accès pour une zone entière plutôt que pour des interfaces individuelles, ce qui facilite la gestion des politiques du pare-feu.

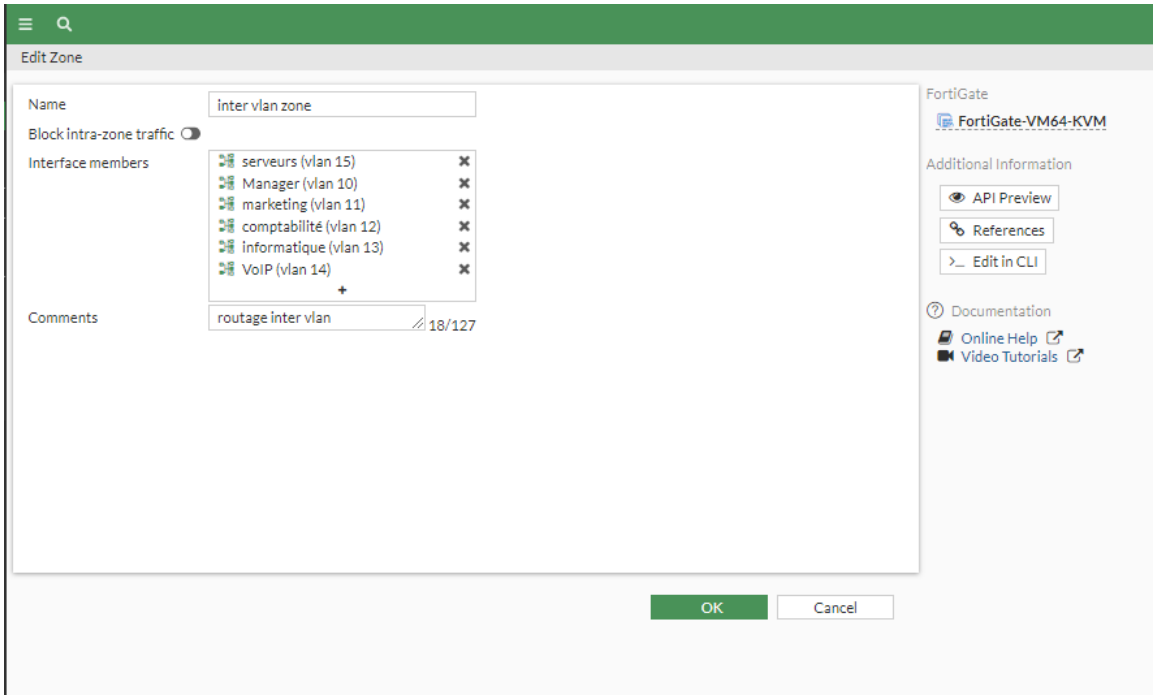


FIGURE 4.20 – Création de l'Inter-Vlan zone sur l'interface web du Fortigate.

4. **Configuration du routage statique :** Le routage de l'interface "External" vise à assurer la connectivité vers le NAT.

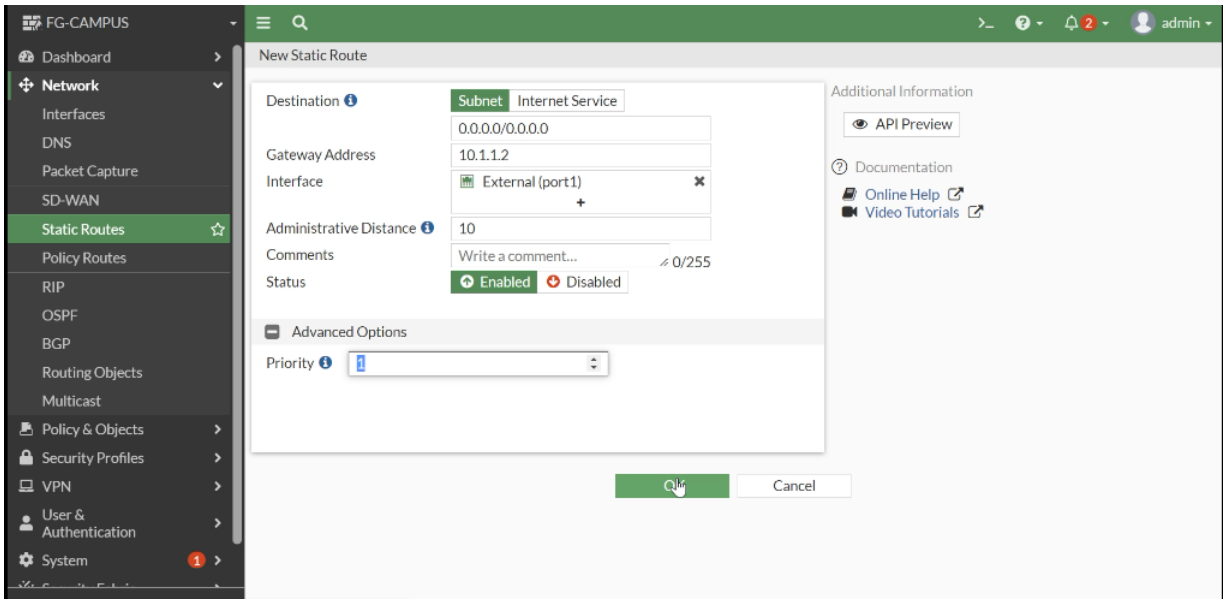


FIGURE 4.21 – Configuration du routage de l'interface External.

5. **Configuration du router :** Nous configurons le nom du routeur sur la console et nous attribuons des adresses IP aux interfaces.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#ho
Router(config)#hostname  FAI
Router(config)#hostname  FAI
FAI(config)#
FAI(config)#
FAI(config)#in
FAI(config)#interface  gi
FAI(config)#interface  gigabitEthernet 0/0
FAI(config-if)#no shu
FAI(config-if)#no shutdown
FAI(config-if)#
FAI(config-if)#ip add
FAI(config-if)#ip address
FAI(config-if)#ip address 192
*Apr  5 14:02:43.761: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Apr  5 14:02:44.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up/
FAI(config-if)#ip address 10.1.1.2 255.255.255.0
FAI(config-if)#
FAI(config-if)#ip address 10.1.1.2 255.255.255.252
FAI(config-if)#
```

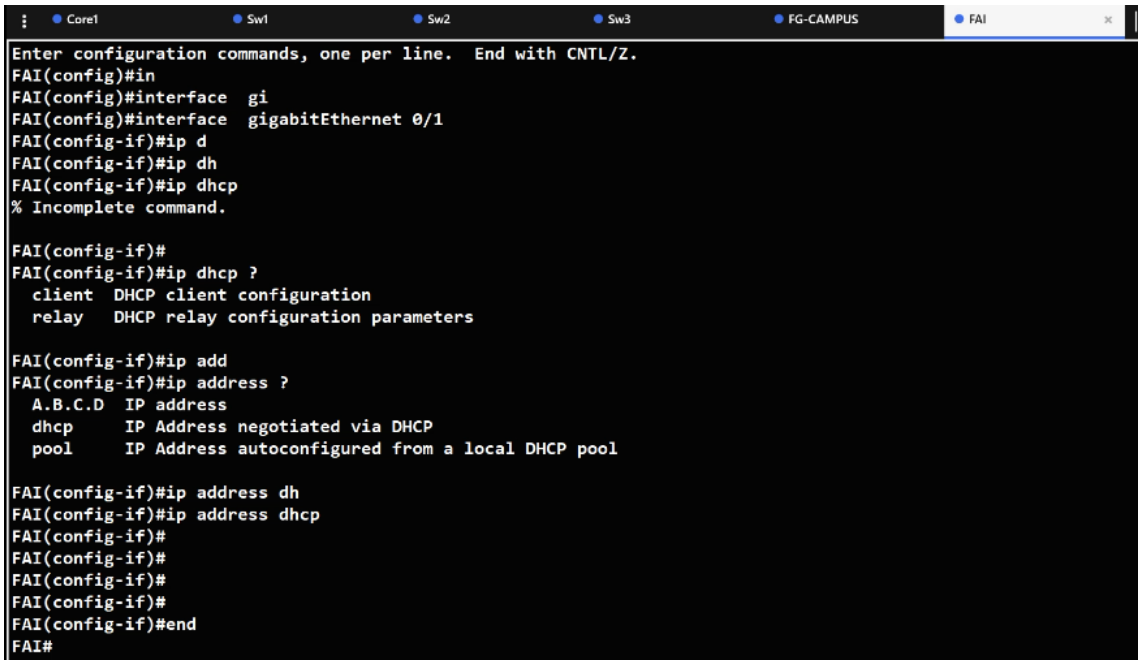


FIGURE 4.22 – Configuration du router.

4.8.3 Partie supervision :

Pour mettre en place la supervision de notre infrastructure, nous avons suivis les étapes d'installation et de réalisation de la solution Zabbix comme suit :

1. **Installation Zabbix pour la supervision :** Notre solution de supervision sera implémentée sur un server, et pour cela nous avons suivis des étapes pour assurer une installation correcte.
2. **Ajout et configuration d'un serveur Zabbix :** Nous ajoutons une machine virtuelle avec l'image de Ubuntu puis avec les commandes d'installations on va installer les packages de Zabbix :

FIGURE 4.23 – Installation de Zabbix.

3. **Attribution d'une adresse IP :** Pour attribuer une adresse à notre serveur, nous allons changer la carte réseau du NAT vers le VLAN 15 et lui attribuer une adresse de cette plage.

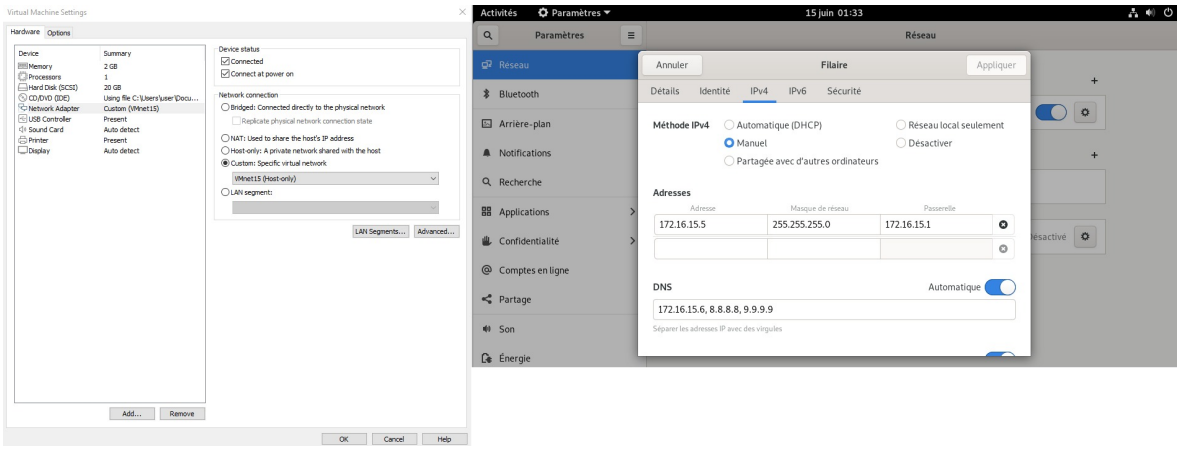


FIGURE 4.24 – Attribution d'une adresse IP pour le serveur.

4. **Installation de l'interface graphique :** Zabbix propose une interface Web qui offre une vue d'ensemble complète de l'environnement surveillé permettant la visualisation des données travers des graphes. Cette interface sera installée en installant les packages de l'interface avec les commandes sur le terminal :

```
libgd3 passé en « installé manuellement ».
libxpm4 est déjà la version la plus récente (1:3.5.12-1.1~deb11u1).
libxpm4 passé en « installé manuellement ».
libxslt1.1 est déjà la version la plus récente (1.1.34-4+deb11u1).
libxslt1.1 passé en « installé manuellement ».
liblua5.3-0 est déjà la version la plus récente (5.3.3-1.1+b1).
liblua5.3-0 passé en « installé manuellement ».
ssl-cert est déjà la version la plus récente (1.1.0+nmu1).
ssl-cert passé en « installé manuellement ».
Les paquets supplémentaires suivants seront installés :
  psmisc
Paquets suggérés :
  php-pear
Les NOUVEAUX paquets suivants seront installés :
  libapache2-mod-php libapache2-mod-php7.4 libonig5 libsodium23 php php-bcmath php-common php-gd php-ldap php-mbstring
  php-mysql php-xml php7.4 php7.4-bcmath php7.4-cli php7.4-common php7.4-gd php7.4-json php7.4-ldap php7.4-mbstring
  php7.4-mysql php7.4-opcache php7.4-readline php7.4-xml psmisc
0 mis à jour, 25 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 5 403 ko dans les archives.
Après cette opération, 22,3 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 psmisc amd64 23.4-2 [198 kB]
Réception de :2 http://deb.debian.org/debian bullseye/main amd64 php-common all 2:76 [15,6 kB]
Réception de :3 http://deb.debian.org/debian bullseye/main amd64 php7.4-common amd64 7.4.33-1+deb11u3 [1 022 kB]
Réception de :4 http://deb.debian.org/debian bullseye/main amd64 php7.4-json amd64 7.4.33-1+deb11u3 [19,3 kB]
Réception de :5 http://deb.debian.org/debian bullseye/main amd64 php7.4-opcache amd64 7.4.33-1+deb11u3 [198 kB]
```

FIGURE 4.25 – Installation de l'interface graphique.

5. **Connexion à l'interface Web de Zabbix :** Pour visualiser les données collectées sur notre tableau de bord, il suffit d'entrer l'adresse IP de Zabbix dans le navigateur :

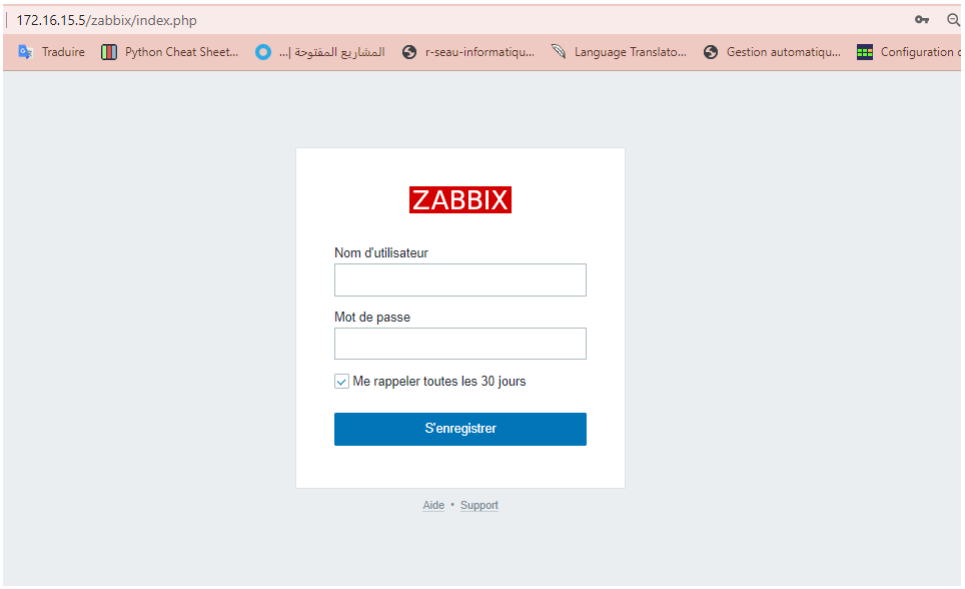


FIGURE 4.26 – L'interface d'authentification de Zabbix.

6. **Tableau de bord :**

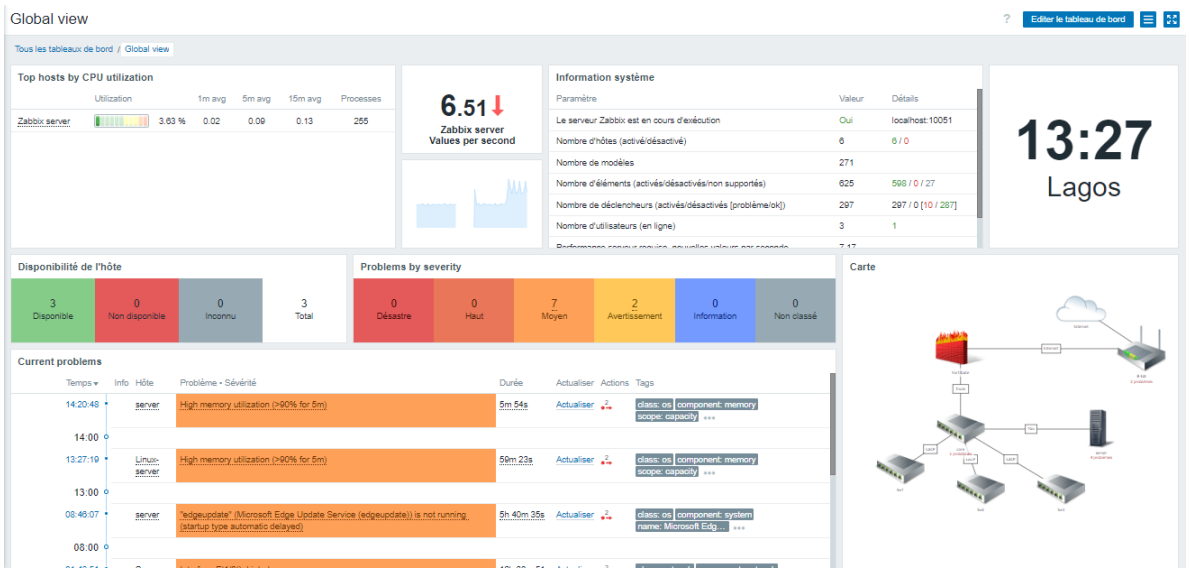


FIGURE 4.27 – Tableau de bord de Zabbix.

7. **Ajout d'un utilisateur :** Cette action présente des avantages en termes de contrôle d'accès, de sécurité et de traçabilité des actions effectuées :

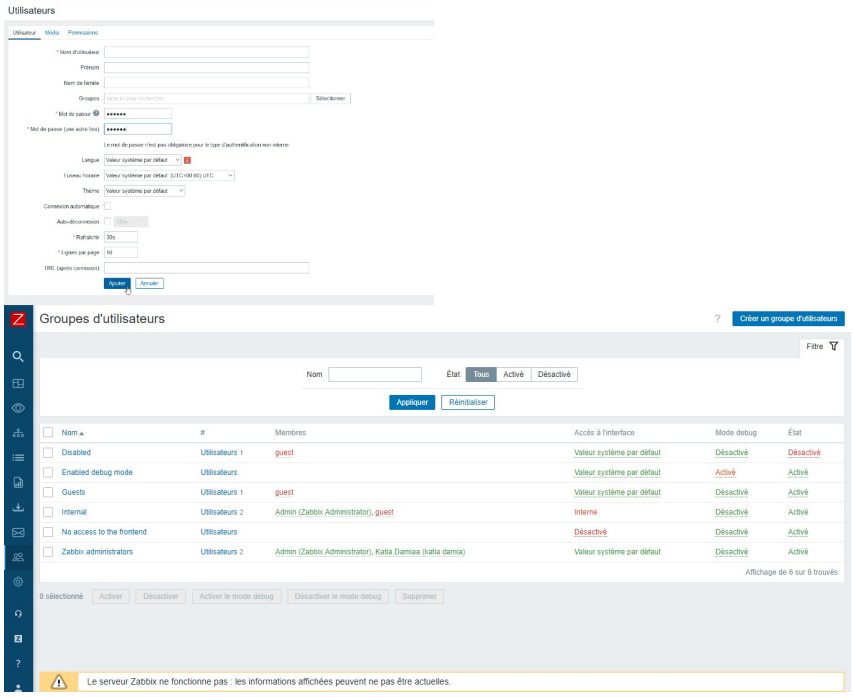


FIGURE 4.28 – Ajouter un utilisateur.

8. **Ajout d'hôtes :** Cela permet une surveillance proactive, la génération d'alertes, etc. Pour ce faire, nous ajoutons l'hôte à la collecte de données et configurons le SNMP sur cet hôte, comme illustré dans la capture d'écran suivante :

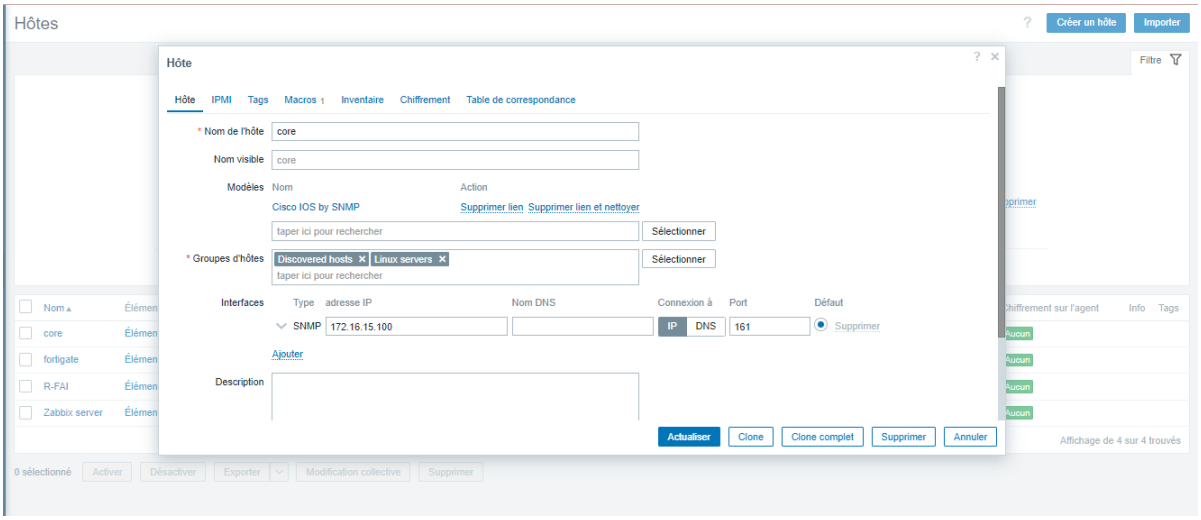


FIGURE 4.29 – Ajouter une hôte.

```
SW-Core(config)#snmp-server c
SW-Core(config)#snmp-server co
SW-Core(config)#snmp-server commu
SW-Core(config)#snmp-server community ?
  WORD  SNMP community string

SW-Core(config)#snmp-server community snmp-core ?
  <1-99>        Std IP accesslist allowing access with this community string
  <1300-1999>   Expanded IP accesslist allowing access with this community
                string
  WORD          Access-list name
  ipv6          Specify IPv6 Named Access-List
  ro            Read-only access with this community string
  rw            Read-write access with this community string
  view          Restrict this community to a named MIB view
  <cr>

SW-Core(config)#snmp-server community snmp-core RO
SW-Core(config)#
```

FIGURE 4.30 – Configurer le SNMP sur cette hôte.

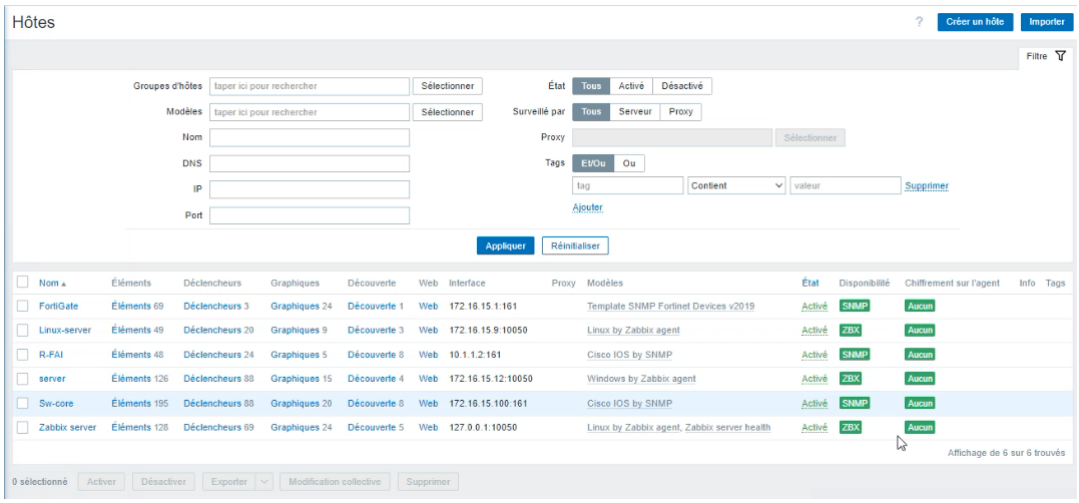


FIGURE 4.31 – Liste des hôtes ajouté.

• Dans le cas où nous ne disposons pas du modèle souhaité pour notre hôte, nous pouvons l'importer comme illustré dans cette figure :

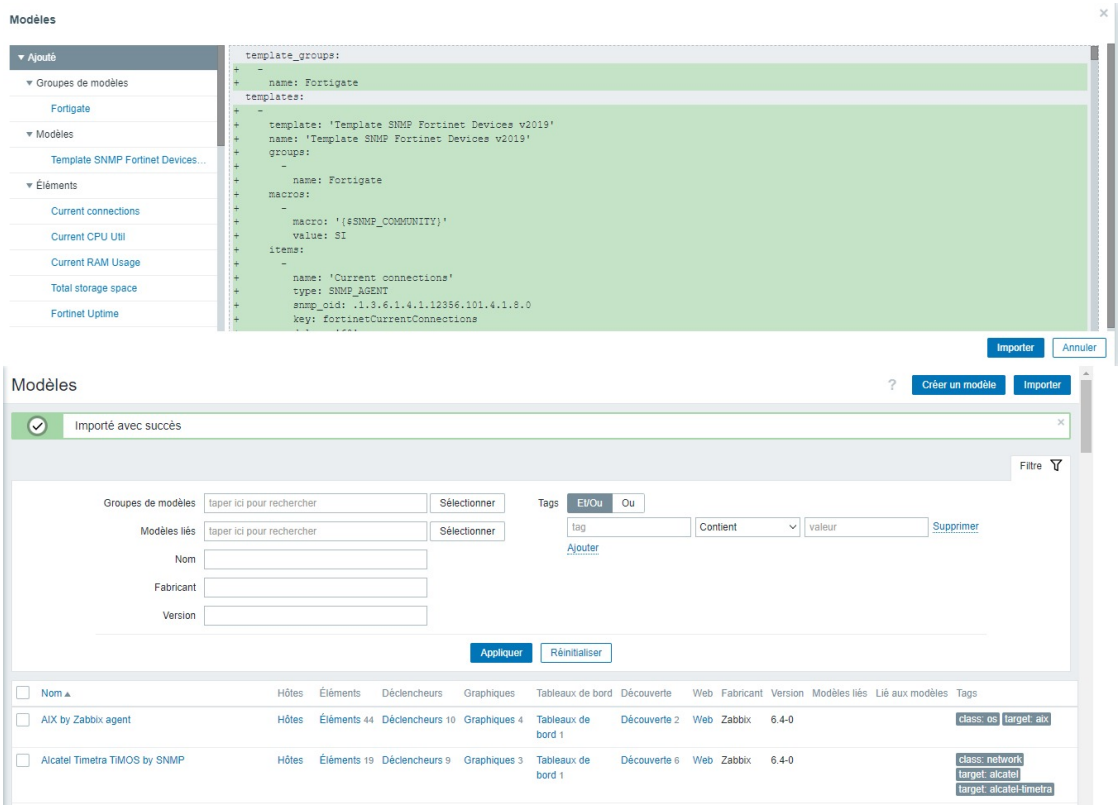


FIGURE 4.32 – Importer un modèle d'hote.

9. **Ajout d'un agent SNMP sur le Fortigate à superviser :**

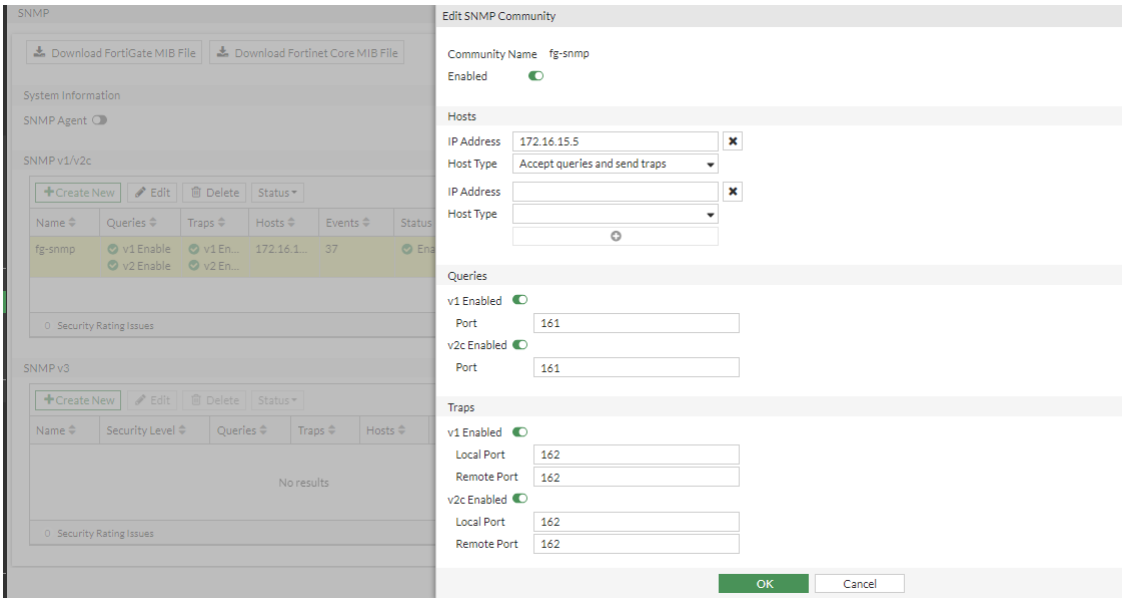


FIGURE 4.33 – Configuration du router.

10. **Ajout d'un serveur à superviser :** Sur chaque serveur que l'on souhaite superviser, nous devons installer et configurer le Zabbix Agent.

— **Installation de l'agent Zabbix :** Un processus qui s'exécute en arrière-plan et collecte les données du serveur pour les envoyer au serveur Zabbix. Vous devrez configurer les paramètres de connexion du Zabbix Agent pour qu'il puisse communiquer avec le serveur Zabbix.la capture ci-dessous nous montre l'interface d'accueil là où on saisit nos données :

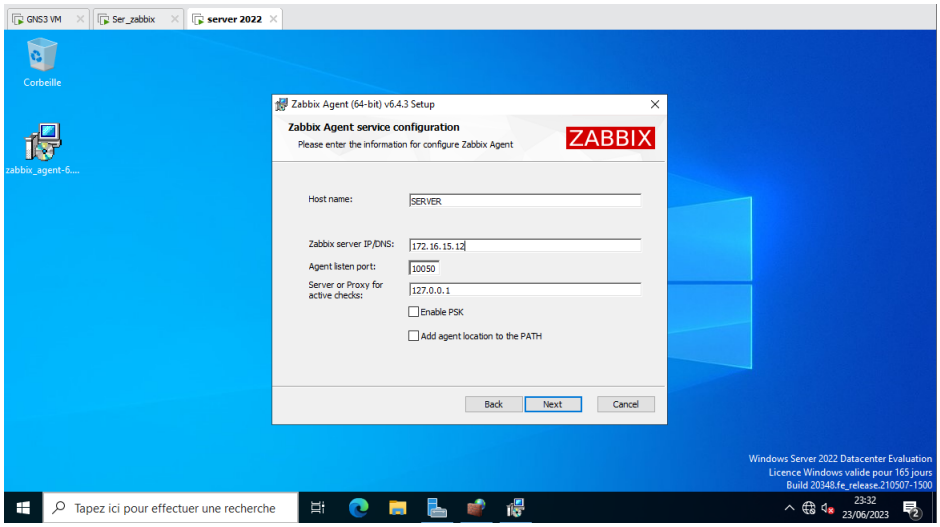


FIGURE 4.34 – L'interface de l'agent Zabbix .

— **Ajout d'un hôte server sur zabbix :** Nous avons créé un hôte dans Zabbix et associer le Zabbix Agents installé sur le serveur à cet hôte. Comme illustré sur la figure suivante :

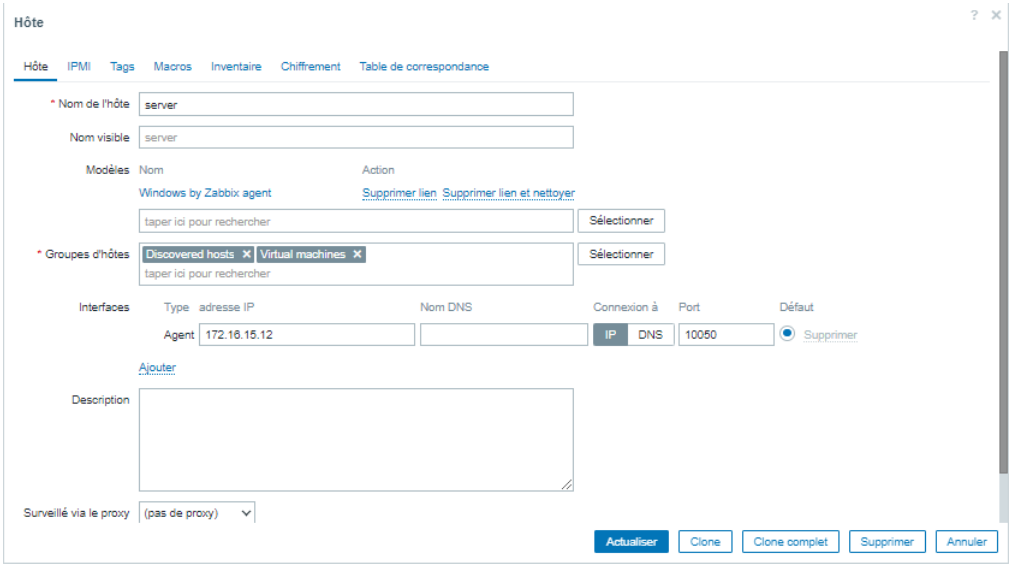


FIGURE 4.35 – Ajout d'un hôte server sur zabbix.

— **Autorisation du trafic sortant :** Pour que l'agent zabbix puisse envoyer son trafic et se connecter au server zabbix, nous avons créé une nouvelle règle qui autorise le trafic sortant par le port 10050 :

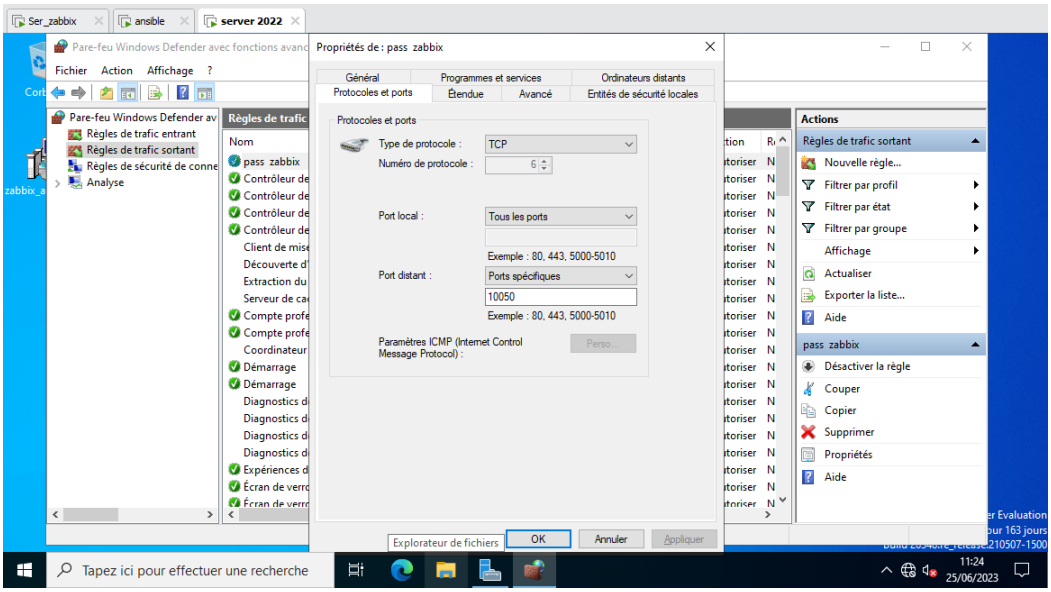


FIGURE 4.36 – Autorisation du trafic sortant.

11. **Ajout d'une carte réseau :** La carte topologique a pour but de représenter graphiquement les relations entre les hôtes, de visualiser la structure la structure et la connectivité de notre réseau surveillé. Dans la figure suivante on a l'affichage de notre carte après sa configuration :

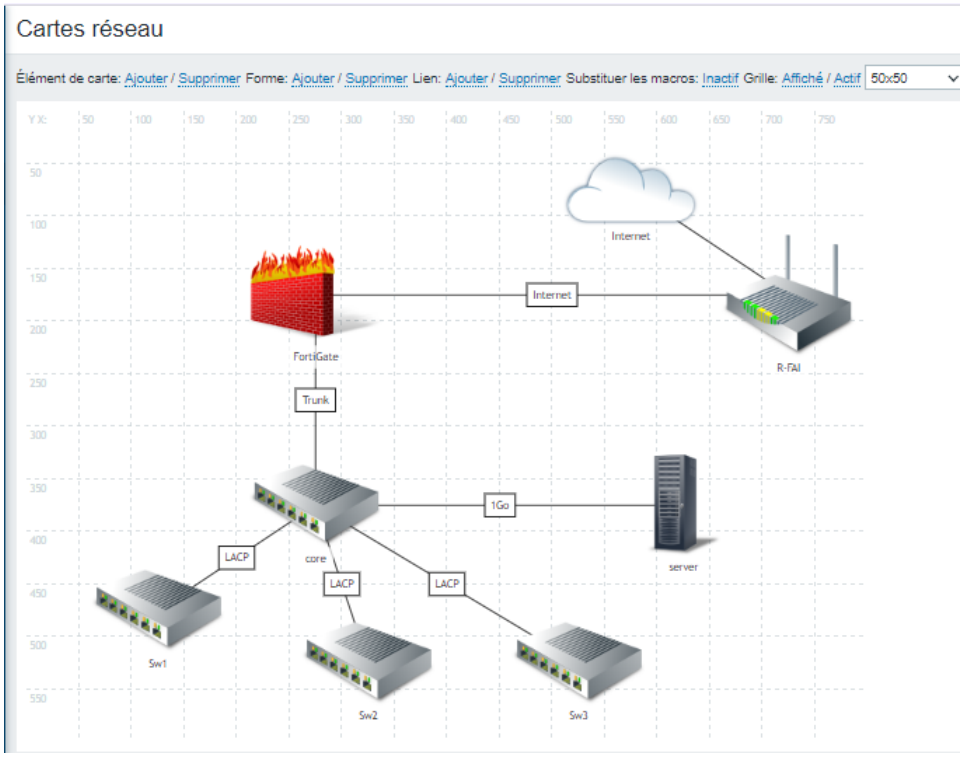


FIGURE 4.37 – carte réseau.

12. **Configuration des alertes :** Cette configuration nous permettra de définir des seuils et des conditions pour déclencher des notifications lorsque des évènements ou des problèmes surviennent dans notre environnement surveillé. Trois étapes sont essentielles pour cela :

— **Génération d'un code des applications :** Sur les configurations du compte Gmail on va générer un code que nous allons utiliser sur le package ssmtp :

FIGURE 4.38 – Génération d'un code des applications.

— **Installation de ssmtp sur zabbix :** Sur le server zabbix (Ubuntu) nous allons installer ssmtp avec les commandes suivantes :

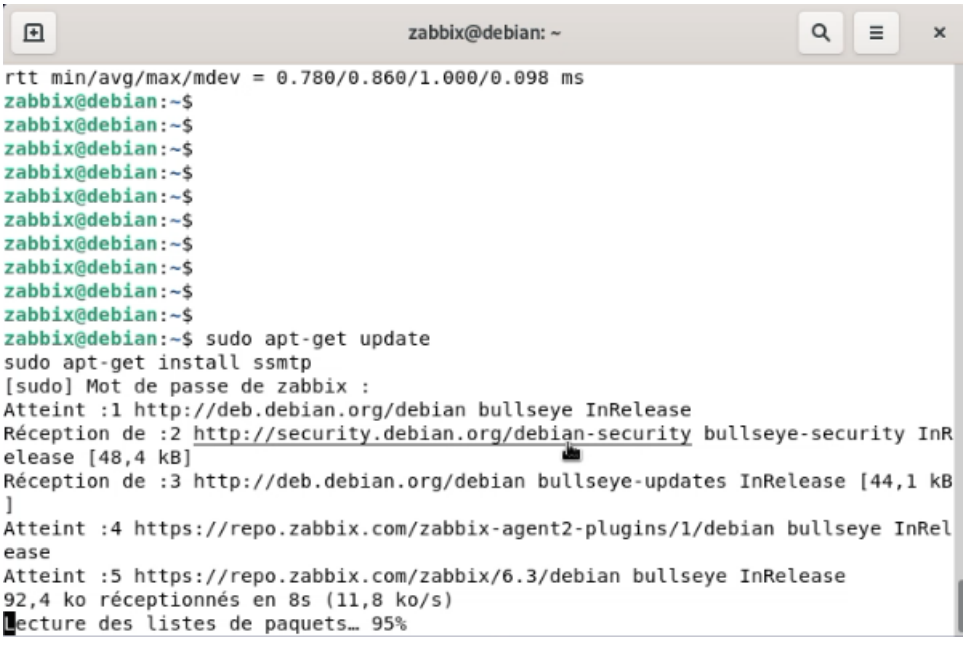


FIGURE 4.39 – Installation de ssmtp sur zabbix.

Puis nous avons saisi nos informations sur le fichier :

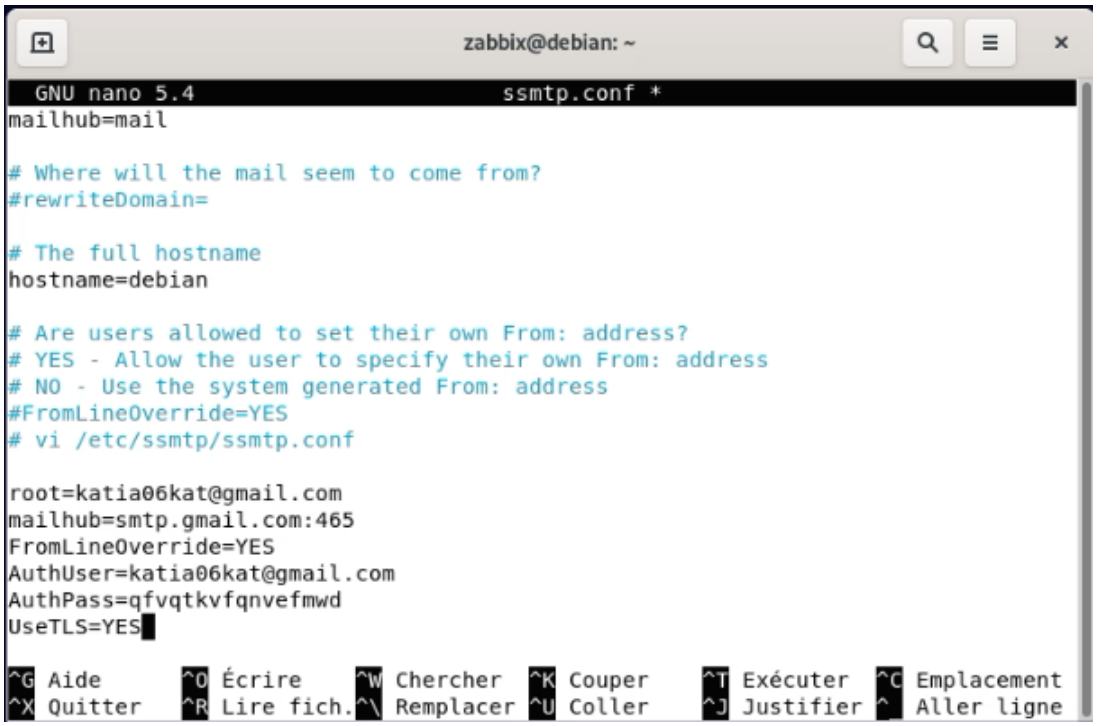


FIGURE 4.40 – Modification du fichier ssmtp.

— **Activation de l'email pour les alertes :** En allant sur alertes, on clique sur type de media et on active l'option Email :

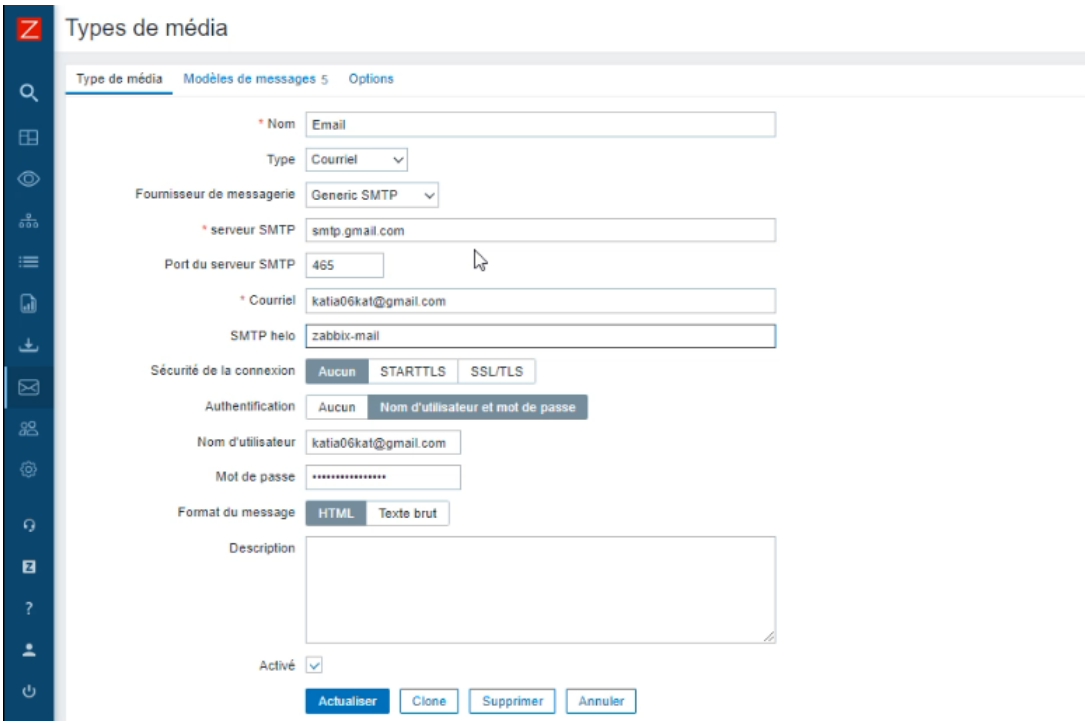


FIGURE 4.41 – Activation de l'email pour les alertes.

- **Test :**

— **Reload routeur :** Nous avons tester de redémarrer le routeur et un message d'alerte a été transmis :

FIGURE 4.42 – Redémarage du routeur

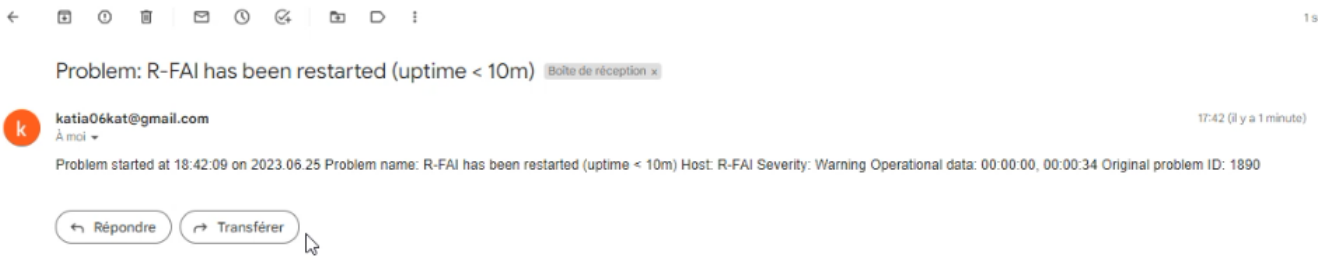


FIGURE 4.43 – Alertre du redémarage du routeur

— **Reboot Pare-feu :** Nous avons essayer aussi de redémarrer notre firewall et nous avons reçu la notification d'alerte sur Gmail :

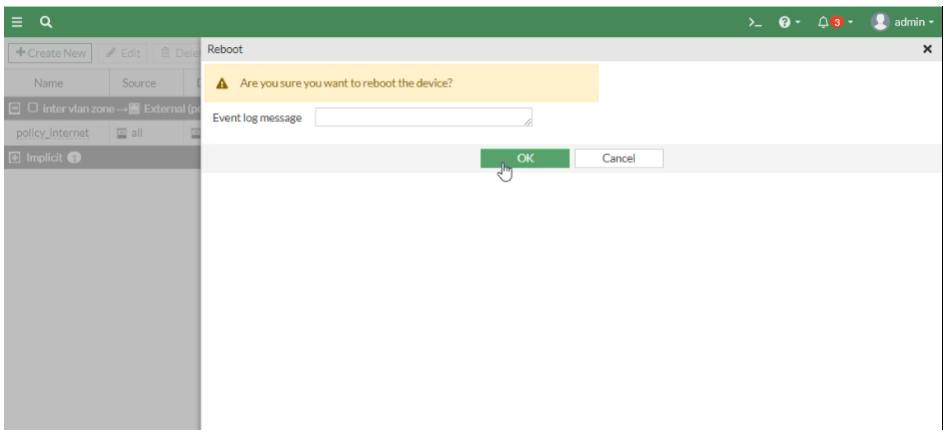


FIGURE 4.44 – Redémarage du pare-feu

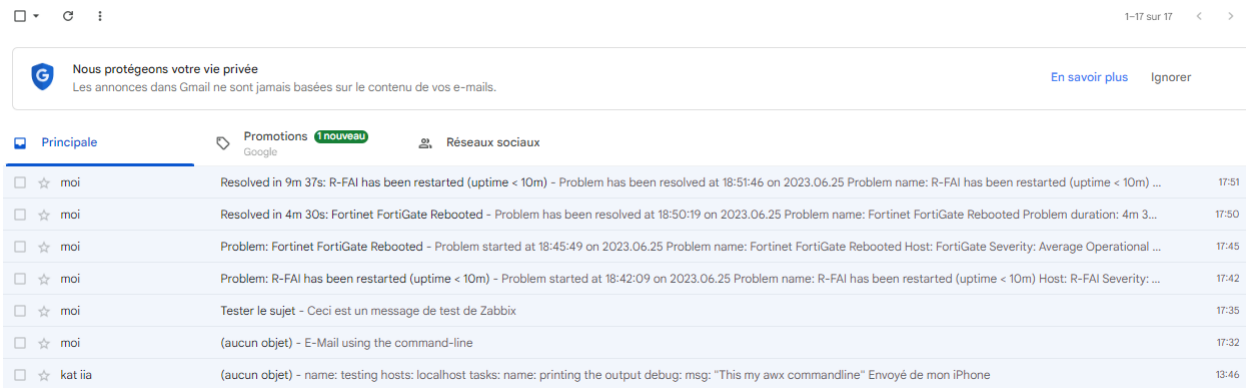


FIGURE 4.45 – Alertre du redémarage du pare-feu

4.8.4 Partie Automatisation :

La réalisation de la solution implique plusieurs étapes clés pour automatiser efficacement les taches et la gestion de l'infrastructure, cette réalisation nécessite une approche itérative, ou nous commençons par des taches simples et évoluons progressivement vers des automatisations plus simples :

1. **Ajout et configuration d'une machine virtuelle :** Sur cette machine on installe Ubuntu avec son image, puis on configure la connectivité réseau de la VM :

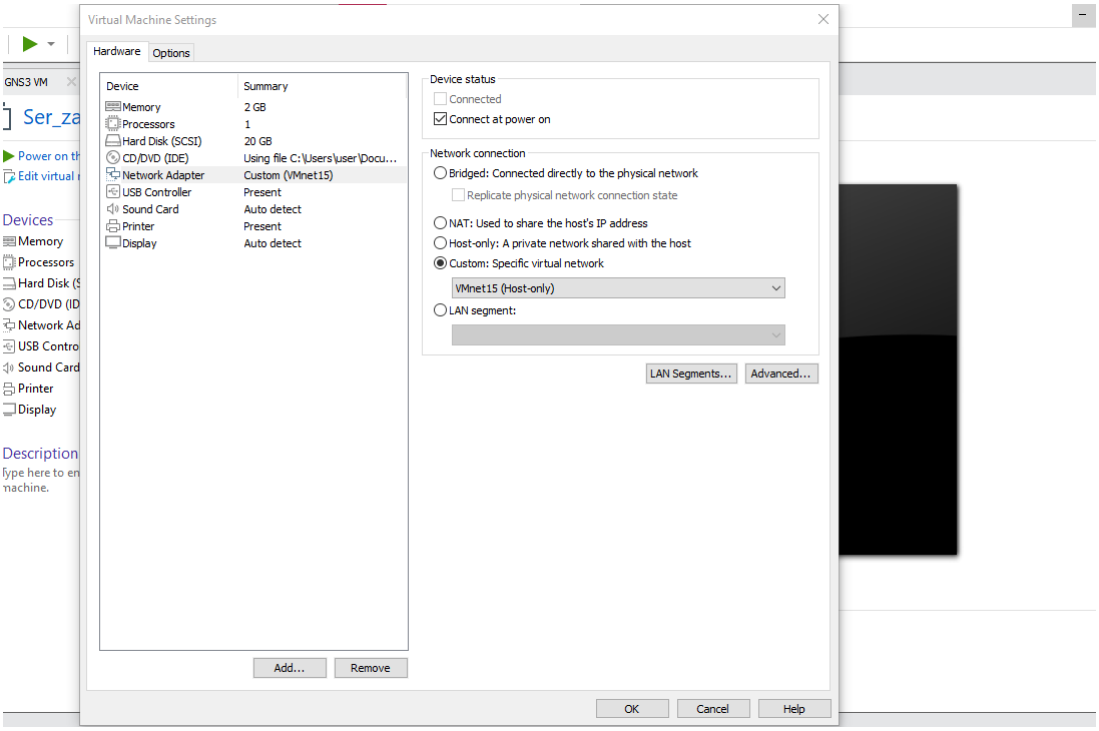


FIGURE 4.46 – Configuration de la carte réseau de Ansible.

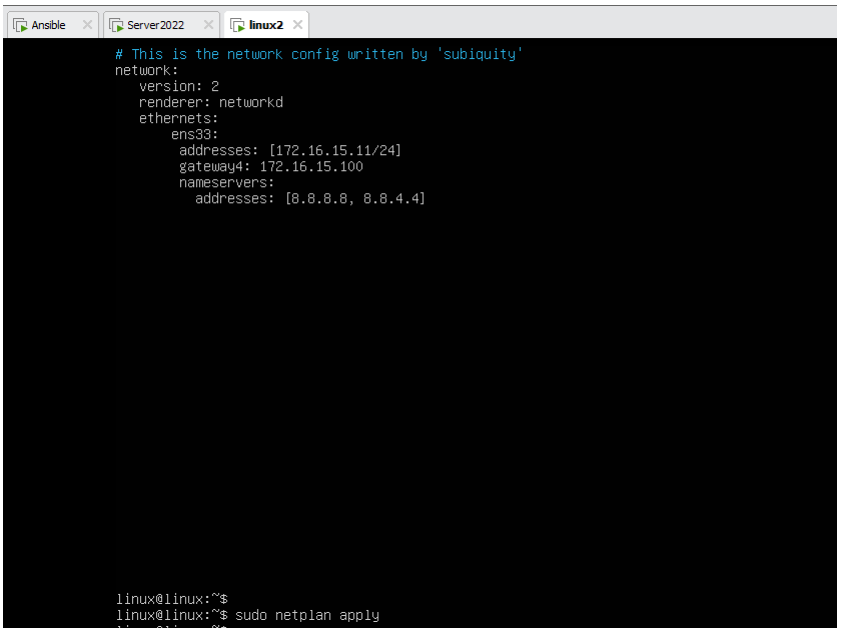


FIGURE 4.47 – Changement d'adresse du serveur Ansible.

2. **Installation de Ansible :** nous avons utilisé l'outil de gestion des packages Python, Pip, pour installer Ansible, et exécuté une suite de commande dans la console :

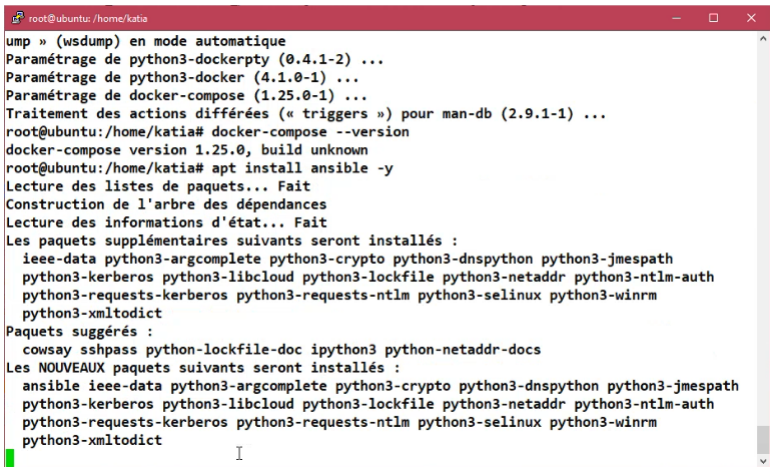


FIGURE 4.48 – Installation d'Ansible.

3. **Vérification de l'installation :** Après l'installation nous avons exécuté la commande suivante pour vérifier qu'Ansible est installé correctement :

```
Last login: Wed Jun 14 12:50:17 2023
ansible@ubuntuserver20:~$ ansible --version
ansible 2.9.6
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/home/ansible/.ansible/plugins/modules', '/u
sr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3/dist-packages/ansible
  executable location = /usr/bin/ansible
  python version = 3.8.10 (default, May 26 2023, 14:05:08) [GCC 9.4.0]
```

FIGURE 4.49 – Vérification de l'installation.

4. **Installation de l'interface graphique :** AWX est l'interface graphique open source d'Ansible, qui fournit une interface web conviviale pour la gestion et l'automatisation des tâches avec Ansible. Nous utilisons des commandes pour le téléchargement du code source AWX, puis nous éditons le fichier d'inventaire pour configurer les informations de l'authentification et finalement l'installer :

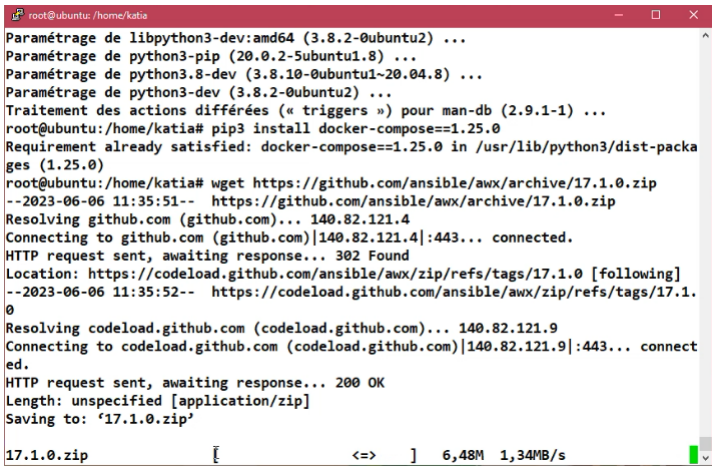


FIGURE 4.50 – Installation de l'interface graphique AWX.

5. **Affichage de l'interface AWX :** Apres l'installation précédente, nous avons obtenu les interfaces suivantes en utilisant l'adresse IP du serveur Ansible :

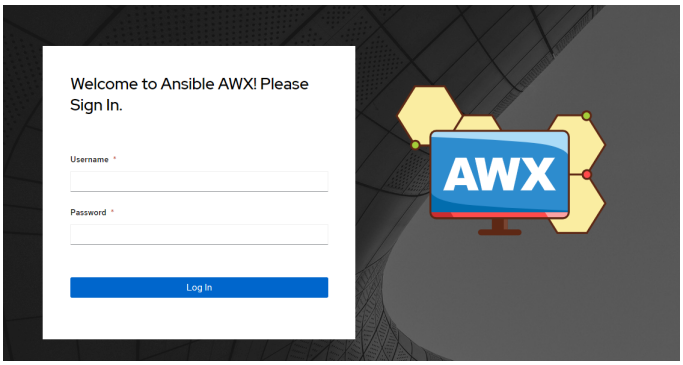


FIGURE 4.51 – Interface d'authentification AWX.

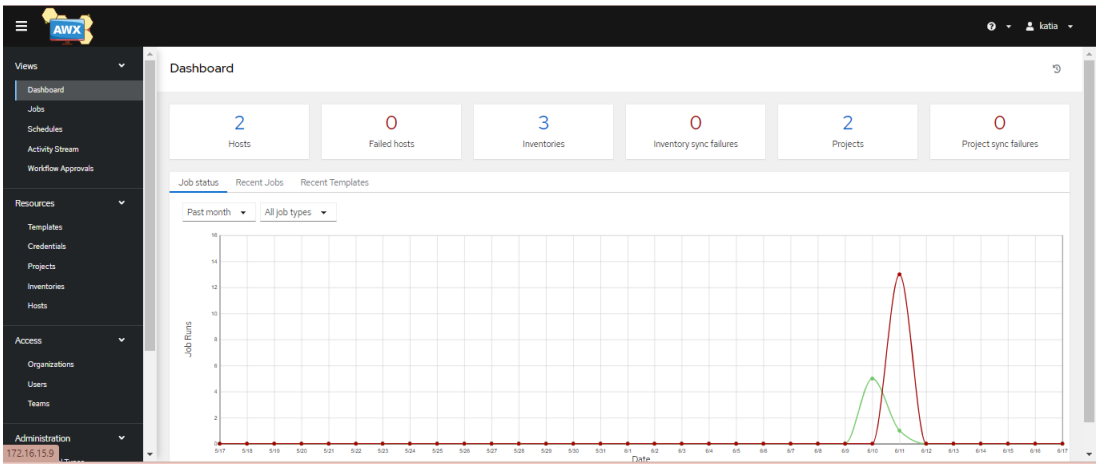


FIGURE 4.52 – L'interface d'accueil AWX.

— **Ajout des modèles de projets :** En ajoutant ces modèles nous pourrions automatiser et simplifier le déploiement de nos configurations et gagner en efficacité dans la gestion de notre infrastructure.

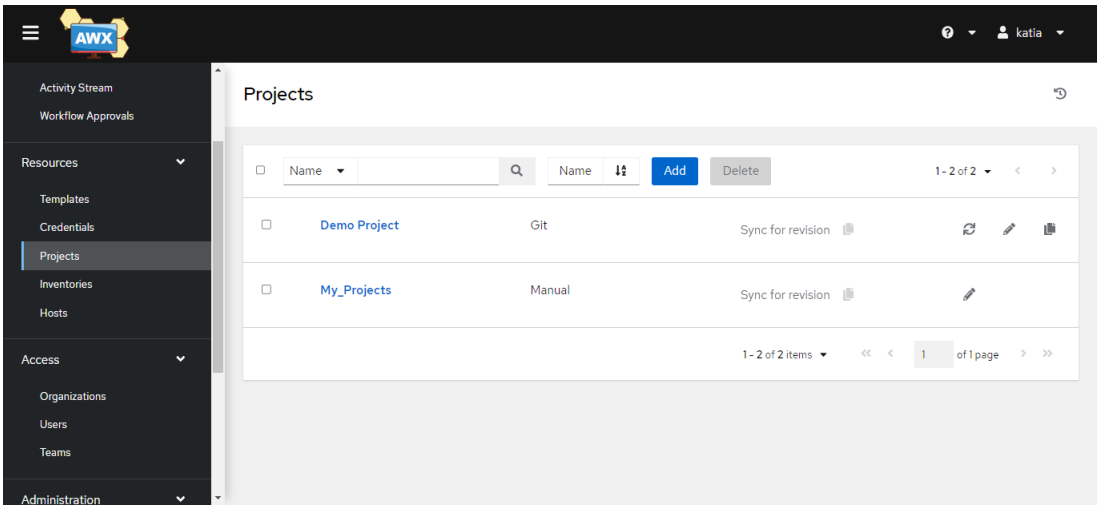


FIGURE 4.53 – Ajout des projets.

6. **Ajout du service SNMP à l'active directory du server :** Pour ajouter le service SNMP à un contrôleur de domaine dans le server Windows nous allons suivre les étapes suivantes :

— **Configuration de l'inventaire :** Il suffit de créer un fichier inventaire et de spécifier les informations sur notre server AD, y compris l'adresse IP :

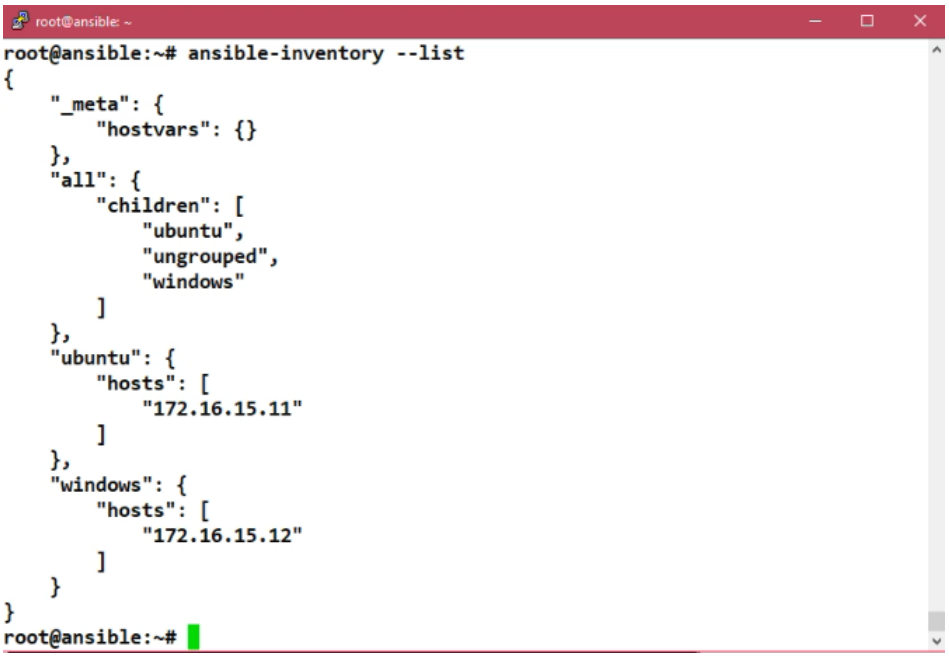


FIGURE 4.54 – Inventaire de l'agent snmp.

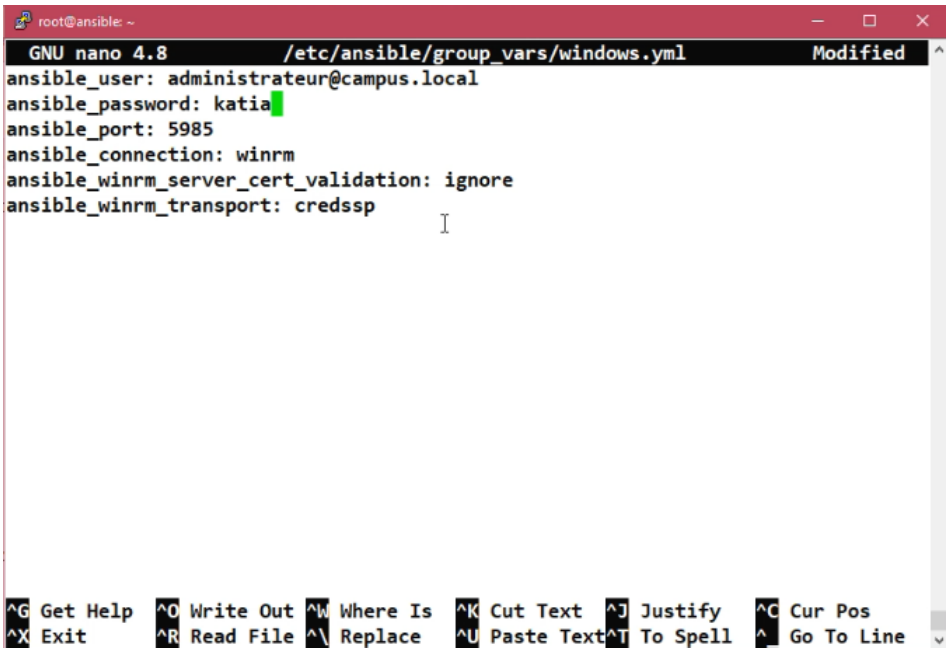


FIGURE 4.55 – Définir les variables.

— **Création d'un playbook d'ajout de SNMP :** Dans ce fichier YAML nous allons spécifier les taches nécessaires pour ajouter le service snmp à l'active directory :

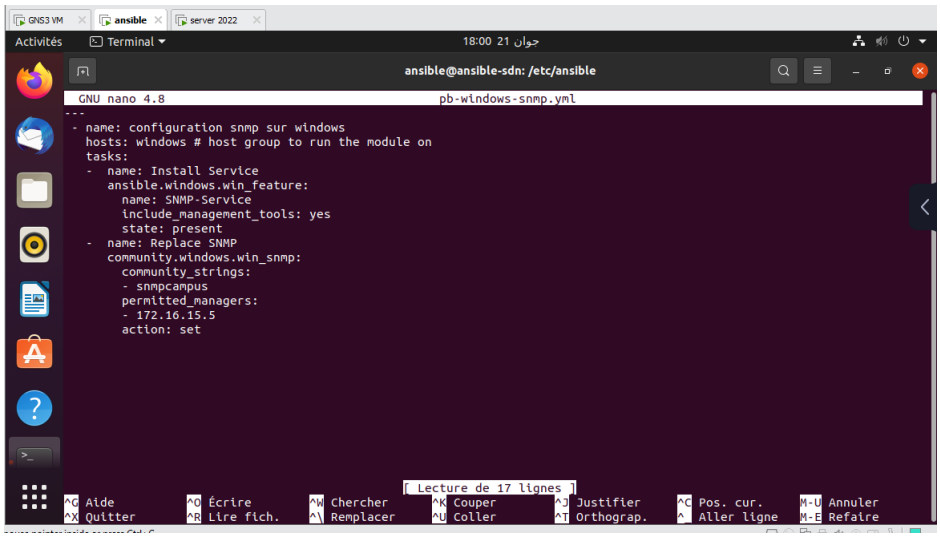


FIGURE 4.56 – Playbook snmp.

— **Affichage :** Apres l'exécution du playbook à l'aide de la commande qui configura les taches définies sur le serveur Active directory, le service snmp sera ajouter sur l'AD :

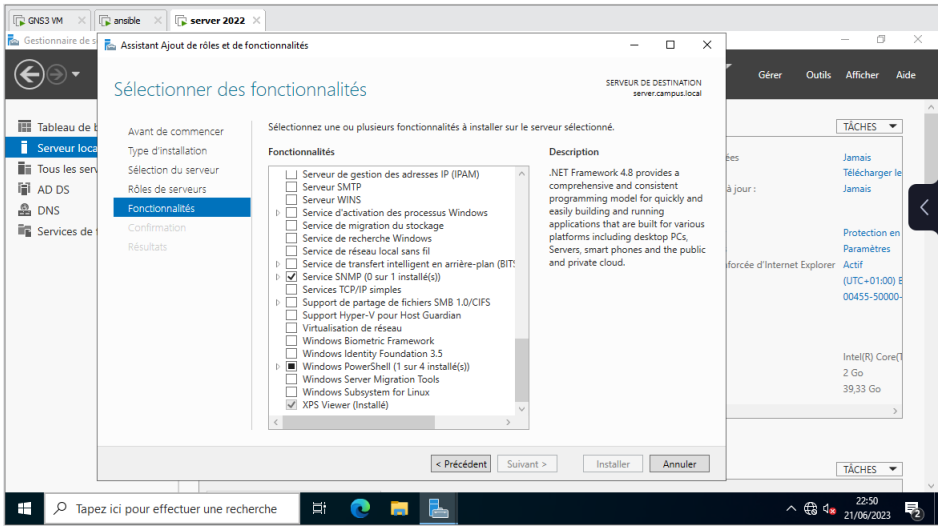


FIGURE 4.57 – L'ajout de snmp sur l'active directory.

7. **Mise à jour du server :** Ansible permet une gestion centralisée des taches de mise à jour, en définissant et en gérant les playbook depuis un emplacement central.

— **Création d'un playbook de mise à jour :** Dans ce cas nous n'avons pas besoin de créer l'inventaire vu qu'il a déjà été créé. Nous avons créé le fichier pb-apdate.yml :

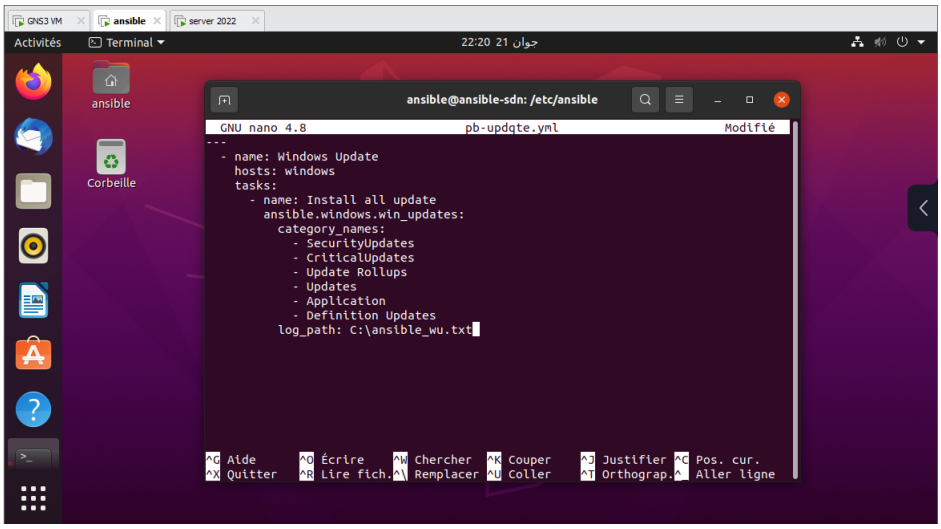


FIGURE 4.58 – Création du fichier pb-apdate.yml .

— **Affichage :** Apres l'exécution du playbook, nous allons voir que le serveur a démarré la mise à jour :

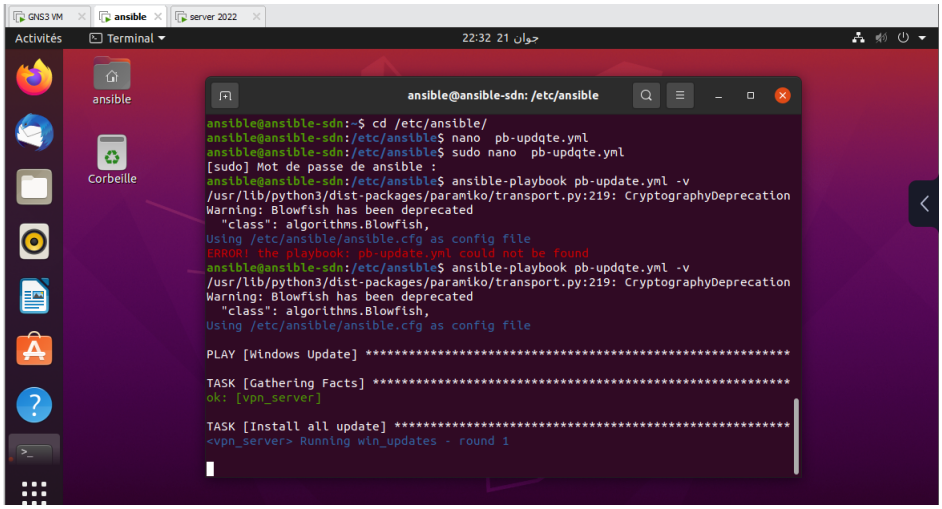


FIGURE 4.59 – Exécution du playbook.

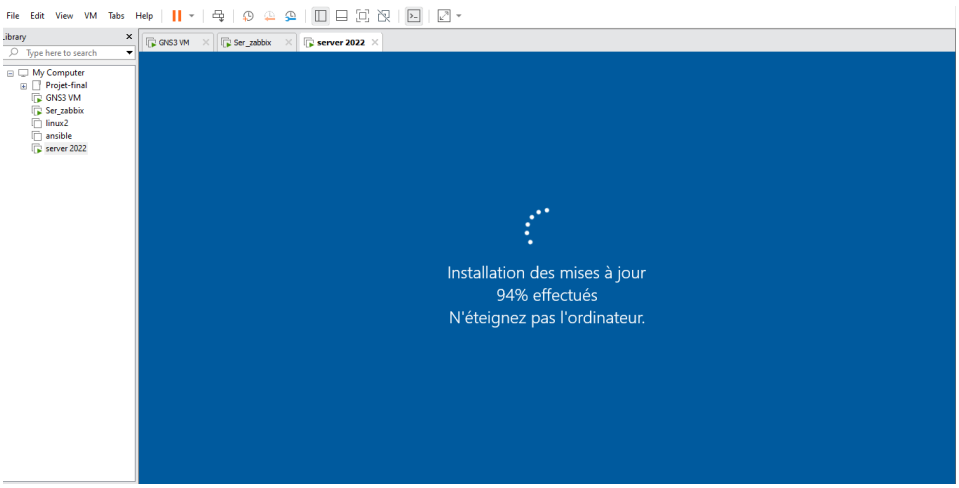


FIGURE 4.60 – Lancement de la mise à jour .

4.9 Conclusion et perspectives

En combinant ces deux solutions complémentaires Ansible et Zabbix, il est possible de bénéficier d'une infrastructure automatisée et supervisée de manière proactive, une gestion efficace, que ce soit pour le déploiement de nouvelles configuration, les mises à jour, surveillance des performances ou la solution proactive des problèmes.

Conclusion

En conclusion, ce mémoire a présenté une étude sur les réseaux informatiques et la sécurité des systèmes d'information. Nous avons commencé par une étude et une analyse des besoins de l'entreprise ngtmeziani en matière de sécurité et de gestion de réseau, en examinant les équipements existants, les exigences de performance, les objectifs de sécurité, et les contraintes budgétaires. Nous avons utilisé cette analyse pour identifier les solutions d'automatisation et de supervision de réseau les plus pertinentes pour répondre aux besoins de l'entreprise.

Nous avons utilisé GNS3 et la VMWARE WORKSTATION PRO pour la réalisation et la simulation là où nous avons créé des Vlans pour l'entreprise et configurer les protocoles nécessaires comme le VTP, LACP, Trunk, comme nous avons configurer le pare-feu. Puis Nous avons présenté les étapes de mise en œuvre de la solution Zabbix pour la supervision et celle de Ansible pour la supervision de notre réseau, les problèmes rencontrés.

Les résultats obtenus ont montré que l'automatisation et la supervision de réseau peuvent améliorer considérablement la performance, la fiabilité et la sécurité du réseau.
En termes de perspectives, l'évolution des solutions Ansible et Zabbix se concentrera probablement sur l'amélioration des convivialité et l'intégration avec d'autres outils technologique, Comme nous envisageons utiliser l'automatisation à distance avec Ansible sur l'ensemble de notre infrastructure réseau pour garantir une configuration cohérente et sans erreurs humaines.

Bibliographie

[1] https://www.iso.org/fr/standard/80585.html, (Consulter le 15 avril 2023).

[2] https://www.orangecyberdefense.com/fr/insights/blog/gestion-des-vulnerabilites/vulnerabilites-de-quoi-parle-t-on, (Consulté le 02 mai 2023).

[3] https://www.pdfdrive.com/tout-sur-la-s%C3%A9curit%C3%A9-informatique-e186515890.html, (Consulté le 02 mai 2023).

[4] https://resources.infosecinstitute.com/topic/vlan-network-chapter-5/, (Consulté le 02 mai 2023).

[5] http://www.univ-bejaia.dz/xmlui/bitstream/handle/123456789/20673/Audit%20de\%20s%C3%A9curit%C3%A9.pdf?sequence=1&isAllowed=y, (Consulté le 07 avril 2023).

[6] http://dspace.univ-bouira.dz:8080/jspui/bitstream/123456789/9323/1/bouaoud\%20katia%20%C2%A7%20arabi%20selma.pdf, (Consulté le 07 juin 2023).

[7] https://www.iso.org/fr/isoiec-27001-information-security.html, (Consulté le 10 avril 2023).

[8] N.kammaOuandji,ÂńMonitoring:supervisionetmÃľtrologie|Supervision|IT-Connect|Base,Historique,EtatÂż,

[9] https://www.appvizer.fr/magazine/services-informatiques/supervision-applicative/supervision-reseau-enjeux\-bonnes-pratiques-logiciels,
(Consulté le 10 juin 2023).

[10] Wileyreseauxinformatiques6ed,

[11] https://definir-tech.com/redondance-du-reseau/,
(Consulté le 10 mai 2023).

[12] https://profilbaru.com/article/Network_monitoring,
(Consulté le 11 juin 2023).

[13] http://www.o00o.org/monitoring/solutions.html,
(Consulté le 11 juin 2023).

[14] https://wiki-tech.io/Supervision/Centreon/Pr%C3%A9sentation,
(Consulté le 12 juin 2023).

[15] https://fr.scribd.com/document/621478373/comparatifsystsupervision-calasguilhem#,
(Consulté le 12 juin 2023).

[16] https://www.iso.org/fr/standard/80585.html,
(Consulté le 15 avril 2023).

[17] https://fr.wikibooks.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_informatiques/S%C3%A9curit%C3%A9_informatique/Chiffrement_de_flux_et_VPN,
(Consulté le 15 mai 2023).

[18] https://gandalsmart.com/securite-informatique-les-mecanismes-\dauthentification-utilisateurs-systemes/,
(Consulté le 20 avril 2023).

[19] https://goteleport.com/blog/ssh-tunneling-explained/,
(Consulté le 20 mai 2023).

[20] https://geekflare.com/fr/ids-vs-ips-network-security-solutions/,
(Consulté le 20 mai 2023).

[21] https://www.syloe.com/glossaire/centralisation-de-logs/,
(Consulté le 21 mai 2023).

[22] https://shs.hal.science/halshs-02560339/document,
(Consulté le 22 avril 2023).

[23] https://www.dnsstuff.com/fr/qu-est-ce-que-syslog,
(Consulté le 22 mai 2023).

[24] https://www.pdfdrive.com/les-r%C3%A9seaux-informatiques-e50017792.html.,
(Consulté le 27 mars 2023).

[25] http://math.unilyon1.fr/irem/Formation_ISN/formation_reseau/reseaux_generalites\/generalites.html.,
(Consulté le 27 mars 2023).

[26] https://www.pidaxy.com/2019/10/09/securite-de-\linformation-pour-tous/,
(Consulté le 27 mars 2023).

[27] https://community.fs.com/fr/blog/tcpip-vs-osi-whats\-the-difference-between-the-two-models.html.,
(Consulté le 27 mars 2023).

[28] https://www.pdfdrive.com/r%C3%A9seux-et-\transmissions-6e-ed-e185908612.html,
(Consulté le 27 mars 2023).

[29] https://www.pdfdrive.com/network-programmability-and-\automation-e183876785.html,
(Consulté le 30 mai 2023).

Résumé

Le réseau informatique dans une entreprise est son cerveau, car il joue un rôle crucial en assurant la communication efficace et le partage de données tout en garantissant la confidentialité et la sécurité de cette infrastructure. C'est en allant de ce principe que nous avons travaillé dans le but d'améliorer l'efficacité opérationnelle, la fiabilité et de réduire les erreurs humaines.
Nous avons installé et configuré notre architecture réseau, en la sécurisant avec la segmentation du réseau LAN en VLANs et en configurant les protocoles VTP, LACP, TRUNK, puis nous avons installé et configuré les solutions Zabbix pour supervision et Ansible pour l'automatisation, au final nous avons simulé ces solutions sur VMWARE PRO 17 et GNS3.

Mots clés : segmentation du réseau, LAN, VLAN, VTP, LACP, TRUNK, Zabbix, Ansible, VMWARE PRO 17, GNS3.

Abstract

The computer network in a company is like its brain, as it plays a crucial role in ensuring effective communication and data sharing while also guaranteeing the confidentiality and security of this infrastructure. With this principle in mind, we worked towards improving operational efficiency, reliability, and reducing human errors.
We installed and configured our network architecture, securing it with LAN network segmentation into VLANs and configuring protocols such as VTP, LACP, and TRUNK. We then installed and configured Zabbix for supervision and Ansible for automation, and finally simulated these solutions on VMWARE PRO 17 and GNS3.

Keywords : network segmentation, LAN, VLAN, VTP, LACP, TRUNK, Zabbix, Ansible, VMWARE PRO 17, GNS3.