19/12/2025

# Conception et mise en place d'une infrastructure réseau sécurisée et supervisée pour une PME fictive

**Projet réalisé dans le cadre du module SAE 51 – Administration, Sécurité et Supervision des Réseaux**

SAE 51 – NetSecure Solutions – IUT de Rouen – 2025–2026
Réalisé par : Cécilia Emmanuelle Boukaka/Camila Kamga/Yassmine Habil

## Table des matières

## Introduction et Contexte du Projet

Ce document présente l'architecture technique complète conçue et déployée pour la PME fictive "NetSecure Solutions". Forte d'environ 30 collaborateurs, l'entreprise est structurée en trois pôles distincts : administratif, commercial et technique/IT. La mission principale de ce projet consistait à bâtir une infrastructure réseau et système entièrement virtualisée, répondant à des exigences strictes en matière de sécurité, de supervision et d'automatisation partielle.

L'objectif étant de créer un environnement informatique robuste, segmenté et facilement administrable. Réalisé dans le cadre de la SAE 51 du BUT R&T, ce dossier d'architecture se veut à la fois un livrable professionnel réaliste et un support pédagogique détaillant chaque décision technique.

L'ensemble de la conception présentée ci-après découle directement des besoins et contraintes formalisés dans le cahier des charges de l'entreprise, qui constitue le fondement de toutes les décisions techniques du projet.

# Premier CHAPITRE :

# Cahier de Charge de NetSecure

# I. Introduction & Contexte

La PME **NetSecure Solutions**, spécialiser dans le conseil et intégration IT, support technique, maintenance, développement interne basée à Rouen (Normandie), compte environ **30 collaborateurs** répartis en 3 pôles :

- Service administratif (gestion, finances, RH),
- Service commercial (prospection, vente, relation client),
- Service technique / IT (support, maintenance, Développeur).

L'entreprise souhaite **moderniser** son infrastructure pour :

- Sécuriser les échanges,
- Centraliser les services (AD, DNS, fichiers),
- Superviser en temps réel ses équipements,
- Automatiser des tâches répétitives.

Ce projet est conduit dans le cadre du **module SAE 51 – Administration, Sécurité et Supervision des Réseaux** du **BUT Réseaux & Télécommunications**. Il permet de mettre en pratique la virtualisation, la sécurité réseau, l'administration système et la supervision.

*Pré-requis :*

Compétences Réseaux, Administration Systèmes, Supervision

# II. Objectifs du projet

## 1) Objectifs techniques

Mettre en place une infrastructure réseau moderne, sécurisée et supervisée

- Concevoir une **architecture réseau hiérarchisée** avec **segmentation VLAN**.
- Mettre en place un **pare-feu pfSense** pour le filtrage, le NAT, les ACL inter-VLAN et le VPN.
- Installer un **serveur de supervision Zabbix**.
- Déployer un **serveur Windows Server 2022** (AD, DNS, DHCP).
- Mettre en place un **système d'automatisation Ansible**.

- Documenter toutes les configurations.

## 2) Objectifs pédagogiques

L'objectif est :

- Appliquer les connaissances vues en **réseaux, systèmes, sécurité, supervision**.
- Travailler en **mode projet** (répartition, Gantt, livrables).
- Utiliser **GitHub/GitLab** la communication et le survi du projet.
- Produire une **documentation technique + utilisateur**.

En fin de concevoir, réaliser et présenter une solution technique.

Deuxième CHAPITRE :

# Documentation Technique

## III. Analyse/Contexte et des Besoins Métier

L'organisation de NetSecure Solutions en trois pôles distincts (Administratif, Commercial, Technique) impose une communication fluide mais contrôlée. La principale nécessité est de protéger les actifs informationnels critiques, tels que les données financières du pôle administratif et les données clients du pôle commercial, contre tout accès non autorisé.

Il est impératif de mettre en œuvre une architecture de "moindre privilège" où chaque pôle n'a accès qu'aux ressources strictement nécessaires à ses fonctions, afin de minimiser la surface d'attaque interne et de se conformer aux bonnes pratiques de sécurité.

## IV. Problématique et justification du choix

**Problématique :**

*Comment fournir à une PME une infrastructure réseau **sécurisée, segmentée, supervisée et automatisée** en utilisant principalement des solutions open source et un environnement virtualisé ?*

Résumé : Ce projet a pour objectif la conception et le déploiement d'une infrastructure virtualisée complète pour la PME fictive NetSecure Solutions, en se basant sur quatre machines virtuelles distinctes (VM). Le travail est structuré en trois grandes parties thématiques couvrant **la fondation réseau, les services essentiels, et les outils de gestion opérationnelle**. L'objectif de ce travail consiste à proposer infrastructures virtuelle réseau sécurisée, supervisée et fonctionnelle pour l'Entreprise NetSecure.

En se basant sur quatre machines virtuelles distinctes (VM). Le travail est structuré en trois grandes parties thématiques couvrant la fondation réseau, les services essentiels, et les outils de gestion opérationnelle.

**Première Partie : Architecture Réseau et Sécurité Fondamentale**

Cette partie établit les fondations de l'infrastructure et garantit la sécurité.

La sécurité est assurée par la VM **pfSense** (Pare-feu / Routeur, IP 10.10.99.1 sur le VLAN 99), qui est configurée pour gérer les interfaces, le **pare-feu**, le **NAT**, et le **relais DHCP**.

Nous avons mis en place un **plan d'adressage complet des VLANs** (dans la plage 10 à 99). La segmentation et le routage sécurisé sont assurés par le **Trunk / Tagging des interfaces VirtualBox** et l'application stricte d'**ACL inter-VLAN et de règles de sécurité**.

**Deuxième Partie : Services Centralisés Windows Server**

Cette partie se concentre sur les services essentiels à l'entreprise, hébergés sur la machine **WinServ2022** (AD + DNS + DHCP, IP 10.10.10.2 sur le VLAN 10).

Nous avons configuré les services suivants :

1. **Active Directory (AD) :** Création du domaine, des **GPO** (Stratégies de Groupe), et gestion des comptes utilisateurs.

2. **DNS :** Mise en place des **zones et des enregistrements** nécessaires (A, MX, CNAME).

3. **DHCP :** Définition des **portées et des réservations** pour l'attribution des adresses.

4. Nous avons également veillé à l'**intégration** fonctionnelle de ces services avec pfSense et Zabbix.

**Troisième Partie : Supervision, Automatisation et Validation**

Dans cette étude, nous avons mis en place et configuré une station de surveillance Zabbix chargée d'alerter l'administrateur en cas de pannes ou de surcharge sur le réseau. Certaines fonctionnalités tel qu'Agent-Zabbix et le protocole SNMP qui permettent de surveiller les machines utilisant les systèmes d'exploitation Linux et Windows ont été configurés.

1. **Services Linux (Debian 12) :**

◦ **Supervision :** Le déploiement de **Zabbix** sur la machine **Debian-Zabbix** (IP 10.10.40.10) permet la **supervision des hôtes** et la présentation des données via des **tableaux de bord**.

◦ **Automatisation :** La VM **Debian-Ansible** (IP 10.10.30.10) est dédiée à l'automatisation, avec la création de l'**inventaire** et des **playbooks** pour les sauvegardes et les déploiements. Des **scripts d'automatisation** sont également fournis, comme l'exemple en bash pour la sauvegarde des fichiers de configuration de Zabbix.

2. **Tests et Validation :** Le bon fonctionnement du système est prouvé par les **résultats des tests** effectués. La validation inclut les tests de **Supervision** (vérification via **ping, SNMP, remontées Zabbix**), les tests de **Sécurité** (tests d'accès inter-VLAN et l'efficacité du **pare-feu pfSense**), et la preuve de l'**exécution réussie des playbooks Ansible**. Enfin, des **captures** d'écran des tableaux de bord Grafana et des consoles AD et pfSense documentent la validation.

GNS3. La seconde partie, concerne la supervision du réseau de Cevital. Les différentes configurations sont faites sur une machine virtuelle VMware utilisant le système d'exploitation Linux

# V. Analyse et Justification des Choix Technologiques

## 1) Comprendre le rôle de Pfsense

**Pare-feu et Routeur : pfSense** Le choix s'est porté sur pfSense en raison de sa maturité et de son modèle open-source. Sa réputation éprouvée dans les PME, son écosystème de paquets additionnels (tels que Suricata pour l'IDS/IPS ou HAProxy pour la répartition de charge) et sa communauté active en font une solution pérenne et évolutive sans coût de licence. Il offre un ensemble de fonctionnalités complet, couvrant le routage inter-VLAN, le filtrage stateful et les capacités VPN, répondant parfaitement aux exigences de sécurité.

## 2) Comprendre le rôle de Windows Server 2022

**Services d'Annuaire et Réseau : Windows Server 2022** Pour la gestion centralisée des identités, Windows Server 2022 a été retenu. L'écosystème Active Directory (AD) offre une granularité de contrôle inégalée via les GPO (Group Policy Objects), permettant de forcer des politiques de mots de passe complexes, de restreindre l'exécution de logiciels et de mapper des lecteurs réseau de manière centralisée, ce qui est indispensable pour gérer un parc de

30 collaborateurs de manière sécurisée et efficace. L'intégration native des services DNS et DHCP garantit une administration simplifiée et une fiabilité maximale.

### 3) Comprendre le rôle de Zabbix

**Supervision** : Zabbix a été choisi pour sa puissance et sa flexibilité. Zabbix est un outil de collecte de métriques extrêmement puissant, capable de superviser une vaste gamme d'équipements. Il est peux être couplé à Grafana, une plateforme de visualisation de premier plan qui permet de créer des tableaux de bord dynamiques et hautement personnalisables. Cette combinaison open-source offre une solution de supervision proactive complète sans coût de licence.

### 4) Comprendre le rôle de Ansible

**Automatisation : Ansible** Ansible a été sélectionné pour sa simplicité d'approche et sa puissance. Son architecture agentless, qui s'appuie sur le protocole SSH natif pour Linux et WinRM pour Windows, élimine le besoin de déployer et maintenir un client sur chaque serveur. Cela réduit la charge administrative, diminue la surface d'attaque de l'infrastructure et simplifie considérablement l'intégration de nouvelles machines dans le périmètre d'automatisation. Ses playbooks en YAML sont idéaux pour automatiser la configuration et les sauvegardes.

Ces choix technologiques constituent le socle sur lequel repose l'architecture globale de la solution.

Pour répondre à ces besoins, les exigences suivantes ont été définies

## 5) Besoins fonctionnels

| Composant | Choix technique | Raisons principales |
|---|---|---|
| Pare-feu | pfSense | Open source, robuste, VPN, ACL, très utilisé en PME |
| Supervision | Zabbix + Grafana | Supervision + visuels |
| Automatisation | Ansible | Sans agent, simple, reproductible |
| Virtualisation | VirtualBox / Proxmox | Gratuit, adapté aux TP et projets étudiants |
| Systèmes | Windows Server 2022 + Debian / Ubuntu | Mix réaliste (AD + Linux supervision) |

### 5.1 Avantages

- Solutions peu coûteuses / open source
- Sécurité : VLAN + pare-feu à états
- Évolutivité : ajout futur VoIP, portail captif
- Simplicité d'administration : interfaces web

### 5.2 *Périmètre du projet*

**Inclus**

- VLANs, routage inter-VLAN, ACL
- pfSense
- Windows Server 2022 (AD/DNS/DHCP)
- Supervision Zabbix
- Automatisation Ansible
- Documentation

**Exclus**

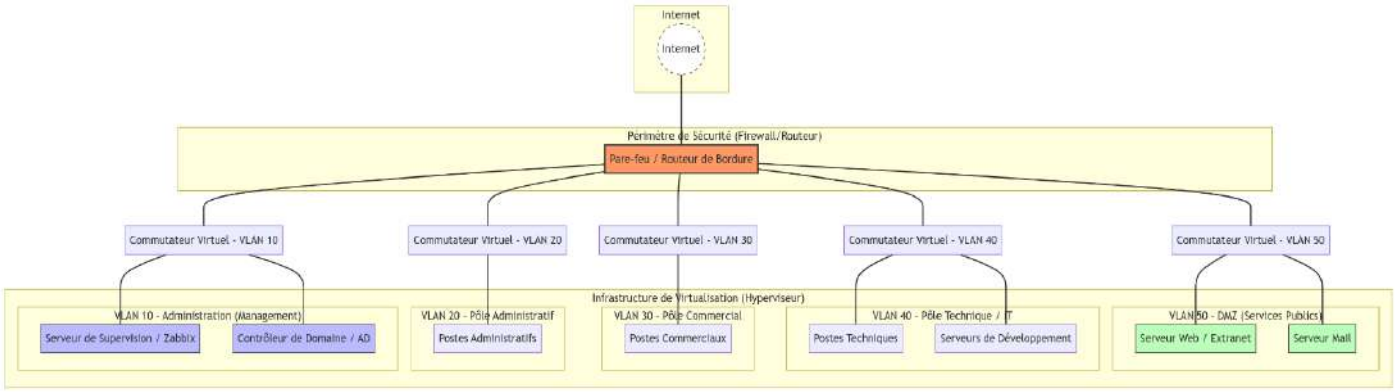
- Wi-Fi réel
- Applications métiers
- VoIP (si pas le temps)

## 6) Architecture Proposé

Cette section présente la conception d'ensemble de l'infrastructure, en détaillant l'architecture réseau logique qui assure la segmentation et la sécurité, ainsi que l'architecture système qui décrit le rôle et la configuration de chaque machine virtuelle.

### *6.1 Architecture Réseau et Plan d'Adressage*

### *6.2 Architecture cible (VLANs, pfSense, serveurs)*




**Présentation générale**

- L'architecture du réseau cible repose sur une **segmentation par VLANs**, un **pare-feu pfSense**, un **switch L3** pour le routage inter-VLAN, et des serveurs virtualisés pour les services d'annuaire, supervision et

automatisation.
Chaque VLAN correspond à un service de l'entreprise, afin de cloisonner les flux et d'améliorer la sécurité.

### *6.3 Plan d'adressage* et segmentation VLAN

Afin de garantir une segmentation efficace du réseau, plusieurs VLANs ont été définis en fonction des rôles et des usages. Chaque VLAN dispose d'un plan d'adressage IP distinct et d'une passerelle associée au pare-feu pfSense permettant un contrôle précis des flux inter-VLAN et une amélioration globale de la sécurité du réseau.

*Le tableau ci-dessous présente les VLANs mis en place dans l'infrastructure, leurs usages, leurs plages d'adressage IP, ainsi que les équipements associés à chaque VLAN.*

| VLAN | Nom du VLAN | Usage principal | Plage IP | Passerelle | Équipements / Hôtes associés |
|---|---|---|---|---|---|
| 40 | SERVEURS | Serveurs internes critiques | 192.168.1.0/24 | 192.168.1.1 | pfSense (LAN), Windows Server 2022 (AD/DNS/DHCP – 192.168.1.10), Serveur Debian (Zabbix/Ansible – 192.168.1.20) |
| 10 | ADMIN-DSI | Administration et bureautique DSI | 192.168.10.0/24 | 192.168.10.1 | Postes administrateurs, accès DSI |
| 20 | UTILISATEURS | Postes utilisateurs standards | 192.168.20.0/24 | 192.168.20.1 | Postes clients Windows 11 (ex. 192.168.20.10) |
| 30 | TECHNIQUE | Supervision et automatisation | 192.168.30.0/24 | 192.168.30.1 | Postes techniques, supervision avancée |
| 50 | INVITES | Accès Internet limité | 192.168.50.0/24 | 192.168.50.1 | Postes invités |
| 99 | MANAGEMENT | Gestion des équipements réseau | 192.168.99.0/24 | 192.168.99.1 | Accès management pfSense, switchs |
| 100 | TRANSIT (optionnel) | Lien de transit L3 ↔ pare-feu | 192.168.100.0/30 | 192.168.100.1 | Lien pfSense – switch de niveau 3 |

*Justificatif du choix d'adressage :*

Le but est d'isole les postes de travail et les serveurs critiques de l'administration, contenant des données sensible, avec des accès potentiellement plus larges.

*Rôles principaux :*

- **pfSense :** Pare-feu, NAT, routage vers Internet, VPN, ACL inter-VLAN.

- **Switch L3 Cisco :** SVI inter-VLAN, routage interne, ACL, trunk 802.1Q.
- **Switchs L2 :** Accès utilisateurs, trunks vers L3.
- **Windows Server 2022 :** Active Directory, DNS, DHCP.
- **Ubuntu Server :** Supervision (Zabbix + Grafana) et automatisation (Ansible).
- **Postes clients :** Windows 11 (Admin/Com) et Ubuntu Desktop (Technique).

## 7) Architecture Système Virtualisé

L'intégralité de l'infrastructure de services repose sur un ensemble de machines virtuelles (VM), ce qui offre une grande flexibilité, une isolation des services et une optimisation de l'utilisation des ressources matérielles. Chaque VM a un rôle clairement défini ci-dessus.

### 7.1 Caractéristiques des équipements informatiques

*Pour mettre en œuvre il faut :*

| **Élément** | **Exigence minimale** |
|---|---|
| pfSense | 2 CPU, 1 Go RAM, 8 Go disque |
| Windows Server 2022 | 2 CPU, 4 Go RAM, 40 Go disque |
| Debian Zabbix/Grafana | 2 CPU, 2 Go RAM |
| VM Ansible | 1 CPU, 1 Go RAM |
| Réseau virtuel | 6 VLANs minimum + 1 VLAN management |
| Disponibilité visée | **> 98 %** pour les services essentiels |
| Hyperviseur | VirtualBox / Proxmox / VMware Workstation 4CPU |

*Sécurité – Pare-feu, segmentation et VPN*

Pare-feu et segmentation

Le pare-feu pfSense assure :

- Le NAT vers Internet via l'interface WAN
- Le filtrage des flux inter-VLAN.
- La protection des serveurs internes.

Routage et ACL

Les VLANs sont routés au niveau du switch L3, avec des ACLs restreignant les communications inutiles pour par exemple l'interdiction du VLAN 50(client) vers les serveurs internes

Accès distant et sécurité

Le VPN distant sécurisé (OpenVPN).

- VPN OpenVPN pour les employés en télétravail.
- Authentification locale et journaux d'accès.

Sauvegarde automatique de la configuration pfSense sur un partage réseau sécurisé.

*Justicatif du choix :*

*Routage ACL : Le routage inter-VLAN est mis en place afin de permettre la communication contrôlée entre les différents segments du réseau. Les listes de contrôle d'accès (ACL) permettent de restreindre les flux non nécessaires entre les VLANs, en appliquant le principe du moindre privilège et en renforçant la sécurité globale de l'infrastructure.*

*VPN OpenVPN : Le VPN OpenVPN est utilisé pour permettre un accès distant sécurisé aux ressources internes de l'entreprise. Il assure la confidentialité et l'intégrité des communications grâce au chiffrement des données et à une authentification sécurisée des utilisateurs distants.*

*Pare-feu pfsense : Le pare-feu pfSense centralise la gestion de la sécurité réseau. Il assure le filtrage des flux entrants et sortants, le NAT vers Internet, la gestion des règles inter-VLAN et la mise en place du VPN. Son caractère open*

*source, sa fiabilité et sa flexibilité en font une solution adaptée aux besoins d'une PME.*

## VI. Supervision et automatisation

*Supervision – Zabbix & Grafana*

Le serveur **Zabbix** installé sur Ubuntu assure la surveillance de l'ensemble du réseau :

- Surveillance SNMP des équipements (pfSense, switchs, routeurs).
- Agents Zabbix sur les serveurs et postes clients (CPU, RAM, réseau).
- Notifications en cas d'incident (email ou dashboard).
- Intégration avec **Grafana** pour la visualisation graphique (tableaux dynamiques).

*Automatisation – Ansible*

L'outil **Ansible** permet d'automatiser :

- L'installation et configuration des agents Zabbix.
- Les sauvegardes pfSense et Windows Server.
- Les déploiements d'applications et mises à jour.

**Avantages clés :**

- Gain de temps.
- Réduction des erreurs humaines.
- Traçabilité via les playbooks YAML stockés sur GitHub.

## VII. Inventaire

1. Estimation du cout matériel et logiciels utilisés

Besoin Matériel

| **Catégorie** | **Désignation** | **Quantité** | **Prix unitaire (€)** | **Total (€)** |
|---|---|---|---|---|
| Routeur / Pare-feu | Netgate / Cisco ISR (ou pfSense VM) | 1 | 500 | 500 |
| Switch L3 manageable | Cisco Catalyst | 1 | 350 | 350 |
| Switchs L2 | Cisco Catalyst | 2 | 250 | 500 |
| Point d'accès Wi-Fi | Cisco AP | 1 | 150 | 150 |
| Serveur physique (virtualisation) | Dell/HP | 1 | 1200 | 1200 |
| Onduleur (UPS) | APC | 1 | 250 | 250 |
| Postes clients | PC Pro (Windows/Linux) | 3 | 600 | 1800 |
| Imprimante réseau | HP LaserJet | 1 | 200 | 200 |
| Téléphones IP (optionnel) | Cisco SPA | 2 | 100 | 200 |
| **Total matériel** | | | | **≈ 5 150 €** |

Besoin Logiciels

| **Logiciel** | **Rôle** | **Coût (€)** |
|---|---|---|
| pfSense / OPNsense | Pare-feu open-source | 0 |
| Zabbix / Grafana | Supervision open-source | 0 |
| Ansible | Automatisation | 0 |
| Windows Server 2022 | AD / DNS / DHCP | 900 |

| | | |
|---|---|---|
| Licences CAL (10 users) | Authentification | 350 |
| **Total logiciels** | | **≈ 1 250 €** |

## VIII. Méthodologie & étapes de réalisation

Méthode agile :

Le projet est conduit selon une **méthode séquentielle structurée** inspirée du cycle en V.
Chaque étape produit des livrables validés avant de passer à la suivante.

Explications du choix de méthode de travail :

**Cycle V :**

Concept : Une extension de la cascade, axée sur la vérification et la validation systématiques. Chaque phase de conception (branche gauche du V) a une phase de test correspondante (branche droite du V) pour s'assurer que les livrables respectent les spécifications.

Pourquoi le Cycle en V ?

• Réduction des risques : Les problèmes sont détectés plus tôt, là où ils sont moins coûteux à corriger.

• Qualité et Fiabilité : Idéal pour les systèmes critiques ou complexes où la sécurité et la conformité sont non négociables.

• Traçabilité : Chaque étape de test valide une étape de conception précise.

**Méthode de travail**

- Réunions hebdomadaires pour le suivi de Trello.
- Utilisation de **GitHub** pour la gestion de versions et le partage des fichiers.

- Répartition claire des rôles :

**Camila/Cécilia : Chef de projet** : coordination, suivi Gantt, GitHub.

**Cécilia BOUKAKA : Réseau & Sécurité** : pfSense, VLAN, VPN.

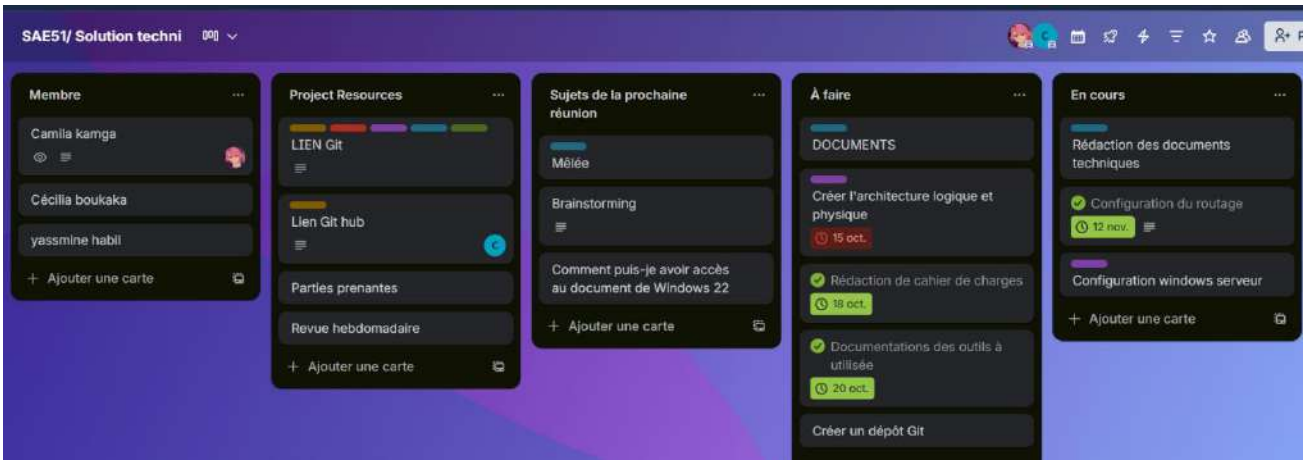
**Camila : Systèmes** : Windows Server (AD/DNS/DHCP).

**Cécilia : Supervision & Automatisation** : Zabbix, Ansible, scripts.

**Yassmine** : architecture réseaux Packet Tracer

- Validation à chaque jalon avec un compte rendu d'équipe.

Figure de Trello



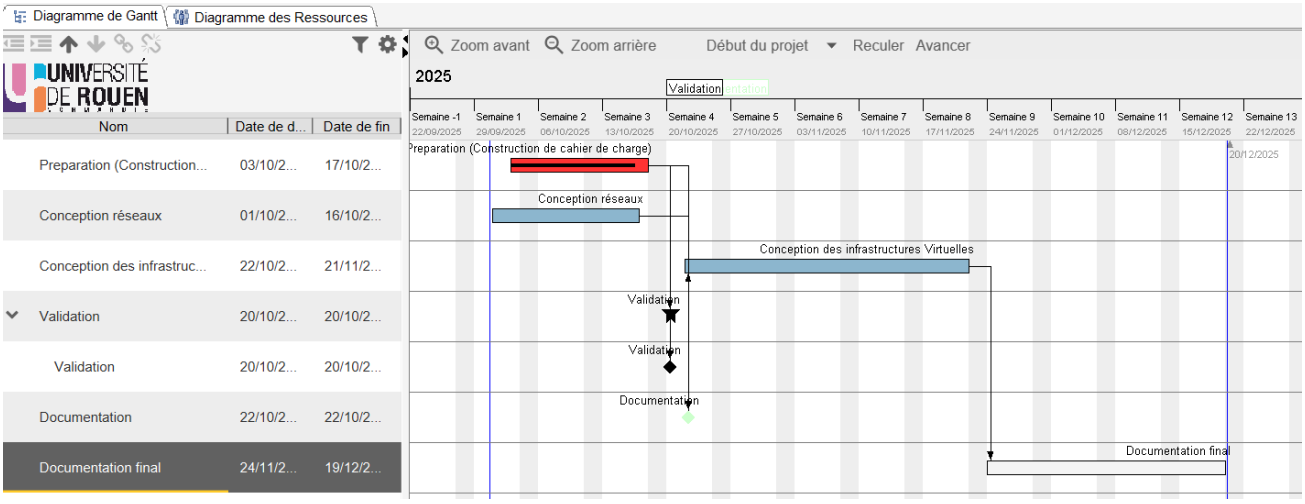

## IX. Planning

Gantt prévisionnel et théorique

*Planning prévisionnel* :

| ID | Tâche | Responsable | Phase | ébut (sem | Fin (sem.) | urée (sem | S1 | S2 | S3 | S4 | S5 | S6 | S7 | S8 | S9 | S10 | S11 | S12 | S13 | S14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Cadrage / Cahier des charges | Cécilia/Camila | Préparation | 1 | 2 | 2 | ■ | ■ | | | | | | | | | | | | |
| 2 | Conception réseau (VLAN, adressage) | Yassmine | Préparation | 2 | 3 | 2 | | ■ | ■ | | | | | | | | | | | |
| 3 | Mise en place virtualisation (VM) | Cécilia | Déploiement | 3 | 4 | 2 | | | ■ | ■ | | | | | | | | | | |
| 4 | Configuration pfSense / routage | Cécilia | Déploiement | 4 | 5 | 2 | | | | ■ | ■ | | | | | | | | | |
| 5 | AD / DNS / DHCP Windows | Camila | Déploiement | 5 | 6 | 2 | | | | | ■ | ■ | | | | | | | | |
| 6 | Supervision (Zabbix / Grafana) | Cécilia | Déploiement | 6 | 8 | 3 | | | | | | ■ | ■ | ■ | | | | | | |
| 7 | Automatisation Ansible | Cécilia | Déploiement | 7 | 9 | 3 | | | | | | | ■ | ■ | ■ | | | | | |
| 8 | Tests et validation | Cécilia/Camila | Validation | 9 | 11 | 3 | | | | | | | | | ■ | ■ | ■ | | | |
| 9 | Documentation (technique + utilisateur) | Camila | Validation | 10 | 12 | 3 | | | | | | | | | | ■ | ■ | ■ | | |
| 10 | Préparation soutenance | Cécilia/Camila/Yassm | Validation | 12 | 14 | 3 | | | | | | | | | | | | ■ | ■ | ■ |

*Planning théorique :*




## X. Budget prévisionnel et clarification PME / prototype

- **Budget PME (déploiement réel)**

  Matériel pro, maintenance, M.O. → **≈ 17 900 € TTC**

- **Budget prototype étudiant (version virtualisée)**

  Matériel réduit + solutions open source → **≈ 3 430 €**

*Inventaire des équipements informatiques pour le PME*

| **Matériel** | **Quantité** | **Coût unitaire (€)** | **Total (€)** |
|---|---|---|---|
| Routeur pfSense / Netgate | 1 | 500 | 500 |
| Switch L3 manageable | 1 | 350 | 350 |
| Switchs L2 (24 ports) | 2 | 250 | 500 |
| Point d'accès Wi-Fi | 1 | 150 | 150 |
| Serveur physique | 1 | 1200 | 1200 |
| Onduleur (UPS) | 1 | 250 | 250 |
| Postes clients | 3 | 600 | 1800 |
| Imprimante réseau | 1 | 200 | 200 |
| Téléphones IP (optionnel) | 2 | 100 | 200 |

| | | | |
|---|---|---|---|
| **Total matériel** | | | **≈ 5 150 €** |

Logiciels

| **Logiciel** | **Licence** | **Coût (€)** |
|---|---|---|
| pfSense / OPNsense | Open-source | 0 |
| Zabbix / Grafana / Ansible | Open-source | 0 |
| Windows Server 2022 | Licence PME | 900 |
| CALs (10 utilisateurs) | Licence Microsoft | 350 |
| **Total logiciels** | | **≈ 1 250 €** |

Main œuvre

| **Poste** | **Jours** | **Coût journalier (€)** | **Total (€)** |
|---|---|---|---|
| Conception & architecture | 5 | 500 | 2 500 |
| Installation & configuration | 10 | 500 | 5 000 |
| Documentation & formation | 3 | 500 | 1 500 |
| **Total main-d'œuvre** | | | **≈ 9 000 €** |

Maintenance annuelle

| **Service** | **Coût (€)** |
|---|---|
| Contrat de maintenance | 1 500 |
| Mises à jour et supervision | 1 000 |
| **Total maintenance** | **≈ 2 500 €** |

**Budget global estimé :**

- Matériel : 5 150 €
- Logiciels : 1 250 €
- Main-d'œuvre : 9 000 €

- Maintenance : 2 500 €
  **Total général : ≈ 17 900 € TTC**

***À noter que*** *Le budget global de* ***17 900 €*** *correspond à un déploiement réel en PME (matériel physique, licences Windows, main-d'œuvre d'intégration et maintenance annuelle).*
*Dans le cadre du projet pédagogique SAE 51, une* ***version virtualisée*** *de la solution a été réalisée pour un coût estimé à* ***3 430 €*** *correspondant aux ressources nécessaires au prototype étudiant (serveur de virtualisation, temps concencré).*

## XI. Difficultés anticipées & solutions envisagées

### XI.1 Analyse des risques

| **Risque** | **Impact** | **Probabilité** | **Prévention / Atténuation** |
|---|---|---|---|
| Panne pfSense | Élevé | Moyenne | Sauvegarde auto + export config + snapshot VM |
| Perte d'une VM | Élevé | Faible | Snapshots hebdo + export OVA |
| Mauvaise synchro AD/DNS | Moyen | Moyenne | Tests préalables en labo + vérification DHCP |
| Communication inter-VLAN KO | Moyen | Moyenne | Revue des ACL / règles pfSense / routes statiques |
| Mauvaise communication d'équipe | Moyen | Moyenne | Réunions hebdo + suivi GitHub + Gantt partagé |
| Retard sur la documentation | Moyen | Moyenne | Modèle commun + remplissage au fil du projet |

### XI.2 Risque critique

| Difficulté anticipée | Type | Solution envisagée |
|---|---|---|
| Compatibilité VLAN sous VirtualBox | Technique | Passage à Proxmox avec pont réseau |
| Rétention d'informations entre membres | Organisationnelle | Utilisation de GitHub et Trello |
| Retard dans le Gantt | Planification | Réévaluation hebdomadaire du planning |
| Supervision trop lourde sur petites VM | Technique | Allègement du polling et optimisation des intervalles |
| Communication inter-VLAN bloquée | Configuration | Vérification ACL / pfSense / routes statiques |

## XII. Conclusion et perspectives

En conclusion, ce projet nous a permis de déployer avec succès une infrastructure réseau et système virtualisée pour NetSecure. La solution mise en place répond pleinement aux exigences du cahier des charges en fournissant un environnement sécurisé, fiable et efficace grâce à la supervision proactive et à l'automatisation.

Cette architecture robuste et moderne qui fournit à l'entreprise NetSecure une fondation technologique sécurisée et évolutive, lui permettant de se concentrer sur son cœur de métier en toute sérénité.

Perspectives d'Évolution L'infrastructure actuelle constitue une base solide qui peut être enrichie par plusieurs améliorations futures :

• Mise en place d'un accès distant sécurisé pour les collaborateurs nomades ou en télétravail, via la configuration d'un serveur VPN (type OpenVPN ou IPsec) sur le pare-feu pfSense.

• Extension de l'automatisation avec Ansible pour inclure le déploiement complet ("provisioning") de nouvelles machines virtuelles depuis des modèles prédéfinis.

• Renforcement de la supervision avec Zabbix en créant des scénarios de surveillance plus complexes (ex: tests applicatifs) et en affinant les seuils d'alerte pour une détection encore plus précoce des incidents.

• Mise en place d'une solution de sauvegarde centralisée plus robuste, incluant la sauvegarde complète des machines virtuelles et des bases de données, avec une politique de rétention et des tests de restauration réguliers.

En outre ce projet nous a permis de mobiliser des compétences en réseaux, systèmes, sécurité, virtualisation et supervision, tout en valorisant le **travail collaboratif** et la **documentation professionnelle**.
Les solutions choisies sont **open-source, fiables et évolutives**, garantissant une infrastructure durable et économique.

## Remerciements

Merci à mes collaborateurs du projet **SAE 51** pour leur implication, leur rigueur et leur esprit d'équipe.

Ce projet fut une expérience riche, combinant compétences techniques, organisation et collaboration, préparant ainsi aux réalités du monde professionnel.

## XIII. Annexes

Des captures d'écran illustrant les configurations clés (interface de pfSense, console Active Directory, tableaux de bord Grafana).

• Les fichiers de configuration complets des services principaux.

• Les playbooks Ansible développés pour l'automatisation.

• Une documentation utilisateur détaillée pour l'administration quotidienne des services.

## XIV. Glossaires

ACL Access Control List

VM Machines Virtuelles

AD DS Active Directory et Domain Services

ARPANET Advanced Research Projects Agency NETwork

BDD Base De Donnée

CPU Central Processing Unit

DHCP Dynamic Host Configuration Protocol

DMAP Distributed Management Application Processus

DNS Domain Name System

DSI Direction des Systèmes d'Information

GNS3 Graphical Network Simulator-3

GNU General Public Licence

HSE Hygiène, Sécurité et Environnement

HTTP HyperText Transfer Protocol

ICMP Internet Control Message Protocol

IPMI Intelligent Platform Management Interface

IR Infra Rouge

ISO Organisation internationale de normalisation

JMX Java Management Extensions

LAN Local Area Network

LDAP Lightweight Directory Access Protocol

MAN Metropolitain Area Network

MIB Management Information Base

MSA Managed System and Agents

NMS Network Management Station

OID Object IDentifier

OS Operating System

OSI Open System Interconnexion

P2P Peer to Peer

PAN Personale Area Network

PHP Hypertext Preprocessor

RAM Random Access Memory

RMON Remote Network Monitoring

RRD Round-Robin Database

SIA Signs Partnership Agreement

STP Spanning Tree Protocol

SMFA Specific Management Function Area

SMS Short Message Service

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

SQL Structured Query Language Server

SSH Secure Shell

SSMTP Secure Simple Mail Transfer Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TIC Technologies d'Information et de Communication

UDP User Datagram Protocol

USB Universal Serial Bus

USM User-based Security Model

VLAN Virtual Local Area Network

VTP Vlan Trunking Protocol

WIFI WIreless FIdelity

WMI Windows Management Instrumentation

WAN Wide Area Network