**École Supérieure Privée d'Ingénierie et de Technologies**

# Conception et déploiement d'une infrastructure réseau multi-sites sécurisée

Backbone OSPF, VPN IPsec, NAT, DHCP et ACL

**Réalisé par :**

Aya Fdhila
Soumaya Dridi
Malek Melki
Ramzi Ben Hmida
Ahmed Ben Chouikha
Akrem Zaied

**Encadrantes :**

Mme Imen Dakhli
Mme Radhia Werghemmi

# Table des matières

# Table des figures

# Introduction

Dans le cadre du projet d'intégration, il est demandé de concevoir et déployer une infrastructure réseau complète simulée sous GNS3, représentant le réseau d'une entreprise structurée en plusieurs départements (Web, IT / Supervision, partage de fichiers, base de données), interconnectés via un backbone.

L'objectif est de mettre en pratique les notions vues en cours : plan d'adressage, routage dynamique, accès Internet via NAT, tunnels VPN, sécurisation des flux à l'aide d'ACL, ainsi que la mise en place de services critiques (DHCP, services applicatifs, supervision).

Ce rapport présente dans un premier temps le contexte et le cahier des charges, puis l'architecture globale retenue, le plan d'adressage et la configuration du routage. Les services réseau déployés et les mécanismes de sécurité (NAT, VPN, ACL) sont ensuite détaillés. Enfin, une section est consacrée aux tests de validation et à la supervision, avant de conclure sur les apports et les perspectives d'amélioration.

# Chapitre 1

# Contexte et cahier des charges

## 1.1 Contexte du projet

Le projet consiste à concevoir une infrastructure réseau multi-sites en utilisant l'outil de simulation GNS3. L'entreprise est répartie en plusieurs départements logiques (Site Web, Site IT / Supervision, autres services), reliés par un backbone central.

L'infrastructure doit permettre :

— la communication entre les différents départements,
— l'accès à des services tels que le Web, la base de données, le partage de fichiers et la supervision,
— la sécurisation des communications inter-sites,
— un accès Internet simulé pour les clients internes.

## 1.2 Objectifs généraux

Les objectifs principaux sont les suivants :

— Concevoir un plan d'adressage cohérent et évolutif pour l'ensemble des sites.
— Mettre en place un backbone assurant l'interconnexion des départements.
— Déployer un routage dynamique reposant sur OSPF.
— Fournir un accès Internet aux clients internes via du NAT.
— Sécuriser les communications inter-sites à l'aide d'un VPN IPsec.
— Déployer les services nécessaires : DHCP, Web, base de données, partage, supervision.
— Utiliser des ACL pour contrôler les flux entre les différentes zones réseau.

## 1.3 Exigences du cahier des charges

Le cahier des charges impose notamment :

— la création d'un backbone avec routage dynamique (OSPF) entre les routeurs,
— l'utilisation d'adresses privées avec un découpage en sous-réseaux adapté au nombre de clients de chaque département,
— l'accès Internet des clients internes via un mécanisme de NAT (PAT),
— la mise en place de VPN site-à-site pour sécuriser les échanges entre sites distants,
— la mise en place d'ACL pour autoriser les flux applicatifs nécessaires (Web, base de données, partage) et bloquer les autres,

— la présence d'un serveur de supervision pour surveiller l'état des équipements.

# Chapitre 2

# Architecture globale de l'infrastructure

## 2.1 Vue d'ensemble

L'infrastructure repose sur un backbone constitué de plusieurs routeurs (R-BACKBONE-1 à R-BACKBONE-5), interconnectés via des liens point à point configurés en /30. Chaque site (Site Web, Site IT / Supervision, etc.) est relié au backbone via un routeur de zone (RZ-1, RZ-2, ...).

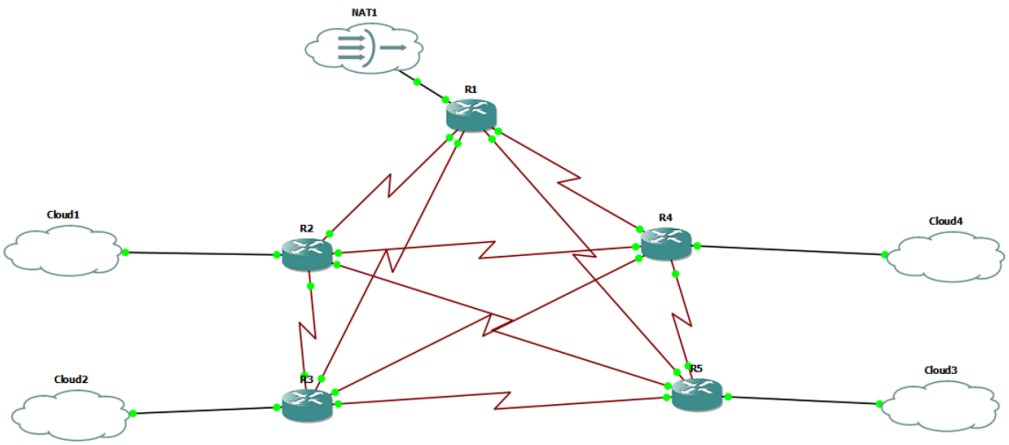


FIGURE 2.1 – Topologie globale de l'infrastructure réseau

Comme illustré dans la figure 2.1, l'architecture met en évidence une séparation claire entre le backbone, les sites distants et les réseaux locaux de chaque département.

## 2.2 Rôle des différentes zones

### 2.2.1 Backbone

Le backbone joue le rôle de cœur de réseau. Il assure le transit du trafic entre les différents sites distants. Les liens backbone sont configurés en /30 afin d'optimiser l'utilisation des adresses IP et de représenter des liaisons WAN point à point.

### 2.2.2 Site Web (RZ-1)

Le site Web comprend :
— un LAN utilisateurs (172.24.0.0/18),
— un routeur de zone RZ-1 jouant le rôle de passerelle,
— un serveur Web.
RZ-1 assure également les fonctions de DHCP, de NAT et la terminaison des tunnels VPN vers les autres sites.

### 2.2.3 Site IT / Supervision (RZ-2)

Le site IT / Supervision comprend :
— un LAN IT (172.24.64.0/21),
— un routeur de zone RZ-2,
— un serveur de supervision (Prometheus / Grafana).
Ce site est dédié à la gestion, au contrôle et à la supervision de l'infrastructure réseau.

### 2.2.4 Site de partage et base de données

Ce site héberge les serveurs de partage de fichiers et de base de données. L'accès à ces ressources est strictement contrôlé par des ACL afin de limiter les flux aux seuls services autorisés.

## 2.3 Topologies détaillées des sites

### 2.3.1 Topologie du site Web (RZ-1)

La figure 2.2 présente la topologie interne du site Web. Le routeur RZ-1 assure l'interconnexion entre le LAN utilisateurs, le backbone et les autres sites via des tunnels VPN.

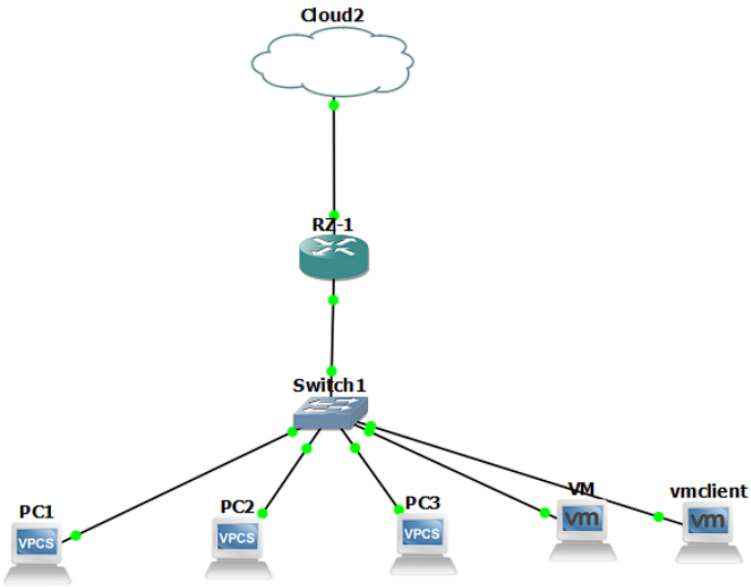


FIGURE 2.2 – Topologie du site Web (RZ-1)

### 2.3.2 Topologie du site IT / Supervision (RZ-2)

La figure 2.3 illustre l'architecture du site IT. Le serveur de supervision permet de surveiller l'état des équipements réseau et des services critiques.

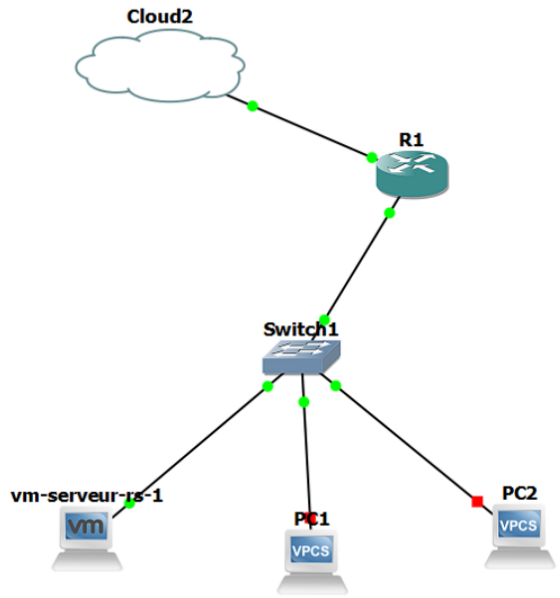


FIGURE 2.3 – Topologie du site IT / Supervision (RZ-2)

### 2.3.3 Topologie du site de partage et base de données

La figure 2.4 montre le site dédié au partage de fichiers et aux bases de données. L'accès à ces serveurs est filtré afin de garantir la sécurité des données.

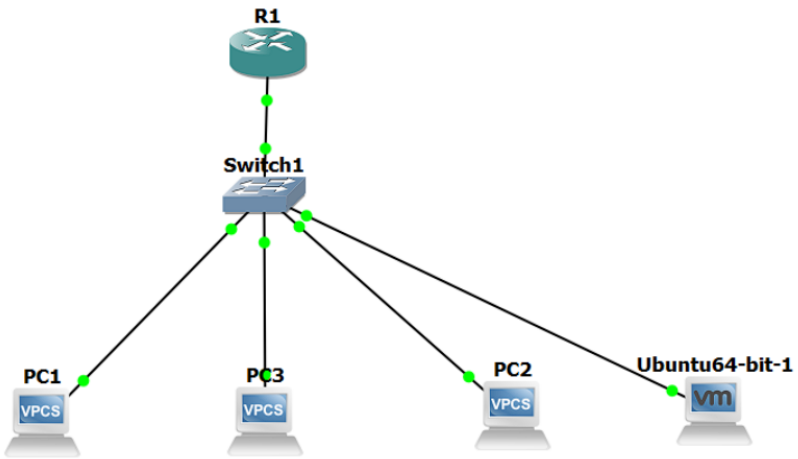


FIGURE 2.4 – Topologie du site de partage et base de données

### 2.3.4 Plan d'adressage du backbone

Le backbone est interconnecté à l'aide de liaisons WAN point à point, chacune configurée avec un masque /30 afin d'optimiser l'utilisation des adresses IP. Le tableau **??** présente le plan d'adressage détaillé des liaisons entre les routeurs du backbone.

TABLE 2.1 – Plan d'adressage du backbone – Liaisons avec R-BACKBONE-1

| Lien | Réseau (/30) | Interface R1 | IP R1 | IP distant |
|---|---|---|---|---|
| R1–R2 | 138.100.1.0/30 | S0/0 | 138.100.1.1 | 138.100.1.2 |
| R1–R3 | 138.100.1.4/30 | S0/1 | 138.100.1.5 | 138.100.1.6 |
| R1–R4 | 138.100.1.8/30 | S0/2 | 138.100.1.9 | 138.100.1.10 |
| R1–R5 | 138.100.1.12/30 | S2/0 | 138.100.1.13 | 138.100.1.14 |

TABLE 2.2 – Plan d'adressage du backbone – Autres liaisons inter-routeurs

| Lien | Réseau (/30) | Routeur A | IP A | Routeur B | IP B |
|---|---|---|---|---|---|
| R2–R3 | 138.100.1.16/30 | R2 | 138.100.1.17 | R3 | 138.100.1.18 |
| R2–R4 | 138.100.1.20/30 | R2 | 138.100.1.21 | R4 | 138.100.1.22 |
| R2–R5 | 138.100.1.24/30 | R2 | 138.100.1.25 | R5 | 138.100.1.26 |
| R3–R4 | 138.100.1.28/30 | R3 | 138.100.1.29 | R4 | 138.100.1.30 |
| R3–R5 | 138.100.1.32/30 | R3 | 138.100.1.33 | R5 | 138.100.1.34 |
| R4–R5 | 138.100.1.36/30 | R4 | 138.100.1.37 | R5 | 138.100.1.38 |

## 2.4 Connexion aux services externes

Une partie du backbone joue le rôle de passerelle vers « Internet ». Les routeurs de zone réalisent un NAT de type PAT afin de permettre aux clients internes d'accéder à l'extérieur tout en conservant un plan d'adressage privé.

# Chapitre 3

# Plan d'adressage et routage

## 3.1 Plan d'adressage IP

Le plan d'adressage s'appuie sur le bloc privé 172.24.0.0/16, découpé en plusieurs sous-réseaux adaptés aux besoins de chaque site. Les liaisons point à point du backbone et des liens sites–backbone utilisent des réseaux distincts dans la plage 100.10.10.0/30 et 100.10.20.0/30.

Table 3.1 – Résumé du plan d'adressage

| Zone | Réseau | Remarques |
|---|---|---|
| LAN Site Web (RZ-1) | 172.24.0.0/18 | Passerelle : 172.24.0.1 |
| LAN Site IT (RZ-2) | 172.24.64.0/21 | Passerelle : 172.24.64.1 |
| Liens backbone | 100.10.10.x/30 | Liens entre R-BACKBONE |
| Liens sites–backbone | 100.10.20.x/30 | RZ-1/RZ-2 vers backbone |
| Tunnels GRE | 10.255.x.0/30 | Tunnels entre sites |

## 3.2 Justification de l'utilisation de /30

Les sous-réseaux en /30 sont utilisés sur les liens point à point entre routeurs (backbone et liaisons sites–backbone). Un /30 fournit deux adresses IP utilisables, ce qui est parfaitement adapté à une liaison entre deux équipements uniquement, tout en évitant le gaspillage d'adresses.

## 3.3 Routage dynamique OSPF

Le protocole OSPF est configuré sur l'ensemble des routeurs. Un exemple de configuration sur RZ-1 est donné ci-dessous :

Listing 3.1 – Extrait de configuration OSPF sur RZ-1

```
router ospf 1
 router-id 10.1.1.1
 network 172.24.0.0 0.0.63.255 area 0
 network 10.255.1.0 0.0.0.3 area 0
 network 10.255.2.0 0.0.0.3 area 0
 network 10.255.3.0 0.0.0.3 area 0
```

Les commandes de vérification suivantes ont été utilisées :
— `show ip ospf neighbor` pour vérifier les adjacences,
— `show ip route` pour contrôler la présence des routes OSPF,
— `ping` et `traceroute` pour valider la connectivité.

### 3.3.1 Validation des interfaces OSPF du backbone

Afin de confirmer le bon fonctionnement du routage dynamique au sein du backbone, la commande `show ip ospf interface brief` a été exécutée sur tous les routeurs.

```
R-BACKBONE-1# show ip ospf interface brief
Interface    PID   Area    IP Address/Mask    Cost  State  Nbrs F/C
Se2/0        1     0       138.100.1.13/30    64    P2P    0/0
Se0/2        1     0       138.100.1.9/30     64    P2P    1/1
Se0/1        1     0       138.100.1.5/30     64    P2P    1/1
Se0/0        1     0       138.100.1.1/30     64    P2P    1/1
```

FIGURE 3.1 – État des interfaces OSPF sur R-BACKBONE-1

```
R-BACKBONE-2# show ip ospf interface brief
Interface    PID   Area    IP Address/Mask    Cost  State  Nbrs F/C
Fa0/0        1     0       138.100.2.1/30      10    DR     0/0
Se2/0        1     0       138.100.1.25/30    64    P2P    1/1
Se0/2        1     0       138.100.1.21/30    64    P2P    1/1
Se0/1        1     0       138.100.1.17/30    64    P2P    1/1
Se0/0        1     0       138.100.1.2/30     64    P2P    1/1
```

FIGURE 3.2 – État des interfaces OSPF sur R-BACKBONE-2

```
R-BACKBONE-3# show ip ospf interface brief
Interface    PID   Area    IP Address/Mask    Cost  State  Nbrs F/C
Fa0/0        1     0       138.100.2.5/30      10    DR     0/0
Se2/0        1     0       138.100.1.33/30    64    P2P    1/1
Se0/2        1     0       138.100.1.29/30    64    P2P    1/1
Se0/1        1     0       138.100.1.18/30    64    P2P    1/1
Se0/0        1     0       138.100.1.6/30     64    P2P    1/1
```

FIGURE 3.3 – État des interfaces OSPF sur R-BACKBONE-3

```
R-BACKBONE-4# show ip ospf interface brief
Interface    PID   Area    IP Address/Mask    Cost  State  Nbrs F/C
Fa0/0        1     0       138.100.2.9/30      10    DR     0/0
Se2/0        1     0       138.100.1.37/30     64    P2P    1/1
Se0/2        1     0       138.100.1.30/30     64    P2P    1/1
Se0/1        1     0       138.100.1.22/30     64    P2P    1/1
Se0/0        1     0       138.100.1.10/30     64    P2P    1/1
```

FIGURE 3.4 – État des interfaces OSPF sur R-BACKBONE-4

```
R-BACKBONE-5# show ip ospf interface brief
Interface    PID   Area    IP Address/Mask    Cost  State  Nbrs F/C
Fa0/0        1     0       138.100.2.13/30     10    DR     0/0
Se2/0        1     0       138.100.1.38/30     64    P2P    1/1
Se0/2        1     0       138.100.1.34/30     64    P2P    1/1
Se0/1        1     0       138.100.1.26/30     64    P2P    1/1
Se0/0        1     0       138.100.1.14/30     64    DOWN   0/0
```

FIGURE 3.5 – État des interfaces OSPF sur R-BACKBONE-5 (une interface DOWN)

**Analyse :** L'ensemble des interfaces participe à l'aire 0, les liens WAN sont en mode point-à-point et les voisinages OSPF sont établis (Nbrs 1/1), ce qui confirme la convergence du protocole et la continuité du routage. L'interface DOWN sur R-BACKBONE-5 correspond à une liaison non utilisée dans la topologie.

## 3.4 Routes par défaut

Les routeurs de zone disposent d'une route par défaut vers le backbone. Par exemple, sur RZ-2 :

Listing 3.2 – Route par défaut sur RZ-2

```
ip route 0.0.0.0 0.0.0.0 100.10.20.5
```

La présence de la route par défaut est vérifiée via `show ip route`, où elle apparaît comme une route statique marquée d'une étoile.

chapterServices réseau et sécurité

## 3.5 Service DHCP

Sur les routeurs de zone, le service DHCP est utilisé pour distribuer automatiquement les adresses IP aux clients des LANs.

### 3.5.1 DHCP sur le site Web (RZ-1)

Listing 3.3 – Pool DHCP pour le LAN du site Web

```
ip dhcp excluded-address 172.24.0.1 172.24.0.20
```

```
ip dhcp pool RZ1-LAN
 network 172.24.0.0 255.255.192.0
 default-router 172.24.0.1
 dns-server 172.27.1.10
 domain-name rz1.local
```

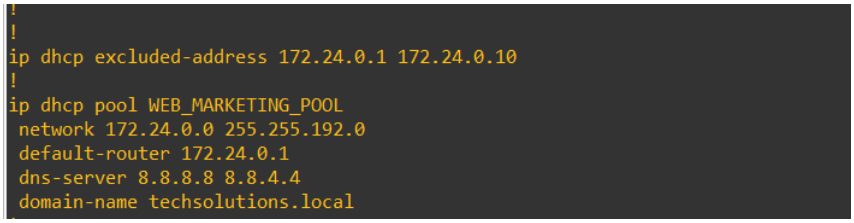


FIGURE 3.6 – Capture d'écran du service DHCP sur RZ-1

### 3.5.2 DHCP sur le site IT (RZ-2)

Listing 3.4 – Pool DHCP pour le LAN du site IT

```
ip dhcp excluded-address 172.24.64.1 172.24.64.20
ip dhcp pool SUPERVISION_IT_POOL
 network 172.24.64.0 255.255.248.0
 default-router 172.24.64.1
 dns-server 8.8.8.8
 domain-name rz2.local
```

FIGURE 3.7 – Capture d'écran du service DHCP sur RZ-2

## 3.6 NAT et accès Internet

Le NAT de type PAT (overload) permet aux clients internes d'accéder à Internet en partageant l'adresse IP de sortie du routeur.

Listing 3.5 – Exemple de configuration NAT sur RZ-1

```
access-list 101 deny   ip 172.24.0.0 0.0.63.255 172.24.64.0
   0.0.7.255
access-list 101 deny   ip 172.24.0.0 0.0.63.255 172.24.72.0
   0.0.1.255
access-list 101 deny   ip 172.24.0.0 0.0.63.255 172.24.74.0
   0.0.0.255
access-list 101 permit ip 172.24.0.0 0.0.63.255 any

interface FastEthernet0/0
 ip nat inside
!
interface FastEthernet0/1
 ip nat outside
!
```

```
ip nat inside source list 101 interface FastEthernet0/1 overload
```

```
RZ-1#show running-config | section ip nat
 ip nat inside
 ip nat outside
ip nat inside source list 101 interface FastEthernet0/1 overload
RZ-1#
```

FIGURE 3.8 – Capture d'écran de la configuration NAT sur RZ-1

## 3.7 VPN IPsec et tunnels GRE

Les communications inter-sites sont sécurisées à l'aide d'un VPN IPsec associé à des tunnels GRE.

### 3.7.1 Tunnel GRE sur RZ-1

Listing 3.6 – Exemple de configuration du tunnel GRE sur RZ-1

```
interface Tunnel12
 description VPN Tunnel to RZ-2
 ip address 10.255.1.1 255.255.255.252
 tunnel source FastEthernet0/1
 tunnel destination 100.10.20.6
```

### 3.7.2 Configuration IPsec sur RZ-1

Listing 3.7 – Exemple de configuration IPsec sur RZ-1

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14

crypto isakmp key VPN_RZ1_TO_RZ2_Secret address 100.10.20.6

crypto ipsec transform-set STRONG_SET esp-aes 256 esp-sha256-hmac

ip access-list extended VPN_TO_RZ2
 permit gre host 100.10.20.2 host 100.10.20.6

crypto map VPN_MAP 10 ipsec-isakmp
 set peer 100.10.20.6
 set transform-set STRONG_SET
 match address VPN_TO_RZ2

interface FastEthernet0/1
 crypto map VPN_MAP
```

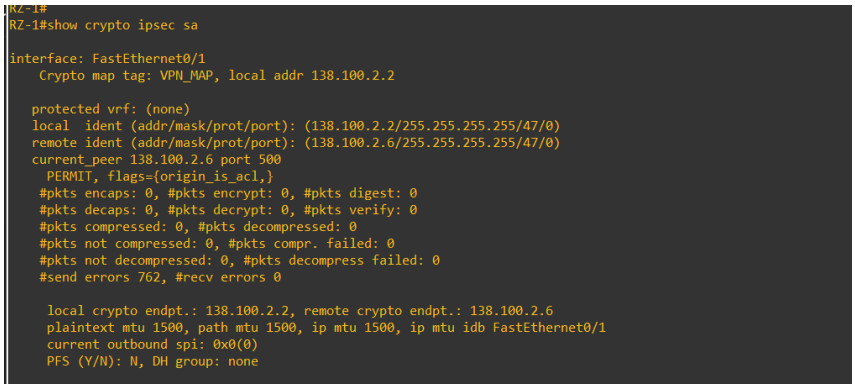


FIGURE 3.9 – Capture d'écran de la configuration IPsec sur RZ-1

## 3.8 ACL de sécurité

En complément de l'ACL utilisée pour le NAT, des ACL de sécurité peuvent être appliquées sur les interfaces pour contrôler les flux entre zones.

```
!
!
access-list 101 deny   ip 172.24.0.0 0.0.63.255 172.24.64.0 0.0.7.255
access-list 101 deny   ip 172.24.0.0 0.0.63.255 172.24.72.0 0.0.1.255
access-list 101 deny   ip 172.24.0.0 0.0.63.255 172.24.74.0 0.0.0.255
access-list 101 permit ip 172.24.0.0 0.0.63.255 any
!
```

FIGURE 3.10 – Capture d'écran de l'ACL

## 3.9 Services spécifiques et captures d'écran

Pour documenter la disponibilité et la configuration des services réseau, des captures d'écran ont été prévues pour chaque service :

— **Monitoring :** État et alertes du réseau et des routeurs.

Nous avons déployé une solution de supervision complète basée sur Prometheus et Grafana pour surveiller l'état du réseau et des équipements. Cette solution comprend :

1. **Serveur de supervision :** Installé sur une machine virtuelle avec l'adresse IP 172.24.64.10
2. **Clients Node Exporter :** Déployés sur les machines à superviser pour collecter les métriques système
3. **Règles d'alerte :** Configurées pour détecter automatiquement les problèmes

**Configuration réseau du serveur :**

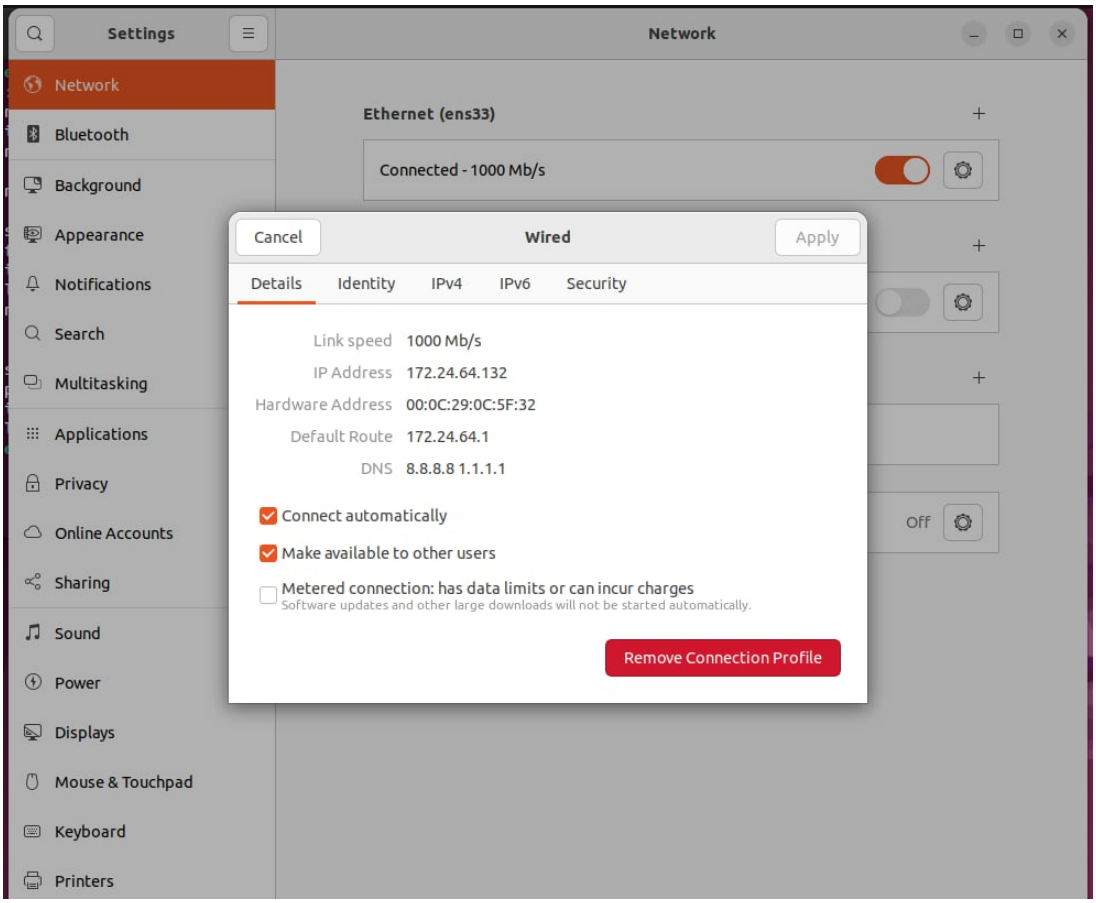


FIGURE 3.11 – Configuration réseau de la machine serveur (172.24.64.132)

**Installation automatisée du serveur :**

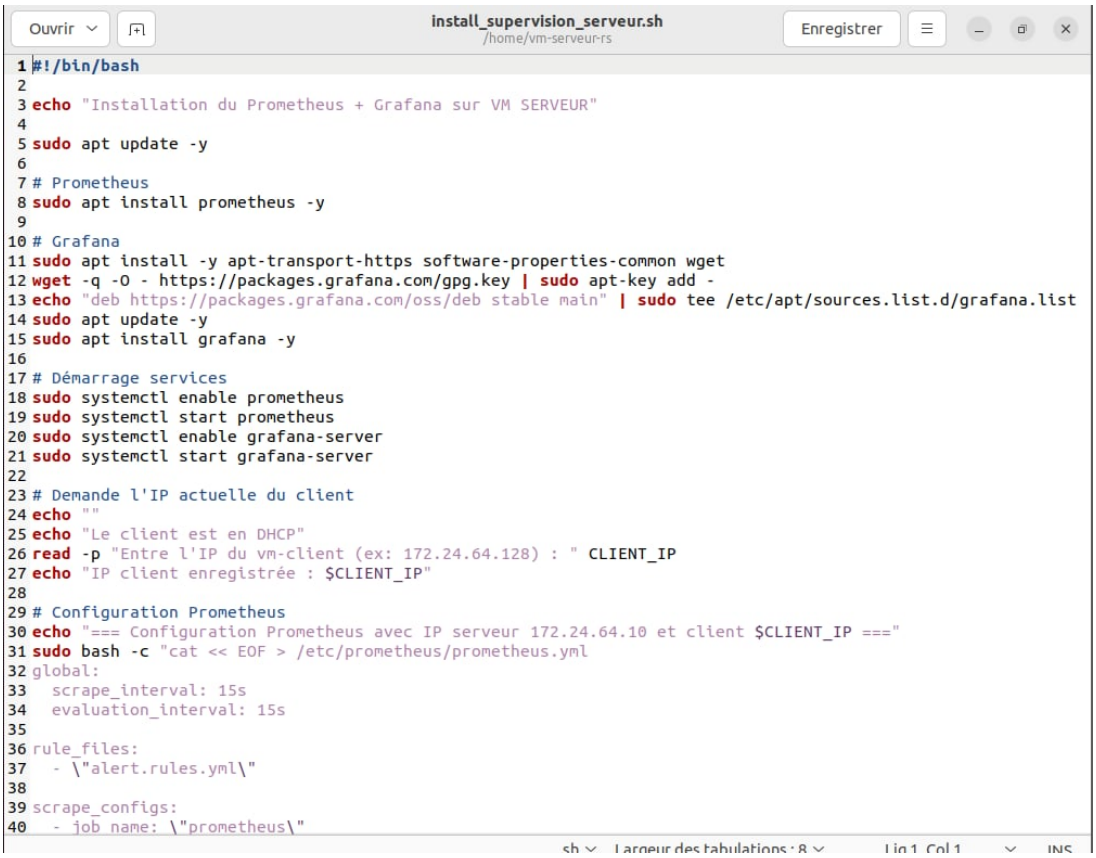


FIGURE 3.12 – Script d'installation de Prometheus et Grafana sur le serveur de supervision

**Configuration de Prometheus :**

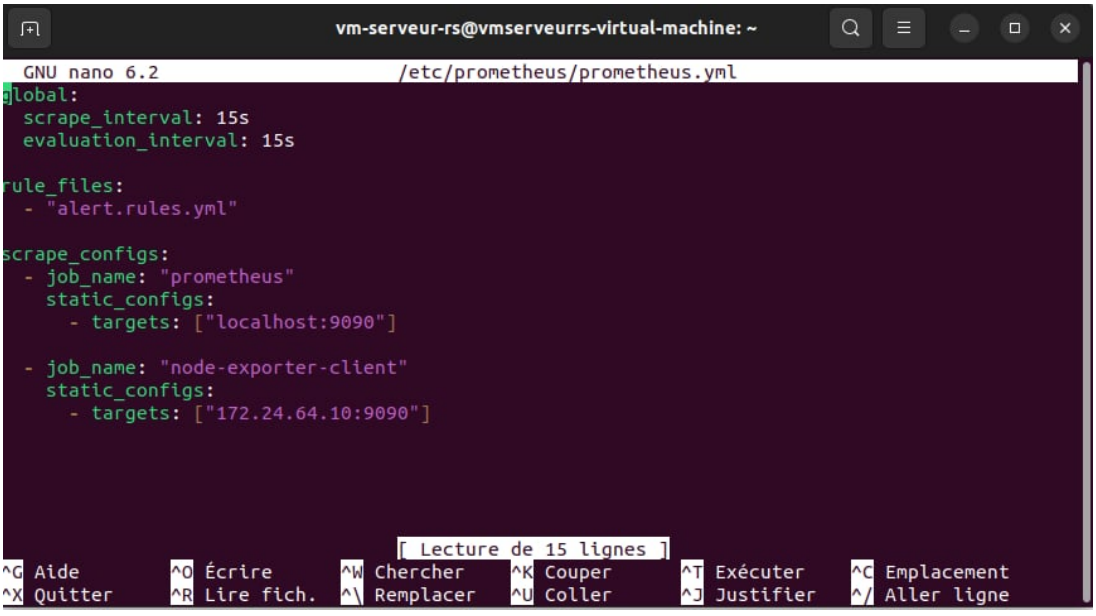


FIGURE 3.13 – Configuration du fichier prometheus.yml avec les cibles de supervision

**Règles d'alerte :**

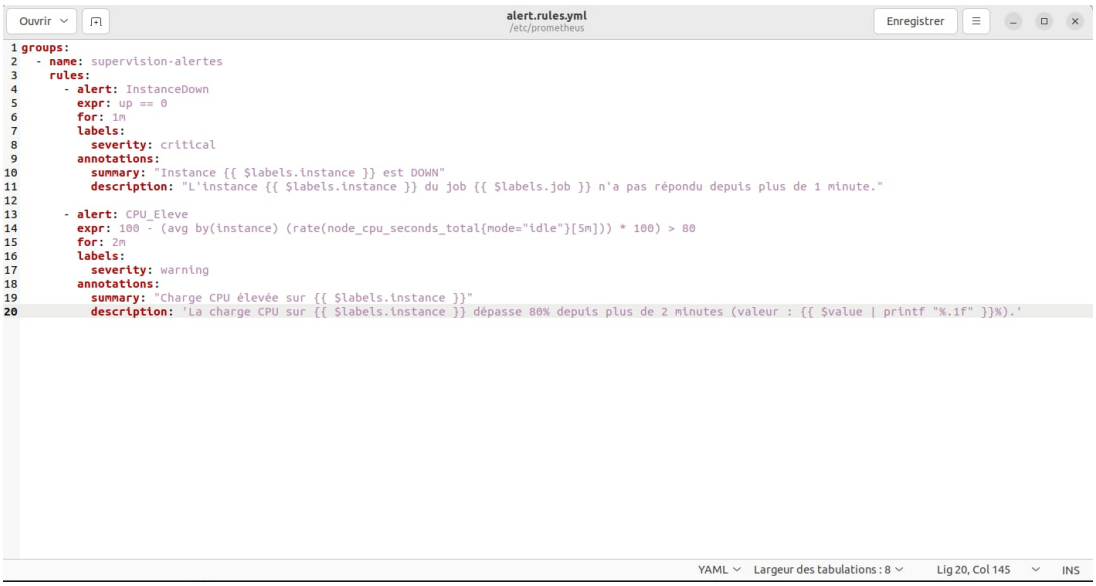


FIGURE 3.14 – Règles d'alerte Prometheus pour détecter les pannes et les surcharges CPU

**Installation du client Node Exporter :**

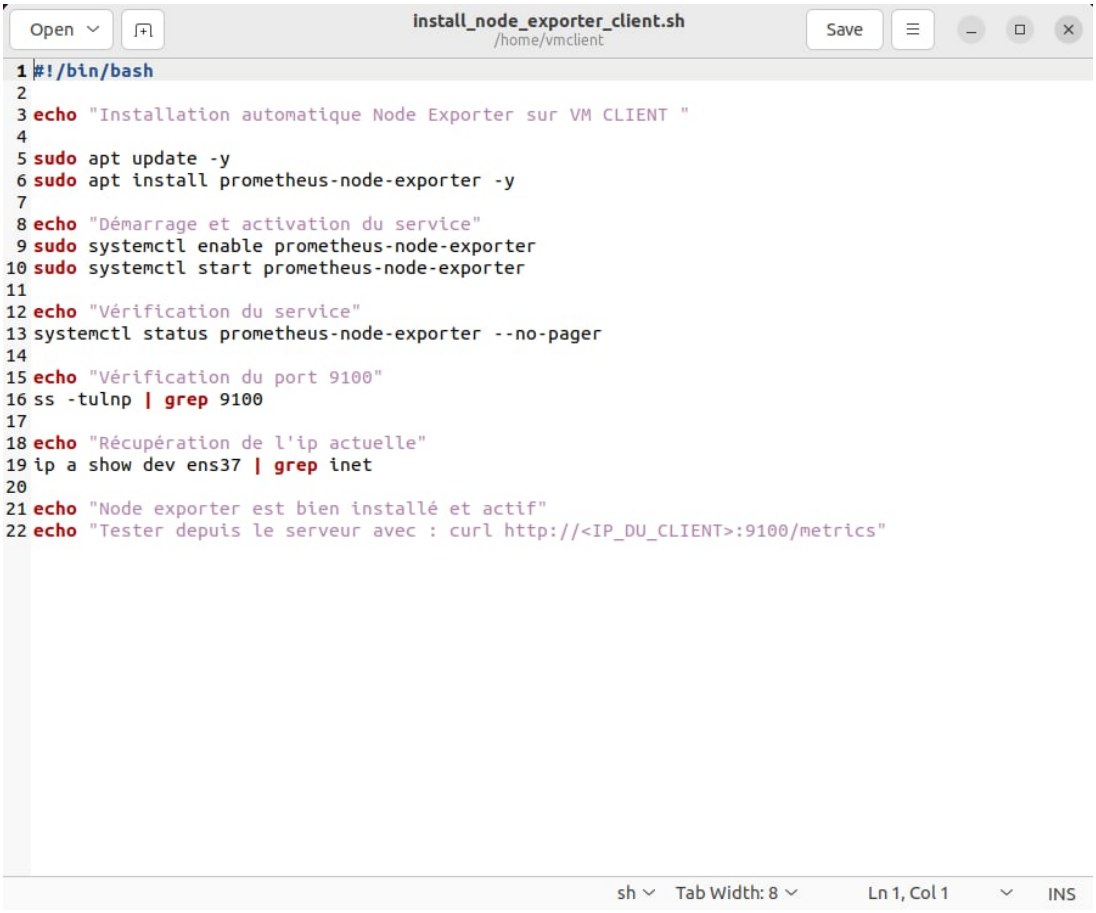


FIGURE 3.15 – Script d'installation de Node Exporter sur les machines clientes

**Architecture de la solution :**

TABLE 3.2 – Configuration des composants de supervision

| Composant | Adresse IP | Rôle |
|---|---|---|
| Serveur Prometheus | 172.24.64.10 | Collecte et stockage des métriques |
| Serveur Grafana | 172.24.64.10 | Visualisation des données |
| Client Node Exporter | 172.24.64.132 | Export des métriques système |

Cette solution permet de surveiller en temps réel :

— Disponibilité des équipements réseau
— Utilisation CPU et mémoire
— Charge réseau
— État des services

Les alertes sont configurées pour notifier automatiquement les administrateurs en cas de :

— Panne d'un équipement (InstanceDown)
— Charge CPU excessive (>80% pendant 2 minutes)
— Problèmes de connectivité réseau

**Base de données :** Accès et configuration de la base de données interne.


FIGURE 3.16 – Capture d'écran du service base de données

```
ubuntu@ubuntu-virtual-machine:~$ mysql -h 172.24.72.10 -u web_user -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.43-0ubuntu0.22.04.2 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

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

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

mysql> use gestion_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SELECT * FROM employes;
ERROR 1146 (42S02): Table 'gestion_db.employes' doesn't exist
mysql>
mysql> SELECT * FROM Employes;
+----+-------+--------+-------------+
| id | nom   | prenom | poste       |
+----+-------+--------+-------------+
|  1 | Alice | Dupont | Gestionnaire |
|  2 | Bob   | Martin | Comptable    |
+----+-------+--------+-------------+
2 rows in set (0.30 sec)

mysql>
```

FIGURE 3.17 – Test service base de données du web

**Web :** Disponibilité du serveur Web et configuration.

Open — setup_web_mysql_login.sh — Save

```
#!/bin/bash
DB_NAME="webdb"

APP_DB_USER="webapp"
APP_DB_PASS="WebApp@123"

echo "[1] Install Apache + PHP + MySQL + driver PHP"
sudo apt update -y
sudo apt install -y apache2 php libapache2-mod-php php-mysql mysql-server

echo "[2] Enable + start services"
sudo systemctl enable --now apache2
sudo systemctl enable --now mysql

echo "[3] Create database + users table"
sudo mysql <<SQL
CREATE DATABASE IF NOT EXISTS \`${DB_NAME}\`;
USE \`${DB_NAME}\`;

CREATE TABLE IF NOT EXISTS users (
  id INT AUTO_INCREMENT PRIMARY KEY,
  username VARCHAR(50) UNIQUE NOT NULL,
  password_hash VARCHAR(255) NOT NULL,
  role ENUM('admin','user') NOT NULL
);
SQL

echo "[4] Create MySQL user for the web app + grant privileges"
sudo mysql <<SQL
CREATE USER IF NOT EXISTS '${APP_DB_USER}'@'localhost' IDENTIFIED BY '${APP_DB_PASS}';
GRANT SELECT, INSERT, UPDATE, DELETE ON \`${DB_NAME}\`.* TO '${APP_DB_USER}'@'localhost';
FLUSH PRIVILEGES;
SQL

echo "[5] Quick checks"
sudo systemctl status apache2
sudo systemctl status mysql

echo "[OK] Done."
echo "  DB=${DB_NAME}  USER=${APP_DB_USER}  PASS=${APP_DB_PASS}"
echo "Test from client: http://<SERVER_IP>/app/login.php"
```

FIGURE 3.18 – Capture d'écran du service Web

**Partage et collaboration :** Services de partage de fichiers et collaboration interne.

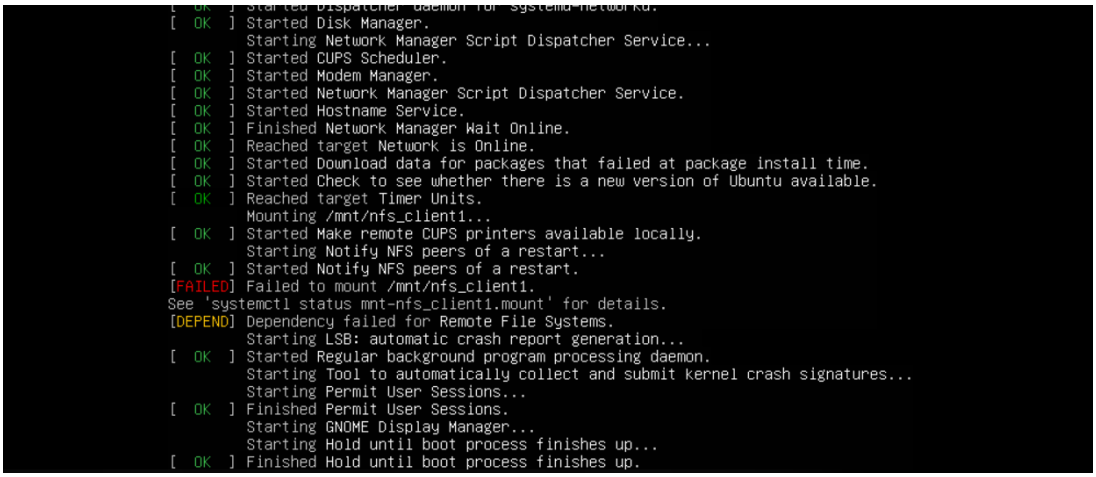


FIGURE 3.19 – Capture d'écran du service de partage et collaboration

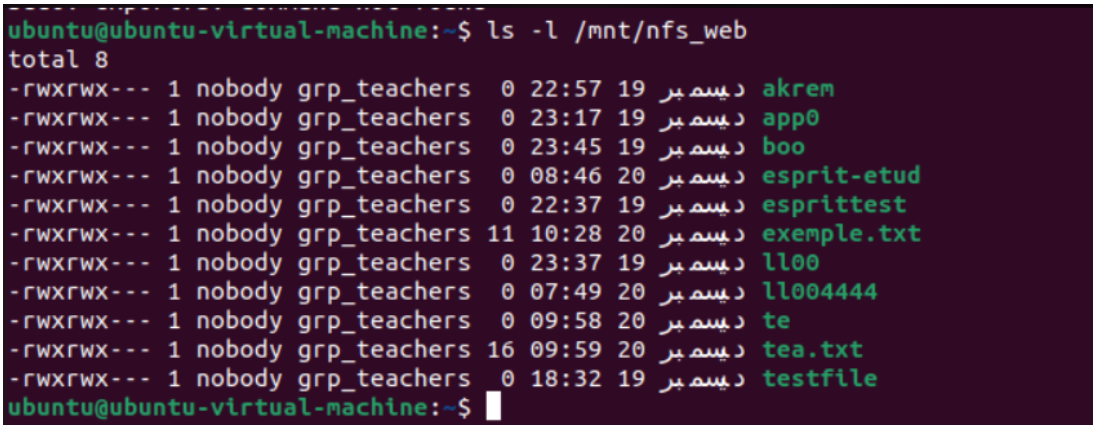


FIGURE 3.20 – Accès aux fichiers partagés via NFS depuis un autre ordinateur client

# Chapitre 4

# Tests, validation et supervision

## 4.1 Tests de connectivité

Des tests de connectivité ont été réalisés à chaque étape du projet :

— ping entre les routeurs du backbone,
— ping entre les routeurs de zone et le backbone,
— ping entre clients des différents sites (Web ↔ IT),
— traceroute pour vérifier le chemin des paquets.

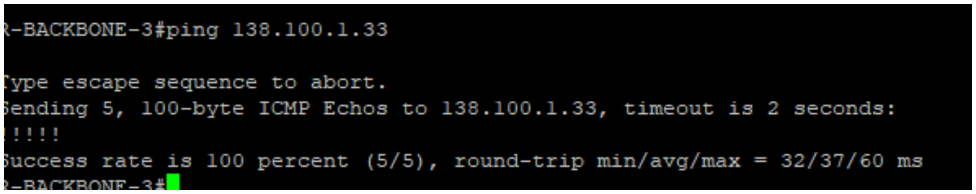


FIGURE 4.1 – Test de ping entre deux routeurs backbone

## 4.2 Validation du routage dynamique et des tunnels VPN

Afin de vérifier le bon fonctionnement du routage inter-sites, la table de routage du routeur RZ-1 a été consultée à l'aide de la commande :

```
show ip route
```

La figure 4.2 montre les différentes routes présentes.

On observe notamment :

— une route par défaut pointant vers l'accès Internet (`0.0.0.0/0 via 138.100.2.1`) ;
— des routes directement connectées (`C`) correspondant aux interfaces locales du routeur ;
— des routes apprises dynamiquement via OSPF (`O`) montrant le bon fonctionnement du routage dynamique ;
— des routes associées aux interfaces Tunnel (Tunnel12, Tunnel13, Tunnel14), confirmant l'établissement correct des tunnels GRE/IPsec et leur utilisation pour joindre les réseaux distants.

La présence de ces routes valide le bon échange des informations de routage, l'interconnexion des différents sites via le backbone ainsi que la fonctionnalité des mécanismes VPN.

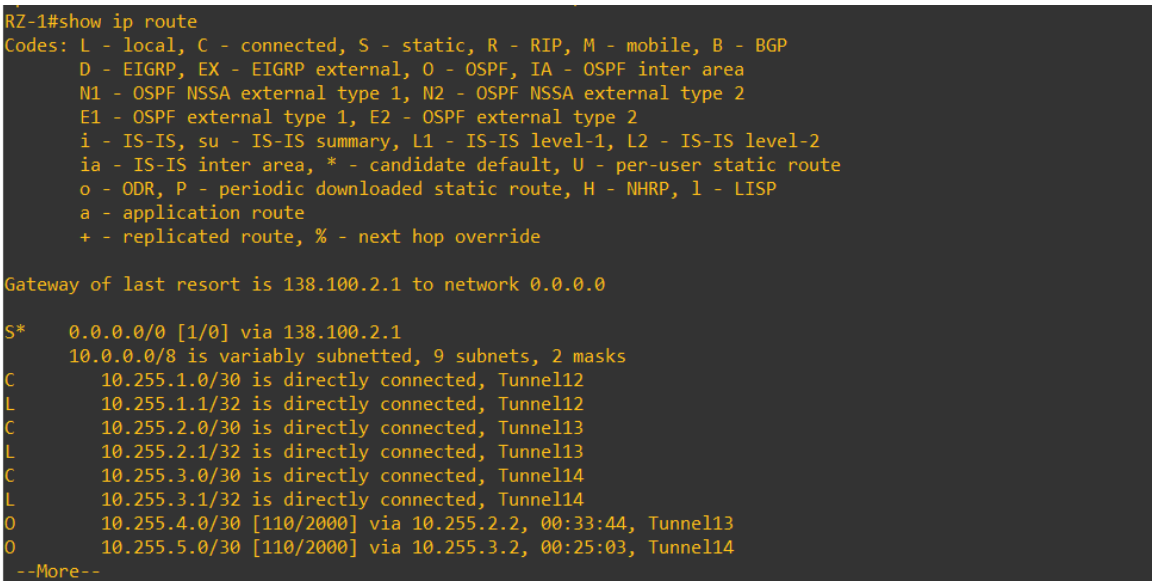


FIGURE 4.2 – Table de routage de RZ-1 montrant les routes OSPF et tunnels VPN

La bonne propagation des routes a été confirmée via la commande `show ip route`. Les tunnels IPsec ont été validés à l'aide de `show crypto isakmp sa` et `show crypto ipsec sa`, qui indiquent l'état des associations de sécurité et le nombre de paquets chiffrés/déchiffrés.

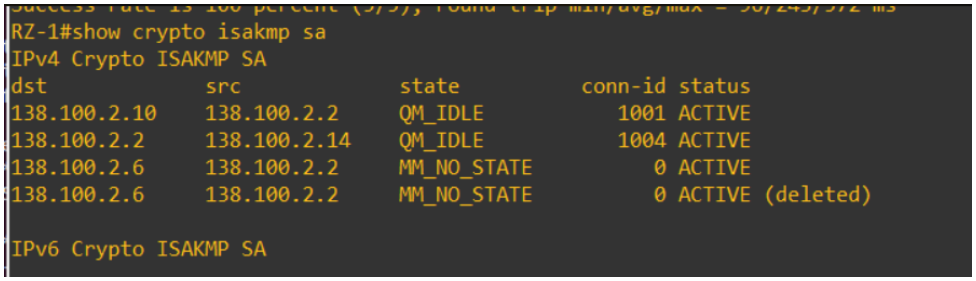


FIGURE 4.3 – Validation du tunnel IPsec entre RZ-1 et RZ-2

## 4.3 Validation de l'application Web sur le client NFS

L'application Web de gestion des employés est déployée sur le serveur du département Base de Données et accessible depuis le client du département Web via le partage NFS. Les captures suivantes illustrent les principales fonctionnalités offertes par l'application.

### 4.3.1 Modification d'un employé (client Web sur NFS)

La figure 4.4 montre le formulaire d'édition d'un employé. L'utilisateur peut modifier le nom, le département ainsi que le salaire, puis enregistrer les changements. Cette page est servie à partir des fichiers applicatifs stockés sur le partage NFS, ce qui illustre l'intégration entre le service NFS et l'application Web.


FIGURE 4.4 – Formulaire de modification d'un employé depuis le client Web (NFS)

### 4.3.2 Tableau de bord utilisateur (lecture seule)

La figure 4.5 présente le tableau de bord utilisateur. L'utilisateur connecté dispose d'une vue en lecture seule de la liste des employés (ID, nom, département et salaire) sans possibilité de modifier les données. Cela permet de séparer les profils "utilisateur" et "administrateur", tout en accédant aux données stockées sur le serveur via NFS.

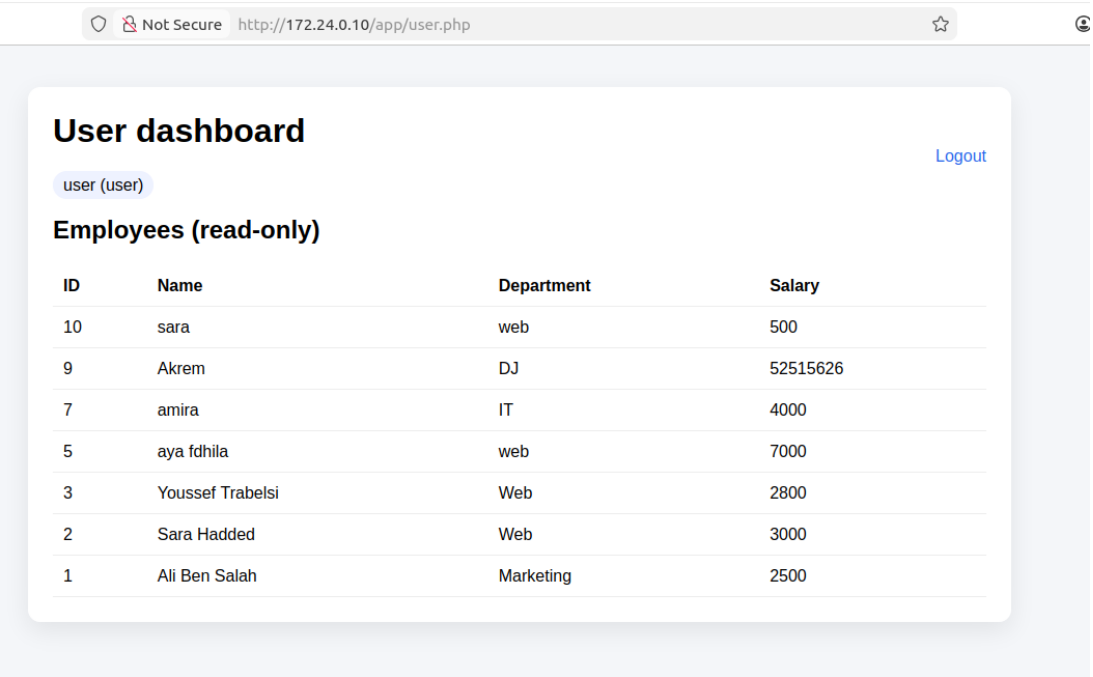


FIGURE 4.5 – Tableau de bord utilisateur : consultation des employés en lecture seule

### 4.3.3 Ajout d'un nouvel employé

La figure 4.6 illustre le formulaire d'ajout d'un nouvel employé. L'administrateur saisit le nom, le département et le salaire, puis enregistre l'entrée. Cette opération déclenche une écriture en base de données et confirme que l'application est pleinement fonctionnelle depuis le client NFS.

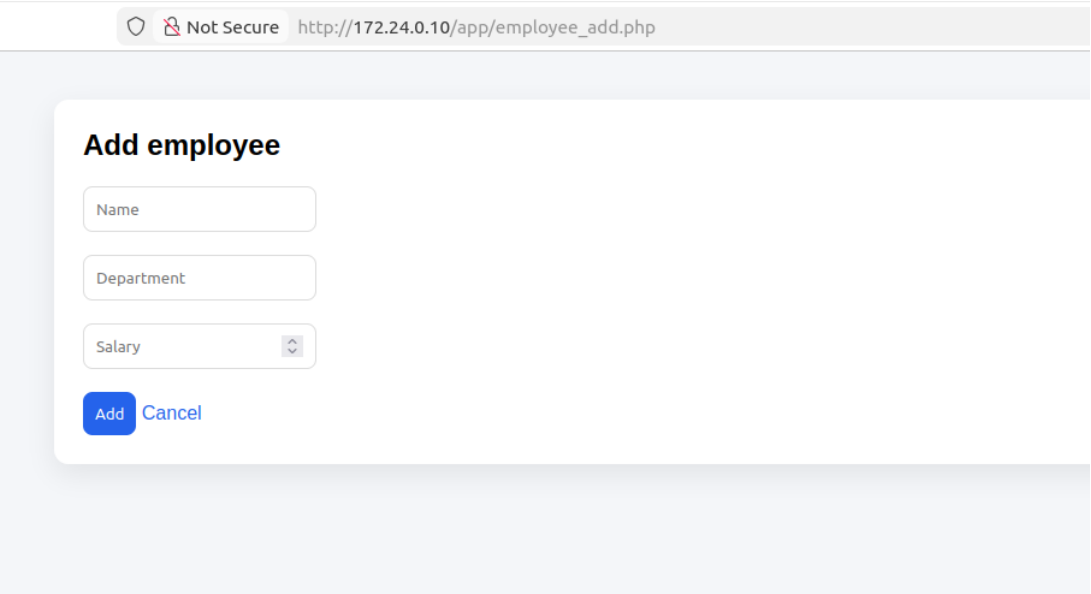


FIGURE 4.6 – Formulaire d'ajout d'un nouvel employé

### 4.3.4 Tableau de bord administrateur (gestion complète)

La figure 4.7 montre le tableau de bord administrateur. Celui-ci dispose d'une vue complète sur les employés avec les actions *Edit* et *Delete* pour chaque ligne. Ce tableau de bord prouve la capacité de l'application à gérer les opérations CRUD (Create, Read, Update, Delete) tout en s'appuyant sur les fichiers de l'application situés sur le partage NFS et la base de données du département dédié.

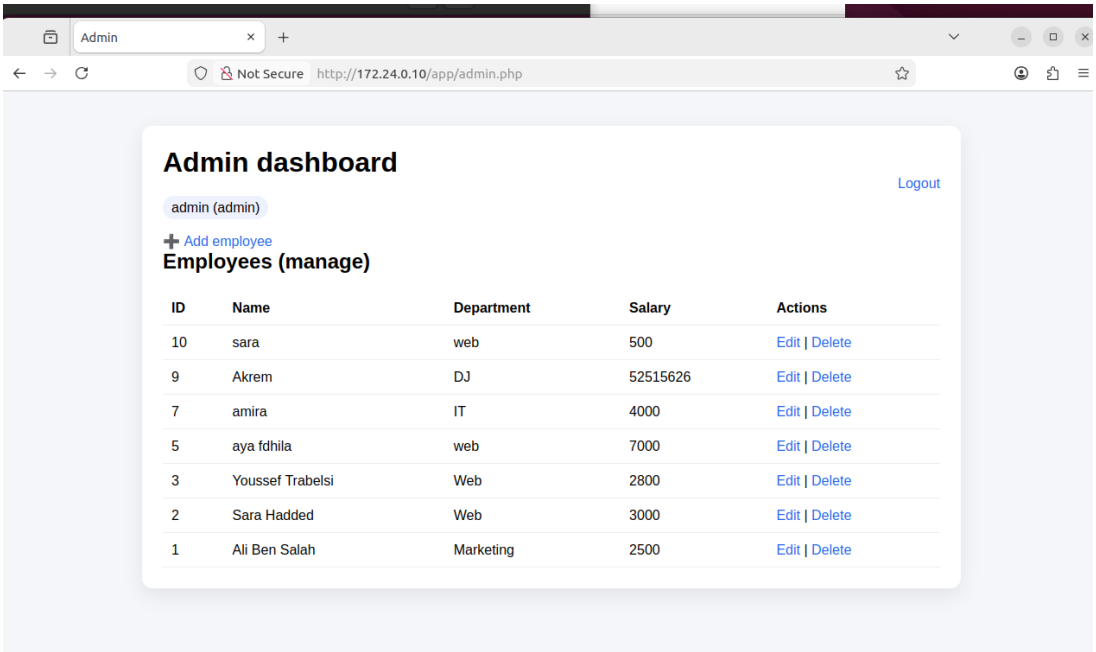


FIGURE 4.7 – Tableau de bord administrateur : gestion complète des employés

## 4.4 Validation de la base de données depuis le département IT

Afin de vérifier l'accessibilité et le bon fonctionnement du service Base de Données, un test de connexion MySQL a été effectué depuis une machine du département IT vers le serveur MySQL du département Base de Données.

La figure 4.8 montre la connexion distante via la commande :

```
mysql -h 172.24.72.10 -u web_user -p
```

Après authentification, la base de données `gestion_db` est sélectionnée et une requête SQL `SELECT * FROM Employes;` est exécutée. L'affichage du contenu de la table confirme que :

— la connectivité réseau entre les départements est fonctionnelle ;
— le serveur MySQL est opérationnel ;
— les comptes utilisateurs et privilèges sont correctement configurés ;
— les données de la base sont accessibles et cohérentes.

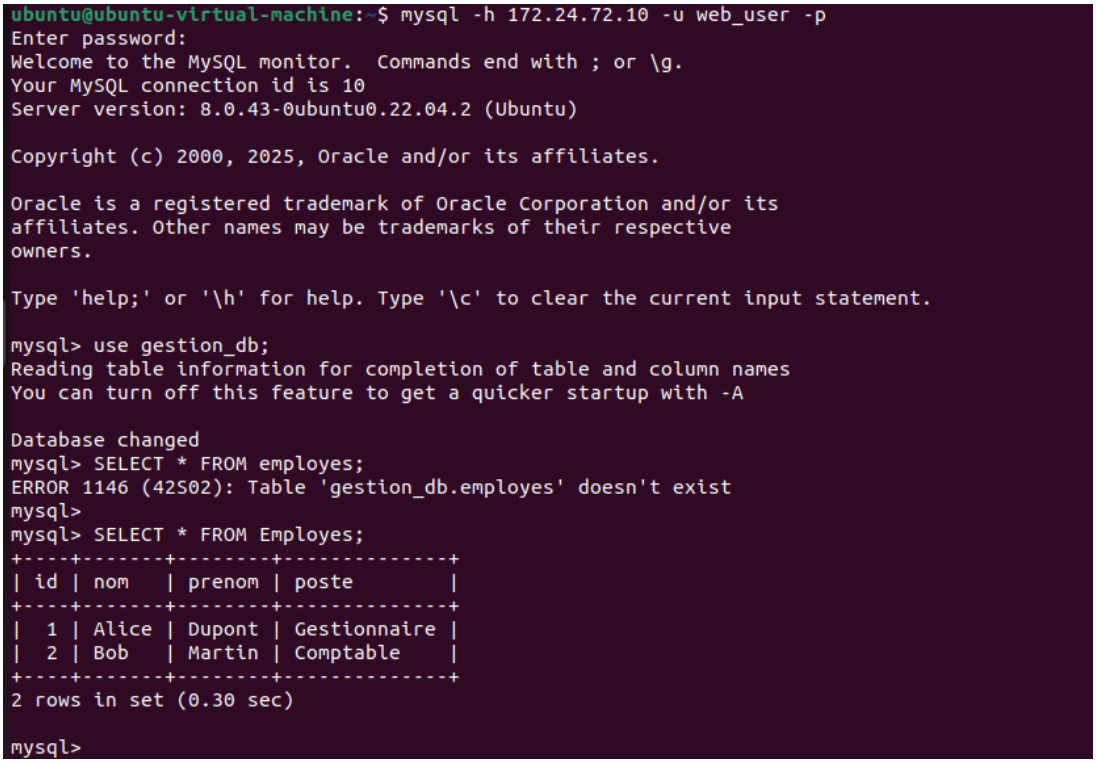


FIGURE 4.8 – Validation du service Base de Données depuis le département IT

## 4.5 Validation du service NFS

Afin de valider le bon fonctionnement du service NFS mis en place pour le département concerné, une série de tests a été réalisée depuis un client distant. Le principe consiste à accéder au répertoire partagé exporté par le serveur NFS et vérifier la possibilité de lecture et d'écriture à distance.

### 4.5.1 Montage du partage NFS

Depuis une machine cliente, le répertoire partagé du serveur a été monté à travers un point de montage local. La figure 4.9 montre la connexion réussie au serveur NFS.

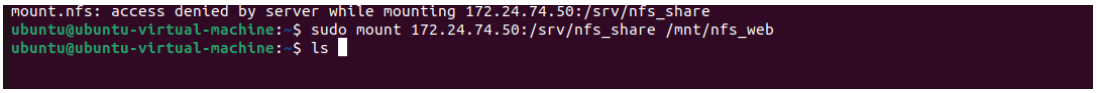


FIGURE 4.9 – Montage du partage NFS sur le client

### 4.5.2 Consultation des fichiers

Une fois le partage monté, nous avons accédé au dossier partagé afin de vérifier la visibilité des fichiers présents sur le serveur. Comme illustré dans la figure 4.10, le client peut consulter l'ensemble des fichiers stockés sur le répertoire NFS.


FIGURE 4.10 – Consultation du contenu du répertoire partagé via NFS

### 4.5.3 Test d'écriture distante

Pour finaliser la validation, un fichier de test a été créé depuis le client. L'apparition de ce fichier dans le répertoire partagé confirme la possibilité d'écriture à distance et donc le bon fonctionnement du service NFS. La figure 4.11 montre la création du fichier et sa présence dans le dossier partagé.

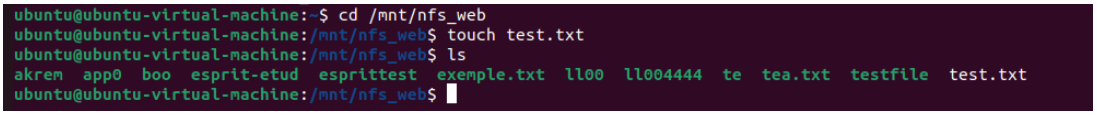


FIGURE 4.11 – Création d'un fichier à distance confirmant le bon fonctionnement du service NFS

Ces tests prouvent que le partage de fichiers via NFS est opérationnel, permettant une communication fiable entre le serveur et les clients, en conformité avec les exigences du cahier des charges.

## 4.6 Supervision

Un serveur de supervision est déployé sur le site IT pour surveiller l'état des routeurs et des principaux serveurs (Web, base de données, partage). Les métriques collectées

(disponibilité, charge CPU, utilisation réseau, etc.) sont visualisées via un tableau de bord.

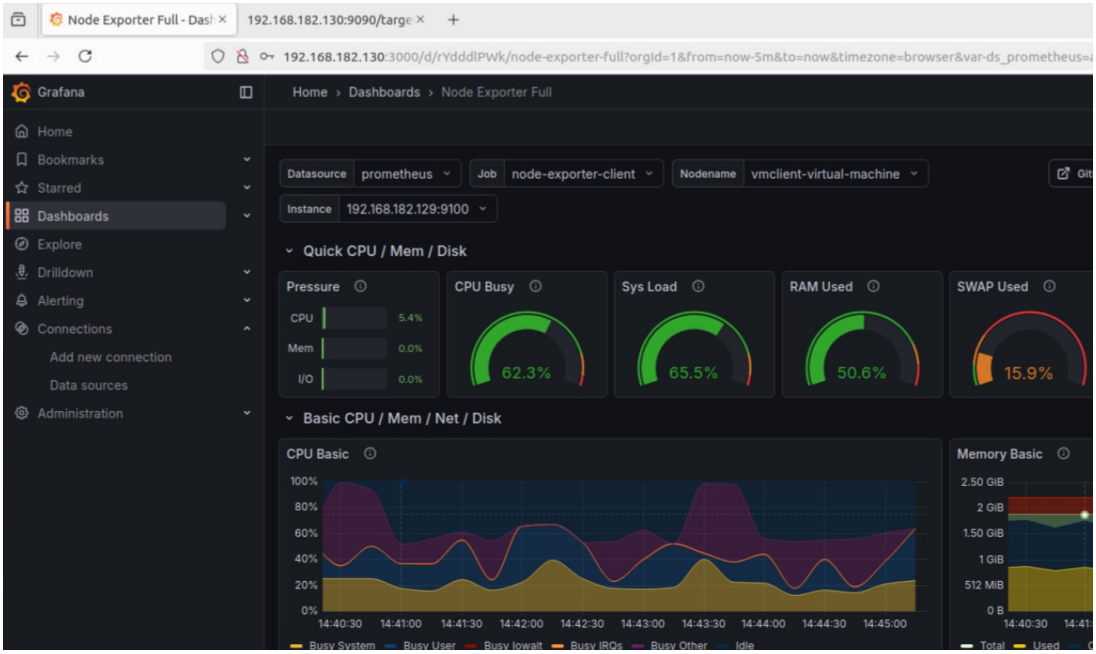


FIGURE 4.12 – Exemple de tableau de bord de supervision

## 4.7 Problèmes rencontrés et solutions apportées

Cette phase de tests a permis d'identifier plusieurs problèmes techniques liés à la configuration du routage, des services réseau et de la sécurité. Les principales difficultés rencontrées ainsi que les solutions apportées sont présentées ci-dessous.

### 4.7.1 Problème de connectivité inter-sites

**Problème :** Lors des premiers tests, les machines du site Web (RZ-1) ne pouvaient pas communiquer avec celles du site IT (RZ-2).

**Cause :** Les réseaux LAN des sites n'étaient pas correctement annoncés dans le processus de routage OSPF, ce qui empêchait la propagation des routes.

**Solution :** Les réseaux manquants ont été ajoutés dans la configuration OSPF sur les routeurs de zone.

```
router ospf 1
 network 172.24.0.0 0.0.63.255 area 0
 network 10.255.1.0 0.0.0.3 area 0
```

**Validation :** Les commandes `ping` et `traceroute` ont confirmé le passage correct du trafic entre les sites via le backbone et les tunnels GRE.

### 4.7.2 Traduction NAT incorrecte du trafic interne

**Problème :** Le trafic entre les sites internes était traduit par NAT, ce qui empêchait la communication directe entre les réseaux privés.

**Cause :** L'ACL utilisée pour le NAT ne filtrait pas correctement les destinations internes.

**Solution :** Des règles de refus ont été ajoutées afin d'exclure les réseaux internes de la traduction d'adresses.

```
access-list 101 deny ip 172.24.0.0 0.0.63.255 172.24.64.0
   0.0.7.255
access-list 101 permit ip 172.24.0.0 0.0.63.255 any
```

**Validation :** Les échanges inter-sites ont été rétablis sans NAT, tandis que l'accès Internet est resté fonctionnel.

### 4.7.3 Problème d'attribution des adresses IP par DHCP

**Problème :** Les postes clients du site IT ne recevaient pas d'adresse IP automatiquement.

**Cause :** Une erreur de configuration du routeur par défaut dans le pool DHCP.

**Solution :** Correction du paramètre `default-router` dans la configuration DHCP.

```
default-router 172.24.64.1
```

**Validation :** Les clients ont obtenu une adresse IP valide, ainsi que les paramètres réseau nécessaires (passerelle et DNS).

### 4.7.4 Échec initial du tunnel VPN IPsec

**Problème :** Le tunnel IPsec entre les sites restait à l'état inactif.

**Cause :** Une incohérence dans la clé pré-partagée utilisée pour l'authentification ISAKMP.

**Solution :** Synchronisation des clés IPsec et vérification des paramètres de sécurité sur les deux routeurs.

**Validation :** La commande `show crypto isakmp sa` a affiché l'état `QM_IDLE`, confirmant le bon fonctionnement du tunnel sécurisé.

### 4.7.5 Absence de visibilité dans la supervision

**Problème :** Certains équipements n'étaient pas visibles dans l'outil de supervision.

**Cause :** Le service SNMP n'était pas activé sur l'ensemble des routeurs.

**Solution :** Activation et configuration du protocole SNMP sur les équipements réseau.

```
snmp-server community public RO
```

**Validation :** Les routeurs et serveurs sont désormais visibles et supervisés via le tableau de bord centralisé.

# Conclusion

Ce projet a permis de mettre en oeuvre une infrastructure réseau complète incluant un backbone OSPF, des sites distants reliés via des tunnels GRE et des VPN IPsec, ainsi que des services indispensables tels que le DHCP, le NAT, des services applicatifs et la supervision.

La conception du plan d'adressage, le choix d'OSPF comme protocole de routage ainsi que la mise en place d'ACL de sécurité ont permis de répondre aux principaux objectifs du cahier des charges, en assurant à la fois la connectivité et la maîtrise des flux entre zones.

Plusieurs pistes d'amélioration sont envisageables :

— la mise en place de redondance matérielle (HSRP/VRRP) pour les routeurs de zone,
— le durcissement de la sécurité (pare-feu dédié, IDS/IPS),
— l'extension de la supervision à l'ensemble du système d'information.

Ce projet constitue une base solide pour la conception d'infrastructures réseau d'entreprise plus complexes et renforce la maîtrise pratique des technologies de routage, de VPN et de sécurité.