LEIDOSCOPE

Projet AP1 Infrasite

Document technique final



Deniz Elhasoglu et Nathan Ogoreck

Lycée Saint Adjutor
Groupe 5 • Mme PITOIS
Année scolaire 2026–2027

BTS SIO • OPTION SISR • DEUXIÈME ANNÉE

13 octobre 2026

Sommaire

Contexte et organisation de la solution
Activité 2 – Schéma réseau et adressage
Activité 3 – Initialisation des équipements
Activité 4 – Administration distante sécurisée
Activité 5 – Installation et câblage
Activité 6 – Routage RIPv2 et routes par défaut
Activité 7 – Serveur TFTP et sauvegardes
Activité 8 – NAT/PAT et NAT statique
Activité 9 – Politique finale du pare-feu
Activité 10 – ACL des services
Reprise et maintenance de la configuration
Bilan du projet

Objet du document

Ce document présente la mise en place de l’infrastructure, activité par activité. Chaque étape indique les réglages appliqués et les captures de configuration correspondantes. Les résultats des tests sont regroupés dans le rapport de tests.

Le schéma, l’adressage et les liaisons sont détaillés dans l’activité 2. Les comptes et mots de passe sont conservés dans le Notion partagé du groupe.

Contexte et organisation de la solution

LEIDOSCOPE dispose d’un LAN organisé par services. Le projet AP1 Infrasite ajoute une zone DMZ et une liaison vers Internet tout en conservant le cloisonnement des utilisateurs. L’infrastructure doit permettre les accès aux ressources communes, l’administration sécurisée et la sauvegarde des équipements.

Répartition des fonctions

Élément	Fonction dans la solution
SwCoeur	Routage des VLAN du LAN et filtrage inter-services.
SwE1 et SwRC	Raccordement des postes et affectation des ports aux VLAN des services.
SwE2Serveur	Raccordement de l’hôte Hyper-V et du VLAN serveurs.
Pare-feu Zyxel	Interconnexion et filtrage entre LAN, DMZ et transit Internet.
SwNET et SwDMZ	Commutation des zones de transit et de DMZ.
RNET1	Sortie vers le campus et traduction NAT/PAT.
Ubuntu TFTP	Réception des sauvegardes de configuration Cisco.

Contraintes de mise en œuvre

Le protocole RIPv2 est imposé. Le routeur du campus à 192.168.4.254 n’est pas administrable par le groupe. Les services doivent accéder à l’AD et à Internet, sans communiquer directement entre eux. L’administration des équipements est réservée à IT ; le serveur TFTP doit être protégé.

La lettre de mission prévoit la mise en production d’un serveur Web dans la DMZ. Le schéma fait apparaître les serveurs prévus, et les flux correspondants sont préparés sur le pare-feu (activité 9).

Activité 2 – Schéma réseau et adressage

Étape 1 – Lire les zones et les interconnexions

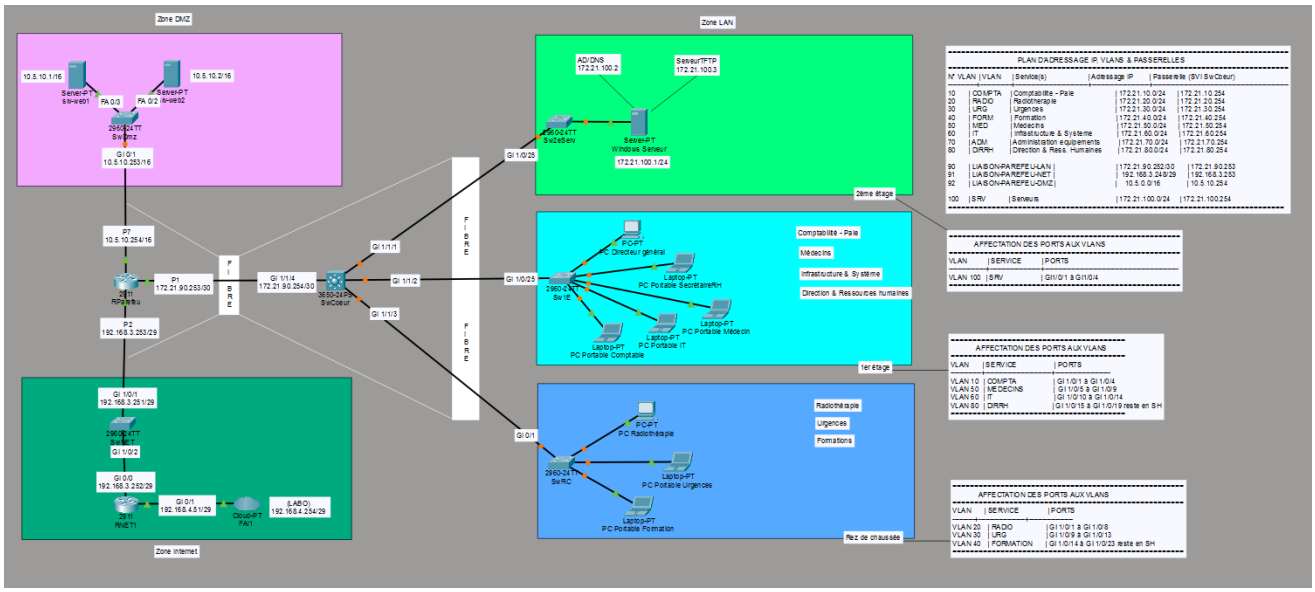

Figure 1 – Schéma réseau fourni et actualisé

Le cœur centralise les trois commutateurs du LAN. Sa liaison avec le pare-feu utilise le VLAN 90. Le pare-feu rejoint SwNET, puis RNET1, pour la sortie vers le campus ; il rejoint également SwDMZ pour la zone des serveurs exposés.

Le VLAN 100 rassemble l'hôte Hyper-V et les services AD/DNS et TFTP. Les VLAN des utilisateurs possèdent chacun une passerelle sur SwCoeur. Les réseaux de transit ne sont pas des VLAN utilisateurs : ils relient les équipements d'interconnexion.

Lecture des masques

Le lien cœur–pare-feu utilise 172.21.90.252/30, le transit vers RNET1 utilise 192.168.3.248/29 et la DMZ utilise 10.5.0.0/16.

Côté campus, RNET1 utilise l'adresse 192.168.4.51/24 sur Gi0/1, dans le même réseau que le routeur du labo 192.168.4.254.

Étape 2 – Identifier les VLAN et les passerelles

VLAN	Nom du schéma	Réseau IP	Passerelle
10	COMPTA	172.21.10.0/24	172.21.10.254
20	RADIO	172.21.20.0/24	172.21.20.254
30	URG	172.21.30.0/24	172.21.30.254
40	FORM	172.21.40.0/24	172.21.40.254
50	MED	172.21.50.0/24	172.21.50.254
60	IT	172.21.60.0/24	172.21.60.254
70	ADM	172.21.70.0/24	172.21.70.254
80	DIRRH	172.21.80.0/24	172.21.80.254

VLAN	Nom du schéma	Réseau IP	Passerelle
90	Liaison cœur pare-feu	172.21.90.252/30	Zyxel 172.21.90.253
91	Liaison pare-feu NET	192.168.3.248/29	Zyxel 192.168.3.253
92	Liaison pare-feu DMZ	10.5.0.0/16	Zyxel 10.5.10.254
100	SRV	172.21.100.0/24	172.21.100.254

Les interfaces VLAN du cœur assurent la passerelle des services LAN. Le VLAN 60 est réservé au service Infrastructure et Systèmes ; le VLAN 70 sert à l'administration des équipements. Ils ne reçoivent pas ACL-SERVICES, contrairement aux six VLAN utilisateurs concernés par l'isolation.

Sur les commutateurs de niveau 2, l'adresse de gestion identifie le commutateur lui-même. Elle est unique pour chaque commutateur afin de pouvoir l'administrer individuellement en SSH.

Étape 3 – Repérer les interfaces et les adresses

Équipement	Interface ou rôle	Adresse
SwCoeur	SVI VLAN 70	172.21.70.254/24
SwE1	Gestion VLAN 70	172.21.70.1/24
SwE2Serveur	Gestion VLAN 70	172.21.70.2/24
SwRC	Gestion VLAN 70	172.21.70.3/24
SwCoeur	SVI VLAN 90	172.21.90.254/30
Zyxel	SFP vers cœur	172.21.90.253/30
Zyxel	WAN1 vers transit	192.168.3.253/29
SwNET	Gestion VLAN 91	192.168.3.251/29
RNET1	Gi0/0 vers SwNET	192.168.3.252/29
RNET1	Gi0/1 vers campus	192.168.4.51/24
Zyxel	DMZ vers SwDMZ	10.5.10.254/16
SwDMZ	SVI VLAN 92	10.5.10.253/16
Hyper-V	VLAN 100	172.21.100.1/24
AD et DNS	VLAN 100	172.21.100.2/24
TFTP Ubuntu	VLAN 100	172.21.100.3/24

Le schéma place srv-web1 à 10.5.10.1/16 et srv-web2 à 10.5.10.2/16. Le serveur 10.5.10.1 est publié vers le campus par NAT statique (activité 8).

Étape 4 – Associer les ports aux liaisons et aux services

Liaison	Port indiqué au schéma
SwCoeur vers SwE2Serveur	Gi1/1/1 vers Gi1/0/25
SwCoeur vers SwE1	Gi1/1/2 vers Gi1/0/25

Liaison	Port indiqué au schéma
SwCoeur vers SwRC	Gi1/1/3 vers Gi0/1
SwCoeur vers Zyxel	Gi1/1/4 vers P1 au schéma ; SFP sur le Zyxel réel
Zyxel vers SwNET	P2 au schéma ; WAN1 sur le Zyxel réel, vers Gi1/0/1
SwNET vers RNET1	Gi1/0/2 vers Gi0/0
Zyxel vers SwDMZ	P7 au schéma ; DMZ sur le Zyxel réel, vers Gi0/1

Commutateur	VLAN	Ports du schéma
SwE2Serveur	100	Gi1/0/1 à Gi1/0/4
SwE1	10	Gi1/0/1 à Gi1/0/4
SwE1	50	Gi1/0/5 à Gi1/0/9
SwE1	60	Gi1/0/10 à Gi1/0/14
SwE1	80	Gi1/0/15 à Gi1/0/19
SwRC	20	Gi1/0/1 à Gi1/0/8
SwRC	30	Gi1/0/9 à Gi1/0/13
SwRC	40	Gi1/0/14 à Gi1/0/23

Les tableaux reprennent les noms de ports du schéma. Les ports non affectés sont désactivés.

Sur le schéma Packet Tracer, le pare-feu est représenté par un routeur (ports P1, P2 et P7). Sur le Zyxel réel, ces liaisons correspondent aux interfaces SFP, WAN1 et DMZ.

Activité 3 – Initialisation des équipements

Étape 1 – Préserver la configuration existante

Avant toute réinitialisation, exporter la configuration présente sur l’équipement et relever son modèle, sa version et ses interfaces.

Étape 2 – Réinitialiser uniquement si nécessaire

Appliquer la procédure de remise à zéro propre au modèle (Cisco ou Zyxel), uniquement après sauvegarde de l’ancienne configuration.

Étape 3 – Préparer l’administration

Définir le nom d’hôte, le compte local, l’adresse de gestion et la passerelle appropriée. Vérifier l’accès console ou local avant d’activer l’administration distante, puis enregistrer la configuration.

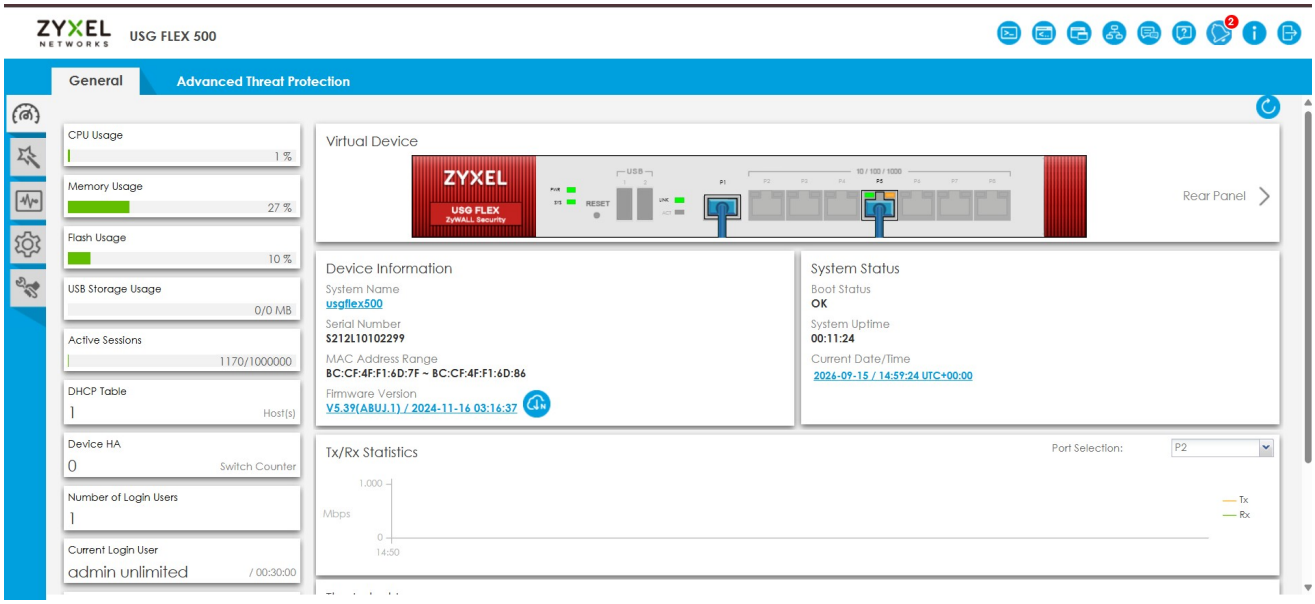

Figure 2 – Interface du Zyxel

Activité 4 – Administration distante sécurisée

Principe de la configuration SSH

Ordre de configuration

Commencer par l’accès console et l’adressage de gestion. Définir ensuite le nom de domaine, créer le compte local, générer la clé RSA et activer SSH. Configurer les lignes VTY avant d’appliquer la restriction d’origine, en gardant la session console ouverte pour pouvoir corriger en cas d’erreur.

Adresses de gestion individualisées

Chaque commutateur interne reçoit l’adresse indiquée dans l’activité 2. Le VLAN 70 sert de réseau de gestion et le poste administrateur se trouve dans le VLAN 60 ; le cœur assure le routage entre les deux.

Rôle des paramètres SSH

Le domaine participe à la préparation des clés. RSA 2048 bits et SSH version 2 définissent le service sécurisé. Le délai de 60 secondes et les trois tentatives concernent l’authentification ; exec-timeout 5 0 ferme une session devenue inactive après cinq minutes. login local utilise la base de comptes propre à l’équipement.

Restriction des origines

SSH-IT est une ACL standard appliquée sur les lignes VTY : seules les adresses du VLAN 60 IT peuvent ouvrir une session d’administration. Elle est distincte d’ACL-SERVICES, qui filtre le trafic des utilisateurs. Les équipements situés derrière le pare-feu (SwNET, SwDMZ et RNET1) sont administrés depuis le VLAN 60 grâce aux règles IT_TO_WAN_Admin et IT_TO_DMZ_Admin (activité 9).

SSH v2 remplace Telnet. Chaque commutateur LAN possède une adresse propre dans le VLAN 70 : SwE1 172.21.70.1, SwE2Serveur 172.21.70.2, SwRC 172.21.70.3 et SwCoeur 172.21.70.254. Le poste d’administration appartient au VLAN 60 IT.

Étape 1 – Préparer le domaine et la bannière

Configurer le domaine leidoscope.local sur les équipements internes et ajouter une bannière d'avertissement d'accès réservé. SwNET utilise le domaine leidoscope.exter.

```
ip domain-name leidoscope.local
```

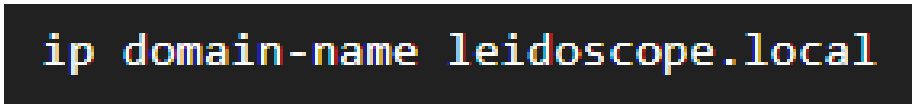

Figure 3 – Domaine interne

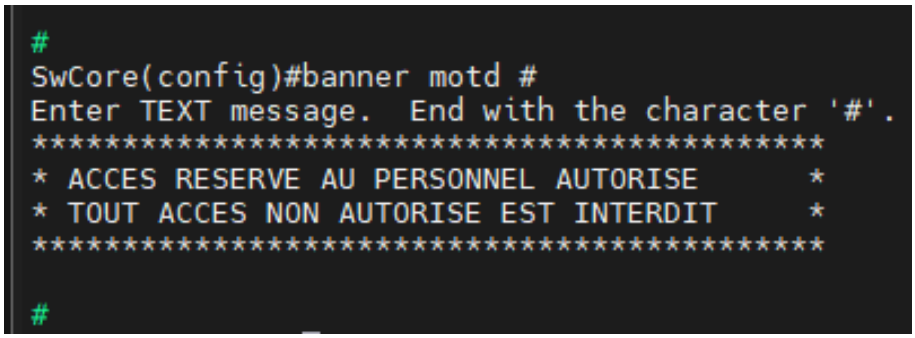

Figure 4 – Bannière de connexion

Étape 2 – Générer la clé et activer SSH v2

Utiliser une clé RSA de 2048 bits, trois tentatives d'authentification et un délai de 60 secondes.

```
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh authentication-retries 3
ip ssh time-out 60
```

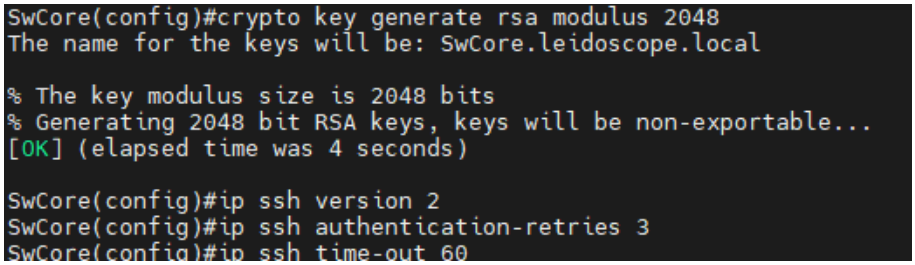

Figure 5 – Clés RSA et SSH v2

Étape 3 – Configurer les lignes VTY

Utiliser le compte local, limiter le transport à SSH et fermer les sessions inactives après cinq minutes. Les identifiants sont conservés dans le Notion du groupe.

```
line vty 0 15
 login local
 transport input ssh
 exec-timeout 5 0
exit
```

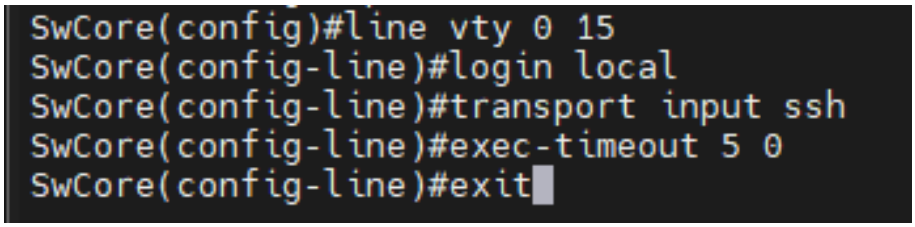

Figure 6 – Sécurisation des lignes VTY

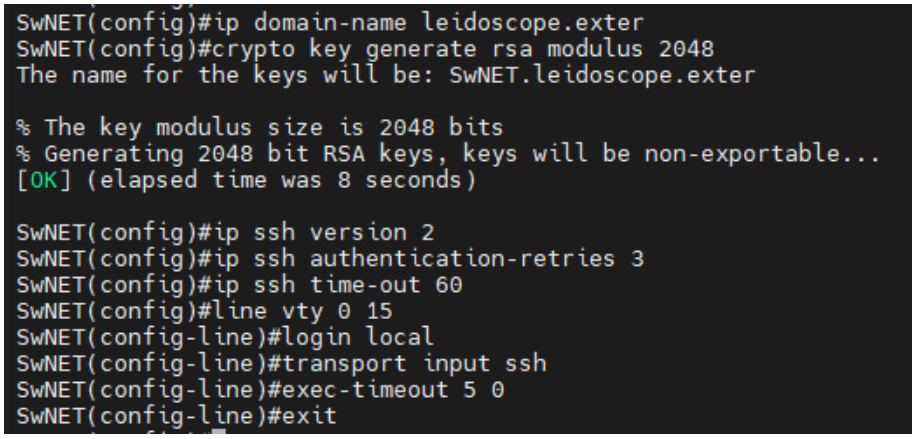

Figure 7 – SSH sur SwNET

Étape 4 – Limiter les origines au VLAN IT

Appliquer SSH-IT en entrée sur les lignes VTY de chaque équipement Cisco. L’autorisation porte sur 172.21.60.0/24 ; les autres sources sont refusées.

```
ip access-list standard SSH-IT
 permit 172.21.60.0 0.0.0.255
 deny any
exit
line vty 0 15
 access-class SSH-IT in
 transport input ssh
end
write memory
```

Cette configuration est appliquée sur l’ensemble des équipements Cisco du projet.

Activité 5 – Installation et câblage

Étape 1 – Installer les équipements dans la baie

La baie regroupe les commutateurs, le routeur RNET1 et le pare-feu. Le cœur relie les commutateurs LAN et le Zyxel ; le pare-feu rejoint ensuite SwNET côté transit et SwDMZ côté DMZ.

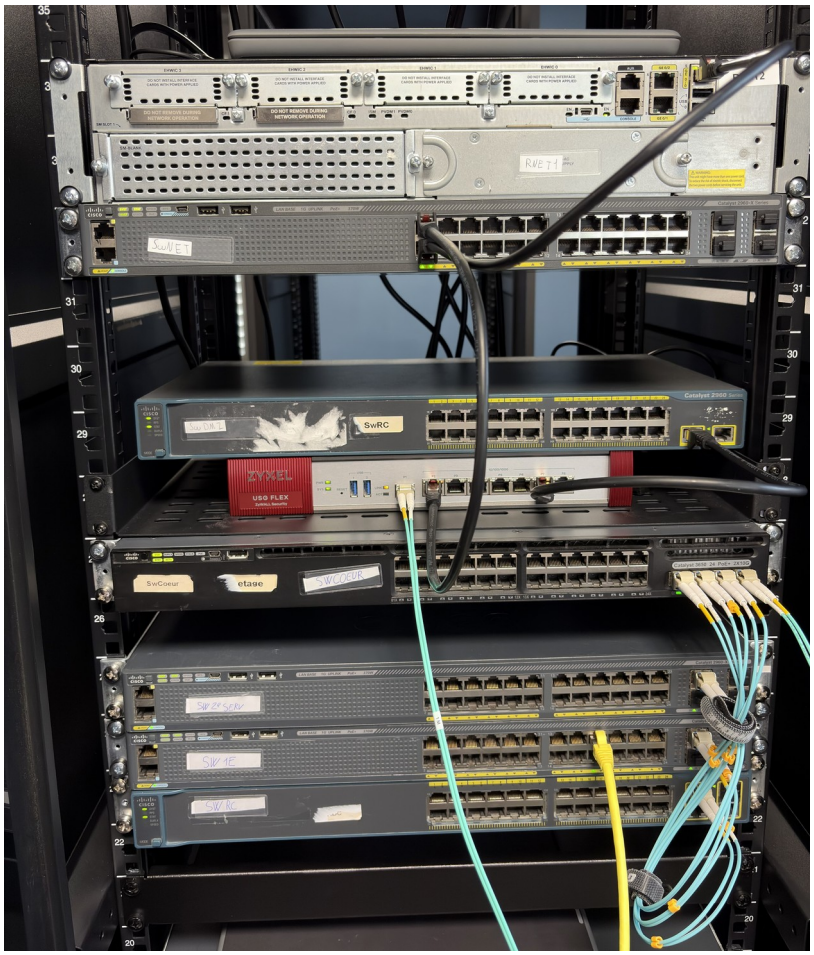

Figure 8 – Installation en baie

Le port Gi1/0/2 de SwNET est placé dans le VLAN 91 pour la liaison vers RNET1. Le détail du brassage figure sur le schéma réseau.

Activité 6 – Routage RIPv2 et routes par défaut

Organiser le routage de bout en bout

Préparer les interfaces avant RIP

Avant de mettre en place le routage, chaque interface de liaison reçoit son adresse et son masque : VLAN 90 entre le cœur et le Zyxel, 192.168.3.248/29 entre le Zyxel, SwNET et RNET1, et 10.5.0.0/16 pour la DMZ. SwNET et SwDMZ reçoivent une passerelle par défaut pour leur propre trafic de gestion.

Routage interne et route de sortie

SwCoeur connaît directement ses VLAN. RIPv2 permet aux équipements de routage d’apprendre les réseaux situés au-delà de leurs liaisons. Les routes par défaut donnent ensuite le chemin vers Internet : cœur vers Zyxel, Zyxel vers RNET1 et RNET1 vers le routeur du campus.

Appliquer les configurations aux bons équipements

RIPv2 est configuré sur SwCoeur, RNET1 et le Zyxel. SwNET et SwDMZ restent des commutateurs de zone.

Sortie vers le campus

Sur RNET1, l'interface Gi0/1 vers le campus est déclarée passive pour ne pas envoyer d'annonces RIP vers le réseau du labo. Elle est adressée en 192.168.4.51/24.

Étape 1 – Configurer SwCoeur

Le cœur annonce les réseaux du LAN en RIPv2, sans sommation automatique. La route par défaut utilise le Zyxel, 172.21.90.253, sur la liaison VLAN 90 en 172.21.90.252/30.

```
router rip
 version 2
 no auto-summary
 network 172.21.0.0
exit
ip route 0.0.0.0 0.0.0.0 172.21.90.253
```

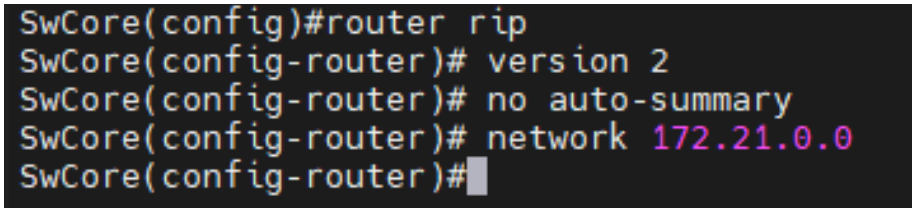

Figure 9 – RIPv2 sur SwCoeur

Étape 2 – Configurer RNET1

RNET1 annonce les réseaux 192.168.3.0 et 192.168.4.0. Gi0/1 est passive pour ne pas envoyer les annonces RIP vers le campus. La route par défaut vise 192.168.4.254.

```
router rip
 version 2
 no auto-summary
 network 192.168.3.0
 network 192.168.4.0
 passive-interface GigabitEthernet0/1
exit
ip route 0.0.0.0 0.0.0.0 192.168.4.254
```

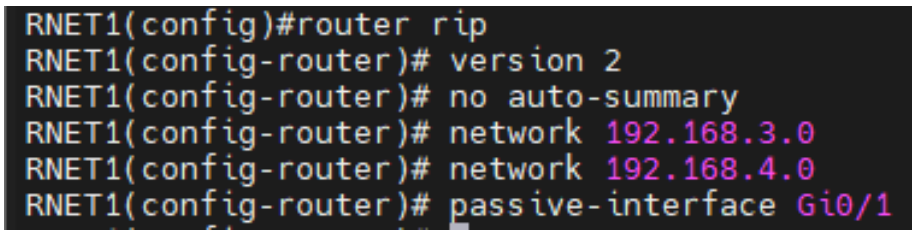

Figure 10 – RIPv2 sur RNET1

Étape 3 – Adresser le pare-feu

Configurer les trois interfaces du pare-feu et sa route par défaut vers RNET1.

Interface Zyxel	Adresse	Rôle
SFP	172.21.90.253/30	Liaison au cœur 172.21.90.254
WAN1	192.168.3.253/29	Transit vers RNET1 192.168.3.252

Interface Zyxel	Adresse	Rôle
DMZ	10.5.10.254/16	Passerelle de la DMZ

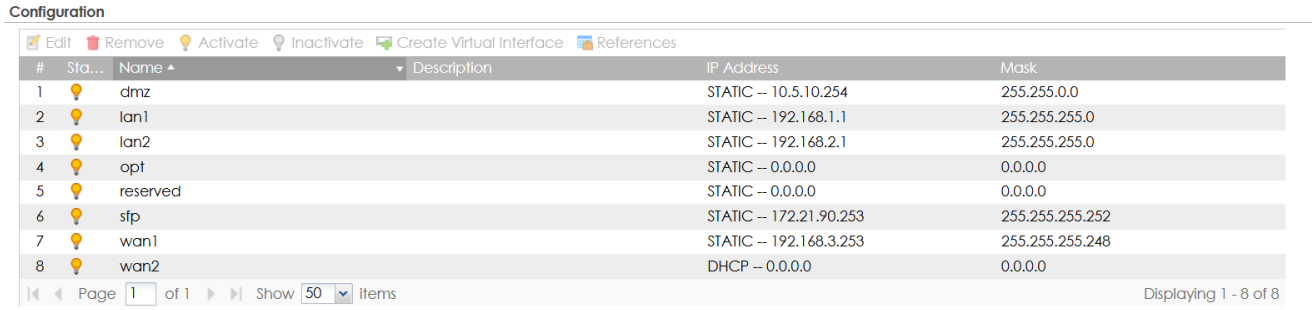

Figure 11 – Interfaces du Zyxel

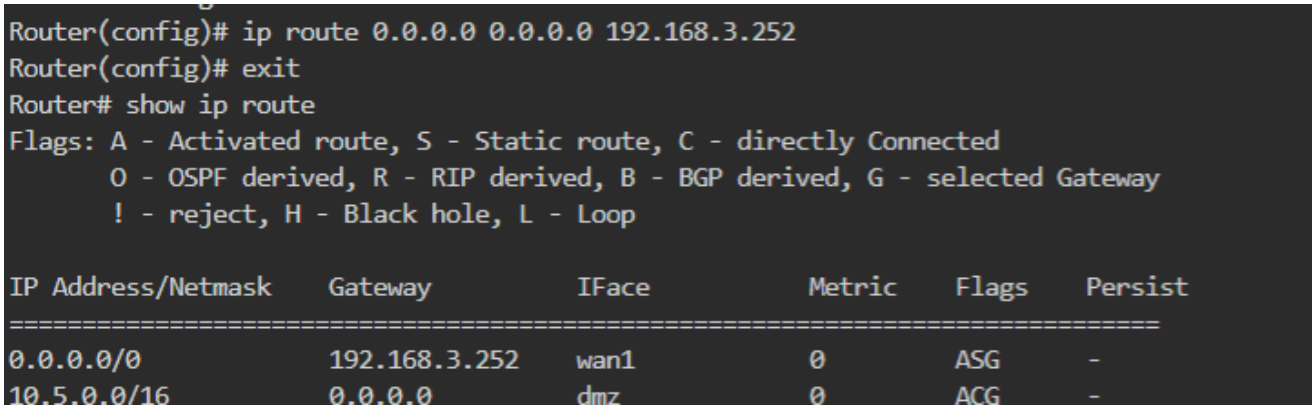

Figure 12 – Route par défaut du Zyxel

RIPv2 est activé sur les interfaces du Zyxel reliées au cœur et au transit.

Étape 4 – Définir la gestion des commutateurs externes

SwNET utilise 192.168.3.251/29 et la passerelle 192.168.3.253. SwDMZ utilise 10.5.10.253/16 sur le VLAN 92 et la passerelle 10.5.10.254.

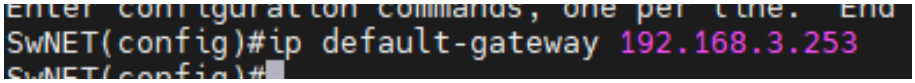

Figure 13 – Passerelle de SwNET

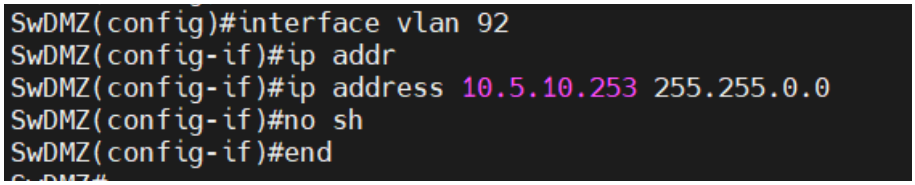

Figure 14 – Gestion de SwDMZ

Route statique vers la DMZ

RNET1 dispose d’une route statique vers le réseau DMZ 10.5.0.0/16 par le Zyxel (192.168.3.253). Elle permet le retour vers le serveur 10.5.10.1 publié par NAT statique.

```
ip route 10.5.0.0 255.255.0.0 192.168.3.253
```

Activité 7 – Serveur TFTP et sauvegardes

Principe de la sauvegarde

Configurer le serveur avant les équipements

Le serveur Ubuntu reçoit une adresse fixe dans le VLAN 100, avec la passerelle du VLAN et le DNS de l'AD. L'installation du paquet TFTP nécessite un accès Internet ; elle a donc été réalisée après la mise en place du NAT/PAT.

Distinguer les deux sauvegardes Cisco

write memory enregistre la configuration sur l'équipement pour le redémarrage. La copie TFTP crée en plus une sauvegarde externe, stockée sur le serveur Ubuntu.

Associer politique et occurrences

La policy-list BACKUP_TFTP contient la commande de copie. Chaque occurrence définit un horaire et appelle cette politique. L'ensemble est appliqué sur chaque équipement Cisco, puis enregistré.

Horloge et calendrier

La date et l'heure des équipements sont réglées avant la mise en service du planning. Les sauvegardes sont programmées le mardi et le jeudi à 17 h 30, et le vendredi à 12 h 30, comme demandé dans la lettre de mission.

Sauvegarde du Zyxel

Le pare-feu Zyxel n'utilise pas Kron : il dispose de son propre mécanisme de sauvegarde planifiée.

Étape 1 – Préparer la VM Ubuntu

Attribuer 172.21.100.3/24 à la VM, 172.21.100.254 comme passerelle et 172.21.100.2 comme DNS. Le serveur appartient au VLAN 100, avec l'AD et l'hôte Hyper-V.

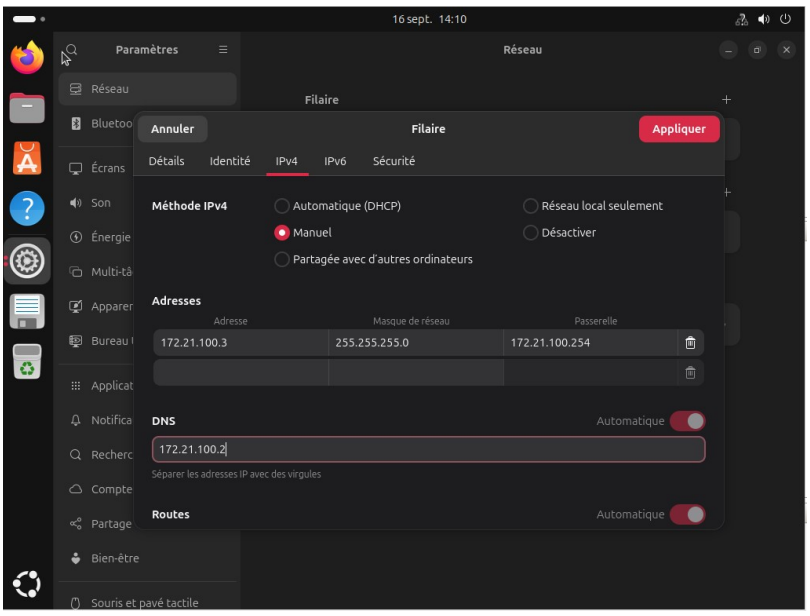

Figure 15 – Adressage du serveur TFTP

Étape 2 – Installer le service TFTP

Installer le service tftpd-hpa.

```
sudo apt install tftpd-hpa
```

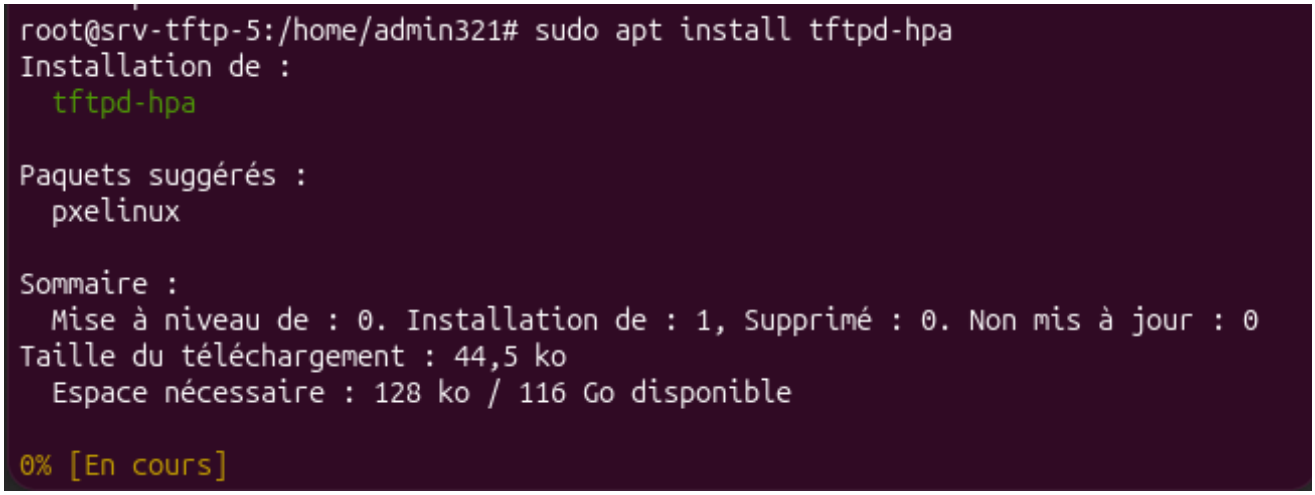

Figure 16 – Installation de tftpd-hpa

Répertoire de réception et options du service

Le service tftpd-hpa utilise /srv/tftp comme racine. Le sous-dossier /srv/tftp/backups est créé pour ranger les sauvegardes, et le compte tftp devient propriétaire du dossier.

```
sudo mkdir -p /srv/tftp/backups
sudo chown -R tftp:tftp /srv/tftp
```

Dans /etc/default/tftpd-hpa, les paramètres utilisés sont les suivants. L'option --create autorise la création de nouveaux fichiers et --secure limite le service à son dossier racine.

```
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure --create -l"
sudo systemctl restart tftpd-hpa
```

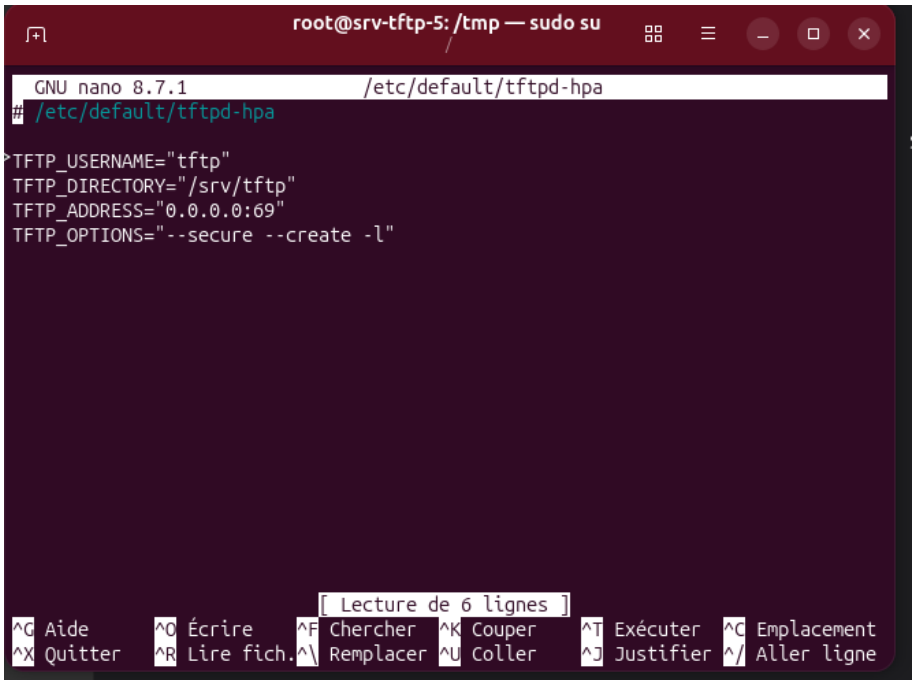

Figure 17 – Racine et options du service tftpd-hpa

Étape 3 – Créer la politique Kron

La politique BACKUP_TFTP copie la configuration active vers le serveur 172.21.100.3.

```
kron policy-list BACKUP_TFTP
 cli copy running-config tftp://172.21.100.3/$(hostname)-$(date).cfg
exit
```

```
Sw1E(config)#kron policy-list BACKUP_TFTP
Sw1E(config-kron-policy)# cli copy running-config tftp://172.21.100.3/$(hostname)-$(date).cfg
Sw1E(config-kron-policy)# exit
```

Figure 18 – Politique BACKUP_TFTP

Étape 4 – Définir les trois occurrences

Programmer BACKUP_MAR le mardi à 17 h 30, BACKUP_JEU le jeudi à 17 h 30 et BACKUP_VEN le vendredi à 12 h 30. Chaque occurrence appelle BACKUP_TFTP, puis la configuration est enregistrée avec write memory.

```
Sw1E(config)#kron occurrence BACKUP_MAR at 17:30 Tue recurring
Sw1E(config-kron-occurrence)# policy-list BACKUP_TFTP
Sw1E(config-kron-occurrence)# exit
Sw1E(config)#kron occurrence BACKUP_JEU at 17:30 Thu recurring
Sw1E(config-kron-occurrence)# policy-list BACKUP_TFTP
Sw1E(config-kron-occurrence)# exit
Sw1E(config)#kron occurrence BACKUP_VEN at 12:30 Fri recurring
Sw1E(config-kron-occurrence)# policy-list BACKUP_TFTP
Sw1E(config-kron-occurrence)# exit
Sw1E(config)#end
Sw1E#write memory
```

Figure 19 – Occurrences hebdomadaires

```
Sw1E#show kron schedule
Kron Occurrence Schedule
BACKUP_MAR inactive, will run again in 6 days 05:35:53 at 17:30 on Tue
BACKUP_JEU inactive, will run again in 1 days 05:35:53 at 17:30 on Thu
BACKUP_VEN inactive, will run again in 2 days 00:35:54 at 12:30 on Fri
```

Figure 20 – Planning Kron de SwE1

La commande show kron schedule permet de vérifier les prochaines exécutions programmées.

BACKUP_TFTP est déployée sur SwCoeur, SwE1, SwE2Serveur et SwRC.

```
SwCore(config)#kron policy-list BACKUP_TFTP
SwCore(config-kron-policy)# cli copy running-config tftp://172.21.100.3/$(hostname)-$(date).cfg
SwCore(config-kron-policy)# exit
SwCore(config)#kron occurrence BACKUP_MAR at 17:30 Tue recurring
Clock currently not set it reads 12:13:45 UTC Wed Sep 30 2026
SwCore(config-kron-occurrence)# policy-list BACKUP_TFTP
SwCore(config-kron-occurrence)# exit
SwCore(config)#kron occurrence BACKUP_JEU at 17:30 Thu recurring
Clock currently not set it reads 12:13:55 UTC Wed Sep 30 2026
SwCore(config-kron-occurrence)# policy-list BACKUP_TFTP
SwCore(config-kron-occurrence)# exit
SwCore(config)#kron occurrence BACKUP_VEN at 12:30 Fri recurring
Clock currently not set it reads 12:14:02 UTC Wed Sep 30 2026
SwCore(config-kron-occurrence)# policy-list BACKUP_TFTP
SwCore(config-kron-occurrence)# exit
SwCore(config)#end
SwCore#write memory
Building configuration...
[OK]
SwCore#show kron
SwCore#show kron sc
SwCore#show kron schedule
Kron Occurrence Schedule
BACKUP_MAR inactive, will run again in 6 days 05:15:31 at 17:30 on Tue
BACKUP_JEU inactive, will run again in 1 days 05:15:31 at 17:30 on Thu
BACKUP_VEN inactive, will run again in 2 days 00:15:31 at 12:30 on Fri
```

Figure 21 – Kron sur SwCoeur

```
Sw2eServ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw2eServ(config)#kron policy-list BACKUP_TFTP
Sw2eServ(config-kron-policy)# cli copy running-config tftp://172.21.100.3/$(hostname)-$(date).cfg
Sw2eServ(config-kron-policy)# exit
Sw2eServ(config)#kron occurrence BACKUP_MAR at 17:30 Tue recurring
Sw2eServ(config-kron-occurrence)# policy-list BACKUP_TFTP
Sw2eServ(config-kron-occurrence)# exit
Sw2eServ(config)#kron occurrence BACKUP_JEU at 17:30 Thu recurring
Sw2eServ(config-kron-occurrence)# policy-list BACKUP_TFTP
Sw2eServ(config-kron-occurrence)# exit
Sw2eServ(config)#kron occurrence BACKUP_VEN at 12:30 Fri recurring
Sw2eServ(config-kron-occurrence)# policy-list BACKUP_TFTP
Sw2eServ(config-kron-occurrence)# exit
Sw2eServ(config)#end
Sw2eServ#write memory
Building configuration...
[OK]
Sw2eServ#sh
Sw2eServ#show kr
Sw2eServ#show kron sc
Sw2eServ#show kron schedule
Kron Occurrence Schedule
BACKUP_MAR inactive, will run again in 3 days 15:43:01 at 17:30 on Tue
BACKUP_JEU inactive, will run again in 5 days 15:43:01 at 17:30 on Thu
BACKUP_VEN inactive, will run again in 6 days 10:43:02 at 12:30 on Fri
```

Figure 22 – Kron sur SwE2Serveur

```
SwRC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SwRC(config)#kron policy-list BACKUP_TFTP
SwRC(config-kron-policy)# cli copy running-config tftp://172.21.100.3/$(hostname)-$(date).cfg
SwRC(config-kron-policy)# exit
SwRC(config)#kron occurrence BACKUP_MAR at 17:30 Tue recurring
Clock currently not set it reads 01:55:24 UTC Mon Mar 1 1993
SwRC(config-kron-occurrence)# policy-list BACKUP_TFTP
SwRC(config-kron-occurrence)# exit
SwRC(config)#kron occurrence BACKUP_JEU at 17:30 Thu recurring
Clock currently not set it reads 01:55:36 UTC Mon Mar 1 1993
SwRC(config-kron-occurrence)# policy-list BACKUP_TFTP
SwRC(config-kron-occurrence)# exit
SwRC(config)#kron occurrence BACKUP_VEN at 12:30 Fri recurring
Clock currently not set it reads 01:55:43 UTC Mon Mar 1 1993
SwRC(config-kron-occurrence)# policy-list BACKUP_TFTP
SwRC(config-kron-occurrence)# exit
SwRC(config)#end
SwRC#write memory
Building configuration...
[OK]
SwRC#show kron schedule
Kron Occurrence Schedule
BACKUP_MAR inactive, will run again in 1 days 15:33:55 at 17:30 on Tue
BACKUP_JEU inactive, will run again in 3 days 15:33:54 at 17:30 on Thu
BACKUP_VEN inactive, will run again in 4 days 10:33:54 at 12:30 on Fri
```

Figure 23 – Kron sur SwRC

L’horloge de chaque équipement doit être à l’heure pour que les sauvegardes partent aux bons horaires.

```
SwDMZ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SwDMZ(config)#kron policy-list BACKUP_TFTP
SwDMZ(config-kron-policy)# cli copy running-config tftp://172.21.100.3/$(hostname)-$(date).cfg
SwDMZ(config-kron-policy)# exit
SwDMZ(config)#kron occurrence BACKUP_MAR at 17:30 Tue recurring
Clock currently not set it reads 01:52:09 UTC Mon Mar 1 1993
SwDMZ(config-kron-occurrence)# policy-list BACKUP_TFTP
SwDMZ(config-kron-occurrence)# exit
SwDMZ(config)#kron occurrence BACKUP_JEU at 17:30 Thu recurring
Clock currently not set it reads 01:52:21 UTC Mon Mar 1 1993
SwDMZ(config-kron-occurrence)# policy-list BACKUP_TFTP
SwDMZ(config-kron-occurrence)# exit
SwDMZ(config)#kron occurrence BACKUP_VEN at 12:30 Fri recurring
Clock currently not set it reads 01:52:36 UTC Mon Mar 1 1993
SwDMZ(config-kron-occurrence)# policy-list BACKUP_TFTP
SwDMZ(config-kron-occurrence)# exit
SwDMZ(config)#end
SwDMZ#write memory
Building configuration...
[OK]
SwDMZ#show kr
SwDMZ#show kron sch
SwDMZ#show kron schedule
Kron Occurrence Schedule
BACKUP_MAR inactive, will run again in 1 days 15:37:12 at 17:30 on Tue
BACKUP_JEU inactive, will run again in 3 days 15:37:24 at 17:30 on Thu
BACKUP_VEN inactive, will run again in 4 days 10:37:40 at 12:30 on Fri
```

Figure 24 – Kron sur SwDMZ

```
SwNET#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SwNET(config)#kron policy-list BACKUP_TFTP
SwNET(config-kron-policy)# cli copy running-config tftp://172.21.100.3/$(hostname)-$(date).cfg
SwNET(config-kron-policy)# exit
SwNET(config)#kron occurrence BACKUP_MAR at 17:30 Tue recurring
SwNET(config-kron-occurrence)# policy-list BACKUP_TFTP
SwNET(config-kron-occurrence)# exit
SwNET(config)#kron occurrence BACKUP_JEU at 17:30 Thu recurring
SwNET(config-kron-occurrence)# policy-list BACKUP_TFTP
SwNET(config-kron-occurrence)# exit
SwNET(config)#kron occurrence BACKUP_VEN at 12:30 Fri recurring
SwNET(config-kron-occurrence)# policy-list BACKUP_TFTP
SwNET(config-kron-occurrence)# exit
SwNET(config)#end
SwNET#write memory
Building configuration...
[OK]
SwNET#show kro
SwNET#show kron sc
SwNET#show kron schedule
Kron Occurrence Schedule
BACKUP_MAR inactive, will run again in 3 days 15:33:53 at 17:30 on Tue
BACKUP_JEU inactive, will run again in 5 days 15:33:53 at 17:30 on Thu
BACKUP_VEN inactive, will run again in 6 days 10:33:53 at 12:30 on Fri
```

Figure 25 – Kron sur SwNET

```
RNET1#show kron schedule
Kron Occurrence Schedule
BACKUP_MAR inactive, will run again in 6 days 04:31:45 at 17:30 on Tue
BACKUP_JEU inactive, will run again in 1 days 04:31:44 at 17:30 on Thu
BACKUP_VEN inactive, will run again in 1 days 23:31:44 at 12:30 on Fri
BACKUP_MER inactive, will run again in 0 days 01:31:45 at 14:30 on Wed
```

Figure 26 – Planning Kron de RNET1

La politique est également déployée sur SwDMZ, SwNET et RNET1. Le pare-feu autorise ces trois équipements à joindre le serveur TFTP (règle Save_TFTP, activité 9).

Étape 5 – Sauvegarder le pare-feu séparément

Le Zyxel utilise son mécanisme de sauvegarde natif, programmé le 31 de chaque mois à 17 h 25.

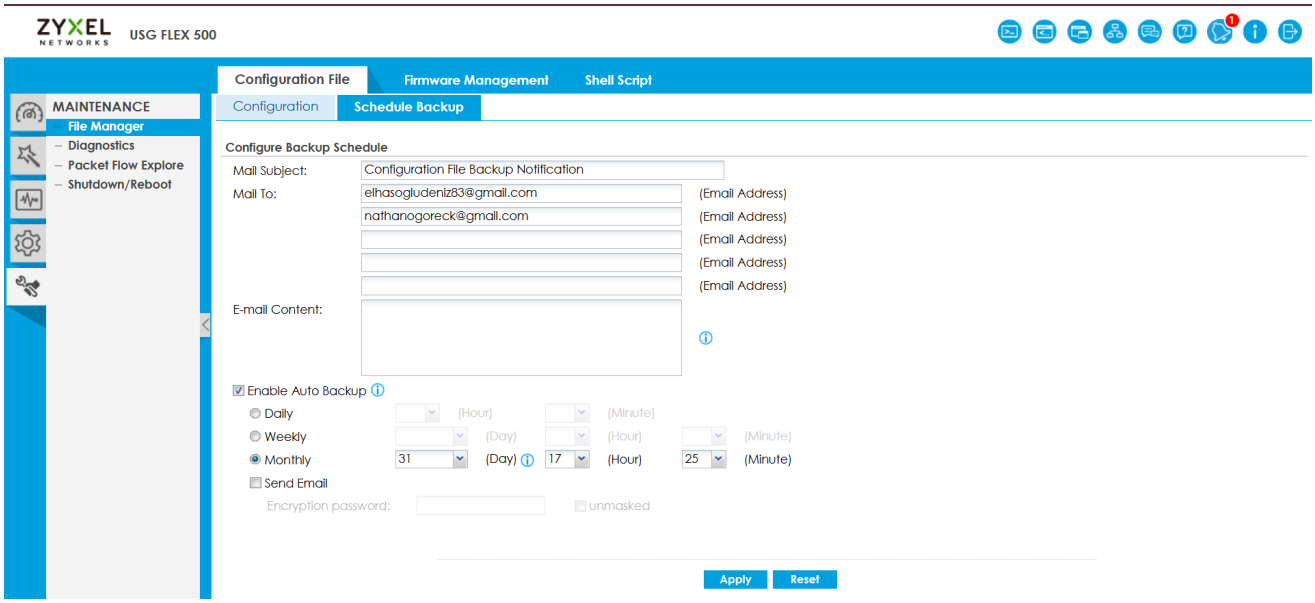

Figure 27 – Sauvegarde native du Zyxel

Activité 8 – NAT/PAT et NAT statique

Interfaces et sélection des sources

RNET1 réalise la traduction d'adresses entre le réseau de transit 192.168.3.248/29 et le campus. Gi0/0 est l'interface inside et Gi0/1 l'interface outside. L'ACL 1 sélectionne les adresses sources à traduire.

```
interface GigabitEthernet0/0
 ip nat inside
exit
interface GigabitEthernet0/1
 ip nat outside
exit
```

Pool final et surcharge

Le pool NAT-POOL1 couvre les adresses 192.168.4.52 à 192.168.4.58. L'option overload permet à tous les postes du LAN 172.21.0.0/16 de partager ces adresses pour sortir sur Internet.

```
ip nat pool NAT-POOL1 192.168.4.52 192.168.4.58 netmask 255.255.255.0
access-list 1 permit 172.21.0.0 0.0.255.255
ip nat inside source list 1 pool NAT-POOL1 overload
ip route 0.0.0.0 0.0.0.0 192.168.4.254
```

Publication statique du serveur DMZ

La traduction statique associe le serveur DMZ 10.5.10.1 à l'adresse 192.168.4.59, en dehors du pool dynamique. Les services réellement accessibles sont limités par les règles du pare-feu. Le retour vers la DMZ utilise la route statique décrite dans l'activité 6.

```
ip nat inside source static 10.5.10.1 192.168.4.59
```

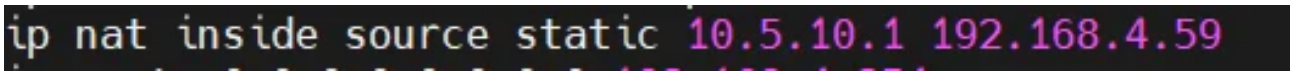

Figure 28 – Commande NAT statique appliquée sur RNET1

Les tests de traduction et de joignabilité sont présentés dans le rapport de tests.

Activité 9 – Politique finale du pare-feu

Zones et sens de circulation

L’interface sfp, reliée au cœur, a été placée dans sa propre zone SFP au lieu de la zone LAN1. Les flux sortant du LAN utilisent donc From = SFP et les flux destinés au LAN utilisent To = SFP. Le transit vers RNET1 appartient à la zone WAN et les serveurs exposés à la zone DMZ. ZyWALL désigne le pare-feu lui-même.



Figure 29 – Zones finales du Zyxel avec la zone SFP indépendante

Objets réseau corrigés

Un équipement précis est déclaré en objet HOST, un réseau en objet SUBNET.

Objet	Type	Adresse
RNET_1	HOST	192.168.3.252
SWCORE	HOST	172.21.90.254
SWNET	HOST	192.168.3.251
SWDMZ	HOST	10.5.10.253
TFTP_SERVEUR	HOST	172.21.100.3
WEB_DMZ	HOST	10.5.10.1
LAN_ALL	SUBNET	172.21.0.0/16
Vlan60_IT	SUBNET	172.21.60.0/24
DMZ_NET	SUBNET	10.5.0.0/16
NET_TRANSIT	SUBNET	192.168.3.248/29

IPv4 Address Configuration

Add Edit Remove References

#	Name	Type	IPv4 Address	Reference
1	DMZ_NET	SUBNET	10.5.0.0/16	1
2	DMZ_SUBNET	INTERFACE SUBNET	dmz-10.5.0.0/16	0
3	IP6to4-Relay	HOST	192.88.99.1	0
4	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24	0
5	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24	0
6	LAN_ALL	SUBNET	172.21.0.0/16	2
7	NET_TRANSIT	SUBNET	192.168.3.248/29	0
8	RFC1918_1	SUBNET	10.0.0.0/8	1
9	RFC1918_2	SUBNET	172.16.0.0/12	1
10	RFC1918_3	SUBNET	192.168.0.0/16	1
11	RNET_1	HOST	192.168.3.252	3
12	SWCORE	HOST	172.21.90.254	1
13	SWDMZ	HOST	10.5.10.253	2
14	SWNET	HOST	192.168.3.251	2
15	TFTP_SERVEUR	HOST	172.21.100.3	1
16	Vlan60_IT	SUBNET	172.21.60.0/24	3
17	WEB_DMZ	HOST	10.5.10.1	2

Page 1 of 1 Show 50 items Displaying 1 - 17 of 17

Figure 30 – Objets corrigés retenus pour la configuration finale

Services et groupes

IT_ADMIN regroupe les services d'administration et WEB_SERVICES les services Web. Le groupe Equipement liste les équipements administrables depuis IT et EQUIP_BAK les équipements autorisés à envoyer leurs sauvegardes au TFTP.

Services SSH et WEB_SERVICES

17		SSH	1
18		WEB_SERVICES	2

Groupe IT_ADMIN

11		IT_ADMIN	1

Ordre des règles finales

Les onze règles du projet sont placées en tête de la politique, avant les règles par défaut du Zyxel. Les autorisations sont journalisées.

Ordre et règle	Zones	Source	Destination	Service	Action
1 IT_TO_DMZ_Admin	SFP → DMZ	Vlan60_IT	SWDMZ	IT_ADMIN	Autoriser
2 IT_TO_WAN_Admin	SFP → WAN	Vlan60_IT	Equipement	IT_ADMIN	Autoriser
3 IT_to_device	SFP → ZyWALL	Vlan60_IT	any	IT_ADMIN	Autoriser
4 CORE_RIP_TO_DEVICE	SFP → ZyWALL	SWCORE	any	RIP	Autoriser
5 RNET_RIP_TO_DEVICE	WAN → ZyWALL	RNET_1	any	RIP	Autoriser
6 Save_TFTP	any → SFP	EQUIP_BAK	TFTP_SERVEUR	TFTP	Autoriser
7 LAN_TO_WAN	SFP → WAN	LAN_ALL	any	any	Autoriser
8 WAN_TO_DMZ_WEB	WAN → DMZ	any	WEB_DMZ	WEB_SERVICES	Autoriser
9 LAN_TO_DMZ_WEB	SFP → DMZ	LAN_ALL	WEB_DMZ	WEB_SERVICES	Autoriser
10 DMZ_TO_WAN	DMZ → WAN	DMZ_NET	any	any	Autoriser
11 Isolation_DMZ_LAN	DMZ → SFP	any	any	any	Refuser

1	IT_TO_DMZ_Admin	SFP	DMZ	Vlan60_IT	SWDMZ	IT_ADMIN	any	any	n...	al...	log
2	IT_TO_WAN_Admin	SFP	WAN	Vlan60_IT	Equipement_...	IT_ADMIN	any	any	n...	al...	log
3	IT_to_device	SFP	ZyWALL	Vlan60_IT	any	IT_ADMIN	any	any	n...	al...	log
4	CORE_RIP_TO_DEVICE	SFP	ZyWALL	SWCORE	any	RIP	any	any	n...	al...	log
5	RNET_RIP_TO_DEVICE	WAN	ZyWALL	RNET_1	any	RIP	any	any	n...	al...	log
6	Save_TFTP	any	SFP	EQUIP_BAK	TFTP_SERVEUR	TFTP	any	any	n...	al...	log
7	LAN_TO_WAN	SFP	WAN	LAN_ALL	any	any	any	any	n...	al...	log
8	WAN_TO_DMZ_WEB	WAN	DMZ	any	WEB_DMZ	WEB_SERVICES	any	any	n...	al...	log
9	LAN_TO_DMZ_WEB	SFP	DMZ	LAN_ALL	WEB_DMZ	WEB_SERVICES	any	any	n...	al...	log
10	DMZ_TO_WAN	DMZ	WAN	DMZ_NET	any	any	any	any	n...	al...	log
11	Isolation_DMZ_LAN	DMZ	SFP	any	any	any	any	any	n...	d...	no
12	LAN1_Outgoing	LAN1	any (E...	any	any	any	any	any	n...	al...	no
13	LAN2_Outgoing	LAN2	any (E...	any	any	any	any	any	n...	al...	no
14	DMZ_to_WAN	DMZ	WAN	any	any	any	any	any	n...	al...	no
15	IPSec_VPN_Outgoing	IPSec_VPN	any (E...	any	any	any	any	any	n...	al...	no
16	SSL_VPN_Outgoing	SSL_VPN	any (E...	any	any	any	any	any	n...	al...	no
17	TUNNEL_Outgoing	TUNNEL	any (E...	any	any	any	any	any	n...	al...	no
18	LAN1_to_Device	LAN1	ZyWALL	any	any	any	any	any	n...	al...	no
19	LAN2_to_Device	LAN2	ZyWALL	any	any	any	any	any	n...	al...	no
20	DMZ_to_Device	DMZ	ZyWALL	any	any	Default_Allow_D...	any	any	n...	al...	no
21	WAN_to_Device	WAN	ZyWALL	any	any	Default_Allow_...	any	any	n...	al...	no

Figure 31 – Politique finale avec les règles spécifiques en tête

IT_TO_DMZ_Admin ne donne accès qu'à SwDMZ. LAN_TO_DMZ_WEB et WAN_TO_DMZ_WEB ne donnent accès qu'au serveur WEB_DMZ, avec les services Web uniquement. Isolation_DMZ_LAN bloque les connexions initiées depuis la DMZ vers le LAN.

Après enregistrement, la configuration du Zyxel est exportée. Les tests correspondants figurent dans le rapport de tests.

Activité 10 – ACL des services

Construire le filtrage au niveau du cœur

Séparer administration et trafic utilisateur

SSH-IT contrôle qui peut administrer les équipements. ACL-SERVICES est une ACL étendue appliquée sur les interfaces VLAN du cœur : elle filtre le trafic des services lorsqu'il est routé vers un autre réseau. Deux postes d'un même VLAN communiquent sans passer par le cœur et ne sont donc pas concernés.

Respecter l'ordre des entrées

Les autorisations vers l'AD et pour le DHCP sont placées avant les refus. Viennent ensuite le refus TFTP vers 172.21.100.3, puis le refus du trafic entre réseaux 172.21.0.0/16, et enfin l'autorisation générale. L'ordre est important : une autorisation générale placée en tête rendrait les refus inutiles.

Interfaces concernées

ACL-SERVICES est appliquée en entrée sur les VLAN 10, 20, 30, 40, 50 et 80, c'est-à-dire sur le trafic qui arrive au cœur depuis ces services. Les VLAN 60 (IT, qui garde tous les droits) et 70 (gestion) ne la reçoivent pas.

Portée du filtrage

Le refus inter-services porte sur le LAN 172.21.0.0/16. Le filtrage vers la DMZ 10.5.0.0/16 est assuré par le pare-feu.

Étape 1 – Construire l’ACL

Autoriser l’AD/DNS à 172.21.100.2 et le trafic DHCP nécessaire. Refuser TFTP vers 172.21.100.3 sur le port 69, puis refuser les échanges entre réseaux de services avant de terminer par une autorisation générale pour les autres destinations.

ACL :

▼ 🔐 **1. ACL-SERVICES — SwCœur**

(AD autorisé + TFTP protégé + isolation des services + Internet autorisé)

Plain Text

```
conf t

ip access-list extended ACL-SERVICES

 (AUTORISER ACCES AU SERVEUR AD)
 permit ip 172.21.0.0 0.0.255.255 host 172.21.100.2

 (AUTORISER DHCP)
 permit udp any eq bootpc any eq bootps

 (INTERDIRE TFTP AUX SERVICES)
 deny udp 172.21.0.0 0.0.255.255 host 172.21.100.3 eq 69

 (INTERDIRE COMMUNICATION ENTRE SERVICES)
 deny ip 172.21.0.0 0.0.255.255 172.21.0.0 0.0.255.255

 (AUTORISER LE RESTE VERS EXTERIEUR)
 permit ip 172.21.0.0 0.0.255.255 any
```

```
SwCore(config)#
SwCore(config)#ip access-list extended ACL-SERVICES
SwCore(config-ext-nacl)# permit ip 172.21.0.0 0.0.255.255 host 172.21.10
0.2
SwCore(config-ext-nacl)# permit udp any eq bootpc any eq bootps
SwCore(config-ext-nacl)#$72.21.0.0 0.0.255.255 host 172.21.100.3 eq 69
SwCore(config-ext-nacl)#$2.21.0.0 0.0.255.255 172.21.0.0 0.0.255.255
SwCore(config-ext-nacl)# permit ip any any
SwCore(config-ext-nacl)#exit
SwCore(config)#do wr
Building configuration...
[OK]
SwCore(config)#interface vlan 10
SwCore(config-if)# ip access-group ACL-SERVICES in
SwCore(config-if)#exit
SwCore(config)#
SwCore(config)#interface vlan 20
SwCore(config-if)# ip access-group ACL-SERVICES in
SwCore(config-if)#exit
SwCore(config)#
SwCore(config)#interface vlan 30
SwCore(config-if)# ip access-group ACL-SERVICES in
SwCore(config-if)#exit
SwCore(config)#
SwCore(config)#interface vlan 40
SwCore(config-if)# ip access-group ACL-SERVICES in
SwCore(config-if)#exit
SwCore(config)#
SwCore(config)#interface vlan 50
SwCore(config-if)# ip access-group ACL-SERVICES in
SwCore(config-if)#exit
SwCore(config)#
SwCore(config)#interface vlan 80
SwCore(config-if)# ip access-group ACL-SERVICES in
SwCore(config-if)#exit
```

Figure 32 – ACL des services sur le cœur

Étape 2 – Appliquer ACL-SERVICES en entrée

Associer l'ACL aux interfaces VLAN 10, 20, 30, 40, 50 et 80 du cœur. Les VLAN 60 IT et 70 Gestion ne reçoivent pas cette ACL.

Exemple pour le VLAN 10, à répéter sur les cinq autres interfaces :

```
interface Vlan10
 ip access-group ACL-SERVICES in
exit
```

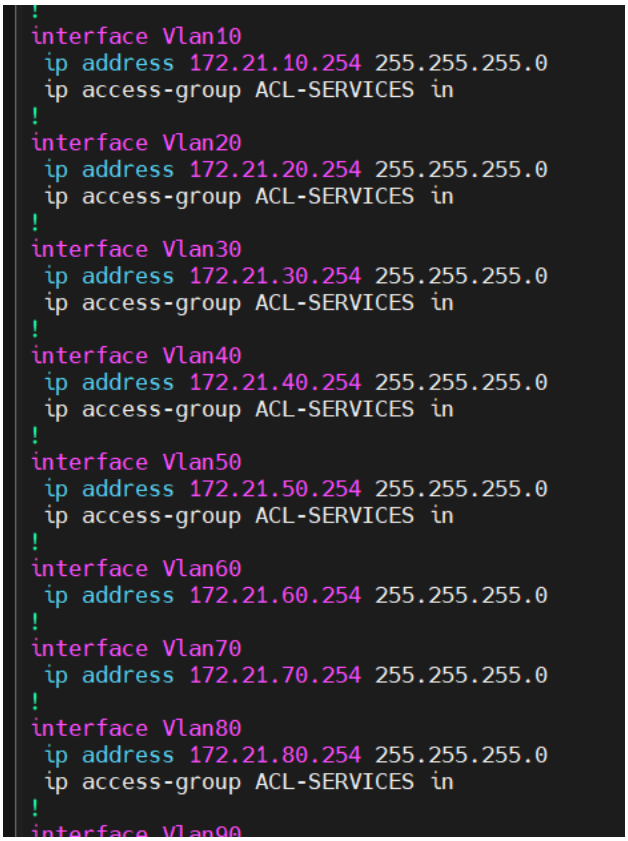

Figure 33 – ACL sur les interfaces VLAN

Le filtrage des accès vers la DMZ est assuré par le pare-feu Zyxel.

Reprise et maintenance de la configuration

Cette partie regroupe les bonnes pratiques à suivre pour reprendre ou faire évoluer l'infrastructure.

Accéder à un équipement sans perdre la main

Se connecter depuis un poste du VLAN IT, sur l'adresse de gestion de l'équipement. Les comptes sont dans le Notion du groupe. En cas de perte de l'accès distant, passer par le câble console avant de modifier les filtres.

Sauvegarder avant toute modification

Exporter la configuration active et conserver une copie datée hors de l'équipement : par TFTP vers 172.21.100.3 pour les Cisco, et par la sauvegarde native pour le Zyxel.

Restaurer une configuration

Utiliser une sauvegarde correspondant au modèle et à la version de l’équipement, et réaliser la restauration pendant une fenêtre de maintenance, avec un accès console disponible.

Sur Cisco, une copie vers running-config fusionne les commandes avec la configuration active : vérifier le résultat avant d’enregistrer. Sur Zyxel, utiliser la restauration native.

Diagnostic des problèmes courants

Symptôme	Contrôles à effectuer
SSH interne impossible	Adresse de gestion propre au commutateur, origine VLAN 60, routage vers VLAN 70, compte local et lignes VTY.
SSH externe impossible depuis IT	Chemin vers les équipements externes, zone SFP indépendante avec membre sfp, règles Zyxel et restriction VTY de la cible.
Équipement de DMZ injoignable	Ports de la liaison DMZ, VLAN 92, masque /16, passerelle SwDMZ et routes de retour.
Routes LAN absentes sur le Zyxel	Liaison SFP, VLAN 90, RIPv2 sur le cœur et règles nécessaires au routage.
Sortie Internet indisponible	Gi1/0/2 de SwNET dans VLAN 91, interfaces RNET1, route de sortie et cohérence WAN avant NAT.
Sauvegarde non reçue	Service et permissions TFTP, filtres réseau, politique Kron, horloge, nom du fichier et éventuelle demande interactive.
Service utilisateur sans AD ou DHCP	Ordre ACL-SERVICES, exceptions nécessaires et interface VLAN réellement concernée.

Bilan du projet

Résultat obtenu

L’infrastructure de LEIDOSCOPE est opérationnelle. Le LAN est cloisonné par services, la DMZ et la liaison vers Internet sont en place, et le routage RIPv2 associé au NAT/PAT permet aux services et aux serveurs de sortir sur Internet. Le serveur de la DMZ est publié vers le campus par NAT statique, l’administration des équipements est réservée au service IT en SSH, et les configurations Cisco sont sauvegardées automatiquement sur le serveur TFTP.

Difficultés rencontrées

Réinitialisation de RNET1. Le routeur s’est réinitialisé en cours de projet : sa configuration et son accès SSH ont dû être refaits.

Adressage des liaisons. Plusieurs interfaces de liaison (SwCoeur, pare-feu, SwNET, SwDMZ et RNET1) n’avaient pas d’adresse IP. Les VLAN de liaison 90, 91 et 92 ont été créés pour corriger l’adressage.

Configuration non enregistrée. Le routage RIP avait disparu de SwCoeur et le port Gi1/0/2 de SwNET n’était plus dans le VLAN 91, ce qui bloquait la sortie vers Internet.

Horloge des équipements. La clé RSA ne pouvait pas être générée tant que l’horloge de l’équipement était incorrecte.

Installation du TFTP. L’installation du paquet nécessitait un accès Internet : elle a été réalisée après la mise en place du NAT/PAT.

Zone SFP du pare-feu. Le passage de l’interface sfp dans une zone dédiée, plus sûre que la zone LAN1, a demandé d’adapter les règles du pare-feu pour rétablir l’accès Internet du LAN.

Suite du projet

Le projet se poursuit avec l’AP2, au cours duquel le nommage des fichiers de sauvegarde TFTP a été revu.

Compétences mobilisées

Configuration d’équipements Cisco (VLAN, routage RIPv2, ACL, NAT/PAT, SSH, Kron), paramétrage d’un pare-feu Zyxel (zones, objets, règles), mise en place d’un serveur Ubuntu (TFTP), et organisation du travail en binôme avec Trello et un diagramme de Gantt.