Épreuve E6 Dossier : Borne WiFi

By Antonin Barateau

Sommaire

1. Présentation Générale du Projet

1.1 Contexte et Objectifs

L'objectif de ce projet est la mise en place d'une infrastructure réseau et système complète, segmentée et sécurisée. Cette maquette simule un environnement d'entreprise intégrant du Wi-Fi, du stockage centralisé avec TrueNas, et une gestion des utilisateurs avec un Active Directory.

1.2 Architecture Réseau

L'infrastructure repose sur une segmentation en 4 réseaux virtuels pour isoler les différents services et types d'utilisateurs :

VLAN	Nom	Adressage	Rôle
15	Utilisateurs	172.19.15.0/24	Accueil des clients Wi-Fi via la borne Netgear. Accès restreint.
25	SI (Admin)	172.19.25.0/24	Zone de gestion et d'hébergement des serveurs critiques (AD, Proxmox,TrueNas, Apache).
35	R&D	172.19.35.0/24	Zone de développement, isolée du Wi-Fi mais ayant accès aux serveurs.
100	Transit	172.19.11.253/30	Lien d'interconnexion entre le Switch L3 et le Firewall pfSense.

1.3 Présentation des Équipements et Services

A. Le Switch Cisco 3750

Il est le garant du routage inter-VLAN. Ses fonctions principales sont :

- **Routage IP** : Permettre (ou interdire) la communication entre les sous-réseaux.
- **Serveur DHCP** : Distribution dynamique des adresses IP pour l'ensemble des VLANs.
- **Filtrage (ACL)** : Application de règles de sécurité strictes en entrée des VLANs pour empêcher les accès non autorisés (ex: bloquer le Wi-Fi vers l'administration).

B. Le Firewall pfSense

Il assure la sécurité périmétrique et le lien avec l'extérieur :

- **Filtrage WAN/LAN/DMZ** : Contrôle des flux entrant et sortant.
- **NAT Outbound** : Traduction d'adresses pour permettre aux réseaux privés d'accéder à Internet.

C. L'Hyperviseur Proxmox et ses VMs

Le serveur Proxmox (172.19.25.200) héberge l'intelligence du système :

- **Windows Server** : Contrôleur de domaine gérant l'annuaire des utilisateurs.
- **TrueNAS** : Solution de stockage réseau jointe au domaine pour le partage de fichiers sécurisés.
- **Apache :** Serveur Apache qui héberge le site web de la DMZ.
- **Clients (Debian/Windows)** : Postes de travail utilisés pour valider le fonctionnement des services et les restrictions de sécurité ainsi que configurer les différents services.

D. Le Point d'Accès Wi-Fi (Netgear)

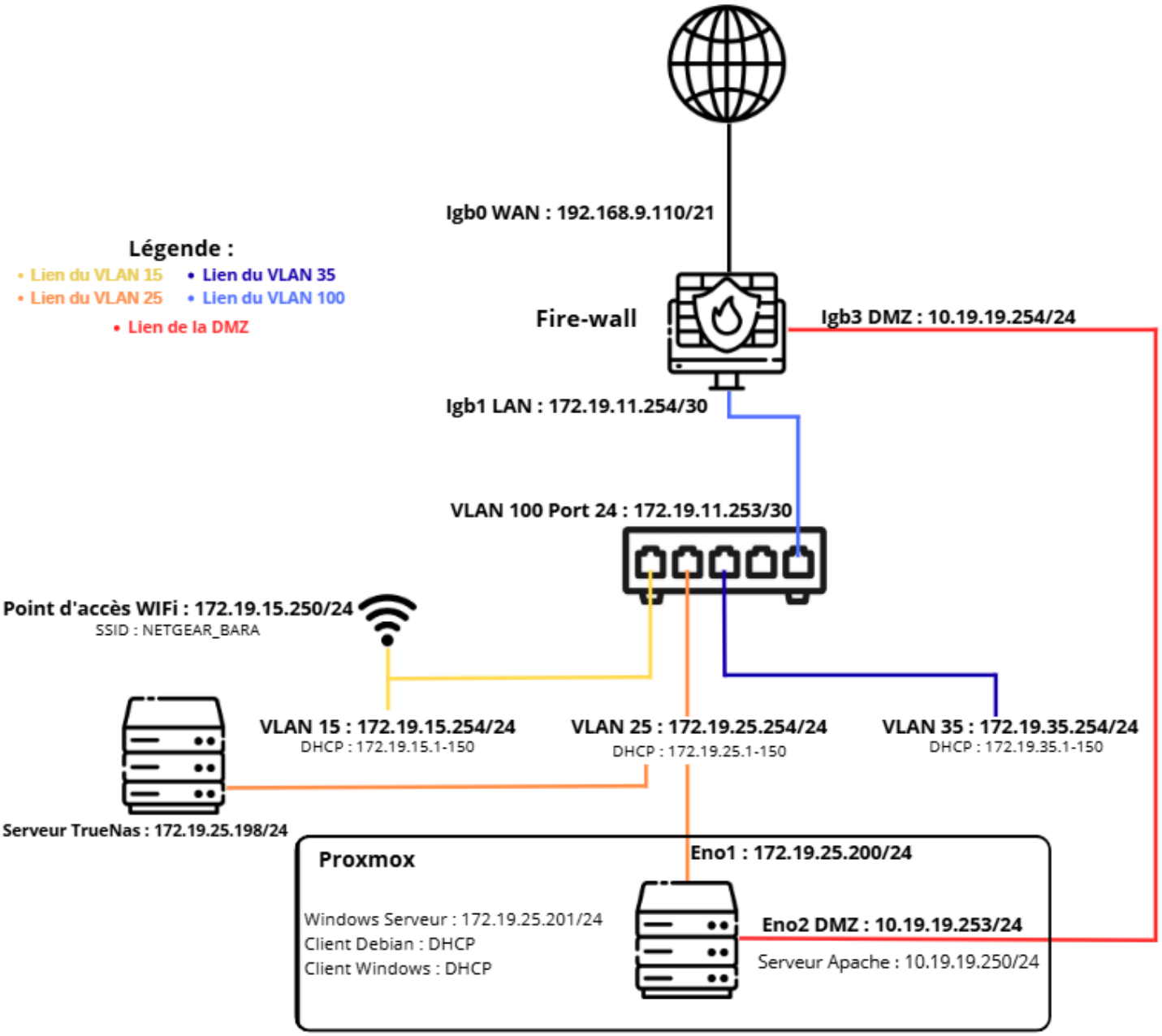
La borne Netgear (172.19.15.250) assure la mobilité. Elle est configurée en mode "Pont" (Bridge), ce qui signifie qu'elle transmet les demandes des clients directement au serveur DHCP du switch Cisco.

1.4 Flux du Switch

Le projet met en œuvre une politique de sécurité dite de "**moindre privilège**" :

- Le **VLAN SI** peut administrer tous les équipements.
- Le **VLAN Utilisateurs** n'a accès qu'à Internet et aux partages spécifiques de TrueNAS.
- Le **VLAN R&D** a accès au serveur du proxmox a internet mais n'a pas d'accès au VLAN Utilisateur

2. Schéma du réseaux



3. Mise en œuvre de l'Infrastructure

Cette étape détaille la configuration des équipements actifs permettant l'interconnexion sécurisée des différents services.

Plan d'adressage

Équipement / Interface	Zone / VLAN	Adresse IP / Masque	Passerelle	Plage DHCP	Rôle / Description
Firewall (Igb0)	WAN	192.168.9.110/21	192.168.10.254	-	Accès Internet
Firewall (Igb1)	Interco LAN	172.19.11.254/30	-	-	Lien vers Switch Port 24
Firewall (Igb3)	DMZ	10.19.19.254/24	-	-	Passerelle par défaut DMZ
Switch (Port 24)	VLAN 100	172.19.11.253/30	-	-	Lien vers Firewall
Switch (VLAN 15)	WiFi	172.19.15.254/24	-	.1 à .150	Passerelle VLAN 15
Switch (VLAN 25)	Serveurs	172.19.25.254/24	-	.1 à .150	Passerelle VLAN 25
Switch (VLAN 35)	Clients	172.19.35.254/24	-	.1 à .150	Passerelle VLAN 35
Point d'accès WiFi	VLAN 15	172.19.15.250/24	172.19.15.254	-	SSID: NETGEAR_BARA
Serveur TrueNAS	VLAN 25	172.19.25.198/24	172.19.25.254	-	Stockage réseau
Proxmox (Eno1)	VLAN 25	172.19.25.200/24	172.19.25.254	-	Interface Management
Proxmox (Eno2)	DMZ	10.19.19.253/24	10.19.19.254	-	Interface Services DMZ
Windows Serveur (VM)	VLAN 25	172.19.25.201/24	172.19.25.254	-	Contrôleur de domaine
Client Debian (VM)	VLAN 25	DHCP	172.19.25.254	-	Poste client Linux
Client Windows (VM)	VLAN 25	DHCP	172.19.25.254	-	Poste client Windows
Serveur Apache (VM)	DMZ	10.19.19.250/24	10.19.19.254	-	Serveur Web public

3.1 Switch de Niveau 3

Pour cette maquette, le choix s'est porté sur un switch Cisco 3750, un équipement capable d'opérer au niveau 2 (Liaison) et au niveau 3 (Réseau), il s'occupera du routage dans cette maquette.

Vous pouvez retrouver la configuration complète du Switch en annexe.

3.2 Configuration du Switch Cisco

Le switch est configuré sur trois axes majeurs : la segmentation, la distribution d'adressage et le filtrage.

A. Segmentation par VLANs et Routage

Chaque service est isolé dans son propre VLAN. Le routage est activé via la commande ip routing. Des interfaces virtuelles (SVI) servent de passerelles pour chaque réseau :

- VLAN 15 : Utilisateur, Sert pour les Utilisateur lambda
- VLAN 25 : SI, Sert pour les serveur
- VLAN 35 : R&D, Sert pour la Recherche et Développement a accès au différents service du Proxmox.
- VLAN 100 : Réseau de transit dédié à la liaison avec le pfSense.

B. Serveur DHCP Centralisé

Pour simplifier l'administration, le switch fait office de serveur DHCP. Il est capable d'identifier de quel VLAN provient une requête "DHCP Discover" et de puiser dans le "pool" d'adresses correspondant au VLAN demandeur de la requête (plages configurées de .1 à .150).

- Configuration des Plages :

VLAN 15 : 172.19.15.1-150
VLAN 25 : 172.19.25.1-150
VLAN 35 : 172.19.35.1-150

```
ip dhcp pool POOL_UTILISATEURS
   network 172.19.15.0 255.255.255.0
   default-router 172.19.15.254
   dns-server 8.8.8.8 1.1.1.1
!
ip dhcp pool POOL_SI
   network 172.19.25.0 255.255.255.0
   default-router 172.19.25.254
   dns-server 8.8.8.8 1.1.1.1
!
ip dhcp pool POOL_R&D
   network 172.19.35.0 255.255.255.0
   default-router 172.19.35.254
   dns-server 8.8.8.8 1.1.1.1
!
```

C. Sécurisation des flux par ACL et Accès Distant

- **Accès Distant**

Le protocole SSH (Secure Shell) a été activé pour permettre une administration sécurisée depuis le VLAN 25. Les ports inutilisés ont été désactivés pour prévenir toute intrusion physique sur le switch.

Pour la connexion SSH une commande différente doit être utilisée car la debian 12 utilisé pour se connecter est trop “moderne” comparer au switch Cisco 3750.

```
root@debian:~# ssh admin@172.19.25.254
Unable to negotiate with 172.19.25.254 port 22: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1
root@debian:~#
```

Commande à utiliser :
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa -c aes128-cbc admin@172.19.25.254

```
root@debian:~# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa -c aes128-cbc admin@172.19.25.254
(admin@172.19.25.254) Password:
```

- **Sécurisation des flux par ACL**

Le routage inter-VLAN, bien qu'efficace pour la communication, expose l'ensemble des réseaux à des risques de sécurité. Pour pallier cela, j'ai mis en place des ACL (Access Control List).

- **Principe de fonctionnement :**

Les ACL sont lues de haut en bas. Dès qu'une règle correspond au trafic, elle est appliquée et la lecture s'arrête.

A. Le filtrage du VLAN 15 (Utilisateurs Wi-Fi)

C'est le réseau le plus critique car il accueille des différents matériels moins maîtrisés à cause du WIFI. L'objectif est de permettre l'accès aux services nécessaires tout en isolant l'administration.

- **Accès aux services métiers** : Autorisation des flux SMB (port 445) vers TrueNAS
- **Protection de l'infrastructure** : Interdiction stricte d'accéder aux interfaces de gestion (SSH du switch et Web du pfSense sur les ports 22, 80 et 443).
- **Cloisonnement inter-VLAN** : Blocage de tout trafic vers les réseaux SI (VLAN 25) et R&D (VLAN 35).
- **Exception de gestion** : Une règle spécifique autorise la réponse de la borne Wi-Fi (`172.19.15.250`) vers le VLAN 25 pour permettre son administration à distance.
- **Accès Internet** : Une règle `permit ip any any` en fin de liste permet aux utilisateurs de sortir via le pfSense.

```
ip access-list extended ACL_VLAN_15
 permit tcp 172.19.15.0 0.0.0.255 host 172.19.25.201 eq www
 permit tcp 172.19.15.0 0.0.0.255 host 172.19.25.202 eq 445
 deny   tcp 172.19.15.0 0.0.0.255 host 172.19.15.254 eq 22
 deny   tcp 172.19.15.0 0.0.0.255 host 172.19.11.254 eq 443
 deny   tcp 172.19.15.0 0.0.0.255 host 172.19.11.254 eq www
 deny   ip 172.19.15.0 0.0.0.255 172.19.25.0 0.0.0.255
 deny   ip 172.19.15.0 0.0.0.255 172.19.35.0 0.0.0.255
 permit ip host 172.19.15.250 172.19.25.0 0.0.0.255
 permit ip any any
```

B. Le filtrage du VLAN 35 (R&D)

Le réseau R&D doit pouvoir travailler avec les serveurs sans pour autant compromettre la sécurité des autres utilisateurs.

- **Privilège de développement** : Autorisation complète vers le VLAN 25 pour accéder aux ressources de l'hyperviseur Proxmox.
- **Isolation** : Interdiction d'accéder au VLAN 15 (Wi-Fi) pour éviter tout rebond depuis un poste utilisateur vers la zone de recherche.

```
ip access-list extended ACL_VLAN_35
 permit ip 172.19.35.0 0.0.0.255 172.19.25.0 0.0.0.255
 deny   ip 172.19.35.0 0.0.0.255 172.19.15.0 0.0.0.255
 deny   tcp 172.19.35.0 0.0.0.255 host 172.19.35.254 eq 22
 deny   tcp 172.19.35.0 0.0.0.255 host 172.19.11.254 eq 443
 deny   tcp 172.19.35.0 0.0.0.255 host 172.19.11.254 eq www
 permit ip any any
```

C. Le VLAN 25 (Système d'Information)

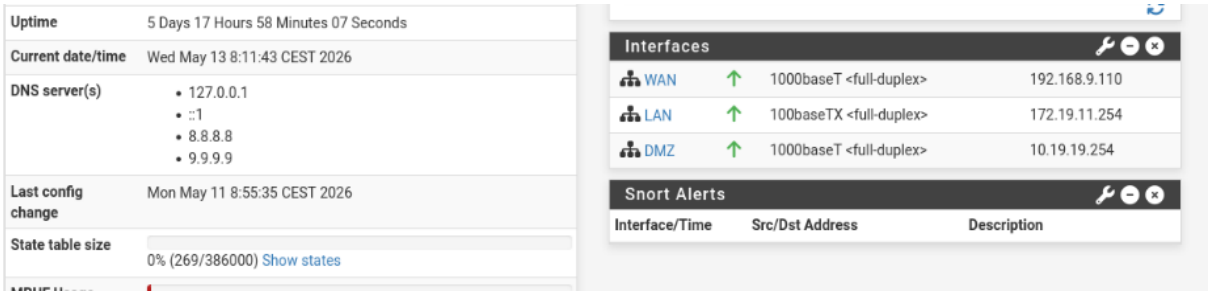
Ce VLAN ne possède pas d'ACL restrictive en entrée. En tant que réseau d'administration, il possède un accès vers tous les autres VLANs. C'est depuis cette zone que s'effectue la maintenance de l'ensemble de la maquette.

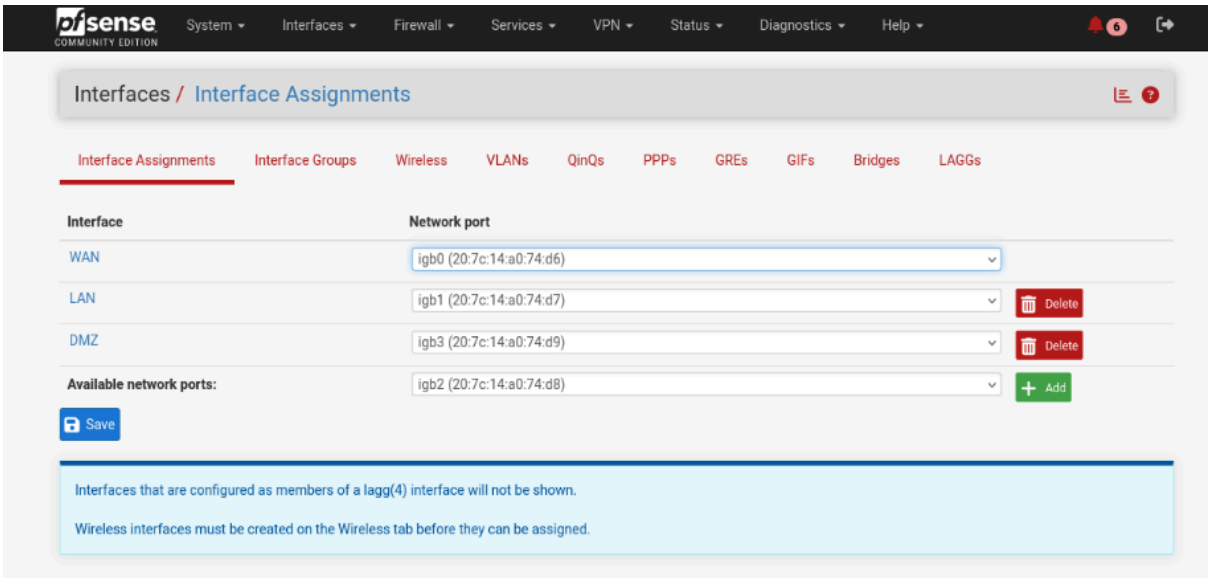
3.3 Configuration du Pare-feu (pfSense)

Le pfSense agit comme la frontière entre l'infrastructure interne et le monde extérieur. Il assure la sécurité des flux.

A. Interfaces et Adressage

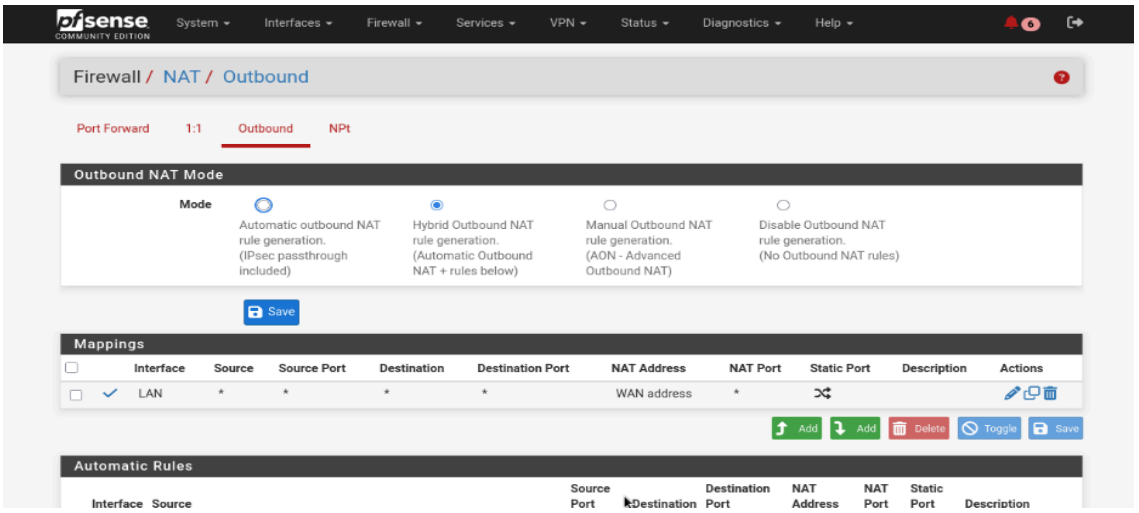
- **WAN (Igb0)** : Interface connectée à la sortie Internet (IP `192.168.9.110`).
- **LAN (Igb1)** : Interface de transit connectée au switch via le VLAN 100. L'IP `172.19.11.254/30` est utilisée ici pour limiter le nombre d'adresses disponibles au strict nécessaire (Switch <-> Firewall).
- **DMZ (Igb3)** : Interface isolée accueillant le serveur Apache (`10.19.19.254`).





B. Routage Statique et NAT

- **Route Statique** : Le pfSense ne connaissant pas physiquement les réseaux 172.19.15.0, 25.0 et 35.0, des routes statiques ont été ajoutées.
- **NAT Outbound** : Pour permettre aux clients internes de naviguer, un NAT a été configuré pour masquer les adresses privées derrière l'adresse publique du pfSense.



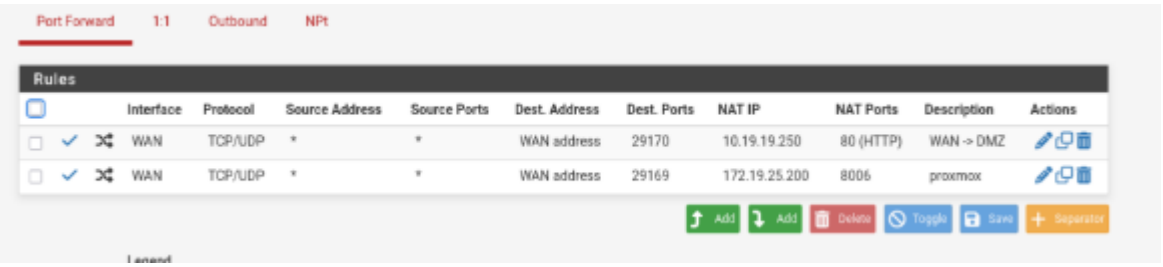
Port Forwarding

1. **Accès à l'Hyperviseur (Proxmox)** :

Comme nous sommes dans une maquette et que l'infrastructure est située derrière un pfSense, j'ai préféré utiliser une redirection de port plutôt que de tirer un câble. Il me suffit donc d'utiliser une VM depuis un poste de travail de la salle, configurée sur le réseau (192.168.9.110/21), et d'appeler l'IP (192.168.9.110:29169) pour accéder à mon Proxmox.

2. **Accès au Serveur Web (Apache en DMZ)** :

Le site de la DMZ devait être visible depuis le WAN. Pour cela, une redirection de port a été mise en place pour que, quand l'adresse du WAN est appelée avec le bon port, cela nous renvoie vers le serveur Apache (192.168.9.110:29170).



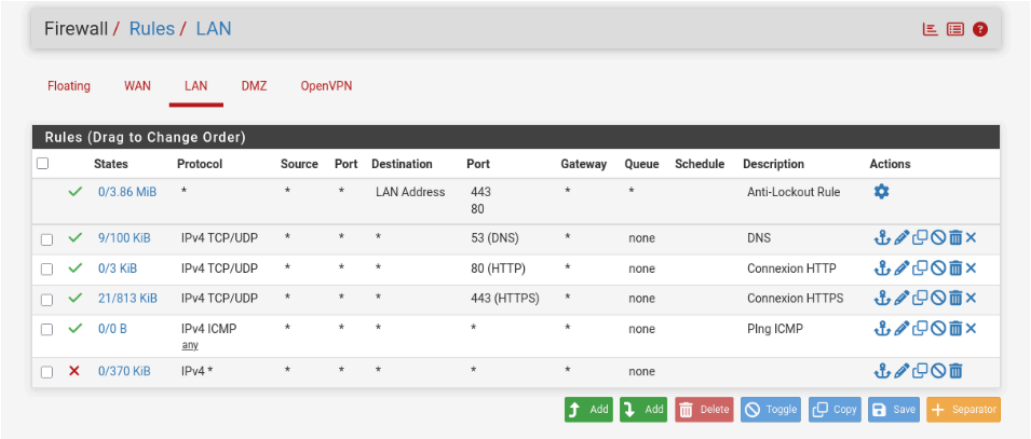
C. Règles de Filtrage

1. Interface LAN

Seuls les flux indispensables sont autorisés vers l'adresse du firewall pour le bon fonctionnement du réseau.

- Autorisation du DNS port 53
- Autorisation de l'HTTP et HTTPS port 80/443
- Autorisation du protocol ICMP pour les ping.

Tout le reste est bloqué.

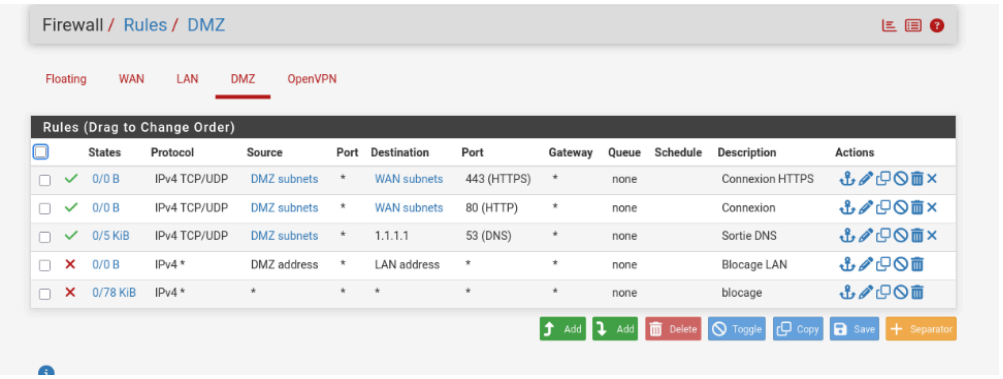


2. Interface DMZ

La DMZ est configurée pour ne jamais initier de connexion vers le LAN. Elle peut répondre aux requêtes externes (Web).

- Autorisation du DNS port 53
- Autorisation de l'HTTP et HTTPS port 80/443
- Refus des requêtes de la DMZ vers le LAN

Tout le reste est bloqué.



3. Interface WAN

Aucune configuration a été faite sur l'interface WAN a par les règles pour le Forwarding créé automatiquement par pfSense.

3.4 L'Hyperviseur Proxmox

A. Installation de Proxmox

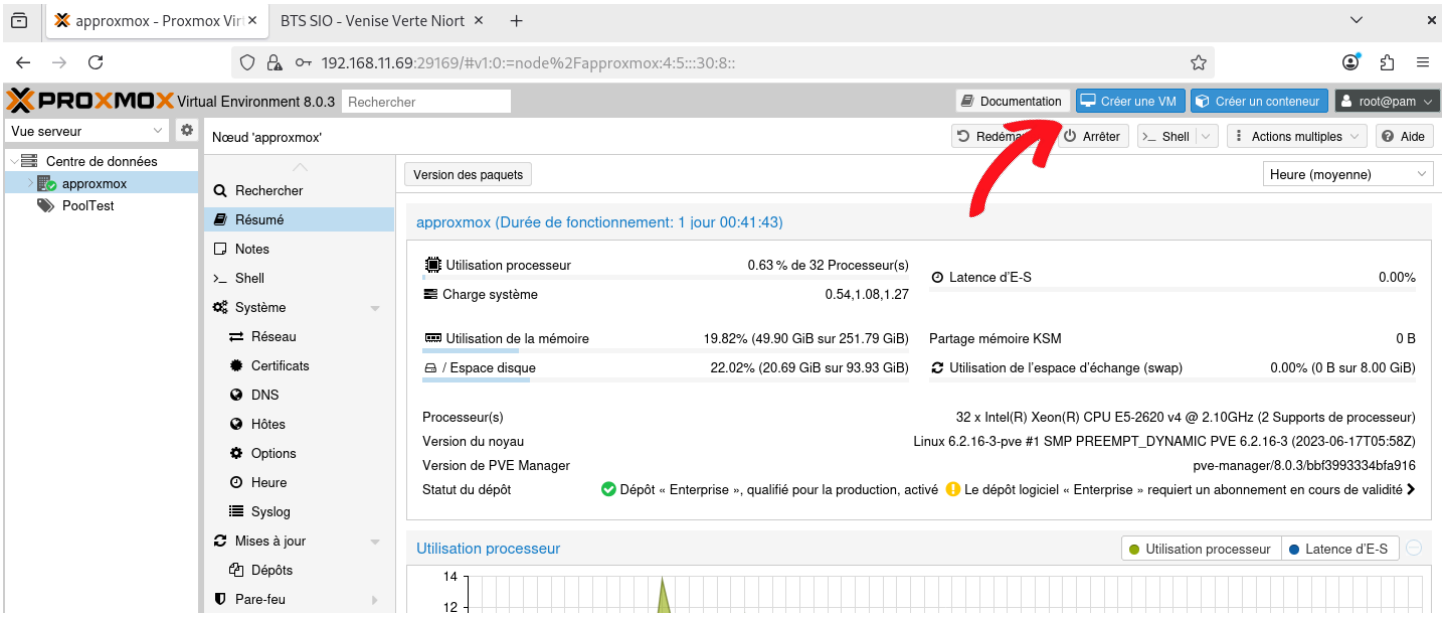
Commencer par télécharger un l'iso de Proxmox pour cela aller sur le site de Proxmox et allez dans la partie downloads. Une fois fait crée une clé bootable avec l'ISO de Proxmox avec le logiciel rufus par exemple.
Après avoir créé la clé vous pouvez la brancher à votre serveur et booter sur cette clé pour installer Proxmox, suivez les étapes d'installation dans notre cas nous allons entrer les informations suivantes durant ce processus.

- Interface : Sélection de la carte réseau principale.
- Hostname : pve-bts.antonin.lan
- IP Address : 172.19.25.200
- Gateway : 172.19.25.254
- DNS : 172.19.25.201

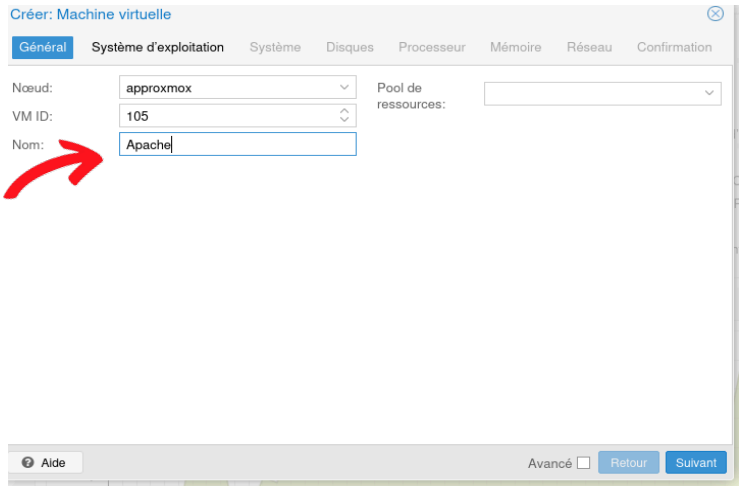
Finalisation : Redémarrage et accès à l'interface Web via http://172.19.25.200:8006

B. Création d'une machine virtuelle

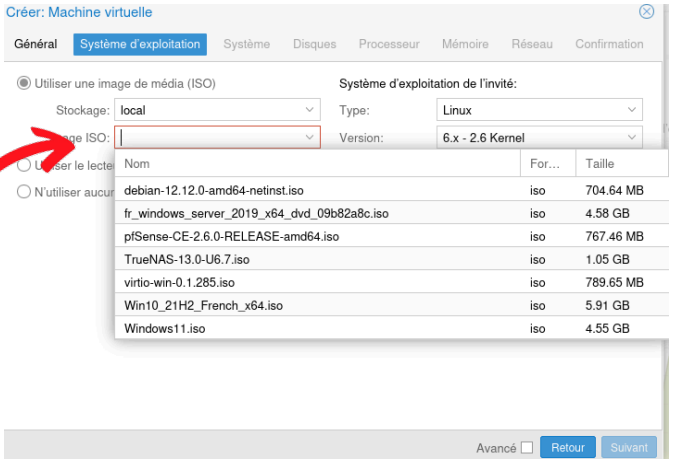
Pour créer une machine virtuelle sur Proxmox, cliquer sur créer une VM.



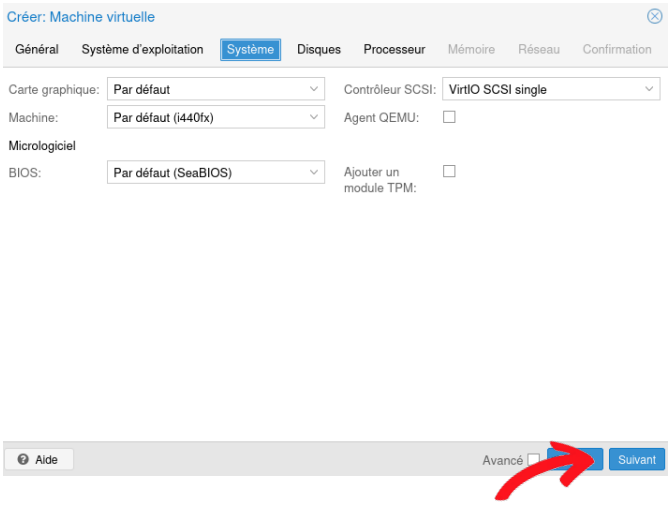
Ensuite nommé votre Vm.



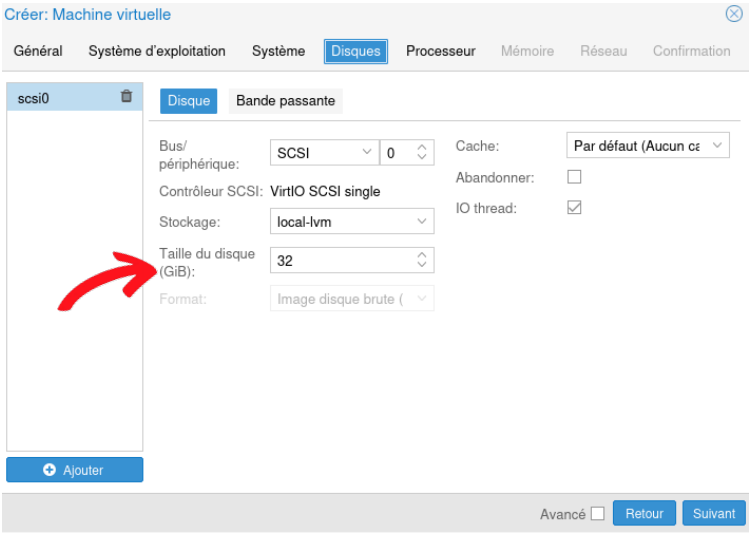
Sélectionner l'image iso que vous souhaitez.



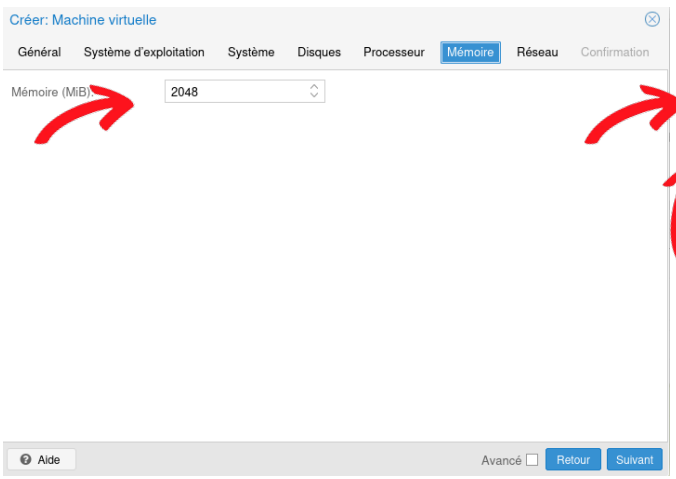
Cliquer sur suivant.

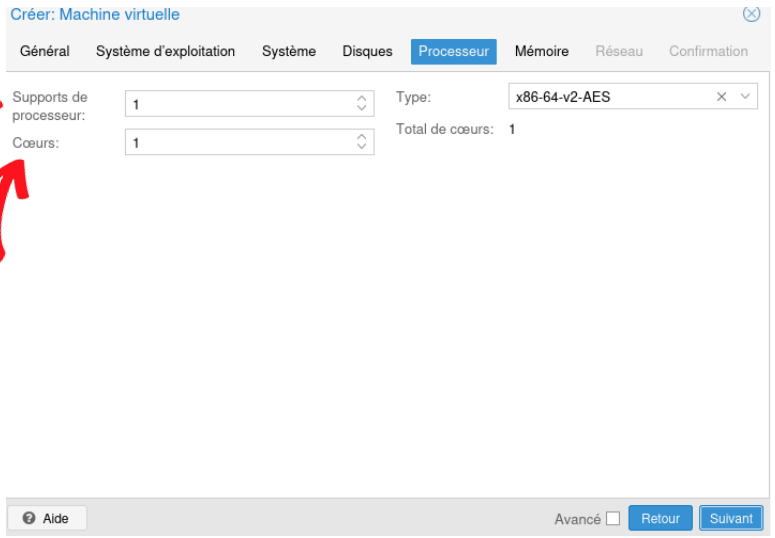


Définissez la taille du disque souhaité.

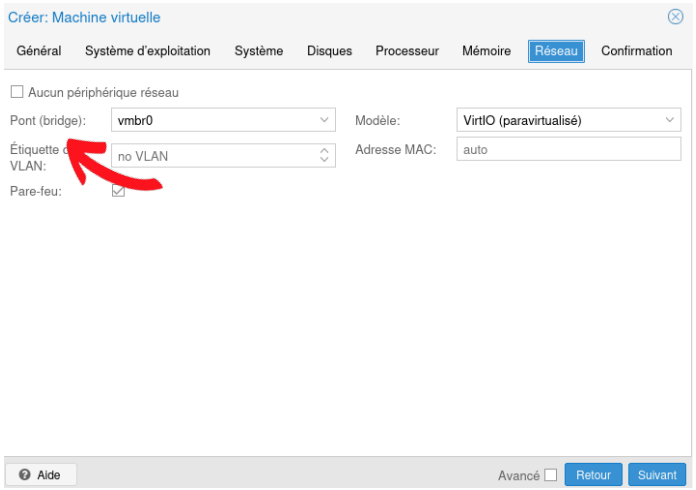


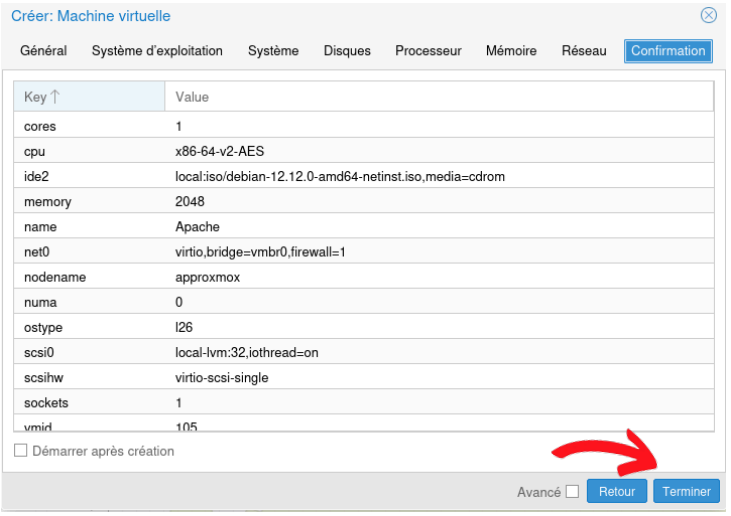
Définissez le nombre de processeur et de coeur que vous voulez ainsi que la mémoire.





Définissez la carte réseaux que vous voulez attribuer et cliquez sur terminer.





C. Détail des Machines Virtuelle

VM ID	Nom	OS	Rôle	Réseau (VLAN)
101	ServerWin	Windows Server 2019	Contrôleur de domaine, DNS	VLAN 25 (eno1)
202	ServerApache	Debian 12	Hébergement du site public	DMZ (eno2)
103	WindowsClient	Windows 10	Poste de test utilisateur	DHCP (VLAN 25) (eno1)
104	DebianClient	debian 12	Poste de test utilisateur	DHCP (VLAN 25) (eno1)

3.5 Windows Serveur 2019

Le serveur Windows Serveur (`172.19.25.201`) . Assure la cohérence des comptes et des droits d'accès.

A. Rôles et Services Installés

Pour remplir ses fonctions, deux rôles principaux ont été configurés :

- **ADDS (Active Directory Domain Services)** : Fournit l'annuaire centralisé. Il permet de gérer les objets du réseau (utilisateurs, groupes, ordinateurs) de manière hiérarchisée.
- **DNS (Domain Name System)** : Indispensable au fonctionnement de l'Active Directory. Il permet aux machines de résoudre les noms d'hôtes (ex: `WWW.google.com`) en adresses IP.

1. Installation et Promotion du Domaine

Étape A : Installation du rôle AD DS

1. Ouvrez le **Gestionnaire de serveur** > **Gérer** > **Ajouter des rôles et fonctionnalités**.
2. Choisissez **Installation basée sur un rôle ou une fonctionnalité**.
3. Sélectionnez votre serveur cible.
4. Cochez **Services de domaine Active Directory (AD DS)** et validez l'ajout des fonctionnalités requises.
5. Poursuivez jusqu'à l'installation et attendez la fin du processus.

Étape B : Promotion en Contrôleur de Domaine

1. Cliquez sur l'icône de notification (le drapeau jaune) et sélectionnez **Promouvoir ce serveur en contrôleur de domaine**.
2. Sélectionnez **Ajouter une nouvelle forêt** et saisissez votre nom de domaine racine (`antonin.lan`).
3. Définissez un mot de passe pour le **DSRM** (Mode de restauration des services d'annuaire) et conservez-le.
4. Laissez les options DNS et NetBIOS par défaut, puis lancez l'installation. Le serveur redémarrera automatiquement.

2. Création des Unités d'Organisation (OU) et Utilisateur

Les OU servent à structurer votre parc (utilisateurs, ordinateurs) de manière hiérarchique.

1. Allez dans **Outils** > **Utilisateurs et ordinateurs Active Directory**.
2. Faites un clic droit sur votre domaine (antonin.lan) > **Nouveau** > **Unité d'organisation**.
3. Donnez un nom (`SI`, `Utilisateurs`, `R&D`)

Créer un Utilisateur.

1. Création d'utilisateur > **Nouveau** > **Utilisateur.**
   Entrer les informations concernant cet utilisateur (nom, prénom, nom de session) et définissez un mot de passe.
2. Cochez l'option **"L'utilisateur doit changer le mot de passe à la prochaine session"** pour plus de sécurité.

Ajouter l'utilisateur au groupe

1. Double-cliquez sur l'utilisateur créé.
2. Allez dans l'onglet **Membre de** > **Ajouter**.
3. Tapez le nom de votre groupe (ex: `admin`), cliquez sur **Vérifier les noms**, puis validez par **OK**.

B. Structuration de l'entreprise (Unités d'Organisation)

Afin de simuler un environnement d'entreprise réel, j'ai structuré notre annuaire en utilisant des **Unités d'Organisation (OU)**. Cette organisation permet de segmenter les objets de l'annuaire par service ou par fonction :

- **OU Admin** : Regroupe les comptes ayant des privilèges élevés pour l'administration de l'infrastructure.
- **OU R&D** : Permet de classer les utilisateurs selon leur département métier.
- **OU Utilisateurs** : Unité racine regroupant les comptes standards de l'entreprise.

C. Création des utilisateurs et stratégie de test

Pour valider le bon fonctionnement de notre infrastructure, nous avons créé des comptes utilisateurs types (ex: `Antonin`, Martin Eden). Chaque utilisateur est rattaché à son service respectif, ce qui nous permet de vérifier :

1. La bonne connexion sur les postes clients Windows 10.
2. L'application des droits d'accès spécifiques sur le réseau.

D. Gestion des groupes pour le partage TrueNAS

La gestion des droits d'accès sur le serveur de fichiers ne se fait jamais par utilisateur individuel, mais par **Groupes de Sécurité**. Cette méthode, conforme aux bonnes pratiques de l'administration système, facilite la maintenance.

- **Groupe :** `Utilisateur_Partage`
  - **Type** : Groupe de sécurité.
  - **Rôle** : Ce groupe est le pivot du partage de fichiers. Il a été utilisé comme référence dans les **ACL (Access Control Lists)** de TrueNAS.
  - **Fonctionnement** : Tout utilisateur ajouté à ce groupe hérite automatiquement des droits d'écriture sur le partage réseau `WindowsPartage`. Cela nous permet d'ajouter ou de retirer l'accès à un nouvel employé en une seule manipulation dans l'AD, sans avoir à modifier la configuration du serveur TrueNAS.

3.6 Le Serveur Web Apache (Zone DMZ)

A. Pourquoi une zone DMZ (DeMilitarized Zone) ?

La DMZ est un sous-réseau isolé qui agit comme une zone tampon entre Internet (non sécurisé) et le réseau local (sécurisé).

- **Objectif** : Si un pirate parvient à exploiter une faille sur le serveur Web Apache, il se retrouve "enfermé" dans la DMZ.
- **Isolation** : Grâce aux règles du ton pfSense, le serveur en DMZ n'a aucun droit d'initier une connexion vers les VLANs 15, 25 ou 35.

B. Une carte réseau différente

L'utilisation d'une interface réseau distincte est une mesure de **cloisonnement matériel et logique** :

- **Sur Proxmox** : La VM Apache utilise une carte réseau spécifique **Eno2**.
- **Sur pfSense** : La carte physique est branchée sur l'interface **Igb3**.
- **Avantage** : Cela garantit que le flux "Public" ne circule jamais sur le même câble ou le même commutateur que les données sensibles (AD, TrueNAS). C'est une protection contre les attaques.

C. Installation d'un serveur Web Apache sur Debian 12

Ce tutoriel détaille la mise en place du service sur une base Linux Debian, reconnue pour sa stabilité en environnement serveur.

Étape 1 : Préparation du système

Avant l'installation, il est crucial de mettre à jour les dépôts et les paquets existants :

```
sudo apt update && sudo apt upgrade -y
```

Étape 2 : Installation du service Apache2

1. Installez le paquet Apache :

```
sudo apt install apache2 -y
```

Vérifiez que le service est actif et démarre automatiquement :

```
sudo systemctl status apache2
sudo systemctl enable apache2
```

Étape 3 : Personnalisation de la page Web

Par défaut, Apache affiche une page de test située dans /var/www/html/index.html. Modification de cette page pour intégrer le code voulu.

```
nano /var/www/html/index.html
```

Étape 4 : Test de fonctionnement

- **En local** : Taper l'IP du serveur (10.19.19.250) dans le navigateur d'une machine ayant accès à la DMZ.
- **Depuis l'extérieur** : Utiliser l'IP WAN du pfSense avec le port (29170) grâce à la règle de **Port Forwarding** créé précédemment nous pouvons avoir accès à la page web.

3.7 La Borne WiFi (Netgear)

A. Rôle dans l'Architecture Réseau

Afin de permettre une connectivité sans fil sécurisée et flexible pour les collaborateurs et les terminaux mobiles au sein de l'entreprise, nous avons intégré un point d'accès Wi-Fi physique. Cette borne est directement reliée au Switch de Couche 3, sur le VLAN 15.

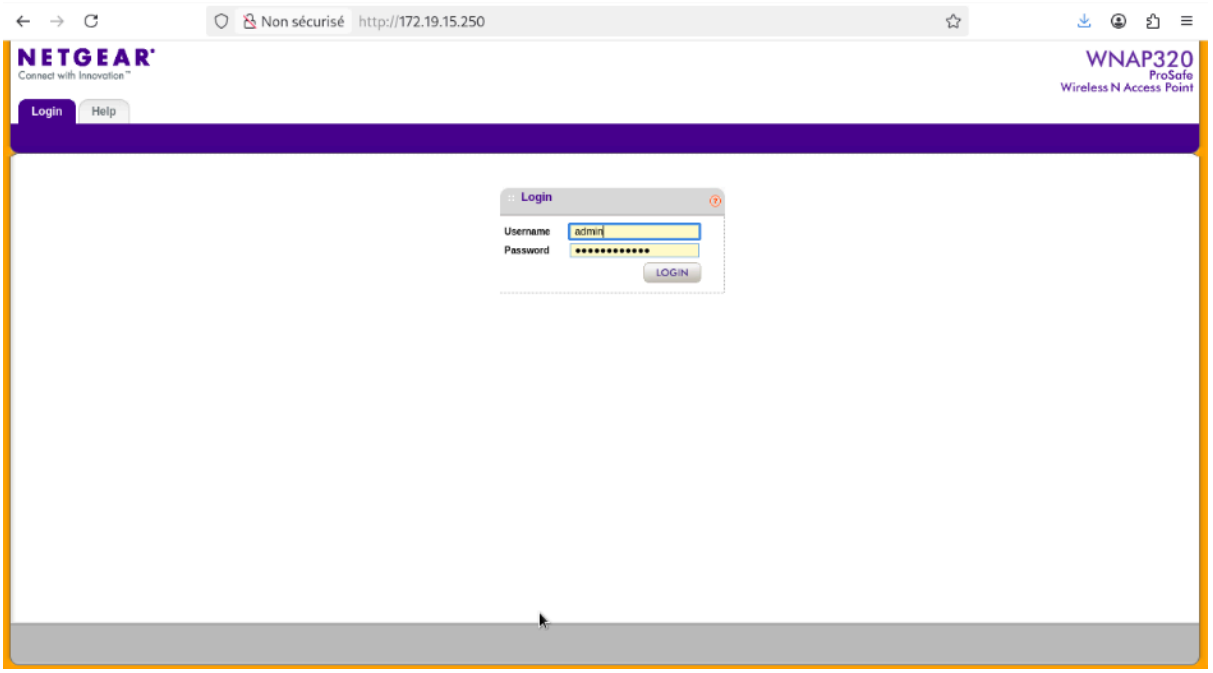
B. Procédure de Mise en Œuvre et Configuration

1. Réinitialisation matérielle (Reset)

Le matériel utilisé provenant d'une ancienne configuration, il a d'abord été nécessaire de réaliser un Reset d'usine, à l'aide d'un outil comme un petit fils de fer appuyé sur le bouton de réinitialisation de la borne. Cette action essentielle permet de purger les anciennes configurations, et de remettre l'ip par défaut (192.168.1.1/24).

2. Accès à l'interface d'administration Web

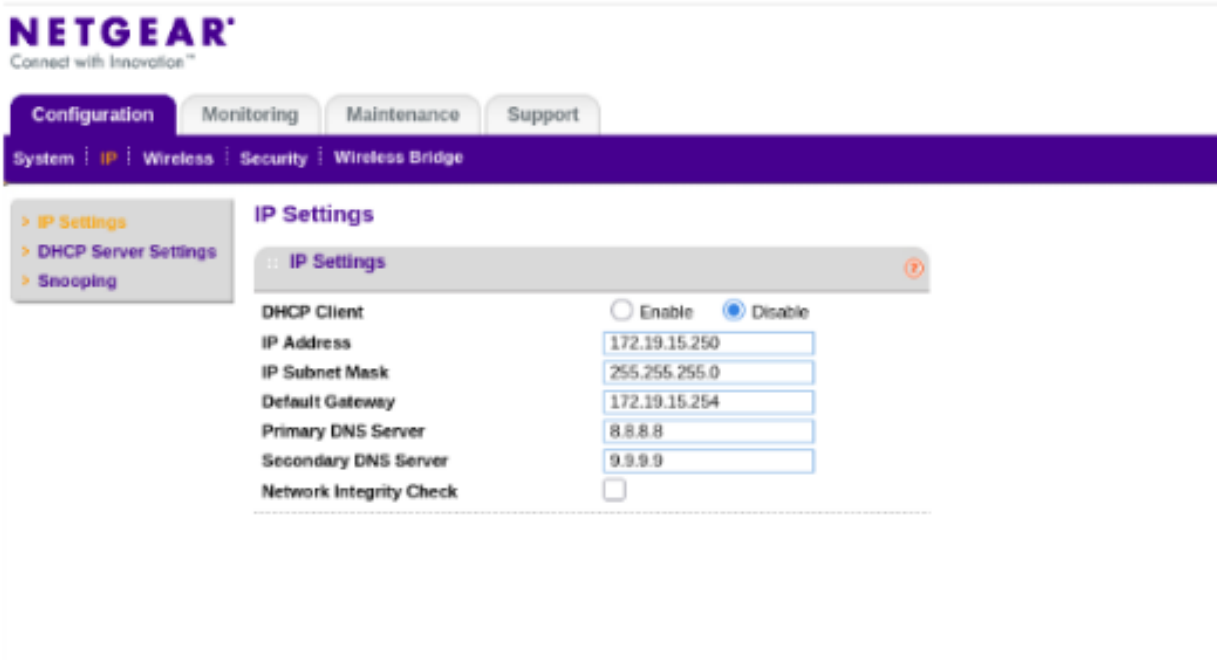
Une fois la borne réinitialisée, il suffisait de se connecter au réseau par défaut pour accéder à son interface de gestion locale via un navigateur Web.



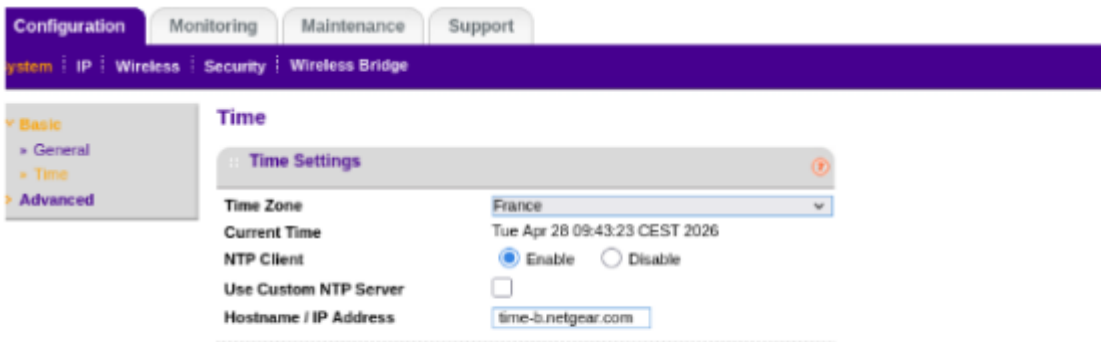
3. Configuration des paramètres Système et Réseau

Pour assurer la cohérence de l'infrastructure, nous avons ajusté les paramètres de base de la borne :

- Paramétrage IP : Attribution d'une adresse IP fixe dédiée dans notre plage de management afin de garantir la joignabilité de l'interface d'administration depuis le VLAN d'Administration.



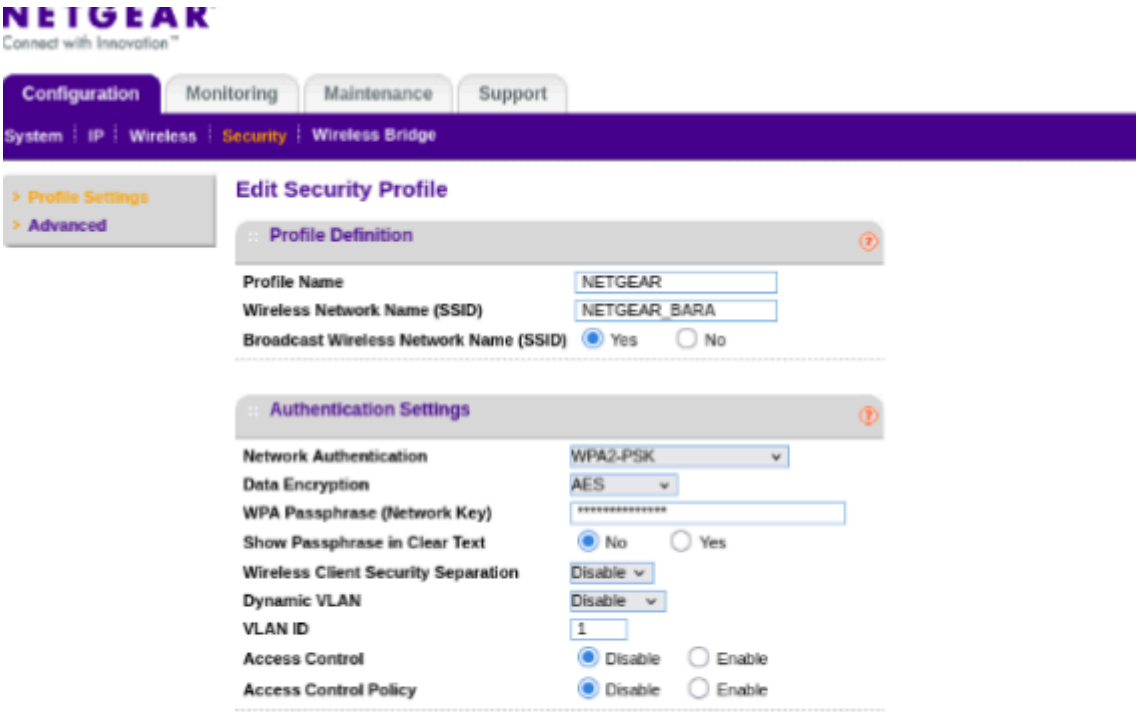
- Configuration de la Time Zone : Réglage du fuseau horaire (Europe/Paris). Cette étape est indispensable pour la cohérence des journaux d'événements (logs) de la borne en cas d'audit de sécurité ou de diagnostic de panne.

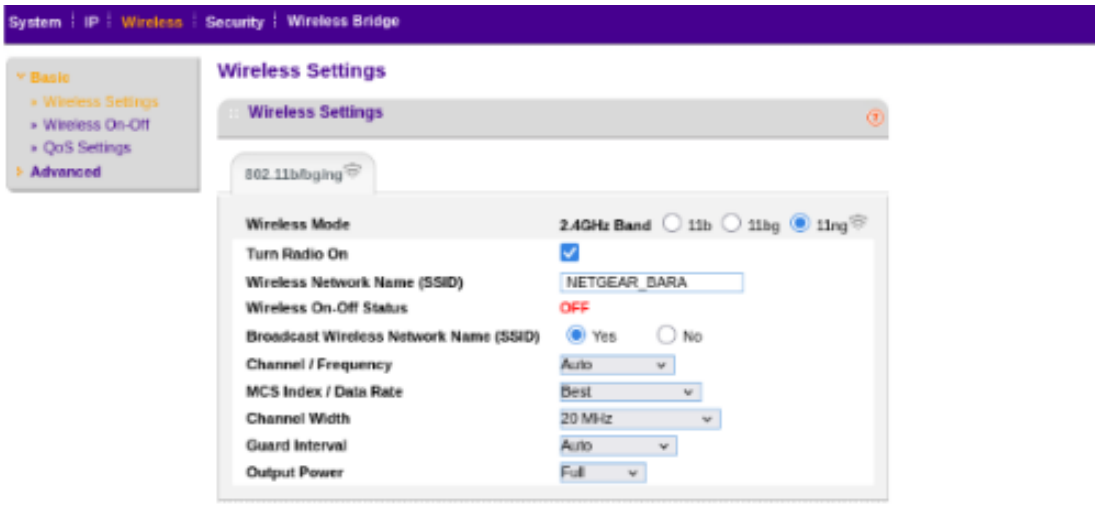


4. Configuration et Sécurisation du Réseau Sans Fil (SSID)

Nous avons ensuite créé et sécurisé le réseau Wi-Fi principal destiné à l'entreprise :

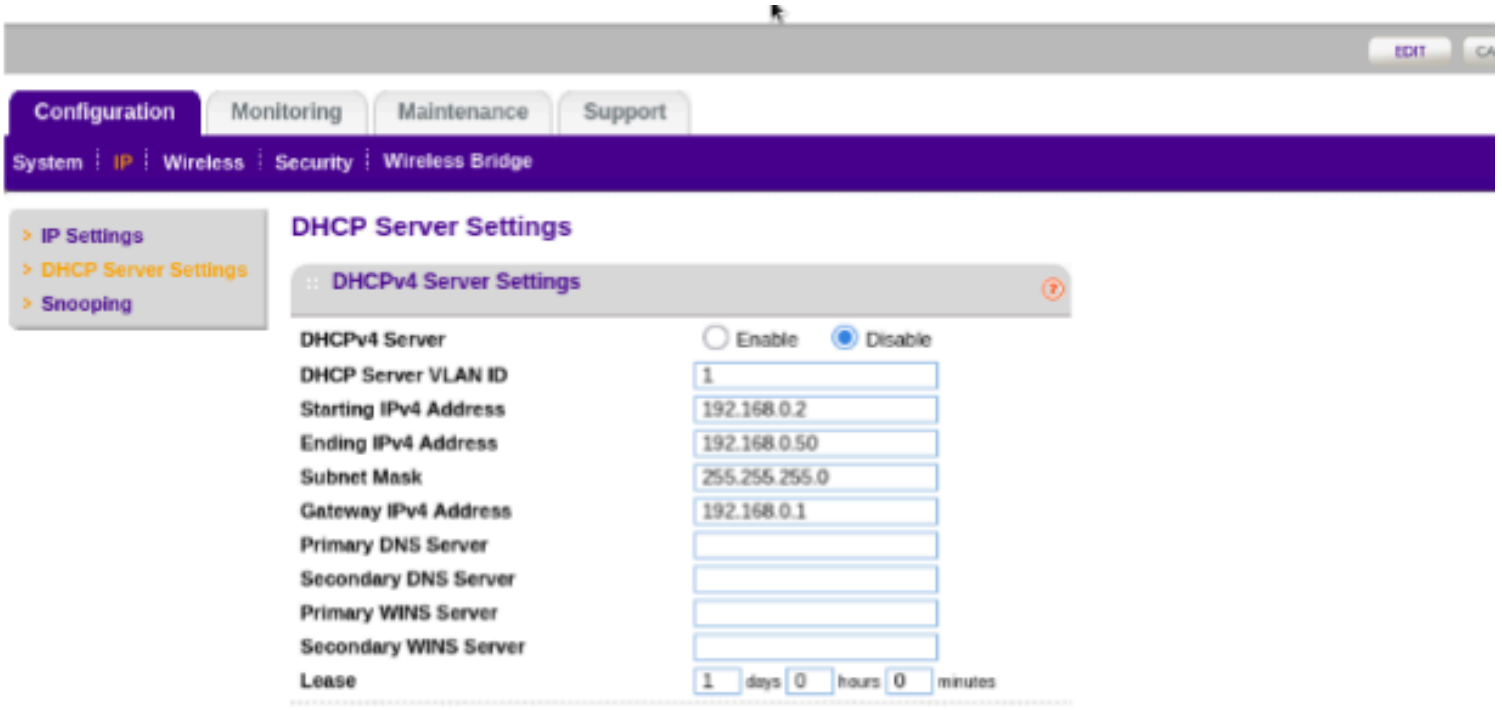
- Nom du réseau (SSID) : Netgear_BARA
- Sécurité & Chiffrement : Utilisation du protocole WPA2-PSK (AES). Ce choix garantit un chiffrement robuste des données circulant dans l'air, protégeant le réseau contre les écoutes clandestines.
- Clé de sécurité : Superbtssio123





C. Gestion de l'adressage IP

Le Switch L3 comme Serveur DHCP : La borne Wi-Fi n'intègre aucune fonction de routage ni de distribution d'adresses (le DHCP de la borne est désactivé). C'est notre **Switch de Couche 3** qui fait office de serveur DHCP centralisé pour l'ensemble des VLANs.



4. Conclusion du Dossier : Borne WIFI

La réalisation de cette infrastructure complète a permis de simuler un environnement d'entreprise réel, allant de la couche physique (Switching/Routing) à la couche applicative (Partages de fichiers, Web).

A. Synthèse de l'Infrastructure

Ce projet repose sur la complémentarité de trois piliers technologiques :

1. **La Maîtrise du Réseau (Cisco & pfSense)** :

Grâce à la segmentation en **VLANs** et à l'utilisation d'un **Switch de Niveau 3**, nous avons optimisé les performances de routage interne. Le pare-feu **pfSense** assure une protection, notamment via la gestion d'une **DMZ** isolée pour les services publics et l'utilisation du **NAT Outbound/Inbound** pour la communication extérieure.

2. **La Virtualisation (Proxmox)** :

L'adoption de l'hyperviseur **Proxmox** a été le pilier central de cette infrastructure, offrant une flexibilité et une agilité indispensables à la mise en œuvre de services. Plutôt que de multiplier les équipements physiques, nous avons fait le choix d'une **virtualisation complète**.

3. **La Connectivité Sans Fil Sécurisée (Borne Wi-Fi & Centralisation DHCP)**

L'intégration d'un point d'accès Wi-Fi physique autonome complète l'infrastructure en étendant le réseau local sans fil de manière sécurisée. La borne diffuse le SSID (`Netgear_BARA`) protégé par un chiffrement WPA2-PSK.

Pour garantir une architecture propre et éviter tout cloisonnement, les fonctions de routage et de serveur DHCP de la borne ont été désactivées : c'est le **Switch de Couche 3 (L3)** qui distribue dynamiquement les adresses IP à travers la borne, permettant aux utilisateurs sans fil d'obtenir un adressage cohérent.

B. Bilan de la Sécurisation

La sécurité a été le fil conducteur de chaque étape :

- **Cloisonnement** : Les **ACL Cisco** filtrent le trafic Wi-Fi et R&D pour protéger le cœur du SI.
- **Isolation** : La DMZ empêche toute compromission du réseau interne depuis Internet.
- **Authentification** : Aucun partage n'est accessible sans une identification valide auprès de l'annuaire.

C. Perspectives de développement

Cette maquette constitue une base solide qui pourrait évoluer vers :

- **Le déploiement de GPO** : Pour automatiser la configuration des postes clients (déploiement de logiciels, montage de lecteurs réseau).
- **La mise en place d'un VPN** : Pour permettre aux administrateurs un accès sécurisé à distance sans passer par une redirection de port simple.
- **La supervision** : L'ajout d'un serveur Zabbix pour surveiller l'état de santé des services en temps réel.

Bilan Personnel

Ce projet de fin d'études a été l'occasion de mettre en pratique les compétences théoriques acquises durant le cycle de **BTS SIO (option SISR)**. La confrontation aux réalités techniques — telles que les problématiques de routage inter-VLAN ou la complexité des permissions SMB — a renforcé ma capacité à diagnostiquer des pannes et à concevoir des architectures réseau sécurisées et évolutives.

5. Annexe

configuration du Switch :

```
Building configuration…
Current configuration : 4997 bytes
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname SWBARA
boot-start-marker
boot-end-marker
enable secret 5 $1$Odq9$R/pn8OHnJ/5Aza5y3kcXV.
username admin privilege 15 secret 5 $1$lP42$XdgxleSP11J7Zti5GsRzl.
no aaa new-model
switch 1 provision ws-c3750-24p
system mtu routing 1500
ip subnet-zero
ip routing
ip domain-name antonin.lan
no ip dhcp use vrf connected
ip dhcp excluded-address 172.19.15.254
ip dhcp excluded-address 172.19.25.254
ip dhcp excluded-address 172.19.35.254
ip dhcp pool POOL_UTILISATEURS
   network 172.19.15.0 255.255.255.0
   default-router 172.19.15.254
   dns-server 8.8.8.8 1.1.1.1
ip dhcp pool POOL_SI
   network 172.19.25.0 255.255.255.0
   default-router 172.19.25.254
   dns-server 8.8.8.8 1.1.1.1
ip dhcp pool POOL_R&D
   network 172.19.35.0 255.255.255.0
   default-router 172.19.35.254
   dns-server 8.8.8.8 1.1.1.1
spanning-tree mode pvst
spanning-tree extend system-id
no spanning-tree vlan 15,25,35,100
!
vlan internal allocation policy ascending
ip ssh version 2
interface FastEthernet1/0/1
 description PORTS_UTILISATEURS
 switchport access vlan 15
 switchport mode access
```

```
interface FastEthernet1/0/2
 description PORTS_UTILISATEURS
 switchport access vlan 15
 switchport mode access
interface FastEthernet1/0/3
 description PORTS_UTILISATEURS
 switchport access vlan 15
 switchport mode access
interface FastEthernet1/0/4
 description PORTS_UTILISATEURS
 switchport access vlan 15
 switchport mode access
interface FastEthernet1/0/5
 description PORTS_UTILISATEURS
 switchport access vlan 15
 switchport mode access
interface FastEthernet1/0/6
 description PORTS_SI
 switchport access vlan 25
 switchport mode access
interface FastEthernet1/0/7
 description PORTS_SI
 switchport access vlan 25
 switchport mode access
interface FastEthernet1/0/8
 description PORTS_SI
 switchport access vlan 25
 switchport mode access
interface FastEthernet1/0/9
 description PORTS_SI
 switchport access vlan 25
 switchport mode access
interface FastEthernet1/0/10
 description PORTS_SI
 switchport access vlan 25
 switchport mode access
interface FastEthernet1/0/11
 description PORTS_ADMIN
 switchport access vlan 35
 switchport mode access
interface FastEthernet1/0/12
 description PORTS_ADMIN
 switchport access vlan 35
 switchport mode access
interface FastEthernet1/0/13
 description PORTS_ADMIN
 switchport access vlan 35
 switchport mode access
interface FastEthernet1/0/14
 description PORTS_ADMIN
 switchport access vlan 35
 switchport mode access
```

```
interface FastEthernet1/0/15
 description PORTS_ADMIN
 switchport access vlan 35
 switchport mode access
interface FastEthernet1/0/16
 description PORT_INUTILISE_SECURITE
 shutdown
interface FastEthernet1/0/17
 description PORT_INUTILISE_SECURITE
 shutdown
interface FastEthernet1/0/18
 description PORT_INUTILISE_SECURITE
 shutdown
interface FastEthernet1/0/19
 description PORT_INUTILISE_SECURITE
 shutdown
interface FastEthernet1/0/20
 description PORT_INUTILISE_SECURITE
 shutdown
interface FastEthernet1/0/21
 description PORT_INUTILISE_SECURITE
 shutdown
interface FastEthernet1/0/22
 description PORT_INUTILISE_SECURITE
 shutdown
interface FastEthernet1/0/23
 description PORT_INUTILISE_SECURITE
 shutdown
interface FastEthernet1/0/24
 description LIEN_VERS_PFSENSE
 switchport access vlan 100
 switchport mode access
interface GigabitEthernet1/0/1
interface GigabitEthernet1/0/2
interface Vlan1
 no ip address
 shutdown
interface Vlan15
 ip address 172.19.15.254 255.255.255.0
interface Vlan25
 ip address 172.19.25.254 255.255.255.0
interface Vlan35
 ip address 172.19.35.254 255.255.255.0
 ip access-group ACL_VLAN_35 in
interface Vlan100
 description LIEN_VERS_PFSENSE
 ip address 172.19.11.253 255.255.255.252
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.11.254
ip http server
ip http secure-server
ip access-list extended ACL_VLAN_15
```

```
 permit tcp 172.19.15.0 0.0.0.255 host 172.19.25.201 eq www
 permit tcp 172.19.15.0 0.0.0.255 host 172.19.25.202 eq 445
 deny   tcp 172.19.15.0 0.0.0.255 host 172.19.15.254 eq 22
 deny   tcp 172.19.15.0 0.0.0.255 host 172.19.11.254 eq 443
 deny   tcp 172.19.15.0 0.0.0.255 host 172.19.11.254 eq www
 deny   ip 172.19.15.0 0.0.0.255 172.19.25.0 0.0.0.255
 deny   ip 172.19.15.0 0.0.0.255 172.19.35.0 0.0.0.255
 permit ip host 172.19.15.250 172.19.25.0 0.0.0.255
 permit ip any any
ip access-list extended ACL_VLAN_35
 permit ip 172.19.35.0 0.0.0.255 172.19.25.0 0.0.0.255
 deny   ip 172.19.35.0 0.0.0.255 172.19.15.0 0.0.0.255
 deny   tcp 172.19.35.0 0.0.0.255 host 172.19.35.254 eq 22
 deny   tcp 172.19.35.0 0.0.0.255 host 172.19.11.254 eq 443
 deny   tcp 172.19.35.0 0.0.0.255 host 172.19.11.254 eq www
 permit ip any any
control-plane
line con 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
end
```

Show Run :

VLAN	Name	Status	Ports
1	default	Active	Fa1/0/16 a Fa1/0/23, Gi1/0/1, Gi1/0/2
15	VLAN_Utilisateurs	Active	Fa1/0/1 a Fa1/0/5
25	VLAN_SI	Active	Fa1/0/6 a Fa1/0/10
35	VLAN_R&D	Active	Fa1/0/11 a Fa1/0/15