BTSSIO

ÉPREUVE E6 dossier:

Candidat : Noé Leguay
Option : Solutions d’infrastructure, systèmes et réseaux (SISR)
Session : 2024 - 2026
Établissement : Lycée Venise Verte, Niort

SOMMAIRE ANALYTIQUE

- **PARTIE 1 :PRÉSENTATION GÉNÉRALE DU PROJET ET DE L'ARCHITECTURE**
  - 1.1 Contexte et Objectifs
  - 1.2 Architecture Réseau et Adressage IP
  - 1.3 Présentation des Équipements et Services
- **PARTIE 2 : CONFIGURATION ET MISE EN ŒUVRE DES SERVICES DE L'INFRASTRUCTURE**
  - 2.1 L'Hyperviseur (Proxmox VE 8.0.3)
  - 2.2Le Pare-feu (pfSense)
  - 2.3 Le Commutateur de Cœur de Réseau (Cisco 2960)
  - 2.4 Centralisation des Identités et des Noms (Windows Server AD DS & DNS)
  - 2.5 Centralisation et Déploiement de Parc (FOG Server)
- **PARTIE 3 : SÉCURISATION APPLICATIVE ET DÉFENSE ACTIVE (FAIL2BAN)**
  - 3.1 Installation de Fail2ban
  - 3.2Configuration de Fail2ban
  - 3.3Test et Validation : Scénario d'attaque et de défense active via SSH
- **PARTIE 4 :** CONCLUSION ET BILANS DE LA RÉALISATION
  - Synthèse de l'Infrastructure
  - Bilan Personnel

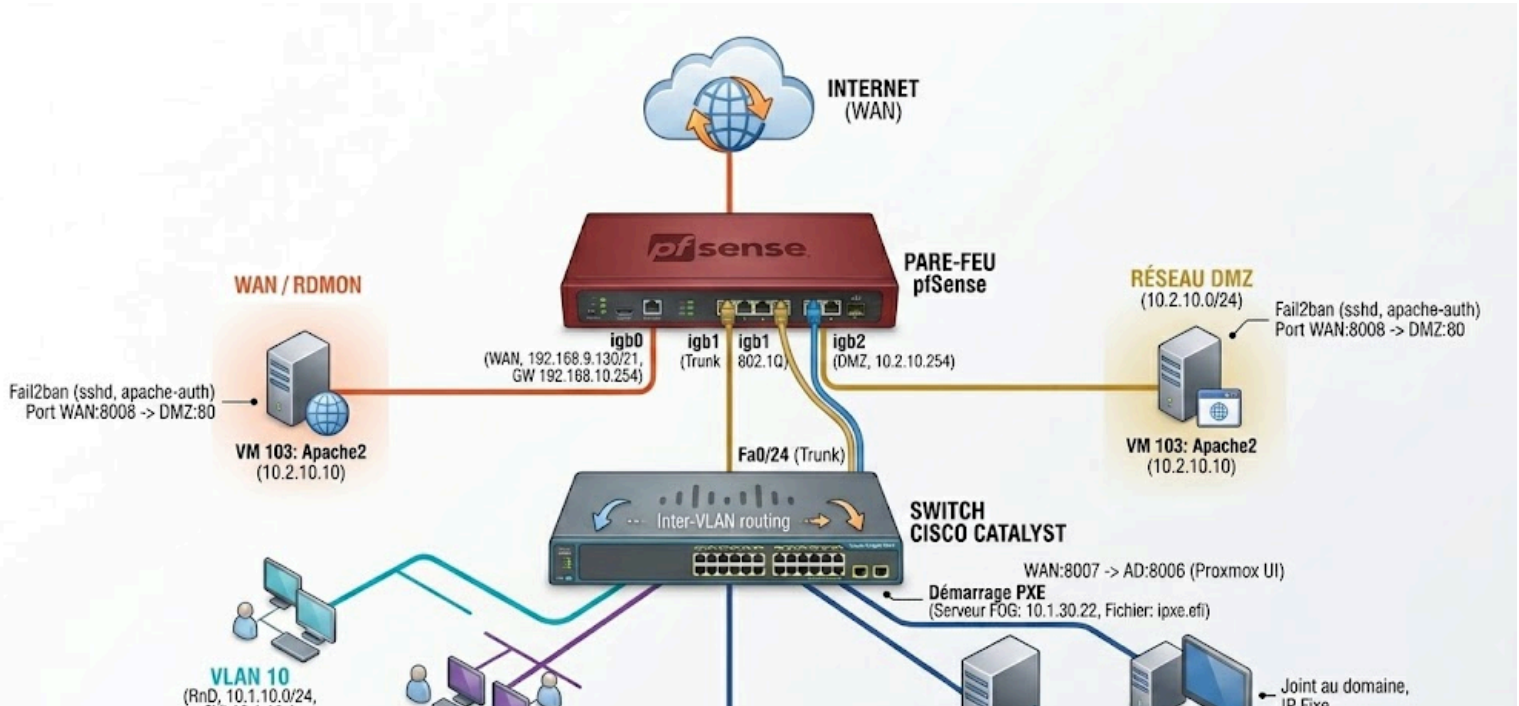
PARTIE 1 : PRÉSENTATION GÉNÉRALE DU PROJET ET DE L'ARCHITECTURE

1.1 Contexte et Objectifs

Cette maquette simule une entreprise comprenant un Firewall pfsense, un switch cisco 2960, un hyperviseur proxmox sur lequel est hébergé un serveur Fog, un Windows serveur (Active Directory) et un serveur apache2/Fail2ban.

1.2 Architecture Réseau et Adressage IP

La topologie s'appuie sur une segmentation logique par VLAN (Virtual Local Area Network) de niveau 2 selon la norme IEEE 802.1Q, isolant les différents services de l'établissement.



Fiche d'Adressage IP Global de la Maquette :

Segment Réseau	Interface Physique / Virtuelle	Sous-réseau IP	Passerelle (pfSense)	Rôle Technique et Équipements Connectés
WAN	igb0	192.168.9.130/21	192.168.10.254	Interface de sortie vers l'infrastructure d'accueil.
LAN	igb1 (Natif)	10.1.1.0/24	10.1.1.254	Segment natif dédié à l'administration d'origine du pare-feu.
VLAN 10	igb1.10 (RnD)	10.1.10.0/24	10.1.10.254	Zone utilisateurs / Postes clients pédagogiques (Pôle R&D).
VLAN 20	igb1.20 (RH)	10.1.20.0/24	10.1.20.254	Zone utilisateurs / Services administratifs et Ressources Humaines.
VLAN 30	igb1.30 (SI)	10.1.30.0/24	10.1.30.254	Périmètre Infrastructure Critique (FOG, AD, Winclient, Masters DHCP).

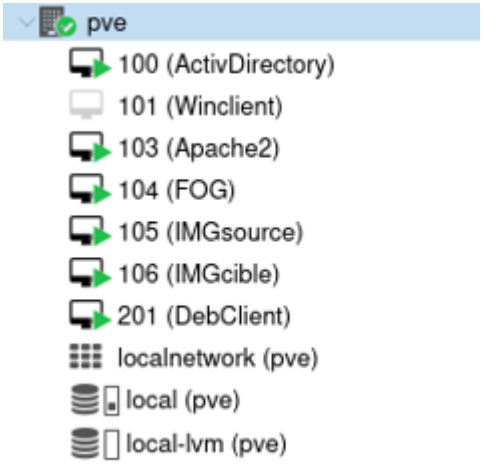
DMZ	igb2	10.2.10.0/24	10.2.10.254	Zone étanche isolée accueillant le serveur Web public Apache2.

1.3 Présentation des Équipements et Services

A. L'Hyperviseur (Proxmox VE 8.0.3)

Proxmox VE est une solution d'hypervision complète de type 1 (bare-metal) basée sur la distribution Linux Debian, combinant la virtualisation de machines virtuelles (KVM) et de conteneurs. Dans le cadre de cette maquette, il fait office de plateforme d'accueil unique pour l'ensemble des serveurs et clients virtuels de l'établissement.

L'intégralité des serveurs et clients de l'infrastructure est virtualisée et centralisée sur un nœud physique unique nommé `pve` exécutant la solution Proxmox VE 8.0.3.



B. Le Pare-feu Périmétrique (pfSense)

Le pare-feu pfSense agit comme la passerelle de sécurité et le routeur central de la maquette. Ses fonctions principales incluent :

- **Routage Inter-VLAN :** Interconnexion des sous-réseaux et application de politiques de filtrage par interface**Translation d'adresses (NAT)**

- **Serveur DHCP Centralisé :** Distribution dynamique des baux réseau et gestion de la section *Network Booting* indispensable à l'amorçage à distance.

C. Le Commutateur de Cœur de Réseau (Cisco 2960)

Le commutateur Cisco assure la distribution physique et le confinement matériel des domaines de diffusion.

- **Liaison Montante (Trunk 802.1Q) :** L'interface physique `FastEthernet0/24` est configurée comme liaison Trunk inter-équipements afin de véhiculer les trames étiquetées vers l'interface réseau du pare-feu.

- **Sécurisation des interfaces inutilisées :** Toutes les interfaces n'accueillant aucun équipement actif (de `Fa0/16` à `Fa0/23`, ainsi que `Gi0/1` et `Gi0/2`) sont administrativement désactivées (`shutdown`) afin de bloquer les intrusions par connexion physique directe.

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 switchport trunk allowed vlan 1,10,20,30
 switchport mode trunk
!
```

PARTIE 2 : CONFIGURATION ET MISE EN ŒUVRE DES SERVICES DE L'INFRASTRUCTURE

2.1 L'Hyperviseur (Proxmox VE 8.0.3)

- **Rôle :** Plateforme d'accueil de l'ensemble des serveurs et clients virtuels de la maquette.

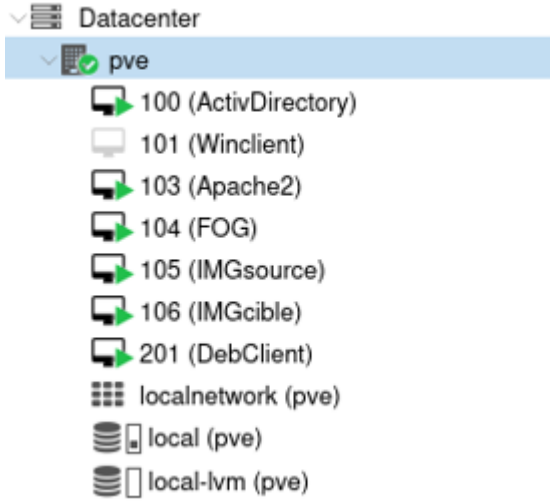
- **Configuration clé :**

  Paramétrage du commutateur virtuel principal `vmbr0` en mode *VLAN Aware*, relié directement au switch.

Paramétrage du commutateur virtuel secondaire `vmbr10`, relié au pfsense afin de poser ma machine Apache2/fail2ban dans la DMZ en 10.2.10.10.

- **Inventaire :** Liste des VMIDs et répartition de la charge CPU/RAM du nœud `pve`:

Type ↑	Description	Disk usage…	Memory us…	CPU usage	Uptime	Host CPU …	Host Mem…
qemu	100 (ActivDirectory)	0.0 %	94.1 %	4.9% of 4 …	13 days 19:4…	0.6% of 32…	21.9 %
qemu	101 (Winclient)				-		
qemu	103 (Apache2)	0.0 %	4.1 %	0.3% of 2 …	6 days 21:47…	0.0% of 32…	0.2 %
qemu	104 (FOG)	0.0 %	64.0 %	2.0% of 2 …	7 days 01:33…	0.1% of 32…	2.5 %
qemu	105 (IMGsource)	0.0 %	18.9 %	0.3% of 2 …	5 days 00:13…	0.0% of 32…	0.4 %
qemu	106 (IMGcible)	0.0 %	14.8 %	0.3% of 2 …	5 days 00:56…	0.0% of 32…	0.5 %
qemu	201 (DebClient)	0.0 %	63.5 %	0.5% of 2 …	6 days 20:44…	0.0% of 32…	0.5 %
sdn	localnetwork (pve)				-		
storage	local (pve)	37.8 %			-		
storage	local-lvm (pve)	1.3 %			-		



2.2 Le Pare-feu (pfSense)

A Rôle Fonctionnel et Positionnement dans l'Architecture

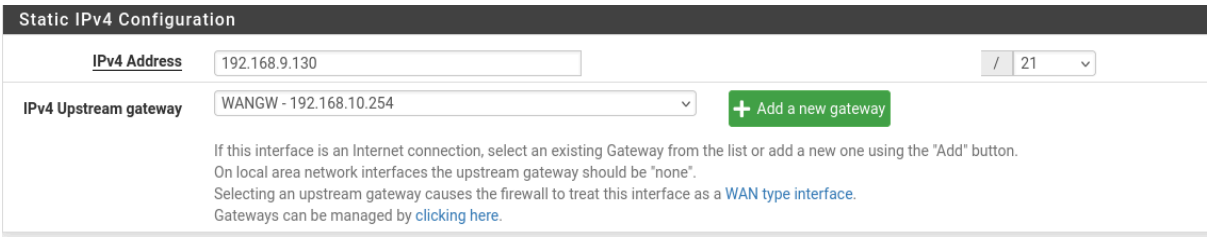
- **Pivot de sécurité** : Il est positionné à la frontière entre le réseau externe non de confiance (WAN) et les réseaux internes de l'établissement.

- **Inspection à états (Stateful Packet Inspection) :** Chaque paquet traversant le pare-feu est analysé selon son état de connexion (création, établie, fermeture), interdisant les paquets orphelins ou falsifiés.

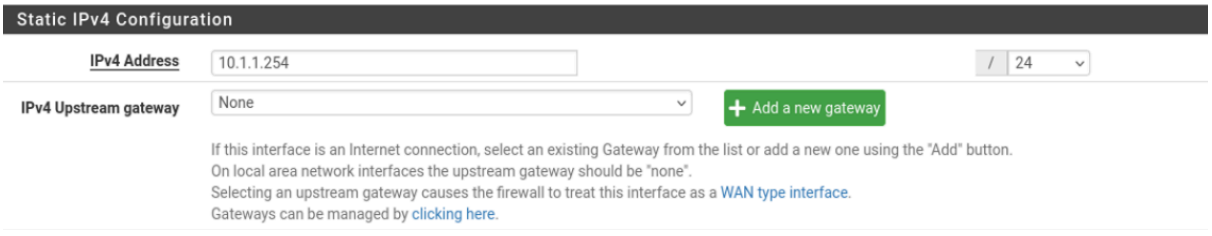
- **Multi-services centralisés :** En plus du filtrage brut, il assure l'étanchéité de la DMZ, la translation d'adresses réseau (NAT) et l'aiguillage de la chaîne d'amorçage via son serveur DHCP.

B Configuration Globale et Assignation des Interfaces

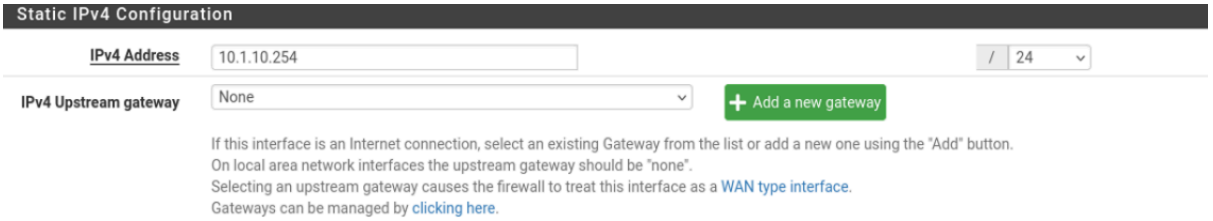
- igb0 (WAN) : Interface connectée à la sortie Internet. Elle récupère son adresse IP via l'infrastructure d'accueil (`192.168.9.130/21`) et pointe vers la passerelle externe `192.168.10.254`.



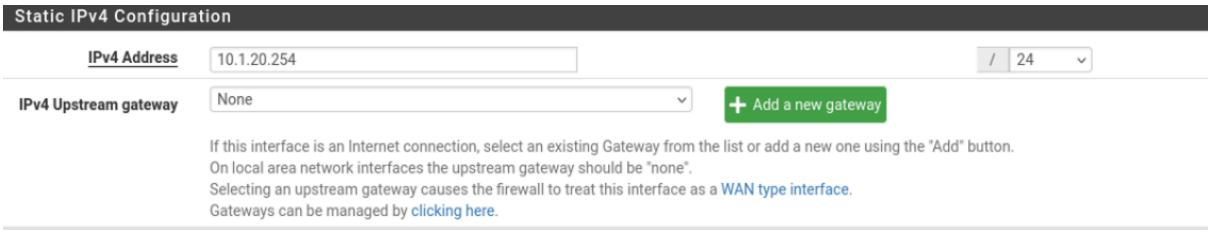
- `igb1` (LAN / Trunk Virtuel) : Interface connectée au commutateur Cisco 2960. C'est sur ce segment que sont rattachés les sous-réseaux logiques (VLAN 10, VLAN 20 et VLAN 30). Son adresse IP d'administration native est `10.1.1.254/24`.



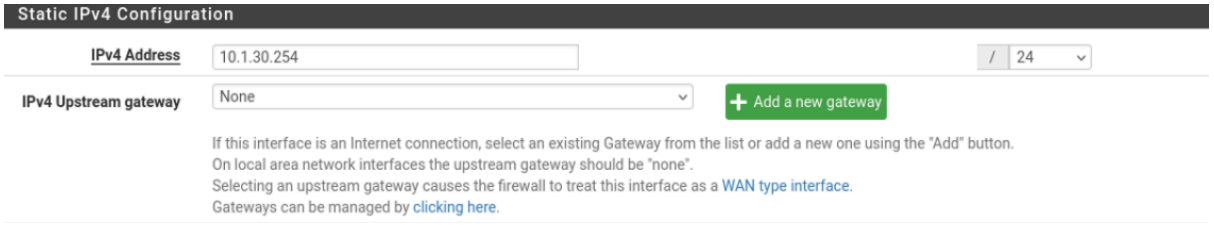
- vlan10 (sur le port physique igb1): Interface qui permet de joindre les utilisateurs du vlan 10 . (ip:10.1.10.254)



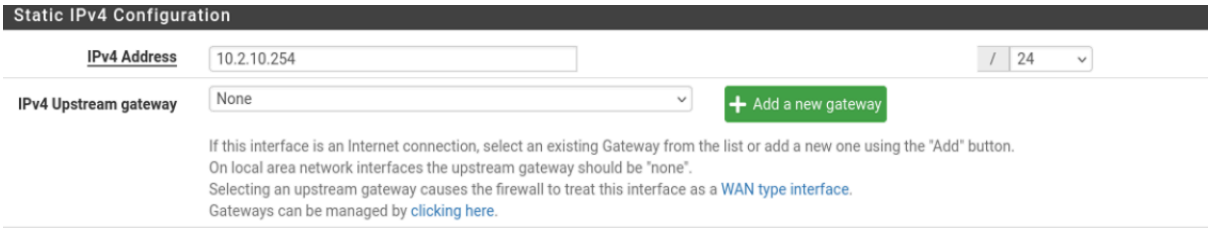
- vlan20 (sur le port physique igb1): interface qui permet de joindre les utilisateurs du vlan 20.(ip:10.1.20.254)



- vlan30 (sur le port physique igb1): interface qui permet de joindre les utilisateurs du vlan 30.(ip:10.1.30.254)



- `igb2` (DMZ) : Interface réseau totalement isolée dédiée exclusivement à l'hébergement du serveur Web public Apache2. Son adressage est fixé sur le réseau `10.2.10.254/24`.



C Politique de Translation d'Adresses (NAT - Network Address Translation)

Afin d'exposer les services internes nécessaires sur Internet sans divulguer l'architecture du réseau privé, j'ai configuré deux règles de redirection de ports strictes :

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
✓	WAN	TCP/UDP	*	*	WAN address	8008	10.2.10.10	80 (HTTP)	Wan->apache	
✓	WAN	TCP/UDP	*	*	WAN address	8007	10.1.30.100	8006		

Le premier NAT permet d’atteindre la page web de mon serveur apache de l’exterieur du reseau, il suffit de tapper:
“http://192.168.9.130:8008”
afin d’accéder a mon site web a condition d’etre dans le reseaux du lycée.

Le deuxieme NAT permet d’acceder a mon interface de configuration proxmox sans me brancher sur mon switch, cela me permettait de pouvoir modifier ma maquette sans devoir m’y déplacer a chaques fois.

D Règles de Filtrage Avancées par Interface (Firewall Rules)

La politique globale appliquée sur le pare-feu est le blocage implicite :

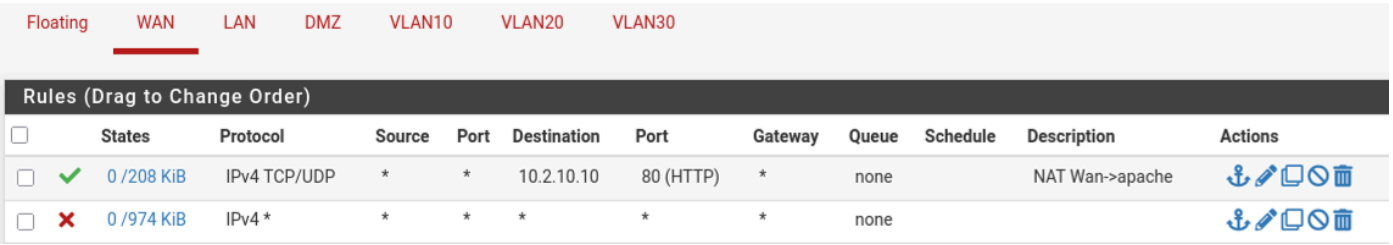
Tout ce qui n'est pas explicitement autorisé est interdit (`Default Deny`).

I) Règles de l'interface WAN

L'interface WAN bloque par défaut toutes les connexions initiées depuis l'extérieur, sauf celles autorisées par les règles de Port Forwarding.

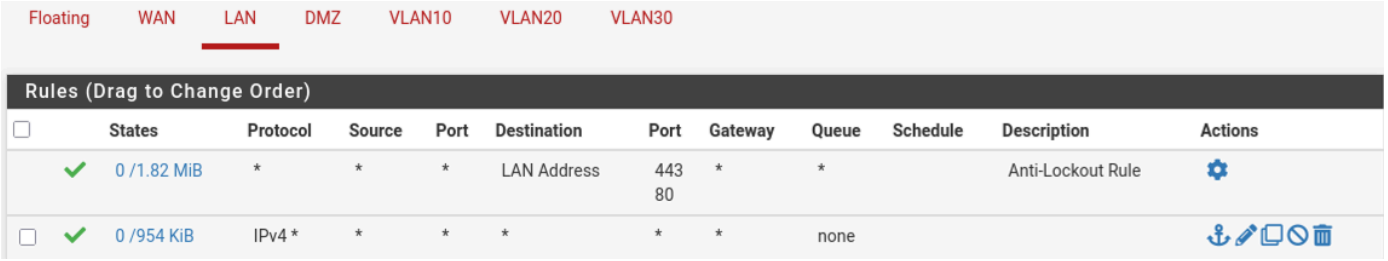
- **Option Sécurité 1 (*Block private networks*) :** Activée. Elle rejette les paquets entrants ayant une adresse IP source de type RFC 1918 (adresses privées), évitant ainsi le spoofing réseau sur l'interface publique.

- **Option Sécurité 2 (*Block bogon networks*) :** Activée. Elle détruit les trames provenant d'adresses IP non allouées ou réservées par l'IANA.



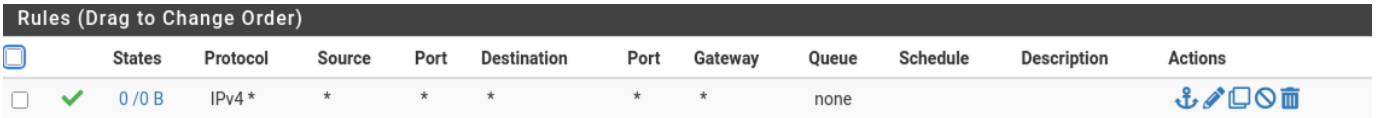
II) Règles de l'interface LAN

L'interface LAN est ouverte car personne ne l'emploie je n'ai donc pas mis de regles speciales



III) Règles des interfaces VLAN 10 & 20

J'ai laissé les interfaces VLAN 10 & 20 completement ouvertes.



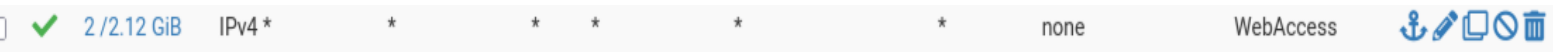
IIII) Règles de l’interface VLAN 30

L'interface VLAN 30 (SI / Infrastructure) regroupe les actifs les plus critiques de la maquette (Active Directory, FOG Server, clients d'infrastructure). Sa politique de filtrage applique des règles d'accès strictes pour concilier l'administration et le déploiement réseau, tout en bloquant les flux non autorisés :

- **Autorisation des flux d'industrialisation (FOG) :** Permet à l'ensemble du sous-réseau `VLAN30_net` de communiquer avec le serveur FOG (`10.1.30.22`) sur les protocoles essentiels au déploiement (HTTP/S, TFTP pour le boot iPXE, et NFS pour le transfert de l'image Partclone).

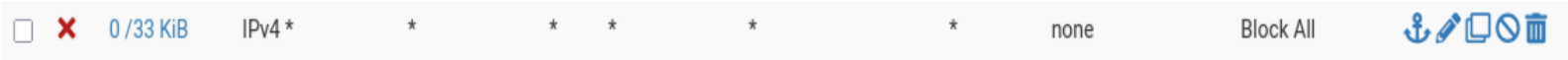
- **Autorisation des services d'identité (Active Directory & DNS) :** Permet la communication vers le contrôleur de domaine (`10.1.30.110`) pour les requêtes d'authentification de session, l'application des droits AD et les résolutions de noms DNS internes (port `UDP/53`).

- **Accès Internet contrôlé :** J’active ou désactive cette règle en fonction de l’envie ou non d’acceder à internet.

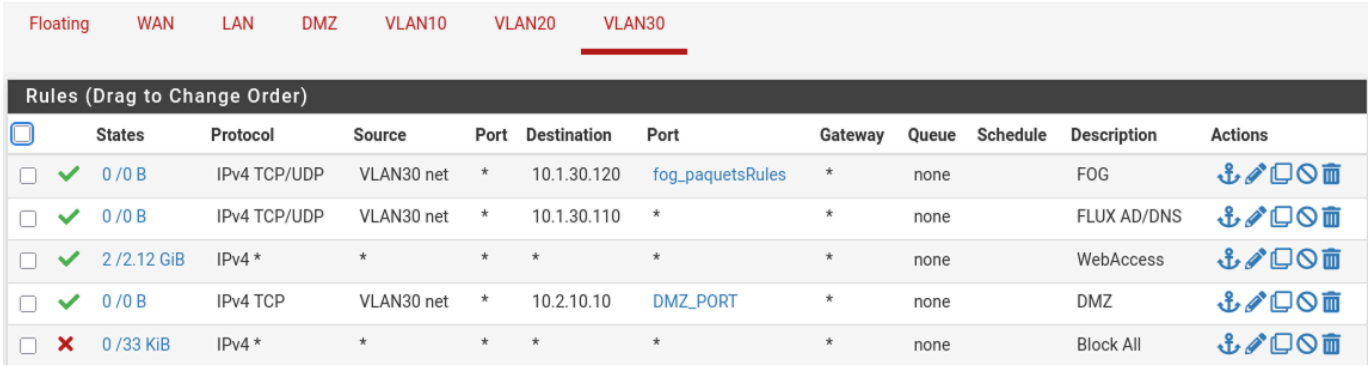


- **Accès à Apache :** cette règle me permet d’acceder au serveur apache quand la règle de juste au dessus est désactivé.

- **Cloisonnement et fermeture :** Application d'une règle de rejet implicite (`Default Deny`) en fin de liste, interdisant toute initiation de flux non planifiée vers le LAN pour limiter les risques de compromission par rebond.



Toutes les règles VLAN 30 :

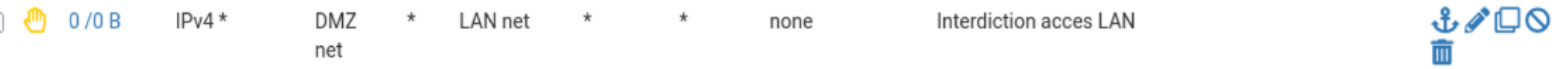


IIII Règles de l’interface DMZ

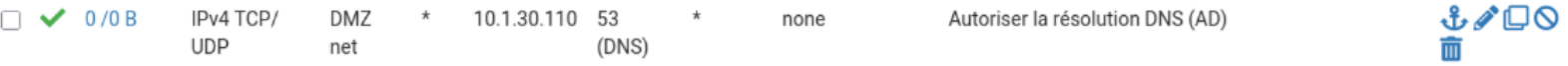
L'interface **DMZ** (Zone Démilitarisée) accueille le serveur Web public Apache2 (`10.2.10.10`) et applique la règle fondamentale

de l'isolement périmétrique : le serveur peut répondre aux sollicitations, mais il ne peut en aucun cas initier de flux vers l'interne. Sa politique de filtrage se structure ainsi :

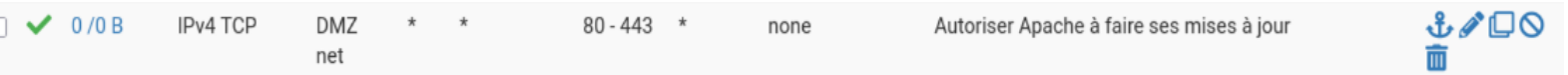
- **Étanchéité et confinement critiques :** Interdiction absolue d'initier une connexion vers le réseau d'administration (LAN) ou vers la zone d'infrastructure (VLAN 30) afin de bloquer toute tentative de pivotement ou d'attaque par rebond si le site web venait à être compromis.



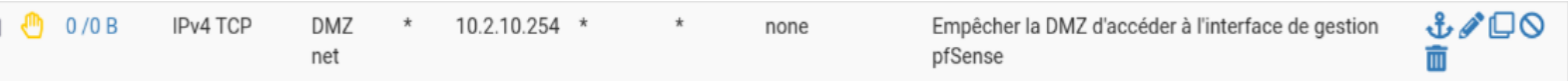
- **Résolution DNS contrôlée :** Autorisation unique d'émettre des requêtes DNS vers le contrôleur de domaine de confiance (`10.1.30.110`) sur le port `UDP/53` pour ses besoins de résolution internes.



- **Accès WAN restrictif :** Autorise la machine à sortir vers Internet uniquement sur les ports `80 (HTTP)` et `443 (HTTPS)` pour l'exécution des mises à jour système et la récupération des dépendances logicielles.



- **Accès Pfsense interdit :** empeche les tentatives de connexion des machines de la DMZ a l'interface graphique du Pfsense.



- **Blocage par défaut :** Application de la règle de fermeture implicite (`Default Deny`) détruisant instantanément tout paquet non explicitement répertorié.

☐	✖	0 /342 KiB	IPv4 *	*	*	*	*	*	none	Block All	⚓ ✎ ⧉ ⊘ 🗑

Toutes les règles :

Floating | WAN | LAN | DMZ | VLAN10 | VLAN20 | VLAN30

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✔	0 /0 B	IPv4 TCP	DMZ net	*	*	80 - 443	*	none		Autoriser Apache à faire ses mises à jour	⚓ ✎ ⧉ ⊘ 🗑
☐	✔	0 /0 B	IPv4 TCP/ UDP	DMZ net	*	10.1.30.110	53 (DNS)	*	none		Autoriser la résolution DNS (AD)	⚓ ✎ ⧉ ⊘ 🗑
☐	✋	0 /0 B	IPv4 TCP	DMZ net	*	10.2.10.254	*	*	none		Empêcher la DMZ d'accéder à l'interface de gestion pfSense	⚓ ✎ ⧉ ⊘ 🗑
☐	✋	0 /0 B	IPv4 *	DMZ net	*	LAN net	*	*	none		Interdiction acces LAN	⚓ ✎ ⧉ ⊘ 🗑
☐	✖	0 /342 KiB	IPv4 *	*	*	*	*	*	none		Block All	⚓ ✎ ⧉ ⊘ 🗑

2.3 Le Commutateur de Cœur de Réseau (Cisco 2960)

2.3.1 Rôle Opérationnel dans l'Architecture

Commutation de niveau 2 : Il assure la connectivité physique de l'ensemble des équipements et serveurs de la maquette (Active Directory, FOG, postes clients).

Isolation par domaine de diffusion : Grâce au protocole de VLAN, il fragmente un commutateur physique unique en plusieurs réseaux logiques étanches.

Sécurisation locale : Il constitue la première ligne de défense contre les intrusions physiques ou logiques au sein des salles de cours de l'établissement.

2.3.2 Configuration et Affectation des Ports d'Accès

La base de données des VLANs (`show vlan brief`) répartit les interfaces physiques par blocs de 5 ports configurés en mode accès statique

```
Switch(config-if)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Gi0/1, Gi0/2
10   RnD                              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
20   RH                               active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
30   SI                               active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

2.3.3 Sécurisation des Ports

Principe appliqué : Extinction administrative complète.

Périmètre : L'intégralité des ports non attribués à un service de `Fa0/16` à `Fa0/23`, ainsi que les interfaces `Gi0/1` et `Gi0/2`) sont verrouillés via la commande `shutdown`.

Objectif : Empêcher un utilisateur malveillant de connecter un équipement espion ou pirate sur une prise réseau vacante du switch.

```
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
```

2.3.4 Liaison Montante (Trunk)

Interface dédiée : Le port `FastEthernet0/24` est configuré comme l'Uplink exclusif vers l'interface réseau `igb1` du firewall pfSense.

```
interface FastEthernet0/24
 switchport trunk allowed vlan 1,10,20,30
 switchport mode trunk
```

Commande de restriction : La directive `switchport trunk allowed vlan 1,10,20,30` filtre strictement le transit réseau, interdisant la circulation de trames appartenant à des VLANs non déclarés ou non maîtrisés.

2.4 Centralisation des Identités et des Noms (Windows Server AD DS & DNS)

2.4.1 Rôle et Spécifications du Contrôleur de Domaine

Rôle central : La machine virtuelle de l'infrastructure assure la centralisation des droits, l'authentification des sessions et la résolution de noms pour le domaine racine.

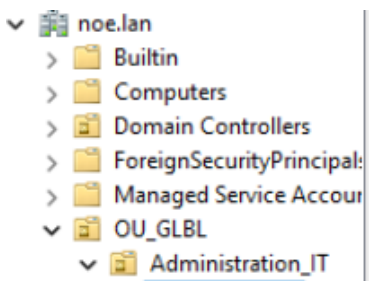
- **Identité du serveur :** Le rôle AD DS (Active Directory Domain Services) est hébergé sur le serveur Windows Server nommé **`WIN-404E0VHC5V2`**.
- **Nom de domaine étendu :** L'arbre de l'annuaire est configuré sous le suffixe racine unique **`noe.lan`**.

2.4.2 Organisation de l'Annuaire (Active Directory)

Afin de structurer le parc et d'appliquer des stratégies de groupe (GPO) distinctes.
J'ai mis en place une Unité d'Organisation (OU) principale découpée selon les services du lycée :

`OU_GLBL` (Racine de la structure organisationnelle)

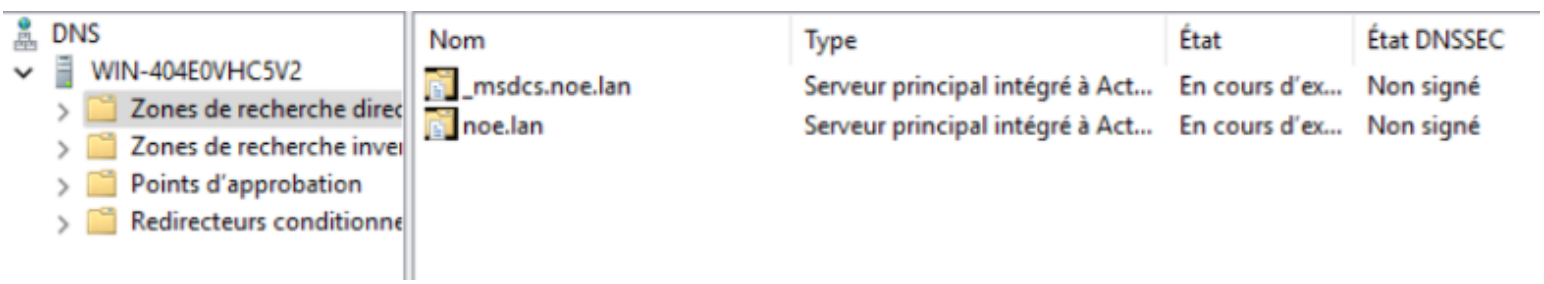
- **`Administration_IT`** (Comptes d'administration et d'infrastructure informatique)
  - `acc_Admin` ➔ Contient le compte utilisateur administrateur du concepteur de la maquette : **Noé NL. Leguay**.
  - `acc_Serv` ➔ Destiné au confinement des comptes de services applicatifs.
- **`Production`** (Objets et utilisateurs métiers du domaine)
  - `Aministration` ➔ Services administratifs de l'établissement.
  - `poste-libres-servi` ➔ Objets ordinateurs des terminaux en accès libre.
  - `RH` ➔ Personnel du pôle Ressources Humaines.



2.4.3 Résolution de Noms (Serveur DNS)

Le rôle DNS est intégré directement à Active Directory, assurant la réplication automatique et la sécurité des enregistrements réseau. Le serveur gère deux zones de recherche directe principales :

- **`noe.lan` :** Zone de recherche principale de l'établissement. Elle contient les enregistrements d'hôtes (A), les alias (CNAME) et les pointeurs de l'ensemble des serveurs fixes de l'infrastructure (serveur FOG, base de données, etc.).
- **`_msdcs.noe.lan` :** Zone DNS spécifique à Microsoft Active Directory. Elle est critique car elle référence les identifiants uniques (GUID) du contrôleur de domaine, les catalogues globaux (GC) et les protocoles d'authentification réseau (enregistrements LDAP et Kerberos SRV).



2.5 Centralisation et Déploiement de Parc (FOG Server)

2.5.1 Rôle et Spécifications de la VM FOG

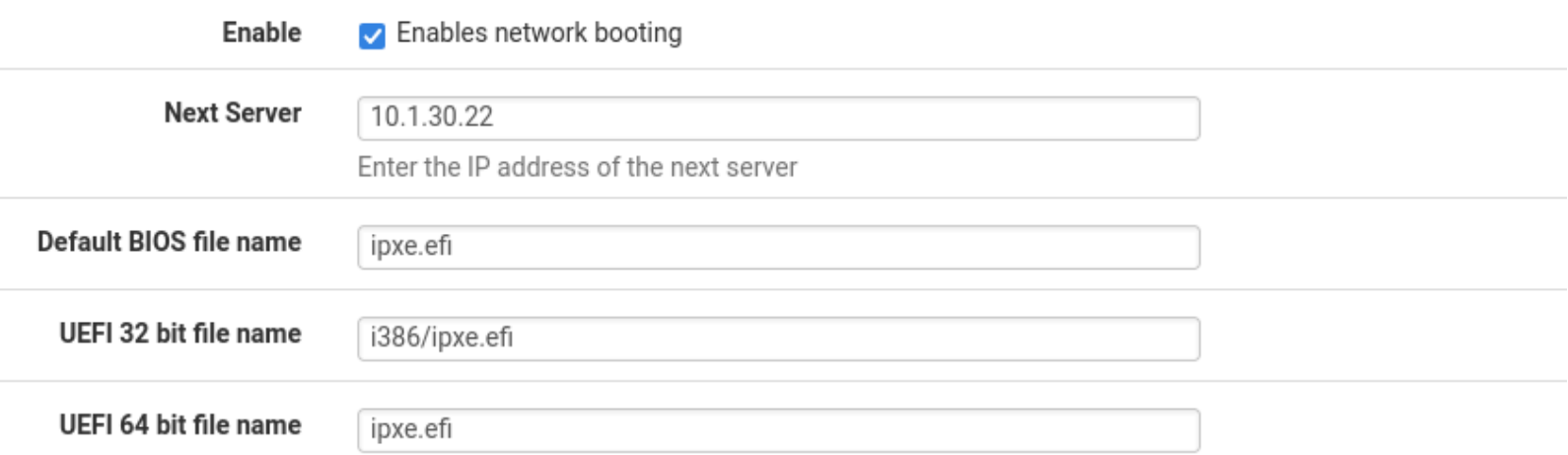
- **Rôle industriel :** Solution centralisée d'imagerie réseau permettant l'automatisation du clonage, de la capture et de la télédistribution des systèmes d'exploitation (Linux Debian 12) pour l'établissement.
- **Système d'exploitation :** Instance virtuelle propulsée par une distribution Linux Debian 12 propre.
- **Ancrage réseau :** Configuré avec l'adresse IP fixe `10.1.30.22` et confiné au sein du VLAN 30 (SI / Infrastructure) pour isoler les flux de réplication lourds.

2.5.2 Dépendance DHCP et Mécanisme d'Amorçage (iPXE)

Pour intégrer le service FOG à l'infrastructure, le serveur s'appuie sur le serveur DHCP centralisé du pare-feu pfSense qui distribue les directives de boot réseau (*Network Booting*) sur le scope du VLAN 30 :

- **Option DHCP 66 (Next Server) :** Renseignement de l'IP du serveur FOG (`10.1.30.22`) comme serveur TFTP légitime.

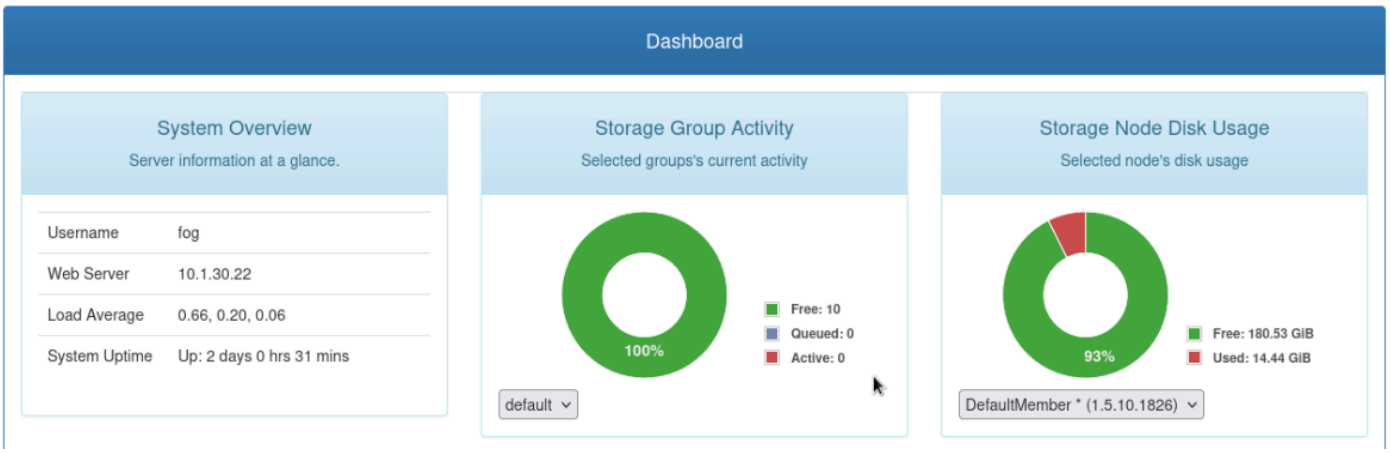
- **Option DHCP 67 (Bootfile Name) :** Injection du binaire `ipxe.efi` adapté aux architectures UEFI modernes de l'hyperviseur.



Lors du démarrage d'une machine vierge, la carte réseau intercepte ces options, charge le micro-noyau iPXE via HTTP à haute vitesse et affiche le menu graphique FOG sans aucune intervention humaine locale.

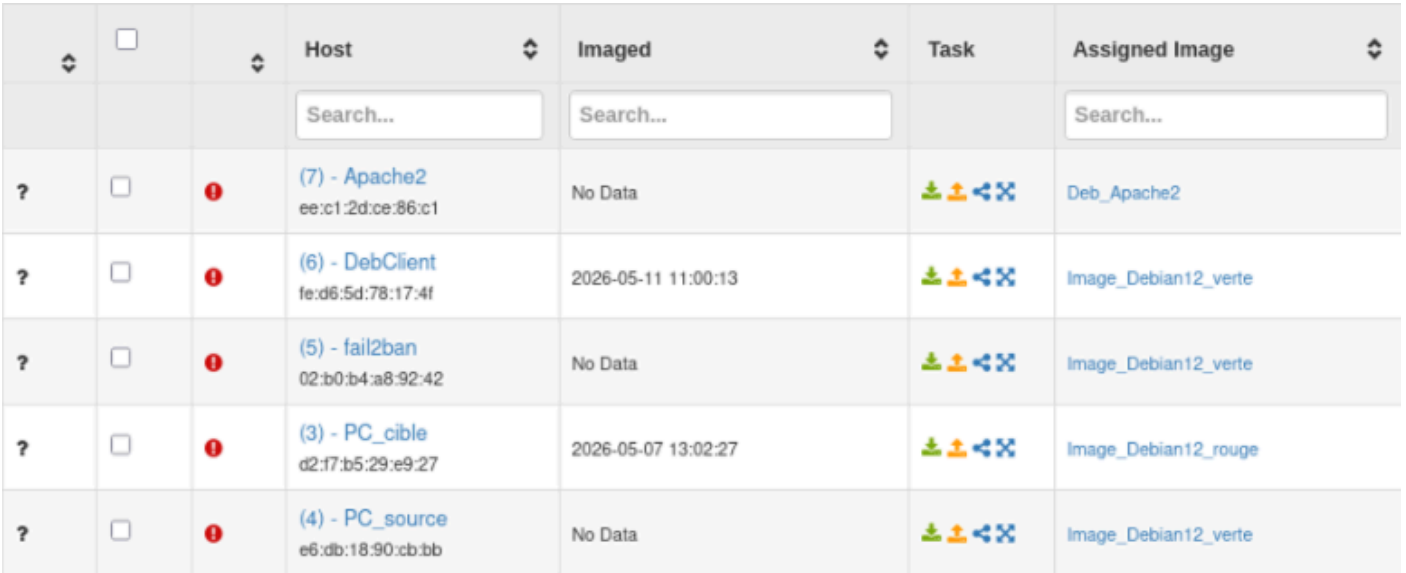
2.5.3 Stratégie d'Imagerie, Stockage et Registre des Hôtes

- **Capacité du Storage Node** : Monitorage et validation de la santé de l'espace disque du nœud par défaut (`default`) affichant **180.53 GiB libres** (93 % d'espace disponible) pour stocker la bibliothèque de masters.



- **Format dynamique des images :** Les profils d'images utilisent le format universel **Single Disk - Resizable** opéré par le moteur de blocs **Partclone Zstd (niveau de compression 6)**. FOG ne copie que les blocs de données utiles et réadapte automatiquement la géométrie des partitions à la taille du disque de destination lors du déploiement.

- **Contrôle d'accès par adresse MAC :** Sécurisation et authentification de la chaîne de déploiement. FOG rejette tout terminal inconnu : chaque hôte de la maquette (`PC_source`, `PC_cible`) doit être explicitement enregistré dans la base via son adresse MAC physique.



PARTIE 3 : SÉCURISATION APPLICATIVE ET DÉFENSE ACTIVE (FAIL2BAN)

3.1 Installation de Fail2ban

3.1.1 Préparation de l'environnement hôte

Actif cible : Le service de protection est déployé directement sur le serveur Web public `Apache2` (VMID 103).

Vous pouvez néanmoins l’installer sur n’importe quelle machine Debian 12.

Objectif de sécurité : Mettre en œuvre un système de prévention des intrusions (HIPS) pour analyser les journaux système et bloquer dynamiquement au niveau réseau les comportements malveillants (attaques par force brute, scans de vulnérabilités).

3.1.2 Processus d'installation des paquets

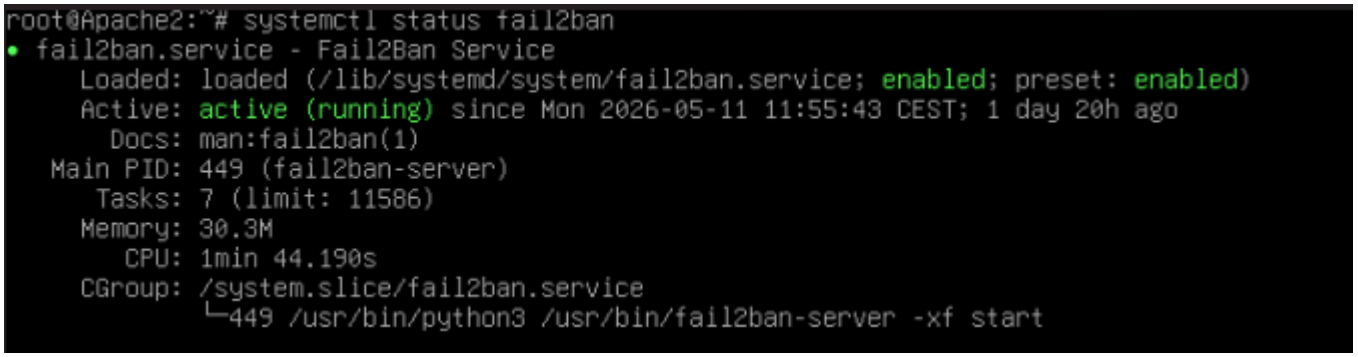
mise a jour des paquets :
su -
apt update

installation du paquet fail2ban :
apt install fail2ban -y

3.1.3 Vérification de l'état initial du service

tappez la commande suivante :
systemctl status fail2ban

la commande devrais vous afficher ceci :



3.2 Configuration de Fail2ban

3.2.1 Stratégie de gestion des fichiers de configuration

- **Règle d'or de l'administration :** Le fichier d'origine `/etc/fail2ban/jail.conf` ne doit jamais être modifié manuellement afin d'éviter l'écrasement des paramètres lors des futures mises à jour du paquet.

- **Méthodologie appliquée :** Création d'un fichier de surcharge local nommé **`jail.local`** pour accueillir nos directives et écraser de manière propre la configuration d'usine.

tapez donc la commande:

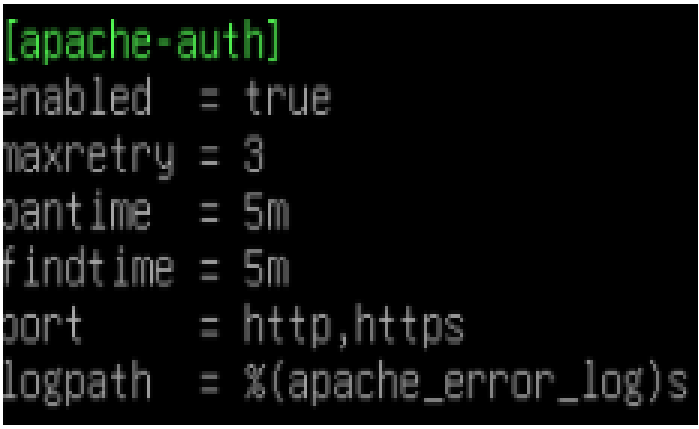
sudo /etc/fail2ban/jail.local

et commençons par créer/modifier la jail apache-auth.

A. Configuration de la prison Web

Les jails se présentent sous ce format:

[apache-auth]
enabled = true
maxretry = 3
bantime = 5m
findtime =5m
port = http,https
logpath = /var/log/apache2/error.log



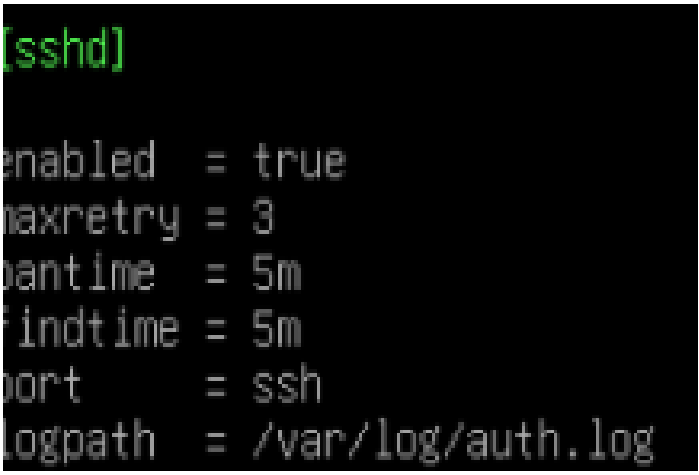
Avec
“maxretry” le nombre d’essai maximum avant le bannissement
“bantime” le temp de bannissement et “m” pour minute
“findtime” le temp durant lequel le nombre maximum de tentatives défectueuses doivent être effectuée pour être banni
“logpath” l’emplacement du fichier de log a analyser.

Mécanisme : Elle scrute en continu le journal d'authentification système `/var/log/auth.log` à la recherche des chaînes d'erreurs de type *Failed password* ou *Invalid user*.

B. Configuration de la prison SSH

[sshd]

enabled = true
maxretry = 3
bantime = 5
findtime =5m
port   = ssh
logpath = /var/log/auth.log



Mécanisme : Elle analyse le journal d'erreurs Apache `/var/log/apache2/error.log` pour détecter les échecs d'authentification HTTP répétés (codes erreurs 401 Unauthorized ou 403 Forbidden provoqués par des fichiers `.htaccess`).

3.2.4 Application des modifications

Pour valider et charger la nouvelle configuration réseau chiffrée, le démon doit être redémarré:

```
sudo systemctl restart fail2ban
```

3.3 Test et Validation : Scénario d'attaque et de défense active via SSH

Le scénario de recette simule une attaque par force brute SSH menée depuis un poste client de test présent sur le réseau afin de valider la réponse automatique de l'infrastructure.

3.3.1 Simulation de l'attaque force brute depuis la machine de test

IP de l'attaquant : `10.1.30.11` (Poste client d'infrastructure ou de test)

Action menée : Exécution de 3 tentatives de connexion SSH consécutives avec le mauvais mot de passe vers la VM Apache2 en DMZ (`10.2.10.10`).

ssh portal@10.2.10.10

```
root@IMGsource:/home/btssio# ssh portal@10.2.10.10
The authenticity of host '10.2.10.10 (10.2.10.10)' can't be established.
ED25519 key fingerprint is SHA256:wureLs3ekG2gjgaK/B1G5Q725MspTSiboHh2vesBd7o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yr^[[2~eyes
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.2.10.10' (ED25519) to the list of known hosts.
portal@10.2.10.10's password:
Permission denied, please try again.
portal@10.2.10.10's password:
Permission denied, please try again.
portal@10.2.10.10's password:
portal@10.2.10.10: Permission denied (publickey,password).
root@IMGsource:/home/btssio# ssh portal@10.2.10.10
ssh: connect to host 10.2.10.10 port 22: Connection refused
root@IMGsource:/home/btssio#
```

Résultat immédiat : À la troisième tentative erronée, la session SSH est brutalement interrompue et le terminal de l'attaquant affiche le message restrictif `ssh: connect to host 10.2.10.10 port 22: Connection refused`.

3.3.2 Phase 2 : Analyse de la détection sur le serveur sécurisé

Sur la machine virtuelle `Apache2` (`10.2.10.10`), l'analyse des journaux d'activité confirme la prise en compte de l'attaque et le déclenchement des contre-mesures.

Interrogation en temps réel de la prison SSH :

sudo fail2ban-client status sshd

L'analyse du retour de la commande valide l'activité du filtre : le compteur d'IP bannies passe à 1 (`Currently banned: 1`) et l'adresse IP exacte de l'attaquant (`10.1.30.11`) apparaît explicitement dans la liste noire (*Banned IP list*).

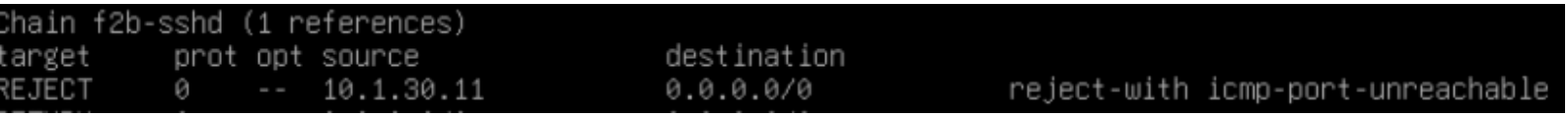
3.3.3 Phase 3 : Vérification du blocage réseau dynamique au niveau du Pare-feu local

Pour neutraliser la menace, Fail2ban interagit directement avec le noyau Linux en modifiant les chaînes de filtrage de l'utilitaire `iptables`.

Commande d'affichage des règles de filtrage actives :

sudo iptables -L -n

Analyse de la table de décision : Le logiciel a injecté de manière dynamique une règle d'interception majeure au sein de la chaîne dédiée `f2b-sshd` :



Conséquence technique : Tout paquet réseau émanant de l'IP source `10.1.30.11` à destination du serveur est instantanément détruit et rejeté avec une notification d'inaccessibilité de port ICMP (`REJECT reject-with icmp-port-unreachable`), garantissant la protection absolue des ressources du serveur face à cette menace.

PARTIE 4 : CONCLUSION ET BILANS DE LA RÉALISATION

4.1 Synthèse de l'Infrastructure

La conception et la mise en œuvre de cette maquette réseau et système valident l'interconnexion complète des services du Lycée Venise Verte. En associant la virtualisation (**Proxmox VE**), le routage périmétrique (**pfSense**), la commutation de niveau 2 (**Cisco**) et la défense active (**Fail2ban**), l'infrastructure répond de manière cohérente aux exigences de centralisation, de haute disponibilité et de contrôle des flux requises pour l'épreuve E6.

4.2 Bilan Personnel

La réalisation de ce projet de fin d'études m'a permis de consolider l'ensemble des compétences théoriques et pratiques acquises durant

mon cursus de **BTS SIO option SISR**. Être confronté à la mise en œuvre concrète de mécanismes de défense active comme Fail2ban, aux subtilités du filtrage d'un pare-feu périmétrique et à la gestion de l'amorçage réseau a développé mon autonomie et ma rigueur méthodologique, des qualités indispensables pour mon futur parcours d'administrateur systèmes et réseaux.