ÉPREUVE E6 dossier: FOG

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

SOMMAIRE ANALYTIQUE

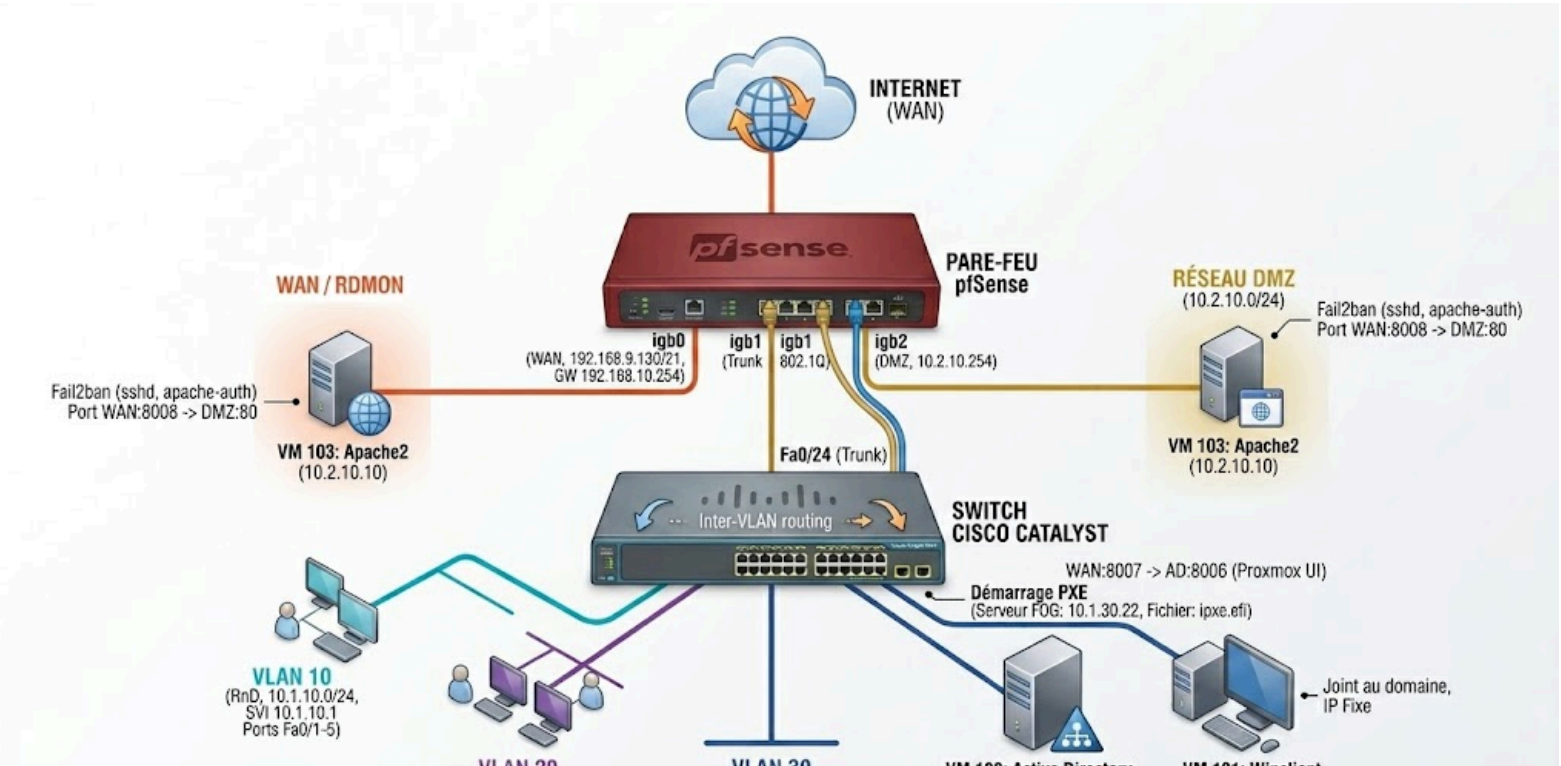
PARTIE 1 : PRÉSENTATION GÉNÉRALE DU PROJET ET DE L'ARCHITECTURE

1.1 Contexte et Objectifs

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 situé dans la DMZ.

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 :

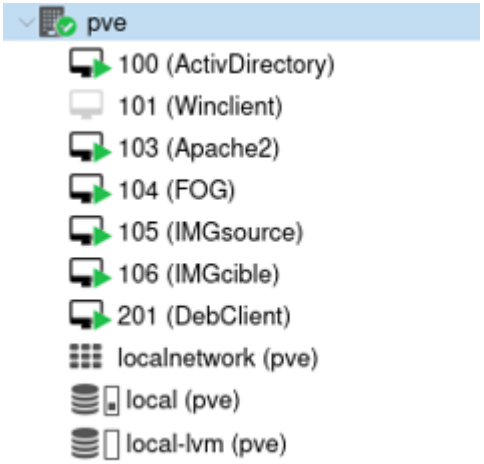
Segment Réseau	Interface Physique / Virtuelle	Sous-réseau IP	Passerelle (pfSense)	Rôle Technique et Équipements Connectés
WAN	igb0	192.168.9.130/21	192.168.10.254	Interface de sortie vers l'infrastructure d'accueil.
LAN	igb1 (Natif)	10.1.1.0/24	10.1.1.254	Segment natif dédié à l'administration d'origine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

```
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.

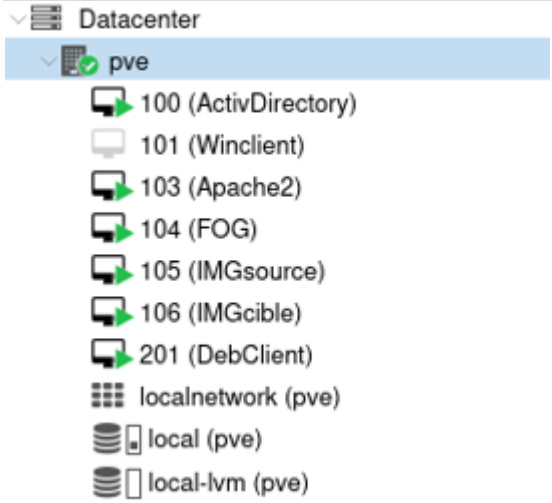
- **Configuration clé :**

  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

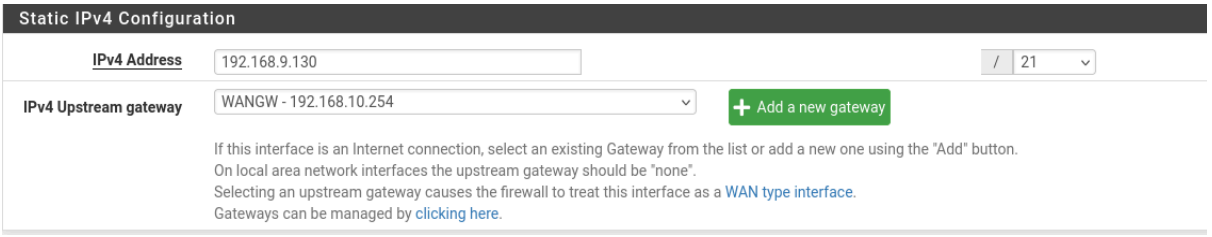
- **Pivot de sécurité** : Il est positionné à la frontière entre le réseau externe non de confiance (WAN) et les réseaux internes de l'établissement.

- **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.

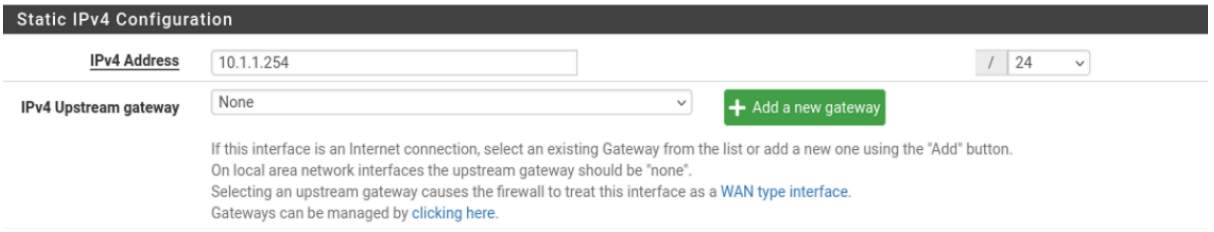
- **Multi-services centralisés :** En plus du filtrage brut, il assure l'étanchéité de la DMZ, la translation d'adresses réseau (NAT) et l'aiguillage de la chaîne d'amorçage via son serveur DHCP.

B Configuration Globale et Assignation des Interfaces

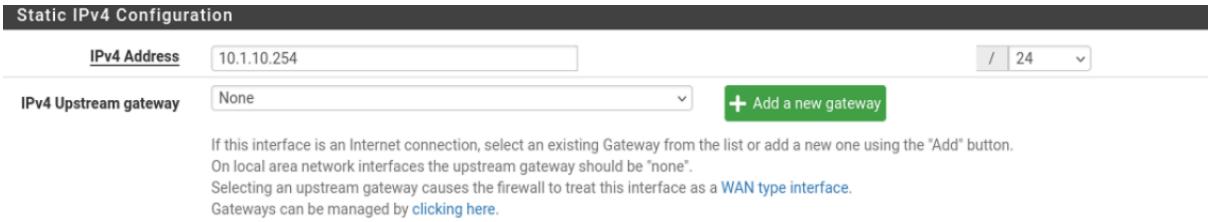
- igb0 (WAN) : Interface connectée à la sortie Internet. Elle récupère son adresse IP via l'infrastructure d'accueil (192.168.9.130/21) et pointe vers la passerelle externe 192.168.10.254.



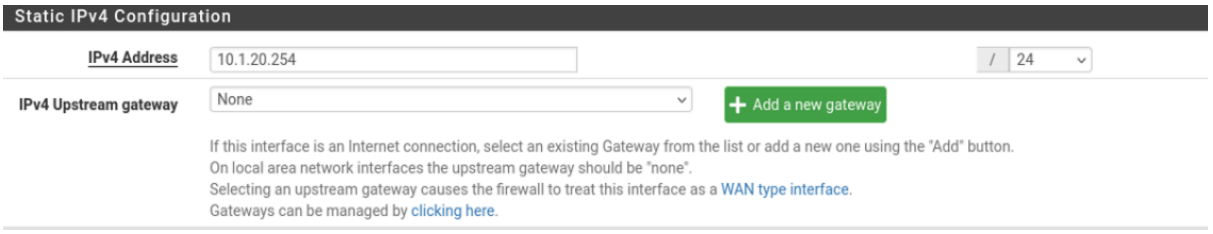
- igb1 (LAN / Trunk Virtuel) : Interface connectée au commutateur Cisco 2960. C'est sur ce segment que sont rattachés les sous-réseaux logiques (VLAN 10, VLAN 20 et VLAN 30).
  Son adresse IP d'administration native est 10.1.1.254/24.



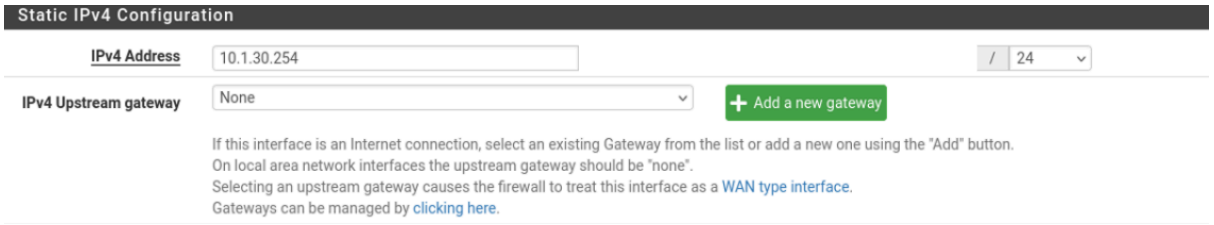
  - vlan10 (sur le port physique igb1): Interface qui permet de joindre les utilisateurs du vlan 10 . (ip:10.1.10.254)



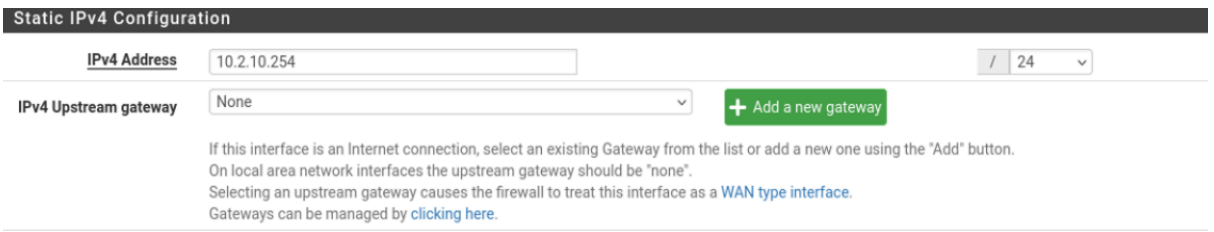
- vlan20 (sur le port physique igb1): interface qui permet de joindre les utilisateurs du vlan 20.(ip:10.1.20.254)



- 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)

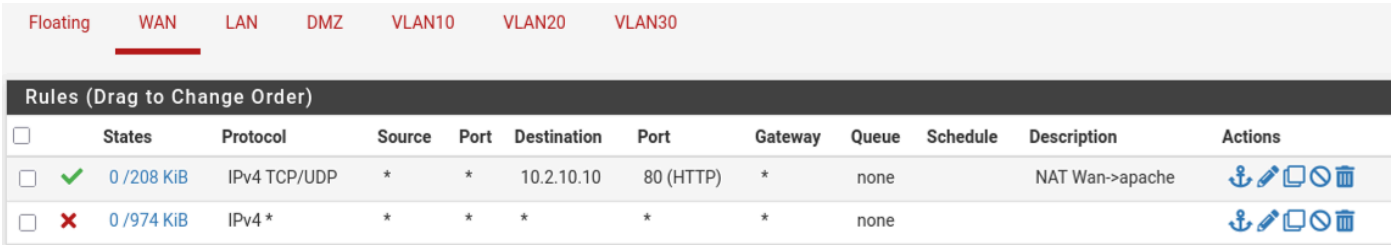
La politique globale appliquée sur le pare-feu est le blocage implicite :

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

I) Règles de l'interface WAN

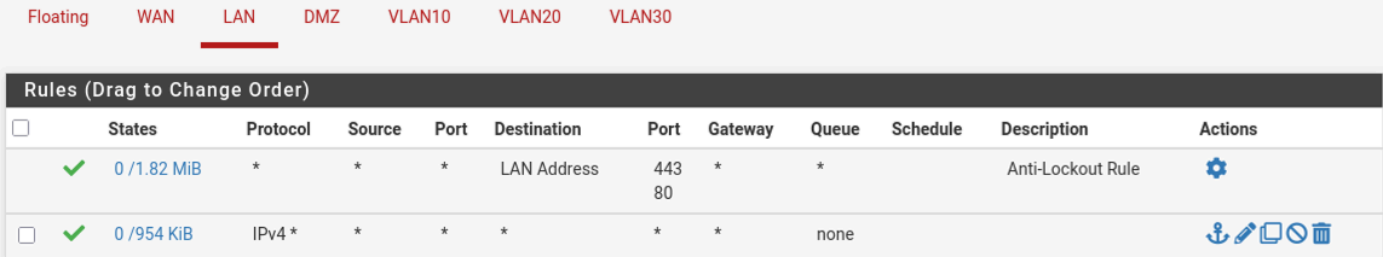
L'interface WAN bloque par défaut toutes les connexions initiées depuis l'extérieur, sauf celles autorisées par les règles de Port Forwarding.

- **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

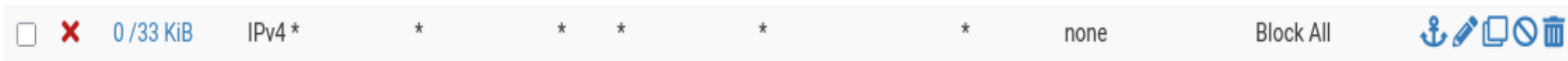
déploiement (HTTP/S, TFTP pour le boot iPXE, et NFS pour le transfert de l'image Partclone).

- **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`).

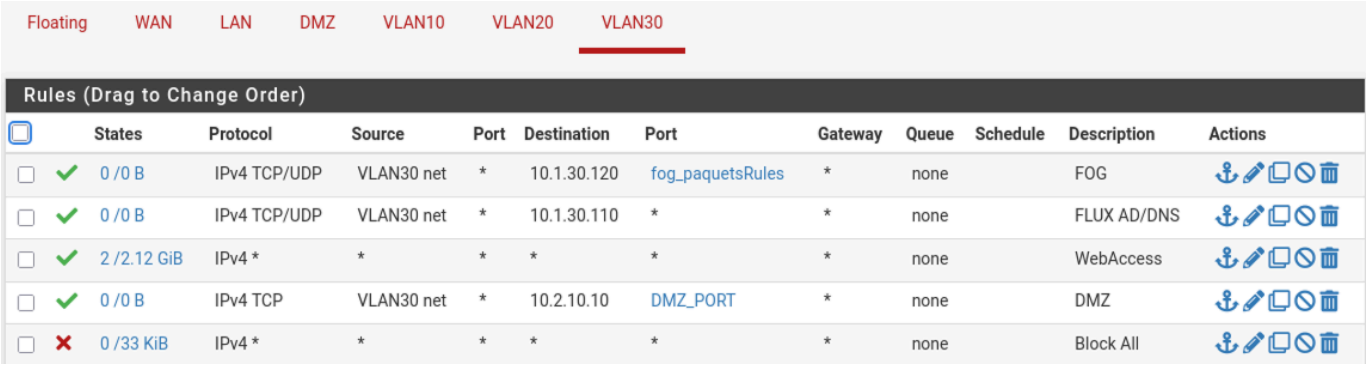
- **Accès Internet contrôlé :** J’active ou désactive cette règle en fonction de l’envie ou non d’acceder à internet.

- **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 :



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/UDP	VLAN30 net	*	10.1.30.120	fog_paquetsRules	*	none		FOG	
✓	0 /0 B	IPv4 TCP/UDP	VLAN30 net	*	10.1.30.110	*	*	none		FLUX AD/DNS	
✓	2 /2.12 GiB	IPv4 *	*	*	*	*	*	none		WebAccess	
✓	0 /0 B	IPv4 TCP	VLAN30 net	*	10.2.10.10	DMZ_PORT	*	none		DMZ	
✗	0 /33 KiB	IPv4 *	*	*	*	*	*	none		Block All	

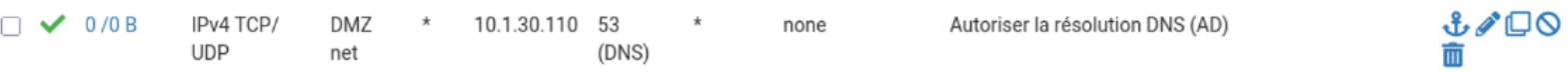
IIII Règles de l'interface DMZ

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 :

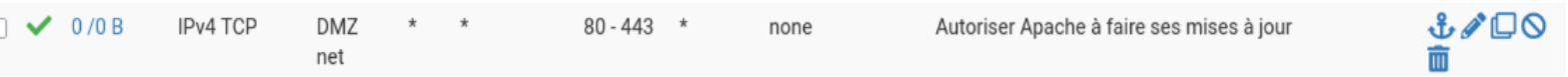
- **Étanchéité et confinement critiques :** Interdiction absolue d'initier une connexion vers le réseau d'administration (LAN) ou vers la zone d'infrastructure (VLAN 30) afin de bloquer toute tentative de pivotement ou d'attaque par rebond si le site web venait à être compromis.

	0 /0 B	IPv4 *	DMZ net	*	LAN net	*	*	none	Interdiction acces LAN	

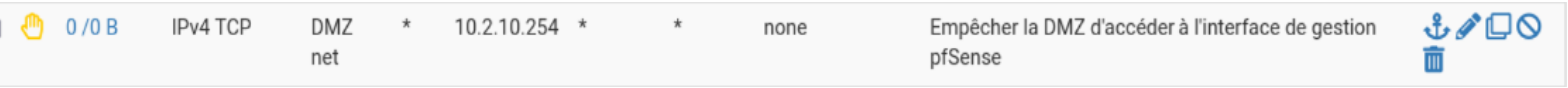
- **Résolution DNS contrôlée :** Autorisation unique d'émettre des requêtes DNS vers le contrôleur de domaine de confiance (`10.1.30.110`) sur le port `UDP/53` pour ses besoins de résolution internes.



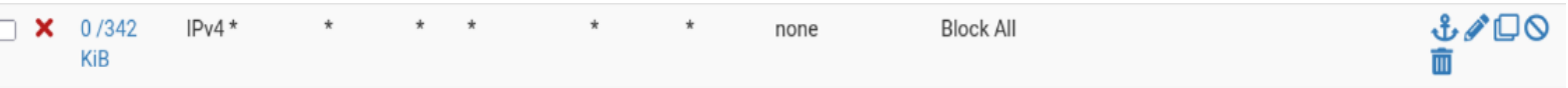
- **Accès WAN restrictif :** Autorise la machine à sortir vers Internet uniquement sur les ports `80 (HTTP)` et `443 (HTTPS)` pour l'exécution des mises à jour système et la récupération des dépendances logicielles.



- **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.



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.

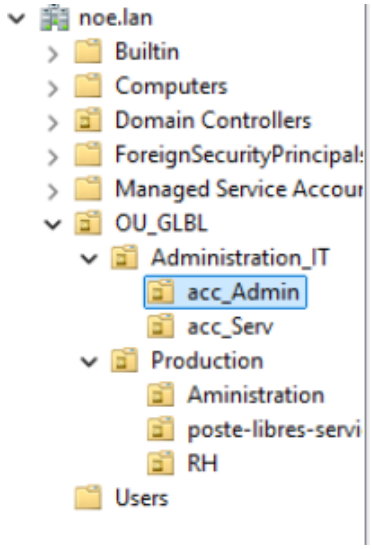
- **Identité du serveur :** Le rôle AD DS (Active Directory Domain Services) est hébergé sur le serveur Windows Server nommé **`WIN-404E0VHC5V2`**.
- **Nom de domaine étendu :** L'arbre de l'annuaire est configuré sous le suffixe racine unique **`noe.lan`**.

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)

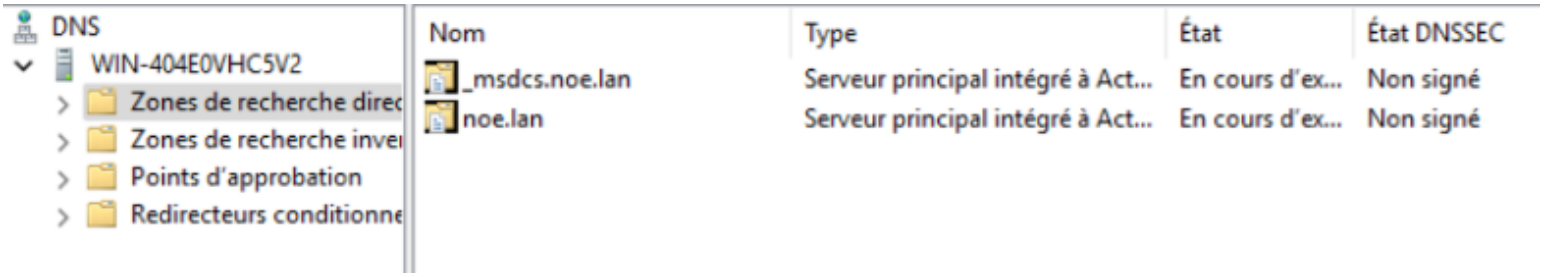
- `Administration_IT` (Comptes d'administration et d'infrastructure informatique)
    - `acc_Admin` ➔ Contient le compte utilisateur administrateur du concepteur de la maquette : **Noé NL. Leguay**.
    - `acc_Serv` ➔ Destiné au confinement des comptes de services applicatifs.
- `Production` (Objets 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 Hébergement Web et Sécurité Système (Coexistence Apache2 & Fail2ban)

2.5.1 Rôle et Confinement en DMZ

- **Hébergement de production :** La machine virtuelle propulse le site Web vitrine de l'établissement (fichiers sources stockés dans le répertoire `/var/www/html/`).

```
root@Apache2:~# ls /var/www/html
index.html  LyceeVV.jpg  post-bac.html  sport-options.html  style.css  voie-generale.html
```

- **Système d'exploitation :** Instance virtuelle basée sur une distribution Linux Debian 12.

- **Isolation réseau :** Implantée sur l'adresse IP fixe `10.2.10.10` au sein d'une zone démilitarisée (DMZ) étanche afin de confiner le serveur public et de protéger le cœur de réseau en cas de compromission.

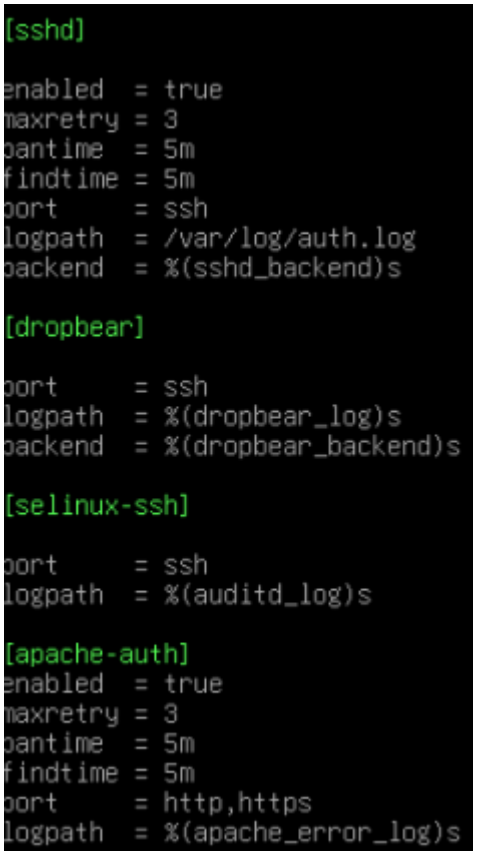
2.5.2 Coexistence et Durcissement Local (Fail2ban)

Pour protéger le serveur contre les attaques par force brute ou par dictionnaire, le service de détection et de prévention d'intrusions **Fail2ban** coexiste sur le même système d'exploitation que le serveur HTTP **Apache2**.

Le fichier local de configuration (`/etc/fail2ban/jail.local`) active deux prisons (**jails**) de surveillance active :

- **Prison `[sshd]` :** Elle scrute le journal d'authentification système `/var/log/auth.log`. Elle bloque l'adresse IP source d'un attaquant après 3 échecs de connexion SSH.

- **Prison `[apache-auth]` :** Elle surveille le journal d'erreurs `/var/log/apache2/error.log`. Elle bannit toute IP générant des accès répétés non autorisés (erreurs d'authentification HTTP 401 ou 403 sur des répertoires protégés).



PARTIE 3 : CENTRALISATION, CLONAGE ET DÉPLOIEMENT DE PARC (FOG SERVER)

3.1 Installation de FOG

Le déploiement du serveur d'imagerie s'exécute sur une machine virtuelle dédiée au sein de notre hyperviseur Proxmox VE.

Spécifications de la VM (VMID 104) :

- **Système d'exploitation :** Linux Debian 12 (Minimal / Netinst).
- **Ressources allouées :** 2 vCPU, 4 Go de RAM, disque de 200 Go (Stockage local-lvm).
- **Ancrage réseau :** Interface virtuelle `ens18` taguée sur le VLAN 30 (SI / Infrastructure).

Configuration de l'adressage IP statique :

```
su -
nano /etc/network/interfaces
auto ens18
iface ens18 inet static
        address 10.1.30.22
        netmask 255.255.255.0
        gateway 10.1.30.254
        dns-nameservers 10.1.30.110
```

contrôle x et entrée

Mise à jour complète des dépôts et des paquets existants :

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

Installation des prérequis système (Git et Curl) :

```
sudo apt install git curl -y
```

Clonage du dépôt officiel de FOG Project dans le répertoire de déploiement :

```
cd /opt
sudo git clone https://github.com/FOGProject/fogproject.git
```

Le projet FOG fournit un script d'installation automatique qui gère toutes les dépendances (Apache, MariaDB, PHP, TFTP, etc.).

Lancement de l'installateur :

```
cd /opt/fogproject/bin/
sudo ./installfog.sh
```

Réponses aux questions du script :

What version of Linux... : 2 (Debian).
Installation Type : N (Normal).
Interface réseau : ens18
Router Address : 10.1.30.254
DNS Address : 10.1.30.100, 8.8.8.8.
DHCP Server : N
Internationalization : `Y` ou `N` selon votre préférence.

Pendant que le script tourne, il va s'arrêter pour nous demander de valider l'installation via l'interface Web

1. Ouvrez votre navigateur et allez à l'adresse : `http://votre_ip_serveur(10.1.30.22)/fog/management`
2. Cliquez sur le bouton "Install/Update Now".
3. Une fois terminé, revenez dans votre terminal et appuyez sur *Entrée* pour finaliser le script FOG.

Une fois l'installation terminée, vous pouvez vous connecter à la console d'administration.
**URL ** : `http://votre_ip_serveur/fog/`
Utilisateur par défau t : `fog`
Mot de passe par défaut : `password`

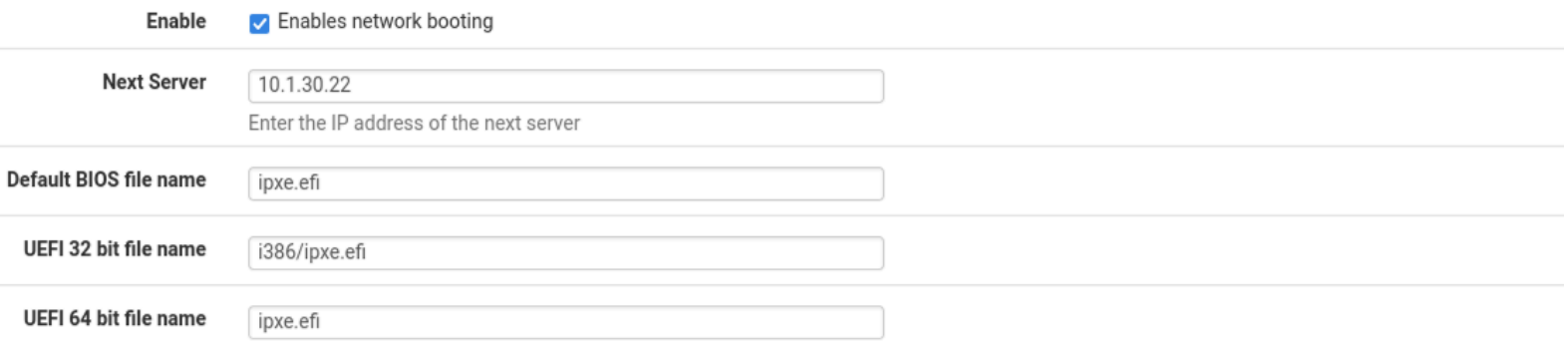
3.2 Configuration de FOG

A. Automatisation du Boot Réseau (Aiguillage pfSense)

Pour lier l'infrastructure réseau au serveur d'imagerie, la section *Network Booting* est activée sur le serveur DHCP du pare-feu pfSense (Scope VLAN 30) :

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

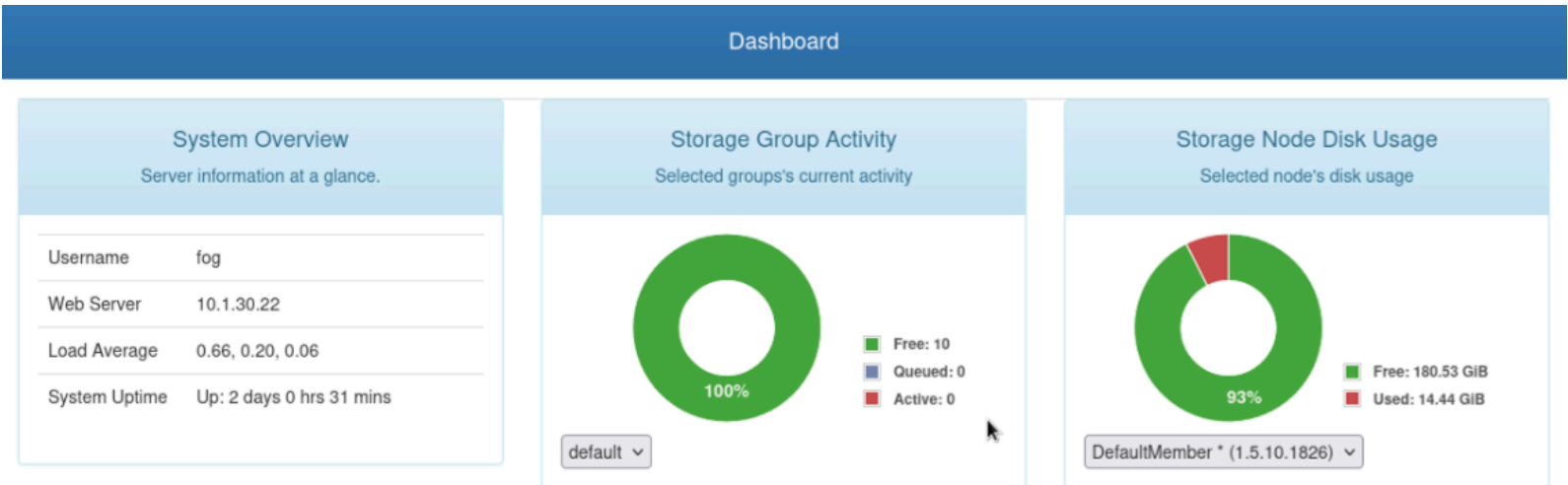
Option DHCP 67 (Bootfile Name) : Renseignement du binaire iPXE compilé pour les architectures UEFI de Proxmox : **`ipxe.efi`**



Monitorage de l'Espace Disque (Storage Node)

La prise en main de la console Web de FOG permet de valider la santé du nœud de stockage par défaut (`default`):

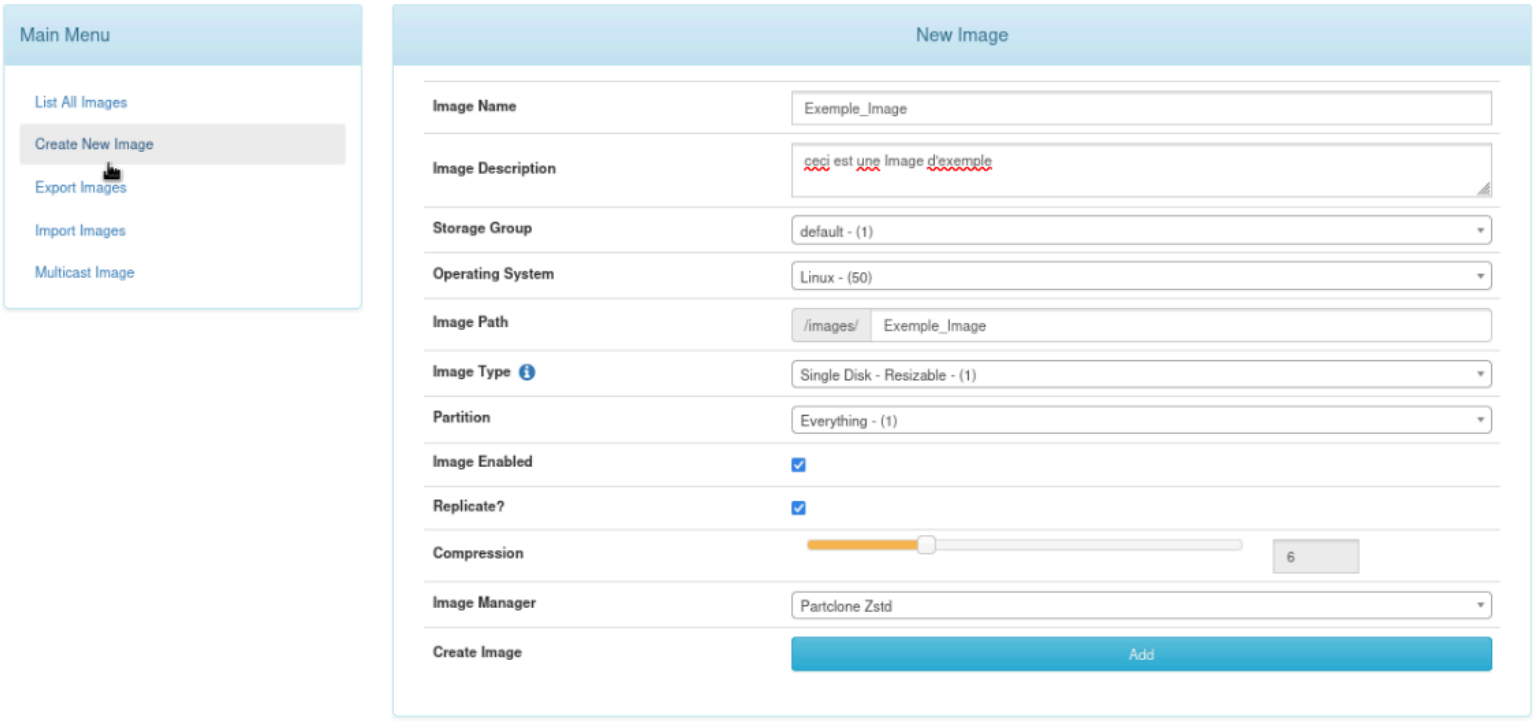
- **Espace disque libre : 180.53 GiB** disponibles (93 % d'espace vacant pour stocker la bibliothèque de masters).
- **Espace disque consommé : 14.44 GiB** occupés (7 % d'occupation).



Stratégie d'Imagerie Disque

Création du profil d'image de référence nommé **`Exemple_Image`** avec les variables de capture suivantes :

- **Image Type : `Single Disk - Resizable`** ➔ FOG analyse le système de fichiers pour ne copier que les blocs de données réels. À la redescente de l'image, il adapte automatiquement la table des partitions à la taille du disque de la machine cible.
- **Image Manager : `Partclone Zstd`** ➔ Utilisation de l'utilitaire de blocs Partclone associé à l'algorithme de compression **Zstandard (Zstd)** réglé au niveau **6** pour optimiser le transit réseau sans surcharger le processeur.



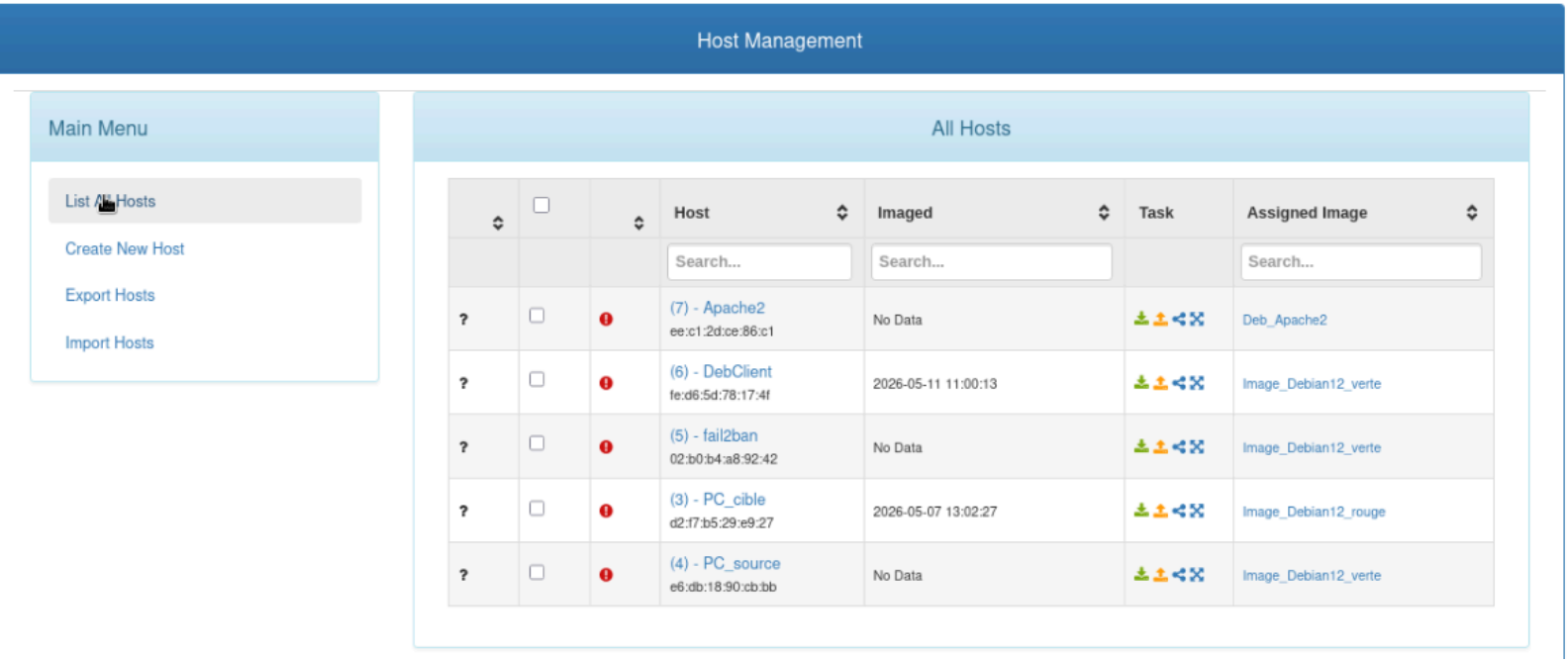
Registre de Contrôle des Hôtes (Host Management)

Pour interagir avec le serveur, chaque machine virtuelle cliente est enregistrée dans la base de données de confiance de FOG via l'adresse MAC physique de sa carte réseau :

`PC_source` (Machine Master de référence) ➔ MAC : `e6:db:18:90:cb:bb`

`PC_cible` (Machine vierge de destination) ➔ MAC : `d2:f7:b5:29:e9:27`

`DebClient` (Poste utilisateur Linux déployé) ➔ MAC : `fe:d6:5d:78:17:4f`

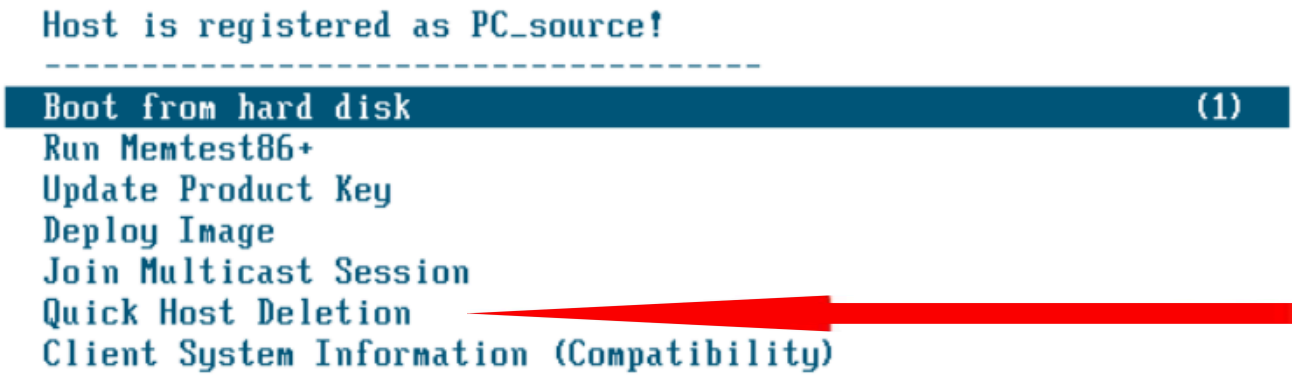


3.3 Déploiement d'une Image

Phase de Capture (PoC Upload)

Étape 1 : Enregistrer le PC source (S'il est nouveau)

1. Allumez le PC (ou la VM) et faites-le démarrer sur le réseau (**PXE**).
2. Dans le menu bleu de FOG, choisissez **Quick Registration and Inventory**.



(Sur le screen il est écris “quick host deletion” car je suis deja enregistré)

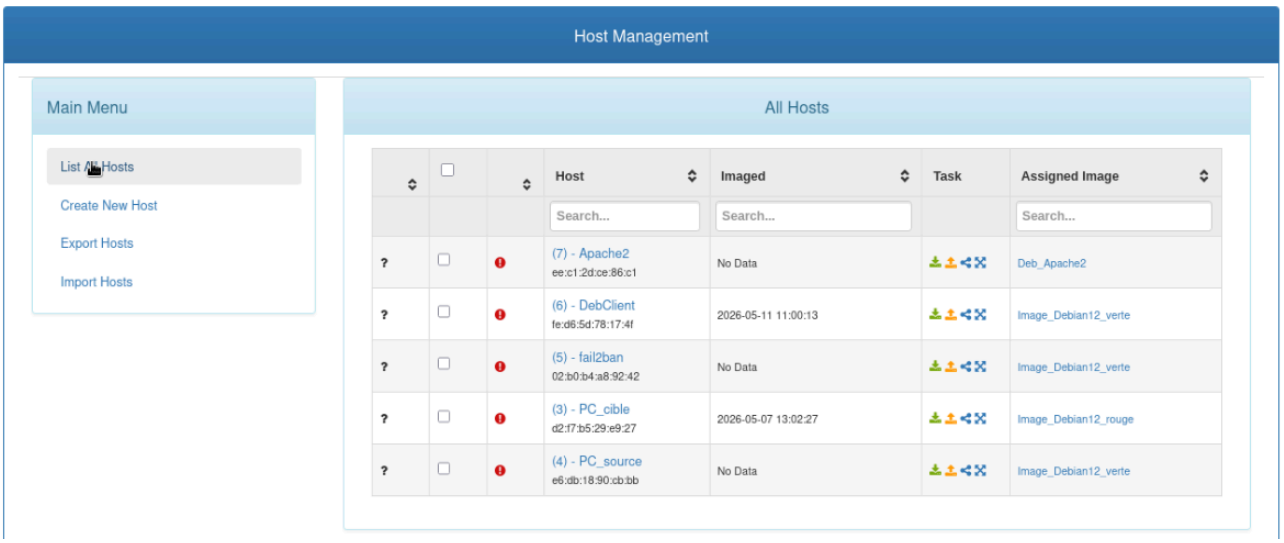
3. Le PC va s'enregistrer auprès du serveur puis s'éteindre (ou redémarrer).

Étape 2 : Assigner l'image au PC (Interface Web)

FOG doit savoir quelle image envoyer à quel ordinateur.

1. Connectez-vous à l'interface Web de votre FOG (http://10.1.30.22/fog/management).

2. Allez dans le menu **Hosts** (l'icône d'ordinateur) > **List All Hosts**.



3. Cliquez sur le nom de votre PC cible (par défaut, son nom est son adresse MAC).

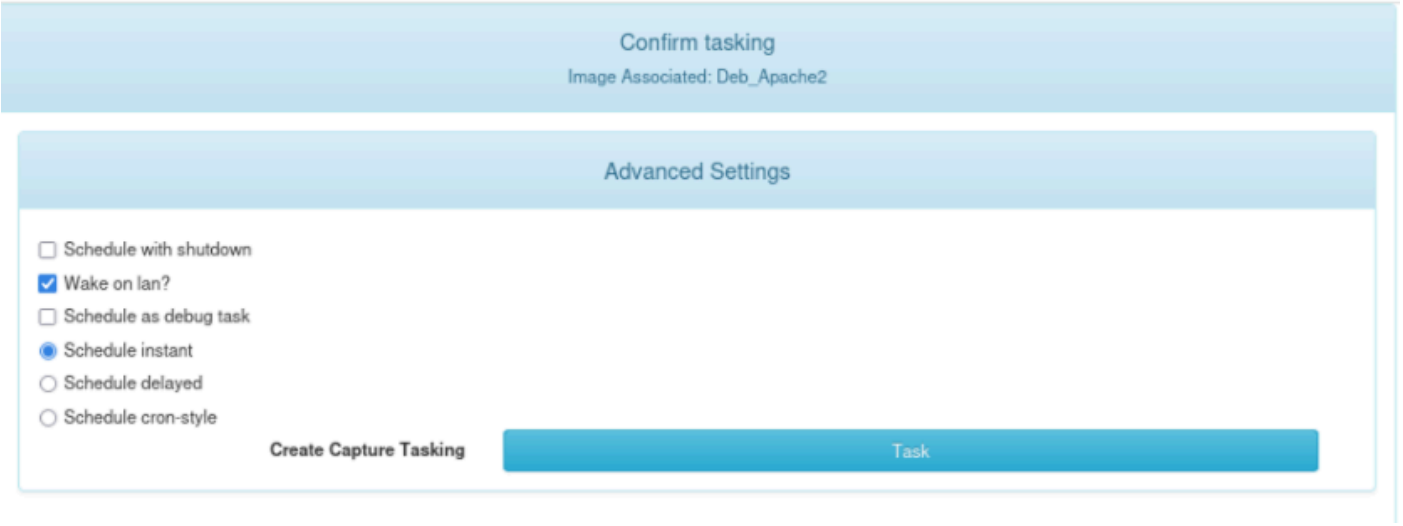
4. Cherchez le champ déroulant **Host Image** et sélectionnez l'image que vous voulez lui associer

5. Cliquez sur le bouton **Update** (en bas ou à droite) pour sauvegarder.

Étape 3 : Lancer la tâche de Capture

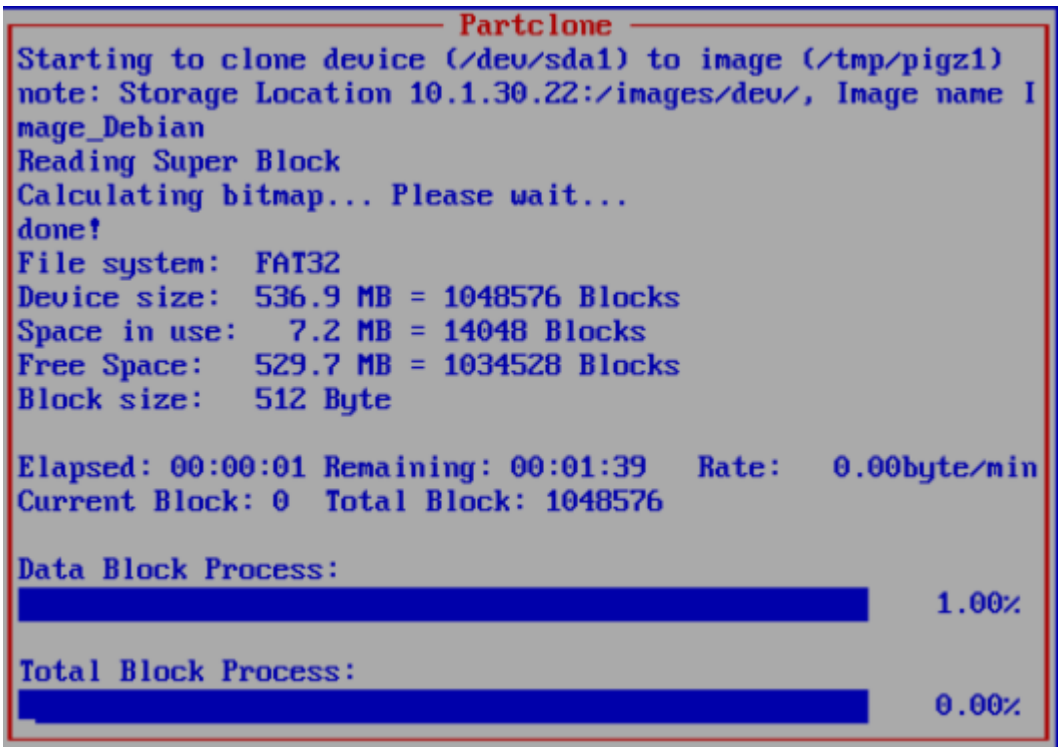
Toujours sur la fiche All Host de votre PC dans l'interface Web, cliquez sur le bouton **Capture** (il ressemble à un nuage avec une **flèche qui pointe vers le haut**).

Une page de confirmation apparaît. Cliquez sur **Create Task**.



Étape 4 : La capture

1. Démarrez votre PC client en vous assurant qu'il boot bien sur le réseau (**PXE**) en premier.
2. Cette fois-ci, le menu bleu n'apparaîtra pas. Le PC va détecter qu'une tâche de capture l'attend.
3. Il va charger **Partclone** (l'écran bleu avec la barre de progression).



4. Une fois arrivé à 100%, le PC redémarrera tout seul.

Etape 5 : Le déploiement

1 : Dans l'interface web de Fog dans All Host , choisissez le pc sur le quel vous voulez déployer votre image.

2 : Ensuite, sélectionnez l'image que vous voulez lui attribuer et appuyez sur save.

3 : Dans All Host cliquez sur le bouton vert avec une flèche qui pointe vers le bas sur la machine concernée. 

4 : Créez ensuite une Task comme pour la capture et répétez le même processus avec le PC client.

PARTIE 4 : SYNTHESE ET BILANS DE LA RÉALISATION

4.1 Synthèse de l'Infrastructure

La mise en œuvre de cette maquette réseau et système valide l'interconnexion complète des services structurels du Lycée Venise Verte. En associant la virtualisation brute (**Proxmox VE**), le routage périmétrique (**pfSense**), la segmentation de niveau 2 (**Cisco**) et l'industrialisation (**FOG**), l'infrastructure répond précisément aux exigences de centralisation, de performance et de maîtrise des flux requises pour l'épreuve E6.

4.2 Bilan Personnel

La conception et la réalisation de ce projet de fin d'études m'ont permis de consolider l'intégralité des compétences acquises durant mon cycle de **BTS SIO option SISR**. Être confronté aux réalités du terrain — comme les subtilités de l'amorçage iPXE en environnement UEFI ou l'analyse des logs réseau — a grandement développé mon autonomie et ma capacité de diagnostic, des atouts indispensables pour mon évolution future dans les métiers de l'administration systèmes et réseaux.