Installation et configuration de pfSense

Démonstration technique (E5)

Installation de pfSense sur une maquette virtualisée (VMware Workstation), puis segmentation du réseau en VLAN et construction d'une politique de filtrage : alias réutilisables, règles inter-segments, NAT, le tout selon une logique deny-by-default.

Le périmètre de cette réalisation est centré sur le pare-feu : installation, segmentation en VLAN et politique de filtrage. Les serveurs présents (Active Directory, fichiers, GLPI, Zabbix, sauvegarde) servent à justifier et à éprouver les règles ; leur configuration détaillée relève des réalisations associées.

Contexte de production et objectifs

Cette réalisation s'inscrit dans le cloisonnement réseau d'un établissement scolaire. En production, pfSense serait un boîtier physique placé en cœur de réseau, segmentant l'ensemble des usages et assurant l'accès Internet filtré. La maquette VMware Workstation reproduit fidèlement cette architecture : chaque VMnet correspond à un VLAN de production et chaque interface OPT à un segment. Le double NAT VMware isole la maquette du réseau physique sans en modifier la logique.

Objectifs (cahier des charges simplifié)

- Cloisonner les usages par segment selon le principe de moindre privilège (Zero Trust).
- Appliquer une politique deny-by-default : aucun flux n'est autorisé sans règle explicite.
- Mettre à disposition de chaque profil d'utilisateur les seuls services nécessaires : Internet filtré pour les élèves, enseignants et le Wi-Fi invités ; services internes (GLPI, Active Directory, fichiers) réservés aux segments légitimes.
- Protéger les sauvegardes : segment BACKUP (VLAN 99) isolé, flux push-only, pour résister à un rançongiciel.
- Préparer la supervision (Zabbix) et la détection d'intrusion (Suricata).

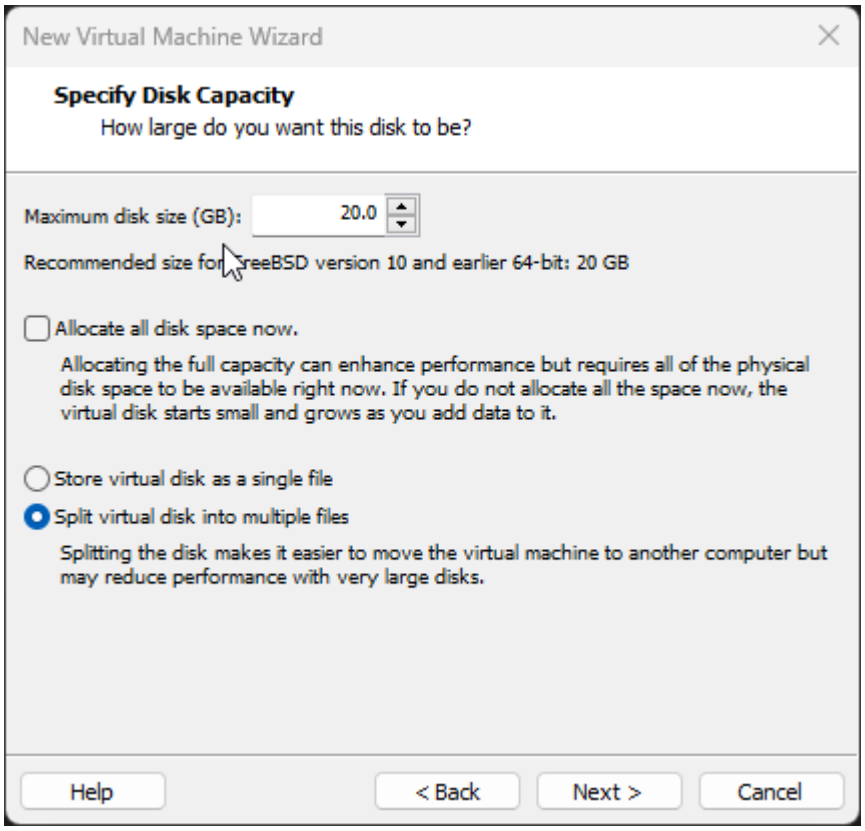
Compétences E5 visées

B1.4 Travailler en mode projet : analyse des objectifs et planification des étapes (installation → adressage → DHCP → filtrage → recette). B1.5 Mettre à disposition des utilisateurs un service informatique : déploiement de l'accès sécurisé aux services et recette des flux par profil (voir les tests d'acceptation en fin de document).

Installation de pfSense

pfSense = 4 Go de RAM, prévoir une marge pour Suricata

Dans pfSense, faire :



Au premier boot de la VM, le choix se portera sur une installation automatique en ZFS (Zettabyte File System), comme recommandé par pfSense depuis la version 2.6.0 (on évite UFS, robuste et utile dans certains cas mais plus sensible à la corruption). En effet, ZFS garantit l'intégrité des données par calcul de checksum, évitant ainsi la corruption du fichier XML du firewall. ZFS ajoute de plus des snapshots instantanés du système, qui présentent un intérêt en cas de corruption du

système.

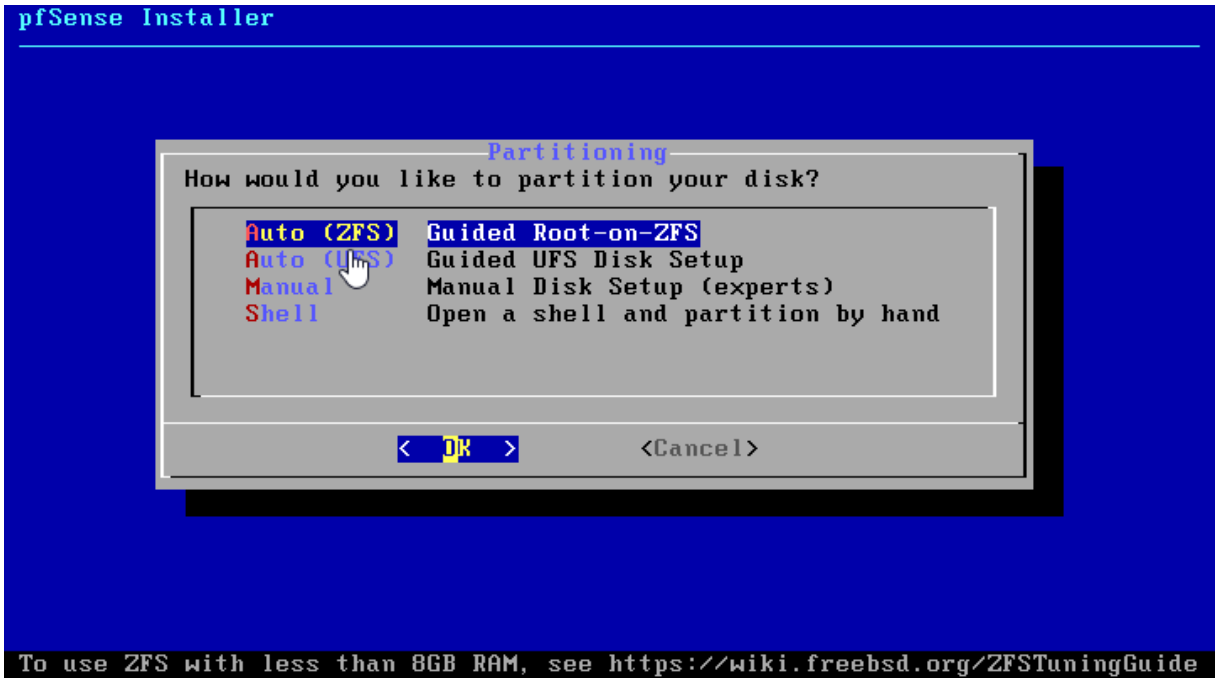


Figure 1: choix de l'installation auto ZFS

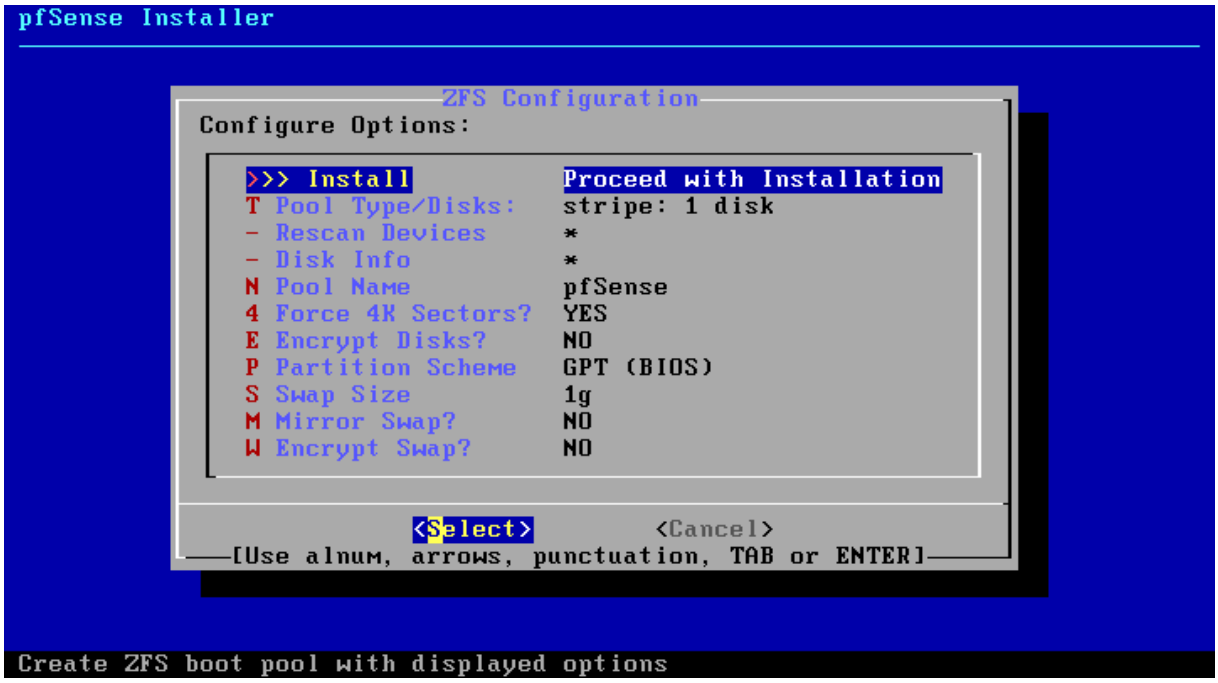


Figure 2: configuration du disque, des partitions, du swap

Assignation et adressage des interfaces

L'installation est dorénavant terminée. Nous allons procéder à l'assignation des interfaces dans VMware puis dans pfSense.

- WAN → em8 (interface qui assure le NAT sur VMware) : interface configurée en **DHCP** derrière le **NAT de VMware** (lequel obtient lui-même une adresse via la box FAI), assurant la translation d'adresses (Double NAT) pour isoler la maquette du réseau physique tout en fournissant un accès Internet sortant aux VLANs internes.
- LAN → em1 (VMnet50)
-

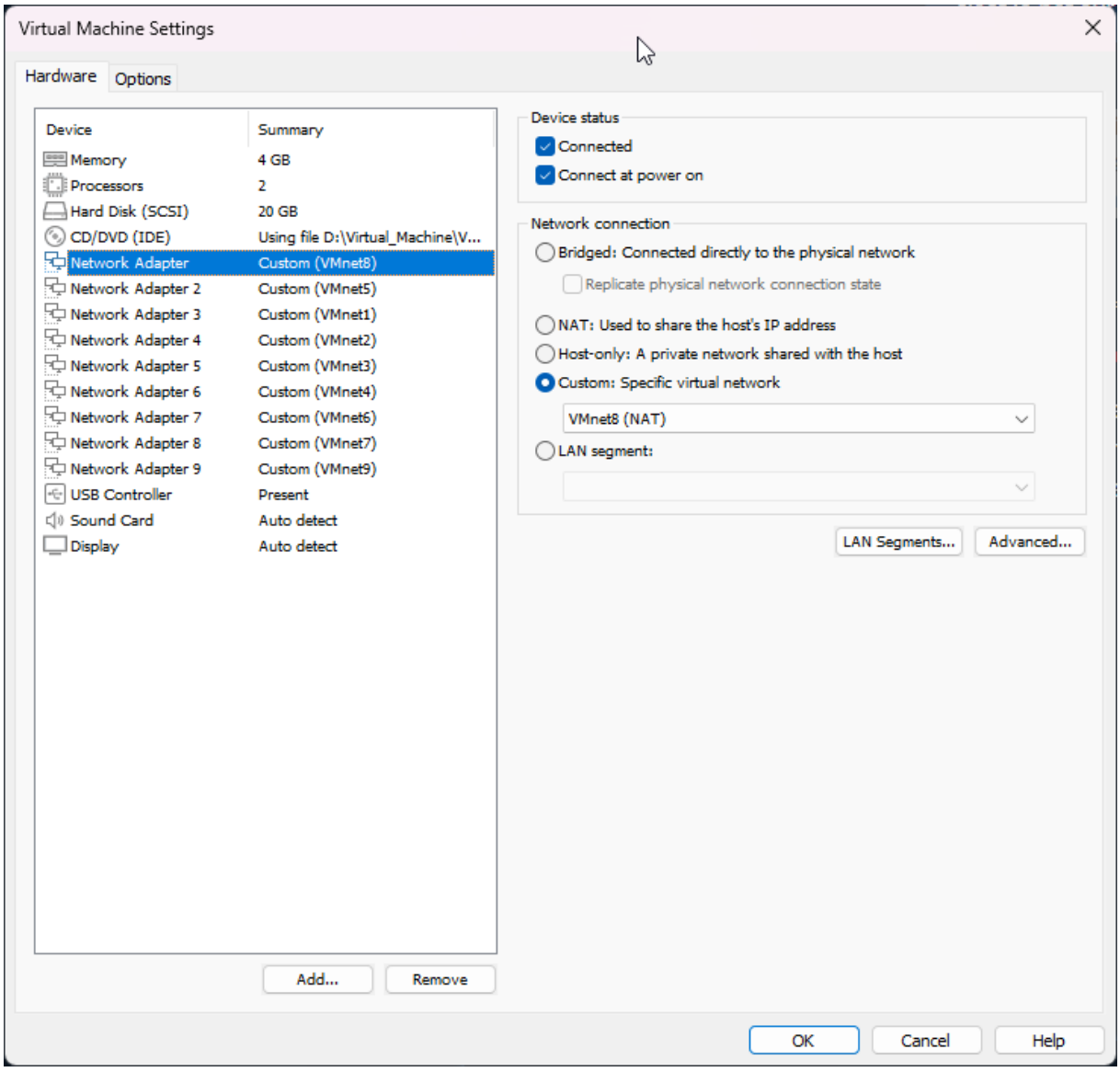


Figure 3: ajout des cartes réseau sur VMware

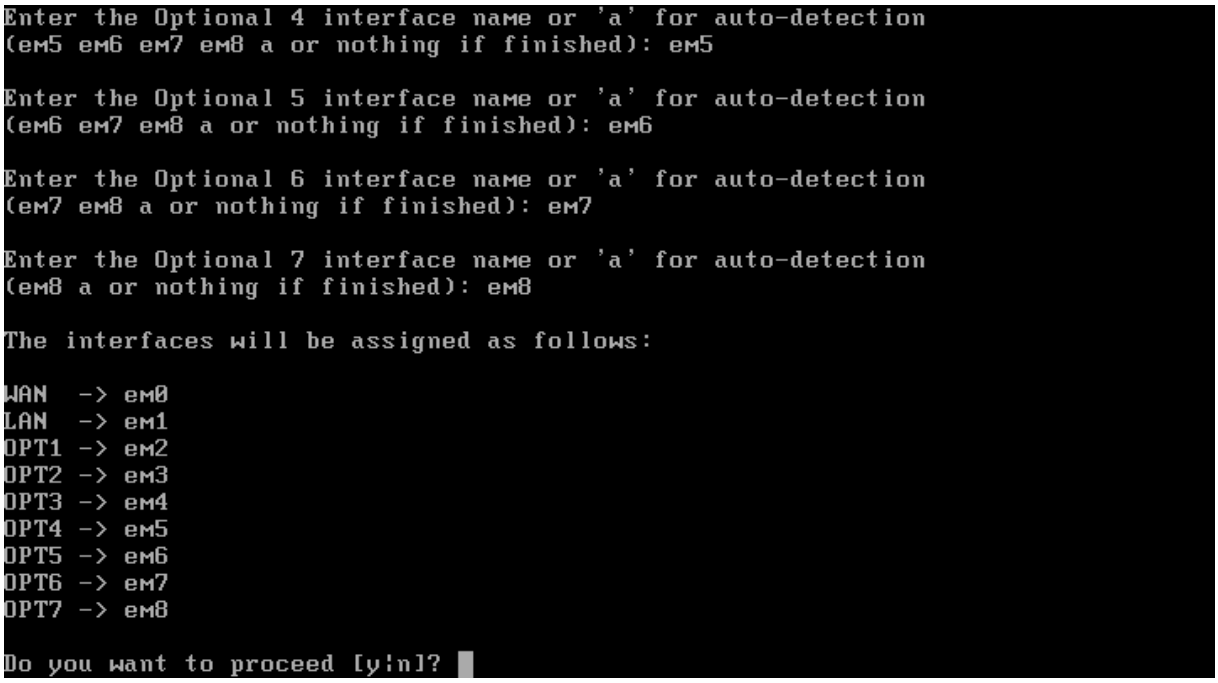


Figure 4: assignation du réseau WAN et du LAN

- WAN -> em0 VMnet8 NAT
- LAN -> em1 VMnet5 MANAGEMENT
- OPT1 -> em2 VMnet1 ADMIN
- OPT2 -> em3 VMnet2 ELEVES
- OPT3 -> em4 VMnet3 ENSEIGNANTS
- OPT4 -> em5 VMnet4 SERVEURS
- OPT5 -> em6 VMnet6 WIFI
- OPT6 -> em7 VMnet7 SERVICES
- OPT7 -> em8 VMnet9 BACKUP

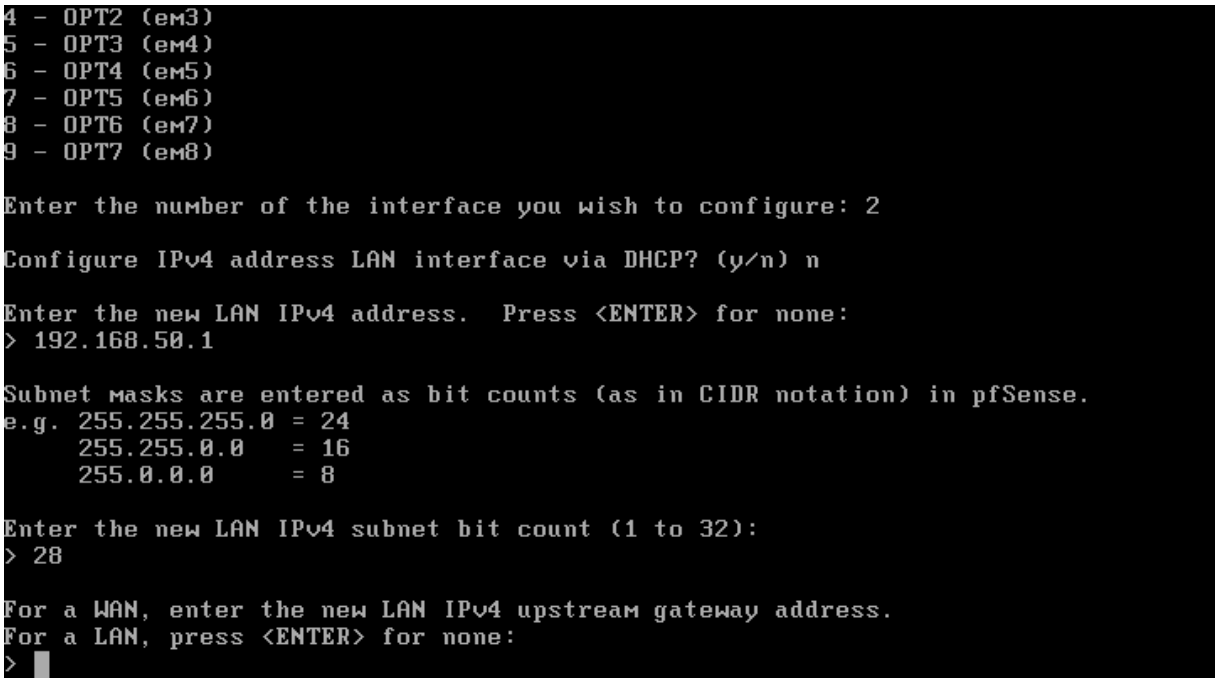


Figure 5: configuration réseau de l'interface LAN sur le VLAN management 50

À l'option "Do you want to revert to HTTP as the webConfigurator protocol? (y/n)", on répond « n » pour maintenir l'accès en HTTPS à l'interface d'administration de pfSense.

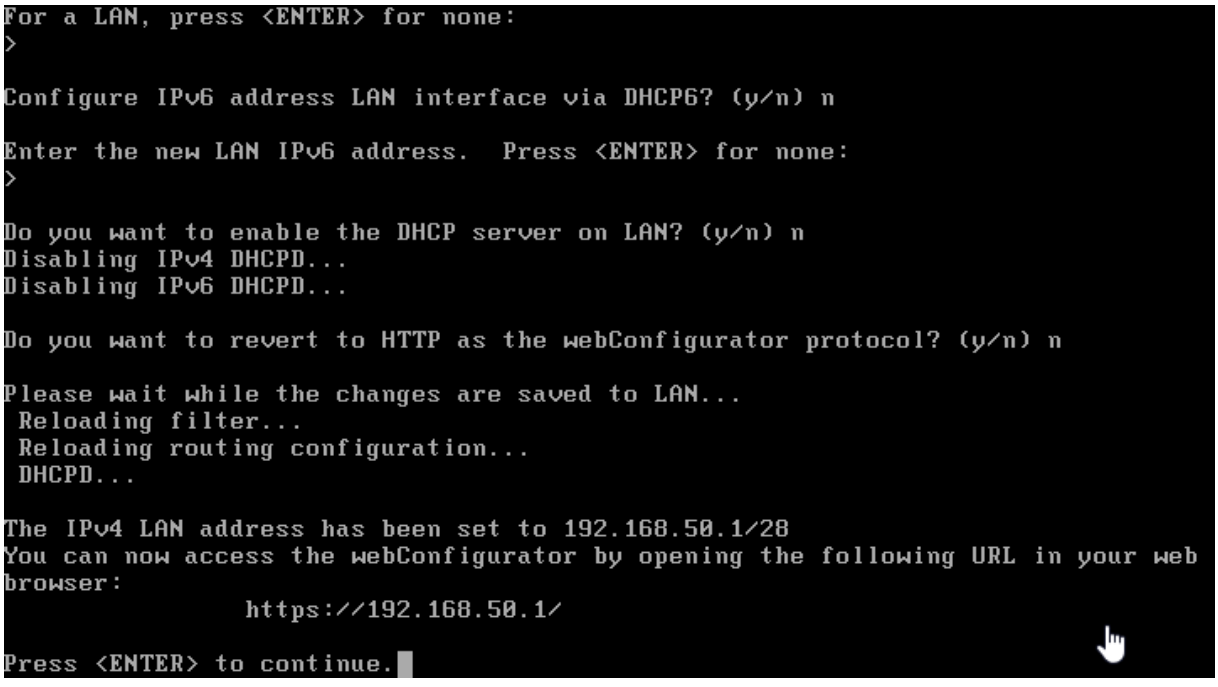


Figure 6: on peut dorénavant se connecter à l'interface web avec l'IP https://192.168.50.1/

Nous allons en plus fixer manuellement l'IP de l'adaptateur VMnet5 : le PC ThinkPad devient ainsi directement relié au VLAN 50 management et servira de station pour administrer tous les postes et serveurs de la maquette.

:

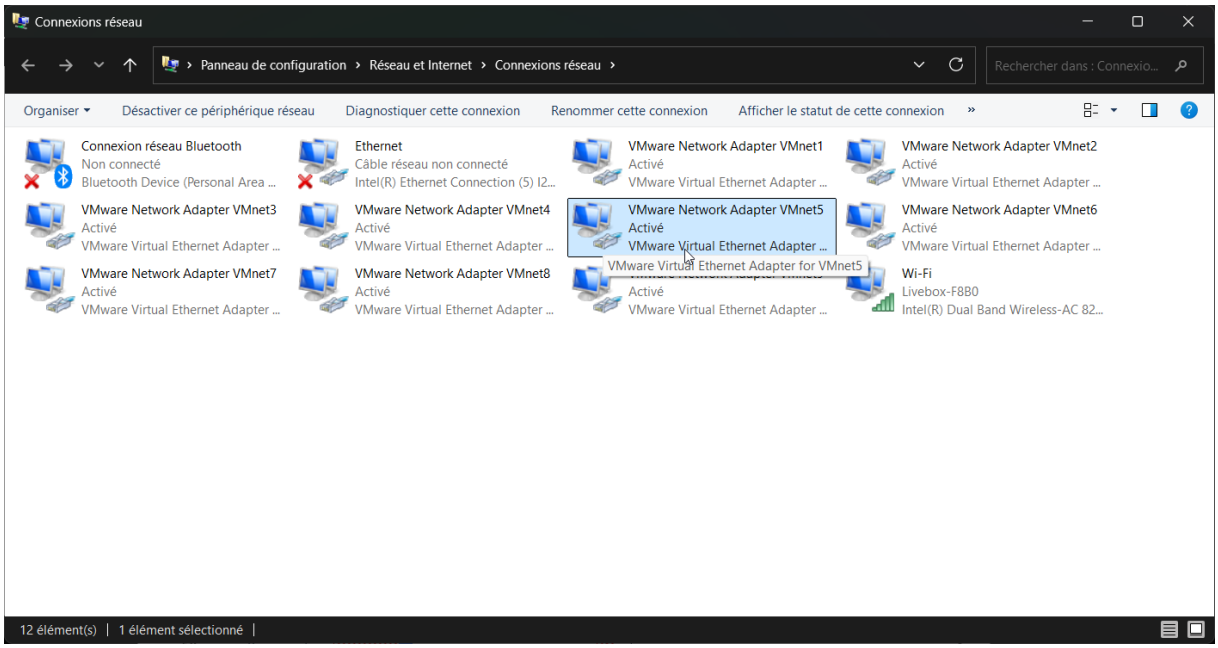


Figure 7: sélection de l'adaptateur VMnet 5

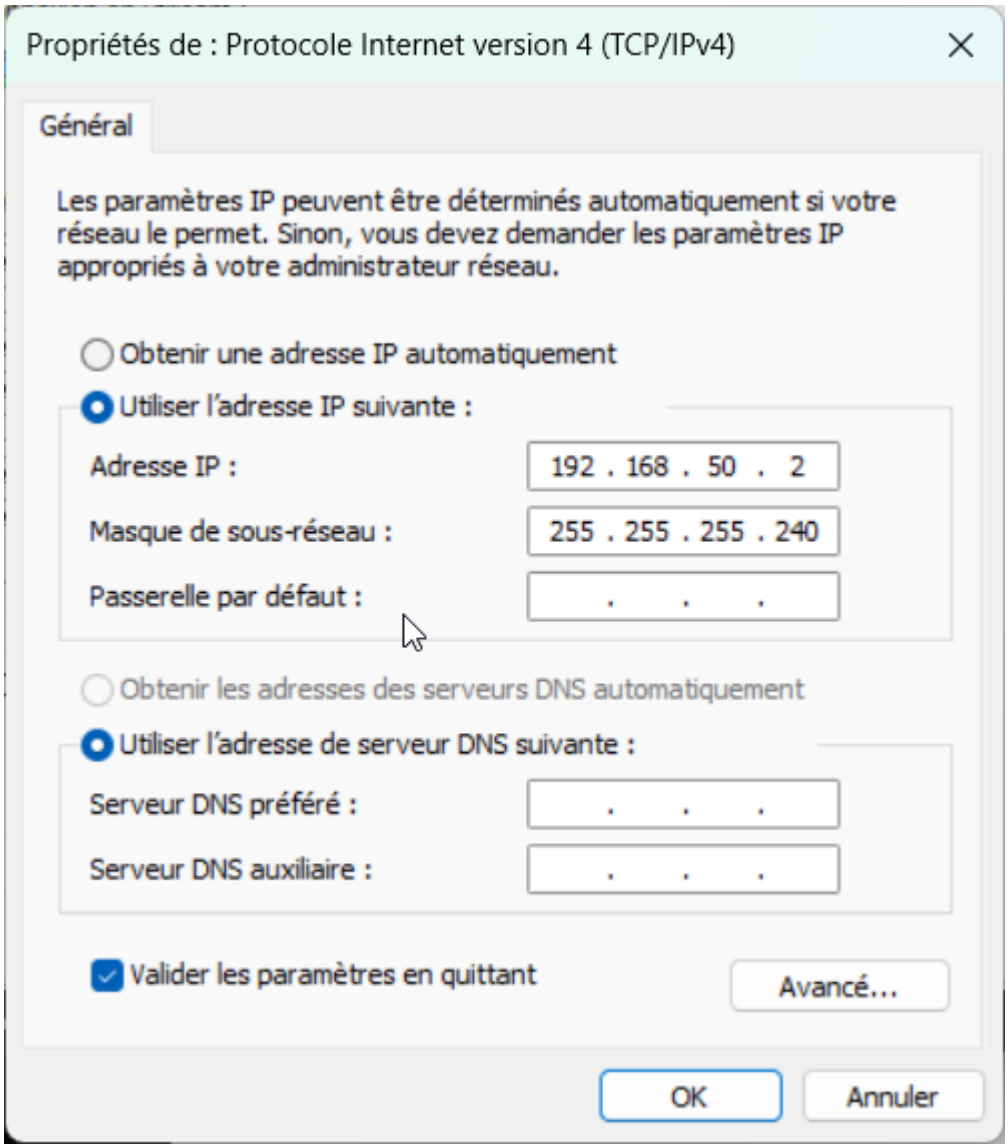


Figure 8: configuration de l'IP en 192.168.50.2

Vérification avec un test ping sur 192.168.50.1

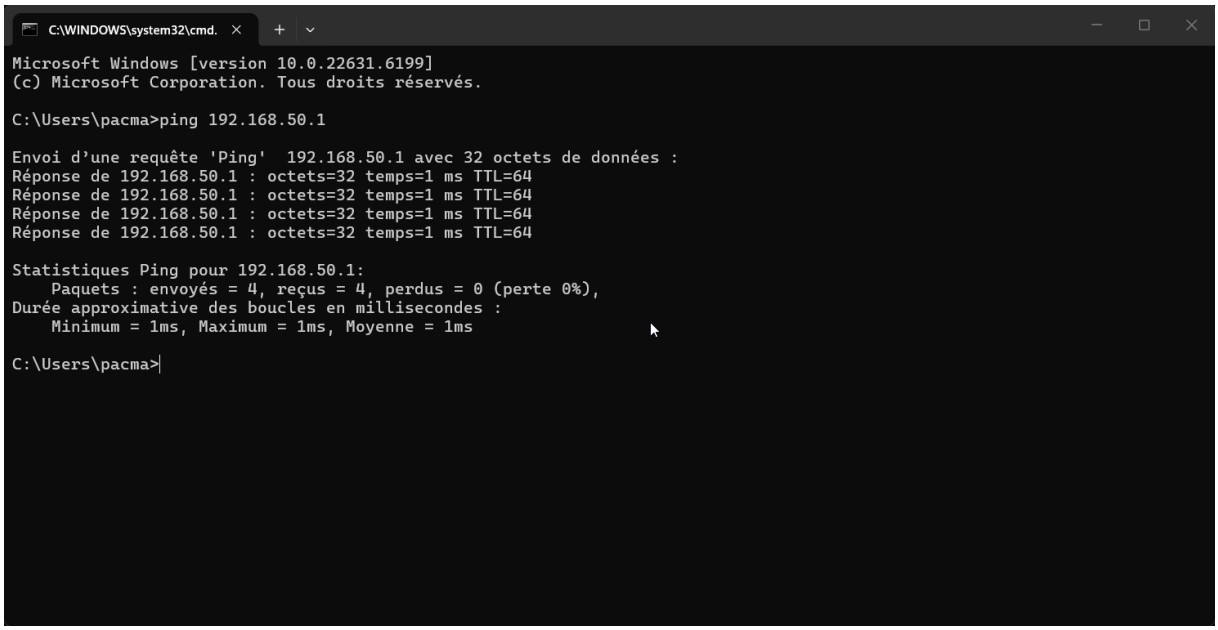


Figure 9: pfSense reçoit bien les paquets

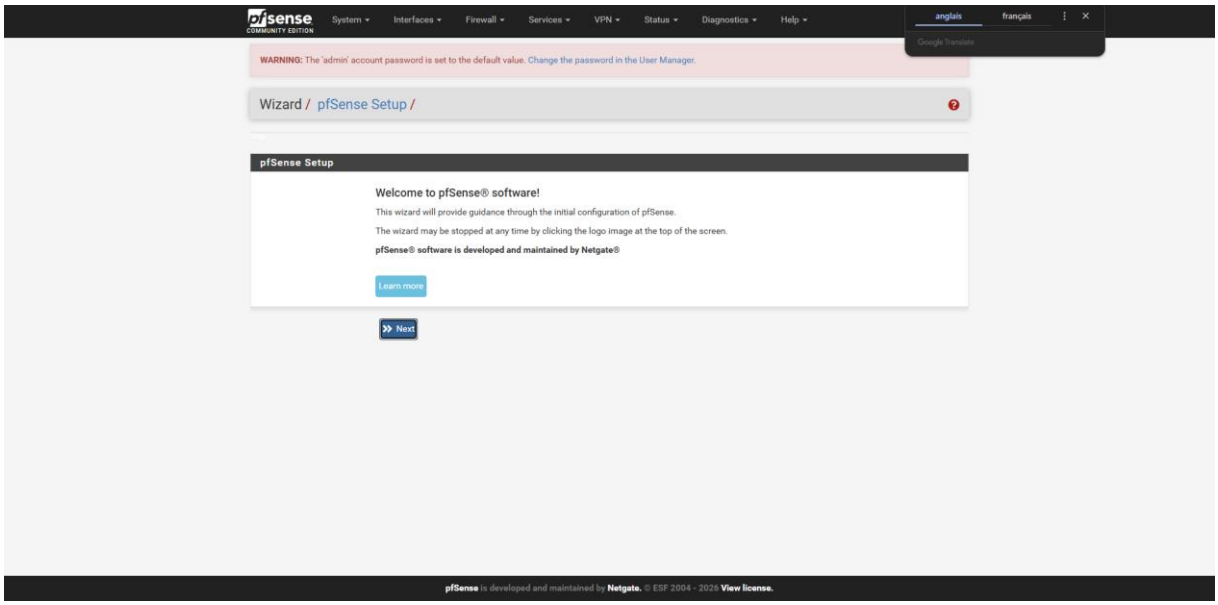
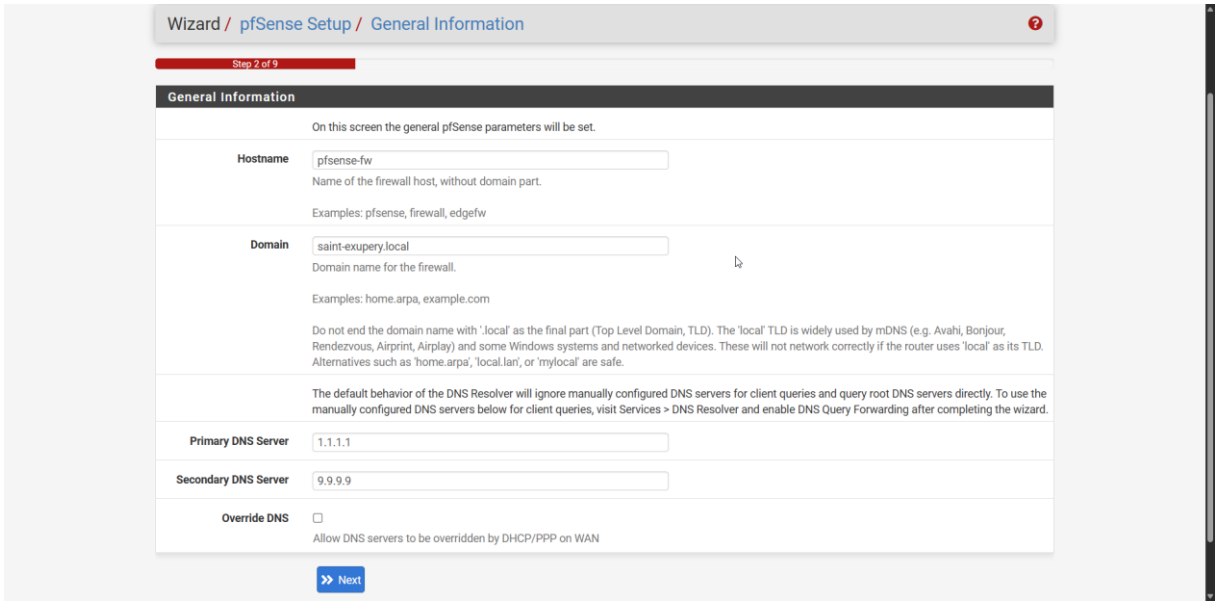
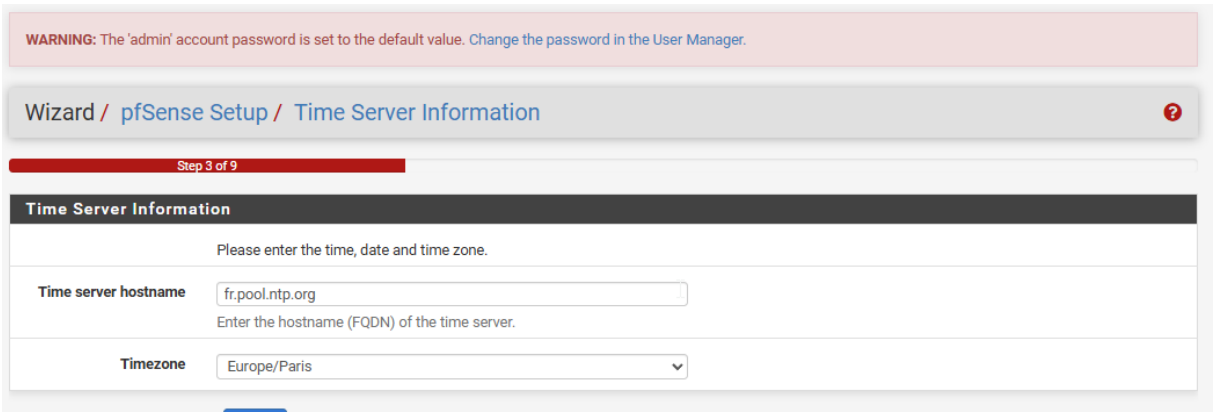


Figure 10: première connexion réussie avec le login admin et le mot de passe pfsense

Passons à la première configuration : choix du hostname, du domaine (lab.local) et des deux serveurs DNS (1.1.1.1, 9.9.9.9), sans chevauchement avec le DNS de VMware. Les DNS seront à changer ultérieurement pour ceux des deux contrôleurs Active Directory.



Serveur NTP français, proche géographiquement = latence minimale, fiabilité maximale pour une maquette en France.



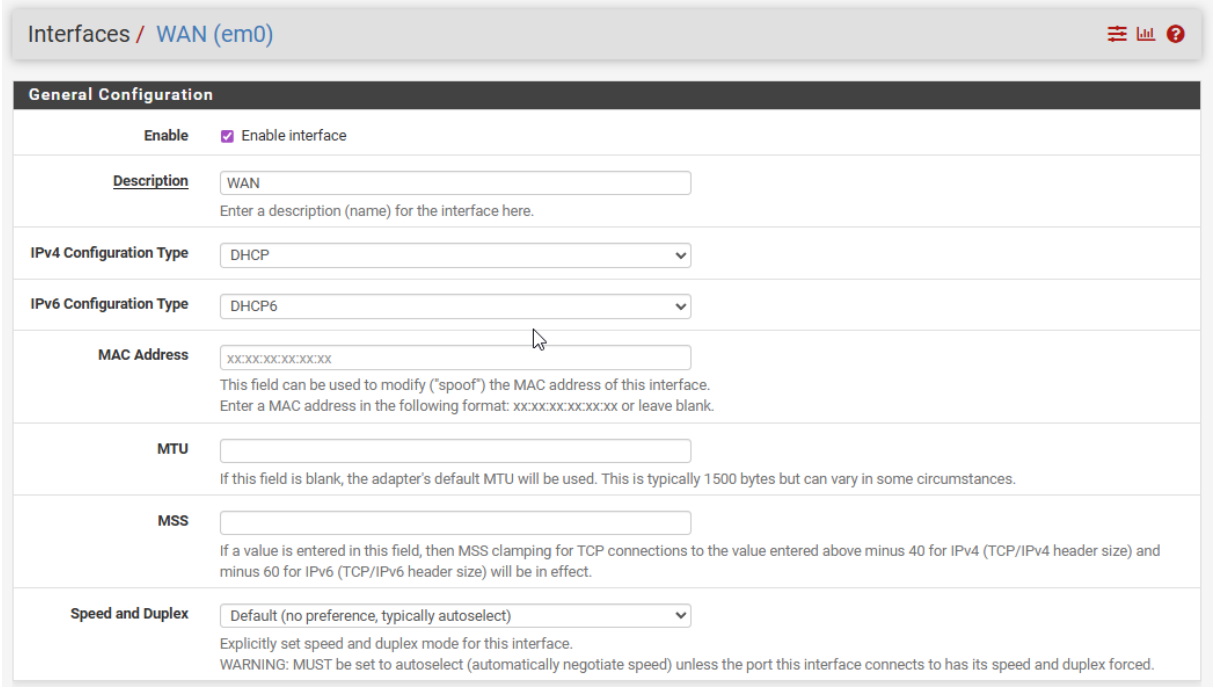


Figure 11: configuration du wan en GUI

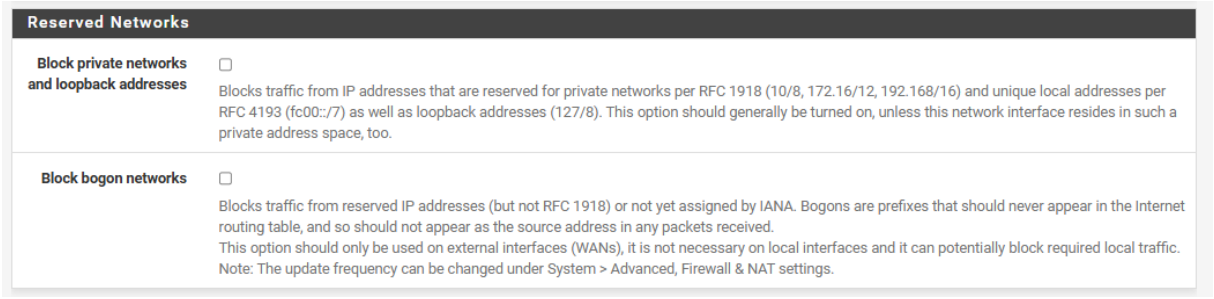


Figure 12: on décoche les deux cases pour éviter tout blocage du trafic interne

Problème : en consultant les interfaces, j'ai constaté que les adresses MAC des OPT1 à OPT7 ne correspondent pas à celles des VMnet configurées sur VMware

Workstation. J’ai donc décidé de réaffecter manuellement les interfaces directement dans le menu Interface Assignments de pfSense.

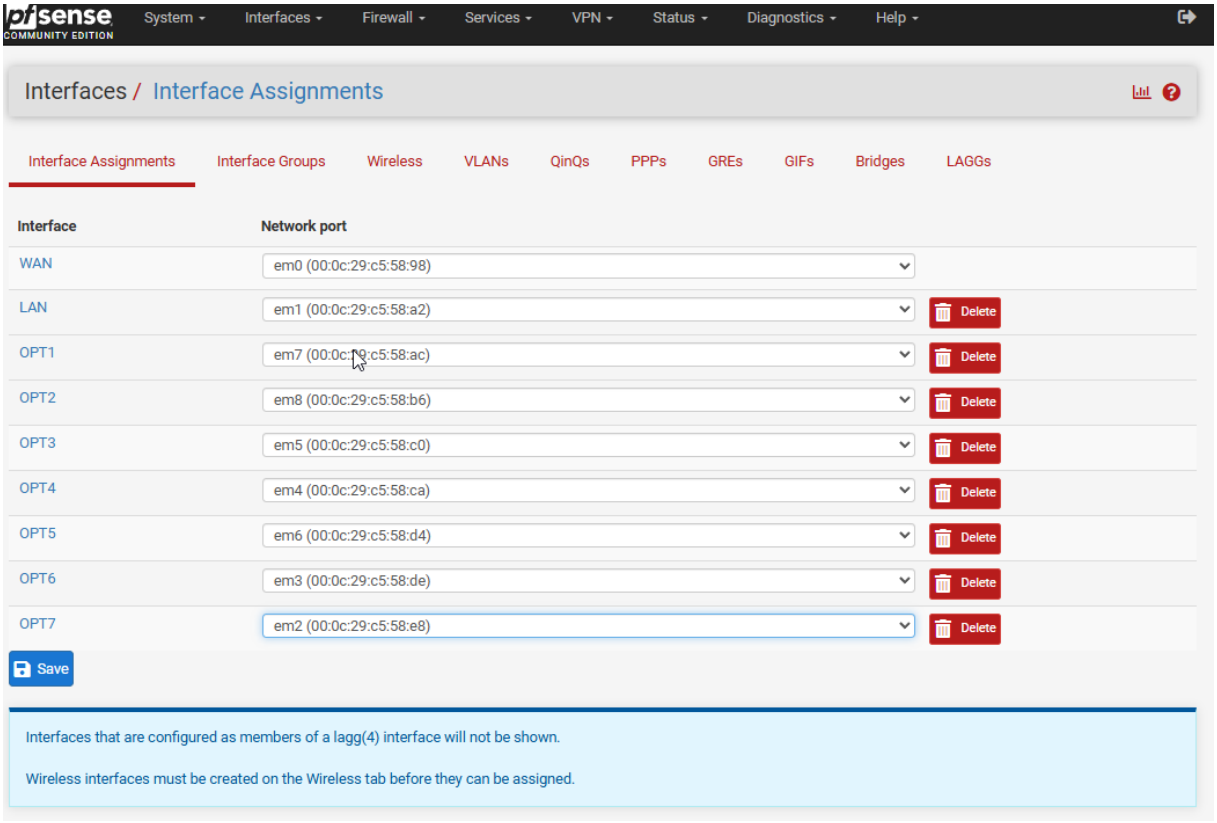


Figure 13: les adresses MAC des interfaces opérationnelles correspondent bien aux adresses MAC des différents VMnet

Nous allons maintenant configurer chaque interface opérationnelle sur pfSense afin qu’elles respectent l’adressage des différents VMnet configurés précédemment.

Sur OPT1 ADMINISTRATION, la configuration sera en IPv4 statique avec l'adresse 192.168.10.1 et un masque de sous-réseau en /26.

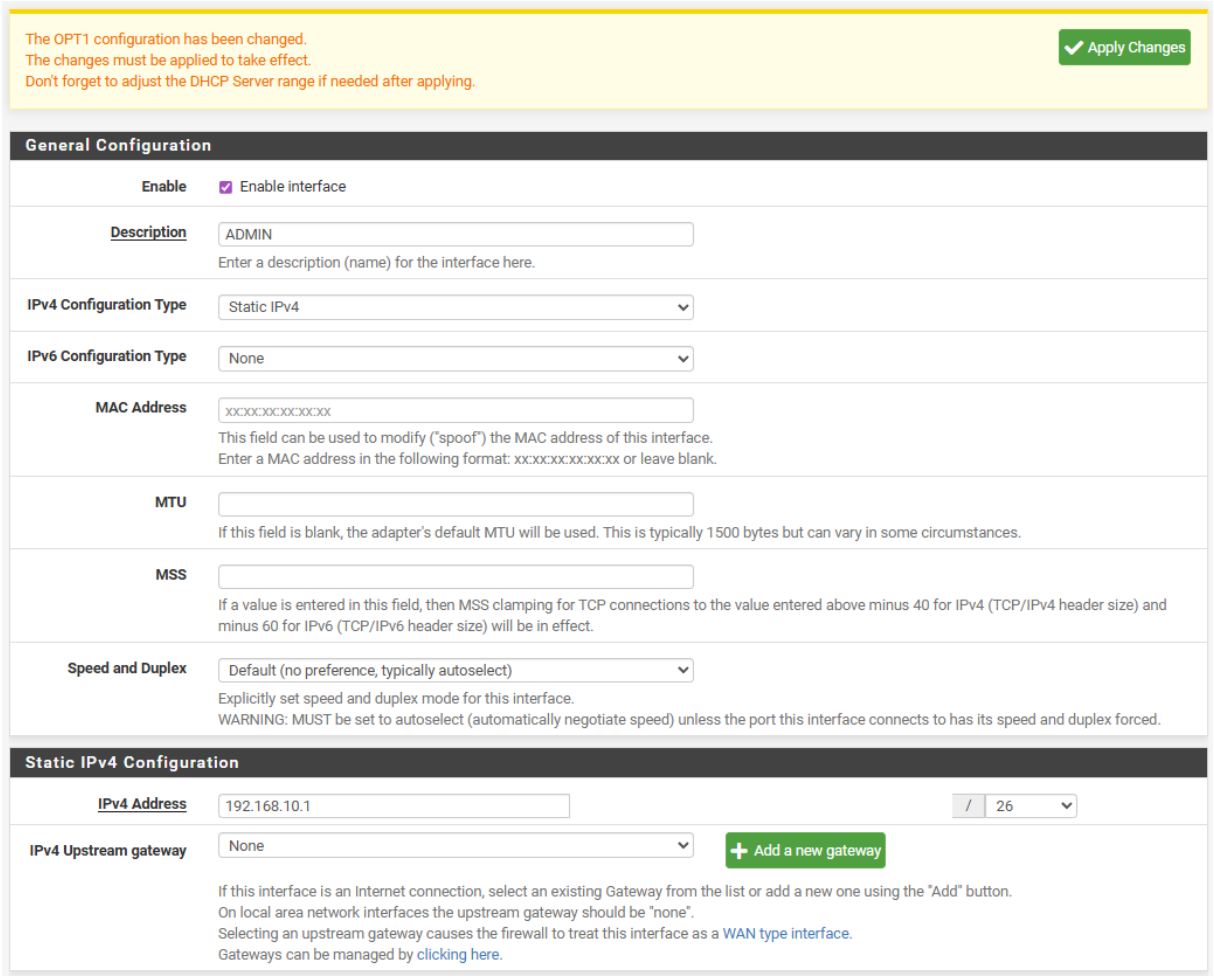


Figure 14: configuration de OPT1 administration

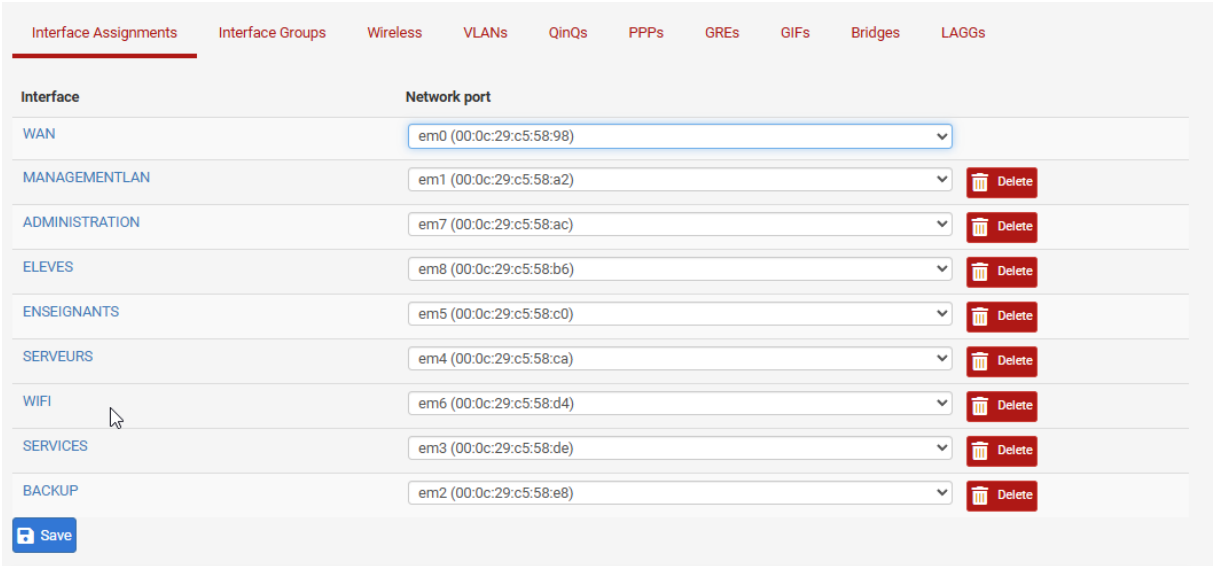


Figure 15: toutes les interfaces ont été assignées

Service DHCP par segment

S’ensuit l’activation du DHCP pour les segments clients via Services > DHCP Server > [chaque interface], en respectant l’adressage et en laissant volontairement des adresses en réserve pour d’éventuels équipements fixes (environ 20 %).

ADMINISTRATION (192.168.10.0/26)
Enable DHCP server on ADMINISTRATION : coché
Range : 192.168.10.10 - 192.168.10.50
DNS servers : 1.1.1.1 / 9.9.9.9 (temporaire, changera après AD)
Save + Apply

ELEVES (192.168.20.0/24)
Range : 192.168.20.10 - 192.168.20.200
DNS : 1.1.1.1 / 9.9.9.9

ENSEIGNANTS (192.168.30.0/26)
Range : 192.168.30.10 - 192.168.30.50
DNS : 1.1.1.1 / 9.9.9.9

WIFI (192.168.60.0/24)
Range : 192.168.60.10 - 192.168.60.200
DNS : 1.1.1.1 / 9.9.9.9

SERVICES (192.168.70.0/27)
Range : 192.168.70.10 - 192.168.70.20
DNS : 1.1.1.1 / 9.9.9.9

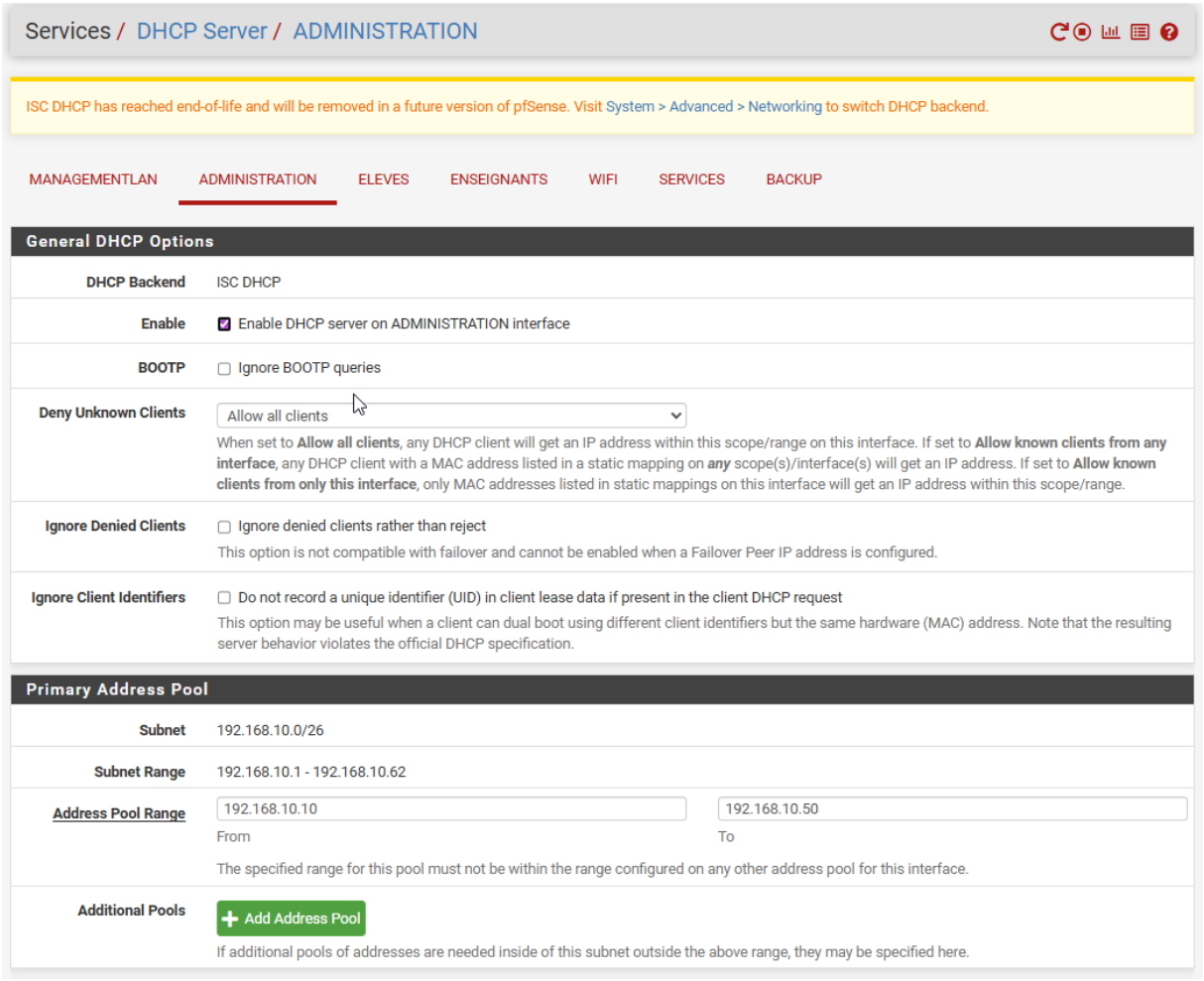


Figure 16: configuration du DHCP sur l'interface administration

Politique de filtrage du pare-feu

Passons à la suite avec la configuration des règles du pare-feu. En premier lieu, nous allons élaborer des alias réutilisables dans toutes les règles créées ultérieurement, sans devoir tout réécrire à chaque fois.

- NETS_INTERNES → blocage global tous segments internes a mettre tout en bas en fin de configuration
- RFC1918 → blocage trafic RFC1918 sur le WAN
- SERVEURS_AD → cible précise vers les 2 DC
- SRV_ADMIN → cible précise vers GLPI/Zabbix
- SRV_FS → cible précise vers le serveur de fichiers
- PORTS_AD_CLIENTS → ports clients standards (séparation sécurité)
- PORTS_AD_REPLICATION → RPC dynamique restreint à l'inter-DC

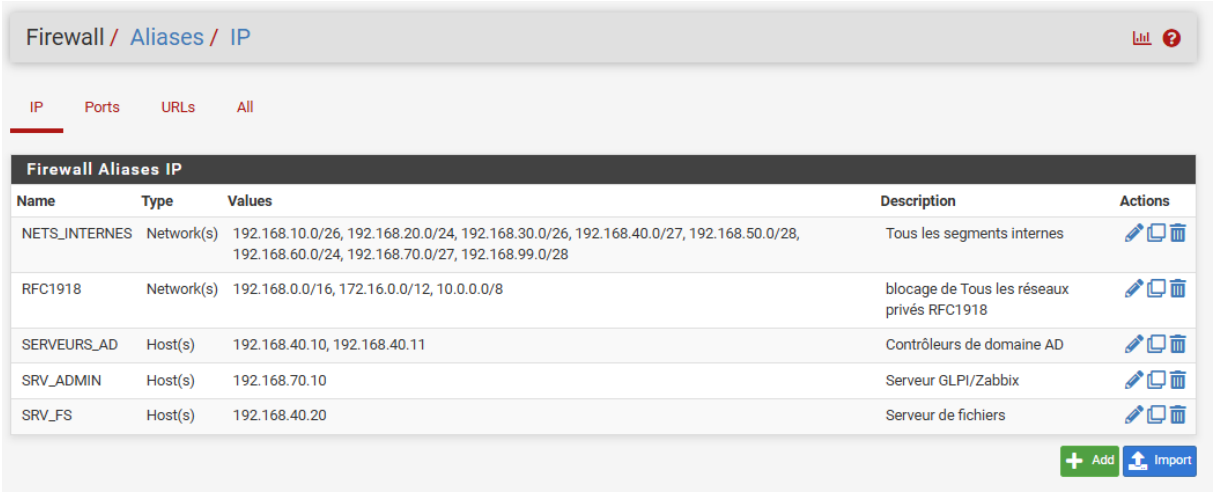


Figure 17: alias pour les adresses IP

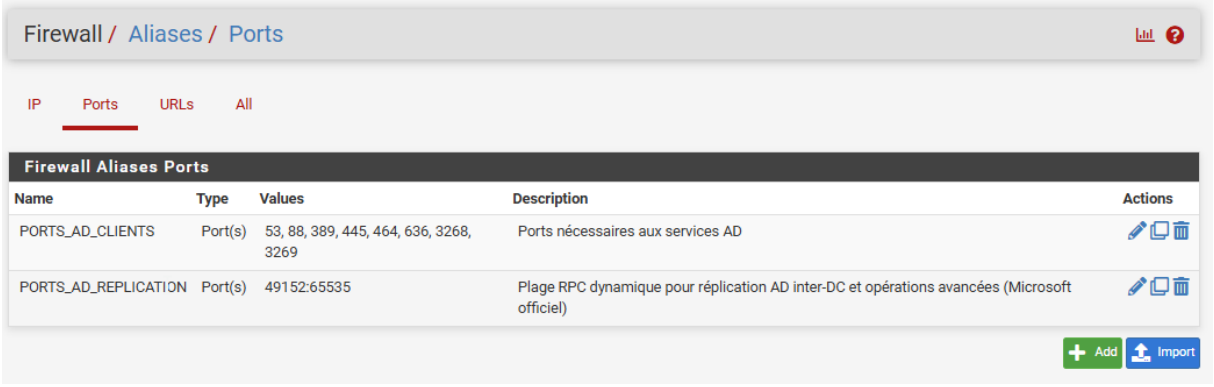


Figure 18: alias pour les ports

Étape suivante Règle 1, pare-feu WIFI invités :
L'objectif de cette règle est de bloquer tout trafic depuis les invités Wi-Fi vers tous les segments internes (administration, élèves, enseignants, serveurs, services, backup, management). Le résultat est une isolation totale du réseau invité, conformément au principe Zero Trust.

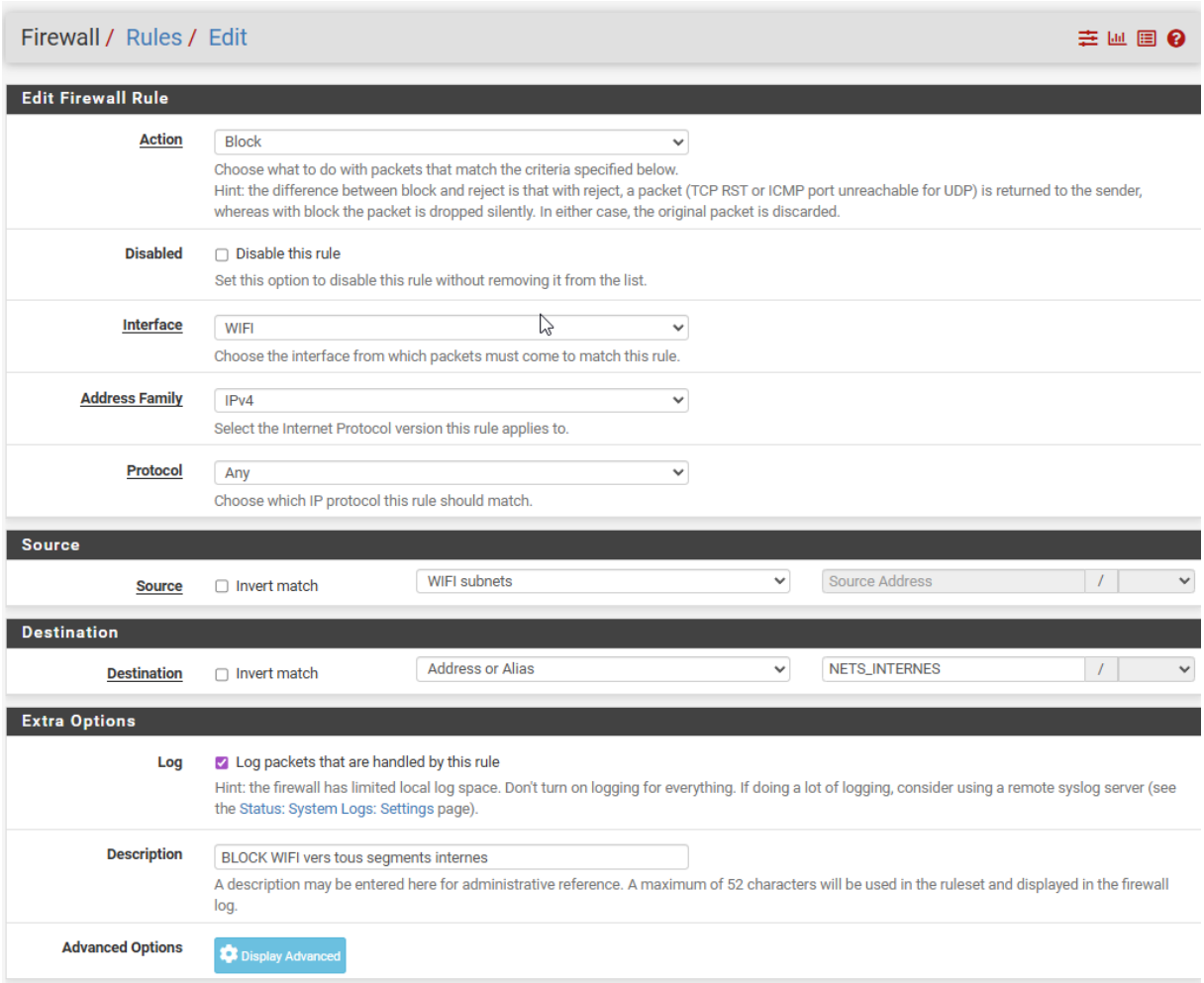


Figure 19: blocage de tous les protocoles vers les réseaux internes sur le segment WIFI

Règle 2 : autoriser le DNS sur le segment WIFI

Pourquoi TCP/UDP est-il choisi dans la partie protocole ?
DNS utilise principalement UDP 53. Mais pour les requêtes longues (>512 octets) et certaines réponses étendues (DNSSEC), DNS bascule en TCP 53. Autoriser les deux permet de couvrir tous les cas.

Pourquoi « This Firewall (self) » est-il sélectionné ?
C'est une notion propre à pfSense : elle désigne "toutes les IP de pfSense, quelle que soit l'interface". Plus propre que de mettre 192.168.60.1 en dur : si un jour l'IP de l'interface WIFI change, la règle reste valide.

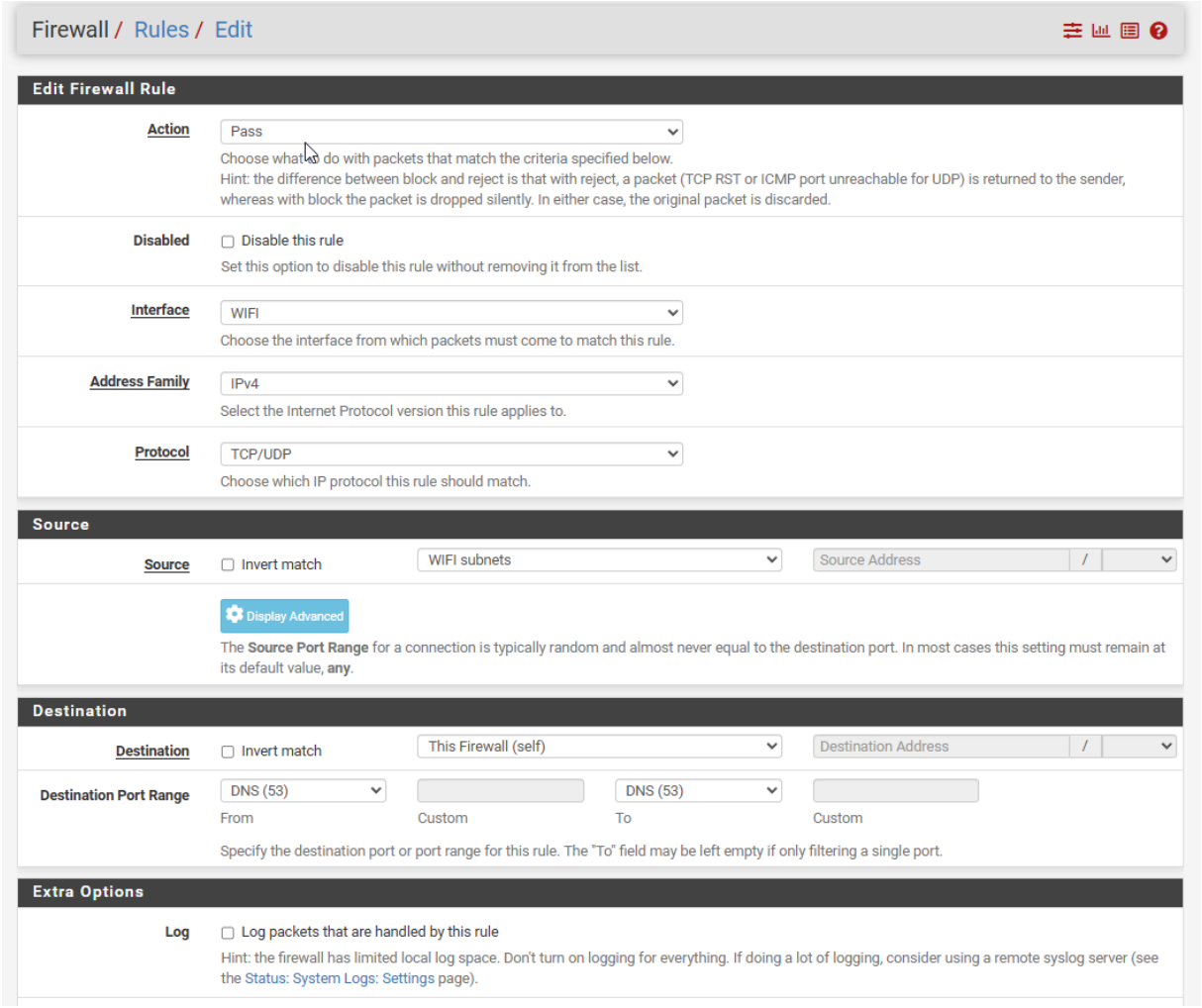


Figure 20: on autorise les flux TCP/UDP 53 (DNS) sur le segment WIFI

Maintenant les règles 3 et 4, autorisant le WIFI vers HTTP et HTTPS

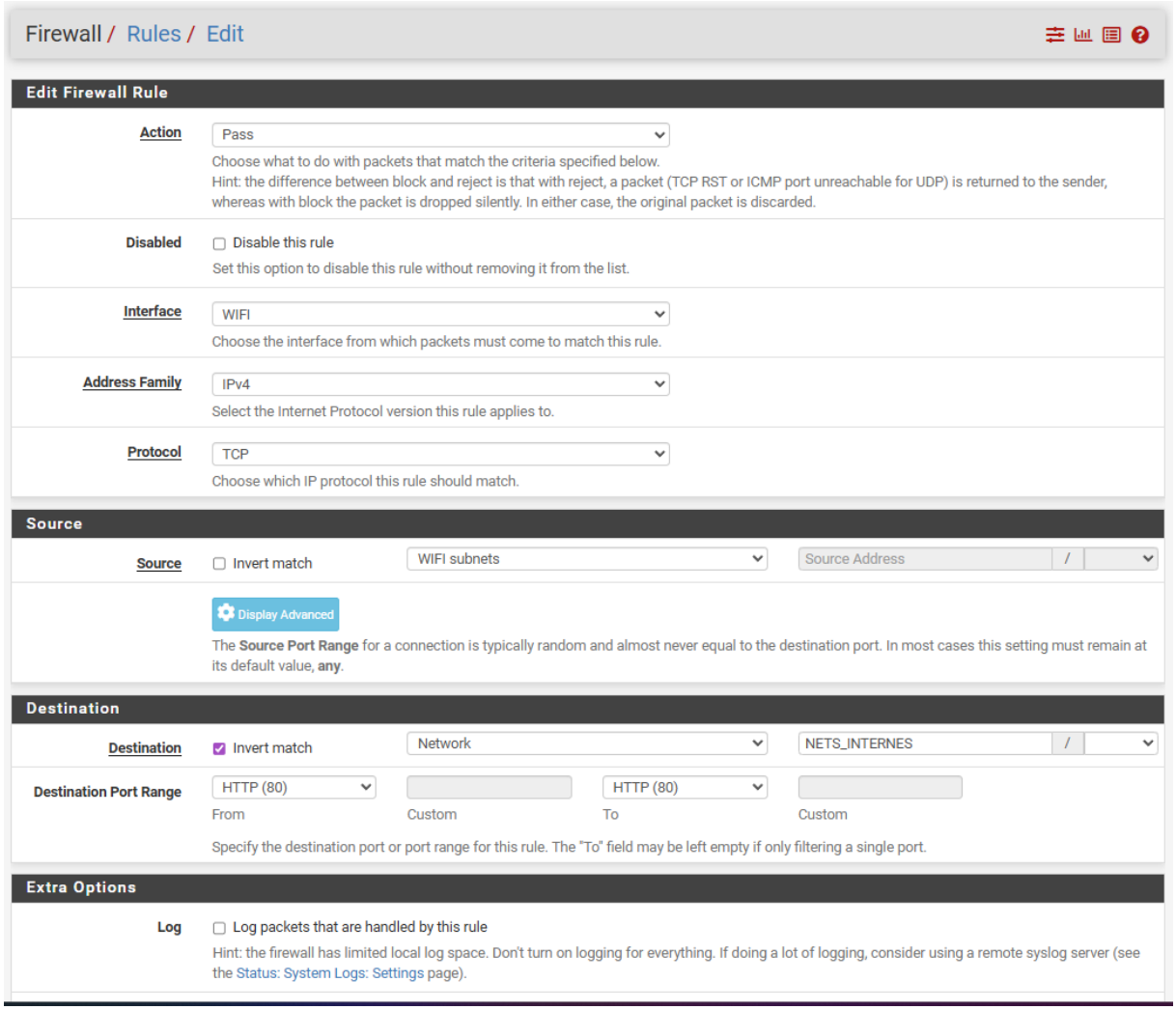


Figure 21: règle HTTP ok ; on coche « invert match » pour inverser la règle : on autorise vers tout sauf les réseaux internes

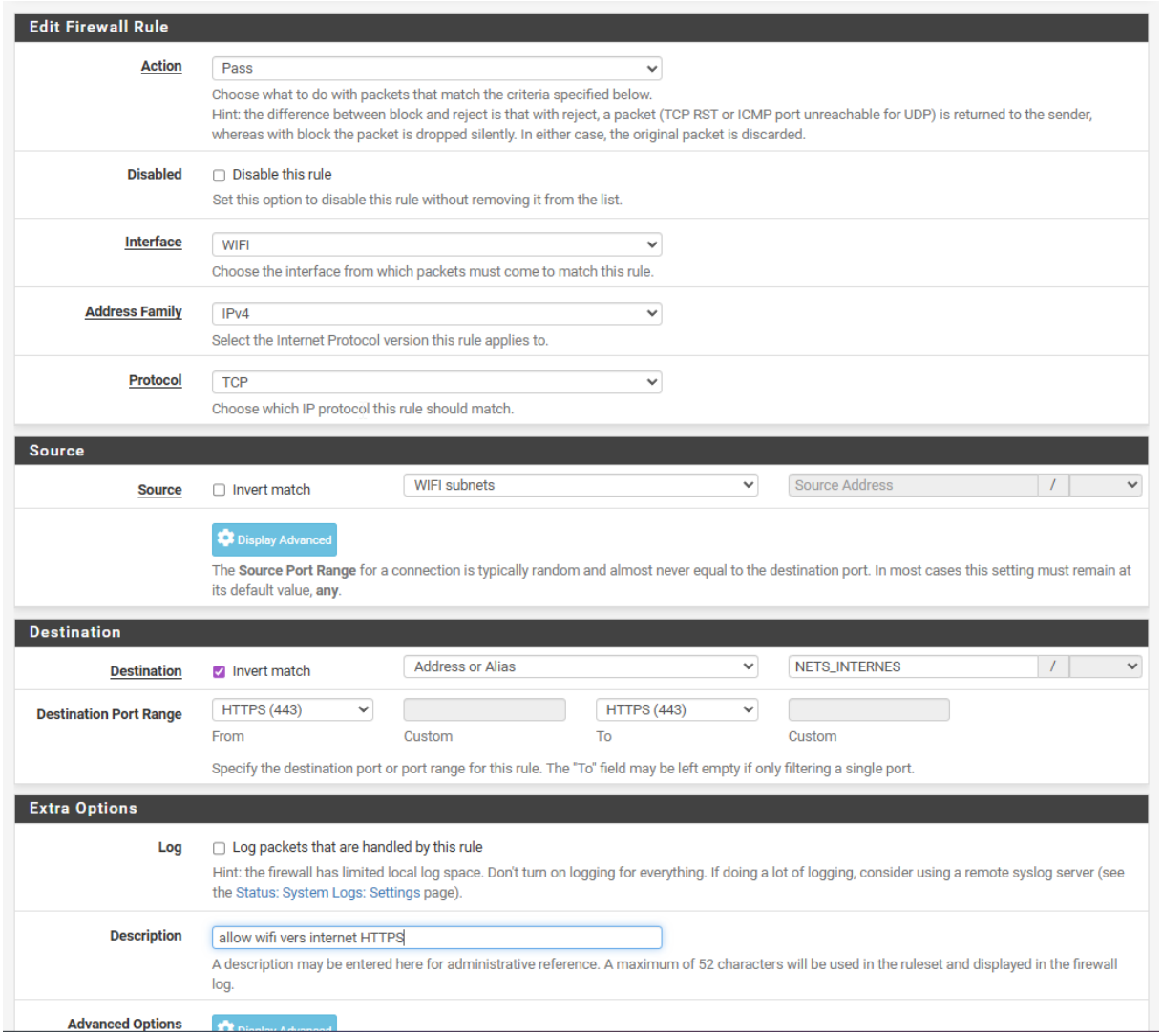


Figure 22: règle HTTPS ok, obéissant à la même logique que HTTP

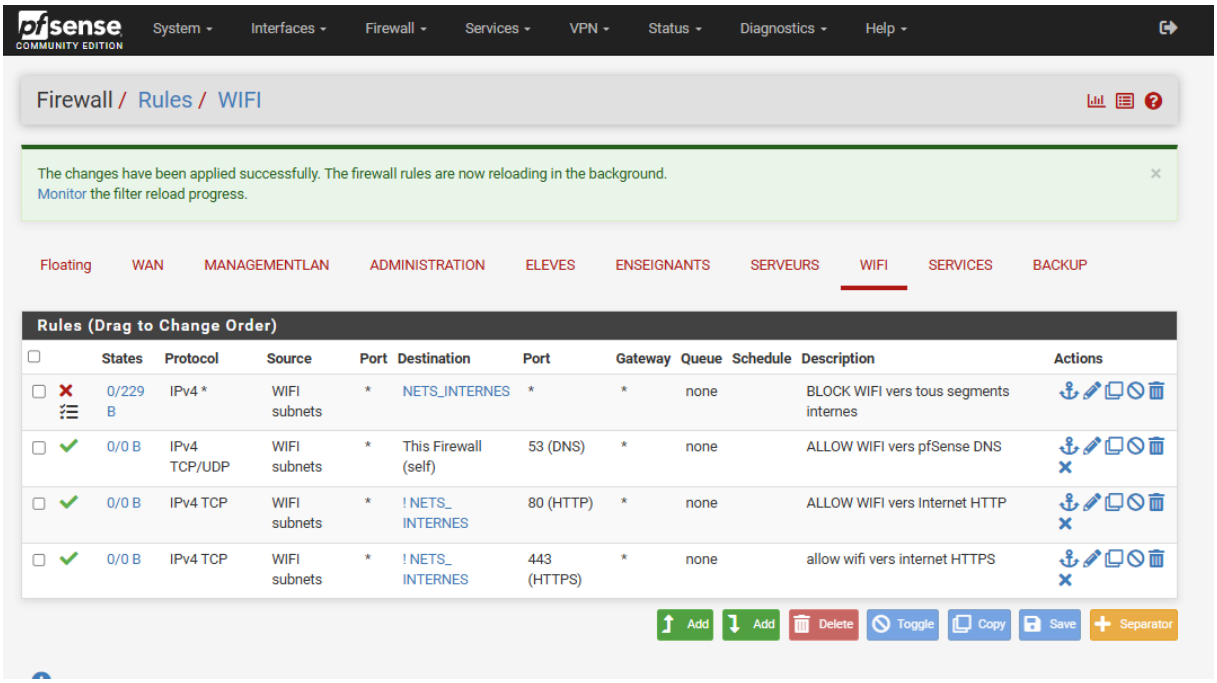


Figure 23: ensemble des règles du segment WIFI

Segment élèves :

Mêmes principes que pour le Wi-Fi invités, adaptés au profil élèves : accès Internet filtré (DNS, HTTP, HTTPS) et blocage des segments sensibles.

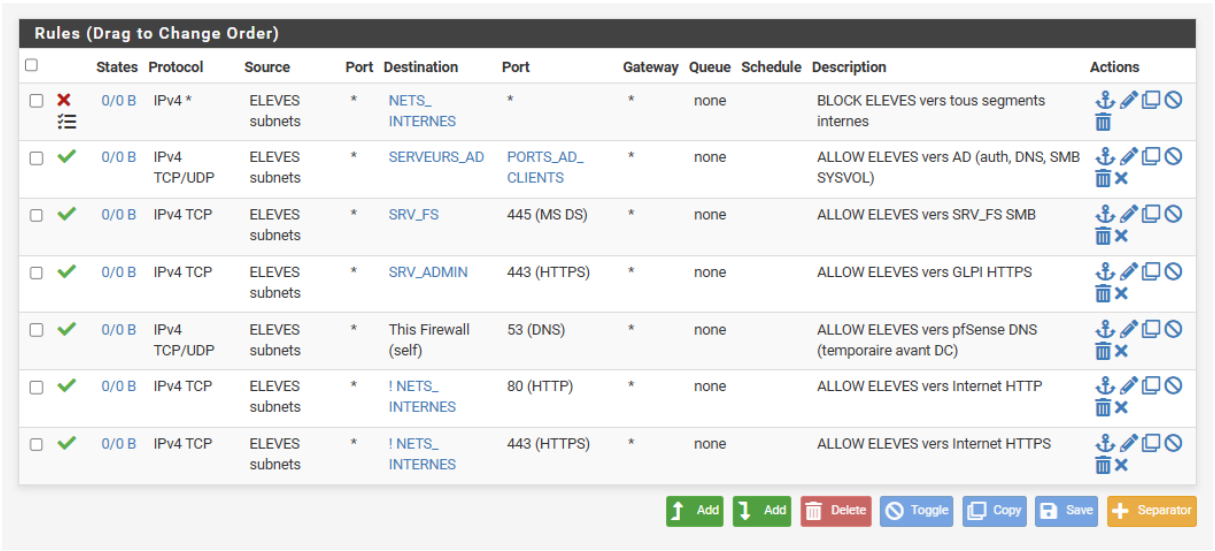
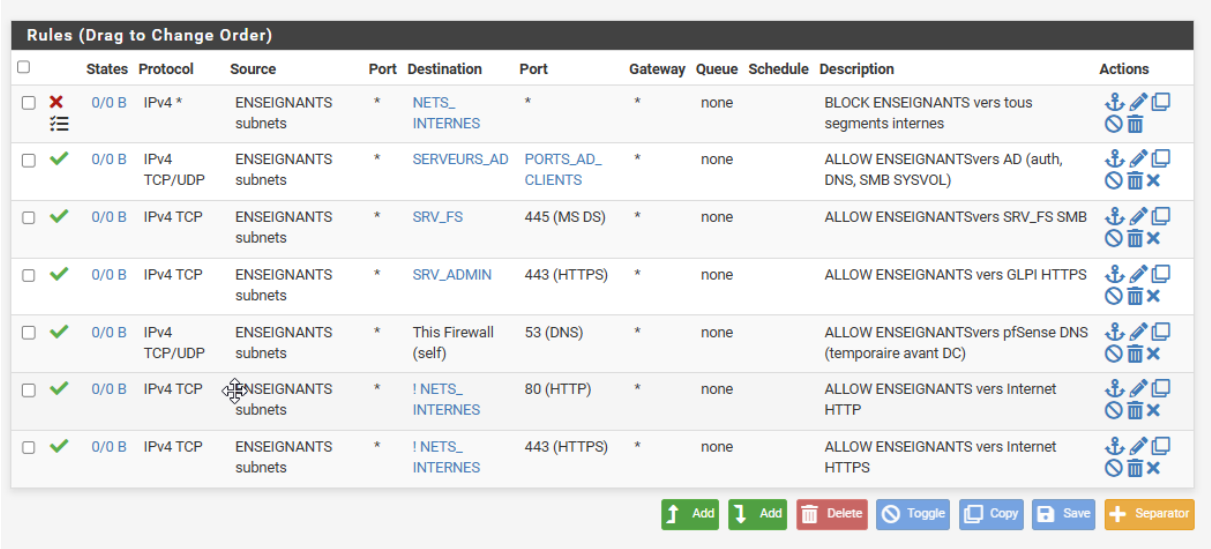


Figure 24: règles pour le segment élèves, qui seront copiées-collées pour le segment enseignants

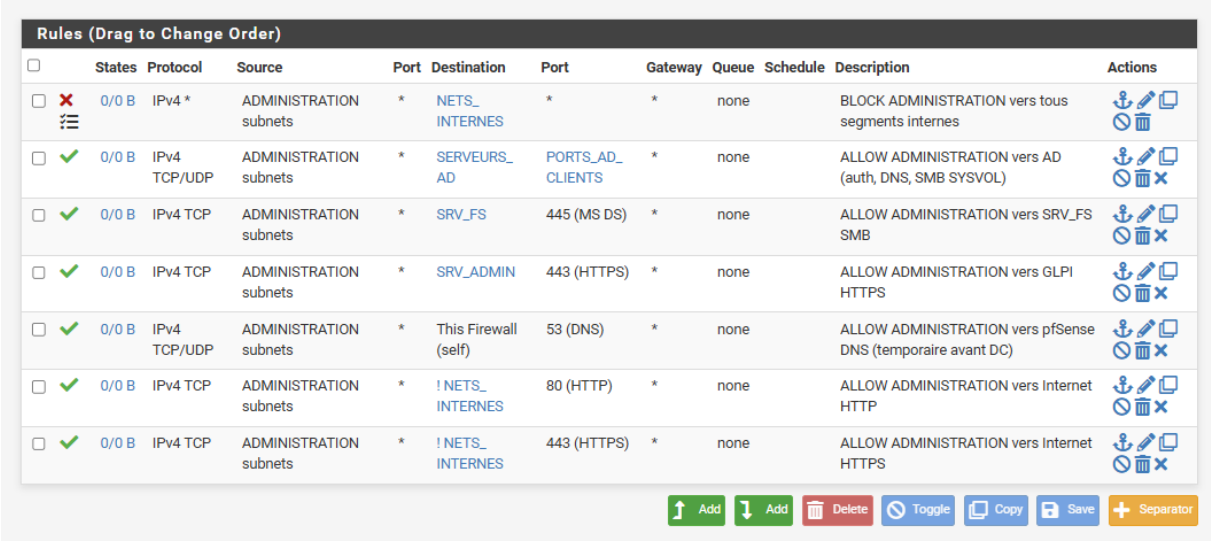


Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0/0 B	IPv4 *	ENSEIGNANTS subnets	*	NETS_ INTERNES	*	*	none		BLOCK ENSEIGNANTS vers tous segments internes	
✓	0/0 B	IPv4 TCP/UDP	ENSEIGNANTS subnets	*	SERVEURS_AD	PORTS_AD_ CLIENTS	*	none		ALLOW ENSEIGNANTSvers AD (auth, DNS, SMB SYSVOL)	
✓	0/0 B	IPv4 TCP	ENSEIGNANTS subnets	*	SRV_FS	445 (MS DS)	*	none		ALLOW ENSEIGNANTSvers SRV_FS SMB	
✓	0/0 B	IPv4 TCP	ENSEIGNANTS subnets	*	SRV_ADMIN	443 (HTTPS)	*	none		ALLOW ENSEIGNANTS vers GLPI HTTPS	
✓	0/0 B	IPv4 TCP/UDP	ENSEIGNANTS subnets	*	This Firewall (self)	53 (DNS)	*	none		ALLOW ENSEIGNANTSvers pfSense DNS (temporaire avant DC)	
✓	0/0 B	IPv4 TCP	ENSEIGNANTS subnets	*	! NETS_ INTERNES	80 (HTTP)	*	none		ALLOW ENSEIGNANTS vers Internet HTTP	
✓	0/0 B	IPv4 TCP	ENSEIGNANTS subnets	*	! NETS_ INTERNES	443 (HTTPS)	*	none		ALLOW ENSEIGNANTS vers Internet HTTPS	

Add Add Delete Toggle Copy Save Separator

Figure 25: règles enseignants, identiques à élèves



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0/0 B	IPv4 *	ADMINISTRATION subnets	*	NETS_ INTERNES	*	*	none		BLOCK ADMINISTRATION vers tous segments internes	
✓	0/0 B	IPv4 TCP/UDP	ADMINISTRATION subnets	*	SERVEURS_ AD	PORTS_AD_ CLIENTS	*	none		ALLOW ADMINISTRATION vers AD (auth, DNS, SMB SYSVOL)	
✓	0/0 B	IPv4 TCP	ADMINISTRATION subnets	*	SRV_FS	445 (MS DS)	*	none		ALLOW ADMINISTRATION vers SRV_FS SMB	
✓	0/0 B	IPv4 TCP	ADMINISTRATION subnets	*	SRV_ADMIN	443 (HTTPS)	*	none		ALLOW ADMINISTRATION vers GLPI HTTPS	
✓	0/0 B	IPv4 TCP/UDP	ADMINISTRATION subnets	*	This Firewall (self)	53 (DNS)	*	none		ALLOW ADMINISTRATION vers pfSense DNS (temporaire avant DC)	
✓	0/0 B	IPv4 TCP	ADMINISTRATION subnets	*	! NETS_ INTERNES	80 (HTTP)	*	none		ALLOW ADMINISTRATION vers Internet HTTP	
✓	0/0 B	IPv4 TCP	ADMINISTRATION subnets	*	! NETS_ INTERNES	443 (HTTPS)	*	none		ALLOW ADMINISTRATION vers Internet HTTPS	

Add Add Delete Toggle Copy Save Separator

Figure 26: règles administration, identiques à enseignants

La configuration des règles SERVEURS ajoutera les règles suivantes :

- replications AD inter DC qui autorise les contrôleurs de domaine SRV-AD1 et SRV-AD2 à se répliquer entre eux via RPC dynamique (ports éphémères 49152-65535). Source et destination restreintes à l'alias SERVEURS_AD pour limiter strictement cette plage de ports sensible aux 2 DC, sans l'exposer aux autres serveurs du segment. Indispensable pour la réplication du schéma AD et de la base SYSVOL entre DC.
- les communications inter DC LDAP/Kerberos qui autorise les communications AD standards (LDAP, Kerberos, DNS, SMB, Global Catalog) entre les contrôleurs de domaine via l'alias PORTS_AD_CLIENTS. Nécessaire à la promotion de SRV-AD2 en DC secondaire, à la synchronisation FSMO et aux échanges d'authentification inter-DC. Restriction stricte à l'alias SERVEURS_AD (2 IP host).

- Autorise les serveurs (SRV-AD1, SRV-AD2, SRV-FS) à pousser leurs sauvegardes vers SRV-BACKUP via SMB (port 445) sur le segment BACKUP isolé (VLAN 99). L'architecture push-only fait qu'un seul sens, SERVEURS → BACKUP, est autorisé. Aucune règle inverse n'existe, ce qui protège les sauvegardes contre une compromission par ransomware (l'attaquant sur un serveur ne peut pas modifier ou supprimer les sauvegardes existantes).
- Regle NTP : Active Directory / Kerberos exigent une synchronisation horaire stricte (max 5 min d'écart). Si un serveur subit un décalage, plus de Kerberos, plus d'authentification.

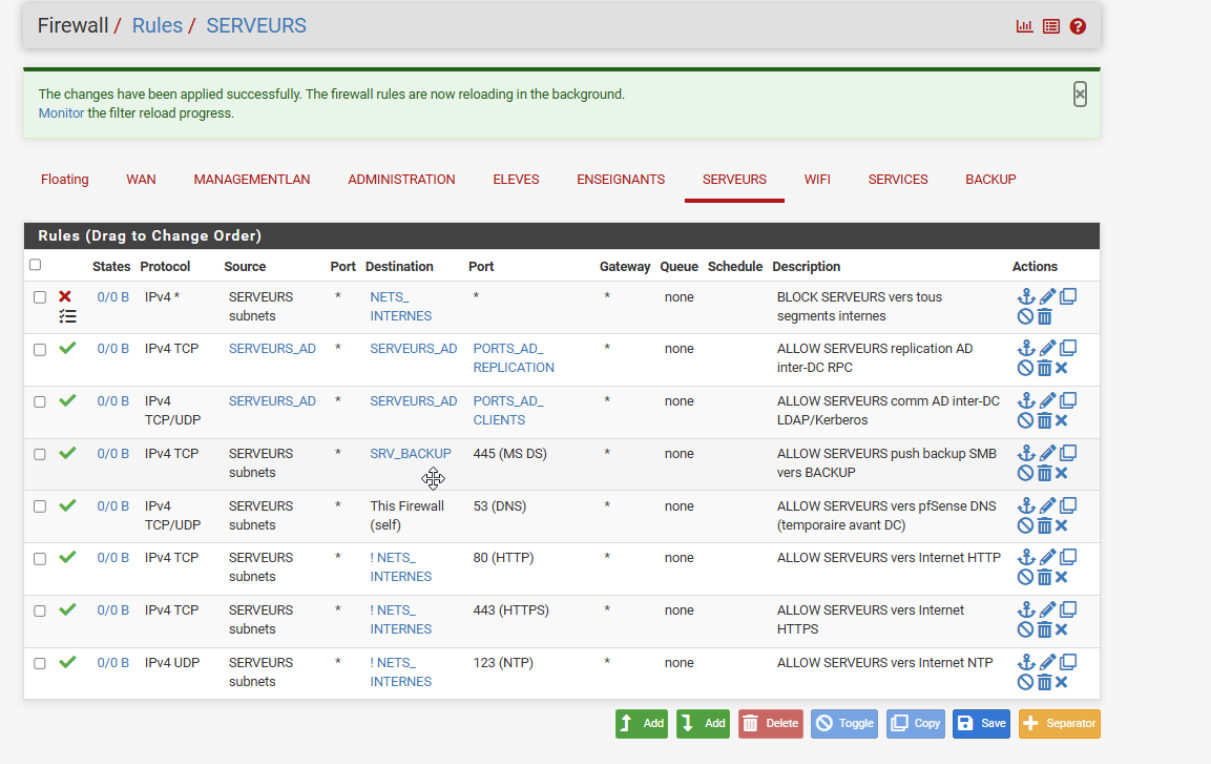


Figure 27:regles pour le segment serveurs

L'ordre des règles pfSense respecte une logique du plus restrictif au plus permissif, et du plus spécifique au plus général. Les règles BLOCK explicites sont placées en bas pour appliquer la politique deny-by-default avant toute autorisation. Les règles AD inter-DC, les plus critiques pour le bon fonctionnement de l'authentification, sont prioritaires. Les autorisations Internet, plus larges, sont en bas pour ne pas masquer des règles plus spécifiques au-dessus. À noter : la règle de blocage global NETS_INTERNES sera basculée en position basse en fin de projet. Ainsi, les autorisations inter-segments spécifiques placées au-dessus sont évaluées en premier (premier match gagnant), et NETS_INTERNES ne joue plus qu'un rôle de filet, refusant les flux internes non explicitement autorisés, sans gêner les flux légitimes.

Pour le segment SERVICES, un nouvel alias va être créé : il concernera la supervision avec Zabbix et listera les segments supervisés.

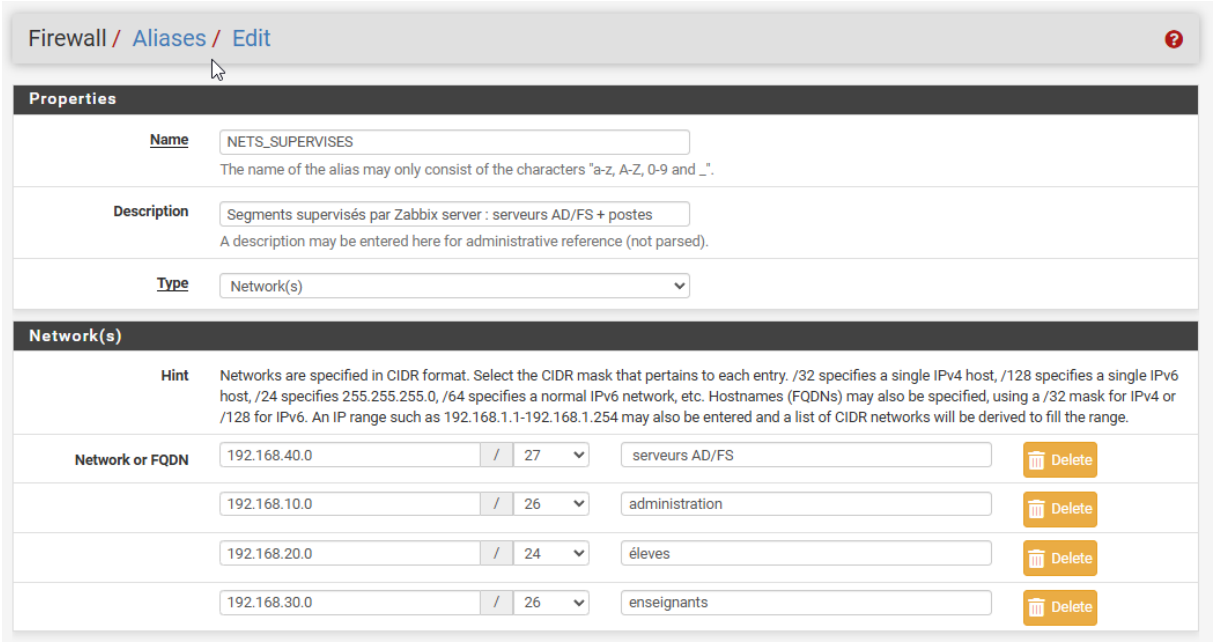


Figure 28: alias des réseaux supervisés par Zabbix

On enchaîne avec les règles du segment SERVICES. SERVICES dispose des 6 règles communes au segment serveurs, comme exposé dans la capture suivante.

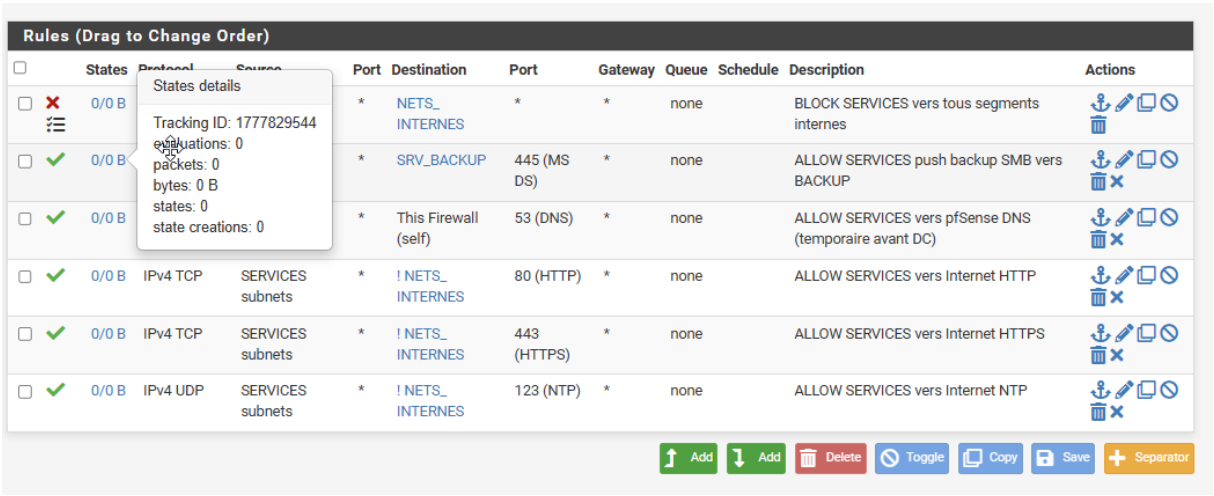


Figure 29: copie dans SERVICES des règles communes présentes dans serveurs ; on n'oublie pas de changer le nommage

La nouveauté : deux règles supplémentaires qui permettront à l'applicatif GLPI de SERVICES de communiquer avec l'Active Directory, et au serveur de supervision Zabbix de collecter les données et l'état des équipements surveillés sur le port TCP 10050.

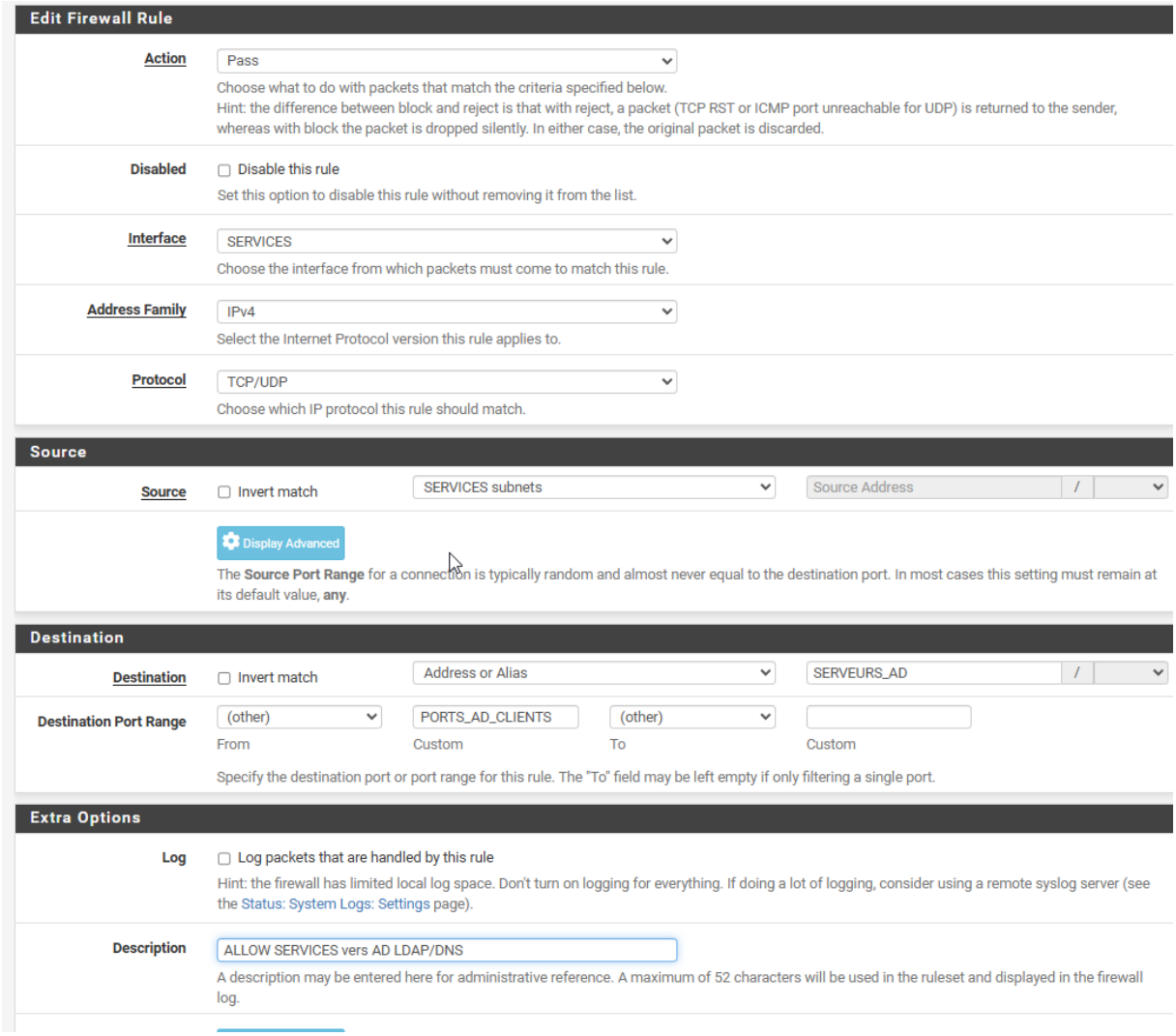


Figure 30: règle permettant la communication entre GLPI et l'AD

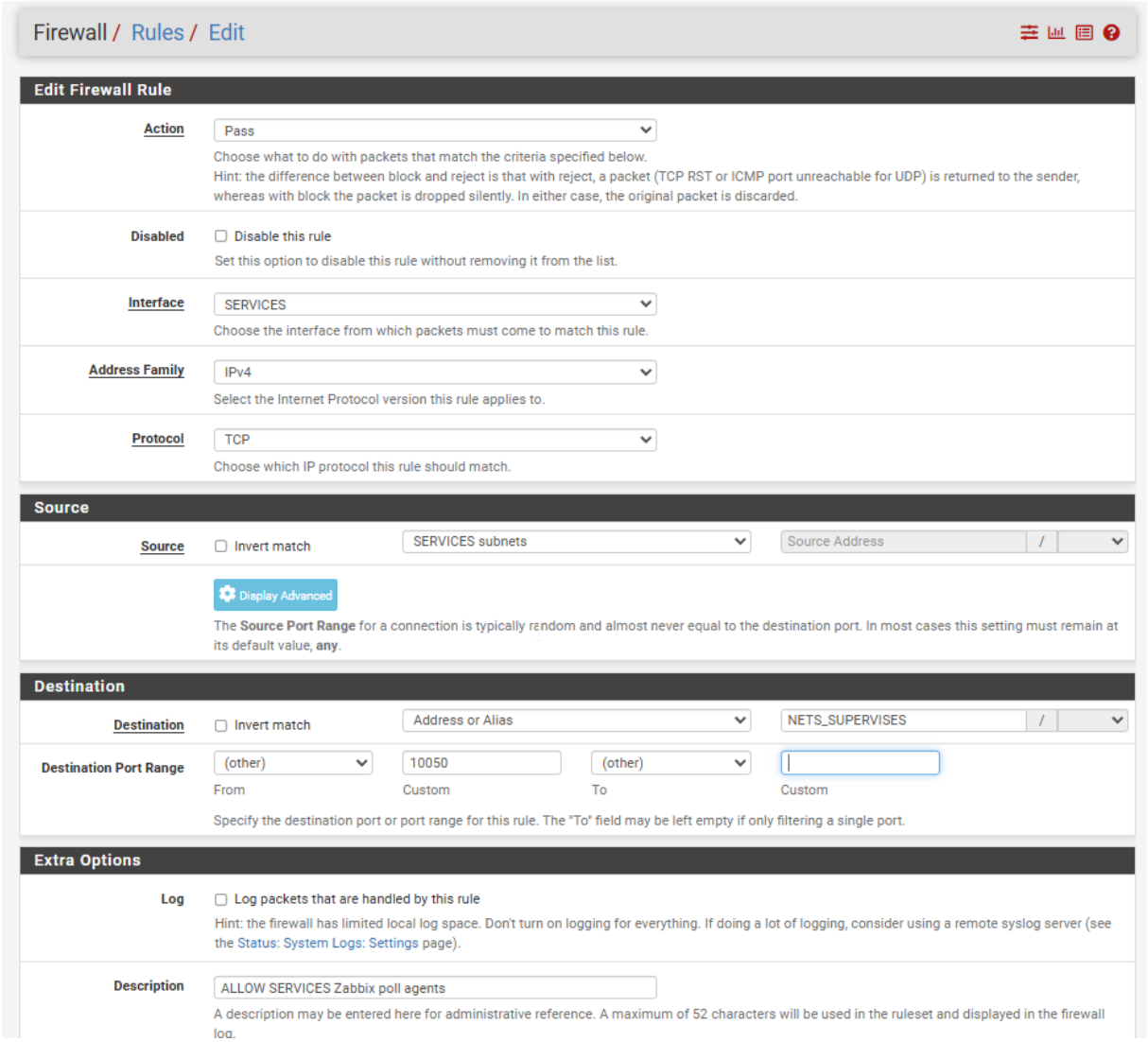


Figure 31: règle permettant la communication de Zabbix avec les segments concernés sur le port 10050

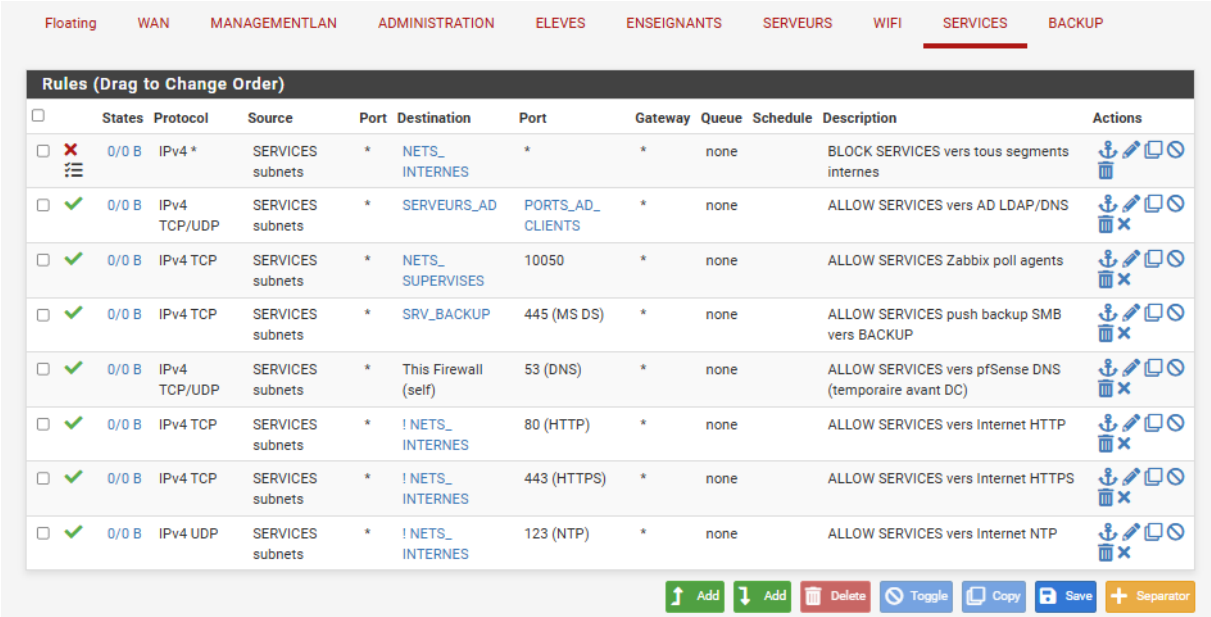


Figure 32: règles terminées et classées par ordre d'importance

Le segment backup devra être totalement isolé, mais doit disposer des logs pour pouvoir vérifier qu'aucune émission de flux n'est effectuée par le VLAN 99.

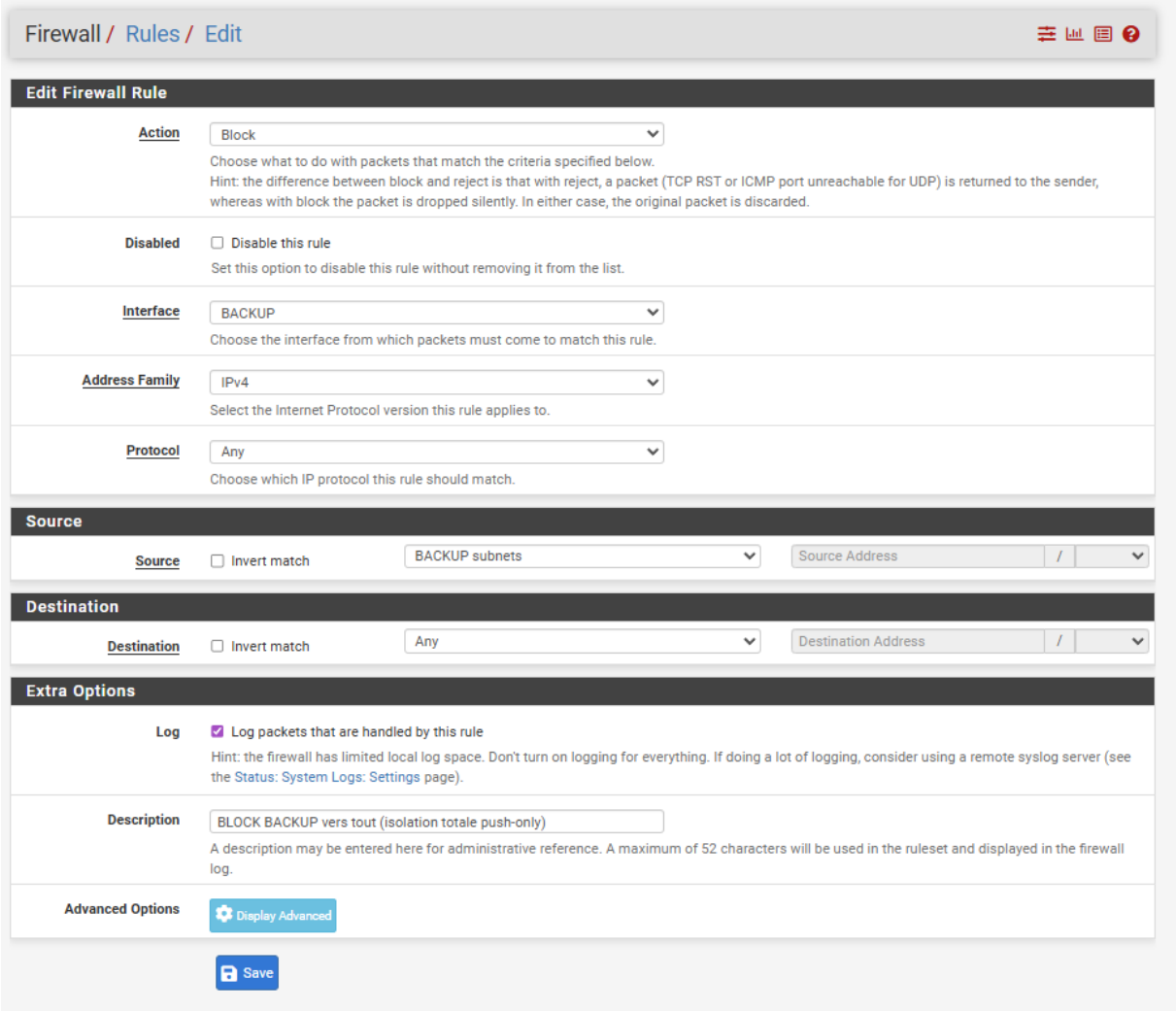


Figure 33: règles segment backup

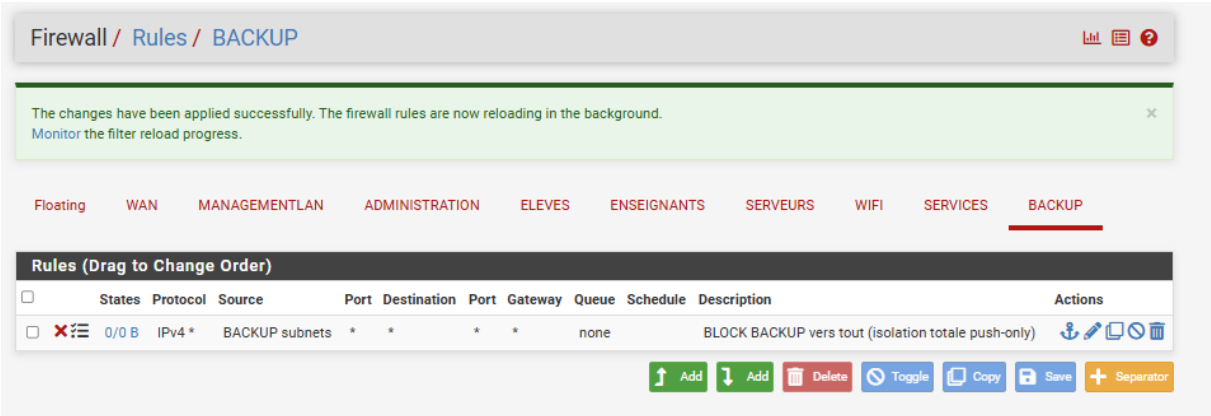


Figure 34: règles activées

Le LAN Management dispose de deux règles par défaut (autorisant tous les flux vers le LAN) à supprimer. On les supprime après avoir effectué un snapshot, puis on ajoute les 5 règles (3 copies + 2 nouvelles).

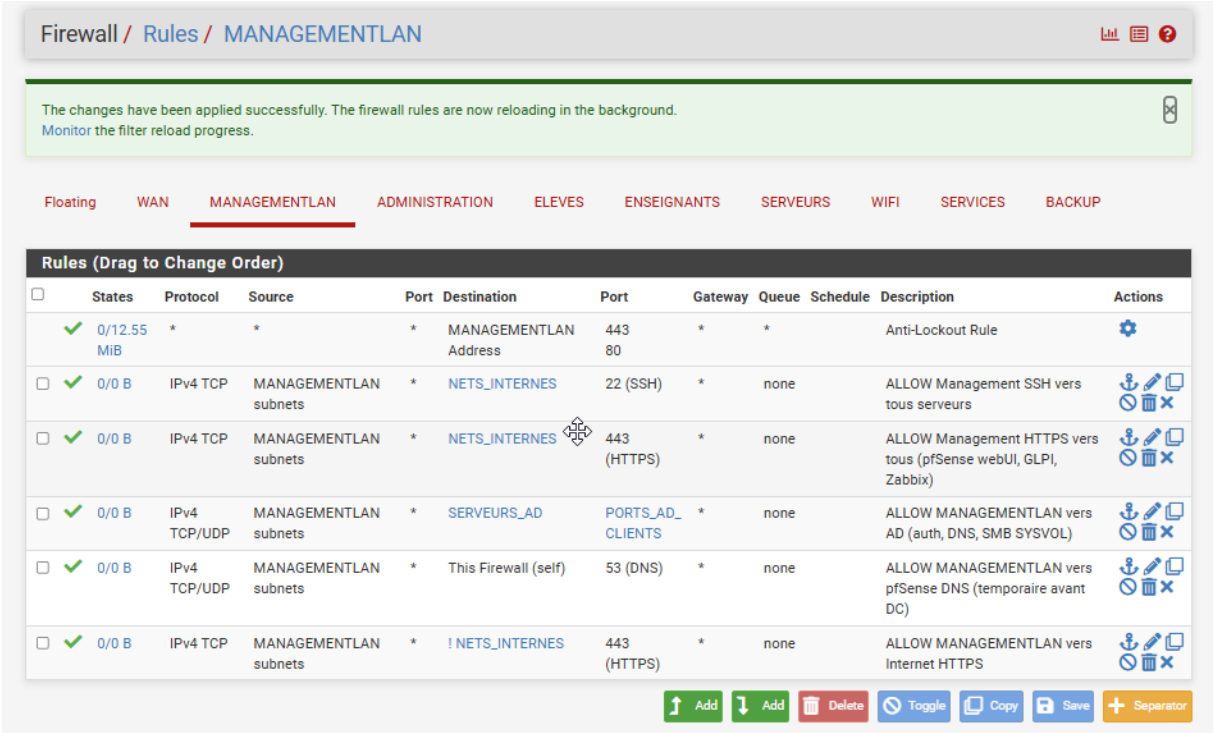
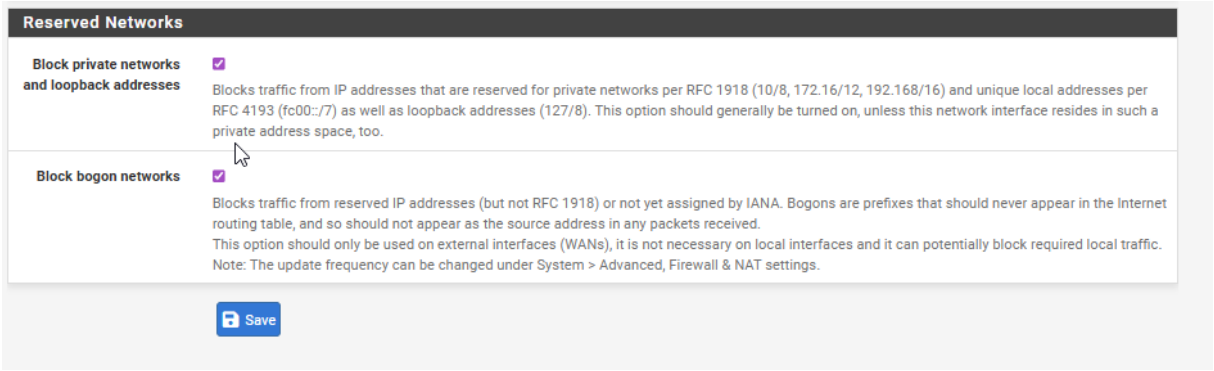
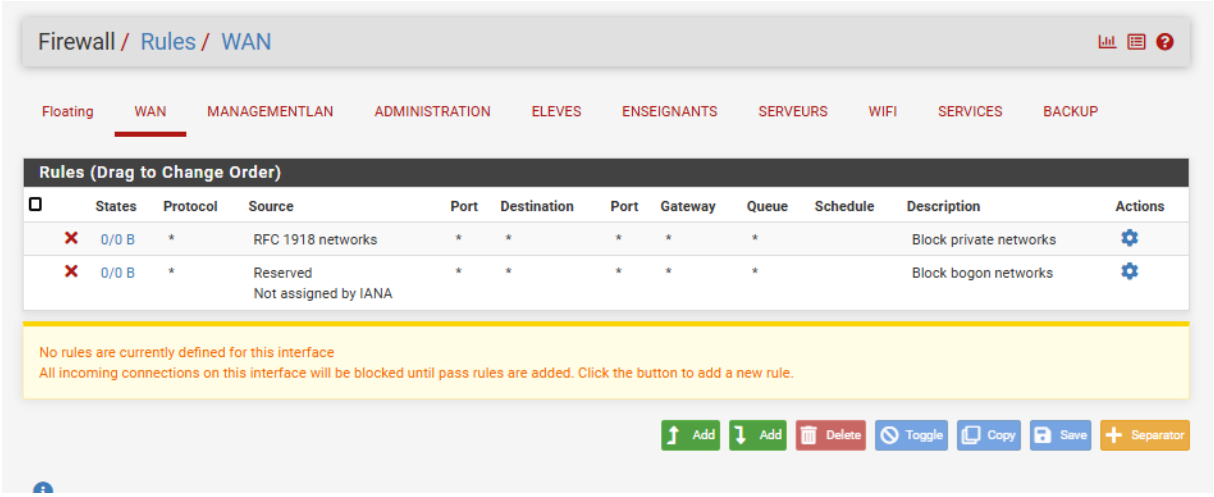


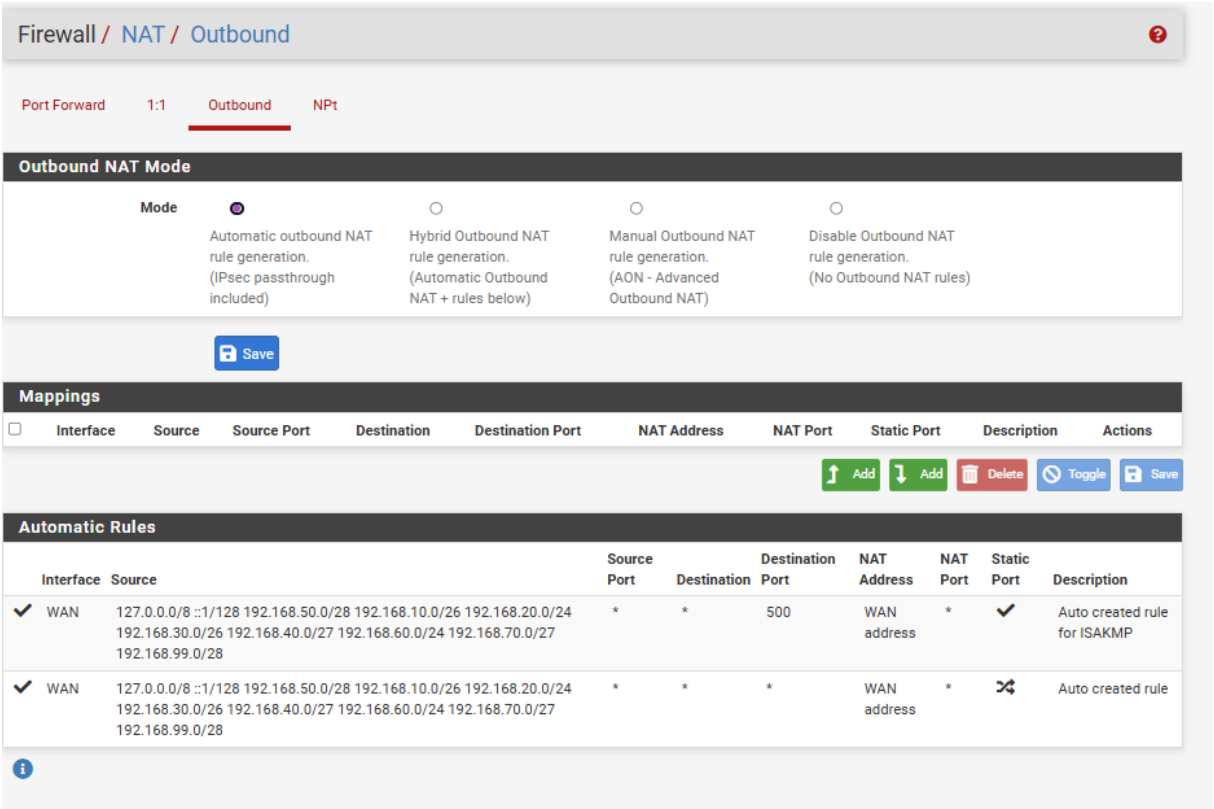
Figure 35: le segment management doit pouvoir se connecter en SSH (port 22), accéder aux interfaces web en HTTPS (port 443), en plus des habituels DNS résolveur et de l'authentification sur l'AD

Enfin, pour le WAN, on retourne dans la section interfaces et on coche le blocage de toutes les IP privées et des IP bogons, qui ne sont pas censées être routées sur Internet.

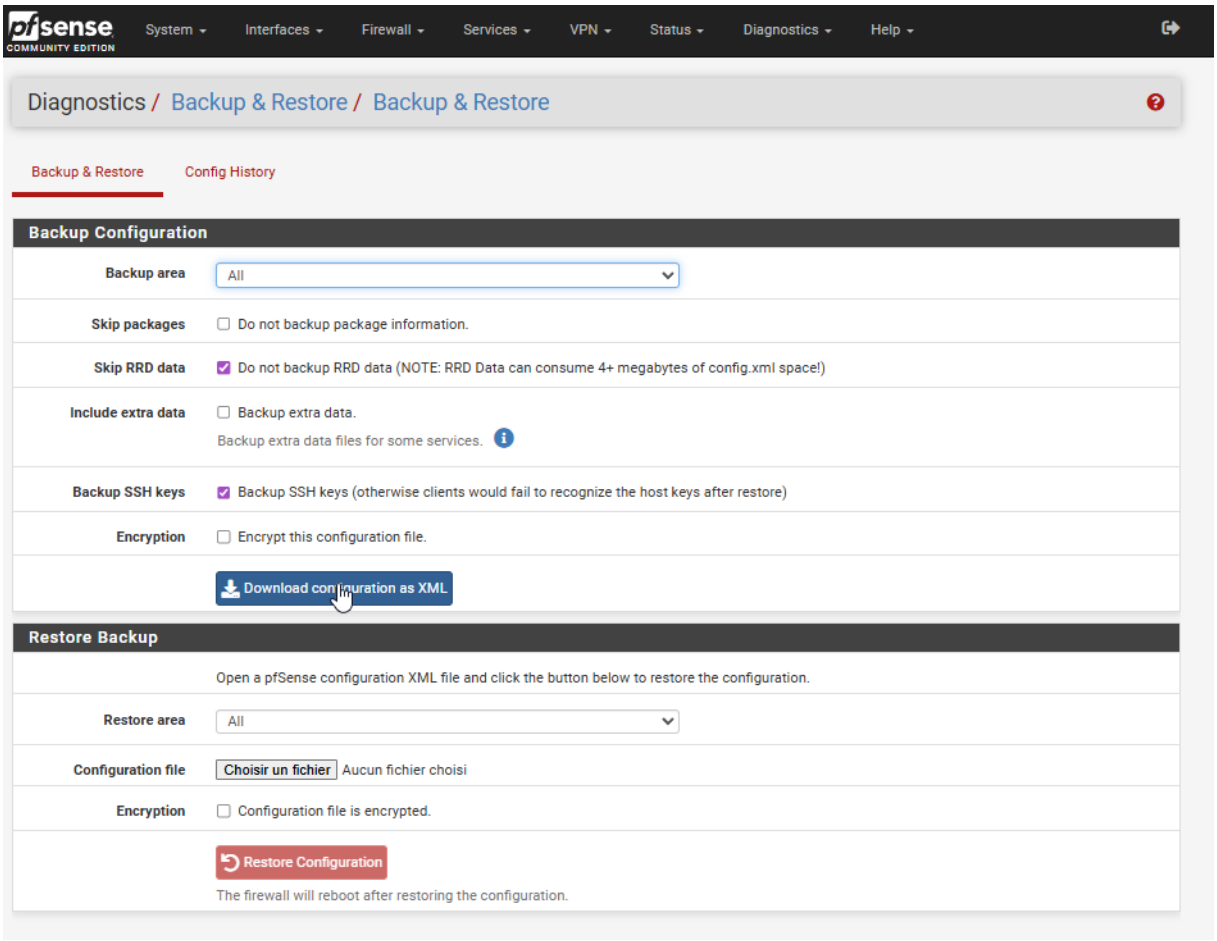




Vérification des règles outbound dans la partie NAT pour s'assurer que la configuration est correcte.



N’oublions pas de sauvegarder la configuration au format XML, qui sera stockée ultérieurement.



System
> Advanced
> Networking Disable hardware checksum offload

Disable hardware TCP segmentation offload

Disable hardware large receive offload

Bilan, difficultés et perspectives

Difficultés rencontrées

- Décalage entre les adresses MAC des interfaces OPT1→OPT7 et celles des VMnet : résolu par réaffectation manuelle dans Interface Assignments (Fig. 13).
- Synchronisation horaire : un écart NTP supérieur à 5 min casse Kerberos et donc l'authentification AD. Point de vigilance permanent.