

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).

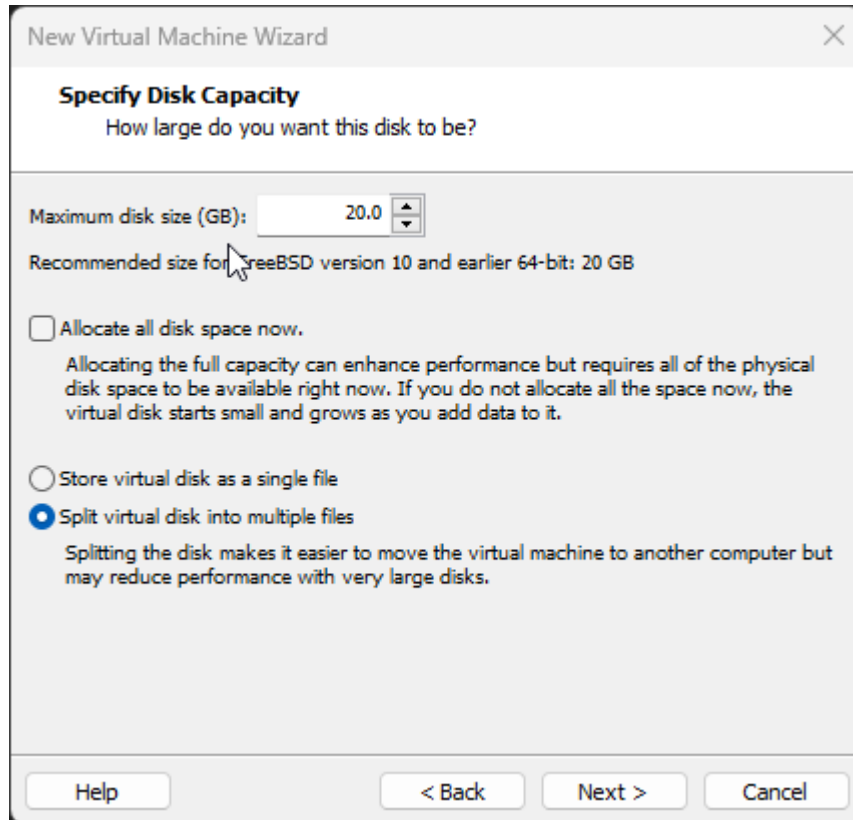
Compétences E5 visées

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.

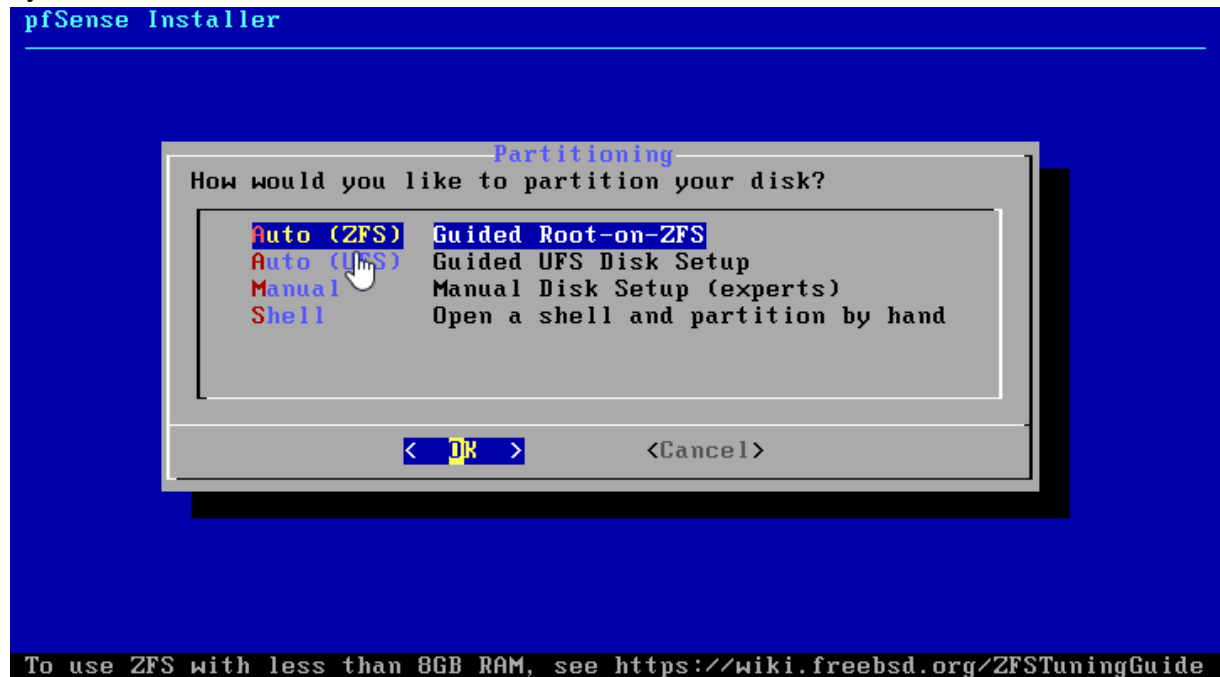


Figure 1: choix de l'installation auto ZFS

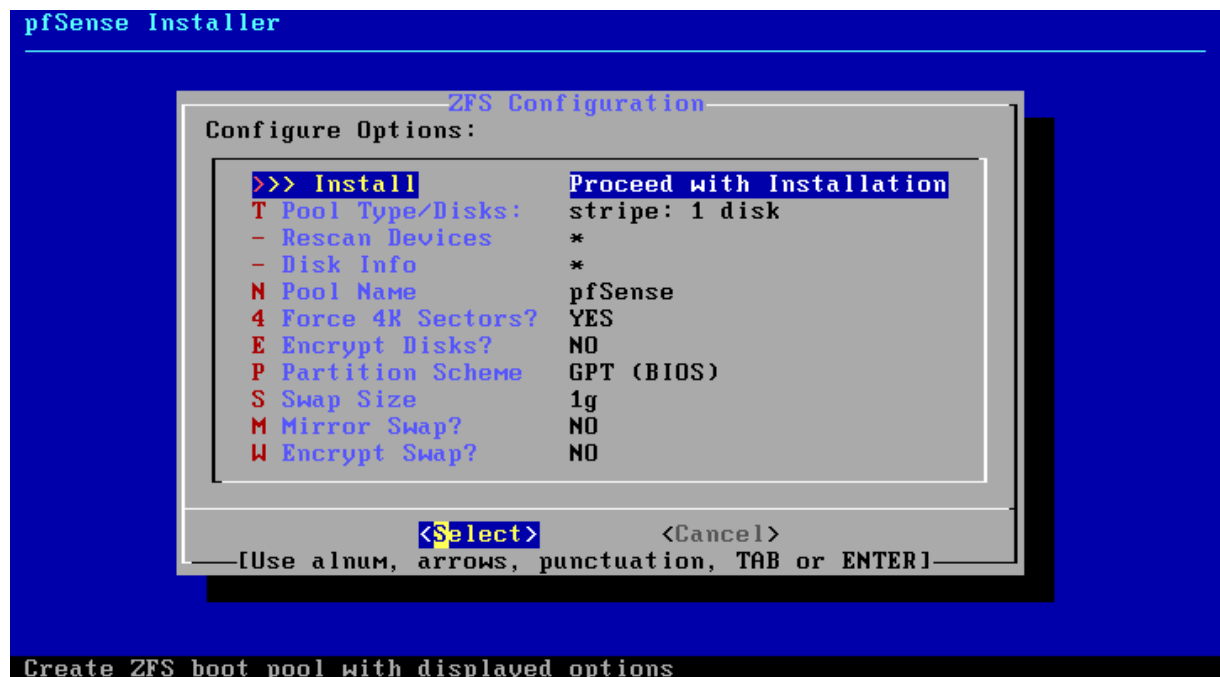


Figure 2: configuration du disque, des partitions, du swap

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)
-

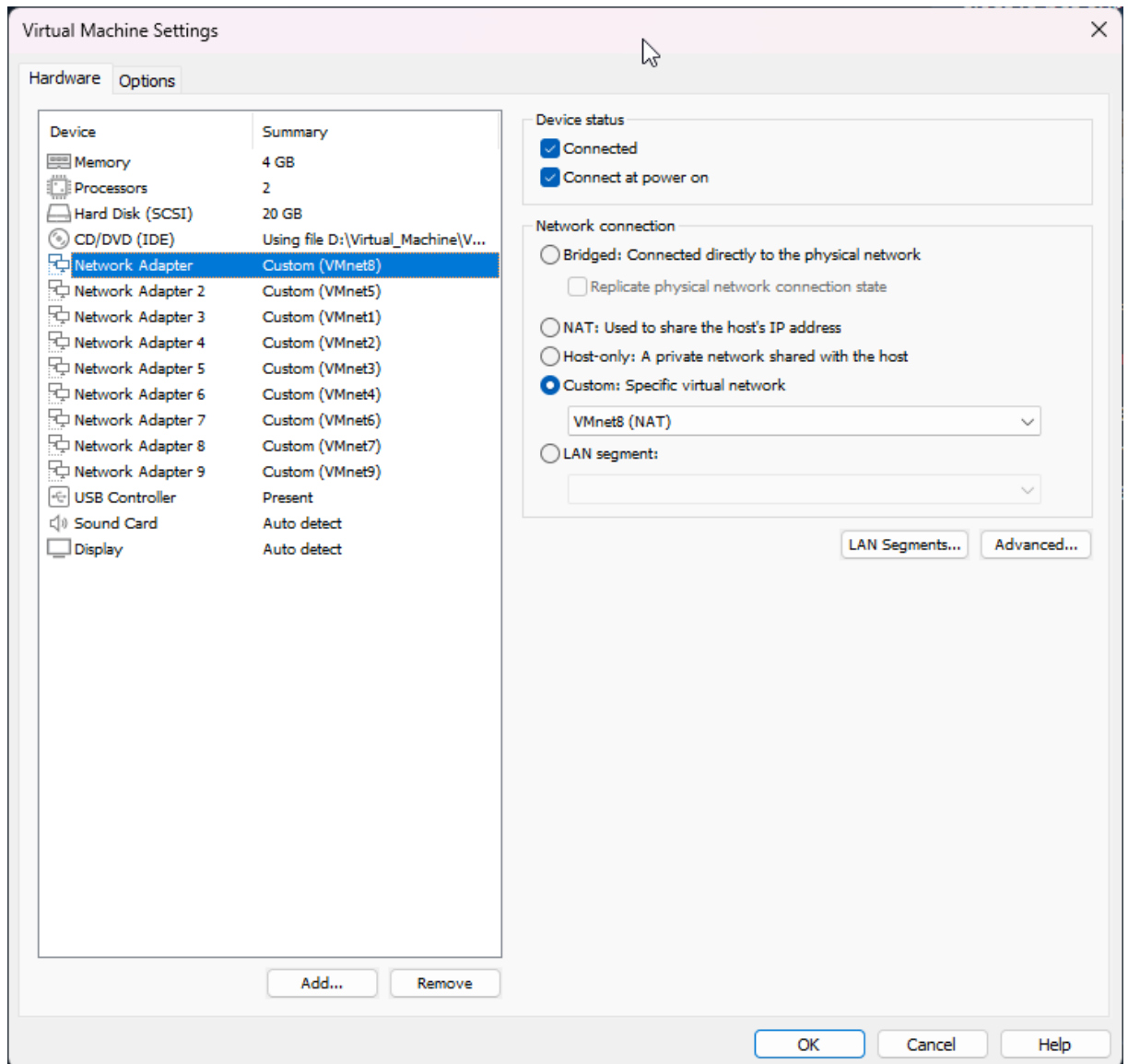


Figure 3: ajout des cartes réseau sur VMware

```
Enter the Optional 4 interface name or 'a' for auto-detection
(em5 em6 em7 em8 a or nothing if finished): em5

Enter the Optional 5 interface name or 'a' for auto-detection
(em6 em7 em8 a or nothing if finished): em6

Enter the Optional 6 interface name or 'a' for auto-detection
(em7 em8 a or nothing if finished): em7

Enter the Optional 7 interface name or 'a' for auto-detection
(em8 a or nothing if finished): em8

The interfaces will be assigned as follows:

WAN   -> em0
LAN   -> em1
OPT1  -> em2
OPT2  -> em3
OPT3  -> em4
OPT4  -> em5
OPT5  -> em6
OPT6  -> em7
OPT7  -> em8

Do you want to proceed [y'n]? █
```

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

```

4 - OPT2 (em3)
5 - OPT3 (em4)
6 - OPT4 (em5)
7 - OPT5 (em6)
8 - OPT6 (em7)
9 - OPT7 (em8)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.50.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 28

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

```

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.

```

For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.50.1/28
You can now access the webConfigurator by opening the following URL in your web
browser:
        https://192.168.50.1/

Press <ENTER> to continue.

```

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.

:

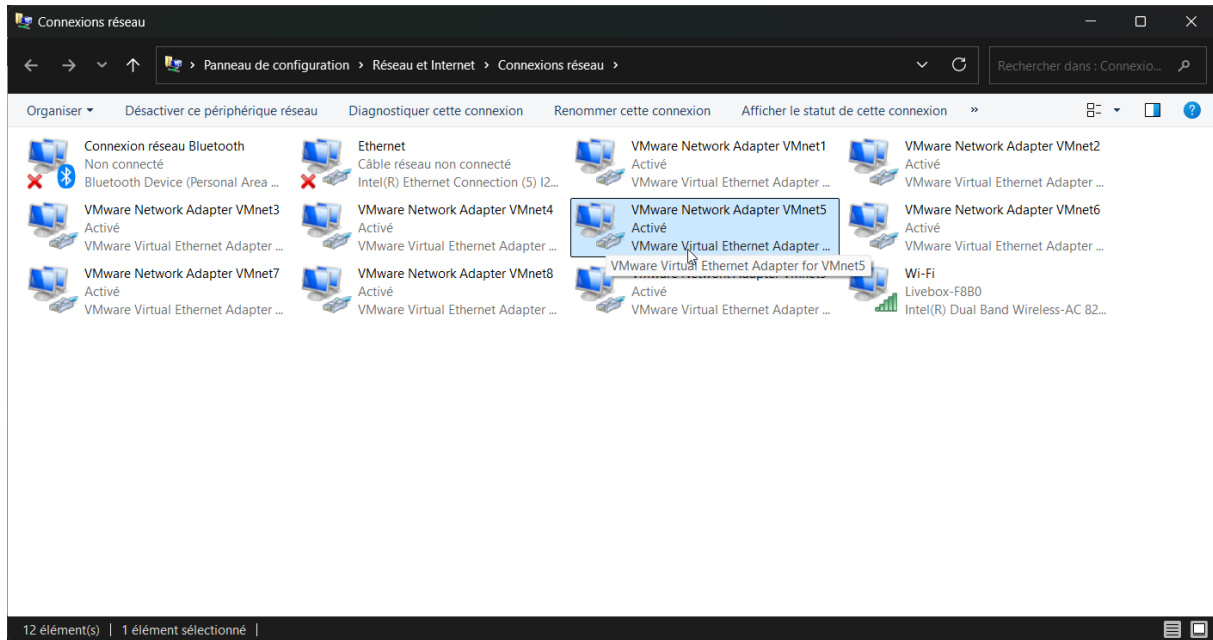


Figure 7: sélection de l'adaptateur VMnet 5

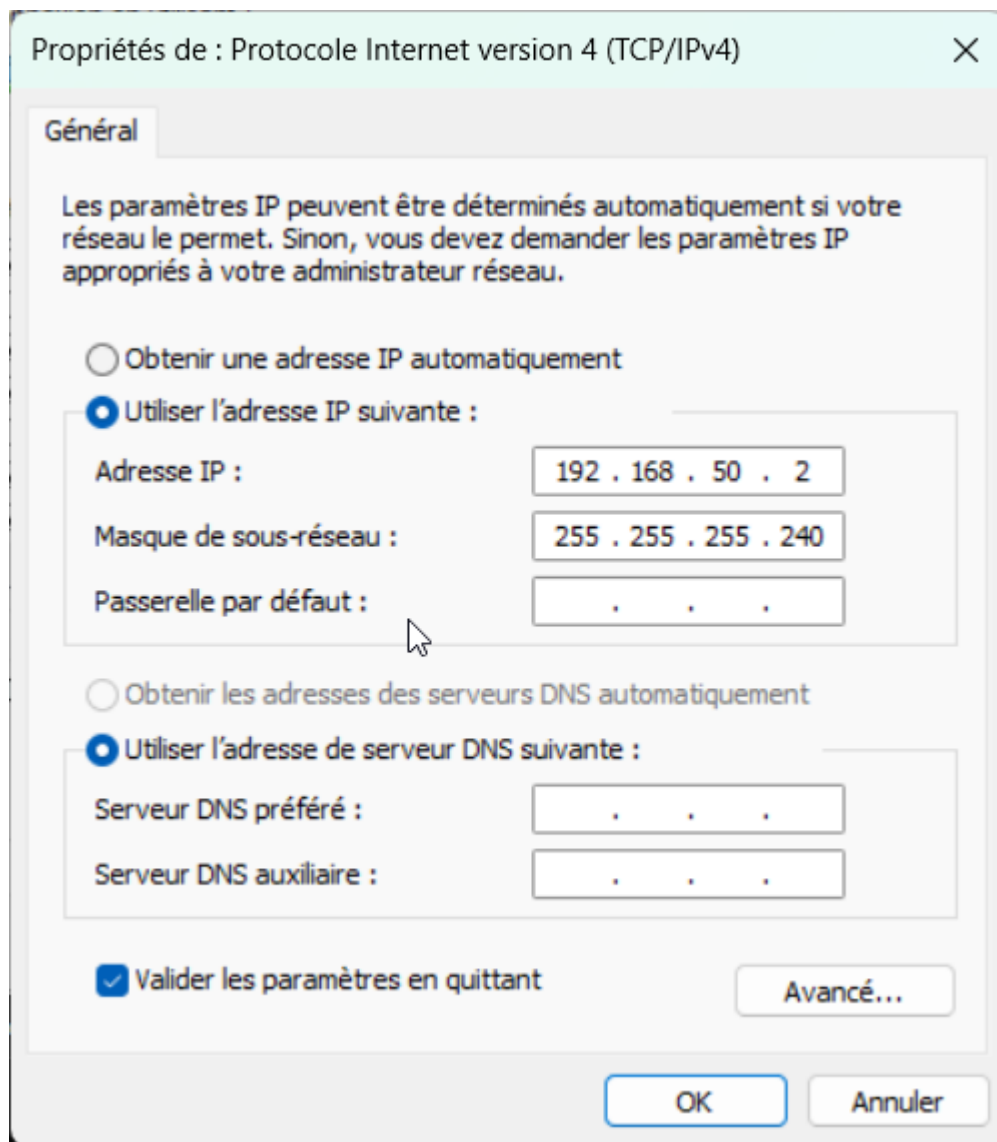


Figure 8: configuration de l'IP en 192.168.50.2

Vérification avec un test ping sur 192.168.50.1

```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [version 10.0.22631.6199]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\pacma>ping 192.168.50.1

Envoi d'une requête 'Ping' 192.168.50.1 avec 32 octets de données :
Réponse de 192.168.50.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.50.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.50.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.50.1 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 192.168.50.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\pacma>
```

Figure 9: pfSense reçoit bien les paquets

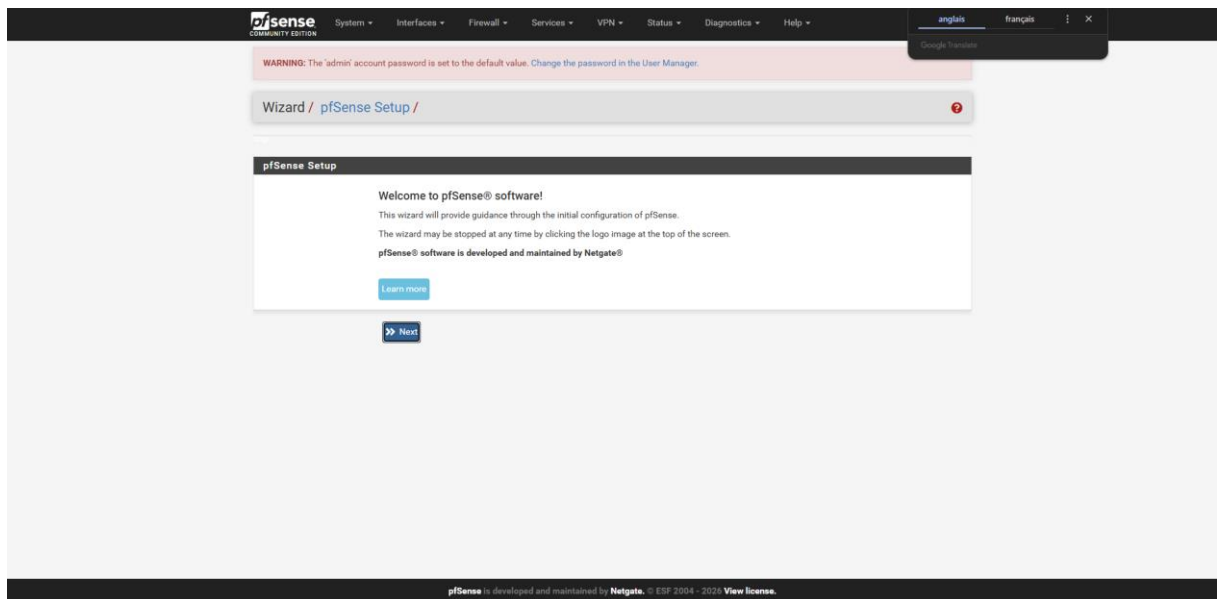
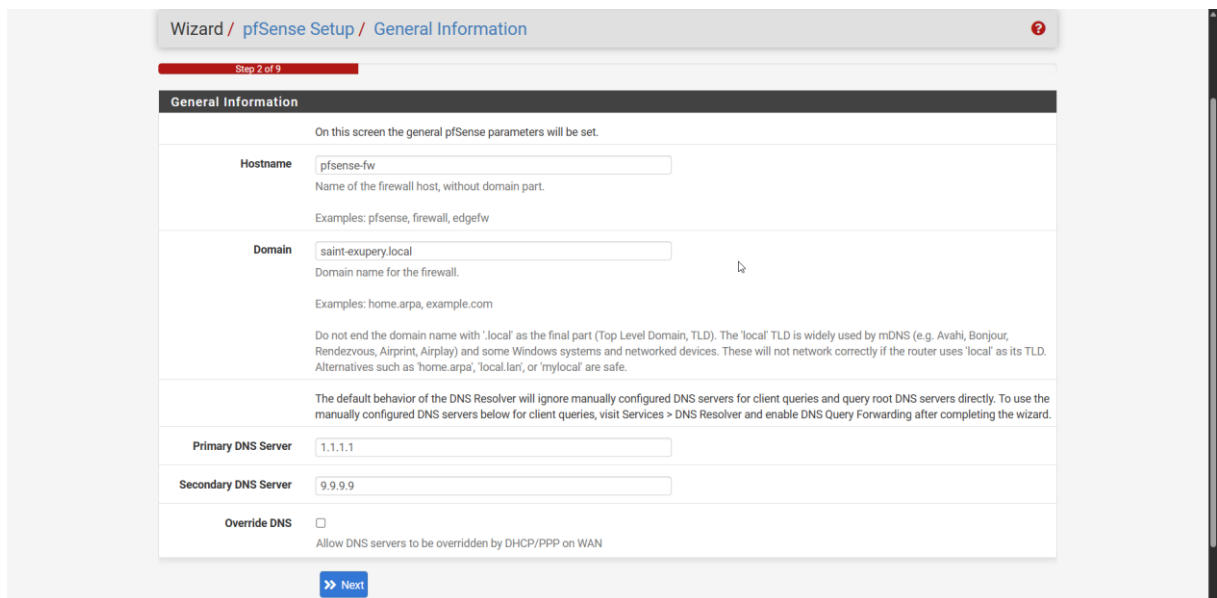


Figure 10: première connexion réussie avec le login admin et le mot de passe pfsense

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.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Time Server Information ?

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname	fr.pool.ntp.org
Enter the hostname (FQDN) of the time server.	
Timezone	Europe/Paris

Interfaces / WAN (em0) ≡ ?

General Configuration

Enable	☒ Enable interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	DHCP
IPv6 Configuration Type	DHCP6
MAC Address	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Figure 11: configuration du wan en GUI

Reserved Networks

Block private networks and loopback addresses	☐ Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	☐ Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

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.

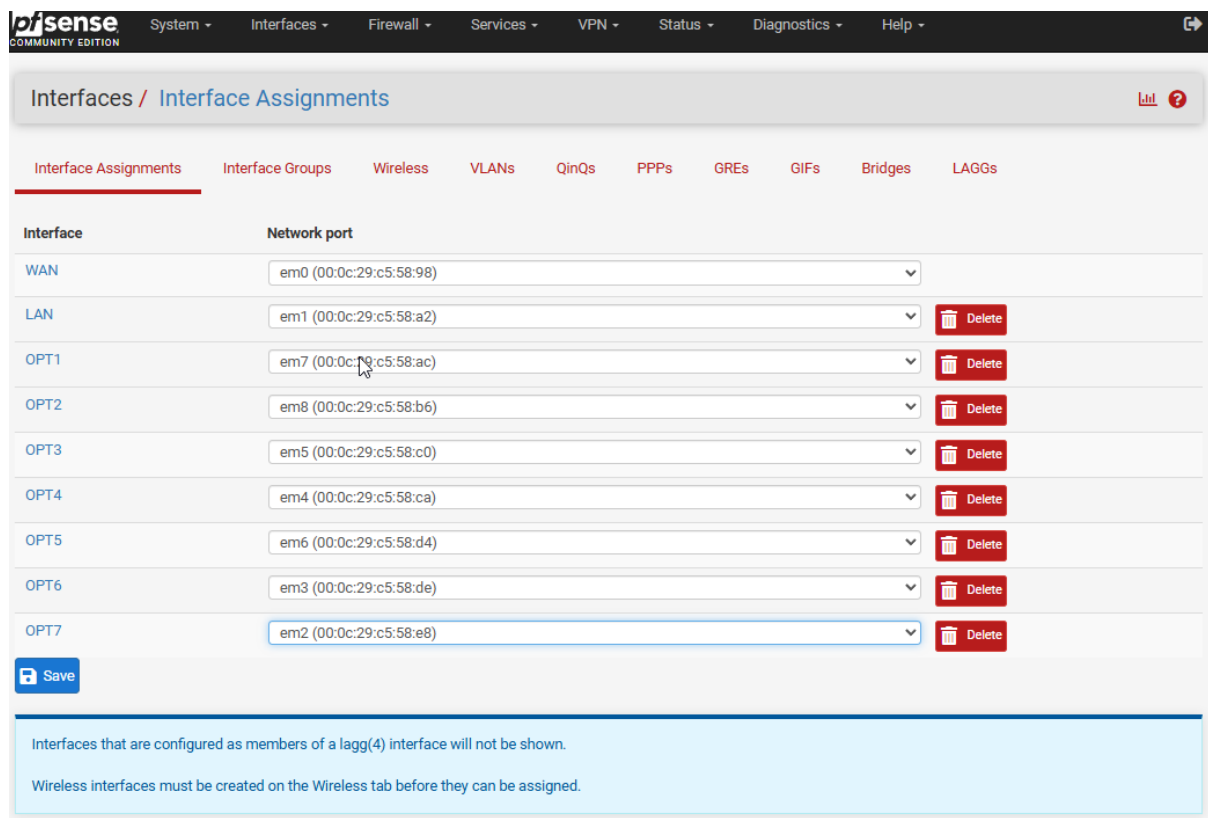


Figure 13: les adresses MAC des interfaces opérationnelles correspondent bien aux adresses MAC des différents VMnet

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.

The OPT1 configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Figure 14: configuration de OPT1 administration

Interface Assignments		Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs
Interface	Network port									
WAN	em0 (00:0c:29:c5:58:98)									
MANAGEMENTLAN	em1 (00:0c:29:c5:58:a2)									Delete
ADMINISTRATION	em7 (00:0c:29:c5:58:ac)									Delete
ELEVES	em8 (00:0c:29:c5:58:b6)									Delete
ENSEIGNANTS	em5 (00:0c:29:c5:58:c0)									Delete
SERVEURS	em4 (00:0c:29:c5:58:ca)									Delete
WIFI	em6 (00:0c:29:c5:58:d4)									Delete
SERVICES	em3 (00:0c:29:c5:58:de)									Delete
BACKUP	em2 (00:0c:29:c5:58:e8)									Delete

[Save](#)

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

Services / DHCP Server / ADMINISTRATION

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

MANAGEMENTLANADMINISTRATIONELEVESENSEIGNANTSWIFISERVICESTRANSPORTSBACKUP

General DHCP Options

DHCP Backend	ISC DHCP
Enable	☒ Enable DHCP server on ADMINISTRATION interface
BOOTP	☐ Ignore BOOTP queries
Deny Unknown Clients	Allow all clients When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients	☐ Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet	192.168.10.0/26
Subnet Range	192.168.10.1 - 192.168.10.62
Address Pool Range	192.168.10.10 From 192.168.10.50 To The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	+ Add Address Pool If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

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

Firewall / Aliases / IP					
IP Ports URLs All					
Firewall Aliases IP					
Name	Type	Values	Description	Actions	
NETS_INTERNES	Network(s)	192.168.10.0/26, 192.168.20.0/24, 192.168.30.0/26, 192.168.40.0/27, 192.168.50.0/28, 192.168.60.0/24, 192.168.70.0/27, 192.168.99.0/28	Tous les segments internes	  	
RFC1918	Network(s)	192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8	blochage de Tous les réseaux privés RFC1918	  	
SERVEURS_AD	Host(s)	192.168.40.10, 192.168.40.11	Contrôleurs de domaine AD	  	
SRV_ADMIN	Host(s)	192.168.70.10	Serveur GLPI/Zabbix	  	
SRV_FS	Host(s)	192.168.40.20	Serveur de fichiers	  	
					+ Add  Import

Figure 17: alias pour les adresses IP

Firewall / Aliases / Ports					
IP Ports URLs All					
Firewall Aliases Ports					
Name	Type	Values	Description	Actions	
PORTS_AD_CLIENTS	Port(s)	53, 88, 389, 445, 464, 636, 3268, 3269	Ports nécessaires aux services AD	  	
PORTS_AD_REPLICATION	Port(s)	49152:65535	Plage RPC dynamique pour réplcation AD inter-DC et opérations avancées (Microsoft officiel)	  	
					+ Add  Import

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.

Firewall / Rules / Edit

Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface WIFI
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match WIFI subnets Source Address /

Destination

Destination ☐ Invert match Address or Alias NETS_INTERNES /

Extra Options

Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description BLOCK WIFI vers tous segments internes
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

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

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

System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Firewall / Rules / WIFI

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating
WAN
MANAGEMENTLAN
ADMINISTRATION
ELEVES
ENSEIGNANTS
SERVEURS
WIFI
SERVICES
BACKUP

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐		0/229 B	IPv4 *	WIFI subnets	* NETS_INTERNES	*	*	none		BLOCK WIFI vers tous segments internes	
☐		0/0 B	IPv4 TCP/UDP	WIFI subnets	This Firewall (self)	53 (DNS)	*	none		ALLOW WIFI vers pfSense DNS	
☐		0/0 B	IPv4 TCP	WIFI subnets	! NETS_INTERNES	80 (HTTP)	*	none		ALLOW WIFI vers Internet HTTP	
☐		0/0 B	IPv4 TCP	WIFI subnets	! NETS_INTERNES	443 (HTTPS)	*	none		allow wifi vers internet HTTPS	

Add
Add
Delete
Toggle
Copy
Save
Separator

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.

Rules (Drag to Change Order)

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

Add
Add
Delete
Toggle
Copy
Save
Separator

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 ENSEIGNANTS vers AD (auth, DNS, SMB SYSVOL)	
☐		0/0 B	IPv4 TCP	ENSEIGNANTS subnets	* SRV_FS	445 (MS DS)	*	none		ALLOW ENSEIGNANTS vers 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 ENSEIGNANTS vers 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 répllication 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).
- Règle 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.

Firewall / Rules / SERVEURS

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating WAN MANAGEMENTLAN ADMINISTRATION ELEVES ENSEIGNANTS **SERVEURS** WIFI SERVICES BACKUP

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✗	0/0 B	IPv4 *	SERVEURS subnets	* NETS_ INTERNES	*	*	none		BLOCK SERVEURS vers tous segments internes	
☐	✓	0/0 B	IPv4 TCP	SERVEURS_AD	* SERVEURS_AD	PORTS_AD_REPLICATION	*	none		ALLOW SERVEURS replication AD inter-DC RPC	
☐	✓	0/0 B	IPv4 TCP/UDP	SERVEURS_AD	* SERVEURS_AD	PORTS_AD_CLIENTS	*	none		ALLOW SERVEURS comm AD inter-DC LDAP/Kerberos	
☐	✓	0/0 B	IPv4 TCP	SERVEURS subnets	* SRV_BACKUP	445 (MS DS)	*	none		ALLOW SERVEURS push backup SMB vers BACKUP	
☐	✓	0/0 B	IPv4 TCP/UDP	SERVEURS subnets	* This Firewall (self)	53 (DNS)	*	none		ALLOW SERVEURS vers pfSense DNS (temporaire avant DC)	
☐	✓	0/0 B	IPv4 TCP	SERVEURS subnets	* ! NETS_ INTERNES	80 (HTTP)	*	none		ALLOW SERVEURS vers Internet HTTP	
☐	✓	0/0 B	IPv4 TCP	SERVEURS subnets	* ! NETS_ INTERNES	443 (HTTPS)	*	none		ALLOW SERVEURS vers Internet HTTPS	
☐	✓	0/0 B	IPv4 UDP	SERVEURS subnets	* ! NETS_ INTERNES	123 (NTP)	*	none		ALLOW SERVEURS vers Internet NTP	

↑ Add ↓ Add Delete Toggle Copy Save + Separator

Figure 27: règles 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.

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
A description may be entered here for administrative reference (not parsed).

Type

Network(s)

Hint Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN					
192.168.40.0	/	27	serveurs AD/FS	Delete	
192.168.10.0	/	26	administration	Delete	
192.168.20.0	/	24	élèves	Delete	
192.168.30.0	/	26	enseignants	Delete	

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.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✗ 0/0 B			*	NETS_ INTERNES	*	*	none		BLOCK SERVICES vers tous segments internes	Add Edit Delete
☐	✓ 0/0 B			*	SRV_BACKUP	445 (MS DS)	*	none		ALLOW SERVICES push backup SMB vers BACKUP	Add Edit Delete
☐	✓ 0/0 B			*	This Firewall (self)	53 (DNS)	*	none		ALLOW SERVICES vers pfSense DNS (temporaire avant DC)	Add Edit Delete
☐	✓ 0/0 B	IPv4 TCP	SERVICES subnets	*	! NETS_ INTERNES	80 (HTTP)	*	none		ALLOW SERVICES vers Internet HTTP	Add Edit Delete
☐	✓ 0/0 B	IPv4 TCP	SERVICES subnets	*	! NETS_ INTERNES	443 (HTTPS)	*	none		ALLOW SERVICES vers Internet HTTPS	Add Edit Delete
☐	✓ 0/0 B	IPv4 UDP	SERVICES subnets	*	! NETS_ INTERNES	123 (NTP)	*	none		ALLOW SERVICES vers Internet NTP	Add Edit Delete

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'applétif 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.

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface

SERVICES

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP/UDP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

SERVICES subnets

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

Address or Alias

SERVEURS_AD

/

Destination Port Range

(other)

PORTS_AD_CLIENTS

(other)

FromCustomToCustom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

ALLOW SERVICES vers AD LDAP/DNS

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

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

FloatingWANMANAGEMENTLANADMINISTRATIONELEVSENEIGNANTSSEURVERSWIFISERVICESBACKUP

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐		0/0 B	IPv4 *	SERVICES subnets	*	NETS_ INTERNES	*	*	none	BLOCK SERVICES vers tous segments internes	
☐		0/0 B	IPv4 TCP/UDP	SERVICES subnets	*	SERVEURS_AD	PORTS_AD_ CLIENTS	*	none	ALLOW SERVICES vers AD LDAP/DNS	
☐		0/0 B	IPv4 TCP	SERVICES subnets	*	NETS_ SUPERVISES	10050	*	none	ALLOW SERVICES Zabbix poll agents	
☐		0/0 B	IPv4 TCP	SERVICES subnets	*	SRV_BACKUP	445 (MS DS)	*	none	ALLOW SERVICES push backup SMB vers BACKUP	
☐		0/0 B	IPv4 TCP/UDP	SERVICES subnets	*	This Firewall (self)	53 (DNS)	*	none	ALLOW SERVICES vers pfSense DNS (temporaire avant DC)	
☐		0/0 B	IPv4 TCP	SERVICES subnets	*	! NETS_ INTERNES	80 (HTTP)	*	none	ALLOW SERVICES vers Internet HTTP	
☐		0/0 B	IPv4 TCP	SERVICES subnets	*	! NETS_ INTERNES	443 (HTTPS)	*	none	ALLOW SERVICES vers Internet HTTPS	
☐		0/0 B	IPv4 UDP	SERVICES subnets	*	! NETS_ INTERNES	123 (NTP)	*	none	ALLOW SERVICES vers Internet NTP	

Add

Add

Delete

Toggle

Copy

Save

Separator

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.

Firewall / Rules / Edit

Edit Firewall Rule

Action Block
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface BACKUP
 Choose the interface from which packets must come to match this rule.

Address Family IPv4
 Select the Internet Protocol version this rule applies to.

Protocol Any
 Choose which IP protocol this rule should match.

Source

Source ☐ Invert match BACKUP subnets Source Address /

Destination

Destination ☐ Invert match Any Destination Address /

Extra Options

Log ☒ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description BLOCK BACKUP vers tout (isolation totale push-only)
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Save

Figure 33: règles segment backup

Firewall / Rules / BACKUP

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

Floating WAN MANAGEMENTLAN ADMINISTRATION ELEVES ENSEIGNANTS SERVEURS WIFI SERVICES **BACKUP**

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐		0/0 B	IPv4 *	BACKUP subnets	*	*	*	*	none	BLOCK BACKUP vers tout (isolation totale push-only)	

↑ Add ↓ Add Delete Toggle Copy Save + Separator

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).

Firewall / Rules / MANAGEMENTLAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

Floating WAN **MANAGEMENTLAN** ADMINISTRATION ELEVES ENSEIGNANTS SERVEURS WIFI SERVICES BACKUP

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓ 0/12.55 MIB	*	*	*	MANAGEMENTLAN Address	443 80	*	*		Anti-Lockout Rule	
☐	✓ 0/0 B	IPv4 TCP	MANAGEMENTLAN subnets	*	NETS_INTERNES	22 (SSH)	*	none		ALLOW Management SSH vers tous serveurs	
☐	✓ 0/0 B	IPv4 TCP	MANAGEMENTLAN subnets	*	NETS_INTERNES	443 (HTTPS)	*	none		ALLOW Management HTTPS vers tous (pfSense webUI, GLPI, Zabbix)	
☐	✓ 0/0 B	IPv4 TCP/UDP	MANAGEMENTLAN subnets	*	SERVEURS_AD	PORTS_AD_CLIENTS	*	none		ALLOW MANAGEMENTLAN vers AD (auth, DNS, SMB SYSVOL)	
☐	✓ 0/0 B	IPv4 TCP/UDP	MANAGEMENTLAN subnets	*	This Firewall (self)	53 (DNS)	*	none		ALLOW MANAGEMENTLAN vers pfSense DNS (temporaire avant DC)	
☐	✓ 0/0 B	IPv4 TCP	MANAGEMENTLAN subnets	*	! NETS_INTERNES	443 (HTTPS)	*	none		ALLOW MANAGEMENTLAN vers Internet HTTPS	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

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.

Reserved Networks

Block private networks and loopback addresses ☒ Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks ☒ Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

Firewall / Rules / WAN

Floating **WAN** MANAGEMENTLAN ADMINISTRATION ELEVES ENSEIGNANTS SERVEURS WIFI SERVICES BACKUP

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
☒	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add Add Delete Toggle Copy Save Separator

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

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NPt

Outbound NAT Mode

Mode ☒ Automatic outbound NAT rule generation. (IPsec passthrough included) ☐ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below) ☐ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT) ☐ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

☐	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
	Add		Add		Delete		Toggle		Save	

Automatic Rules

☐	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
☒	WAN	127.0.0.0/8 ::1/128 192.168.50.0/28 192.168.10.0/26 192.168.20.0/24 192.168.30.0/26 192.168.40.0/27 192.168.60.0/24 192.168.70.0/27 192.168.99.0/28	*	*	500	WAN address	*	☒	Auto created rule for ISAKMP
☒	WAN	127.0.0.0/8 ::1/128 192.168.50.0/28 192.168.10.0/26 192.168.20.0/24 192.168.30.0/26 192.168.40.0/27 192.168.60.0/24 192.168.70.0/27 192.168.99.0/28	*	*	*	WAN address	*		Auto created rule

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

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Diagnostics / Backup & Restore / Backup & Restore ?

Backup & Restore Config History

Backup Configuration

Backup area: All ▾

Skip packages: ☐ Do not backup package information.

Skip RRD data: ☒ Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)

Include extra data: ☐ Backup extra data.
Backup extra data files for some services. ⓘ

Backup SSH keys: ☒ Backup SSH keys (otherwise clients would fail to recognize the host keys after restore)

Encryption: ☐ Encrypt this configuration file.

[Download configuration as XML](#)

Restore Backup

Open a pfSense configuration XML file and click the button below to restore the configuration.

Restore area: All ▾

Configuration file: [Choisir un fichier](#) Aucun fichier choisi

Encryption: ☐ Configuration file is encrypted.

[Restore Configuration](#)

The firewall will reboot after restoring the configuration.

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.

