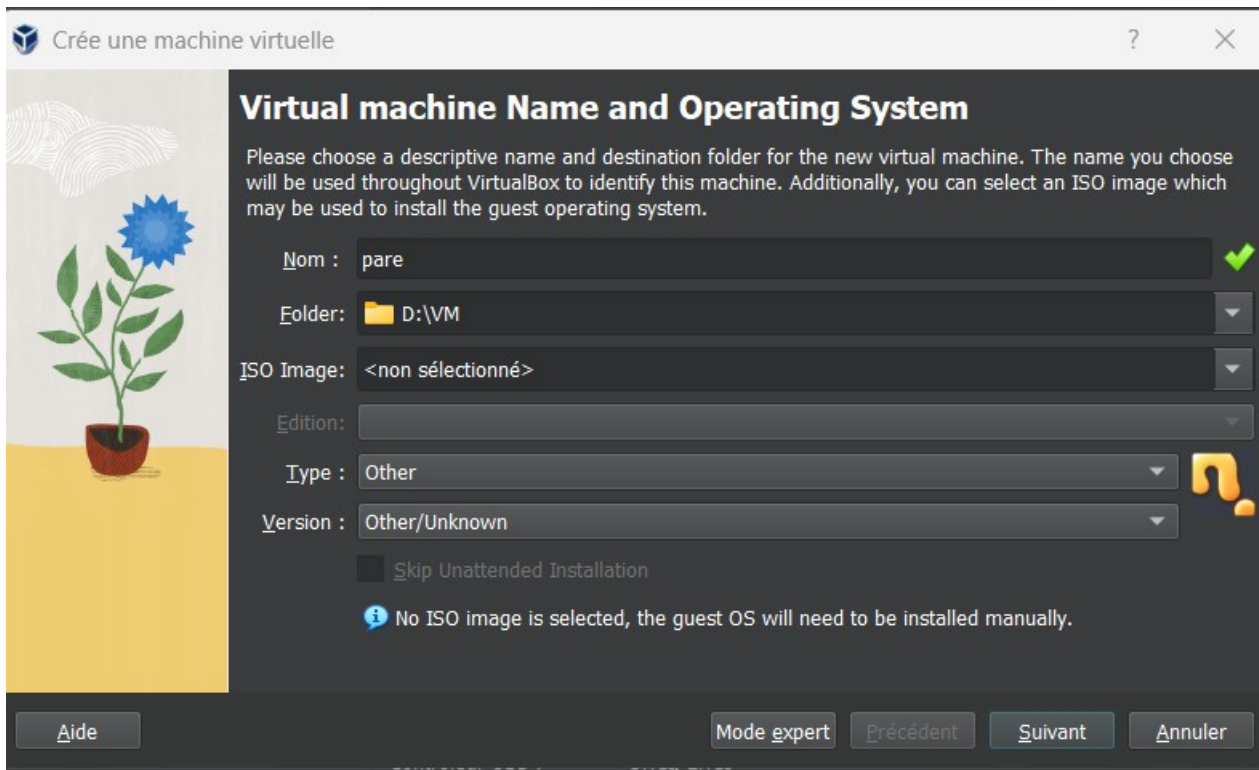


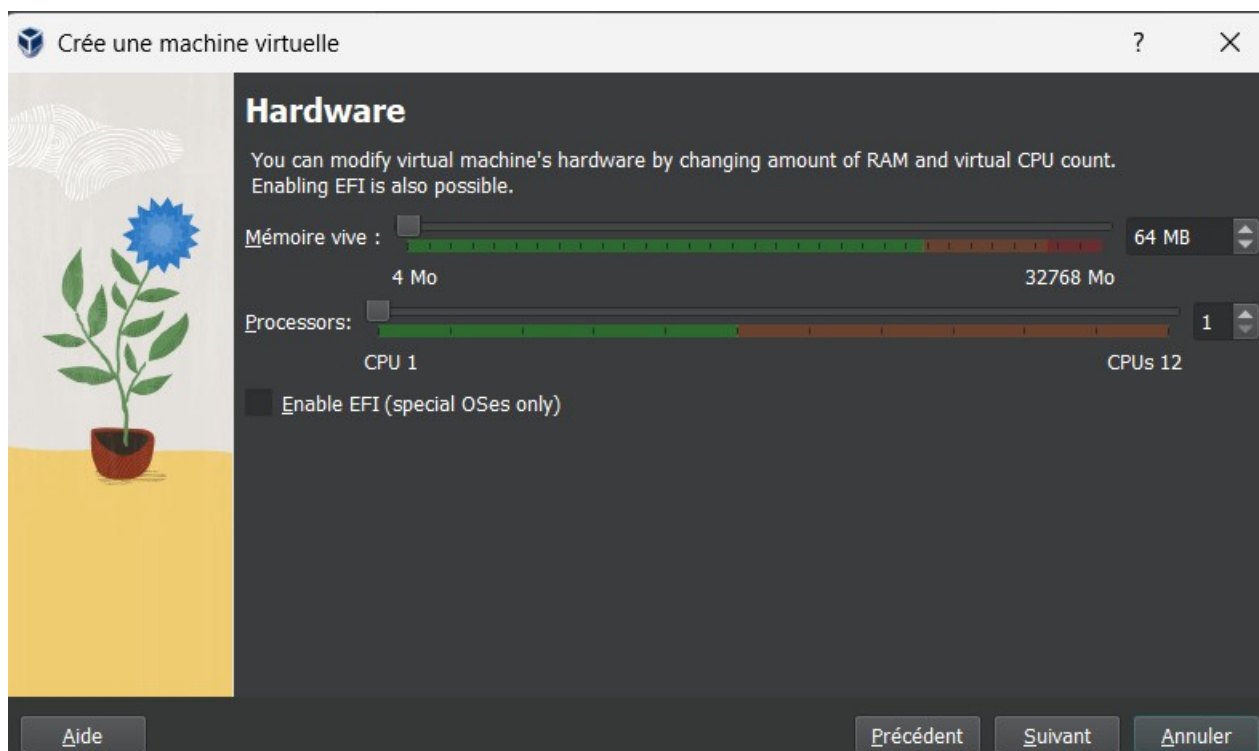
Pare-feu PFsense

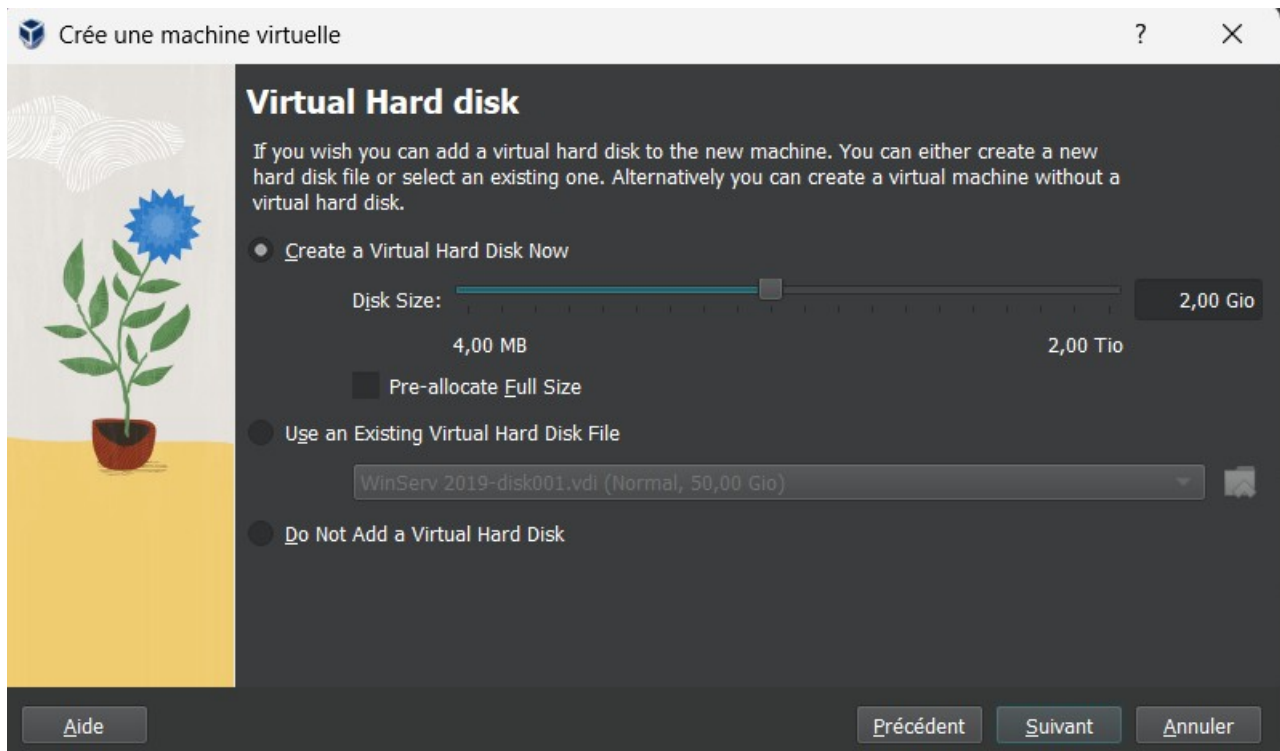
Installation du pare-feu (Pfsense)

Créer un nouvelle machine virtuel

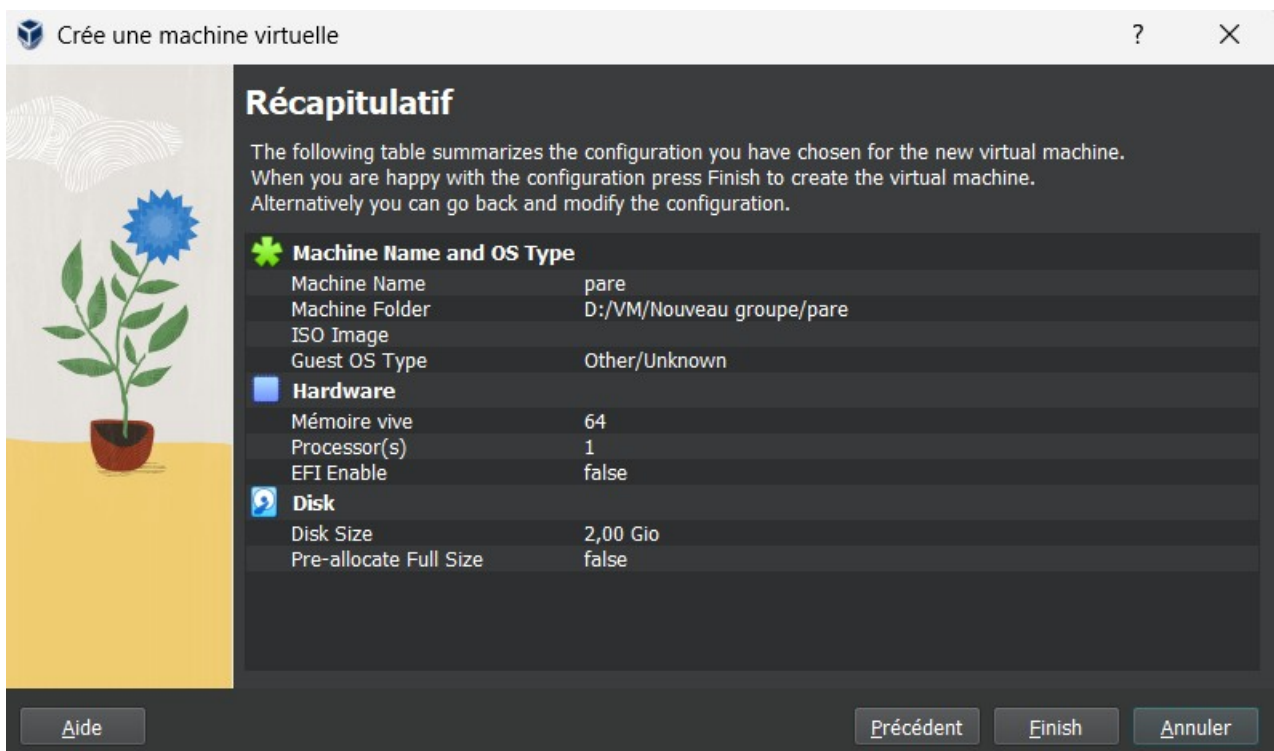


puis la configurer





puis finish

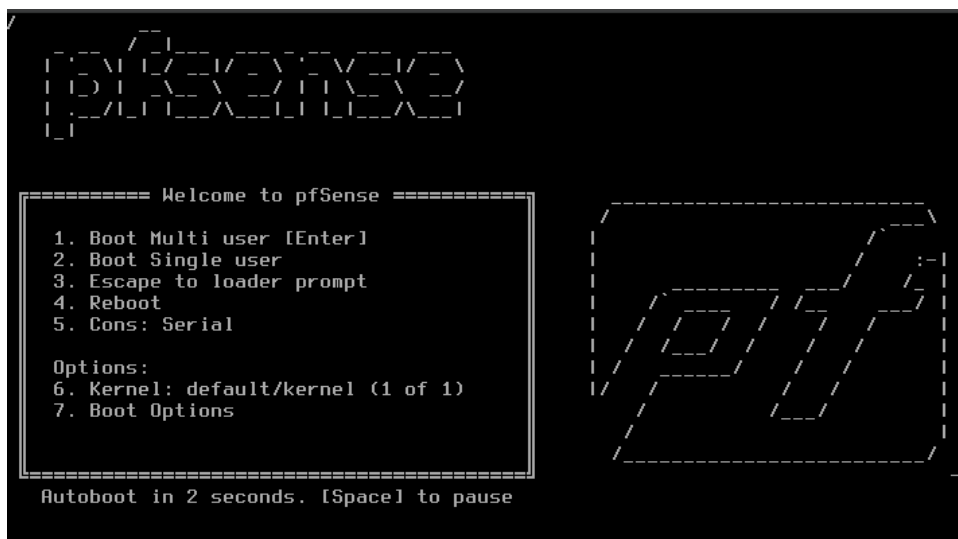


puis dans configuration ajoute le fichier
pfSense-CE-2.7.2-RELEASE-amd64.iso

Lancer la machine virtuel et faire la configuration de Pfsense

Maël Poisson

début de l'installation



fin de l'installation

```
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

KVM Guest - Netgate Device ID: c052b21e1760760aee55

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.27.16.62/24

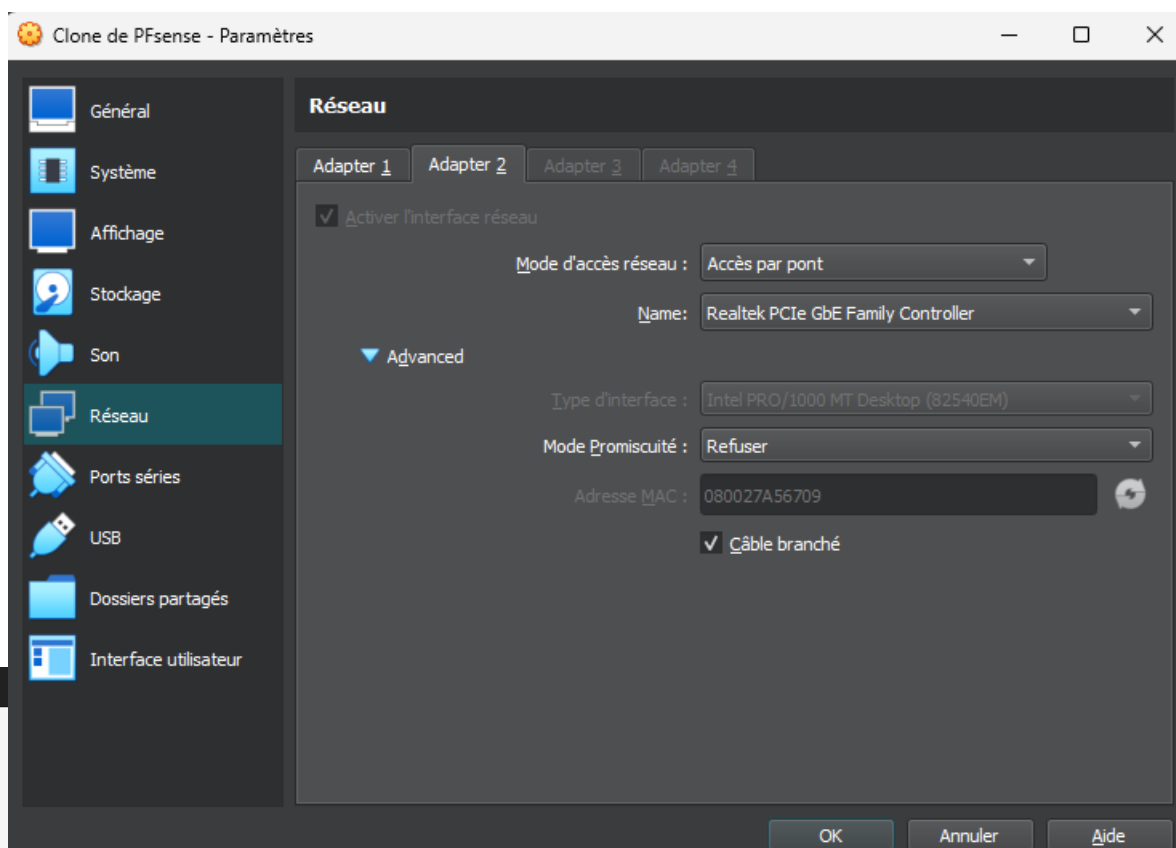
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

aller dans un moteur de recherche et écrire : <http://172.27.16.62>
en fonction de l'adresse ip donnée par la vm(elle peut changé)

pour ajouté le LAN

il faut aller dans les configuration de la vm et créer une deuxième interfaces réseaux



Système	ID de périphérique Netgate invité KVM : c052b21e1760760aee55
BIOS	Fournisseur : innotek GmbH Version : VirtualBox Date de sortie : vendredi 1er décembre 2006
Version	2.7.2-RELEASE (amd64) construit le mercredi 6 décembre 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT Impossible de vérifier les mises à jour
Type de processeur	Intel(R) Core(TM) i5-11400H de 11e génération à 2,70 GHz Crypto CPU AES-NI : Oui (inactif) Crypto QAT : Non
Chiffrement matériel	Inactif
PTI du noyau	Désactivé
Atténuation des SMD	Inactif
Temps de disponibilité	00 heure 04 minutes 19 secondes

RESSOURCES DE SUPPORT COMMUNAUTAIRE NETGATE ET pfSense

Si vous avez acheté votre dispositif de pare-feu de passerelle pfSense auprès de Netgate et choisi **le support communautaire** au point de vente ou installé pfSense sur votre propre matériel, vous avez accès à diverses ressources de support communautaire. Cela inclut la [BIBLIOTHÈQUE DE RESSOURCES NETGATE](#).

Vous pouvez également passer à un abonnement au support Netgate Global Technical Assistance Center (TAC). Nous sommes toujours actifs ! Notre équipe est composée de personnel 24 heures sur 24, 7 jours sur 7, 365 jours par an et s'engage à fournir une assistance mondiale de classe entreprise à un prix plus que compétitif par rapport à d'autres dans notre secteur.

- [Améliorez votre assistance](#)
- [FAQ de l'assistance mondiale Netgate](#)
- [Services professionnels Netgate](#)
- [Ressources de soutien communautaire](#)
- [Formation officielle pfSense par Netgate](#)
- [Visitez Netgate.com](#)

Si vous décidez d'acheter un abonnement Netgate Global TAC Support, vous

Maël Poisson

puis aller sur le navigateur est rentre sur le Pfsense

interfaces => Assignement => puis cliquez sur add situé a la place de Delete

Interface	Network port
WAN	em0 (08:00:27:dd:7f:1c) 
LAN	em1 (08:00:27:a5:67:09) 

 Save  Delete

Configuration du pare-feu

1. Refusé tout les protocoles

Firewall / Rules / Floating / 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.

Quick

☐ Apply the action immediately on match.

Set this option to apply this action to traffic that matches this rule immediately.

Interface

Any
WAN

Choose the interface(s) for this rule.

Direction

any

Address Family

IPv4+IPv6

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Résultat

Firewall / Rules / Floating

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN

Rules (Drag to Change Order)

	States	Interfaces	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✗	0/0 B	Any	IPv4+6 *	*	*	*	*	none			

↑ Add

↓ Add

Delete

Toggle

Save

Separator

i

2. Ajout des règles

Protocoles a autoriser

Protocole	Port(s)	Ports improbable	Autorisé/ Bloqué	Justification
HTTP	80	8075	Autorisé	Trafic Web standard
HTTPS	443	8443	Autorisé	Trafic Web sécurisé
SSH	22	22789	Autorisé	Connexions sécurisées à distance
FTP	21	2109	Autorisé	Transfert de fichiers
SMTP	25	587	Autorisé	Envoi de courriers électroniques
DNS	53	53991	Autorisé	Résolution de noms de domaine
ICMP	N/A	N/A	Autorisé	Autoriser le ping pour la gestion du réseau
MySQL	3306	3306	Autorisé	Système de gestion de bases de données MySQL
FTPS	990 (implicit)	990	Autorisé	Transfert de fichiers sécurisé (implicit FTPS)
DHCP	67(serveur)-68(client)	64 321(serveur)-64 322(client)	Autorisé	Attribution dynamique des adresses IP aux clients
IMAP	143	7777	Autorisé	accéder aux e-mails

Ex pour http et https

http

Destination

Destination

☐ Invert match

Any

▼

Destination Address

/

▼

Destination Port Range

HTTP (80)

▼

From

Custom

To

(other)

▼

8075

Custom

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

https

Destination

Destination

☐ Invert match

Any

▼

Destination Address

/

▼

Destination Port Range

HTTPS (443)

▼

From

Custom

To

(other)

▼

8443

Custom

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

Résultat

Pour le WAN

FloatingWANLAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐		0/11 KiB	*	Reserved Not assigned by IANA	*	*	*	*		Block bogon networks	
☐		0/0 B	IPv4 TCP	*	*	68 - 64322	*	none			
☐		0/0 B	IPv4 TCP	*	*	67 - 64321	*	none			
☐		0/0 B	IPv4 TCP	*	*	3306	*	none			
☐		0/0 B	IPv4 TCP	*	*	990	*	none			
☐		0/1 KiB	IPv4 TCP/UDP	*	*	143 - 7777	*	none			
☐		0/72 B	IPv4 ICMP any	*	*	*	*	none			
☐		0/0 B	IPv4 TCP	*	*	53 - 53991	*	none			
☐		0/0 B	IPv4 TCP	172.27.16.26/24	*	172.27.16.73/24	*	none			
☐		0/0 B	IPv4 TCP	*	*	22 - 22789	*	none			
☐		0/0 B	IPv4 TCP	*	*	443 - 8443	*	none			
☐		0/16 KiB	IPv4 TCP/UDP	*	*	80 - 8075	*	none			
☐		0/0 B	IPv4 TCP	*	*	25 - 587	*	none			
☐		0/1 KiB	IPv4 TCP/UDP	*	*	21 - 2109	*	none			

Add

Add

Delete

Toggle

Copy

Save

Separator

Résultat pour le LAN

FloatingWANLAN

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	✓ 0/3.71 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
☐	✓ 0/0 B	IPv4 TCP	*	*	*	7777	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	64322	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	64321	*	none			
☐	✓ 0/432 B	IPv4 ICMP any	*	*	*	*	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	990	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	3306	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	53991	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	587 (SUBMISSION)	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	2109	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	22789	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	8443	*	none			
☐	✓ 0/0 B	IPv4 TCP	*	*	*	8075	*	none			
☐	✓ 0/132 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
☐	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add

Add

Delete

Toggle

Copy

Save

Separator

3. ajout de règle adresse ip

Pour le WAN

Exemple

Disabled

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

Interface

WAN

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

Network

172.27.0.210

/

16

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**.

Interface

WAN

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

Network

172.27.0.211

/

16

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**.

Résultat

☐	✓	1/168 B	IPv4 TCP/UDP	172.27.0.219/16	*	*	*	*	none					
☐	✓	0/0 B	IPv4 TCP/UDP	172.27.0.218/16	*	*	*	*	none					
☐	✓	0/0 B	IPv4 TCP/UDP	172.27.0.217/16	*	*	*	*	none					
☐	✓	0/0 B	IPv4 TCP/UDP	172.27.0.216/16	*	*	*	*	none					
☐	✓	0/0 B	IPv4 TCP/UDP	172.27.0.215/16	*	*	*	*	none					
☐	✓	0/0 B	IPv4 TCP/UDP	172.27.0.214/16	*	*	*	*	none					
☐	✓	0/0 B	IPv4 TCP/UDP	172.27.0.213/16	*	*	*	*	none					
☐	✓	0/0 B	IPv4 TCP/UDP	172.27.0.212/16	*	*	*	*	none					
☐	✓	0/0 B	IPv4 TCP/UDP	172.27.0.211/16	*	*	*	*	none					
☐	✓	0/0 B	IPv4 TCP/UDP	172.27.0.210/16	*	*	*	*	none					

Maël Poisson

Pour le LAN

Exemple

Interface

LAN

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

Network

172.27.0.219

/

16

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**.

Interface

LAN

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

Network

172.27.0.218

/

16

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**.

Résultat

☐	✓ 1/84 B	IPv4 TCP/UDP	172.27.0.219/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕
☐	✓ 0/0 B	IPv4 TCP/UDP	172.27.0.218/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕
☐	✓ 0/0 B	IPv4 TCP/UDP	172.27.0.217/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕
☐	✓ 0/0 B	IPv4 TCP/UDP	172.27.0.216/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕
☐	✓ 0/0 B	IPv4 TCP/UDP	172.27.0.215/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕
☐	✓ 0/0 B	IPv4 TCP/UDP	172.27.0.214/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕
☐	✓ 0/0 B	IPv4 TCP/UDP	172.27.0.213/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕
☐	✓ 0/0 B	IPv4 TCP/UDP	172.27.0.212/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕
☐	✓ 0/0 B	IPv4 TCP/UDP	172.27.0.211/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕
☐	✓ 0/0 B	IPv4 TCP/UDP	172.27.0.210/16	*	*	*	*	none	📌 ✎ 📄 🕒 🗑 ✕