

PRÉSENTÉ PAR DRUELLE NICOLAS

TP-PFSENSE

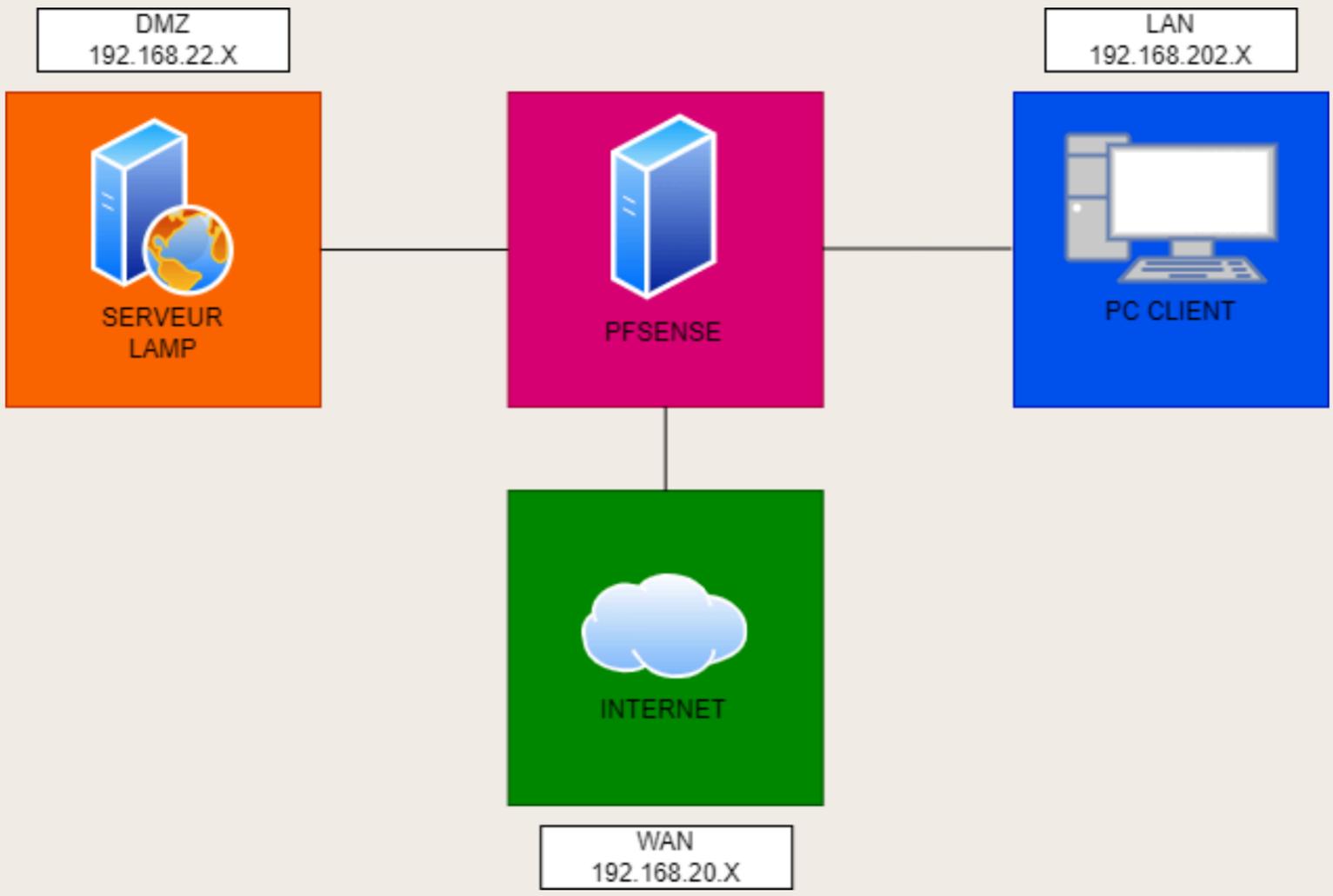
CAHIER DES CHARGES

- Mise en place du Pfsense
 - Configuration des interfaces (WAN, LAN, DMZ)
 - Configuration des règles
 - Configuration du portforward
- Autorisation du WAN et du LAN d'accès au serveur sur la DMZ

- Mise en place du serveur web
- Configuration du serveur dans la DMZ

- Réalisation des tests
 - Test LAN vers WAN et DMZ
 - Test WAN vers LAN et DMZ
 - Test DMZ vers LAN et WAN

TOPOLOGIE



ADRESSAGE IP

Nom	Adresse IP
PFSENSE (LAN)	192.168.202.20
PFSENSE (WAN)	192.168.20.86
PFSENSE (DMZ)	192.168.22.1
Serveur LAMP	192.168.22.2
Poste client LAN	192.168.202.11

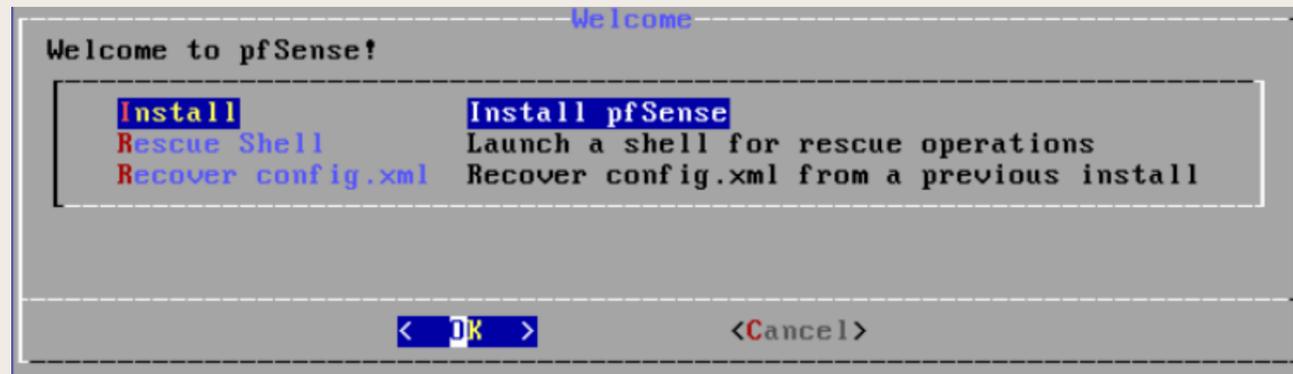
MISE EN PLACE DU PFSENSE

INSTALLATION PFSENSE

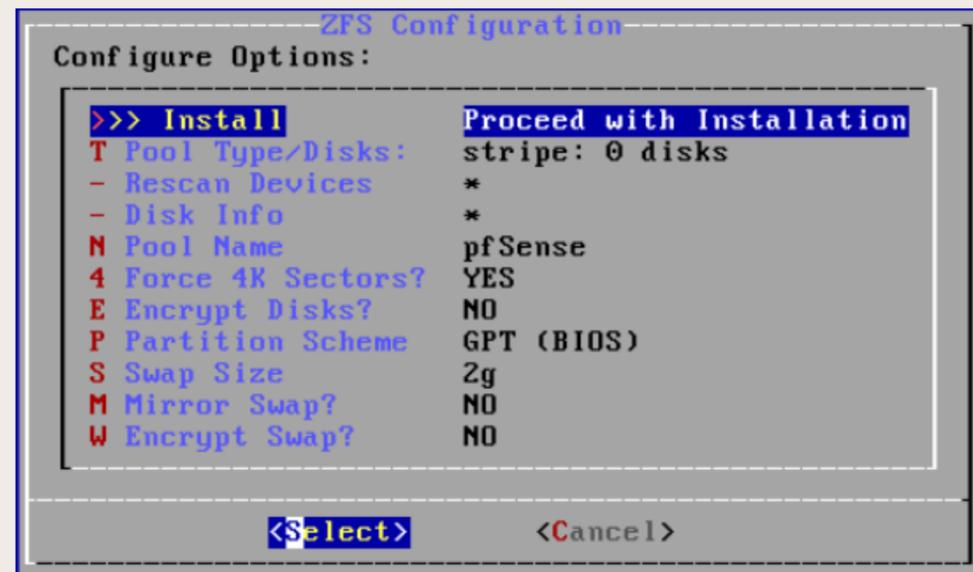
	Add	Remove	Edit	Disk Action	Revert	
Memory						2.00 GiB
Processors						1 (1 sockets, 1 cores) [x86-64-v2-AES]
BIOS						Default (SeaBIOS)
Display						Default
Machine						Default (i440fx)
SCSI Controller						VirtIO SCSI single
CD/DVD Drive (ide2)						local:iso/pfSense-CE-2.5.2-RELEASE-amd64.iso,media=cdrom,size=636498K
Hard Disk (scsi0)						local-lvm:vm-204-disk-0,iosthread=1,size=10G
Network Device (net0)						virtio=BC:24:11:54:4A:21,bridge=vibr0,firewall=1
Network Device (net1)						virtio=BC:24:11:71:D3:9C,bridge=vibr0,firewall=1
Network Device (net2)						virtio=BC:24:11:5D:DA:6D,bridge=vibr0,firewall=1

Dans un premier temps je vais installer PFSENSE sur le Proxmox en ajoutant 2 interfaces réseau supplémentaire

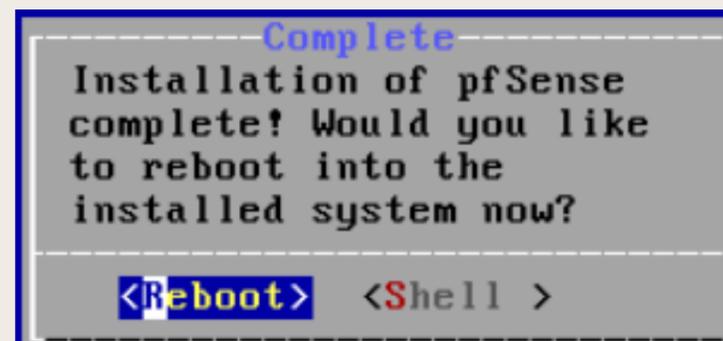
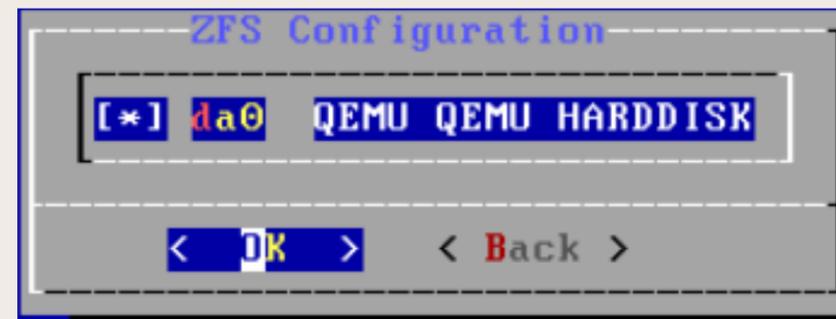
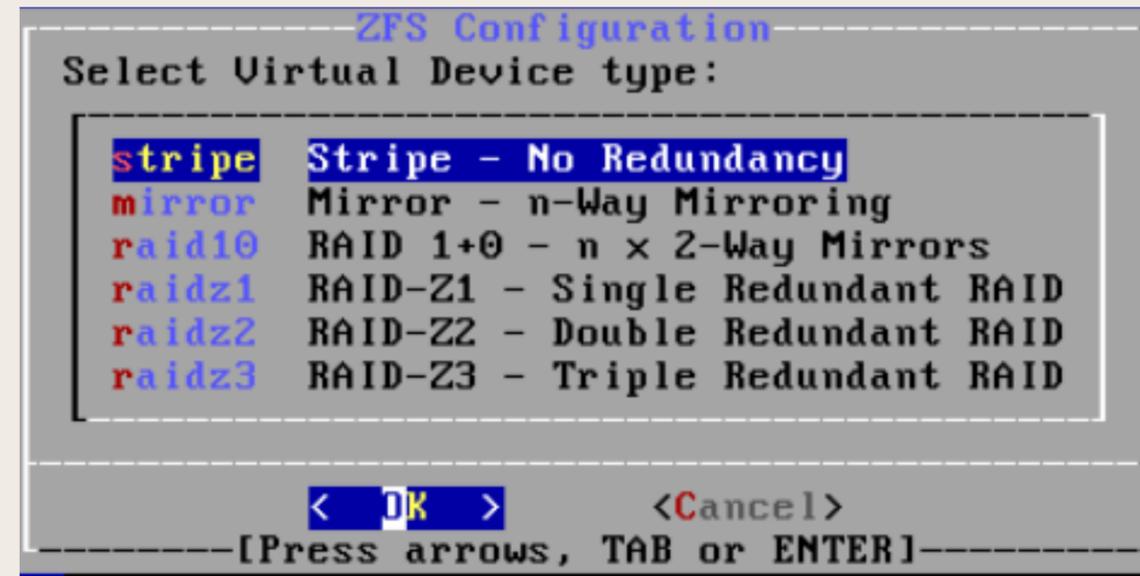
INSTALLATION PFSENSE



Une fois les interfaces ajoutées je démarre la VM et procède à l'installation



INSTALLATION PFSENSE



CONFIGURATION PFSENSE

```
(Local Database)

FreeBSD/amd64 (pfSensenicolas.home.arpa) (ttyv0)
KUM Guest - Netgate Device ID: 38df5bb6885c0c08f512
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSensenicolas ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.20.86/24
LAN (lan)      -> vtnet1      -> v4: 192.168.202.20/24
OPT1 (opt1)    -> vtnet2      -> v4: 192.168.22.1/24

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: 1

Valid interfaces are:

vtnet0  bc:24:11:54:4a:21  (up) VirtIO Networking Adapter
vtnet1  bc:24:11:71:d3:9c  (up) VirtIO Networking Adapter
vtnet2  bc:24:11:5d:da:6d  (up) VirtIO Networking Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [yn]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.
```

```
Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 vtnet2 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 vtnet2 a or nothing if finished): vtnet1

Optional interface 1 description found: OPT1
Enter the Optional 1 interface name or 'a' for auto-detection
(vtnet2 a or nothing if finished): vtnet2

The interfaces will be assigned as follows:

WAN -> vtnet0
LAN -> vtnet1
OPT1 -> vtnet2

Do you want to proceed [yn]? y
```

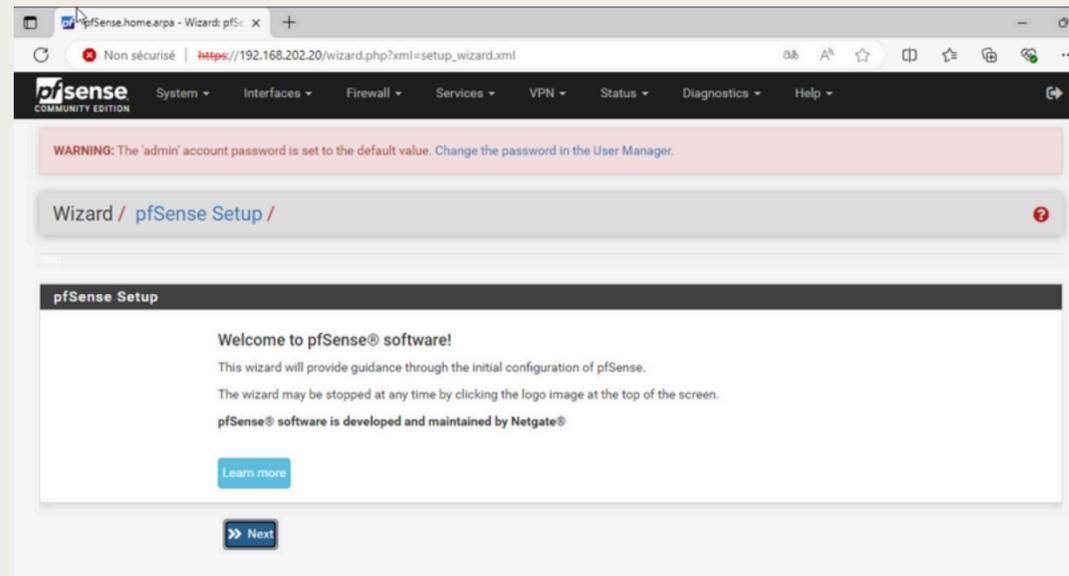
Une fois l'installation fini j'assigne le LAN, WAN et la DMZ à une interface créer précédemment avec l'option "1"

CONFIGURATION PFSENSE

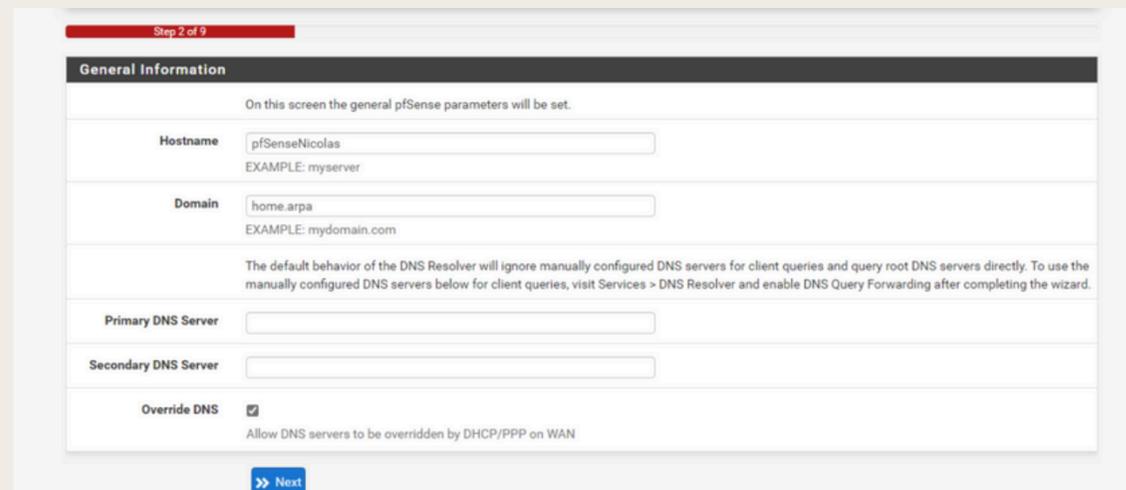
```
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.20.86/24
LAN (lan)      -> vtnet1      -> v4: 192.168.202.20/24
OPT1 (opt1)    -> vtnet2      -> v4: 192.168.22.1/24
```

Ensuite avec l'option "2" je donne une ip en suivant le tableau d'adressage en page 4 sur chacune des interfaces

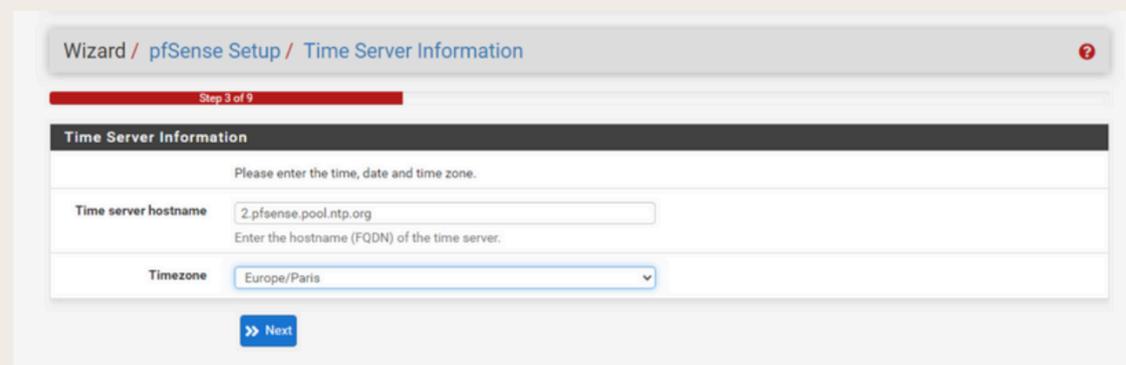
CONFIGURATION PFSENSE



Une fois les adresses ip mise sur les interfaces avec le poste client LAN je me connecte au site du PFSENSE afin de commencer la configuration



Dans un premier temps je renseigne les configurations de base comme le nom de l'hôte et la plage horaire



CONFIGURATION PFSENSE

The screenshot shows the PPTP configuration interface. At the top, there is a dropdown menu for 'pptplocalsubnet' set to '32'. Below it is a text input field for 'PPTP Remote IP Address'. The 'PPTP Dial on demand' section has an unchecked checkbox for 'Enable Dial-On-Demand mode' and a descriptive paragraph. The 'PPTP Idle timeout' section has a text input field and a descriptive paragraph. There are two sections for blocking networks: 'RFC1918 Networks' with an unchecked checkbox for 'Block RFC1918 Private Networks', and 'Block bogon networks' with an unchecked checkbox for 'Block bogon networks'. Both sections have descriptive paragraphs. At the bottom, there is a blue button with a right-pointing arrow and the text 'Next'.

Ensuite on passe la configuration des interface.

Sur l'interface WAN on décoche "block rfc1918 private networks" afin d'avoir une ip privée sur celle-ci

The screenshot shows the 'Configure LAN Interface' step in the pfSense setup wizard. The breadcrumb trail at the top reads 'Wizard / pfSense Setup / Configure LAN Interface'. A progress bar indicates 'Step 5 of 9'. The main heading is 'Configure LAN Interface'. Below it, a message states: 'On this screen the Local Area Network information will be configured.' There are two input fields: 'LAN IP Address' with the value '192.168.202.20' and a subtext 'Type dhcp if this interface uses DHCP to obtain its IP address.', and 'Subnet Mask' with the value '24'. At the bottom, there is a blue button with a right-pointing arrow and the text 'Next'.

Après l'interface WAN, c'est au tour de l'interface LAN on vérifie donc si l'ip mise précédemment est bien la bonne

CONFIGURATION PFSENSE

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password:

Admin Password AGAIN:

[Next](#)

Enfin la dernière configuration est le changement du mot de passe par défaut car il ne faut jamais laissé le mot de passe de base sur un serveur

Une fois cela fait je peux accéder à la page d'accueil du serveur

pfSense COMMUNITY EDITION

System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

Status / Dashboard

System Information

Name	pfSensenicolas.home.arpa
User	admin@192.168.202.11 (Local Database)
System	KVM Guest Netgate Device ID: 38df5bb6885c0c08f512
Version	2.5.2-RELEASE (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE Obtaining update status
CPU Type	QEMU Virtual CPU version 2.5+ AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	23 Hours 29 Minutes 12 Seconds
Current date/time	Sat Sep 28 17:43:48 CEST 2024
DNS server(s)	• 127.0.0.1 • 185.156.80.7

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

Active Windows

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to

EXPLICATION RÈGLE

ACTION :

PASS (AUTORISER), BLOCK (BLOQUER SANS RETOUR), OU REJECT (BLOQUER AVEC NOTIFICATION).

INTERFACE :

SUR QUELLE INTERFACE LA RÈGLE S'APPLIQUE : LAN, WAN, DMZ, ETC.

PROTOCOL :

TYPE DE PROTOCOLE FILTRÉ : TCP, UDP, ICMP (PING), OU ANY (TOUS LES PROTOCOLES).

SOURCE :

ORIGINE DU TRAFIC : ANY (TOUT), SINGLE HOST OR ALIAS (ADRESSE IP UNIQUE), OU NETWORK (UN SOUS-RÉSEAU).

DESTINATION :

DESTINATION DU TRAFIC, AVEC LES MÊMES OPTIONS QUE POUR LA SOURCE.

PORTS :

SOURCE PORT ET DESTINATION PORT : PLAGES DE PORTS SPÉCIFIQUES À FILTRER (EX. : 80 POUR HTTP, 443 POUR HTTPS).

DESCRIPTION :

CHAMP POUR NOMMER LA RÈGLE POUR MIEUX L'IDENTIFIER.

CONFIGURATION RÈGLE LAN

Edit Firewall Rule

Action ▼
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.

Associated filter rule This is associated with a NAT rule.
Editing the interface, protocol, source, or destination of associated filter rules is not permitted.
[View the NAT rule](#)

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

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

Protocol ▼
Choose which IP protocol this rule should match.

Source

Source Invert match ▼ / ▼

 **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 ▼ / ▼

Destination Port Range ▼ ▼
From Custom To Custom

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
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.

CONFIGURATION RÈGLE WAN

Edit Firewall Rule

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

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

Protocol
 Choose which IP protocol this rule should match.

Source

Source Invert match /

[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 /

Destination Port Range
 From Custom To Custom
 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
 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](#)

QU'EST CE QUE LE PORTFORWARD

Le “port forwarding” (redirection de port) est une technique permettant de rediriger le trafic réseau destiné à une adresse IP publique et un port spécifique vers une adresse IP privée et un port sur un réseau interne (comme un LAN ou une DMZ).

Cela permet d'accéder à des services internes (serveurs web) depuis l'extérieur du réseau, tout en conservant la sécurité offerte par le pare-feu et le NAT (Network Address Translation).

CONFIGURATION PORT FORWARD LAN

Interface	LAN	Choose which interface this rule applies to. In most cases "WAN" is specified.	
Address Family	IPv4	Select the Internet Protocol version this rule applies to.	
Protocol	TCP	Choose which protocol this rule should match. In most cases "TCP" is specified.	
Source	Display Advanced		
Destination	<input type="checkbox"/> Invert match.	LAN address	Address/mask
Destination port range	HTTP	HTTP	
Redirect target IP	Single host	192.168.22.2	

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Pour la configuration du port forward sur le lan on redirige l'adresse LAN vers l'ip du serveur ici "192.168.22.2" sur le port 80 (HTTP)

Redirect target port	HTTP	
Description		
No XMLRPC Sync	<input type="checkbox"/> Do not automatically sync to other CARP members	
NAT reflection	Use system default	
Filter rule association	Rule NAT	

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

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

This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

[View the filter rule](#)

CONFIGURATION PORTFORWARD WAN

Edit Redirect Entry

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination Invert match. WAN address /
Type Address/mask

Destination port range HTTP From port Custom HTTP To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Single host 192.168.22.2

Redirect target port HTTP Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.

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

No XMLRPC Sync Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Rule NAT
[View the filter rule](#)

Pour la configuration du port forward sur le lan on redirige l'adresse WAN vers l'ip du serveur ici "192.168.22.2" sur le port 80 (HTTP)

TEST

TEST PING LAN

```
C:\Users\Windows>ping 192.168.20.86

Envoi d'une requête 'Ping' 192.168.20.86 avec 32 octets de données :
Réponse de 192.168.20.86 : octets=32 temps<1ms TTL=64
Réponse de 192.168.20.86 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.20.86 : octets=32 temps<1ms TTL=64
Réponse de 192.168.20.86 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.20.86:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 2ms, Moyenne = 0ms
```

Ping vers WAN

```
C:\Users\Windows>ping 192.168.22.2

Envoi d'une requête 'Ping' 192.168.22.2 avec 32 octets de données :
Réponse de 192.168.22.2 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.22.2 : octets=32 temps=2 ms TTL=63
Réponse de 192.168.22.2 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.22.2 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 192.168.22.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

Ping vers DMZ

TEST PING WAN

```
C:\Users\Nico>ping 192.168.202.11  
Envoi d'une requête 'Ping' 192.168.202.11 avec 32 octets de données :  
Délai d'attente de la demande dépassé.  
Délai d'attente de la demande dépassé.  
Délai d'attente de la demande dépassé.  
Délai d'attente de la demande dépassé.
```

Ping vers LAN

```
C:\Users\Nico>ping 192.168.22.2  
Envoi d'une requête 'Ping' 192.168.22.2 avec 32 octets de données :  
Délai d'attente de la demande dépassé.  
  
Statistiques Ping pour 192.168.22.2:  
Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Ping vers DMZ

TEST PING DMZ

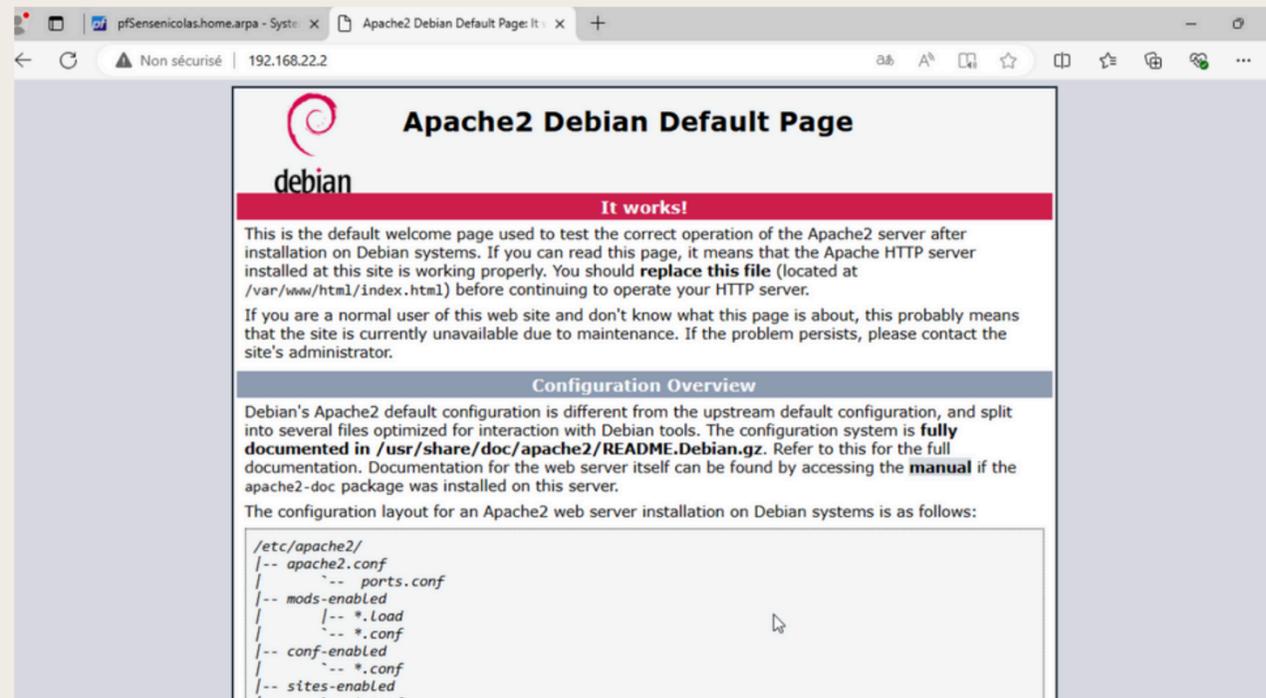
```
root@debian:~# ping 192.168.202.20
PING 192.168.202.20 (192.168.202.20) 56(84) bytes of data.
^C
--- 192.168.202.20 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5103ms
```

Ping vers LAN

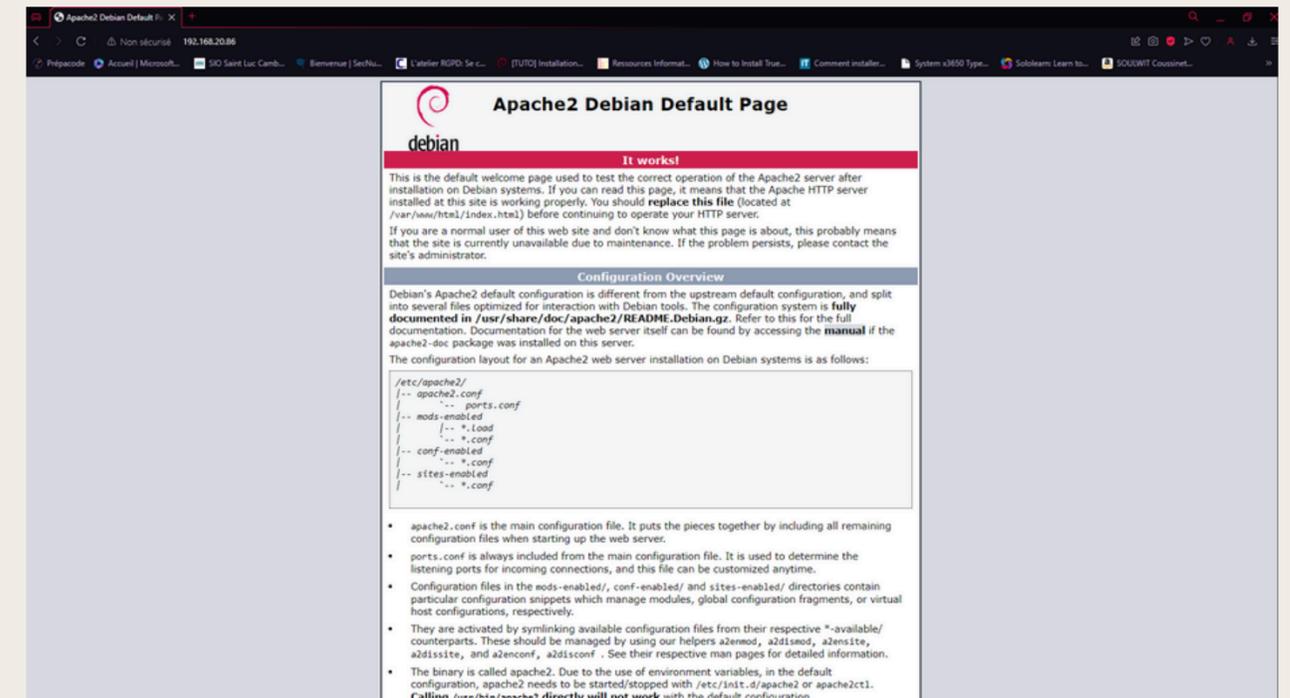
```
root@debian:~# ping 192.168.20.86
PING 192.168.20.86 (192.168.20.86) 56(84) bytes of data.
^C
--- 192.168.20.86 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3072ms
```

Ping vers WAN

TEST CONNECTION SITE



Connection
avec le LAN



Connection
avec le WAN