

Créer une machine virtuelle

Create: Virtual Machine ⊗

General OS System Disks CPU Memory Network **Confirm**

Key ↑	Value
cores	2
cpu	x86-64-v2-AES
ide2	local:iso/pfSense-CE-2.7.2-RELEASE-amd64.iso,media=cdrom
memory	8192
name	pfSense
net0	virtio,bridge=vmbr0,firewall=1
nodename	pve
numa	0
ostype	l26
scsi0	local-lvm:32,iouthread=on
scsihw	virtio-scsi-single
sockets	3
vmid	104

Start after created

Advanced **Back** **Finish**

Démarrer la VM

Virtual Machine 104 (pfSense) on node 'pve' No Tags ▶ Start ⏻ Shutdown >_ Console More Help

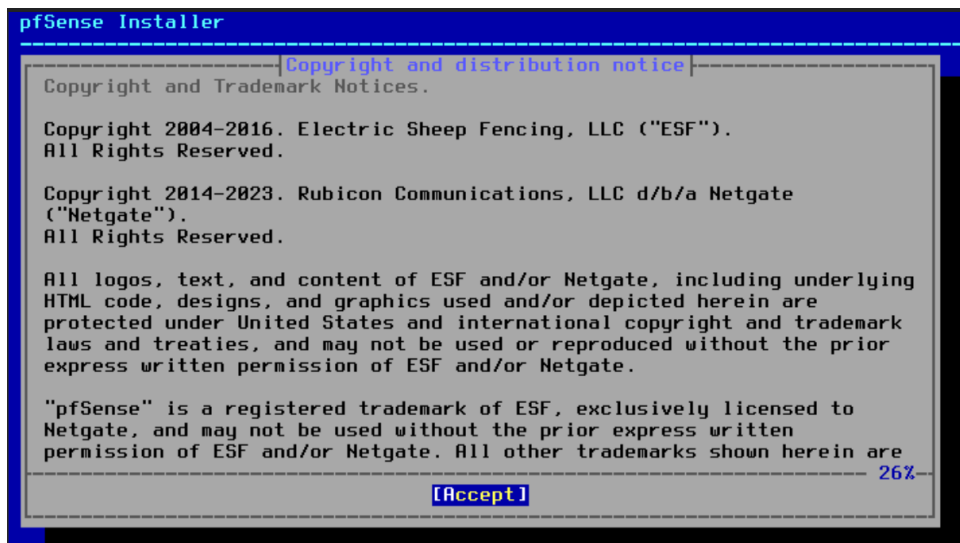
- Summary
- >_ Console
- Hardware
- Cloud-Init
- Options
- Task History
- Monitor
- Backup
- Replication
- Snapshots
- Firewall
- Permissions

VNC

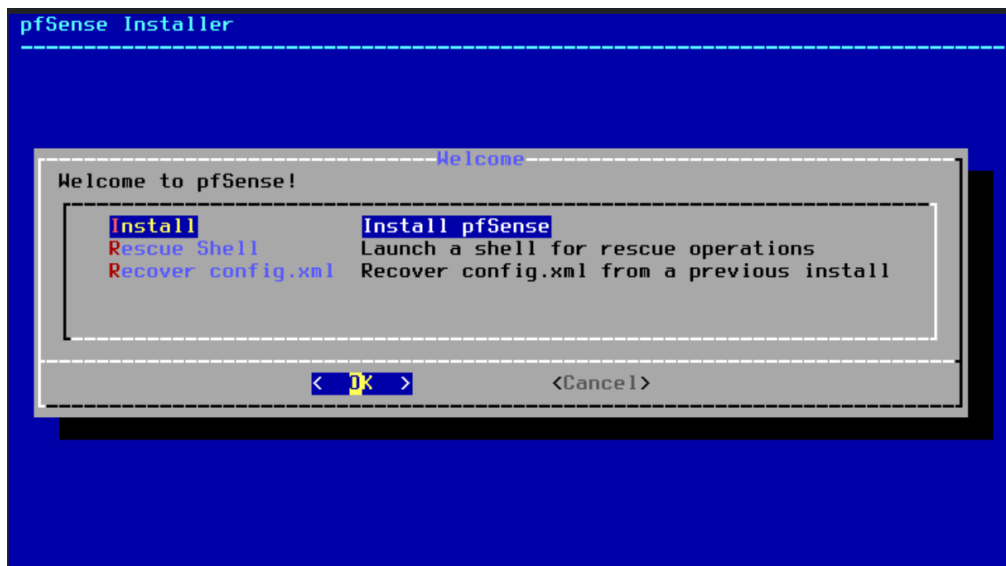
Guest not running

Start Now

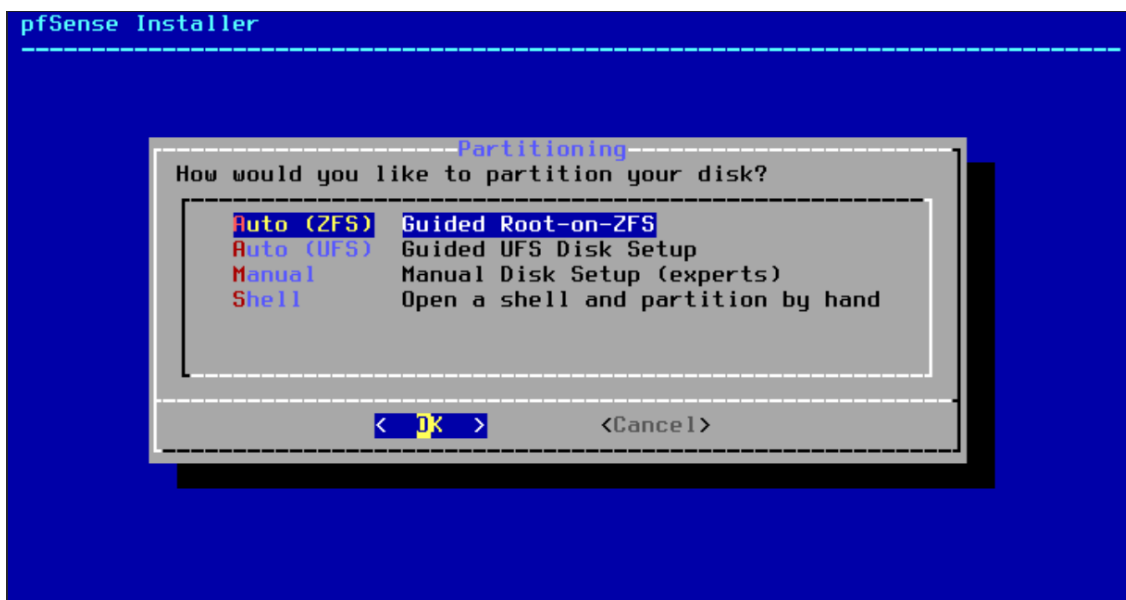
Sélectionner Accept et Entrer



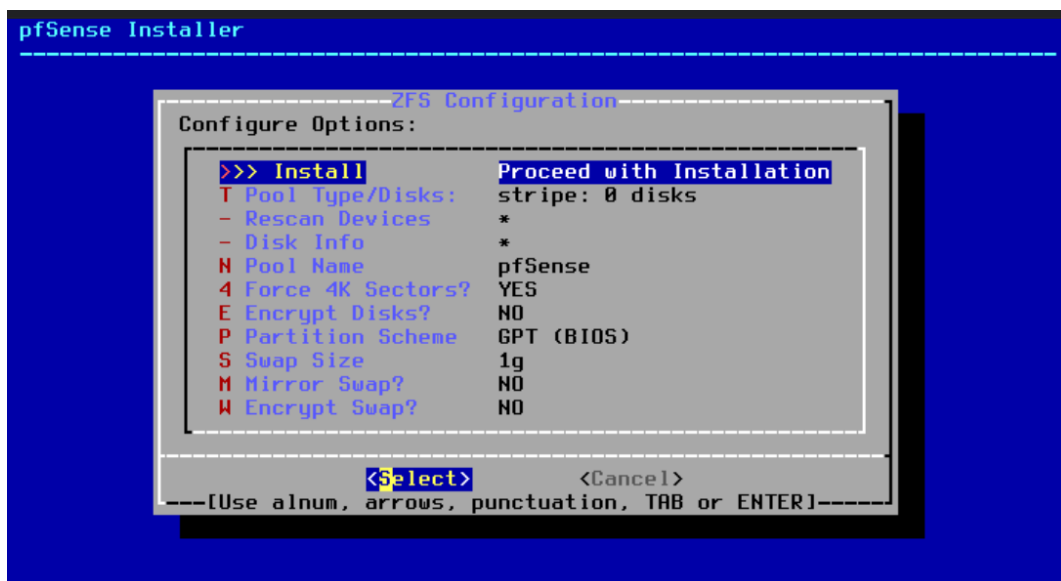
Sélectionner Install et OK



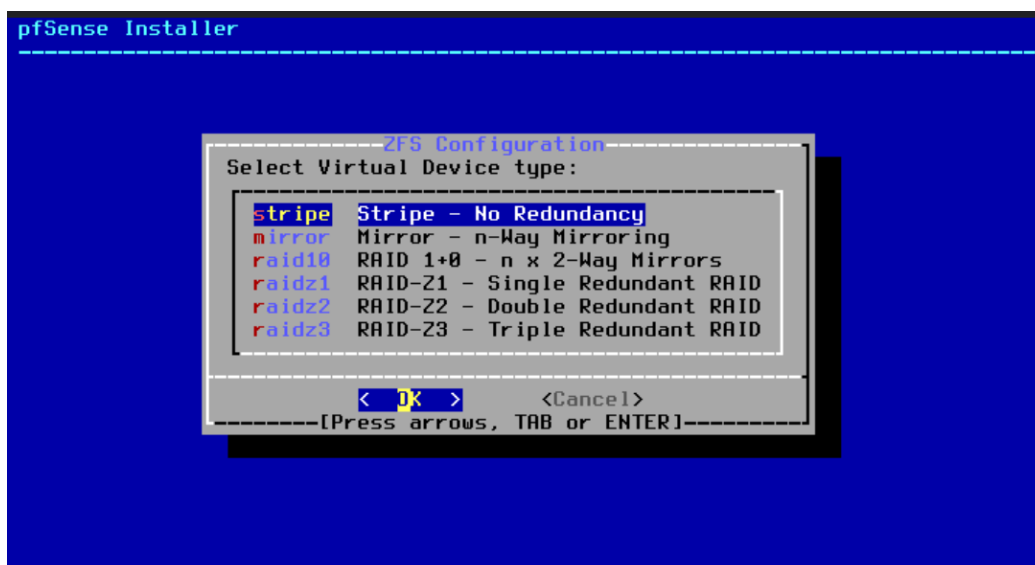
Sélectionner Auto (ZFS) et OK



Sélectionner Install et Select



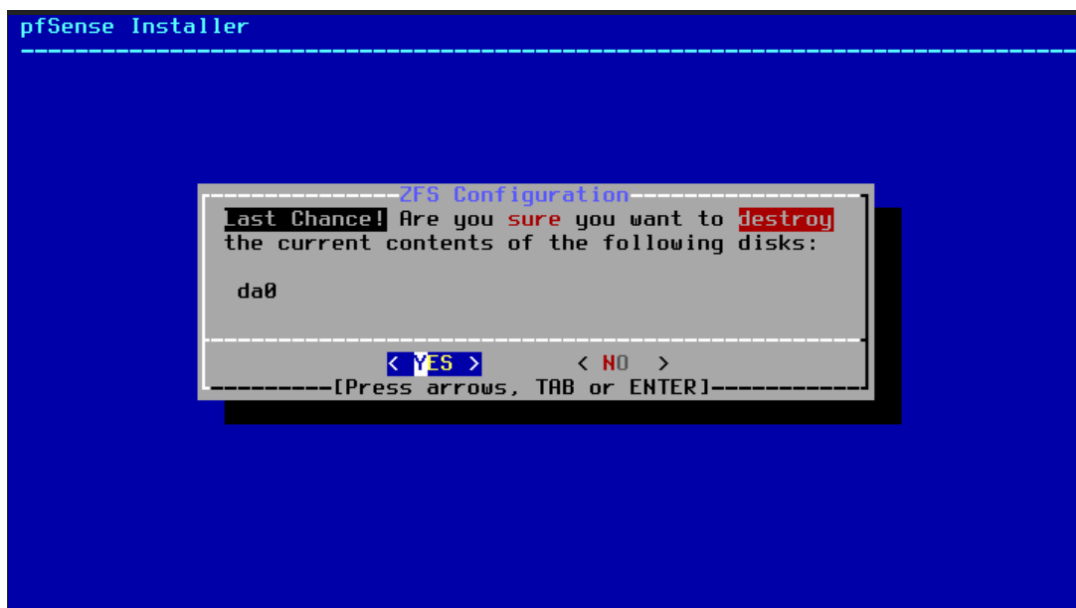
Sélectionner **Stripe** et OK



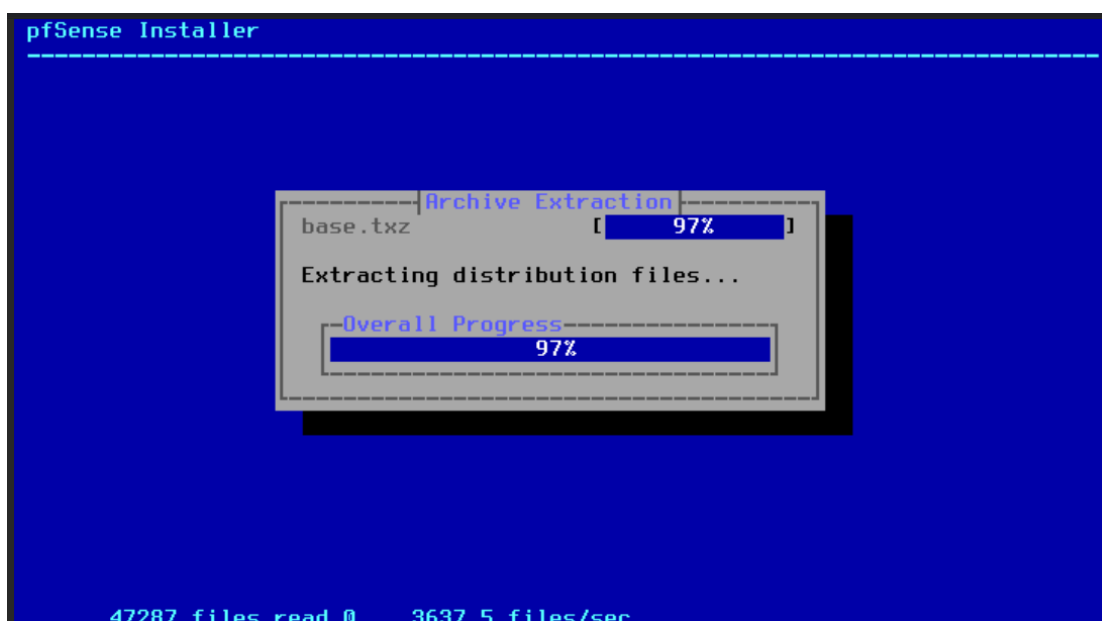
Appuyer sur Espace pour cocher la case et OK



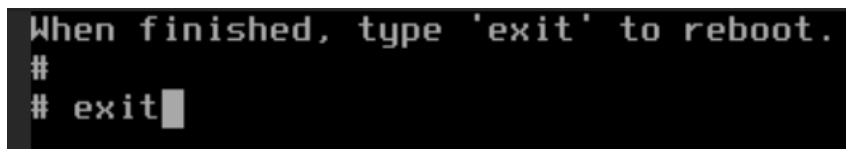
Sélectionner YES et entrer



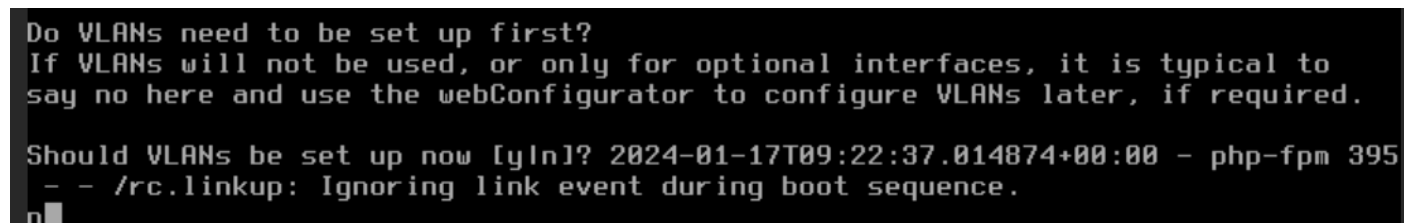
Attendre



Ecrire exit puis entrer



Taper « n » puis entrer



Taper le nom de l'interface (ici vtnet0)

```
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 or a): vtnet0
```

Appuyer sur entrer

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

Taper « y » puis entrer

```
The interfaces will be assigned as follows:

WAN -> vtnet0

Do you want to proceed [y/n]? y
```

Taper 2 puis entrer

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

WAN (wan) -> vtnet0 -> v4: 10.74.3.230/22

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:
```

Répondre aux questions comme ci-dessous

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 10.74.3.230

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 WAN IPv4 subnet bit count (1 to 32):
> 22

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

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

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

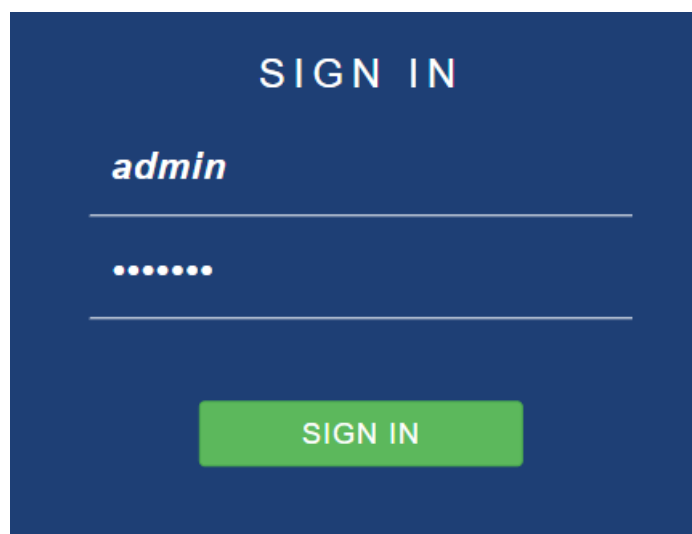
Do you want to enable the DHCP server on WAN? (y/n) n
```

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

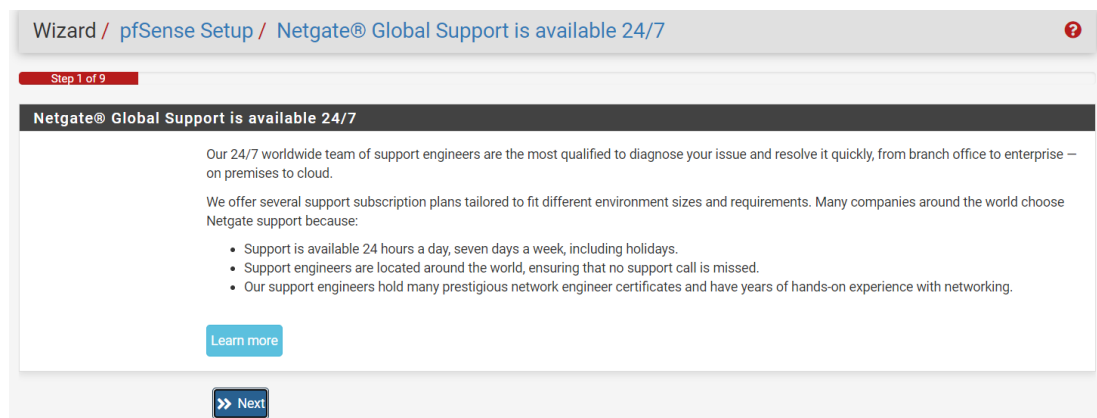
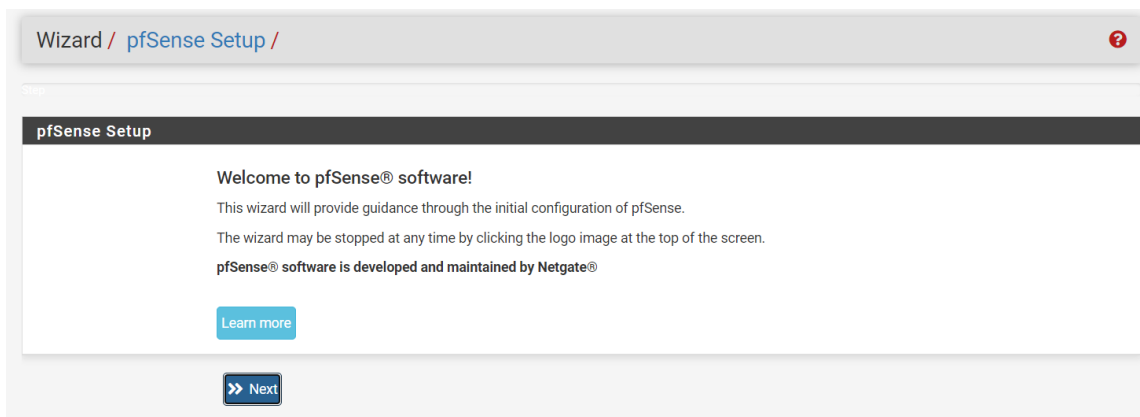
The IPv4 WAN address has been set to 10.74.3.230/22
You can now access the webConfigurator by opening the following URL in your web
browser:
      https://10.74.3.230/

Press <ENTER> to continue. █
```

Aller sur <https://10.74.3.230/> (l'ip du pfsense que l'on vient de mettre en place)



Se connecter avec « admin » « pfsense »



Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

[Next](#)

Wizard / pfSense Setup / Time Server Information ?

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

[Next](#)

Wizard / pfSense Setup / Configure WAN Interface ?

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

General configuration

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address

Subnet Mask

Upstream Gateway

DHCP client configuration

DHCP Hostname

The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

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](#)

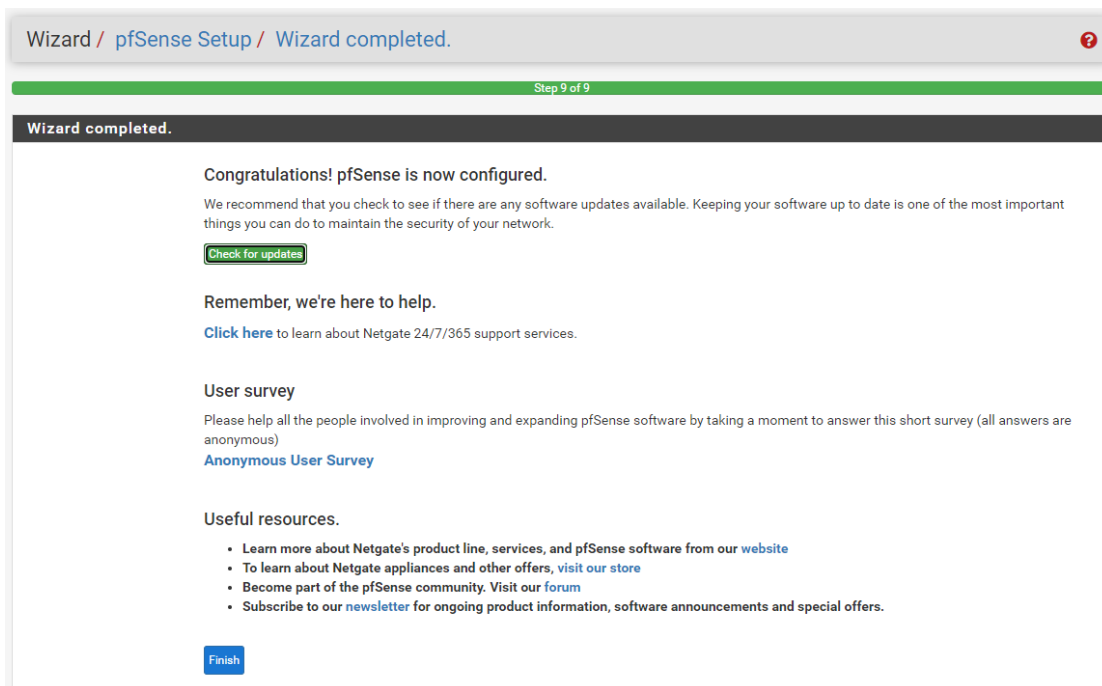
Wizard / pfSense Setup / Reload configuration ?

Step 7 of 9

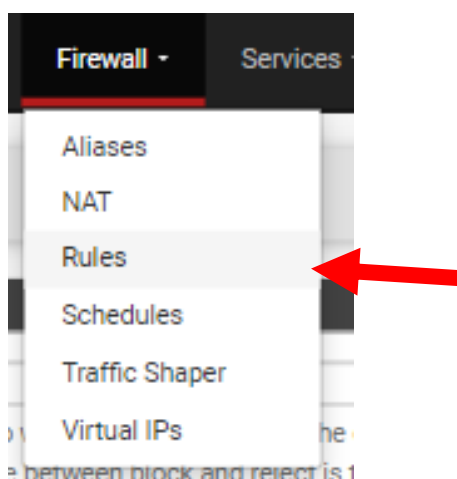
Reload configuration

Click 'Reload' to reload pfSense with new changes.

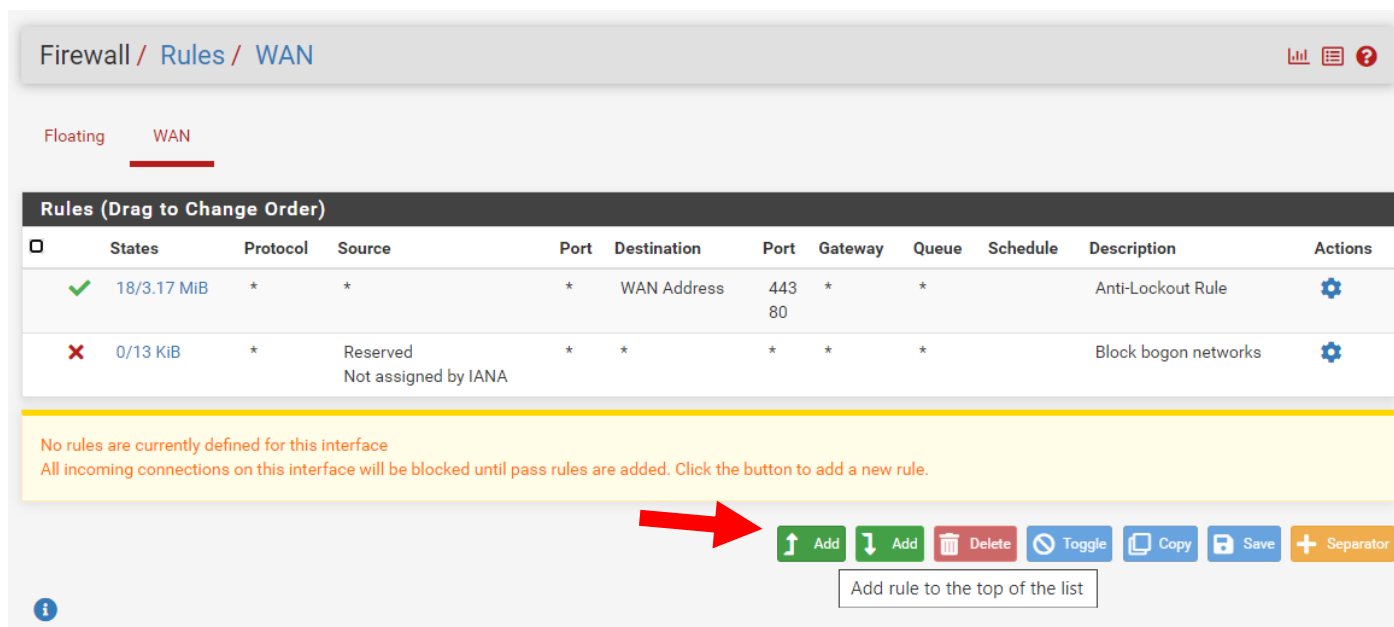
[» Reload](#)



Aller dans Firewall puis Rules



Appuyer sur ADD



Laisser les paramètres par défauts pour ouvrir tout les ports

Firewall / Rules / Edit ☰ 📊 📄 ?

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 ▼ / ▼

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

Appliquer les changements

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

Aller sur Proxmox, dans la vm pfsense

Hardware > Add > Network Device

Virtual Machine 104 (pfSense) on node 'pve'

Start Shutdown Console More Help

Summary Console Hardware Cloud-Init Options Task History Monitor Backup Replication Snapshots Firewall Permissions

Add Remove Edit Disk Action Revert

Hard Disk	8.00 GiB
CD/DVD Drive	6 (3 sockets, 2 cores) [x86-64-v2-AES]
Network Device	Default (SeaBIOS)
EFI Disk	Default
TPM State	Default (i440fx)
USB Device	VirtIO SCSI single
PCI Device	2)
Serial Port	local:iso/pfSense-CE-2.7.2-RELEASE-amd64.iso,media=cdrrom,size=854172K
CloudInit Drive	local-lvm:vm-104-disk-0,iotthread=1,size=32G
Audio Device	et0) virtio=96:28:98:88:C9:9E,bridge=vibr0,firewall=1
VirtIO RNG	

Sélectionner la deuxième interface réseau

Add: Network Device

Bridge: vibr1 Model: VirtIO (paravirtualized)

Bridge	Active	Comment
vibr0	Yes	
vibr1	Yes	

Firewall: Rate limit (MB/s): unlimited

Disconnect: MTU: 1500 (1 = bridge MTU) Multiqueue:

Help Advanced Add

Retourner sur pfSense puis aller dans Interfaces > Assignments

Interfaces Firewalls

Assignments

WAN

Appuyer sur Add

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	vtnet0 (96:28:98:88:c9:9e)
Available network ports:	vtnet1 (aa:2f:0e:ab:c1:32) <input type="button" value="Add"/>

Save

Appuyer sur LAN

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	vtnet0 (96:28:98:88:c9:9e)
LAN	vtnet1 (aa:2f:0e:ab:c1:32)

Save Delete

Activer l'interface et mettre une IPv4

Interfaces / LAN (vtnet1)

The LAN 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.

Apply Changes

General Configuration

Enable Enable interface

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

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

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

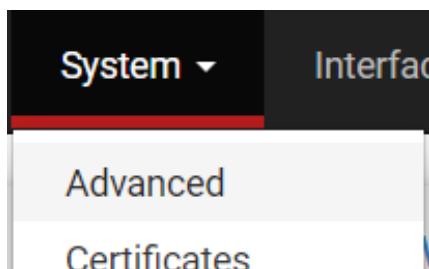
Static IPv4 Configuration

IPv4 Address 192.168.10.1 / 24

IPv4 Upstream gateway None [+ 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.

Aller dans System > Advanced



Aller dans Networking

Cocher Kea DHCP

Décocher Allow IPv6

Puis sauvegarder en bas

DHCP Options

Server Backend Kea DHCP ISC DHCP (Deprecated) Ignore Deprecation Warning

ISC DHCP has reached end-of-life and will be removed from a future version of pfSense. Kea DHCP is the newer, modern DHCP distribution from ISC that includes the most-requested features.

RADVD Debug Log all radvd log levelsDHCP6 Debug Start DHCP6 client in debug modeDo not allow PD/Address release dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sentDHCP6 DUID

A DHCPv6 Unique Identifier (DUID) is used by the firewall when requesting an IPv6 address.

By default, the firewall automatically creates a dynamic DUID-LLT which is not saved in the firewall configuration. To ensure that the same DUID is retained by the firewall at all times, enter a DUID in this section. The new DUID will take effect after a reboot or when the WAN interface(s) are reconfigured by the firewall.

If the firewall is configured to use a RAM disk for /var, the best practice is to store a DUID here; otherwise, the DUID will change on each reboot.

Raw DUID [Copy DUID](#)

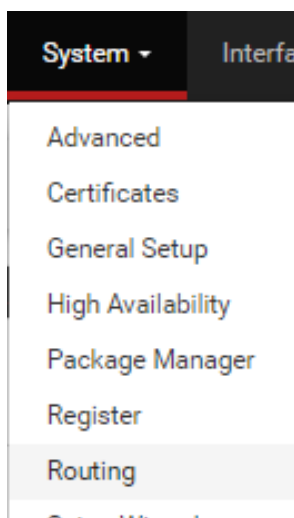
You may use the Copy DUID button to copy the system detected DUID shown in the placeholder.

IPv6 Options

Allow IPv6 All IPv6 traffic will be blocked by the firewall unless this box is checked

NOTE: This does not disable any IPv6 features on the firewall, it only blocks traffic.

Aller dans System > Routing



Ajouter une nouvelle Gateway

Sélectionner l'interface LAN

System / Routing / Gateways / Edit

Edit Gateway

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

Interface
Choose which interface this gateway applies to.

Address Family
Choose the Internet Protocol this gateway uses.

Name
Gateway name

Gateway
Gateway IP address

Gateway Monitoring Disable Gateway Monitoring
This will consider this gateway as always being up.

Gateway Action Disable Gateway Monitoring Action
No action will be taken on gateway events. The gateway is always considered up.

Monitor IP
Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).

Static route Do not add static route for gateway monitor IP address via the chosen interface
By default the firewall adds static routes for gateway monitor IP addresses to ensure traffic to the monitor IP address leaves via the correct interface. Enabling this checkbox overrides that behavior.

Force state Mark Gateway as Down
This will force this gateway to be considered down.

State Killing on Gateway Failure
Controls the state killing behavior when this specific gateway goes down. Killing states for specific down gateways only affects states created by policy routing rules and reply-to. Has no effect if gateway monitoring or its action are disabled or if the gateway is forced down. May not have any effect on dynamic gateways during a link loss event.

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

[Display Advanced](#)

[Save](#)

Sauvegarder les modifications

Gateways Static Routes Gateway Groups

Gateways

	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WANGW		WAN	10.74.0.1	10.74.0.1	WAN Gateway	
<input type="checkbox"/>	<input checked="" type="checkbox"/> LANGW		LAN	192.168.10.1	192.168.10.1	LAN Gateway	

[Save](#) [+ Add](#)

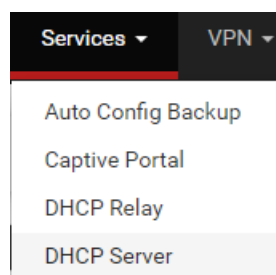
Default gateway

Default gateway IPv4
Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6
Select a gateway or failover gateway group to use as the default gateway.

[Save](#)

Aller dans Services > DHCP Server



Sélectionner LAN en haut

(Le DNS peut être laissé par défaut mais ici nous avons un serveur DNS)

A screenshot of the PfSense DHCP Server configuration page for the LAN interface. The breadcrumb trail at the top reads 'Services / DHCP Server / LAN'. The 'LAN' tab is selected. The page is divided into several sections: 'General DHCP Options', 'Primary Address Pool', and 'Server Options'.
General DHCP Options:

- DHCP Backend:** Kea DHCP
- Enable:** Enable DHCP server on LAN interface
- Deny Unknown Clients:** Allow all clients (dropdown menu). A detailed explanation follows: '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 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:** 192.168.10.0/24
- Subnet Range:** 192.168.10.1 - 192.168.10.254
- Address Pool Range:** From 192.168.10.100 To 192.168.10.200. A note states: 'The specified range for this pool must not be within the range configured on any other address pool for this interface.'
- Additional Pools:** A green button labeled '+ Add Address Pool'. A note states: 'If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.'

Server Options:

- WINS Servers:** WINS Server 1, WINS Server 2
- DNS Servers:** 192.168.10.10 (highlighted with a blue border)