

Installation PfSense

Fait en entreprise et dans le cadre de l'épreuve E4 du BTS SIO 2022-2024

[Télécharger en PDF](#)

Sommaire

- [Pour Commencer](#)
 - [Prérequis](#)
 - [Installation](#)
 - [Formatage de la clé USB](#)
 - [Système](#)
 - [Configuration Interne](#)
 - [Configuration GUI](#)
 - [Configuration Interfaces](#)
 - [Configuration VLANs](#)
 - [Configuration DHCP](#)
 - [Configuration Firewall](#)
 - [Configuration Applications](#)
 - [Suricata](#)
 - [SSH](#)

Pour Commencer

Mon entreprise, KNCO, a pris la décision de passer du routeur de notre FAI à un routeur PfSense, afin de pouvoir mieux gérer la sécurisation du réseau et débrider la vitesse de connexion dans les locaux, bridée par la maigre puissance du routeur original, causant des problèmes lors d'interventions à distance mais aussi lors de connexions sur notre serveur SAP, se faisant en Remote Desktop (RDP)

Il a également été demandé de gérer le réseau interne et le réseau du WiFi invité séparément, pour cela nous créeront deux VLAN, un interne et un pour le WiFi invité

Le besoin principal est donc de pouvoir gérer la sécurisation du réseau et de se débarrasser de l'équipement de base de notre fournisseur internet

Prérequis

- [Rufus](#), [Balena Etcher](#) ou tout autre logiciel du genre
- Clé/Stockage USB de 4Go minimum
- ISO de [PfSense](#)
- Un serveur 2 coeurs et 2Go minimum **avec ici, trois cartes réseaux ou plus**

Installation

Formatage de la clé USB

1. Téléchargez l'ISO de PfSense (ici 2.7.0, AMD64, DVD Image)

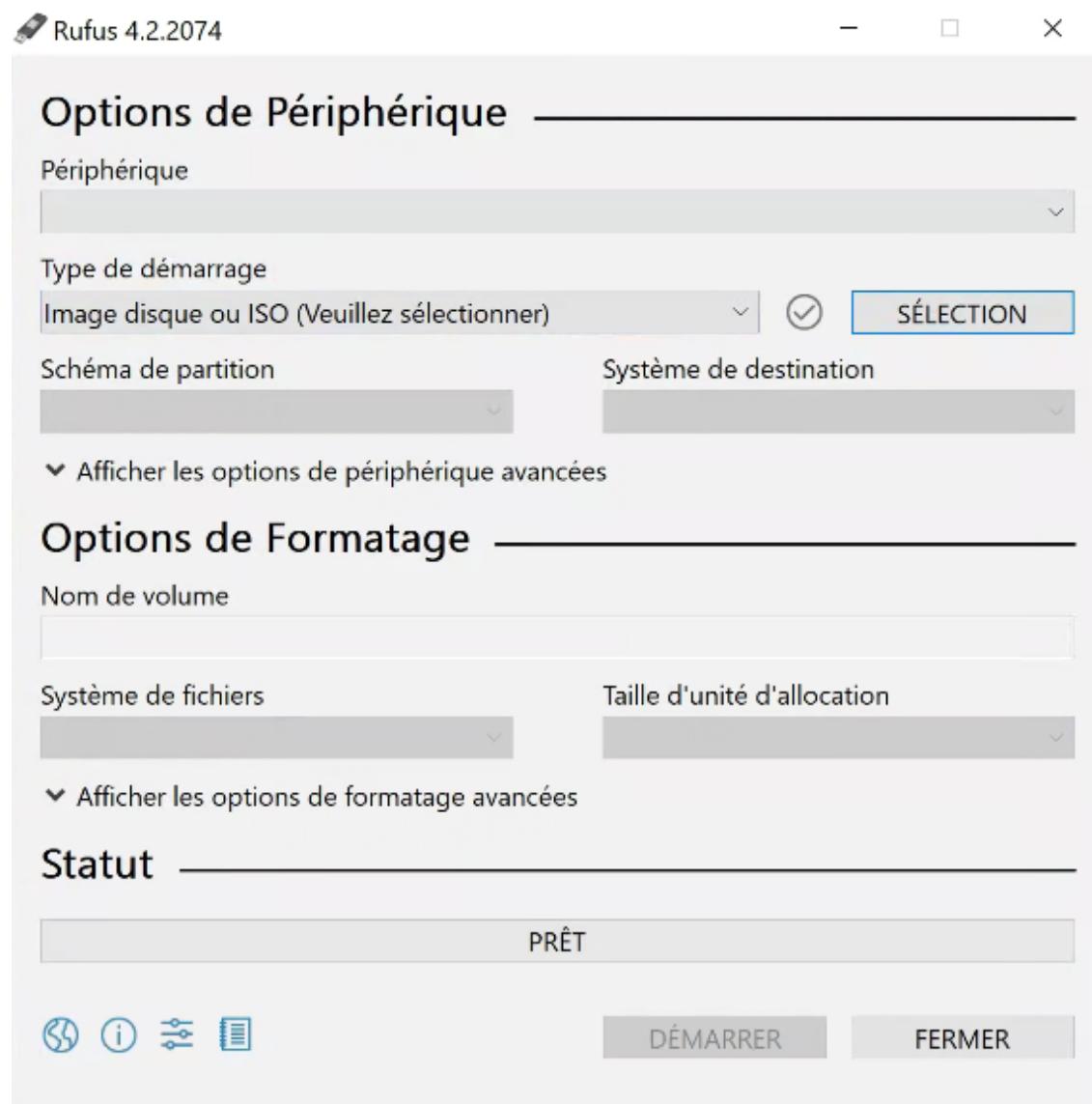
The screenshot shows the pfSense download page. At the top, there are social media links and navigation links for Get Started, Cloud, Products, Services, Support, Training, Community, and Download. Below that, the pfSense logo is displayed with the text "Latest Stable Version (Community Edition)". A note states that this is the most recent stable release and the recommended version for all installations. It links to Upgrade Guides and Installation Guides. For pre-configured systems, it links to pfSense® firewall appliances from Netgate. There are two tabs at the top: "RELEASE NOTES" and "SOURCE CODE". The "RELEASE NOTES" tab is selected. On the left, a form allows selecting the "Version" (2.7.0), "Architecture" (AMD64 (64-bit)), "Installer" (DVD Image (ISO) Installer), and "Mirror" (Austin, TX USA). A large blue "DOWNLOAD" button is prominently displayed. To the right, there is a section titled "Subscribe To The Netgate Newsletter" with fields for email address and newsletter interests. A note about accepting the newsletter terms is present. Below the newsletter section, there is a "Supported by" logo for Netgate.

2. Téléchargez Rufus

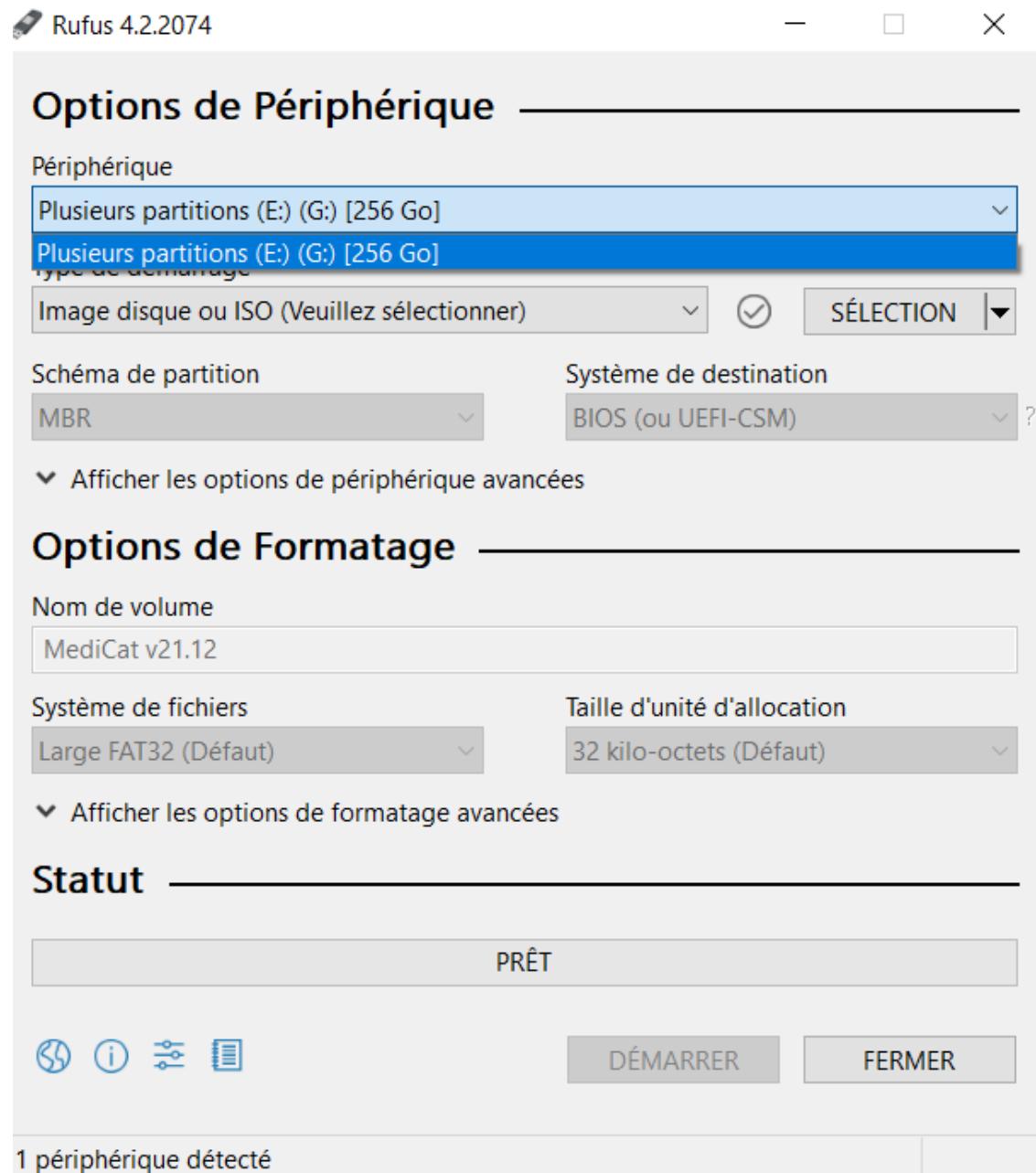
The screenshot shows the GitHub releases page for Rufus 4.3. The page header includes navigation links for Code, Issues (12), Pull requests (1), Actions, Projects (1), Wiki, Security, and Insights. The main content area shows the "Rufus 4.3" release, which was released last month by pbatard. It has 3 commits to master since this release and is v4.3. The commit hash is 020e0b7. The release notes list several improvements and fixes, including support for symbolic link preservation, enforcement of NTFS for Linux Mint's LMDE, and expert mode for Windows installations. Below the release notes is a "Assets" section with two files: "rufus-4.3.exe" and "rufus-4.3.exe.sig". Both files are 1.37 MB and were uploaded last month.

3. Branchez la clé USB sur le PC

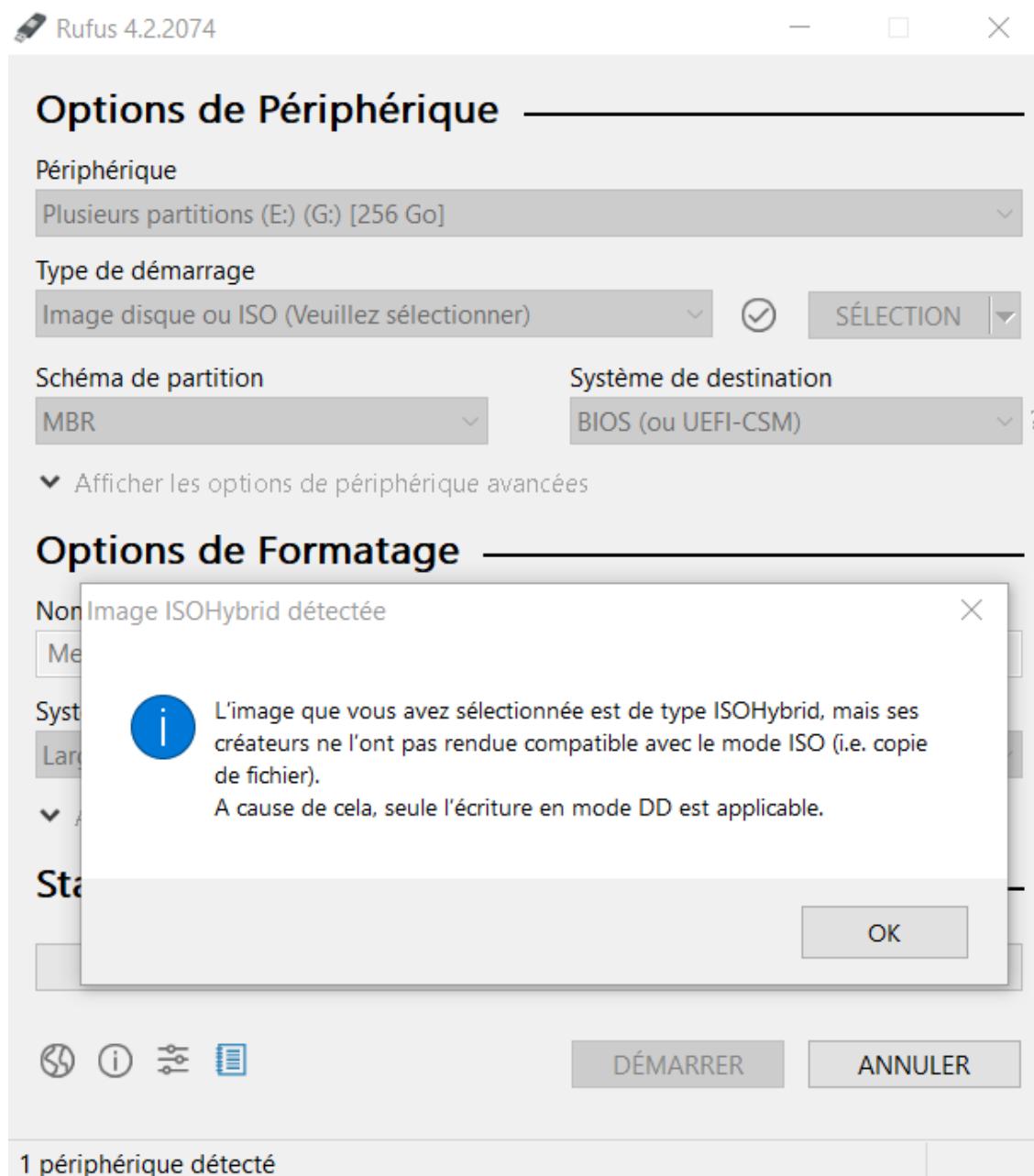
4. Ouvrir Rufus

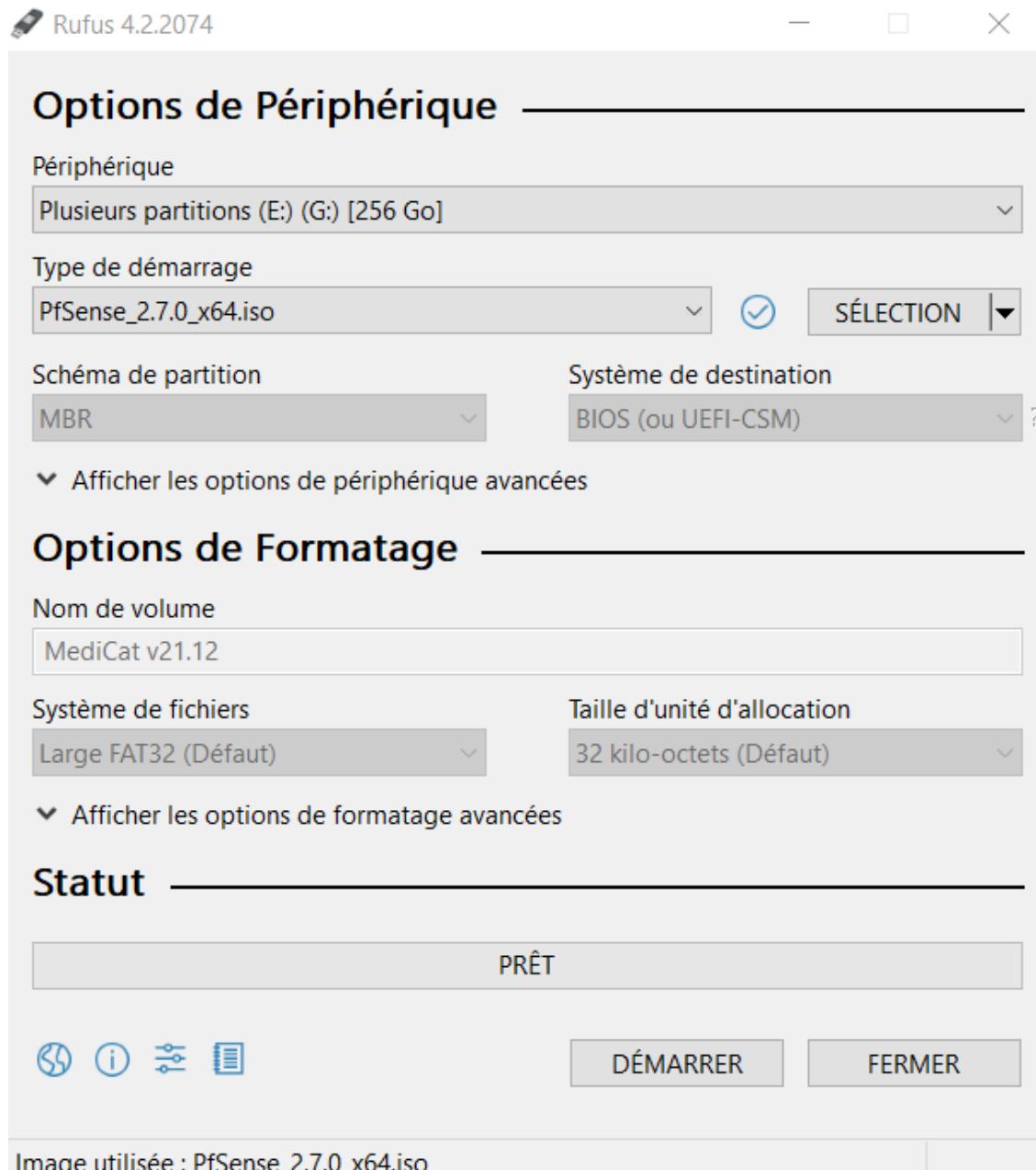


5. Sélectionnez la clé USB



6. Sélectionnez l'ISO de PfSense, continuez si vous avez une erreur "ISOHybrid"





7. Lancez le formatage

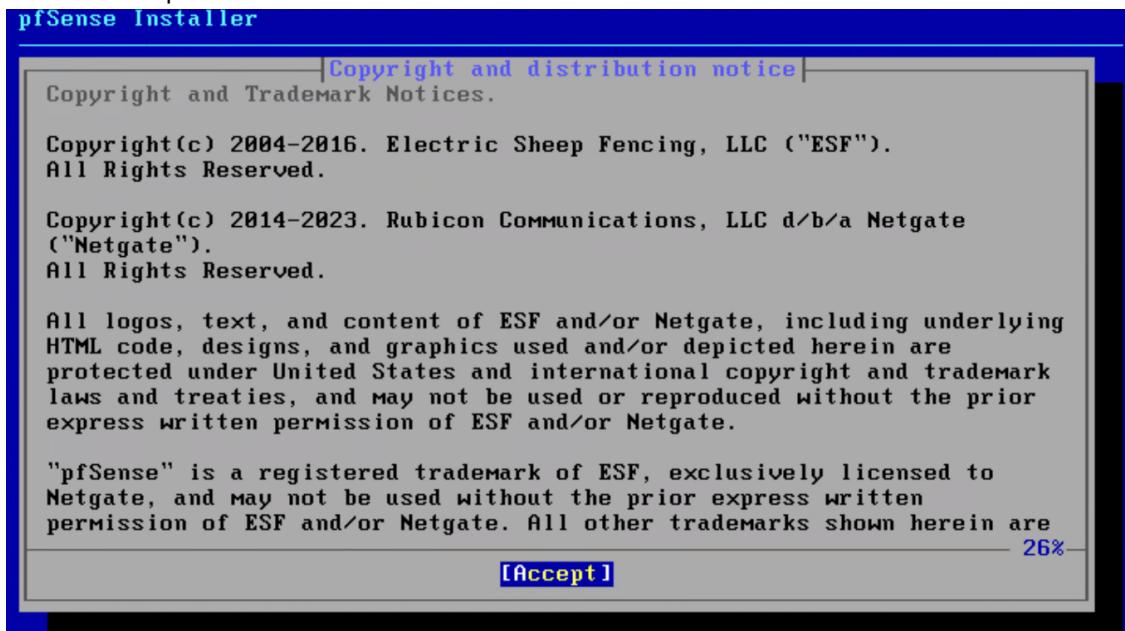
Système

1. Branchez la clé USB sur le serveur
2. Démarrez le serveur
3. Appuyez sur F11 pour accéder au boot menu

4. Sélectionnez la clé USB



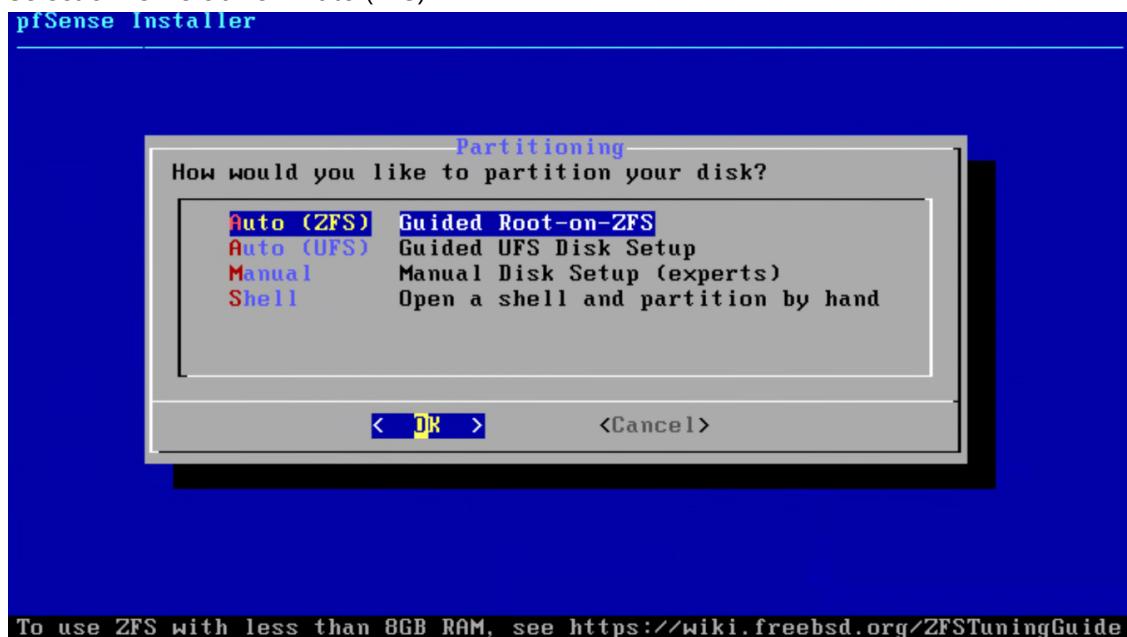
5. Faites entrer pour démarrer l'installation



6. Sélectionnez "Install"

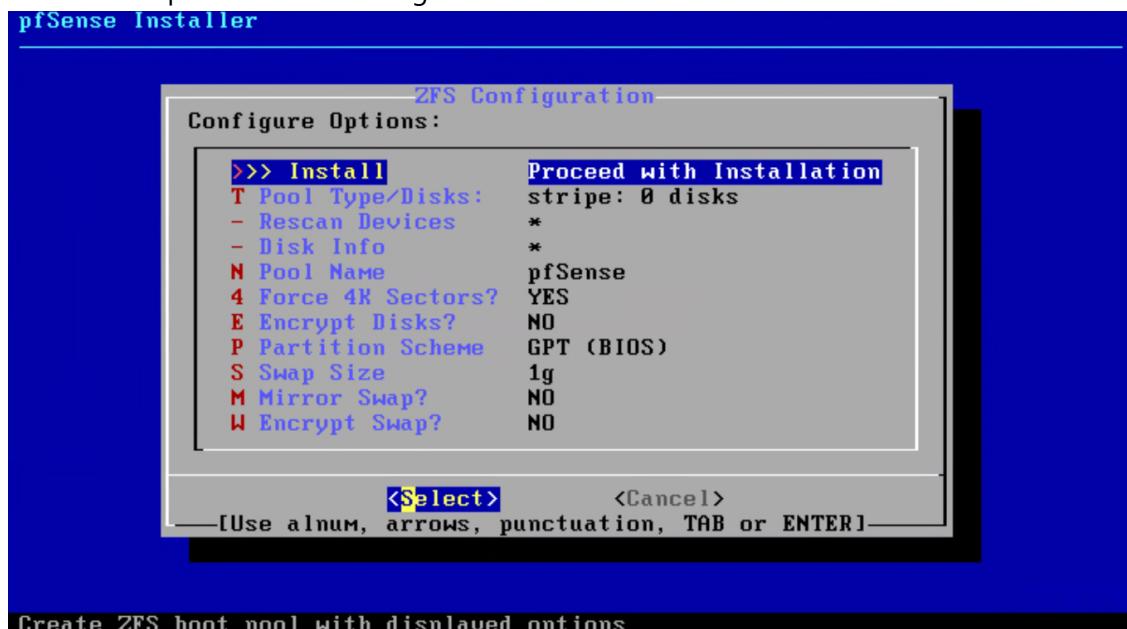


7. Sélectionnez le clavier "Auto (ZFS)"



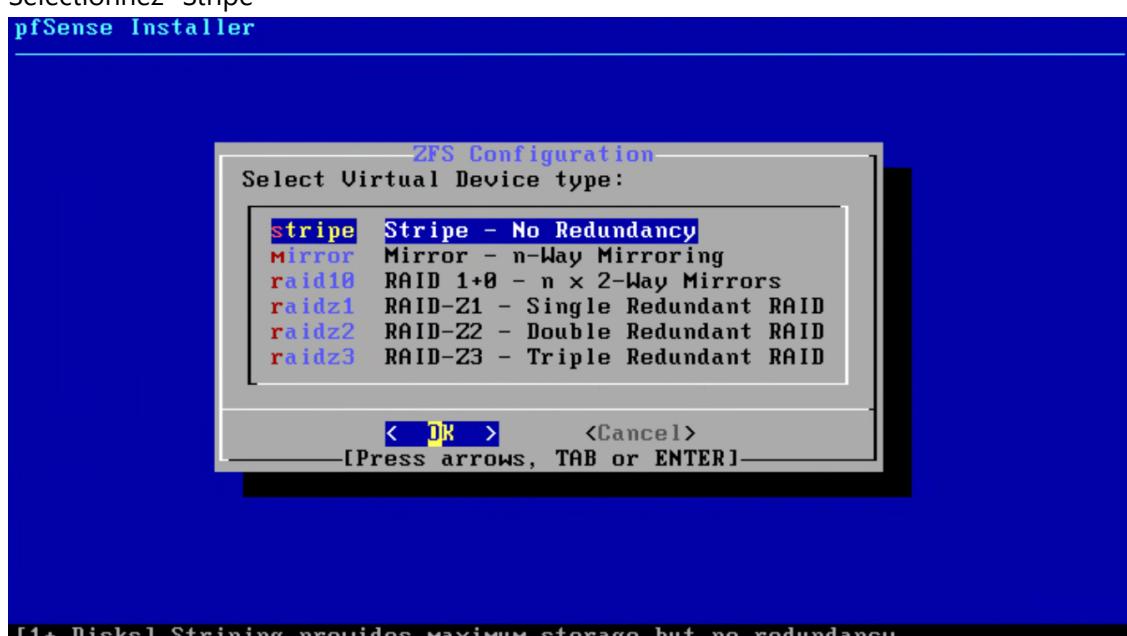
To use ZFS with less than 8GB RAM, see <https://wiki.freebsd.org/ZFSTuningGuide>

8. Faites entrer pour valider la configuration



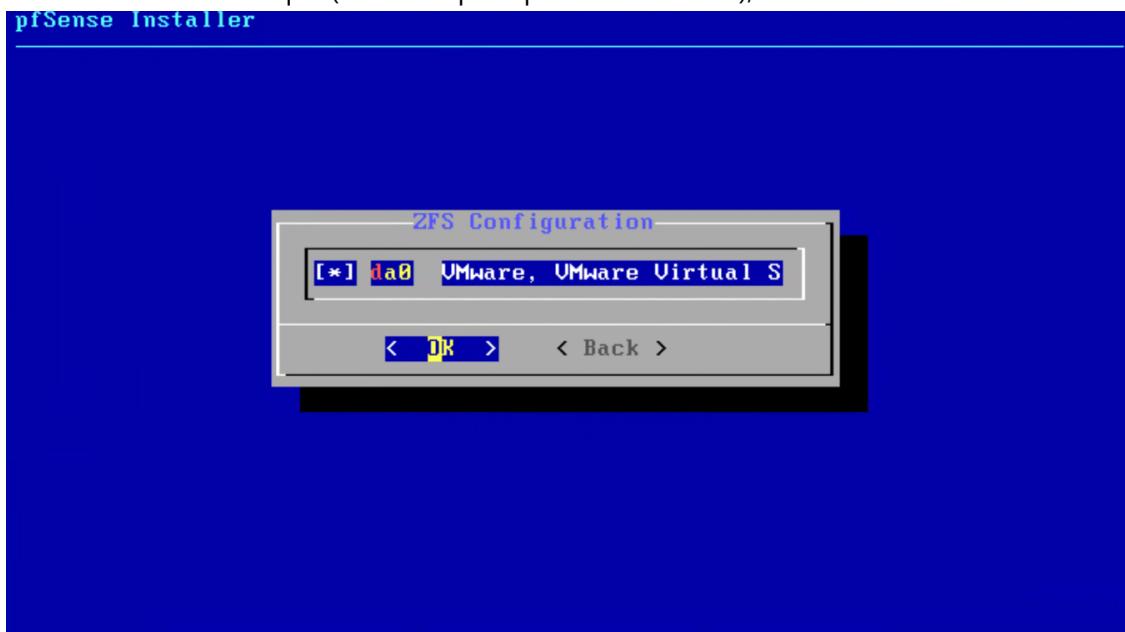
Create ZFS boot pool with displayed options

9. Sélectionnez "Stripe"

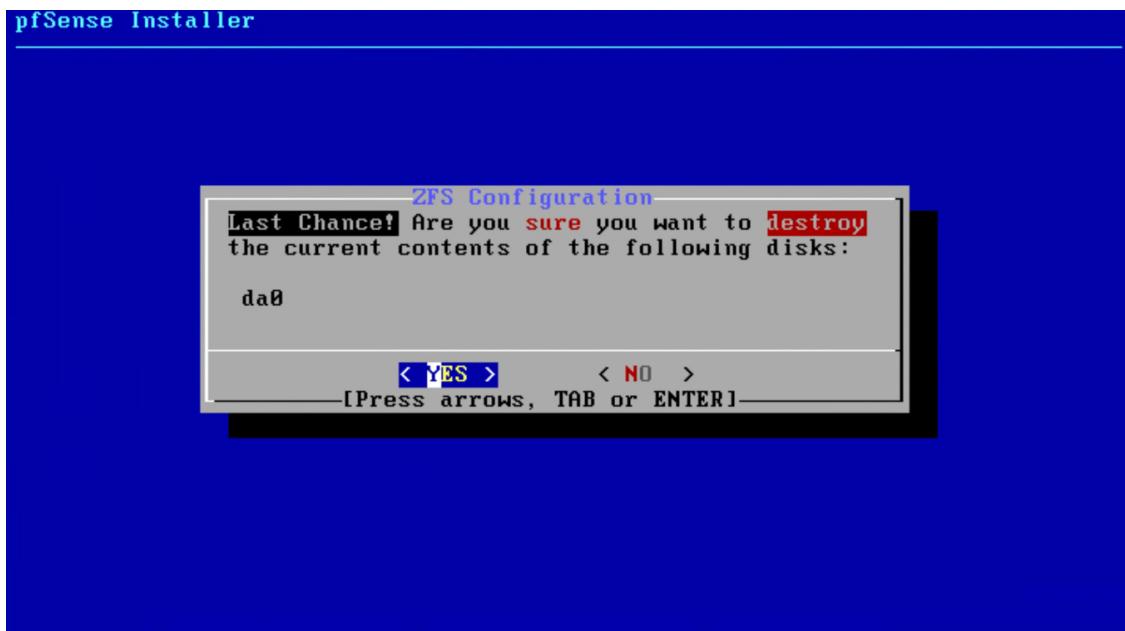


[1+ Disks] Stripping provides maximum storage but no redundancy

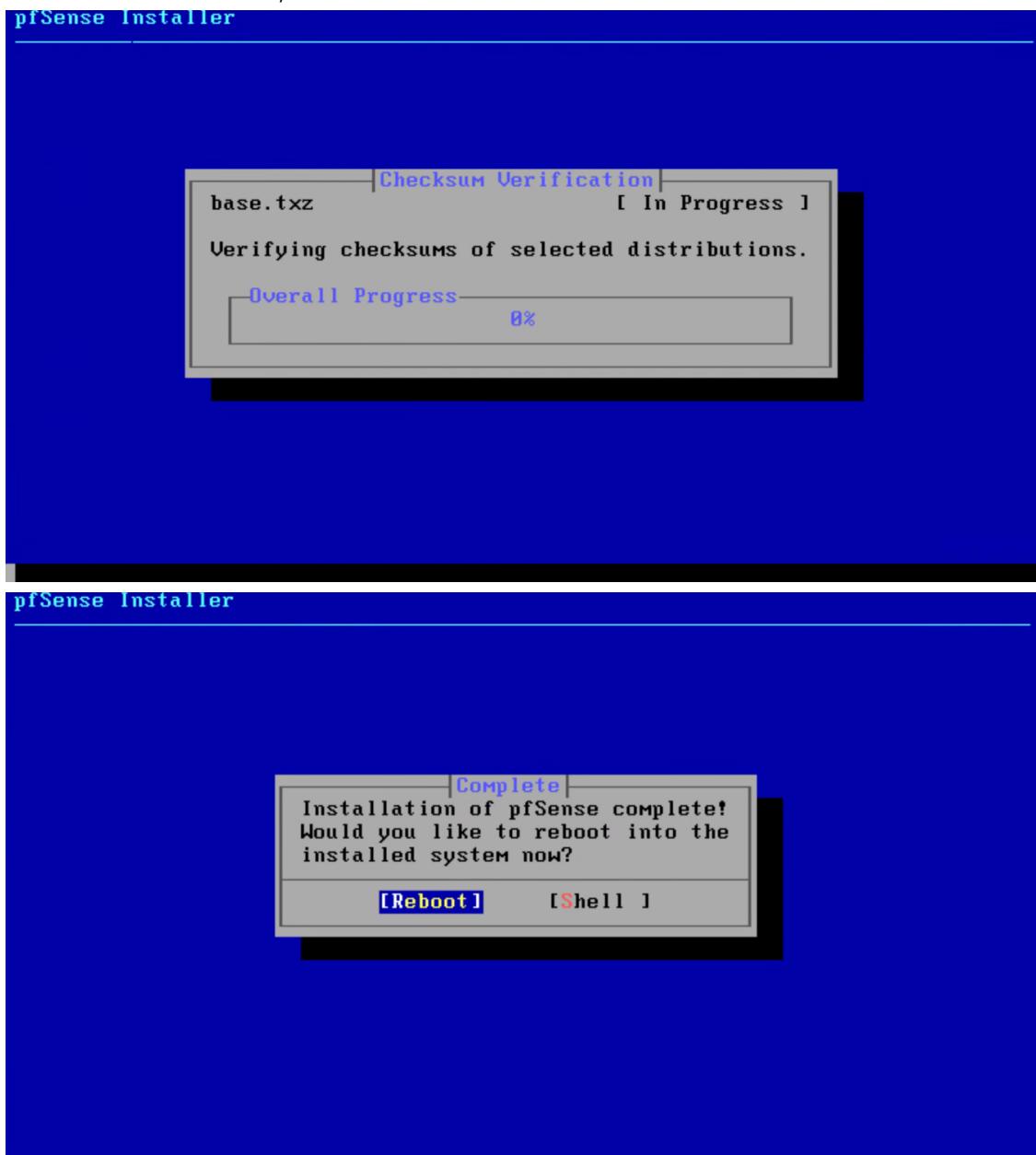
10. Sélectionnez votre disque (touche espace pour sélectionner), ici "da0"



11. Sélectionnez "Yes"



12. L'installation commence, sélectionnez "Reboot" une fois terminé



Configuration Interne

0. Laissez le serveur démarrer
1. Faites "a" pour détecter automatiquement l'inteface WAN et LAN, en cas d'erreur, sélectionnez les manuellement

2. Appuyez sur 2 pour configurer l'interface WAN

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: 2ca1a6bddf1395f3152d

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.202.144/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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: 2
```

3. Sélectionnez l'interface WAN avec le numéro correspondant (ici 1)

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1
```

4. Faites "y" pour configurer l'interface WAN en DHCP pour l'IpV4

5. Faites de même pour l'IpV6

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1

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

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

6. Si demandé, refusez l'http pour le webconfigurator

```
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 WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 WAN address has been set to dhcp

The IPv6 WAN address has been set to dhcp6

Press <ENTER> to continue.■
```

7. Faites "Entrer" pour valider la configuration

8. Appuyez sur 2 pour configurer l'interface LAN

9. Sélectionnez l'interface LAN avec le numéro correspondant (ici 2)

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.202.144/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

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

10. Faites "n" pour configurer l'interface LAN en statique pour l'IpV4

11. L'adresse LAN est 192.168.1.1

12. Le masque est 24

13. Faites "Entrer" pour la Gateway car c'est le serveur PfSense lui-même

```
Available interfaces:
1 - WAN (em1 - dhcp, dhcp6)
2 - LAN (em0 - static)

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:
> 192.168.1.1

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):
> 24

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

14. Faites "y" pour configurer l'interface LAN en DHCP pour l'IPv6, la raison étant que nous n'en avons pas besoin en LAN dans cette infrastructure
15. Faites "y" pour configurer le serveur DHCP pour l'IPv4

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

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

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

16. L'adresse de départ est 192.168.1.2
17. L'adresse de fin est 192.168.1.2
18. Nous gardons cette IP dans le cas où nous aurions besoin d'accéder au serveur PfSense en direct
19. Faites "Entrer" pour valider la configuration

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.2
Enter the end address of the IPv4 client address range: 192.168.1.5
Disabling IPv6 DHCPD...

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

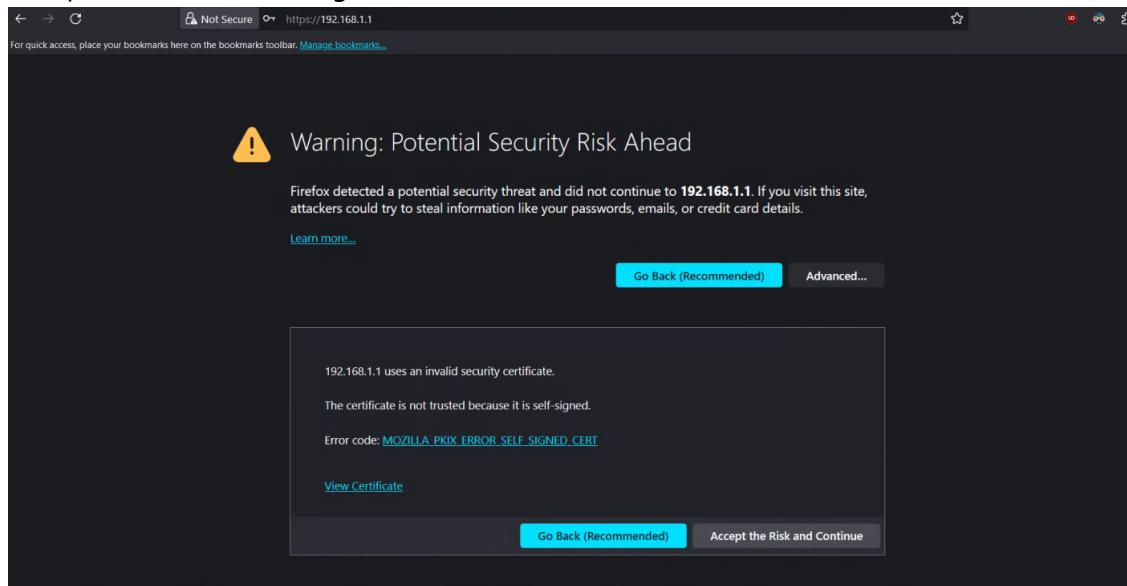
The IPv4 LAN address has been set to 192.168.1.1/24

The IPv6 LAN address has been set to dhcp6

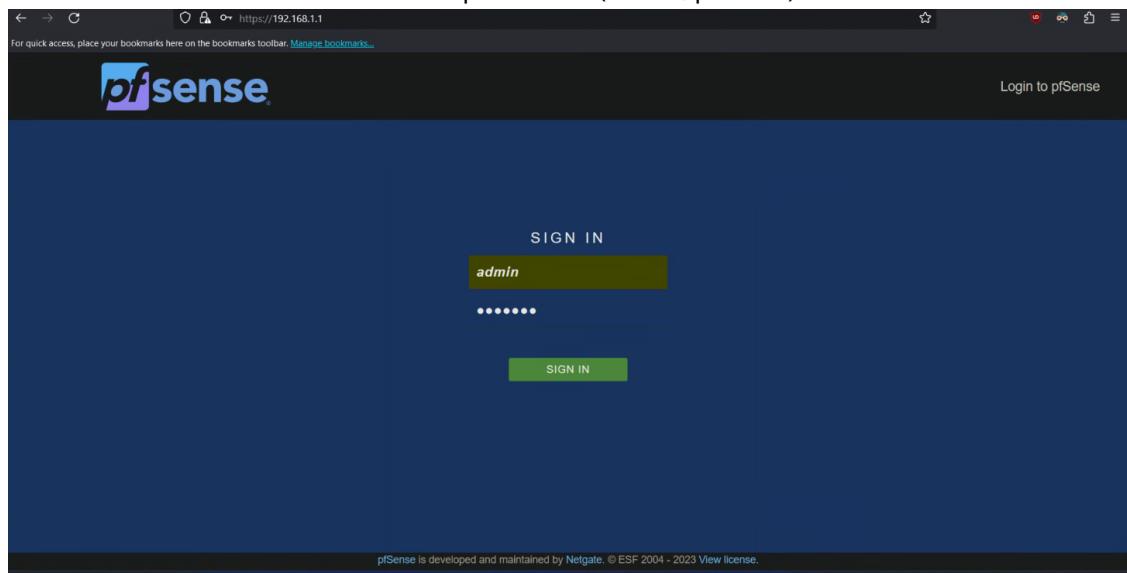
Press <ENTER> to continue.
```

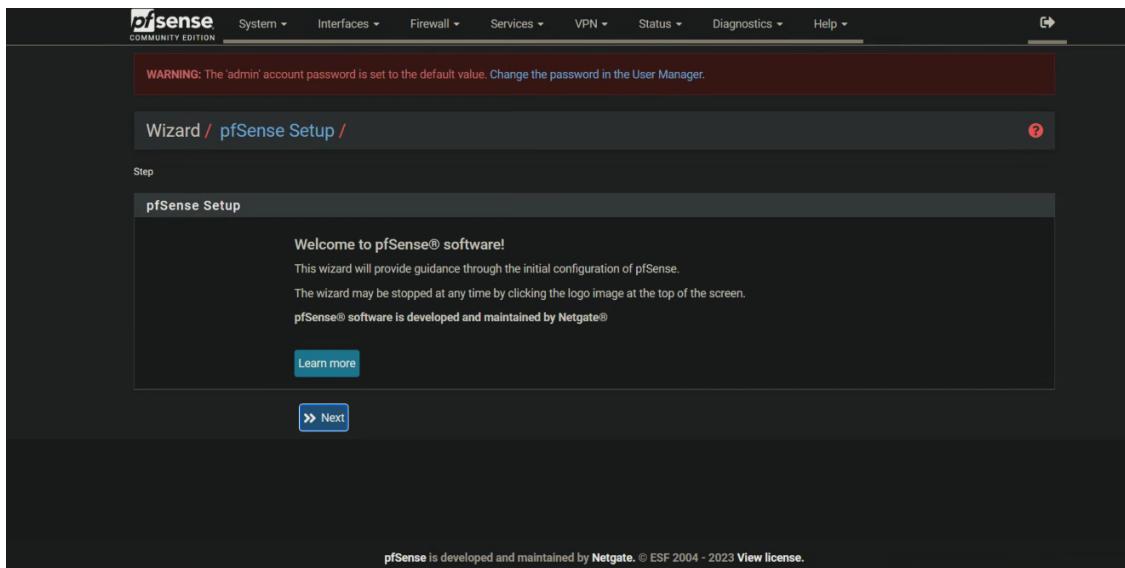
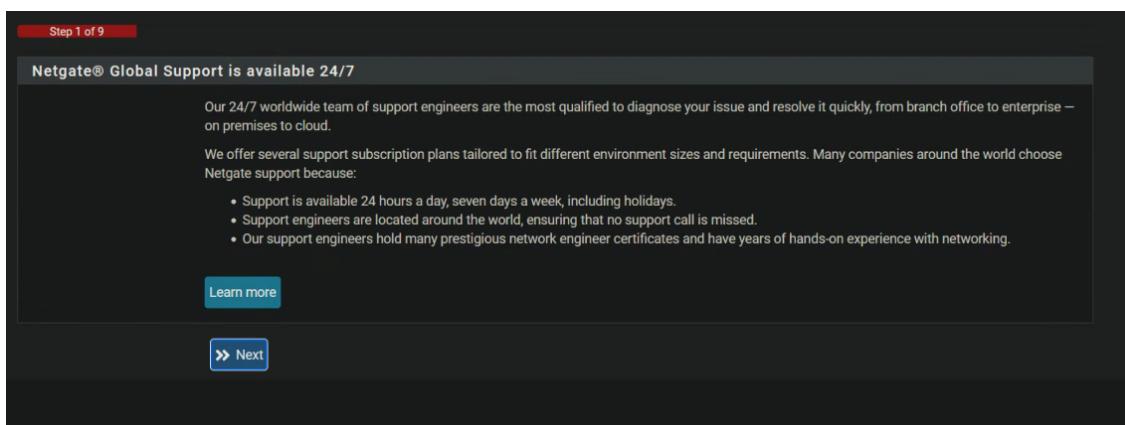
Configuration GUI

1. Connectez un ordinateur au port LAN du serveur, vous devriez ainsi obtenir l'adresse 192.168.1.2
2. Ouvrez un navigateur
3. Allez sur l'adresse https://192.168.1.1/
4. Acceptez et continuez malgré le certificat invalide



5. Connectez-vous avec les identifiants par défaut (admin/pfsense)



6. Faites "Next"**7. Faites "Next"****8. Remplissez les informations :**

- "Pf-Entreprise" pour le hostname
- "1.1.1.1" pour le DNS principal
- "8.8.8.8" pour le DNS secondaire

8. Faites "Next"

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

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

Domain home.arpa
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.

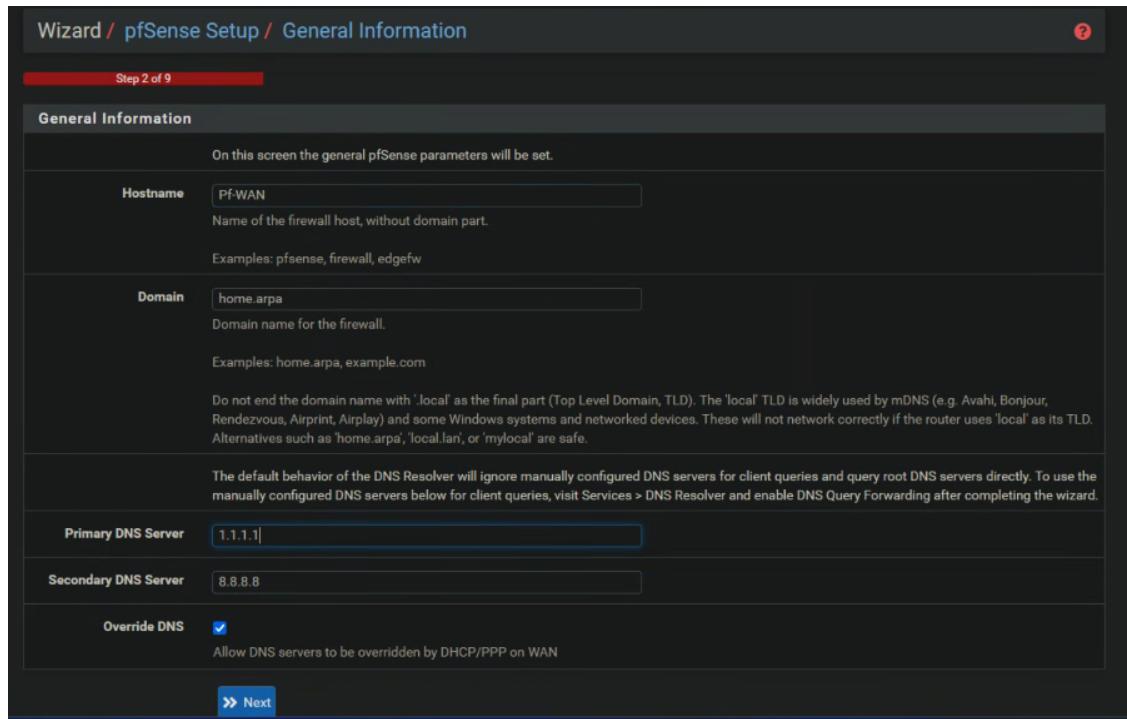
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server 1.1.1.1

Secondary DNS Server 8.8.8.8

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

>> Next



9. Sélectionnez votre fuseau horaire (ici Europe/Paris)

10. Faites "Next"

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

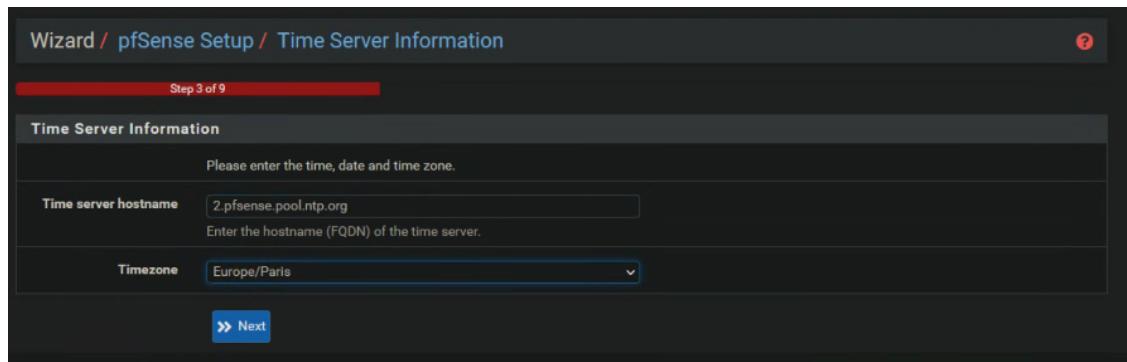
Time Server Information

Please enter the time, date and time zone.

Time server hostname 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone Europe/Paris

>> Next



11. Faites "Next", aucune modification n'est nécessaire pour le WAN

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: DHCP

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: 1492

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: 1492

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: 32

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).

PPPoE configuration

PPPoE Username:

PPPoE Password:

Show PPPoE password: Reveal password characters

PPPoE Service name: Hint: this field can usually be left empty

PPPoE Dial on demand: Enable Dial-On-Demand mode

PPPoE Service name: [Input field] Hint: this field can usually be left empty

PPPoE Dial on demand: Enable Dial-On-Demand mode
This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPPoE Idle timeout: [Input field]
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

PPTP configuration:

- PPTP Username:** [Input field]
- PPTP Password:** [Input field]
- Show PPTP password:** Reveal password characters
- PPTP Local IP Address:** [Input field]
- pptplocalsubnet:** [Input field] 32
- PPTP Remote IP Address:** [Input field]

PPTP Dial on demand: Enable Dial-On-Demand mode
This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout: [Input field]
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

RFC1918 Networks:

- Block RFC1918 Private Networks:** Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.
- Block bogon networks:** Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

>> Next

12. Faites "Next", aucune modification n'est nécessaire pour le LAN

Configure LAN Interface
On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.1.1
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

>> Next

13. Changez le mot de passe de l'admin ("admin" pour l'exemple, mais il se doit d'être sécurisé)

14. Faites "Next"

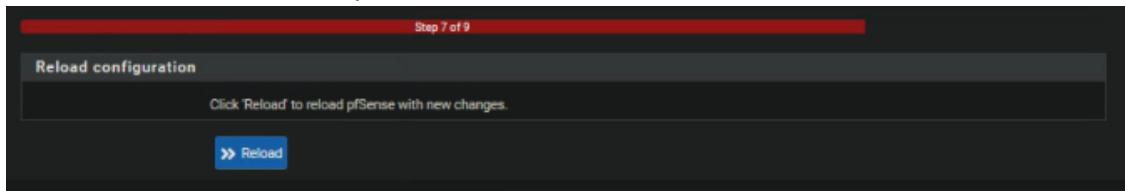
Set Admin WebGUI Password
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: *****

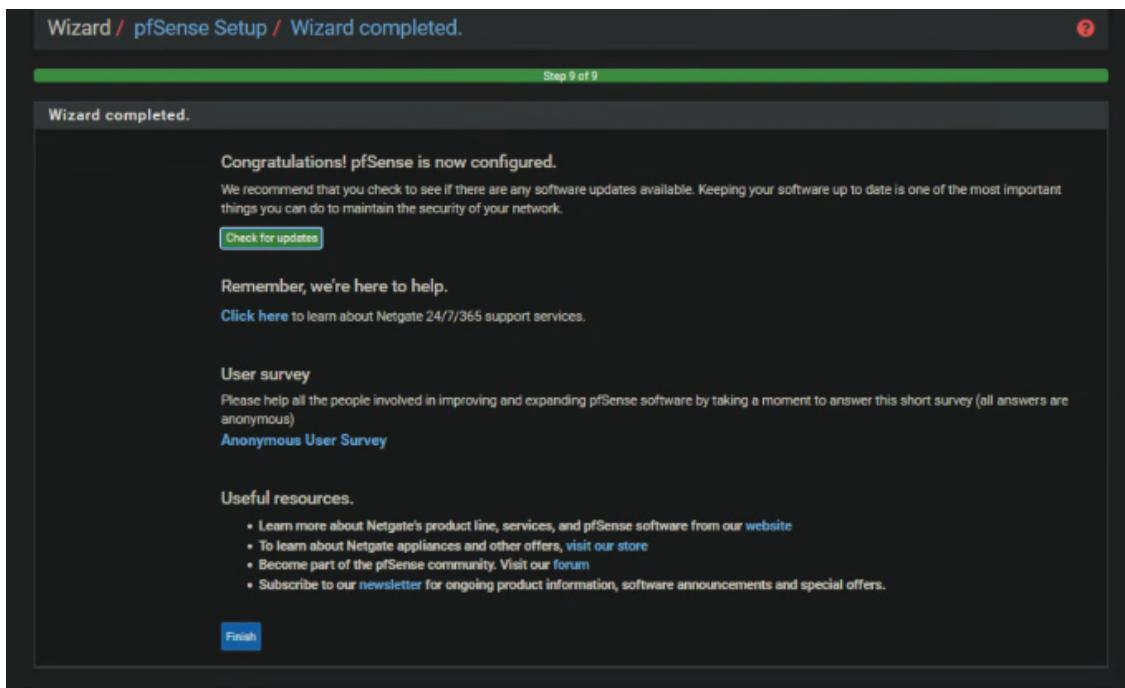
Admin Password AGAIN: *****

>> Next

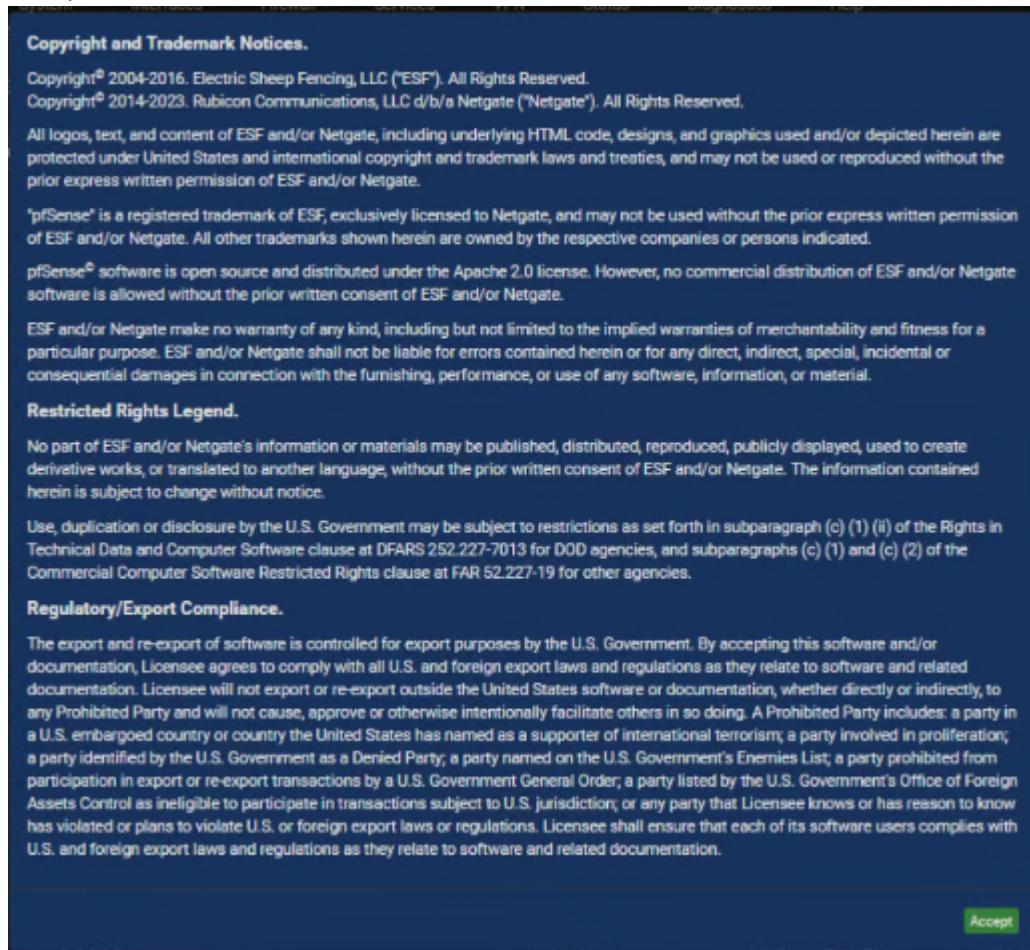
15. Faites "Reload" et attendez que le serveur redémarre



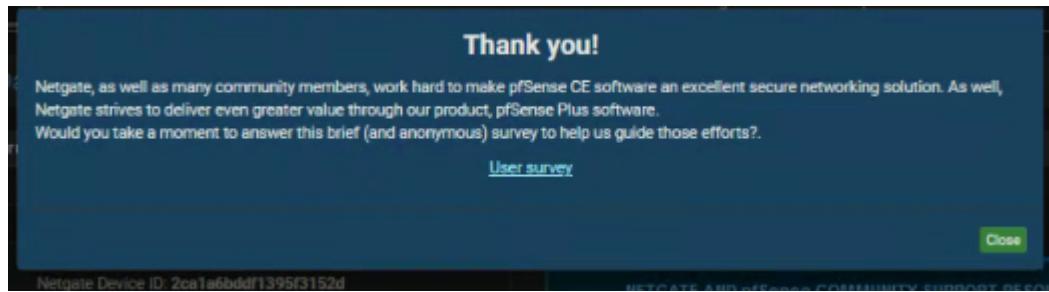
16. Une fois la page rechargée, faites "Check for updates" si l'ISO utilisée est ancienne, sinon faites "Finish"



17. Acceptez les conditions d'utilisation



18. Faites "Close"

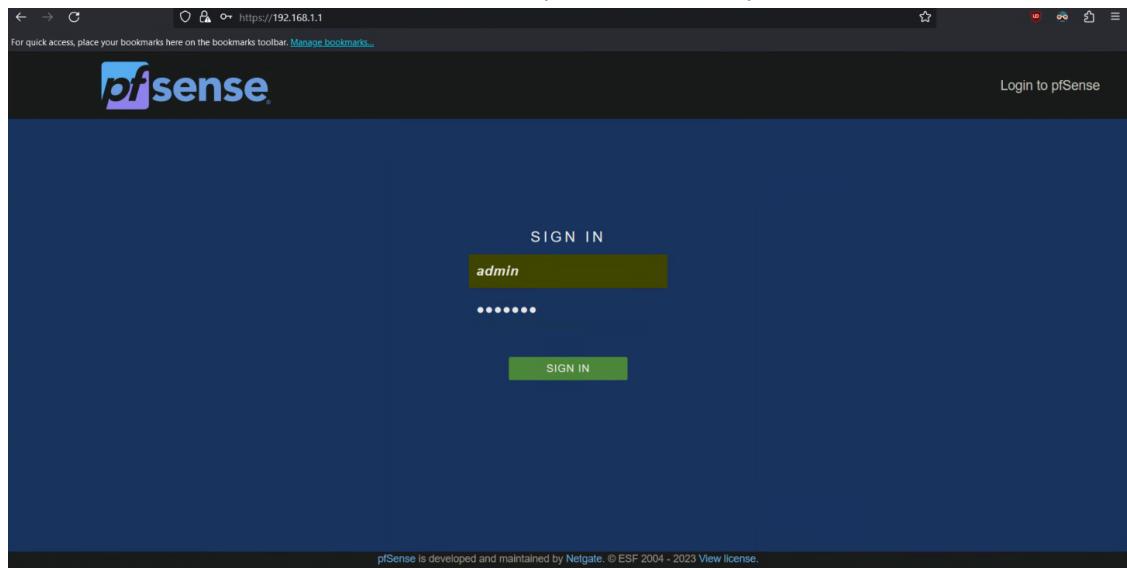


Configuration Interfaces

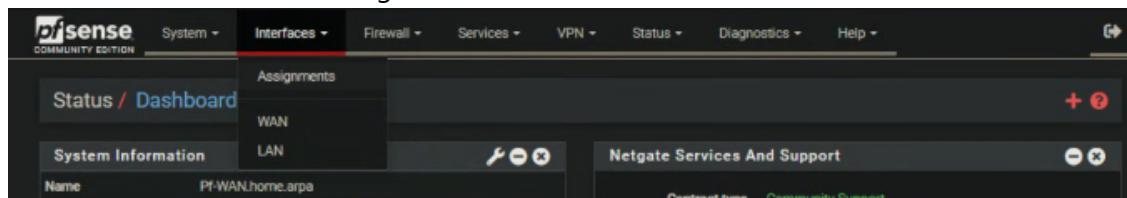
Configuration VLANs

- Connectez un ordinateur au port LAN du serveur, vous devriez ainsi obtenir l'adresse 192.168.1.2
- Ouvrez un navigateur
- Allez sur l'adresse <https://192.168.1.1/>

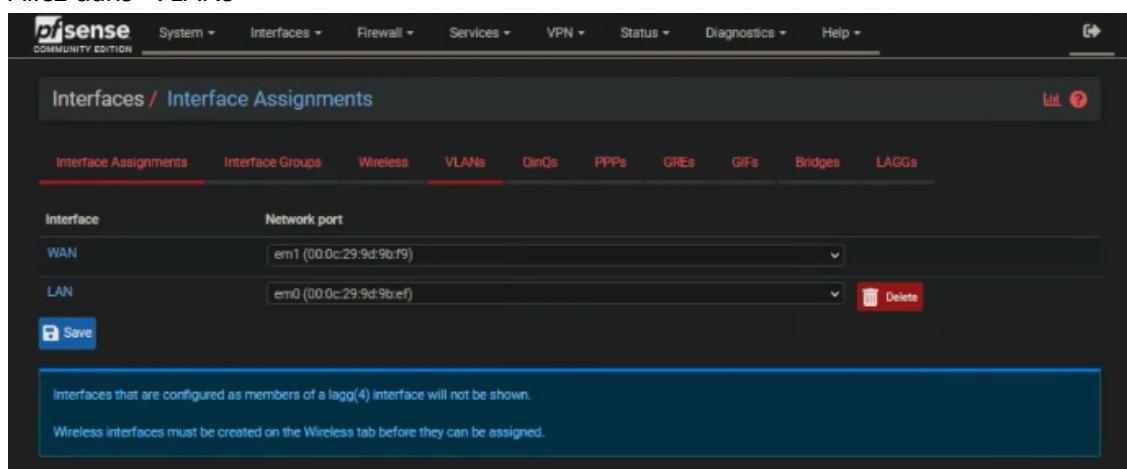
4. Connectez-vous avec les identifiants défini (ici admin/admin)



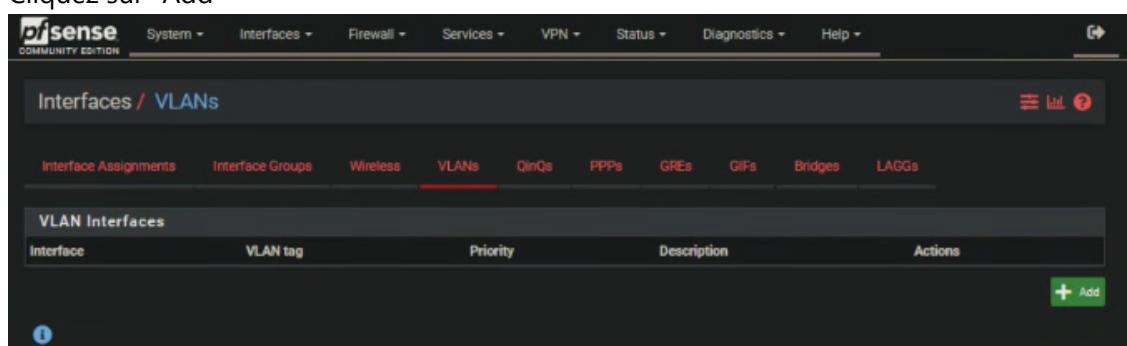
5. Allez dans "Interfaces" > "Assignments"



6. Allez dans "VLANS"



7. Cliquez sur "Add"



8. Sélectionnez l'interface LAN (ici em0)

9. Entrez le VLAN (ici 100)

10. Entrez une description (ici "Ethernet + Wifi")

11. Faites "Save"

The screenshot shows the 'Interfaces / VLANs / Edit' page. In the 'VLAN Configuration' section, the 'Parent Interface' is set to 'em0 (00:0c:29:9d:9b:ef) - lan'. The 'VLAN Tag' is set to '100'. The 'VLAN Priority' is set to '0'. The 'Description' is 'Serv1 Light-Snoop'. A blue 'Save' button is visible at the bottom.

12. Cliquez sur "Add"

The screenshot shows the 'Interfaces / VLANs' page with the 'VLANs' tab selected. A table titled 'VLAN Interfaces' lists one entry: 'Interface' (em0 (lan)), 'VLAN tag' (100), 'Priority' (0), and 'Description' (Serv1 Light-Snoop). An 'Actions' column shows edit and delete icons. A green '+' icon labeled 'Add' is located at the bottom right.

13. Sélectionnez l'interface LAN (ici em0)

14. Entrez le VLAN (ici 200)

15. Entrez une description (ici "Wifi Invité")

16. Faites "Save"

The screenshot shows the 'Interfaces / VLANs / Edit' page. In the 'VLAN Configuration' section, the 'Parent Interface' is set to 'em0 (00:0c:29:9d:9b:ef) - lan'. The 'VLAN Tag' is set to '200'. The 'VLAN Priority' is set to '0'. The 'Description' is 'Serv2 Light-Snoop'. A blue 'Save' button is visible at the bottom.

17. Allez dans "Interfaces Assignments"

Interface	VLAN tag	Priority	Description	Actions
em0 (lan)	100		Serv1 Light-Snoop	
em0 (lan)	200		Serv2 Light-Snoop	

18. Faites "Add"

WAN: em1 (00:0c:29:9d:9b:f9)

LAN: em0 (00:0c:29:9d:9b:ef)

Available network ports: VLAN 100 on em0 - lan (Serv1 Light-Snoop)

19. Faites à nouveau "Add"

Interface has been added.

WAN: em1 (00:0c:29:9d:9b:f9)

LAN: em0 (00:0c:29:9d:9b:ef)

OPT1: VLAN 100 on em0 - lan (Serv1 Light-Snoop)

Available network ports: VLAN 200 on em0 - lan (Serv2 Light-Snoop)

20. Cliquez sur l'interface OPT1 (VLAN 100)

Interface	Network port
WAN	em1 (00:0c:29:9d:9b:f9)
LAN	em0 (00:0c:29:9d:9b:ef)
OPT1	VLAN 100 on em0 - lan (Serv1 Light-Snoop)
OPT2	VLAN 200 on em0 - lan (Serv2 Light-Snoop)

21. Activez l'interface
22. Passez l'IPv4 en statique
23. Entrez l'adresse IP (ici 192.168.100.254)
24. Précisez le masque (ici 24)

25. Faites "Save"

The screenshot shows the 'Interfaces / OPT1 (em0.100)' configuration page in pfSense. The 'General Configuration' section includes fields for Enable (checked), Description (OPT1), IPv4 Configuration Type (Static IPv4), IPv6 Configuration Type (None), MAC Address (xx:xx:xx:xx:xx:xx), MTU (blank), MSS (blank), and Speed and Duplex (Default). The 'Static IPv4 Configuration' section shows an IPv4 Address of 192.168.100.254 and a subnet mask of 24. The 'Reserved Networks' section contains options for Block private networks and loopback addresses (unchecked) and Block bogon networks (unchecked). A 'Save' button is at the bottom.

26. Retournez dans "Interfaces" > "Assignments"

The OPT1 configuration has been modified. The changes must be applied to the interface after applying. Don't forget to adjust the DHCP.

General Configuration

- Enable:** Enable interface
- Description:** OPT1
- IPv4 Configuration Type:** Static IPv4
- IPv6 Configuration Type:** None
- MAC Address:** XX:XX:XX:XX:XX:XX
- MTU:** (Blank)
- MSS:** (Blank)
- Speed and Duplex:** Default (no preference, typically autoselect)

Static IPv4 Configuration

- IPv4 Address:** 192.168.100.254 / 24
- IPv4 Upstream gateway:** None

Reserved Networks

- Block private networks and loopback addresses:**
- Block bogon networks:**

Save

27. Cliquez sur l'interface OPT2 (VLAN 200)

Interface	Network port
WAN	em1 (00:0c:29:9d:9b:f9)
LAN	em0 (00:0c:29:9d:9b:ef)
OPT1	VLAN 100 on em0 - lan (Serv1 Light-Snoop)
OPT2	VLAN 200 on em0 - lan (Serv2 Light-Snoop)

Save

Interfaces that are configured as members of a lag(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.

28. Activez l'interface
29. Passez l'IPv4 en statique
30. Entrez l'adresse IP (ici 192.168.200.254)
31. Précisez le masque (ici 24)
32. Faites "Save"

The OPT2 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.

Enable interface

Description: OPT2
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: XX:XX:XX:XX:XX:XX
The MAC address of a VLAN interface must be set on its parent interface.

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: 192.168.200.254 / 24

IPv4 Upstream gateway: None
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.

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.

Configuration DHCP

1. Allez dans "Services" > "DHCP Server"

2. Allez dans "OPT1"

3. Activez le serveur DHCP

4. Entrez le range d'adresse (ici 192.168.100.1 - 192.168.100.5, adaptez en fonction de vos besoins, si vous avez plus d'ordinateurs et autres appareils ou que vous allez augmenter)

votre parc, augmentez le range. Préférez prendre une range adaptée avec une petite marge pour minimiser les risques)

5. Faites "Save"

General Options

- Enable: Enable DHCP server on OPT1 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.

Subnet: 192.168.100.0
Subnet mask: 255.255.255.0
Available range: 192.168.100.1 - 192.168.100.254
Range: From: 192.168.100.1 To: 192.168.100.5

Additional Pools

Add + Add pool

If additional pools of addresses are needed inside of this subnet outside of the above Range, they may be specified here.

6. Allez dans "OPT2"

The changes have been applied successfully.

General Options

- Enable: Enable DHCP server on OPT1 interface
- BOOTP: Ignore BOOTP queries
- Deny unknown clients: Allow all clients

7. Activez le serveur DHCP

8. Entrez le range d'adresse (ici 192.168.200.1 - 192.168.200.254, la range est plus grande car nous ne savons pas combien d'appareils vont se connecter au Wifi invité et que celui-ci sera plus contrôlé)

9. Faites "Save"

General Options

- Enable: Enable DHCP server on OPT2 interface
- BOOTP: Ignore BOOTP queries
- Deny unknown clients: Allow all clients
- Ignore denied clients: Ignore denied clients rather than reject
- Ignore client identifiers: Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

Subnet: 192.168.200.0
Subnet mask: 255.255.255.0
Available range: 192.168.200.1 - 192.168.200.254
Range: From 192.168.200.1 To 192.168.200.5

Additional Pools

Add **+ Add pool**

If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.

Configuration Firewall

1. Allez dans "Firewall" > "Rules"

The changes have been applied successfully.

2. Allez dans "OPT1"

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/5 KIB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	⚙️
0/0 B	*	Reserved	*	*	*	*	*	*	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.

Actions: **⬆️ Add** **⬇️ Add** **Delete** **Toggle** **Copy** **Save** **+ Separator**

3. Faites "Add"

The screenshot shows the pfSense Firewall / Rules / OPT1 interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation is a breadcrumb trail: Firewall / Rules / OPT1. The main content area has tabs for Floating, WAN, LAN, OPT1 (which is selected), and OPT2. A sub-header "Rules (Drag to Change Order)" is followed by a table with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A message at the bottom states: "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." Below the message are several action buttons: Add, Add, Delete, Toggle, Copy, Save, and Separator.

4. Changer le "Protocol" en "Any"
5. Changer la "Source" en "OPT1 net"
6. Mettez "Default allow LAN to any rule" en description
7. Faites "Save"

The screenshot shows the pfSense Firewall / Rules / Edit interface for a new rule. The top navigation bar and breadcrumb trail are identical to the previous screenshot. The main form is titled "Edit Firewall Rule". It contains several sections:

- Action:** Pass (selected). A hint below says: "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. A hint below says: "Set this option to disable this rule without removing it from the list."
- Interface:** OPT1. A hint below says: "Choose the interface from which packets must come to match this rule."
- Address Family:** IPv4. A hint below says: "Select the Internet Protocol version this rule applies to."
- Protocol:** Any. A hint below says: "Choose which IP protocol this rule should match."

 Below these are sections for **Source** and **Destination**, each with fields for Source/Destination, Invert match, and Destination Address.

Extra Options section includes:

- Log:** Log packets that are handled by this rule. A hint below says: "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:** Default allow LAN to any rule. A hint below says: "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."

 At the bottom are "Display Advanced" and "Save" buttons.

8. Faites "Add"

The screenshot shows the pfSense Firewall Rules list. A message at the top states: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." There is a blue "Apply Changes" button. Below this, the rules table has tabs for Floating, WAN, LAN, OPT1 (which is selected), and OPT2. The table lists one rule:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	OPT1 net	*	*	*	*	none		Default allow LAN to any rule	

Below the table are several action buttons: Add, Add, Delete, Toggle, Copy, Save, and Separator.

9. Changer l' "Address Family" en "IPv6"
10. Changer le "Protocol" en "Any"
11. Changer la "Source" en "OPT1 net"
12. Mettez "Default allow LAN to any rule" en description
13. Faites "Save"

The screenshot shows the "Edit Firewall Rule" configuration page. The rule is named "Pass". The configuration fields are as follows:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** OPT1
- Address Family:** IPv6
- Protocol:** Any

Source: Source: OPT1 net, Invert match:

Destination: Destination: any, Invert match:

Extra Options:

- Log:** Log packets that are handled by this rule
- Description:** Default allow LAN to any rule
- Advanced Options:**

At the bottom is a blue "Save" button.

14. Allez dans "OPT2"

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

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/0 B	IPv6 *	OPT1 net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv4 *	OPT1 net	*	*	*	*	none		Default allow LAN to any rule	

Actions: Add Add Delete Toggle Copy Save Separator

15. Faites "Add"

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

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
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.										

Actions: Add Add Delete Toggle Copy Save Separator

16. Changer le "Protocol" en "Any"

17. Changer la "Source" en "OPT2 net"

18. Mettez "Default allow LAN to any rule" en description

19. Faites "Save"

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' is set to 'Pass'. The 'Disabled' checkbox is unchecked. The 'Interface' is set to 'OPT2'. The 'Address Family' is set to 'IPv4'. The 'Protocol' is set to 'Any'. In the 'Source' section, the 'Source' dropdown is set to 'OPT2 net'. In the 'Destination' section, the 'Destination' dropdown is set to 'any'. Under 'Extra Options', the 'Log' checkbox is unchecked. The 'Description' field contains 'Default allow LAN to any rule'. A 'Display Advanced' button is visible. At the bottom is a 'Save' button.

20. Faites "Add"

The screenshot shows the 'Firewall / Rules / OPT2' page. A message at the top says 'The firewall rule configuration has been changed. The changes must be applied for them to take effect.' A green 'Apply Changes' button is visible. Below is a table titled 'Rules (Drag to Change Order)'. It shows one rule: '0/0 B' with 'IPv4 *' selected. The table includes columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. Action buttons include Add, Delete, Toggle, Copy, Save, and Separator. A small info icon is at the bottom left.

21. Changer l' "Address Family" en "IPv6"
22. Changer le "Protocol" en "Any"
23. Changer la "Source" en "OPT2 net"
24. Mettez "Default allow LAN to any rule" en description

25. Faites "Save"

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' dropdown is set to 'Pass'. The 'Disabled' checkbox is unchecked. The 'Interface' is set to 'OPT2'. The 'Address Family' is 'IPv6'. The 'Protocol' is 'Any'. In the 'Source' section, the source is 'OPT2 net'. In the 'Destination' section, the destination is 'any'. Under 'Extra Options', there is a 'Log' checkbox which is unchecked. A note says: '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.)'. The 'Description' field contains 'Default allow LAN to any rule'. An 'Advanced Options' button is present. At the bottom is a 'Save' button.

26. Redémarrez le serveur PfSense pour que tout les changements soient pris en compte :

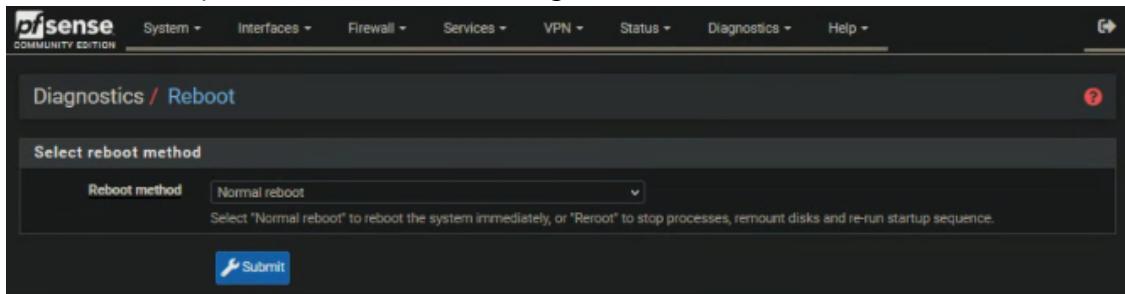
"Diagnostics" > "Reboot"

The screenshot shows the 'Firewall / Rules / OPT2' screen with a message: 'The firewall rule configuration has been changed. The changes must be applied for them to take effect.' Below is a table of rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedul
<input type="checkbox"/>	0/0 B	IPv6 *	OPT2.net	*	*	*	*	none	
<input type="checkbox"/>	0/0 B	IPv4 *	OPT2.net	*	*	*	*	none	

To the right is a sidebar with 'Diagnostics' selected. Under 'Actions' for the first rule, there is a 'Reboot' button. The sidebar also lists other diagnostic tools like ARP Table, Authentication, and DNS Lookup.

27. Faites "Submit" pour confirmer le redémarrage

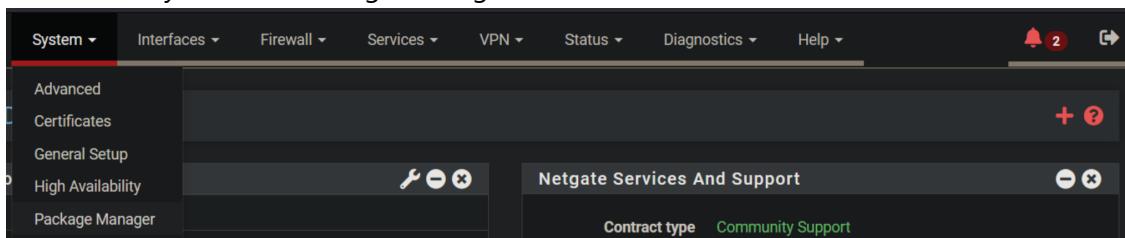


Configuration Applications

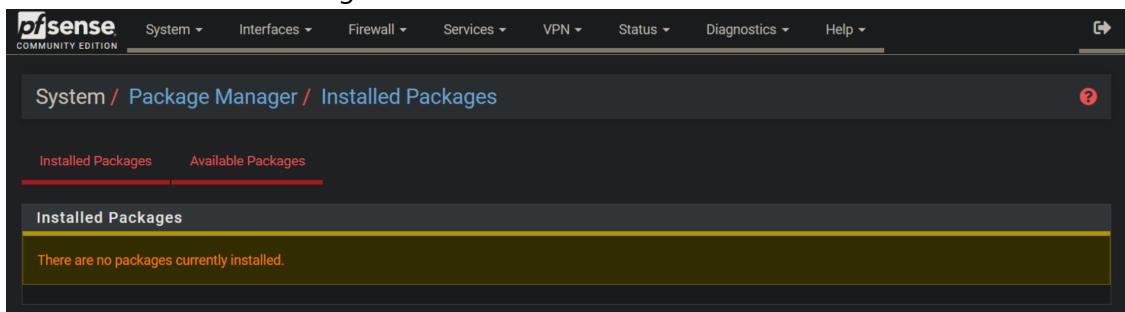
Il nous faut un packet qui puisse gérer la sécurisation du réseau, nous utilisons ici Suricata
Afin de pouvoir intervenir en CLI sur le PfSense à distance, il nous faut un accès SSH

Suricata

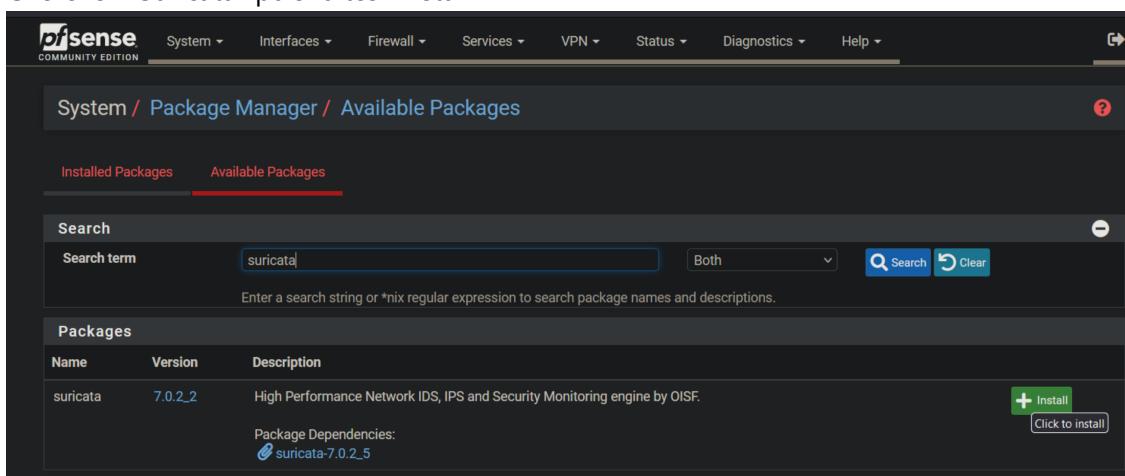
1. Allez dans "System" > "Package Manager"



2. Allez dans "Available Packages"



3. Cherchez "Suricata" puis faites "Install"



4. Faites "Confirm" pour lancer l'installation et attendez la fin de celle-ci

The image consists of two vertically stacked screenshots of the pfSense Package Manager interface.

Screenshot 1 (Top): This screenshot shows a confirmation dialog box. The title bar says "System / Package Manager / Package Installer". The main content area displays the message "Confirmation Required to install package pfSense-pkg-suricata.". Below this is a green button labeled "Confirm" with a checkmark icon. The navigation tabs at the top are "Installed Packages", "Available Packages", and "Package Installer", with "Package Installer" being the active tab.

Screenshot 2 (Bottom): This screenshot shows the results of the package installation. The title bar is identical. The main content area now displays the message "pfSense-pkg-suricata installation successfully completed." in a green box. The navigation tabs are the same, and the overall status is indicated by a large green progress bar at the bottom of the screen.

5. Allez dans "Services" > "Suricata"

pfSense-pkg-suricata installation successfully completed.

Available Packages	Package Installation
Auto Config Backup	RULES: Suricata IDS/IPS Engine comes without rules by add rules by yourself and set an updating strategy. To
Captive Portal	http://www.openinfosecfoundation.org/documentation/rule
DHCP Relay	http://www.openinfosecfoundation.org/documentation/et
DHCP Server	You may want to try BPF in zero-copy mode to test perfo
DHCPv6 Relay	sysctl -w net.bpf.zero-copy_enable=1
DHCPv6 Server	Don't forget to add net.bpf.zero-copy enable=1 to /etc/sysctl.conf
DNS Forwarder	
DNS Resolver	
Dynamic DNS	
IGMP Proxy	
NTP	
PPPoE Server	
Router Advertisement	
SNMP	
Suricata	
UPnP & NAT-PMP	
Wake-on-LAN	

6. Allez dans "Global Settings"

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions

7. Activez l'option "ETOpen" puis faites "Save" en bas de la page

Please Choose The Type Of Rules You Wish To Download

Install ETOpen Emerging Threats rules ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro. Use a custom URL for ETOpen downloads

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.

8. Allez ensuite dans "Updates" puis faites "Update"

Interfaces	Global Settings	Updates	Alerts	Blocks	Files	Pass Lists	Suppress	Logs View	Logs Mgmt	SID Mgmt
Sync	IP Lists									

INSTALLED RULE SET MD5 SIGNATURES

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
ABUSE.ch SSL Blacklist Rules	Not Enabled	Not Enabled

UPDATE YOUR RULE SET

Last Update: Unknown
Result: Unknown

Update Force

9. Une fois la pop-up fermée automatiquement, allez dans "Pass Lists"

INSTALLED RULE SET MD5 SIGNATURES

10. Faites "Add"

Configured Pass Lists

List Name	Assigned	Description	Actions
			<input type="button"/> + Add

11. Ajoutez les deux réseaux, 192.168.100.0/24 et 192.168.200.0/24 et faites "Save"

General Information

Name: passlist_43003
The list name may only consist of the characters 'a-z, A-Z, 0-9 and _'.

Description: You may enter a description here for your reference.

Auto-Generated IP Addresses

- Local Networks: Add firewall Locally-Attached Networks to the list (excluding WAN). Default is Checked.
- WAN Gateways: Add WAN Gateways to the list. Default is Checked.
- WAN DNS Servers: Add WAN DNS servers to the list. Default is Checked.
- Virtual IP Networks: Add Virtual IP Networks to the list. Default is Checked.
- VPN Addresses: Add VPN Addresses to the list. Default is Checked.

Custom IP Addresses and Configured Firewall Aliases

Hint: Enter as many IP addresses or alias names as desired. Enter ONLY an IP address, IP subnet or alias name! Do NOT enter a FQDN (fully qualified domain name) directly! To use a FQDN, first create the necessary firewall alias, and then provide the alias name here. FQDN aliases are periodically re-resolved and updated by the firewall. You can also provide an IP subnet with a proper netmask of the form network/mask such as 1.2.3.0/24.

IP or Alias:	192.168.100.0/24	
	192.168.200.0/24	

Save + Add IP

12. Allez dans "Interfaces"

Services / Suricata / Pass List / Edit

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

General Information

Name: passlist_43003

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions

13. Enfin, faites "Add" puis allez en bas de la page et faites "Save"

Services / Suricata

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

Interface Settings Overview

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions

SSH

1. Connectez vous sur le PfSense physiquement
2. Tapez "14"

```
SSHD is currently disabled. Would you like to enable? [y/n]? y
Writing configuration... done.

Enabling SSHD...
Reloading firewall rules. done.

VMware Virtual Machine - Netgate Device ID: 4010f35d3c753035d649

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.202.169/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

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: █
```

3. Il est désormais possible de se connecter en SSH par l'adresse 192.168.100.254 avec les identifiants du PfSense, acceptez la clé SSH pour vous connecter

