



Réalisation Technique

Sujet : Cluster PfSense

RÉALISÉ par : Darius ILOKI NZOUSSI



TABLE DES MATIERES

1. Introduction	3
1.1 Résumé	3
2. Présentation de la réalisation	3
2.1 Contexte	3
2.2 Objectifs et problématique	3
2.2.1 Objectifs.....	3
2.2.2 Problématique	3
3. Analyse fonctionnelle	3
4. Plan d'implémentation.....	3
5. Installation des deux machines pfsenses.	4
5.1 Assigner les adresses IP statique sur les interface WAN et LAN	9
5.2. Configuration de PfSense01 via l'interface Web.....	12
5.3 Configurer un cluster de 2 PfSense redondants (Failover)	20
5.3.1 Principe de fonctionnement	20
5.3.2 Configurer les adresses IP virtuelles	21
5.3.3 Configuration du NAT (Network Address Translation)	23
5.3.4 Configuration de la Haute Disponibilité	26
5.3.5 Autorisation des flux de réplication dans les règles du firewall.....	28
5.3.6 Vérification du bon fonctionnement de la haute disponibilité	32
8. Conclusion.....	34



1. INTRODUCTION

1.1 Résumé

Dans le cadre de mon BTS SIO option SISR, j'ai réalisé une réalisation technique visant à mettre en place un cluster de pare-feu avec PFSENse afin d'assurer une haute disponibilité et une gestion optimisée du trafic réseau. Ce travail permet de garantir la continuité de service en cas de panne d'un nœud. Pour cela, j'ai mis en place une infrastructure comprenant :

- ❖ Deux serveurs PFSENse configurés en cluster avec CARP,
- ❖ Un serveur DHCP et des règles NAT,
- ❖ Une gestion centralisée de la sécurité réseau.

Cette réalisation m'a permis d'acquérir des compétences en haute disponibilité, administration de pare-feu et répartition de charge. afin d'assurer une haute disponibilité et une gestion optimisée du trafic réseau.

2. PRESENTATION DE LA REALISATION

2.1 Contexte

Dans un environnement réseau, la sécurité et la disponibilité des services sont primordiales. L'utilisation d'un cluster PFSENse permet d'éviter les interruptions de service en cas de panne d'un nœud.

2.2 Objectifs et problématique

2.2.1 Objectifs

- ❖ Mettre en place un cluster PFSENse en mode HA (High Availability).
- ❖ Assurer la redondance des services réseau.
- ❖ Configurer le répartition de charge et la synchronisation des configurations.

2.2.2 Problématique

Comment garantir une haute disponibilité du pare-feu tout en maintenant une gestion centralisée et automatisée des configurations ?

3. ANALYSE FONCTIONNELLE

L'infrastructure est constituée de deux machines **PFSENse** configurées en mode CARP (Common Address Redundancy Protocol) pour assurer la redondance. Un serveur DHCP, des règles NAT et un VPN sont également configurés.

4. PLAN D'IMPLEMENTATION

1. Installation de deux machines PFSENse.
2. Configuration du protocole CARP pour la haute disponibilité.
3. Synchronisation des règles de pare-feu et NAT.
4. Tests de bascule et validation.

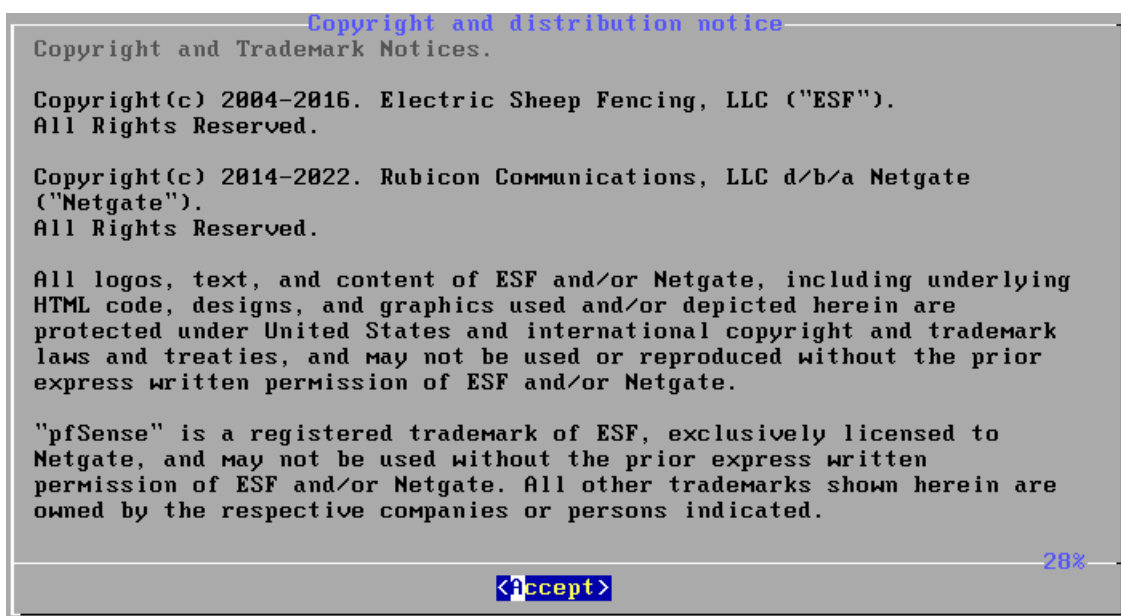


5. INSTALLATION DES DEUX MACHINES PFSENSES.

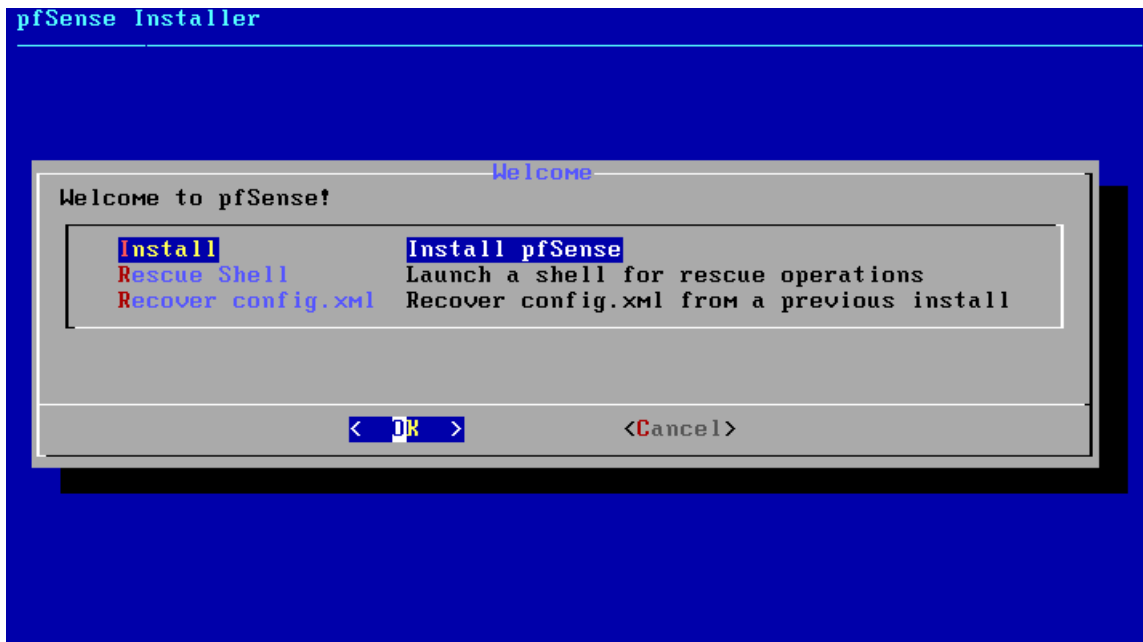
❖ Installation de Pfsense-1



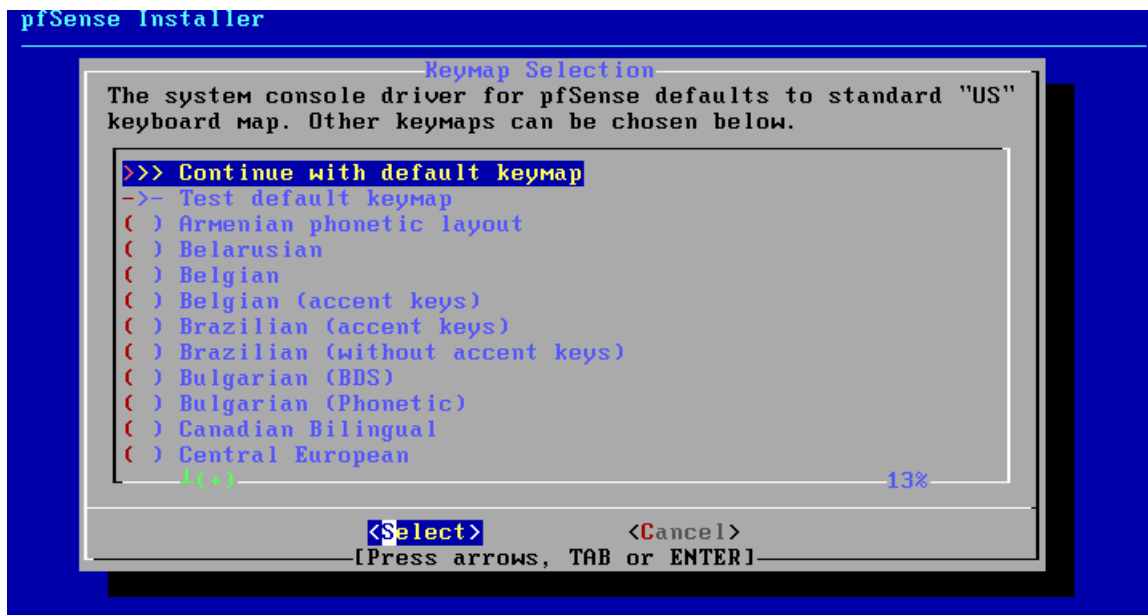
PfSense choisira automatiquement le mode de démarrage adapté lors de la première mise en marche de la machine virtuelle. Il démarrera depuis le fichier ISO de l'installation que vous avez sélectionné précédemment.



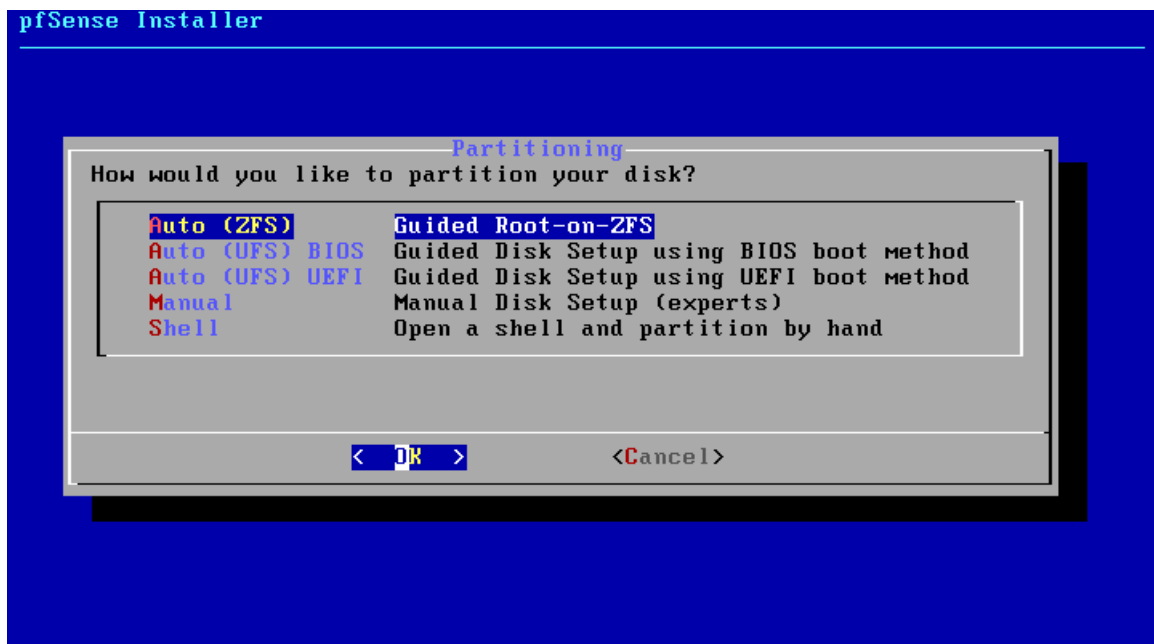
Cliquez sur Accepter.



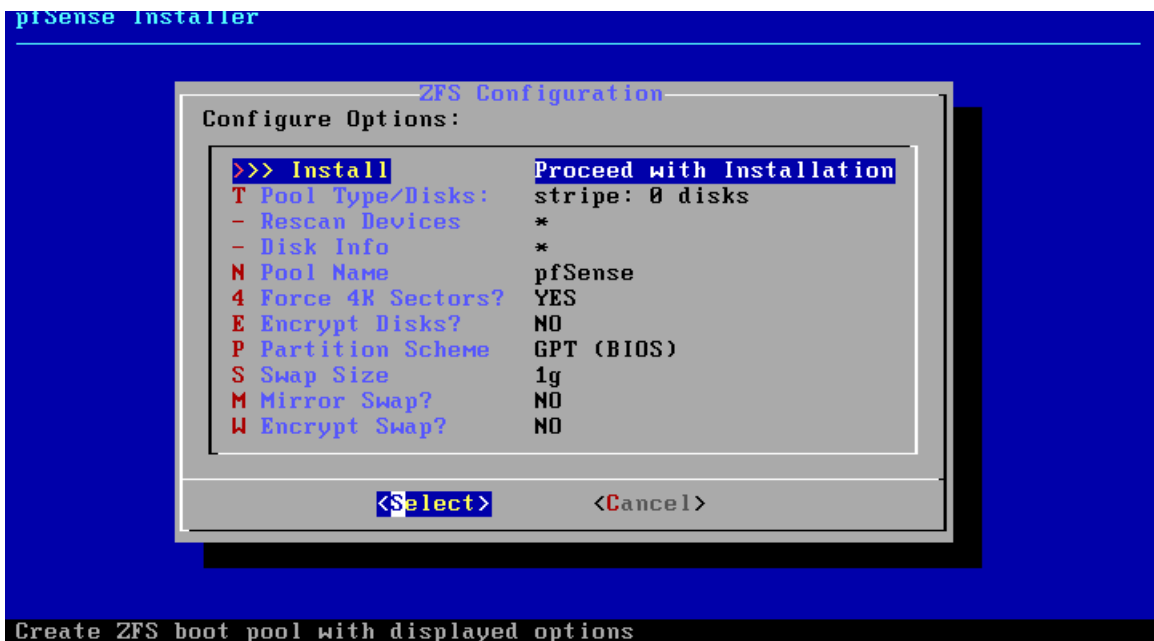
Cliquez sur ok pour continuer.



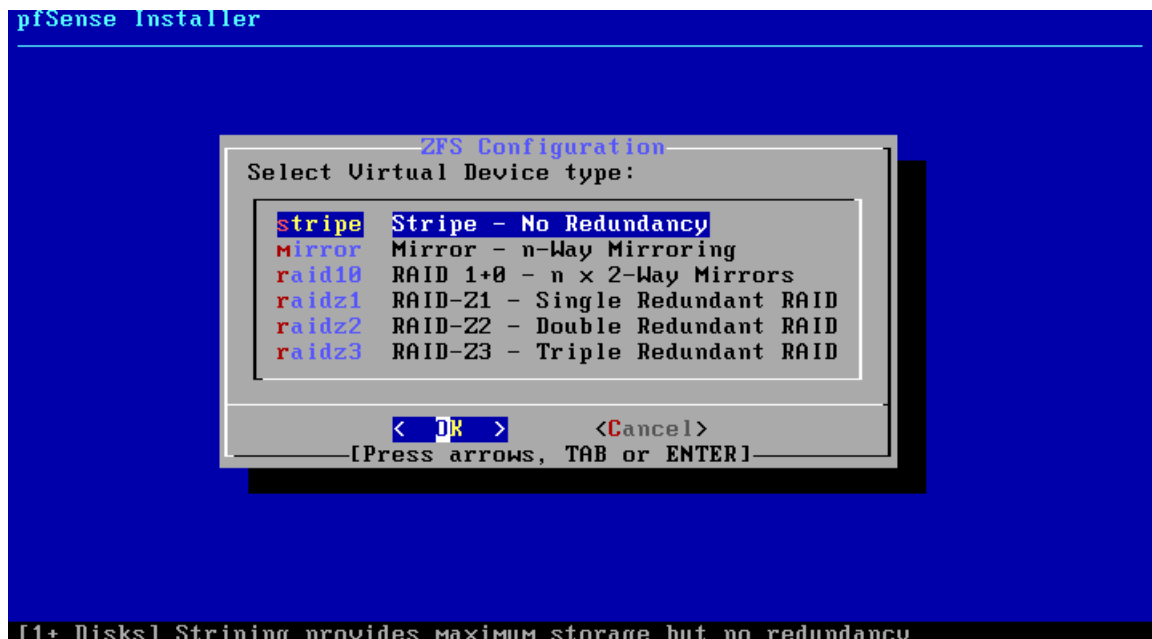
Cliquez sur Select pour continuer l'Installation.



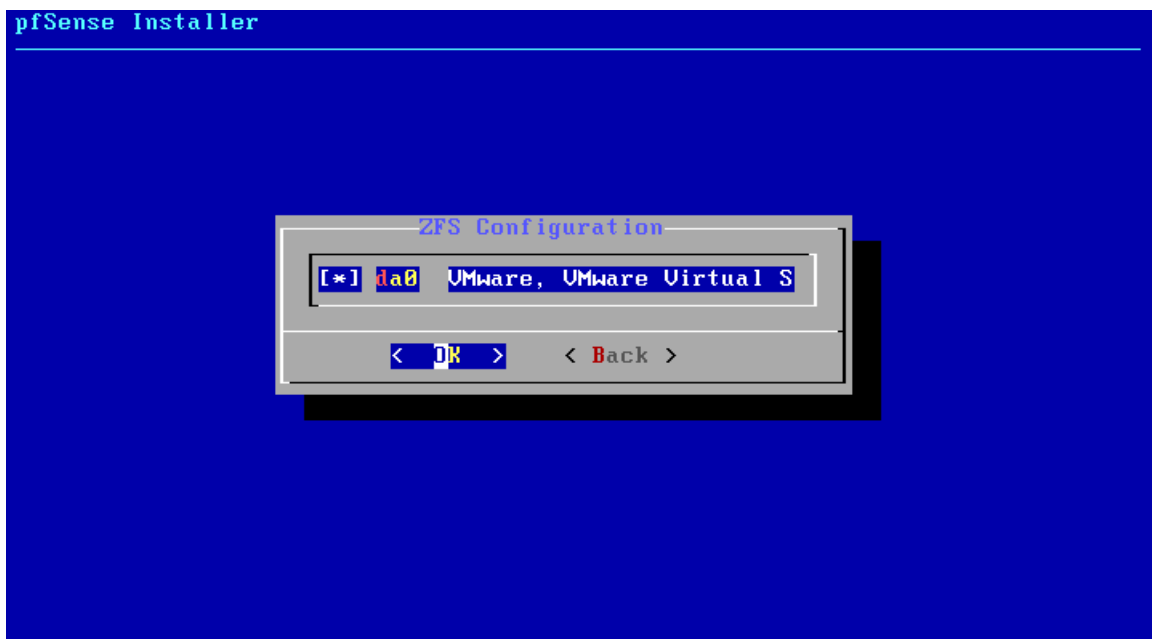
en sélectionnant **Auto (ZFS)** pour le système de fichiers, puis choisissez **Root-on-ZFS** pour le mode de démarrage.



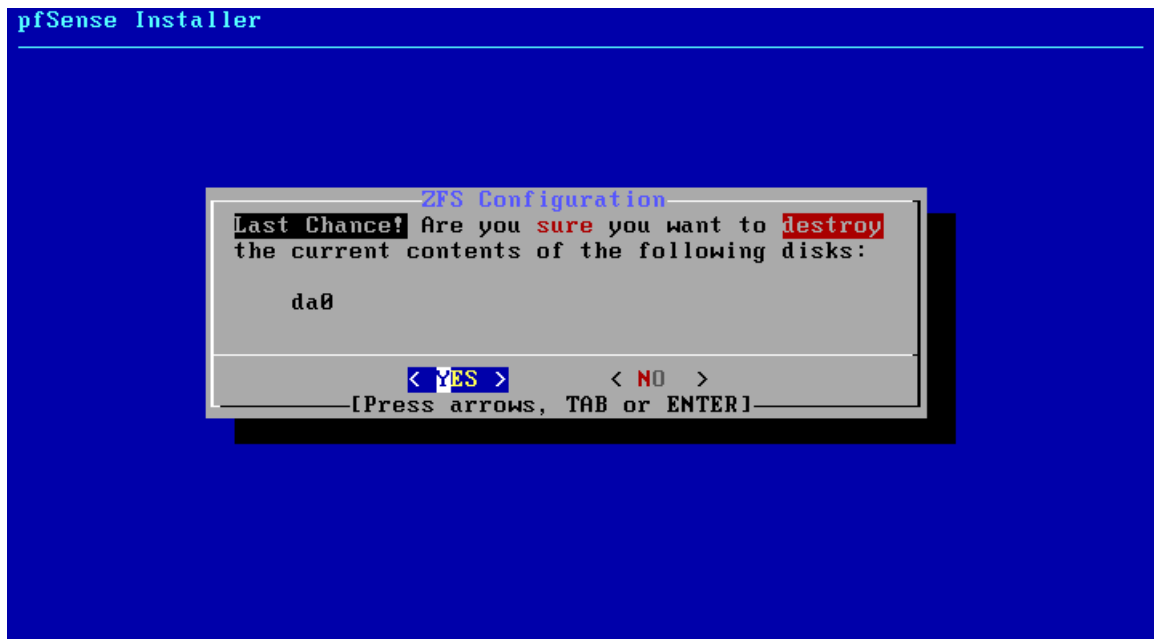
En clic sur Select .



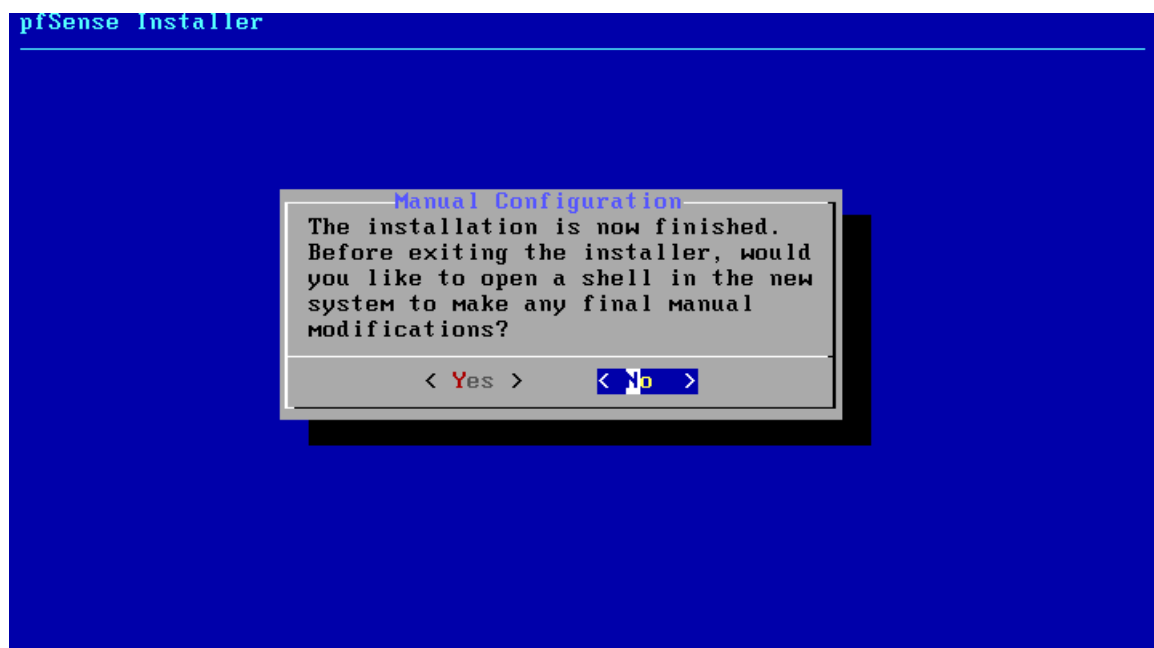
On sélectionne OK.



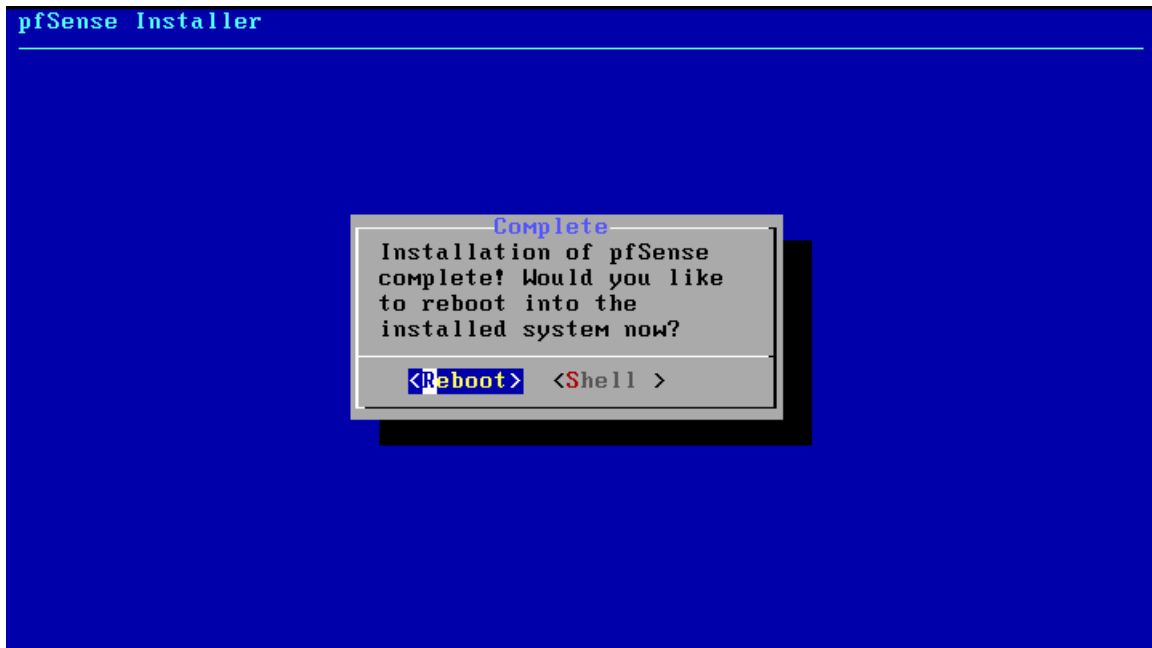
On appuie sur la touche Espace du clavier pour sélectionner le disque ensuite on choisit OK .



On choisit YES pour formater notre disque En mode ZFS.



On sélectionne NO car on a pas des configurations manuelles à faire.



Nous allons faire Reboot pour redémarrer le système.

5.1 Assigner les adresses IP statique sur les interface WAN et LAN

- Choisissez l'option 2 pour configurer

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: f892c96f10e90bfe58c3
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.49/24
                                   v6/DHCP6: 2a01:cb08:c5b:2e00:20c:29ff:fe5d:8f4
a/64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
                                   v6/t6: 2a01:cb08:c5b:2ecc:20c:29ff:fe5d:8f54/6
4

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
```



```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1 - static)

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.49

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):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.254
```

Accédez aux paramètres du WAN en sélectionnant 1 et configurez l'adresse IP en fonction de vos besoins. Assurez-vous de choisir une adresse adaptée à votre réseau et à votre fournisseur d'accès.

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.254

Should this gateway be set as the default gateway? (y/n) y

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
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 192.168.1.49/24

Press <ENTER> to continue.
```

Dans la section IPv6, aucune configuration n'est nécessaire. Vous pouvez laisser les paramètres par défaut.



```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1 - 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:
> 172.16.30.30

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:
> 172.16.30.254
```

Accédez aux paramètres du LAN et configurez l'adresse IP selon vos besoins. Assurez-vous qu'elle soit compatible avec votre réseau local pour une connectivité optimale.

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.16.30.254

Should this gateway be set as the default gateway? (y/n) y

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

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

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

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

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

The IPv4 LAN address has been set to 172.16.30.30/24

Press <ENTER> to continue.
```

Dans la section IPv6, aucune configuration n'est requise. Vous pouvez laisser les paramètres par défaut.



```
8) Shell

Enter an option:

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

VMware Virtual Machine - Netgate Device ID: f892c96f10e90bfe58c3

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

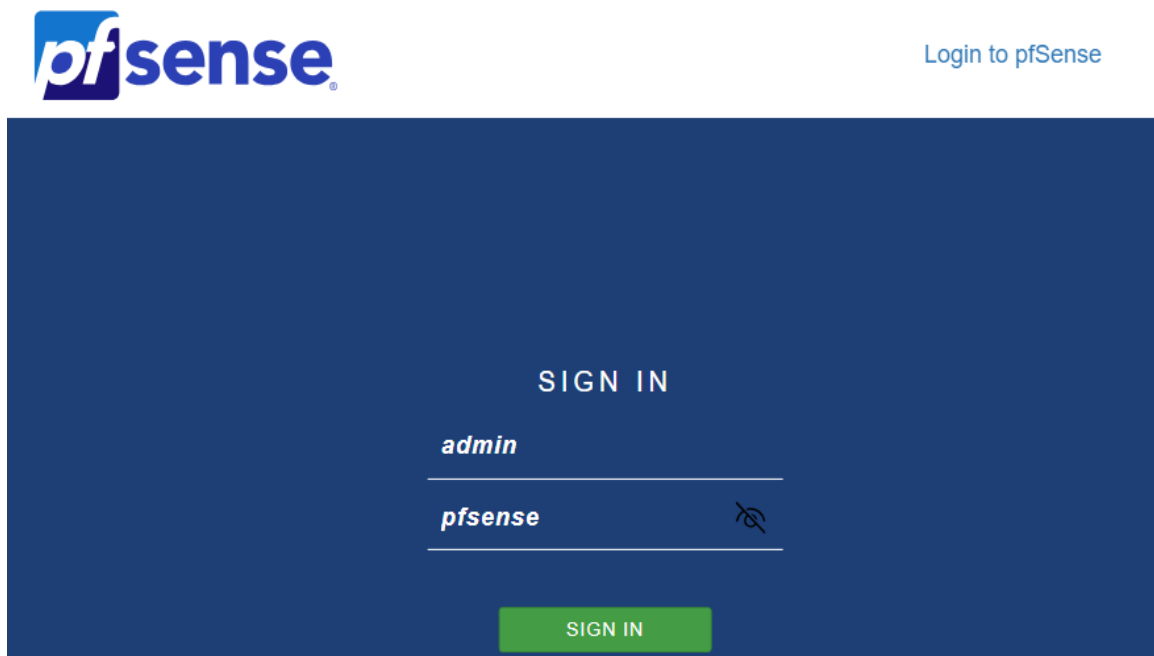
WAN (wan)      -> em0      -> v4: 192.168.1.49/24
LAN (lan)      -> em1      -> v4: 172.16.30.30/24

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: █
```

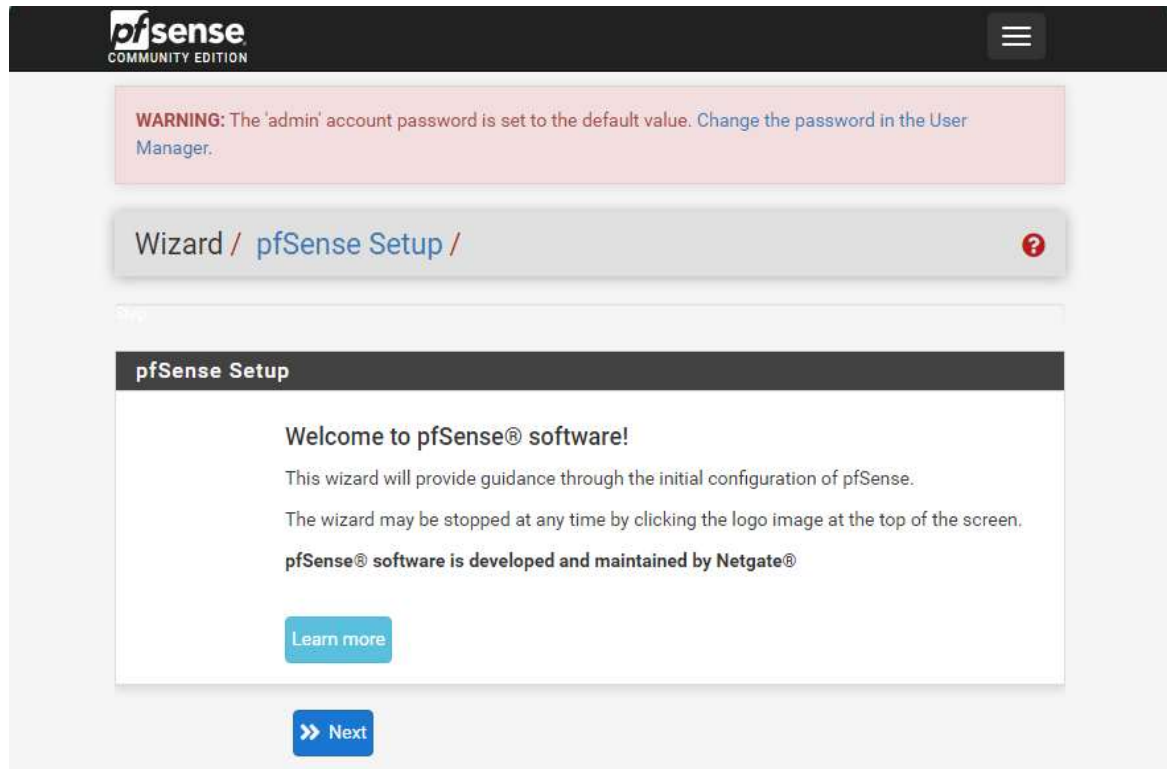
Parfait ! Le **PfSense-1** est maintenant configuré avec les paramètres WAN et LAN selon vos besoins.

5.2. Configuration de PfSense01 via l'interface Web

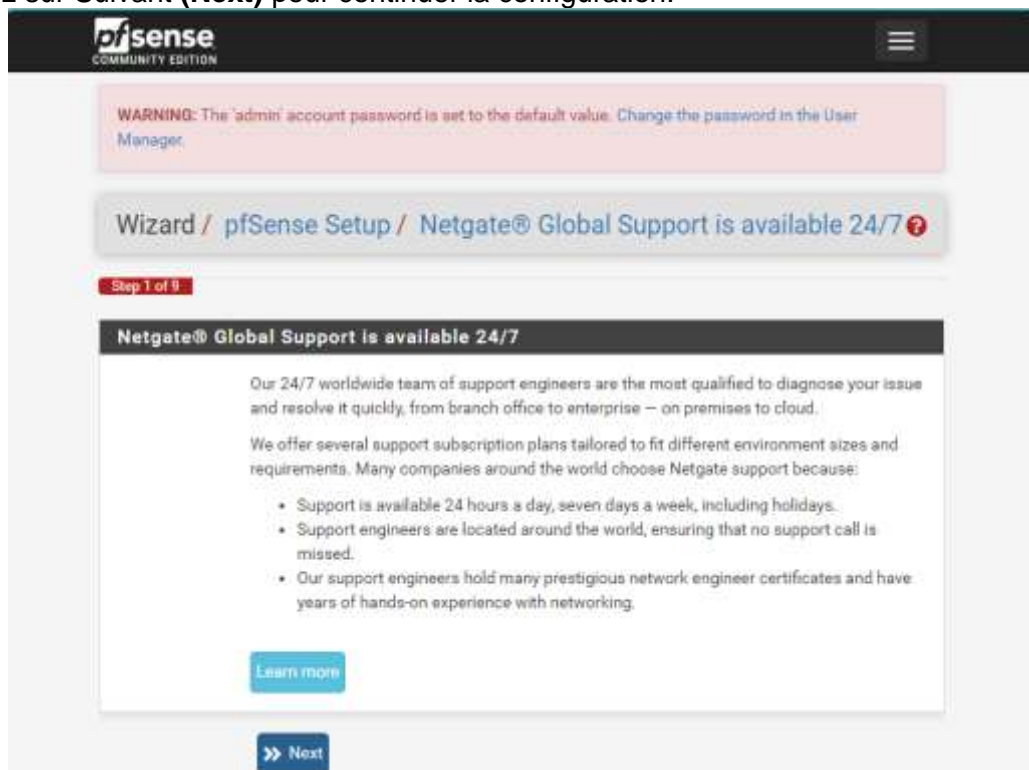


Finalisez la configuration, puis ouvrez votre navigateur Web pour accéder à l'interface de PfSense via son adresse IP.

Connectez-vous en utilisant **admin** comme nom d'utilisateur et **pfsense** comme mot de passe.



Cliquez sur Suivant (**Next**) pour continuer la configuration.



Cliquez également sur **Next** pour poursuivre le processus.



Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
EXAMPLE: myserver

Domain
EXAMPLE: mydomain.com

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](#)

Ici, ce n'est pas obligatoire, mais j'ai choisi de définir **1.1.1.1** comme serveur DNS primaire. Ensuite, cliquez sur **Next** pour continuer.

pfSense
COMMUNITY EDITION ☰

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

Wizard / pfSense Setup / Time Server Information ?

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

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

Timezone

[» Next](#)

Cliquez sur 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

DHCP

General configuration

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 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

Ici, nous allons décocher la case "**Block private networks from entering via WAN**". Ensuite, cliquez sur **Next** pour continuer.



pfSense
COMMUNITY EDITION

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

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

LAN IP Address: 172.16.30.30
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

>> Next

Cliquez sur Next

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

Nous avons changé le mot de passe par défaut de l'admin pour mettre un mot de passe plus sécurisé et cliquer sur NEXT.



Wizard / pfSense Setup / Reload configuration

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload

Cliquez sur Reload.

Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

Check for updates

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

Finish

Cliquez sur Finish

CLUSTER PFSense
Darius ILOKI NZOUSSI



Status / Dashboard



System Information



Name	pfSense.home.arpa
User	admin@172.16.30.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: f892c96f10e90bfe58c3
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE Version 2.7.0 is available. Version information updated at Thu Mar 20 9:30:31 CET 2025

Name	pfSense.home.arpa	Contract type	Community Support Community Support Only									
User	admin@172.16.30.1 (Local Database)	NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES										
System	VMware Virtual Machine Netgate Device ID: f892c96f10e90bfe58c3	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 .										
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020	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.										
Version	2.7.2-RELEASE (amd64) built on Mon Mar 4 20:53:00 CET 2024 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Thu Mar 20 10:07:12 CET 2025	<ul style="list-style-type: none">Upgrade Your SupportCommunity Support ResourcesNetgate Global Support FAQOfficial pfSense Training by NetgateNetgate Professional ServicesVisit Netgate.com										
CPU Type	AMD Ryzen 7 5825U with Radeon Graphics 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	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 validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here .										
Hardware crypto	Inactive	Interfaces										
Kernel PTI	Disabled	<table><tr><td>WAN</td><td>1000baseT <full-duplex></td><td>192.168.1.49</td></tr><tr><td></td><td></td><td>2a01:cb08:c5b:2e00:20c:29ff:fe5d:8f4a</td></tr><tr><td>LAN</td><td>1000baseT <full-duplex></td><td>172.16.30.30</td></tr></table>		WAN	1000baseT <full-duplex>	192.168.1.49			2a01:cb08:c5b:2e00:20c:29ff:fe5d:8f4a	LAN	1000baseT <full-duplex>	172.16.30.30
WAN	1000baseT <full-duplex>	192.168.1.49										
		2a01:cb08:c5b:2e00:20c:29ff:fe5d:8f4a										
LAN	1000baseT <full-duplex>	172.16.30.30										
MDS Mitigation	Inactive											
Uptime	00 Hour 06 Minutes 53 Seconds											
Current date/time	Thu Mar 20 10:12:41 CET 2025											
DNS server(s)	<ul style="list-style-type: none">127.0.0.1192.168.1.12a01:cb08:c5b:2e00:3ab5:c9ff:fe47:2100fe80:3ab5:c9ff:fe47:21001.1.1.1											
Last config change	Thu Mar 20 10:06:46 CET 2025											



- Pour **PfSense-2**, procédez de la même manière :

```
VMware Virtual Machine - Netgate Device ID: 92296faeba122ebdff18

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.50/24
                                v6/DHCP6: 2a01:cb08:c5b:2e00:20c:29ff:fee2:33f
0/64
LAN (lan)      -> em1      -> v4: 172.16.30.15/24

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:
Message from syslogd@pfSense at Mar 20 10:52:54 ...
php-fpm[27861]: /index.php: Successful login for user 'admin' from: 172.16.30.1 (
Local Database)
```

System Information

Name	pfSense.home.arpa
User	admin@172.16.30.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 92296faeba122ebdff18
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Mon Mar 4 20:53:00 CET 2024 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Thu Mar 20 10:52:49 CET 2025
CPU Type	AMD Ryzen 7 5825U with Radeon Graphics AES-NI CPU Crypto: Yes (Inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 03 Minutes 37 Seconds
Current date/time	Thu Mar 20 10:54:45 CET 2025
DNS server(s)	<ul style="list-style-type: none">127.0.0.1192.168.1.12a01:cb08:c5b:2e00:3ab5:c9ff:fe47:2100fe80:3ab5:c9ff:fe47:21001.1.1.1
Last config	Thu Mar 20 10:52:18 CET 2025

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

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 validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).

Interfaces

WAN	1000baseT <full-duplex>	192.168.1.50 2a01:cb08:c5b:2e00:20c:29ff:fee2:33f0
LAN	1000baseT <full-duplex>	172.16.30.15

CLUSTER PFSense

Darius ILOKI NZOUSSI



Une fois la configuration terminée, vous aurez **PfSense-1** et **PfSense-2** prêts à l'emploi, chacun configuré selon vos préférences. Vous pouvez maintenant gérer vos deux pare-feux et réseaux depuis leur interface respective pour assurer la sécurité et l'optimisation de votre réseau.

5.3 Configurer un cluster de 2 PfSense redondants (Failover)

pour garantir une haute disponibilité et une continuité de service en cas de défaillance.

5.3.1 Principe de fonctionnement

PfSense communique sur les réseaux LAN et WAN en utilisant ses adresses IP virtuelles, et non l'adresse IP assignée à ses interfaces physiques. En cas de défaillance de **PfSense01** (le primaire), **PfSense02** (le secondaire) prend automatiquement le relais, sans aucune interruption de service. Cette bascule est totalement transparente pour le réseau.

Pour garantir une réplication efficace de **PfSense01** vers **PfSense02**, trois éléments doivent être configurés :

❖ CARP (Common Address Redundancy Protocol)

CARP permet à plusieurs hôtes d'un même réseau de partager une adresse IP. Ici, il est utilisé pour partager à la fois l'adresse IP **WAN** et l'adresse IP **LAN** entre les deux serveurs **PfSense**. Cette adresse IP virtuelle sera utilisée pour la communication réseau. En cas de défaillance de **PfSense01**, **PfSense02** prend automatiquement le relais, récupérant l'adresse IP virtuelle et maintenant la continuité des services sans interruption.

❖ 2. Pfsync

Pfsync est un protocole qui permet de synchroniser l'état des connexions entre deux serveurs **PfSense**. Cela garantit que, même en cas de défaillance du serveur primaire, les connexions en cours sont maintenues sur le serveur secondaire, évitant ainsi toute coupure dans le service. Il est recommandé d'utiliser un lien dédié pour cette synchronisation, bien que le lien **LAN** puisse également être utilisé. La réplication peut être effectuée du serveur primaire vers un ou plusieurs serveurs secondaires.

❖ 3. XML-RPC

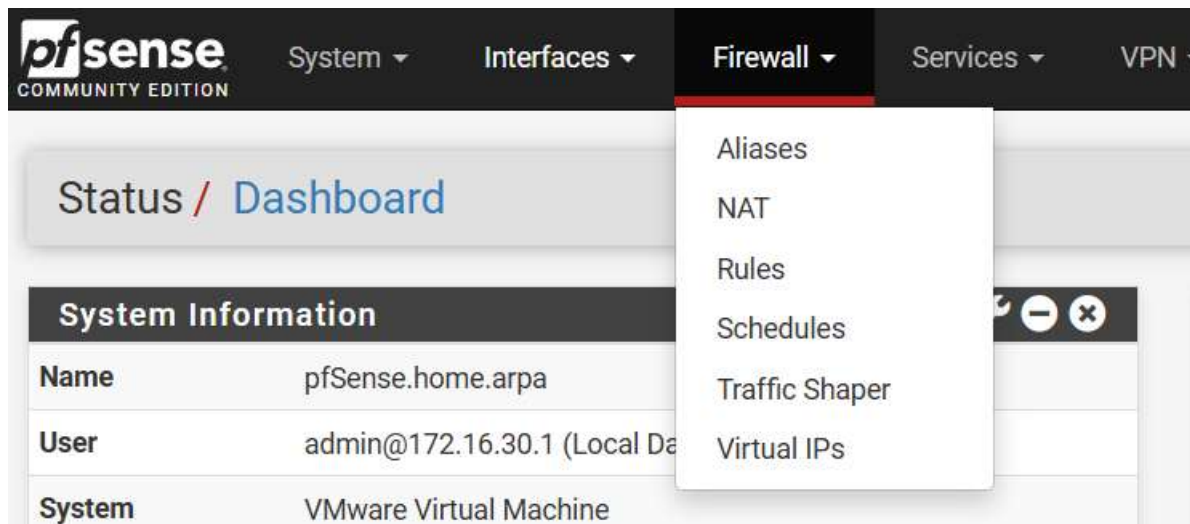
XML-RPC est un protocole utilisé pour répliquer les données de configuration d'un serveur à un autre. Dans **PfSense**, il est utilisé pour répliquer la configuration de **PfSense01** vers **PfSense02**, assurant ainsi que les paramètres et configurations sont identiques entre les deux serveurs pour un basculement sans erreur.

Avec cette configuration, le cluster PfSense redondant garantit une haute disponibilité et une récupération rapide en cas de panne, assurant une continuité des services sans interruption pour les utilisateurs finaux.



5.3.2 Configurer les adresses IP virtuelles

Pour que tout fonctionne correctement, chaque serveur **PfSense** doit avoir une adresse IP sur son interface ainsi qu'une adresse IP virtuelle partagée entre les deux serveurs **PfSense**. Ainsi, chaque réseau nécessite 3 adresses IP.



Pour configurer l'adresse IP virtuelle, rendez-vous dans "**Firewall**" > "**Virtual IPs**".

Cliquez sur l'icône "**+ Add**" pour ajouter une nouvelle adresse IP virtuelle.

- ✓ Sélectionnez **CARP** dans le champ **Type**.



- ✓ **Adresse** : Entrez l'adresse VIP (par exemple **192.168.1.254**) et le masque de sous-réseau **/24**.
- ✓ **Virtual IP Password** : Choisissez un mot de passe pour sécuriser les échanges au sein du groupe partageant la VIP.
- ✓ **VHID Groupe** : Attribuez le groupe **1**.
- ✓ **Advertising frequency** : Laissez **BASE** à **1** et **SKEW** à **0**.
- ✓ **Description** : Entrez une description, comme "**CARP WAN**".
- ✓ Cliquez ensuite sur **Save** pour sauvegarder la configuration.

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface: LAN

Address type: Single address

Address(es): 172.16.30.254 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password:
Enter the VHID group password. Confirm

VHID Group: 2
Enter the VHID group that the machines will share.

Advertising frequency: Base: 1 Skew: 100
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

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

Faites la même chose pour le **LAN** en remplaçant l'adresse par **172.16.30.254 /24**.

- ✓ Remplacez **VHID Group** par **2**.
- ✓ Dans la **Description**, changez-la en "**CARP LAN**".
- ✓ Cliquez ensuite sur **Save** pour enregistrer la configuration.

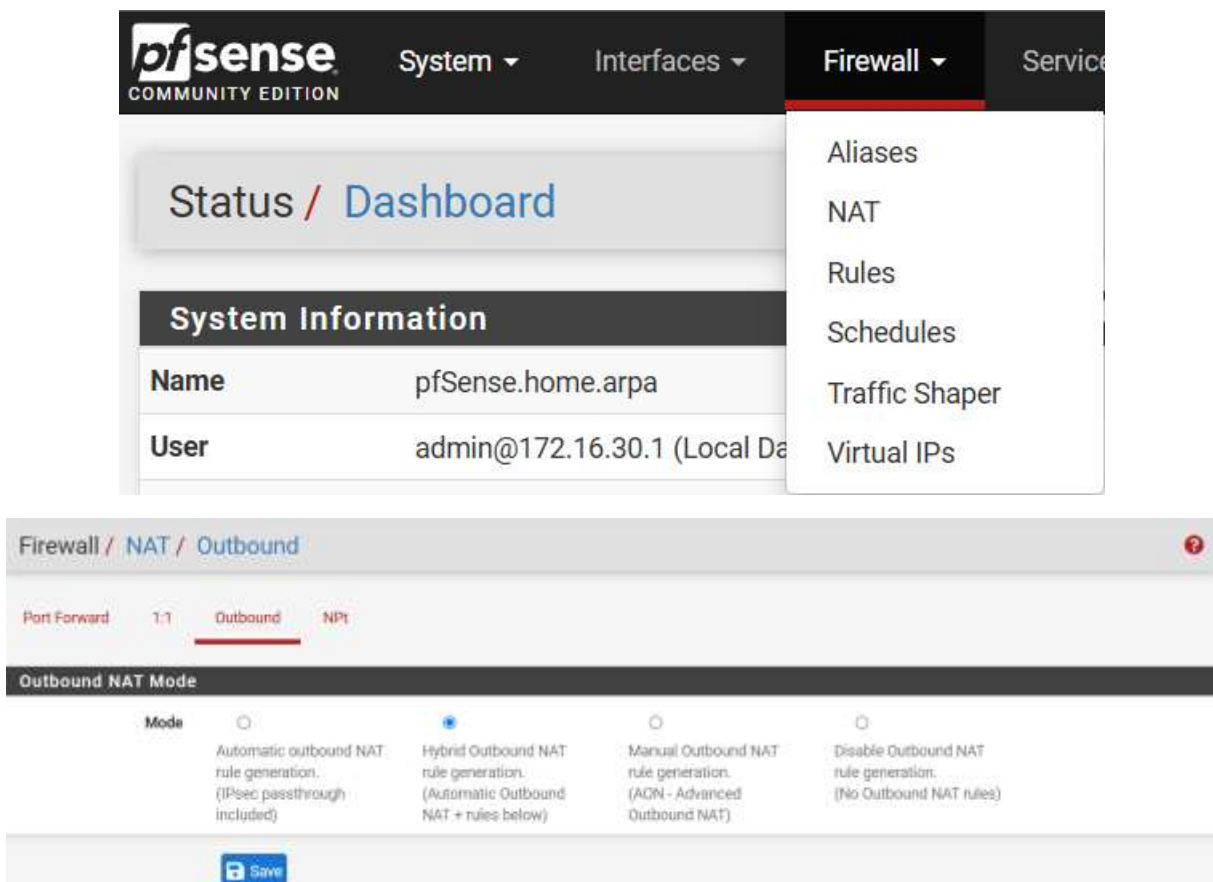


Firewall / Virtual IPs				
Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.1.254/24 (vhid: 1)	WAN	CARP	CARP WAN	 
172.16.30.254/24 (vhid: 2)	LAN	CARP	CARP LAN	 
				

Super ! Si tout a été configuré correctement, vous devriez maintenant voir les adresses IP virtuelles configurées pour le **WAN** et le **LAN** avec les paramètres appropriés pour chaque interface **PfSense**. Les adresses IP devraient être partagées entre **PfSense-1** et **PfSense-2**, et le basculement devrait être fonctionnel en cas de défaillance de l'un des serveurs.

5.3.3 Configuration du NAT (Network Address Translation)

Pour configurer le **NAT** sur **PfSense**, nous allons permettre la traduction d'adresses réseau afin de permettre la communication entre les machines internes et l'extérieur, tout en gardant un certain niveau de sécurité.



The screenshot shows the PfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', and 'Services'. The 'Firewall' menu is open, showing options like 'Aliases', 'NAT', 'Rules', 'Schedules', 'Traffic Shaper', and 'Virtual IPs'. The 'NAT' menu item is selected, leading to the 'Outbound' tab. The 'Outbound NAT Mode' section displays four radio button options: 'Automatic outbound NAT rule generation. (IPsec passthrough included)', 'Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)' (which is selected), 'Manual Outbound NAT rule generation. (AGN - Advanced Outbound NAT)', and 'Disable Outbound NAT rule generation. (No Outbound NAT rules)'. A 'Save' button is visible at the bottom of the configuration area.

Nous allons dans le menu **Firewall > NAT**. Ensuite, dans l'onglet **Outbound**, nous cochons la case "**Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + <below>)**".



Nous modifions les règles ou ajoutons une nouvelle règle pour que le trafic sortant utilise l'adresse **VIP**. Voici les paramètres à configurer :

I. Edit Advanced Outbound NAT Entry

- ✓ **Disabled** : Ne pas cocher cette case.
- ✓ **Do not NAT** : Ne pas cocher cette case.
- ✓ **Interface** : Sélectionnez l'interface sur laquelle vous souhaitez appliquer cette règle NAT, dans notre cas, choisissez "**WAN**".
- ✓ **Address Family** : Sélectionnez "**IPv4**".
- ✓ **Protocol** : Choisissez "**any**".
- ✓ **Source** : Choisissez "**NETWORK**" et saisissez "**192.168.1.0/24**".
- ✓ **Port** : Laissez ce champ vide.
- ✓ **Destination** : Choisissez "**any**" et laissez ce champ vide.

II. Translation

- ✓ **Adresse** : Choisissez **192.168.1.254** (l'adresse **CARP WAN**).
- ✓ **Port or Range** : Laissez ce champ vide.

III. Misc

- ✓ Laissez cette section vide.
- ✓ **No XMLRPC Sync** : Ne pas cocher cette case pour éviter que cette règle ne soit copiée sur le **PfSense** secondaire. Laissez cette case **non cochée**.

Enfin, cliquez sur **Save** pour enregistrer la règle.

Firewall / NAT / Outbound / Edit

Edit Advanced Outbound NAT Entry

Disabled ☐ Disable this rule

Do not NAT ☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.

Interface
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

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

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

Source /
Type: Source network for the outbound NAT mapping. Port or Range

Destination /
Type: Destination network for the outbound NAT mapping. Port or Range

☐ Not
Invert the sense of the destination match.



Translation

Address

192.168.1.254 (CARP WAN)

Type

Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

Port or Range

☐ Static Port

Enter the external source Port or Range used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by "-".
Leave blank when Static Port is checked.

Misc

No XMLRPC Sync

☐

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

Description

Utilisation de l'adresse VIP sur le WAN

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

Rule Information

Created

3/20/25 11:43:31 by admin@172.16.30.1 (Local Database)

Updated

3/20/25 13:15:55 by admin@172.16.30.1 (Local Database)

Save

Firewall / NAT / Outbound

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

Port Forward

1:1

Outbound

NAT

Outbound NAT Mode

Mode

☐ Automatic outbound NAT rule generation, (IPsec passthrough included)

☒ Hybrid Outbound NAT rule generation, (Automatic Outbound NAT + rules below)

☐ Manual Outbound NAT rule generation, (AON - Advanced Outbound NAT)

☐ Disable Outbound NAT rule generation, (No Outbound NAT rules)

Save

Mappings

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	192.168.1.0/24	*	*	192.168.1.254 (CARP WAN)	*	<input checked="" type="checkbox"/>	Utilisation de l'adresse VIP sur le WAN	<div><div></div><div></div><div></div><div></div><div></div></div>

↑ Add

↓ Add

Delete

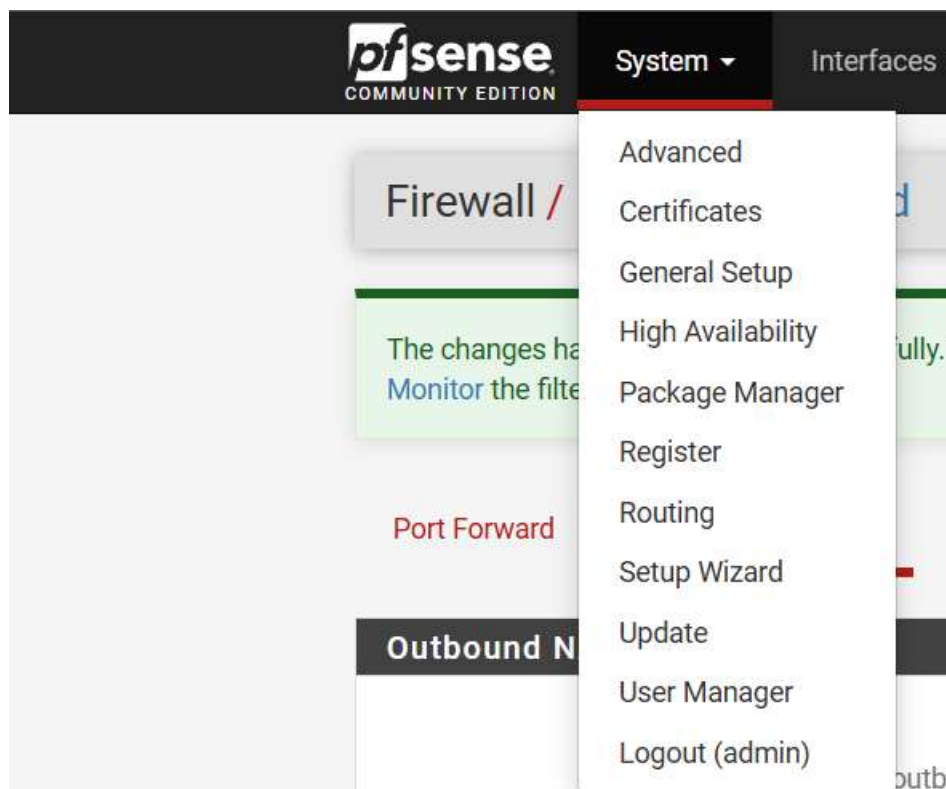
Toggle

Save



5.3.4 Configuration de la Haute Disponibilité

Il ne reste plus qu'à configurer la **haute disponibilité**. Pour cela, accédez à "**System**" > "**High Availability**".



Depuis cette page, deux éléments doivent être configurés : **Pfsync** (pour la synchronisation des états) et **XMLRPC Sync** (pour la synchronisation de la configuration).

❖ State Synchronization Settings (Pfsync)

- ✓ **Synchronize states** : Cochez cette case pour activer la synchronisation des états (à configurer sur **PfSense-1** et **PfSense-2**).
- ✓ **Synchronize Interface** : Sélectionnez l'interface de synchronisation, ici "**LAN**".
- ✓ **pfsync Synchronize Peer IP** : Saisissez **172.16.30.30**.

❖ Configuration Synchronization Settings (XMLRPC Sync)

- ✓ **Synchronize Config to IP** : Entrez **172.16.30.30**.
- ✓ **Remote System Username** : Sur **PfSense-1** (primaire), saisissez l'identifiant utilisé pour se connecter au WebGUI de **PfSense-2** ("**admin**" par défaut). Ce champ doit rester vide sur **PfSense-2** (secondaire).
- ✓ **Remote System Password** : Sur **PfSense-1**, saisissez le mot de passe de connexion au WebGUI de **PfSense-2** ("**admin**" par défaut). Ce champ doit rester vide sur **PfSense-2**.
- ✓ **Synchronize admin** : Cochez cette case.
- ✓ **Select options to sync** : Cochez toutes les cases pour synchroniser l'ensemble des paramètres.

Enfin, cliquez sur **Save** pour valider la configuration.



State Synchronization Settings (pfsync)

Synchronize states

☒ pfsync transfers state insertion, update, and deletion messages between firewalls.

Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.

This setting should be enabled on all members of a failover group.

Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface

LAN

If Synchronize States is enabled this interface will be used for communication.

It is recommended to set this to an interface other than LAN! A dedicated interface works the best.

An IP must be defined on each machine participating in this failover group.

An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID

2etdfffffa

Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.

Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).

Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer

IP

172.16.30.30

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

172.16.30.30

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!

Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System

Username

admin

Enter the webConfigurator username of the system entered above for synchronizing the configuration.

Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System

Password

Enter the webConfigurator password of the system entered above for synchronizing the configuration.

Do not use the Synchronize Config to IP and password option on backup cluster members!

Confirm



Synchronize admin ☒ synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

- ☒ User manager users and groups
- ☒ Authentication servers (e.g. LDAP, RADIUS)
- ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☒ Firewall rules
- ☒ Firewall schedules
- ☒ Firewall aliases
- ☒ NAT configuration
- ☒ IPsec configuration
- ☒ OpenVPN configuration (implies CA/Cert/CRL Sync)
- ☒ DHCP Server settings
- ☒ DHCP Relay settings
- ☒ DHCPv6 Relay settings
- ☒ WoL Server settings
- ☒ Static Route configuration
- ☒ Virtual IPs
- ☒ Traffic Shaper configuration
- ☒ Traffic Shaper Limiters configuration
- ☒ DNS Forwarder and DNS Resolver configurations
- ☒ Captive Portal

☒ Toggle All

5.3.5 Autorisation des flux de réplication dans les règles du firewall

Accédez à **"Firewall" > "Aliases"** pour configurer les autorisations de réplication.

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ **Firewall ▾** Services ▾

System / High Availability

State Synchronization Settings (pfsync)

Synchronize states ☒ pfsync transfers
Each firewall sends
interface for similar

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

and deletion
multicast c
walls. and

Ensuite, allez dans l'onglet **"IP"**, puis cliquez sur **"Add"** pour ajouter une nouvelle entrée.



Firewall / Aliases / Edit



Properties

Name

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

Description

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

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

Entry added Thu, 20 Mar 2025 13



Delete

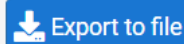
Entry added Thu, 20 Mar 2025 13



Delete



Save



Export to file



Add Host

- ✓ **Name** : Saisissez "**Cluster**".
- ✓ **Type** : Sélectionnez "**Host**".
- ✓ **IP or FQDN** : Renseignez **192.168.1.49** et **192.168.1.50**.

Cliquez sur **Save** pour enregistrer la configuration.

Firewall / Aliases / IP



IP Ports URLs All

Firewall Aliases IP

Name	Type	Values	Description	Actions
cluster	Host(s)	172.16.1.49, 172.16.1.50		

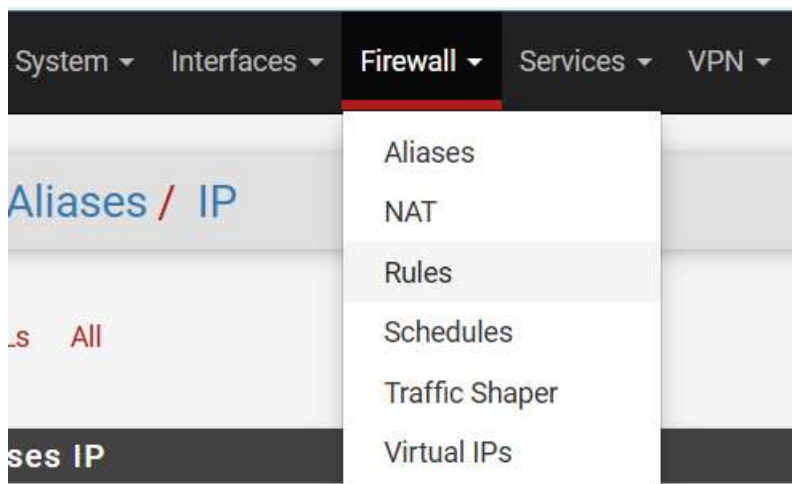
Add Import



Il ne reste plus qu'à **autoriser les flux de réplication** sur les firewalls.

- ✓ Accédez à "**Firewall**" > "**Rules**".
- ✓ Si la réplication s'effectue via l'interface **LAN**, appliquez les règles sur cette interface.
- ✓ Si une **interface dédiée** est utilisée pour la synchronisation, appliquez les règles sur cette interface.

Cela garantit une communication fluide et sécurisée entre **PfSense-1** et **PfSense-2**



- ✓ Accédez à l'onglet **LAN**.
- ✓ Cliquez sur "**Add**" pour ajouter une nouvelle règle.

I. Configuration de la règle Firewall pour HTTPS

❖ Edit Firewall Rule

- ✓ **Action** : Sélectionnez "**Pass**".
- ✓ **Disabled** : Ne pas cocher cette case.
- ✓ **Interface** : Choisissez **LAN**.
- ✓ **Address Family** : Sélectionnez **IPV4**.
- ✓ **Protocol** : Choisissez **TCP**.
- **Source**
- ✓ **Source** : Ne pas cocher cette case, sélectionnez "**Single host or alias**", puis entrez **Cluster**.
- **Destination**
- ✓ **Destination** : Ne pas cocher cette case, sélectionnez "**This Firewall (self)**".
- **Destination Port Range** :
- ✓ **From** : Choisissez **HTTPS (443)**.
- ✓ **To** : Choisissez **HTTPS (443)**.
- ✓ **Custom** : Ne rien modifier.
- **Extra Options**
- ✓ **Log** : Ne pas cocher cette case.
- ✓ **Description** : Entrez "**Autorisation des flux HTTPS pour la réplication**".

Cliquez sur **SAVE**.



II. Configuration de la règle Firewall pour PFSYNC

❖ Edit Firewall Rule

- ✓ **Action** : Sélectionnez **"Pass"**.
- ✓ **Disabled** : Ne pas cocher cette case.
- ✓ **Interface** : Choisissez **LAN**.
- ✓ **Address Family** : Sélectionnez **IPV4**.
- ✓ **Protocol** : Choisissez **PFSYNC**.
- **Source**
- ✓ **Source** : Ne pas cocher cette case, sélectionnez **"Single host or alias"**, puis entrez **Cluster**.
- **Destination**
- ✓ **Destination** : Ne pas cocher cette case, sélectionnez **"This Firewall (self)"**.
- **Extra Options**
- ✓ **Log** : Ne pas cocher cette case.
- ✓ **Description** : Entrez **"Autorisation des flux PFSYNC pour la réplication"**.

Cliquez sur **SAVE**.

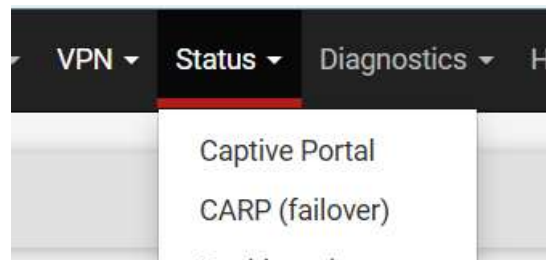
Firewall / Rules / LAN											
Floating WAN LAN											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3/189 KB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 PFSYNC	cluster	*	This Firewall (self)	*	*	none		Autorisation flux pfsync pour la replication	
<input type="checkbox"/>	0/0 B	IPv4 TCP	cluster	*	This Firewall (self)	443 (HTTPS)	*	none		Autorisation flux https pour la replication	
<input type="checkbox"/>	19/130 KB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
Add Add Delete Toggle Copy Save Separator											



5.3.6 Vérification du bon fonctionnement de la haute disponibilité

❖ Vérification du statut du CARP (adresse VIP)

Nous pouvons vérifier l'état de nos adresses **IP virtuelles** depuis le menu "**Status**" > "**CARP (failover)**". Cela nous permettra de voir si la réplication et le basculement fonctionnent correctement entre **PfSense-1** et **PfSense-2**.



Les adresses **VIP** doivent avoir le statut "**MASTER**" sur **PfSense-2** (primaire) et "**BACKUP**" sur **PfSense-1** (secondaire). Cela indique que le **PfSense-2** est actuellement actif pour gérer le trafic, tandis que **PfSense-1** est prêt à prendre le relais en cas de défaillance.

❖ PfSense-2

172.16.30.15

System Interfaces Firewall Services VPN Status Diagnostics Help

Status / CARP

CARP Maintenance

Temporarily Disable CARP Enter Persistent CARP Maintenance Mode

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
WAN@1	192.168.1.254/24	CARP WAN	MASTER
LAN@2	172.16.30.254/24	CARP LAN	MASTER

State Synchronization Status

State Creator Host IDs:

- 2ebdff18 (This node)

When state synchronization is enabled and functioning properly the list of state creator host IDs will be identical on each node participating in state synchronization.

The state creator host ID for this node can be set to a custom value under System > High Avail Sync. If the state creator host ID has recently changed, the old ID will remain until all states using the old ID expire or are removed.



❖ PfSense-1

The screenshot shows the PfSense-1 web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Status / CARP". Below this, there is a "CARP Maintenance" section with two buttons: "Temporarily Disable CARP" and "Enter Persistent CARP Maintenance Mode". The "CARP Status" section contains a table with the following data:

Interface and VHID	Virtual IP Address	Description	Status
WAN@1	192.168.1.254/24	CARP WAN	BACKUP
LAN@2	172.16.30.254/24	CARP LAN	BACKUP

Below the table is the "State Synchronization Status" section, which shows the "State Creator Host IDs" as "bfe58c3 (This node)". A blue box contains information about state synchronization, stating that the list of state creator host IDs will be identical on each node participating in state synchronization. It also mentions that the state creator host ID can be set to a custom value under System > High Avail Sync.

❖ PfSense-2 éteint et PfSense-1 allumé

The screenshot shows the PfSense-1 web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Status / CARP". Below this, there is a "CARP Maintenance" section with two buttons: "Temporarily Disable CARP" and "Enter Persistent CARP Maintenance Mode". The "CARP Status" section contains a table with the following data:

Interface and VHID	Virtual IP Address	Description	Status
WAN@1	192.168.1.254/24	CARP WAN	MASTER
LAN@2	172.16.30.254/24	CARP LAN	MASTER

Below the table is the "State Synchronization Status" section, which shows the "State Creator Host IDs" as "bfe58c3 (This node)".



Exactement ! Si **PfSense-2** est éteint, **PfSense-1** prendra automatiquement le relais en tant que serveur actif. Le statut de l'adresse **VIP** sur **PfSense-1** passera en "**MASTER**", ce qui signifie qu'il gère le trafic réseau. En revanche, **PfSense-2** restera en "**BACKUP**" jusqu'à ce qu'il soit réactivé et que la synchronisation des états et de la configuration reprenne.

8. CONCLUSION