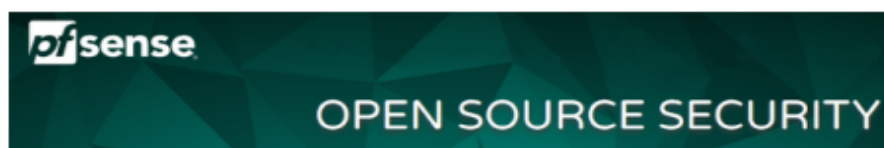


Installation PFSENSE

Tutoriel pour le déploiement de pfSense, solution de pare-feu openSource

PfSense est une solution de **pare-feu (Firewall) openSource** basée sur le système d'exploitation FreeBSD. Dans le cadre de cet article, nous vous proposons un tutoriel qui présente le déploiement d'un firewall pour sécuriser les accès internet d'une entreprise.



Historiquement, pfSense est un fork de mOnOWall. Il offre une solution de firewall complète pour les entreprises :

- Gestion des interfaces réseau
- Filtrage
- NAT
- Gestion des accès internet
- Services VPN (IPSEC, SSL, ...)
- Qualité de Service
- Gestion des VLAN
- Serveur DHCP
- Serveur DNS
- Portail Captif
- Solution proxy
- Filtrage d'urls
- Antivirus sur certains flux

Certilience propose des formations pfSense depuis Septembre 2013. Cette formation est l'occasion pour les participants d'aborder l'ensemble des briques de cette solution Firewall complète et de les mettre en pratique directement.

Avec à son actif plus de 2500 boitiers déployés sous cette technologie, Certilience dispose d'une solide expérience dans cet environnement et peut ainsi répondre aux questions de tous les utilisateurs.

La distribution peut s'installer directement depuis une image ISO disponible sur pfsense.org.

Pfsense peut s'installer sur plusieurs types de hardware. La configuration minimum recommandée par Certilience :

- CPU : 1Ghz
- RAM 1 Go
- Disque : 1Go

Installation

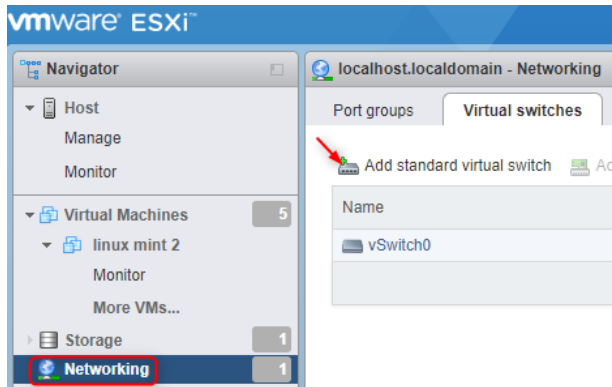
Pour procéder à l'installation de pfSense, il est nécessaire dans un premier temps de télécharger la distribution :

- Au format ISO
- Au format clef USB

En fonction de l'architecture de votre processeur, il faudra utiliser la bonne version de la distribution. Après avoir préparé votre média, vous pouvez démarrer dessus et débiter la configuration :

2 cartes réseaux obligatoires pour l'installation

Sur VMWARE ESXI

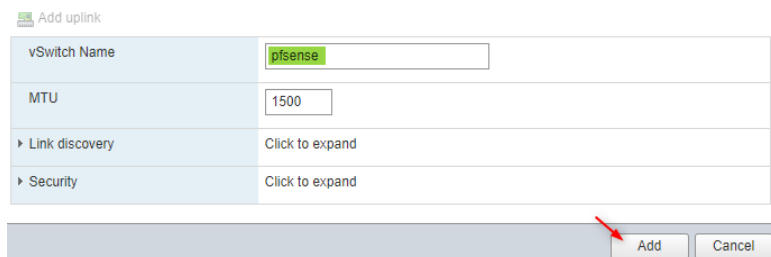


Sélectionner **Networking**

Ensuite cliquer sur **Add standard Virtual switch**

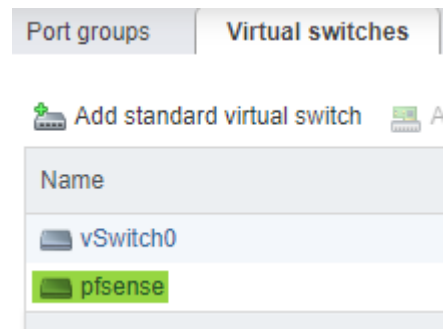
Il faudra créer une deuxième carte réseaux

1) Nommer, le nom de votre carte réseaux

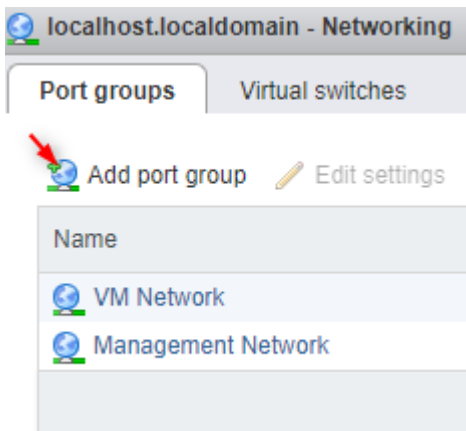


2) La carte réseaux a été

bien créer

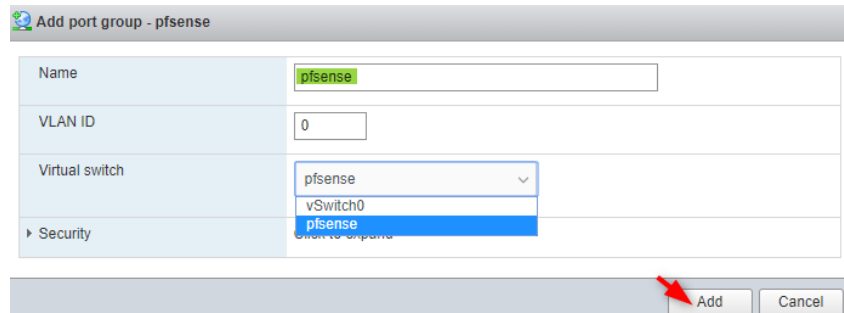


3) Il faut maintenant l'ajouter dans le groupe de Port



4) Nommer le nom de votre carte de nouveau, puis sur

Virtual switch sélectionner le nom de votre carte réseau



Pour l'installation il faut **Créer une VM -> système exploitation -> other -> Free BSD 12 ou version ultérieure** -> sélectionner votre ISO

Lors de l'installation de PFSENSE assurer d'avoir cette configuration

Edit settings - pfsense (ESXi 6.7 virtual machine)

Virtual Hardware VM Options

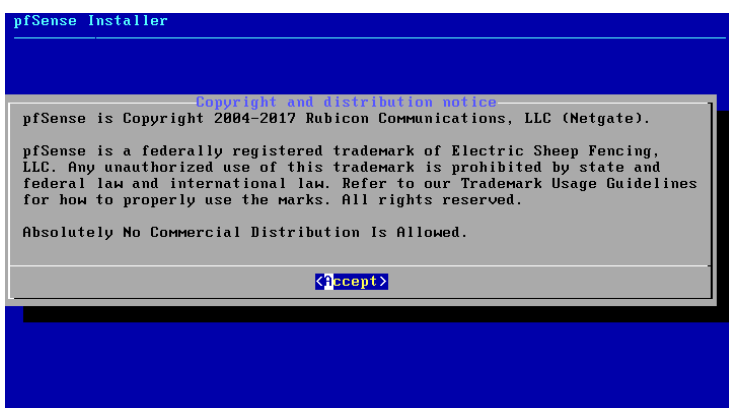
Add hard disk Add network adapter Add other device

CPU	1	
Memory	1024	MB
Hard disk 1	8	GB
SCSI Controller 0	LSI Logic SAS	
SATA Controller 0		
USB controller 1	USB 2.0	
Network Adapter 1	VM Network	Wan
Status	<input checked="" type="checkbox"/> Connect at power on	
Adapter Type	E1000e	
MAC Address	Automatic	00:0c:29:f2:85:0e
Network Adapter 2	pfsense	Lan
Status	<input checked="" type="checkbox"/> Connect at power on	
Adapter Type	VMXNET 3	
MAC Address	Automatic	00:0c:29:f2:85:18
CD/DVD Drive 1	Datastore ISO file	<input type="checkbox"/> Connect
Status	<input checked="" type="checkbox"/> Connect at power on	
CD/DVD Media	[datastore1] pfSense-CE-2.4.4-RELEASE-amd64.iso	<input type="button" value="Browse..."/>
Controller location	SATA controller 0	SATA (0:0)
Video Card	Default settings	

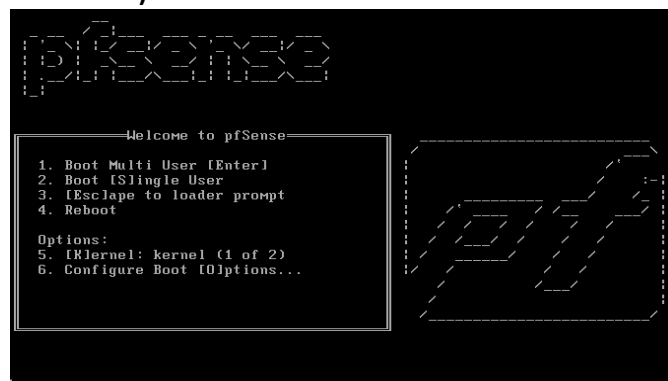
Installation PFSENSE

- Avec les flèches clavier, cherchez : **French ISO-8859-1**
- Appuyez sur **Entrée** pour valider le choix
- Montez d'un cran pour sélectionnez **Continue with fr.iso.kbd keymap** et Entrée
- **Partitioning : Auto (UFS) : Entrée**
- **Manual Configuration**, laissez sur **No : Entrée**
- **Complete, Reboot : Entrée**
- Dans la foulée, menu **Périphériques > Lecteurs optiques > Ejecter le disque du lecteur virtuel**
- Menu : **Machine > Redémarrage**

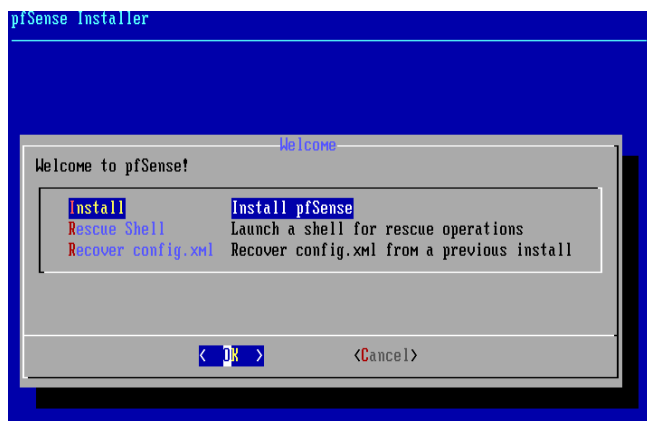
1)



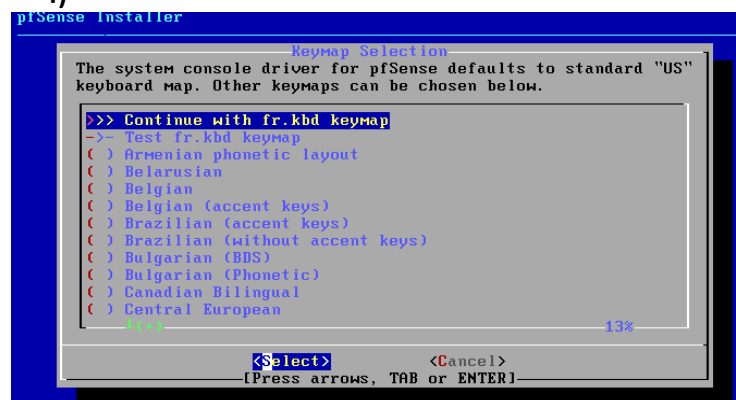
2)



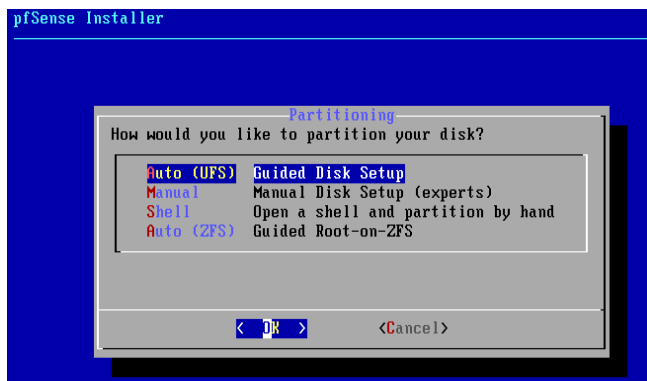
3)



4)



5)



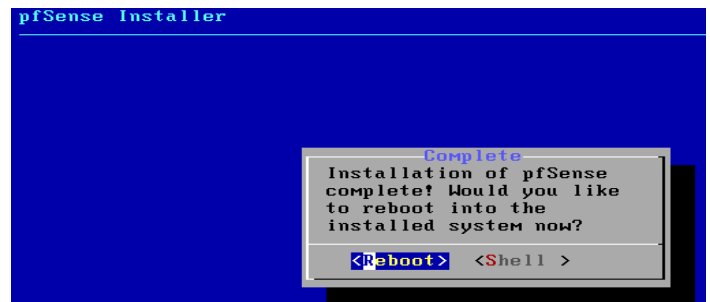
6)



7)



8)



9)

```
Structured Extended Features3=0xbc000000<IBPB,STIBP,ARCH_CAP,SSBD>
IA32_ARCH_CAPS=0xc
TSC: P-state invariant
Hypervisor: Origin = "VMwareVMware"
Done.
..... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration.....done.
Warning: Configuration references interfaces that do not exist: em1

Network interface mismatch -- Running interface assignment option.
vmx0: link state changed to UP

Valid interfaces are:
em0      00:0c:29:f2:85:8e  (up) Intel(R) PRO/1000 Network Connection 7.6.1-k
vmx0     00:0c:29:f2:85:18  (down) VMware VMXNET3 Ethernet Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required
Should VLANs be set up now [y/n]?
```

n

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

Enter the WAN interface name or 'a' for auto-detection
(em0 vmx0 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vmx0 a or nothing if finished): vmx0
```

Configurer votre carte WAN et LAN

```
The interfaces will be assigned as follows:
WAN -> em0
LAN -> vmx0

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

y

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.4-RELEASE amd64 Thu Sep 20 09:03:12 EDT 2018
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 43aeb27eda88a821dd9d

*** Welcome to pfSense 2.4.4-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.2.17/24
LAN (lan)     -> vmx0         -> 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: 
```

Maintenant, il faudra se connecter avec IP de votre Lan

Comme machine client j'utiliserai Windows 10, je vais utiliser qu'une seule carte réseaux sa sera le LAN du PFSENSE

Network Adapter 1	pfsense	Lan
Status	<input checked="" type="checkbox"/> Connect at power on	
Adapter Type	VMXNET 3	
MAC Address	Automatic	00:0c:29:95:bd:6b

Lancer la machine

Mettez IP du Lan PFSENSE sur votre URL de navigateur web

Not secure | 192.168.1.1



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Hide advanced

Back to safety

This server could not prove that it is **192.168.1.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.1.1 \(unsafe\)](#)



Login to pfSense

SIGN IN

admin

.....

SIGN IN

identifiant : admin

mdp : admin

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

Wizard / pfSense Setup /

pfSense Setup

Welcome to pfSense® software!
This wizard will provide guidance through the initial configuration of pfSense.
The wizard may be stopped at any time by clicking the logo image at the top of the screen.
pfSense® software is developed and maintained by Netgate®

Learn more

Next

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.
We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

Learn more

Next

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

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

Static IP Configuration	
IP Address	<input type="text"/>
Subnet Mask	<input type="text" value="32"/>
Upstream Gateway	<input type="text"/>
DHCP client configuration	
DHCP Hostname	<input type="text"/>
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	<input type="text"/>
PPPoE Password	<input type="text"/>
Show PPPoE password	<input type="checkbox"/> Reveal password characters
PPPoE Service name	<input type="text"/>
Hint: this field can usually be left empty	
PPPoE Dial on demand	<input type="checkbox"/> 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 configuration	
PPTP Username	<input type="text"/>
PPTP Password	<input type="text"/>
Show PPTP password	<input type="checkbox"/> Reveal password characters
PPTP Local IP Address	<input type="text"/>
pptplocalsubnet	<input type="text" value="32"/>
PPTP Remote IP Address	<input type="text"/>
PPTP Dial on demand	<input type="checkbox"/> 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 type="text"/>
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	<input type="checkbox"/> 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	<input type="checkbox"/> 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.	
 <input type="button" value="» Next"/>	

Décocher ces 2 case

Step 4 of 9

Configure WAN Interface

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

SelectedType

General configuration

MAC Address

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

MTU

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

MSS

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

Step 5 of 9

Configure LAN Interface

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

LAN IP Address

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

 Next

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

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

 Reload

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.

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

Copyright © 2004-2018. Electric Sheep Fencing LLC ("ESF"). All Rights Reserved.

NO COMMERCIAL DISTRIBUTION OF THE PFSense® CE SOFTWARE IS ALLOWED.

pfSense® is a federally and internationally registered trademark and service mark of ESF, and is exclusively licensed to Rubicon Communications, LLC (d/b/a Netgate) ("Netgate").

Any unauthorized use of the pfSense® mark is prohibited by United States and international law. Please refer to the [Trademark Usage Guidelines](#) for how to properly use the mark.

 Accept

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

Status / Dashboard + ?

System Information 🔧 - ✕	
Name	pfSense.localdomain
User	admin@192.168.1.102 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 6ba11cb48e333cb58eb2
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Fri Apr 13 2018
Version	2.4.4-RELEASE (amd64) built on Thu Sep 20 09:03:12 EDT 2018 FreeBSD 11.2-RELEASE-p3 Version 2.4.4_3 is available. 📄 Version information updated at Thu Sep 26 13:07:51 UTC 2019 🔄
CPU Type	Intel(R) Xeon(R) CPU E3-1225 V2 @ 3.20GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled

Netgate Services And Support - ✕	
Contract type	Community Support Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES	
<p>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.</p> <p>You also may upgrade to a Netgate Global 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.</p>	
<ul style="list-style-type: none"> Upgrade Your Support Netgate Global Support 	<ul style="list-style-type: none"> Community Support Resources Official pfSense Training by

Schéma d'infrastructures

Pour une machine physique il suffit de prendre un câble RJ45 et de le brancher sur la 2^{ème} carte réseau et le brasser sur une autre machine ou un switch la configuration se fera automatiquement, assurer de garder votre PFSense toujours allumé que ça soit en physique ou en virtuel

