

Mise en place d'un Pare-feu logiciel sur VM

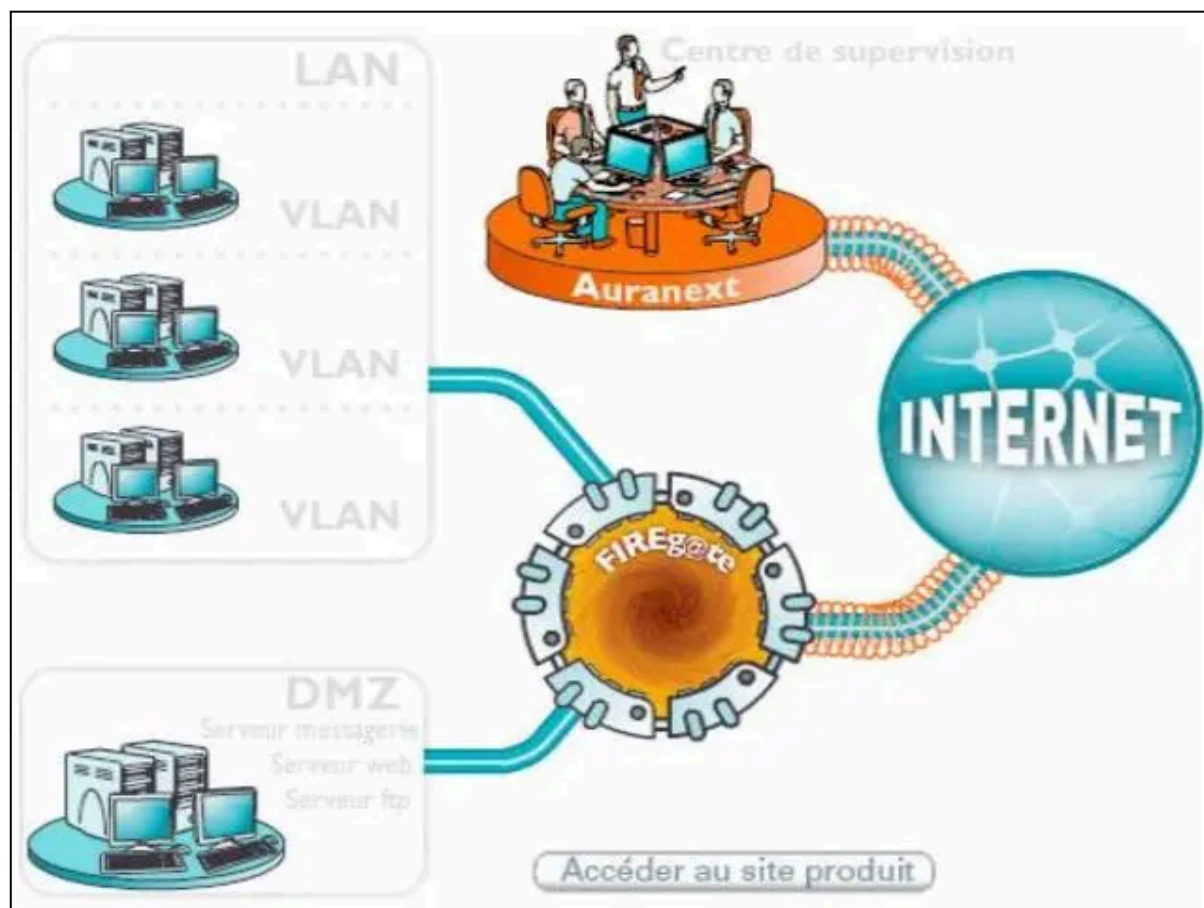


TABLEAU D'HISTORIQUES DES MODIFICATIONS

DATE	AUTEUR	NATURE DE LA MODIFICATION

Contexte :

La Société d'eau Raillée, spécialisée dans le développement de logiciels, utilise une infrastructure virtuelle pour ses applications et services internes. Récemment, l'entreprise a rencontré des problèmes de sécurité et de confidentialité des données, poussant le département informatique à renforcer la sécurité de son réseau. La décision a été prise d'installer un pare-feu logiciel sur une machine virtuelle (VM) dédiée pour protéger l'infrastructure.

Le technicien doit d'abord sélectionner une machine virtuelle (VM) avec des ressources suffisantes pour assurer des performances optimales du pare-feu logiciel. Ensuite, il procède à l'installation d'un système d'exploitation minimaliste et sécurisé sur la VM afin de réduire les vulnérabilités potentielles. Une fois le système d'exploitation en place, il installe et configure le pare-feu logiciel, en définissant des règles pour filtrer le trafic réseau selon les besoins de l'entreprise. Cela inclut le blocage des connexions non autorisées, la limitation de l'accès à certains services et l'ouverture de ports spécifiques.

Après l'installation de base, le technicien configure des fonctionnalités avancées telles que la surveillance du trafic, la détection des intrusions et la prévention des fuites de données, en fonction des exigences spécifiques de l'entreprise. Pour s'assurer du bon fonctionnement du pare-feu, il effectue des tests dans diverses situations, vérifiant notamment le blocage des connexions non autorisées, la redirection du trafic et la gestion des performances.

Enfin, le technicien documente toutes les étapes de la mise en place du pare-feu, y compris les configurations, les règles de pare-feu et les tests effectués. Cette documentation est essentielle pour la maintenance future et la formation des membres de l'équipe.

Définition des termes

NAT (Network Address Translation) :

Description : NAT est une technique utilisée pour modifier les adresses IP dans les en-têtes des paquets IP en cours de transfert à travers un routeur ou un pare-feu.

Fonction : Permet plusieurs appareils sur un réseau local (LAN) de partager une seule adresse IP publique pour accéder à Internet. Cela améliore la sécurité en masquant les adresses IP internes et permet une économie d'adresses IP publiques.

WAN (Wide Area Network) :

Description : Un WAN est un réseau de télécommunications qui couvre une large zone géographique, souvent un pays ou un continent entier.

Fonction : Connecte plusieurs réseaux locaux (LAN) et autres types de réseaux pour permettre la communication entre eux. Internet est le plus grand exemple de WAN.

LAN (Local Area Network) :

Description : Un LAN est un réseau de télécommunications qui couvre une petite zone géographique, comme une maison, un bureau ou un bâtiment.

Fonction : Permet la connexion et la communication entre les appareils situés à proximité physique, facilitant le partage de ressources comme les fichiers, les imprimantes et les applications.

Firewall (Pare-feu) :

Description : Un pare-feu est un dispositif de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant en fonction de règles de sécurité prédéfinies.

Fonction : Protège les réseaux internes (LAN) contre les accès non autorisés provenant de réseaux externes (comme Internet). Il peut filtrer les paquets, bloquer des connexions non autorisées, et prévenir les attaques de sécurité. Les pare-feux peuvent être matériels ou logiciels, ou une combinaison des deux.

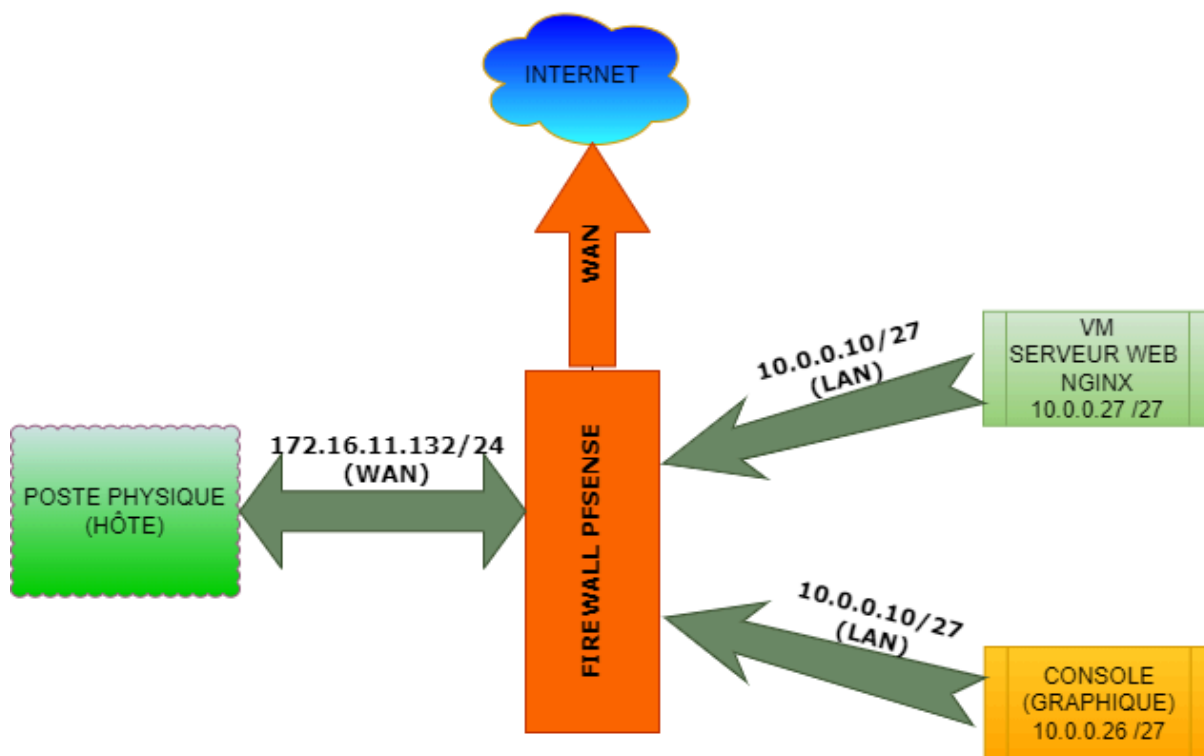
SOMMAIRE

1. SCHÉMA DE L'INFRASTRUCTURE

2. INSTALLATION DU FIREWALL PFSENSE

3. TESTS DE VALIDATIONS

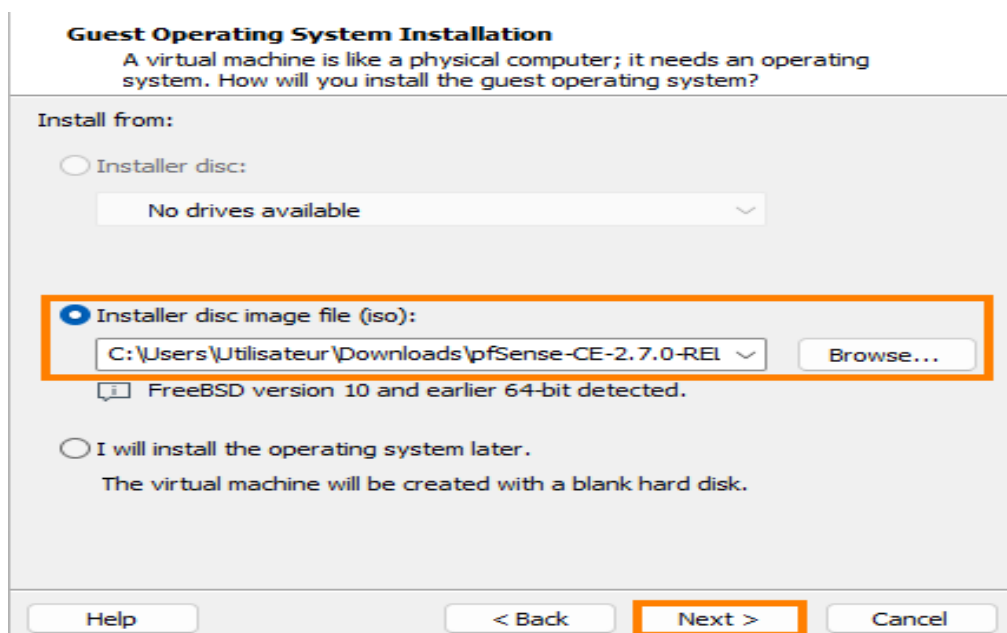
1. SCHÉMA DE L'INFRASTRUCTURE



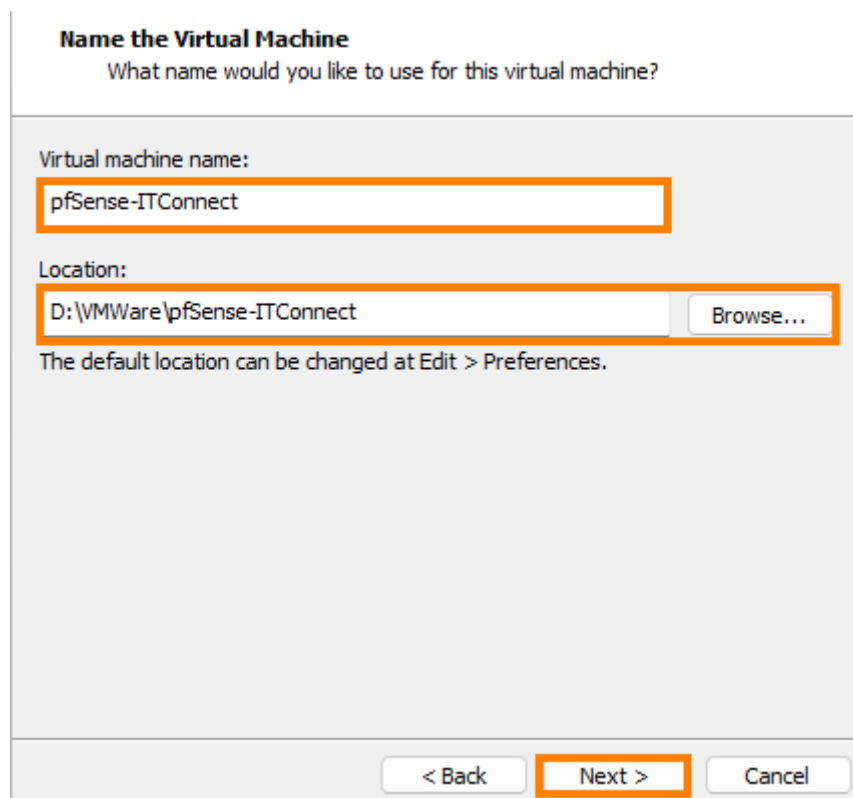
2. INSTALLATION DU FIREWALL PFSENSE

Pour installer pfSense il vous faudra d'abord l'ISO de celui-ci télécharger au préalable.

Tout d'abord, créer notre machine virtuelle, ensuite choisir l'ISO pfSENSE:



Ensuite, nous allons nommer notre machine virtuelle et définir l'emplacement où stocker les données de la VM



Name the Virtual Machine
What name would you like to use for this virtual machine?

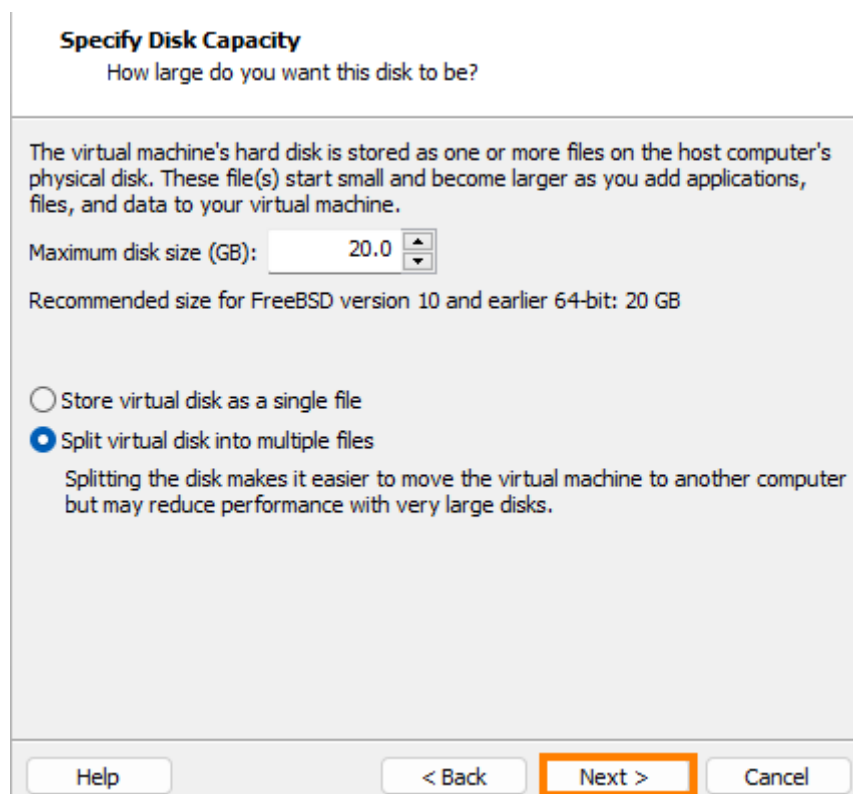
Virtual machine name:
pfSense-ITConnect

Location:
D:\VMWare\pfSense-ITConnect Browse...

The default location can be changed at Edit > Preferences.

< Back **Next >** Cancel

Ensuite nous choisissons le stockage la VM:



Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 20.0

Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB

☐ Store virtual disk as a single file
☒ Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help < Back **Next >** Cancel

Ready to Create Virtual Machine
Click Finish to create the virtual machine and start installing FreeBSD version 10 and earlier 64-bit.

The virtual machine will be created with the following settings:

Name:	
Location:	
Version:	Workstation 17.x
Operating System:	FreeBSD version 10 and earlier 64-bit
Hard Disk:	20 GB, Split
Memory:	256 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

Customize Hardware...

☐ Power on this virtual machine after creation

< Back Finish Cancel

Nous créons la VM pfSense via les besoins de notre client bien évidemment.
Ici on nous demande de mettre 2 cartes réseaux sur notre pfSense:
1 en NAT pour simuler un réseau WAN et 1 en host-only pour simuler notre LAN(sans DHCP):

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Host-only	-	Connected	Enabled	172.16.1.0
VMnet1	Host-only	-	Connected	-	192.168.163.0
VMnet8	NAT	NAT	Connected	Enabled	172.16.11.0

Add Network... Remove Network Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)
Bridged to: Automatic Settings...

☐ NAT (shared host's IP address with VMs)
NAT Settings...

☒ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet1

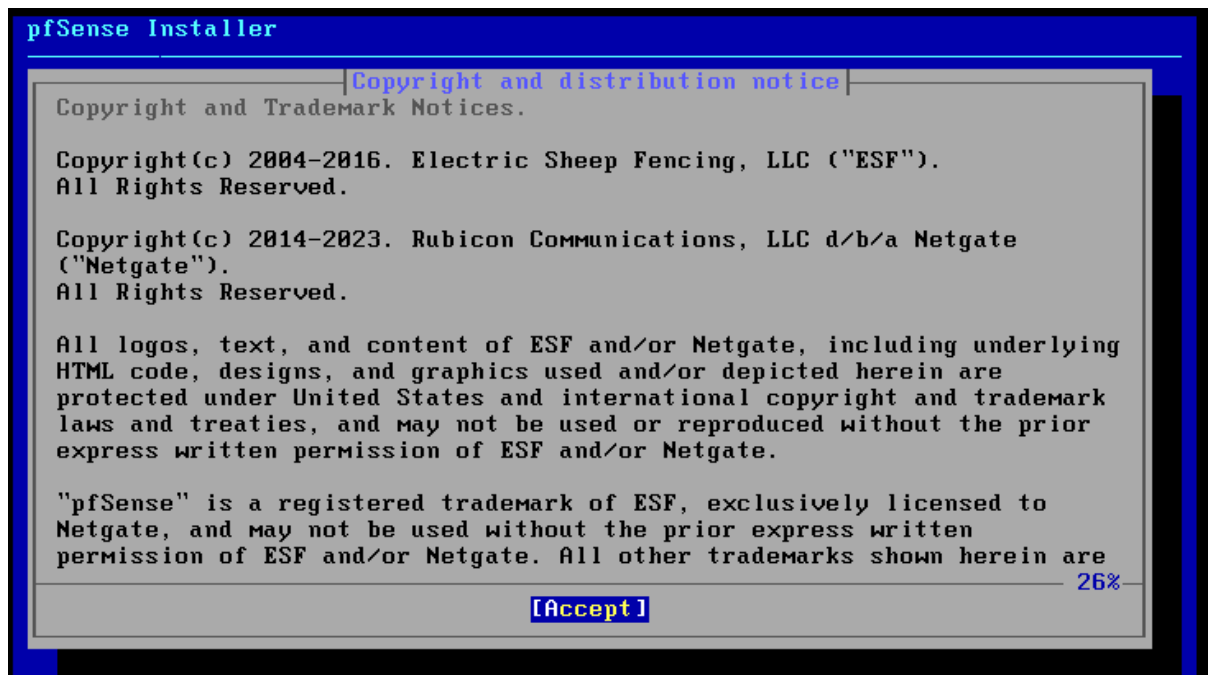
☐ Use local DHCP service to distribute IP address to VMs
DHCP Settings...

Subnet IP: 192.168.163.0 Subnet mask: 255.255.255.224

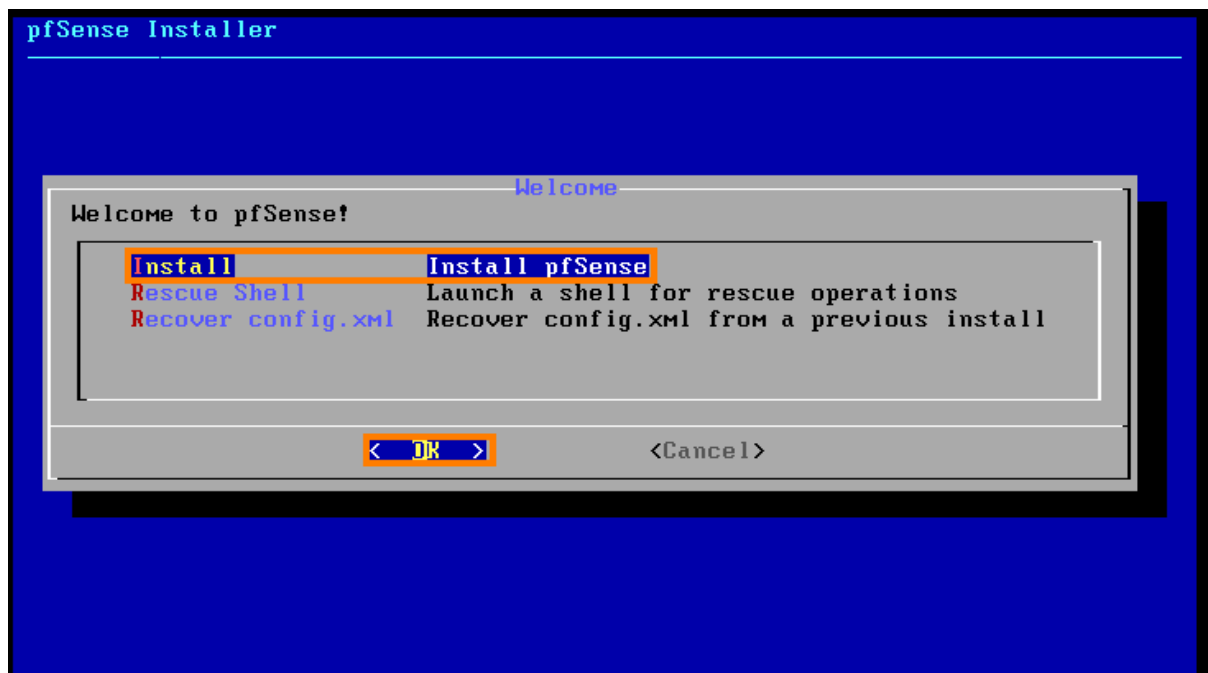
Restore Defaults Import... Export... OK Cancel Apply Help

A la création de la VM, la première carte réseau a été configuré en NAT.
Ici on ajoute une carte réseau en host-only, on remarque qu'on a bien décocher l'option "Use local DHCP service" comme demandé.

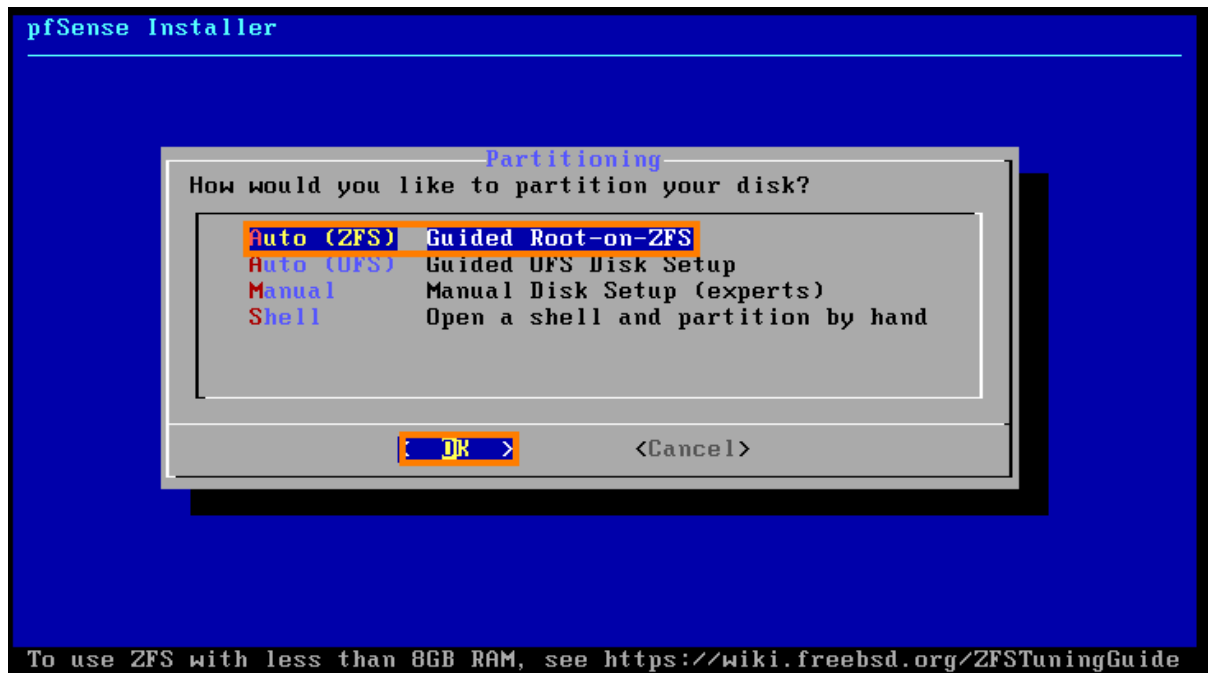
Ensuite nous lançons la VM, il y aura un chargement. Une fois celui-ci terminé, veuillez accepter le contrat d'utilisation de pfSense (Tapez sur Entrée)



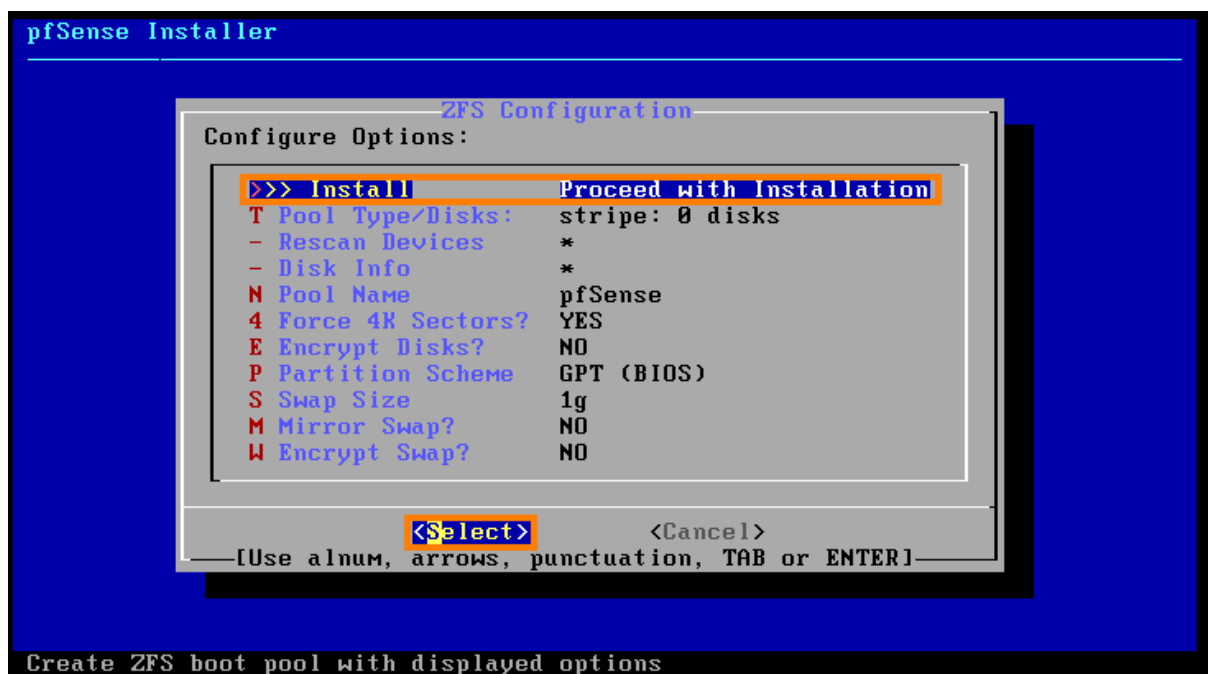
Pour poursuivre l'installation, sélectionnez "Install pfSense" et appuyez sur Entrée



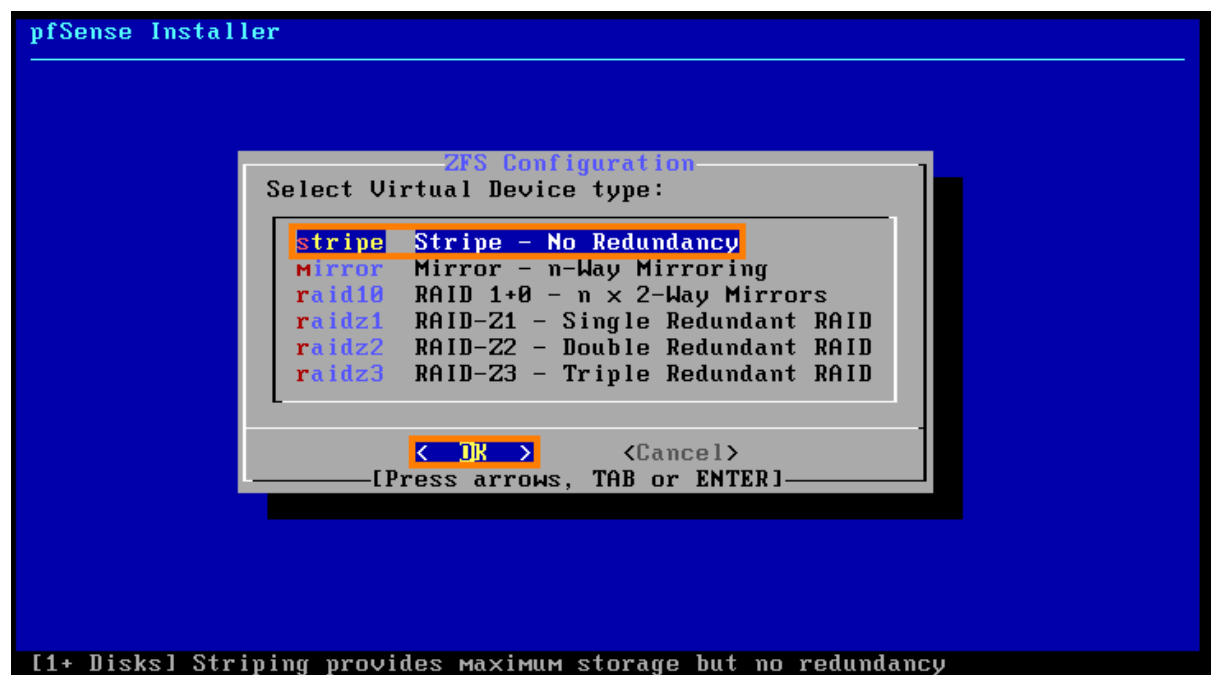
A l'étape de partitionnement du disque, nous allons utiliser le mode "Auto (ZFS)" présélectionné:



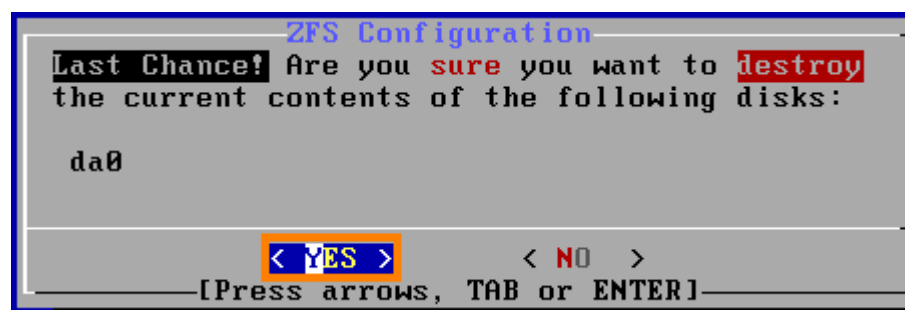
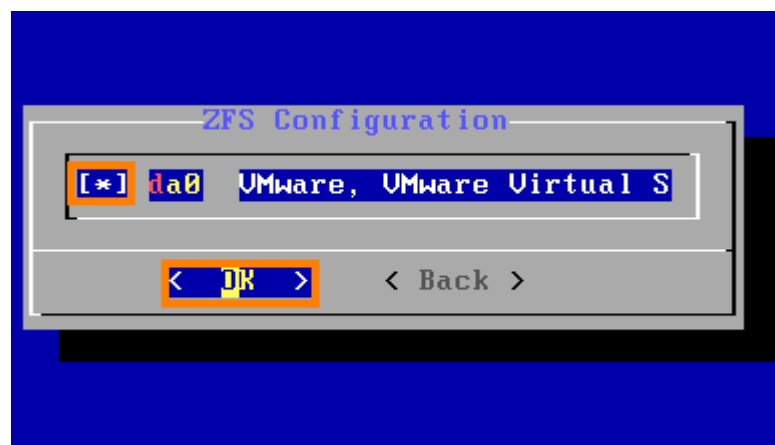
A cette étape, un récapitulatif du partitionnement automatique ZFS est présenté, appuyez sur Entrée pour valider.



Dans notre cas, nous allons faire une installation sans redondance (mode stripe).



Pour sélectionner le disque dur virtuel, appuyez sur Espace puis sur Entrée et sélectionner "Yes"



L'installation est relativement rapide. Une fois achevé, validez le redémarrage de la VM.

Au premier démarrage, pfSense détecte automatiquement les interfaces réseau. La plupart du temps, vous verrez l'interface WAN rattachée à l'interface em0 correspondant à la première interface ajoutée. L'interface LAN quant à elle sera rattachée à l'interface em1, correspondant à la deuxième interface ajoutée à la VM.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: 27d60df29732ef3a0a80

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.16.11.132/24
LAN (lan)      -> em1      -> v4: 10.0.0.10/27

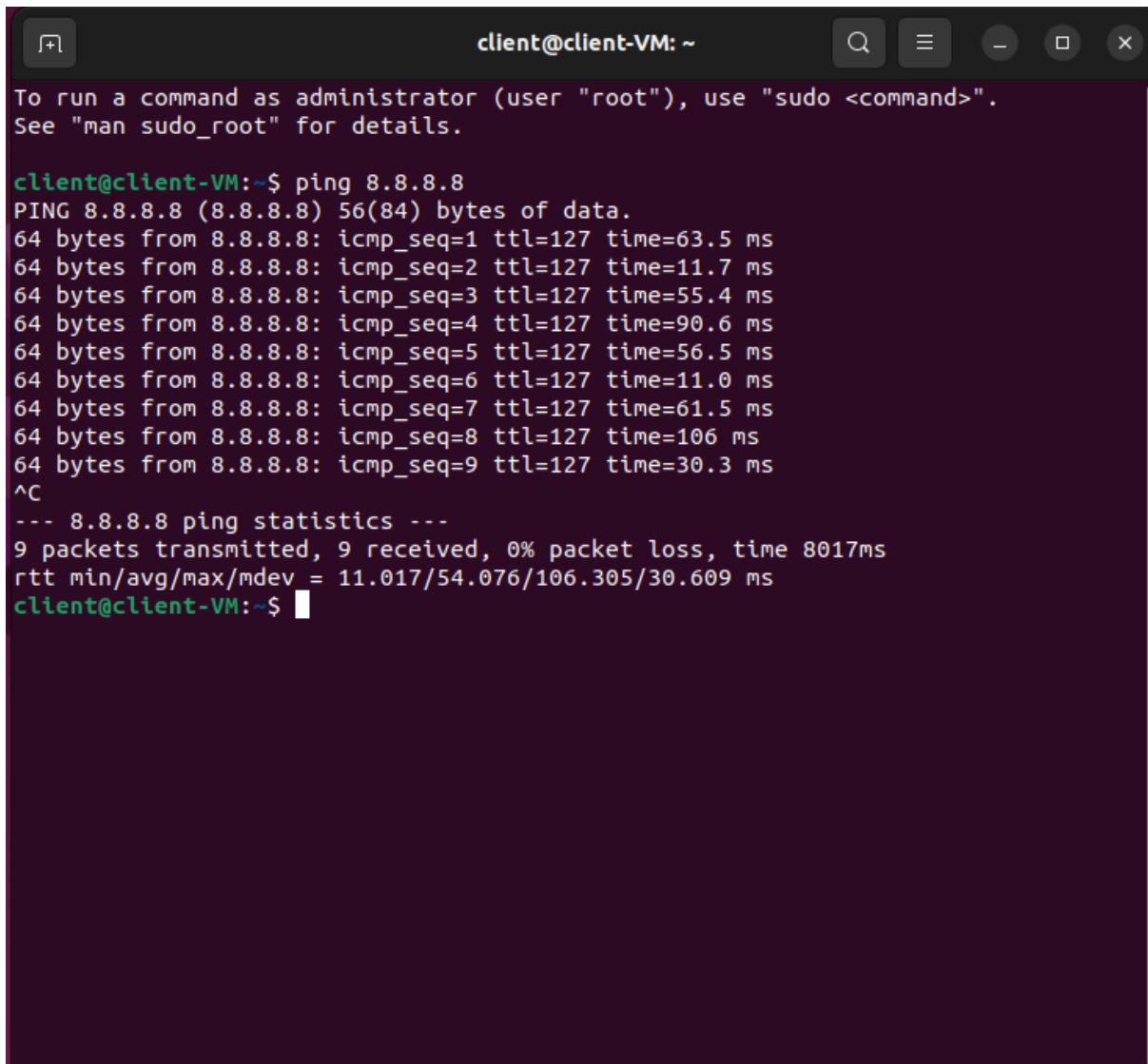
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Comme on peut le voir, la configuration IP de l'interface WAN a été attribuée par le serveur DHCP de mon réseau. Nous allons configurer l'interface LAN avec sa configuration IP adéquate.

3. TESTS DE VALIDATIONS

J'effectue des tests pour vérifier le bon fonctionnement de mon Firewall pfSense. En premier lieu je vérifie que ma Vm Console (client) et ma Vm Serveur ont tous les deux accès à internet via le pfSense;

A terminal window titled 'client@client-VM: ~' with standard window controls. It displays the output of a 'ping 8.8.8.8' command. The output shows 9 successful pings with varying response times. A summary line indicates '9 packets transmitted, 9 received, 0% packet loss, time 8017ms'.

```
client@client-VM: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

client@client-VM:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=63.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=11.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=55.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=90.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=56.5 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=11.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=61.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=106 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=127 time=30.3 ms
^C
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8017ms
rtt min/avg/max/mdev = 11.017/54.076/106.305/30.609 ms
client@client-VM:~$
```

Ici ma Vm console à bien accès à Internet.

Ici la Vm serveur sans interface graphique;

```
serveur@serveur:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=8.84 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=80.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=80.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=33.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=13.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=7.44 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=48.8 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=106 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=127 time=70.0 ms
^C
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8106ms
rtt min/avg/max/mdev = 7.442/49.842/106.447/34.325 ms
serveur@serveur:~$ _
```

Ensuite je veux savoir si mes 2 Vms Linux ping l'adresse LAN du pfSense;

```
client@client-VM:~$ ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=64 time=0.403 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=64 time=0.362 ms
64 bytes from 10.0.0.10: icmp_seq=3 ttl=64 time=0.315 ms
64 bytes from 10.0.0.10: icmp_seq=4 ttl=64 time=0.449 ms
64 bytes from 10.0.0.10: icmp_seq=5 ttl=64 time=0.336 ms
64 bytes from 10.0.0.10: icmp_seq=6 ttl=64 time=0.305 ms
64 bytes from 10.0.0.10: icmp_seq=7 ttl=64 time=0.367 ms
64 bytes from 10.0.0.10: icmp_seq=8 ttl=64 time=0.392 ms
64 bytes from 10.0.0.10: icmp_seq=9 ttl=64 time=0.326 ms
^C
--- 10.0.0.10 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8177ms
rtt min/avg/max/mdev = 0.305/0.361/0.449/0.044 ms
client@client-VM:~$
```

```
serveur@serveur:~$ ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=64 time=0.388 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=64 time=0.426 ms
64 bytes from 10.0.0.10: icmp_seq=3 ttl=64 time=0.322 ms
64 bytes from 10.0.0.10: icmp_seq=4 ttl=64 time=0.340 ms
64 bytes from 10.0.0.10: icmp_seq=5 ttl=64 time=0.310 ms
64 bytes from 10.0.0.10: icmp_seq=6 ttl=64 time=0.452 ms
64 bytes from 10.0.0.10: icmp_seq=7 ttl=64 time=0.366 ms
64 bytes from 10.0.0.10: icmp_seq=8 ttl=64 time=0.325 ms
64 bytes from 10.0.0.10: icmp_seq=9 ttl=64 time=0.308 ms
^C
--- 10.0.0.10 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8173ms
rtt min/avg/max/mdev = 0.308/0.359/0.452/0.049 ms
serveur@serveur:~$ _
```

Je vérifie que pfSense ping mes Vms Linux;

```
Enter a host name or IP address: 10.0.0.26

PING 10.0.0.26 (10.0.0.26): 56 data bytes
64 bytes from 10.0.0.26: icmp_seq=0 ttl=64 time=0.634 ms
64 bytes from 10.0.0.26: icmp_seq=1 ttl=64 time=0.314 ms
64 bytes from 10.0.0.26: icmp_seq=2 ttl=64 time=0.433 ms

--- 10.0.0.26 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.314/0.460/0.634/0.132 ms

Press ENTER to continue.
```

```
Enter a host name or IP address: 10.0.0.27

PING 10.0.0.27 (10.0.0.27): 56 data bytes
64 bytes from 10.0.0.27: icmp_seq=0 ttl=64 time=0.391 ms
64 bytes from 10.0.0.27: icmp_seq=1 ttl=64 time=0.415 ms
64 bytes from 10.0.0.27: icmp_seq=2 ttl=64 time=0.281 ms

--- 10.0.0.27 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.281/0.362/0.415/0.058 ms

Press ENTER to continue.
```

Et pour finir, je dois vérifier que la machine cliente a accès à l'interface Web de pfSense;

The screenshot shows the pfSense web interface in a browser window. The address bar displays 'https://192.168.0.1'. The interface has a dark header with the pfSense logo and navigation links: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the header, the 'Status / Dashboard' page is visible. It features two main panels: 'System Information' on the left and 'Netgate Services And Support' on the right. The 'System Information' panel lists details such as Name (pfSense.home.arpa), User (admin@192.168.0.2), System (VMware Virtual Machine), BIOS (Phoenix Technologies LTD), Version (2.7.2-RELEASE), CPU Type (Intel(R) Core(TM) i5-6440HQ), and Uptime (00 Hour 41 Minutes 57 Seconds). The 'Netgate Services And Support' panel shows the contract type as 'Community Support' and provides links to various support resources, including the Netgate Resource Library, Upgrade Your Support, and Netgate Global Support FAQ. A red box at the bottom of the support panel contains a warning about the Netgate Device ID (NDI) required for TAC support.

System Information	
Name	pfSense.home.arpa
User	admin@192.168.0.2 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 37ee99554525dfcc7ad1
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 Fri May 31 11:26:50 CEST 2024
CPU Type	Intel(R) Core(TM) i5-6440HQ CPU @ 2.60GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 41 Minutes 57 Seconds
Current date/time	Fri May 31 12:07:18 CEST 2024

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
- Netgate Global Support FAQ
- Netgate Professional Services
- Community Support Resources
- Official pfSense Training by Netgate
- 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 supports [here](#).